



บันทึกข้อความ

การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

ส่วนงาน..... ฝ่ายจัดซื้อและบริการ กองจัดหาพัสดุทั่วไป แผนกจัดหาพัสดุทั่วไป 1 โทร.1667

ที่..... ฉบับ10/290 วันที่..... 20 กรกฎาคม 2566

เรื่อง..... ขอความเห็นชอบรายงานขอจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (Project Progress Monitoring System: PPMS) ประจำปีงบประมาณ 2567 โดยวิธีเฉพาะเจาะจง

เรียน ผอ.ฉจบ.

1. เรื่องเดิม

1.1 ผทท. ได้มีบันทึกที่ ผทท21/97 ลงวันที่ 22 มิถุนายน 2566 จัดส่งร่างขอบเขตของงานและราคากลาง เพื่อจัดหาผู้รับจ้างเพื่อดำเนินการบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (Project Progress Monitoring System: PPMS) ประจำปีงบประมาณ 2567 โดยผู้รับจ้างรายเดิม คือ บริษัท เอทพี โซลูชั่น จำกัด ซึ่งมีคุณสมบัติโดยตรงเพียงรายเดียวและมีความเชี่ยวชาญเป็นพิเศษ รวมทั้งเป็นผู้ออกแบบและพัฒนาระบบดังกล่าวตามมาตรา 56 (2) (ค) แห่งพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 (เอกสารแนบ 1)

1.2 ผอ.ฉจบ. ได้เห็นชอบประกาศเผยแพร่แผนการจัดซื้อจัดจ้าง ประจำปีงบประมาณ พ.ศ. 2567 งานจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (Project Progress Monitoring System: PPMS) ประจำปีงบประมาณ 2567 ในวงเงินงบประมาณ 1,350,000 บาท (หนึ่งล้านสามแสนห้าหมื่นบาทถ้วน) รายละเอียดปรากฏตามบันทึกที่ ฉบับ11/138 ลงวันที่ 11 กรกฎาคม 2566 (เอกสารแนบ 2)

2. ขอกฎหมาย

2.1 พระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ.2560

มาตรา 55 การจัดซื้อจัดจ้างอาจกระทำได้โดยวิธี ดังต่อไปนี้

(3) วิธีเฉพาะเจาะจง ได้แก่ การที่หน่วยงานของรัฐเชิญชวนผู้ประกอบการที่มีคุณสมบัติตรงตามเงื่อนไขที่หน่วยงานของรัฐกำหนดรายใดรายหนึ่งให้เข้ายื่นข้อเสนอ หรือให้เข้ามาเจรจาต่อรองราคา รวมทั้งการจัดซื้อจัดจ้างพัสดุกับผู้ประกอบการโดยตรงในวงเงินเล็กน้อยตามที่กำหนดในกฎกระทรวงที่ออกตามความในมาตรา 96 วรรคสอง

มาตรา 56 การจัดซื้อจัดจ้างพัสดุ ให้หน่วยงานของรัฐเลือกใช้วิธีประกาศเชิญชวนทั่วไปก่อน

เว้นแต่

(2) กรณีดังต่อไปนี้ ให้ใช้วิธีเฉพาะเจาะจง

(ค) การจัดซื้อจัดจ้างพัสดุที่มีผู้ประกอบการซึ่งมีคุณสมบัติโดยตรงเพียงรายเดียวหรือการจัดซื้อจัดจ้างพัสดุกจากผู้ประกอบการซึ่งเป็นตัวแทนจำหน่ายหรือตัวแทนผู้ให้บริการโดยชอบด้วยกฎหมายเพียงรายเดียวในประเทศไทยและไม่มีพัสดุอื่นที่จะใช้ทดแทนได้

/2.2 ระเบียบกระทรวง...

2.2 ระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560

ข้อ 22 ในการซื้อหรือจ้างแต่ละวิธี นอกจากการซื้อที่ดินหรือสิ่งปลูกสร้างตามข้อ 23 และข้อ 79 วรรคสอง ให้เจ้าหน้าที่จัดทำรายงานขอซื้อหรือขอจ้างเสนอหัวหน้าหน่วยงานของรัฐเพื่อขอความเห็นชอบ โดยเสนอผ่านหัวหน้าเจ้าหน้าที่ ตามรายการดังต่อไปนี้

(1) เหตุผลและความจำเป็นที่ต้องซื้อหรือจ้าง

(2) ขอบเขตของงานหรือรายละเอียดคุณลักษณะเฉพาะของพัสดุหรือแบบรูปารายการงานก่อสร้างที่จะซื้อหรือจ้าง แล้วแต่กรณี

(3) ราคากลางของพัสดุที่จะซื้อหรือจ้าง

(4) วงเงินที่จะซื้อหรือจ้างและเหตุผลที่ต้องซื้อหรือจ้างโดยวิธีนั้น

(5) กำหนดเวลาที่ต้องการใช้พัสดุนั้นหรือให้งานนั้นแล้วเสร็จ

(6) วิธีที่จะซื้อหรือจ้างและเหตุผลที่ต้องซื้อหรือจ้างโดยวิธีนั้น

(7) หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

(8) ข้อเสนออื่นๆ เช่น การขออนุมัติแต่งตั้งคณะกรรมการต่างๆ ที่จำเป็นในการซื้อหรือจ้าง

การออกประกาศและเอกสารเชิญชวน และหนังสือเชิญชวน

ข้อ 25 ในการดำเนินการซื้อหรือจ้างแต่ละครั้ง ให้หัวหน้าหน่วยงานของรัฐแต่งตั้งคณะกรรมการซื้อหรือจ้างขึ้น เพื่อปฏิบัติการตามระเบียบนี้ พร้อมกับกำหนดระยะเวลาในการพิจารณาของคณะกรรมการ แล้วแต่กรณี คือ

(4) คณะกรรมการซื้อหรือจ้างโดยวิธีเฉพาะเจาะจง

(5) คณะกรรมการตรวจรับพัสดุ

ให้คณะกรรมการซื้อหรือจ้างแต่ละคณะ รายงานผลการพิจารณาต่อหัวหน้าหน่วยงานของรัฐภายในระยะเวลาที่กำหนด ถ้ามีเหตุที่ทำให้การรายงานล่าช้า ให้เสนอหัวหน้าหน่วยงานของรัฐพิจารณาขยายเวลาให้ตามความจำเป็น

ข้อ 26 คณะกรรมการซื้อหรือจ้างตามข้อ 25 แต่ละคณะประกอบด้วย ประธานกรรมการ 1 คน และกรรมการอย่างน้อย 2 คน ซึ่งแต่งตั้งจากราชการ ลูกจ้างประจำ พนักงานราชการ พนักงานรัฐวิสาหกิจ พนักงานของรัฐ หรือพนักงานของหน่วยงานของรัฐที่เรียกชื่ออย่างอื่น โดยให้คำนึงถึงลักษณะหน้าที่และความรับผิดชอบของผู้ที่ได้รับแต่งตั้งเป็นสำคัญ

ข้อ 78 เมื่อหัวหน้าหน่วยงานของรัฐให้ความเห็นชอบรายงานขอซื้อหรือจ้างตามข้อ 22 แล้ว ให้คณะกรรมการซื้อหรือจ้างโดยวิธีเฉพาะเจาะจง ดำเนินการดังต่อไปนี้

(1) จัดทำหนังสือเชิญชวนผู้ประกอบการที่มีคุณสมบัติตรงตามเงื่อนไขที่หน่วยงานของรัฐกำหนด รายใดรายหนึ่งให้เข้ายื่นข้อเสนอหรือให้เข้ามาเจรจาต่อรองราคา โดยให้ดำเนินการดังต่อไปนี้

(ข) กรณีตามมาตรา 56 วรรคหนึ่ง (2) (ค) (ง) ให้เชิญผู้ประกอบการที่มีอาชีพขายหรือรับจ้างนั้นโดยตรงมายื่นข้อเสนอราคา หากเห็นว่าราคาที่เสนอนั้นยังสูงกว่าราคาในท้องถิ่น หรือราคาที่ประมาณได้ หรือราคาที่คณะกรรมการเห็นสมควร ให้ต่อรองราคาลงเท่าที่จะทำได้

ข้อ 86 การส่งซื้อหรือส่งจ้างโดยวิธีเฉพาะเจาะจงครั้งหนึ่ง ให้เป็นอำนาจของผู้ดำรงตำแหน่งและภายในวงเงิน

(1) หัวหน้าหน่วยงานของรัฐ ไม่เกิน 50,000,000 บาท

2.3 คำสั่งการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย ที่ 98/2564 ลงวันที่ 5 เมษายน 2564 เรื่อง มอบอำนาจเกี่ยวกับการจัดซื้อหรือจัดจ้างพัสดุ

2. มอบอำนาจดำเนินการและอำนาจสั่งซื้อหรือสั่งจ้าง ดังนี้

2.3 การสั่งซื้อหรือสั่งจ้างโดยวิธีเฉพาะเจาะจงครั้งหนึ่ง ให้เป็นอำนาจของผู้ดำรงตำแหน่งและภายในวงเงิน ดังต่อไปนี้

- (1) ผู้อำนวยการกองจัดหาพัสดุทั่วไป ไม่เกิน 500,000 บาท (ห้าแสนบาทถ้วน)
- (2) ผู้อำนวยการฝ่ายจัดซื้อและบริการ ไม่เกิน 5,000,000 บาท (ห้าล้านบาทถ้วน)
- (3) รองผู้ว่าการ (บริหาร) ไม่เกิน 10,000,000 บาท (สิบล้านบาทถ้วน)

3. การมอบอำนาจตามคำสั่งนี้ให้ครอบคลุมถึงการดำเนินการทุกกระบวนการตามพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 ระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 กฎกระทรวง และประกาศที่ออกตามความในพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 และมติคณะรัฐมนตรีที่เกี่ยวข้อง ภายในอำนาจและวงเงินตามข้อ 2 ทั้งนี้ สำหรับการบอกเลิกหรือการตกลงเลิกสัญญาหรือข้อตกลง การแก้ไขสัญญาหรือข้อตกลง การงดหรือลดค่าปรับให้แก่คู่สัญญา หรือการขยายเวลาทำการตามสัญญาหรือข้อตกลง ให้เสนอผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย พิจารณาให้ความเห็นชอบก่อน และเมื่อผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทยได้พิจารณาให้ความเห็นชอบแล้ว ให้ผู้รับมอบอำนาจตามข้อ 2.1 ข้อ 2.2 และข้อ 2.3 มีหนังสือแจ้งการบอกเลิก หรือการตกลงเลิกสัญญาหรือข้อตกลง การงดหรือลดค่าปรับให้แก่คู่สัญญา การขยายเวลาทำการตามสัญญาหรือข้อตกลงหรือลงนามในสัญญาหรือข้อตกลง แล้วแต่กรณีต่อไป เว้นแต่ ผู้รับมอบอำนาจตามข้อ 2.3 (1) ให้สามารถดำเนินการได้โดยไม่ต้องเสนอผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทยพิจารณาให้ความเห็นชอบก่อน

3. ข้อพิจารณา

กพท. พิจารณาแล้ว ขอรายงานการจ้างตามระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 ข้อ 22 ดังนี้

3.1 เหตุผลและความจำเป็นที่ต้องจ้าง

รฟม. ได้มีระบบติดตามความก้าวหน้าโครงการ (Project Progress Monitoring System: PPMS) เพื่อใช้สำหรับรองรับการติดตามความก้าวหน้าการก่อสร้างโครงการรถไฟฟ้าของ รฟม. โดยระบบดังกล่าวจะสิ้นสุดระยะเวลาการรับประกัน ในวันที่ 30 กันยายน 2566 ทั้งนี้ เพื่อให้ระบบติดตามความก้าวหน้าโครงการ (PPMS) สามารถใช้งานได้อย่างต่อเนื่องและมีประสิทธิภาพ รฟม. จึงจำเป็นต้องจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ต่อไป

3.2 ขอบเขตของงานหรือรายละเอียดคุณลักษณะเฉพาะของพัสดุ

ตามขอบเขตของงานจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (Project Progress Monitoring System: PPMS) ประจำปีงบประมาณ 2567 (เอกสารแนบ 3)

3.3 ราคากลางของพัสดุที่จะจ้าง

ราคากลางเป็นจำนวนเงินทั้งสิ้น 650,000 บาท (หกแสนห้าหมื่นบาทถ้วน) รวมภาษีมูลค่าเพิ่มแล้ว ซึ่งเป็นราคาที่ได้มาจากราคาที่สืบจากท้องตลาด รายละเอียดปรากฏตามตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง) การจัดซื้อจัดจ้างที่มีในงานก่อสร้าง (เอกสารแนบ 4)

3.4 วงเงินที่จะจ้าง

เงินนอกงบประมาณจากรายได้ของหน่วยงาน 1,350,000 บาท (หนึ่งล้านสามแสนห้าหมื่นบาทถ้วน) ซึ่งเป็นวงเงินที่รวมภาษีมูลค่าเพิ่มตลอดจนภาษีอากรอื่น ๆ และค่าใช้จ่ายที่คงค้างแล้ว

3.5 กำหนดเวลาที่ต้องการใช้พัสดุนั้นหรือให้งานนั้นแล้วเสร็จ

ตั้งแต่วันที่ 1 ตุลาคม 2566 ถึงวันที่ 30 กันยายน 2567

3.6 วิธีที่จะจ้างและเหตุผลที่ต้องจ้างโดยวิธีนั้น

โดยวิธีเฉพาะเจาะจง เนื่องจาก รฟม. ได้จัดซื้อซอฟต์แวร์ระบบติดตามความก้าวหน้าโครงการ (Project Progress Monitoring System: PPMS) กับบริษัท เอทูพี โซลูชั่น จำกัด ซึ่งเป็นผู้ออกแบบและพัฒนาระบบดังกล่าว และเพื่อให้ระบบดังกล่าวสามารถใช้งานได้ต่อเนื่อง รฟม. ได้จ้างบริษัทฯ เป็นผู้ดำเนินการบำรุงรักษาระบบฯ ทุกปี ดังนั้น จึงมีความจำเป็นต้องจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (Project Progress Monitoring System: PPMS) ประจำปีงบประมาณ 2567 กับ บริษัท เอทูพี โซลูชั่น จำกัด ซึ่งเป็นผู้มีคุณสมบัติโดยตรงเพียงรายเดียว และมีความเชี่ยวชาญเป็นพิเศษ ตามพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ.2560 มาตรา 56 (2) (ค)

3.7 หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

ในการพิจารณาผลการคัดเลือกข้อเสนอการจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (Project Progress Monitoring System: PPMS) ครั้งนี้ รฟม. จะพิจารณาตัดสินโดยใช้เกณฑ์ราคา

3.8 ข้อเสนออื่น ๆ

การแต่งตั้งคณะกรรมการดำเนินการ

3.8.1 คณะกรรมการจ้างโดยวิธีเฉพาะเจาะจง

- | | |
|--------------------------------------|---------------|
| (1) นางสาวศิวลี เกตุคง | ประธานกรรมการ |
| หัวหน้าแผนกแผนงานและบริหารเอกสาร 2-3 | |
| กองแผนงานและบริหารเอกสาร 2 | |
| ฝ่ายบริหารงานก่อสร้าง 2 | |
| (2) นางสาววิสุดา ชลายนเดชะ | กรรมการ |
| หัวหน้าแผนกแผนงานและบริหารเอกสาร 1-3 | |
| กองแผนงานและบริหารเอกสาร 1 | |
| ฝ่ายบริหารงานก่อสร้าง 1 | |

/(3) นางสาว...

- | | |
|---|---------------------|
| (3) นางสาวปวีณา เปล่งเสียง
พนักงานวิเคราะห์ระบบ ระดับ 7
แผนกพัฒนาระบบงานคอมพิวเตอร์
กองระบบงานคอมพิวเตอร์
ฝ่ายเทคโนโลยีสารสนเทศ | กรรมการ |
| (4) นางสาวไพลิน ปันจัยสิทธิ์
พนักงานบริหารพัสดุ ระดับ 6
แผนกจัดหาพัสดุทั่วไป 1
กองจัดหาพัสดุทั่วไป
ฝ่ายจัดซื้อและบริการ | กรรมการและเลขานุการ |
| 3.8.2 คณะกรรมการตรวจรับพัสดุ | |
| (1) นางสาวสิริพร อุษาสาธิต
หัวหน้าแผนกอาวุโส
แผนกข้อมูลและบริหารงานเอกสาร ฝ่ายวิศวกรรมและสถาปัตยกรรม 1 ระดับ 10
ฝ่ายวิศวกรรมและสถาปัตยกรรม | ประธานกรรมการ |
| (2) นางสาวจตุรพร จารุวัจนกุล
หัวหน้าแผนกประเมินผลโครงการรถไฟฟ้า
กองวางแผนโครงการรถไฟฟ้า
ฝ่ายพัฒนาโครงการรถไฟฟ้า | กรรมการ |
| (3) นางสาวสุพรรณษา นิลสมบุญ
โปรแกรมเมอร์ ระดับ 7
แผนกสนับสนุนระบบงานคอมพิวเตอร์
กองระบบงานคอมพิวเตอร์
ฝ่ายเทคโนโลยีสารสนเทศ | กรรมการและเลขานุการ |
| (4) นางสาวไพลิน ปันจัยสิทธิ์
พนักงานบริหารพัสดุ ระดับ 6
แผนกจัดหาพัสดุทั่วไป 1
กองจัดหาพัสดุทั่วไป
ฝ่ายจัดซื้อและบริการ | ผู้ช่วยเลขานุการ |

โดยให้คณะกรรมการทั้ง 2 ชุด ปฏิบัติหน้าที่ตามที่กำหนดไว้ในระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560

4. ข้อเสนอ

จึงเรียนมาเพื่อโปรดพิจารณา

4.1 เห็นชอบให้ดำเนินการจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (Project Progress Monitoring System: PPMS) ประจำปีงบประมาณ 2567 โดยวิธีเฉพาะเจาะจง

4.2 ลงนามในคำสั่งแต่งตั้งคณะกรรมการจ้างโดยวิธีเฉพาะเจาะจงและคณะกรรมการตรวจรับพัสดุ สำหรับงานจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (Project Progress Monitoring System: PPMS) ประจำปีงบประมาณ 2567 โดยวิธีเฉพาะเจาะจง



(นางจิตาจารย์ ศรีอารุธ)

ผอ.กพท.

20 ก.ค. 66

เห็นชอบตามเสนอ

+

ลงนามแล้ว



(นายวิฑูรย์ พึ่งตน)

ผอ.ฝจบ.

20/7/66



เอกสารแนบ 1

ฝทท.(ภายใน)
เลขที่ 1832
วันที่ 23 มิ.ย. 66
เวลา 08.41 น.กรค.(ภายใน)
เลขที่ 1136
วันที่ 22 มิ.ย. 66
เวลา 15.41 น.

บันทึกข้อความ

การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

ฝจบ

กพท.
เลขรับ 1344
วันที่ 23 มิ.ย.66 เวลา 11.03 น.เลขรับ 2540
วันที่ 23/06/66
เวลา 09.39

ส่วนงาน ฝ่ายเทคโนโลยีสารสนเทศ โทร. 2587

ที่ ฝทท21/ 97 วันที่ 22 มิถุนายน 2566

เรื่อง ขอบจัดสร้างขอบเขตของงานและราคากลางจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ประจำปีงบประมาณ 2567

เรียน ผอ.ฝจบ. ผ่าน ผอ.ฝทท. ผอ.กรค. ทน.สค. 22 มิ.ย. 66

1. ข้อเท็จจริง

1.1 ฝทท. ได้มีบันทึกที่ ฝทท/429 ลงวันที่ 12 กรกฎาคม 2565 จัดส่งรายละเอียดคำขอตั้งงบประมาณรายจ่าย หมวดค่าใช้สอย รายการค่าซ่อมแซมครุภัณฑ์ ประจำปีงบประมาณ 2567 เพื่อให้ ฝจบ. รวบรวมคำขอตั้งงบประมาณฯ ดังกล่าว โดยขอตั้งงบประมาณสำหรับจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ประจำปีงบประมาณ 2567 เป็นจำนวนเงินทั้งสิ้น 1,350,000 บาท (หนึ่งล้านสามแสนห้าหมื่นบาทถ้วน) (รวมภาษีมูลค่าเพิ่ม) ทั้งนี้ คณะกรรมการ รพม. ในคราวประชุมครั้งที่ 12/2565 เมื่อวันที่ 30 พฤศจิกายน 2565 ได้มีมติเห็นชอบกรอบงบประมาณประจำปีงบประมาณ 2567 แล้ว (เอกสารแนบ 1)

1.2 รพม. ได้ดำเนินการจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) จากบริษัท เอทูพี โซลูชั่น จำกัด ตามสัญญาเลขที่ จ(ข)5/2566 ลงวันที่ 3 ตุลาคม 2565 ซึ่งสัญญาดังกล่าวจะสิ้นสุดในวันที่ 30 กันยายน 2566 (เอกสารแนบ 2)

1.3 ฝทท. ได้มีบันทึกที่ ฝทท/228 ลงวันที่ 7 เมษายน 2566 เพื่อขอความเห็นชอบแต่งตั้ง นางสาวสุพรรณษา นิลสมบุรณ์ โปรแกรมเมอร์ ระดับ 7 แผนกสนับสนุนระบบงานคอมพิวเตอร์ กองระบบงานคอมพิวเตอร์ ฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบในการจัดทำขอบเขตของงานและราคากลางจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ประจำปีงบประมาณ 2567 โดย ผอ.ฝจบ. ได้เห็นชอบตามท้ายบันทึกดังกล่าว เรียบร้อยแล้ว (เอกสารแนบ 3)

1.4 ฝทท. ได้มีบันทึกที่ ฝทท/ว283 ลงวันที่ 26 เมษายน 2566 ขอความอนุเคราะห์ ฝบก.1 ฝบก.2 ฝพค. และ ฝวส. มอบหมายพนักงานเข้าร่วมเป็นคณะกรรมการจ้างและคณะกรรมการตรวจรับพัสดุจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ประจำปีงบประมาณ 2567 โดย ฝบก.1 ได้มีบันทึกที่ ฝบก1/249 ลงวันที่ 8 พฤษภาคม 2566 ฝบก.2 ได้มีบันทึกที่ ฝบก2/223 ลงวันที่ 28 เมษายน 2566 ฝพค. ได้มีบันทึกที่ ฝพค/482 ลงวันที่ 2 พฤษภาคม 2566 และ ฝวส. ได้มีบันทึกที่ ฝวส/294 ลงวันที่ 27 เมษายน 2566 แจ้งรายชื่อพนักงานในสังกัดเข้าร่วมเป็นคณะกรรมการฯ เพื่อให้ ฝทท. ดำเนินการในส่วนที่เกี่ยวข้องต่อไป ทั้งนี้ ข้าพเจ้า ได้จัดทำรายชื่อคณะกรรมการฯ จ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ประจำปีงบประมาณ 2567 เรียบร้อยแล้ว (เอกสารแนบ 4)

2. ข้อกฎหมาย

2.1 พระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560

มาตรา 4

“ราคากลาง” หมายความว่า ราคาเพื่อใช้เป็นฐานสำหรับเปรียบเทียบราคาที่ยื่นข้อเสนอได้ยื่นเสนอไว้ซึ่งสามารถจัดซื้อจัดจ้างได้จริงตามลำดับ ดังต่อไปนี้

/ (1) ราคาที่ได้มา...

- (1) ราคาที่ได้มาจากการคำนวณตามหลักเกณฑ์ที่คณะกรรมการราคากลางกำหนด
- (2) ราคาที่ได้มาจากฐานข้อมูลราคาอ้างอิงของพัสดุที่กรมบัญชีกลางจัดทำ
- (3) ราคามาตรฐานที่สำนักงบประมาณหรือหน่วยงานกลางอื่นกำหนด
- (4) ราคาที่ได้มาจากการสืบราคาจากท้องตลาด
- (5) ราคาที่เคยซื้อหรือจ้างครั้งหลังสุดภายในระยะเวลาสองปีงบประมาณ
- (6) ราคาอื่นใดตามหลักเกณฑ์ วิธีการ หรือแนวทางปฏิบัติของหน่วยงานของรัฐนั้น ๆ

ในกรณีที่มีราคาตาม (1) ให้ใช้ราคาตาม (1) ก่อน ในกรณีที่ไม่มีราคาตาม (1) แต่มีราคาตาม (2) หรือ (3) ให้ใช้ราคาตาม (2) หรือ (3) ก่อน โดยจะใช้ราคาใดตาม (2) หรือ (3) ให้คำนึงถึงประโยชน์ของหน่วยงานของรัฐเป็นสำคัญ ในกรณีที่ไม่มีราคาตาม (1) (2) และ (3) ให้ใช้ราคาตาม (4) (5) หรือ (6) โดยจะใช้ราคาใดตาม (4) (5) หรือ (6) ให้คำนึงถึงประโยชน์ของหน่วยงานของรัฐเป็นสำคัญ

มาตรา 56 การจัดซื้อจัดจ้างพัสดุ ให้หน่วยงานของรัฐเลือกใช้วิธีประกาศเชิญชวนทั่วไปก่อน เว้นแต่

- (2) กรณีดังต่อไปนี้ ให้ใช้วิธีเฉพาะเจาะจง

(ค) การจัดซื้อจัดจ้างพัสดุที่มีผู้ประกอบการซึ่งมีคุณสมบัติโดยตรงเพียงรายเดียว หรือการจัดซื้อจัดจ้างพัสดุจากผู้ประกอบการซึ่งเป็นตัวแทนจำหน่ายหรือตัวแทนผู้ให้บริการโดยชอบด้วยกฎหมายเพียงรายเดียวในประเทศไทยและไม่มีพัสดุนั้นที่จะใช้ทดแทนได้

2.2 ระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560

ข้อ 9 การดำเนินการจัดซื้อจัดจ้างและการบริหารพัสดุตามระเบียบนี้ด้วยวิธีการทางอิเล็กทรอนิกส์ ให้หน่วยงานของรัฐดำเนินการในระบบเครือข่ายสารสนเทศของกรมบัญชีกลางผ่านทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement: e - GP) ตามวิธีการที่กรมบัญชีกลางกำหนด

ให้หน่วยงานของรัฐใช้เอกสารที่จัดพิมพ์จากระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ เป็นเอกสารประกอบการดำเนินการจัดซื้อจัดจ้างตามวิธีการที่กำหนดในระเบียบนี้

ข้อ 21 ในการซื้อหรือจ้างที่มีใช้การจ้างก่อสร้าง ให้หัวหน้าหน่วยงานของรัฐแต่งตั้งคณะกรรมการขึ้นมาคณะหนึ่ง หรือจะให้เจ้าหน้าที่หรือบุคคลใดบุคคลหนึ่งรับผิดชอบในการจัดทำร่างขอบเขตของงานหรือรายละเอียดคุณลักษณะเฉพาะของพัสดุที่จะซื้อหรือจ้าง รวมทั้งกำหนดหลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอด้วยองค์ประกอบ ระยะเวลาการพิจารณา และการประชุมของคณะกรรมการตามวรรคหนึ่ง และวรรคสอง ให้เป็นไปตามที่หัวหน้าหน่วยงานของรัฐกำหนดตามความจำเป็นและเหมาะสม

ข้อ 25 ในการดำเนินการซื้อหรือจ้างแต่ละครั้ง ให้หัวหน้าหน่วยงานของรัฐแต่งตั้งคณะกรรมการซื้อหรือจ้างขึ้น เพื่อปฏิบัติการตามระเบียบนี้ พร้อมกับกำหนดระยะเวลาในการพิจารณาของคณะกรรมการ แล้วแต่กรณี คือ

- (4) คณะกรรมการซื้อหรือจ้างโดยวิธีเฉพาะเจาะจง

- (5) คณะกรรมการตรวจรับพัสดุ

ข้อ 26 คณะกรรมการซื้อหรือจ้างตามข้อ 25 แต่ละคณะประกอบด้วย ประธานกรรมการ 1 คน และกรรมการอย่างน้อย 2 คน ซึ่งแต่งตั้งจากราชการ ลูกจ้างประจำ พนักงานราชการ พนักงานมหาวิทยาลัย พนักงานของรัฐ หรือพนักงานของหน่วยงานของรัฐที่เรียกชื่ออย่างอื่น โดยให้คำนึงถึงลักษณะหน้าที่และความรับผิดชอบของผู้ที่ได้รับแต่งตั้งเป็นสำคัญ

ในกรณีจำเป็นหรือเพื่อประโยชน์ของหน่วยงานของรัฐจะแต่งตั้งบุคคลอื่นร่วมเป็นกรรมการด้วยก็ได้ แต่จำนวนกรรมการที่เป็นบุคคลอื่นนั้นจะต้องไม่มากกว่าจำนวนกรรมการตามวรรคหนึ่ง

ในการซื้อหรือจ้างครั้งเดียวกัน ห้ามแต่งตั้งผู้ที่เป็นกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์ กรรมการพิจารณาผลการประกวดราคา หรือกรรมการซื้อหรือจ้างโดยวิธีคัดเลือกเป็นกรรมการตรวจรับพัสดุ

2.3 คำสั่งการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย ที่ 98/2564 ลงวันที่ 5 เมษายน 2564 เรื่อง มอบอำนาจเกี่ยวกับการจัดซื้อหรือจัดจ้างพัสดุ

2. มอบอำนาจดำเนินการและอำนาจสั่งซื้อหรือสั่งจ้าง ดังนี้

2.3 การสั่งซื้อหรือสั่งจ้างโดยวิธีเฉพาะเจาะจงครั้งหนึ่ง ให้เป็นอำนาจของผู้ดำรงตำแหน่งและภายในวงเงิน ดังต่อไปนี้

(1) ผู้อำนวยการกองจัดหาพัสดุทั่วไป ไม่เกิน 500,000 บาท (ห้าแสนบาทถ้วน)

(2) ผู้อำนวยการฝ่ายจัดซื้อและบริการ ไม่เกิน 5,000,000 บาท (ห้าล้านบาทถ้วน)

(3) รองผู้ว่าการ (บริหาร) ไม่เกิน 10,000,000 บาท (สิบล้านบาทถ้วน)

3. การมอบอำนาจตามคำสั่งนี้ให้ครอบคลุมถึงการดำเนินการทุกกระบวนการตามพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 ระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 กฎกระทรวง และประกาศที่ออกตามความในพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 และมติคณะรัฐมนตรีที่เกี่ยวข้อง ภายในอำนาจและวงเงินตามข้อ 2 ทั้งนี้ สำหรับการบอกเลิกหรือการตกลงเลิกสัญญาหรือข้อตกลง การแก้ไขสัญญาหรือข้อตกลง การงดหรือลดค่าปรับให้แก่คู่สัญญาหรือการขยายเวลาทำการตามสัญญาหรือข้อตกลง ให้เสนอผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทยพิจารณาให้ความเห็นชอบก่อน และเมื่อผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทยได้พิจารณาให้ความเห็นชอบแล้ว ให้ผู้รับมอบอำนาจตามข้อ 2.1 ข้อ 2.2 และข้อ 2.3 มีหนังสือแจ้งการบอกเลิก หรือการตกลงเลิกสัญญาหรือข้อตกลง การงดหรือลดค่าปรับให้แก่คู่สัญญา การขยายเวลาทำการตามสัญญาหรือข้อตกลงหรือลงนามในสัญญาหรือข้อตกลงแล้วแต่กรณีต่อไป เว้นแต่ ผู้รับมอบอำนาจตามข้อ 2.3 (1) ให้สามารถดำเนินการได้โดยไม่ต้องเสนอผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทยพิจารณาให้ความเห็นชอบก่อน

3. ข้อพิจารณา

ข้าพเจ้า ได้จัดทำร่างขอบเขตของงานจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ประจำปีงบประมาณ 2567 มีการกำหนดหลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ (เอกสารแนบ 5) และกำหนดราคากลาง (เอกสารแนบ 6) เสร็จเรียบร้อยแล้ว ซึ่งเห็นว่าผู้รับจ้างรายเดิม คือ บริษัท เอทพี โซลูชั่น จำกัด มีคุณสมบัติโดยตรงเพียงรายเดียว และมีความเชี่ยวชาญเป็นพิเศษ รวมทั้งเป็นผู้ออกแบบและพัฒนาระบบดังกล่าว จึงเห็นควรให้ผลจบ. ดำเนินการจ้างบำรุงรักษาระบบฯ เพื่อให้ระบบสามารถใช้งานได้อย่างต่อเนื่องและมีประสิทธิภาพ โดยอาศัยอำนาจแห่งพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 ประกอบกับระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 และคำสั่ง รพม. ที่ 98/2564 ลงวันที่ 5 เมษายน 2564 เรื่อง มอบอำนาจเกี่ยวกับการจัดซื้อหรือจัดจ้างพัสดุ

4. ข้อเสนอ

จึงเรียนมาเพื่อโปรดดำเนินการ ตามข้อ 3. ต่อไป จะขอคุณยิ่ง



(นางสาวสุพรรณ นิลสมบุญ)

โปรแกรมเมอร์ ระดับ 7



บันทึก การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

ที่..... ผทท/429.....วันที่..... 12 กรกฎาคม 2565.....

เรื่อง.....การจัดทำรายละเอียดค่าขอตังงบประมาณประจำปี 2567.....

เรียน ผอ.ฝจบ.

ตามที่ ฝจบ. ได้มีบันทึกด่วนที่สุดที่ ฝจบ/ว665 ลงวันที่ 20 มิถุนายน 2565 ขอให้ ฝ่าย/สำนัก จัดทำรายละเอียดค่าขอตังงบประมาณประจำปี 2567 ในรายการงบประมาณส่วนที่ ฝจบ. เป็นผู้ขอตังงบและรวบรวม ได้แก่ ค่าซ่อมแซมครุภัณฑ์ (งท.07) ค่าวัสดุสำนักงาน (งท.13) และค่าใช้จ่ายครุภัณฑ์ (งท.15) ภายในวันที่ 12 กรกฎาคม 2565 นั้น

ผทท. ได้ดำเนินการจัดทำค่าขอตังงบประมาณประจำปี 2567 ในรายการดังกล่าวข้างต้นเสร็จเรียบร้อยแล้ว โดยมีรายละเอียดตามเอกสารแนบ พร้อมทั้งได้จัดส่ง Soft file ให้ ฝจบ. ไปยัง E-mail prisana@mrtta.co.th เรียบร้อยแล้ว

(นายสมคิด สีสิตธรรม)

ผอ.ผทท.

รายละเอียดค่าใช้จ่ายการขอตั้งงบประมาณรายจ่าย หมวด ค่าใช้สอย

รายการ ค่าซ่อมแซมครุภัณฑ์

ประจำปีงบประมาณ 2567

หน่วยงาน ฝ่ายเทคโนโลยีสารสนเทศ

หน่วย : บาท (ทศนิยม 0 ตำแหน่ง)

ลำดับ	จำนวนเงิน	คำชี้แจง	
6	880,000.00	เพื่อบำรุงรักษาระบบงานสารสนเทศ ให้สามารถใช้งานได้อย่างต่อเนื่องตลอดเวลา	
7	200,000.00		
8	1,000,000.00		
9	800,000.00		
10	800,000.00		
11	1,350,000.00		
12	900,000.00		
13	4,000,000.00		
14	2,400,000.00		
15	750,000.00		
16	2,400,000.00		
17	4,300,000.00		
18	1,900,000.00		
19	3,400,000.00		
20	800,000.00		
21	500,000.00		
22	1,300,000.00		
23	77,000.00		
	รวมทั้งสิ้น		
	77,887,250.00		

เพื่อใช้เป็นค่าซ่อมแซมครุภัณฑ์ต่างๆ อุปกรณ์ที่เกี่ยวข้องภายในส่วนงาน และครุภัณฑ์สำนักงานอื่น ๆ ที่เกี่ยวข้อง เช่น โต๊ะ เก้าอี้ เครื่องโทรสาร เป็นต้น

หมายเหตุ : แบบฟอร์มข้างต้นใช้เพื่อบันทึกข้อมูลรวมของทั้งฝ่าย/สำนักเท่านั้น

ผู้จัดทำ..... โทร.....



ด่วนที่สุด

บันทึก

การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

ที่..... สผว/ว845 วันที่..... 8 ธันวาคม 2565
เรื่อง..... มติคณะกรรมการ รฟม. ครั้งที่ 12/2565 เมื่อวันที่ 30 พฤศจิกายน 2565

เรียน รผบ. รผง. รผว. รผก. รผบ. ผชก.(นายถนอมฯ) ผชก.(นายกิตติฯ) ผชก.(นางสาวจิรนนท์ฯ)
ผชก.(นายณัฐพงศ์ฯ) ผอ.สผว. ผอ.สสอ. ผอ.สกม. ผอ.सनก. ผอ.สตส. ผอ.ผนย.
ผอ.ผพค. ผอ.ผทท. ผอ.ผชง. ผอ.ผชด. ผอ.ผวส. ผอ.ผบก.1 ผอ.ผบก.2
ผอ.ผพธ. ผอ.ผรฟ. ผอ.ผปก. ผอ.ผรภ. ผอ.ผกท. ผอ.ผจบ. ผอ.ผทบ. ผอ.สปอ.
ผอ.สปร.

สผว. ใคร่ขอส่งมติคณะกรรมการ รฟม. ครั้งที่ 12/2565 เมื่อวันที่ 30 พฤศจิกายน 2565 มาเพื่อโปรดทราบและพิจารณาดำเนินการในส่วนที่เกี่ยวข้องต่อไป

(นางมลทิรา ลักษณะสิริศักดิ์)

ผอ.สผว.

สำเนาเรียน ผวก.



ด่วนที่สุด

บันทึกข้อความ

การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

ผชก.

เลขที่...2445...DCS.....

วันที่...7 ธ.ค. 65...เวลา...15.14..

ผวก. ภายใน

เลขรับ...5687.....

วันที่...8/12/65...เวลา...8.34..

ส่วนงาน.....สำนักผู้ว่าการ กองกิจกรรมคณะกรรมการ โทร. 1761 , 1727

ที่.....สผว/840.....วันที่.....7 ธันวาคม 2565

เรื่อง.....มติคณะกรรมการ รพม. ครั้งที่ 12/2565 เมื่อวันพุธที่ 30 พฤศจิกายน 2565

ACM 78-0.65

เรียน ผวก. ผ่าน ผชก.(นายถนอมฯ)

1. เรื่องเดิม

คณะกรรมการ รพม. ได้มีการประชุมครั้งที่ 12/2565 เมื่อวันพุธที่ 30 พฤศจิกายน 2565

2. ข้อเท็จจริง

สผว. ได้จัดทำมติคณะกรรมการ รพม. ตามข้อ 1. ดังนี้

2.1 ระเบียบวาระที่ 1.1 : การจัดประชุมผ่านสื่ออิเล็กทรอนิกส์ด้วยระบบ Video Teleconference

มติ : รับทราบ

2.2 ระเบียบวาระที่ 1.2 : กรรมการลาประชุม

มติ : รับทราบ

2.3 ระเบียบวาระที่ 1.3 : งานสวดพระอภิธรรมศพมารดาของท่านอภิรัฐ ไชยวงศ์น้อย

มติ : รับทราบ

2.4 ระเบียบวาระที่ 1.4 : ความคืบหน้าการดำเนินการในกรณีการอนุญาตให้บริษัท อนันดา ดีเวลลอปเม้นท์ ทู จำกัด ก่อสร้างอาคารชุดพักอาศัยขนาดใหญ่พิเศษ

มติ : รับทราบ และให้ รฟม. ประสานหารือกับหน่วยงานที่เกี่ยวข้องเพื่อร่วมกันพิจารณาแนวทางในการแก้ไขปัญหาการอนุญาตในกรณีนี้ และประเด็นแก้ไขร่างกฎกระทรวง ฉบับที่ 33 (พ.ศ. 2535) ออกตามความในพระราชบัญญัติควบคุมอาคาร พ.ศ. 2522 ฯ ภายในกรอบระยะเวลาตามคำพิพากษาของศาล โดยพิจารณาเชิญผู้แทนกรมโยธาธิการและผังเมืองเข้าร่วมด้วย

2.5 ระเบียบวาระที่ 2 : รับรองรายงานการประชุมคณะกรรมการ รฟม. ครั้งที่ 11/2565 เมื่อวันที่ 20 ตุลาคม 2565

มติ : รับรองรายงานการประชุมคณะกรรมการ รฟม. ครั้งที่ 11/2565 เมื่อวันที่ 20 ตุลาคม 2565

2.6 ระเบียบวาระที่ 4.1 : กรอบงบประมาณประจำปีงบประมาณ พ.ศ. 2567 ของ รฟม.

มติ : เห็นชอบกรอบงบประมาณประจำปีงบประมาณ พ.ศ. 2567 ของ รฟม. โดยมีวงเงินงบประมาณเพื่อดำเนินการ จำนวน 180,543.34 ล้านบาท และวงเงินเบิกจ่าย จำนวน 49,628.34 ล้านบาท ซึ่งจะเสนอขอรับการจัดสรรงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. 2567 จากสำนักงานงบประมาณ เป็นจำนวน 30,927.45 ล้านบาท และให้นำเสนอกระทรวงคมนาคมให้ความเห็นชอบก่อนจัดส่งสำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ และสำนักงานงบประมาณต่อไป ทั้งนี้ ให้ รฟม. รับข้อสังเกตของคณะกรรมการ รฟม. ไปพิจารณาดำเนินการต่อไป

3.10 ระเบียบวาระที่ 5.2
ให้ทุกฝ่ายทราบ

3.11 ระเบียบวาระที่ 5.3
ให้ทุกฝ่ายทราบ และให้ ฝพค. ดำเนินการตามมติต่อไป

3.12 ระเบียบวาระที่ 5.4
ให้ทุกฝ่ายทราบ

3.13 ระเบียบวาระที่ 5.5
ให้ทุกฝ่ายทราบ

4. ข้อเสนอ

จึงเรียนมาเพื่อโปรดพิจารณาสั่งการให้ฝ่ายต่างๆ ดำเนินการในส่วนที่เกี่ยวข้องต่อไป



(นางมลทิรา ลักษณะสิริศักดิ์)

ผอ.สพว.

เรียน ผอ.ฝ่าย/ สำนัก
เพื่อโปรดทราบและ
ดำเนินการในส่วนที่เกี่ยวข้องต่อไป



(นายภคพงศ์ ศิริกันทรมาศ)

ผวก.

8 ธ.ค. 65



สัญญาจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ
(Project Progress Monitoring System: PPMS)
ประจำปีงบประมาณ ๒๕๖๖

ระหว่าง

การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

กับ

บริษัท เอทูพี โซลูชั่น จำกัด
สัญญาเลขที่ จ(ข)๕/๒๕๖๖



สัญญาจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (Project Progress Monitoring System: PPMS) ประจำปีงบประมาณ ๒๕๖๖

สัญญาเลขที่ จ(ข)๕/๒๕๖๖

สัญญาฉบับนี้ทำขึ้น ณ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย สำนักงาน ตั้งอยู่เลขที่ ๑๗๕ ถนนพระราม ๙ แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร เมื่อวันที่ ๓ ตุลาคม พ.ศ. ๒๕๖๕ ระหว่าง การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย โดย นายทวิช พึ่งตน ผู้อำนวยการฝ่ายจัดซื้อและบริการ ปฏิบัติการแทน ผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย ซึ่งต่อไปในสัญญานี้เรียกว่า “ผู้ว่าจ้าง” ฝ่ายหนึ่ง กับ บริษัท เอทูพี โซลูชั่น จำกัด ซึ่งจดทะเบียนเป็นนิติบุคคล ณ สำนักงานทะเบียนหุ้นส่วนบริษัทกลาง กรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ มีสำนักงานใหญ่อยู่ เลขที่ ๕๐๓/๕ อาคารเค.เอส.แอล ทาวเวอร์ ชั้น ๔ ถนนศรีอยุธยา แขวงถนนพญาไท เขตราชเทวี กรุงเทพมหานคร โดยนายยุทธศักดิ์ สว่างผล ผู้มีอำนาจลงนาม ผูกพันนิติบุคคลปรากฏตามหนังสือรับรองของสำนักงานทะเบียนหุ้นส่วนบริษัทกลาง กรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ ที่ สจ.๓ ๐๐๑๓๒๐ ลงวันที่ ๗ กุมภาพันธ์ ๒๕๖๕ แนบท้ายสัญญานี้ ซึ่งต่อไปในสัญญานี้ เรียกว่า “ผู้รับจ้าง” อีกฝ่ายหนึ่ง

คู่สัญญาได้ตกลงกันมีข้อความดังต่อไปนี้

ข้อ ๑ ข้อตกลงว่าจ้าง

ผู้ว่าจ้างตกลงจ้างและผู้รับจ้างตกลงรับจ้างทำงาน บำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (Project Progress Monitoring System: PPMS) ประจำปีงบประมาณ ๒๕๖๖ ณ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย สำนักงาน ตั้งอยู่เลขที่ ๑๗๕ ถนนพระราม ๙ แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร ตามข้อกำหนดและเงื่อนไขแห่งสัญญานี้รวมทั้งเอกสารแนบท้ายสัญญา

ผู้รับจ้างตกลงที่จะจัดหาแรงงานและวัสดุ เครื่องมือเครื่องใช้ ตลอดจนอุปกรณ์ต่างๆ ชนิดดีเพื่อใช้ในการงานจ้างตามสัญญานี้

ข้อ ๒ เอกสารอันเป็นส่วนหนึ่งของสัญญา

เอกสารแนบท้ายสัญญาดังต่อไปนี้ให้ถือเป็นส่วนหนึ่งของสัญญานี้

๒.๑ ผนวก ๑ ขอบเขตของงานจ้างบำรุงรักษา จำนวน ๑๙ (สิบเก้า) หน้า

ระบบติดตามความก้าวหน้าโครงการ (Project Progress Monitoring System: PPMS) ประจำปีงบประมาณ ๒๕๖๖

๒.๒ ผนวก ๒ ใบเสนอราคาและหนังสือยืนยันราคา จำนวน ๒ (สอง) หน้า

๒.๓ ผนวก ๓ เอกสารเกี่ยวกับนิติบุคคลของผู้รับจ้าง จำนวน ๑๔ (สิบสี่) หน้า

หลักประกันสัญญา และเอกสารอื่นๆ ที่เกี่ยวข้อง

ความใดในเอกสารแนบท้ายสัญญาที่ขัดหรือแย้งกับข้อความในสัญญานี้ ให้ใช้ข้อความในสัญญานี้บังคับ และในกรณีที่เอกสารแนบท้ายสัญญาขัดแย้งกันเอง ผู้รับจ้างจะต้องปฏิบัติตามคำวินิจฉัยของคู่สัญญา คำวินิจฉัยของผู้ว่าจ้างให้ถือเป็นที่สุด และผู้รับจ้างไม่มีสิทธิเรียกร้องค่าจ้าง หรือค่าเสียหาย หรือค่าใช้จาในใดๆ เพิ่มเติมจากผู้ว่าจ้างทั้งสิ้น



ข้อ ๓ หลักประกันการปฏิบัติตามสัญญา

ในขณะที่ทำสัญญานี้ผู้รับจ้างได้นำหลักประกันเป็นเงินสด เป็นจำนวนเงิน ๓๐,๐๐๐.๐๐ บาท (สามหมื่นบาทถ้วน) ซึ่งเท่ากับร้อยละ ๕ (ห้า) ของราคาค่าจ้างตามสัญญา มามอบให้แก่ผู้ว่าจ้างเพื่อเป็นหลักประกันการปฏิบัติตามสัญญานี้

หลักประกันที่ผู้รับจ้างนำมามอบให้ตามวรรคหนึ่ง จะต้องมียุครอบคลุมความรับผิดชอบทั้งปวงของผู้รับจ้างตลอดอายุสัญญา ถ้าหลักประกันที่ผู้รับจ้างนำมามอบให้ดังกล่าวลดลงหรือเสื่อมค่าลง หรือมีอายุไม่ครอบคลุมถึงความรับผิดชอบของผู้รับจ้างตลอดอายุสัญญา ไม่ว่าด้วยเหตุใดๆ ก็ตาม รวมถึงกรณี ผู้รับจ้างส่งมอบงานล่าช้าเป็นเหตุให้ระยะเวลาแล้วเสร็จหรือวันครบกำหนดความรับผิดชอบในความชำรุดบกพร่องตามสัญญาเปลี่ยนแปลงไป ไม่ว่าจะเกิดขึ้นคราวใด ผู้รับจ้างต้องหาหลักประกันใหม่หรือหลักประกันเพิ่มเติมให้มีจำนวนครบถ้วนตามวรรคหนึ่งมามอบให้แก่ผู้ว่าจ้างภายใน ๑๕ (สิบห้า) วัน นับถัดจากวันที่ได้รับแจ้งเป็นหนังสือจากผู้ว่าจ้าง

หลักประกันที่ผู้รับจ้างนำมามอบไว้ตามข้อนี้ ผู้ว่าจ้างจะคืนให้แก่ผู้รับจ้างโดยไม่มีดอกเบี้ยเมื่อผู้รับจ้างพ้นจากข้อผูกพันและความรับผิดชอบทั้งปวงตามสัญญานี้แล้ว

ข้อ ๔ ค่าจ้างและการจ่ายเงิน

ผู้ว่าจ้างตกลงจ่ายและผู้รับจ้างตกลงรับเงินค่าจ้างจำนวนเงิน ๖๐๐,๐๐๐.๐๐ บาท (หกแสนบาทถ้วน) ซึ่งได้รวมภาษีมูลค่าเพิ่ม จำนวน ๓๙,๒๕๒.๓๔ บาท (สามหมื่นเก้าพันสองร้อยห้าสิบบาทสามสิบลีตต่างค์) ตลอดจนภาษีอากรอื่นๆ และค่าใช้จ่ายทั้งปวงด้วยแล้ว โดยกำหนดการจ่ายเงินเป็นงวดๆ จำนวน ๔ งวด งวดละ ๑๕๐,๐๐๐.๐๐ บาท (หนึ่งแสนห้าหมื่นบาทถ้วน) ซึ่งได้รวมภาษีมูลค่าเพิ่ม ตลอดจนภาษีอากรอื่น ๆ และค่าใช้จ่ายทั้งปวงด้วยแล้ว ซึ่งแต่ละงวดจะจ่ายทุกๆ สิ้นไตรมาส เมื่อผู้รับจ้างได้ปฏิบัติงานทั้งหมดให้แล้วเสร็จเรียบร้อยตามสัญญาและผู้ว่าจ้างได้ตรวจรับงานจ้างตามข้อ ๙ ไว้โดยครบถ้วนแล้ว

ข้อ ๕ กำหนดเวลาแล้วเสร็จและสิทธิของผู้ว่าจ้างในการบอกเลิกสัญญา

ผู้รับจ้างต้องเริ่มทำงานที่รับจ้างตั้งแต่วันที่ ๑ ตุลาคม ๒๕๖๕ และจะต้องทำงานให้แล้วเสร็จบริบูรณ์ภายในวันที่ ๓๐ กันยายน ๒๕๖๖ ถ้าผู้รับจ้างมิได้ลงมือทำงานภายในกำหนดเวลา หรือไม่สามารถทำงานให้แล้วเสร็จตามกำหนดเวลา หรือมีเหตุให้เชื่อได้ว่าผู้รับจ้างไม่สามารถทำงานให้แล้วเสร็จภายในกำหนดเวลา หรือจะแล้วเสร็จล่าช้าเกินกว่ากำหนดเวลา หรือผู้รับจ้างทำผิดสัญญาข้อใดข้อหนึ่ง หรือตกเป็นผู้ถูกพิทักษ์ทรัพย์เด็ดขาดหรือตกเป็นผู้ล้มละลาย หรือเพิกเฉยไม่ปฏิบัติตามคำสั่งของคณะกรรมการตรวจรับพัสดุ ผู้ว่าจ้างมีสิทธิที่จะบอกเลิกสัญญานี้ได้ และมีสิทธิจ้างผู้รับจ้างรายใหม่เข้าทำงานของผู้รับจ้างให้ลุ่ลวงไปได้ด้วย การใช้สิทธิบอกเลิกสัญญานี้ไม่กระทบสิทธิของผู้ว่าจ้างที่จะเรียกร้องค่าเสียหายจากผู้รับจ้าง

การที่ผู้ว่าจ้างมิใช้สิทธิเลิกสัญญาดังกล่าวข้างต้นนั้น ไม่เป็นเหตุให้ผู้รับจ้างพ้นจากความรับผิดชอบตามสัญญา

ข้อ ๖ การจ้างช่วง

ผู้รับจ้างจะต้องไม่เองงานทั้งหมดหรือแต่บางส่วนแห่งสัญญานี้ไปจ้างช่วงอีกทอดหนึ่ง เว้นแต่การจ้างช่วงงานแต่บางส่วนที่ได้รับอนุญาตเป็นหนังสือจากผู้ว่าจ้างแล้ว การที่ผู้ว่าจ้างได้อนุญาตให้จ้างช่วงงานแต่บางส่วนดังกล่าวนี้ ไม่เป็นเหตุให้ผู้รับจ้างหลุดพ้นจากความรับผิดชอบหรือพันธะหน้าที่ตามสัญญานี้ และผู้รับจ้างจะยังคงต้องรับผิดชอบในความผิดและความประมาทเลินเล่อของผู้รับจ้างช่วง หรือของตัวแทนหรือลูกจ้างของผู้รับจ้างช่วงนั้นทุกประการ



A2P SOLUTION CO., LTD.
/กรณีผู้รับจ้าง...

Yuan
Yuan

กรณีผู้รับจ้างไปจ้างช่างงานแต่บางส่วนโดยฝ่าฝืนความในวรรคหนึ่ง ผู้รับจ้างต้องชำระค่าปรับให้แก่ผู้ว่าจ้างเป็นจำนวนเงินในอัตราร้อยละ ๑๐ (สิบ) ของวงเงินของงานที่จ้างช่วงตามสัญญา ทั้งนี้ไม่ตัดสิทธิผู้ว่าจ้างในการบอกเลิกสัญญา

ข้อ ๗ ความรับผิดชอบของผู้รับจ้าง

ผู้รับจ้างจะต้องรับผิดชอบต่ออุบัติเหตุ ความเสียหาย หรือภัยอันตรายใดๆ อันเกิดจากการปฏิบัติงานของผู้รับจ้าง และจะต้องรับผิดชอบต่อความเสียหายจากการกระทำของลูกจ้างหรือตัวแทนของผู้รับจ้าง และจากการปฏิบัติงานของผู้รับจ้างช่วงด้วย (ถ้ามี)

ความเสียหายใดๆ อันเกิดแก่งานที่ผู้รับจ้างได้ทำขึ้น แม้จะเกิดขึ้นเพราะเหตุสุดวิสัยก็ตาม ผู้รับจ้างจะต้องรับผิดชอบโดยซ่อมแซมให้คืนดีหรือเปลี่ยนให้ใหม่โดยค่าใช้จ่ายของผู้รับจ้างเอง เว้นแต่ความเสียหายนั้นเกิดจากความผิดของผู้ว่าจ้าง ทั้งนี้ ความรับผิดชอบของผู้รับจ้างดังกล่าวในข้อนี้จะสิ้นสุดลงเมื่อผู้ว่าจ้างได้รับมอบงานครั้งสุดท้าย

ผู้รับจ้างจะต้องรับผิดชอบต่อบุคคลภายนอกในความเสียหายใดๆ อันเกิดจากการปฏิบัติงานของผู้รับจ้าง หรือลูกจ้างหรือตัวแทนของผู้รับจ้าง รวมถึงผู้รับจ้างช่วง (ถ้ามี) ตามสัญญานี้ หากผู้ว่าจ้างถูกเรียกร้องหรือฟ้องร้องหรือต้องชดใช้ค่าเสียหายให้แก่บุคคลภายนอกไปแล้ว ผู้รับจ้างจะต้องดำเนินการใดๆ เพื่อให้มีการว่าต่างแก่ต่างให้แก่ผู้ว่าจ้างโดยค่าใช้จ่ายของผู้รับจ้างเอง รวมทั้งผู้รับจ้างจะต้องชดใช้ค่าเสียหายนั้นๆ ตลอดจนค่าใช้จ่ายใดๆ อันเกิดจากการถูกเรียกร้องหรือถูกฟ้องร้องให้แก่ผู้ว่าจ้างทันที

ข้อ ๘ การจ่ายเงินแก่ลูกจ้าง

ผู้รับจ้างจะต้องจ่ายเงินแก่ลูกจ้างที่ผู้รับจ้างได้จ้างมาในอัตราและตามกำหนดเวลาที่ผู้รับจ้างได้ตกลงหรือทำสัญญาไว้ต่อลูกจ้างดังกล่าว

ถ้าผู้รับจ้างไม่จ่ายเงินค่าจ้างหรือค่าทดแทนอื่นใดแก่ลูกจ้างดังกล่าวในวรรคหนึ่ง ผู้ว่าจ้างมีสิทธิที่จะเอาเงินค่าจ้างที่จะต้องจ่ายแก่ผู้รับจ้างมาจ่ายให้แก่ลูกจ้างของผู้รับจ้างดังกล่าว และให้ถือว่าผู้ว่าจ้างได้จ่ายเงินจำนวนนั้นเป็นค่าจ้างให้แก่ผู้รับจ้างตามสัญญาแล้ว

ผู้รับจ้างจะต้องจัดให้มีประกันภัยสำหรับลูกจ้างทุกคนที่จ้างมาทำงาน โดยให้ครอบคลุมถึงความรับผิดชอบทั้งปวงของผู้รับจ้าง รวมทั้งผู้รับจ้างช่วง (ถ้ามี) ในกรณีความเสียหายที่คิดค่าสินไหมทดแทนได้ตามกฎหมาย ซึ่งเกิดจากอุบัติเหตุหรือภัยอันตรายใดๆ ต่อลูกจ้างหรือบุคคลอื่นที่ผู้รับจ้างหรือผู้รับจ้างช่วงจ้างมาทำงาน ผู้รับจ้างจะต้องส่งมอบกรมธรรม์ประกันภัยดังกล่าวพร้อมทั้งหลักฐานการชำระเบี้ยประกันให้แก่ผู้ว่าจ้างเมื่อผู้ว่าจ้างเรียกร้อง

ข้อ ๙ การตรวจรับงานจ้าง

เมื่อผู้ว่าจ้างได้ตรวจรับงานจ้างที่ส่งมอบและเห็นว่าถูกต้องครบถ้วนตามสัญญาแล้ว ผู้ว่าจ้างจะออกหลักฐานการรับมอบเป็นหนังสือไว้ให้ เพื่อผู้รับจ้างนำมาเป็นหลักฐานประกอบการขอรับเงินค่างานจ้างนั้น

ถ้าผลของการตรวจรับงานจ้างปรากฏว่างานจ้างที่ผู้รับจ้างส่งมอบไม่ตรงตามสัญญาผู้ว่าจ้างทรงไว้ซึ่งสิทธิที่จะไม่รับงานจ้างนั้น ในกรณีเช่นว่านี้ ผู้รับจ้างต้องทำการแก้ไขให้ถูกต้องตามสัญญาด้วยค่าใช้จ่ายของผู้รับจ้างเอง และระยะเวลาที่เสียไปเพราะเหตุดังกล่าวผู้รับจ้างจะนำมาอ้างเป็นเหตุขอชดเชยเวลาส่งมอบงานจ้างตามสัญญาหรือของดหรือลดค่าปรับไม่ได้

ข้อ ๑๐ รายละเอียดของงานจ้างคลาดเคลื่อน

ผู้รับจ้างรับรองว่าได้ตรวจสอบและทำความเข้าใจในรายละเอียดของงานจ้างโดยถี่ถ้วนแล้ว หากปรากฏว่ารายละเอียดของงานจ้างนั้นผิดพลาดหรือคลาดเคลื่อนไปจากหลักการทางวิศวกรรมหรือทางเทคนิค ผู้รับจ้างตกลงที่จะปฏิบัติตามคำวินิจฉัยของผู้ว่าจ้าง คณะกรรมการตรวจรับพัสดุ เพื่อให้งานแล้วเสร็จบริบูรณ์ คำวินิจฉัยดังกล่าวให้ถือเป็นที่สุด โดยผู้รับจ้างจะคิดค่าจ้าง ค่าเสียหาย หรือค่าใช้จ่ายใดๆ เพิ่มขึ้นจากผู้ว่าจ้าง หรือขอขยายอายุสัญญาไม่ได้

ข้อ ๑๑ ค่าปรับ

หากผู้รับจ้างไม่สามารถทำงานให้แล้วเสร็จภายในเวลาที่กำหนดไว้ในสัญญาและผู้ว่าจ้างยังมีได้บอกเลิกสัญญา ผู้รับจ้างจะต้องชำระค่าปรับให้แก่ผู้ว่าจ้าง โดยรายละเอียดค่าปรับให้เป็นไปตามที่กำหนดไว้ในขอบเขตของงานจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (Project Progress Monitoring System: PPMS) ประจำปีงบประมาณ ๒๕๖๖ ในผนวก ๑ นอกจากนี้ ผู้รับจ้างยอมให้ผู้ว่าจ้างเรียกค่าเสียหายอันเกิดขึ้นจากการที่ผู้รับจ้างทำงานล่าช้าเฉพาะส่วนที่เกินกว่าจำนวนค่าปรับดังกล่าวได้อีกด้วย

ในระหว่างที่ผู้ว่าจ้างยังมีได้บอกเลิกสัญญานั้น หากผู้ว่าจ้างเห็นว่าผู้รับจ้างจะไม่สามารถปฏิบัติตามสัญญาต่อไปได้ ผู้ว่าจ้างจะใช้สิทธิบอกเลิกสัญญาและใช้สิทธิตามข้อ ๑๒ ก็ได้ และถ้าผู้ว่าจ้างได้แจ้งข้อเรียกร้องไปยังผู้รับจ้างเมื่อครบกำหนดเวลาแล้วเสร็จของงานขอให้ชำระค่าปรับแล้ว ผู้ว่าจ้างมีสิทธิที่จะปรับผู้รับจ้างจนถึงวันบอกเลิกสัญญาได้อีกด้วย

ข้อ ๑๒ สิทธิของผู้ว่าจ้างภายหลังบอกเลิกสัญญา

ในกรณีที่ผู้ว่าจ้างบอกเลิกสัญญา ผู้ว่าจ้างอาจทำงานนั้นเองหรือว่าจ้างผู้อื่นให้ทำงานนั้นต่อจนแล้วเสร็จก็ได้ และในกรณีดังกล่าว ผู้ว่าจ้างมีสิทธิริบหรือบังคับจากหลักประกันการปฏิบัติตามสัญญาทั้งหมดหรือบางส่วนตามแต่จะเห็นสมควร นอกจากนั้น ผู้รับจ้างจะต้องรับผิดชอบในค่าเสียหายซึ่งเป็นจำนวนเกินกว่าหลักประกันการปฏิบัติตามสัญญา รวมทั้งค่าใช้จ่ายที่เพิ่มขึ้นในการทำงานนั้นต่อให้แล้วเสร็จตามสัญญา ซึ่งผู้ว่าจ้างจะหักเอาจากจำนวนเงินใดๆ ที่จะจ่ายให้แก่ผู้รับจ้างก็ได้

ข้อ ๑๓ การบังคับค่าปรับ ค่าเสียหาย และค่าใช้จ่าย

ในกรณีที่ผู้รับจ้างไม่ปฏิบัติตามสัญญาข้อใดข้อหนึ่งด้วยเหตุใดๆ ก็ตาม จนเป็นเหตุให้เกิดค่าปรับ ค่าเสียหาย หรือค่าใช้จ่ายแก่ผู้ว่าจ้าง ผู้รับจ้างต้องชดใช้ค่าปรับ ค่าเสียหาย หรือค่าใช้จ่ายดังกล่าวให้แก่ผู้ว่าจ้างโดยสิ้นเชิงภายในกำหนด ๑๕ (สิบห้า) วัน นับถัดจากวันที่ได้รับแจ้งเป็นหนังสือจากผู้ว่าจ้าง หากผู้รับจ้างไม่ชดใช้ให้ถูกต้องครบถ้วนภายในระยะเวลาดังกล่าวให้ผู้ว่าจ้างมีสิทธิที่จะหักเอาจากจำนวนเงินค่าจ้างที่ต้องชำระหรือบังคับจากหลักประกันการปฏิบัติตามสัญญาได้ทันที

หากค่าปรับ ค่าเสียหาย หรือค่าใช้จ่ายที่บังคับจากเงินค่าจ้างที่ต้องชำระ หรือหลักประกันการปฏิบัติตามสัญญาแล้วยังไม่เพียงพอ ผู้รับจ้างยินยอมชำระส่วนที่เหลือที่ยังขาดอยู่จนครบถ้วนตามจำนวนค่าปรับ ค่าเสียหาย หรือค่าใช้จ่ายนั้น ภายในกำหนด ๑๕ (สิบห้า) วัน นับถัดจากวันที่ได้รับแจ้งเป็นหนังสือจากผู้ว่าจ้าง

หากมีเงินค่าจ้างตามสัญญาที่หักไว้จ่ายเป็นค่าปรับ ค่าเสียหาย หรือค่าใช้จ่ายแล้ว ยังเหลืออยู่อีกเท่าใด ผู้ว่าจ้างจะคืนให้แก่ผู้รับจ้างทั้งหมด



ช่อ ๑๔...
สมชาย งาม
คุณวิภา

ข้อ ๑๔ การงดหรือลดค่าปรับ หรือการขยายเวลาปฏิบัติงานตามสัญญา

ในกรณีที่มีเหตุเกิดจากความผิดหรือความบกพร่องของฝ่ายผู้ว่าจ้าง หรือเหตุสุดวิสัย หรือเกิดจากเหตุการณ์อันหนึ่งอันใดที่ผู้รับจ้างไม่ต้องรับผิดชอบตามกฎหมาย หรือเหตุอื่นตามที่กำหนดในกฎกระทรวง ซึ่งออกตามความในกฎหมายว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ ทำให้ผู้รับจ้างไม่สามารถทำงานให้แล้วเสร็จตามเงื่อนไขและกำหนดเวลาแห่งสัญญานี้ได้ ผู้รับจ้างจะต้องแจ้งเหตุหรือเหตุการณ์ดังกล่าวพร้อมหลักฐานเป็นหนังสือให้ผู้ว่าจ้างทราบ เพื่อของดหรือลดค่าปรับ หรือขยายเวลาทำงานออกไปภายใน ๑๕ (สิบห้า) วันนับถัดจากวันที่เหตุนั้นสิ้นสุดลง หรือตามที่กำหนดในกฎกระทรวงดังกล่าว แล้วแต่กรณี

ถ้าผู้รับจ้างไม่ปฏิบัติให้เป็นไปตามความในวรรคหนึ่ง ให้ถือว่าผู้รับจ้างได้ละสิทธิเรียกร้องในการที่จะของดหรือลดค่าปรับ หรือขยายเวลาทำงานออกไปโดยไม่มีเงื่อนไขใดๆ ทั้งสิ้น เว้นแต่กรณีเหตุเกิดจากความผิดหรือความบกพร่องของฝ่ายผู้ว่าจ้าง ซึ่งมีหลักฐานชัดเจน หรือผู้ว่าจ้างทราบที่อยู่แล้วตั้งแต่วันที่

การงดหรือลดค่าปรับ หรือขยายกำหนดเวลาทำงานตามวรรคหนึ่ง อยู่ในดุลพินิจของผู้ว่าจ้างที่จะพิจารณาตามที่เห็นสมควร

ข้อ ๑๕ การใช้เรือไทย

ในการปฏิบัติตามสัญญานี้ หากผู้รับจ้างจะต้องส่งหรือนำของเข้ามาจากต่างประเทศ รวมทั้งเครื่องมือและอุปกรณ์ที่ต้องนำเข้ามาเพื่อปฏิบัติงานตามสัญญา ไม่ว่าผู้รับจ้างจะเป็นผู้นำของเข้ามาเอง หรือนำเข้ามาโดยผ่านตัวแทนหรือบุคคลอื่นใด ถ้าสิ่งของนั้นต้องนำเข้ามาโดยทางเรือในเส้นทางเดินเรือที่มีเรือไทยเดินอยู่และสามารถให้บริการรับขนได้ตามที่รัฐมนตรีว่าการกระทรวงคมนาคมประกาศกำหนด ผู้รับจ้างต้องจัดการให้สิ่งของดังกล่าวบรรทุกโดยเรือไทยหรือเรือที่มีสิทธิเช่นเดียวกับเรือไทยจากต่างประเทศมายังประเทศไทย เว้นแต่จะได้รับอนุญาตจากกรมเจ้าท่าก่อนบรรทุกของนั้นลงเรืออื่นที่มีใช้เรือไทยหรือเป็นของที่รัฐมนตรีว่าการกระทรวงคมนาคมประกาศยกเว้นให้บรรทุกโดยเรืออื่นได้ ทั้งนี้ไม่ว่าการส่งหรือนำเข้าสิ่งของดังกล่าวจากต่างประเทศจะเป็นแบบใด

ในการส่งมอบงานตามสัญญาให้แก่ผู้ว่าจ้าง ถ้างานนั้นมีสิ่งของตามวรรคหนึ่ง ผู้รับจ้างจะต้องส่งมอบใบตราส่ง (Bill of Lading) หรือสำเนาใบตราส่งสำหรับของนั้น ซึ่งแสดงว่าได้บรรทุกมาโดยเรือไทยหรือเรือที่มีสิทธิเช่นเดียวกับเรือไทยให้แก่ผู้ว่าจ้างพร้อมกับการส่งมอบงานด้วย

ในกรณีที่สิ่งของดังกล่าวไม่ได้บรรทุกจากต่างประเทศมายังประเทศไทยโดยเรือไทยหรือเรือที่มีสิทธิเช่นเดียวกับเรือไทย ผู้รับจ้างต้องส่งมอบหลักฐานซึ่งแสดงว่าได้รับอนุญาตจากกรมเจ้าท่า ให้บรรทุกของโดยเรืออื่นได้ หรือหลักฐานซึ่งแสดงว่าได้ชำระค่าธรรมเนียมพิเศษเนื่องจากการไม่บรรทุกของโดยเรือไทยตามกฎหมายว่าด้วยการส่งเสริมการพาณิชย์แล้วอย่างใดอย่างหนึ่งแก่ผู้ว่าจ้างด้วย

ในกรณีที่ผู้รับจ้างไม่ส่งมอบหลักฐานอย่างใดอย่างหนึ่งดังกล่าวในวรรคสองและวรรคสาม ให้แก่ผู้ว่าจ้าง แต่จะขอส่งมอบงานดังกล่าวให้ผู้ว่าจ้างก่อนโดยไม่รับชำระเงินค่าจ้าง ผู้ว่าจ้าง มีสิทธิรับเงินดังกล่าวไว้ก่อน และชำระเงินค่าจ้างเมื่อผู้รับจ้างได้ปฏิบัติถูกต้องครบถ้วนดังกล่าวแล้วได้


/สัญญานี้...
A2P SOLUTION CO., LTD.

สมชาย งาม
วิมล

สัญญานี้มีผลย้อนหลังไปตั้งแต่วันที่ ๑ ตุลาคม ๒๕๖๕

สัญญานี้ทำขึ้นเป็นสองฉบับ มีข้อความถูกต้องตรงกัน คู่สัญญาได้อ่านและเข้าใจข้อความโดยละเอียด
ตลอดแล้ว จึงได้ลงลายมือชื่อ พร้อมทั้งประทับตรา (ถ้ามี) ไว้เป็นสำคัญต่อหน้าพยาน และคู่สัญญาต่างยึดถือไว้
ฝ่ายละหนึ่งฉบับ

(ลงชื่อ)..... *ทวิ*ผู้ว่าจ้าง

(นายทวิ พิงตน)

ผู้อำนวยการฝ่ายจัดซื้อและบริการ
ปฏิบัติการแทน ผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

(ลงชื่อ)..... *สมชาย*ผู้รับจ้าง

(นายยุทธศักดิ์ สว่างผล)

ผู้มีอำนาจลงนามผูกพัน
บริษัท เอทพี โซลูชั่น จำกัด



(ลงชื่อ)..... *จิน*พยาน

(นางจิตตารีย์ ศรีอาวุธ)

ผู้อำนวยการกองจัดหาพัสดุทั่วไป
การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

(ลงชื่อ)..... *สุวิ*พยาน

(นายสุรียา อินทรasmบัติ)

บริษัท เอทพี โซลูชั่น จำกัด

เลขที่โครงการ ๖๕๐๓๗๑๕๔๓๘๓

เลขคุมสัญญา ๖๕๐๕๒๔๐๐๓๖๐๓

ทวิ



บันทึกข้อความ

การรถไฟฟ้านครหลวงแห่งประเทศไทย

เอกสารแนบ 3

เลขรับ 1423
วันที่ 7/4/66
เวลา 15.08

ส่วนงาน 2 ฝ่ายเทคโนโลยีสารสนเทศ โทร. 2587

ที่ ผทท/228 วันที่ 227 เมษายน 2566

เรื่อง 22 ขออนุมัติแต่งตั้งผู้รับผิดชอบในการจัดทำขอบเขตของงานและราคากลางจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ประจำปีงบประมาณ 2567

เรียน ผอ.ฝจบ.

1. ข้อเท็จจริง

1.1 ผทท. ได้มีบันทึกที่ ผทท/429 ลงวันที่ 12 กรกฎาคม 2565 จัดส่งรายละเอียดคำขอตั้งงบประมาณรายจ่าย หมวดค่าใช้สอย รายการค่าซ่อมแซมครุภัณฑ์ ประจำปีงบประมาณ 2567 เพื่อให้ ฝจบ. รวบรวมคำขอตั้งงบประมาณฯ ดังกล่าว โดยขอตั้งงบประมาณสำหรับจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ประจำปีงบประมาณ 2567 เป็นจำนวนเงินทั้งสิ้น 1,350,000 บาท (หนึ่งล้านสามแสนห้าหมื่นบาทถ้วน) (รวมภาษีมูลค่าเพิ่ม) ทั้งนี้ คณะกรรมการ รพม. ในคราวประชุมครั้งที่ 12/2565 เมื่อวันที่ 30 พฤศจิกายน 2565 ได้มีมติเห็นชอบกรอบงบประมาณประจำปีงบประมาณ 2567 แล้ว (เอกสารแนบ 1)

1.2 รพม. ได้ดำเนินการจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) จากบริษัท เอทพี โซลูชั่น จำกัด ตามสัญญาเลขที่ จ(ข) 5/2566 ลงวันที่ 3 ตุลาคม 2565 ซึ่งสัญญาดังกล่าวจะสิ้นสุดในวันที่ 30 กันยายน 2566 (เอกสารแนบ 2)

1.3 ผทท. ได้ประสาน ฝจบ. ตามข้อ 1.1 แล้ว ทราบว่า รายการฯ ดังกล่าวเป็นรายการที่อยู่ในงบทำการ ซึ่งมีแหล่งเบิกจ่ายจากรายได้ของ รพม. จึงสามารถดำเนินการร่างขอบเขตของงานฯ ได้

2. ข้อกฎหมาย

2.1 พระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560

มาตรา 6 เพื่อให้การปฏิบัติเกี่ยวกับการจัดซื้อจัดจ้างและการบริหารพัสดุโดยใช้เงินงบประมาณเป็นไปอย่างมีประสิทธิภาพ เกิดความคุ้มค่าต่อภารกิจของรัฐ และป้องกันปัญหาการทุจริต ให้หน่วยงานของรัฐปฏิบัติตามแนวทางของพระราชบัญญัตินี้ และกฎกระทรวง ระเบียบ และประกาศที่ออกตามความในพระราชบัญญัตินี้

มาตรา 61 ในการจัดซื้อจัดจ้างพัสดุแต่ละครั้ง ให้ผู้มีอำนาจแต่งตั้งผู้รับผิดชอบการจัดซื้อจัดจ้างนั้น ซึ่งจะกระทำโดยคณะกรรมการการจัดซื้อจัดจ้างหรือเจ้าหน้าที่คนใดคนหนึ่งก็ได้

องค์ประกอบและองค์ประชุมซึ่งกระทำโดยคณะกรรมการ และหน้าที่ของผู้รับผิดชอบการจัดซื้อจัดจ้างตามวรรคหนึ่ง ให้เป็นไปตามระเบียบที่รัฐมนตรีกำหนด

2.2 ระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560

ข้อ 21 ในการซื้อหรือจ้างที่มีใช้การจ้างก่อสร้าง ให้หัวหน้าหน่วยงานของรัฐแต่งตั้งคณะกรรมการขึ้นมาคณะหนึ่ง หรือจะให้เจ้าหน้าที่หรือบุคคลใดบุคคลหนึ่งรับผิดชอบในการจัดทำร่างขอบเขตของงานหรือรายละเอียดคุณลักษณะเฉพาะของพัสดุที่จะซื้อหรือจ้าง รวมทั้งกำหนดหลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอด้วย

องค์ประกอบ ระยะเวลาการพิจารณา และการประชุมของคณะกรรมการตามวรรคหนึ่งและวรรคสอง ให้เป็นไปตามที่หัวหน้าหน่วยงานของรัฐกำหนดตามความจำเป็นและเหมาะสม

2.3 คำสั่งการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย ที่ 98/2564 ลงวันที่ 5 เมษายน 2564 เรื่อง มอบอำนาจเกี่ยวกับการจัดซื้อหรือจัดจ้างพัสดุ

2. การมอบอำนาจดำเนินการและอำนาจสั่งซื้อหรือสั่งจ้าง ดังนี้

2.3 การสั่งซื้อหรือสั่งจ้างโดยวิธีเฉพาะเจาะจงครั้งหนึ่ง ให้เป็นอำนาจของผู้ดำรงตำแหน่งและภายในวงเงิน ดังต่อไปนี้

(1) ผู้อำนวยการกองจัดหาพัสดุทั่วไป ไม่เกิน 500,000 บาท (ห้าแสนบาทถ้วน)

(2) ผู้อำนวยการฝ่ายจัดซื้อและบริการ ไม่เกิน 5,000,000 บาท (ห้าล้านบาทถ้วน)

3. การมอบอำนาจตามคำสั่งนี้ให้ครอบคลุมถึงการดำเนินการทุกกระบวนการตามพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 ระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 กฎกระทรวง และประกาศที่ออกตามความในพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 และมติคณะรัฐมนตรีที่เกี่ยวข้อง ภายในอำนาจและวงเงินตามข้อ 2 ทั้งนี้ สำหรับการบอกเลิกหรือการตกลงเลิกสัญญาหรือข้อตกลง การแก้ไขสัญญาหรือข้อตกลง การงดหรือลดค่าปรับให้แก่คู่สัญญาหรือการขยายเวลาทำการตามสัญญาหรือข้อตกลง ให้เสนอผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย พิจารณาให้ความเห็นชอบก่อน และเมื่อผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทยได้พิจารณาให้ความเห็นชอบแล้ว ให้ผู้รับมอบอำนาจตามข้อ 2.1 ข้อ 2.2 และข้อ 2.3 มีหนังสือแจ้งการบอกเลิก หรือการตกลงเลิกสัญญาหรือข้อตกลง การงดหรือลดค่าปรับให้แก่คู่สัญญา การขยายเวลาทำการตามสัญญาหรือข้อตกลงหรือลงนามในสัญญาหรือข้อตกลง แล้วแต่กรณีต่อไป เว้นแต่ ผู้รับมอบอำนาจตามข้อ 2.3 (1) ให้สามารถดำเนินการได้โดยไม่ต้องเสนอผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทยพิจารณาให้ความเห็นชอบก่อน

3. ข้อพิจารณา

ผทท. พิจารณาแล้วเห็นว่า เพื่อให้การจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ประจำปีงบประมาณ 2567 สอดคล้องกับระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 จึงเห็นควรเสนอ ผอ.ฝจบ. แต่งตั้ง นางสาวสุพรรณษา นิลสมบุญณ์ โปรแกรมเมอร์ ระดับ 7 แผนกสนับสนุนระบบงานคอมพิวเตอร์ กองระบบงานคอมพิวเตอร์ ฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบในการจัดทำขอบเขตของงาน กำหนดหลักเกณฑ์การพิจารณา และราคากลางจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ประจำปีงบประมาณ 2567 ตามระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 ข้อ 21 ทั้งนี้ การแต่งตั้งนางสาวสุพรรณษา เป็นผู้รับผิดชอบการจัดทำขอบเขตของงานฯ ดังกล่าว เนื่องจากการดำเนินการต่อเนื่องเป็นประจำทุกปี ขอบเขตของงานฯ ไม่มีความซับซ้อน และเป็นหน้าที่ความรับผิดชอบโดยตรงของนางสาวสุพรรณษา ซึ่งมีหน้าที่ให้คำแนะนำและแก้ไขปัญหาการใช้งาน รวมทั้งบริหารจัดการและควบคุมให้ผู้รับจ้างบำรุงรักษาระบบฯ ให้สามารถใช้งานได้อย่างต่อเนื่องตลอดเวลา

4. ข้อเสนอ

จึงเรียนมาเพื่อโปรดพิจารณา หากเห็นชอบขอได้โปรดอนุมัติแต่งตั้งผู้รับผิดชอบฯ ตามข้อ 3. และ ผทท. จะได้ดำเนินการในส่วนที่เกี่ยวข้องต่อไป จะขอบคุณยิ่ง



(นางสาวสิริพร ชนเฉิดสิริกุล)

ผอ.กรค.

รท.ผอ.ฝทท.

อนุมัติตามเสนอ



(นายวิท ทุ่งตัน)

ผอ.ฝจบ.

7/4/66

รายชื่อคณะกรรมการจ้างและคณะกรรมการตรวจรับพัสดุ
จ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS)
ประจำปีงบประมาณ 2567

คณะกรรมการซื้อหรือจ้างโดยวิธีเฉพาะเจาะจง

1. นางสาวศิวลี เกตุคง	หัวหน้าแผนกแผนงานและบริหารเอกสาร 2-3 กองแผนงานและบริหารเอกสาร 2 ฝ่ายบริหารงานก่อสร้าง 2	ประธานกรรมการ
2. นางสาววิสุตา ชลาชนเดชะ	หัวหน้าแผนกแผนงานและบริหารเอกสาร 1-3 กองแผนงานและบริหารเอกสาร 1 ฝ่ายบริหารงานก่อสร้าง 1	กรรมการ
3. นางสาวปวีณา เปล่งเสียง	พนักงานวิเคราะห์ระบบ ระดับ 7 แผนกพัฒนาระบบงานคอมพิวเตอร์ กองระบบงานคอมพิวเตอร์ ฝ่ายเทคโนโลยีสารสนเทศ	กรรมการ

คณะกรรมการตรวจรับพัสดุ

1. นางสาวสิริพร อุซสาธิต	หัวหน้าแผนกอาวุโส ระดับ 10 แผนกข้อมูลและบริหารงานเอกสาร ฝ่ายวิศวกรรมและสถาปัตยกรรม 1 ฝ่ายวิศวกรรมและสถาปัตยกรรม	ประธานกรรมการ
2. นางสาวจตุรพร จารุวัจนกุล	หัวหน้าแผนกประเมินผลโครงการรถไฟฟ้า กองวางแผนโครงการรถไฟฟ้า ฝ่ายพัฒนาโครงการรถไฟฟ้า	กรรมการ
3. นางสาวสุพรรณษา นิลสมบุญ	โปรแกรมเมอร์ ระดับ 7 แผนกสนับสนุนระบบงานคอมพิวเตอร์ กองระบบงานคอมพิวเตอร์ ฝ่ายเทคโนโลยีสารสนเทศ	กรรมการและ เลขานุการ

ขอบเขตของงานจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ(Project Progress Monitoring System: PPMS)

ประจำปีงบประมาณ 2567

1. ความเป็นมา

การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย (รฟม.) ได้มีระบบติดตามความก้าวหน้าโครงการ (Project Progress Monitoring System: PPMS) เพื่อใช้สำหรับรองรับการติดตามความก้าวหน้าการก่อสร้างโครงการรถไฟฟ้าของ รฟม. โดยระบบฯ ดังกล่าว จะสิ้นสุดระยะเวลาการรับประกัน ในวันที่ 30 กันยายน 2566 ทั้งนี้ เพื่อให้ระบบติดตามความก้าวหน้าโครงการ (PPMS) สามารถใช้งานได้อย่างต่อเนื่องและมีประสิทธิภาพ รฟม. จึงจำเป็นต้องจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ต่อไป

2. วัตถุประสงค์

รฟม. มีความประสงค์จะจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) เพื่อให้ระบบฯ สามารถใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และตอบสนองความต้องการของผู้ใช้งานในองค์กรได้ดียิ่งขึ้น

3. คุณสมบัติของผู้ยื่นข้อเสนอ

- 3.1 มีความสามารถตามกฎหมาย
- 3.2 ไม่เป็นบุคคลล้มละลาย
- 3.3 ไม่อยู่ระหว่างเลิกกิจการ
- 3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง
- 3.5 ผู้รับจ้างต้องไม่เป็นผู้ที่ถูกระงับชื่อไว้ในบัญชีรายชื่อผู้ทำงานตามระเบียบของทางราชการและได้แจ้งเวียนชื่อแล้ว หรือไม่เป็นผู้ที่ได้รับผลของการสั่งให้นิติบุคคลหรือบุคคลอื่นเป็นผู้ทำงานตามระเบียบของทางราชการ
- 3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ กำหนดในราชกิจจานุเบกษา
- 3.7 ผู้รับจ้างต้องเป็นนิติบุคคลซึ่งมีอาชีพในการประกอบธุรกิจงานด้านการพัฒนาระบบสารสนเทศหรือประเภทเดียวกับงานที่ประกาศ
- 3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย ณ วันคัดเลือก หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรม ในการคัดเลือกครั้งนี้
- 3.9 ผู้รับจ้างต้องไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้เสนอราคาได้มีคำสั่งให้สละสิทธิ์ความคุ้มกันเช่นนั้น
- 3.10 ผู้ยื่นข้อเสนอต้องลงทะเบียนในระบบจัดซื้อจัดจ้างด้วยวิธีการอิเล็กทรอนิกส์ (Electronic Government Procurement : e - GP) ของกรมบัญชีกลาง

- 3.11 ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการเป็นไปตามเงื่อนไขข้อ 1.1 - 1.2 ของหนังสือคณะกรรมการวินิจฉัยปัญหาการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ กรมบัญชีกลาง ด่วนที่สุด ที่ กค(กวจ) 0405.2/ว124 ลงวันที่ 1 มีนาคม 2566 เรื่อง แนวทางปฏิบัติในการเร่งรัดการปฏิบัติงานตามสัญญาและการกำหนดคุณสมบัติของผู้มีสิทธิยื่นข้อเสนอ

4. ขอบเขตของงานจ้างบำรุงรักษา

- 4.1 ผู้รับจ้างดำเนินการดูแล ตรวจสอบ และบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ให้สามารถใช้งานได้อย่างต่อเนื่องตลอดระยะเวลาการบำรุงรักษา
- 4.2 ผู้รับจ้างต้องมีเจ้าหน้าที่ที่มีประสบการณ์และความเชี่ยวชาญ เพื่อบริการให้คำปรึกษา และตอบปัญหาทางโทรศัพท์ โทรศัพท์เคลื่อนที่ โทรสาร ไปรษณีย์อิเล็กทรอนิกส์ (E-Mail) หรือ Line ในวันและเวลาทำการของ รพม. (จันทร์ - ศุกร์ ระหว่างเวลา 08.00 น. - 17.00 น.) เมื่อได้รับแจ้งปัญหา จะต้องตอบปัญหาขั้นต้นภายใน 1 ชั่วโมง หลังจากได้รับแจ้ง โดยจะต้องดำเนินการตรวจสอบและแก้ไขให้แล้วเสร็จภายใน 5 วันทำการ นับแต่เวลาที่ผู้ว่าจ้างได้แจ้งข้อขัดข้อง ยกเว้นในกรณีที่การขัดข้องนั้น เป็นปัญหาที่มีความซับซ้อน ผู้รับจ้างจะต้องจัดทำแผนการดำเนินงาน พร้อมทั้งชี้แจงรายละเอียดของปัญหา และการแก้ปัญหาฯ ดังกล่าวจัดส่งให้แก่คณะกรรมการตรวจรับพัสดุฯ พิจารณาให้ความเห็นชอบ
- 4.3 ผู้รับจ้างจะต้องดำเนินการแก้ไขปัญหาข้อผิดพลาดของซอฟต์แวร์ (Debugging) เมื่อผู้ใช้ไม่สามารถใช้งานได้
- 4.4 ผู้รับจ้างต้องจัดให้มีเจ้าหน้าที่ ผู้ที่มีความรู้ ความชำนาญระบบติดตามความก้าวหน้าโครงการ (PPMS) เข้าดูแลรักษาระบบ (Preventive Maintenance: PM) ไตรมาสละ 1 ครั้ง เป็นอย่างน้อย พร้อมทั้งจัดทำรายงานผลการตรวจสอบระบบติดตามความก้าวหน้าโครงการ (PPMS) ตามที่ รพม. กำหนด
- 4.5 ในกรณีที่ รพม. มีความประสงค์จะเปลี่ยนแปลงเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์คอมพิวเตอร์อื่น ๆ สำหรับระบบติดตามความก้าวหน้าโครงการ (PPMS) ใหม่ ผู้รับจ้างจะต้องดำเนินการโอนย้ายระบบฯ ให้และเมื่อโอนย้ายแล้ว ระบบฯ จะต้องสามารถใช้งานได้ดังเดิม โดยไม่ก่อให้เกิดความเสียหายในการปฏิบัติงานของ รพม.
- 4.6 ในกรณีที่เครื่องคอมพิวเตอร์แม่ข่ายของ รพม. ไม่สามารถใช้งานได้ มีความจำเป็นต้องใช้เครื่องคอมพิวเตอร์แม่ข่ายที่ศูนย์คอมพิวเตอร์สำรอง (DR - site) ผู้รับจ้างจะต้องดำเนินการติดตั้งระบบติดตามความก้าวหน้าโครงการ (PPMS) พร้อมให้คำแนะนำหรือคำปรึกษาเกี่ยวกับปัญหาที่เกิดขึ้นให้สามารถใช้งานได้ โดยไม่มีค่าใช้จ่ายเพิ่มเติม
- 4.7 หากมีการปรับปรุงระบบติดตามความก้าวหน้าโครงการ (PPMS) เป็นเวอร์ชันใหม่ ผู้รับจ้างจะต้องนำมาปรับปรุงให้ รพม. โดยไม่มีค่าใช้จ่ายเพิ่มเติม
- 4.8 การบริการบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ให้ครอบคลุมถึงค่าแรงงาน ค่าให้คำปรึกษาที่เกี่ยวข้อง ค่าใช้จ่ายในการเดินทาง ค่าวัสดุอุปกรณ์ที่จำเป็น และค่าใช้จ่ายอื่นใดทั้งหลายทั้งปวงที่เกี่ยวข้องกับการบำรุงรักษา โดยที่ รพม. ไม่ต้องเสียค่าใช้จ่ายใด ๆ ทั้งสิ้นเพิ่มเติมจากราคาค่าจ้างในงานที่กำหนดไว้ในสัญญา

- 4.9 การติดตามปัญหา ความก้าวหน้าและแก้ไขปัญหา เมื่อดำเนินการเสร็จเรียบร้อยแล้ว ผู้รับจ้างต้องแจ้งผลให้ผู้แจ้งทราบ และรวบรวมเป็นรายงานสรุปการแจ้งปัญหาและการแก้ไขระบบติดตามความก้าวหน้าโครงการ (PPMS) ตามที่ รฟม. กำหนด
- 4.10 เมื่อผู้รับจ้างจะเข้าดำเนินการเพื่อแก้ไขปัญหาต่าง ๆ จะต้องแจ้งให้เจ้าหน้าที่ผู้รับผิดชอบของ รฟม. ทราบล่วงหน้า
- 4.11 การปรับปรุงแก้ไข Source Code ส่วนใด ๆ ของระบบติดตามความก้าวหน้าโครงการ (PPMS) ให้ผู้รับจ้างจัดทำรายละเอียดการแก้ไข (Log statement) ที่มีรายละเอียดครบถ้วน เข้าใจง่าย และจัดส่งให้แก่ รฟม. เพื่อใช้สำหรับอ้างอิงการแก้ไขระบบฯ ในอนาคต
- 4.12 Source code ที่ได้ปรับปรุงแก้ไข รวมทั้งรายงานหรือเอกสารใด ๆ ที่ผู้รับจ้างได้ทำขึ้น อันเนื่องมาจากการปฏิบัติงานตามสัญญาฯ ให้ตกเป็นกรรมสิทธิ์และลิขสิทธิ์ของ รฟม. ทั้งหมดอย่างไรก็ตาม ผู้รับจ้างอาจเก็บสำเนารายงานและเอกสารอื่นดังกล่าวไว้ เพื่อเป็นประวัติการทำงานของผู้รับจ้างเองได้
- 4.13 การปรับปรุงแก้ไข Source Code ส่วนใด ๆ ผู้รับจ้างต้องแก้ไขและออกแบบระบบให้ปลอดภัยตามมาตรฐาน Open Web Application Security Project (OWASP) Top 10 ล่าสุด หรือมาตรฐาน Common Weakness Enumeration (CWE) Top 25 ล่าสุด ณ ปีที่ส่งมอบงาน นับถัดจากวันที่ลงนามในสัญญา หรือมาตรฐานที่ยอมรับในสากล หรือกำหนดซอฟต์แวร์ให้เป็นเวอร์ชันล่าสุดที่ได้รับการอัปเดตแล้ว
- 4.14 ผู้รับจ้างต้องจัดทำเอกสาร Version Control ของระบบติดตามความก้าวหน้าโครงการ (PPMS) และจัดส่งให้แก่ รฟม. ทราบทุกครั้ง ก่อนนำ Source Code ที่ได้ปรับปรุงแก้ไข ไป Deploy ขึ้นระบบจริง เพื่อใช้สำหรับควบคุมและอ้างอิงการแก้ไขระบบ
- 4.15 การปรับปรุงแก้ไข Source Code ส่วนใด ๆ ผู้รับจ้างต้องตรวจสอบความมั่นคงปลอดภัยของ Source Code (Source Code Review) ตามมาตรฐานที่ รฟม. กำหนด
- 4.16 การปรับปรุงแก้ไข Source Code ส่วนใด ๆ ผู้รับจ้างต้องแก้ไขและออกแบบระบบให้มีการตรวจสอบความถูกต้องของข้อมูลนำเข้า (Input Validation) ก่อนการบันทึกและ/หรือประมวลผลข้อมูล รวมทั้งตรวจสอบข้อมูลที่ส่งออกจากระบบ (Output Validation) เพื่อป้องกันการแสดงผลหรือการประมวลผลข้อมูลที่ไม่เหมาะสม
- 4.17 ผู้รับจ้างและผู้ปฏิบัติงานของผู้รับจ้างจะต้องไม่เปิดเผยความลับของข้อมูลหรือข้อมูลอื่นใดทั้งหมดหรือบางส่วนที่ได้รับหรือรับรู้มาจาก รฟม. ให้ผู้อื่นทราบโดยมิได้รับความยินยอมจาก รฟม. และหากมีการนำข้อมูลใด ๆ ออกจาก รฟม. ผู้รับจ้างฯ จะต้องทำลายข้อมูลทั้งที่เป็นเอกสาร หรือข้อมูลในรูปแบบอิเล็กทรอนิกส์ทันทีที่สิ้นสุดสัญญาจ้าง โดยผู้รับจ้างฯ ต้องลงนามในเอกสารข้อตกลงในการไม่เปิดเผยข้อมูล (Non - Disclosure Agreement) และ รฟม. ขอสงวนสิทธิ์ในการเรียกร้องค่าเสียหายอันเนื่องมาจากการละเมิดข้อตกลงดังกล่าว
- 4.18 ผู้รับจ้างต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รฟม. ที่ปรากฏดัง ภาคผนวก ก.
- 4.19 ผู้รับจ้างจะต้องส่งบุคลากรเข้าร่วมการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness) เพื่อสร้างความตระหนักที่เหมาะสม ทบทวนนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและขั้นตอนปฏิบัติของ รฟม.

- 4.20 ระบบที่มีลักษณะเป็น Web Based Application ต้องใช้งานผ่านโปรโตคอล Hypertext Transfer Protocol Secure (HTTPS) โดยใช้ใบรับรอง SSL Certificate ที่ รฟม. กำหนด ทั้งนี้ หากใบรับรอง SSL Certificate หมดอายุ ผู้รับจ้างต้องปรับปรุงให้ระบบฯ ใช้งานผ่าน SSL Certificate ที่ รฟม. ต่ออายุแล้วต่อไป
- 4.21 ผู้รับจ้างต้องปิดช่องโหว่ (Hardening) ของระบบติดตามความก้าวหน้าโครงการ (PPMS) และซอฟต์แวร์ที่ใช้ในการพัฒนา หากซอฟต์แวร์นั้น ๆ มีการประกาศช่องโหว่ รวมทั้งช่องโหว่ที่ รฟม. ตรวจพบ พร้อมทั้งจัดทำรายงานผลการปิดช่องโหว่ระบบติดตามความก้าวหน้าโครงการ (PPMS) ตามที่ รฟม. กำหนด โดยที่ รฟม. ไม่ต้องเสียค่าใช้จ่ายใด ๆ เพิ่มเติมจากราคาค่าจ้างงานตามที่กำหนดไว้ตามสัญญา ทั้งนี้หากผู้รับจ้างไม่สามารถปิดช่องโหว่ให้แล้วเสร็จภายในระยะเวลาการรับประกัน จะต้องจัดทำแผนการดำเนินงานปิดช่องโหว่ ซึ่งระบุรายละเอียดและสาเหตุที่ไม่สามารถปิดช่องโหว่ภายในระยะเวลาการรับประกัน พร้อมทั้งจัดส่งให้คณะกรรมการตรวจรับพัสดุฯ พิจารณาให้ความเห็นชอบ
- 4.22 การติดตามความคืบหน้าการปิดช่องโหว่ เมื่อดำเนินการเสร็จเรียบร้อยแล้ว ผู้รับจ้างต้องแจ้งผลให้ผู้แจ้งทราบ และรวบรวมเป็นรายงานผลการปิดช่องโหว่ระบบติดตามความก้าวหน้าโครงการ (PPMS) ตามที่ รฟม. กำหนด
- 4.23 ผู้รับจ้างจะต้อง ทบทวน/ ปรับปรุง คู่มือการใช้งานระบบติดตามความก้าวหน้าโครงการ (PPMS) และจัดส่งให้แก่ รฟม. เมื่อมีการปรับปรุงระบบฯ ดังกล่าว โดยไม่มีค่าใช้จ่ายเพิ่มเติม
- 4.24 ผู้รับจ้างต้องจัดส่งรายงานผลการบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ให้แก่ รฟม. เพื่อทราบ ทุกสิ้นไตรมาส โดยส่งมอบภายในวันที่ 15 ของไตรมาสถัดไป (ภาคผนวก ข.) ซึ่งประกอบด้วย
- 1) รายงานผลการตรวจสอบระบบติดตามความก้าวหน้าโครงการ (PPMS)
 - 2) รายงานการตรวจสอบสิทธิการเข้าถึงระบบ (Role Matrix)
 - 3) รายงานสรุปการแจ้งปัญหาและการแก้ไขระบบติดตามความก้าวหน้าโครงการ (PPMS)
 - 4) รายงานผลการปิดช่องโหว่ระบบติดตามความก้าวหน้าโครงการ (PPMS) (หากมี)
 - 5) รายงานทะเบียนทรัพย์สิน (Asset Inventory)
- 4.25 ผู้รับจ้างจะต้องไม่เอางานทั้งหมดหรือแต่บางส่วนไปจ้างช่วงอีกทอดหนึ่ง เว้นแต่การจ้างช่วงงาน แต่บางส่วนที่ได้รับอนุญาตเป็นหนังสือจาก รฟม. แล้ว การที่ รฟม. ได้อนุญาตให้จ้างช่วงงานแต่บางส่วนดังกล่าวนี้ไม่เป็นเหตุให้ผู้รับจ้างหลุดพ้นจากความรับผิดชอบหรือพันธหน้าที่ และผู้รับจ้างจะยังคงต้องรับผิดชอบในความผิดและความประมาทเลินเล่อของผู้รับจ้างช่วง หรือของตัวแทนหรือลูกจ้างของผู้รับจ้างช่วงนั้นทุกประการ (หากมี)

5. กำหนดเวลาส่งมอบพัสดุ

นับตั้งแต่วันที่ 1 ตุลาคม 2566 – วันที่ 30 กันยายน 2567

6. หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

ในการพิจารณาผลการคัดเลือกข้อเสนอการจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ครั้งนี้ รฟม. จะพิจารณาคัดเลือกโดยใช้หลักเกณฑ์ **ราคารวม** ที่เป็นราคาต่ำสุด อยู่ในวงเงินงบประมาณ และเป็นผู้มีคุณสมบัติครบถ้วน ถูกต้อง ตรงตามรายละเอียดและเงื่อนไขที่ รฟม. กำหนด

7. วงเงินงบประมาณ/วงเงินที่ได้รับจัดสรร2

วงเงินสำหรับการจัดการจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ประจำปีงบประมาณ 2567 เป็นจำนวนทั้งสิ้น 1,350,000.00 บาท (หนึ่งล้านสามแสนห้าหมื่นบาทถ้วน) รวมภาษีมูลค่าเพิ่มตลอดจนภาษีอากรอื่น ๆ และค่าใช้จ่ายทั้งปวงแล้ว

8. งวดงานและการจ่ายเงิน

รฟม. จะชำระเงินค่าจ้างงานให้แก่ผู้รับจ้าง โดยแบ่งจ่ายเป็น 4 งวด เป็นจำนวนเงินเท่ากัน (รวมภาษีมูลค่าเพิ่ม) ซึ่งแต่ละงวดจะจ่ายทุก ๆ สิ้นไตรมาส หลังจาก รฟม. ได้รับรายงานผลการบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) และคณะกรรมการตรวจรับพัสดุฯ ได้มีการตรวจรับงานแต่ละงวดเรียบร้อยแล้ว

9. อัตราค่าปรับ2

ในกรณีที่ผู้ใช้งานไม่สามารถใช้งานระบบติดตามความก้าวหน้าโครงการ (PPMS) ได้ ผู้รับจ้างต้องดำเนินการตรวจสอบและแก้ไขให้แล้วเสร็จภายใน 5 วันทำการ นับแต่เวลาที่ผู้ว่าจ้างได้แจ้งข้อขัดข้องให้ผู้รับจ้างทราบทางโทรศัพท์ โทรศัพท์เคลื่อนที่ โทรสาร ไปรษณีย์อิเล็กทรอนิกส์ (E-Mail) หรือ Line ในวันและเวลาทำการของ รฟม. (จันทร์ - ศุกร์ ระหว่างเวลา 08.00 น. - 17.00 น.) ยกเว้นในกรณีที่การขัดข้องนั้นเป็นปัญหาที่มีความซับซ้อน ผู้รับจ้างจะต้องจัดทำแผนการดำเนินงานจัดส่งให้แก่คณะกรรมการตรวจรับพัสดุฯ พิจารณาให้ความเห็นชอบ ทั้งนี้หากไม่สามารถดำเนินการแก้ไขได้แล้วเสร็จตามแผนฯ (ภายใน 5 วันทำการ หรือตามที่คณะกรรมการตรวจรับพัสดุฯ ได้ให้ความเห็นชอบแล้วแต่กรณี) ผู้รับจ้างจะต้องเสียค่าปรับเป็นรายวันในอัตราร้อยละ 1,500.00 บาท (หนึ่งพันห้าร้อยบาทถ้วน) เฉพาะของวันให้คิดเป็น 1 วัน

2

2

2

2

2

2

2

ภาคผนวก ก.2



การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

MASS RAPID TRANSIT AUTHORITY OF THAILAND

รัฐวิสาหกิจภายใต้กำกับของรัฐมนตรีว่าการกระทรวงคมนาคม

A STATE ENTERPRISE UNDER SUPERVISION OF MINISTER OF TRANSPORT

ประกาศการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (ฉบับปรับปรุงครั้งที่ 11)

ด้วยพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 มาตรา 5 กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ มีความมั่นคงปลอดภัยและเชื่อถือได้ จึงส่งผลให้ระบบเทคโนโลยีสารสนเทศของการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย (รฟม.) ต้องมีการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศอย่างครบถ้วนเพื่อธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) และความน่าเชื่อถือ (Reliability)

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ 2) พ.ศ. 2556 ข้อ 14 กำหนดให้หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer: CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

อาศัยอำนาจตามความในมาตรา 25 แห่งพระราชบัญญัติการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย พ.ศ. 2543 ผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย จึงออกประกาศการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ดังต่อไปนี้

1. วัตถุประสงค์และขอบเขต

เพื่อให้การใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาและลดผลกระทบจากการใช้งานระบบเทคโนโลยีสารสนเทศ ในลักษณะที่ไม่ถูกต้องหรือจากการถูกคุกคามจากภัยต่าง ๆ จึงได้กำหนดนโยบายเพื่อควบคุมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ดังนี้

1.1 การเข้าถึงหรือควบคุมการใช้งานสารสนเทศครอบคลุม 4 ด้าน คือ

1.1.1 การเข้าถึงระบบสารสนเทศ (Access control) ต้องตรวจสอบการอนุมัติสิทธิ์การเข้าถึงระบบและกำหนดรหัสผ่าน การลงทะเบียนผู้ใช้งานเพื่อให้ผู้ใช้ที่มีสิทธิ์ (User authentication) เท่านั้นที่สามารถ

สมบูรณ์

/เข้าถึง ...
สิทธิ์

เข้าถึงระบบได้ รวมถึงมีการเก็บบันทึกข้อมูลการเข้าถึงระบบ (Access log) และข้อมูลจราจรทางคอมพิวเตอร์ ทั้งนี้ การให้สิทธิ์การใช้งานระบบสารสนเทศนั้นต้องให้สิทธิ์ที่เหมาะสมและเพียงพอ (Need to know and Need to use)

1.1.2 การเข้าถึงระบบเครือข่าย (Network access control) ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ การรับ - ส่ง หรือการไหลเวียนข้อมูลหรือสารสนเทศจะต้องผ่านระบบการรักษาความปลอดภัยที่องค์กรจัดสรรไว้ เช่น Firewall IDS/IPS Proxy หรือการตรวจสอบไวรัสคอมพิวเตอร์ เป็นต้น เพื่อควบคุมและป้องกันภัยคุกคามอย่างเป็นระบบ

1.1.3 การเข้าถึงระบบปฏิบัติการ (Operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการ โดยไม่ได้รับอนุญาต โดยกำหนดให้มีการยืนยันตัวตนเพื่อระบุถึงตัวตนของผู้ใช้งาน รวมทั้งกำหนดให้มีการจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้ความมั่นคงปลอดภัยมากยิ่งขึ้น

1.1.4 การเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information access control) ต้องกำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศ โดยให้สิทธิ์เฉพาะระบบงานสารสนเทศที่ต้องปฏิบัติตามหน้าที่เท่านั้น รวมทั้งมีการทบทวนสิทธิ์การใช้งานระบบสารสนเทศอย่างสม่ำเสมอ

1.2 มีระบบสารสนเทศและระบบสำรองที่อยู่ในสภาพพร้อมใช้งาน รวมทั้งมีแผนเตรียมพร้อมในกรณีฉุกเฉินหรือกรณีที่ไม่สามารถดำเนินการตามวิธีการทางอิเล็กทรอนิกส์ได้ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

1.3 ตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศอย่างสม่ำเสมอ

2. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รพม.

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รพม. ใช้แนวทางและกระบวนการอ้างอิงตาม 1) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานรัฐ พ.ศ. 2553 2) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555 และ 3) มาตรฐาน ISO/IEC 27001:2013 โดยแบ่งแนวปฏิบัติออกเป็น 16 ส่วนตามเอกสารแนบท้ายประกาศ ดังต่อไปนี้

2.1 นโยบายการบริหารจัดการความมั่นคงปลอดภัยสำหรับผู้บริหาร (ส่วนที่ 1)

2.2 ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร (ส่วนที่ 2)

2.3 การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (ส่วนที่ 3)

2.4 การจัดการทรัพย์สิน (ส่วนที่ 4)

2.5 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (ส่วนที่ 5)

2.6 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ (ส่วนที่ 6)

2.7 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (ส่วนที่ 7)

2.8 การควบคุมหน่วยงานภายนอกและผู้ใช้งาน (บุคคลภายนอก) เข้าถึงระบบเทคโนโลยีสารสนเทศ (ส่วนที่ 8)

2.9 การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ของ รพม. (ส่วนที่ 9)

2.10 การใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์ (ส่วนที่ 10)

- 2.11 การใช้งานจดหมายอิเล็กทรอนิกส์ (ส่วนที่ 11)
- 2.12 การสำรองข้อมูลและการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (ส่วนที่ 12)
- 2.13 การตรวจสอบและประเมินความเสี่ยง (ส่วนที่ 13)
- 2.14 การถ่ายโอน และการแลกเปลี่ยนข้อมูลสารสนเทศ (ส่วนที่ 14)
- 2.15 การควบคุมการเข้ารหัส (ส่วนที่ 15)
- 2.16 การนำอุปกรณ์ส่วนตัวมาใช้งาน (Bring your own device) (ส่วนที่ 16)

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศตามข้อ 2. จัดเป็นมาตรฐานด้านความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. ซึ่งบุคลากรของ รฟม. หน่วยงานภายนอก รวมถึงผู้ใช้บริการระบบสารสนเทศของ รฟม. ที่เกี่ยวข้องจะต้องปฏิบัติตามอย่างเคร่งครัด

3. กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้ว่าการการรถไฟฟ้ามหานครแห่งประเทศไทย (Chief Executive Officer: CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น และดำเนินการตรวจสอบข้อเท็จจริงกรณีที่ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด รวมทั้งให้พิจารณาลงโทษตามเหตุอันควร

นโยบายนี้ให้ใช้บังคับเมื่อพ้นกำหนด 7 วัน นับแต่วันที่ผู้มีอำนาจลงนาม

ประกาศ ณ วันที่ 7 กันยายน พ.ศ. 2565



(นายภคพงศ์ ศิริกันทรมาศ)

ผู้ว่าการการรถไฟฟ้ามหานครแห่งประเทศไทย



ภคพงศ์

เอกสารแนบท้ายประกาศ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ของ รฟม.

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

1. รฟม. หมายถึง การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
2. ผทท. หมายถึง ฝ่ายเทคโนโลยีสารสนเทศ
3. ผู้บริหารระดับสูงสุด หมายถึง ผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
4. ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของ รฟม.
5. ผู้ใช้งาน หมายถึง บุคคลที่ได้รับอนุญาตให้สามารถเข้าใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. ดังนี้
 - บุคลากรของ รฟม.
 - บุคคลภายนอกที่ รฟม. อนุญาตให้เข้ามาใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. ได้ชั่วคราว เพื่อประโยชน์ในการดำเนินการของ รฟม. ได้แก่ พนักงานหรือลูกจ้างบริษัทภายนอกที่เข้ามาติดตั้งหรือดูแลรักษาระบบให้กับ รฟม. ที่ปรึกษา ผู้ปฏิบัติงานตามสัญญา หรือนิสิตนักศึกษาฝึกงาน
6. ผู้ใช้งานภายนอก หมายถึง ลูกค้าหรือบุคคลภายนอกที่ไม่ใช่กลุ่มผู้ใช้งานตามข้อ 5. ที่ใช้บริการระบบงานสารสนเทศของ รฟม. ผ่านเครือข่ายสาธารณะ (Internet)
7. หน่วยงานภายนอก หมายถึง องค์กร ซึ่ง รฟม. อนุญาตให้มีสิทธิ์ในการเข้าถึง หรือใช้ข้อมูล หรือสินทรัพย์ต่าง ๆ ของ รฟม. โดยจะได้รับสิทธิ์ในการใช้ระบบตามประเภทงานตามอำนาจและต้องรับผิดชอบในการรักษาความลับของข้อมูล
8. ผู้ดูแลระบบ หมายถึง พนักงานที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบสารสนเทศ
9. เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
10. มาตรฐาน หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย
11. ขั้นตอนปฏิบัติ หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานตามที่ได้กำหนดไว้ตามวัตถุประสงค์
12. แนวปฏิบัติ หมายถึง แนวทางที่ต้องปฏิบัติตามเพื่อให้สามารถบรรลุวัตถุประสงค์หรือเป้าหมายได้ง่ายขึ้น
13. ระบบเทคโนโลยีสารสนเทศ (Information technology system) หมายถึง ระบบงานของ รฟม. ที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายสื่อสารข้อมูลมาช่วยในการสร้างสารสนเทศที่ รฟม. สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุน การให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ ได้แก่ ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลและสารสนเทศ เป็นต้น

14. ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด ที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์
15. ข้อมูลจราจรทางคอมพิวเตอร์ (Traffic log) หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เวลา วันที่ ปริมาณ ระยะเวลา หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น
16. สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งข้อมูลอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิกให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ
17. ระบบคอมพิวเตอร์ (Computer system) หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่งหรือสิ่งอื่นใด และแนวปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
18. ระบบเครือข่ายสื่อสารข้อมูล (Network system) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของ รพม. เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น
19. สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกักระบบสารสนเทศของหน่วยงาน
20. ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) และความน่าเชื่อถือ (Reliability)
21. เหตุการณ์ด้านความมั่นคงปลอดภัย หมายถึง เหตุการณ์ที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย มาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
22. สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม
23. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้
24. สินทรัพย์ (Assets) หมายถึง สินทรัพย์ด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารของ รพม. เช่น อุปกรณ์คอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีค่าลิขสิทธิ์ ข้อมูล ระบบข้อมูล ฯลฯ
25. จดหมายอิเล็กทรอนิกส์ (e-mail) หมายถึง ระบบที่บุคคลใช้ในการรับ - ส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว

และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ โดยข่าวสารที่ส่งนั้นจะถูกเก็บไว้ในตู้จดหมาย (Mail box) ที่กำหนดไว้สำหรับผู้ใช้งาน ผู้รับสามารถเปิดอ่าน พิมพ์ลงกระดาษ หรือจะลบทิ้งก็ได้

26. ชุดคำสั่งไม่พึงประสงค์ (Malicious code) หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ชัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
27. เครื่องคอมพิวเตอร์ หมายถึง เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ และเครื่องคอมพิวเตอร์แบบพกพา
28. อุปกรณ์เคลื่อนที่ (Mobile device) หมายถึง อุปกรณ์อิเล็กทรอนิกส์แบบพกพา ซึ่งมีความสามารถในการเชื่อมต่อกับอุปกรณ์อื่นเพื่อรับส่งข้อมูลผ่านระบบเครือข่ายโทรคมนาคมไร้สายหรือโดยอาศัยคลื่นแม่เหล็กไฟฟ้าเป็นสื่อกลาง เช่น Tablet, Smart Phone
29. อุปกรณ์ส่วนตัว หมายถึง อุปกรณ์ที่ รพม. ไม่ได้เป็นผู้จัดสรรให้ใช้งาน แต่เป็นอุปกรณ์ส่วนตัวของผู้ใช้งานที่นำมาเชื่อมต่อกับเครือข่ายภายในของ รพม. เช่น เครื่องคอมพิวเตอร์ส่วนบุคคล (Personal computer) เครื่องคอมพิวเตอร์พกพา (Notebook) อุปกรณ์เคลื่อนที่ (Mobile device) หรือ Removable media เป็นต้น

ส่วนที่ 1

นโยบายการบริหารจัดการความมั่นคงปลอดภัยสำหรับผู้บริหาร

วัตถุประสงค์

- เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรมีความสอดคล้องกับมาตรฐานสากลและกฎหมายด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง

ผู้รับผิดชอบ

- ผู้บริหารสูงสุด

อ้างอิงมาตรฐาน

- หมวดที่ 1 นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information security policy)

แนวปฏิบัติ

1. จัดให้มีการทำและทบทวนหรือปรับปรุงนโยบายความมั่นคงปลอดภัย และแนวปฏิบัติที่สนับสนุนการทำงานต่าง ๆ อย่างน้อยปีละ 1 ครั้ง โดยพิจารณาจากปัจจัยนำเข้า ดังนี้
 - 1.1 กลยุทธ์การดำเนินงานขององค์กร
 - 1.2 ข้อมูลกฎหมาย ระเบียบ ข้อบังคับต่าง ๆ ที่ต้องปฏิบัติตาม
 - 1.3 การปรับปรุงนโยบายความมั่นคงปลอดภัยสำหรับปีถัดไป
 - 1.4 ผลการประเมินความเสี่ยงและแผนลดความเสี่ยง
 - 1.5 ผลการแจ้งเตือนโดยระบบป้องกันการบุกรุกในปีที่ผ่านมา
 - 1.6 ผลของการตรวจสอบข้อมูลการปิดช่องโหว่ (Patch) สำหรับระบบต่าง ๆ ในปีที่ผ่านมา
 - 1.7 การจัดทำและต่อสัญญาบำรุงรักษาระบบและอุปกรณ์ต่าง ๆ
 - 1.8 แผนการอบรมทางด้านความมั่นคงปลอดภัยประจำปีซึ่งรวมถึงการสร้างตระหนักรู้
 - 1.9 ผลการทดสอบแผนกู้คืนในปีที่ผ่านมา
 - 1.10 ข้อมูลภัยคุกคามต่าง ๆ ที่เคยเกิดขึ้นในอดีตและปัจจุบัน รวมทั้งภัยคุกคามที่ได้รับแจ้งจากหน่วยงานภายนอก
 - 1.11 ผลการตรวจสอบการปฏิบัติตามนโยบายความมั่นคงปลอดภัยโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก
2. จัดให้มีทรัพยากรด้านบุคลากร งบประมาณ การบริหารจัดการ และวัตถุประสงค์ที่เพียงพอต่อการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศในแต่ละปีงบประมาณ
3. จัดให้มีบุคลากรดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศและกำหนดหน้าที่ความรับผิดชอบรวมทั้งปรับปรุงโครงสร้างดังกล่าวตามความจำเป็น
4. แสดงเจตนาชัดเจนหรือสื่อสารอย่างสม่ำเสมอเพื่อให้ผู้ใช้งานทั้งหมดได้เห็นถึงความสำคัญของการปฏิบัติตามนโยบายความมั่นคงปลอดภัยและนโยบายสนับสนุนต่าง ๆ โดยเคร่งครัดและเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับสารสนเทศขององค์กร รวมถึงสร้างความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

ส่วนที่ 2

ความมั่นคงปลอดภัยเกี่ยวกับบุคลากร

วัตถุประสงค์

- เพื่อให้ผู้ใช้งานเข้าใจถึงบทบาท หน้าที่ความรับผิดชอบ ทั้งก่อนการจ้างงาน ระหว่างการจ้างงาน และสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน ตลอดจนตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศเพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง การใช้งานระบบเทคโนโลยีสารสนเทศผิดวัตถุประสงค์และความผิดพลาดในการปฏิบัติหน้าที่ ซึ่งอาจส่งผลกระทบต่อหรือทำให้ รพม. เกิดความเสียหาย

ผู้รับผิดชอบ

- ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ ผู้อำนวยการฝ่ายทรัพยากรบุคคล ผู้อำนวยการฝ่าย/สำนัก ที่กำกับดูแลงานที่มีการว่าจ้างหน่วยงานภายนอก

อ้างอิงมาตรฐาน

- หมวดที่ 3 ความมั่นคงปลอดภัยสำหรับบุคลากร (Organization of information security)
- หมวดที่ 4 การบริหารจัดการทรัพย์สิน (Asset management)
- หมวดที่ 9 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)

แนวปฏิบัติ

1. การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to employment) เพื่อคัดสรรบุคลากรก่อนที่จะเข้ามาปฏิบัติงาน และเพื่อลดความเสี่ยงจากการปฏิบัติงานผิดพลาด การขโมย การปลอมแปลง และการนำระบบสารสนเทศหรือทรัพยากรสารสนเทศของ รพม. ไปใช้ในทางที่ไม่เหมาะสม รวมทั้งเพื่อให้ผู้ใช้งานเข้าใจในหน้าที่ความรับผิดชอบของตนเอง
 - 1.1 การตรวจสอบคุณสมบัติของผู้สมัคร (Screening)

ฝ่ายทรัพยากรบุคคล หรือฝ่าย/สำนัก ที่กำกับดูแลงานที่มีการว่าจ้างหน่วยงานภายนอกต้องตรวจสอบคุณสมบัติของผู้สมัคร (ทั้งกรณีการจ้างเป็นพนักงาน ลูกจ้าง การว่าจ้างหน่วยงานภายนอกเพื่อปฏิบัติงานให้ รพม. รวมทั้งนิสิตนักศึกษาฝึกงาน) โดยผู้สมัครต้องไม่เคยกระทำผิดกฎหมาย ระเบียบ ข้อบังคับ หรือจริยธรรม รวมทั้งไม่มีประวัติในการบุกรุก แก่ไข ทำลาย หรือโจรกรรมข้อมูลในระบบเทคโนโลยีสารสนเทศมาก่อน และมีคุณสมบัติตามที่ รพม. กำหนด
 - 1.2 การกำหนดเงื่อนไขการจ้างงาน (Terms and conditions of employment) การว่าจ้างให้มีเงื่อนไขการจ้างงานให้ครอบคลุมในเรื่องดังต่อไปนี้
 - 1.2.1 กำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศอย่างเป็นลายลักษณ์อักษร (Information security roles and responsibilities) แก่ผู้ใช้งาน โดยกำหนดให้สอดคล้องกับนโยบายความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของ รพม.
 - 1.2.2 กำหนดให้มีการลงนามในสัญญาว่าจะไม่เปิดเผยความลับของ รพม. (Non-Disclosure Agreement : NDA)
 - 1.2.3 ระบบเทคโนโลยีสารสนเทศที่สร้างหรือพัฒนาโดยผู้ใช้งานในระหว่างการว่าจ้างถือเป็นสินทรัพย์ของ รพม.

- 1.2.4 กำหนดความรับผิดชอบหรือบทลงโทษ หากผู้ใช้งานไม่ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รฟม. รวมทั้ง กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
2. การสร้างความมั่นคงปลอดภัยในระหว่างการจ้างงาน (During employment) เพื่อสร้างความตระหนักแก่ผู้ใช้งานเกี่ยวกับภัยที่เกี่ยวข้องกับการปฏิบัติงานสารสนเทศ รวมถึงให้ความรู้เพื่อให้สามารถป้องกันภัยดังกล่าวได้
 - 2.1 หน้าที่ในการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management responsibilities) ผู้บริหาร รฟม. ทุกระดับชั้นมีหน้าที่สนับสนุนและส่งเสริมเรื่องดังต่อไปนี้ แก่ผู้ใช้งาน
 - 2.1.1 ประกาศนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ รฟม. เป็นลายลักษณ์อักษรให้ทุกคนรับทราบและปฏิบัติตาม
 - 2.1.2 จูงใจให้ผู้ใช้งานปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ รฟม.
 - 2.1.3 สร้างความตระหนักถึงความมั่นคงปลอดภัยด้านสารสนเทศที่เกี่ยวข้องกับหน้าที่ความรับผิดชอบของตนเองและของ รฟม.
 - 2.2 การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่ผู้ใช้งาน (Information security awareness, education and training) การสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยอย่างสม่ำเสมอ
 - 2.2.1 ผู้ดูแลระบบต้องแจ้งเตือนภัยคุกคาม และช่องโหว่ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศแก่ผู้ใช้งานที่เกี่ยวข้อง นอกจากนี้ต้องแจ้งเตือนให้ผู้ใช้งานเพิ่มความระมัดระวังความเสี่ยงต่าง ๆ เช่น ไวรัสมัลแวร์ เทคนิคการหลอกล่อทางจิตวิทยา (Social engineering) และช่องโหว่ทางเทคนิค เป็นต้น
 - 2.2.2 ผทท. ต้องดำเนินการฝึกอบรม หรือประชาสัมพันธ์เพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศแก่ผู้ใช้งานเป็นประจำทุกปี
 - 2.2.3 ผทท. ต้องแจ้งผู้ใช้งานให้ทราบ เมื่อมีการเปลี่ยนแปลงนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศของ รฟม. รวมทั้งอธิบายผลกระทบจากการเปลี่ยนแปลงดังกล่าว
 - 2.3 การกำหนดบทลงโทษ
 - 2.3.1 ความรับผิดชอบตามกฎหมาย
นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ไม่ได้ก่อให้เกิดสิทธิ์ทางกฎหมายที่ทำให้ผู้ใช้งานพ้นผิดแม้จะได้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ และผู้ใช้งานตกลงยินยอมที่จะไม่ดำเนินการใด ๆ ทางกฎหมายต่อ รฟม. ซึ่งได้ปฏิบัติตามระเบียบนี้ แต่อย่างไรก็ตามหากผู้ใช้งานกระทำการละเมิดหรือกระทำผิดตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ อาจเป็นความผิดทางวินัยและเป็นเหตุให้ถูกลงโทษทางวินัยได้ รฟม. ไม่มีส่วนรับผิดชอบต่อการละเมิดทรัพย์สินทางปัญญาที่เกิดจากการใช้ระบบคอมพิวเตอร์

2.3.2 การพิจารณาโทษผู้กระทำผิด

ผู้ใช้งานที่กระทำความผิด ฝ่าท. จะเพิกถอนสิทธิ์การใช้งานและอาจเป็นความผิดทางวินัย หรือความผิดตามกฎหมายที่เกี่ยวข้อง

- 1) พนักงาน/ลูกจ้างที่ฝ่าฝืนหรือละเมิดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รพม. ต้องถูกลงโทษตามกระบวนการทางวินัยของ รพม. รวมถึงกฎหมายที่เกี่ยวข้อง
- 2) หน่วยงานภายนอกที่กระทำความผิด จะมีโทษตามที่ระบุไว้ในสัญญาหรือถูกเพิกถอนสิทธิ์การใช้งาน รวมถึงดำเนินการตามกฎหมายที่เกี่ยวข้อง

3. การสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน (Termination and change of employment)

เพื่อกำหนดหน้าที่ความรับผิดชอบเมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน ซึ่งรวมถึงการคืนทรัพย์สินและการถอดถอนสิทธิ์ในการเข้าถึง

3.1 การแจ้งการสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน

3.1.1 ฝ่ายทรัพยากรบุคคลต้องแจ้งให้ฝ่ายเทคโนโลยีสารสนเทศทราบทันทีหากพนักงานมีการลาออก โยกย้าย เกษียณ หรือเสียชีวิต เพื่อฝ่ายเทคโนโลยีสารสนเทศจะได้ตรวจสอบและบริหารจัดการสิทธิ์ในการเข้าถึงระบบเทคโนโลยีสารสนเทศ

3.1.2 ฝ่าย/สำนัก ที่กำกับดูแลงานที่มีการว่าจ้างหน่วยงานภายนอก ต้องแจ้งให้ฝ่ายเทคโนโลยีสารสนเทศทราบทันทีในกรณีที่ผู้รับจ้างภายนอกสิ้นสุดสัญญาจ้างหรือมีการยกเลิกสัญญาจ้างเพื่อให้ ฝ่าท. ตรวจสอบการใช้งานระบบสารสนเทศและถอดถอนสิทธิ์ในการเข้าถึงระบบสารสนเทศของ รพม.

3.2 การคืนสินทรัพย์ของ รพม.

ผู้ดูแลระบบต้องตรวจสอบเพื่อเรียกคืนสินทรัพย์ของ รพม. จากผู้ใช้งาน เมื่อการสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน

3.3 การถอดถอนสิทธิ์ในการเข้าถึง

3.3.1 ผู้ดูแลระบบต้องถอดถอนสิทธิ์ในการเข้าถึงของผู้ใช้งาน เมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน

3.3.2 การถอดถอนสิทธิ์ในการเข้าถึงหมายถึงทางกายภาพ (Physical) และทางตรรกะ (Logical) เช่น กุญแจ บัตรแสดงตน บัตรประจำตัวผู้ใช้งาน และบัญชีผู้ใช้งาน เป็นต้น

3.3.3 ในกรณีที่ผู้ใช้งานที่สิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน มีการใช้บัญชีผู้ใช้งานร่วมกับ (Shared user ID) กับผู้ใช้งานอื่น ผู้บังคับบัญชาต้องเปลี่ยนรหัสผ่านทันทีหลังจากสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน

ส่วนที่ 23

การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

วัตถุประสงค์

- เพื่อควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าถึงอาคารสถานที่ และพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area)

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้อำนวยการฝ่ายจัดซื้อและบริการ

อ้างอิงมาตรฐาน

- หมวดที่ 7 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security)

แนวปฏิบัติ

1. ผู้ดูแลระบบ ต้องออกแบบ และติดตั้งอุปกรณ์หรือระบบสนับสนุน (Facilities) เพื่อป้องกันการรักษาความมั่นคงปลอดภัยด้านกายภาพ เช่น อุปกรณ์ดับเพลิง ระบบสำรองไฟฟ้า เครื่องกำเนิดไฟฟ้า ระบบปรับอากาศและควบคุมความชื้น ระบบเตือนภัยน้ำรั่ว และต้องมีการบำรุงรักษาอย่างสม่ำเสมอ
2. ผู้ดูแลระบบต้องติดตั้งอุปกรณ์สารสนเทศในตู้แร็ก (Rack) หรือสถานที่ที่มีความมั่นคงปลอดภัยและมีการปิดล็อก
3. ผู้ดูแลระบบ ต้องมีการป้องกันสายเคเบิลที่ใช้เพื่อการสื่อสารหรือสายไฟ มิให้มีการดักจับสัญญาณ (Interception) หรือมีความเสียหายเกิดขึ้น โดยจะต้องเดินสายเคเบิลผ่านท่อร้อยสายหรือทางเดินสายที่มีความมั่นคงปลอดภัยจากการเข้าถึง และไม่เดินสายผ่านพื้นที่ที่เข้าถึงได้อย่างสาธารณะ รวมทั้งสายเคเบิลสื่อสารและสายไฟฟ้าต้องแยกจากกันโดยมีระยะห่างที่เหมาะสม
4. การกำหนดบริเวณที่มีการรักษาความมั่นคงปลอดภัย
กำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม เพื่อเป็นการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้ โดยแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศออกเป็น
 - 4.1 พื้นที่ทำงาน (Working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน
 - 4.2 พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) หมายถึง พื้นที่ศูนย์ของข้อมูล (Data center)
5. การควบคุมการเข้าออก อาคาร สถานที่
 - 5.1 กำหนดสิทธิของผู้ใช้งานและหน่วยงานภายนอกในการเข้าถึงสถานที่ โดยแบ่งแยกได้ ดังนี้
 - 5.1.1 ผู้ดูแลระบบต้องกำหนดสิทธิแก่ผู้ใช้งานที่มีสิทธิ์เข้า - ออก และกำหนดช่วงระยะเวลาที่มีสิทธิ์ในการเข้า - ออกแต่ละพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศอย่างชัดเจน
 - 5.1.2 เจ้าหน้าที่รักษาความปลอดภัย (รปภ.) จะต้องให้หน่วยงานภายนอกหรือบุคคลภายนอกแลกบัตรที่สามารถระบุตัวตนของบุคคลนั้น ๆ ก่อนเข้าถึงอาคารของ รพม. เช่น บัตรประจำตัวประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วบันทึกข้อมูลบัตรในสมุดบันทึกหรือระบบงานสารสนเทศ

- 5.1.3 หน่วยงานภายนอกที่มาติดต่อต้องติดบัตรผู้ติดต่อ (Visitor) ตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ใน รพม. และคืนบัตรผู้ติดต่อ (Visitor) ก่อนออกจากอาคารของ รพม.
- 5.1.4 เจ้าหน้าที่รักษาความปลอดภัย (รปภ.) ต้องตรวจสอบผู้ติดต่อ อุปกรณ์ พร้อมลงเวลาออกที่สมุดบันทึกหรือระบบสารสนเทศให้ถูกต้อง
- 5.2 ผู้ดูแลระบบ ต้องควบคุมการเข้า - ออกพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) ไม่ให้ผู้ไม่มีสิทธิ์เข้าถึงได้ โดยกำหนดพื้นที่การส่งมอบสินค้าและพื้นที่การเตรียมหรือประกอบอุปกรณ์สารสนเทศ (Unpack Area) ก่อนนำเข้าพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) และต้องควบคุมการเข้า - ออก เพื่อหลีกเลี่ยงการเข้าถึงระบบสารสนเทศและข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต โดยปฏิบัติตามขั้นตอนที่ รพม. กำหนด

ส่วนที่ 4 การจัดการทรัพย์สิน

วัตถุประสงค์

- เพื่อบริหารจัดการทรัพย์สินสารสนเทศ ตั้งแต่การจัดการ การใช้งาน จนถึงการยกเลิกใช้งาน โดยมีการระบุสินทรัพย์ขององค์กรและกำหนดหน้าที่ความรับผิดชอบในการปกป้องทรัพย์สินสารสนเทศอย่างเหมาะสม

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- เจ้าของข้อมูล
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 4 การบริหารจัดการทรัพย์สิน (Asset management)

แนวปฏิบัติ

1. หน้าที่ความรับผิดชอบต่อทรัพย์สินสารสนเทศ (Responsibility for assets)
 - 1.1 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องร่วมกันจัดทำบัญชีทรัพย์สิน/ทะเบียนทรัพย์สิน (Asset inventory) และทบทวนทะเบียนทรัพย์สินอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ
 - 1.2 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องระบุเจ้าของทรัพย์สินสารสนเทศทุกรายการ เพื่อรับผิดชอบดูแลความมั่นคงปลอดภัยสารสนเทศตลอดวงจรอายุการใช้งาน
 - 1.3 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องเรียกคืนทรัพย์สินสารสนเทศเมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน
 - 1.4 ผู้ใช้งานต้องใช้ทรัพย์สินสารสนเทศของ รพม. อย่างระมัดระวัง และใช้เพื่อปฏิบัติงานของ รพม. เท่านั้น รวมทั้งต้องปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ และนโยบาย ของ รพม.
2. การจำแนกประเภทของทรัพย์สินสารสนเทศ (Asset classification)
 - 2.1 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจำแนกประเภททรัพย์สินตามขั้นตอนที่ รพม. กำหนด และทบทวนการจำแนกดังกล่าวอย่างสม่ำเสมอ
 - 2.2 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจัดทำป้ายชื่อทรัพย์สินสารสนเทศ (Labeling) ให้ชัดเจน พร้อมทั้งจัดให้มีมาตรการดูแลรักษาความมั่นคงปลอดภัยสารสนเทศที่สอดคล้องกับประเภททรัพย์สินตามระดับชั้นความลับที่ รพม. กำหนด
3. การจัดการสื่อบันทึกข้อมูล (Media handling)
 - 3.1 เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ใช้งานต้องควบคุมการใช้งานและจัดเก็บสื่อบันทึกแบบถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้ (Removable media) ตามที่ รพม. กำหนด
 - 3.2 เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล เพิ่มข้อมูลตามขั้นตอนที่ รพม. กำหนด โดยไม่สามารถกู้คืนข้อมูลกลับมาได้อีกก่อนจะกำจัดอุปกรณ์ดังกล่าวหรือ

ก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อเพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลที่สำคัญได้ โดยพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีทำลาย
กระดาษ	ให้หั่นด้วยเครื่องทำลายเอกสาร
Flash Drive	1) ทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD5220.22M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นการเขียนทับข้อมูลเดิมหลายรอบ 2) ใช้วิธีทุบหรือบดให้เสียหาย
แผ่น CD/DVD	ให้หั่นด้วยเครื่องทำลายเอกสาร
เทป	ใช้วิธีทุบหรือบดให้เสียหายหรือเผาทำลาย
ฮาร์ดดิสก์	1) ทำลายข้อมูลบนฮาร์ดดิสก์ตามมาตรฐาน DOD5220.22M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นการเขียนทับข้อมูลเดิมหลายรอบ 2) ใช้วิธีทุบหรือบดให้เสียหาย

- 3.3 เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ใช้งาน ต้องมีการป้องกันสื่อบันทึกข้อมูลที่ใช้จัดเก็บข้อมูลสารสนเทศ ในกรณีที่มีการเคลื่อนย้ายเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต ให้นำไปใช้งานผิดวัตถุประสงค์ รวมถึงป้องกันสื่อบันทึกข้อมูลไม่ให้เกิดความเสียหาย โดยรักษาความปลอดภัยสารสนเทศตามขั้นตอนที่ รพม. กำหนด

ส่วนที่ 5

การจัดทำ การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

วัตถุประสงค์

- เพื่อควบคุมการจัดทำ พัฒนา และบำรุงรักษาระบบสารสนเทศ ให้มีการกำหนดมาตรการการรักษาความมั่นคงปลอดภัย เพื่อป้องกันความผิดพลาด สูญหาย และการเปลี่ยนแปลงแก้ไขระบบ

ผู้รับผิดชอบ

- ผู้บังคับบัญชา
- ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

- หมวดที่ 10 โครงสร้างการจัดทำ การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (System acquisition, development and maintenance)
- หมวดที่ 11 ความสัมพันธ์กับหน่วยงานภายนอก (Supplier relationships)

แนวปฏิบัติ

1. ผู้บังคับบัญชา ต้องควบคุมให้มีการกำหนดข้อตกลงและความรับผิดชอบที่เกี่ยวข้องกับความเสถียรด้านความมั่นคงปลอดภัยสารสนเทศลงในสัญญากับผู้ให้บริการภายนอก โดยให้ครอบคลุมรวมถึงผู้รับจ้างช่วงด้วย
2. ผู้บังคับบัญชาต้องควบคุมให้มีข้อตกลง (Sign off) ก่อนเริ่มใช้งานระบบจริง (Production) หรือก่อนเริ่ม Go live
3. ผู้ดูแลระบบ ต้องจัดทำข้อกำหนดโดยระบุถึงการควบคุมความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร เช่น วิธีการแบบปลอดภัยในการพัฒนาโปรแกรมตามมาตรฐาน OWASP (Open Web Application Security Project) Top 10 หรือมาตรฐาน CWE (Common Weakness Enumeration) Top 25 หรือมาตรฐานที่ยอมรับในสากล
4. ผู้ดูแลระบบ ต้องมีการออกแบบระบบเพื่อตรวจสอบข้อมูลที่จะรับเข้าสู่แอปพลิเคชัน ข้อมูลที่เกิดจากการประมวลผล และข้อมูลที่อยู่ระหว่างการประมวลผล เพื่อตรวจหาและป้องกันความไม่ถูกต้องที่เกิดขึ้นกับข้อมูล เช่น หน่วยความจำล้น (Buffer overflows) การใช้ตัวแปรผิดประเภท และต้องมีมาตรการป้องกันหรือควบคุมความล้มเหลวระหว่างการประมวลผล (Rollback)
5. ผู้ดูแลระบบต้องมีการควบคุมการเข้าถึงและควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบตามขั้นตอนที่ รพม. กำหนดเพื่อควบคุมผลกระทบที่เกิดขึ้น
6. ผู้ดูแลระบบต้องจำกัดให้มีการเปลี่ยนแปลงใด ๆ ต่อซอฟต์แวร์ที่ใช้งาน (Software package) โดยเปลี่ยนแปลงเฉพาะที่จำเป็นเท่านั้น และควบคุมทุก ๆ การเปลี่ยนแปลงอย่างเข้มงวดตามขั้นตอนที่ รพม. กำหนด
7. ผู้ดูแลระบบต้องจำกัดการเข้าถึง Source code ให้เข้าถึงได้เฉพาะผู้ที่มีสิทธิ์เท่านั้น
8. ผู้ดูแลระบบต้องจัดทำ Source code review เพื่อหาข้อผิดพลาดหรือสิ่งผิดปกติและปรับปรุง Source code ให้มีคุณภาพ
9. ผู้ดูแลระบบต้องปิดบังข้อมูลส่วนบุคคล (Data Masking) ที่จัดเก็บอยู่ในระบบงานสารสนเทศด้วยวิธีการที่เหมาะสม

10. ผู้ดูแลระบบต้องแสดงข้อมูลของผู้ใช้งานอย่างรัดกุม เช่น การปิดบังข้อมูลสำคัญของผู้ใช้งาน (Sensitive data masking) เป็นต้น
11. กรณีของแอปพลิเคชันที่ใช้งานผ่านอุปกรณ์เคลื่อนที่ (Mobile device) ให้ผู้ดูแลระบบดำเนินการ ดังนี้
 - 11.1 ปิดบังหน้าจอเมื่อย่อแอปพลิเคชัน (Application blurring) เพื่อลดความเสี่ยงที่ข้อมูลสำคัญของผู้ใช้งานจะรั่วไหล
 - 11.2 ขอสติธิ์เข้าถึงทรัพยากรหรือบริการโดยแอปพลิเคชัน (Application permission) บนอุปกรณ์เคลื่อนที่ของผู้ใช้งานเท่าที่จำเป็น และมีกระบวนการทบทวนการขอสติธิ์เป็นประจำเพื่อป้องกันการละเมิดสิทธิความเป็นส่วนตัวของผู้ใช้งาน
12. ผู้ดูแลระบบต้องควบคุมข้อมูลที่นำมาใช้ในการทดสอบระบบ (Test data) อย่างเหมาะสม โดยไม่นำข้อมูลจริงมาทดสอบ กรณีจำเป็นต้องใช้ข้อมูลจริงต้องได้รับอนุญาตข้อมูลจากเจ้าของก่อนนำมาใช้งาน และทำลายข้อมูลอย่างเหมาะสมตามขั้นตอนที่ รพม. กำหนด
13. ผู้ดูแลระบบต้องแยกระบบสารสนเทศสำหรับการพัฒนา ทดสอบ และใช้งานจริงออกจากกันเพื่อลดความเสี่ยงที่เกิดจากการเปลี่ยนแปลงระบบสารสนเทศโดยไม่ได้รับอนุญาต และต้องมีการกำหนดสิทธิการเข้าถึงระบบสารสนเทศที่พัฒนา ทดสอบ หรือใช้งานจริง ทั้งระบบสารสนเทศใหม่ และการปรับปรุงแก้ไขระบบสารสนเทศเดิม
14. ผู้ดูแลระบบต้องมีการกำหนดขั้นตอนการทดสอบระบบสารสนเทศก่อนนำไปใช้งานจริง ทั้งในกรณีปรับปรุงระบบสารสนเทศเดิมและการพัฒนาระบบสารสนเทศใหม่
15. ผู้ดูแลระบบต้องติดตั้งซอฟต์แวร์บนระบบสารสนเทศที่ให้บริการ (Production) ตามขั้นตอนที่ รพม. กำหนด และจำกัดสิทธิการติดตั้งซอฟต์แวร์เพื่อให้ระบบสารสนเทศต่าง ๆ มีความถูกต้องครบถ้วนและน่าเชื่อถือ
16. ผู้ดูแลระบบต้องนำซอฟต์แวร์ที่ไม่ละเมิดลิขสิทธิ์มาติดตั้งบนระบบสารสนเทศที่ให้บริการ (Production)
17. ผู้ดูแลระบบต้องกำกับดูแลให้ผู้รับจ้างปฏิบัติตามสัญญาหรือข้อตกลงการให้บริการที่ระบุไว้ โดยครอบคลุมถึงด้านความมั่นคงปลอดภัยสารสนเทศ และการปฏิบัติตามขั้นตอนที่เกี่ยวข้องต่าง ๆ ที่ รพม. กำหนดไว้
18. ผู้ดูแลระบบ ต้องติดตาม ตรวจสอบรายงาน หรือบันทึกการให้บริการของบุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามสัญญาว่าจ้างอย่างสม่ำเสมอ
19. ผู้ดูแลระบบ ต้องดูแลให้ทรัพย์สินสารสนเทศได้รับการบำรุงรักษาและซ่อมแซมตามความต้องการ รวมทั้งต้องมีการบันทึกประวัติการทำงานผิดปกติ การบำรุงรักษา และการซ่อมแซมอุปกรณ์นั้น ๆ อย่างสม่ำเสมอ
20. ผู้ดูแลระบบจะต้องปิดช่องโหว่ของระบบสารสนเทศที่มีระดับความรุนแรงในระดับวิกฤติ (Critical) และระดับความรุนแรงระดับสูง (High) ทั้งหมดก่อนนำไปใช้งานจริง (Production) หรือก่อนเริ่ม Go live โดยเฉพาะระบบที่ให้บริการผ่านเครือข่ายอินเทอร์เน็ต (Internet facing) และระบบที่มีความสำคัญต่อการดำเนินงานของ รพม.
21. ผู้ดูแลระบบต้องพิจารณาเลือกใช้ Version ของ Software ดังนี้
 - 21.1 กรณีนำ Software เดิมมาใช้ในการจัดหาหรือพัฒนาระบบ จะต้องนำผลการตรวจสอบช่องโหว่และผลการทดสอบเจาะระบบมาประกอบการพิจารณาคัดเลือกเวอร์ชันของ Software ด้วย เพื่อป้องกันไม่ให้เกิดช่องโหว่เดิมรวมถึงเพื่อลดภาระงานในการปิดช่องโหว่เดิมซ้ำ
 - 21.2 กรณีเป็น Software ที่ไม่เคยนำมาใช้งานให้เลือกใช้ Software เวอร์ชันล่าสุด

ส่วนที่ 6

การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

- เพื่อควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศตั้งแต่การกำหนดสิทธิ์ กำหนดประเภทของข้อมูล จัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ระดับชั้นการเข้าถึง เวลาที่เข้าถึงได้ และช่องทางการเข้าถึง ทั้งนี้เพื่อควบคุมและป้องกันการเข้าถึง การลวงรู้ และการแก้ไขระบบสารสนเทศของ รพม. โดยไม่ได้รับอนุญาต

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- เจ้าของข้อมูล
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 5 การควบคุมการเข้าถึง (Access control)
- หมวดที่ 8 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations security)
- หมวดที่ 9 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)

แนวปฏิบัติ

1. การควบคุมการเข้าถึงระบบสารสนเทศ (Access control)
 - 1.1 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องร่วมกันกำหนดสิทธิ์ในการเข้าถึงระบบสารสนเทศ (Authorization matrix) ที่เหมาะสมและสอดคล้องกับหน้าที่ความรับผิดชอบของผู้ใช้งาน และทบทวนเมื่อมีการเปลี่ยนแปลง
 - 1.2 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องร่วมกันกำหนดระดับการอนุมัติ (Authorization level) การเข้าถึงระบบเทคโนโลยีสารสนเทศ
 - 1.3 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจัดให้มีการแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties) ในการเข้าถึงระบบเทคโนโลยีสารสนเทศอย่างเหมาะสม เช่น มีการแบ่งแยกหน้าที่ระหว่างการแจ้งความประสงค์ การเข้าถึงและการอนุมัติการเข้าถึง เป็นต้น
 - 1.4 กรณีของแอปพลิเคชันที่ใช้งานผ่านอุปกรณ์เคลื่อนที่ (Mobile device) ผู้ดูแลระบบต้องปฏิบัติ ดังนี้
 - 1.4.1 ไม่อนุญาตให้อุปกรณ์เคลื่อนที่ที่ใช้ระบบปฏิบัติการล้าสมัย (Obsolete operating system) ใช้งานแอปพลิเคชัน หรือหากอนุญาตให้ใช้บริการได้ควรมีมาตรการรองรับเพื่อลดความเสี่ยงที่ รพม. จะได้รับรวมถึงลดผลกระทบต่อผู้ใช้งานตามความเหมาะสม เช่น การเพิ่มมาตรการยืนยันตัวตน เป็นต้น
 - 1.4.2 ไม่อนุญาตให้อุปกรณ์ที่มีการปรับแต่งการเข้าถึงระบบปฏิบัติการ (rooted/jailbroken) ใช้งานแอปพลิเคชัน เพื่อลดความเสี่ยงที่ผู้ไม่ประสงค์ดีสามารถเข้าถึงข้อมูลสำคัญของผู้ใช้งานและละเมิดหรือหลีกเลี่ยงมาตรการการรักษาความมั่นคงปลอดภัยที่ รพม. กำหนดไว้
 - 1.4.3 ไม่อนุญาตให้ผู้ใช้งานใช้แอปพลิเคชันเวอร์ชันต่ำกว่าที่ รพม. กำหนด เพื่อให้แอปพลิเคชันมีการรักษาความมั่นคงปลอดภัยเป็นไปตามมาตรฐานของ รพม.

1.5 ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ใช้งาน ต้องปฏิบัติ ดังนี้

1.5.1 แบ่งประเภทข้อมูล ดังนี้

- 1) ข้อมูลและสารสนเทศสำหรับสนับสนุนการตัดสินใจของผู้บริหาร ได้แก่ ข้อมูลสารสนเทศที่มีความสำคัญหรือมีความจำเป็นเร่งด่วนที่ต้องติดตามอย่างใกล้ชิดเพื่อประกอบการตัดสินใจเชิงนโยบาย กำหนดนโยบาย และการวางแผนของผู้บริหารระดับสูง
- 2) ข้อมูลและสารสนเทศสนับสนุนเชิงยุทธศาสตร์ (Strategy data) ได้แก่ ข้อมูลและสารสนเทศเชิงวิชาการเพื่อสนับสนุนการดำเนินงานตามพันธกิจและยุทธศาสตร์ของ รพม. ให้บรรลุเป้าหมาย รวมทั้งข้อมูลที่เผยแพร่แก่ผู้รับบริการภายนอก
- 3) ข้อมูลและสารสนเทศที่สนับสนุนการปฏิบัติงานประจำ (Operation data) ได้แก่ ข้อมูลที่สนับสนุนการทำงานทั่วไปของ รพม.

1.5.2 จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น 3 ระดับ คือ

- 1) ข้อมูลที่มีระดับความสำคัญมาก หมายถึง ข้อมูลที่ใช้สำหรับสนับสนุนการตัดสินใจของผู้บริหาร
- 2) ข้อมูลที่มีระดับความสำคัญปานกลาง หมายถึง ข้อมูลที่ใช้ปฏิบัติงานเฉพาะกลุ่มงาน แผนก กอง หรือฝ่ายภายในองค์กร
- 3) ข้อมูลที่มีระดับความสำคัญน้อย หมายถึง ข้อมูลที่พนักงาน/ลูกจ้างภายใน รพม. สามารถเข้าถึงร่วมกันได้หรือสามารถเผยแพร่ได้

1.5.3 จัดแบ่งลำดับชั้นความลับของข้อมูลตามที่ รพม. กำหนด

1.5.4 จัดแบ่งระดับชั้นการเข้าถึง

- 1) ระดับชั้นสำหรับผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และภารกิจที่ได้รับมอบหมาย
- 2) ระดับชั้นสำหรับผู้ปฏิบัติงานทั่วไป เข้าถึงข้อมูลที่ได้รับมอบหมายตามอำนาจหน้าที่
- 3) ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย มีสิทธิ์ในการบริหารจัดการระบบและเข้าถึงข้อมูลที่ได้รับมอบหมายตามอำนาจหน้าที่

1.6 เจ้าของข้อมูลและผู้ดูแลระบบต้องกำหนดเวลาการเข้าถึงระบบสารสนเทศ

1.7 ผู้ดูแลระบบต้องจำกัดช่องทางการเข้าถึงระบบเทคโนโลยีสารสนเทศตามช่องทาง ดังนี้

- 1) เครือข่ายภายในของ รพม.
- 2) เครือข่ายภายนอก รพม.
- 3) เครือข่ายอื่นที่จัดไว้ให้ เช่น ระบบเครือข่ายสื่อสารข้อมูล GIN

1.7 ผู้ดูแลระบบต้องกำกับดูแล Default permission ของไฟล์ (File) และ โฟลเดอร์ (Folder) ที่สร้างขึ้นให้มีการจำกัดสิทธิ์ในการเข้าถึง

1.8 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องพิจารณาข้อกำหนดต่าง ๆ ที่มีผลทางกฎหมายซึ่งเกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศของ รพม. เช่น พระราชบัญญัติ ข้อกำหนดทางกฎหมาย ข้อกำหนดในสัญญา

และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่น ๆ เป็นต้น เพื่อกำหนดสิทธิ์การเข้าถึงสารสนเทศและระบบเทคโนโลยีสารสนเทศของ รพม.

- 1.9 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องมีการสอบทานสิทธิ์ในการเข้าถึงระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ พร้อมทั้งเพิกถอนสิทธิ์เมื่อพบเห็นสิทธิ์ที่ไม่ถูกต้องตามสิทธิ์ในการเข้าถึง (Authorization matrix)
2. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)
ให้มีการควบคุมการลงทะเบียนผู้ใช้งาน การบริหารจัดการรหัสผ่าน การบริหารจัดการสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศ และการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน
 - 2.1 การลงทะเบียนผู้ใช้งาน (User registration)
 - 2.1.1 ผู้ดูแลระบบต้องบริหารจัดการและควบคุมบัญชีชื่อผู้ใช้งาน (Username) มิให้มีการใช้งานบัญชีชื่อผู้ใช้งานซ้ำกัน ทั้งนี้ ในส่วนของพนักงาน/ลูกจ้าง รพม. ให้กำหนดชื่อผู้ใช้งาน (Username) ตามมาตรฐานจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ใช้ในองค์กร
 - 2.1.2 เจ้าของข้อมูลต้องเป็นผู้อนุมัติการสร้างบัญชีผู้ใช้งานชั่วคราว (Temporary user) และต้องจำกัดช่วงเวลาการใช้งานเท่าที่จำเป็น
 - 2.2 การบริหารจัดการรหัสผ่าน (User password management)
 - 2.2.1 ผู้ดูแลระบบและผู้รับจ้าง ต้องกำหนดความยาวรหัสผ่านอย่างน้อย 12 หลัก
 - 2.2.2 บุคลากรของ รพม. (พนักงาน/ลูกจ้างของ รพม.) ต้องกำหนดความยาวรหัสผ่านอย่างน้อย 8 หลัก
 - 2.2.3 ผู้ดูแลระบบกำหนดรหัสผ่านแบบชั่วคราวโดยใช้วิธีการสุ่ม และบังคับให้มีการเปลี่ยนรหัสผ่านเมื่อผู้ใช้งานเข้าใช้งานระบบในครั้งแรก (บังคับใช้เฉพาะกรณีข้อ 2.2.1 – 2.2.2)
 - 2.2.4 ผู้ดูแลระบบและผู้รับจ้าง รวมถึงบุคลากรของ รพม. (พนักงาน/ลูกจ้างของ รพม.) ตามข้อ 2.2.1 – 2.2.2 ต้องปฏิบัติเพิ่มเติม ดังนี้
 - 1) รหัสผ่านประกอบด้วย ตัวอักษร ตัวเลข และอักขระพิเศษ เช่น (a-Z) (0-9) (@ , # , & , “ , ‘ , * , = , < , > , % , \$, + , ?) เป็นต้น
 - 2) กำหนดรหัสผ่านที่ง่ายต่อการจดจำ แต่ต้องไม่เป็นคำที่สามารถคาดเดาได้ง่าย เช่น คำที่อยู่ในพจนานุกรม “qwerty” “abcde” “12345” ชื่อ-นามสกุล วันเดือนปีเกิด ที่อยู่ หรือเบอร์โทรศัพท์ เป็นต้น
 - 3) ต้องไม่ใช้งานรหัสผ่านโดยกระบวนการเข้าใช้งานโดยอัตโนมัติ ได้แก่ การกำหนดค่า “Remember Password” เป็นต้น
 - 4) ต้องเก็บรหัสผ่านไว้เป็นความลับเฉพาะบุคคล ไม่เปิดเผยให้ผู้อื่นรับทราบ และไม่พิมพ์รหัสผ่านในลักษณะเปิดเผย เช่น พิมพ์รหัสผ่านต่อหน้าผู้ใช้งานคนอื่น เป็นต้น
 - 5) ต้องไม่ใช้บัญชีชื่อผู้ใช้งานและรหัสผ่านร่วมกันกับผู้อื่น แม้ว่าบัญชีชื่อผู้ใช้งานจะได้รับการอนุญาตจากเจ้าของชื่อผู้ใช้งานบุคคลนั้นก็ตาม
 - 6) ต้องเปลี่ยนแปลงรหัสผ่านเป็นประจำอย่างน้อยทุก 6 เดือน
 - 7) ต้องเปลี่ยนแปลงรหัสผ่านเมื่อมีการแจ้งเตือนจากระบบ หรือสงสัยว่ารหัสผ่านลวงรู้โดยบุคคลอื่น
 - 2.2.5 ผู้ดูแลระบบ ต้องกำหนดให้มีการเข้ารหัสข้อมูลรหัสผ่านในระบบ
 - 2.2.6 ผู้ดูแลระบบ ต้องจัดให้มีการควบคุมรหัสผ่านอย่างเข้มงวด

- 2.2.7 ผู้ดูแลระบบต้องจัดส่งบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ด้วยวิธีการที่ปลอดภัย
- 2.2.8 ผู้ดูแลระบบต้องควบคุมดูแลระบบปฏิบัติการ ฐานข้อมูล และระบบงานสารสนเทศ (Application) ที่จัดเก็บบัญชีผู้ใช้งานและรหัสผ่านอย่างเข้มงวด โดยให้เข้าถึงได้เฉพาะผู้ดูแลระบบที่ได้รับอนุญาตเท่านั้น
- 2.2.9 ผู้ดูแลระบบต้องกำหนดวิธีการหรือกระบวนการยืนยันตัวตนที่ปลอดภัย เช่น กรณีที่ลืมรหัสผ่าน
- 2.2.10 ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานภายนอกที่สมัครใช้บริการระบบงานสารสนเทศของ รพม. ใช้รหัสผ่านอย่างมั่นคงปลอดภัย ดังนี้

กรณีแอปพลิเคชันทั่วไป

- 1) กำหนดความยาวรหัสผ่านอย่างน้อย 8 หลัก ซึ่งประกอบด้วย ตัวอักษร ตัวเลข และอักขระพิเศษ เช่น (a-Z) (0-9) (@ , # , & , “ , ‘ , * , = , < , > , % , \$, + , ?) เป็นต้น
- 2) ไม่บังคับให้เปลี่ยนรหัสผ่าน ทั้งนี้ขึ้นอยู่กับความสมัครใจในการเปลี่ยนรหัสผ่าน และระบบต้องรองรับการเปลี่ยนรหัสผ่านในกรณีต่าง ๆ ด้วยวิธีการที่ปลอดภัย

กรณีแอปพลิเคชันที่ใช้งานผ่านอุปกรณ์เคลื่อนที่ (Mobile device)

- 1) กำหนดรหัสผ่านโดยใช้ PIN code หรือรหัสผ่านที่ซับซ้อน (PIN/Password complexity) โดยกรณี PIN code ต้องใช้รหัสผ่าน 6 หลักขึ้นไป
- 2) ไม่บังคับให้เปลี่ยนรหัสผ่าน ทั้งนี้ขึ้นอยู่กับความสมัครใจในการเปลี่ยนรหัสผ่าน และระบบต้องรองรับการเปลี่ยนรหัสผ่านในกรณีต่าง ๆ ด้วยวิธีการที่ปลอดภัย

2.3 การบริหารจัดการสิทธิ์ (Privilege management)

- 2.3.1 ผู้บังคับบัญชาต้องกำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียน การเพิกถอนสิทธิ์ การเปลี่ยนแปลงสิทธิ์ และการทบทวนสิทธิ์ของผู้ใช้งานอย่างเป็นลายลักษณ์อักษร
- 2.3.2 กำหนดสิทธิ์ที่เหมาะสมกับผู้ใช้งานตามความจำเป็นและสอดคล้องกับหน้าที่ความรับผิดชอบและจัดเก็บประวัติ (Log) การลงทะเบียน การเพิกถอนสิทธิ์ และการเปลี่ยนแปลงสิทธิ์ของผู้ใช้งาน
- 2.3.3 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจัดให้มีการควบคุมและจำกัดสิทธิ์ในการทำงานระบบตามความจำเป็นในการใช้งานเท่านั้น
 - 1) สิทธิ์ในการสร้างข้อมูล (Create)
 - 2) สิทธิ์ในการอ่านข้อมูลหรือเรียกดูข้อมูล (READ)
 - 3) สิทธิ์ในการปรับปรุงข้อมูล (Modify / Update)
 - 4) สิทธิ์ในการลบข้อมูล (Delete)
 - 5) สิทธิ์ในการมอบหมายสิทธิ์ในการดำเนินการแทน (Assign)
 - 6) สิทธิ์ในการรับรองความถูกต้องครบถ้วนของข้อมูล (Approve/Authenticate)
 - 7) ไม่มีสิทธิ์
- 2.3.4 เจ้าของข้อมูลและผู้ดูแลระบบต้องเป็นผู้อนุมัติการให้สิทธิ์เพื่อเข้าถึงสารสนเทศหรือระบบเทคโนโลยีสารสนเทศใด ๆ อย่างเป็นลายลักษณ์อักษร

- 2.3.5 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจำกัดจำนวนผู้ใช้งานที่ทำหน้าที่เป็นผู้ให้สิทธิ์กับผู้ใช้งาน ให้น้อยที่สุดตามความเหมาะสม
- 2.3.6 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจำกัดระยะเวลาการใช้งานระบบเทคโนโลยีสารสนเทศของ รพม. แก่หน่วยงานภายนอกที่เข้ามาปฏิบัติงานร่วมกับ รพม.
- 2.3.7 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจัดให้มีการถอดถอนหรือเปลี่ยนแปลงสิทธิ์การเข้าถึงทันที เมื่อผู้ใช้งานเกษียณ เปลี่ยนแปลงหน้าที่ความรับผิดชอบ เปลี่ยนแปลงการจ้างงาน หรือไม่มีความจำเป็น ในการใช้งานระบบเทคโนโลยีสารสนเทศ
- 2.3.8 ผู้ดูแลระบบต้องลบหรือระงับการใช้งานสิทธิ์ของผู้ใช้งานที่มาจากระบบ (Default user) ในกรณีที่มีความจำเป็นต้องใช้งานต้องกำหนดรหัสผ่านอย่างมั่นคงปลอดภัย
- 2.4 การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of user access rights)
 - 2.4.1 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องมีการสอบทานสิทธิ์การเข้าถึงของผู้ใช้งานระบบ เมื่อ รพม. มีการเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศหรือโครงสร้างองค์กร
 - 2.4.2 ผู้ดูแลระบบ ต้องมีการสอบทานและระงับการใช้งานบัญชีผู้ใช้งานที่ไม่ได้ใช้งานเกิน 180 วัน หากผู้ใช้งานต้องการกลับมาใช้งานจะต้องยืนยันตัวตนให้ ผทท. ทราบ ทั้งนี้ ระยะเวลาที่ไม่ได้ใช้งานของ บัญชีผู้ใช้งานอาจจะขึ้นอยู่กับแต่ละระบบสารสนเทศ
3. การป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล และการควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ไม่ปลอดภัย
 - 3.1 การป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล (Unattended user equipment)
 - 3.1.1 ผู้ดูแลระบบต้องจัดให้มีมาตรการสำหรับป้องกันระบบคอมพิวเตอร์ ระบบเครือข่ายสื่อสาร ข้อมูล และระบบเทคโนโลยีสารสนเทศ โดยการกำหนดค่าของระบบ (Configuration) ให้มีการล็อกหน้าจอสำหรับอุปกรณ์ที่ไม่มีพนักงานดูแล หรือล็อกอุปกรณ์อยู่เสมอ
 - 3.1.2 ผู้ใช้งานและหน่วยงานภายนอก ต้องล็อกหน้าจออัตโนมัติเมื่อไม่มีการใช้งานระบบเทคโนโลยีสารสนเทศของ รพม. ตามระยะเวลาที่กำหนด โดยต้องพักหน้าจอ (Screen saver) อัตโนมัติ หลังจากที่ไม่มีการใช้งานคอมพิวเตอร์เป็นระยะเวลานานกว่า 15 นาที ผู้ใช้งานและหน่วยงานภายนอก จะใช้งานต่อได้เมื่อมีการใส่รหัสผ่านที่ถูกต้อง
 - 3.1.3 ผู้ใช้งานต้อง Log out ออกจากเครื่องคอมพิวเตอร์เมื่อมีความจำเป็นต้องละทิ้งเครื่องคอมพิวเตอร์
 - 3.1.4 ผู้ใช้งานต้องป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ เช่น กล้องดิจิทัล เครื่องสำเนาเอกสาร เครื่องสแกน เอกสารโดยไม่ได้รับอนุญาต
 - 3.2 การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear desk and clear screen control)
 - 3.2.1 ผู้บังคับบัญชาต้องกำหนดให้มีผู้รับผิดชอบในการดูแลสถานที่ที่มีการรับ - ส่งแฟกซ์ หรือจดหมายเข้า - ออก
 - 3.2.2 ผู้ใช้งานต้องออกจากระบบคอมพิวเตอร์ (Log out) ทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
 - 3.2.3 ผู้ใช้งานต้องจัดเก็บข้อมูลสำคัญแยกต่างหาก และป้องกันให้มีความปลอดภัยอย่างพอเพียง
 - 3.2.4 ผู้ใช้งานต้องนำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

4. การควบคุมการเข้าถึงเครือข่าย (Network access control)
ให้มีการควบคุมการใช้งานบริการเครือข่าย การควบคุมการพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอก รพม. การควบคุมการพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย การป้องกันพอร์ต (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ การแบ่งแยกเครือข่าย (Segregation in networks) อย่างเหมาะสม การควบคุมการเชื่อมต่อทางเครือข่าย และการควบคุมการกำหนดเส้นทางบนเครือข่าย
- 4.1 การใช้งานบริการเครือข่าย (Use of network services)
 - 4.1.1 ผู้ดูแลระบบต้องควบคุมการเผยแพร่แผนผังระบบเครือข่ายสื่อสารข้อมูล (Network diagram) รวมถึงโครงสร้าง IP address ของระบบ และชื่ออุปกรณ์สารสนเทศแก่ผู้ที่ไม่ได้รับอนุญาตหรือหน่วยงานภายนอก
 - 4.1.2 ผู้ดูแลระบบต้องควบคุมการใช้งานระบบเครือข่ายสื่อสารข้อมูล เพื่อป้องกันการเข้าถึงระบบเครือข่ายสื่อสารข้อมูลและบริการของระบบเครือข่ายสื่อสารข้อมูลโดยไม่ได้รับอนุญาต
 - 4.1.3 ผู้ดูแลระบบต้องควบคุมการเชื่อมต่อเครือข่ายภายนอก เพื่อใช้งานอินเทอร์เน็ต ซึ่งอาจเป็นช่องทางให้หน่วยงานภายนอกเข้าถึงสารสนเทศหรือระบบเทคโนโลยีสารสนเทศของ รพม. โดยมิได้รับอนุญาต
 - 4.1.4 ผู้ใช้งานต้องแจ้งความประสงค์ในการขอใช้งานบริการเครือข่ายแก่ ผทท. และสามารถใช้บริการเครือข่ายได้หลังจากได้รับการอนุมัติจาก ผทท. แล้ว
 - 4.1.5 ผู้ใช้งาน ต้องไม่ใช้ระบบเครือข่ายสื่อสารข้อมูลเพื่อเป็นช่องทางในการเจาะระบบ (Hacking) หรือการสแกนช่องโหว่ของระบบโดยมิได้รับอนุญาต
- 4.2 การพิสูจน์ตัวตนของผู้ใช้งานที่อยู่ภายนอก รพม. (User authentication for external connections)
ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนผ่านระบบ Active directory ของ รพม. ก่อนอนุญาตให้ผู้ใช้งานที่อยู่ภายนอก รพม. เข้าใช้งานเครือข่ายและระบบสารสนเทศของ รพม.
- 4.3 การพิสูจน์ตัวตนของอุปกรณ์ในระบบเครือข่ายสื่อสารข้อมูล (Equipment identification in networks)
ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนของอุปกรณ์ในระบบเครือข่ายสื่อสารข้อมูล ได้แก่ การตรวจสอบ MAC address
- 4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection)
ผู้ดูแลระบบต้องระงับบริการและพอร์ต (Port) ที่ไม่มีความจำเป็นต้องใช้บนเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่าย
- 4.5 ผู้ดูแลระบบต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion prevention system/ intrusion detection system) ของระบบเครือข่าย
- 4.6 การแบ่งแยกเครือข่าย (Segregation in networks)
 - 4.6.1 ผู้ดูแลระบบต้องจัดให้มีการแบ่งแยกเครือข่ายตามกลุ่มของผู้ใช้งาน หรือกลุ่มของระบบเทคโนโลยีสารสนเทศ เพื่อควบคุมการใช้งานในแต่ละเครือข่ายย่อยอย่างเหมาะสม โดยพิจารณา

จากความต้องการในการเข้าถึงข้อมูล ระดับความสำคัญของข้อมูล รวมถึงการพิจารณาด้านราคา ประสิทธิภาพ และผลกระทบทางด้านความปลอดภัยดังต่อไปนี้

- 1) เครือข่ายที่อนุญาตให้เข้าถึงจากภายนอกและเครือข่ายที่ใช้ภายใน รพม.
- 2) เครือข่ายแอปพลิเคชัน (Application) ที่มีความสำคัญกับเครือข่ายอื่น ๆ ที่มีความสำคัญน้อยกว่า
- 3) เครือข่ายสำหรับเครื่องให้บริการ (Server farm) กับเครือข่ายของผู้ใช้งาน ควรมีการติดตั้งอุปกรณ์ที่สามารถแบ่งแยกเครือข่ายได้ เช่น Firewall หรือ Switch ที่สามารถแบ่ง VLAN ได้ เป็นต้น

4.6.2 ผู้ดูแลระบบจะกำหนดเส้นทางบนเครือข่ายที่เข้มงวด เพื่อจำกัดการเข้าถึงระยะไกลไปเฉพาะเครือข่ายที่กำหนดเท่านั้น

4.6.3 ผู้ดูแลระบบต้องตั้งค่า (Configuration) อุปกรณ์เครือข่าย เช่น Firewall หรือ Router มิให้สามารถบริหารจัดการจากภายนอกเครือข่ายได้ เว้นแต่ในกรณีฉุกเฉินซึ่งต้องได้รับการอนุญาตจากผู้ดูแลระบบเท่านั้น

4.7 การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control)

4.7.1 ผู้ดูแลระบบต้องจำกัดการใช้งานเครือข่ายของผู้ใช้งานในการเชื่อมต่อกับเครือข่ายของ รพม. เช่น Router หรือ Firewall เป็นต้น พร้อมทั้งติดตั้งระบบควบคุมเพื่อกลั่นกรองข้อมูลที่รับ - ส่ง เช่น Web filtering, E-mail filtering เป็นต้น เพื่อให้การเชื่อมต่อมีความปลอดภัย

4.7.2 ผู้ดูแลระบบต้องติดตั้ง Firewall ระหว่างเครือข่ายของ รพม. กับเครือข่ายภายนอก ทั้งนี้ การติดตั้ง Firewall ต้องพิจารณาเรื่องดังต่อไปนี้

- 1) การป้องกันการจราจรจากภายนอก ต้องถูกกำหนดให้ใช้เส้นทางที่ผ่าน First tier firewall ที่มีความมั่นคงปลอดภัยเพื่อป้องกันการรั่วซึมสารสนเทศของ รพม. และโครงสร้างพื้นฐานที่มีความสำคัญจากการเข้าถึงที่ไม่ได้รับอนุญาต
- 2) Firewall ต้องระบุตัวตนและพิสูจน์ตัวตนของผู้ใช้งานก่อนที่จะให้สิทธิ์การเข้าถึงอินเทอร์เน็ตเฟส (Interface) เพื่อการบริหารจัดการ Firewall
- 3) Firewall ต้องตั้งค่าให้ระงับบัญชีผู้ใช้งานหลังจากมีความพยายามที่จะเข้าสู่ระบบไม่สำเร็จ 5 ครั้ง การยกเลิกการระงับต้องดำเนินการโดย ผทท.
- 4) ไม่อนุญาตให้พิสูจน์ตัวตนผ่านทางอินเทอร์เน็ตเฟส (Interface) การจัดการ Firewall จากระยะไกล (Remote)
- 5) ผู้ที่ได้รับการมอบหมายจาก ผทท. เท่านั้นที่มีสิทธิ์ที่จะเปลี่ยนการตั้งค่าด้านความปลอดภัยบน Firewall
- 6) Firewall ต้องตั้งค่าให้บันทึกเหตุการณ์ด้านความมั่นคงปลอดภัย
- 7) Firewall ต้องได้รับการสอบทาน ทดสอบ และตรวจสอบอย่างสม่ำเสมอ
- 8) Firewall ต้องถูกบริหารจัดการผ่านการติดต่อสื่อสารที่มีการเข้ารหัส
- 9) ต้องปิดบริการและพอร์ต (Port) ที่ไม่จำเป็นต้องใช้บน Firewall
- 10) Firewall ประเภทซอฟต์แวร์ (Software) ต้องติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายแยกต่างหาก

- 11) Firewall ต้องสามารถป้องกันตัวเองจากการโจมตี DOS (Denial of service) ได้อย่างเช่น Ping, Sweeps หรือ TCP SYN Floods เป็นต้น
- 12) ต้องใช้เวอร์ชันของซอฟต์แวร์ (Software) Firewall และระบบปฏิบัติการที่เจ้าของผลิตภัณฑ์ยังให้การสนับสนุน
- 13) ผู้ดูแล Firewall ต้องติดตามข้อมูลช่องโหว่จากผู้ให้บริการ (Vendor) เพื่อรับทราบข่าวสารการ Upgrade และแพตช์ (Patch) ที่จำเป็น และต้องติดตั้งแพตช์ (Patch) ทั้งหมดที่เกี่ยวข้อง

4.7.3 ผู้ดูแลระบบต้องติดตั้ง Firewall เพื่อแบ่งแยก Zone ให้มีการใช้ DMZ (Demilitarized zone) โดยต้องพิจารณาเรื่องดังต่อไปนี้

- 1) เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการผ่านอินเทอร์เน็ต เช่น FTP, Email, Web และ External DNS server เป็นต้น ต้องติดตั้งอยู่ใน DMZ
- 2) การเข้าถึงจากระยะไกลต้องพิสูจน์ตัวตนที่ Firewall หรือผ่านบริการที่อยู่ใน DMZ
- 3) DNS Servers ต้องไม่อนุญาตให้มีการแลกเปลี่ยนโซน (Zone transfers) เว้นแต่มีเหตุจำเป็น

4.8 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control)

ผู้ดูแลระบบต้องควบคุมการกำหนดเส้นทางบนเครือข่ายเพื่อให้มั่นใจว่าการเชื่อมต่อเครื่องคอมพิวเตอร์และการไหลเวียนของสารสนเทศบนเครือข่าย โดยมีกลไกในการตรวจสอบที่อยู่ปลายทางและต้นทางของการเชื่อมต่อ เช่น การควบคุมโดย Firewall หรือ Proxy เป็นต้น

5. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)

ให้มีการควบคุมการเข้าถึงระบบปฏิบัติการอย่างมั่นคงปลอดภัย การควบคุมการระบุและพิสูจน์ตัวตนของผู้ใช้งาน การควบคุมระบบบริหารจัดการรหัสผ่าน การควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ (System utilities) การควบคุมการหมดเวลาการใช้งานระบบเทคโนโลยีสารสนเทศ และควบคุมการจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ

5.1 ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on procedures)

5.1.1 ผู้ดูแลระบบ ต้องจัดให้มีการควบคุมการเข้าถึงระบบปฏิบัติการอย่างมั่นคงปลอดภัยโดยขั้นตอนการเข้าสู่ระบบต้องเปิดเผยข้อมูลเกี่ยวกับระบบให้น้อยที่สุดเพื่อหลีกเลี่ยงผู้ใช้งานที่ไม่ได้รับอนุญาต ซึ่งขั้นตอนการ Log-on ต้องพิจารณา ดังนี้

- 1) หากกระบวนการเข้าสู่ระบบไม่สำเร็จ ระบบต้องไม่แสดงข้อมูลของระบบหรือแอปพลิเคชัน (Application) ที่ใช้งานอยู่
- 2) ระบบต้องแสดงข้อความเตือนผู้ใช้งานว่าสามารถเข้าใช้งานเครื่องคอมพิวเตอร์ได้เฉพาะผู้ที่มีสิทธิ์เท่านั้น
- 3) หากกระบวนการเข้าสู่ระบบไม่สำเร็จ ระบบต้องไม่แสดงข้อมูลที่สามารถระบุตัวตนของระบบ เช่น เครือข่ายที่ใช้งาน สถานที่ตั้งของระบบ หรือชื่อเครื่องคอมพิวเตอร์แม่ข่าย เป็นต้น
- 4) ระบบต้องไม่แสดงข้อความที่ชี้เฉพาะเหตุของการเข้าสู่ระบบไม่สำเร็จ เช่น ไม่แสดงข้อความว่า บัญชีผู้ใช้งานผิด หรือ รหัสผ่านผิด เป็นต้น
- 5) ห้ามเข้าสู่ระบบจากบัญชีผู้ใช้งานส่วนบุคคลเดียวกันมากกว่าหนึ่ง Session ในระบบเดียวกัน

- 6) ระบบต้องจำกัดจำนวนครั้งในการพยายามเข้าสู่ระบบที่ไม่สำเร็จ และต้องพิจารณาเงื่อนไขต่อไปนี้
 - (ก) การเก็บบันทึกผลการเข้าสู่ระบบทั้งที่สำเร็จและไม่สำเร็จ
 - (ข) หน่วงระยะเวลาในการเข้าใช้งานระบบครั้งต่อไป
 - (ค) การตัดการเชื่อมต่อ
 - (ง) การแสดงข้อความเตือนที่หน้าจอของผู้ดูแลระบบเมื่อมีการเข้าสู่ระบบเกินจำนวนครั้งที่จำกัดไว้
 - 7) ระบบต้องแสดงวัน เวลา ในการเข้าสู่ระบบที่สำเร็จในครั้งก่อน พร้อมทั้งบันทึกจำนวนครั้งที่พยายามเข้าไม่สำเร็จนับแต่การเข้าสู่ระบบที่สำเร็จในครั้งก่อนของผู้ใช้งาน
 - 8) ระบบต้องไม่ส่งรหัสผ่านแบบ Clear text ผ่านระบบเครือข่ายสื่อสารข้อมูล
 - 9) ผู้ดูแลระบบต้องกำหนดจำนวนครั้งที่ยอมให้ใส่รหัสผ่านผิดได้ไม่เกิน 5 ครั้ง
- 5.2 การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication)
ผู้ดูแลระบบ ต้องจัดให้ผู้ใช้งานมีบัญชีผู้ใช้งานของแต่ละบุคคลเพื่อใช้พิสูจน์ตัวตนในการเข้าถึงระบบเทคโนโลยีสารสนเทศ และต้องใช้ระบบเทคโนโลยีสารสนเทศพิสูจน์ตัวตนผู้ใช้งานในการเข้าถึงระบบปฏิบัติการ โดยผ่านระบบ Active directory หรือ Lightweight Directory Access Protocol (LDAP) ทุกครั้ง พร้อมทั้งบันทึกข้อมูลการเข้าถึง
- 5.3 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities)
ผู้ดูแลระบบ ต้องควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้บนระบบที่ใช้งานจริง (Production system) ดังนี้
- 5.3.1 ต้องจัดทำบัญชีโปรแกรมประเภทยูทิลิตี้ (System utilities) ที่นำมาใช้งาน
 - 5.3.2 กำหนดความรับผิดชอบในการใช้โปรแกรมประเภทยูทิลิตี้ (System utilities) แต่ละรายการอย่างชัดเจนและสื่อสารให้ผู้เกี่ยวข้องทราบเพื่อถือปฏิบัติ
 - 5.3.3 ให้มีการพิสูจน์ตัวตน และกำหนดสิทธิ์ในการใช้งานโปรแกรมประเภทยูทิลิตี้เฉพาะกลุ่มคนที่มีหน้าที่รับผิดชอบ
 - 5.3.4 มีการบันทึกเหตุการณ์ (Log) การใช้งานโปรแกรมประเภทยูทิลิตี้ และต้องสอบทานจากผู้ดูแลระบบอย่างสม่ำเสมอ
 - 5.3.5 ต้องทำการเพิกถอนหรือระงับโปรแกรมประเภทยูทิลิตี้ที่ไม่จำเป็น
- 5.4 การหมดเวลาการใช้งานระบบสารสนเทศ (Session time-out)
- 5.4.1 ผู้ดูแลระบบต้องกำหนด Session time-out ของระบบเทคโนโลยีสารสนเทศที่ไม่มีการใช้งานภายในระยะเวลา 15 นาที ทั้งนี้ ถ้าระบบที่ไม่สามารถตัดการเชื่อมต่อแบบอัตโนมัติได้ กำหนดให้ใช้โปรแกรมพักหน้าจอที่ต้องใส่รหัสผ่านหรือกำหนดให้มีการล็อกหน้าจอ
 - 5.4.2 ผู้ดูแลระบบ และผู้ใช้งาน ต้องตั้งค่าให้โปรแกรมพักหน้าจอที่ต้องใส่รหัสผ่านสำหรับเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์แบบพกพา และเครื่องคอมพิวเตอร์แม่ข่าย ทั้งนี้ โปรแกรมพักหน้าจอกำหนดให้ป้อนรหัสผ่านหลังจากที่มีการทิ้งเครื่องดังกล่าวไว้โดยไม่มีการใช้งานเป็นเวลา 15 นาที

- 5.5 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)
 - 5.5.1 ผู้ดูแลระบบ ต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง โดยต้องคำนึงระยะเวลาที่จำเป็นในกระบวนการดำเนินงานทางธุรกิจ ได้แก่ กำหนดให้เข้าใช้งานได้ในช่วงเวลาทำการของ รพม. 08.00 น. – 17.00 น. และเชื่อมต่อเพื่อใช้งานได้ครั้งละไม่เกิน 3 ชั่วโมง
 - 5.5.2 ผู้ใช้งาน หากมีความจำเป็นต้องใช้งานนอกเวลาที่กำหนดต้องขออนุมัติจากผู้บังคับบัญชาเท่านั้น
6. การควบคุมการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ (Application and information access control)
ให้มีการจำกัดการเข้าถึงสารสนเทศ และการแยกระบบเทคโนโลยีสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณที่ควบคุมเฉพาะ
 - 6.1 การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)
 - 6.1.1 เจ้าของข้อมูลและผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงแก่ผู้ใช้งานเท่าที่จำเป็นต้องใช้ในการปฏิบัติงาน โดยการให้สิทธิ์ต้องพิจารณาในเรื่องดังต่อไปนี้
 - 1) การจำกัดไม่ให้ใช้ตัวเลือก (Options) ที่ไม่ได้รับอนุญาต
 - 2) การจำกัดการเข้าถึง Command Line
 - 3) การจำกัดการเข้าถึงข้อมูลและฟังก์ชันการใช้งานของแอปพลิเคชัน (Application) ที่ไม่เกี่ยวข้องกับหน้าที่ความรับผิดชอบ
 - 4) การจำกัดระดับสิทธิ์ในการเข้าถึงไฟล์ เช่น อ่านอย่างเดียว เป็นต้น
 - 5) การควบคุมการแจกจ่าย การเข้าถึงข้อมูล การนำข้อมูลออกจากระบบสารสนเทศ เช่น รายงาน เป็นต้น
 - 6.1.2 เจ้าของข้อมูลและผู้ดูแลระบบ ควรกำหนดให้ระบบสารสนเทศรองรับการกำหนดสิทธิ์ในการเข้าถึงแบบกลุ่มได้
 - 6.2 การแยกระบบสารสนเทศที่ไวต่อการรบกวน (Sensitive system isolation) มีผลกระทบต่อคนกลุ่มใหญ่ หรือระบบที่มีความสำคัญต่อหน่วยงาน ต้องดำเนินการดังนี้
 - 6.2.1 เจ้าของข้อมูลและผู้ดูแลระบบ แยกระบบซึ่งไวต่อการรบกวนออกจากระบบอื่น ๆ และควบคุมสภาพแวดล้อมของระบบโดยเฉพาะ ได้แก่ ระบบ File sharing ระบบสารสนเทศทางการเงิน และระบบ Active directory โดยเข้าถึงได้ทั้งอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร (Mobile computing and teleworking)
 - 6.2.2 ผู้ดูแลระบบต้องควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์เคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile computing and teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว
 - 6.2.3 เจ้าของข้อมูลที่เป็นเจ้าของระบบสารสนเทศที่มีความสำคัญสูงต้องเป็นผู้อนุญาต ในกรณีที่ระบบสารสนเทศที่มีความสำคัญสูงมีความจำเป็นต้องทำงานร่วมกับระบบสารสนเทศอื่นที่มีความสำคัญน้อยกว่า
7. การควบคุมการปฏิบัติงานจากภายนอก รพม. (Teleworking)
 - 7.1 ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนการใช้งาน และเชื่อมต่อผ่านช่องทางที่มีความปลอดภัยที่มีเทคโนโลยีเข้ารหัสป้องกัน

- 7.2 ผู้ดูแลระบบต้องทำการถอดถอนสิทธิ์ในการเข้าถึงของผู้ใช้งานจากภายนอกสำนักงาน เมื่อครบกำหนดระยะเวลาที่ขออนุญาต
 - 7.3 ผู้ใช้งาน หากจำเป็นต้องมีการปฏิบัติงานจากภายนอกสำนักงานของ รพม. ต้องได้รับการอนุญาตจากผู้บังคับบัญชาอย่างเป็นทางการเป็นลายลักษณ์อักษร ในกรณีเร่งด่วนสามารถดำเนินการก่อน โดยแจ้งให้ผู้บังคับบัญชารับทราบด้วย โดยผู้บังคับบัญชาต้องพิจารณาเงื่อนไขในการเตรียมการ ดังต่อไปนี้
 - 1) ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมของการปฏิบัติงานจากภายนอก รพม.
 - 2) ความมั่นคงปลอดภัยทางการสื่อสาร โดยยึดจากระดับความสำคัญ (Sensitivity) ของข้อมูลที่จะถูกเข้าถึงและส่งผ่านช่องทางการเชื่อมต่อสื่อสาร (Communication link) รวมถึงระดับความสำคัญ (Sensitivity) ของระบบภายใน รพม.
 - 7.4 ผู้ใช้งานต้องจัดเก็บเอกสารที่เป็นความลับในอุปกรณ์ที่ล็อกได้และมีการควบคุมการเข้าถึง โดยใช้หลักเกณฑ์การรักษาความลับเช่นเดียวกับสารสนเทศที่อยู่ในสำนักงานของ รพม.
 - 7.5 ผู้ใช้งาน ต้องติดตั้งโปรแกรมป้องกันไวรัสและ Personal firewall สำหรับอุปกรณ์ส่วนตัวที่ใช้เชื่อมต่อเครือข่ายของ รพม. จากภายนอก
8. ผู้บังคับบัญชา ต้องควบคุมการใช้งานข้อมูลส่วนบุคคลให้มีการใช้งานที่สอดคล้องกับกฎหมาย พระราชบัญญัติ
กฏระเบียบ ข้อบังคับที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ส่วนที่ 7

การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

วัตถุประสงค์

- เพื่อกำหนดมาตรการในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ของ รพม. โดยการกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ
- เพื่อสร้างความมั่นคงปลอดภัยของการทำงานของระบบเครือข่ายไร้สาย

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 5 การควบคุมการเข้าถึง (Access control)
- หมวดที่ 9 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)

แนวปฏิบัติ

1. ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของ รพม. ต้องลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับการอนุญาตจาก ผทท. อย่างเป็นทางการ
2. ผู้ดูแลระบบต้องกำหนดมาตรฐานความปลอดภัยของระบบเครือข่ายไร้สายไม่ต่ำกว่ามาตรฐาน WPA2
3. ผู้ดูแลระบบต้องลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ
4. ผู้ดูแลระบบต้องลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อบนระบบเครือข่ายไร้สาย
5. ผู้ดูแลระบบ ต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีใช้ Access Point (AP) ของ รพม. รับ - ส่งสัญญาณได้
6. ผู้ดูแลระบบต้องเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและต้องสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณอาจช่วยลดการรั่วไหลของสัญญาณให้ดีขึ้น
7. ผู้ดูแลระบบต้องเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำ Access Point (AP) มาใช้งาน
8. ผู้ดูแลระบบต้องเปลี่ยนค่าชื่อ Login และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบต้องเลือกใช้ชื่อ Login และรหัสผ่านที่มีความคาดเดายากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย
9. ผู้ดูแลระบบต้องควบคุม MAC address ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยอนุญาตเฉพาะผู้ใช้งานที่ได้รับอนุญาตให้เข้าใช้เครือข่ายไร้สายได้อย่างถูกต้องเท่านั้น
10. ผู้ดูแลระบบต้องตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ และบันทึกเหตุการณ์น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สายตามขั้นตอนที่ รพม. กำหนด

ส่วนที่ 8

การควบคุมหน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) เข้าถึงระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

- เพื่อควบคุมหน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) ที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของ รพม. ให้เป็นไปอย่างมั่นคงปลอดภัย

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้บังคับบัญชา
- หน่วยงานภายนอก
- ผู้ใช้งาน (บุคคลภายนอก)

อ้างอิงมาตรฐาน

- หมวดที่ 5 การควบคุมการเข้าถึง (Access control)
- หมวดที่ 7 ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environment security)
- หมวดที่ 11 ความสัมพันธ์กับผู้ขาย ผู้ให้บริการภายนอก (Supplier relationships)

แนวปฏิบัติ

1. ผู้ดูแลระบบต้องประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสม ก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศของ รพม.
2. การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก)
 - 2.1 เจ้าของข้อมูลต้องเป็นผู้อนุญาตการให้สิทธิ์แก่หน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) ที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของ รพม. อย่างเป็นลายลักษณ์อักษร
 - 2.2 ผู้บังคับบัญชาต้องกำหนดให้มีการลงนามการไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของ รพม.
 - 2.3 ผู้บังคับบัญชา ต้องควบคุมให้มีการกำหนดข้อตกลงและความรับผิดชอบที่เกี่ยวข้องกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศลงในสัญญากับผู้ให้บริการภายนอกที่ให้บริการด้านสารสนเทศและบริการด้านการสื่อสาร โดยให้ครอบคลุมรวมถึงผู้รับจ้างช่วง
 - 2.4 ผู้บังคับบัญชาต้องกำหนดให้จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) ระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศ ซึ่งมีรายละเอียด ดังนี้
 - 2.4.1 เหตุผลในการขอใช้
 - 2.4.2 ระยะเวลาในการใช้
 - 2.4.3 การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย
 - 2.4.4 การตรวจสอบ MAC address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

- 2.5 ผู้ดูแลระบบมีสิทธิ์ในการตรวจสอบการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) เพื่อควบคุมการใช้งานได้อย่างมั่นคงปลอดภัยตามสัญญา
- 2.6 ผู้ดูแลระบบต้องควบคุมให้หน่วยงานภายนอกจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งต้องปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อใช้สำหรับควบคุมหรือตรวจสอบการทำงาน และเพื่อให้มั่นใจว่าการปฏิบัติงานเป็นไปตามขอบเขตที่ได้กำหนดไว้
3. ผู้ดูแลระบบต้องแจ้งแนวปฏิบัติต่าง ๆ ที่เกี่ยวข้อง แก่ผู้รับจ้างภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) เพื่อให้ปฏิบัติตาม
4. ผู้ดูแลระบบ ต้องกำกับดูแลหน่วยงานภายนอก หรือผู้ใช้งาน (บุคคลภายนอก) ให้ปฏิบัติตามสัญญาหรือข้อตกลงการให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงด้านความมั่นคงปลอดภัย
5. ผู้ดูแลระบบ ต้องติดตาม ตรวจสอบรายงานหรือบันทึกการให้บริการของหน่วยงานภายนอกหรือบุคคลที่ให้บริการแก่หน่วยงานตามที่ว่าจ้างอย่างสม่ำเสมอตามสัญญาว่าจ้าง
6. ผู้ดูแลระบบ ต้องกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีหน้าที่ในการกำกับดูแลหรือหน่วยงานที่เกี่ยวข้องกับการบังคับใช้กฎหมาย รวมทั้งหน่วยงานที่ควบคุมดูแลสถานการณ์ฉุกเฉินภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน
7. ผู้ดูแลระบบ ต้องมีขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีความเชี่ยวชาญเฉพาะด้านหรือหน่วยงานที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน
8. ผู้ดูแลระบบต้องควบคุมการเปลี่ยนแปลงของหน่วยงานภายนอกที่ส่งผลกระทบต่อการให้บริการขององค์กร และต้องประเมินความเสี่ยงอย่างเหมาะสมเพื่อควบคุมผลกระทบอันเนื่องมาจากการเปลี่ยนแปลงนั้น
9. หน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) ต้องใช้งานทรัพย์สินสารสนเทศของ รพม. ด้วยความระมัดระวัง และรักษาความลับของ รพม. ไม่นำไปเปิดเผย และต้องขออนุญาตพร้อมทั้งปฏิบัติตามเงื่อนไขในการเข้าถึงระบบสารสนเทศของ รพม. ทุกครั้ง

ส่วนที่ 9

การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ ของ รพม.

วัตถุประสงค์

- เพื่อควบคุมการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ ที่ รพม. จัดไว้ให้ใช้อย่างเหมาะสม ทั้งนี้ เพื่อป้องกันการสูญหาย เสียหาย หรือถูกเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 2 อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากระยะไกล (Mobile devices and teleworking)
- หมวดที่ 4 การบริหารจัดการทรัพย์สิน (Asset management)
- หมวดที่ 8 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations security)

แนวปฏิบัติ

1. การใช้งานทั่วไป

- 1.1 ผู้ดูแลระบบต้องกำหนดบัญชีซอฟต์แวร์มาตรฐาน (Software standard) ที่อนุญาตให้ติดตั้งบนเครื่องคอมพิวเตอร์ของผู้ใช้งาน และปรับปรุงให้เป็นปัจจุบันเสมอ
- 1.2 ผู้ดูแลระบบต้องเป็นผู้กำหนดการตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) เท่านั้น
- 1.3 ผู้ใช้งานต้องใช้งานอย่างมีประสิทธิภาพเพื่องานของ รพม.
- 1.4 ผู้ใช้งานต้องไม่ติดตั้งโปรแกรมที่ละเมิดลิขสิทธิ์บนเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ของ รพม.
- 1.5 ผู้ใช้งานต้องขออนุญาตติดตั้งโปรแกรมในเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ตามขั้นตอนที่ รพม. กำหนด
- 1.6 ผู้ใช้งานต้องไม่ติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ของ รพม. การดำเนินการดังกล่าวต้องดำเนินการโดยผู้ดูแลระบบเท่านั้น
- 1.7 ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่อย่างละเอียด เพื่อให้สามารถใช้งานอย่างปลอดภัยและมีประสิทธิภาพ
- 1.8 ผู้ใช้งานต้องไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ และรักษาให้มีสภาพเดิม
- 1.9 ผู้ใช้งานต้องแจ้งซ่อมเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่เพื่อให้ ผทท. เป็นผู้ดำเนินการเท่านั้น
- 1.10 ผู้ใช้งานต้องไม่สร้าง Shortcut ไว้บน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของ รพม.
- 1.11 กรณีเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์เคลื่อนที่ ผู้ใช้งานต้องปฏิบัติ ดังนี้
 - 1.11.1 ในกรณีที่มีการใช้งานอุปกรณ์ประเภทพกพาในที่สาธารณะ ห้องประชุม และพื้นที่ภายนอก อื่น ๆ ที่ไม่มีการป้องกัน หรือไม่ได้อยู่ในบริเวณของ รพม. ให้ป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต เช่น ไม่เปิดการเชื่อมต่อแบบไร้สายโดยไม่มีการเข้ารหัสข้อมูล เป็นต้น

- 1.11.2 ต้องระมัดระวังการเคลื่อนย้าย โดยต้องใส่กระเป๋าเพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงานหรือหลุดมือ เป็นต้น
 - 1.11.3 ไม่ใส่ในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับหรืออาจถูกจับโยนได้
 - 1.11.4 การใช้งานเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัดต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะเวลาหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง
 - 1.11.5 หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอย ชีตข่วน หรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้
 - 1.11.6 ไม่วางของทับบนหน้าจอและแป้นพิมพ์
 - 1.11.7 การเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น
 - 1.11.8 ไม่เคลื่อนย้ายเครื่องในขณะที่ Harddisk กำลังทำงาน
 - 1.11.9 ไม่ใช้หรือวางใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่าง ๆ เป็นต้น
 - 1.11.10 ไม่วางใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูง เช่น แม่เหล็ก โทรชั่นส์ ไมโครเวฟ ตู้เย็น เป็นต้น
 - 1.11.11 ไม่ติดตั้งหรือวางในที่ที่มีการสั่นสะเทือน เช่น ในยานพาหนะที่กำลังเคลื่อนที่
 - 1.11.12 การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้
 - 1.11.13 รับผิดชอบในการป้องกันการสูญหาย เช่น ต้องล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย
 - 1.11.14 นำติดตัวไปด้วยเสมอ เช่น ไม่ละทิ้ง อุปกรณ์ประมวลผลประเภทพกพาในรถยนต์ ห้องพักในโรงแรม หรือห้องประชุม เป็นต้น ในกรณีที่มีความจำเป็นต้องละทิ้งให้จัดเก็บไว้ในสถานที่ที่มั่นคงปลอดภัย
 - 1.11.15 ไม่เก็บหรือใช้งานในสถานที่ที่มีความร้อน ความชื้นหรือฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ
 - 1.11.16 ไม่เปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub component) ที่ติดตั้งอยู่ภายใน เช่น แบตเตอรี่ หน่วยความจำ
2. แนวปฏิบัติในการใช้รหัสผ่าน
ให้ผู้ใช้งานปฏิบัติตามการใช้งานรหัสผ่าน (Password Use) (ส่วนที่ 6)
 3. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malicious code)
 - 3.1 ผู้ดูแลระบบต้องควบคุมการ Update ระบบปฏิบัติการ เว็บเบราว์เซอร์ และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ
 - 3.2 ผู้ดูแลระบบต้องติดตั้งและปรับปรุงโปรแกรมป้องกันไวรัสให้ทันสมัยอยู่เสมอ
 - 3.3 ผู้ใช้งานต้องไม่ปิดหรือยกเลิกระบบการป้องกันไวรัสที่ติดตั้งอยู่

- 3.4 ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อบันทึกต่าง ๆ เช่น Thumb drive และ Data storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์ของ รพม.
- 3.5 ผู้ใช้งาน หากพบหรือสงสัยว่าเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ติดชุดคำสั่งไม่พึงประสงค์ ให้รีบยกเลิกเชื่อมต่อเครื่องเข้ากับระบบเครือข่ายสื่อสารข้อมูลเพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่น ๆ ได้ และแจ้ง ผทท. ทราบทันที
4. การสำรองข้อมูลและการกู้คืน
 - 4.1 ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ไว้บนสื่อบันทึกอื่น ๆ เช่น ระบบ File Sharing, CD, DVD, External harddisk เป็นต้น
 - 4.2 ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลสำรองไว้อย่างสม่ำเสมอ
5. ผู้ดูแลระบบ ต้องควบคุมให้เครื่องคอมพิวเตอร์ได้รับการปรับตั้งค่าอย่างเหมาะสม เพื่อป้องกันการใช้งานหรือติดตั้ง Mobile code เช่น Active x, Java จากแหล่งที่ไม่น่าเชื่อถือ

ส่วนที่ 10

การใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์

วัตถุประสงค์

- เพื่อควบคุมการใช้งานอินเทอร์เน็ตและการใช้งานสื่อสังคมออนไลน์ (Social network) ของ รพม. ให้มีความปลอดภัย และป้องกันการละเมิดพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ จนส่งผลกระทบต่อ รพม.

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 5 การควบคุมการเข้าถึง (Access control)
- หมวดที่ 8 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations security)
- หมวดที่ 18 ความสอดคล้อง (Compliance)

แนวปฏิบัติ

1. ผู้ดูแลระบบต้องควบคุมการเชื่อมต่อทางเครือข่ายสำหรับการเข้าถึงอินเทอร์เน็ตโดยพิจารณาเรื่องดังต่อไปนี้
 - 1) ผู้ดูแลระบบต้องไม่อนุญาตให้ใช้งานอุปกรณ์ Video streaming อุปกรณ์ audio streaming หรือ Download ไฟล์ที่มีขนาดใหญ่ ในกรณีที่ต้องได้รับการอนุญาตจากผู้บังคับบัญชาก่อนเท่านั้น
 - 2) ผู้ดูแลระบบต้องจำกัดการใช้งานอินเทอร์เน็ตเพื่อเรื่องส่วนตัวหรือที่ไม่ใช่การดำเนินงานของ รพม. ให้น้อยที่สุดเท่าที่เป็นไปได้ เช่น การระงับการเข้าถึง Website ที่ไม่จำเป็น การระงับการเข้าถึง Website ที่มีเนื้อหาต้องห้ามตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
 - 3) ผู้ดูแลระบบต้องป้องกันไม่ให้มีการรับส่งข้อมูลที่ไม่เหมาะสมจากภายนอก รพม. เช่น
 - (ก) Executable เช่น .EXE .COM เป็นต้น
 - (ข) ไฟล์ (File) เสียง เช่น AUD .WAV และ.MP3 เป็นต้น
 - (ค) ไฟล์ (File) วิดิทัศน์ เช่น .MPG .MPEG .MOV และ .AVI เป็นต้น
 - (ง) Peer to Peer เช่น .torrent เป็นต้นในกรณีที่มีความจำเป็นต้องได้รับอนุญาตจากผู้บังคับบัญชา และ ผทท.
 - 4) ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่ รพม. จัดสรรไว้เท่านั้น เช่น Proxy, Firewall เป็นต้น
 - 5) ผู้ดูแลระบบต้องทดสอบเส้นทางสำหรับการเชื่อมต่ออินเทอร์เน็ตขององค์กรระหว่างเส้นทางที่ใช้งานจริงและเส้นทางสำรองอย่างน้อยปีละ 2 ครั้ง
 - 6) ผู้ใช้งานต้องไม่เชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นมีความจำเป็นและขออนุญาตจาก ผทท. เป็นลายลักษณ์อักษรแล้ว
 - 7) ผู้ใช้งานต้องขออนุญาตติดตั้งซอฟต์แวร์ (Software) ที่ Download จากอินเทอร์เน็ต และการติดตั้งต้องดำเนินการโดยผู้ที่ได้รับมอบหมายจากผู้ดูแลระบบเท่านั้น

2. ผู้ใช้งานต้องไม่มีเจตนาปิดบังหรือบิดเบือนตัวตนเมื่อมีการใช้งานอินเทอร์เน็ต
3. ผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัส พร้อมทั้งต้องปรับปรุง Virus signature ที่เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพาให้มีความทันสมัยอยู่เสมอ ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web browser) และต้องปิดช่องโหว่ของระบบปฏิบัติการที่เว็บเบราว์เซอร์ติดตั้งอยู่
4. ผู้ใช้งานจะต้องตรวจสอบไวรัส (Virus scanning) ก่อนการรับ - ส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ต
5. ผู้ใช้งานต้องไม่ใช่เครือข่ายอินเทอร์เน็ตของ รพม. เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น
6. ผู้ใช้งานจะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของ รพม.
7. ผู้ใช้งานต้องหลีกเลี่ยงการกระทำที่สิ้นเปลืองทรัพยากรของเครือข่ายอินเทอร์เน็ต ดังนี้
 - (ก) ส่งจดหมายอิเล็กทรอนิกส์ที่มีขนาดใหญ่หรือจดหมายอิเล็กทรอนิกส์ลูกโซ่
 - (ข) ใช้เวลาในการเข้าถึงอินเทอร์เน็ตเกินความจำเป็น
 - (ค) เล่นเกม Online
 - (ง) เข้าห้องพูดคุย Online
8. ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับ รพม.
9. ผู้ใช้งานต้องไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของ รพม.
10. ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต
11. ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อเติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ที่จะทำให้อื่นเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย
12. ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน
13. ผู้ใช้งานต้องคำนึงว่าข้อมูลจากอินเทอร์เน็ตอาจไม่มีความทันสมัยหรือไม่มีความถูกต้อง ผู้ใช้งานต้องตรวจสอบความถูกต้องของข้อมูลจากแหล่งที่น่าเชื่อถือก่อนที่จะเผยแพร่ข้อมูลดังกล่าว
14. ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา
15. ผู้ใช้งานต้องไม่ใช่ข้อมูลที่ร้าย ให้ร้ายในการเสนอความคิดเห็นที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของ รพม. การทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น ๆ
16. ผู้ใช้งานต้องไม่บันทึกรหัสผ่านใน Web browser (Remember password) เพื่อป้องกันบุคคลอื่นที่สามารถเข้าถึงคอมพิวเตอร์ของผู้ใช้งานนำรหัสผ่านดังกล่าวไปใช้งานในอินเทอร์เน็ตโดยไม่ได้รับอนุญาต

17. ผู้ใช้งานต้องไม่ Download เอกสาร หรือสารสนเทศต่าง ๆ เช่น ข้อมูล รูปภาพ วิดีโอ เสียง และซอฟต์แวร์ (Software) ที่ละเมิดลิขสิทธิ์ หรือผิดกฎหมาย
18. ผู้ใช้งานต้องปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ ภายหลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว
19. การใช้งานสื่อสังคมออนไลน์ (Social network)
 - 19.1 ผู้ใช้งานต้องระมัดระวังในการนำเสนอข้อมูลข่าวสาร การส่งข้อความ หรือการแสดงความคิดเห็นผ่านสื่อสังคมออนไลน์เพื่อไม่ก่อให้เกิดความเสียหายแก่ รพม.
 - 19.2 ผู้ใช้งานต้องระมัดระวังในการใช้สื่อสังคมออนไลน์ เนื่องจากพื้นที่บนสื่อสังคมออนไลน์เป็นพื้นที่สาธารณะไม่ใช่พื้นที่ส่วนบุคคล ซึ่งข้อมูลการใช้งานต่าง ๆ จะถูกบันทึกไว้และอาจมีผลทางกฎหมายถึงแม้จะเป็นการแสดงความคิดเห็นในนามชื่อบัญชีส่วนตัว และพึงตระหนักถึงผลกระทบที่อาจเกิดขึ้นกับ รพม. ได้
 - 19.3 ผู้ใช้งานที่ใช้สื่อสังคมออนไลน์เป็นเครื่องมือสื่อสารข้อมูลในกิจการของ รพม. หรือชื่อบุคคลที่ทำให้เข้าใจได้ว่าเป็นบุคคลในสังกัด ต้องแสดงภาพ และข้อมูลให้ถูกต้องชัดเจนในข้อมูล โปรไฟล์ (Profile) และพึงใช้ด้วยความสุภาพและมีวิจารณญาณ
 - 19.4 ผู้ใช้งานควรตั้งคำถามที่ใช้ในกรณีกู้คืนบัญชีผู้ใช้งานหรือกู้คืนรหัสผ่าน (Forgot your password) ควรเลือกใช้ข้อมูลหรือคำถามที่เป็นส่วนบุคคลและเป็นข้อมูลที่ผู้อื่นคาดเดาได้ยากเพื่อป้องกันการสุ่มคำถามจากผู้ประสงค์ร้าย
 - 19.5 ผู้ใช้งานต้องไม่ใช้ระบบอีเมลของเว็บไซต์ประเภทสื่อสังคมออนไลน์ หากจำเป็นต้องใช้จะต้องระมัดระวังในการคลิกลิงก์ที่น่าสงสัย โดยเฉพาะอีเมลแจ้งเตือนจากเว็บไซต์ต่าง ๆ ในลักษณะเชิญให้คลิกลิงก์ที่แนบมาในอีเมล ผู้ใช้งานต้องสงสัยว่าลิงก์ดังกล่าวเป็นลิงก์ที่ไม่ปลอดภัย (ลิงก์ที่ถูกสร้างมาเพื่อใช้ขโมยข้อมูลส่วนบุคคล ด้วยการนำไปสู่เว็บไซต์ที่น่าเชื่อถือที่ผู้ประสงค์ร้ายสร้างไว้เพื่อให้ผู้ใช้งานกรอกข้อมูลส่วนตัว เช่น รหัสผ่าน เป็นต้น)
 - 19.6 ผู้ใช้งานต้องศึกษาการตั้งค่าความเป็นส่วนตัวหรือ “Privacy settings” ให้เข้าใจเป็นอย่างดีและปรับแต่งการตั้งค่าความเป็นส่วนตัวให้เหมาะสมเพื่อป้องกันการถูกละเมิดความเป็นส่วนตัวซึ่งอาจจะส่งผลกระทบต่อตนเองหรือ รพม.
 - 19.7 ผู้ใช้งานต้องใช้งานสื่อสังคมออนไลน์อย่างเหมาะสม โดยไม่ละเมิดกฎหมายและไม่ก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานขององค์กร
 - 19.8 ผู้ใช้งานควรปิดการใช้งานระบบโพสต์ข้อความสาธารณะทุก ๆ ส่วนของเว็บไซต์ประเภท Social network หากจำเป็นต้องใช้งานต้องปรับค่าให้มีการตรวจสอบข้อความก่อนเพื่อหลีกเลี่ยงโอกาสแพร่กระจายลิงก์ที่ไม่ปลอดภัยจากผู้ประสงค์ร้าย ซึ่งเป็นหนึ่งในเทคนิคที่ใช้ในการโจมตีประเภท Spear-phishing
 - 19.9 ผู้ใช้งานต้องตรวจสอบก่อนจะรับเพื่อนเข้ากลุ่มในเว็บไซต์ประเภท Social network โดยต้องแน่ใจว่าข้อมูลส่วนตัวของเพื่อนคนนั้น เช่น รูปถ่ายและประวัติส่วนตัวไม่ถูกแก้ไขเพื่อปลอมแปลงตัวตนจากผู้ประสงค์ร้ายที่หวังแอบอ้างเพื่อคุกคามเป้าหมาย

- 19.10 ผู้ใช้งานต้องตระหนักไว้เสมอว่าข้อมูลต่าง ๆ ที่ผู้ใช้งานเผยแพร่ไว้บนบริการสื่อสังคมออนไลน์นั้น คงอยู่ถาวรและผู้อื่นอาจเข้าถึงและเผยแพร่ข้อมูลเหล่านั้นได้
- 19.11 ผู้ใช้งานต้องมีข้อพิจารณาในการรับเพื่อนเข้ากลุ่มที่ชัดเจน และควรประกาศข้อความปฏิเสธความรับผิดชอบที่เกี่ยวกับเนื้อหาหรือข้อความแสดงความคิดเห็นซึ่งถูกโพสต์จากเพื่อนในกลุ่มที่อาจปรากฏในเว็บไซต์ประเภท Social network ของผู้ใช้งานเอง
- 19.12 ผู้ใช้งานต้องติดตั้งซอฟต์แวร์ป้องกันไวรัส และอัปเดตฐานข้อมูลไวรัสของโปรแกรมอยู่เสมอ และต้องหลีกเลี่ยงการใช้โปรแกรมที่ละเมิดลิขสิทธิ์เพราะอาจจะมีโปรแกรมประสงค์ร้ายแฝงตัวอยู่ภายในเพื่อลักลอบ ปลอมแปลง หรือขโมยข้อมูลสำคัญของผู้ใช้งานได้
- 19.13 ผู้ใช้งานต้องระมัดระวังการใช้ถ้อยคำและภาษาที่อาจเป็นการดูหมิ่น ยุ้ง ทำทนาย หรือเป็นการละเมิดต่อบุคคลอื่น กรณีบุคคลอื่นมีความคิดเห็นที่แตกต่างพึงงดเว้นการโต้ตอบด้วยถ้อยคำรุนแรง
- 19.14 ผู้ใช้งานต้องระมัดระวังกระบวนการหาข่าว หรือภาพจากสื่อสังคมออนไลน์ โดยมีการตรวจสอบอย่างถี่ถ้วนรอบด้านและต้องอ้างอิงแหล่งที่มาเมื่อนำเสนอ เว้นแต่สามารถตรวจสอบและอ้างอิงจากแหล่งข่าวได้โดยตรง
- 19.15 หากผู้ใช้งานต้องการใช้สื่อสังคมออนไลน์เป็นเครื่องมือในการรายงานข่าวในนามของบุคคลธรรมดา ต้องแสดงให้เห็นชัดเจนว่า ข้อความใดเป็น "ข่าว" ข้อความใดเป็น "ความคิดเห็นส่วนตัว"
- 19.16 การส่งต่อหรือเผยแพร่ข้อมูลในสื่อสังคมออนไลน์ (Social media)
 - 19.16.1 ผู้ใช้งานต้องไม่ส่งต่อหรือเผยแพร่ข้อมูลที่เป็นเท็จ ข่าวลือ ข่าวไม่ปรากฏที่มา เป็นเพียงการคาดเดา หรือส่งผลเสียหายกับบุคคล สังคม หรือ รฟม.
 - 19.16.2 ผู้ใช้งานต้องไม่ส่งต่อหรือเผยแพร่ข้อมูลเรื่องบุคคลเสียชีวิต เด็กและเยาวชน ผู้สูญหาย ผู้ต้องหา เว้นเสียแต่ตรวจสอบข้อเท็จจริงแล้วและเห็นว่าเป็นประโยชน์ต่อสาธารณะ
 - 19.16.3 ผู้ใช้งานต้องไม่ส่งต่อหรือเผยแพร่ข้อมูลที่กระทบต่อสิทธิความเป็นส่วนตัว และศักดิ์ศรีความเป็นมนุษย์
- 19.17 ผู้ใช้งานต้องตั้งค่าความปลอดภัยของการใช้งานสื่อสังคมออนไลน์ และระมัดระวังการถูกนำข้อมูลจากข้อบัญชีไปใช้โดยไม่เหมาะสม ผิดวัตถุประสงค์ และลักษณะการแอบอ้างโดยบุคคลอื่น
20. ผู้ใช้งานต้องใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์โดยตระหนักถึงพระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่บังคับใช้อยู่เสมอ

ส่วนที่ 11

การใช้งานจดหมายอิเล็กทรอนิกส์

วัตถุประสงค์

- เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ของ รพม. ให้มีความปลอดภัยและมีประสิทธิภาพ

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 5 การควบคุมการเข้าถึง (Access control)
- หมวดที่ 8 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations security)

แนวปฏิบัติ

1. ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของ รพม. ให้เหมาะสมกับหน้าที่ความรับผิดชอบของผู้ใช้งาน รวมทั้งทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ
2. ผู้ดูแลระบบต้องกำหนดบัญชีผู้ใช้งานตามมาตรฐานจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ใช้ในองค์กร
3. ผู้ใช้งานต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ไม่ให้เกิดความเสียหายต่อ รพม. ละเมิดลิขสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น ผิดกฎหมาย ละเมิดศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่น แสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ของ รพม.
4. ผู้ใช้งานต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail address) ของผู้อื่นเพื่ออ่าน รับ - ส่งข้อความ ยกเว้น ได้รับการยินยอมจากเจ้าของบัญชีและให้ถือว่าเจ้าของบัญชีจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน
5. ผู้ใช้งานต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของ รพม. เพื่อปฏิบัติงาน ติดต่อ และประสานงานของ รพม. เท่านั้น
6. ผู้ใช้งานต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ฟรีของเอกชนในการปฏิบัติงาน ติดต่อ และประสานงานของ รพม.
7. ผู้ใช้งานต้อง Logout ออกจากระบบทุกครั้ง หลังจากใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้นเพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์
8. ผู้ใช้งานต้องตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนเปิดอ่าน โดยใช้โปรแกรมป้องกันไวรัส เพื่อตรวจสอบมัลแวร์ต่าง ๆ
9. ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์ที่ได้รับจากผู้ส่งที่ไม่รู้จัก
10. ผู้ใช้งานต้องใช้ข้อความที่สุภาพในการรับ - ส่งจดหมายอิเล็กทรอนิกส์ และไม่จัดส่งจดหมายที่มีเนื้อหาอาจทำให้ รพม. เสียชื่อเสียงหรือทำให้เกิดความแตกแยกภายใน รพม.
11. ผู้ใช้งานต้องไม่ระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์และต้องเข้ารหัสเพื่อป้องกันการเข้าถึงข้อมูลโดยผู้ไม่เกี่ยวข้องเมื่อมีการส่งข้อมูลที่เป็นความลับ
12. ผู้ใช้งานต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และต้องจัดเก็บจดหมายอิเล็กทรอนิกส์ในตู้ของตนให้เหลือจำนวนน้อยที่สุด หากมีข้อมูลที่จำเป็นต้องนำมาใช้อ้างอิงในการปฏิบัติงานภายหลัง ให้ผู้ใช้งานโอนย้ายจดหมายอิเล็กทรอนิกส์มายังเครื่องคอมพิวเตอร์ของตน ทั้งนี้ เพื่อลดปริมาณการใช้เนื้อที่ของระบบจดหมายอิเล็กทรอนิกส์

ส่วนที่ 12

การสำรองข้อมูลและการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

วัตถุประสงค์

- เพื่อให้มีข้อมูลสำรองไว้ใช้งานในกรณีที่ข้อมูลหลักเกิดความเสียหายไม่สามารถใช้งานหรือเข้าถึงได้ หรือเมื่อเกิดภาวะฉุกเฉินต่าง ๆ
- เพื่อให้มีการปฏิบัติที่สอดคล้องกับกฎหมาย พระราชบัญญัติ หรือข้อบังคับภายนอกอื่น ๆ

ผู้รับผิดชอบ

- ผู้บังคับบัญชา
- ผู้ดูแลระบบ
- เจ้าของข้อมูล
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 8 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations security)
- หมวดที่ 14 ความสอดคล้อง (Compliance)

แนวปฏิบัติ

1. การสำรองข้อมูลระบบแม่ข่าย

ข้อมูลระบบแม่ข่ายและข้อมูลสำคัญซึ่งเป็นความลับของ รฟม. ต้องได้รับการเก็บรักษาไว้ที่ระบบเก็บข้อมูลส่วนกลาง และสำรองข้อมูลไว้อย่างสม่ำเสมอ เพื่อให้มีข้อมูลสำรองไว้ใช้ ในกรณีที่ข้อมูลหลักเกิดความเสียหาย หรือไม่สามารถใช้งาน ความถี่ในการดำเนินการสำรองข้อมูลและขั้นตอนการสำรองข้อมูลระบบแม่ข่าย เป็นความรับผิดชอบของ ผทท. โดยมีแนวปฏิบัติ ดังนี้

- 1.1 ผู้บังคับบัญชากำหนดผู้รับผิดชอบในการสำรองข้อมูล
- 1.2 ผู้ดูแลระบบต้องกำหนดชนิดของข้อมูลของระบบที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้ เช่น ข้อมูลค่าคอนฟิกูเรชัน (Configuration) ข้อมูลคู่มือการปฏิบัติงานสำหรับระบบ ข้อมูลในฐานข้อมูลของระบบงาน ข้อมูลซอฟต์แวร์ เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ระบบงาน และซอฟต์แวร์อื่น ๆ เป็นต้น
- 1.3 ผู้ดูแลระบบต้องสำรองข้อมูลตามความถี่ที่กำหนดไว้ ทั้งนี้ หากเป็นข้อมูลที่สนับสนุนกระบวนการทำงานที่สำคัญของ รฟม. ให้สำรองตามความถี่ที่ รฟม. กำหนด
- 1.4 ผู้ดูแลระบบต้องตรวจสอบว่าการสำรองข้อมูลสำเร็จครบถ้วนหรือไม่ หากไม่สำเร็จให้หาสาเหตุและดำเนินการแก้ไขอีกครั้งหนึ่ง
- 1.5 ผู้ดูแลระบบต้องนำข้อมูลที่สำรองไว้ไปเก็บไว้ทั้งภายในและนอก รฟม. อย่างน้อยอย่างละ 1 ชุด
- 1.6 ผู้ดูแลระบบทดสอบกู้คืนข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าข้อมูลที่สำรองไว้มีความถูกต้อง ครบถ้วน และพร้อมใช้งาน

2. การสำรองข้อมูลคอมพิวเตอร์ส่วนบุคคล
ผู้ใช้งานจะต้องสำรองข้อมูลสำคัญที่เก็บรักษาไว้ในเครื่องคอมพิวเตอร์ส่วนบุคคลหรือคอมพิวเตอร์ หรืออุปกรณ์พกพาอื่น ๆ อย่างสม่ำเสมอ ความถี่ในการสำรองข้อมูลขึ้นอยู่กับความถี่ของการเปลี่ยนแปลงของข้อมูล และระดับความสำคัญของข้อมูลหากเกิดการสูญหาย
3. การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์
เพื่อให้สามารถระบุตัวบุคคลผู้ใช้งานได้อย่างถูกต้อง ผู้ดูแลระบบต้องดำเนินการดังนี้
 - 3.1 ตั้งนาฬิกาของอุปกรณ์ที่ให้บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล Stratum - 1 เก็บรักษาข้อมูลจราจรคอมพิวเตอร์ โดยระยะเวลาในการเก็บตามประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 (90 วัน)
 - 3.2 เก็บรักษาข้อมูลจราจรคอมพิวเตอร์ในสื่อที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง มีการเก็บรักษาความลับของข้อมูลตามระดับชั้นความลับในการเข้าถึงตามที่ รพม. กำหนด โดยระบุตัวบุคคลที่สามารถเข้าถึงสื่อดังกล่าวได้
 - 3.3 ประเภทของสารสนเทศที่เก็บรักษา แสดงตามตาราง

ประเภทของสารสนเทศ	กฎหมายที่เกี่ยวข้อง	ระยะเวลาการจัดเก็บรักษา (ปี)
Authentication server logs (RADIUS, TACACS)	1) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	1
Email server logs	2) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560	1
Web application server logs	3) ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564	1
NTP server logs		1
DHCP server logs		1
IPS logs		1
Firewalls logs		1
Routers & Switches logs		1
Active directory logs		1

4. การจัดเก็บบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and monitoring)
 - 4.1 ผู้ดูแลระบบต้องมีการจัดเก็บบันทึกเหตุการณ์ (Event logs) การใช้งานระบบสารสนเทศ
 - 4.2 ผู้ดูแลระบบต้องเก็บบันทึกข้อมูล Audit log ซึ่งบันทึกกิจกรรมการใช้งานของผู้ใช้งานระบบสารสนเทศและเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยต่าง ๆ เพื่อประโยชน์ในการสืบสวน สอบสวน และเพื่อการติดตามการควบคุมการเข้าถึง
 - 4.3 ผู้ดูแลระบบต้องมีการตรวจสอบข้อมูลบันทึกเหตุการณ์อย่างสม่ำเสมอ (Log review)
 - 4.4 ผู้ดูแลระบบต้องไม่ลบข้อมูลล็อก (Log) หรือปิดการใช้งานการบันทึกข้อมูลล็อก (Log)
 - 4.5 ผู้ดูแลระบบต้องป้องกันระบบสารสนเทศที่จัดเก็บล็อก (Log) และข้อมูลล็อก (Log) เพื่อป้องกันการเข้าถึงหรือแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต
5. การเตรียมความพร้อมกรณีฉุกเฉิน

เพื่อให้มีการบริหารจัดการความต่อเนื่องให้กับกระบวนการทางธุรกิจที่สำคัญขององค์กร เมื่อมีเหตุการณ์ที่ทำให้เกิดการหยุดชะงักหรือติดขัดต่อกระบวนการดังกล่าว โดยมีแนวปฏิบัติ ดังนี้

 - 5.1 ผู้ดูแลระบบต้องกำหนดระบบที่มีความสำคัญทั้งหมดขององค์กร และจัดทำเป็นบัญชีรายชื่อระบบดังกล่าวรวมทั้งปรับปรุงรายชื่อระบบสำคัญและบัญชีฯ ตามความเป็นจริง
 - 5.2 เจ้าของข้อมูลและผู้ดูแลระบบประเมินความเสี่ยงสำหรับระบบเหล่านั้น กำหนดมาตรการเพื่อลดความเสี่ยงที่พบและจัดทำรายงานการประเมินความเสี่ยง
 - 5.3 ผู้ดูแลระบบจัดทำและปรับปรุงแผนกู้คืนระบบอย่างน้อยปีละ 1 ครั้ง
 - 5.4 เจ้าของข้อมูลและผู้ดูแลระบบต้องทดสอบแผนกู้คืนระบบอย่างน้อยปีละ 1 ครั้ง บันทึกผลการทดสอบรวมถึงปัญหาที่พบ และนำเสนอผลการทดสอบและแนวทางแก้ไขต่อผู้บังคับบัญชา
 - 5.5 ผู้ดูแลระบบต้องจัดประชุมและชี้แจงให้ผู้ที่เกี่ยวข้องทั้งหมดได้รับทราบเกี่ยวกับแผนและผลของการฝึกซ้อมการกู้คืนระบบ

ส่วนที่ 13

การตรวจสอบและประเมินความเสี่ยง

วัตถุประสงค์

- เพื่อให้มีการตรวจสอบการดำเนินงานของระบบจัดการความมั่นคงปลอดภัยสารสนเทศ และปรับปรุงอย่างต่อเนื่อง
- เพื่อควบคุม และติดตามการปฏิบัติงานของผู้ดูแลระบบสารสนเทศ ให้สอดคล้องตามข้อกำหนด กฎหมาย หรือระเบียบข้อบังคับที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ
- เพื่อประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของสารสนเทศและบริหารจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

ผู้รับผิดชอบ

- ผู้บังคับบัญชา
- ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

- ข้อกำหนดหลัก: การวางแผน (Planning)
- ข้อกำหนดหลัก: การตรวจประเมินภายใน (Internal Audit)
- หมวดที่ 8 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations security)
- หมวดที่ 14 ความสอดคล้อง (Compliance)

แนวปฏิบัติ

1. ผู้บังคับบัญชา ต้องกำหนดให้มีแนวทางในการดำเนินงานของระบบสารสนเทศสอดคล้องกับกฎหมาย พระราชบัญญัติ กฎระเบียบ ข้อบังคับที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศโดยต้องจัดทำเป็นลายลักษณ์อักษร และมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
2. ผู้บังคับบัญชา ต้องกำหนดมาตรการในการควบคุมและบริหารจัดการสินทรัพย์ทางปัญญา ได้แก่ ลิขสิทธิ์ในเอกสาร หรือซอฟต์แวร์ เครื่องหมายการค้า สิทธิบัตร และใบอนุญาตการใช้งานซอร์สโค้ด หรือการใช้งานซอฟต์แวร์ เพื่อให้การดำเนินงานเป็นไปตามข้อกำหนดทั้งในแง่ของข้อสัญญา และด้านกฎหมาย พระราชบัญญัติ กฎระเบียบ ข้อบังคับด้านสินทรัพย์ทางปัญญาที่เกี่ยวข้อง
3. ผู้บังคับบัญชา ต้องควบคุมให้มีการคุ้มครองข้อมูลส่วนบุคคลโดยให้สอดคล้องกับกฎหมาย พระราชบัญญัติ กฎระเบียบ ข้อบังคับที่เกี่ยวข้อง
4. ผู้บังคับบัญชา ต้องกำกับดูแล และควบคุมการปฏิบัติงานของผู้ที่อยู่ใต้การบังคับบัญชา เพื่อป้องกันการใช้งานระบบสารสนเทศผิดวัตถุประสงค์ หรือละเมิดต่อนโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของ รพม.
5. ผู้บังคับบัญชา ต้องควบคุมให้มีการป้องกันข้อมูลสำคัญขององค์กร ข้อมูลสำคัญที่เกี่ยวข้องกับข้อกำหนดทางกฎหมาย ระเบียบ ข้อบังคับ สัญญา ควรได้รับการป้องกันจากการสูญหาย ถูกทำลาย และปลอมแปลง
6. ผู้บังคับบัญชาต้องจัดให้มีการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยผู้ตรวจสอบภายใน (Internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External auditor) ตามระยะเวลาอย่างน้อยปีละ 1 ครั้ง

7. ผู้ดูแลระบบ ต้องติดตามผลการใช้งานทรัพยากรสารสนเทศ (Capacity) และวางแผนด้านทรัพยากรสารสนเทศให้รองรับการปฏิบัติงานในอนาคตอย่างเหมาะสม
8. ผู้ดูแลระบบ ต้องป้องกันการเข้าใช้งานเครื่องมือที่ใช้เพื่อการตรวจสอบ เพื่อมิให้เกิดการใช้งานผิดประเภท หรือถูกละเมิดการใช้งาน (Compromise) โดยควบคุมการเข้าถึง และตรวจสอบการนำเครื่องมือไปใช้งานอย่างสม่ำเสมอ
9. ผู้ดูแลระบบต้องประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
10. ผู้บังคับบัญชาต้องติดตามผลการดำเนินการตามแผนบริหารจัดการความเสี่ยง (Risk treatment plan) เป็นประจำทุกไตรมาส
11. ผู้ดูแลระบบต้องประเมินความเสี่ยงแล้วจัดลำดับความสำคัญของความเสี่ยงนั้นและค้นหาวิธีการเพื่อลดความเสี่ยงตามขั้นตอนที่ รพม. กำหนด พร้อมทั้งพิจารณาข้อดีข้อเสียของวิธีการเหล่านั้นเพื่อให้ผู้บริหารของ รพม. ตัดสินใจเลือกวิธีการเพื่อลดความเสี่ยงหรือยอมรับความเสี่ยง เมื่อเลือกวิธีการลดความเสี่ยงแล้วผู้บริหารต้องจัดสรรทรัพยากรอย่างเพียงพอเพื่อดำเนินการ แนวทางการลดความเสี่ยง แบ่งได้เป็น 3 รูปแบบ ได้แก่
 - 11.1 การเลือกใช้เทคโนโลยี เพื่อใช้ในการลดความเสี่ยงและเพิ่มความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รพม. เป็นวิธีที่จำเป็นต้องใช้งบประมาณและทรัพยากรอย่างเพียงพอในการดำเนินการ เช่น การเลือกใช้อุปกรณ์ Firewall มากกว่าหนึ่งผลิตภัณฑ์ในการป้องกันการเข้าถึงเครือข่ายที่สำคัญ การใช้อุปกรณ์สมาร์ตการ์ด หรือ USB Token ในการตรวจสอบยืนยันตัวตนในการเข้าใช้งานระบบจากภายนอก รพม. เป็นต้น
 - 11.2 การปรับเปลี่ยนขั้นตอนปฏิบัติ ต้องออกแบบขั้นตอนปฏิบัติใหม่ที่รัดกุมและสามารถรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รพม. ได้ดีขึ้น เมื่อออกแบบขั้นตอนปฏิบัติใหม่แล้วต้องมีการพิจารณาหาหรือความเหมาะสม ความเป็นไปได้ และผู้บริหารต้องเป็นผู้อนุมัติให้มีการบังคับใช้ขั้นตอนปฏิบัติใหม่นั้น
 - 11.3 ผู้ดูแลระบบต้องแจ้งขั้นตอนปฏิบัติให้ผู้เกี่ยวข้องรับรู้อย่างทั่วถึง รวมทั้งต้องจัดฝึกอบรมผู้ใช้งานที่เกี่ยวข้องเพื่อให้สามารถปฏิบัติตามขั้นตอนปฏิบัติใหม่ได้อย่างราบรื่นและมีประสิทธิภาพ
12. การตรวจสอบความปลอดภัยของระบบสารสนเทศ
 - 12.1 ผู้ดูแลระบบ ต้องวางแผนการตรวจสอบและประเมินช่องโหว่หรือจุดอ่อนด้านความมั่นคงปลอดภัยสารสนเทศ และแจ้งผู้ที่เกี่ยวข้องเพื่อแก้ไขในกรณีที่พบว่าช่องโหว่หรือจุดอ่อนนั้นอาจเป็นเหตุการณ์ด้านความมั่นคงปลอดภัย อย่างน้อยปีละ 1 ครั้ง
 - 12.2 ผู้ดูแลระบบต้องตรวจสอบระบบสารสนเทศที่จะต้องมีการปรับปรุงเมื่อมีเวอร์ชันใหม่ (Patch) รวมทั้งข้อมูลที่เกี่ยวข้องกับช่องโหว่ด้านเทคนิคอย่างสม่ำเสมอเพื่อให้ทราบถึงภัยคุกคามและความเสี่ยง รวมถึงหาวิธีป้องกันและแก้ไขที่เหมาะสมกับช่องโหว่นั้น
 - 12.3 ผู้ใช้งาน ผู้ดูแลระบบ และหน่วยงานภายนอก ต้องบันทึกและรายงานช่องโหว่หรือจุดอ่อนใด ๆ ด้านความมั่นคงปลอดภัยสารสนเทศ ที่อาจสังเกตพบระหว่างการติดตามการใช้งานระบบสารสนเทศ ผ่านช่องทางบริหารจัดการที่กำหนดไว้อย่างเหมาะสม และต้องดำเนินการปิดช่องโหว่ที่มีการตรวจพบหรือได้รับแจ้ง
13. ผู้ดูแลระบบต้องมีการบริหารจัดการการเปลี่ยนแปลงเกี่ยวกับการจัดเตรียมการให้บริการ การดูแลปรับปรุงนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ขั้นตอนปฏิบัติงาน หรือการควบคุมเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ โดยคำนึงถึงระดับความสำคัญของการดำเนินธุรกิจที่เกี่ยวข้องและการประเมินความเสี่ยงอย่างต่อเนื่อง

ส่วนที่ 14

การถ่ายโอน และแลกเปลี่ยนข้อมูลสารสนเทศ

วัตถุประสงค์

- เพื่อให้มีการควบคุมการถ่ายโอนและแลกเปลี่ยนข้อมูลสารสนเทศ ป้องกันการรั่วไหล หรือมีการแก้ไขข้อมูล โดยที่ไม่ได้รับอนุญาต รวมถึงการป้องกันสื่อบันทึกข้อมูลให้มีความปลอดภัยเป็นไปตามข้อกำหนด

ผู้รับผิดชอบ

- ผู้บังคับบัญชา
- เจ้าของข้อมูล
- ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

- หมวดที่ 9 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)

แนวปฏิบัติ

1. ผู้บังคับบัญชา ต้องควบคุมให้มีการจัดทำนโยบาย และขั้นตอนการปฏิบัติเพื่อป้องกันข้อมูลสารสนเทศที่มีการสื่อสาร หรือแลกเปลี่ยนผ่านระบบสารสนเทศให้เหมาะสมตามระดับชั้นความลับข้อมูลสารสนเทศตามชั้นตอนที่ รพม. กำหนด
2. ผู้บังคับบัญชา และเจ้าของข้อมูล ต้องควบคุมให้มีการจัดทำข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศระหว่างองค์กรกับบุคคลหรือหน่วยงานภายนอก
3. ผู้ดูแลระบบ ต้องมีการป้องกันข้อมูลสารสนเทศที่มีการสื่อสารกันผ่านข้อมูลอิเล็กทรอนิกส์ (Electronic messaging) เช่น จดหมายอิเล็กทรอนิกส์ (E-mail) หรือ Instant messaging ด้วยวิธีการหรือมาตรการที่เหมาะสม
4. ผู้ดูแลระบบ ต้องป้องกันข้อมูลสารสนเทศที่มีการแลกเปลี่ยนในการทำพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce) ผ่านเครือข่ายคอมพิวเตอร์สาธารณะ เพื่อมิให้มีการฉ้อโกง ละเมิดสัญญา หรือมีการรั่วไหลหรือข้อมูลสารสนเทศถูกแก้ไขโดยมิได้รับอนุญาต
5. ผู้ดูแลระบบ ต้องป้องกันข้อมูลสารสนเทศที่มีการสื่อสาร หรือแลกเปลี่ยนในการทำธุรกรรมทางออนไลน์ (Online transaction) เพื่อมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ ส่งข้อมูลไปผิดที่ การรั่วไหลของข้อมูล ข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ หรือถูกส่งซ้ำโดยมิได้รับอนุญาต
6. ผู้ดูแลระบบ ต้องควบคุมการรับส่งข้อมูลสารสนเทศเพื่อป้องกันความผิดพลาด ดังนี้
 - 6.1 ความไม่สมบูรณ์ของข้อมูลสารสนเทศที่รับ-ส่ง
 - 6.2 การส่งข้อมูลสารสนเทศผิดจุดหมายปลายทาง
 - 6.3 การเปลี่ยนแปลงข้อมูลสารสนเทศโดยมิได้รับอนุญาต
 - 6.4 การเปิดเผยข้อมูลสารสนเทศโดยมิได้รับอนุญาต
 - 6.5 การเข้าถึงข้อมูลสารสนเทศโดยมิได้รับอนุญาต
 - 6.6 การนำข้อมูลสารสนเทศกลับมาใช้ใหม่โดยมิได้รับอนุญาต
7. เจ้าของข้อมูล และผู้ดูแลระบบ ต้องมีการป้องกันข้อมูลสารสนเทศที่มีการเผยแพร่ต่อสาธารณชนมิให้มีการแก้ไขเปลี่ยนแปลงโดยมิได้รับอนุญาต เพื่อรักษาความถูกต้องครบถ้วนของข้อมูลสารสนเทศ

ส่วนที่ 15

การควบคุมการเข้ารหัส

วัตถุประสงค์

- เพื่อให้มีการเข้ารหัสข้อมูลอย่างเหมาะสมและมีประสิทธิภาพในการปกป้องความลับ ป้องกัน การปลอมแปลงข้อมูล และควบคุมความถูกต้องของข้อมูล

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- เจ้าของข้อมูล
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 6 การเข้ารหัสข้อมูล (Cryptography)

แนวปฏิบัติ

1. เจ้าของข้อมูล ต้องเข้ารหัส หรือการใส่รหัสผ่านข้อมูลอิเล็กทรอนิกส์ขององค์กรตามระดับชั้นความลับเพื่อป้องกันผู้ไม่มีสิทธิเข้าถึง ตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และตามขั้นตอนที่ รพม. กำหนด
2. เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ใช้งานต้องปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 ในการนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับจะต้องใช้วิธีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล
3. ผู้ดูแลระบบ ต้องใช้วิธีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล หลีกเลี่ยงการใช้รูปแบบการเข้ารหัสที่พัฒนาขึ้นเอง เพื่อให้มั่นใจว่าขั้นตอนวิธี (Algorithm) ที่ใช้ในการเข้ารหัสนั้นมีความมั่นคงปลอดภัย ดังนี้

ประเภทกุญแจ / วิธีการเข้ารหัส	เกณฑ์ขั้นต่ำ	ความยาวกุญแจ (อย่างน้อย)
กุญแจแบบสมมาตร (Symmetric)	AES	256 bits
กุญแจแบบอสมมาตร (Asymmetric)	RSA	1024 bits
การ Hashing	SHA-256	256 bits

4. ผู้ดูแลระบบ ต้องมีการทบทวนขั้นตอนวิธี (Algorithm) และความยาวของกุญแจที่เข้ารหัสอย่างน้อยปีละ 1 ครั้ง เพื่อให้ยังสามารถรักษาไว้ซึ่งความมั่นคงปลอดภัย
5. ผู้ดูแลระบบ ต้องกำหนดให้มีการบริหารจัดการกุญแจที่ใช้ในการเข้ารหัส ดังนี้
 - 5.1 การสร้างกุญแจรหัสควรกระทำในสถานที่ที่มีมาตรการป้องกันความปลอดภัย
 - 5.2 เมื่อมีการสร้างกุญแจรหัสที่เป็นกุญแจลับ (Private key) ควรส่งมอบให้กับเจ้าของกุญแจโดยตรง โดยวิธีการที่ปลอดภัย
 - 5.3 ควรจัดให้มีการเก็บบันทึก Log เพื่อการตรวจสอบสำหรับกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับการจัดการกุญแจรหัส

6. ผู้ใช้งาน ควรรักษาความปลอดภัยในการใช้งานกุญแจ ดังนี้
 - 6.1 เก็บกุญแจรหัสในสถานที่ที่ปลอดภัย เช่น ตู้นิรภัย หรือสื่อบันทึกที่ปลอดภัย และไม่มีใครสามารถเข้าถึงได้
 - 6.2 เมื่อมีการรับกุญแจสาธารณะ (Public key) มาใช้ ก่อนใช้งานจะต้องพิสูจน์ความถูกต้องของกุญแจสาธารณะ โดยสอบถามกับผู้ส่งหรือตรวจสอบกับผู้แทนในการรับรองความถูกต้องของกุญแจสาธารณะ (Certificate authority) ที่เชื่อถือได้เท่านั้น
 - 6.3 ควบคุมการใช้งานและจัดเก็บกุญแจให้สอดคล้องกับการรักษาความลับข้อมูลตามที่ รพม. กำหนด

ส่วนที่ 16

การนำอุปกรณ์ส่วนตัวมาใช้งาน (Bring your own device)

วัตถุประสงค์

- เพื่อควบคุมการนำอุปกรณ์ส่วนตัวมาเชื่อมต่อหรือเข้าถึงระบบสารสนเทศของ รพม. ที่ใช้ในการบริหารจัดการระบบสารสนเทศของ รพม. หรือปฏิบัติงานให้ รพม. ทั้งนี้เพื่อป้องกันภัยคุกคามที่อาจเกิดขึ้นกับระบบสารสนเทศของ รพม. รวมถึงเพื่อป้องกันไม่ให้ข้อมูลของ รพม. เกิดการรั่วไหล

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 2 อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากระยะไกล (Mobile devices and teleworking)

แนวปฏิบัติ

1. ผู้ดูแลระบบต้องกำหนดคุณสมบัติของระบบปฏิบัติการของอุปกรณ์ส่วนตัวที่อนุญาตให้นำมาเชื่อมต่อหรือเข้าถึงระบบงานสารสนเทศของ รพม. ได้ โดยต้องเป็นระบบปฏิบัติการที่ไม่ล้าสมัย (Obsolete operating system) และยังได้รับการสนับสนุนการใช้งานจากเจ้าของผลิตภัณฑ์
2. ผู้ดูแลระบบต้องตัดการเชื่อมต่อหากระบบปฏิบัติการของอุปกรณ์ส่วนตัวที่อนุญาตให้นำมาเชื่อมต่อหรือเข้าถึงระบบงานสารสนเทศของ รพม. เกิดการล้าสมัย (Obsolete operating system) หรือเจ้าของผลิตภัณฑ์ไม่สนับสนุนการใช้งานแล้ว
3. ผู้ดูแลระบบต้องมีมาตรการป้องกันมัลแวร์ และตรวจสอบการอัปเดต Patch เวอร์ชันของระบบปฏิบัติการที่เจ้าของผลิตภัณฑ์ยังให้การสนับสนุนการใช้งาน
4. ผู้ดูแลระบบต้องไม่อนุญาตให้อุปกรณ์ที่มีการปรับแต่งการเข้าถึงระบบปฏิบัติการ (rooted/jailbroken) มาเชื่อมต่อหรือเข้าถึงระบบสารสนเทศของ รพม.
5. ผู้ดูแลระบบต้องแบ่งแยกเครือข่ายของอุปกรณ์ส่วนตัวที่นำมาเชื่อมต่อหรือเข้าถึงระบบสารสนเทศของ รพม.
6. ผู้ใช้งานต้องไม่นำอุปกรณ์ส่วนตัวที่ติดตั้งแอปพลิเคชันนอก Official store มาเชื่อมต่อหรือเข้าถึงระบบงานสารสนเทศของ รพม.
7. ผู้ใช้งานต้องไม่นำอุปกรณ์ส่วนตัวที่ติดตั้งโปรแกรมละเมิดลิขสิทธิ์มาเชื่อมต่อหรือเข้าถึงระบบงานสารสนเทศของ รพม.
8. ผู้ใช้งานต้องอัปเดต Patch ของระบบปฏิบัติการที่อุปกรณ์ส่วนตัวให้เป็นเวอร์ชันล่าสุด รวมถึงต้องเป็นระบบปฏิบัติการที่เจ้าของผลิตภัณฑ์ยังให้การสนับสนุนการใช้งาน
9. ผู้ใช้งานต้องยืนยันตัวตนก่อนเข้าถึงระบบสารสนเทศของ รพม. ทุกครั้ง
10. ผู้ใช้งานต้องติดตั้ง Network Access Control agent (NAC agent) หรือ Mobile Device Management agent (MDM agent) ตามที่ รพม. กำหนด เพื่อควบคุมการใช้งานเครือข่ายและการเข้าถึงระบบสารสนเทศของ รพม.
11. กรณีอุปกรณ์ส่วนตัวสูญหายหรือถูกขโมยผู้ใช้งานต้องแจ้งผู้ดูแลระบบโดยเร็วที่สุด เพื่อจัดการข้อมูลที่จัดเก็บอยู่ในอุปกรณ์ส่วนตัวของผู้ใช้งาน

ภาคผนวก ข.

รายงานผลการบำรุงรักษา
ระบบติดตามความก้าวหน้าโครงการ (PPMS)
ประจำไตรมาสที่ (.....-.....)

สัญญาเลขที่

จัดทำโดย

บริษัท

รายงานผลการตรวจสอบระบบติดตามความก้าวหน้าโครงการ (PPMS)

วันที่ เดือน ปี พ.ศ.

PPMS Web Server (Server Name :)

1. ตรวจสอบการทำงานของเครื่องเซิร์ฟเวอร์ (PPMS Web Server)

1.1 ตรวจสอบเวอร์ชันของระบบปฏิบัติการ

1.1.1 Windows Version

----- รูป -----

1.1.2 Windows Update

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

1.2 ตรวจสอบการใช้งานของ CPU

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

1.3 ตรวจสอบการใช้งานของ Memory

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

1.4 ตรวจสอบพื้นที่การใช้งานของ Hard disk

	4/2566	1/2567	2/2567	3/2567	4/2567
Drive C					
Drive D					

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

ศพธธ

1.5 ตรวจสอบรายละเอียดการเชื่อมต่อเครือข่าย

1.5.1 ตรวจสอบ IP address ของเครื่องคอมพิวเตอร์

----- รูป -----

1.5.2 ทดสอบการเชื่อมต่อเครือข่ายกับเครื่อง PPMS Database Server

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

1.6 ตรวจสอบ Log ของเครื่องเซิร์ฟเวอร์

1.6.1 Application log

----- รูป -----

1.6.2 Security log

----- รูป -----

1.6.3 System log

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

1.7 ตรวจสอบวันที่และเวลาของเครื่อง

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

2. ตรวจสอบการทำงานของ PPMS Application

2.1 ตรวจสอบการทำงานของ Service ของ Web server

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

2.2 ตรวจสอบ Version ของ PPMS Application

2.2.1 PPMS Production

Path ที่จัดเก็บ :

	4/2566	1/2567	2/2567	3/2567	4/2567
version					

----- รูป -----

2.2.2 PPMS Test

Path ที่จัดเก็บ :

	4/2566	1/2567	2/2567	3/2567	4/2567
version					

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

2.3 ตรวจสอบการสำรองข้อมูลของ PPMS Application

Path ที่จัดเก็บ :

	4/2566	1/2567	2/2567	3/2567	4/2567
Folder Size					

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

2.4 ตรวจสอบ Log ของ PPMS Application

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

PPMS Database Server (Server Name :)

3. ตรวจสอบการทำงานของเครื่องเซิร์ฟเวอร์ (PPMS Database Server)

3.1 ตรวจสอบเวอร์ชันของระบบปฏิบัติการ

3.1.1 Windows Version

----- รูป -----

3.1.2 Windows Update

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

3.2 ตรวจสอบการใช้งานของ CPU

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

3.3 ตรวจสอบการใช้งานของ Memory

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

3.4 ตรวจสอบพื้นที่การใช้งานของ Hard disk

	4/2566	1/2567	2/2567	3/2567	4/2567
Drive C					
Drive D					

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

3.5 ตรวจสอบรายละเอียดการเชื่อมต่อเครือข่าย

3.5.1 ตรวจสอบ IP address ของเครื่องคอมพิวเตอร์

----- รูป -----

3.5.2 ทดสอบการเชื่อมต่อเครือข่ายกับเครื่อง PPMS Web Server

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

3.6 ตรวจสอบ Log ของเครื่องเซิร์ฟเวอร์

3.6.1 Application log

----- รูป -----

3.6.2 Security log

----- รูป -----

3.6.3 System log

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

3.7 ตรวจสอบวันที่และเวลาของเครื่อง

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

4. ตรวจสอบการทำงานของ PPMS Database

4.1 ตรวจสอบการทำงานของ Service ของ PPMS Database

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

4.2 ตรวจสอบการใช้พื้นที่ของฐานข้อมูล

4.2.1 PPMS Production

Database file name :

Database log name :

	4/2566	1/2567	2/2567	3/2567	4/2567
Database file size					
Database log size					

----- รูป -----

4.2.2 PPMS Test

Database file name :

Database log name :

	4/2566	1/2567	2/2567	3/2567	4/2567
Database file size					
Database log size					

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

4.3 ตรวจสอบการสำรองข้อมูลของ PPMS Database

Path ที่จัดเก็บ :

	4/2566	1/2567	2/2567	3/2567	4/2567
File size					

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

4.4 ตรวจสอบการทำงานของ JOB

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

5. ตรวจสอบการทำงานของระบบติดตามความก้าวหน้าโครงการ (PPMS)

5.1 ตรวจสอบการเข้าใช้งาน (Authentication Testing)

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

5.2 ตรวจสอบประสิทธิภาพการให้บริการในการตอบสนองการเรียกใช้งาน (Response Time) *

หมายเหตุ:

* ตรวจสอบระยะเวลาในการตอบสนองการเรียกใช้งานไม่ควรเกิน 4 วินาที (อย่างน้อย 3 หน้าจอ)

----- รูป -----

Response Time วินาที

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

5.3 ตรวจสอบการหมดเวลาใช้งานระบบสารสนเทศ (Session Time - Out)

ระบบติดตามความก้าวหน้าโครงการ (PPMS) (15 นาที หรือตามที่ระบบฯ กำหนด)

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

5.4 ตรวจสอบการออกรายงาน

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

ลงชื่อ ผู้ตรวจสอบ

()

วันที่

ศพนงมา

รายงานการตรวจสอบสิทธิการเข้าถึงระบบ (Role Matrix) ระบบติดตามความก้าวหน้าโครงการ (PPMS)

การรถไฟฯขนส่งมวลชนแห่งประเทศไทย

ประจำไตรมาสที่ (ตั้งแต่วันที่ ถึงวันที่

ที่	ชื่อ - สกุล	Application Server				Database Server				Application				DBMS			
		Super Administrator	Administrator	Super User	User	การเข้าถึงเอกสาร (F/C/R/U/D)	Super Administrator	Administrator	Super User	User	การเข้าถึงเอกสาร (F/C/R/U/D)	Super Administrator	Administrator	Super User	User	การเข้าถึงเอกสาร (F/C/R/U/D)	

หมายเหตุ : การเข้าถึงเอกสาร F : Full, C : Create, R : Read, U : Update, D : Delete

* Super Administrator : ผู้มีสิทธิ์สามารถกำหนดสิทธิ์ และบริหารจัดการข้อมูลเครื่องเซิร์ฟเวอร์ ภายใต้ Domain ได้ (Domain Admin)

* Administrator : ผู้มีสิทธิ์สามารถกำหนดสิทธิ์ และบริหารจัดการข้อมูลเครื่องเซิร์ฟเวอร์ที่มีสิทธิ์ได้ (Local Admin) รวมทั้งกำหนดสิทธิ์ให้กับผู้ใช้งานระบบสารสนเทศต่าง ๆ ได้

* Super User : ผู้มีสิทธิ์สามารถจัดการข้อมูลภายในระบบสารสนเทศต่าง ๆ ได้

* User : ผู้ใช้งานทั่วไป เข้าถึง เรียกดูข้อมูลภายในระบบงานสารสนเทศต่าง ๆ ได้

รายงานสรุปการแจ้งปัญหาและการแก้ไขระบบติดตามความก้าวหน้าโครงการ (PPMS)
การรถไฟฟ้ามหานครตามแนวทางประเทศไทย
ประจำไตรมาสที่ (ตั้งแต่วันที่ ถึงวันที่

ลำดับ	วันที่รับแจ้ง	เลขที่รับแจ้ง	ผู้แจ้ง	ช่องทาง การรับแจ้ง	รายละเอียด	วันที่ดำเนินการ แล้วเสร็จ	ผลการ ดำเนินการ/ การแก้ไข	ผู้ดำเนินการแก้ไข	สถานะ

หมายเหตุ หากมีการปรับปรุงเวอร์ชันซอฟต์แวร์ให้ระบุเป็นช่องผลการดำเนินการ/การแก้ไขด้วย

รายงานผลการปิดช่องโหว่ระบบติดตามความก้าวหน้าโครงการ (PPMS)

การรถไฟฟ้ามหานครแห่งประเทศไทย

ประจำไตรมาสที่ (ตั้งแต่วันที่ ถึงวันที่

ลำดับ	วันที่พบ ช่องโหว่	หมายเลข ช่องโหว่	ชื่อช่องโหว่	รายละเอียด	ผลการดำเนินการ/ การแก้ไข/ ผลกระทบ	ผู้ดำเนินการแก้ไข	วันที่ ดำเนินการ แล้วเสร็จ	สถานะ

รายงานทะเบียนทรัพย์สิน (Asset Inventory) ระบบติดตามความก้าวหน้าโครงการ (PPMS)

การรถไฟฯขนส่งมวลชนแห่งประเทศไทย

ประจำไตรมาสที่ (ตั้งแต่วันที่ ถึงวันที่

ลำดับ	รายการทรัพย์สิน	End of Support	End of Life	กลุ่มทรัพย์สิน	ประเภททรัพย์สิน	Firmware/ Patch Version	สถานที่จัดเก็บ	ผู้บันทึก

PPMS

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและรายละเอียดค่าใช้จ่าย
การจัดซื้อจัดจ้างที่มีใ้ใช้งานก่อสร้าง

ชื่อโครงการ	จ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ประจำปีงบประมาณ 2567
1. หน่วยงานเจ้าของโครงการ	ฝ่ายเทคโนโลยีสารสนเทศ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
2. วงเงินงบประมาณที่ได้รับจัดสรร	1,350,000.00 บาท (หนึ่งล้านสามแสนห้าหมื่นบาทถ้วน)
3. วันที่กำหนดราคากลาง (ราคาอ้างอิง) ณ วันที่ เป็นเงิน	23 มิถุนายน 2566 650,000.00 บาท (หกแสนห้าหมื่นบาทถ้วน) (รวมภาษีมูลค่าเพิ่ม)
4. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)	ราคาที่ได้มาจากการสืบราคาจากท้องตลาด โดยสืบราคาจากผู้รับจ้างรายเดิม (บริษัท เอทูพี โซลูชั่น จำกัด)
5. รายชื่อผู้รับผิดชอบกำหนดราคากลาง	นางสาวสุพรรณษา นิลสมบูรณ์ โปรแกรมเมอร์ ระดับ 7

สุพรรณษา

บริษัท เอที โซลูชั่น จำกัด (สนญ.)

503/5 อาคารเค.เอส.แอล ทาวเวอร์ ชั้น 4 ถนนศรีอยุธยา
 แขวงถนนพญาไท เขตราชเทวี กรุงเทพมหานคร 10400
 โทรศัพท์ 02-065-5448, 086-375-5448
 เลขประจำตัวผู้เสียภาษี 0105555029721



ใบเสนอราคา

รหัส	018	วันที่	23/06/2566
นามลูกค้า	การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย	เลขที่ใบเสนอราคา	SO50100
ที่อยู่	175 ถ.พระราม 9 แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพฯ 10310	ผู้เสนอราคา	ยุทธศักดิ์
หมายเหตุ	Tax Id.0994000165706	เงื่อนไขการชำระเงิน	
		วันที่ครบกำหนด	

บริษัทฯ มีความยินดีขอเสนอราคา และ รายละเอียดของสินค้าตามรายการดังต่อไปนี้
 We take pleasure in quoting the following products with price and specification

รหัสสินค้า Code	รายละเอียด Description	จำนวน Qty.	ราคาต่อหน่วย Unit	ส่วนลด Discount	จำนวนเงิน Amount
100035	จ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ของ รฟม. ประจำปีงบประมาณ พ.ศ.2567 (ตุลาคม พ.ศ.2566 - กันยายน พ.ศ.2567)	1 ระบบ	650,000.00		650,000.00

บาท หกแสนห้าหมื่นบาทถ้วน		รวมเป็นเงิน	607,476.64
<ul style="list-style-type: none"> - กำหนดยืนยันราคา 90 วันนับตั้งแต่วันที่ระบุในใบเสนอราคาฉบับนี้ - กรณีลงนามในชื่อ "ผู้สั่งซื้อสินค้า" พร้อมประทับตรา (ถ้ามี) เพื่อยืนยันการสั่งซื้อ 		ภาษีมูลค่าเพิ่ม 7.00%	42,523.36
<ul style="list-style-type: none"> - โอนเงินผ่าน ธนาคารไทยพาณิชย์ เลขที่ 071-285235-3 ชื่อบัญชี บริษัท เอที โซลูชั่น จำกัด 		ยอดเงินสุทธิ	650,000.00

ผู้สั่งซื้อสินค้า	ผู้เสนอราคา	ผู้ตรวจสอบ	ผู้อนุมัติ
วันที่/..../.....	 วันที่ 23 6 2566	วันที่/..../.....	วันที่/..../.....

ยุทธศักดิ์



เอกสารแนบ 2

ฝจบ
เลขรับ 2888
วันที่ 11/07/66
เวลา 17.47

บันทึกข้อความ


กพท.
เลขรับ.....1515.....
วันที่ 12 ก.ค.66 เวลา 9.16 น.

ส่วนราชการ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
ที่ ฝจบ๑๑/๑๓๘ วันที่ ๑๑ กรกฎาคม ๒๕๖๖
เรื่อง ขอความเห็นชอบประกาศเผยแพร่แผนการจัดซื้อจัดจ้าง ประจำปีงบประมาณ พ.ศ. ๒๕๖๗

เรียน ผอ.ฝจบ.

ตามพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ.๒๕๖๐ มาตรา ๑๑ ใหหน่วยงานของรัฐจัดทำแผนการจัดซื้อจัดจ้างประจำปี และประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศกรมบัญชีกลางและของหน่วยงานของรัฐตามวิธีการที่กรมบัญชีกลางกำหนดและให้ปิดประกาศโดยเปิดเผย ณ สถานที่ปิดประกาศของหน่วยงานของรัฐ นั้น

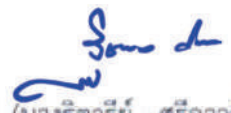
การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย (รฟม.) ได้จัดทำประกาศเผยแพร่แผนการจัดซื้อจัดจ้าง แล้วเสร็จ
จึงเรียนมาเพื่อโปรดพิจารณา หากเห็นชอบขอได้โปรดลงนามประกาศเผยแพร่แผนการจัดซื้อจัดจ้างดังกล่าว



(นางจิติารีย์ ศรีอารุฑ)
ผอ.กพท.
๑๑ ก.ค. ๖๖

เขียน ทน.จท.1 ทน.จท.2 ทน.บพ.
 อื่น ๆ
เพื่อโปรด ดำเนินการ เขียน
 อื่น ๆ

เห็นชอบตามเสนอ
+
ลงนามแล้ว

(นายวิช พึ่งตน)
ผอ.ฝจบ.
12/07/66


(นางจิติารีย์ ศรีอารุฑ)
ผอ.กพท.
12 ก.ค. 66

เรียน คุณณโพลิน
เพื่อดำเนินการต่อไป

12 ก.ค. 66



ประกาศ การรถไฟฟ้านครหลวงแห่งประเทศไทย
เรื่อง เผยแพร่แผนการจัดซื้อจัดจ้าง ประจำปีงบประมาณ พ.ศ. ๒๕๖๗

ตามพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐ กำหนดให้หน่วยงานของรัฐจัดทำแผนการจัดซื้อจัดจ้างประจำปี และประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลางและของหน่วยงานของรัฐตามที่กรมบัญชีกลางกำหนด และให้ปิดประกาศโดยเปิดเผย ณ สถานที่ปิดประกาศของหน่วยงานของรัฐ นั้น

การรถไฟฟ้านครหลวงแห่งประเทศไทย ขอประกาศเผยแพร่แผนการจัดซื้อจัดจ้าง ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ ตามเอกสารที่แนบท้ายประกาศนี้

ประกาศ ณ วันที่ ๑๒ กรกฎาคม พ.ศ. ๒๕๖๖

(นายวิท พึ่งตน)

ผู้อำนวยการฝ่ายจัดซื้อและบริการ
ปฏิบัติการแทน ผู้อำนวยการรถไฟฟ้านครหลวงแห่งประเทศไทย

ผู้อำนวยการกอง.....วันที่ 11 / ก.ค. / 66
หัวหน้าแผนก.....วันที่ 11 / ก.ค. / 66
เจ้าหน้าที่.....วันที่ 11 / ก.ค. / 66

รายละเอียดแนบท้ายประกาศเผยแพร่แผนการจัดซื้อจัดจ้างประจำปีงบประมาณ พ.ศ. ๒๕๖๗
การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย (M๖๖๐๗๐๐๐๗๑๘๗) ลงวันที่ ๑๒ กรกฎาคม พ.ศ. ๒๕๖๖

ลำดับ ที่	รหัสแผนจัดซื้อจัด จ้าง	ชื่อโครงการ	งบประมาณ โครงการ (บาท)	คาดว่าจะ ประกาศจัด ซื้อจัดจ้าง (เดือน/ปี)
๑	P๖๖๐๗๐๐๐๗๑๘๖	งานจ้างบำรุงรักษาระบบติดตามความก้าวหน้า โครงการ (Project Progress Monitoring System PPMS) ประจำปีงบประมาณ ๒๕๖๗	๑,๓๕๐,๐๐๐.๐๐	๐๗/๒๕๖๖



ประกาศ การรถไฟฟ้านครหลวงแห่งประเทศไทย
เรื่อง เผยแพร่แผนการจัดซื้อจัดจ้าง ประจำปีงบประมาณ พ.ศ. ๒๕๖๗

ตามพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐ กำหนดให้หน่วยงานของรัฐจัดทำแผนการจัดซื้อจัดจ้างประจำปี และประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลางและของหน่วยงานของรัฐตามที่กรมบัญชีกลางกำหนด และให้ปิดประกาศโดยเปิดเผย ณ สถานที่ปิดประกาศของหน่วยงานของรัฐ นั้น

การรถไฟฟ้านครหลวงแห่งประเทศไทย ขอประกาศเผยแพร่แผนการจัดซื้อจัดจ้าง ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ ตามเอกสารที่แนบท้ายประกาศนี้

ประกาศ ณ วันที่ ๑๒ กรกฎาคม พ.ศ. ๒๕๖๖

(นายทวิช พึ่งตน)

ผู้อำนวยการฝ่ายจัดซื้อและบริการ
ปฏิบัติการแทน ผู้อำนวยการการรถไฟฟ้านครหลวงแห่งประเทศไทย
ประเทศไทย

รายละเอียดแนบท้ายประกาศเผยแพร่แผนการจัดซื้อจัดจ้างประจำปีงบประมาณ พ.ศ. ๒๕๖๗
การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย (M๖๖๐๗๐๐๐๗๑๘๗) ลงวันที่ ๑๒ กรกฎาคม พ.ศ. ๒๕๖๖

ลำดับ ที่	รหัสแผนจัดซื้อจัด จ้าง	ชื่อโครงการ	งบประมาณ โครงการ (บาท)	คาดว่าจะ ประกาศจัด ซื้อจัดจ้าง (เดือน/ปี)
๑	P๖๖๐๗๐๐๐๗๑๘๖	งานจ้างบำรุงรักษาระบบติดตามความก้าวหน้า โครงการ (Project Progress Monitoring System PPMS) ประจำปีงบประมาณ ๒๕๖๗	๑,๓๕๐,๐๐๐.๐๐	๐๗/๒๕๖๖



บันทึกข้อความ

การรถไฟฟ้านครหลวงแห่งประเทศไทย

ฝทท.(ภายใน)
เลขที่ 1832
วันที่ 23 มิ.ย. 66
เวลา 08.41 น.

กรค.(ภายใน)
เลขที่ 1136
วันที่ 22 มิ.ย. 66
เวลา 15.41 น.

ฝจบ

เลขรับ 2540
วันที่ 23/06/66
เวลา 09.39

กพท.

เลขรับ 1344
วันที่ 23 มิ.ย.66 เวลา 11.03 น.

ส่วนงาน ฝ่ายเทคโนโลยีสารสนเทศ โทร. 2587

ที่ ฝทท21/ 97 วันที่ 22 มิถุนายน 2566

เรื่อง ขอบจัดสร้างขอบเขตของงานและราคากลางจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ประจำปีงบประมาณ 2567

เรียน ผอ.ฝจบ. ผ่าน ผอ.ฝทท. ผอ.กรค. ทน.สค.
22 มิ.ย. 66

1. ข้อเท็จจริง

1.1 ฝทท. ได้มีบันทึกที่ ฝทท/429 ลงวันที่ 12 กรกฎาคม 2565 จัดส่งรายละเอียดคำขอตั้งงบประมาณรายจ่าย หมวดค่าใช้สอย รายการค่าซ่อมแซมครุภัณฑ์ ประจำปีงบประมาณ 2567 เพื่อให้ ฝจบ. รวบรวมคำขอตั้งงบประมาณฯ ดังกล่าว โดยขอตั้งงบประมาณสำหรับจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ประจำปีงบประมาณ 2567 เป็นจำนวนเงินทั้งสิ้น 1,350,000 บาท (หนึ่งล้านสามแสนห้าหมื่นบาทถ้วน) (รวมภาษีมูลค่าเพิ่ม) ทั้งนี้ คณะกรรมการ รพม. ในคราวประชุมครั้งที่ 12/2565 เมื่อวันที่ 30 พฤศจิกายน 2565 ได้มีมติเห็นชอบกรอบงบประมาณประจำปีงบประมาณ 2567 แล้ว (เอกสารแนบ 1)

1.2 รพม. ได้ดำเนินการจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) จากบริษัท เอทูพี โซลูชั่น จำกัด ตามสัญญาเลขที่ จ(ข)5/2566 ลงวันที่ 3 ตุลาคม 2565 ซึ่งสัญญาดังกล่าวจะสิ้นสุดในวันที่ 30 กันยายน 2566 (เอกสารแนบ 2)

1.3 ฝทท. ได้มีบันทึกที่ ฝทท/228 ลงวันที่ 7 เมษายน 2566 เพื่อขอความเห็นชอบแต่งตั้ง นางสาวสุพรรณษา นิลสมบุรณ์ โปรแกรมเมอร์ ระดับ 7 แผนกสนับสนุนระบบงานคอมพิวเตอร์ กองระบบงานคอมพิวเตอร์ ฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบในการจัดทำขอบเขตของงานและราคากลางจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ประจำปีงบประมาณ 2567 โดย ผอ.ฝจบ. ได้เห็นชอบตามท้ายบันทึกดังกล่าว เรียบร้อยแล้ว (เอกสารแนบ 3)

1.4 ฝทท. ได้มีบันทึกที่ ฝทท/ว283 ลงวันที่ 26 เมษายน 2566 ขอความอนุเคราะห์ ฝบก.1 ฝบก.2 ฝพค. และ ฝวส. มอบหมายพนักงานเข้าร่วมเป็นคณะกรรมการจ้างและคณะกรรมการตรวจรับพัสดุจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ประจำปีงบประมาณ 2567 โดย ฝบก.1 ได้มีบันทึกที่ ฝบก1/249 ลงวันที่ 8 พฤษภาคม 2566 ฝบก.2 ได้มีบันทึกที่ ฝบก2/223 ลงวันที่ 28 เมษายน 2566 ฝพค. ได้มีบันทึกที่ ฝพค/482 ลงวันที่ 2 พฤษภาคม 2566 และ ฝวส. ได้มีบันทึกที่ ฝวส/294 ลงวันที่ 27 เมษายน 2566 แจ้งรายชื่อพนักงานในสังกัดเข้าร่วมเป็นคณะกรรมการฯ เพื่อให้ ฝทท. ดำเนินการในส่วนที่เกี่ยวข้องต่อไป ทั้งนี้ ข้าพเจ้า ได้จัดทำรายชื่อคณะกรรมการฯ จ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ประจำปีงบประมาณ 2567 เรียบร้อยแล้ว (เอกสารแนบ 4)

2. ข้อกฎหมาย

2.1 พระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560

มาตรา 4

“ราคากลาง” หมายความว่า ราคาเพื่อใช้เป็นฐานสำหรับเปรียบเทียบราคาที่ยื่นข้อเสนอได้ยื่นเสนอไว้ซึ่งสามารถจัดซื้อจัดจ้างได้จริงตามลำดับ ดังต่อไปนี้

/ (1) ราคาที่ได้มา...

- (1) ราคาที่ได้มาจากการคำนวณตามหลักเกณฑ์ที่คณะกรรมการราคากลางกำหนด
- (2) ราคาที่ได้มาจากฐานข้อมูลราคาอ้างอิงของพัสดุที่กรมบัญชีกลางจัดทำ
- (3) ราคามาตรฐานที่สำนักงบประมาณหรือหน่วยงานกลางอื่นกำหนด
- (4) ราคาที่ได้มาจากการสืบราคาจากท้องตลาด
- (5) ราคาที่เคยซื้อหรือจ้างครั้งหลังสุดภายในระยะเวลาสองปีงบประมาณ
- (6) ราคาอื่นใดตามหลักเกณฑ์ วิธีการ หรือแนวทางปฏิบัติของหน่วยงานของรัฐนั้น ๆ

ในกรณีที่มีราคาตาม (1) ให้ใช้ราคาตาม (1) ก่อน ในกรณีที่ไม่มีราคาตาม (1) แต่มีราคาตาม (2) หรือ (3) ให้ใช้ราคาตาม (2) หรือ (3) ก่อน โดยจะใช้ราคาใดตาม (2) หรือ (3) ให้คำนึงถึงประโยชน์ของหน่วยงานของรัฐเป็นสำคัญ ในกรณีที่ไม่มีราคาตาม (1) (2) และ (3) ให้ใช้ราคาตาม (4) (5) หรือ (6) โดยจะใช้ราคาใดตาม (4) (5) หรือ (6) ให้คำนึงถึงประโยชน์ของหน่วยงานของรัฐเป็นสำคัญ

มาตรา 56 การจัดซื้อจัดจ้างพัสดุ ให้หน่วยงานของรัฐเลือกใช้วิธีประกาศเชิญชวนทั่วไปก่อน เว้นแต่

- (2) กรณีดังต่อไปนี้ ให้ใช้วิธีเฉพาะเจาะจง

(ค) การจัดซื้อจัดจ้างพัสดุที่มีผู้ประกอบการซึ่งมีคุณสมบัติโดยตรงเพียงรายเดียว หรือการจัดซื้อจัดจ้างพัสดุจากผู้ประกอบการซึ่งเป็นตัวแทนจำหน่ายหรือตัวแทนผู้ให้บริการโดยชอบด้วยกฎหมายเพียงรายเดียวในประเทศไทยและไม่มีพัสดุนั้นที่จะใช้ทดแทนได้

2.2 ระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560

ข้อ 9 การดำเนินการจัดซื้อจัดจ้างและการบริหารพัสดุตามระเบียบนี้ด้วยวิธีการทางอิเล็กทรอนิกส์ ให้หน่วยงานของรัฐดำเนินการในระบบเครือข่ายสารสนเทศของกรมบัญชีกลางผ่านทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement: e - GP) ตามวิธีการที่กรมบัญชีกลางกำหนด

ให้หน่วยงานของรัฐใช้เอกสารที่จัดพิมพ์จากระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ เป็นเอกสารประกอบการดำเนินการจัดซื้อจัดจ้างตามวิธีการที่กำหนดในระเบียบนี้

ข้อ 21 ในการซื้อหรือจ้างที่มีใช้การจ้างก่อสร้าง ให้หัวหน้าหน่วยงานของรัฐแต่งตั้งคณะกรรมการขึ้นมาคณะหนึ่ง หรือจะให้เจ้าหน้าที่หรือบุคคลใดบุคคลหนึ่งรับผิดชอบในการจัดทำร่างขอบเขตของงานหรือรายละเอียดคุณลักษณะเฉพาะของพัสดุที่จะซื้อหรือจ้าง รวมทั้งกำหนดหลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอด้วยองค์ประกอบ ระยะเวลาการพิจารณา และการประชุมของคณะกรรมการตามวรรคหนึ่ง และวรรคสอง ให้เป็นไปตามที่หัวหน้าหน่วยงานของรัฐกำหนดตามความจำเป็นและเหมาะสม

ข้อ 25 ในการดำเนินการซื้อหรือจ้างแต่ละครั้ง ให้หัวหน้าหน่วยงานของรัฐแต่งตั้งคณะกรรมการซื้อหรือจ้างขึ้น เพื่อปฏิบัติการตามระเบียบนี้ พร้อมกับกำหนดระยะเวลาในการพิจารณาของคณะกรรมการ แล้วแต่กรณี คือ

- (4) คณะกรรมการซื้อหรือจ้างโดยวิธีเฉพาะเจาะจง

- (5) คณะกรรมการตรวจรับพัสดุ

ข้อ 26 คณะกรรมการซื้อหรือจ้างตามข้อ 25 แต่ละคณะประกอบด้วย ประธานกรรมการ 1 คน และกรรมการอย่างน้อย 2 คน ซึ่งแต่งตั้งจากข้าราชการ ลูกจ้างประจำ พนักงานราชการ พนักงานมหาวิทยาลัย พนักงานของรัฐ หรือพนักงานของหน่วยงานของรัฐที่เรียกชื่ออย่างอื่น โดยให้คำนึงถึงลักษณะหน้าที่และความรับผิดชอบของผู้ที่ได้รับแต่งตั้งเป็นสำคัญ

ในกรณีจำเป็นหรือเพื่อประโยชน์ของหน่วยงานของรัฐจะแต่งตั้งบุคคลอื่นร่วมเป็นกรรมการด้วยก็ได้ แต่จำนวนกรรมการที่เป็นบุคคลอื่นนั้นจะต้องไม่มากกว่าจำนวนกรรมการตามวรรคหนึ่ง

เรียน ผอ.กพท ผอ.กพค ผอ.กสย
 นายณ พฤษ ทน.ขอ.จบ

เพื่อโปรด

ทราบ ตรวจสอบ
 พิจารณา ดำเนินการ
 ติดตาม เวียน
 อื่นๆ.....



(นายวิช พึ่งตน)

ผอ.ฝจบ

23/06/66

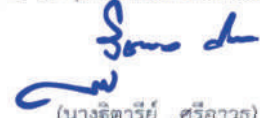
เรียน ทน.จพ.1 ทน.จพ.2 ทน.บพ.

อื่น ๆ

เพื่อโปรด

ดำเนินการ เวียน

อื่น ๆ



(นางฐิตารีย์ ศรีอารุท)

ผอ.กพท.

23 มิ.ย. 66

เรียน คุณไพลิน
เพื่อดำเนินการ



23 มิ.ย. 66

ในการซื้อหรือจ้างครั้งเดียวกัน ห้ามแต่งตั้งผู้ที่เป็นกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์ กรรมการพิจารณาผลการประกวดราคา หรือกรรมการซื้อหรือจ้างโดยวิธีคัดเลือกเป็นกรรมการตรวจรับพัสดุ

2.3 คำสั่งการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย ที่ 98/2564 ลงวันที่ 5 เมษายน 2564 เรื่อง มอบอำนาจเกี่ยวกับการจัดซื้อหรือจัดจ้างพัสดุ

2. มอบอำนาจดำเนินการและอำนาจสั่งซื้อหรือสั่งจ้าง ดังนี้

2.3 การสั่งซื้อหรือสั่งจ้างโดยวิธีเฉพาะเจาะจงครั้งหนึ่ง ให้เป็นอำนาจของผู้ดำรงตำแหน่งและภายในวงเงิน ดังต่อไปนี้

(1) ผู้อำนวยการกองจัดหาพัสดุทั่วไป ไม่เกิน 500,000 บาท (ห้าแสนบาทถ้วน)

(2) ผู้อำนวยการฝ่ายจัดซื้อและบริการ ไม่เกิน 5,000,000 บาท (ห้าล้านบาทถ้วน)

(3) รองผู้ว่าการ (บริหาร) ไม่เกิน 10,000,000 บาท (สิบล้านบาทถ้วน)

3. การมอบอำนาจตามคำสั่งนี้ให้ครอบคลุมถึงการดำเนินการทุกกระบวนการตามพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 ระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 กฎกระทรวง และประกาศที่ออกตามความในพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 และมติคณะรัฐมนตรีที่เกี่ยวข้อง ภายในอำนาจและวงเงินตามข้อ 2 ทั้งนี้ สำหรับการบอกเลิกหรือการตกลงเลิกสัญญาหรือข้อตกลง การแก้ไขสัญญาหรือข้อตกลง การงดหรือลดค่าปรับให้แก่คู่สัญญาหรือการขยายเวลาทำการตามสัญญาหรือข้อตกลง ให้เสนอผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทยพิจารณาให้ความเห็นชอบก่อน และเมื่อผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทยได้พิจารณาให้ความเห็นชอบแล้ว ให้ผู้รับมอบอำนาจตามข้อ 2.1 ข้อ 2.2 และข้อ 2.3 มีหนังสือแจ้งการบอกเลิก หรือการตกลงเลิกสัญญาหรือข้อตกลง การงดหรือลดค่าปรับให้แก่คู่สัญญา การขยายเวลาทำการตามสัญญาหรือข้อตกลงหรือลงนามในสัญญาหรือข้อตกลงแล้วแต่กรณีต่อไป เว้นแต่ ผู้รับมอบอำนาจตามข้อ 2.3 (1) ให้สามารถดำเนินการได้โดยไม่ต้องเสนอผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทยพิจารณาให้ความเห็นชอบก่อน

3. ข้อพิจารณา

ข้าพเจ้า ได้จัดทำร่างขอบเขตของงานจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ประจำปีงบประมาณ 2567 มีการกำหนดหลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ (เอกสารแนบ 5) และกำหนดราคากลาง (เอกสารแนบ 6) เสร็จเรียบร้อยแล้ว ซึ่งเห็นว่าผู้รับจ้างรายเดิม คือ บริษัท เอทพี โซลูชั่น จำกัด มีคุณสมบัติโดยตรงเพียงรายเดียว และมีความเชี่ยวชาญเป็นพิเศษ รวมทั้งเป็นผู้ออกแบบและพัฒนาระบบดังกล่าว จึงเห็นควรให้ผลจบ. ดำเนินการจ้างบำรุงรักษาระบบฯ เพื่อให้ระบบสามารถใช้งานได้อย่างต่อเนื่องและมีประสิทธิภาพ โดยอาศัยอำนาจแห่งพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 ประกอบกับระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 และคำสั่ง รพม. ที่ 98/2564 ลงวันที่ 5 เมษายน 2564 เรื่อง มอบอำนาจเกี่ยวกับการจัดซื้อหรือจัดจ้างพัสดุ

4. ข้อเสนอ

จึงเรียนมาเพื่อโปรดดำเนินการ ตามข้อ 3. ต่อไป จะขอคุณยิ่ง



(นางสาวสุพรรณษา นิลสมบุญ)

โปรแกรมเมอร์ ระดับ 7



บันทึก การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

ที่..... ผทท/429.....วันที่..... 12 กรกฎาคม 2565.....

เรื่อง..... การจัดทำรายละเอียดค่าขอตังงบประมาณประจำปี 2567.....

เรียน ผอ.ฝจบ.

ตามที่ ฝจบ. ได้มีบันทึกด่วนที่สุดที่ ฝจบ/ว665 ลงวันที่ 20 มิถุนายน 2565 ขอให้ ฝ่าย/สำนัก จัดทำรายละเอียดค่าขอตังงบประมาณประจำปี 2567 ในรายการงบประมาณส่วนที่ ฝจบ. เป็นผู้ขอตังงบและรวบรวม ได้แก่ ค่าซ่อมแซมครุภัณฑ์ (งท.07) ค่าวัสดุสำนักงาน (งท.13) และค่าใช้จ่ายครุภัณฑ์ (งท.15) ภายในวันที่ 12 กรกฎาคม 2565 นั้น

ผทท. ได้ดำเนินการจัดทำค่าขอตังงบประมาณประจำปี 2567 ในรายการดังกล่าวข้างต้นเสร็จเรียบร้อยแล้ว โดยมีรายละเอียดตามเอกสารแนบ พร้อมทั้งได้จัดส่ง Soft file ให้ ฝจบ. ไปยัง E-mail prisana@mrtta.co.th เรียบร้อยแล้ว

(นายสมคิด สีสิตธรรม)

ผอ.ผทท.

รายละเอียดค่าใช้จ่ายการขอตั้งงบประมาณรายจ่าย หมวด ค่าใช้สอย

รายการ ค่าซ่อมแซมครุภัณฑ์

ประจำปีงบประมาณ 2567

หน่วยงาน ฝ่ายเทคโนโลยีสารสนเทศ

หน่วย : บาท (ทศนิยม 0 ตำแหน่ง)

ลำดับ	จำนวนเงิน	คำชี้แจง	
6	880,000.00	เพื่อบำรุงรักษาระบบงานสารสนเทศ ให้สามารถใช้งานได้อย่างต่อเนื่องตลอดเวลา	
7	200,000.00		
8	1,000,000.00		
9	800,000.00		
10	800,000.00		
11	1,350,000.00		
12	900,000.00		
13	4,000,000.00		
14	2,400,000.00		
15	750,000.00		
16	2,400,000.00		
17	4,300,000.00		
18	1,900,000.00		
19	3,400,000.00		
20	800,000.00		
21	500,000.00		
22	1,300,000.00		
23	77,000.00		
	รวมทั้งสิ้น		
	77,887,250.00		

เพื่อใช้เป็นค่าซ่อมแซมครุภัณฑ์ต่างๆ อุปกรณ์ที่เกี่ยวข้องภายในส่วนงาน และครุภัณฑ์สำนักงานอื่น ๆ ที่เกี่ยวข้อง เช่น โต๊ะ เก้าอี้ เครื่องโทรสาร เป็นต้น

หมายเหตุ : แบบฟอร์มข้างต้นใช้เพื่อบันทึกข้อมูลรวมของทั้งฝ่าย/สำนักเท่านั้น

ผู้จัดทำ..... โทร.....



ด่วนที่สุด

บันทึก

การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

ที่..... สผว/ว845 วันที่..... 8 ธันวาคม 2565
เรื่อง..... มติคณะกรรมการ รฟม. ครั้งที่ 12/2565 เมื่อวันที่ 30 พฤศจิกายน 2565

เรียน รผบ. รผง. รผว. รผก. รผบ. ผชก.(นายถนอมฯ) ผชก.(นายกิตติฯ) ผชก.(นางสาวจิรนนท์ฯ)
ผชก.(นายณัฐพงศ์ฯ) ผอ.สผว. ผอ.สสอ. ผอ.สกม. ผอ.सनก. ผอ.สตส. ผอ.ผนย.
ผอ.ผพค. ผอ.ผทท. ผอ.ผชง. ผอ.ผธด. ผอ.ผวส. ผอ.ผบก.1 ผอ.ผบก.2
ผอ.ผพธ. ผอ.ผรฟ. ผอ.ผปก. ผอ.ผรภ. ผอ.ผกท. ผอ.ผจบ. ผอ.ผทบ. ผอ.สปอ.
ผอ.สพร.

สผว. ใคร่ขอส่งมติคณะกรรมการ รฟม. ครั้งที่ 12/2565 เมื่อวันที่ 30 พฤศจิกายน 2565 มาเพื่อโปรดทราบและพิจารณาดำเนินการในส่วนที่เกี่ยวข้องต่อไป

(นางมลทิรา ลักษณะสิริศักดิ์)

ผอ.สผว.

สำเนาเรียน ผวก.



ด่วนที่สุด

บันทึกข้อความ

การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

ผชก.

เลขที่...2445...DCS.....

วันที่...7 ธ.ค. 65...เวลา...15.14..

ผวก. ภายใน

เลขรับ...5687.....

วันที่...8/12/65...เวลา...8.34..

ส่วนงาน.....สำนักผู้ว่าการ กองกิจกรรมคณะกรรมการ โทร. 1761 , 1727

ที่.....สผว/840.....วันที่.....7 ธันวาคม 2565

เรื่อง.....มติคณะกรรมการ รพม. ครั้งที่ 12/2565 เมื่อวันพุธที่ 30 พฤศจิกายน 2565

ACM 78-0.65

เรียน ผวก. ผ่าน ผชก.(นายถนอมฯ)

1. เรื่องเดิม

คณะกรรมการ รพม. ได้มีการประชุมครั้งที่ 12/2565 เมื่อวันพุธที่ 30 พฤศจิกายน 2565

2. ข้อเท็จจริง

สผว. ได้จัดทำมติคณะกรรมการ รพม. ตามข้อ 1. ดังนี้

2.1 ระเบียบวาระที่ 1.1 : การจัดประชุมผ่านสื่ออิเล็กทรอนิกส์ด้วยระบบ Video Teleconference

มติ : รับทราบ

2.2 ระเบียบวาระที่ 1.2 : กรรมการลาประชุม

มติ : รับทราบ

2.3 ระเบียบวาระที่ 1.3 : งานสวดพระอภิธรรมศพมารดาของท่านอภิรัฐ ไชยวงศ์น้อย

มติ : รับทราบ

2.4 ระเบียบวาระที่ 1.4 : ความคืบหน้าการดำเนินการในกรณีการอนุญาตให้บริษัท อนันดา ดีเวลลอปเม้นท์ ทู จำกัด ก่อสร้างอาคารชุดพักอาศัยขนาดใหญ่พิเศษ

มติ : รับทราบ และให้ รฟม. ประสานหารือกับหน่วยงานที่เกี่ยวข้องเพื่อร่วมกันพิจารณาแนวทางในการแก้ไขปัญหาการอนุญาตในกรณีนี้ และประเด็นแก้ไขร่างกฎกระทรวง ฉบับที่ 33 (พ.ศ. 2535) ออกตามความในพระราชบัญญัติควบคุมอาคาร พ.ศ. 2522 ฯ ภายในกรอบระยะเวลาตามคำพิพากษาของศาล โดยพิจารณาเชิญผู้แทนกรมโยธาธิการและผังเมืองเข้าร่วมด้วย

2.5 ระเบียบวาระที่ 2 : รับรองรายงานการประชุมคณะกรรมการ รฟม. ครั้งที่ 11/2565 เมื่อวันที่ 20 ตุลาคม 2565

มติ : รับรองรายงานการประชุมคณะกรรมการ รฟม. ครั้งที่ 11/2565 เมื่อวันที่ 20 ตุลาคม 2565

2.6 ระเบียบวาระที่ 4.1 : กรอบงบประมาณประจำปีงบประมาณ พ.ศ. 2567 ของ รฟม.

มติ : เห็นชอบกรอบงบประมาณประจำปีงบประมาณ พ.ศ. 2567 ของ รฟม. โดยมีวงเงินงบประมาณเพื่อดำเนินการ จำนวน 180,543.34 ล้านบาท และวงเงินเบิกจ่าย จำนวน 49,628.34 ล้านบาท ซึ่งจะเสนอขอรับการจัดสรรงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. 2567 จากสำนักงานงบประมาณ เป็นจำนวน 30,927.45 ล้านบาท และให้นำเสนอกระทรวงคมนาคมให้ความเห็นชอบก่อนจัดส่งสำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ และสำนักงานงบประมาณต่อไป ทั้งนี้ ให้ รฟม. รับข้อสังเกตของคณะกรรมการ รฟม. ไปพิจารณาดำเนินการต่อไป

3.10 ระเบียบวาระที่ 5.2
ให้ทุกฝ่ายทราบ

3.11 ระเบียบวาระที่ 5.3
ให้ทุกฝ่ายทราบ และให้ ฝพค. ดำเนินการตามมติต่อไป

3.12 ระเบียบวาระที่ 5.4
ให้ทุกฝ่ายทราบ

3.13 ระเบียบวาระที่ 5.5
ให้ทุกฝ่ายทราบ

4. ข้อเสนอ

จึงเรียนมาเพื่อโปรดพิจารณาสั่งการให้ฝ่ายต่างๆ ดำเนินการในส่วนที่เกี่ยวข้องต่อไป



(นางมลทิรา ลักษณะสิริศักดิ์)

ผอ.สพว.

เรียน ผอ.ฝ่าย/ สำนัก
เพื่อโปรดทราบและ
ดำเนินการในส่วนที่เกี่ยวข้องต่อไป



(นายภคพงศ์ ศิริกันทรมาศ)

ผวก.

8 ธ.ค. 65



สัญญาจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ
(Project Progress Monitoring System: PPMS)
ประจำปีงบประมาณ ๒๕๖๖

ระหว่าง

การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

กับ

บริษัท เอทูปี โซลูชั่น จำกัด
สัญญาเลขที่ จ(ข)๕/๒๕๖๖



สัญญาจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (Project Progress Monitoring System: PPMS) ประจำปีงบประมาณ ๒๕๖๖

สัญญาเลขที่ จ(ข)๕/๒๕๖๖

สัญญาฉบับนี้ทำขึ้น ณ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย สำนักงาน ตั้งอยู่เลขที่ ๑๗๕ ถนนพระราม ๙ แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร เมื่อวันที่ ๓ ตุลาคม พ.ศ. ๒๕๖๕ ระหว่าง การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย โดย นายทวิช พึ่งตน ผู้อำนวยการฝ่ายจัดซื้อและบริการ ปฏิบัติการแทน ผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย ซึ่งต่อไปในสัญญานี้เรียกว่า “ผู้ว่าจ้าง” ฝ่ายหนึ่ง กับ บริษัท เอทูพี โซลูชั่น จำกัด ซึ่งจดทะเบียนเป็นนิติบุคคล ณ สำนักงานทะเบียนหุ้นส่วนบริษัทกลาง กรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ มีสำนักงานใหญ่อยู่ เลขที่ ๕๐๓/๕ อาคารเค.เอส.แอล ทาวเวอร์ ชั้น ๔ ถนนศรีอยุธยา แขวงถนนพญาไท เขตราชเทวี กรุงเทพมหานคร โดยนายยุทธศักดิ์ สว่างผล ผู้มีอำนาจลงนาม ผูกพันนิติบุคคลปรากฏตามหนังสือรับรองของสำนักงานทะเบียนหุ้นส่วนบริษัทกลาง กรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ ที่ สจ.๓ ๐๐๑๓๒๐ ลงวันที่ ๗ กุมภาพันธ์ ๒๕๖๕ แนบท้ายสัญญานี้ ซึ่งต่อไปในสัญญานี้ เรียกว่า “ผู้รับจ้าง” อีกฝ่ายหนึ่ง

คู่สัญญาได้ตกลงกันมีข้อความดังต่อไปนี้

ข้อ ๑ ข้อตกลงว่าจ้าง

ผู้ว่าจ้างตกลงจ้างและผู้รับจ้างตกลงรับจ้างทำงาน บำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (Project Progress Monitoring System: PPMS) ประจำปีงบประมาณ ๒๕๖๖ ณ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย สำนักงาน ตั้งอยู่เลขที่ ๑๗๕ ถนนพระราม ๙ แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร ตามข้อกำหนดและเงื่อนไขแห่งสัญญานี้รวมทั้งเอกสารแนบท้ายสัญญา

ผู้รับจ้างตกลงที่จะจัดหาแรงงานและวัสดุ เครื่องมือเครื่องใช้ ตลอดจนอุปกรณ์ต่างๆ ชนิดดีเพื่อใช้ในการงานจ้างตามสัญญานี้

ข้อ ๒ เอกสารอันเป็นส่วนหนึ่งของสัญญา

เอกสารแนบท้ายสัญญาดังต่อไปนี้ให้ถือเป็นส่วนหนึ่งของสัญญานี้

๒.๑ ผนวก ๑ ขอบเขตของงานจ้างบำรุงรักษา จำนวน ๑๙ (สิบเก้า) หน้า

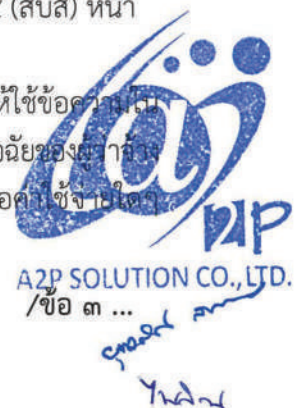
ระบบติดตามความก้าวหน้าโครงการ (Project Progress Monitoring System: PPMS) ประจำปีงบประมาณ ๒๕๖๖

๒.๒ ผนวก ๒ ใบเสนอราคาและหนังสือยืนยันราคา จำนวน ๒ (สอง) หน้า

๒.๓ ผนวก ๓ เอกสารเกี่ยวกับนิติบุคคลของผู้รับจ้าง จำนวน ๑๔ (สิบสี่) หน้า

หลักประกันสัญญา และเอกสารอื่นๆ ที่เกี่ยวข้อง

ความใดในเอกสารแนบท้ายสัญญาที่ขัดหรือแย้งกับข้อความในสัญญานี้ ให้ใช้ข้อความในสัญญานี้บังคับ และในกรณีที่เอกสารแนบท้ายสัญญาขัดแย้งกันเอง ผู้รับจ้างจะต้องปฏิบัติตามคำวินิจฉัยของคู่สัญญา คำวินิจฉัยของผู้ว่าจ้างให้ถือเป็นที่สุด และผู้รับจ้างไม่มีสิทธิเรียกร้องค่าจ้าง หรือค่าเสียหาย หรือค่าใช้จาในใดๆ เพิ่มเติมจากผู้ว่าจ้างทั้งสิ้น



ข้อ ๓ หลักประกันการปฏิบัติตามสัญญา

ในขณะที่ทำสัญญานี้ผู้รับจ้างได้นำหลักประกันเป็นเงินสด เป็นจำนวนเงิน ๓๐,๐๐๐.๐๐ บาท (สามหมื่นบาทถ้วน) ซึ่งเท่ากับร้อยละ ๕ (ห้า) ของราคาค่าจ้างตามสัญญา มามอบให้แก่ผู้ว่าจ้างเพื่อเป็นหลักประกันการปฏิบัติตามสัญญานี้

หลักประกันที่ผู้รับจ้างนำมามอบให้ตามวรรคหนึ่ง จะต้องมียุครอบคลุมความรับผิดชอบทั้งปวงของผู้รับจ้างตลอดอายุสัญญา ถ้าหลักประกันที่ผู้รับจ้างนำมามอบให้ดังกล่าวลดลงหรือเสื่อมค่าลง หรือมีอายุไม่ครอบคลุมถึงความรับผิดชอบของผู้รับจ้างตลอดอายุสัญญา ไม่ว่าด้วยเหตุใดๆ ก็ตาม รวมถึงกรณี ผู้รับจ้างส่งมอบงานล่าช้าเป็นเหตุให้ระยะเวลาแล้วเสร็จหรือวันครบกำหนดความรับผิดชอบในความชำรุดบกพร่องตามสัญญาเปลี่ยนแปลงไป ไม่ว่าจะเกิดขึ้นคราวใด ผู้รับจ้างต้องหาหลักประกันใหม่หรือหลักประกันเพิ่มเติมให้มีจำนวนครบถ้วนตามวรรคหนึ่งมามอบให้แก่ผู้ว่าจ้างภายใน ๑๕ (สิบห้า) วัน นับถัดจากวันที่ได้รับแจ้งเป็นหนังสือจากผู้ว่าจ้าง

หลักประกันที่ผู้รับจ้างนำมามอบไว้ตามข้อนี้ ผู้ว่าจ้างจะคืนให้แก่ผู้รับจ้างโดยไม่มีดอกเบี้ยเมื่อผู้รับจ้างพ้นจากข้อผูกพันและความรับผิดชอบทั้งปวงตามสัญญานี้แล้ว

ข้อ ๔ ค่าจ้างและการจ่ายเงิน

ผู้ว่าจ้างตกลงจ่ายและผู้รับจ้างตกลงรับเงินค่าจ้างจำนวนเงิน ๖๐๐,๐๐๐.๐๐ บาท (หกแสนบาทถ้วน) ซึ่งได้รวมภาษีมูลค่าเพิ่ม จำนวน ๓๙,๒๕๒.๓๔ บาท (สามหมื่นเก้าพันสองร้อยห้าสิบบาทสามสิบลีตต่างค์) ตลอดจนภาษีอากรอื่นๆ และค่าใช้จ่ายทั้งปวงด้วยแล้ว โดยกำหนดการจ่ายเงินเป็นงวดๆ จำนวน ๔ งวด งวดละ ๑๕๐,๐๐๐.๐๐ บาท (หนึ่งแสนห้าหมื่นบาทถ้วน) ซึ่งได้รวมภาษีมูลค่าเพิ่ม ตลอดจนภาษีอากรอื่น ๆ และค่าใช้จ่ายทั้งปวงด้วยแล้ว ซึ่งแต่ละงวดจะจ่ายทุกๆ สิ้นไตรมาส เมื่อผู้รับจ้างได้ปฏิบัติงานทั้งหมดให้แล้วเสร็จเรียบร้อยตามสัญญาและผู้ว่าจ้างได้ตรวจรับงานจ้างตามข้อ ๙ ไว้โดยครบถ้วนแล้ว

ข้อ ๕ กำหนดเวลาแล้วเสร็จและสิทธิของผู้ว่าจ้างในการบอกเลิกสัญญา

ผู้รับจ้างต้องเริ่มทำงานที่รับจ้างตั้งแต่วันที่ ๑ ตุลาคม ๒๕๖๕ และจะต้องทำงานให้แล้วเสร็จบริบูรณ์ภายในวันที่ ๓๐ กันยายน ๒๕๖๖ ถ้าผู้รับจ้างมิได้ลงมือทำงานภายในกำหนดเวลา หรือไม่สามารทำงานให้แล้วเสร็จตามกำหนดเวลา หรือมีเหตุให้เชื่อได้ว่าผู้รับจ้างไม่สามารถทำงานให้แล้วเสร็จภายในกำหนดเวลา หรือจะแล้วเสร็จล่าช้าเกินกว่ากำหนดเวลา หรือผู้รับจ้างทำผิดสัญญาข้อใดข้อหนึ่ง หรือตกเป็นผู้ถูกพิทักษ์ทรัพย์เด็ดขาดหรือตกเป็นผู้ล้มละลาย หรือเพิกเฉยไม่ปฏิบัติตามคำสั่งของคณะกรรมการตรวจรับพัสดุ ผู้ว่าจ้างมีสิทธิที่จะบอกเลิกสัญญานี้ได้ และมีสิทธิจ้างผู้รับจ้างรายใหม่เข้าทำงานของผู้รับจ้างให้ลุ่่วงไปได้ด้วย การใช้สิทธิบอกเลิกสัญญานี้ไม่กระทบสิทธิของผู้ว่าจ้างที่จะเรียกร้องค่าเสียหายจากผู้รับจ้าง

การที่ผู้ว่าจ้างมิใช้สิทธิเลิกสัญญาดังกล่าวข้างต้นนั้น ไม่เป็นเหตุให้ผู้รับจ้างพ้นจากความรับผิดชอบตามสัญญา

ข้อ ๖ การจ้างช่วง

ผู้รับจ้างจะต้องไม่เองงานทั้งหมดหรือแต่บางส่วนแห่งสัญญานี้ไปจ้างช่วงอีกทอดหนึ่ง เว้นแต่การจ้างช่วงงานแต่บางส่วนที่ได้รับอนุญาตเป็นหนังสือจากผู้ว่าจ้างแล้ว การที่ผู้ว่าจ้างได้อนุญาตให้จ้างช่วงงานแต่บางส่วนดังกล่าวนี้ ไม่เป็นเหตุให้ผู้รับจ้างหลุดพ้นจากความรับผิดชอบหรือพันธะหน้าที่ตามสัญญานี้ และผู้รับจ้างจะยังคงต้องรับผิดชอบในความผิดและความประมาทเลินเล่อของผู้รับจ้างช่วง หรือของตัวแทนหรือลูกจ้างของผู้รับจ้างช่วงนั้นทุกประการ



A2P SOLUTION CO., LTD.
/กรณีผู้รับจ้าง...

Yuan
Yuan

กรณีผู้รับจ้างไปจ้างช่างงานแต่บางส่วนโดยฝ่าฝืนความในวรรคหนึ่ง ผู้รับจ้างต้องชำระค่าปรับให้แก่ผู้ว่าจ้างเป็นจำนวนเงินในอัตราร้อยละ ๑๐ (สิบ) ของวงเงินของงานที่จ้างช่วงตามสัญญา ทั้งนี้ไม่ตัดสิทธิผู้ว่าจ้างในการบอกเลิกสัญญา

ข้อ ๗ ความรับผิดชอบของผู้รับจ้าง

ผู้รับจ้างจะต้องรับผิดชอบต่ออุบัติเหตุ ความเสียหาย หรือภัยอันตรายใดๆ อันเกิดจากการปฏิบัติงานของผู้รับจ้าง และจะต้องรับผิดชอบต่อความเสียหายจากการกระทำของลูกจ้างหรือตัวแทนของผู้รับจ้าง และจากการปฏิบัติงานของผู้รับจ้างช่วงด้วย (ถ้ามี)

ความเสียหายใดๆ อันเกิดแก่งานที่ผู้รับจ้างได้ทำขึ้น แม้จะเกิดขึ้นเพราะเหตุสุดวิสัยก็ตาม ผู้รับจ้างจะต้องรับผิดชอบโดยซ่อมแซมให้คืนดีหรือเปลี่ยนให้ใหม่โดยค่าใช้จ่ายของผู้รับจ้างเอง เว้นแต่ความเสียหายนั้นเกิดจากความผิดของผู้ว่าจ้าง ทั้งนี้ ความรับผิดชอบของผู้รับจ้างดังกล่าวในข้อนี้จะสิ้นสุดลงเมื่อผู้ว่าจ้างได้รับมอบงานครั้งสุดท้าย

ผู้รับจ้างจะต้องรับผิดชอบต่อบุคคลภายนอกในความเสียหายใดๆ อันเกิดจากการปฏิบัติงานของผู้รับจ้าง หรือลูกจ้างหรือตัวแทนของผู้รับจ้าง รวมถึงผู้รับจ้างช่วง (ถ้ามี) ตามสัญญานี้ หากผู้ว่าจ้างถูกเรียกร้องหรือฟ้องร้องหรือต้องชดใช้ค่าเสียหายให้แก่บุคคลภายนอกไปแล้ว ผู้รับจ้างจะต้องดำเนินการใดๆ เพื่อให้มีการว่าต่างแก่ต่างให้แก่ผู้ว่าจ้างโดยค่าใช้จ่ายของผู้รับจ้างเอง รวมทั้งผู้รับจ้างจะต้องชดใช้ค่าเสียหายนั้นๆ ตลอดจนค่าใช้จ่ายใดๆ อันเกิดจากการถูกเรียกร้องหรือถูกฟ้องร้องให้แก่ผู้ว่าจ้างทันที

ข้อ ๘ การจ่ายเงินแก่ลูกจ้าง

ผู้รับจ้างจะต้องจ่ายเงินแก่ลูกจ้างที่ผู้รับจ้างได้จ้างมาในอัตราและตามกำหนดเวลาที่ผู้รับจ้างได้ตกลงหรือทำสัญญาไว้ต่อลูกจ้างดังกล่าว

ถ้าผู้รับจ้างไม่จ่ายเงินค่าจ้างหรือค่าทดแทนอื่นใดแก่ลูกจ้างดังกล่าวในวรรคหนึ่ง ผู้ว่าจ้างมีสิทธิที่จะเอาเงินค่าจ้างที่จะต้องจ่ายแก่ผู้รับจ้างมาจ่ายให้แก่ลูกจ้างของผู้รับจ้างดังกล่าว และให้ถือว่าผู้ว่าจ้างได้จ่ายเงินจำนวนนั้นเป็นค่าจ้างให้แก่ผู้รับจ้างตามสัญญาแล้ว

ผู้รับจ้างจะต้องจัดให้มีประกันภัยสำหรับลูกจ้างทุกคนที่จ้างมาทำงาน โดยให้ครอบคลุมถึงความรับผิดชอบทั้งปวงของผู้รับจ้าง รวมทั้งผู้รับจ้างช่วง (ถ้ามี) ในกรณีความเสียหายที่คิดค่าสินไหมทดแทนได้ตามกฎหมาย ซึ่งเกิดจากอุบัติเหตุหรือภัยอันตรายใดๆ ต่อลูกจ้างหรือบุคคลอื่นที่ผู้รับจ้างหรือผู้รับจ้างช่วงจ้างมาทำงาน ผู้รับจ้างจะต้องส่งมอบกรมธรรม์ประกันภัยดังกล่าวพร้อมทั้งหลักฐานการชำระเบี้ยประกันให้แก่ผู้ว่าจ้างเมื่อผู้ว่าจ้างเรียกร้อง

ข้อ ๙ การตรวจรับงานจ้าง

เมื่อผู้ว่าจ้างได้ตรวจรับงานจ้างที่ส่งมอบและเห็นว่าถูกต้องครบถ้วนตามสัญญาแล้ว ผู้ว่าจ้างจะออกหลักฐานการรับมอบเป็นหนังสือไว้ให้ เพื่อผู้รับจ้างนำมาเป็นหลักฐานประกอบการขอรับเงินค่างานจ้างนั้น

ถ้าผลของการตรวจรับงานจ้างปรากฏว่างานจ้างที่ผู้รับจ้างส่งมอบไม่ตรงตามสัญญาผู้ว่าจ้างทรงไว้ซึ่งสิทธิที่จะไม่รับงานจ้างนั้น ในกรณีเช่นว่านี้ ผู้รับจ้างต้องทำการแก้ไขให้ถูกต้องตามสัญญาด้วยค่าใช้จ่ายของผู้รับจ้างเอง และระยะเวลาที่เสียไปเพราะเหตุดังกล่าวผู้รับจ้างจะนำมาอ้างเป็นเหตุขอชดเชยเวลาส่งมอบงานจ้างตามสัญญาหรือของดหรือลดค่าปรับไม่ได้


/ชื่อ ๑๐...
AZP SOLUTION CO., LTD.

Handwritten signature and name
สมชาย งาม
ทนาย

ข้อ ๑๐ รายละเอียดของงานจ้างคลาดเคลื่อน

ผู้รับจ้างรับรองว่าได้ตรวจสอบและทำความเข้าใจในรายละเอียดของงานจ้างโดยถี่ถ้วนแล้ว หากปรากฏว่ารายละเอียดของงานจ้างนั้นผิดพลาดหรือคลาดเคลื่อนไปจากหลักการทางวิศวกรรมหรือทางเทคนิค ผู้รับจ้างตกลงที่จะปฏิบัติตามคำวินิจฉัยของผู้ว่าจ้าง คณะกรรมการตรวจรับพัสดุ เพื่อให้งานแล้วเสร็จบริบูรณ์ คำวินิจฉัยดังกล่าวให้ถือเป็นที่สุด โดยผู้รับจ้างจะคิดค่าจ้าง ค่าเสียหาย หรือค่าใช้จ่ายใดๆ เพิ่มขึ้นจากผู้ว่าจ้าง หรือขอขยายอายุสัญญาไม่ได้

ข้อ ๑๑ ค่าปรับ

หากผู้รับจ้างไม่สามารถทำงานให้แล้วเสร็จภายในเวลาที่กำหนดไว้ในสัญญาและผู้ว่าจ้างยังมีได้บอกเลิกสัญญา ผู้รับจ้างจะต้องชำระค่าปรับให้แก่ผู้ว่าจ้าง โดยรายละเอียดค่าปรับให้เป็นไปตามที่กำหนดไว้ในขอบเขตของงานจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (Project Progress Monitoring System: PPMS) ประจำปีงบประมาณ ๒๕๖๖ ในผนวก ๑ นอกจากนี้ ผู้รับจ้างยอมให้ผู้ว่าจ้างเรียกค่าเสียหายอันเกิดขึ้นจากการที่ผู้รับจ้างทำงานล่าช้าเฉพาะส่วนที่เกินกว่าจำนวนค่าปรับดังกล่าวได้อีกด้วย

ในระหว่างที่ผู้ว่าจ้างยังมีได้บอกเลิกสัญญานั้น หากผู้ว่าจ้างเห็นว่าผู้รับจ้างจะไม่สามารถปฏิบัติตามสัญญาต่อไปได้ ผู้ว่าจ้างจะใช้สิทธิบอกเลิกสัญญาและใช้สิทธิตามข้อ ๑๒ ก็ได้ และถ้าผู้ว่าจ้างได้แจ้งข้อเรียกร้องไปยังผู้รับจ้างเมื่อครบกำหนดเวลาแล้วเสร็จของงานขอให้ชำระค่าปรับแล้ว ผู้ว่าจ้างมีสิทธิที่จะปรับผู้รับจ้างจนถึงวันบอกเลิกสัญญาได้อีกด้วย

ข้อ ๑๒ สิทธิของผู้ว่าจ้างภายหลังบอกเลิกสัญญา

ในกรณีที่ผู้ว่าจ้างบอกเลิกสัญญา ผู้ว่าจ้างอาจทำงานนั้นเองหรือว่าจ้างผู้อื่นให้ทำงานนั้นต่อจนแล้วเสร็จก็ได้ และในกรณีดังกล่าว ผู้ว่าจ้างมีสิทธิริบหรือบังคับจากหลักประกันการปฏิบัติตามสัญญาทั้งหมดหรือบางส่วนตามแต่จะเห็นสมควร นอกจากนั้น ผู้รับจ้างจะต้องรับผิดชอบในค่าเสียหายซึ่งเป็นจำนวนเกินกว่าหลักประกันการปฏิบัติตามสัญญา รวมทั้งค่าใช้จ่ายที่เพิ่มขึ้นในการทำงานนั้นต่อให้แล้วเสร็จตามสัญญา ซึ่งผู้ว่าจ้างจะหักเอาจากจำนวนเงินใดๆ ที่จะจ่ายให้แก่ผู้รับจ้างก็ได้

ข้อ ๑๓ การบังคับค่าปรับ ค่าเสียหาย และค่าใช้จ่าย

ในกรณีที่ผู้รับจ้างไม่ปฏิบัติตามสัญญาข้อใดข้อหนึ่งด้วยเหตุใดๆ ก็ตาม จนเป็นเหตุให้เกิดค่าปรับ ค่าเสียหาย หรือค่าใช้จ่ายแก่ผู้ว่าจ้าง ผู้รับจ้างต้องชดใช้ค่าปรับ ค่าเสียหาย หรือค่าใช้จ่ายดังกล่าวให้แก่ผู้ว่าจ้างโดยสิ้นเชิงภายในกำหนด ๑๕ (สิบห้า) วัน นับถัดจากวันที่ได้รับแจ้งเป็นหนังสือจากผู้ว่าจ้าง หากผู้รับจ้างไม่ชดใช้ให้ถูกต้องครบถ้วนภายในระยะเวลาดังกล่าวให้ผู้ว่าจ้างมีสิทธิที่จะหักเอาจากจำนวนเงินค่าจ้างที่ต้องชำระหรือบังคับจากหลักประกันการปฏิบัติตามสัญญาได้ทันที

หากค่าปรับ ค่าเสียหาย หรือค่าใช้จ่ายที่บังคับจากเงินค่าจ้างที่ต้องชำระ หรือหลักประกันการปฏิบัติตามสัญญาแล้วยังไม่เพียงพอ ผู้รับจ้างยินยอมชำระส่วนที่เหลือที่ยังขาดอยู่จนครบถ้วนตามจำนวนค่าปรับ ค่าเสียหาย หรือค่าใช้จ่ายนั้น ภายในกำหนด ๑๕ (สิบห้า) วัน นับถัดจากวันที่ได้รับแจ้งเป็นหนังสือจากผู้ว่าจ้าง

หากมีเงินค่าจ้างตามสัญญาที่หักไว้จ่ายเป็นค่าปรับ ค่าเสียหาย หรือค่าใช้จ่ายแล้ว ยังเหลืออยู่อีกเท่าใด ผู้ว่าจ้างจะคืนให้แก่ผู้รับจ้างทั้งหมด



ช่อ ๑๔...
สมชาย งาม
คุณวิภา

ข้อ ๑๔ การงดหรือลดค่าปรับ หรือการขยายเวลาปฏิบัติงานตามสัญญา

ในกรณีที่มีเหตุเกิดจากความผิดหรือความบกพร่องของฝ่ายผู้ว่าจ้าง หรือเหตุสุดวิสัย หรือเกิดจากเหตุการณ์อันหนึ่งอันใดที่ผู้รับจ้างไม่ต้องรับผิดชอบตามกฎหมาย หรือเหตุอื่นตามที่กำหนดในกฎกระทรวง ซึ่งออกตามความในกฎหมายว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ ทำให้ผู้รับจ้างไม่สามารถทำงานให้แล้วเสร็จตามเงื่อนไขและกำหนดเวลาแห่งสัญญานี้ได้ ผู้รับจ้างจะต้องแจ้งเหตุหรือเหตุการณ์ดังกล่าวพร้อมหลักฐานเป็นหนังสือให้ผู้ว่าจ้างทราบ เพื่อของดหรือลดค่าปรับ หรือขยายเวลาทำงานออกไปภายใน ๑๕ (สิบห้า) วันนับถัดจากวันที่เหตุนั้นสิ้นสุดลง หรือตามที่กำหนดในกฎกระทรวงดังกล่าว แล้วแต่กรณี

ถ้าผู้รับจ้างไม่ปฏิบัติให้เป็นไปตามความในวรรคหนึ่ง ให้ถือว่าผู้รับจ้างได้ละสิทธิเรียกร้องในการที่จะของดหรือลดค่าปรับ หรือขยายเวลาทำงานออกไปโดยไม่มีเงื่อนไขใดๆ ทั้งสิ้น เว้นแต่กรณีเหตุเกิดจากความผิดหรือความบกพร่องของฝ่ายผู้ว่าจ้าง ซึ่งมีหลักฐานชัดเจน หรือผู้ว่าจ้างทราบที่อยู่แล้วตั้งแต่วันที่

การงดหรือลดค่าปรับ หรือขยายกำหนดเวลาทำงานตามวรรคหนึ่ง อยู่ในดุลพินิจของผู้ว่าจ้างที่จะพิจารณาตามที่เห็นสมควร

ข้อ ๑๕ การใช้เรือไทย

ในการปฏิบัติตามสัญญานี้ หากผู้รับจ้างจะต้องส่งหรือนำของเข้ามาจากต่างประเทศ รวมทั้งเครื่องมือและอุปกรณ์ที่ต้องนำเข้ามาเพื่อปฏิบัติงานตามสัญญา ไม่ว่าผู้รับจ้างจะเป็นผู้นำของเข้ามาเอง หรือนำเข้ามาโดยผ่านตัวแทนหรือบุคคลอื่นใด ถ้าสิ่งของนั้นต้องนำเข้ามาโดยทางเรือในเส้นทางเดินเรือที่มีเรือไทยเดินอยู่และสามารถให้บริการรับขนได้ตามที่รัฐมนตรีว่าการกระทรวงคมนาคมประกาศกำหนด ผู้รับจ้างต้องจัดการให้สิ่งของดังกล่าวบรรทุกโดยเรือไทยหรือเรือที่มีสิทธิเช่นเดียวกับเรือไทยจากต่างประเทศมายังประเทศไทย เว้นแต่จะได้รับอนุญาตจากกรมเจ้าท่าก่อนบรรทุกของนั้นลงเรืออื่นที่มีใช้เรือไทยหรือเป็นของที่รัฐมนตรีว่าการกระทรวงคมนาคมประกาศยกเว้นให้บรรทุกโดยเรืออื่นได้ ทั้งนี้ไม่ว่าการส่งหรือนำเข้าสิ่งของดังกล่าวจากต่างประเทศจะเป็นแบบใด

ในการส่งมอบงานตามสัญญาให้แก่ผู้ว่าจ้าง ถ้างานนั้นมีสิ่งของตามวรรคหนึ่ง ผู้รับจ้างจะต้องส่งมอบใบตราส่ง (Bill of Lading) หรือสำเนาใบตราส่งสำหรับของนั้น ซึ่งแสดงว่าได้บรรทุกมาโดยเรือไทยหรือเรือที่มีสิทธิเช่นเดียวกับเรือไทยให้แก่ผู้ว่าจ้างพร้อมกับการส่งมอบงานด้วย

ในกรณีที่สิ่งของดังกล่าวไม่ได้บรรทุกจากต่างประเทศมายังประเทศไทยโดยเรือไทยหรือเรือที่มีสิทธิเช่นเดียวกับเรือไทย ผู้รับจ้างต้องส่งมอบหลักฐานซึ่งแสดงว่าได้รับอนุญาตจากกรมเจ้าท่า ให้บรรทุกของโดยเรืออื่นได้ หรือหลักฐานซึ่งแสดงว่าได้ชำระค่าธรรมเนียมพิเศษเนื่องจากการไม่บรรทุกของโดยเรือไทยตามกฎหมายว่าด้วยการส่งเสริมการพาณิชย์แล้วอย่างใดอย่างหนึ่งแก่ผู้ว่าจ้างด้วย

ในกรณีที่ผู้รับจ้างไม่ส่งมอบหลักฐานอย่างใดอย่างหนึ่งดังกล่าวในวรรคสองและวรรคสาม ให้แก่ผู้ว่าจ้าง แต่จะขอส่งมอบงานดังกล่าวให้ผู้ว่าจ้างก่อนโดยไม่รับชำระเงินค่าจ้าง ผู้ว่าจ้าง มีสิทธิรับเงินดังกล่าวไว้ก่อน และชำระเงินค่าจ้างเมื่อผู้รับจ้างได้ปฏิบัติถูกต้องครบถ้วนดังกล่าวแล้วได้


/สัญญานี้...
A2P SOLUTION CO., LTD.

สมชาย งาม
วิมล

สัญญานี้มีผลย้อนหลังไปตั้งแต่วันที่ ๑ ตุลาคม ๒๕๖๕

สัญญานี้ทำขึ้นเป็นสองฉบับ มีข้อความถูกต้องตรงกัน คู่สัญญาได้อ่านและเข้าใจข้อความโดยละเอียด
ตลอดแล้ว จึงได้ลงลายมือชื่อ พร้อมทั้งประทับตรา (ถ้ามี) ไว้เป็นสำคัญต่อหน้าพยาน และคู่สัญญาต่างยึดถือไว้
ฝ่ายละหนึ่งฉบับ

(ลงชื่อ)..... *ทวิ*ผู้ว่าจ้าง

(นายทวิ พึ่งตน)

ผู้อำนวยการฝ่ายจัดซื้อและบริการ
ปฏิบัติการแทน ผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

(ลงชื่อ)..... *สมชาย*ผู้รับจ้าง

(นายยุทธศักดิ์ สว่างผล)

ผู้มีอำนาจลงนามผูกพัน
บริษัท เอทพี โซลูชั่น จำกัด



(ลงชื่อ)..... *จิน*พยาน

(นางจิตตารีย์ ศรีอาวุธ)

ผู้อำนวยการกองจัดหาพัสดุทั่วไป
การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

(ลงชื่อ)..... *สุวิ*พยาน

(นายสุรียา อินทรasmบัติ)

บริษัท เอทพี โซลูชั่น จำกัด

เลขที่โครงการ ๖๕๐๓๗๑๕๔๓๘๓

เลขคุมสัญญา ๖๕๐๕๒๔๐๐๓๖๐๓

ทวิ



บันทึกข้อความ

การรถไฟฟ้านครหลวงแห่งประเทศไทย

เอกสารแนบ 3

เลขรับ 1423
วันที่ 7/4/66
เวลา 15.08

ส่วนงาน 2 ฝ่ายเทคโนโลยีสารสนเทศ โทร. 2587

ที่ ผทท/228 วันที่ 227 เมษายน 2566

เรื่อง 22 เอนุมัติแต่งตั้งผู้รับผิดชอบในการจัดทำขอบเขตของงานและราคาากลางจ้างบำรุงรักษาระบบติดตาม
ความก้าวหน้าโครงการ (PPMS) ประจำปีงบประมาณ 2567

เรียน ผอ.ฝจบ.

1. ข้อเท็จจริง

1.1 ผทท. ได้มีบันทึกที่ ผทท/429 ลงวันที่ 12 กรกฎาคม 2565 จัดส่งรายละเอียดคำขอตั้ง
งบประมาณรายจ่าย หมวดค่าใช้สอย รายการค่าซ่อมแซมครุภัณฑ์ ประจำปีงบประมาณ 2567 เพื่อให้ ฝจบ. รวบรวม
คำขอตั้งงบประมาณฯ ดังกล่าว โดยขอตั้งงบประมาณสำหรับจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS)
ประจำปีงบประมาณ 2567 เป็นจำนวนเงินทั้งสิ้น 1,350,000 บาท (หนึ่งล้านสามแสนห้าหมื่นบาทถ้วน)
(รวมภาษีมูลค่าเพิ่ม) ทั้งนี้ คณะกรรมการ รพม. ในคราวประชุมครั้งที่ 12/2565 เมื่อวันที่ 30 พฤศจิกายน 2565
ได้มีมติเห็นชอบกรอบงบประมาณประจำปีงบประมาณ 2567 แล้ว (เอกสารแนบ 1)

1.2 รพม. ได้ดำเนินการจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) จากบริษัท
เอทูปิ โซลูชั่น จำกัด ตามสัญญาเลขที่ จ(ข) 5/2566 ลงวันที่ 3 ตุลาคม 2565 ซึ่งสัญญาดังกล่าวจะสิ้นสุดในวันที่
30 กันยายน 2566 (เอกสารแนบ 2)

1.3 ผทท. ได้ประสาน ฝจบ. ตามข้อ 1.1 แล้ว ทราบว่า รายการฯ ดังกล่าวเป็นรายการที่อยู่ในงบทำการ
ซึ่งมีแหล่งเบิกจ่ายจากรายได้ของ รพม. จึงสามารถดำเนินการร่างขอบเขตของงานฯ ได้

2. ข้อกฎหมาย

2.1 พระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560

มาตรา 6 เพื่อให้การปฏิบัติเกี่ยวกับการจัดซื้อจัดจ้างและการบริหารพัสดุโดยใช้เงิน
งบประมาณเป็นไปอย่างมีประสิทธิภาพ เกิดความคุ้มค่าต่อการกิจของรัฐ และป้องกันปัญหาการทุจริต ให้หน่วยงาน
ของรัฐปฏิบัติตามแนวทางของพระราชบัญญัตินี้ และกฎกระทรวง ระเบียบ และประกาศที่ออกตามความ
ในพระราชบัญญัตินี้

มาตรา 61 ในการจัดซื้อจัดจ้างพัสดุแต่ละครั้ง ให้ผู้มีอำนาจแต่งตั้งผู้รับผิดชอบการจัดซื้อ
จัดจ้างนั้น ซึ่งจะกระทำโดยคณะกรรมการการจัดซื้อจัดจ้างหรือเจ้าหน้าที่คนใดคนหนึ่งก็ได้

องค์ประกอบและองค์ประชุมซึ่งกระทำโดยคณะกรรมการ และหน้าที่ของผู้รับผิดชอบการจัดซื้อ
จัดจ้างตามวรรคหนึ่ง ให้เป็นไปตามระเบียบที่รัฐมนตรีกำหนด

2.2 ระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560

ข้อ 21 ในการซื้อหรือจ้างที่มีใช้การจ้างก่อสร้าง ให้หัวหน้าหน่วยงานของรัฐแต่งตั้ง
คณะกรรมการขึ้นมาคณะหนึ่ง หรือจะให้เจ้าหน้าที่หรือบุคคลใดบุคคลหนึ่งรับผิดชอบในการจัดทำร่างขอบเขตของงาน
หรือรายละเอียดคุณลักษณะเฉพาะของพัสดุที่จะซื้อหรือจ้าง รวมทั้งกำหนดหลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอด้วย

องค์ประกอบ ระยะเวลาการพิจารณา และการประชุมของคณะกรรมการตามวรรคหนึ่งและ
วรรคสอง ให้เป็นไปตามที่หัวหน้าหน่วยงานของรัฐกำหนดตามความจำเป็นและเหมาะสม

2.3 คำสั่งการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย ที่ 98/2564 ลงวันที่ 5 เมษายน 2564 เรื่อง มอบอำนาจเกี่ยวกับการจัดซื้อหรือจัดจ้างพัสดุ

2. การมอบอำนาจดำเนินการและอำนาจสั่งซื้อหรือสั่งจ้าง ดังนี้

2.3 การสั่งซื้อหรือสั่งจ้างโดยวิธีเฉพาะเจาะจงครั้งหนึ่ง ให้เป็นอำนาจของผู้ดำรงตำแหน่งและภายในวงเงิน ดังต่อไปนี้

(1) ผู้อำนวยการกองจัดหาพัสดุทั่วไป ไม่เกิน 500,000 บาท (ห้าแสนบาทถ้วน)

(2) ผู้อำนวยการฝ่ายจัดซื้อและบริการ ไม่เกิน 5,000,000 บาท (ห้าล้านบาทถ้วน)

3. การมอบอำนาจตามคำสั่งนี้ให้ครอบคลุมถึงการดำเนินการทุกกระบวนการตามพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 ระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 กฎกระทรวง และประกาศที่ออกตามความในพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 และมติคณะรัฐมนตรีที่เกี่ยวข้อง ภายในอำนาจและวงเงินตามข้อ 2 ทั้งนี้ สำหรับการบอกเลิกหรือการตกลงเลิกสัญญาหรือข้อตกลง การแก้ไขสัญญาหรือข้อตกลง การงดหรือลดค่าปรับให้แก่คู่สัญญาหรือการขยายเวลาทำการตามสัญญาหรือข้อตกลง ให้เสนอผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย พิจารณาให้ความเห็นชอบก่อน และเมื่อผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทยได้พิจารณาให้ความเห็นชอบแล้ว ให้ผู้รับมอบอำนาจตามข้อ 2.1 ข้อ 2.2 และข้อ 2.3 มีหนังสือแจ้งการบอกเลิก หรือการตกลงเลิกสัญญาหรือข้อตกลง การงดหรือลดค่าปรับให้แก่คู่สัญญา การขยายเวลาทำการตามสัญญาหรือข้อตกลงหรือลงนามในสัญญาหรือข้อตกลง แล้วแต่กรณีต่อไป เว้นแต่ ผู้รับมอบอำนาจตามข้อ 2.3 (1) ให้สามารถดำเนินการได้โดยไม่ต้องเสนอผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทยพิจารณาให้ความเห็นชอบก่อน

3. ข้อพิจารณา

ผทท. พิจารณาแล้วเห็นว่า เพื่อให้การจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ประจำปีงบประมาณ 2567 สอดคล้องกับระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 จึงเห็นควรเสนอ ผอ.ฝจบ. แต่งตั้ง นางสาวสุพรรณษา นิลสมบุญณ์ โปรแกรมเมอร์ ระดับ 7 แผนกสนับสนุนระบบงานคอมพิวเตอร์ กองระบบงานคอมพิวเตอร์ ฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบในการจัดทำขอบเขตของงาน กำหนดหลักเกณฑ์การพิจารณา และราคากลางจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ประจำปีงบประมาณ 2567 ตามระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 ข้อ 21 ทั้งนี้ การแต่งตั้งนางสาวสุพรรณษา เป็นผู้รับผิดชอบการจัดทำขอบเขตของงานฯ ดังกล่าว เนื่องจากการดำเนินการต่อเนื่องเป็นประจำทุกปี ขอบเขตของงานฯ ไม่มีความซับซ้อน และเป็นหน้าที่ความรับผิดชอบโดยตรงของนางสาวสุพรรณษา ซึ่งมีหน้าที่ให้คำแนะนำและแก้ไขปัญหาการใช้งาน รวมทั้งบริหารจัดการและควบคุมให้ผู้รับจ้างบำรุงรักษาระบบฯ ให้สามารถใช้งานได้อย่างต่อเนื่องตลอดเวลา

4. ข้อเสนอ

จึงเรียนมาเพื่อโปรดพิจารณา หากเห็นชอบขอได้โปรดอนุมัติแต่งตั้งผู้รับผิดชอบฯ ตามข้อ 3. และ ผทท. จะได้ดำเนินการในส่วนที่เกี่ยวข้องต่อไป จะขอบคุณยิ่ง



(นางสาวสิริพร ชนเฉิดสิริกุล)

ผอ.กรค.

รท.ผอ.ฝทท.

อนุมัติตามเสนอ



(นายวิท ทุ่งตัน)

ผอ.ฝจบ.

7/4/66

รายชื่อคณะกรรมการจ้างและคณะกรรมการตรวจรับพัสดุ
จ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS)
ประจำปีงบประมาณ 2567

คณะกรรมการซื้อหรือจ้างโดยวิธีเฉพาะเจาะจง

1. นางสาวศิวลี เกตุคง	หัวหน้าแผนกแผนงานและบริหารเอกสาร 2-3 กองแผนงานและบริหารเอกสาร 2 ฝ่ายบริหารงานก่อสร้าง 2	ประธานกรรมการ
2. นางสาววิสุตา ชลาชนเดชะ	หัวหน้าแผนกแผนงานและบริหารเอกสาร 1-3 กองแผนงานและบริหารเอกสาร 1 ฝ่ายบริหารงานก่อสร้าง 1	กรรมการ
3. นางสาวปวีณา เปล่งเสียง	พนักงานวิเคราะห์ระบบ ระดับ 7 แผนกพัฒนาระบบงานคอมพิวเตอร์ กองระบบงานคอมพิวเตอร์ ฝ่ายเทคโนโลยีสารสนเทศ	กรรมการ

คณะกรรมการตรวจรับพัสดุ

1. นางสาวสิริพร อุซสาธิต	หัวหน้าแผนกอาวุโส ระดับ 10 แผนกข้อมูลและบริหารงานเอกสาร ฝ่ายวิศวกรรมและสถาปัตยกรรม 1 ฝ่ายวิศวกรรมและสถาปัตยกรรม	ประธานกรรมการ
2. นางสาวจตุรพร จารุวัจนกุล	หัวหน้าแผนกประเมินผลโครงการรถไฟฟ้า กองวางแผนโครงการรถไฟฟ้า ฝ่ายพัฒนาโครงการรถไฟฟ้า	กรรมการ
3. นางสาวสุพรรณษา นิลสมบุญ	โปรแกรมเมอร์ ระดับ 7 แผนกสนับสนุนระบบงานคอมพิวเตอร์ กองระบบงานคอมพิวเตอร์ ฝ่ายเทคโนโลยีสารสนเทศ	กรรมการและ เลขานุการ

ขอบเขตของงานจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ(Project Progress Monitoring System: PPMS)

ประจำปีงบประมาณ 2567

1. ความเป็นมา

การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย (รฟม.) ได้มีระบบติดตามความก้าวหน้าโครงการ (Project Progress Monitoring System: PPMS) เพื่อใช้สำหรับรองรับการติดตามความก้าวหน้าการก่อสร้างโครงการรถไฟฟ้าของ รฟม. โดยระบบฯ ดังกล่าว จะสิ้นสุดระยะเวลาการรับประกัน ในวันที่ 30 กันยายน 2566 ทั้งนี้ เพื่อให้ระบบติดตามความก้าวหน้าโครงการ (PPMS) สามารถใช้งานได้อย่างต่อเนื่องและมีประสิทธิภาพ รฟม. จึงจำเป็นต้องจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ต่อไป

2. วัตถุประสงค์

รฟม. มีความประสงค์จะจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) เพื่อให้ระบบฯ สามารถใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และตอบสนองความต้องการของผู้ใช้งานในองค์กรได้ดียิ่งขึ้น

3. คุณสมบัติของผู้ยื่นข้อเสนอ

- 3.1 มีความสามารถตามกฎหมาย
- 3.2 ไม่เป็นบุคคลล้มละลาย
- 3.3 ไม่อยู่ระหว่างเลิกกิจการ
- 3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง
- 3.5 ผู้รับจ้างต้องไม่เป็นผู้ที่ถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทำงานตามระเบียบของทางราชการและได้แจ้งเวียนชื่อแล้ว หรือไม่เป็นผู้ที่ได้รับผลของการสั่งให้นิติบุคคลหรือบุคคลอื่นเป็นผู้ทำงานตามระเบียบของทางราชการ
- 3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ กำหนดในราชกิจจานุเบกษา
- 3.7 ผู้รับจ้างต้องเป็นนิติบุคคลซึ่งมีอาชีพในการประกอบธุรกิจงานด้านการพัฒนาระบบสารสนเทศหรือประเภทเดียวกับงานที่ประกาศ
- 3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย ณ วันคัดเลือก หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรม ในการคัดเลือกครั้งนี้
- 3.9 ผู้รับจ้างต้องไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้เสนอราคาได้มีคำสั่งให้สละสิทธิ์ความคุ้มกันเช่นนั้น
- 3.10 ผู้ยื่นข้อเสนอต้องลงทะเบียนในระบบจัดซื้อจัดจ้างด้วยวิธีการอิเล็กทรอนิกส์ (Electronic Government Procurement : e - GP) ของกรมบัญชีกลาง

- 3.11 ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการเป็นไปตามเงื่อนไขข้อ 1.1 - 1.2 ของหนังสือคณะกรรมการวินิจฉัยปัญหาการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ กรมบัญชีกลาง ด่วนที่สุด ที่ กค(กวจ) 0405.2/ว124 ลงวันที่ 1 มีนาคม 2566 เรื่อง แนวทางปฏิบัติในการเร่งรัดการปฏิบัติงานตามสัญญาและการกำหนดคุณสมบัติของผู้มีสิทธิยื่นข้อเสนอ

4. ขอบเขตของงานจ้างบำรุงรักษา

- 4.1 ผู้รับจ้างดำเนินการดูแล ตรวจสอบ และบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ให้สามารถใช้งานได้อย่างต่อเนื่องตลอดระยะเวลาการบำรุงรักษา
- 4.2 ผู้รับจ้างต้องมีเจ้าหน้าที่ที่มีประสบการณ์และความเชี่ยวชาญ เพื่อบริการให้คำปรึกษา และตอบปัญหาทางโทรศัพท์ โทรศัพท์เคลื่อนที่ โทรสาร ไปรษณีย์อิเล็กทรอนิกส์ (E-Mail) หรือ Line ในวันและเวลาทำการของ รพม. (จันทร์ - ศุกร์ ระหว่างเวลา 08.00 น. - 17.00 น.) เมื่อได้รับแจ้งปัญหา จะต้องตอบปัญหาขั้นต้นภายใน 1 ชั่วโมง หลังจากได้รับแจ้ง โดยจะต้องดำเนินการตรวจสอบและแก้ไขให้แล้วเสร็จภายใน 5 วันทำการ นับแต่เวลาที่ผู้ว่าจ้างได้แจ้งข้อขัดข้อง ยกเว้นในกรณีที่มีการขัดข้องนั้น เป็นปัญหาที่มีความซับซ้อน ผู้รับจ้างจะต้องจัดทำแผนการดำเนินงาน พร้อมทั้งชี้แจงรายละเอียดของปัญหา และการแก้ปัญหาฯ ดังกล่าวจัดส่งให้แก่คณะกรรมการตรวจรับพัสดุฯ พิจารณาให้ความเห็นชอบ
- 4.3 ผู้รับจ้างจะต้องดำเนินการแก้ไขปัญหาข้อผิดพลาดของซอฟต์แวร์ (Debugging) เมื่อผู้ใช้ไม่สามารถใช้งานได้
- 4.4 ผู้รับจ้างต้องจัดให้มีเจ้าหน้าที่ ผู้ที่มีความรู้ ความชำนาญระบบติดตามความก้าวหน้าโครงการ (PPMS) เข้าดูแลรักษาระบบ (Preventive Maintenance: PM) ไตรมาสละ 1 ครั้ง เป็นอย่างน้อย พร้อมทั้งจัดทำรายงานผลการตรวจสอบระบบติดตามความก้าวหน้าโครงการ (PPMS) ตามที่ รพม. กำหนด
- 4.5 ในกรณีที่ รพม. มีความประสงค์จะเปลี่ยนแปลงเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์คอมพิวเตอร์อื่น ๆ สำหรับระบบติดตามความก้าวหน้าโครงการ (PPMS) ใหม่ ผู้รับจ้างจะต้องดำเนินการโอนย้ายระบบฯ ให้และเมื่อโอนย้ายแล้ว ระบบฯ จะต้องสามารถใช้งานได้ดังเดิม โดยไม่ก่อให้เกิดความเสียหายในการปฏิบัติงานของ รพม.
- 4.6 ในกรณีที่เครื่องคอมพิวเตอร์แม่ข่ายของ รพม. ไม่สามารถใช้งานได้ มีความจำเป็นต้องใช้เครื่องคอมพิวเตอร์แม่ข่ายที่ศูนย์คอมพิวเตอร์สำรอง (DR - site) ผู้รับจ้างจะต้องดำเนินการติดตั้งระบบติดตามความก้าวหน้าโครงการ (PPMS) พร้อมให้คำแนะนำหรือคำปรึกษาเกี่ยวกับปัญหาที่เกิดขึ้นให้สามารถใช้งานได้ โดยไม่มีค่าใช้จ่ายเพิ่มเติม
- 4.7 หากมีการปรับปรุงระบบติดตามความก้าวหน้าโครงการ (PPMS) เป็นเวอร์ชันใหม่ ผู้รับจ้างจะต้องนำมาปรับปรุงให้ รพม. โดยไม่มีค่าใช้จ่ายเพิ่มเติม
- 4.8 การบริการบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ให้ครอบคลุมถึงค่าแรงงาน ค่าให้คำปรึกษาที่เกี่ยวข้อง ค่าใช้จ่ายในการเดินทาง ค่าวัสดุอุปกรณ์ที่จำเป็น และค่าใช้จ่ายอื่นใดทั้งหลายทั้งปวงที่เกี่ยวข้องกับการบำรุงรักษา โดยที่ รพม. ไม่ต้องเสียค่าใช้จ่ายใด ๆ ทั้งสิ้นเพิ่มเติมจากราคาค่าจ้างในงานที่กำหนดไว้ในสัญญา

- 4.9 การติดตามปัญหา ความก้าวหน้าและแก้ไขปัญหา เมื่อดำเนินการเสร็จเรียบร้อยแล้ว ผู้รับจ้างต้องแจ้งผลให้ผู้แจ้งทราบ และรวบรวมเป็นรายงานสรุปการแจ้งปัญหาและการแก้ไขระบบติดตามความก้าวหน้าโครงการ (PPMS) ตามที่ รฟม. กำหนด
- 4.10 เมื่อผู้รับจ้างจะเข้าดำเนินการเพื่อแก้ไขปัญหาต่าง ๆ จะต้องแจ้งให้เจ้าหน้าที่ผู้รับผิดชอบของ รฟม. ทราบล่วงหน้า
- 4.11 การปรับปรุงแก้ไข Source Code ส่วนใด ๆ ของระบบติดตามความก้าวหน้าโครงการ (PPMS) ให้ผู้รับจ้างจัดทำรายละเอียดการแก้ไข (Log statement) ที่มีรายละเอียดครบถ้วน เข้าใจง่าย และจัดส่งให้แก่ รฟม. เพื่อใช้สำหรับอ้างอิงการแก้ไขระบบฯ ในอนาคต
- 4.12 Source code ที่ได้ปรับปรุงแก้ไข รวมทั้งรายงานหรือเอกสารใด ๆ ที่ผู้รับจ้างได้ทำขึ้น อันเนื่องมาจากการปฏิบัติงานตามสัญญาฯ ให้ตกเป็นกรรมสิทธิ์และลิขสิทธิ์ของ รฟม. ทั้งหมดอย่างไรก็ตาม ผู้รับจ้างอาจเก็บสำเนารายงานและเอกสารอื่นดังกล่าวไว้ เพื่อเป็นประวัติการทำงานของผู้รับจ้างเองได้
- 4.13 การปรับปรุงแก้ไข Source Code ส่วนใด ๆ ผู้รับจ้างต้องแก้ไขและออกแบบระบบให้ปลอดภัยตามมาตรฐาน Open Web Application Security Project (OWASP) Top 10 ล่าสุด หรือมาตรฐาน Common Weakness Enumeration (CWE) Top 25 ล่าสุด ณ ปีที่ส่งมอบงาน นับถัดจากวันที่ลงนามในสัญญา หรือมาตรฐานที่ยอมรับในสากล หรือกำหนดซอฟต์แวร์ให้เป็นเวอร์ชันล่าสุดที่ได้รับการอัปเดตแล้ว
- 4.14 ผู้รับจ้างต้องจัดทำเอกสาร Version Control ของระบบติดตามความก้าวหน้าโครงการ (PPMS) และจัดส่งให้แก่ รฟม. ทราบทุกครั้ง ก่อนนำ Source Code ที่ได้ปรับปรุงแก้ไข ไป Deploy ขึ้นระบบจริง เพื่อใช้สำหรับควบคุมและอ้างอิงการแก้ไขระบบ
- 4.15 การปรับปรุงแก้ไข Source Code ส่วนใด ๆ ผู้รับจ้างต้องตรวจสอบความมั่นคงปลอดภัยของ Source Code (Source Code Review) ตามมาตรฐานที่ รฟม. กำหนด
- 4.16 การปรับปรุงแก้ไข Source Code ส่วนใด ๆ ผู้รับจ้างต้องแก้ไขและออกแบบระบบให้มีการตรวจสอบความถูกต้องของข้อมูลนำเข้า (Input Validation) ก่อนการบันทึกและ/หรือประมวลผลข้อมูล รวมทั้งตรวจสอบข้อมูลที่ส่งออกจากระบบ (Output Validation) เพื่อป้องกันการแสดงผลหรือการประมวลผลข้อมูลที่ไม่เหมาะสม
- 4.17 ผู้รับจ้างและผู้ปฏิบัติงานของผู้รับจ้างจะต้องไม่เปิดเผยความลับของข้อมูลหรือข้อมูลอื่นใดทั้งหมดหรือบางส่วนที่ได้รับหรือรับรู้มาจาก รฟม. ให้ผู้อื่นทราบโดยมิได้รับความยินยอมจากรฟม. และหากมีการนำข้อมูลใด ๆ ออกจาก รฟม. ผู้รับจ้างฯ จะต้องทำลายข้อมูลทั้งที่เป็นเอกสาร หรือข้อมูลในรูปแบบอิเล็กทรอนิกส์ทันทีที่สิ้นสุดสัญญาจ้าง โดยผู้รับจ้างฯ ต้องลงนามในเอกสารข้อตกลงในการไม่เปิดเผยข้อมูล (Non - Disclosure Agreement) และ รฟม. ขอสงวนสิทธิ์ในการเรียกร้องค่าเสียหายอันเนื่องมาจากการละเมิดข้อตกลงดังกล่าว
- 4.18 ผู้รับจ้างต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รฟม. ที่ปรากฏดัง ภาคผนวก ก.
- 4.19 ผู้รับจ้างจะต้องส่งบุคลากรเข้าร่วมการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness) เพื่อสร้างความตระหนักที่เหมาะสม ทบทวนนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและขั้นตอนปฏิบัติของ รฟม.

- 4.20 ระบบที่มีลักษณะเป็น Web Based Application ต้องใช้งานผ่านโปรโตคอล Hypertext Transfer Protocol Secure (HTTPS) โดยใช้ใบรับรอง SSL Certificate ที่ รฟม. กำหนด ทั้งนี้ หากใบรับรอง SSL Certificate หมดอายุ ผู้รับจ้างต้องปรับปรุงให้ระบบฯ ใช้งานผ่าน SSL Certificate ที่ รฟม. ต่ออายุแล้วต่อไป
- 4.21 ผู้รับจ้างต้องปิดช่องโหว่ (Hardening) ของระบบติดตามความก้าวหน้าโครงการ (PPMS) และซอฟต์แวร์ที่ใช้ในการพัฒนา หากซอฟต์แวร์นั้น ๆ มีการประกาศช่องโหว่ รวมทั้งช่องโหว่ที่ รฟม. ตรวจพบ พร้อมทั้งจัดทำรายงานผลการปิดช่องโหว่ระบบติดตามความก้าวหน้าโครงการ (PPMS) ตามที่ รฟม. กำหนด โดยที่ รฟม. ไม่ต้องเสียค่าใช้จ่ายใด ๆ เพิ่มเติมจากราคาค่าจ้างงานตามที่กำหนดไว้ตามสัญญา ทั้งนี้หากผู้รับจ้างไม่สามารถปิดช่องโหว่ให้แล้วเสร็จภายในระยะเวลาการรับประกัน จะต้องจัดทำแผนการดำเนินงานปิดช่องโหว่ ซึ่งระบุรายละเอียดและสาเหตุที่ไม่สามารถปิดช่องโหว่ภายในระยะเวลาการรับประกัน พร้อมทั้งจัดส่งให้คณะกรรมการตรวจรับพัสดุฯ พิจารณาให้ความเห็นชอบ
- 4.22 การติดตามความคืบหน้าการปิดช่องโหว่ เมื่อดำเนินการเสร็จเรียบร้อยแล้ว ผู้รับจ้างต้องแจ้งผลให้ผู้แจ้งทราบ และรวบรวมเป็นรายงานผลการปิดช่องโหว่ระบบติดตามความก้าวหน้าโครงการ (PPMS) ตามที่ รฟม. กำหนด
- 4.23 ผู้รับจ้างจะต้อง ทบทวน/ ปรับปรุง คู่มือการใช้งานระบบติดตามความก้าวหน้าโครงการ (PPMS) และจัดส่งให้แก่ รฟม. เมื่อมีการปรับปรุงระบบฯ ดังกล่าว โดยไม่มีค่าใช้จ่ายเพิ่มเติม
- 4.24 ผู้รับจ้างต้องจัดส่งรายงานผลการบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ให้แก่ รฟม. เพื่อทราบ ทุกสิ้นไตรมาส โดยส่งมอบภายในวันที่ 15 ของไตรมาสถัดไป (ภาคผนวก ข.) ซึ่งประกอบด้วย
- 1) รายงานผลการตรวจสอบระบบติดตามความก้าวหน้าโครงการ (PPMS)
 - 2) รายงานการตรวจสอบสิทธิการเข้าถึงระบบ (Role Matrix)
 - 3) รายงานสรุปการแจ้งปัญหาและการแก้ไขระบบติดตามความก้าวหน้าโครงการ (PPMS)
 - 4) รายงานผลการปิดช่องโหว่ระบบติดตามความก้าวหน้าโครงการ (PPMS) (หากมี)
 - 5) รายงานทะเบียนทรัพย์สิน (Asset Inventory)
- 4.25 ผู้รับจ้างจะต้องไม่เอางานทั้งหมดหรือแต่บางส่วนไปจ้างช่วงอีกทอดหนึ่ง เว้นแต่การจ้างช่วงงาน แต่บางส่วนที่ได้รับอนุญาตเป็นหนังสือจาก รฟม. แล้ว การที่ รฟม. ได้อนุญาตให้จ้างช่วงงานแต่บางส่วนดังกล่าวนี้ ไม่เป็นเหตุให้ผู้รับจ้างหลุดพ้นจากความรับผิดชอบหรือพันธหน้าที่ และผู้รับจ้างจะยังคงต้องรับผิดชอบในความผิดและความประมาทเลินเล่อของผู้รับจ้างช่วง หรือของตัวแทนหรือลูกจ้างของผู้รับจ้างช่วงนั้นทุกประการ (หากมี)

5. กำหนดเวลาส่งมอบพัสดุ

นับตั้งแต่วันที่ 1 ตุลาคม 2566 – วันที่ 30 กันยายน 2567

6. หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

ในการพิจารณาผลการคัดเลือกข้อเสนอการจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ครั้งนี้ รฟม. จะพิจารณาคัดเลือกโดยใช้หลักเกณฑ์ **ราคารวม** ที่เป็นราคาต่ำสุด อยู่ในวงเงินงบประมาณ และเป็นผู้มีคุณสมบัติครบถ้วน ถูกต้อง ตรงตามรายละเอียดและเงื่อนไขที่ รฟม. กำหนด

7. วงเงินงบประมาณ/วงเงินที่ได้รับจัดสรร

วงเงินสำหรับการจัดการจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ประจำปีงบประมาณ 2567 เป็นจำนวนทั้งสิ้น 1,350,000.00 บาท (หนึ่งล้านสามแสนห้าหมื่นบาทถ้วน) รวมภาษีมูลค่าเพิ่มตลอดจนภาษีอากรอื่น ๆ และค่าใช้จ่ายทั้งปวงแล้ว

8. งวดงานและการจ่ายเงิน

รพม. จะชำระเงินค่าจ้างงานให้แก่ผู้รับจ้าง โดยแบ่งจ่ายเป็น 4 งวด เป็นจำนวนเงินเท่ากัน (รวมภาษีมูลค่าเพิ่ม) ซึ่งแต่ละงวดจะจ่ายทุก ๆ สิ้นไตรมาส หลังจาก รพม. ได้รับรายงานผลการบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) และคณะกรรมการตรวจรับพัสดุฯ ได้มีการตรวจรับงานแต่ละงวดเรียบร้อยแล้ว

9. อัตราค่าปรับ

ในกรณีที่ผู้ใช้งานไม่สามารถใช้งานระบบติดตามความก้าวหน้าโครงการ (PPMS) ได้ ผู้รับจ้างต้องดำเนินการตรวจสอบและแก้ไขให้แล้วเสร็จภายใน 5 วันทำการ นับแต่เวลาที่ผู้ว่าจ้างได้แจ้งข้อขัดข้องให้ผู้รับจ้างทราบทางโทรศัพท์ โทรศัพท์เคลื่อนที่ โทรสาร ไปรษณีย์อิเล็กทรอนิกส์ (E-Mail) หรือ Line ในวันและเวลาทำการของ รพม. (จันทร์ - ศุกร์ ระหว่างเวลา 08.00 น. - 17.00 น.) ยกเว้นในกรณีที่การขัดข้องนั้นเป็นปัญหาที่มีความซับซ้อน ผู้รับจ้างจะต้องจัดทำแผนการดำเนินงานจัดส่งให้แก่คณะกรรมการตรวจรับพัสดุฯ พิจารณาให้ความเห็นชอบ ทั้งนี้หากไม่สามารถดำเนินการแก้ไขได้แล้วเสร็จตามแผนฯ (ภายใน 5 วันทำการ หรือตามที่คณะกรรมการตรวจรับพัสดุฯ ได้ให้ความเห็นชอบแล้วแต่กรณี) ผู้รับจ้างจะต้องเสียค่าปรับเป็นรายวันในอัตราวันละ 1,500.00 บาท (หนึ่งพันห้าร้อยบาทถ้วน) เฉพาะของวันให้คิดเป็น 1 วัน

2

2

2

2

2

2

2

ภาคผนวก ก.2



การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

MASS RAPID TRANSIT AUTHORITY OF THAILAND

รัฐวิสาหกิจภายใต้กำกับของรัฐมนตรีว่าการกระทรวงคมนาคม

A STATE ENTERPRISE UNDER SUPERVISION OF MINISTER OF TRANSPORT

ประกาศการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (ฉบับปรับปรุงครั้งที่ 11)

ด้วยพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 มาตรา 5 กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ มีความมั่นคงปลอดภัยและเชื่อถือได้ จึงส่งผลให้ระบบเทคโนโลยีสารสนเทศของการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย (รฟม.) ต้องมีการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศอย่างครบถ้วนเพื่อธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) และความน่าเชื่อถือ (Reliability)

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ 2) พ.ศ. 2556 ข้อ 14 กำหนดให้หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer: CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

อาศัยอำนาจตามความในมาตรา 25 แห่งพระราชบัญญัติการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย พ.ศ. 2543 ผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย จึงออกประกาศการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ดังต่อไปนี้

1. วัตถุประสงค์และขอบเขต

เพื่อให้การใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาและลดผลกระทบจากการใช้งานระบบเทคโนโลยีสารสนเทศ ในลักษณะที่ไม่ถูกต้องหรือจากการถูกคุกคามจากภัยต่าง ๆ จึงได้กำหนดนโยบายเพื่อควบคุมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ดังนี้

1.1 การเข้าถึงหรือควบคุมการใช้งานสารสนเทศครอบคลุม 4 ด้าน คือ

1.1.1 การเข้าถึงระบบสารสนเทศ (Access control) ต้องตรวจสอบการอนุมัติสิทธิ์การเข้าถึงระบบและกำหนดรหัสผ่าน การลงทะเบียนผู้ใช้งานเพื่อให้ผู้ใช้ที่มีสิทธิ์ (User authentication) เท่านั้นที่สามารถ

สมบูรณ์

/เข้าถึง ...
สิทธิ์

เข้าถึงระบบได้ รวมถึงมีการเก็บบันทึกข้อมูลการเข้าถึงระบบ (Access log) และข้อมูลจราจรทางคอมพิวเตอร์ ทั้งนี้ การให้สิทธิ์การใช้งานระบบสารสนเทศนั้นต้องให้สิทธิ์ที่เหมาะสมและเพียงพอ (Need to know and Need to use)

1.1.2 การเข้าถึงระบบเครือข่าย (Network access control) ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ การรับ - ส่ง หรือการไหลเวียนข้อมูลหรือสารสนเทศจะต้องผ่านระบบการรักษาความปลอดภัยที่องค์กรจัดสรรไว้ เช่น Firewall IDS/IPS Proxy หรือการตรวจสอบไวรัสคอมพิวเตอร์ เป็นต้น เพื่อควบคุมและป้องกันภัยคุกคามอย่างเป็นระบบ

1.1.3 การเข้าถึงระบบปฏิบัติการ (Operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการ โดยไม่ได้รับอนุญาต โดยกำหนดให้มีการยืนยันตัวตนเพื่อระบุถึงตัวตนของผู้ใช้งาน รวมทั้งกำหนดให้มีการจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้ความมั่นคงปลอดภัยมากยิ่งขึ้น

1.1.4 การเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information access control) ต้องกำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศ โดยให้สิทธิ์เฉพาะระบบงานสารสนเทศที่ต้องปฏิบัติตามหน้าที่เท่านั้น รวมทั้งมีการทบทวนสิทธิ์การใช้งานระบบสารสนเทศอย่างสม่ำเสมอ

1.2 มีระบบสารสนเทศและระบบสำรองที่อยู่ในสภาพพร้อมใช้งาน รวมทั้งมีแผนเตรียมพร้อมในกรณีฉุกเฉินหรือกรณีที่ไม่สามารถดำเนินการตามวิธีการทางอิเล็กทรอนิกส์ได้ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

1.3 ตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศอย่างสม่ำเสมอ

2. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รพม.

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รพม. ใช้แนวทางและกระบวนการอ้างอิงตาม 1) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานรัฐ พ.ศ. 2553 2) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555 และ 3) มาตรฐาน ISO/IEC 27001:2013 โดยแบ่งแนวปฏิบัติออกเป็น 16 ส่วนตามเอกสารแนบท้ายประกาศ ดังต่อไปนี้

2.1 นโยบายการบริหารจัดการความมั่นคงปลอดภัยสำหรับผู้บริหาร (ส่วนที่ 1)

2.2 ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร (ส่วนที่ 2)

2.3 การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (ส่วนที่ 3)

2.4 การจัดการทรัพย์สิน (ส่วนที่ 4)

2.5 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (ส่วนที่ 5)

2.6 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ (ส่วนที่ 6)

2.7 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (ส่วนที่ 7)

2.8 การควบคุมหน่วยงานภายนอกและผู้ใช้งาน (บุคคลภายนอก) เข้าถึงระบบเทคโนโลยีสารสนเทศ (ส่วนที่ 8)

2.9 การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ของ รพม. (ส่วนที่ 9)

2.10 การใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์ (ส่วนที่ 10)

- 2.11 การใช้งานจดหมายอิเล็กทรอนิกส์ (ส่วนที่ 11)
- 2.12 การสำรองข้อมูลและการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (ส่วนที่ 12)
- 2.13 การตรวจสอบและประเมินความเสี่ยง (ส่วนที่ 13)
- 2.14 การถ่ายโอน และการแลกเปลี่ยนข้อมูลสารสนเทศ (ส่วนที่ 14)
- 2.15 การควบคุมการเข้ารหัส (ส่วนที่ 15)
- 2.16 การนำอุปกรณ์ส่วนตัวมาใช้งาน (Bring your own device) (ส่วนที่ 16)

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศตามข้อ 2. จัดเป็นมาตรฐานด้านความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. ซึ่งบุคลากรของ รฟม. หน่วยงานภายนอก รวมถึงผู้ใช้บริการระบบสารสนเทศของ รฟม. ที่เกี่ยวข้องจะต้องปฏิบัติตามอย่างเคร่งครัด

3. กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้ว่าการการรถไฟฟ้ามหานครแห่งประเทศไทย (Chief Executive Officer: CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น และดำเนินการตรวจสอบข้อเท็จจริงกรณีที่ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด รวมทั้งให้พิจารณาลงโทษตามเหตุอันควร

นโยบายนี้ให้ใช้บังคับเมื่อพ้นกำหนด 7 วัน นับแต่วันที่ผู้มีอำนาจลงนาม

ประกาศ ณ วันที่ 7 กันยายน พ.ศ. 2565



(นายภคพงศ์ ศิริกันทรมาศ)

ผู้ว่าการการรถไฟฟ้ามหานครแห่งประเทศไทย



ภคพงศ์

เอกสารแนบท้ายประกาศ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ของ รฟม.

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

1. รฟม. หมายถึง การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
2. ผทท. หมายถึง ฝ่ายเทคโนโลยีสารสนเทศ
3. ผู้บริหารระดับสูงสุด หมายถึง ผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
4. ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของ รฟม.
5. ผู้ใช้งาน หมายถึง บุคคลที่ได้รับอนุญาตให้สามารถเข้าใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. ดังนี้
 - บุคลากรของ รฟม.
 - บุคคลภายนอกที่ รฟม. อนุญาตให้เข้ามาใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. ได้ชั่วคราว เพื่อประโยชน์ในการดำเนินการของ รฟม. ได้แก่ พนักงานหรือลูกจ้างบริษัทภายนอกที่เข้ามาติดตั้งหรือดูแลรักษาระบบให้กับ รฟม. ที่ปรึกษา ผู้ปฏิบัติงานตามสัญญา หรือนิสิตนักศึกษาฝึกงาน
6. ผู้ใช้งานภายนอก หมายถึง ลูกค้าหรือบุคคลภายนอกที่ไม่ใช่กลุ่มผู้ใช้งานตามข้อ 5. ที่ใช้บริการระบบงานสารสนเทศของ รฟม. ผ่านเครือข่ายสาธารณะ (Internet)
7. หน่วยงานภายนอก หมายถึง องค์กร ซึ่ง รฟม. อนุญาตให้มีสิทธิ์ในการเข้าถึง หรือใช้ข้อมูล หรือสินทรัพย์ต่าง ๆ ของ รฟม. โดยจะได้รับสิทธิ์ในการใช้ระบบตามประเภทงานตามอำนาจและต้องรับผิดชอบในการรักษาความลับของข้อมูล
8. ผู้ดูแลระบบ หมายถึง พนักงานที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบสารสนเทศ
9. เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
10. มาตรฐาน หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย
11. ขั้นตอนปฏิบัติ หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานตามที่ได้กำหนดไว้ตามวัตถุประสงค์
12. แนวปฏิบัติ หมายถึง แนวทางที่ต้องปฏิบัติตามเพื่อให้สามารถบรรลุวัตถุประสงค์หรือเป้าหมายได้ง่ายขึ้น
13. ระบบเทคโนโลยีสารสนเทศ (Information technology system) หมายถึง ระบบงานของ รฟม. ที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายสื่อสารข้อมูลมาช่วยในการสร้างสารสนเทศที่ รฟม. สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุน การให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ ได้แก่ ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลและสารสนเทศ เป็นต้น

14. ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด ที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์
15. ข้อมูลจราจรทางคอมพิวเตอร์ (Traffic log) หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เวลา วันที่ ปริมาณ ระยะเวลา หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น
16. สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งข้อมูลอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิกให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ
17. ระบบคอมพิวเตอร์ (Computer system) หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่งหรือสิ่งอื่นใด และแนวปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
18. ระบบเครือข่ายสื่อสารข้อมูล (Network system) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของ รพม. เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น
19. สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกักระบบสารสนเทศของหน่วยงาน
20. ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) และความน่าเชื่อถือ (Reliability)
21. เหตุการณ์ด้านความมั่นคงปลอดภัย หมายถึง เหตุการณ์ที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย มาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
22. สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม
23. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้
24. สินทรัพย์ (Assets) หมายถึง สินทรัพย์ด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารของ รพม. เช่น อุปกรณ์คอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีค่าลิขสิทธิ์ ข้อมูล ระบบข้อมูล ฯลฯ
25. จดหมายอิเล็กทรอนิกส์ (e-mail) หมายถึง ระบบที่บุคคลใช้ในการรับ - ส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว

และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ โดยข่าวสารที่ส่งนั้นจะถูกเก็บไว้ในตู้จดหมาย (Mail box) ที่กำหนดไว้สำหรับผู้ใช้งาน ผู้รับสามารถเปิดอ่าน พิมพ์ลงกระดาษ หรือจะลบทิ้งก็ได้

26. ชุดคำสั่งไม่พึงประสงค์ (Malicious code) หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ชัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
27. เครื่องคอมพิวเตอร์ หมายถึง เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ และเครื่องคอมพิวเตอร์แบบพกพา
28. อุปกรณ์เคลื่อนที่ (Mobile device) หมายถึง อุปกรณ์อิเล็กทรอนิกส์แบบพกพา ซึ่งมีความสามารถในการเชื่อมต่อกับอุปกรณ์อื่นเพื่อรับส่งข้อมูลผ่านระบบเครือข่ายโทรคมนาคมไร้สายหรือโดยอาศัยคลื่นแม่เหล็กไฟฟ้าเป็นสื่อกลาง เช่น Tablet, Smart Phone
29. อุปกรณ์ส่วนตัว หมายถึง อุปกรณ์ที่ รพม. ไม่ได้เป็นผู้จัดสรรให้ใช้งาน แต่เป็นอุปกรณ์ส่วนตัวของผู้ใช้งานที่นำมาเชื่อมต่อกับเครือข่ายภายในของ รพม. เช่น เครื่องคอมพิวเตอร์ส่วนบุคคล (Personal computer) เครื่องคอมพิวเตอร์พกพา (Notebook) อุปกรณ์เคลื่อนที่ (Mobile device) หรือ Removable media เป็นต้น

ส่วนที่ 1

นโยบายการบริหารจัดการความมั่นคงปลอดภัยสำหรับผู้บริหาร

วัตถุประสงค์

- เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรมีความสอดคล้องกับมาตรฐานสากลและกฎหมายด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง

ผู้รับผิดชอบ

- ผู้บริหารสูงสุด

อ้างอิงมาตรฐาน

- หมวดที่ 1 นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information security policy)

แนวปฏิบัติ

1. จัดให้มีการทำและทบทวนหรือปรับปรุงนโยบายความมั่นคงปลอดภัย และแนวปฏิบัติที่สนับสนุนการทำงานต่าง ๆ อย่างน้อยปีละ 1 ครั้ง โดยพิจารณาจากปัจจัยนำเข้า ดังนี้
 - 1.1 กลยุทธ์การดำเนินงานขององค์กร
 - 1.2 ข้อมูลกฎหมาย ระเบียบ ข้อบังคับต่าง ๆ ที่ต้องปฏิบัติตาม
 - 1.3 การปรับปรุงนโยบายความมั่นคงปลอดภัยสำหรับปีถัดไป
 - 1.4 ผลการประเมินความเสี่ยงและแผนลดความเสี่ยง
 - 1.5 ผลการแจ้งเตือนโดยระบบป้องกันการบุกรุกในปีที่ผ่านมา
 - 1.6 ผลของการตรวจสอบข้อมูลการปิดช่องโหว่ (Patch) สำหรับระบบต่าง ๆ ในปีที่ผ่านมา
 - 1.7 การจัดทำและต่อสัญญาบำรุงรักษาระบบและอุปกรณ์ต่าง ๆ
 - 1.8 แผนการอบรมทางด้านความมั่นคงปลอดภัยประจำปีซึ่งรวมถึงการสร้างตระหนักรู้
 - 1.9 ผลการทดสอบแผนกู้คืนในปีที่ผ่านมา
 - 1.10 ข้อมูลภัยคุกคามต่าง ๆ ที่เคยเกิดขึ้นในอดีตและปัจจุบัน รวมทั้งภัยคุกคามที่ได้รับแจ้งจากหน่วยงานภายนอก
 - 1.11 ผลการตรวจสอบการปฏิบัติตามนโยบายความมั่นคงปลอดภัยโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก
2. จัดให้มีทรัพยากรด้านบุคลากร งบประมาณ การบริหารจัดการ และวัตถุประสงค์ที่เพียงพอต่อการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศในแต่ละปีงบประมาณ
3. จัดให้มีบุคลากรดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศและกำหนดหน้าที่ความรับผิดชอบรวมทั้งปรับปรุงโครงสร้างดังกล่าวตามความจำเป็น
4. แสดงเจตนาชัดเจนหรือสื่อสารอย่างสม่ำเสมอเพื่อให้ผู้ใช้งานทั้งหมดได้เห็นถึงความสำคัญของการปฏิบัติตามนโยบายความมั่นคงปลอดภัยและนโยบายสนับสนุนต่าง ๆ โดยเคร่งครัดและเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับสารสนเทศขององค์กร รวมถึงสร้างความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

ส่วนที่ 2

ความมั่นคงปลอดภัยเกี่ยวกับบุคลากร

วัตถุประสงค์

- เพื่อให้ผู้ใช้งานเข้าใจถึงบทบาท หน้าที่ความรับผิดชอบ ทั้งก่อนการจ้างงาน ระหว่างการจ้างงาน และสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน ตลอดจนตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศเพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง การใช้งานระบบเทคโนโลยีสารสนเทศผิดวัตถุประสงค์และความผิดพลาดในการปฏิบัติหน้าที่ ซึ่งอาจส่งผลกระทบต่อหรือทำให้ รพม. เกิดความเสียหาย

ผู้รับผิดชอบ

- ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ ผู้อำนวยการฝ่ายทรัพยากรบุคคล ผู้อำนวยการฝ่าย/สำนัก ที่กำกับดูแลงานที่มีการว่าจ้างหน่วยงานภายนอก

อ้างอิงมาตรฐาน

- หมวดที่ 3 ความมั่นคงปลอดภัยสำหรับบุคลากร (Organization of information security)
- หมวดที่ 4 การบริหารจัดการทรัพย์สิน (Asset management)
- หมวดที่ 9 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)

แนวปฏิบัติ

1. การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to employment) เพื่อคัดสรรบุคลากรก่อนที่จะเข้ามาปฏิบัติงาน และเพื่อลดความเสี่ยงจากการปฏิบัติงานผิดพลาด การขโมย การปลอมแปลง และการนำระบบสารสนเทศหรือทรัพยากรสารสนเทศของ รพม. ไปใช้ในทางที่ไม่เหมาะสม รวมทั้งเพื่อให้ผู้ใช้งานเข้าใจในหน้าที่ความรับผิดชอบของตนเอง
 - 1.1 การตรวจสอบคุณสมบัติของผู้สมัคร (Screening)

ฝ่ายทรัพยากรบุคคล หรือฝ่าย/สำนัก ที่กำกับดูแลงานที่มีการว่าจ้างหน่วยงานภายนอกต้องตรวจสอบคุณสมบัติของผู้สมัคร (ทั้งกรณีการจ้างเป็นพนักงาน ลูกจ้าง การว่าจ้างหน่วยงานภายนอกเพื่อปฏิบัติงานให้ รพม. รวมทั้งนิสิตนักศึกษาฝึกงาน) โดยผู้สมัครต้องไม่เคยกระทำผิดกฎหมาย ระเบียบ ข้อบังคับ หรือจริยธรรม รวมทั้งไม่มีประวัติในการบุกรุก แก๊ง ทำลาย หรือโจรกรรมข้อมูลในระบบเทคโนโลยีสารสนเทศมาก่อน และมีคุณสมบัติตามที่ รพม. กำหนด
 - 1.2 การกำหนดเงื่อนไขการจ้างงาน (Terms and conditions of employment) การว่าจ้างให้มีเงื่อนไขการจ้างงานให้ครอบคลุมในเรื่องดังต่อไปนี้
 - 1.2.1 กำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศอย่างเป็นลายลักษณ์อักษร (Information security roles and responsibilities) แก่ผู้ใช้งาน โดยกำหนดให้สอดคล้องกับนโยบายความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของ รพม.
 - 1.2.2 กำหนดให้มีการลงนามในสัญญาว่าจะไม่เปิดเผยความลับของ รพม. (Non-Disclosure Agreement : NDA)
 - 1.2.3 ระบบเทคโนโลยีสารสนเทศที่สร้างหรือพัฒนาโดยผู้ใช้งานในระหว่างการว่าจ้างถือเป็นสินทรัพย์ของ รพม.

- 1.2.4 กำหนดความรับผิดชอบหรือบทลงโทษ หากผู้ใช้งานไม่ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รฟม. รวมทั้ง กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
2. การสร้างความมั่นคงปลอดภัยในระหว่างการจ้างงาน (During employment) เพื่อสร้างความตระหนักแก่ผู้ใช้งานเกี่ยวกับภัยที่เกี่ยวข้องกับการปฏิบัติงานสารสนเทศ รวมถึงให้ความรู้เพื่อให้สามารถป้องกันภัยดังกล่าวได้
 - 2.1 หน้าที่ในการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management responsibilities) ผู้บริหาร รฟม. ทุกระดับชั้นมีหน้าที่สนับสนุนและส่งเสริมเรื่องดังต่อไปนี้ แก่ผู้ใช้งาน
 - 2.1.1 ประกาศนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ รฟม. เป็นลายลักษณ์อักษรให้ทุกคนรับทราบและปฏิบัติตาม
 - 2.1.2 จูงใจให้ผู้ใช้งานปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ รฟม.
 - 2.1.3 สร้างความตระหนักถึงความมั่นคงปลอดภัยด้านสารสนเทศที่เกี่ยวข้องกับหน้าที่ความรับผิดชอบของตนเองและของ รฟม.
 - 2.2 การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่ผู้ใช้งาน (Information security awareness, education and training) การสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยอย่างสม่ำเสมอ
 - 2.2.1 ผู้ดูแลระบบต้องแจ้งเตือนภัยคุกคาม และช่องโหว่ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศแก่ผู้ใช้งานที่เกี่ยวข้อง นอกจากนี้ก็ต้องแจ้งเตือนให้ผู้ใช้งานเพิ่มความระมัดระวัง ความเสี่ยงต่าง ๆ เช่น ไวรัสมัลแวร์ เทคนิคการหลอกล่อทางจิตวิทยา (Social engineering) และช่องโหว่ทางเทคนิค เป็นต้น
 - 2.2.2 ผทท. ต้องดำเนินการฝึกอบรม หรือประชาสัมพันธ์เพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศแก่ผู้ใช้งานเป็นประจำทุกปี
 - 2.2.3 ผทท. ต้องแจ้งผู้ใช้งานให้ทราบ เมื่อมีการเปลี่ยนแปลงนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศของ รฟม. รวมทั้งอธิบายผลกระทบจากการเปลี่ยนแปลงดังกล่าว
 - 2.3 การกำหนดบทลงโทษ
 - 2.3.1 ความรับผิดชอบตามกฎหมาย
นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ไม่ได้ก่อให้เกิดสิทธิ์ทางกฎหมายที่ทำให้ผู้ใช้งานพ้นผิดแม้จะได้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ และผู้ใช้งานตกลงยินยอมที่จะไม่ดำเนินการใด ๆ ทางกฎหมายต่อ รฟม. ซึ่งได้ปฏิบัติตามระเบียบนี้ แต่อย่างไรก็ตามหากผู้ใช้งานกระทำการละเมิดหรือกระทำผิดตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ อาจเป็นความผิดทางวินัยและเป็นเหตุให้ถูกลงโทษทางวินัยได้ รฟม. ไม่มีส่วนรับผิดชอบต่อการละเมิดทรัพย์สินทางปัญญาที่เกิดจากการใช้ระบบคอมพิวเตอร์

2.3.2 การพิจารณาโทษผู้กระทำผิด

ผู้ใช้งานที่กระทำความผิด ฝ่าท. จะเพิกถอนสิทธิ์การใช้งานและอาจเป็นความผิดทางวินัย หรือความผิดตามกฎหมายที่เกี่ยวข้อง

- 1) พนักงาน/ลูกจ้างที่ฝ่าฝืนหรือละเมิดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รพม. ต้องถูกลงโทษตามกระบวนการทางวินัยของ รพม. รวมถึงกฎหมายที่เกี่ยวข้อง
- 2) หน่วยงานภายนอกที่กระทำความผิด จะมีโทษตามที่ระบุไว้ในสัญญาหรือถูกเพิกถอนสิทธิ์การใช้งาน รวมถึงดำเนินการตามกฎหมายที่เกี่ยวข้อง

3. การสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน (Termination and change of employment)

เพื่อกำหนดหน้าที่ความรับผิดชอบเมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน ซึ่งรวมถึงการคืนทรัพย์สินและการถอดถอนสิทธิ์ในการเข้าถึง

3.1 การแจ้งการสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน

3.1.1 ฝ่ายทรัพยากรบุคคลต้องแจ้งให้ฝ่ายเทคโนโลยีสารสนเทศทราบทันทีหากพนักงานมีการลาออก โยกย้าย เกษียณ หรือเสียชีวิต เพื่อฝ่ายเทคโนโลยีสารสนเทศจะได้ตรวจสอบและบริหารจัดการสิทธิ์ในการเข้าถึงระบบเทคโนโลยีสารสนเทศ

3.1.2 ฝ่าย/สำนัก ที่กำกับดูแลงานที่มีการว่าจ้างหน่วยงานภายนอก ต้องแจ้งให้ฝ่ายเทคโนโลยีสารสนเทศทราบทันทีในกรณีที่ผู้รับจ้างภายนอกสิ้นสุดสัญญาจ้างหรือมีการยกเลิกสัญญาจ้างเพื่อให้ ฝ่าท. ตรวจสอบการใช้งานระบบสารสนเทศและถอดถอนสิทธิ์ในการเข้าถึงระบบสารสนเทศของ รพม.

3.2 การคืนสินทรัพย์ของ รพม.

ผู้ดูแลระบบต้องตรวจสอบเพื่อเรียกคืนสินทรัพย์ของ รพม. จากผู้ใช้งาน เมื่อการสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน

3.3 การถอดถอนสิทธิ์ในการเข้าถึง

3.3.1 ผู้ดูแลระบบต้องถอดถอนสิทธิ์ในการเข้าถึงของผู้ใช้งาน เมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน

3.3.2 การถอดถอนสิทธิ์ในการเข้าถึงหมายถึงทางกายภาพ (Physical) และทางตรรกะ (Logical) เช่น กุญแจ บัตรแสดงตน บัตรประจำตัวผู้ใช้งาน และบัญชีผู้ใช้งาน เป็นต้น

3.3.3 ในกรณีที่ผู้ใช้งานที่สิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน มีการใช้บัญชีผู้ใช้งานร่วมกัน (Shared user ID) กับผู้ใช้งานอื่น ผู้บังคับบัญชาต้องเปลี่ยนรหัสผ่านทันทีหลังจากสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน

ส่วนที่ 23

การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

วัตถุประสงค์

- เพื่อควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าถึงอาคารสถานที่ และพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area)

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้อำนวยการฝ่ายจัดซื้อและบริการ

อ้างอิงมาตรฐาน

- หมวดที่ 7 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security)

แนวปฏิบัติ

1. ผู้ดูแลระบบ ต้องออกแบบ และติดตั้งอุปกรณ์หรือระบบสนับสนุน (Facilities) เพื่อป้องกันการรักษาความมั่นคงปลอดภัยด้านกายภาพ เช่น อุปกรณ์ดับเพลิง ระบบสำรองไฟฟ้า เครื่องกำเนิดไฟฟ้า ระบบปรับอากาศและควบคุมความชื้น ระบบเตือนภัยน้ำรั่ว และต้องมีการบำรุงรักษาอย่างสม่ำเสมอ
2. ผู้ดูแลระบบต้องติดตั้งอุปกรณ์สารสนเทศในตู้แร็ก (Rack) หรือสถานที่ที่มีความมั่นคงปลอดภัยและมีการปิดล็อก
3. ผู้ดูแลระบบ ต้องมีการป้องกันสายเคเบิลที่ใช้เพื่อการสื่อสารหรือสายไฟ มิให้มีการดักจับสัญญาณ (Interception) หรือมีความเสียหายเกิดขึ้น โดยจะต้องเดินสายเคเบิลผ่านท่อร้อยสายหรือทางเดินสายที่มีความมั่นคงปลอดภัยจากการเข้าถึง และไม่เดินสายผ่านพื้นที่ที่เข้าถึงได้อย่างสาธารณะ รวมทั้งสายเคเบิลสื่อสารและสายไฟฟ้าต้องแยกจากกันโดยมีระยะห่างที่เหมาะสม
4. การกำหนดบริเวณที่มีการรักษาความมั่นคงปลอดภัย
กำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม เพื่อเป็นการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้ โดยแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศออกเป็น
 - 4.1 พื้นที่ทำงาน (Working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน
 - 4.2 พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) หมายถึง พื้นที่ศูนย์ของข้อมูล (Data center)
5. การควบคุมการเข้าออก อาคาร สถานที่
 - 5.1 กำหนดสิทธิของผู้ใช้งานและหน่วยงานภายนอกในการเข้าถึงสถานที่ โดยแบ่งแยกได้ ดังนี้
 - 5.1.1 ผู้ดูแลระบบต้องกำหนดสิทธิแก่ผู้ใช้งานที่มีสิทธิ์เข้า - ออก และกำหนดช่วงระยะเวลาที่มีสิทธิ์ในการเข้า - ออกแต่ละพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศอย่างชัดเจน
 - 5.1.2 เจ้าหน้าที่รักษาความปลอดภัย (รปภ.) จะต้องให้หน่วยงานภายนอกหรือบุคคลภายนอกแลกบัตรที่สามารถระบุตัวตนของบุคคลนั้น ๆ ก่อนเข้าถึงอาคารของ รพม. เช่น บัตรประจำตัวประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วบันทึกข้อมูลบัตรในสมุดบันทึกหรือระบบงานสารสนเทศ

- 5.1.3 หน่วยงานภายนอกที่มาติดต่อต้องติดบัตรผู้ติดต่อ (Visitor) ตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ใน รพม. และคืนบัตรผู้ติดต่อ (Visitor) ก่อนออกจากอาคารของ รพม.
- 5.1.4 เจ้าหน้าที่รักษาความปลอดภัย (รปภ.) ต้องตรวจสอบผู้ติดต่อ อุปกรณ์ พร้อมลงเวลาออกที่สมุดบันทึกหรือระบบสารสนเทศให้ถูกต้อง
- 5.2 ผู้ดูแลระบบ ต้องควบคุมการเข้า - ออกพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) ไม่ให้ผู้ไม่มีสิทธิ์เข้าถึงได้ โดยกำหนดพื้นที่การส่งมอบสินค้าและพื้นที่การเตรียมหรือประกอบอุปกรณ์สารสนเทศ (Unpack Area) ก่อนนำเข้าพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) และต้องควบคุมการเข้า - ออก เพื่อหลีกเลี่ยงการเข้าถึงระบบสารสนเทศและข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต โดยปฏิบัติตามขั้นตอนที่ รพม. กำหนด

ส่วนที่ 4 การจัดการทรัพย์สิน

วัตถุประสงค์

- เพื่อบริหารจัดการทรัพย์สินสารสนเทศ ตั้งแต่การจัดการหา การใช้งาน จนถึงการยกเลิกใช้งาน โดยมีการระบุสินทรัพย์ขององค์กรและกำหนดหน้าที่ความรับผิดชอบในการปกป้องทรัพย์สินสารสนเทศอย่างเหมาะสม

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- เจ้าของข้อมูล
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 4 การบริหารจัดการทรัพย์สิน (Asset management)

แนวปฏิบัติ

1. หน้าที่ความรับผิดชอบต่อทรัพย์สินสารสนเทศ (Responsibility for assets)
 - 1.1 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องร่วมกันจัดทำบัญชีทรัพย์สิน/ทะเบียนทรัพย์สิน (Asset inventory) และทบทวนทะเบียนทรัพย์สินอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ
 - 1.2 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องระบุเจ้าของทรัพย์สินสารสนเทศทุกรายการ เพื่อรับผิดชอบดูแลความมั่นคงปลอดภัยสารสนเทศตลอดวงจรอายุการใช้งาน
 - 1.3 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องเรียกคืนทรัพย์สินสารสนเทศเมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน
 - 1.4 ผู้ใช้งานต้องใช้ทรัพย์สินสารสนเทศของ รพม. อย่างระมัดระวัง และใช้เพื่อปฏิบัติงานของ รพม. เท่านั้น รวมทั้งต้องปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ และนโยบาย ของ รพม.
2. การจำแนกประเภทของทรัพย์สินสารสนเทศ (Asset classification)
 - 2.1 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจำแนกประเภททรัพย์สินตามขั้นตอนที่ รพม. กำหนด และทบทวนการจำแนกดังกล่าวอย่างสม่ำเสมอ
 - 2.2 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจัดทำป้ายชื่อทรัพย์สินสารสนเทศ (Labeling) ให้ชัดเจน พร้อมทั้งจัดให้มีมาตรการดูแลรักษาความมั่นคงปลอดภัยสารสนเทศที่สอดคล้องกับประเภททรัพย์สินตามระดับชั้นความลับที่ รพม. กำหนด
3. การจัดการสื่อบันทึกข้อมูล (Media handling)
 - 3.1 เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ใช้งานต้องควบคุมการใช้งานและจัดเก็บสื่อบันทึกแบบถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้ (Removable media) ตามที่ รพม. กำหนด
 - 3.2 เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล เพิ่มข้อมูลตามขั้นตอนที่ รพม. กำหนด โดยไม่สามารถกู้คืนข้อมูลกลับมาได้อีกก่อนจะกำจัดอุปกรณ์ดังกล่าวหรือ

ก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อเพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลที่สำคัญได้ โดยพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีทำลาย
กระดาษ	ให้หั่นด้วยเครื่องทำลายเอกสาร
Flash Drive	1) ทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD5220.22M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นการเขียนทับข้อมูลเดิมหลายรอบ 2) ใช้วิธีทุบหรือบดให้เสียหาย
แผ่น CD/DVD	ให้หั่นด้วยเครื่องทำลายเอกสาร
เทป	ใช้วิธีทุบหรือบดให้เสียหายหรือเผาทำลาย
ฮาร์ดดิสก์	1) ทำลายข้อมูลบนฮาร์ดดิสก์ตามมาตรฐาน DOD5220.22M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นการเขียนทับข้อมูลเดิมหลายรอบ 2) ใช้วิธีทุบหรือบดให้เสียหาย

- 3.3 เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ใช้งาน ต้องมีการป้องกันสื่อบันทึกข้อมูลที่ใช้จัดเก็บข้อมูลสารสนเทศ ในกรณีที่มีการเคลื่อนย้ายเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต ถูกนำไปใช้งานผิดวัตถุประสงค์ รวมถึงป้องกันสื่อบันทึกข้อมูลไม่ให้เกิดความเสียหาย โดยรักษาความปลอดภัยสารสนเทศตามขั้นตอนที่ รพม. กำหนด

ส่วนที่ 5

การจัดทำ การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

วัตถุประสงค์

- เพื่อควบคุมการจัดทำ พัฒนา และบำรุงรักษาระบบสารสนเทศ ให้มีการกำหนดมาตรการการรักษาความมั่นคงปลอดภัย เพื่อป้องกันความผิดพลาด สูญหาย และการเปลี่ยนแปลงแก้ไขระบบ

ผู้รับผิดชอบ

- ผู้บังคับบัญชา
- ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

- หมวดที่ 10 โครงสร้างการจัดทำ การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (System acquisition, development and maintenance)
- หมวดที่ 11 ความสัมพันธ์กับหน่วยงานภายนอก (Supplier relationships)

แนวปฏิบัติ

1. ผู้บังคับบัญชา ต้องควบคุมให้มีการกำหนดข้อตกลงและความรับผิดชอบที่เกี่ยวข้องกับความเสถียรด้านความมั่นคงปลอดภัยสารสนเทศลงในสัญญากับผู้ให้บริการภายนอก โดยให้ครอบคลุมรวมถึงผู้รับจ้างช่วงด้วย
2. ผู้บังคับบัญชาต้องควบคุมให้มีข้อตกลง (Sign off) ก่อนเริ่มใช้งานระบบจริง (Production) หรือก่อนเริ่ม Go live
3. ผู้ดูแลระบบ ต้องจัดทำข้อกำหนดโดยระบุถึงการควบคุมความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร เช่น วิธีการแบบปลอดภัยในการพัฒนาโปรแกรมตามมาตรฐาน OWASP (Open Web Application Security Project) Top 10 หรือมาตรฐาน CWE (Common Weakness Enumeration) Top 25 หรือมาตรฐานที่ยอมรับในสากล
4. ผู้ดูแลระบบ ต้องมีการออกแบบระบบเพื่อตรวจสอบข้อมูลที่จะรับเข้าสู่แอปพลิเคชัน ข้อมูลที่เกิดจากการประมวลผล และข้อมูลที่อยู่ระหว่างการประมวลผล เพื่อตรวจหาและป้องกันความไม่ถูกต้องที่เกิดขึ้นกับข้อมูล เช่น หน่วยความจำล้น (Buffer overflows) การใช้ตัวแปรผิดประเภท และต้องมีมาตรการป้องกันหรือควบคุมความล้มเหลวระหว่างการประมวลผล (Rollback)
5. ผู้ดูแลระบบต้องมีการควบคุมการเข้าถึงและควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบตามขั้นตอนที่ รพม. กำหนดเพื่อควบคุมผลกระทบที่เกิดขึ้น
6. ผู้ดูแลระบบต้องจำกัดให้มีการเปลี่ยนแปลงใด ๆ ต่อซอฟต์แวร์ที่ใช้งาน (Software package) โดยเปลี่ยนแปลงเฉพาะที่จำเป็นเท่านั้น และควบคุมทุก ๆ การเปลี่ยนแปลงอย่างเข้มงวดตามขั้นตอนที่ รพม. กำหนด
7. ผู้ดูแลระบบต้องจำกัดการเข้าถึง Source code ให้เข้าถึงได้เฉพาะผู้มีสิทธิ์เท่านั้น
8. ผู้ดูแลระบบต้องจัดทำ Source code review เพื่อหาข้อผิดพลาดหรือสิ่งผิดปกติและปรับปรุง Source code ให้มีคุณภาพ
9. ผู้ดูแลระบบต้องปิดบังข้อมูลส่วนบุคคล (Data Masking) ที่จัดเก็บอยู่ในระบบงานสารสนเทศด้วยวิธีการที่เหมาะสม

10. ผู้ดูแลระบบต้องแสดงข้อมูลของผู้ใช้งานอย่างรัดกุม เช่น การปิดบังข้อมูลสำคัญของผู้ใช้งาน (Sensitive data masking) เป็นต้น
11. กรณีของแอปพลิเคชันที่ใช้งานผ่านอุปกรณ์เคลื่อนที่ (Mobile device) ให้ผู้ดูแลระบบดำเนินการ ดังนี้
 - 11.1 ปิดบังหน้าจอเมื่อย่อแอปพลิเคชัน (Application blurring) เพื่อลดความเสี่ยงที่ข้อมูลสำคัญของผู้ใช้งานจะรั่วไหล
 - 11.2 ขอสสิทธิ์เข้าถึงทรัพยากรหรือบริการโดยแอปพลิเคชัน (Application permission) บนอุปกรณ์เคลื่อนที่ของผู้ใช้งานเท่าที่จำเป็น และมีกระบวนการทบทวนการขอสสิทธิ์เป็นประจำเพื่อป้องกันการละเมิดสิทธิ์ความเป็นส่วนตัวของผู้ใช้งาน
12. ผู้ดูแลระบบต้องควบคุมข้อมูลที่นำมาใช้ในการทดสอบระบบ (Test data) อย่างเหมาะสม โดยไม่นำข้อมูลจริงมาทดสอบ กรณีจำเป็นต้องใช้ข้อมูลจริงต้องได้รับอนุญาตข้อมูลจากเจ้าของก่อนนำมาใช้งาน และทำลายข้อมูลอย่างเหมาะสมตามขั้นตอนที่ รพม. กำหนด
13. ผู้ดูแลระบบต้องแยกระบบสารสนเทศสำหรับการพัฒนา ทดสอบ และใช้งานจริงออกจากกันเพื่อลดความเสี่ยงที่เกิดจากการเปลี่ยนแปลงระบบสารสนเทศโดยไม่ได้รับอนุญาต และต้องมีการกำหนดสิทธิ์การเข้าถึงระบบสารสนเทศที่พัฒนา ทดสอบ หรือใช้งานจริง ทั้งระบบสารสนเทศใหม่ และการปรับปรุงแก้ไขระบบสารสนเทศเดิม
14. ผู้ดูแลระบบต้องมีการกำหนดขั้นตอนการทดสอบระบบสารสนเทศก่อนนำไปใช้งานจริง ทั้งในกรณีปรับปรุงระบบสารสนเทศเดิมและการพัฒนาระบบสารสนเทศใหม่
15. ผู้ดูแลระบบต้องติดตั้งซอฟต์แวร์บนระบบสารสนเทศที่ให้บริการ (Production) ตามขั้นตอนที่ รพม. กำหนด และจำกัดสิทธิ์การติดตั้งซอฟต์แวร์เพื่อให้ระบบสารสนเทศต่าง ๆ มีความถูกต้องครบถ้วนและน่าเชื่อถือ
16. ผู้ดูแลระบบต้องนำซอฟต์แวร์ที่ไม่ละเมิดลิขสิทธิ์มาติดตั้งบนระบบสารสนเทศที่ให้บริการ (Production)
17. ผู้ดูแลระบบต้องกำกับดูแลให้ผู้รับจ้างปฏิบัติตามสัญญาหรือข้อตกลงการให้บริการที่ระบุไว้ โดยครอบคลุมถึงด้านความมั่นคงปลอดภัยสารสนเทศ และการปฏิบัติตามขั้นตอนที่เกี่ยวข้องต่าง ๆ ที่ รพม. กำหนดไว้
18. ผู้ดูแลระบบ ต้องติดตาม ตรวจสอบรายงาน หรือบันทึกการให้บริการของบุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามสัญญาว่าจ้างอย่างสม่ำเสมอ
19. ผู้ดูแลระบบ ต้องดูแลให้ทรัพย์สินสารสนเทศได้รับการบำรุงรักษาและซ่อมแซมตามความต้องการ รวมทั้งต้องมีการบันทึกประวัติการทำงานผิดปกติ การบำรุงรักษา และการซ่อมแซมอุปกรณ์นั้น ๆ อย่างสม่ำเสมอ
20. ผู้ดูแลระบบจะต้องปิดช่องโหว่ของระบบสารสนเทศที่มีระดับความรุนแรงในระดับวิกฤติ (Critical) และระดับความรุนแรงระดับสูง (High) ทั้งหมดก่อนนำไปใช้งานจริง (Production) หรือก่อนเริ่ม Go live โดยเฉพาะระบบที่ให้บริการผ่านเครือข่ายอินเทอร์เน็ต (Internet facing) และระบบที่มีความสำคัญต่อการดำเนินงานของ รพม.
21. ผู้ดูแลระบบต้องพิจารณาเลือกใช้ Version ของ Software ดังนี้
 - 21.1 กรณีนำ Software เดิมมาใช้ในการจัดหาหรือพัฒนาระบบ จะต้องนำผลการตรวจสอบช่องโหว่และผลการทดสอบเจาะระบบมาประกอบการพิจารณาคัดเลือกเวอร์ชันของ Software ด้วย เพื่อป้องกันไม่ให้เกิดช่องโหว่เดิมรวมถึงเพื่อลดภาระงานในการปิดช่องโหว่เดิมซ้ำ
 - 21.2 กรณีเป็น Software ที่ไม่เคยนำมาใช้งานให้เลือกใช้ Software เวอร์ชันล่าสุด

ส่วนที่ 6

การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

- เพื่อควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศตั้งแต่การกำหนดสิทธิ์ กำหนดประเภทของข้อมูล จัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ระดับชั้นการเข้าถึง เวลาที่เข้าถึงได้ และช่องทางการเข้าถึง ทั้งนี้เพื่อควบคุมและป้องกันการเข้าถึง การลวงรู้ และการแก้ไขระบบสารสนเทศของ รพม. โดยไม่ได้รับอนุญาต

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- เจ้าของข้อมูล
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 5 การควบคุมการเข้าถึง (Access control)
- หมวดที่ 8 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations security)
- หมวดที่ 9 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)

แนวปฏิบัติ

1. การควบคุมการเข้าถึงระบบสารสนเทศ (Access control)
 - 1.1 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องร่วมกันกำหนดสิทธิ์ในการเข้าถึงระบบสารสนเทศ (Authorization matrix) ที่เหมาะสมและสอดคล้องกับหน้าที่ความรับผิดชอบของผู้ใช้งาน และทบทวนเมื่อมีการเปลี่ยนแปลง
 - 1.2 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องร่วมกันกำหนดระดับการอนุมัติ (Authorization level) การเข้าถึงระบบเทคโนโลยีสารสนเทศ
 - 1.3 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจัดให้มีการแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties) ในการเข้าถึงระบบเทคโนโลยีสารสนเทศอย่างเหมาะสม เช่น มีการแบ่งแยกหน้าที่ระหว่างการแจ้งความประสงค์ การเข้าถึงและการอนุมัติการเข้าถึง เป็นต้น
 - 1.4 กรณีของแอปพลิเคชันที่ใช้งานผ่านอุปกรณ์เคลื่อนที่ (Mobile device) ผู้ดูแลระบบต้องปฏิบัติ ดังนี้
 - 1.4.1 ไม่อนุญาตให้อุปกรณ์เคลื่อนที่ที่ใช้ระบบปฏิบัติการล้าสมัย (Obsolete operating system) ใช้งานแอปพลิเคชัน หรือหากอนุญาตให้ใช้บริการได้ควรมีมาตรการรองรับเพื่อลดความเสี่ยงที่ รพม. จะได้รับรวมถึงลดผลกระทบต่อผู้ใช้งานตามความเหมาะสม เช่น การเพิ่มมาตรการยืนยันตัวตน เป็นต้น
 - 1.4.2 ไม่อนุญาตให้อุปกรณ์ที่มีการปรับแต่งการเข้าถึงระบบปฏิบัติการ (rooted/jailbroken) ใช้งานแอปพลิเคชัน เพื่อลดความเสี่ยงที่ผู้ไม่ประสงค์ดีสามารถเข้าถึงข้อมูลสำคัญของผู้ใช้งานและละเมิดหรือหลีกเลี่ยงมาตรการการรักษาความมั่นคงปลอดภัยที่ รพม. กำหนดไว้
 - 1.4.3 ไม่อนุญาตให้ผู้ใช้งานใช้แอปพลิเคชันเวอร์ชันต่ำกว่าที่ รพม. กำหนด เพื่อให้แอปพลิเคชันมีการรักษาความมั่นคงปลอดภัยเป็นไปตามมาตรฐานของ รพม.

1.5 ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ใช้งาน ต้องปฏิบัติ ดังนี้

1.5.1 แบ่งประเภทข้อมูล ดังนี้

- 1) ข้อมูลและสารสนเทศสำหรับสนับสนุนการตัดสินใจของผู้บริหาร ได้แก่ ข้อมูลสารสนเทศที่มีความสำคัญหรือมีความจำเป็นเร่งด่วนที่ต้องติดตามอย่างใกล้ชิดเพื่อประกอบการตัดสินใจเชิงนโยบาย กำหนดนโยบาย และการวางแผนของผู้บริหารระดับสูง
- 2) ข้อมูลและสารสนเทศสนับสนุนเชิงยุทธศาสตร์ (Strategy data) ได้แก่ ข้อมูลและสารสนเทศเชิงวิชาการเพื่อสนับสนุนการดำเนินงานตามพันธกิจและยุทธศาสตร์ของ รพม. ให้บรรลุเป้าหมาย รวมทั้งข้อมูลที่เผยแพร่แก่ผู้รับบริการภายนอก
- 3) ข้อมูลและสารสนเทศที่สนับสนุนการปฏิบัติงานประจำ (Operation data) ได้แก่ ข้อมูลที่สนับสนุนการทำงานทั่วไปของ รพม.

1.5.2 จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น 3 ระดับ คือ

- 1) ข้อมูลที่มีระดับความสำคัญมาก หมายถึง ข้อมูลที่ใช้สำหรับสนับสนุนการตัดสินใจของผู้บริหาร
- 2) ข้อมูลที่มีระดับความสำคัญปานกลาง หมายถึง ข้อมูลที่ใช้ปฏิบัติงานเฉพาะกลุ่มงาน แผนก กอง หรือฝ่ายภายในองค์กร
- 3) ข้อมูลที่มีระดับความสำคัญน้อย หมายถึง ข้อมูลที่พนักงาน/ลูกจ้างภายใน รพม. สามารถเข้าถึงร่วมกันได้หรือสามารถเผยแพร่ได้

1.5.3 จัดแบ่งลำดับชั้นความลับของข้อมูลตามที่ รพม. กำหนด

1.5.4 จัดแบ่งระดับชั้นการเข้าถึง

- 1) ระดับชั้นสำหรับผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และภารกิจที่ได้รับมอบหมาย
- 2) ระดับชั้นสำหรับผู้ปฏิบัติงานทั่วไป เข้าถึงข้อมูลที่ได้รับมอบหมายตามอำนาจหน้าที่
- 3) ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย มีสิทธิ์ในการบริหารจัดการระบบและเข้าถึงข้อมูลที่ได้รับมอบหมายตามอำนาจหน้าที่

1.6 เจ้าของข้อมูลและผู้ดูแลระบบต้องกำหนดเวลาการเข้าถึงระบบสารสนเทศ

1.7 ผู้ดูแลระบบต้องจำกัดช่องทางการเข้าถึงระบบเทคโนโลยีสารสนเทศตามช่องทาง ดังนี้

- 1) เครือข่ายภายในของ รพม.
- 2) เครือข่ายภายนอก รพม.
- 3) เครือข่ายอื่นที่จัดไว้ให้ เช่น ระบบเครือข่ายสื่อสารข้อมูล GIN

1.7 ผู้ดูแลระบบต้องกำกับดูแล Default permission ของไฟล์ (File) และ โฟลเดอร์ (Folder) ที่สร้างขึ้นให้มีการจำกัดสิทธิ์ในการเข้าถึง

1.8 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องพิจารณาข้อกำหนดต่าง ๆ ที่มีผลทางกฎหมายซึ่งเกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศของ รพม. เช่น พระราชบัญญัติ ข้อกำหนดทางกฎหมาย ข้อกำหนดในสัญญา

และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่น ๆ เป็นต้น เพื่อกำหนดสิทธิ์การเข้าถึงสารสนเทศและระบบเทคโนโลยีสารสนเทศของ รพม.

- 1.9 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องมีการสอบทานสิทธิ์ในการเข้าถึงระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ พร้อมทั้งเพิกถอนสิทธิ์เมื่อพบเห็นสิทธิ์ที่ไม่ถูกต้องตามสิทธิ์ในการเข้าถึง (Authorization matrix)
2. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)
ให้มีการควบคุมการลงทะเบียนผู้ใช้งาน การบริหารจัดการรหัสผ่าน การบริหารจัดการสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศ และการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน
 - 2.1 การลงทะเบียนผู้ใช้งาน (User registration)
 - 2.1.1 ผู้ดูแลระบบต้องบริหารจัดการและควบคุมบัญชีชื่อผู้ใช้งาน (Username) มิให้มีการใช้งานบัญชีชื่อผู้ใช้งานซ้ำกัน ทั้งนี้ ในส่วนของพนักงาน/ลูกจ้าง รพม. ให้กำหนดชื่อผู้ใช้งาน (Username) ตามมาตรฐานจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ใช้ในองค์กร
 - 2.1.2 เจ้าของข้อมูลต้องเป็นผู้อนุมัติการสร้างบัญชีผู้ใช้งานชั่วคราว (Temporary user) และต้องจำกัดช่วงเวลาการใช้งานเท่าที่จำเป็น
 - 2.2 การบริหารจัดการรหัสผ่าน (User password management)
 - 2.2.1 ผู้ดูแลระบบและผู้รับจ้าง ต้องกำหนดความยาวรหัสผ่านอย่างน้อย 12 หลัก
 - 2.2.2 บุคลากรของ รพม. (พนักงาน/ลูกจ้างของ รพม.) ต้องกำหนดความยาวรหัสผ่านอย่างน้อย 8 หลัก
 - 2.2.3 ผู้ดูแลระบบกำหนดรหัสผ่านแบบชั่วคราวโดยใช้วิธีการสุ่ม และบังคับให้มีการเปลี่ยนรหัสผ่านเมื่อผู้ใช้งานเข้าใช้งานระบบในครั้งแรก (บังคับใช้เฉพาะกรณีข้อ 2.2.1 – 2.2.2)
 - 2.2.4 ผู้ดูแลระบบและผู้รับจ้าง รวมถึงบุคลากรของ รพม. (พนักงาน/ลูกจ้างของ รพม.) ตามข้อ 2.2.1 – 2.2.2 ต้องปฏิบัติเพิ่มเติม ดังนี้
 - 1) รหัสผ่านประกอบด้วย ตัวอักษร ตัวเลข และอักขระพิเศษ เช่น (a-Z) (0-9) (@ , # , & , “ , ‘ , * , = , < , > , % , \$, + , ?) เป็นต้น
 - 2) กำหนดรหัสผ่านที่ง่ายต่อการจดจำ แต่ต้องไม่เป็นคำที่สามารถคาดเดาได้ง่าย เช่น คำที่อยู่ในพจนานุกรม “qwerty” “abcde” “12345” ชื่อ-นามสกุล วันเดือนปีเกิด ที่อยู่ หรือเบอร์โทรศัพท์ เป็นต้น
 - 3) ต้องไม่ใช้งานรหัสผ่านโดยกระบวนการเข้าใช้งานโดยอัตโนมัติ ได้แก่ การกำหนดค่า “Remember Password” เป็นต้น
 - 4) ต้องเก็บรหัสผ่านไว้เป็นความลับเฉพาะบุคคล ไม่เปิดเผยให้ผู้อื่นรับทราบ และไม่พิมพ์รหัสผ่านในลักษณะเปิดเผย เช่น พิมพ์รหัสผ่านต่อหน้าผู้ใช้งานคนอื่น เป็นต้น
 - 5) ต้องไม่ใช้บัญชีชื่อผู้ใช้งานและรหัสผ่านร่วมกันกับผู้อื่น แม้ว่าบัญชีชื่อผู้ใช้งานจะได้รับการอนุญาตจากเจ้าของชื่อผู้ใช้งานบุคคลนั้นก็ตาม
 - 6) ต้องเปลี่ยนแปลงรหัสผ่านเป็นประจำอย่างน้อยทุก 6 เดือน
 - 7) ต้องเปลี่ยนแปลงรหัสผ่านเมื่อมีการแจ้งเตือนจากระบบ หรือสงสัยว่ารหัสผ่านลวงรู้โดยบุคคลอื่น
 - 2.2.5 ผู้ดูแลระบบ ต้องกำหนดให้มีการเข้ารหัสข้อมูลรหัสผ่านในระบบ
 - 2.2.6 ผู้ดูแลระบบ ต้องจัดให้มีการควบคุมรหัสผ่านอย่างเข้มงวด

- 2.2.7 ผู้ดูแลระบบต้องจัดส่งบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ด้วยวิธีการที่ปลอดภัย
- 2.2.8 ผู้ดูแลระบบต้องควบคุมดูแลระบบปฏิบัติการ ฐานข้อมูล และระบบงานสารสนเทศ (Application) ที่จัดเก็บบัญชีผู้ใช้งานและรหัสผ่านอย่างเข้มงวด โดยให้เข้าถึงได้เฉพาะผู้ดูแลระบบที่ได้รับอนุญาตเท่านั้น
- 2.2.9 ผู้ดูแลระบบต้องกำหนดวิธีการหรือกระบวนการยืนยันตัวตนที่ปลอดภัย เช่น กรณีที่ลืมรหัสผ่าน
- 2.2.10 ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานภายนอกที่สมัครใช้บริการระบบงานสารสนเทศของ รพม. ใช้รหัสผ่านอย่างมั่นคงปลอดภัย ดังนี้

กรณีแอปพลิเคชันทั่วไป

- 1) กำหนดความยาวรหัสผ่านอย่างน้อย 8 หลัก ซึ่งประกอบด้วย ตัวอักษร ตัวเลข และอักขระพิเศษ เช่น (a-Z) (0-9) (@, #, &, “, ‘, *, =, <, >, %, \$, +, ?) เป็นต้น
- 2) ไม่บังคับให้เปลี่ยนรหัสผ่าน ทั้งนี้ขึ้นอยู่กับความสมัครใจในการเปลี่ยนรหัสผ่าน และระบบต้องรองรับการเปลี่ยนรหัสผ่านในกรณีต่าง ๆ ด้วยวิธีการที่ปลอดภัย

กรณีแอปพลิเคชันที่ใช้งานผ่านอุปกรณ์เคลื่อนที่ (Mobile device)

- 1) กำหนดรหัสผ่านโดยใช้ PIN code หรือรหัสผ่านที่ซับซ้อน (PIN/Password complexity) โดยกรณี PIN code ต้องใช้รหัสผ่าน 6 หลักขึ้นไป
- 2) ไม่บังคับให้เปลี่ยนรหัสผ่าน ทั้งนี้ขึ้นอยู่กับความสมัครใจในการเปลี่ยนรหัสผ่าน และระบบต้องรองรับการเปลี่ยนรหัสผ่านในกรณีต่าง ๆ ด้วยวิธีการที่ปลอดภัย

2.3 การบริหารจัดการสิทธิ์ (Privilege management)

- 2.3.1 ผู้บังคับบัญชาต้องกำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียน การเพิกถอนสิทธิ์ การเปลี่ยนแปลงสิทธิ์ และการทบทวนสิทธิ์ของผู้ใช้งานอย่างเป็นลายลักษณ์อักษร
- 2.3.2 กำหนดสิทธิ์ที่เหมาะสมกับผู้ใช้งานตามความจำเป็นและสอดคล้องกับหน้าที่ความรับผิดชอบและจัดเก็บประวัติ (Log) การลงทะเบียน การเพิกถอนสิทธิ์ และการเปลี่ยนแปลงสิทธิ์ของผู้ใช้งาน
- 2.3.3 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจัดให้มีการควบคุมและจำกัดสิทธิ์ในการทำงานระบบตามความจำเป็นในการใช้งานเท่านั้น
 - 1) สิทธิ์ในการสร้างข้อมูล (Create)
 - 2) สิทธิ์ในการอ่านข้อมูลหรือเรียกดูข้อมูล (READ)
 - 3) สิทธิ์ในการปรับปรุงข้อมูล (Modify / Update)
 - 4) สิทธิ์ในการลบข้อมูล (Delete)
 - 5) สิทธิ์ในการมอบหมายสิทธิ์ในการดำเนินการแทน (Assign)
 - 6) สิทธิ์ในการรับรองความถูกต้องครบถ้วนของข้อมูล (Approve/Authenticate)
 - 7) ไม่มีสิทธิ์
- 2.3.4 เจ้าของข้อมูลและผู้ดูแลระบบต้องเป็นผู้อนุมัติการให้สิทธิ์เพื่อเข้าถึงสารสนเทศหรือระบบเทคโนโลยีสารสนเทศใด ๆ อย่างเป็นลายลักษณ์อักษร

- 2.3.5 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจำกัดจำนวนผู้ใช้งานที่ทำหน้าที่เป็นผู้ให้สิทธิ์กับผู้ใช้งาน ให้น้อยที่สุดตามความเหมาะสม
- 2.3.6 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจำกัดระยะเวลาการใช้งานระบบเทคโนโลยีสารสนเทศของ รพม. แก่หน่วยงานภายนอกที่เข้ามาปฏิบัติงานร่วมกับ รพม.
- 2.3.7 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจัดให้มีการถอดถอนหรือเปลี่ยนแปลงสิทธิ์การเข้าถึงทันที เมื่อผู้ใช้งานเกษียณ เปลี่ยนแปลงหน้าที่ความรับผิดชอบ เปลี่ยนแปลงการจ้างงาน หรือไม่มีความจำเป็น ในการใช้งานระบบเทคโนโลยีสารสนเทศ
- 2.3.8 ผู้ดูแลระบบต้องลบหรือระงับการใช้งานสิทธิ์ของผู้ใช้งานที่มากับระบบ (Default user) ในกรณีที่มีความจำเป็นต้องใช้งานต้องกำหนดรหัสผ่านอย่างมั่นคงปลอดภัย
- 2.4 การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of user access rights)
 - 2.4.1 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องมีการสอบทานสิทธิ์การเข้าถึงของผู้ใช้งานระบบ เมื่อ รพม. มีการเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศหรือโครงสร้างองค์กร
 - 2.4.2 ผู้ดูแลระบบ ต้องมีการสอบทานและระงับการใช้งานบัญชีผู้ใช้งานที่ไม่ได้ใช้งานเกิน 180 วัน หากผู้ใช้งานต้องการกลับมาใช้งานจะต้องยืนยันตัวตนให้ ผทท. ทราบ ทั้งนี้ ระยะเวลาที่ไม่ได้ใช้งานของ บัญชีผู้ใช้งานอาจจะขึ้นอยู่กับแต่ละระบบสารสนเทศ
3. การป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล และการควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ไม่ปลอดภัย
 - 3.1 การป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล (Unattended user equipment)
 - 3.1.1 ผู้ดูแลระบบต้องจัดให้มีมาตรการสำหรับป้องกันระบบคอมพิวเตอร์ ระบบเครือข่ายสื่อสาร ข้อมูล และระบบเทคโนโลยีสารสนเทศ โดยการกำหนดค่าของระบบ (Configuration) ให้มีการล็อกหน้าจอสำหรับอุปกรณ์ที่ไม่มีพนักงานดูแล หรือล็อกอุปกรณ์อยู่เสมอ
 - 3.1.2 ผู้ใช้งานและหน่วยงานภายนอก ต้องล็อกหน้าจออัตโนมัติเมื่อไม่มีการใช้งานระบบเทคโนโลยีสารสนเทศของ รพม. ตามระยะเวลาที่กำหนด โดยต้องพักหน้าจอ (Screen saver) อัตโนมัติ หลังจากที่ไม่มีการใช้งานคอมพิวเตอร์เป็นระยะเวลานานกว่า 15 นาที ผู้ใช้งานและหน่วยงานภายนอก จะใช้งานต่อได้เมื่อมีการใส่รหัสผ่านที่ถูกต้อง
 - 3.1.3 ผู้ใช้งานต้อง Log out ออกจากเครื่องคอมพิวเตอร์เมื่อมีความจำเป็นต้องละทิ้งเครื่องคอมพิวเตอร์
 - 3.1.4 ผู้ใช้งานต้องป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ เช่น กล้องดิจิทัล เครื่องสำเนาเอกสาร เครื่องสแกน เอกสารโดยไม่ได้รับอนุญาต
 - 3.2 การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear desk and clear screen control)
 - 3.2.1 ผู้บังคับบัญชาต้องกำหนดให้มีผู้รับผิดชอบในการดูแลสถานที่ที่มีการรับ - ส่งแฟกซ์ หรือจดหมายเข้า - ออก
 - 3.2.2 ผู้ใช้งานต้องออกจากระบบคอมพิวเตอร์ (Log out) ทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
 - 3.2.3 ผู้ใช้งานต้องจัดเก็บข้อมูลสำคัญแยกต่างหาก และป้องกันให้มีความปลอดภัยอย่างพอเพียง
 - 3.2.4 ผู้ใช้งานต้องนำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

4. การควบคุมการเข้าถึงเครือข่าย (Network access control)
ให้มีการควบคุมการใช้งานบริการเครือข่าย การควบคุมการพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอก รพม. การควบคุมการพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย การป้องกันพอร์ต (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ การแบ่งแยกเครือข่าย (Segregation in networks) อย่างเหมาะสม การควบคุมการเชื่อมต่อทางเครือข่าย และการควบคุมการกำหนดเส้นทางบนเครือข่าย
- 4.1 การใช้งานบริการเครือข่าย (Use of network services)
 - 4.1.1 ผู้ดูแลระบบต้องควบคุมการเผยแพร่แผนผังระบบเครือข่ายสื่อสารข้อมูล (Network diagram) รวมถึงโครงสร้าง IP address ของระบบ และชื่ออุปกรณ์สารสนเทศแก่ผู้ที่ไม่ได้รับอนุญาตหรือหน่วยงานภายนอก
 - 4.1.2 ผู้ดูแลระบบต้องควบคุมการใช้งานระบบเครือข่ายสื่อสารข้อมูล เพื่อป้องกันการเข้าถึงระบบเครือข่ายสื่อสารข้อมูลและบริการของระบบเครือข่ายสื่อสารข้อมูลโดยไม่ได้รับอนุญาต
 - 4.1.3 ผู้ดูแลระบบต้องควบคุมการเชื่อมต่อเครือข่ายภายนอก เพื่อใช้งานอินเทอร์เน็ต ซึ่งอาจเป็นช่องทางให้หน่วยงานภายนอกเข้าถึงสารสนเทศหรือระบบเทคโนโลยีสารสนเทศของ รพม. โดยมิได้รับอนุญาต
 - 4.1.4 ผู้ใช้งานต้องแจ้งความประสงค์ในการขอใช้งานบริการเครือข่ายแก่ ผทท. และสามารถใช้บริการเครือข่ายได้หลังจากได้รับการอนุมัติจาก ผทท. แล้ว
 - 4.1.5 ผู้ใช้งาน ต้องไม่ใช้ระบบเครือข่ายสื่อสารข้อมูลเพื่อเป็นช่องทางในการเจาะระบบ (Hacking) หรือการสแกนช่องโหว่ของระบบโดยมิได้รับอนุญาต
- 4.2 การพิสูจน์ตัวตนของผู้ใช้งานที่อยู่ภายนอก รพม. (User authentication for external connections)
ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนผ่านระบบ Active directory ของ รพม. ก่อนอนุญาตให้ผู้ใช้งานที่อยู่ภายนอก รพม. เข้าใช้งานเครือข่ายและระบบสารสนเทศของ รพม.
- 4.3 การพิสูจน์ตัวตนของอุปกรณ์ในระบบเครือข่ายสื่อสารข้อมูล (Equipment identification in networks)
ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนของอุปกรณ์ในระบบเครือข่ายสื่อสารข้อมูล ได้แก่ การตรวจสอบ MAC address
- 4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection)
ผู้ดูแลระบบต้องระงับบริการและพอร์ต (Port) ที่ไม่มีความจำเป็นต้องใช้บนเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่าย
- 4.5 ผู้ดูแลระบบต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion prevention system/ intrusion detection system) ของระบบเครือข่าย
- 4.6 การแบ่งแยกเครือข่าย (Segregation in networks)
 - 4.6.1 ผู้ดูแลระบบต้องจัดให้มีการแบ่งแยกเครือข่ายตามกลุ่มของผู้ใช้งาน หรือกลุ่มของระบบเทคโนโลยีสารสนเทศ เพื่อควบคุมการใช้งานในแต่ละเครือข่ายย่อยอย่างเหมาะสม โดยพิจารณา

จากความต้องการในการเข้าถึงข้อมูล ระดับความสำคัญของข้อมูล รวมถึงการพิจารณาด้านราคา ประสิทธิภาพ และผลกระทบทางด้านความปลอดภัยดังต่อไปนี้

- 1) เครือข่ายที่อนุญาตให้เข้าถึงจากภายนอกและเครือข่ายที่ใช้ภายใน รพม.
- 2) เครือข่ายแอปพลิเคชัน (Application) ที่มีความสำคัญกับเครือข่ายอื่น ๆ ที่มีความสำคัญน้อยกว่า
- 3) เครือข่ายสำหรับเครื่องให้บริการ (Server farm) กับเครือข่ายของผู้ใช้งาน ควรมีการติดตั้งอุปกรณ์ที่สามารถแบ่งแยกเครือข่ายได้ เช่น Firewall หรือ Switch ที่สามารถแบ่ง VLAN ได้ เป็นต้น

4.6.2 ผู้ดูแลระบบจะกำหนดเส้นทางบนเครือข่ายที่เข้มงวด เพื่อจำกัดการเข้าถึงระยะไกลไปเฉพาะเครือข่ายที่กำหนดเท่านั้น

4.6.3 ผู้ดูแลระบบต้องตั้งค่า (Configuration) อุปกรณ์เครือข่าย เช่น Firewall หรือ Router มิให้สามารถบริหารจัดการจากภายนอกเครือข่ายได้ เว้นแต่ในกรณีฉุกเฉินซึ่งต้องได้รับการอนุญาตจากผู้ดูแลระบบเท่านั้น

4.7 การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control)

4.7.1 ผู้ดูแลระบบต้องจำกัดการใช้งานเครือข่ายของผู้ใช้งานในการเชื่อมต่อกับเครือข่ายของ รพม. เช่น Router หรือ Firewall เป็นต้น พร้อมทั้งติดตั้งระบบควบคุมเพื่อกลั่นกรองข้อมูลที่รับ - ส่ง เช่น Web filtering, E-mail filtering เป็นต้น เพื่อให้การเชื่อมต่อมีความปลอดภัย

4.7.2 ผู้ดูแลระบบต้องติดตั้ง Firewall ระหว่างเครือข่ายของ รพม. กับเครือข่ายภายนอก ทั้งนี้ การติดตั้ง Firewall ต้องพิจารณาเรื่องดังต่อไปนี้

- 1) การป้องกันการจราจรจากภายนอก ต้องถูกกำหนดให้ใช้เส้นทางที่ผ่าน First tier firewall ที่มีความมั่นคงปลอดภัยเพื่อป้องกันการรั่วซึมสารสนเทศของ รพม. และโครงสร้างพื้นฐานที่มีความสำคัญจากการเข้าถึงที่ไม่ได้รับอนุญาต
- 2) Firewall ต้องระบุตัวตนและพิสูจน์ตัวตนของผู้ใช้งานก่อนที่จะให้สิทธิ์การเข้าถึงอินเทอร์เน็ตเฟส (Interface) เพื่อการบริหารจัดการ Firewall
- 3) Firewall ต้องตั้งค่าให้ระงับบัญชีผู้ใช้งานหลังจากมีความพยายามที่จะเข้าสู่ระบบไม่สำเร็จ 5 ครั้ง การยกเลิกการระงับต้องดำเนินการโดย ฝพท.
- 4) ไม่อนุญาตให้พิสูจน์ตัวตนผ่านทางอินเทอร์เน็ตเฟส (Interface) การจัดการ Firewall จากระยะไกล (Remote)
- 5) ผู้ที่ได้รับการมอบหมายจาก ฝพท. เท่านั้นที่มีสิทธิ์ที่จะเปลี่ยนการตั้งค่าด้านความปลอดภัยบน Firewall
- 6) Firewall ต้องตั้งค่าให้บันทึกเหตุการณ์ด้านความมั่นคงปลอดภัย
- 7) Firewall ต้องได้รับการสอบทาน ทดสอบ และตรวจสอบอย่างสม่ำเสมอ
- 8) Firewall ต้องถูกบริหารจัดการผ่านทาง การติดต่อสื่อสารที่มีการเข้ารหัส
- 9) ต้องปิดบริการและพอร์ต (Port) ที่ไม่จำเป็นต้องใช้บน Firewall
- 10) Firewall ประเภทซอฟต์แวร์ (Software) ต้องติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายแยกต่างหาก

- 11) Firewall ต้องสามารถป้องกันตัวเองจากการโจมตี DOS (Denial of service) ได้อย่างเช่น Ping, Sweeps หรือ TCP SYN Floods เป็นต้น
- 12) ต้องใช้เวอร์ชันของซอฟต์แวร์ (Software) Firewall และระบบปฏิบัติการที่เจ้าของผลิตภัณฑ์ยังให้การสนับสนุน
- 13) ผู้ดูแล Firewall ต้องติดตามข้อมูลช่องโหว่จากผู้ให้บริการ (Vendor) เพื่อรับทราบข่าวสารการ Upgrade และแพตช์ (Patch) ที่จำเป็น และต้องติดตั้งแพตช์ (Patch) ทั้งหมดที่เกี่ยวข้อง

4.7.3 ผู้ดูแลระบบต้องติดตั้ง Firewall เพื่อแบ่งแยก Zone ให้มีการใช้ DMZ (Demilitarized zone) โดยต้องพิจารณาเรื่องดังต่อไปนี้

- 1) เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการผ่านอินเทอร์เน็ต เช่น FTP, Email, Web และ External DNS server เป็นต้น ต้องติดตั้งอยู่ใน DMZ
- 2) การเข้าถึงจากระยะไกลต้องพิสูจน์ตัวตนที่ Firewall หรือผ่านบริการที่อยู่ใน DMZ
- 3) DNS Servers ต้องไม่อนุญาตให้มีการแลกเปลี่ยนโซน (Zone transfers) เว้นแต่มีเหตุจำเป็น

4.8 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control)

ผู้ดูแลระบบต้องควบคุมการกำหนดเส้นทางบนเครือข่ายเพื่อให้มั่นใจว่าการเชื่อมต่อเครื่องคอมพิวเตอร์และการไหลเวียนของสารสนเทศบนเครือข่าย โดยมีกลไกในการตรวจสอบที่อยู่ปลายทางและต้นทางของการเชื่อมต่อ เช่น การควบคุมโดย Firewall หรือ Proxy เป็นต้น

5. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)

ให้มีการควบคุมการเข้าถึงระบบปฏิบัติการอย่างมั่นคงปลอดภัย การควบคุมการระบุและพิสูจน์ตัวตนของผู้ใช้งาน การควบคุมระบบบริหารจัดการรหัสผ่าน การควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ (System utilities) การควบคุมการหมดเวลาการใช้งานระบบเทคโนโลยีสารสนเทศ และควบคุมการจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ

5.1 ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on procedures)

5.1.1 ผู้ดูแลระบบ ต้องจัดให้มีการควบคุมการเข้าถึงระบบปฏิบัติการอย่างมั่นคงปลอดภัยโดยขั้นตอนการเข้าสู่ระบบต้องเปิดเผยข้อมูลเกี่ยวกับระบบให้น้อยที่สุดเพื่อหลีกเลี่ยงผู้ใช้งานที่ไม่ได้รับอนุญาต ซึ่งขั้นตอนการ Log-on ต้องพิจารณา ดังนี้

- 1) หากกระบวนการเข้าสู่ระบบไม่สำเร็จ ระบบต้องไม่แสดงข้อมูลของระบบหรือแอปพลิเคชัน (Application) ที่ใช้งานอยู่
- 2) ระบบต้องแสดงข้อความเตือนผู้ใช้งานว่าสามารถเข้าใช้งานเครื่องคอมพิวเตอร์ได้เฉพาะผู้ที่มีสิทธิ์เท่านั้น
- 3) หากกระบวนการเข้าสู่ระบบไม่สำเร็จ ระบบต้องไม่แสดงข้อมูลที่สามารถระบุตัวตนของระบบ เช่น เครือข่ายที่ใช้งาน สถานที่ตั้งของระบบ หรือชื่อเครื่องคอมพิวเตอร์แม่ข่าย เป็นต้น
- 4) ระบบต้องไม่แสดงข้อความที่ชี้เฉพาะเหตุของการเข้าสู่ระบบไม่สำเร็จ เช่น ไม่แสดงข้อความว่า บัญชีผู้ใช้งานผิด หรือ รหัสผ่านผิด เป็นต้น
- 5) ห้ามเข้าสู่ระบบจากบัญชีผู้ใช้งานส่วนบุคคลเดียวกันมากกว่าหนึ่ง Session ในระบบเดียวกัน

- 6) ระบบต้องจำกัดจำนวนครั้งในการพยายามเข้าสู่ระบบที่ไม่สำเร็จ และต้องพิจารณาเงื่อนไขต่อไปนี้
 - (ก) การเก็บบันทึกผลการเข้าสู่ระบบทั้งที่สำเร็จและไม่สำเร็จ
 - (ข) หน่วงระยะเวลาในการเข้าใช้งานระบบครั้งต่อไป
 - (ค) การตัดการเชื่อมต่อ
 - (ง) การแสดงข้อความเตือนที่หน้าจอของผู้ดูแลระบบเมื่อมีการเข้าสู่ระบบเกินจำนวนครั้งที่จำกัดไว้
 - 7) ระบบต้องแสดงวัน เวลา ในการเข้าสู่ระบบที่สำเร็จในครั้งก่อน พร้อมทั้งบันทึกจำนวนครั้งที่พยายามเข้าไม่สำเร็จนับแต่การเข้าสู่ระบบที่สำเร็จในครั้งก่อนของผู้ใช้งาน
 - 8) ระบบต้องไม่ส่งรหัสผ่านแบบ Clear text ผ่านระบบเครือข่ายสื่อสารข้อมูล
 - 9) ผู้ดูแลระบบต้องกำหนดจำนวนครั้งที่ยอมให้ใส่รหัสผ่านผิดได้ไม่เกิน 5 ครั้ง
- 5.2 การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication)
ผู้ดูแลระบบ ต้องจัดให้ผู้ใช้งานมีบัญชีผู้ใช้งานของแต่ละบุคคลเพื่อใช้พิสูจน์ตัวตนในการเข้าถึงระบบเทคโนโลยีสารสนเทศ และต้องใช้ระบบเทคโนโลยีสารสนเทศพิสูจน์ตัวตนผู้ใช้งานในการเข้าถึงระบบปฏิบัติการ โดยผ่านระบบ Active directory หรือ Lightweight Directory Access Protocol (LDAP) ทุกครั้ง พร้อมทั้งบันทึกข้อมูลการเข้าถึง
- 5.3 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities)
ผู้ดูแลระบบ ต้องควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้บนระบบที่ใช้งานจริง (Production system) ดังนี้
- 5.3.1 ต้องจัดทำบัญชีโปรแกรมประเภทยูทิลิตี้ (System utilities) ที่นำมาใช้งาน
 - 5.3.2 กำหนดความรับผิดชอบในการใช้โปรแกรมประเภทยูทิลิตี้ (System utilities) แต่ละรายการอย่างชัดเจนและสื่อสารให้ผู้เกี่ยวข้องทราบเพื่อถือปฏิบัติ
 - 5.3.3 ให้มีการพิสูจน์ตัวตน และกำหนดสิทธิ์ในการใช้งานโปรแกรมประเภทยูทิลิตี้เฉพาะกลุ่มคนที่มีหน้าที่รับผิดชอบ
 - 5.3.4 มีการบันทึกเหตุการณ์ (Log) การใช้งานโปรแกรมประเภทยูทิลิตี้ และต้องสอบทานจากผู้ดูแลระบบอย่างสม่ำเสมอ
 - 5.3.5 ต้องทำการเพิกถอนหรือระงับโปรแกรมประเภทยูทิลิตี้ที่ไม่จำเป็น
- 5.4 การหมดเวลาการใช้งานระบบสารสนเทศ (Session time-out)
- 5.4.1 ผู้ดูแลระบบต้องกำหนด Session time-out ของระบบเทคโนโลยีสารสนเทศที่ไม่มีการใช้งานภายในระยะเวลา 15 นาที ทั้งนี้ ถ้าระบบที่ไม่สามารถตัดการเชื่อมต่อแบบอัตโนมัติได้ กำหนดให้ใช้โปรแกรมพักหน้าจอที่ต้องใส่รหัสผ่านหรือกำหนดให้มีการล็อกหน้าจอ
 - 5.4.2 ผู้ดูแลระบบ และผู้ใช้งาน ต้องตั้งค่าให้โปรแกรมพักหน้าจอที่ต้องใส่รหัสผ่านสำหรับเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์แบบพกพา และเครื่องคอมพิวเตอร์แม่ข่าย ทั้งนี้ โปรแกรมพักหน้าจอกำหนดให้ป้อนรหัสผ่านหลังจากที่มีการทิ้งเครื่องดังกล่าวไว้โดยไม่มีการใช้งานเป็นเวลา 15 นาที

- 5.5 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)
 - 5.5.1 ผู้ดูแลระบบ ต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง โดยต้องคำนึงระยะเวลาที่จำเป็นในกระบวนการดำเนินงานทางธุรกิจ ได้แก่ กำหนดให้เข้าใช้งานได้ในช่วงเวลาทำการของ รพม. 08.00 น. – 17.00 น. และเชื่อมต่อเพื่อใช้งานได้ครั้งละไม่เกิน 3 ชั่วโมง
 - 5.5.2 ผู้ใช้งาน หากมีความจำเป็นต้องใช้งานนอกเวลาที่กำหนดต้องขออนุมัติจากผู้บังคับบัญชาเท่านั้น
6. การควบคุมการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ (Application and information access control)
ให้มีการจำกัดการเข้าถึงสารสนเทศ และการแยกระบบเทคโนโลยีสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณที่ควบคุมเฉพาะ
 - 6.1 การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)
 - 6.1.1 เจ้าของข้อมูลและผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงแก่ผู้ใช้งานเท่าที่จำเป็นต้องใช้ในการปฏิบัติงาน โดยการให้สิทธิ์ต้องพิจารณาในเรื่องดังต่อไปนี้
 - 1) การจำกัดไม่ให้ใช้ตัวเลือก (Options) ที่ไม่ได้รับอนุญาต
 - 2) การจำกัดการเข้าถึง Command Line
 - 3) การจำกัดการเข้าถึงข้อมูลและฟังก์ชันการใช้งานของแอปพลิเคชัน (Application) ที่ไม่เกี่ยวข้องกับหน้าที่ความรับผิดชอบ
 - 4) การจำกัดระดับสิทธิ์ในการเข้าถึงไฟล์ เช่น อ่านอย่างเดียว เป็นต้น
 - 5) การควบคุมการแจกจ่าย การเข้าถึงข้อมูล การนำข้อมูลออกจากระบบสารสนเทศ เช่น รายงาน เป็นต้น
 - 6.1.2 เจ้าของข้อมูลและผู้ดูแลระบบ ควรกำหนดให้ระบบสารสนเทศรองรับการกำหนดสิทธิ์ในการเข้าถึงแบบกลุ่มได้
 - 6.2 การแยกระบบสารสนเทศที่ไวต่อการรบกวน (Sensitive system isolation) มีผลกระทบต่อคนกลุ่มใหญ่ หรือระบบที่มีความสำคัญต่อหน่วยงาน ต้องดำเนินการดังนี้
 - 6.2.1 เจ้าของข้อมูลและผู้ดูแลระบบ แยกระบบซึ่งไวต่อการรบกวนออกจากระบบอื่น ๆ และควบคุมสภาพแวดล้อมของระบบโดยเฉพาะ ได้แก่ ระบบ File sharing ระบบสารสนเทศทางการเงิน และระบบ Active directory โดยเข้าถึงได้ทั้งอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร (Mobile computing and teleworking)
 - 6.2.2 ผู้ดูแลระบบต้องควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์เคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile computing and teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว
 - 6.2.3 เจ้าของข้อมูลที่เป็นเจ้าของระบบสารสนเทศที่มีความสำคัญสูงต้องเป็นผู้อนุญาต ในกรณีที่ระบบสารสนเทศที่มีความสำคัญสูงมีความจำเป็นต้องทำงานร่วมกับระบบสารสนเทศอื่นที่มีความสำคัญน้อยกว่า
7. การควบคุมการปฏิบัติงานจากภายนอก รพม. (Teleworking)
 - 7.1 ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนการใช้งาน และเชื่อมต่อผ่านช่องทางที่มีความปลอดภัยที่มีเทคโนโลยีเข้ารหัสป้องกัน

- 7.2 ผู้ดูแลระบบต้องทำการถอดถอนสิทธิ์ในการเข้าถึงของผู้ใช้งานจากภายนอกสำนักงาน เมื่อครบกำหนดระยะเวลาที่ขออนุญาต
- 7.3 ผู้ใช้งาน หากจำเป็นต้องมีการปฏิบัติงานจากภายนอกสำนักงานของ รพม. ต้องได้รับการอนุญาตจากผู้บังคับบัญชาอย่างเป็นทางการเป็นลายลักษณ์อักษร ในกรณีเร่งด่วนสามารถดำเนินการก่อน โดยแจ้งให้ผู้บังคับบัญชารับทราบด้วย โดยผู้บังคับบัญชาต้องพิจารณาเงื่อนไขในการเตรียมการ ดังต่อไปนี้
 - 1) ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมของการปฏิบัติงานจากภายนอก รพม.
 - 2) ความมั่นคงปลอดภัยทางการสื่อสาร โดยยึดจากระดับความสำคัญ (Sensitivity) ของข้อมูลที่จะถูกเข้าถึงและส่งผ่านช่องทางการเชื่อมต่อสื่อสาร (Communication link) รวมถึงระดับความสำคัญ (Sensitivity) ของระบบภายใน รพม.
- 7.4 ผู้ใช้งานต้องจัดเก็บเอกสารที่เป็นความลับในอุปกรณ์ที่ล็อกได้และมีการควบคุมการเข้าถึง โดยใช้หลักเกณฑ์การรักษาความลับเช่นเดียวกับสารสนเทศที่อยู่ในสำนักงานของ รพม.
- 7.5 ผู้ใช้งาน ต้องติดตั้งโปรแกรมป้องกันไวรัสและ Personal firewall สำหรับอุปกรณ์ส่วนตัวที่ใช้เชื่อมต่อเครือข่ายของ รพม. จากภายนอก
8. ผู้บังคับบัญชา ต้องควบคุมการใช้งานข้อมูลส่วนบุคคลให้มีการใช้งานที่สอดคล้องกับกฎหมาย พระราชบัญญัติกฏระเบียบ ข้อบังคับที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ส่วนที่ 7

การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

วัตถุประสงค์

- เพื่อกำหนดมาตรการในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ของ รพม. โดยการกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ
- เพื่อสร้างความมั่นคงปลอดภัยของการทำงานของระบบเครือข่ายไร้สาย

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 5 การควบคุมการเข้าถึง (Access control)
- หมวดที่ 9 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)

แนวปฏิบัติ

1. ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของ รพม. ต้องลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับการอนุญาตจาก ผทท. อย่างเป็นทางการ
2. ผู้ดูแลระบบต้องกำหนดมาตรฐานความปลอดภัยของระบบเครือข่ายไร้สายไม่ต่ำกว่ามาตรฐาน WPA2
3. ผู้ดูแลระบบต้องลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ
4. ผู้ดูแลระบบต้องลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อบนระบบเครือข่ายไร้สาย
5. ผู้ดูแลระบบ ต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีใช้ Access Point (AP) ของ รพม. รับ - ส่งสัญญาณได้
6. ผู้ดูแลระบบต้องเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและต้องสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณอาจช่วยลดการรั่วไหลของสัญญาณให้ดีขึ้น
7. ผู้ดูแลระบบต้องเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำ Access Point (AP) มาใช้งาน
8. ผู้ดูแลระบบต้องเปลี่ยนค่าชื่อ Login และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบต้องเลือกใช้ชื่อ Login และรหัสผ่านที่มีความคาดเดายากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย
9. ผู้ดูแลระบบต้องควบคุม MAC address ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยอนุญาตเฉพาะผู้ใช้งานที่ได้รับอนุญาตให้เข้าใช้เครือข่ายไร้สายได้อย่างถูกต้องเท่านั้น
10. ผู้ดูแลระบบต้องตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ และบันทึกเหตุการณ์น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สายตามขั้นตอนที่ รพม. กำหนด

ส่วนที่ 8

การควบคุมหน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) เข้าถึงระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

- เพื่อควบคุมหน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) ที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของ รพม. ให้เป็นไปอย่างมั่นคงปลอดภัย

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้บังคับบัญชา
- หน่วยงานภายนอก
- ผู้ใช้งาน (บุคคลภายนอก)

อ้างอิงมาตรฐาน

- หมวดที่ 5 การควบคุมการเข้าถึง (Access control)
- หมวดที่ 7 ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environment security)
- หมวดที่ 11 ความสัมพันธ์กับผู้ขาย ผู้ให้บริการภายนอก (Supplier relationships)

แนวปฏิบัติ

1. ผู้ดูแลระบบต้องประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสม ก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศของ รพม.
2. การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก)
 - 2.1 เจ้าของข้อมูลต้องเป็นผู้อนุญาตการให้สิทธิ์แก่หน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) ที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของ รพม. อย่างเป็นลายลักษณ์อักษร
 - 2.2 ผู้บังคับบัญชาต้องกำหนดให้มีการลงนามการไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของ รพม.
 - 2.3 ผู้บังคับบัญชา ต้องควบคุมให้มีการกำหนดข้อตกลงและความรับผิดชอบที่เกี่ยวข้องกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศลงในสัญญากับผู้ให้บริการภายนอกที่ให้บริการด้านสารสนเทศและบริการด้านการสื่อสาร โดยให้ครอบคลุมรวมถึงผู้รับจ้างช่วง
 - 2.4 ผู้บังคับบัญชาต้องกำหนดให้จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) ระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศ ซึ่งมีรายละเอียด ดังนี้
 - 2.4.1 เหตุผลในการขอใช้
 - 2.4.2 ระยะเวลาในการใช้
 - 2.4.3 การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย
 - 2.4.4 การตรวจสอบ MAC address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

- 2.5 ผู้ดูแลระบบมีสิทธิ์ในการตรวจสอบการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) เพื่อควบคุมการใช้งานได้อย่างมั่นคงปลอดภัยตามสัญญา
- 2.6 ผู้ดูแลระบบต้องควบคุมให้หน่วยงานภายนอกจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งต้องปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อใช้สำหรับควบคุมหรือตรวจสอบการทำงาน และเพื่อให้มั่นใจว่าการปฏิบัติงานเป็นไปตามขอบเขตที่ได้กำหนดไว้
3. ผู้ดูแลระบบต้องแจ้งแนวปฏิบัติต่าง ๆ ที่เกี่ยวข้อง แก่ผู้รับจ้างภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) เพื่อให้ปฏิบัติตาม
4. ผู้ดูแลระบบ ต้องกำกับดูแลหน่วยงานภายนอก หรือผู้ใช้งาน (บุคคลภายนอก) ให้ปฏิบัติตามสัญญาหรือข้อตกลงการให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงด้านความมั่นคงปลอดภัย
5. ผู้ดูแลระบบ ต้องติดตาม ตรวจสอบรายงานหรือบันทึกการให้บริการของหน่วยงานภายนอกหรือบุคคลที่ให้บริการแก่หน่วยงานตามที่ว่าจ้างอย่างสม่ำเสมอตามสัญญาว่าจ้าง
6. ผู้ดูแลระบบ ต้องกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีหน้าที่ในการกำกับดูแลหรือหน่วยงานที่เกี่ยวข้องกับการบังคับใช้กฎหมาย รวมทั้งหน่วยงานที่ควบคุมดูแลสถานการณ์ฉุกเฉินภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน
7. ผู้ดูแลระบบ ต้องมีขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีความเชี่ยวชาญเฉพาะด้านหรือหน่วยงานที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน
8. ผู้ดูแลระบบต้องควบคุมการเปลี่ยนแปลงของหน่วยงานภายนอกที่ส่งผลกระทบต่อการทำงานขององค์กร และต้องประเมินความเสี่ยงอย่างเหมาะสมเพื่อควบคุมผลกระทบอันเนื่องมาจากการเปลี่ยนแปลงนั้น
9. หน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) ต้องใช้งานทรัพย์สินสารสนเทศของ รฟม. ด้วยความระมัดระวัง และรักษาความลับของ รฟม. ไม่นำไปเปิดเผย และต้องขออนุญาตพร้อมทั้งปฏิบัติตามเงื่อนไขในการเข้าถึงระบบสารสนเทศของ รฟม. ทุกครั้ง

ส่วนที่ 9

การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ ของ รพม.

วัตถุประสงค์

- เพื่อควบคุมการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ ที่ รพม. จัดไว้ให้ใช้อย่างเหมาะสม ทั้งนี้ เพื่อป้องกันการสูญหาย เสียหาย หรือถูกเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 2 อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากระยะไกล (Mobile devices and teleworking)
- หมวดที่ 4 การบริหารจัดการทรัพย์สิน (Asset management)
- หมวดที่ 8 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations security)

แนวปฏิบัติ

1. การใช้งานทั่วไป

- 1.1 ผู้ดูแลระบบต้องกำหนดบัญชีซอฟต์แวร์มาตรฐาน (Software standard) ที่อนุญาตให้ติดตั้งบนเครื่องคอมพิวเตอร์ของผู้ใช้งาน และปรับปรุงให้เป็นปัจจุบันเสมอ
- 1.2 ผู้ดูแลระบบต้องเป็นผู้กำหนดการตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) เท่านั้น
- 1.3 ผู้ใช้งานต้องใช้งานอย่างมีประสิทธิภาพเพื่องานของ รพม.
- 1.4 ผู้ใช้งานต้องไม่ติดตั้งโปรแกรมที่ละเมิดลิขสิทธิ์บนเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ของ รพม.
- 1.5 ผู้ใช้งานต้องขออนุญาตติดตั้งโปรแกรมในเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ตามขั้นตอนที่ รพม. กำหนด
- 1.6 ผู้ใช้งานต้องไม่ติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ของ รพม. การดำเนินการดังกล่าวต้องดำเนินการโดยผู้ดูแลระบบเท่านั้น
- 1.7 ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่อย่างละเอียด เพื่อให้สามารถใช้งานอย่างปลอดภัยและมีประสิทธิภาพ
- 1.8 ผู้ใช้งานต้องไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ และรักษาให้มีสภาพเดิม
- 1.9 ผู้ใช้งานต้องแจ้งซ่อมเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่เพื่อให้ ผทท. เป็นผู้ดำเนินการเท่านั้น
- 1.10 ผู้ใช้งานต้องไม่สร้าง Shortcut ไว้บน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของ รพม.
- 1.11 กรณีเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์เคลื่อนที่ ผู้ใช้งานต้องปฏิบัติ ดังนี้
 - 1.11.1 ในกรณีที่มีการใช้งานอุปกรณ์ประเภทพกพาในที่สาธารณะ ห้องประชุม และพื้นที่ภายนอก อื่น ๆ ที่ไม่มีการป้องกัน หรือไม่ได้อยู่ในบริเวณของ รพม. ให้ป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต เช่น ไม่เปิดการเชื่อมต่อแบบไร้สายโดยไม่มีการเข้ารหัสข้อมูล เป็นต้น

- 1.11.2 ต้องระมัดระวังการเคลื่อนย้าย โดยต้องใส่กระเป๋าเพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงานหรือหลุดมือ เป็นต้น
 - 1.11.3 ไม่ใส่ในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับหรืออาจถูกจับโยนได้
 - 1.11.4 การใช้งานเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัดต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะเวลาหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง
 - 1.11.5 หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอย ชีตข่วน หรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้
 - 1.11.6 ไม่วางของทับบนหน้าจอและแป้นพิมพ์
 - 1.11.7 การเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น
 - 1.11.8 ไม่เคลื่อนย้ายเครื่องในขณะที่ Harddisk กำลังทำงาน
 - 1.11.9 ไม่ใช่หรือวางใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่าง ๆ เป็นต้น
 - 1.11.10 ไม่วางใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูง เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น
 - 1.11.11 ไม่ติดตั้งหรือวางในที่ที่มีการสั่นสะเทือน เช่น ในยานพาหนะที่กำลังเคลื่อนที่
 - 1.11.12 การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้
 - 1.11.13 รับผิดชอบในการป้องกันการสูญหาย เช่น ต้องล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย
 - 1.11.14 นำติดตัวไปด้วยเสมอ เช่น ไม่ละทิ้ง อุปกรณ์ประมวลผลประเภทพกพาในรถยนต์ ห้องพักในโรงแรม หรือห้องประชุม เป็นต้น ในกรณีที่มีความจำเป็นต้องละทิ้งให้จัดเก็บไว้ในสถานที่ที่มั่นคงปลอดภัย
 - 1.11.15 ไม่เก็บหรือใช้งานในสถานที่ที่มีความร้อน ความชื้นหรือฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ
 - 1.11.16 ไม่เปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub component) ที่ติดตั้งอยู่ภายใน เช่น แบตเตอรี่ หน่วยความจำ
2. แนวปฏิบัติในการใช้รหัสผ่าน
ให้ผู้ใช้งานปฏิบัติตามการใช้งานรหัสผ่าน (Password Use) (ส่วนที่ 6)
 3. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malicious code)
 - 3.1 ผู้ดูแลระบบต้องควบคุมการ Update ระบบปฏิบัติการ เว็บเบราว์เซอร์ และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ
 - 3.2 ผู้ดูแลระบบต้องติดตั้งและปรับปรุงโปรแกรมป้องกันไวรัสให้ทันสมัยอยู่เสมอ
 - 3.3 ผู้ใช้งานต้องไม่ปิดหรือยกเลิกระบบการป้องกันไวรัสที่ติดตั้งอยู่

- 3.4 ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อบันทึกต่าง ๆ เช่น Thumb drive และ Data storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์ของ รพม.
- 3.5 ผู้ใช้งาน หากพบหรือสงสัยว่าเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ติดชุดคำสั่งไม่พึงประสงค์ ให้รีบยกเลิกเชื่อมต่อเครื่องเข้ากับระบบเครือข่ายสื่อสารข้อมูลเพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่น ๆ ได้ และแจ้ง ผทท. ทราบทันที
4. การสำรองข้อมูลและการกู้คืน
 - 4.1 ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ไว้บนสื่อบันทึกอื่น ๆ เช่น ระบบ File Sharing, CD, DVD, External harddisk เป็นต้น
 - 4.2 ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลสำรองไว้อย่างสม่ำเสมอ
5. ผู้ดูแลระบบ ต้องควบคุมให้เครื่องคอมพิวเตอร์ได้รับการปรับตั้งค่าอย่างเหมาะสม เพื่อป้องกันการใช้งานหรือติดตั้ง Mobile code เช่น Active x, Java จากแหล่งที่ไม่น่าเชื่อถือ

ส่วนที่ 10

การใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์

วัตถุประสงค์

- เพื่อควบคุมการใช้งานอินเทอร์เน็ตและการใช้งานสื่อสังคมออนไลน์ (Social network) ของ รพม. ให้มีความปลอดภัย และป้องกันการละเมิดพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ จนส่งผลกระทบต่อ รพม.

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 5 การควบคุมการเข้าถึง (Access control)
- หมวดที่ 8 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations security)
- หมวดที่ 18 ความสอดคล้อง (Compliance)

แนวปฏิบัติ

1. ผู้ดูแลระบบต้องควบคุมการเชื่อมต่อทางเครือข่ายสำหรับการเข้าถึงอินเทอร์เน็ตโดยพิจารณาเรื่องดังต่อไปนี้
 - 1) ผู้ดูแลระบบต้องไม่อนุญาตให้ใช้งานอุปกรณ์ Video streaming อุปกรณ์ audio streaming หรือ Download ไฟล์ที่มีขนาดใหญ่ ในกรณีที่ต้องได้รับการอนุญาตจากผู้บังคับบัญชาก่อนเท่านั้น
 - 2) ผู้ดูแลระบบต้องจำกัดการใช้งานอินเทอร์เน็ตเพื่อเรื่องส่วนตัวหรือที่ไม่ใช่การดำเนินงานของ รพม. ให้น้อยที่สุดเท่าที่เป็นไปได้ เช่น การระงับการเข้าถึง Website ที่ไม่จำเป็น การระงับการเข้าถึง Website ที่มีเนื้อหาต้องห้ามตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
 - 3) ผู้ดูแลระบบต้องป้องกันไม่ให้มีการรับส่งข้อมูลที่ไม่เหมาะสมจากภายนอก รพม. เช่น
 - (ก) Executable เช่น .EXE .COM เป็นต้น
 - (ข) ไฟล์ (File) เสียง เช่น AUD .WAV และ.MP3 เป็นต้น
 - (ค) ไฟล์ (File) วิดิทัศน์ เช่น .MPG .MPEG .MOV และ .AVI เป็นต้น
 - (ง) Peer to Peer เช่น .torrent เป็นต้นในกรณีที่มีความจำเป็นต้องได้รับอนุญาตจากผู้บังคับบัญชา และ ผทท.
 - 4) ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่ รพม. จัดสรรไว้เท่านั้น เช่น Proxy, Firewall เป็นต้น
 - 5) ผู้ดูแลระบบต้องทดสอบเส้นทางสำหรับการเชื่อมต่ออินเทอร์เน็ตขององค์กรระหว่างเส้นทางที่ใช้งานจริงและเส้นทางสำรองอย่างน้อยปีละ 2 ครั้ง
 - 6) ผู้ใช้งานต้องไม่เชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นมีความจำเป็นและขออนุญาตจาก ผทท. เป็นลายลักษณ์อักษรแล้ว
 - 7) ผู้ใช้งานต้องขออนุญาตติดตั้งซอฟต์แวร์ (Software) ที่ Download จากอินเทอร์เน็ต และการติดตั้งต้องดำเนินการโดยผู้ที่ได้รับมอบหมายจากผู้ดูแลระบบเท่านั้น

2. ผู้ใช้งานต้องไม่มีเจตนาปิดบังหรือบิดเบือนตัวตนเมื่อมีการใช้งานอินเทอร์เน็ต
3. ผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัส พร้อมทั้งต้องปรับปรุง Virus signature ที่เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพาให้มีความทันสมัยอยู่เสมอ ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web browser) และต้องปิดช่องโหว่ของระบบปฏิบัติการที่เว็บเบราว์เซอร์ติดตั้งอยู่
4. ผู้ใช้งานจะต้องตรวจสอบไวรัส (Virus scanning) ก่อนการรับ - ส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ต
5. ผู้ใช้งานต้องไม่ใช่เครือข่ายอินเทอร์เน็ตของ รพม. เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น
6. ผู้ใช้งานจะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของ รพม.
7. ผู้ใช้งานต้องหลีกเลี่ยงการกระทำที่สิ้นเปลืองทรัพยากรของเครือข่ายอินเทอร์เน็ต ดังนี้
 - (ก) ส่งจดหมายอิเล็กทรอนิกส์ที่มีขนาดใหญ่หรือจดหมายอิเล็กทรอนิกส์ลูกโซ่
 - (ข) ใช้เวลาในการเข้าถึงอินเทอร์เน็ตเกินความจำเป็น
 - (ค) เล่นเกม Online
 - (ง) เข้าห้องพูดคุย Online
8. ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับ รพม.
9. ผู้ใช้งานต้องไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของ รพม.
10. ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต
11. ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อเติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ที่จะทำให้อื่นเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย
12. ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน
13. ผู้ใช้งานต้องคำนึงว่าข้อมูลจากอินเทอร์เน็ตอาจไม่มีความทันสมัยหรือไม่มีความถูกต้อง ผู้ใช้งานต้องตรวจสอบความถูกต้องของข้อมูลจากแหล่งที่น่าเชื่อถือก่อนที่จะเผยแพร่ข้อมูลดังกล่าว
14. ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา
15. ผู้ใช้งานต้องไม่ใช่ข้อมูลที่ร้ายๆ ให้อภัยในการเสนอความคิดเห็นที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของ รพม. การทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น ๆ
16. ผู้ใช้งานต้องไม่บันทึกรหัสผ่านใน Web browser (Remember password) เพื่อป้องกันบุคคลอื่นที่สามารถเข้าถึงคอมพิวเตอร์ของผู้ใช้งานนำรหัสผ่านดังกล่าวไปใช้งานในอินเทอร์เน็ตโดยไม่ได้รับอนุญาต

17. ผู้ใช้งานต้องไม่ Download เอกสาร หรือสารสนเทศต่าง ๆ เช่น ข้อมูล รูปภาพ วิดีโอ เสียง และซอฟต์แวร์ (Software) ที่ละเมิดลิขสิทธิ์ หรือผิดกฎหมาย
18. ผู้ใช้งานต้องปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ ภายหลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว
19. การใช้งานสื่อสังคมออนไลน์ (Social network)
 - 19.1 ผู้ใช้งานต้องระมัดระวังในการนำเสนอข้อมูลข่าวสาร การส่งข้อความ หรือการแสดงความคิดเห็นผ่านสื่อสังคมออนไลน์เพื่อไม่ก่อให้เกิดความเสียหายแก่ รพม.
 - 19.2 ผู้ใช้งานต้องระมัดระวังในการใช้สื่อสังคมออนไลน์ เนื่องจากพื้นที่บนสื่อสังคมออนไลน์เป็นพื้นที่สาธารณะไม่ใช่พื้นที่ส่วนบุคคล ซึ่งข้อมูลการใช้งานต่าง ๆ จะถูกบันทึกไว้และอาจมีผลทางกฎหมายถึงแม้จะเป็นการแสดงความคิดเห็นในนามชื่อบัญชีส่วนตัว และพึงตระหนักถึงผลกระทบที่อาจเกิดขึ้นกับ รพม. ได้
 - 19.3 ผู้ใช้งานที่ใช้สื่อสังคมออนไลน์เป็นเครื่องมือสื่อสารข้อมูลในกิจการของ รพม. หรือชื่อบุคคลที่ทำให้เข้าใจได้ว่าเป็นบุคคลในสังกัด ต้องแสดงภาพ และข้อมูลให้ถูกต้องชัดเจนในข้อมูล โปรไฟล์ (Profile) และพึงใช้ด้วยความสุภาพและมีวิจารณญาณ
 - 19.4 ผู้ใช้งานควรตั้งคำถามที่ใช้ในกรณีกู้คืนบัญชีผู้ใช้งานหรือกู้คืนรหัสผ่าน (Forgot your password) ควรเลือกใช้ข้อมูลหรือคำถามที่เป็นส่วนบุคคลและเป็นข้อมูลที่ผู้อื่นคาดเดาได้ยากเพื่อป้องกันการสุ่มคำถามจากผู้ประสงค์ร้าย
 - 19.5 ผู้ใช้งานต้องไม่ใช้ระบบอีเมลของเว็บไซต์ประเภทสื่อสังคมออนไลน์ หากจำเป็นต้องใช้จะต้องระมัดระวังในการคลิกลิงก์ที่น่าสงสัย โดยเฉพาะอีเมลแจ้งเตือนจากเว็บไซต์ต่าง ๆ ในลักษณะเชื้อเชิญให้คลิกลิงก์ที่แนบมาในอีเมล ผู้ใช้งานต้องสงสัยว่าลิงก์ดังกล่าวเป็นลิงก์ที่ไม่ปลอดภัย (ลิงก์ที่ถูกสร้างมาเพื่อใช้ขโมยข้อมูลส่วนบุคคล ด้วยการนำไปสู่เว็บไซต์ที่ดูน่าเชื่อถือที่ผู้ประสงค์ร้ายสร้างไว้เพื่อให้ผู้ใช้งานกรอกข้อมูลส่วนตัว เช่น รหัสผ่าน เป็นต้น)
 - 19.6 ผู้ใช้งานต้องศึกษาการตั้งค่าความเป็นส่วนตัวหรือ “Privacy settings” ให้เข้าใจเป็นอย่างดีและปรับแต่งการตั้งค่าความเป็นส่วนตัวให้เหมาะสมเพื่อป้องกันการถูกละเมิดความเป็นส่วนตัวซึ่งอาจจะส่งผลกระทบต่อตนเองหรือ รพม.
 - 19.7 ผู้ใช้งานต้องใช้งานสื่อสังคมออนไลน์อย่างเหมาะสม โดยไม่ละเมิดกฎหมายและไม่ก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานขององค์กร
 - 19.8 ผู้ใช้งานควรปิดการใช้งานระบบโพสต์ข้อความสาธารณะทุก ๆ ส่วนของเว็บไซต์ประเภท Social network หากจำเป็นต้องใช้งานต้องปรับค่าให้มีการตรวจสอบข้อความก่อนเพื่อหลีกเลี่ยงโอกาสแพร่กระจายลิงก์ที่ไม่ปลอดภัยจากผู้ประสงค์ร้าย ซึ่งเป็นหนึ่งในเทคนิคที่ใช้ในการโจมตีประเภท Spear-phishing
 - 19.9 ผู้ใช้งานต้องตรวจสอบก่อนจะรับเพื่อนเข้ากลุ่มในเว็บไซต์ประเภท Social network โดยต้องแน่ใจว่าข้อมูลส่วนตัวของเพื่อนคนนั้น เช่น รูปถ่ายและประวัติส่วนตัวไม่ถูกแก้ไขเพื่อปลอมแปลงตัวตนจากผู้ประสงค์ร้ายที่หวังแอบอ้างเพื่อคุกคามเป้าหมาย

- 19.10 ผู้ใช้งานต้องตระหนักไว้เสมอว่าข้อมูลต่าง ๆ ที่ผู้ใช้งานเผยแพร่ไว้บนบริการสื่อสังคมออนไลน์นั้น คงอยู่ถาวรและผู้อื่นอาจเข้าถึงและเผยแพร่ข้อมูลเหล่านั้นได้
- 19.11 ผู้ใช้งานต้องมีข้อพิจารณาในการรับเพื่อนเข้ากลุ่มที่ชัดเจน และควรประกาศข้อความปฏิเสธความรับผิดชอบที่เกี่ยวกับเนื้อหาหรือข้อความแสดงความคิดเห็นซึ่งถูกโพสต์จากเพื่อนในกลุ่มที่อาจปรากฏในเว็บไซต์ประเภท Social network ของผู้ใช้งานเอง
- 19.12 ผู้ใช้งานต้องติดตั้งซอฟต์แวร์ป้องกันไวรัส และอัปเดตฐานข้อมูลไวรัสของโปรแกรมอยู่เสมอ และต้องหลีกเลี่ยงการใช้โปรแกรมที่ละเมิดลิขสิทธิ์เพราะอาจจะมีโปรแกรมประสงค์ร้ายแฝงตัวอยู่ภายในเพื่อลักลอบ ปลอมแปลง หรือขโมยข้อมูลสำคัญของผู้ใช้งานได้
- 19.13 ผู้ใช้งานต้องระมัดระวังการใช้ถ้อยคำและภาษาที่อาจเป็นการดูหมิ่น ยุ้ง ทำทนาย หรือเป็นการละเมิดต่อบุคคลอื่น กรณีบุคคลอื่นมีความคิดเห็นที่แตกต่างพึงงดเว้นการโต้ตอบด้วยถ้อยคำรุนแรง
- 19.14 ผู้ใช้งานต้องระมัดระวังกระบวนการหาข่าว หรือภาพจากสื่อสังคมออนไลน์ โดยมีการตรวจสอบอย่างถี่ถ้วนรอบด้านและต้องอ้างอิงแหล่งที่มาเมื่อนำเสนอ เว้นแต่สามารถตรวจสอบและอ้างอิงจากแหล่งข่าวได้โดยตรง
- 19.15 หากผู้ใช้งานต้องการใช้สื่อสังคมออนไลน์เป็นเครื่องมือในการรายงานข่าวในนามของบุคคลธรรมดา ต้องแสดงให้เห็นชัดเจนว่า ข้อความใดเป็น "ข่าว" ข้อความใดเป็น "ความคิดเห็นส่วนตัว"
- 19.16 การส่งต่อหรือเผยแพร่ข้อมูลในสื่อสังคมออนไลน์ (Social media)
 - 19.16.1 ผู้ใช้งานต้องไม่ส่งต่อหรือเผยแพร่ข้อมูลที่เป็นเท็จ ข่าวลือ ข่าวไม่ปรากฏที่มา เป็นเพียงการคาดเดา หรือส่งผลเสียหายกับบุคคล สังคม หรือ รฟม.
 - 19.16.2 ผู้ใช้งานต้องไม่ส่งต่อหรือเผยแพร่ข้อมูลเรื่องบุคคลเสียชีวิต เด็กและเยาวชน ผู้สูญหาย ผู้ต้องหา เว้นเสียแต่ตรวจสอบข้อเท็จจริงแล้วและเห็นว่าเป็นประโยชน์ต่อสาธารณะ
 - 19.16.3 ผู้ใช้งานต้องไม่ส่งต่อหรือเผยแพร่ข้อมูลที่กระทบต่อสิทธิความเป็นส่วนตัว และศักดิ์ศรีความเป็นมนุษย์
- 19.17 ผู้ใช้งานต้องตั้งค่าความปลอดภัยของการใช้งานสื่อสังคมออนไลน์ และระมัดระวังการถูกนำข้อมูลจากข้อบัญชีไปใช้โดยไม่เหมาะสม ผิดวัตถุประสงค์ และลักษณะการแอบอ้างโดยบุคคลอื่น
20. ผู้ใช้งานต้องใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์โดยตระหนักถึงพระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่บังคับใช้อยู่เสมอ

ส่วนที่ 11

การใช้งานจดหมายอิเล็กทรอนิกส์

วัตถุประสงค์

- เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ของ รพม. ให้มีความปลอดภัยและมีประสิทธิภาพ

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 5 การควบคุมการเข้าถึง (Access control)
- หมวดที่ 8 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations security)

แนวปฏิบัติ

1. ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของ รพม. ให้เหมาะสมกับหน้าที่ความรับผิดชอบของผู้ใช้งาน รวมทั้งทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ
2. ผู้ดูแลระบบต้องกำหนดบัญชีผู้ใช้งานตามมาตรฐานจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ใช้ในองค์กร
3. ผู้ใช้งานต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ไม่ให้เกิดความเสียหายต่อ รพม. ละเมิดลิขสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น ผิดกฎหมาย ละเมิดศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่น แสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ของ รพม.
4. ผู้ใช้งานต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail address) ของผู้อื่นเพื่ออ่าน รับ - ส่งข้อความ ยกเว้น ได้รับการยินยอมจากเจ้าของบัญชีและให้ถือว่าเจ้าของบัญชีจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน
5. ผู้ใช้งานต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของ รพม. เพื่อปฏิบัติงาน ติดต่อ และประสานงานของ รพม. เท่านั้น
6. ผู้ใช้งานต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ฟรีของเอกชนในการปฏิบัติงาน ติดต่อ และประสานงานของ รพม.
7. ผู้ใช้งานต้อง Logout ออกจากระบบทุกครั้ง หลังจากใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้นเพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์
8. ผู้ใช้งานต้องตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนเปิดอ่าน โดยใช้โปรแกรมป้องกันไวรัส เพื่อตรวจสอบมัลแวร์ต่าง ๆ
9. ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์ที่ได้รับจากผู้ส่งที่ไม่รู้จัก
10. ผู้ใช้งานต้องใช้ข้อความที่สุภาพในการรับ - ส่งจดหมายอิเล็กทรอนิกส์ และไม่จัดส่งจดหมายที่มีเนื้อหาอาจทำให้อับอาย รพม. เสียชื่อเสียงหรือทำให้เกิดความแตกแยกภายใน รพม.
11. ผู้ใช้งานต้องไม่ระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์และต้องเข้ารหัสเพื่อป้องกันการเข้าถึงข้อมูลโดยผู้ไม่เกี่ยวข้องเมื่อมีการส่งข้อมูลที่เป็นความลับ
12. ผู้ใช้งานต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และต้องจัดเก็บจดหมายอิเล็กทรอนิกส์ในตู้ของตนให้เหลือจำนวนน้อยที่สุด หากมีข้อมูลที่จำเป็นต้องนำมาใช้อ้างอิงในการปฏิบัติงานภายหลัง ให้ผู้ใช้งานโอนย้ายจดหมายอิเล็กทรอนิกส์มายังเครื่องคอมพิวเตอร์ของตน ทั้งนี้ เพื่อลดปริมาณการใช้เนื้อที่ของระบบจดหมายอิเล็กทรอนิกส์

ส่วนที่ 12

การสำรองข้อมูลและการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

วัตถุประสงค์

- เพื่อให้มีข้อมูลสำรองไว้ใช้งานในกรณีที่ข้อมูลหลักเกิดความเสียหายไม่สามารถใช้งานหรือเข้าถึงได้ หรือเมื่อเกิดภาวะฉุกเฉินต่าง ๆ
- เพื่อให้มีการปฏิบัติที่สอดคล้องกับกฎหมาย พระราชบัญญัติ หรือข้อบังคับภายนอกอื่น ๆ

ผู้รับผิดชอบ

- ผู้บังคับบัญชา
- ผู้ดูแลระบบ
- เจ้าของข้อมูล
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 8 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations security)
- หมวดที่ 14 ความสอดคล้อง (Compliance)

แนวปฏิบัติ

1. การสำรองข้อมูลระบบแม่ข่าย

ข้อมูลระบบแม่ข่ายและข้อมูลสำคัญซึ่งเป็นความลับของ รพม. ต้องได้รับการเก็บรักษาไว้ที่ระบบเก็บข้อมูลส่วนกลาง และสำรองข้อมูลไว้อย่างสม่ำเสมอ เพื่อให้มีข้อมูลสำรองไว้ใช้ ในกรณีที่ข้อมูลหลักเกิดความเสียหายหรือไม่สามารถใช้งาน ความถี่ในการดำเนินการสำรองข้อมูลและขั้นตอนการสำรองข้อมูลระบบแม่ข่าย เป็นความรับผิดชอบของ ผทท. โดยมีแนวปฏิบัติ ดังนี้

- 1.1 ผู้บังคับบัญชากำหนดผู้รับผิดชอบในการสำรองข้อมูล
- 1.2 ผู้ดูแลระบบต้องกำหนดชนิดของข้อมูลของระบบที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้ เช่น ข้อมูลค่าคอนฟิกูเรชัน (Configuration) ข้อมูลคู่มือการปฏิบัติงานสำหรับระบบ ข้อมูลในฐานข้อมูลของระบบงาน ข้อมูลซอฟต์แวร์ เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ระบบงาน และซอฟต์แวร์อื่น ๆ เป็นต้น
- 1.3 ผู้ดูแลระบบต้องสำรองข้อมูลตามความถี่ที่กำหนดไว้ ทั้งนี้ หากเป็นข้อมูลที่สนับสนุนกระบวนการทำงานที่สำคัญของ รพม. ให้สำรองตามความถี่ที่ รพม. กำหนด
- 1.4 ผู้ดูแลระบบต้องตรวจสอบว่าการสำรองข้อมูลสำเร็จครบถ้วนหรือไม่ หากไม่สำเร็จให้หาสาเหตุและดำเนินการแก้ไขอีกครั้งหนึ่ง
- 1.5 ผู้ดูแลระบบต้องนำข้อมูลที่สำรองไว้ไปเก็บไว้ทั้งภายในและนอก รพม. อย่างน้อยอย่างละ 1 ชุด
- 1.6 ผู้ดูแลระบบทดสอบกู้คืนข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าข้อมูลที่สำรองไว้มีความถูกต้อง ครบถ้วน และพร้อมใช้งาน

2. การสำรองข้อมูลคอมพิวเตอร์ส่วนบุคคล
ผู้ใช้งานจะต้องสำรองข้อมูลสำคัญที่เก็บรักษาไว้ในเครื่องคอมพิวเตอร์ส่วนบุคคลหรือคอมพิวเตอร์ หรืออุปกรณ์พกพาอื่น ๆ อย่างสม่ำเสมอ ความถี่ในการสำรองข้อมูลขึ้นอยู่กับความถี่ของการเปลี่ยนแปลงของข้อมูล และระดับความสำคัญของข้อมูลหากเกิดการสูญหาย
3. การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์
เพื่อให้สามารถระบุตัวบุคคลผู้ใช้งานได้อย่างถูกต้อง ผู้ดูแลระบบต้องดำเนินการดังนี้
 - 3.1 ตั้งนาฬิกาของอุปกรณ์ที่ให้บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล Stratum - 1 เก็บรักษาข้อมูลจราจรคอมพิวเตอร์ โดยระยะเวลาในการเก็บตามประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 (90 วัน)
 - 3.2 เก็บรักษาข้อมูลจราจรคอมพิวเตอร์ในสื่อที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง มีการเก็บรักษาความลับของข้อมูลตามระดับชั้นความลับในการเข้าถึงตามที่ รพม. กำหนด โดยระบุตัวบุคคลที่สามารถเข้าถึงสื่อดังกล่าวได้
 - 3.3 ประเภทของสารสนเทศที่เก็บรักษา แสดงตามตาราง

ประเภทของสารสนเทศ	กฎหมายที่เกี่ยวข้อง	ระยะเวลาการจัดเก็บรักษา (ปี)
Authentication server logs (RADIUS, TACACS)	1) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	1
Email server logs	2) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560	1
Web application server logs	3) ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564	1
NTP server logs		1
DHCP server logs		1
IPS logs		1
Firewalls logs		1
Routers & Switches logs		1
Active directory logs		1

4. การจัดเก็บบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and monitoring)
 - 4.1 ผู้ดูแลระบบต้องมีการจัดเก็บบันทึกเหตุการณ์ (Event logs) การใช้งานระบบสารสนเทศ
 - 4.2 ผู้ดูแลระบบต้องเก็บบันทึกข้อมูล Audit log ซึ่งบันทึกกิจกรรมการใช้งานของผู้ใช้งานระบบสารสนเทศและเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยต่าง ๆ เพื่อประโยชน์ในการสืบสวน สอบสวน และเพื่อการติดตามการควบคุมการเข้าถึง
 - 4.3 ผู้ดูแลระบบต้องมีการตรวจสอบข้อมูลบันทึกเหตุการณ์อย่างสม่ำเสมอ (Log review)
 - 4.4 ผู้ดูแลระบบต้องไม่ลบข้อมูลล็อก (Log) หรือปิดการใช้งานการบันทึกข้อมูลล็อก (Log)
 - 4.5 ผู้ดูแลระบบต้องป้องกันระบบสารสนเทศที่จัดเก็บล็อก (Log) และข้อมูลล็อก (Log) เพื่อป้องกันการเข้าถึงหรือแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต
5. การเตรียมความพร้อมกรณีฉุกเฉิน

เพื่อให้มีการบริหารจัดการความต่อเนื่องให้กับกระบวนการทางธุรกิจที่สำคัญขององค์กร เมื่อมีเหตุการณ์ที่ทำให้เกิดการหยุดชะงักหรือติดขัดต่อกระบวนการดังกล่าว โดยมีแนวปฏิบัติ ดังนี้

 - 5.1 ผู้ดูแลระบบต้องกำหนดระบบที่มีความสำคัญทั้งหมดขององค์กร และจัดทำเป็นบัญชีรายชื่อระบบดังกล่าวรวมทั้งปรับปรุงรายชื่อระบบสำคัญและบัญชีฯ ตามความเป็นจริง
 - 5.2 เจ้าของข้อมูลและผู้ดูแลระบบประเมินความเสี่ยงสำหรับระบบเหล่านั้น กำหนดมาตรการเพื่อลดความเสี่ยงที่พบและจัดทำรายงานการประเมินความเสี่ยง
 - 5.3 ผู้ดูแลระบบจัดทำและปรับปรุงแผนกู้คืนระบบอย่างน้อยปีละ 1 ครั้ง
 - 5.4 เจ้าของข้อมูลและผู้ดูแลระบบต้องทดสอบแผนกู้คืนระบบอย่างน้อยปีละ 1 ครั้ง บันทึกผลการทดสอบรวมถึงปัญหาที่พบ และนำเสนอผลการทดสอบและแนวทางแก้ไขต่อผู้บังคับบัญชา
 - 5.5 ผู้ดูแลระบบต้องจัดประชุมและชี้แจงให้ผู้ที่เกี่ยวข้องทั้งหมดได้รับทราบเกี่ยวกับแผนและผลของการฝึกซ้อมการกู้คืนระบบ

ส่วนที่ 13

การตรวจสอบและประเมินความเสี่ยง

วัตถุประสงค์

- เพื่อให้มีการตรวจสอบการดำเนินงานของระบบจัดการความมั่นคงปลอดภัยสารสนเทศ และปรับปรุงอย่างต่อเนื่อง
- เพื่อควบคุม และติดตามการปฏิบัติงานของผู้ดูแลระบบสารสนเทศ ให้สอดคล้องตามข้อกำหนด กฎหมาย หรือระเบียบข้อบังคับที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ
- เพื่อประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของสารสนเทศและบริหารจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

ผู้รับผิดชอบ

- ผู้บังคับบัญชา
- ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

- ข้อกำหนดหลัก: การวางแผน (Planning)
- ข้อกำหนดหลัก: การตรวจประเมินภายใน (Internal Audit)
- หมวดที่ 8 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations security)
- หมวดที่ 14 ความสอดคล้อง (Compliance)

แนวปฏิบัติ

1. ผู้บังคับบัญชา ต้องกำหนดให้มีแนวทางในการดำเนินงานของระบบสารสนเทศสอดคล้องกับกฎหมาย พระราชบัญญัติ กฎระเบียบ ข้อบังคับที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศโดยต้องจัดทำเป็นลายลักษณ์อักษร และมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
2. ผู้บังคับบัญชา ต้องกำหนดมาตรการในการควบคุมและบริหารจัดการสินทรัพย์ทางปัญญา ได้แก่ ลิขสิทธิ์ในเอกสาร หรือซอฟต์แวร์ เครื่องหมายการค้า สิทธิบัตร และใบอนุญาตการใช้งานซอร์สโค้ด หรือการใช้งานซอฟต์แวร์ เพื่อให้การดำเนินงานเป็นไปตามข้อกำหนดทั้งในแง่ของข้อสัญญา และด้านกฎหมาย พระราชบัญญัติ กฎระเบียบ ข้อบังคับด้านสินทรัพย์ทางปัญญาที่เกี่ยวข้อง
3. ผู้บังคับบัญชา ต้องควบคุมให้มีการคุ้มครองข้อมูลส่วนบุคคลโดยให้สอดคล้องกับกฎหมาย พระราชบัญญัติ กฎระเบียบ ข้อบังคับที่เกี่ยวข้อง
4. ผู้บังคับบัญชา ต้องกำกับดูแล และควบคุมการปฏิบัติงานของผู้ที่อยู่ใต้การบังคับบัญชา เพื่อป้องกันการใช้งานระบบสารสนเทศผิดวัตถุประสงค์ หรือละเมิดต่อนโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของ รพม.
5. ผู้บังคับบัญชา ต้องควบคุมให้มีการป้องกันข้อมูลสำคัญขององค์กร ข้อมูลสำคัญที่เกี่ยวข้องกับข้อกำหนดทางกฎหมาย ระเบียบ ข้อบังคับ สัญญา ควรได้รับการป้องกันจากการสูญหาย ถูกทำลาย และปลอมแปลง
6. ผู้บังคับบัญชาต้องจัดให้มีการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยผู้ตรวจสอบภายใน (Internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External auditor) ตามระยะเวลาอย่างน้อยปีละ 1 ครั้ง

7. ผู้ดูแลระบบ ต้องติดตามผลการใช้งานทรัพยากรสารสนเทศ (Capacity) และวางแผนด้านทรัพยากรสารสนเทศให้รองรับการปฏิบัติงานในอนาคตอย่างเหมาะสม
8. ผู้ดูแลระบบ ต้องป้องกันการเข้าใช้งานเครื่องมือที่ใช้เพื่อการตรวจสอบ เพื่อมิให้เกิดการใช้งานผิดประเภท หรือถูกละเมิดการใช้งาน (Compromise) โดยควบคุมการเข้าถึง และตรวจสอบการนำเครื่องมือไปใช้งานอย่างสม่ำเสมอ
9. ผู้ดูแลระบบต้องประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
10. ผู้บังคับบัญชาต้องติดตามผลการดำเนินการตามแผนบริหารจัดการความเสี่ยง (Risk treatment plan) เป็นประจำทุกไตรมาส
11. ผู้ดูแลระบบต้องประเมินความเสี่ยงแล้วจัดลำดับความสำคัญของความเสี่ยงนั้นและค้นหาวิธีการเพื่อลดความเสี่ยงตามขั้นตอนที่ รพม. กำหนด พร้อมทั้งพิจารณาข้อดีข้อเสียของวิธีการเหล่านั้นเพื่อให้ผู้บริหารของ รพม. ตัดสินใจเลือกวิธีการเพื่อลดความเสี่ยงหรือยอมรับความเสี่ยง เมื่อเลือกวิธีการลดความเสี่ยงแล้วผู้บริหารต้องจัดสรรทรัพยากรอย่างเพียงพอเพื่อดำเนินการ แนวทางการลดความเสี่ยง แบ่งได้เป็น 3 รูปแบบ ได้แก่
 - 11.1 การเลือกใช้เทคโนโลยี เพื่อใช้ในการลดความเสี่ยงและเพิ่มความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รพม. เป็นวิธีที่จำเป็นต้องใช้งบประมาณและทรัพยากรอย่างเพียงพอในการดำเนินการ เช่น การเลือกใช้อุปกรณ์ Firewall มากกว่าหนึ่งผลิตภัณฑ์ในการป้องกันการเข้าถึงเครือข่ายที่สำคัญ การใช้อุปกรณ์สมาร์ตการ์ด หรือ USB Token ในการตรวจสอบยืนยันตัวตนในการเข้าใช้งานระบบจากภายนอก รพม. เป็นต้น
 - 11.2 การปรับเปลี่ยนขั้นตอนปฏิบัติ ต้องออกแบบขั้นตอนปฏิบัติใหม่ที่รัดกุมและสามารถรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รพม. ได้ดีขึ้น เมื่อออกแบบขั้นตอนปฏิบัติใหม่แล้วต้องมีการพิจารณาหาหรือความเหมาะสม ความเป็นไปได้ และผู้บริหารต้องเป็นผู้อนุมัติให้มีการบังคับใช้ขั้นตอนปฏิบัติใหม่นั้น
 - 11.3 ผู้ดูแลระบบต้องแจ้งขั้นตอนปฏิบัติให้ผู้เกี่ยวข้องรับรู้อย่างทั่วถึง รวมทั้งต้องจัดฝึกอบรมผู้ใช้งานที่เกี่ยวข้องเพื่อให้สามารถปฏิบัติตามขั้นตอนปฏิบัติใหม่ได้อย่างราบรื่นและมีประสิทธิภาพ
12. การตรวจสอบความปลอดภัยของระบบสารสนเทศ
 - 12.1 ผู้ดูแลระบบ ต้องวางแผนการตรวจสอบและประเมินช่องโหว่หรือจุดอ่อนด้านความมั่นคงปลอดภัยสารสนเทศ และแจ้งผู้ที่เกี่ยวข้องเพื่อแก้ไขในกรณีที่พบว่าช่องโหว่หรือจุดอ่อนนั้นอาจเป็นเหตุการณ์ด้านความมั่นคงปลอดภัย อย่างน้อยปีละ 1 ครั้ง
 - 12.2 ผู้ดูแลระบบต้องตรวจสอบระบบสารสนเทศที่จะต้องมีการปรับปรุงเมื่อมีเวอร์ชันใหม่ (Patch) รวมทั้งข้อมูลที่เกี่ยวข้องกับช่องโหว่ด้านเทคนิคอย่างสม่ำเสมอเพื่อให้ทราบถึงภัยคุกคามและความเสี่ยง รวมถึงหาวิธีป้องกันและแก้ไขที่เหมาะสมกับช่องโหว่นั้น
 - 12.3 ผู้ใช้งาน ผู้ดูแลระบบ และหน่วยงานภายนอก ต้องบันทึกและรายงานช่องโหว่หรือจุดอ่อนใด ๆ ด้านความมั่นคงปลอดภัยสารสนเทศ ที่อาจสังเกตพบระหว่างการติดตามการใช้งานระบบสารสนเทศ ผ่านช่องทางบริหารจัดการที่กำหนดไว้อย่างเหมาะสม และต้องดำเนินการปิดช่องโหว่ที่มีการตรวจพบหรือได้รับแจ้ง
13. ผู้ดูแลระบบต้องมีการบริหารจัดการการเปลี่ยนแปลงเกี่ยวกับการจัดเตรียมการให้บริการ การดูแลปรับปรุงนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ขั้นตอนปฏิบัติงาน หรือการควบคุมเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ โดยคำนึงถึงระดับความสำคัญของการดำเนินธุรกิจที่เกี่ยวข้องและการประเมินความเสี่ยงอย่างต่อเนื่อง

ส่วนที่ 14

การถ่ายโอน และแลกเปลี่ยนข้อมูลสารสนเทศ

วัตถุประสงค์

- เพื่อให้มีการควบคุมการถ่ายโอนและแลกเปลี่ยนข้อมูลสารสนเทศ ป้องกันการรั่วไหล หรือมีการแก้ไขข้อมูล โดยที่ไม่ได้รับอนุญาต รวมถึงการป้องกันสื่อบันทึกข้อมูลให้มีความปลอดภัยเป็นไปตามข้อกำหนด

ผู้รับผิดชอบ

- ผู้บังคับบัญชา
- เจ้าของข้อมูล
- ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

- หมวดที่ 9 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)

แนวปฏิบัติ

1. ผู้บังคับบัญชา ต้องควบคุมให้มีการจัดทำนโยบาย และขั้นตอนการปฏิบัติเพื่อป้องกันข้อมูลสารสนเทศที่มีการสื่อสาร หรือแลกเปลี่ยนผ่านระบบสารสนเทศให้เหมาะสมตามระดับชั้นความลับข้อมูลสารสนเทศตามชั้นตอนที่ รพม. กำหนด
2. ผู้บังคับบัญชา และเจ้าของข้อมูล ต้องควบคุมให้มีการจัดทำข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศระหว่างองค์กรกับบุคคลหรือหน่วยงานภายนอก
3. ผู้ดูแลระบบ ต้องมีการป้องกันข้อมูลสารสนเทศที่มีการสื่อสารกันผ่านข้อมูลอิเล็กทรอนิกส์ (Electronic messaging) เช่น จดหมายอิเล็กทรอนิกส์ (E-mail) หรือ Instant messaging ด้วยวิธีการหรือมาตรการที่เหมาะสม
4. ผู้ดูแลระบบ ต้องป้องกันข้อมูลสารสนเทศที่มีการแลกเปลี่ยนในการทำพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce) ผ่านเครือข่ายคอมพิวเตอร์สาธารณะ เพื่อมิให้มีการฉ้อโกง ละเมิดสัญญา หรือมีการรั่วไหลหรือข้อมูลสารสนเทศถูกแก้ไขโดยมิได้รับอนุญาต
5. ผู้ดูแลระบบ ต้องป้องกันข้อมูลสารสนเทศที่มีการสื่อสาร หรือแลกเปลี่ยนในการทำธุรกรรมทางออนไลน์ (Online transaction) เพื่อมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ ส่งข้อมูลไปผิดที่ การรั่วไหลของข้อมูล ข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ หรือถูกส่งซ้ำโดยมิได้รับอนุญาต
6. ผู้ดูแลระบบ ต้องควบคุมการรับส่งข้อมูลสารสนเทศเพื่อป้องกันความผิดพลาด ดังนี้
 - 6.1 ความไม่สมบูรณ์ของข้อมูลสารสนเทศที่รับ-ส่ง
 - 6.2 การส่งข้อมูลสารสนเทศผิดจุดหมายปลายทาง
 - 6.3 การเปลี่ยนแปลงข้อมูลสารสนเทศโดยมิได้รับอนุญาต
 - 6.4 การเปิดเผยข้อมูลสารสนเทศโดยมิได้รับอนุญาต
 - 6.5 การเข้าถึงข้อมูลสารสนเทศโดยมิได้รับอนุญาต
 - 6.6 การนำข้อมูลสารสนเทศกลับมาใช้ใหม่โดยมิได้รับอนุญาต
7. เจ้าของข้อมูล และผู้ดูแลระบบ ต้องมีการป้องกันข้อมูลสารสนเทศที่มีการเผยแพร่ต่อสาธารณชนมิให้มีการแก้ไขเปลี่ยนแปลงโดยมิได้รับอนุญาต เพื่อรักษาความถูกต้องครบถ้วนของข้อมูลสารสนเทศ

ส่วนที่ 15 การควบคุมการเข้ารหัส

วัตถุประสงค์

- เพื่อให้มีการเข้ารหัสข้อมูลอย่างเหมาะสมและมีประสิทธิภาพในการปกป้องความลับ ป้องกัน การปลอมแปลงข้อมูล และควบคุมความถูกต้องของข้อมูล

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- เจ้าของข้อมูล
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 6 การเข้ารหัสข้อมูล (Cryptography)

แนวปฏิบัติ

1. เจ้าของข้อมูล ต้องเข้ารหัส หรือการใส่รหัสผ่านข้อมูลอิเล็กทรอนิกส์ขององค์กรตามระดับชั้นความลับเพื่อป้องกันผู้ไม่มีสิทธิเข้าถึง ตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และตามขั้นตอนที่ รพม. กำหนด
2. เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ใช้งานต้องปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 ในการนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับจะต้องใช้วิธีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล
3. ผู้ดูแลระบบ ต้องใช้วิธีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล หลีกเลี่ยงการใช้รูปแบบการเข้ารหัสที่พัฒนาขึ้นเอง เพื่อให้มั่นใจว่าขั้นตอนวิธี (Algorithm) ที่ใช้ในการเข้ารหัสนั้นมีความมั่นคงปลอดภัย ดังนี้

ประเภทกุญแจ / วิธีการเข้ารหัส	เกณฑ์ขั้นต่ำ	ความยาวกุญแจ (อย่างน้อย)
กุญแจแบบสมมาตร (Symmetric)	AES	256 bits
กุญแจแบบอสมมาตร (Asymmetric)	RSA	1024 bits
การ Hashing	SHA-256	256 bits

4. ผู้ดูแลระบบ ต้องมีการทบทวนขั้นตอนวิธี (Algorithm) และความยาวของกุญแจที่เข้ารหัสอย่างน้อยปีละ 1 ครั้ง เพื่อให้ยังสามารถรักษาไว้ซึ่งความมั่นคงปลอดภัย
5. ผู้ดูแลระบบ ต้องกำหนดให้มีการบริหารจัดการกุญแจที่ใช้ในการเข้ารหัส ดังนี้
 - 5.1 การสร้างกุญแจรหัสควรกระทำในสถานที่ที่มีมาตรการป้องกันความปลอดภัย
 - 5.2 เมื่อมีการสร้างกุญแจรหัสที่เป็นกุญแจลับ (Private key) ควรส่งมอบให้กับเจ้าของกุญแจโดยตรง โดยวิธีการที่ปลอดภัย
 - 5.3 ควรจัดให้มีการเก็บบันทึก Log เพื่อการตรวจสอบสำหรับกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับการจัดการกุญแจรหัส

6. ผู้ใช้งาน ควรรักษาความปลอดภัยในการใช้งานกุญแจ ดังนี้
 - 6.1 เก็บกุญแจรหัสในสถานที่ที่ปลอดภัย เช่น ตู้นิรภัย หรือสื่อบันทึกที่ปลอดภัย และไม่มีใครสามารถเข้าถึงได้
 - 6.2 เมื่อมีการรับกุญแจสาธารณะ (Public key) มาใช้ ก่อนใช้งานจะต้องพิสูจน์ความถูกต้องของกุญแจสาธารณะ โดยสอบถามกับผู้ส่งหรือตรวจสอบกับผู้แทนในการรับรองความถูกต้องของกุญแจสาธารณะ (Certificate authority) ที่เชื่อถือได้เท่านั้น
 - 6.3 ควบคุมการใช้งานและจัดเก็บกุญแจให้สอดคล้องกับการรักษาความลับข้อมูลตามที่ รพม. กำหนด

ส่วนที่ 16

การนำอุปกรณ์ส่วนตัวมาใช้งาน (Bring your own device)

วัตถุประสงค์

- เพื่อควบคุมการนำอุปกรณ์ส่วนตัวมาเชื่อมต่อหรือเข้าถึงระบบสารสนเทศของ รพม. ที่ใช้ในการบริหารจัดการระบบสารสนเทศของ รพม. หรือปฏิบัติงานให้ รพม. ทั้งนี้เพื่อป้องกันภัยคุกคามที่อาจเกิดขึ้นกับระบบสารสนเทศของ รพม. รวมถึงเพื่อป้องกันไม่ให้ข้อมูลของ รพม. เกิดการรั่วไหล

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 2 อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากระยะไกล (Mobile devices and teleworking)

แนวปฏิบัติ

1. ผู้ดูแลระบบต้องกำหนดคุณสมบัติของระบบปฏิบัติการของอุปกรณ์ส่วนตัวที่อนุญาตให้นำมาเชื่อมต่อหรือเข้าถึงระบบงานสารสนเทศของ รพม. ได้ โดยต้องเป็นระบบปฏิบัติการที่ไม่ล้าสมัย (Obsolete operating system) และยังได้รับการสนับสนุนการใช้งานจากเจ้าของผลิตภัณฑ์
2. ผู้ดูแลระบบต้องตัดการเชื่อมต่อหากระบบปฏิบัติการของอุปกรณ์ส่วนตัวที่อนุญาตให้นำมาเชื่อมต่อหรือเข้าถึงระบบงานสารสนเทศของ รพม. เกิดการล้าสมัย (Obsolete operating system) หรือเจ้าของผลิตภัณฑ์ไม่สนับสนุนการใช้งานแล้ว
3. ผู้ดูแลระบบต้องมีมาตรการป้องกันมัลแวร์ และตรวจสอบการอัปเดต Patch เวอร์ชันของระบบปฏิบัติการที่เจ้าของผลิตภัณฑ์ยังให้การสนับสนุนการใช้งาน
4. ผู้ดูแลระบบต้องไม่อนุญาตให้อุปกรณ์ที่มีการปรับแต่งการเข้าถึงระบบปฏิบัติการ (rooted/jailbroken) มาเชื่อมต่อหรือเข้าถึงระบบสารสนเทศของ รพม.
5. ผู้ดูแลระบบต้องแบ่งแยกเครือข่ายของอุปกรณ์ส่วนตัวที่นำมาเชื่อมต่อหรือเข้าถึงระบบสารสนเทศของ รพม.
6. ผู้ใช้งานต้องไม่นำอุปกรณ์ส่วนตัวที่ติดตั้งแอปพลิเคชันนอก Official store มาเชื่อมต่อหรือเข้าถึงระบบงานสารสนเทศของ รพม.
7. ผู้ใช้งานต้องไม่นำอุปกรณ์ส่วนตัวที่ติดตั้งโปรแกรมละเมิดลิขสิทธิ์มาเชื่อมต่อหรือเข้าถึงระบบงานสารสนเทศของ รพม.
8. ผู้ใช้งานต้องอัปเดต Patch ของระบบปฏิบัติการที่อุปกรณ์ส่วนตัวให้เป็นเวอร์ชันล่าสุด รวมถึงต้องเป็นระบบปฏิบัติการที่เจ้าของผลิตภัณฑ์ยังให้การสนับสนุนการใช้งาน
9. ผู้ใช้งานต้องยืนยันตัวตนก่อนเข้าถึงระบบสารสนเทศของ รพม. ทุกครั้ง
10. ผู้ใช้งานต้องติดตั้ง Network Access Control agent (NAC agent) หรือ Mobile Device Management agent (MDM agent) ตามที่ รพม. กำหนด เพื่อควบคุมการใช้งานเครือข่ายและการเข้าถึงระบบสารสนเทศของ รพม.
11. กรณีอุปกรณ์ส่วนตัวสูญหายหรือถูกขโมยผู้ใช้งานต้องแจ้งผู้ดูแลระบบโดยเร็วที่สุด เพื่อจัดการข้อมูลที่จัดเก็บอยู่ในอุปกรณ์ส่วนตัวของผู้ใช้งาน

ภาคผนวก ข.

รายงานผลการบำรุงรักษา
ระบบติดตามความก้าวหน้าโครงการ (PPMS)
ประจำไตรมาสที่ (.....-.....)

สัญญาเลขที่

จัดทำโดย

บริษัท

รายงานผลการตรวจสอบระบบติดตามความก้าวหน้าโครงการ (PPMS)

วันที่ เดือน ปี พ.ศ.

PPMS Web Server (Server Name :

1. ตรวจสอบการทำงานของเครื่องเซิร์ฟเวอร์ (PPMS Web Server)

1.1 ตรวจสอบเวอร์ชันของระบบปฏิบัติการ

1.1.1 Windows Version

----- รูป -----

1.1.2 Windows Update

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

1.2 ตรวจสอบการใช้งานของ CPU

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

1.3 ตรวจสอบการใช้งานของ Memory

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

1.4 ตรวจสอบพื้นที่การใช้งานของ Hard disk

	4/2566	1/2567	2/2567	3/2567	4/2567
Drive C					
Drive D					

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

ศุภรณญา

1.5 ตรวจสอบรายละเอียดการเชื่อมต่อเครือข่าย

1.5.1 ตรวจสอบ IP address ของเครื่องคอมพิวเตอร์

----- รูป -----

1.5.2 ทดสอบการเชื่อมต่อเครือข่ายกับเครื่อง PPMS Database Server

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

1.6 ตรวจสอบ Log ของเครื่องเซิร์ฟเวอร์

1.6.1 Application log

----- รูป -----

1.6.2 Security log

----- รูป -----

1.6.3 System log

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

1.7 ตรวจสอบวันที่และเวลาของเครื่อง

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

2. ตรวจสอบการทำงานของ PPMS Application

2.1 ตรวจสอบการทำงานของ Service ของ Web server

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

2.2 ตรวจสอบ Version ของ PPMS Application

2.2.1 PPMS Production

Path ที่จัดเก็บ :

	4/2566	1/2567	2/2567	3/2567	4/2567
version					

----- รูป -----

2.2.2 PPMS Test

Path ที่จัดเก็บ :

	4/2566	1/2567	2/2567	3/2567	4/2567
version					

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

2.3 ตรวจสอบการสำรองข้อมูลของ PPMS Application

Path ที่จัดเก็บ :

	4/2566	1/2567	2/2567	3/2567	4/2567
Folder Size					

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

2.4 ตรวจสอบ Log ของ PPMS Application

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

PPMS Database Server (Server Name :)

3. ตรวจสอบการทำงานของเครื่องเซิร์ฟเวอร์ (PPMS Database Server)

3.1 ตรวจสอบเวอร์ชันของระบบปฏิบัติการ

3.1.1 Windows Version

----- รูป -----

3.1.2 Windows Update

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

3.2 ตรวจสอบการใช้งานของ CPU

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

3.3 ตรวจสอบการใช้งานของ Memory

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

3.4 ตรวจสอบพื้นที่การใช้งานของ Hard disk

	4/2566	1/2567	2/2567	3/2567	4/2567
Drive C					
Drive D					

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

3.5 ตรวจสอบรายละเอียดการเชื่อมต่อเครือข่าย

3.5.1 ตรวจสอบ IP address ของเครื่องคอมพิวเตอร์

----- รูป -----

3.5.2 ทดสอบการเชื่อมต่อเครือข่ายกับเครื่อง PPMS Web Server

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

3.6 ตรวจสอบ Log ของเครื่องเซิร์ฟเวอร์

3.6.1 Application log

----- รูป -----

3.6.2 Security log

----- รูป -----

3.6.3 System log

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

3.7 ตรวจสอบวันที่และเวลาของเครื่อง

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

4. ตรวจสอบการทำงานของ PPMS Database

4.1 ตรวจสอบการทำงานของ Service ของ PPMS Database

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

4.2 ตรวจสอบการใช้พื้นที่ของฐานข้อมูล

4.2.1 PPMS Production

Database file name :

Database log name :

	4/2566	1/2567	2/2567	3/2567	4/2567
Database file size					
Database log size					

----- รูป -----

4.2.2 PPMS Test

Database file name :

Database log name :

	4/2566	1/2567	2/2567	3/2567	4/2567
Database file size					
Database log size					

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

4.3 ตรวจสอบการสำรองข้อมูลของ PPMS Database

Path ที่จัดเก็บ :

	4/2566	1/2567	2/2567	3/2567	4/2567
File size					

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

4.4 ตรวจสอบการทำงานของ JOB

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

5. ตรวจสอบการทำงานของระบบติดตามความก้าวหน้าโครงการ (PPMS)

5.1 ตรวจสอบการเข้าใช้งาน (Authentication Testing)

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

5.2 ตรวจสอบประสิทธิภาพการให้บริการในการตอบสนองการเรียกใช้งาน (Response Time) *

หมายเหตุ:

* ตรวจสอบระยะเวลาในการตอบสนองการเรียกใช้งานไม่ควรเกิน 4 วินาที (อย่างน้อย 3 หน้าจอ)

----- รูป -----

Response Time วินาที

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

5.3 ตรวจสอบการหมดเวลาใช้งานระบบสารสนเทศ (Session Time - Out)

ระบบติดตามความก้าวหน้าโครงการ (PPMS) (15 นาที หรือตามที่ระบบฯ กำหนด)

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

5.4 ตรวจสอบการออกรายงาน

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

ลงชื่อ ผู้ตรวจสอบ

()

วันที่

ศพธธ

รายงานการตรวจสอบสิทธิการเข้าถึงระบบ (Role Matrix) ระบบติดตามความก้าวหน้าโครงการ (PPMS)

การรถไฟฯขนส่งมวลชนแห่งประเทศไทย

ประจำไตรมาสที่ (ตั้งแต่วันที่ ถึงวันที่

ที่	ชื่อ - สกุล	Application Server				Database Server				Application				DBMS			
		Super Administrator	Administrator	Super User	User	การเข้าถึงเอกสาร (F/C/R/U/D)	Super Administrator	Administrator	Super User	User	การเข้าถึงเอกสาร (F/C/R/U/D)	Super Administrator	Administrator	Super User	User	การเข้าถึงเอกสาร (F/C/R/U/D)	

หมายเหตุ : การเข้าถึงเอกสาร F : Full, C : Create, R : Read, U : Update, D : Delete

* Super Administrator : ผู้มีสิทธิ์สามารถกำหนดสิทธิ์ และบริหารจัดการข้อมูลเครื่องเซิร์ฟเวอร์ ภายใต้ Domain ได้ (Domain Admin)

* Administrator : ผู้มีสิทธิ์สามารถกำหนดสิทธิ์ และบริหารจัดการข้อมูลเครื่องเซิร์ฟเวอร์ที่มีสิทธิ์ได้ (Local Admin) รวมทั้งกำหนดสิทธิ์ให้กับผู้ใช้งานระบบสารสนเทศต่าง ๆ ได้

* Super User : ผู้มีสิทธิ์สามารถจัดการข้อมูลภายในระบบสารสนเทศต่าง ๆ ได้

* User : ผู้ใช้งานทั่วไป เข้าถึง เรียกดูข้อมูลภายในระบบงานสารสนเทศต่าง ๆ ได้

รายงานสรุปการแจ้งปัญหาและการแก้ไขระบบติดตามความก้าวหน้าโครงการ (PPMS)

การรถไฟฯ ขอส่งมอบผลงานแห่งประเทศไทย

ประจำไตรมาสที่ (ตั้งแต่วันที่ ถึงวันที่)

ลำดับ	วันที่รับแจ้ง	เลขที่รับแจ้ง	ผู้แจ้ง	ช่องทาง การ รับแจ้ง	รายละเอียด	วันที่ดำเนินการ แล้วเสร็จ	ผลการ ดำเนินการ/ การแก้ไข	ผู้ดำเนินการแก้ไข	สถานะ

หมายเหตุ หากมีการปรับปรุงเวอร์ชันซอฟต์แวร์ให้ระบุเป็นช่องผลการดำเนินการ/การแก้ไขด้วย

รายงานผลการปิดช่องโหว่ระบบติดตามความก้าวหน้าโครงการ (PPMS)

การรถไฟฟ้ามหานครแห่งประเทศไทย

ประจำไตรมาสที่ (ตั้งแต่วันที่ ถึงวันที่))

ลำดับ	วันที่พบ ช่องโหว่	หมายเลข ช่องโหว่	ชื่อช่องโหว่	รายละเอียด	ผลการดำเนินการ/ การแก้ไข/ ผลกระทบ	ผู้ดำเนินการแก้ไข	วันที่ ดำเนินการ แล้วเสร็จ	สถานะ

รายงานทะเบียนทรัพย์สิน (Asset Inventory) ระบบติดตามความก้าวหน้าโครงการ (PPMS)

การรถไฟฯขนส่งมวลชนแห่งประเทศไทย

ประจำไตรมาสที่ (ตั้งแต่วันที่ ถึงวันที่

ลำดับ	รายการทรัพย์สิน	End of Support	End of Life	กลุ่มทรัพย์สิน	ประเภททรัพย์สิน	Firmware/ Patch Version	สถานที่จัดเก็บ	ผู้บันทึก

PPMS

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและรายละเอียดค่าใช้จ่าย
การจัดซื้อจัดจ้างที่มีใ้ใช้งานก่อสร้าง

ชื่อโครงการ	จ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ประจำปีงบประมาณ 2567
1. หน่วยงานเจ้าของโครงการ	ฝ่ายเทคโนโลยีสารสนเทศ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
2. วงเงินงบประมาณที่ได้รับจัดสรร	1,350,000.00 บาท (หนึ่งล้านสามแสนห้าหมื่นบาทถ้วน)
3. วันที่กำหนดราคากลาง (ราคาอ้างอิง) ณ วันที่ เป็นเงิน	23 มิถุนายน 2566 650,000.00 บาท (หกแสนห้าหมื่นบาทถ้วน) (รวมภาษีมูลค่าเพิ่ม)
4. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)	ราคาที่ได้มาจากการสืบราคาจากท้องตลาด โดยสืบราคาจากผู้รับจ้างรายเดิม (บริษัท เอทูพี โซลูชั่น จำกัด)
5. รายชื่อผู้รับผิดชอบกำหนดราคากลาง	นางสาวสุพรรณษา นิลสมบูรณ์ โปรแกรมเมอร์ ระดับ 7

สุพรรณษา

บริษัท เอที โซลูชั่น จำกัด (สนญ.)

503/5 อาคารเค.เอส.แอล ทาวเวอร์ ชั้น 4 ถนนศรีอยุธยา
 แขวงถนนพญาไท เขตราชเทวี กรุงเทพมหานคร 10400
 โทรศัพท์ 02-065-5448, 086-375-5448
 เลขประจำตัวผู้เสียภาษี 0105555029721



ใบเสนอราคา

รหัส	018	วันที่	23/06/2566
นามลูกค้า	การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย	เลขที่ใบเสนอราคา	SO50100
ที่อยู่	175 ถ.พระราม 9 แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพฯ 10310	ผู้เสนอราคา	ยุทธศักดิ์
หมายเหตุ	Tax Id.0994000165706	เงื่อนไขการชำระเงิน	
		วันที่ครบกำหนด	

บริษัทฯ มีความยินดีขอเสนอราคา และ รายละเอียดของสินค้าตามรายการดังต่อไปนี้
 We take pleasure in quoting the following products with price and specification

รหัสสินค้า Code	รายละเอียด Description	จำนวน Qty.	ราคาต่อหน่วย Unit	ส่วนลด Discount	จำนวนเงิน Amount
100035	จ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ของ รฟม. ประจำปีงบประมาณ พ.ศ.2567 (ตุลาคม พ.ศ.2566 - กันยายน พ.ศ.2567)	1 ระบบ	650,000.00		650,000.00

บาท หกแสนห้าหมื่นบาทถ้วน		รวมเป็นเงิน	607,476.64
- กำหนดยืนยันราคา 90 วันนับตั้งแต่วันที่ระบุในใบเสนอราคาฉบับนี้		ภาษีมูลค่าเพิ่ม 7.00%	42,523.36
- กรณาลงนามในช่อง "ผู้สั่งซื้อสินค้า" พร้อมประทับตรา (ถ้ามี) เพื่อยืนยันการสั่งซื้อ		ยอดเงินสุทธิ	650,000.00
- โอนเงินผ่าน ธนาคารไทยพาณิชย์ เลขที่ 071-285235-3 ชื่อบัญชี บริษัท เอที โซลูชั่น จำกัด			

ผู้สั่งซื้อสินค้า	ผู้เสนอราคา	ผู้ตรวจสอบ	ผู้อนุมัติ
วันที่/..../.....	 วันที่ 23 6 2566	วันที่/..../.....	วันที่/..../.....

ยุทธศักดิ์

ขอบเขตของงานจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ(Project Progress Monitoring System: PPMS)

ประจำปีงบประมาณ 2567

1. ความเป็นมา

การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย (รฟม.) ได้มีระบบติดตามความก้าวหน้าโครงการ (Project Progress Monitoring System: PPMS) เพื่อใช้สำหรับรองรับการติดตามความก้าวหน้าการก่อสร้างโครงการรถไฟฟ้าของ รฟม. โดยระบบฯ ดังกล่าว จะสิ้นสุดระยะเวลาการรับประกัน ในวันที่ 30 กันยายน 2566 ทั้งนี้ เพื่อให้ระบบติดตามความก้าวหน้าโครงการ (PPMS) สามารถใช้งานได้อย่างต่อเนื่องและมีประสิทธิภาพ รฟม. จึงจำเป็นต้องจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ต่อไป

2. วัตถุประสงค์

รฟม. มีความประสงค์จะจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) เพื่อให้ระบบฯ สามารถใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และตอบสนองความต้องการของผู้ใช้งานในองค์กรได้ดียิ่งขึ้น

3. คุณสมบัติของผู้ยื่นข้อเสนอ

- 3.1 มีความสามารถตามกฎหมาย
- 3.2 ไม่เป็นบุคคลล้มละลาย
- 3.3 ไม่อยู่ระหว่างเลิกกิจการ
- 3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง
- 3.5 ผู้รับจ้างต้องไม่เป็นผู้ที่ถูกระงับชื่อไว้ในบัญชีรายชื่อผู้ทำงานตามระเบียบของทางราชการและได้แจ้งเวียนชื่อแล้ว หรือไม่เป็นผู้ที่ได้รับผลของการสั่งให้นิติบุคคลหรือบุคคลอื่นเป็นผู้ทำงานตามระเบียบของทางราชการ
- 3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ กำหนดในราชกิจจานุเบกษา
- 3.7 ผู้รับจ้างต้องเป็นนิติบุคคลซึ่งมีอาชีพในการประกอบธุรกิจงานด้านการพัฒนาระบบสารสนเทศหรือประเภทเดียวกับงานที่ประกาศ
- 3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย ณ วันคัดเลือก หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรม ในการคัดเลือกครั้งนี้
- 3.9 ผู้รับจ้างต้องไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้เสนอราคาได้มีคำสั่งให้สละสิทธิ์ความคุ้มกันเช่นนั้น
- 3.10 ผู้ยื่นข้อเสนอต้องลงทะเบียนในระบบจัดซื้อจัดจ้างด้วยวิธีการอิเล็กทรอนิกส์ (Electronic Government Procurement : e - GP) ของกรมบัญชีกลาง

- 3.11 ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการเป็นไปตามเงื่อนไขข้อ 1.1 - 1.2 ของหนังสือคณะกรรมการวินิจฉัยปัญหาการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ กรมบัญชีกลาง ด่วนที่สุด ที่ กค(กวจ) 0405.2/ว124 ลงวันที่ 1 มีนาคม 2566 เรื่อง แนวทางปฏิบัติในการเร่งรัดการปฏิบัติงานตามสัญญาและการกำหนดคุณสมบัติของผู้มีสิทธิยื่นข้อเสนอ

4. ขอบเขตของงานจ้างบำรุงรักษา

- 4.1 ผู้รับจ้างดำเนินการดูแล ตรวจสอบ และบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ให้สามารถใช้งานได้อย่างต่อเนื่องตลอดระยะเวลาการบำรุงรักษา
- 4.2 ผู้รับจ้างต้องมีเจ้าหน้าที่ที่มีประสบการณ์และความเชี่ยวชาญ เพื่อบริการให้คำปรึกษา และตอบปัญหาทางโทรศัพท์ โทรศัพท์เคลื่อนที่ โทรสาร ไปรษณีย์อิเล็กทรอนิกส์ (E-Mail) หรือ Line ในวันและเวลาทำการของ รพม. (จันทร์ - ศุกร์ ระหว่างเวลา 08.00 น. - 17.00 น.) เมื่อได้รับแจ้งปัญหา จะต้องตอบปัญหาขั้นต้นภายใน 1 ชั่วโมง หลังจากได้รับแจ้ง โดยจะต้องดำเนินการตรวจสอบและแก้ไขให้แล้วเสร็จภายใน 5 วันทำการ นับแต่เวลาที่ผู้ว่าจ้างได้แจ้งข้อขัดข้อง ยกเว้นในกรณีที่การขัดข้องนั้น เป็นปัญหาที่มีความซับซ้อน ผู้รับจ้างจะต้องจัดทำแผนการดำเนินงาน พร้อมทั้งชี้แจงรายละเอียดของปัญหา และการแก้ปัญหาฯ ดังกล่าวจัดส่งให้แก่คณะกรรมการตรวจรับพัสดุฯ พิจารณาให้ความเห็นชอบ
- 4.3 ผู้รับจ้างจะต้องดำเนินการแก้ไขปัญหาข้อผิดพลาดของซอฟต์แวร์ (Debugging) เมื่อผู้ใช้ไม่สามารถใช้งานได้
- 4.4 ผู้รับจ้างต้องจัดให้มีเจ้าหน้าที่ ผู้ที่มีความรู้ ความชำนาญระบบติดตามความก้าวหน้าโครงการ (PPMS) เข้าดูแลรักษาระบบ (Preventive Maintenance: PM) ไตรมาสละ 1 ครั้ง เป็นอย่างน้อย พร้อมทั้งจัดทำรายงานผลการตรวจสอบระบบติดตามความก้าวหน้าโครงการ (PPMS) ตามที่ รพม. กำหนด
- 4.5 ในกรณีที่ รพม. มีความประสงค์จะเปลี่ยนแปลงเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์คอมพิวเตอร์อื่น ๆ สำหรับระบบติดตามความก้าวหน้าโครงการ (PPMS) ใหม่ ผู้รับจ้างจะต้องดำเนินการโอนย้ายระบบฯ ให้และเมื่อโอนย้ายแล้ว ระบบฯ จะต้องสามารถใช้งานได้ดังเดิม โดยไม่ก่อให้เกิดความเสียหายในการปฏิบัติงานของ รพม.
- 4.6 ในกรณีที่เครื่องคอมพิวเตอร์แม่ข่ายของ รพม. ไม่สามารถใช้งานได้ มีความจำเป็นต้องใช้เครื่องคอมพิวเตอร์แม่ข่ายที่ศูนย์คอมพิวเตอร์สำรอง (DR - site) ผู้รับจ้างจะต้องดำเนินการติดตั้งระบบติดตามความก้าวหน้าโครงการ (PPMS) พร้อมให้คำแนะนำหรือคำปรึกษาเกี่ยวกับปัญหาที่เกิดขึ้นให้สามารถใช้งานได้ โดยไม่มีค่าใช้จ่ายเพิ่มเติม
- 4.7 หากมีการปรับปรุงระบบติดตามความก้าวหน้าโครงการ (PPMS) เป็นเวอร์ชันใหม่ ผู้รับจ้างจะต้องนำมาปรับปรุงให้ รพม. โดยไม่มีค่าใช้จ่ายเพิ่มเติม
- 4.8 การบริการบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ให้ครอบคลุมถึงค่าแรงงาน ค่าให้คำปรึกษาที่เกี่ยวข้อง ค่าใช้จ่ายในการเดินทาง ค่าวัสดุอุปกรณ์ที่จำเป็น และค่าใช้จ่ายอื่นใดทั้งหลายทั้งปวงที่เกี่ยวข้องกับการบำรุงรักษา โดยที่ รพม. ไม่ต้องเสียค่าใช้จ่ายใด ๆ ทั้งสิ้นเพิ่มเติมจากราคาค่าจ้างในงานที่กำหนดไว้ในสัญญา

- 4.9 การติดตามปัญหา ความก้าวหน้าและแก้ไขปัญหา เมื่อดำเนินการเสร็จเรียบร้อยแล้ว ผู้รับจ้างต้องแจ้งผลให้ผู้แจ้งทราบ และรวบรวมเป็นรายงานสรุปการแจ้งปัญหาและการแก้ไขระบบติดตามความก้าวหน้าโครงการ (PPMS) ตามที่ รฟม. กำหนด
- 4.10 เมื่อผู้รับจ้างจะเข้าดำเนินการเพื่อแก้ไขปัญหาดังกล่าว จะต้องแจ้งให้เจ้าหน้าที่ผู้รับผิดชอบของ รฟม. ทราบล่วงหน้า
- 4.11 การปรับปรุงแก้ไข Source Code ส่วนใด ๆ ของระบบติดตามความก้าวหน้าโครงการ (PPMS) ให้ผู้รับจ้างจัดทำรายละเอียดการแก้ไข (Log statement) ที่มีรายละเอียดครบถ้วน เข้าใจง่าย และจัดส่งให้แก่ รฟม. เพื่อใช้สำหรับอ้างอิงการแก้ไขระบบฯ ในอนาคต
- 4.12 Source code ที่ได้ปรับปรุงแก้ไข รวมทั้งรายงานหรือเอกสารใด ๆ ที่ผู้รับจ้างได้ทำขึ้น อันเนื่องมาจากการปฏิบัติงานตามสัญญาฯ ให้ตกเป็นกรรมสิทธิ์และลิขสิทธิ์ของ รฟม. ทั้งหมดอย่างไรก็ตาม ผู้รับจ้างอาจเก็บสำเนารายงานและเอกสารอื่นดังกล่าวไว้ เพื่อเป็นประวัติการทำงานของผู้รับจ้างเองได้
- 4.13 การปรับปรุงแก้ไข Source Code ส่วนใด ๆ ผู้รับจ้างต้องแก้ไขและออกแบบระบบให้ปลอดภัยตามมาตรฐาน Open Web Application Security Project (OWASP) Top 10 ล่าสุด หรือมาตรฐาน Common Weakness Enumeration (CWE) Top 25 ล่าสุด ณ ปีที่ส่งมอบงาน นับถัดจากวันที่ลงนามในสัญญา หรือมาตรฐานที่ยอมรับในสากล หรือกำหนดซอฟต์แวร์ให้เป็นเวอร์ชันล่าสุดที่ได้รับการอัปเดตแล้ว
- 4.14 ผู้รับจ้างต้องจัดทำเอกสาร Version Control ของระบบติดตามความก้าวหน้าโครงการ (PPMS) และจัดส่งให้แก่ รฟม. ทราบทุกครั้ง ก่อนนำ Source Code ที่ได้ปรับปรุงแก้ไข ไป Deploy ขึ้นระบบจริง เพื่อใช้สำหรับควบคุมและอ้างอิงการแก้ไขระบบ
- 4.15 การปรับปรุงแก้ไข Source Code ส่วนใด ๆ ผู้รับจ้างต้องตรวจสอบความมั่นคงปลอดภัยของ Source Code (Source Code Review) ตามมาตรฐานที่ รฟม. กำหนด
- 4.16 การปรับปรุงแก้ไข Source Code ส่วนใด ๆ ผู้รับจ้างต้องแก้ไขและออกแบบระบบให้มีการตรวจสอบความถูกต้องของข้อมูลนำเข้า (Input Validation) ก่อนการบันทึกและ/หรือประมวลผลข้อมูล รวมทั้งตรวจสอบข้อมูลที่ส่งออกจากระบบ (Output Validation) เพื่อป้องกันการแสดงผลหรือการประมวลผลข้อมูลที่ไม่เหมาะสม
- 4.17 ผู้รับจ้างและผู้ปฏิบัติงานของผู้รับจ้างจะต้องไม่เปิดเผยความลับของข้อมูลหรือข้อมูลอื่นใดทั้งหมดหรือบางส่วนที่ได้รับหรือรับรู้มาจาก รฟม. ให้ผู้อื่นทราบโดยมิได้รับความยินยอมจาก รฟม. และหากมีการนำข้อมูลใด ๆ ออกจาก รฟม. ผู้รับจ้างฯ จะต้องทำลายข้อมูลทั้งที่เป็นเอกสาร หรือข้อมูลในรูปแบบอิเล็กทรอนิกส์ที่สิ้นสุดสัญญาจ้าง โดยผู้รับจ้างฯ ต้องลงนามในเอกสารข้อตกลงในการไม่เปิดเผยข้อมูล (Non - Disclosure Agreement) และ รฟม. ขอสงวนสิทธิ์ในการเรียกร้องค่าเสียหายอันเนื่องมาจากการละเมิดข้อตกลงดังกล่าว
- 4.18 ผู้รับจ้างต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รฟม. ที่ปรากฏดัง ภาคผนวก ก.
- 4.19 ผู้รับจ้างจะต้องส่งบุคลากรเข้าร่วมการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness) เพื่อสร้างความตระหนักที่เหมาะสม ทบทวนนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและขั้นตอนปฏิบัติของ รฟม.

- 4.20 ระบบที่มีลักษณะเป็น Web Based Application ต้องใช้งานผ่านโปรโตคอล Hypertext Transfer Protocol Secure (HTTPS) โดยใช้ใบรับรอง SSL Certificate ที่ รฟม. กำหนด ทั้งนี้ หากใบรับรอง SSL Certificate หมดอายุ ผู้รับจ้างต้องปรับปรุงให้ระบบฯ ใช้งานผ่าน SSL Certificate ที่ รฟม. ต่ออายุแล้วต่อไป
- 4.21 ผู้รับจ้างต้องปิดช่องโหว่ (Hardening) ของระบบติดตามความก้าวหน้าโครงการ (PPMS) และซอฟต์แวร์ที่ใช้ในการพัฒนา หากซอฟต์แวร์นั้น ๆ มีการประกาศช่องโหว่ รวมทั้งช่องโหว่ที่ รฟม. ตรวจพบ พร้อมทั้งจัดทำรายงานผลการปิดช่องโหว่ระบบติดตามความก้าวหน้าโครงการ (PPMS) ตามที่ รฟม. กำหนด โดยที่ รฟม. ไม่ต้องเสียค่าใช้จ่ายใด ๆ เพิ่มเติมจากราคาค่าจ้างงานตามที่กำหนดไว้ตามสัญญา ทั้งนี้หากผู้รับจ้างไม่สามารถปิดช่องโหว่ให้แล้วเสร็จภายในระยะเวลาการรับประกัน จะต้องจัดทำแผนการดำเนินงานปิดช่องโหว่ ซึ่งระบุรายละเอียดและสาเหตุที่ไม่สามารถปิดช่องโหว่ภายในระยะเวลาการรับประกัน พร้อมทั้งจัดส่งให้คณะกรรมการตรวจรับพัสดุฯ พิจารณาให้ความเห็นชอบ
- 4.22 การติดตามความคืบหน้าการปิดช่องโหว่ เมื่อดำเนินการเสร็จเรียบร้อยแล้ว ผู้รับจ้างต้องแจ้งผลให้ผู้แจ้งทราบ และรวบรวมเป็นรายงานผลการปิดช่องโหว่ระบบติดตามความก้าวหน้าโครงการ (PPMS) ตามที่ รฟม. กำหนด
- 4.23 ผู้รับจ้างจะต้อง ทบทวน/ ปรับปรุง คู่มือการใช้งานระบบติดตามความก้าวหน้าโครงการ (PPMS) และจัดส่งให้แก่ รฟม. เมื่อมีการปรับปรุงระบบฯ ดังกล่าว โดยไม่มีค่าใช้จ่ายเพิ่มเติม
- 4.24 ผู้รับจ้างต้องจัดส่งรายงานผลการบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ให้แก่ รฟม. เพื่อทราบ ทุกสิ้นไตรมาส โดยส่งมอบภายในวันที่ 15 ของไตรมาสถัดไป (ภาคผนวก ข.) ซึ่งประกอบด้วย
- 1) รายงานผลการตรวจสอบระบบติดตามความก้าวหน้าโครงการ (PPMS)
 - 2) รายงานการตรวจสอบสิทธิการเข้าถึงระบบ (Role Matrix)
 - 3) รายงานสรุปการแจ้งปัญหาและการแก้ไขระบบติดตามความก้าวหน้าโครงการ (PPMS)
 - 4) รายงานผลการปิดช่องโหว่ระบบติดตามความก้าวหน้าโครงการ (PPMS) (หากมี)
 - 5) รายงานทะเบียนทรัพย์สิน (Asset Inventory)
- 4.25 ผู้รับจ้างจะต้องไม่เอางานทั้งหมดหรือแต่บางส่วนไปจ้างช่วงอีกทอดหนึ่ง เว้นแต่การจ้างช่วงงาน แต่บางส่วนที่ได้รับอนุญาตเป็นหนังสือจาก รฟม. แล้ว การที่ รฟม. ได้อนุญาตให้จ้างช่วงงานแต่บางส่วนดังกล่าวนี้ไม่เป็นเหตุให้ผู้รับจ้างหลุดพ้นจากความรับผิดชอบหรือพันธหน้าที่ และผู้รับจ้างจะยังคงต้องรับผิดชอบในความผิดและความประมาทเลินเล่อของผู้รับจ้างช่วง หรือของตัวแทนหรือลูกจ้างของผู้รับจ้างช่วงนั้นทุกประการ (หากมี)

5. กำหนดเวลาส่งมอบพัสดุ

นับตั้งแต่วันที่ 1 ตุลาคม 2566 – วันที่ 30 กันยายน 2567

6. หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

ในการพิจารณาผลการคัดเลือกข้อเสนอการจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ครั้งนี้ รฟม. จะพิจารณาคัดเลือกโดยใช้หลักเกณฑ์ **ราคารวม** ที่เป็นราคาต่ำสุด อยู่ในวงเงินงบประมาณ และเป็นผู้มีคุณสมบัติครบถ้วน ถูกต้อง ตรงตามรายละเอียดและเงื่อนไขที่ รฟม. กำหนด

7. วงเงินงบประมาณ/วงเงินที่ได้รับจัดสรร2

วงเงินสำหรับการจัดการจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ประจำปีงบประมาณ 2567 เป็นจำนวนทั้งสิ้น 1,350,000.00 บาท (หนึ่งล้านสามแสนห้าหมื่นบาทถ้วน) รวมภาษีมูลค่าเพิ่มตลอดจนภาษีอากรอื่น ๆ และค่าใช้จ่ายทั้งปวงแล้ว

8. งวดงานและการจ่ายเงิน

รพม. จะชำระเงินค่าจ้างงานให้แก่ผู้รับจ้าง โดยแบ่งจ่ายเป็น 4 งวด เป็นจำนวนเงินเท่ากัน (รวมภาษีมูลค่าเพิ่ม) ซึ่งแต่ละงวดจะจ่ายทุก ๆ สิ้นไตรมาส หลังจาก รพม. ได้รับรายงานผลการบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) และคณะกรรมการตรวจรับพัสดุฯ ได้มีการตรวจรับงานแต่ละงวดเรียบร้อยแล้ว

9. อัตราค่าปรับ2

ในกรณีที่ผู้ใช้งานไม่สามารถใช้งานระบบติดตามความก้าวหน้าโครงการ (PPMS) ได้ ผู้รับจ้างต้องดำเนินการตรวจสอบและแก้ไขให้แล้วเสร็จภายใน 5 วันทำการ นับแต่เวลาที่ผู้ว่าจ้างได้แจ้งข้อขัดข้องให้ผู้รับจ้างทราบทางโทรศัพท์ โทรศัพท์เคลื่อนที่ โทรสาร ไปรษณีย์อิเล็กทรอนิกส์ (E-Mail) หรือ Line ในวันและเวลาทำการของ รพม. (จันทร์ - ศุกร์ ระหว่างเวลา 08.00 น. - 17.00 น.) ยกเว้นในกรณีที่การขัดข้องนั้นเป็นปัญหาที่มีความซับซ้อน ผู้รับจ้างจะต้องจัดทำแผนการดำเนินงานจัดส่งให้แก่คณะกรรมการตรวจรับพัสดุฯ พิจารณาให้ความเห็นชอบ ทั้งนี้หากไม่สามารถดำเนินการแก้ไขได้แล้วเสร็จตามแผนฯ (ภายใน 5 วันทำการ หรือตามที่คณะกรรมการตรวจรับพัสดุฯ ได้ให้ความเห็นชอบแล้วแต่กรณี) ผู้รับจ้างจะต้องเสียค่าปรับเป็นรายวันในอัตราร้อยละ 1,500.00 บาท (หนึ่งพันห้าร้อยบาทถ้วน) เฉพาะของวันให้คิดเป็น 1 วัน

2

2

2

2

2

2

2

ภาคผนวก ก.2



การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

MASS RAPID TRANSIT AUTHORITY OF THAILAND

รัฐวิสาหกิจภายใต้กำกับของรัฐมนตรีว่าการกระทรวงคมนาคม

A STATE ENTERPRISE UNDER SUPERVISION OF MINISTER OF TRANSPORT

ประกาศการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (ฉบับปรับปรุงครั้งที่ 11)

ด้วยพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 มาตรา 5 กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ มีความมั่นคงปลอดภัยและเชื่อถือได้ จึงส่งผลให้ระบบเทคโนโลยีสารสนเทศของการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย (รฟม.) ต้องมีการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศอย่างครบถ้วนเพื่อธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) และความน่าเชื่อถือ (Reliability)

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ 2) พ.ศ. 2556 ข้อ 14 กำหนดให้หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer: CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

อาศัยอำนาจตามความในมาตรา 25 แห่งพระราชบัญญัติการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย พ.ศ. 2543 ผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย จึงออกประกาศการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ดังต่อไปนี้

1. วัตถุประสงค์และขอบเขต

เพื่อให้การใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาและลดผลกระทบจากการใช้งานระบบเทคโนโลยีสารสนเทศ ในลักษณะที่ไม่ถูกต้องหรือจากการถูกคุกคามจากภัยต่าง ๆ จึงได้กำหนดนโยบายเพื่อควบคุมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ดังนี้

1.1 การเข้าถึงหรือควบคุมการใช้งานสารสนเทศครอบคลุม 4 ด้าน คือ

1.1.1 การเข้าถึงระบบสารสนเทศ (Access control) ต้องตรวจสอบการอนุมัติสิทธิ์การเข้าถึงระบบและกำหนดรหัสผ่าน การลงทะเบียนผู้ใช้งานเพื่อให้ผู้ใช้ที่มีสิทธิ์ (User authentication) เท่านั้นที่สามารถ

สมบูรณ์

/เข้าถึง ...
สิทธิ์

เข้าถึงระบบได้ รวมถึงมีการเก็บบันทึกข้อมูลการเข้าถึงระบบ (Access log) และข้อมูลจราจรทางคอมพิวเตอร์ ทั้งนี้ การให้สิทธิ์การใช้งานระบบสารสนเทศนั้นต้องให้สิทธิ์ที่เหมาะสมและเพียงพอ (Need to know and Need to use)

1.1.2 การเข้าถึงระบบเครือข่าย (Network access control) ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ การรับ - ส่ง หรือการไหลเวียนข้อมูลหรือสารสนเทศจะต้องผ่านระบบการรักษาความปลอดภัยที่องค์กรจัดสรรไว้ เช่น Firewall IDS/IPS Proxy หรือการตรวจสอบไวรัสคอมพิวเตอร์ เป็นต้น เพื่อควบคุมและป้องกันภัยคุกคามอย่างเป็นระบบ

1.1.3 การเข้าถึงระบบปฏิบัติการ (Operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการ โดยไม่ได้รับอนุญาต โดยกำหนดให้มีการยืนยันตัวตนเพื่อระบุถึงตัวตนของผู้ใช้งาน รวมทั้งกำหนดให้มีการจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้ความมั่นคงปลอดภัยมากยิ่งขึ้น

1.1.4 การเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information access control) ต้องกำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศ โดยให้สิทธิ์เฉพาะระบบงานสารสนเทศที่ต้องปฏิบัติตามหน้าที่เท่านั้น รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานระบบสารสนเทศอย่างสม่ำเสมอ

1.2 มีระบบสารสนเทศและระบบสำรองที่อยู่ในสภาพพร้อมใช้งาน รวมทั้งมีแผนเตรียมพร้อมในกรณีฉุกเฉินหรือกรณีที่ไม่สามารถดำเนินการตามวิธีการทางอิเล็กทรอนิกส์ได้ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

1.3 ตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศอย่างสม่ำเสมอ

2. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รพม.

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รพม. ใช้แนวทางและกระบวนการอ้างอิงตาม 1) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานรัฐ พ.ศ. 2553 2) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555 และ 3) มาตรฐาน ISO/IEC 27001:2013 โดยแบ่งแนวปฏิบัติออกเป็น 16 ส่วนตามเอกสารแนบท้ายประกาศ ดังต่อไปนี้

2.1 นโยบายการบริหารจัดการความมั่นคงปลอดภัยสำหรับผู้บริหาร (ส่วนที่ 1)

2.2 ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร (ส่วนที่ 2)

2.3 การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (ส่วนที่ 3)

2.4 การจัดการทรัพย์สิน (ส่วนที่ 4)

2.5 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (ส่วนที่ 5)

2.6 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ (ส่วนที่ 6)

2.7 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (ส่วนที่ 7)

2.8 การควบคุมหน่วยงานภายนอกและผู้ใช้งาน (บุคคลภายนอก) เข้าถึงระบบเทคโนโลยีสารสนเทศ (ส่วนที่ 8)

2.9 การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ของ รพม. (ส่วนที่ 9)

2.10 การใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์ (ส่วนที่ 10)

- 2.11 การใช้งานจดหมายอิเล็กทรอนิกส์ (ส่วนที่ 11)
- 2.12 การสำรองข้อมูลและการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (ส่วนที่ 12)
- 2.13 การตรวจสอบและประเมินความเสี่ยง (ส่วนที่ 13)
- 2.14 การถ่ายโอน และการแลกเปลี่ยนข้อมูลสารสนเทศ (ส่วนที่ 14)
- 2.15 การควบคุมการเข้ารหัส (ส่วนที่ 15)
- 2.16 การนำอุปกรณ์ส่วนตัวมาใช้งาน (Bring your own device) (ส่วนที่ 16)

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศตามข้อ 2. จัดเป็นมาตรฐานด้านความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. ซึ่งบุคลากรของ รฟม. หน่วยงานภายนอก รวมถึงผู้ใช้บริการระบบสารสนเทศของ รฟม. ที่เกี่ยวข้องจะต้องปฏิบัติตามอย่างเคร่งครัด

3. กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้ว่าการการรถไฟฟ้ามหานครแห่งประเทศไทย (Chief Executive Officer: CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น และดำเนินการตรวจสอบข้อเท็จจริงกรณีที่ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด รวมทั้งให้พิจารณาลงโทษตามเหตุอันควร

นโยบายนี้ให้ใช้บังคับเมื่อพ้นกำหนด 7 วัน นับแต่วันที่ผู้มีอำนาจลงนาม

ประกาศ ณ วันที่ 7 กันยายน พ.ศ. 2565



(นายภคพงศ์ ศิริกันทรมาศ)

ผู้ว่าการการรถไฟฟ้ามหานครแห่งประเทศไทย



ภคพงศ์

เอกสารแนบท้ายประกาศ การรถไฟฟ้ายานขนส่งมวลชนแห่งประเทศไทย
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ของ รฟม.

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

1. รฟม. หมายถึง การรถไฟฟ้ายานขนส่งมวลชนแห่งประเทศไทย
2. ผทท. หมายถึง ฝ่ายเทคโนโลยีสารสนเทศ
3. ผู้บริหารระดับสูงสุด หมายถึง ผู้ว่าการการรถไฟฟ้ายานขนส่งมวลชนแห่งประเทศไทย
4. ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของ รฟม.
5. ผู้ใช้งาน หมายถึง บุคคลที่ได้รับอนุญาตให้สามารถเข้าใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. ดังนี้
 - บุคลากรของ รฟม.
 - บุคคลภายนอกที่ รฟม. อนุญาตให้เข้ามาใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. ได้ชั่วคราว เพื่อประโยชน์ในการดำเนินการของ รฟม. ได้แก่ พนักงานหรือลูกจ้างบริษัทภายนอกที่เข้ามาติดตั้งหรือดูแลรักษาระบบให้กับ รฟม. ที่ปรึกษา ผู้ปฏิบัติงานตามสัญญา หรือนิสิตนักศึกษาฝึกงาน
6. ผู้ใช้งานภายนอก หมายถึง ลูกค้าหรือบุคคลภายนอกที่ไม่ใช่กลุ่มผู้ใช้งานตามข้อ 5. ที่ใช้บริการระบบงานสารสนเทศของ รฟม. ผ่านเครือข่ายสาธารณะ (Internet)
7. หน่วยงานภายนอก หมายถึง องค์กร ซึ่ง รฟม. อนุญาตให้มีสิทธิ์ในการเข้าถึง หรือใช้ข้อมูล หรือสินทรัพย์ต่าง ๆ ของ รฟม. โดยจะได้รับสิทธิ์ในการใช้ระบบตามประเภทงานตามอำนาจและต้องรับผิดชอบในการรักษาความลับของข้อมูล
8. ผู้ดูแลระบบ หมายถึง พนักงานที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบสารสนเทศ
9. เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
10. มาตรฐาน หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย
11. ขั้นตอนปฏิบัติ หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานตามที่ได้กำหนดไว้ตามวัตถุประสงค์
12. แนวปฏิบัติ หมายถึง แนวทางที่ต้องปฏิบัติตามเพื่อให้สามารถบรรลุวัตถุประสงค์หรือเป้าหมายได้ง่ายขึ้น
13. ระบบเทคโนโลยีสารสนเทศ (Information technology system) หมายถึง ระบบงานของ รฟม. ที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายสื่อสารข้อมูลมาช่วยในการสร้างสารสนเทศที่ รฟม. สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุน การให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ ได้แก่ ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลและสารสนเทศ เป็นต้น

14. ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด ที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์
15. ข้อมูลจราจรทางคอมพิวเตอร์ (Traffic log) หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เวลา วันที่ ปริมาณ ระยะเวลา หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น
16. สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งข้อมูลอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิกให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ
17. ระบบคอมพิวเตอร์ (Computer system) หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่งหรือสิ่งอื่นใด และแนวปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
18. ระบบเครือข่ายสื่อสารข้อมูล (Network system) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของ รพม. เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น
19. สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกักระบบสารสนเทศของหน่วยงาน
20. ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) และความน่าเชื่อถือ (Reliability)
21. เหตุการณ์ด้านความมั่นคงปลอดภัย หมายถึง เหตุการณ์ที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย มาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
22. สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม
23. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้
24. สินทรัพย์ (Assets) หมายถึง สินทรัพย์ด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารของ รพม. เช่น อุปกรณ์คอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีค่าลิขสิทธิ์ ข้อมูล ระบบข้อมูล ฯลฯ
25. จดหมายอิเล็กทรอนิกส์ (e-mail) หมายถึง ระบบที่บุคคลใช้ในการรับ - ส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว

และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ โดยข่าวสารที่ส่งนั้นจะถูกเก็บไว้ในตู้จดหมาย (Mail box) ที่กำหนดไว้สำหรับผู้ใช้งาน ผู้รับสามารถเปิดอ่าน พิมพ์ลงกระดาษ หรือจะลบทิ้งก็ได้

26. ชุดคำสั่งไม่พึงประสงค์ (Malicious code) หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ชัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
27. เครื่องคอมพิวเตอร์ หมายถึง เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ และเครื่องคอมพิวเตอร์แบบพกพา
28. อุปกรณ์เคลื่อนที่ (Mobile device) หมายถึง อุปกรณ์อิเล็กทรอนิกส์แบบพกพา ซึ่งมีความสามารถในการเชื่อมต่อกับอุปกรณ์อื่นเพื่อรับส่งข้อมูลผ่านระบบเครือข่ายโทรคมนาคมไร้สายหรือโดยอาศัยคลื่นแม่เหล็กไฟฟ้าเป็นสื่อกลาง เช่น Tablet, Smart Phone
29. อุปกรณ์ส่วนตัว หมายถึง อุปกรณ์ที่ รพม. ไม่ได้เป็นผู้จัดสรรให้ใช้งาน แต่เป็นอุปกรณ์ส่วนตัวของผู้ใช้งานที่นำมาเชื่อมต่อกับเครือข่ายภายในของ รพม. เช่น เครื่องคอมพิวเตอร์ส่วนบุคคล (Personal computer) เครื่องคอมพิวเตอร์พกพา (Notebook) อุปกรณ์เคลื่อนที่ (Mobile device) หรือ Removable media เป็นต้น

ส่วนที่ 1

นโยบายการบริหารจัดการความมั่นคงปลอดภัยสำหรับผู้บริหาร

วัตถุประสงค์

- เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรมีความสอดคล้องกับมาตรฐานสากลและกฎหมายด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง

ผู้รับผิดชอบ

- ผู้บริหารสูงสุด

อ้างอิงมาตรฐาน

- หมวดที่ 1 นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information security policy)

แนวปฏิบัติ

1. จัดให้มีการทำและทบทวนหรือปรับปรุงนโยบายความมั่นคงปลอดภัย และแนวปฏิบัติที่สนับสนุนการทำงานต่าง ๆ อย่างน้อยปีละ 1 ครั้ง โดยพิจารณาจากปัจจัยนำเข้า ดังนี้
 - 1.1 กลยุทธ์การดำเนินงานขององค์กร
 - 1.2 ข้อมูลกฎหมาย ระเบียบ ข้อบังคับต่าง ๆ ที่ต้องปฏิบัติตาม
 - 1.3 การปรับปรุงนโยบายความมั่นคงปลอดภัยสำหรับปีถัดไป
 - 1.4 ผลการประเมินความเสี่ยงและแผนลดความเสี่ยง
 - 1.5 ผลการแจ้งเตือนโดยระบบป้องกันการบุกรุกในปีที่ผ่านมา
 - 1.6 ผลของการตรวจสอบข้อมูลการปิดช่องโหว่ (Patch) สำหรับระบบต่าง ๆ ในปีที่ผ่านมา
 - 1.7 การจัดทำและต่อสัญญาบำรุงรักษาระบบและอุปกรณ์ต่าง ๆ
 - 1.8 แผนการอบรมทางด้านความมั่นคงปลอดภัยประจำปีซึ่งรวมถึงการสร้างตระหนักรู้
 - 1.9 ผลการทดสอบแผนกู้คืนในปีที่ผ่านมา
 - 1.10 ข้อมูลภัยคุกคามต่าง ๆ ที่เคยเกิดขึ้นในอดีตและปัจจุบัน รวมทั้งภัยคุกคามที่ได้รับแจ้งจากหน่วยงานภายนอก
 - 1.11 ผลการตรวจสอบการปฏิบัติตามนโยบายความมั่นคงปลอดภัยโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก
2. จัดให้มีทรัพยากรด้านบุคลากร งบประมาณ การบริหารจัดการ และวัตถุประสงค์ที่เพียงพอต่อการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศในแต่ละปีงบประมาณ
3. จัดให้มีบุคลากรดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศและกำหนดหน้าที่ความรับผิดชอบรวมทั้งปรับปรุงโครงสร้างดังกล่าวตามความจำเป็น
4. แสดงเจตนาชัดเจนหรือสื่อสารอย่างสม่ำเสมอเพื่อให้ผู้ใช้งานทั้งหมดได้เห็นถึงความสำคัญของการปฏิบัติตามนโยบายความมั่นคงปลอดภัยและนโยบายสนับสนุนต่าง ๆ โดยเคร่งครัดและเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับสารสนเทศขององค์กร รวมถึงสร้างความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

ส่วนที่ 2

ความมั่นคงปลอดภัยเกี่ยวกับบุคลากร

วัตถุประสงค์

- เพื่อให้ผู้ใช้งานเข้าใจถึงบทบาท หน้าที่ความรับผิดชอบ ทั้งก่อนการจ้างงาน ระหว่างการจ้างงาน และสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน ตลอดจนตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศเพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง การใช้งานระบบเทคโนโลยีสารสนเทศผิดวัตถุประสงค์และความผิดพลาดในการปฏิบัติหน้าที่ ซึ่งอาจส่งผลกระทบต่อหรือทำให้ รพม.เกิดความเสียหาย

ผู้รับผิดชอบ

- ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ ผู้อำนวยการฝ่ายทรัพยากรบุคคล ผู้อำนวยการฝ่าย/สำนัก ที่กำกับดูแลงานที่มีการว่าจ้างหน่วยงานภายนอก

อ้างอิงมาตรฐาน

- หมวดที่ 3 ความมั่นคงปลอดภัยสำหรับบุคลากร (Organization of information security)
- หมวดที่ 4 การบริหารจัดการทรัพย์สิน (Asset management)
- หมวดที่ 9 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)

แนวปฏิบัติ

1. การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to employment) เพื่อคัดสรรบุคลากรก่อนที่จะเข้ามาปฏิบัติงาน และเพื่อลดความเสี่ยงจากการปฏิบัติงานผิดพลาด การขโมย การปลอมแปลง และการนำระบบสารสนเทศหรือทรัพยากรสารสนเทศของ รพม. ไปใช้ในทางที่ไม่เหมาะสม รวมทั้งเพื่อให้ผู้ใช้งานเข้าใจในหน้าที่ความรับผิดชอบของตนเอง
 - 1.1 การตรวจสอบคุณสมบัติของผู้สมัคร (Screening)

ฝ่ายทรัพยากรบุคคล หรือฝ่าย/สำนัก ที่กำกับดูแลงานที่มีการว่าจ้างหน่วยงานภายนอกต้องตรวจสอบคุณสมบัติของผู้สมัคร (ทั้งกรณีการจ้างเป็นพนักงาน ลูกจ้าง การว่าจ้างหน่วยงานภายนอกเพื่อปฏิบัติงานให้ รพม. รวมทั้งนิสิตนักศึกษาฝึกงาน) โดยผู้สมัครต้องไม่เคยกระทำผิดกฎหมาย ระเบียบ ข้อบังคับ หรือจริยธรรม รวมทั้งไม่มีประวัติในการบุกรุก แก๊ง ทำลาย หรือโจรกรรมข้อมูลในระบบเทคโนโลยีสารสนเทศมาก่อน และมีคุณสมบัติตามที่ รพม. กำหนด
 - 1.2 การกำหนดเงื่อนไขการจ้างงาน (Terms and conditions of employment) การว่าจ้างให้มีเงื่อนไขการจ้างงานให้ครอบคลุมในเรื่องดังต่อไปนี้
 - 1.2.1 กำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศอย่างเป็นลายลักษณ์อักษร (Information security roles and responsibilities) แก่ผู้ใช้งาน โดยกำหนดให้สอดคล้องกับนโยบายความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของ รพม.
 - 1.2.2 กำหนดให้มีการลงนามในสัญญาว่าจะไม่เปิดเผยความลับของ รพม. (Non-Disclosure Agreement : NDA)
 - 1.2.3 ระบบเทคโนโลยีสารสนเทศที่สร้างหรือพัฒนาโดยผู้ใช้งานในระหว่างการว่าจ้างถือเป็นสินทรัพย์ของ รพม.

- 1.2.4 กำหนดความรับผิดชอบหรือบทลงโทษ หากผู้ใช้งานไม่ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รฟม. รวมทั้ง กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
2. การสร้างความมั่นคงปลอดภัยในระหว่างการจ้างงาน (During employment) เพื่อสร้างความตระหนักแก่ผู้ใช้งานเกี่ยวกับภัยที่เกี่ยวข้องกับการปฏิบัติงานสารสนเทศ รวมถึงให้ความรู้เพื่อให้สามารถป้องกันภัยดังกล่าวได้
 - 2.1 หน้าที่ในการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management responsibilities)
ผู้บริหาร รฟม. ทุกระดับชั้นมีหน้าที่สนับสนุนและส่งเสริมเรื่องดังต่อไปนี้ แก่ผู้ใช้งาน
 - 2.1.1 ประกาศนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ รฟม. เป็นลายลักษณ์อักษรให้ทุกคนรับทราบและปฏิบัติตาม
 - 2.1.2 จูงใจให้ผู้ใช้งานปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ รฟม.
 - 2.1.3 สร้างความตระหนักถึงความมั่นคงปลอดภัยด้านสารสนเทศที่เกี่ยวข้องกับหน้าที่ความรับผิดชอบของตนเองและของ รฟม.
 - 2.2 การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่ผู้ใช้งาน (Information security awareness, education and training) การสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยอย่างสม่ำเสมอ
 - 2.2.1 ผู้ดูแลระบบต้องแจ้งเตือนภัยคุกคาม และช่องโหว่ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศแก่ผู้ใช้งานที่เกี่ยวข้อง นอกจากนี้ก็ต้องแจ้งเตือนให้ผู้ใช้งานเพิ่มความระมัดระวังความเสี่ยงต่าง ๆ เช่น ไวรัสมัลแวร์ เทคนิคการหลอกล่อทางจิตวิทยา (Social engineering) และช่องโหว่ทางเทคนิค เป็นต้น
 - 2.2.2 ผทท. ต้องดำเนินการฝึกอบรม หรือประชาสัมพันธ์เพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศแก่ผู้ใช้งานเป็นประจำทุกปี
 - 2.2.3 ผทท. ต้องแจ้งผู้ใช้งานให้ทราบ เมื่อมีการเปลี่ยนแปลงนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศของ รฟม. รวมทั้งอธิบายผลกระทบจากการเปลี่ยนแปลงดังกล่าว
 - 2.3 การกำหนดบทลงโทษ
 - 2.3.1 ความรับผิดตามกฎหมาย
นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ไม่ได้ก่อให้เกิดสิทธิ์ทางกฎหมายที่ทำให้ผู้ใช้งานพ้นผิดแม้จะได้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ และผู้ใช้งานตกลงยินยอมที่จะไม่ดำเนินการใด ๆ ทางกฎหมายต่อ รฟม. ซึ่งได้ปฏิบัติตามระเบียบนี้ แต่อย่างไรก็ตามหากผู้ใช้งานกระทำการละเมิดหรือกระทำผิดตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ อาจเป็นความผิดทางวินัยและเป็นเหตุให้ถูกลงโทษทางวินัยได้ รฟม. ไม่มีส่วนรับผิดชอบต่อการละเมิดทรัพย์สินทางปัญญาที่เกิดจากการใช้ระบบคอมพิวเตอร์

2.3.2 การพิจารณาโทษผู้กระทำผิด

ผู้ใช้งานที่กระทำความผิด ฝ่าท. จะเพิกถอนสิทธิ์การใช้งานและอาจเป็นความผิดทางวินัย หรือความผิดตามกฎหมายที่เกี่ยวข้อง

- 1) พนักงาน/ลูกจ้างที่ฝ่าฝืนหรือละเมิดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รฟม. ต้องถูกลงโทษตามกระบวนการทางวินัยของ รฟม. รวมถึงกฎหมายที่เกี่ยวข้อง
- 2) หน่วยงานภายนอกที่กระทำความผิด จะมีโทษตามที่ระบุไว้ในสัญญาหรือถูกเพิกถอนสิทธิ์การใช้งาน รวมถึงดำเนินการตามกฎหมายที่เกี่ยวข้อง

3. การสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน (Termination and change of employment)

เพื่อกำหนดหน้าที่ความรับผิดชอบเมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน ซึ่งรวมถึงการคืนทรัพย์สินและการถอดถอนสิทธิ์ในการเข้าถึง

3.1 การแจ้งการสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน

3.1.1 ฝ่ายทรัพยากรบุคคลต้องแจ้งให้ฝ่ายเทคโนโลยีสารสนเทศทราบทันทีหากพนักงานมีการลาออก โยกย้าย เกษียณ หรือเสียชีวิต เพื่อฝ่ายเทคโนโลยีสารสนเทศจะได้ตรวจสอบและบริหารจัดการสิทธิ์ในการเข้าถึงระบบเทคโนโลยีสารสนเทศ

3.1.2 ฝ่าย/สำนัก ที่กำกับดูแลงานที่มีการว่าจ้างหน่วยงานภายนอก ต้องแจ้งให้ฝ่ายเทคโนโลยีสารสนเทศทราบทันทีในกรณีที่ผู้รับจ้างภายนอกสิ้นสุดสัญญาจ้างหรือมีการยกเลิกสัญญาจ้างเพื่อให้ ฝ่าท. ตรวจสอบการใช้งานระบบสารสนเทศและถอดถอนสิทธิ์ในการเข้าถึงระบบสารสนเทศของ รฟม.

3.2 การคืนสินทรัพย์ของ รฟม.

ผู้ดูแลระบบต้องตรวจสอบเพื่อเรียกคืนสินทรัพย์ของ รฟม. จากผู้ใช้งาน เมื่อการสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน

3.3 การถอดถอนสิทธิ์ในการเข้าถึง

3.3.1 ผู้ดูแลระบบต้องถอดถอนสิทธิ์ในการเข้าถึงของผู้ใช้งาน เมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน

3.3.2 การถอดถอนสิทธิ์ในการเข้าถึงหมายถึงทางกายภาพ (Physical) และทางตรรกะ (Logical) เช่น กุญแจ บัตรแสดงตน บัตรประจำตัวผู้ใช้งาน และบัญชีผู้ใช้งาน เป็นต้น

3.3.3 ในกรณีที่ผู้ใช้งานที่สิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน มีการใช้บัญชีผู้ใช้งานร่วมกับผู้อื่น (Shared user ID) กับผู้ใช้งานอื่น ผู้บังคับบัญชาต้องเปลี่ยนรหัสผ่านทันทีหลังจากสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน

ส่วนที่ 23

การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

วัตถุประสงค์

- เพื่อควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าถึงอาคารสถานที่ และพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area)

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้อำนวยการฝ่ายจัดซื้อและบริการ

อ้างอิงมาตรฐาน

- หมวดที่ 7 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security)

แนวปฏิบัติ

1. ผู้ดูแลระบบ ต้องออกแบบ และติดตั้งอุปกรณ์หรือระบบสนับสนุน (Facilities) เพื่อป้องกันการรักษาความมั่นคงปลอดภัยด้านกายภาพ เช่น อุปกรณ์ดับเพลิง ระบบสำรองไฟฟ้า เครื่องกำเนิดไฟฟ้า ระบบปรับอากาศและควบคุมความชื้น ระบบเตือนภัยน้ำรั่ว และต้องมีการบำรุงรักษาอย่างสม่ำเสมอ
2. ผู้ดูแลระบบต้องติดตั้งอุปกรณ์สารสนเทศในตู้แร็ก (Rack) หรือสถานที่ที่มีความมั่นคงปลอดภัยและมีการปิดล็อก
3. ผู้ดูแลระบบ ต้องมีการป้องกันสายเคเบิลที่ใช้เพื่อการสื่อสารหรือสายไฟ มิให้มีการดักจับสัญญาณ (Interception) หรือมีความเสียหายเกิดขึ้น โดยจะต้องเดินสายเคเบิลผ่านท่อร้อยสายหรือทางเดินสายที่มีความมั่นคงปลอดภัยจากการเข้าถึง และไม่เดินสายผ่านพื้นที่ที่เข้าถึงได้อย่างสาธารณะ รวมทั้งสายเคเบิลสื่อสารและสายไฟฟ้าต้องแยกจากกันโดยมีระยะห่างที่เหมาะสม
4. การกำหนดบริเวณที่มีการรักษาความมั่นคงปลอดภัย
กำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม เพื่อเป็นการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้ โดยแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศออกเป็น
 - 4.1 พื้นที่ทำงาน (Working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน
 - 4.2 พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) หมายถึง พื้นที่ศูนย์ของข้อมูล (Data center)
5. การควบคุมการเข้าออก อาคาร สถานที่
 - 5.1 กำหนดสิทธิของผู้ใช้งานและหน่วยงานภายนอกในการเข้าถึงสถานที่ โดยแบ่งแยกได้ ดังนี้
 - 5.1.1 ผู้ดูแลระบบต้องกำหนดสิทธิแก่ผู้ใช้งานที่มีสิทธิ์เข้า - ออก และกำหนดช่วงระยะเวลาที่มีสิทธิ์ในการเข้า - ออกแต่ละพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศอย่างชัดเจน
 - 5.1.2 เจ้าหน้าที่รักษาความปลอดภัย (รปภ.) จะต้องให้หน่วยงานภายนอกหรือบุคคลภายนอกแลกบัตรที่สามารถระบุตัวตนของบุคคลนั้น ๆ ก่อนเข้าถึงอาคารของ รพม. เช่น บัตรประจำตัวประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วบันทึกข้อมูลบัตรในสมุดบันทึกหรือระบบงานสารสนเทศ

- 5.1.3 หน่วยงานภายนอกที่มาติดต่อต้องติดบัตรผู้ติดต่อ (Visitor) ตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ใน รพม. และคืนบัตรผู้ติดต่อ (Visitor) ก่อนออกจากอาคารของ รพม.
- 5.1.4 เจ้าหน้าที่รักษาความปลอดภัย (รปภ.) ต้องตรวจสอบผู้ติดต่อ อุปกรณ์ พร้อมลงเวลาออกที่สมุดบันทึกหรือระบบสารสนเทศให้ถูกต้อง
- 5.2 ผู้ดูแลระบบ ต้องควบคุมการเข้า - ออกพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) ไม่ให้ผู้ไม่มีสิทธิ์เข้าถึงได้ โดยกำหนดพื้นที่การส่งมอบสินค้าและพื้นที่การเตรียมหรือประกอบอุปกรณ์สารสนเทศ (Unpack Area) ก่อนนำเข้าพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) และต้องควบคุมการเข้า - ออก เพื่อหลีกเลี่ยงการเข้าถึงระบบสารสนเทศและข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต โดยปฏิบัติตามขั้นตอนที่ รพม. กำหนด

ส่วนที่ 4 การจัดการทรัพย์สิน

วัตถุประสงค์

- เพื่อบริหารจัดการทรัพย์สินสารสนเทศ ตั้งแต่การจัดการหา การใช้งาน จนถึงการยกเลิกใช้งาน โดยมีการระบุสินทรัพย์ขององค์กรและกำหนดหน้าที่ความรับผิดชอบในการปกป้องทรัพย์สินสารสนเทศอย่างเหมาะสม

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- เจ้าของข้อมูล
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 4 การบริหารจัดการทรัพย์สิน (Asset management)

แนวปฏิบัติ

1. หน้าที่ความรับผิดชอบต่อทรัพย์สินสารสนเทศ (Responsibility for assets)
 - 1.1 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องร่วมกันจัดทำบัญชีทรัพย์สิน/ทะเบียนทรัพย์สิน (Asset inventory) และทบทวนทะเบียนทรัพย์สินอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ
 - 1.2 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องระบุเจ้าของทรัพย์สินสารสนเทศทุกรายการ เพื่อรับผิดชอบดูแลความมั่นคงปลอดภัยสารสนเทศตลอดวงจรอายุการใช้งาน
 - 1.3 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องเรียกคืนทรัพย์สินสารสนเทศเมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน
 - 1.4 ผู้ใช้งานต้องใช้ทรัพย์สินสารสนเทศของ รพม. อย่างระมัดระวัง และใช้เพื่อปฏิบัติงานของ รพม. เท่านั้น รวมทั้งต้องปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ และนโยบาย ของ รพม.
2. การจำแนกประเภทของทรัพย์สินสารสนเทศ (Asset classification)
 - 2.1 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจำแนกประเภททรัพย์สินตามขั้นตอนที่ รพม. กำหนด และทบทวนการจำแนกดังกล่าวอย่างสม่ำเสมอ
 - 2.2 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจัดทำป้ายชื่อทรัพย์สินสารสนเทศ (Labeling) ให้ชัดเจน พร้อมทั้งจัดให้มีมาตรการดูแลรักษาความมั่นคงปลอดภัยสารสนเทศที่สอดคล้องกับประเภททรัพย์สินตามระดับชั้นความลับที่ รพม. กำหนด
3. การจัดการสื่อบันทึกข้อมูล (Media handling)
 - 3.1 เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ใช้งานต้องควบคุมการใช้งานและจัดเก็บสื่อบันทึกแบบถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้ (Removable media) ตามที่ รพม. กำหนด
 - 3.2 เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล เพิ่มข้อมูลตามขั้นตอนที่ รพม. กำหนด โดยไม่สามารถกู้คืนข้อมูลกลับมาได้อีกก่อนจะกำจัดอุปกรณ์ดังกล่าวหรือ

ก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อเพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลที่สำคัญได้ โดยพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีทำลาย
กระดาษ	ให้หั่นด้วยเครื่องทำลายเอกสาร
Flash Drive	1) ทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD5220.22M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นการเขียนทับข้อมูลเดิมหลายรอบ 2) ใช้วิธีทุบหรือบดให้เสียหาย
แผ่น CD/DVD	ให้หั่นด้วยเครื่องทำลายเอกสาร
เทป	ใช้วิธีทุบหรือบดให้เสียหายหรือเผาทำลาย
ฮาร์ดดิสก์	1) ทำลายข้อมูลบนฮาร์ดดิสก์ตามมาตรฐาน DOD5220.22M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นการเขียนทับข้อมูลเดิมหลายรอบ 2) ใช้วิธีทุบหรือบดให้เสียหาย

- 3.3 เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ใช้งาน ต้องมีการป้องกันสื่อบันทึกข้อมูลที่ใช้จัดเก็บข้อมูลสารสนเทศ ในกรณีที่มีการเคลื่อนย้ายเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต ถูกนำไปใช้งานผิดวัตถุประสงค์ รวมถึงป้องกันสื่อบันทึกข้อมูลไม่ให้เกิดความเสียหาย โดยรักษาความปลอดภัยสารสนเทศตามขั้นตอนที่ รพม. กำหนด

ส่วนที่ 5

การจัดทำ การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

วัตถุประสงค์

- เพื่อควบคุมการจัดทำ พัฒนา และบำรุงรักษาระบบสารสนเทศ ให้มีการกำหนดมาตรการการรักษาความมั่นคงปลอดภัย เพื่อป้องกันความผิดพลาด สูญหาย และการเปลี่ยนแปลงแก้ไขระบบ

ผู้รับผิดชอบ

- ผู้บังคับบัญชา
- ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

- หมวดที่ 10 โครงสร้างการจัดทำ การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (System acquisition, development and maintenance)
- หมวดที่ 11 ความสัมพันธ์กับหน่วยงานภายนอก (Supplier relationships)

แนวปฏิบัติ

1. ผู้บังคับบัญชา ต้องควบคุมให้มีการกำหนดข้อตกลงและความรับผิดชอบที่เกี่ยวข้องกับความเสถียรด้านความมั่นคงปลอดภัยสารสนเทศลงในสัญญากับผู้ให้บริการภายนอก โดยให้ครอบคลุมรวมถึงผู้รับจ้างช่วงด้วย
2. ผู้บังคับบัญชาต้องควบคุมให้มีข้อตกลง (Sign off) ก่อนเริ่มใช้งานระบบจริง (Production) หรือก่อนเริ่ม Go live
3. ผู้ดูแลระบบ ต้องจัดทำข้อกำหนดโดยระบุถึงการควบคุมความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร เช่น วิธีการแบบปลอดภัยในการพัฒนาโปรแกรมตามมาตรฐาน OWASP (Open Web Application Security Project) Top 10 หรือมาตรฐาน CWE (Common Weakness Enumeration) Top 25 หรือมาตรฐานที่ยอมรับในสากล
4. ผู้ดูแลระบบ ต้องมีการออกแบบระบบเพื่อตรวจสอบข้อมูลที่จะรับเข้าสู่แอปพลิเคชัน ข้อมูลที่เกิดจากการประมวลผล และข้อมูลที่อยู่ระหว่างการประมวลผล เพื่อตรวจหาและป้องกันความไม่ถูกต้องที่เกิดขึ้นกับข้อมูล เช่น หน่วยความจำล้น (Buffer overflows) การใช้ตัวแปรผิดประเภท และต้องมีมาตรการป้องกันหรือควบคุมความล้มเหลวระหว่างการประมวลผล (Rollback)
5. ผู้ดูแลระบบต้องมีการควบคุมการเข้าถึงและควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบตามขั้นตอนที่ รพม. กำหนดเพื่อควบคุมผลกระทบที่เกิดขึ้น
6. ผู้ดูแลระบบต้องจำกัดให้มีการเปลี่ยนแปลงใด ๆ ต่อซอฟต์แวร์ที่ใช้งาน (Software package) โดยเปลี่ยนแปลงเฉพาะที่จำเป็นเท่านั้น และควบคุมทุก ๆ การเปลี่ยนแปลงอย่างเข้มงวดตามขั้นตอนที่ รพม. กำหนด
7. ผู้ดูแลระบบต้องจำกัดการเข้าถึง Source code ให้เข้าถึงได้เฉพาะผู้มีสิทธิ์เท่านั้น
8. ผู้ดูแลระบบต้องจัดทำ Source code review เพื่อหาข้อผิดพลาดหรือสิ่งผิดปกติและปรับปรุง Source code ให้มีคุณภาพ
9. ผู้ดูแลระบบต้องปิดบังข้อมูลส่วนบุคคล (Data Masking) ที่จัดเก็บอยู่ในระบบงานสารสนเทศด้วยวิธีการที่เหมาะสม

10. ผู้ดูแลระบบต้องแสดงข้อมูลของผู้ใช้งานอย่างรัดกุม เช่น การปิดบังข้อมูลสำคัญของผู้ใช้งาน (Sensitive data masking) เป็นต้น
11. กรณีของแอปพลิเคชันที่ใช้งานผ่านอุปกรณ์เคลื่อนที่ (Mobile device) ให้ผู้ดูแลระบบดำเนินการ ดังนี้
 - 11.1 ปิดบังหน้าจอเมื่อย่อแอปพลิเคชัน (Application blurring) เพื่อลดความเสี่ยงที่ข้อมูลสำคัญของผู้ใช้งานจะรั่วไหล
 - 11.2 ขอสื่อสิทธิ์เข้าถึงทรัพยากรหรือบริการโดยแอปพลิเคชัน (Application permission) บนอุปกรณ์เคลื่อนที่ของผู้ใช้งานเท่าที่จำเป็น และมีกระบวนการทบทวนการขอสื่อสิทธิ์เป็นประจำเพื่อป้องกันการละเมิดสิทธิ์ความเป็นส่วนตัวของผู้ใช้งาน
12. ผู้ดูแลระบบต้องควบคุมข้อมูลที่นำมาใช้ในการทดสอบระบบ (Test data) อย่างเหมาะสม โดยไม่นำข้อมูลจริงมาทดสอบ กรณีจำเป็นต้องใช้ข้อมูลจริงต้องได้รับอนุญาตข้อมูลจากเจ้าของก่อนนำมาใช้งาน และทำลายข้อมูลอย่างเหมาะสมตามขั้นตอนที่ รพม. กำหนด
13. ผู้ดูแลระบบต้องแยกระบบสารสนเทศสำหรับการพัฒนา ทดสอบ และใช้งานจริงออกจากกันเพื่อลดความเสี่ยงที่เกิดจากการเปลี่ยนแปลงระบบสารสนเทศโดยไม่ได้รับอนุญาต และต้องมีการกำหนดสิทธิ์การเข้าถึงระบบสารสนเทศที่พัฒนา ทดสอบ หรือใช้งานจริง ทั้งระบบสารสนเทศใหม่ และการปรับปรุงแก้ไขระบบสารสนเทศเดิม
14. ผู้ดูแลระบบต้องมีการกำหนดขั้นตอนการทดสอบระบบสารสนเทศก่อนนำไปใช้งานจริง ทั้งในกรณีปรับปรุงระบบสารสนเทศเดิมและการพัฒนาระบบสารสนเทศใหม่
15. ผู้ดูแลระบบต้องติดตั้งซอฟต์แวร์บนระบบสารสนเทศที่ให้บริการ (Production) ตามขั้นตอนที่ รพม. กำหนด และจำกัดสิทธิ์การติดตั้งซอฟต์แวร์เพื่อให้ระบบสารสนเทศต่าง ๆ มีความถูกต้องครบถ้วนและน่าเชื่อถือ
16. ผู้ดูแลระบบต้องนำซอฟต์แวร์ที่ไม่ละเมิดลิขสิทธิ์มาติดตั้งบนระบบสารสนเทศที่ให้บริการ (Production)
17. ผู้ดูแลระบบต้องกำกับดูแลให้ผู้รับจ้างปฏิบัติตามสัญญาหรือข้อตกลงการให้บริการที่ระบุไว้ โดยครอบคลุมถึงด้านความมั่นคงปลอดภัยสารสนเทศ และการปฏิบัติตามขั้นตอนที่เกี่ยวข้องต่าง ๆ ที่ รพม. กำหนดไว้
18. ผู้ดูแลระบบ ต้องติดตาม ตรวจสอบรายงาน หรือบันทึกการให้บริการของบุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามสัญญาว่าจ้างอย่างสม่ำเสมอ
19. ผู้ดูแลระบบ ต้องดูแลให้ทรัพย์สินสารสนเทศได้รับการบำรุงรักษาและซ่อมแซมตามความต้องการ รวมทั้งต้องมีการบันทึกประวัติการทำงานผิดปกติ การบำรุงรักษา และการซ่อมแซมอุปกรณ์นั้น ๆ อย่างสม่ำเสมอ
20. ผู้ดูแลระบบจะต้องปิดช่องโหว่ของระบบสารสนเทศที่มีระดับความรุนแรงในระดับวิกฤติ (Critical) และระดับความรุนแรงระดับสูง (High) ทั้งหมดก่อนนำไปใช้งานจริง (Production) หรือก่อนเริ่ม Go live โดยเฉพาะระบบที่ให้บริการผ่านเครือข่ายอินเทอร์เน็ต (Internet facing) และระบบที่มีความสำคัญต่อการดำเนินงานของ รพม.
21. ผู้ดูแลระบบต้องพิจารณาเลือกใช้ Version ของ Software ดังนี้
 - 21.1 กรณีนำ Software เดิมมาใช้ในการจัดหาหรือพัฒนาระบบ จะต้องนำผลการตรวจสอบช่องโหว่และผลการทดสอบเจาะระบบมาประกอบการพิจารณาคัดเลือกเวอร์ชันของ Software ด้วย เพื่อป้องกันไม่ให้เกิดช่องโหว่เดิมรวมถึงเพื่อลดภาระงานในการปิดช่องโหว่เดิมซ้ำ
 - 21.2 กรณีเป็น Software ที่ไม่เคยนำมาใช้งานให้เลือกใช้ Software เวอร์ชันล่าสุด

ส่วนที่ 6

การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

- เพื่อควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศตั้งแต่การกำหนดสิทธิ์ กำหนดประเภทของข้อมูล จัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ระดับชั้นการเข้าถึง เวลาที่เข้าถึงได้ และช่องทางการเข้าถึง ทั้งนี้เพื่อควบคุมและป้องกันการเข้าถึง การลวงรู้ และการแก้ไขระบบสารสนเทศของ รพม. โดยไม่ได้รับอนุญาต

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- เจ้าของข้อมูล
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 5 การควบคุมการเข้าถึง (Access control)
- หมวดที่ 8 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations security)
- หมวดที่ 9 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)

แนวปฏิบัติ

1. การควบคุมการเข้าถึงระบบสารสนเทศ (Access control)
 - 1.1 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องร่วมกันกำหนดสิทธิ์ในการเข้าถึงระบบสารสนเทศ (Authorization matrix) ที่เหมาะสมและสอดคล้องกับหน้าที่ความรับผิดชอบของผู้ใช้งาน และทบทวนเมื่อมีการเปลี่ยนแปลง
 - 1.2 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องร่วมกันกำหนดระดับการอนุมัติ (Authorization level) การเข้าถึงระบบเทคโนโลยีสารสนเทศ
 - 1.3 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจัดให้มีการแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties) ในการเข้าถึงระบบเทคโนโลยีสารสนเทศอย่างเหมาะสม เช่น มีการแบ่งแยกหน้าที่ระหว่างการแจ้งความประสงค์ การเข้าถึงและการอนุมัติการเข้าถึง เป็นต้น
 - 1.4 กรณีของแอปพลิเคชันที่ใช้งานผ่านอุปกรณ์เคลื่อนที่ (Mobile device) ผู้ดูแลระบบต้องปฏิบัติ ดังนี้
 - 1.4.1 ไม่อนุญาตให้อุปกรณ์เคลื่อนที่ที่ใช้ระบบปฏิบัติการล้าสมัย (Obsolete operating system) ใช้งานแอปพลิเคชัน หรือหากอนุญาตให้ใช้บริการได้ควรมีมาตรการรองรับเพื่อลดความเสี่ยงที่ รพม. จะได้รับรวมถึงลดผลกระทบต่อผู้ใช้งานตามความเหมาะสม เช่น การเพิ่มมาตรการยืนยันตัวตน เป็นต้น
 - 1.4.2 ไม่อนุญาตให้อุปกรณ์ที่มีการปรับแต่งการเข้าถึงระบบปฏิบัติการ (rooted/jailbroken) ใช้งานแอปพลิเคชัน เพื่อลดความเสี่ยงที่ผู้ไม่ประสงค์ดีสามารถเข้าถึงข้อมูลสำคัญของผู้ใช้งานและละเมิดหรือหลีกเลี่ยงมาตรการการรักษาความมั่นคงปลอดภัยที่ รพม. กำหนดไว้
 - 1.4.3 ไม่อนุญาตให้ผู้ใช้งานใช้แอปพลิเคชันเวอร์ชันต่ำกว่าที่ รพม. กำหนด เพื่อให้แอปพลิเคชันมีการรักษาความมั่นคงปลอดภัยเป็นไปตามมาตรฐานของ รพม.

1.5 ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ใช้งาน ต้องปฏิบัติ ดังนี้

1.5.1 แบ่งประเภทข้อมูล ดังนี้

- 1) ข้อมูลและสารสนเทศสำหรับสนับสนุนการตัดสินใจของผู้บริหาร ได้แก่ ข้อมูลสารสนเทศที่มีความสำคัญหรือมีความจำเป็นเร่งด่วนที่ต้องติดตามอย่างใกล้ชิดเพื่อประกอบการตัดสินใจเชิงนโยบาย กำหนดนโยบาย และการวางแผนของผู้บริหารระดับสูง
- 2) ข้อมูลและสารสนเทศสนับสนุนเชิงยุทธศาสตร์ (Strategy data) ได้แก่ ข้อมูลและสารสนเทศเชิงวิชาการเพื่อสนับสนุนการดำเนินงานตามพันธกิจและยุทธศาสตร์ของ รพม. ให้บรรลุเป้าหมาย รวมทั้งข้อมูลที่เผยแพร่แก่ผู้รับบริการภายนอก
- 3) ข้อมูลและสารสนเทศที่สนับสนุนการปฏิบัติงานประจำ (Operation data) ได้แก่ ข้อมูลที่สนับสนุนการทำงานทั่วไปของ รพม.

1.5.2 จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น 3 ระดับ คือ

- 1) ข้อมูลที่มีระดับความสำคัญมาก หมายถึง ข้อมูลที่ใช้สำหรับสนับสนุนการตัดสินใจของผู้บริหาร
- 2) ข้อมูลที่มีระดับความสำคัญปานกลาง หมายถึง ข้อมูลที่ใช้ปฏิบัติงานเฉพาะกลุ่มงาน แผนก กอง หรือฝ่ายภายในองค์กร
- 3) ข้อมูลที่มีระดับความสำคัญน้อย หมายถึง ข้อมูลที่พนักงาน/ลูกจ้างภายใน รพม. สามารถเข้าถึงร่วมกันได้หรือสามารถเผยแพร่ได้

1.5.3 จัดแบ่งลำดับชั้นความลับของข้อมูลตามที่ รพม. กำหนด

1.5.4 จัดแบ่งระดับชั้นการเข้าถึง

- 1) ระดับชั้นสำหรับผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และภารกิจที่ได้รับมอบหมาย
- 2) ระดับชั้นสำหรับผู้ปฏิบัติงานทั่วไป เข้าถึงข้อมูลที่ได้รับมอบหมายตามอำนาจหน้าที่
- 3) ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย มีสิทธิ์ในการบริหารจัดการระบบและเข้าถึงข้อมูลที่ได้รับมอบหมายตามอำนาจหน้าที่

1.6 เจ้าของข้อมูลและผู้ดูแลระบบต้องกำหนดเวลาการเข้าถึงระบบสารสนเทศ

1.7 ผู้ดูแลระบบต้องจำกัดช่องทางการเข้าถึงระบบเทคโนโลยีสารสนเทศตามช่องทาง ดังนี้

- 1) เครือข่ายภายในของ รพม.
- 2) เครือข่ายภายนอก รพม.
- 3) เครือข่ายอื่นที่จัดไว้ให้ เช่น ระบบเครือข่ายสื่อสารข้อมูล GIN

1.7 ผู้ดูแลระบบต้องกำกับดูแล Default permission ของไฟล์ (File) และ โฟลเดอร์ (Folder) ที่สร้างขึ้นให้มีการจำกัดสิทธิ์ในการเข้าถึง

1.8 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องพิจารณาข้อกำหนดต่าง ๆ ที่มีผลทางกฎหมายซึ่งเกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศของ รพม. เช่น พระราชบัญญัติ ข้อกำหนดทางกฎหมาย ข้อกำหนดในสัญญา

และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่น ๆ เป็นต้น เพื่อกำหนดสิทธิ์การเข้าถึงสารสนเทศและระบบเทคโนโลยีสารสนเทศของ รพม.

- 1.9 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องมีการสอบทานสิทธิ์ในการเข้าถึงระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ พร้อมทั้งเพิกถอนสิทธิ์เมื่อพบเห็นสิทธิ์ที่ไม่ถูกต้องตามสิทธิ์ในการเข้าถึง (Authorization matrix)
2. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)
ให้มีการควบคุมการลงทะเบียนผู้ใช้งาน การบริหารจัดการรหัสผ่าน การบริหารจัดการสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศ และการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน
 - 2.1 การลงทะเบียนผู้ใช้งาน (User registration)
 - 2.1.1 ผู้ดูแลระบบต้องบริหารจัดการและควบคุมบัญชีชื่อผู้ใช้งาน (Username) มิให้มีการใช้งานบัญชีชื่อผู้ใช้งานซ้ำกัน ทั้งนี้ ในส่วนของพนักงาน/ลูกจ้าง รพม. ให้กำหนดชื่อผู้ใช้งาน (Username) ตามมาตรฐานจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ใช้ในองค์กร
 - 2.1.2 เจ้าของข้อมูลต้องเป็นผู้อนุมัติการสร้างบัญชีผู้ใช้งานชั่วคราว (Temporary user) และต้องจำกัดช่วงเวลาการใช้งานเท่าที่จำเป็น
 - 2.2 การบริหารจัดการรหัสผ่าน (User password management)
 - 2.2.1 ผู้ดูแลระบบและผู้รับจ้าง ต้องกำหนดความยาวรหัสผ่านอย่างน้อย 12 หลัก
 - 2.2.2 บุคลากรของ รพม. (พนักงาน/ลูกจ้างของ รพม.) ต้องกำหนดความยาวรหัสผ่านอย่างน้อย 8 หลัก
 - 2.2.3 ผู้ดูแลระบบกำหนดรหัสผ่านแบบชั่วคราวโดยใช้วิธีการสุ่ม และบังคับให้มีการเปลี่ยนรหัสผ่านเมื่อผู้ใช้งานเข้าใช้งานระบบในครั้งแรก (บังคับใช้เฉพาะกรณีข้อ 2.2.1 – 2.2.2)
 - 2.2.4 ผู้ดูแลระบบและผู้รับจ้าง รวมถึงบุคลากรของ รพม. (พนักงาน/ลูกจ้างของ รพม.) ตามข้อ 2.2.1 – 2.2.2 ต้องปฏิบัติเพิ่มเติม ดังนี้
 - 1) รหัสผ่านประกอบด้วย ตัวอักษร ตัวเลข และอักขระพิเศษ เช่น (a-Z) (0-9) (@ , # , & , “ , ‘ , * , = , < , > , % , \$, + , ?) เป็นต้น
 - 2) กำหนดรหัสผ่านที่ง่ายต่อการจดจำ แต่ต้องไม่เป็นคำที่สามารถคาดเดาได้ง่าย เช่น คำที่อยู่ในพจนานุกรม “qwerty” “abcde” “12345” ชื่อ-นามสกุล วันเดือนปีเกิด ที่อยู่ หรือเบอร์โทรศัพท์ เป็นต้น
 - 3) ต้องไม่ใช้งานรหัสผ่านโดยกระบวนการเข้าใช้งานโดยอัตโนมัติ ได้แก่ การกำหนดค่า “Remember Password” เป็นต้น
 - 4) ต้องเก็บรหัสผ่านไว้เป็นความลับเฉพาะบุคคล ไม่เปิดเผยให้ผู้อื่นรับทราบ และไม่พิมพ์รหัสผ่านในลักษณะเปิดเผย เช่น พิมพ์รหัสผ่านต่อหน้าผู้ใช้งานคนอื่น เป็นต้น
 - 5) ต้องไม่ใช้บัญชีชื่อผู้ใช้งานและรหัสผ่านร่วมกันกับผู้อื่น แม้ว่าบัญชีชื่อผู้ใช้งานจะได้รับการอนุญาตจากเจ้าของชื่อผู้ใช้งานบุคคลนั้นก็ตาม
 - 6) ต้องเปลี่ยนแปลงรหัสผ่านเป็นประจำอย่างน้อยทุก 6 เดือน
 - 7) ต้องเปลี่ยนแปลงรหัสผ่านเมื่อมีการแจ้งเตือนจากระบบ หรือสงสัยว่ารหัสผ่านลวงรู้โดยบุคคลอื่น
 - 2.2.5 ผู้ดูแลระบบ ต้องกำหนดให้มีการเข้ารหัสข้อมูลรหัสผ่านในระบบ
 - 2.2.6 ผู้ดูแลระบบ ต้องจัดให้มีการควบคุมรหัสผ่านอย่างเข้มงวด

- 2.2.7 ผู้ดูแลระบบต้องจัดส่งบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ด้วยวิธีการที่ปลอดภัย
- 2.2.8 ผู้ดูแลระบบต้องควบคุมดูแลระบบปฏิบัติการ ฐานข้อมูล และระบบงานสารสนเทศ (Application) ที่จัดเก็บบัญชีผู้ใช้งานและรหัสผ่านอย่างเข้มงวด โดยให้เข้าถึงได้เฉพาะผู้ดูแลระบบที่ได้รับอนุญาตเท่านั้น
- 2.2.9 ผู้ดูแลระบบต้องกำหนดวิธีการหรือกระบวนการยืนยันตัวตนที่ปลอดภัย เช่น กรณีที่ลืมรหัสผ่าน
- 2.2.10 ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานภายนอกที่สมัครใช้บริการระบบงานสารสนเทศของ รพม. ใช้รหัสผ่านอย่างมั่นคงปลอดภัย ดังนี้

กรณีแอปพลิเคชันทั่วไป

- 1) กำหนดความยาวรหัสผ่านอย่างน้อย 8 หลัก ซึ่งประกอบด้วย ตัวอักษร ตัวเลข และอักขระพิเศษ เช่น (a-Z) (0-9) (@ , # , & , “ , ‘ , * , = , < , > , % , \$, + , ?) เป็นต้น
- 2) ไม่บังคับให้เปลี่ยนรหัสผ่าน ทั้งนี้ขึ้นอยู่กับความสมัครใจในการเปลี่ยนรหัสผ่าน และระบบต้องรองรับการเปลี่ยนรหัสผ่านในกรณีต่าง ๆ ด้วยวิธีการที่ปลอดภัย

กรณีแอปพลิเคชันที่ใช้งานผ่านอุปกรณ์เคลื่อนที่ (Mobile device)

- 1) กำหนดรหัสผ่านโดยใช้ PIN code หรือรหัสผ่านที่ซับซ้อน (PIN/Password complexity) โดยกรณี PIN code ต้องใช้รหัสผ่าน 6 หลักขึ้นไป
- 2) ไม่บังคับให้เปลี่ยนรหัสผ่าน ทั้งนี้ขึ้นอยู่กับความสมัครใจในการเปลี่ยนรหัสผ่าน และระบบต้องรองรับการเปลี่ยนรหัสผ่านในกรณีต่าง ๆ ด้วยวิธีการที่ปลอดภัย

2.3 การบริหารจัดการสิทธิ์ (Privilege management)

- 2.3.1 ผู้บังคับบัญชาต้องกำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียน การเพิกถอนสิทธิ์ การเปลี่ยนแปลงสิทธิ์ และการทบทวนสิทธิ์ของผู้ใช้งานอย่างเป็นลายลักษณ์อักษร
- 2.3.2 กำหนดสิทธิ์ที่เหมาะสมกับผู้ใช้งานตามความจำเป็นและสอดคล้องกับหน้าที่ความรับผิดชอบและจัดเก็บประวัติ (Log) การลงทะเบียน การเพิกถอนสิทธิ์ และการเปลี่ยนแปลงสิทธิ์ของผู้ใช้งาน
- 2.3.3 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจัดให้มีการควบคุมและจำกัดสิทธิ์ในการทำงานระบบตามความจำเป็นในการใช้งานเท่านั้น
 - 1) สิทธิ์ในการสร้างข้อมูล (Create)
 - 2) สิทธิ์ในการอ่านข้อมูลหรือเรียกดูข้อมูล (READ)
 - 3) สิทธิ์ในการปรับปรุงข้อมูล (Modify / Update)
 - 4) สิทธิ์ในการลบข้อมูล (Delete)
 - 5) สิทธิ์ในการมอบหมายสิทธิ์ในการดำเนินการแทน (Assign)
 - 6) สิทธิ์ในการรับรองความถูกต้องครบถ้วนของข้อมูล (Approve/Authenticate)
 - 7) ไม่มีสิทธิ์
- 2.3.4 เจ้าของข้อมูลและผู้ดูแลระบบต้องเป็นผู้อนุมัติการให้สิทธิ์เพื่อเข้าถึงสารสนเทศหรือระบบเทคโนโลยีสารสนเทศใด ๆ อย่างเป็นลายลักษณ์อักษร

- 2.3.5 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจำกัดจำนวนผู้ใช้งานที่ทำหน้าที่เป็นผู้ให้สิทธิ์กับผู้ใช้งาน ให้น้อยที่สุดตามความเหมาะสม
- 2.3.6 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจำกัดระยะเวลาการใช้งานระบบเทคโนโลยีสารสนเทศของ รพม. แก่หน่วยงานภายนอกที่เข้ามาปฏิบัติงานร่วมกับ รพม.
- 2.3.7 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจัดให้มีการถอดถอนหรือเปลี่ยนแปลงสิทธิ์การเข้าถึงทันที เมื่อผู้ใช้งานเกษียณ เปลี่ยนแปลงหน้าที่ความรับผิดชอบ เปลี่ยนแปลงการจ้างงาน หรือไม่มีความจำเป็น ในการใช้งานระบบเทคโนโลยีสารสนเทศ
- 2.3.8 ผู้ดูแลระบบต้องลบหรือระงับการใช้งานสิทธิ์ของผู้ใช้งานที่มาจากระบบ (Default user) ในกรณีที่มีความจำเป็นต้องใช้งานต้องกำหนดรหัสผ่านอย่างมั่นคงปลอดภัย
- 2.4 การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of user access rights)
 - 2.4.1 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องมีการสอบทานสิทธิ์การเข้าถึงของผู้ใช้งานระบบ เมื่อ รพม. มีการเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศหรือโครงสร้างองค์กร
 - 2.4.2 ผู้ดูแลระบบ ต้องมีการสอบทานและระงับการใช้งานบัญชีผู้ใช้งานที่ไม่ได้ใช้งานเกิน 180 วัน หากผู้ใช้งานต้องการกลับมาใช้งานจะต้องยืนยันตัวตนให้ ผทพ. ทราบ ทั้งนี้ ระยะเวลาที่ไม่ได้ใช้งานของ บัญชีผู้ใช้งานอาจจะขึ้นอยู่กับแต่ละระบบสารสนเทศ
3. การป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล และการควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ไม่ปลอดภัย
 - 3.1 การป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล (Unattended user equipment)
 - 3.1.1 ผู้ดูแลระบบต้องจัดให้มีมาตรการสำหรับป้องกันระบบคอมพิวเตอร์ ระบบเครือข่ายสื่อสาร ข้อมูล และระบบเทคโนโลยีสารสนเทศ โดยการกำหนดค่าของระบบ (Configuration) ให้มีการล็อกหน้าจอสำหรับอุปกรณ์ที่ไม่มีพนักงานดูแล หรือล็อกอุปกรณ์อยู่เสมอ
 - 3.1.2 ผู้ใช้งานและหน่วยงานภายนอก ต้องล็อกหน้าจออัตโนมัติเมื่อไม่มีการใช้งานระบบเทคโนโลยีสารสนเทศของ รพม. ตามระยะเวลาที่กำหนด โดยต้องพักหน้าจอ (Screen saver) อัตโนมัติ หลังจากที่ไม่มีการใช้งานคอมพิวเตอร์เป็นระยะเวลานานกว่า 15 นาที ผู้ใช้งานและหน่วยงานภายนอก จะใช้งานต่อได้เมื่อมีการใส่รหัสผ่านที่ถูกต้อง
 - 3.1.3 ผู้ใช้งานต้อง Log out ออกจากเครื่องคอมพิวเตอร์เมื่อมีความจำเป็นต้องละทิ้งเครื่องคอมพิวเตอร์
 - 3.1.4 ผู้ใช้งานต้องป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ เช่น กล้องดิจิทัล เครื่องสำเนาเอกสาร เครื่องสแกน เอกสารโดยไม่ได้รับอนุญาต
 - 3.2 การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear desk and clear screen control)
 - 3.2.1 ผู้บังคับบัญชาต้องกำหนดให้มีผู้รับผิดชอบในการดูแลสถานที่ที่มีการรับ - ส่งแฟกซ์ หรือจดหมายเข้า - ออก
 - 3.2.2 ผู้ใช้งานต้องออกจากระบบคอมพิวเตอร์ (Log out) ทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
 - 3.2.3 ผู้ใช้งานต้องจัดเก็บข้อมูลสำคัญแยกต่างหาก และป้องกันให้มีความปลอดภัยอย่างพอเพียง
 - 3.2.4 ผู้ใช้งานต้องนำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

4. การควบคุมการเข้าถึงเครือข่าย (Network access control)
ให้มีการควบคุมการใช้งานบริการเครือข่าย การควบคุมการพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอก รพม. การควบคุมการพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย การป้องกันพอร์ต (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ การแบ่งแยกเครือข่าย (Segregation in networks) อย่างเหมาะสม การควบคุมการเชื่อมต่อทางเครือข่าย และการควบคุมการกำหนดเส้นทางบนเครือข่าย
- 4.1 การใช้งานบริการเครือข่าย (Use of network services)
 - 4.1.1 ผู้ดูแลระบบต้องควบคุมการเผยแพร่แผนผังระบบเครือข่ายสื่อสารข้อมูล (Network diagram) รวมถึงโครงสร้าง IP address ของระบบ และชื่ออุปกรณ์สารสนเทศแก่ผู้ที่ไม่ได้รับอนุญาตหรือหน่วยงานภายนอก
 - 4.1.2 ผู้ดูแลระบบต้องควบคุมการใช้งานระบบเครือข่ายสื่อสารข้อมูล เพื่อป้องกันการเข้าถึงระบบเครือข่ายสื่อสารข้อมูลและบริการของระบบเครือข่ายสื่อสารข้อมูลโดยไม่ได้รับอนุญาต
 - 4.1.3 ผู้ดูแลระบบต้องควบคุมการเชื่อมต่อเครือข่ายภายนอก เพื่อใช้งานอินเทอร์เน็ต ซึ่งอาจเป็นช่องทางให้หน่วยงานภายนอกเข้าถึงสารสนเทศหรือระบบเทคโนโลยีสารสนเทศของ รพม. โดยมิได้รับอนุญาต
 - 4.1.4 ผู้ใช้งานต้องแจ้งความประสงค์ในการขอใช้งานบริการเครือข่ายแก่ ผทท. และสามารถใช้บริการเครือข่ายได้หลังจากได้รับการอนุมัติจาก ผทท. แล้ว
 - 4.1.5 ผู้ใช้งาน ต้องไม่ใช้ระบบเครือข่ายสื่อสารข้อมูลเพื่อเป็นช่องทางในการเจาะระบบ (Hacking) หรือการสแกนช่องโหว่ของระบบโดยมิได้รับอนุญาต
- 4.2 การพิสูจน์ตัวตนของผู้ใช้งานที่อยู่ภายนอก รพม. (User authentication for external connections)
ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนผ่านระบบ Active directory ของ รพม. ก่อนอนุญาตให้ผู้ใช้งานที่อยู่ภายนอก รพม. เข้าใช้งานเครือข่ายและระบบสารสนเทศของ รพม.
- 4.3 การพิสูจน์ตัวตนของอุปกรณ์ในระบบเครือข่ายสื่อสารข้อมูล (Equipment identification in networks)
ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนของอุปกรณ์ในระบบเครือข่ายสื่อสารข้อมูล ได้แก่ การตรวจสอบ MAC address
- 4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection)
ผู้ดูแลระบบต้องระงับบริการและพอร์ต (Port) ที่ไม่มีความจำเป็นต้องใช้บนเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่าย
- 4.5 ผู้ดูแลระบบต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion prevention system/ intrusion detection system) ของระบบเครือข่าย
- 4.6 การแบ่งแยกเครือข่าย (Segregation in networks)
 - 4.6.1 ผู้ดูแลระบบต้องจัดให้มีการแบ่งแยกเครือข่ายตามกลุ่มของผู้ใช้งาน หรือกลุ่มของระบบเทคโนโลยีสารสนเทศ เพื่อควบคุมการใช้งานในแต่ละเครือข่ายย่อยอย่างเหมาะสม โดยพิจารณา

จากความต้องการในการเข้าถึงข้อมูล ระดับความสำคัญของข้อมูล รวมถึงการพิจารณาด้านราคา ประสิทธิภาพ และผลกระทบทางด้านความปลอดภัยดังต่อไปนี้

- 1) เครือข่ายที่อนุญาตให้เข้าถึงจากภายนอกและเครือข่ายที่ใช้ภายใน รพม.
- 2) เครือข่ายแอปพลิเคชัน (Application) ที่มีความสำคัญกับเครือข่ายอื่น ๆ ที่มีความสำคัญน้อยกว่า
- 3) เครือข่ายสำหรับเครื่องให้บริการ (Server farm) กับเครือข่ายของผู้ใช้งาน ควรมีการติดตั้งอุปกรณ์ที่สามารถแบ่งแยกเครือข่ายได้ เช่น Firewall หรือ Switch ที่สามารถแบ่ง VLAN ได้ เป็นต้น

4.6.2 ผู้ดูแลระบบจะกำหนดเส้นทางบนเครือข่ายที่เข้มงวด เพื่อจำกัดการเข้าถึงระยะไกลไปเฉพาะเครือข่ายที่กำหนดเท่านั้น

4.6.3 ผู้ดูแลระบบต้องตั้งค่า (Configuration) อุปกรณ์เครือข่าย เช่น Firewall หรือ Router มิให้สามารถบริหารจัดการจากภายนอกเครือข่ายได้ เว้นแต่ในกรณีฉุกเฉินซึ่งต้องได้รับการอนุญาตจากผู้ดูแลระบบเท่านั้น

4.7 การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control)

4.7.1 ผู้ดูแลระบบต้องจำกัดการใช้งานเครือข่ายของผู้ใช้งานในการเชื่อมต่อกับเครือข่ายของ รพม. เช่น Router หรือ Firewall เป็นต้น พร้อมทั้งติดตั้งระบบควบคุมเพื่อกลั่นกรองข้อมูลที่รับ - ส่ง เช่น Web filtering, E-mail filtering เป็นต้น เพื่อให้การเชื่อมต่อมีความปลอดภัย

4.7.2 ผู้ดูแลระบบต้องติดตั้ง Firewall ระหว่างเครือข่ายของ รพม. กับเครือข่ายภายนอก ทั้งนี้ การติดตั้ง Firewall ต้องพิจารณาเรื่องดังต่อไปนี้

- 1) การป้องกันการจราจรจากภายนอก ต้องถูกกำหนดให้ใช้เส้นทางที่ผ่าน First tier firewall ที่มีความมั่นคงปลอดภัยเพื่อป้องกันการรั่วซึมของข้อมูลของ รพม. และโครงสร้างพื้นฐานที่มีความสำคัญจากการเข้าถึงที่ไม่ได้รับอนุญาต
- 2) Firewall ต้องระบุตัวตนและพิสูจน์ตัวตนของผู้ใช้งานก่อนที่จะให้สิทธิ์การเข้าถึงอินเทอร์เน็ตเฟส (Interface) เพื่อการบริหารจัดการ Firewall
- 3) Firewall ต้องตั้งค่าให้ระงับบัญชีผู้ใช้งานหลังจากมีความพยายามที่จะเข้าสู่ระบบไม่สำเร็จ 5 ครั้ง การยกเลิกการระงับต้องดำเนินการโดย ผทท.
- 4) ไม่อนุญาตให้พิสูจน์ตัวตนผ่านทางอินเทอร์เน็ตเฟส (Interface) การจัดการ Firewall จากระยะไกล (Remote)
- 5) ผู้ที่ได้รับการมอบหมายจาก ผทท. เท่านั้นที่มีสิทธิ์ที่จะเปลี่ยนการตั้งค่าด้านความปลอดภัยบน Firewall
- 6) Firewall ต้องตั้งค่าให้บันทึกเหตุการณ์ด้านความมั่นคงปลอดภัย
- 7) Firewall ต้องได้รับการสอบทาน ทดสอบ และตรวจสอบอย่างสม่ำเสมอ
- 8) Firewall ต้องถูกบริหารจัดการผ่านการติดต่อสื่อสารที่มีการเข้ารหัส
- 9) ต้องปิดบริการและพอร์ต (Port) ที่ไม่จำเป็นต้องใช้บน Firewall
- 10) Firewall ประเภทซอฟต์แวร์ (Software) ต้องติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายแยกต่างหาก

- 11) Firewall ต้องสามารถป้องกันตัวเองจากการโจมตี DOS (Denial of service) ได้อย่างเช่น Ping, Sweeps หรือ TCP SYN Floods เป็นต้น
- 12) ต้องใช้เวอร์ชันของซอฟต์แวร์ (Software) Firewall และระบบปฏิบัติการที่เจ้าของผลิตภัณฑ์ยังให้การสนับสนุน
- 13) ผู้ดูแล Firewall ต้องติดตามข้อมูลช่องโหว่จากผู้ให้บริการ (Vendor) เพื่อรับทราบข่าวสารการ Upgrade และแพตช์ (Patch) ที่จำเป็น และต้องติดตั้งแพตช์ (Patch) ทั้งหมดที่เกี่ยวข้อง

4.7.3 ผู้ดูแลระบบต้องติดตั้ง Firewall เพื่อแบ่งแยก Zone ให้มีการใช้ DMZ (Demilitarized zone) โดยต้องพิจารณาเรื่องดังต่อไปนี้

- 1) เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการผ่านอินเทอร์เน็ต เช่น FTP, Email, Web และ External DNS server เป็นต้น ต้องติดตั้งอยู่ใน DMZ
- 2) การเข้าถึงจากระยะไกลต้องพิสูจน์ตัวตนที่ Firewall หรือผ่านบริการที่อยู่ใน DMZ
- 3) DNS Servers ต้องไม่อนุญาตให้มีการแลกเปลี่ยนโซน (Zone transfers) เว้นแต่มีเหตุจำเป็น

4.8 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control)

ผู้ดูแลระบบต้องควบคุมการกำหนดเส้นทางบนเครือข่ายเพื่อให้มั่นใจว่าการเชื่อมต่อเครื่องคอมพิวเตอร์และการไหลเวียนของสารสนเทศบนเครือข่าย โดยมีกลไกในการตรวจสอบที่อยู่ปลายทางและต้นทางของการเชื่อมต่อ เช่น การควบคุมโดย Firewall หรือ Proxy เป็นต้น

5. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)

ให้มีการควบคุมการเข้าถึงระบบปฏิบัติการอย่างมั่นคงปลอดภัย การควบคุมการระบุและพิสูจน์ตัวตนของผู้ใช้งาน การควบคุมระบบบริหารจัดการรหัสผ่าน การควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ (System utilities) การควบคุมการหมดเวลาการใช้งานระบบเทคโนโลยีสารสนเทศ และควบคุมการจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ

5.1 ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on procedures)

5.1.1 ผู้ดูแลระบบ ต้องจัดให้มีการควบคุมการเข้าถึงระบบปฏิบัติการอย่างมั่นคงปลอดภัยโดยขั้นตอนการเข้าสู่ระบบต้องเปิดเผยข้อมูลเกี่ยวกับระบบให้น้อยที่สุดเพื่อหลีกเลี่ยงผู้ใช้งานที่ไม่ได้รับอนุญาต ซึ่งขั้นตอนการ Log-on ต้องพิจารณา ดังนี้

- 1) หากกระบวนการเข้าสู่ระบบไม่สำเร็จ ระบบต้องไม่แสดงข้อมูลของระบบหรือแอปพลิเคชัน (Application) ที่ใช้งานอยู่
- 2) ระบบต้องแสดงข้อความเตือนผู้ใช้งานว่าสามารถเข้าใช้งานเครื่องคอมพิวเตอร์ได้เฉพาะผู้ที่มีสิทธิ์เท่านั้น
- 3) หากกระบวนการเข้าสู่ระบบไม่สำเร็จ ระบบต้องไม่แสดงข้อมูลที่สามารถระบุตัวตนของระบบ เช่น เครือข่ายที่ใช้งาน สถานที่ตั้งของระบบ หรือชื่อเครื่องคอมพิวเตอร์แม่ข่าย เป็นต้น
- 4) ระบบต้องไม่แสดงข้อความที่ชี้เฉพาะเหตุของการเข้าสู่ระบบไม่สำเร็จ เช่น ไม่แสดงข้อความว่า บัญชีผู้ใช้งานผิด หรือ รหัสผ่านผิด เป็นต้น
- 5) ห้ามเข้าสู่ระบบจากบัญชีผู้ใช้งานส่วนบุคคลเดียวกันมากกว่าหนึ่ง Session ในระบบเดียวกัน

- 6) ระบบต้องจำกัดจำนวนครั้งในการพยายามเข้าสู่ระบบที่ไม่สำเร็จ และต้องพิจารณาเงื่อนไขต่อไปนี้
 - (ก) การเก็บบันทึกผลการเข้าสู่ระบบทั้งที่สำเร็จและไม่สำเร็จ
 - (ข) หน่วงระยะเวลาในการเข้าใช้งานระบบครั้งต่อไป
 - (ค) การตัดการเชื่อมต่อ
 - (ง) การแสดงข้อความเตือนที่หน้าจอของผู้ดูแลระบบเมื่อมีการเข้าสู่ระบบเกินจำนวนครั้งที่จำกัดไว้
 - 7) ระบบต้องแสดงวัน เวลา ในการเข้าสู่ระบบที่สำเร็จในครั้งก่อน พร้อมทั้งบันทึกจำนวนครั้งที่พยายามเข้าไม่สำเร็จนับแต่การเข้าสู่ระบบที่สำเร็จในครั้งก่อนของผู้ใช้งาน
 - 8) ระบบต้องไม่ส่งรหัสผ่านแบบ Clear text ผ่านระบบเครือข่ายสื่อสารข้อมูล
 - 9) ผู้ดูแลระบบต้องกำหนดจำนวนครั้งที่ยอมให้ใส่รหัสผ่านผิดได้ไม่เกิน 5 ครั้ง
- 5.2 การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication)
ผู้ดูแลระบบ ต้องจัดให้ผู้ใช้งานมีบัญชีผู้ใช้งานของแต่ละบุคคลเพื่อใช้พิสูจน์ตัวตนในการเข้าถึงระบบเทคโนโลยีสารสนเทศ และต้องใช้ระบบเทคโนโลยีสารสนเทศพิสูจน์ตัวตนผู้ใช้งานในการเข้าถึงระบบปฏิบัติการ โดยผ่านระบบ Active directory หรือ Lightweight Directory Access Protocol (LDAP) ทุกครั้ง พร้อมทั้งบันทึกข้อมูลการเข้าถึง
- 5.3 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities)
ผู้ดูแลระบบ ต้องควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้บนระบบที่ใช้งานจริง (Production system) ดังนี้
- 5.3.1 ต้องจัดทำบัญชีโปรแกรมประเภทยูทิลิตี้ (System utilities) ที่นำมาใช้งาน
 - 5.3.2 กำหนดความรับผิดชอบในการใช้โปรแกรมประเภทยูทิลิตี้ (System utilities) แต่ละรายการอย่างชัดเจนและสื่อสารให้ผู้เกี่ยวข้องทราบเพื่อถือปฏิบัติ
 - 5.3.3 ให้มีการพิสูจน์ตัวตน และกำหนดสิทธิ์ในการใช้งานโปรแกรมประเภทยูทิลิตี้เฉพาะกลุ่มคนที่มีหน้าที่รับผิดชอบ
 - 5.3.4 มีการบันทึกเหตุการณ์ (Log) การใช้งานโปรแกรมประเภทยูทิลิตี้ และต้องสอบทานจากผู้ดูแลระบบอย่างสม่ำเสมอ
 - 5.3.5 ต้องทำการเพิกถอนหรือระงับโปรแกรมประเภทยูทิลิตี้ที่ไม่จำเป็น
- 5.4 การหมดเวลาการใช้งานระบบสารสนเทศ (Session time-out)
- 5.4.1 ผู้ดูแลระบบต้องกำหนด Session time-out ของระบบเทคโนโลยีสารสนเทศที่ไม่มีการใช้งานภายในระยะเวลา 15 นาที ทั้งนี้ ถ้าระบบที่ไม่สามารถตัดการเชื่อมต่อแบบอัตโนมัติได้ กำหนดให้ใช้โปรแกรมพักหน้าจอที่ต้องใส่รหัสผ่านหรือกำหนดให้มีการล็อกหน้าจอ
 - 5.4.2 ผู้ดูแลระบบ และผู้ใช้งาน ต้องตั้งค่าให้โปรแกรมพักหน้าจอที่ต้องใส่รหัสผ่านสำหรับเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์แบบพกพา และเครื่องคอมพิวเตอร์แม่ข่าย ทั้งนี้ โปรแกรมพักหน้าจอกำหนดให้ป้อนรหัสผ่านหลังจากที่มีการทิ้งเครื่องดังกล่าวไว้โดยไม่มีการใช้งานเป็นเวลา 15 นาที

- 5.5 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)
 - 5.5.1 ผู้ดูแลระบบ ต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง โดยต้องคำนึงระยะเวลาที่จำเป็นในกระบวนการดำเนินงานทางธุรกิจ ได้แก่ กำหนดให้เข้าใช้งานได้ในช่วงเวลาทำการของ รพม. 08.00 น. – 17.00 น. และเชื่อมต่อเพื่อใช้งานได้ครั้งละไม่เกิน 3 ชั่วโมง
 - 5.5.2 ผู้ใช้งาน หากมีความจำเป็นต้องใช้งานนอกเวลาที่กำหนดต้องขออนุมัติจากผู้บังคับบัญชาเท่านั้น
6. การควบคุมการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ (Application and information access control)
ให้มีการจำกัดการเข้าถึงสารสนเทศ และการแยกระบบเทคโนโลยีสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณที่ควบคุมเฉพาะ
 - 6.1 การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)
 - 6.1.1 เจ้าของข้อมูลและผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงแก่ผู้ใช้งานเท่าที่จำเป็นต้องใช้ในการปฏิบัติงาน โดยการให้สิทธิ์ต้องพิจารณาในเรื่องดังต่อไปนี้
 - 1) การจำกัดไม่ให้ใช้ตัวเลือก (Options) ที่ไม่ได้รับอนุญาต
 - 2) การจำกัดการเข้าถึง Command Line
 - 3) การจำกัดการเข้าถึงข้อมูลและฟังก์ชันการใช้งานของแอปพลิเคชัน (Application) ที่ไม่เกี่ยวข้องกับหน้าที่ความรับผิดชอบ
 - 4) การจำกัดระดับสิทธิ์ในการเข้าถึงไฟล์ เช่น อ่านอย่างเดียว เป็นต้น
 - 5) การควบคุมการแจกจ่าย การเข้าถึงข้อมูล การนำข้อมูลออกจากระบบสารสนเทศ เช่น รายงาน เป็นต้น
 - 6.1.2 เจ้าของข้อมูลและผู้ดูแลระบบ ควรกำหนดให้ระบบสารสนเทศรองรับการกำหนดสิทธิ์ในการเข้าถึงแบบกลุ่มได้
 - 6.2 การแยกระบบสารสนเทศที่ไวต่อการรบกวน (Sensitive system isolation) มีผลกระทบต่อคนกลุ่มใหญ่ หรือระบบที่มีความสำคัญต่อหน่วยงาน ต้องดำเนินการดังนี้
 - 6.2.1 เจ้าของข้อมูลและผู้ดูแลระบบ แยกระบบซึ่งไวต่อการรบกวนออกจากระบบอื่น ๆ และควบคุมสภาพแวดล้อมของระบบโดยเฉพาะ ได้แก่ ระบบ File sharing ระบบสารสนเทศทางการเงิน และระบบ Active directory โดยเข้าถึงได้ทั้งอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร (Mobile computing and teleworking)
 - 6.2.2 ผู้ดูแลระบบต้องควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์เคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile computing and teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว
 - 6.2.3 เจ้าของข้อมูลที่เป็นเจ้าของระบบสารสนเทศที่มีความสำคัญสูงต้องเป็นผู้อนุญาต ในกรณีที่ระบบสารสนเทศที่มีความสำคัญสูงมีความจำเป็นต้องทำงานร่วมกับระบบสารสนเทศอื่นที่มีความสำคัญน้อยกว่า
7. การควบคุมการปฏิบัติงานจากภายนอก รพม. (Teleworking)
 - 7.1 ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนการใช้งาน และเชื่อมต่อผ่านช่องทางที่มีความปลอดภัยที่มีเทคโนโลยีเข้ารหัสป้องกัน

- 7.2 ผู้ดูแลระบบต้องทำการถอดถอนสิทธิ์ในการเข้าถึงของผู้ใช้งานจากภายนอกสำนักงาน เมื่อครบกำหนดระยะเวลาที่ขออนุญาต
- 7.3 ผู้ใช้งาน หากจำเป็นต้องมีการปฏิบัติงานจากภายนอกสำนักงานของ รพม. ต้องได้รับการอนุญาตจากผู้บังคับบัญชาอย่างเป็นทางการเป็นลายลักษณ์อักษร ในกรณีเร่งด่วนสามารถดำเนินการก่อน โดยแจ้งให้ผู้บังคับบัญชารับทราบด้วย โดยผู้บังคับบัญชาต้องพิจารณาเงื่อนไขในการเตรียมการ ดังต่อไปนี้
 - 1) ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมของการปฏิบัติงานจากภายนอก รพม.
 - 2) ความมั่นคงปลอดภัยทางการสื่อสาร โดยยึดจากระดับความสำคัญ (Sensitivity) ของข้อมูลที่จะถูกเข้าถึงและส่งผ่านช่องทางการเชื่อมต่อสื่อสาร (Communication link) รวมถึงระดับความสำคัญ (Sensitivity) ของระบบภายใน รพม.
- 7.4 ผู้ใช้งานต้องจัดเก็บเอกสารที่เป็นความลับในอุปกรณ์ที่ล็อกได้และมีการควบคุมการเข้าถึง โดยใช้หลักเกณฑ์การรักษาความลับเช่นเดียวกับสารสนเทศที่อยู่ในสำนักงานของ รพม.
- 7.5 ผู้ใช้งาน ต้องติดตั้งโปรแกรมป้องกันไวรัสและ Personal firewall สำหรับอุปกรณ์ส่วนตัวที่ใช้เชื่อมต่อเครือข่ายของ รพม. จากภายนอก
8. ผู้บังคับบัญชา ต้องควบคุมการใช้งานข้อมูลส่วนบุคคลให้มีการใช้งานที่สอดคล้องกับกฎหมาย พระราชบัญญัติกฏระเบียบ ข้อบังคับที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ส่วนที่ 7

การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

วัตถุประสงค์

- เพื่อกำหนดมาตรการในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ของ รพม. โดยการกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ
- เพื่อสร้างความมั่นคงปลอดภัยของการทำงานของระบบเครือข่ายไร้สาย

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 5 การควบคุมการเข้าถึง (Access control)
- หมวดที่ 9 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)

แนวปฏิบัติ

1. ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของ รพม. ต้องลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับการอนุญาตจาก ผทท. อย่างเป็นทางการ
2. ผู้ดูแลระบบต้องกำหนดมาตรฐานความปลอดภัยของระบบเครือข่ายไร้สายไม่ต่ำกว่ามาตรฐาน WPA2
3. ผู้ดูแลระบบต้องลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ
4. ผู้ดูแลระบบต้องลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อบนระบบเครือข่ายไร้สาย
5. ผู้ดูแลระบบ ต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีใช้ Access Point (AP) ของ รพม. รับ - ส่งสัญญาณได้
6. ผู้ดูแลระบบต้องเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและต้องสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณอาจช่วยลดการรั่วไหลของสัญญาณให้ดีขึ้น
7. ผู้ดูแลระบบต้องเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำ Access Point (AP) มาใช้งาน
8. ผู้ดูแลระบบต้องเปลี่ยนค่าชื่อ Login และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบต้องเลือกใช้ชื่อ Login และรหัสผ่านที่มีความคาดเดายากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย
9. ผู้ดูแลระบบต้องควบคุม MAC address ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยอนุญาตเฉพาะผู้ใช้งานที่ได้รับอนุญาตให้เข้าใช้เครือข่ายไร้สายได้อย่างถูกต้องเท่านั้น
10. ผู้ดูแลระบบต้องตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ และบันทึกเหตุการณ์น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สายตามขั้นตอนที่ รพม. กำหนด

ส่วนที่ 8

การควบคุมหน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) เข้าถึงระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

- เพื่อควบคุมหน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) ที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของ รพม. ให้เป็นไปอย่างมั่นคงปลอดภัย

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้บังคับบัญชา
- หน่วยงานภายนอก
- ผู้ใช้งาน (บุคคลภายนอก)

อ้างอิงมาตรฐาน

- หมวดที่ 5 การควบคุมการเข้าถึง (Access control)
- หมวดที่ 7 ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environment security)
- หมวดที่ 11 ความสัมพันธ์กับผู้ขาย ผู้ให้บริการภายนอก (Supplier relationships)

แนวปฏิบัติ

1. ผู้ดูแลระบบต้องประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสม ก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศของ รพม.
2. การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก)
 - 2.1 เจ้าของข้อมูลต้องเป็นผู้อนุญาตการให้สิทธิ์แก่หน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) ที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของ รพม. อย่างเป็นลายลักษณ์อักษร
 - 2.2 ผู้บังคับบัญชาต้องกำหนดให้มีการลงนามการไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของ รพม.
 - 2.3 ผู้บังคับบัญชา ต้องควบคุมให้มีการกำหนดข้อตกลงและความรับผิดชอบที่เกี่ยวข้องกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศลงในสัญญากับผู้ให้บริการภายนอกที่ให้บริการด้านสารสนเทศและบริการด้านการสื่อสาร โดยให้ครอบคลุมรวมถึงผู้รับจ้างช่วง
 - 2.4 ผู้บังคับบัญชาต้องกำหนดให้จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) ระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศ ซึ่งมีรายละเอียด ดังนี้
 - 2.4.1 เหตุผลในการขอใช้
 - 2.4.2 ระยะเวลาในการใช้
 - 2.4.3 การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย
 - 2.4.4 การตรวจสอบ MAC address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

- 2.5 ผู้ดูแลระบบมีสิทธิ์ในการตรวจสอบการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) เพื่อควบคุมการใช้งานได้อย่างมั่นคงปลอดภัยตามสัญญา
- 2.6 ผู้ดูแลระบบต้องควบคุมให้หน่วยงานภายนอกจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งต้องปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อใช้สำหรับควบคุมหรือตรวจสอบการทำงาน และเพื่อให้มั่นใจว่าการปฏิบัติงานเป็นไปตามขอบเขตที่ได้กำหนดไว้
3. ผู้ดูแลระบบต้องแจ้งแนวปฏิบัติต่าง ๆ ที่เกี่ยวข้อง แก่ผู้รับจ้างภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) เพื่อให้ปฏิบัติตาม
4. ผู้ดูแลระบบ ต้องกำกับดูแลหน่วยงานภายนอก หรือผู้ใช้งาน (บุคคลภายนอก) ให้ปฏิบัติตามสัญญาหรือข้อตกลงการให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงด้านความมั่นคงปลอดภัย
5. ผู้ดูแลระบบ ต้องติดตาม ตรวจสอบรายงานหรือบันทึกการให้บริการของหน่วยงานภายนอกหรือบุคคลที่ให้บริการแก่หน่วยงานตามที่ว่าจ้างอย่างสม่ำเสมอตามสัญญาว่าจ้าง
6. ผู้ดูแลระบบ ต้องกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีหน้าที่ในการกำกับดูแลหรือหน่วยงานที่เกี่ยวข้องกับการบังคับใช้กฎหมาย รวมทั้งหน่วยงานที่ควบคุมดูแลสถานการณ์ฉุกเฉินภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน
7. ผู้ดูแลระบบ ต้องมีขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีความเชี่ยวชาญเฉพาะด้านหรือหน่วยงานที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน
8. ผู้ดูแลระบบต้องควบคุมการเปลี่ยนแปลงของหน่วยงานภายนอกที่ส่งผลกระทบต่อการให้บริการขององค์กร และต้องประเมินความเสี่ยงอย่างเหมาะสมเพื่อควบคุมผลกระทบอันเนื่องมาจากการเปลี่ยนแปลงนั้น
9. หน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) ต้องใช้งานทรัพย์สินสารสนเทศของ รฟม. ด้วยความระมัดระวัง และรักษาความลับของ รฟม. ไม่นำไปเปิดเผย และต้องขออนุญาตพร้อมทั้งปฏิบัติตามเงื่อนไขในการเข้าถึงระบบสารสนเทศของ รฟม. ทุกครั้ง

ส่วนที่ 9

การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ ของ รพม.

วัตถุประสงค์

- เพื่อควบคุมการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ ที่ รพม. จัดไว้ให้ใช้อย่างเหมาะสม ทั้งนี้ เพื่อป้องกันการสูญหาย เสียหาย หรือถูกเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 2 อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากระยะไกล (Mobile devices and teleworking)
- หมวดที่ 4 การบริหารจัดการทรัพย์สิน (Asset management)
- หมวดที่ 8 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations security)

แนวปฏิบัติ

1. การใช้งานทั่วไป

- 1.1 ผู้ดูแลระบบต้องกำหนดบัญชีซอฟต์แวร์มาตรฐาน (Software standard) ที่อนุญาตให้ติดตั้งบนเครื่องคอมพิวเตอร์ของผู้ใช้งาน และปรับปรุงให้เป็นปัจจุบันเสมอ
- 1.2 ผู้ดูแลระบบต้องเป็นผู้กำหนดการตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) เท่านั้น
- 1.3 ผู้ใช้งานต้องใช้งานอย่างมีประสิทธิภาพเพื่องานของ รพม.
- 1.4 ผู้ใช้งานต้องไม่ติดตั้งโปรแกรมที่ละเมิดลิขสิทธิ์บนเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ของ รพม.
- 1.5 ผู้ใช้งานต้องขออนุญาตติดตั้งโปรแกรมในเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ตามขั้นตอนที่ รพม. กำหนด
- 1.6 ผู้ใช้งานต้องไม่ติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ของ รพม. การดำเนินการดังกล่าวต้องดำเนินการโดยผู้ดูแลระบบเท่านั้น
- 1.7 ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่อย่างละเอียด เพื่อให้สามารถใช้งานอย่างปลอดภัยและมีประสิทธิภาพ
- 1.8 ผู้ใช้งานต้องไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ และรักษาให้มีสภาพเดิม
- 1.9 ผู้ใช้งานต้องแจ้งซ่อมเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่เพื่อให้ ผทท. เป็นผู้ดำเนินการเท่านั้น
- 1.10 ผู้ใช้งานต้องไม่สร้าง Shortcut ไว้บน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของ รพม.
- 1.11 กรณีเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์เคลื่อนที่ ผู้ใช้งานต้องปฏิบัติ ดังนี้
 - 1.11.1 ในกรณีที่มีการใช้งานอุปกรณ์ประเภทพกพาในที่สาธารณะ ห้องประชุม และพื้นที่ภายนอก อื่น ๆ ที่ไม่มีการป้องกัน หรือไม่ได้อยู่ในบริเวณของ รพม. ให้ป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต เช่น ไม่เปิดการเชื่อมต่อแบบไร้สายโดยไม่มีการเข้ารหัสข้อมูล เป็นต้น

- 1.11.2 ต้องระมัดระวังการเคลื่อนย้าย โดยต้องใส่กระเป๋าเพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงานหรือหลุดมือ เป็นต้น
 - 1.11.3 ไม่ใส่ในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับหรืออาจถูกจับโยนได้
 - 1.11.4 การใช้งานเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัดต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะเวลาหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง
 - 1.11.5 หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอย ชีตข่วน หรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้
 - 1.11.6 ไม่วางของทับบนหน้าจอและแป้นพิมพ์
 - 1.11.7 การเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น
 - 1.11.8 ไม่เคลื่อนย้ายเครื่องในขณะที่ Harddisk กำลังทำงาน
 - 1.11.9 ไม่ใช่หรือวางใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่าง ๆ เป็นต้น
 - 1.11.10 ไม่วางใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูง เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น
 - 1.11.11 ไม่ติดตั้งหรือวางในที่ที่มีการสั่นสะเทือน เช่น ในยานพาหนะที่กำลังเคลื่อนที่
 - 1.11.12 การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้
 - 1.11.13 รับผิดชอบในการป้องกันการสูญหาย เช่น ต้องล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย
 - 1.11.14 นำติดตัวไปด้วยเสมอ เช่น ไม่ละทิ้ง อุปกรณ์ประมวลผลประเภทพกพาในรถยนต์ ห้องพักในโรงแรม หรือห้องประชุม เป็นต้น ในกรณีที่มีความจำเป็นต้องละทิ้งให้จัดเก็บไว้ในสถานที่ที่มั่นคงปลอดภัย
 - 1.11.15 ไม่เก็บหรือใช้งานในสถานที่ที่มีความร้อน ความชื้นหรือฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ
 - 1.11.16 ไม่เปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub component) ที่ติดตั้งอยู่ภายใน เช่น แบตเตอรี่ หน่วยความจำ
2. แนวปฏิบัติในการใช้รหัสผ่าน
ให้ผู้ใช้งานปฏิบัติตามการใช้งานรหัสผ่าน (Password Use) (ส่วนที่ 6)
 3. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malicious code)
 - 3.1 ผู้ดูแลระบบต้องควบคุมการ Update ระบบปฏิบัติการ เว็บเบราว์เซอร์ และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ
 - 3.2 ผู้ดูแลระบบต้องติดตั้งและปรับปรุงโปรแกรมป้องกันไวรัสให้ทันสมัยอยู่เสมอ
 - 3.3 ผู้ใช้งานต้องไม่ปิดหรือยกเลิกระบบการป้องกันไวรัสที่ติดตั้งอยู่

- 3.4 ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อบันทึกต่าง ๆ เช่น Thumb drive และ Data storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์ของ รพม.
- 3.5 ผู้ใช้งาน หากพบหรือสงสัยว่าเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ติดชุดคำสั่งไม่พึงประสงค์ ให้รีบยกเลิกเชื่อมต่อเครื่องเข้ากับระบบเครือข่ายสื่อสารข้อมูลเพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่น ๆ ได้ และแจ้ง ผทท. ทราบทันที
4. การสำรองข้อมูลและการกู้คืน
 - 4.1 ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ไว้บนสื่อบันทึกอื่น ๆ เช่น ระบบ File Sharing, CD, DVD, External harddisk เป็นต้น
 - 4.2 ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลสำรองไว้อย่างสม่ำเสมอ
5. ผู้ดูแลระบบ ต้องควบคุมให้เครื่องคอมพิวเตอร์ได้รับการปรับตั้งค่าอย่างเหมาะสม เพื่อป้องกันการใช้งานหรือติดตั้ง Mobile code เช่น Active x, Java จากแหล่งที่ไม่น่าเชื่อถือ

ส่วนที่ 10

การใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์

วัตถุประสงค์

- เพื่อควบคุมการใช้งานอินเทอร์เน็ตและการใช้งานสื่อสังคมออนไลน์ (Social network) ของ รพม. ให้มีความปลอดภัย และป้องกันการละเมิดพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ จนส่งผลกระทบต่อ รพม.

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 5 การควบคุมการเข้าถึง (Access control)
- หมวดที่ 8 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations security)
- หมวดที่ 18 ความสอดคล้อง (Compliance)

แนวปฏิบัติ

1. ผู้ดูแลระบบต้องควบคุมการเชื่อมต่อทางเครือข่ายสำหรับการเข้าถึงอินเทอร์เน็ตโดยพิจารณาเรื่องดังต่อไปนี้
 - 1) ผู้ดูแลระบบต้องไม่อนุญาตให้ใช้งานอุปกรณ์ Video streaming อุปกรณ์ audio streaming หรือ Download ไฟล์ที่มีขนาดใหญ่ ในกรณีที่ต้องได้รับการอนุญาตจากผู้บังคับบัญชาก่อนเท่านั้น
 - 2) ผู้ดูแลระบบต้องจำกัดการใช้งานอินเทอร์เน็ตเพื่อเรื่องส่วนตัวหรือที่ไม่ใช่การดำเนินงานของ รพม. ให้น้อยที่สุดเท่าที่เป็นไปได้ เช่น การระงับการเข้าถึง Website ที่ไม่จำเป็น การระงับการเข้าถึง Website ที่มีเนื้อหาต้องห้ามตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
 - 3) ผู้ดูแลระบบต้องป้องกันไม่ให้มีการรับส่งข้อมูลที่ไม่เหมาะสมจากภายนอก รพม. เช่น
 - (ก) Executable เช่น .EXE .COM เป็นต้น
 - (ข) ไฟล์ (File) เสียง เช่น AUD .WAV และ.MP3 เป็นต้น
 - (ค) ไฟล์ (File) วิดิทัศน์ เช่น .MPG .MPEG .MOV และ .AVI เป็นต้น
 - (ง) Peer to Peer เช่น .torrent เป็นต้นในกรณีที่มีความจำเป็นต้องได้รับอนุญาตจากผู้บังคับบัญชา และ ผทท.
 - 4) ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่ รพม. จัดสรรไว้เท่านั้น เช่น Proxy, Firewall เป็นต้น
 - 5) ผู้ดูแลระบบต้องทดสอบเส้นทางสำหรับการเชื่อมต่ออินเทอร์เน็ตขององค์กรระหว่างเส้นทางที่ใช้งานจริงและเส้นทางสำรองอย่างน้อยปีละ 2 ครั้ง
 - 6) ผู้ใช้งานต้องไม่เชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นมีความจำเป็นและขออนุญาตจาก ผทท. เป็นลายลักษณ์อักษรแล้ว
 - 7) ผู้ใช้งานต้องขออนุญาตติดตั้งซอฟต์แวร์ (Software) ที่ Download จากอินเทอร์เน็ต และการติดตั้งต้องดำเนินการโดยผู้ที่ได้รับมอบหมายจากผู้ดูแลระบบเท่านั้น

2. ผู้ใช้งานต้องไม่มีเจตนาปิดบังหรือบิดเบือนตัวตนเมื่อมีการใช้งานอินเทอร์เน็ต
3. ผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัส พร้อมทั้งต้องปรับปรุง Virus signature ที่เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพาให้มีความทันสมัยอยู่เสมอ ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web browser) และต้องปิดช่องโหว่ของระบบปฏิบัติการที่เว็บเบราว์เซอร์ติดตั้งอยู่
4. ผู้ใช้งานจะต้องตรวจสอบไวรัส (Virus scanning) ก่อนการรับ - ส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ต
5. ผู้ใช้งานต้องไม่ใช่เครือข่ายอินเทอร์เน็ตของ รพม. เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น
6. ผู้ใช้งานจะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของ รพม.
7. ผู้ใช้งานต้องหลีกเลี่ยงการกระทำที่สิ้นเปลืองทรัพยากรของเครือข่ายอินเทอร์เน็ต ดังนี้
 - (ก) ส่งจดหมายอิเล็กทรอนิกส์ที่มีขนาดใหญ่หรือจดหมายอิเล็กทรอนิกส์ลูกโซ่
 - (ข) ใช้เวลาในการเข้าถึงอินเทอร์เน็ตเกินความจำเป็น
 - (ค) เล่นเกม Online
 - (ง) เข้าห้องพูดคุย Online
8. ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับ รพม.
9. ผู้ใช้งานต้องไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของ รพม.
10. ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต
11. ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อเติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ที่จะทำให้อื่นเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย
12. ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน
13. ผู้ใช้งานต้องคำนึงว่าข้อมูลจากอินเทอร์เน็ตอาจไม่มีความทันสมัยหรือไม่มีความถูกต้อง ผู้ใช้งานต้องตรวจสอบความถูกต้องของข้อมูลจากแหล่งที่น่าเชื่อถือก่อนที่จะเผยแพร่ข้อมูลดังกล่าว
14. ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา
15. ผู้ใช้งานต้องไม่ใช่ข้อมูลที่ร้ายๆ ให้อภัยในการเสนอความคิดเห็นที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของ รพม. การทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น ๆ
16. ผู้ใช้งานต้องไม่บันทึกรหัสผ่านใน Web browser (Remember password) เพื่อป้องกันบุคคลอื่นที่สามารถเข้าถึงคอมพิวเตอร์ของผู้ใช้งานนำรหัสผ่านดังกล่าวไปใช้งานในอินเทอร์เน็ตโดยไม่ได้รับอนุญาต

17. ผู้ใช้งานต้องไม่ Download เอกสาร หรือสารสนเทศต่าง ๆ เช่น ข้อมูล รูปภาพ วิดีโอ เสียง และซอฟต์แวร์ (Software) ที่ละเมิดลิขสิทธิ์ หรือผิดกฎหมาย
18. ผู้ใช้งานต้องปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ ภายหลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว
19. การใช้งานสื่อสังคมออนไลน์ (Social network)
 - 19.1 ผู้ใช้งานต้องระมัดระวังในการนำเสนอข้อมูลข่าวสาร การส่งข้อความ หรือการแสดงความคิดเห็นผ่านสื่อสังคมออนไลน์เพื่อไม่ก่อให้เกิดความเสียหายแก่ รพม.
 - 19.2 ผู้ใช้งานต้องระมัดระวังในการใช้สื่อสังคมออนไลน์ เนื่องจากพื้นที่บนสื่อสังคมออนไลน์เป็นพื้นที่สาธารณะไม่ใช่พื้นที่ส่วนบุคคล ซึ่งข้อมูลการใช้งานต่าง ๆ จะถูกบันทึกไว้และอาจมีผลทางกฎหมายถึงแม้จะเป็นการแสดงความคิดเห็นในนามชื่อบัญชีส่วนตัว และพึงตระหนักถึงผลกระทบที่อาจเกิดขึ้นกับ รพม. ได้
 - 19.3 ผู้ใช้งานที่ใช้สื่อสังคมออนไลน์เป็นเครื่องมือสื่อสารข้อมูลในกิจการของ รพม. หรือชื่อบุคคลที่ทำให้เข้าใจได้ว่าเป็นบุคคลในสังกัด ต้องแสดงภาพ และข้อมูลให้ถูกต้องชัดเจนในข้อมูล โปรไฟล์ (Profile) และพึงใช้ด้วยความสุภาพและมีวิจารณญาณ
 - 19.4 ผู้ใช้งานควรตั้งคำถามที่ใช้ในกรณีกู้คืนบัญชีผู้ใช้งานหรือกู้คืนรหัสผ่าน (Forgot your password) ควรเลือกใช้ข้อมูลหรือคำถามที่เป็นส่วนบุคคลและเป็นข้อมูลที่ผู้อื่นคาดเดาได้ยากเพื่อป้องกันการสุ่มคำถามจากผู้ประสงค์ร้าย
 - 19.5 ผู้ใช้งานต้องไม่ใช้ระบบอีเมลของเว็บไซต์ประเภทสื่อสังคมออนไลน์ หากจำเป็นต้องใช้จะต้องระมัดระวังในการคลิกลิงก์ที่น่าสงสัย โดยเฉพาะอีเมลแจ้งเตือนจากเว็บไซต์ต่าง ๆ ในลักษณะเชื้อเชิญให้คลิกลิงก์ที่แนบมาในอีเมล ผู้ใช้งานต้องสงสัยว่าลิงก์ดังกล่าวเป็นลิงก์ที่ไม่ปลอดภัย (ลิงก์ที่ถูกสร้างมาเพื่อใช้ขโมยข้อมูลส่วนบุคคล ด้วยการนำไปสู่เว็บไซต์ที่ดูน่าเชื่อถือที่ผู้ประสงค์ร้ายสร้างไว้เพื่อให้ผู้ใช้งานกรอกข้อมูลส่วนตัว เช่น รหัสผ่าน เป็นต้น)
 - 19.6 ผู้ใช้งานต้องศึกษาการตั้งค่าความเป็นส่วนตัวหรือ “Privacy settings” ให้เข้าใจเป็นอย่างดีและปรับแต่งการตั้งค่าความเป็นส่วนตัวให้เหมาะสมเพื่อป้องกันการถูกละเมิดความเป็นส่วนตัวซึ่งอาจจะส่งผลกระทบต่อตนเองหรือ รพม.
 - 19.7 ผู้ใช้งานต้องใช้งานสื่อสังคมออนไลน์อย่างเหมาะสม โดยไม่ละเมิดกฎหมายและไม่ก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานขององค์กร
 - 19.8 ผู้ใช้งานควรปิดการใช้งานระบบโพสต์ข้อความสาธารณะทุก ๆ ส่วนของเว็บไซต์ประเภท Social network หากจำเป็นต้องใช้งานต้องปรับค่าให้มีการตรวจสอบข้อความก่อนเพื่อหลีกเลี่ยงโอกาสแพร่กระจายลิงก์ที่ไม่ปลอดภัยจากผู้ประสงค์ร้าย ซึ่งเป็นหนึ่งในเทคนิคที่ใช้ในการโจมตีประเภท Spear-phishing
 - 19.9 ผู้ใช้งานต้องตรวจสอบก่อนจะรับเพื่อนเข้ากลุ่มในเว็บไซต์ประเภท Social network โดยต้องแน่ใจว่าข้อมูลส่วนตัวของเพื่อนคนนั้น เช่น รูปถ่ายและประวัติส่วนตัวไม่ถูกแก้ไขเพื่อปลอมแปลงตัวตนจากผู้ประสงค์ร้ายที่หวังแอบอ้างเพื่อคุกคามเป้าหมาย

- 19.10 ผู้ใช้งานต้องตระหนักไว้เสมอว่าข้อมูลต่าง ๆ ที่ผู้ใช้งานเผยแพร่ไว้บนบริการสื่อสังคมออนไลน์นั้น คงอยู่ถาวรและผู้อื่นอาจเข้าถึงและเผยแพร่ข้อมูลเหล่านั้นได้
- 19.11 ผู้ใช้งานต้องมีข้อพิจารณาในการรับเพื่อนเข้ากลุ่มที่ชัดเจน และควรประกาศข้อความปฏิเสธความรับผิดชอบที่เกี่ยวกับเนื้อหาหรือข้อความแสดงความคิดเห็นซึ่งถูกโพสต์จากเพื่อนในกลุ่มที่อาจปรากฏในเว็บไซต์ประเภท Social network ของผู้ใช้งานเอง
- 19.12 ผู้ใช้งานต้องติดตั้งซอฟต์แวร์ป้องกันไวรัส และอัปเดตฐานข้อมูลไวรัสของโปรแกรมอยู่เสมอ และต้องหลีกเลี่ยงการใช้โปรแกรมที่ละเมิดลิขสิทธิ์เพราะอาจจะมีโปรแกรมประสงค์ร้ายแฝงตัวอยู่ภายในเพื่อลักลอบ ปลอมแปลง หรือขโมยข้อมูลสำคัญของผู้ใช้งานได้
- 19.13 ผู้ใช้งานต้องระมัดระวังการใช้ถ้อยคำและภาษาที่อาจเป็นการดูหมิ่น ยุ้ง ทำทนาย หรือเป็นการละเมิดต่อบุคคลอื่น กรณีบุคคลอื่นมีความคิดเห็นที่แตกต่างพึงงดเว้นการโต้ตอบด้วยถ้อยคำรุนแรง
- 19.14 ผู้ใช้งานต้องระมัดระวังกระบวนการหาข่าว หรือภาพจากสื่อสังคมออนไลน์ โดยมีการตรวจสอบอย่างถี่ถ้วนรอบด้านและต้องอ้างอิงแหล่งที่มาเมื่อนำเสนอ เว้นแต่สามารถตรวจสอบและอ้างอิงจากแหล่งข่าวได้โดยตรง
- 19.15 หากผู้ใช้งานต้องการใช้สื่อสังคมออนไลน์เป็นเครื่องมือในการรายงานข่าวในนามของบุคคลธรรมดา ต้องแสดงให้เห็นชัดเจนว่า ข้อความใดเป็น "ข่าว" ข้อความใดเป็น "ความคิดเห็นส่วนตัว"
- 19.16 การส่งต่อหรือเผยแพร่ข้อมูลในสื่อสังคมออนไลน์ (Social media)
 - 19.16.1 ผู้ใช้งานต้องไม่ส่งต่อหรือเผยแพร่ข้อมูลที่เป็นเท็จ ข่าวลือ ข่าวไม่ปรากฏที่มา เป็นเพียงการคาดเดา หรือส่งผลเสียหายกับบุคคล สังคม หรือ รฟม.
 - 19.16.2 ผู้ใช้งานต้องไม่ส่งต่อหรือเผยแพร่ข้อมูลเรื่องบุคคลเสียชีวิต เด็กและเยาวชน ผู้สูญหาย ผู้ต้องหา เว้นเสียแต่ตรวจสอบข้อเท็จจริงแล้วและเห็นว่าเป็นประโยชน์ต่อสาธารณะ
 - 19.16.3 ผู้ใช้งานต้องไม่ส่งต่อหรือเผยแพร่ข้อมูลที่กระทบต่อสิทธิความเป็นส่วนตัว และศักดิ์ศรีความเป็นมนุษย์
- 19.17 ผู้ใช้งานต้องตั้งค่าความปลอดภัยของการใช้งานสื่อสังคมออนไลน์ และระมัดระวังการถูกนำข้อมูลจากข้อบัญชีไปใช้โดยไม่เหมาะสม ผิดวัตถุประสงค์ และลักษณะการแอบอ้างโดยบุคคลอื่น
20. ผู้ใช้งานต้องใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์โดยตระหนักถึงพระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่บังคับใช้อยู่เสมอ

ส่วนที่ 11

การใช้งานจดหมายอิเล็กทรอนิกส์

วัตถุประสงค์

- เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ของ รพม. ให้มีความปลอดภัยและมีประสิทธิภาพ

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 5 การควบคุมการเข้าถึง (Access control)
- หมวดที่ 8 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations security)

แนวปฏิบัติ

1. ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของ รพม. ให้เหมาะสมกับหน้าที่ความรับผิดชอบของผู้ใช้งาน รวมทั้งทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ
2. ผู้ดูแลระบบต้องกำหนดบัญชีผู้ใช้งานตามมาตรฐานจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ใช้ในองค์กร
3. ผู้ใช้งานต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ไม่ให้เกิดความเสียหายต่อ รพม. ละเมิดลิขสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น ผิดกฎหมาย ละเมิดศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่น แสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ของ รพม.
4. ผู้ใช้งานต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail address) ของผู้อื่นเพื่ออ่าน รับ - ส่งข้อความ ยกเว้น ได้รับการยินยอมจากเจ้าของบัญชีและให้ถือว่าเจ้าของบัญชีจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน
5. ผู้ใช้งานต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของ รพม. เพื่อปฏิบัติงาน ติดต่อ และประสานงานของ รพม. เท่านั้น
6. ผู้ใช้งานต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ฟรีของเอกชนในการปฏิบัติงาน ติดต่อ และประสานงานของ รพม.
7. ผู้ใช้งานต้อง Logout ออกจากระบบทุกครั้ง หลังจากใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้นเพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์
8. ผู้ใช้งานต้องตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนเปิดอ่าน โดยใช้โปรแกรมป้องกันไวรัส เพื่อตรวจสอบมัลแวร์ต่าง ๆ
9. ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์ที่ได้รับจากผู้ส่งที่ไม่รู้จัก
10. ผู้ใช้งานต้องใช้ข้อความที่สุภาพในการรับ - ส่งจดหมายอิเล็กทรอนิกส์ และไม่จัดส่งจดหมายที่มีเนื้อหาอาจทำให้อับอาย รพม. เสียชื่อเสียงหรือทำให้เกิดความแตกแยกภายใน รพม.
11. ผู้ใช้งานต้องไม่ระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์และต้องเข้ารหัสเพื่อป้องกันการเข้าถึงข้อมูลโดยผู้ไม่เกี่ยวข้องเมื่อมีการส่งข้อมูลที่เป็นความลับ
12. ผู้ใช้งานต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และต้องจัดเก็บจดหมายอิเล็กทรอนิกส์ในตู้ของตนให้เหลือจำนวนน้อยที่สุด หากมีข้อมูลที่จำเป็นต้องนำมาใช้อ้างอิงในการปฏิบัติงานภายหลัง ให้ผู้ใช้งานโอนย้ายจดหมายอิเล็กทรอนิกส์มายังเครื่องคอมพิวเตอร์ของตน ทั้งนี้ เพื่อลดปริมาณการใช้เนื้อที่ของระบบจดหมายอิเล็กทรอนิกส์

ส่วนที่ 12

การสำรองข้อมูลและการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

วัตถุประสงค์

- เพื่อให้มีข้อมูลสำรองไว้ใช้งานในกรณีที่ข้อมูลหลักเกิดความเสียหายไม่สามารถใช้งานหรือเข้าถึงได้ หรือเมื่อเกิดภาวะฉุกเฉินต่าง ๆ
- เพื่อให้มีการปฏิบัติที่สอดคล้องกับกฎหมาย พระราชบัญญัติ หรือข้อบังคับภายนอกอื่น ๆ

ผู้รับผิดชอบ

- ผู้บังคับบัญชา
- ผู้ดูแลระบบ
- เจ้าของข้อมูล
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 8 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations security)
- หมวดที่ 14 ความสอดคล้อง (Compliance)

แนวปฏิบัติ

1. การสำรองข้อมูลระบบแม่ข่าย

ข้อมูลระบบแม่ข่ายและข้อมูลสำคัญซึ่งเป็นความลับของ รฟม. ต้องได้รับการเก็บรักษาไว้ที่ระบบเก็บข้อมูลส่วนกลาง และสำรองข้อมูลไว้อย่างสม่ำเสมอ เพื่อให้มีข้อมูลสำรองไว้ใช้ ในกรณีที่ข้อมูลหลักเกิดความเสียหายหรือไม่สามารถใช้งาน ความถี่ในการดำเนินการสำรองข้อมูลและขั้นตอนการสำรองข้อมูลระบบแม่ข่าย เป็นความรับผิดชอบของ ผทท. โดยมีแนวปฏิบัติ ดังนี้

- 1.1 ผู้บังคับบัญชากำหนดผู้รับผิดชอบในการสำรองข้อมูล
- 1.2 ผู้ดูแลระบบต้องกำหนดชนิดของข้อมูลของระบบที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้ เช่น ข้อมูลค่าคอนฟิกูเรชัน (Configuration) ข้อมูลคู่มือการปฏิบัติงานสำหรับระบบ ข้อมูลในฐานข้อมูลของระบบงาน ข้อมูลซอฟต์แวร์ เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ระบบงาน และซอฟต์แวร์อื่น ๆ เป็นต้น
- 1.3 ผู้ดูแลระบบต้องสำรองข้อมูลตามความถี่ที่กำหนดไว้ ทั้งนี้ หากเป็นข้อมูลที่สนับสนุนกระบวนการทำงานที่สำคัญของ รฟม. ให้สำรองตามความถี่ที่ รฟม. กำหนด
- 1.4 ผู้ดูแลระบบต้องตรวจสอบว่าการสำรองข้อมูลสำเร็จครบถ้วนหรือไม่ หากไม่สำเร็จให้หาสาเหตุและดำเนินการแก้ไขอีกครั้งหนึ่ง
- 1.5 ผู้ดูแลระบบต้องนำข้อมูลที่สำรองไว้ไปเก็บไว้ทั้งภายในและนอก รฟม. อย่างน้อยอย่างละ 1 ชุด
- 1.6 ผู้ดูแลระบบทดสอบกู้คืนข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าข้อมูลที่สำรองไว้มีความถูกต้อง ครบถ้วน และพร้อมใช้งาน

2. การสำรองข้อมูลคอมพิวเตอร์ส่วนบุคคล
ผู้ใช้งานจะต้องสำรองข้อมูลสำคัญที่เก็บรักษาไว้ในเครื่องคอมพิวเตอร์ส่วนบุคคลหรือคอมพิวเตอร์ หรืออุปกรณ์พกพาอื่น ๆ อย่างสม่ำเสมอ ความถี่ในการสำรองข้อมูลขึ้นอยู่กับความถี่ของการเปลี่ยนแปลงของข้อมูล และระดับความสำคัญของข้อมูลหากเกิดการสูญหาย
3. การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์
เพื่อให้สามารถระบุตัวบุคคลผู้ใช้งานได้อย่างถูกต้อง ผู้ดูแลระบบต้องดำเนินการดังนี้
 - 3.1 ตั้งนาฬิกาของอุปกรณ์ที่ให้บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล Stratum - 1 เก็บรักษาข้อมูลจราจรคอมพิวเตอร์ โดยระยะเวลาในการเก็บตามประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 (90 วัน)
 - 3.2 เก็บรักษาข้อมูลจราจรคอมพิวเตอร์ในสื่อที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง มีการเก็บรักษาความลับของข้อมูลตามระดับชั้นความลับในการเข้าถึงตามที่ รพม. กำหนด โดยระบุตัวบุคคลที่สามารถเข้าถึงสื่อดังกล่าวได้
 - 3.3 ประเภทของสารสนเทศที่เก็บรักษา แสดงตามตาราง

ประเภทของสารสนเทศ	กฎหมายที่เกี่ยวข้อง	ระยะเวลาการจัดเก็บรักษา (ปี)
Authentication server logs (RADIUS, TACACS)	1) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	1
Email server logs	2) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560	1
Web application server logs	3) ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564	1
NTP server logs		1
DHCP server logs		1
IPS logs		1
Firewalls logs		1
Routers & Switches logs		1
Active directory logs		1

4. การจัดเก็บบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and monitoring)
 - 4.1 ผู้ดูแลระบบต้องมีการจัดเก็บบันทึกเหตุการณ์ (Event logs) การใช้งานระบบสารสนเทศ
 - 4.2 ผู้ดูแลระบบต้องเก็บบันทึกข้อมูล Audit log ซึ่งบันทึกกิจกรรมการใช้งานของผู้ใช้งานระบบสารสนเทศและเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยต่าง ๆ เพื่อประโยชน์ในการสืบสวน สอบสวน และเพื่อการติดตามการควบคุมการเข้าถึง
 - 4.3 ผู้ดูแลระบบต้องมีการตรวจสอบข้อมูลบันทึกเหตุการณ์อย่างสม่ำเสมอ (Log review)
 - 4.4 ผู้ดูแลระบบต้องไม่ลบข้อมูลล็อก (Log) หรือปิดการใช้งานการบันทึกข้อมูลล็อก (Log)
 - 4.5 ผู้ดูแลระบบต้องป้องกันระบบสารสนเทศที่จัดเก็บล็อก (Log) และข้อมูลล็อก (Log) เพื่อป้องกันการเข้าถึงหรือแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต
5. การเตรียมความพร้อมกรณีฉุกเฉิน

เพื่อให้มีการบริหารจัดการความต่อเนื่องให้กับกระบวนการทางธุรกิจที่สำคัญขององค์กร เมื่อมีเหตุการณ์ที่ทำให้เกิดการหยุดชะงักหรือติดขัดต่อกระบวนการดังกล่าว โดยมีแนวปฏิบัติ ดังนี้

 - 5.1 ผู้ดูแลระบบต้องกำหนดระบบที่มีความสำคัญทั้งหมดขององค์กร และจัดทำเป็นบัญชีรายชื่อระบบดังกล่าวรวมทั้งปรับปรุงรายชื่อระบบสำคัญและบัญชีฯ ตามความเป็นจริง
 - 5.2 เจ้าของข้อมูลและผู้ดูแลระบบประเมินความเสี่ยงสำหรับระบบเหล่านั้น กำหนดมาตรการเพื่อลดความเสี่ยงที่พบและจัดทำรายงานการประเมินความเสี่ยง
 - 5.3 ผู้ดูแลระบบจัดทำและปรับปรุงแผนกู้คืนระบบอย่างน้อยปีละ 1 ครั้ง
 - 5.4 เจ้าของข้อมูลและผู้ดูแลระบบต้องทดสอบแผนกู้คืนระบบอย่างน้อยปีละ 1 ครั้ง บันทึกผลการทดสอบรวมถึงปัญหาที่พบ และนำเสนอผลการทดสอบและแนวทางแก้ไขต่อผู้บังคับบัญชา
 - 5.5 ผู้ดูแลระบบต้องจัดประชุมและชี้แจงให้ผู้ที่เกี่ยวข้องทั้งหมดได้รับทราบเกี่ยวกับแผนและผลของการฝึกซ้อมการกู้คืนระบบ

ส่วนที่ 13

การตรวจสอบและประเมินความเสี่ยง

วัตถุประสงค์

- เพื่อให้มีการตรวจสอบการดำเนินงานของระบบจัดการความมั่นคงปลอดภัยสารสนเทศ และปรับปรุงอย่างต่อเนื่อง
- เพื่อควบคุม และติดตามการปฏิบัติงานของผู้ดูแลระบบสารสนเทศ ให้สอดคล้องตามข้อกำหนด กฎหมาย หรือระเบียบข้อบังคับที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ
- เพื่อประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของสารสนเทศและบริหารจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

ผู้รับผิดชอบ

- ผู้บังคับบัญชา
- ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

- ข้อกำหนดหลัก: การวางแผน (Planning)
- ข้อกำหนดหลัก: การตรวจประเมินภายใน (Internal Audit)
- หมวดที่ 8 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations security)
- หมวดที่ 14 ความสอดคล้อง (Compliance)

แนวปฏิบัติ

1. ผู้บังคับบัญชา ต้องกำหนดให้มีแนวทางในการดำเนินงานของระบบสารสนเทศสอดคล้องกับกฎหมาย พระราชบัญญัติ กฎระเบียบ ข้อบังคับที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศโดยต้องจัดทำเป็นลายลักษณ์อักษร และมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
2. ผู้บังคับบัญชา ต้องกำหนดมาตรการในการควบคุมและบริหารจัดการสินทรัพย์ทางปัญญา ได้แก่ ลิขสิทธิ์ในเอกสาร หรือซอฟต์แวร์ เครื่องหมายการค้า สิทธิบัตร และใบอนุญาตการใช้งานซอร์สโค้ด หรือการใช้งานซอฟต์แวร์ เพื่อให้การดำเนินงานเป็นไปตามข้อกำหนดทั้งในแง่ของข้อสัญญา และด้านกฎหมาย พระราชบัญญัติ กฎระเบียบ ข้อบังคับด้านสินทรัพย์ทางปัญญาที่เกี่ยวข้อง
3. ผู้บังคับบัญชา ต้องควบคุมให้มีการคุ้มครองข้อมูลส่วนบุคคลโดยให้สอดคล้องกับกฎหมาย พระราชบัญญัติ กฎระเบียบ ข้อบังคับที่เกี่ยวข้อง
4. ผู้บังคับบัญชา ต้องกำกับดูแล และควบคุมการปฏิบัติงานของผู้ที่อยู่ใต้การบังคับบัญชา เพื่อป้องกันการใช้งานระบบสารสนเทศผิดวัตถุประสงค์ หรือละเมิดต่อนโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของ รพม.
5. ผู้บังคับบัญชา ต้องควบคุมให้มีการป้องกันข้อมูลสำคัญขององค์กร ข้อมูลสำคัญที่เกี่ยวข้องกับข้อกำหนดทางกฎหมาย ระเบียบ ข้อบังคับ สัญญา ควรได้รับการป้องกันจากการสูญหาย ถูกทำลาย และปลอมแปลง
6. ผู้บังคับบัญชาต้องจัดให้มีการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยผู้ตรวจสอบภายใน (Internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External auditor) ตามระยะเวลาอย่างน้อยปีละ 1 ครั้ง

7. ผู้ดูแลระบบ ต้องติดตามผลการใช้งานทรัพยากรสารสนเทศ (Capacity) และวางแผนด้านทรัพยากรสารสนเทศให้รองรับการปฏิบัติงานในอนาคตอย่างเหมาะสม
8. ผู้ดูแลระบบ ต้องป้องกันการเข้าใช้งานเครื่องมือที่ใช้เพื่อการตรวจสอบ เพื่อมิให้เกิดการใช้งานผิดประเภท หรือถูกละเมิดการใช้งาน (Compromise) โดยควบคุมการเข้าถึง และตรวจสอบการนำเครื่องมือไปใช้งานอย่างสม่ำเสมอ
9. ผู้ดูแลระบบต้องประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
10. ผู้บังคับบัญชาต้องติดตามผลการดำเนินการตามแผนบริหารจัดการความเสี่ยง (Risk treatment plan) เป็นประจำทุกไตรมาส
11. ผู้ดูแลระบบต้องประเมินความเสี่ยงแล้วจัดลำดับความสำคัญของความเสี่ยงนั้นและค้นหาวิธีการเพื่อลดความเสี่ยงตามขั้นตอนที่ รพม. กำหนด พร้อมทั้งพิจารณาข้อดีข้อเสียของวิธีการเหล่านั้นเพื่อให้ผู้บริหารของ รพม. ตัดสินใจเลือกวิธีการเพื่อลดความเสี่ยงหรือยอมรับความเสี่ยง เมื่อเลือกวิธีการลดความเสี่ยงแล้วผู้บริหารต้องจัดสรรทรัพยากรอย่างเพียงพอเพื่อดำเนินการ แนวทางการลดความเสี่ยง แบ่งได้เป็น 3 รูปแบบ ได้แก่
 - 11.1 การเลือกใช้เทคโนโลยี เพื่อใช้ในการลดความเสี่ยงและเพิ่มความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รพม. เป็นวิธีที่จำเป็นต้องใช้งบประมาณและทรัพยากรอย่างเพียงพอในการดำเนินการ เช่น การเลือกใช้อุปกรณ์ Firewall มากกว่าหนึ่งผลิตภัณฑ์ในการป้องกันการเข้าถึงเครือข่ายที่สำคัญ การใช้อุปกรณ์สมาร์ทการ์ด หรือ USB Token ในการตรวจสอบยืนยันตัวตนในการเข้าใช้งานระบบจากภายนอก รพม. เป็นต้น
 - 11.2 การปรับเปลี่ยนขั้นตอนปฏิบัติ ต้องออกแบบขั้นตอนปฏิบัติใหม่ที่รัดกุมและสามารถรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รพม. ได้ดีขึ้น เมื่อออกแบบขั้นตอนปฏิบัติใหม่แล้วต้องมีการพิจารณาหาหรือความเหมาะสม ความเป็นไปได้ และผู้บริหารต้องเป็นผู้อนุมัติให้มีการบังคับใช้ขั้นตอนปฏิบัติใหม่นั้น
 - 11.3 ผู้ดูแลระบบต้องแจ้งขั้นตอนปฏิบัติให้ผู้เกี่ยวข้องรับรู้อย่างทั่วถึง รวมทั้งต้องจัดฝึกอบรมผู้ใช้งานที่เกี่ยวข้องเพื่อให้สามารถปฏิบัติตามขั้นตอนปฏิบัติใหม่ได้อย่างราบรื่นและมีประสิทธิภาพ
12. การตรวจสอบความปลอดภัยของระบบสารสนเทศ
 - 12.1 ผู้ดูแลระบบ ต้องวางแผนการตรวจสอบและประเมินช่องโหว่หรือจุดอ่อนด้านความมั่นคงปลอดภัยสารสนเทศ และแจ้งผู้ที่เกี่ยวข้องเพื่อแก้ไขในกรณีที่พบว่าช่องโหว่หรือจุดอ่อนนั้นอาจเป็นเหตุการณ์ด้านความมั่นคงปลอดภัย อย่างน้อยปีละ 1 ครั้ง
 - 12.2 ผู้ดูแลระบบต้องตรวจสอบระบบสารสนเทศที่จะต้องมีการปรับปรุงเมื่อมีเวอร์ชันใหม่ (Patch) รวมทั้งข้อมูลที่เกี่ยวข้องกับช่องโหว่ด้านเทคนิคอย่างสม่ำเสมอเพื่อให้ทราบถึงภัยคุกคามและความเสี่ยง รวมถึงหาวิธีป้องกันและแก้ไขที่เหมาะสมกับช่องโหว่นั้น
 - 12.3 ผู้ใช้งาน ผู้ดูแลระบบ และหน่วยงานภายนอก ต้องบันทึกและรายงานช่องโหว่หรือจุดอ่อนใด ๆ ด้านความมั่นคงปลอดภัยสารสนเทศ ที่อาจสังเกตพบระหว่างการติดตามการใช้งานระบบสารสนเทศ ผ่านช่องทางบริหารจัดการที่กำหนดไว้อย่างเหมาะสม และต้องดำเนินการปิดช่องโหว่ที่มีการตรวจพบหรือได้รับแจ้ง
13. ผู้ดูแลระบบต้องมีการบริหารจัดการการเปลี่ยนแปลงเกี่ยวกับการจัดเตรียมการให้บริการ การดูแลปรับปรุงนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ขั้นตอนปฏิบัติงาน หรือการควบคุมเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ โดยคำนึงถึงระดับความสำคัญของการดำเนินธุรกิจที่เกี่ยวข้องและการประเมินความเสี่ยงอย่างต่อเนื่อง

ส่วนที่ 14

การถ่ายโอน และแลกเปลี่ยนข้อมูลสารสนเทศ

วัตถุประสงค์

- เพื่อให้มีการควบคุมการถ่ายโอนและแลกเปลี่ยนข้อมูลสารสนเทศ ป้องกันการรั่วไหล หรือมีการแก้ไขข้อมูล โดยที่ไม่ได้รับอนุญาต รวมถึงการป้องกันสื่อบันทึกข้อมูลให้มีความปลอดภัยเป็นไปตามข้อกำหนด

ผู้รับผิดชอบ

- ผู้บังคับบัญชา
- เจ้าของข้อมูล
- ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

- หมวดที่ 9 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)

แนวปฏิบัติ

1. ผู้บังคับบัญชา ต้องควบคุมให้มีการจัดทำนโยบาย และขั้นตอนการปฏิบัติเพื่อป้องกันข้อมูลสารสนเทศที่มีการสื่อสาร หรือแลกเปลี่ยนผ่านระบบสารสนเทศให้เหมาะสมตามระดับชั้นความลับข้อมูลสารสนเทศตามชั้นตอนที่ รพม. กำหนด
2. ผู้บังคับบัญชา และเจ้าของข้อมูล ต้องควบคุมให้มีการจัดทำข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศระหว่างองค์กรกับบุคคลหรือหน่วยงานภายนอก
3. ผู้ดูแลระบบ ต้องมีการป้องกันข้อมูลสารสนเทศที่มีการสื่อสารกันผ่านข้อมูลอิเล็กทรอนิกส์ (Electronic messaging) เช่น จดหมายอิเล็กทรอนิกส์ (E-mail) หรือ Instant messaging ด้วยวิธีการหรือมาตรการที่เหมาะสม
4. ผู้ดูแลระบบ ต้องป้องกันข้อมูลสารสนเทศที่มีการแลกเปลี่ยนในการทำพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce) ผ่านเครือข่ายคอมพิวเตอร์สาธารณะ เพื่อมิให้มีการฉ้อโกง ละเมิดสัญญา หรือมีการรั่วไหลหรือข้อมูลสารสนเทศถูกแก้ไขโดยมิได้รับอนุญาต
5. ผู้ดูแลระบบ ต้องป้องกันข้อมูลสารสนเทศที่มีการสื่อสาร หรือแลกเปลี่ยนในการทำธุรกรรมทางออนไลน์ (Online transaction) เพื่อมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ ส่งข้อมูลไปผิดที่ การรั่วไหลของข้อมูล ข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ หรือถูกส่งซ้ำโดยมิได้รับอนุญาต
6. ผู้ดูแลระบบ ต้องควบคุมการรับส่งข้อมูลสารสนเทศเพื่อป้องกันความผิดพลาด ดังนี้
 - 6.1 ความไม่สมบูรณ์ของข้อมูลสารสนเทศที่รับ-ส่ง
 - 6.2 การส่งข้อมูลสารสนเทศผิดจุดหมายปลายทาง
 - 6.3 การเปลี่ยนแปลงข้อมูลสารสนเทศโดยมิได้รับอนุญาต
 - 6.4 การเปิดเผยข้อมูลสารสนเทศโดยมิได้รับอนุญาต
 - 6.5 การเข้าถึงข้อมูลสารสนเทศโดยมิได้รับอนุญาต
 - 6.6 การนำข้อมูลสารสนเทศกลับมาใช้ใหม่โดยมิได้รับอนุญาต
7. เจ้าของข้อมูล และผู้ดูแลระบบ ต้องมีการป้องกันข้อมูลสารสนเทศที่มีการเผยแพร่ต่อสาธารณชนมิให้มีการแก้ไขเปลี่ยนแปลงโดยมิได้รับอนุญาต เพื่อรักษาความถูกต้องครบถ้วนของข้อมูลสารสนเทศ

ส่วนที่ 15

การควบคุมการเข้ารหัส

วัตถุประสงค์

- เพื่อให้มีการเข้ารหัสข้อมูลอย่างเหมาะสมและมีประสิทธิภาพในการปกป้องความลับ ป้องกัน การปลอมแปลงข้อมูล และควบคุมความถูกต้องของข้อมูล

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- เจ้าของข้อมูล
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 6 การเข้ารหัสข้อมูล (Cryptography)

แนวปฏิบัติ

1. เจ้าของข้อมูล ต้องเข้ารหัส หรือการใส่รหัสผ่านข้อมูลอิเล็กทรอนิกส์ขององค์กรตามระดับชั้นความลับเพื่อป้องกันผู้ไม่มีสิทธิเข้าถึง ตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และตามขั้นตอนที่ รพม. กำหนด
2. เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ใช้งานต้องปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 ในการนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับจะต้องใช้วิธีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล
3. ผู้ดูแลระบบ ต้องใช้วิธีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล หลีกเลี่ยงการใช้รูปแบบการเข้ารหัสที่พัฒนาขึ้นเอง เพื่อให้มั่นใจว่าขั้นตอนวิธี (Algorithm) ที่ใช้ในการเข้ารหัสนั้นมีความมั่นคงปลอดภัย ดังนี้

ประเภทกุญแจ / วิธีการเข้ารหัส	เกณฑ์ขั้นต่ำ	ความยาวกุญแจ (อย่างน้อย)
กุญแจแบบสมมาตร (Symmetric)	AES	256 bits
กุญแจแบบอสมมาตร (Asymmetric)	RSA	1024 bits
การ Hashing	SHA-256	256 bits

4. ผู้ดูแลระบบ ต้องมีการทบทวนขั้นตอนวิธี (Algorithm) และความยาวของกุญแจที่เข้ารหัสอย่างน้อยปีละ 1 ครั้ง เพื่อให้ยังสามารถรักษาไว้ซึ่งความมั่นคงปลอดภัย
5. ผู้ดูแลระบบ ต้องกำหนดให้มีการบริหารจัดการกุญแจที่ใช้ในการเข้ารหัส ดังนี้
 - 5.1 การสร้างกุญแจรหัสควรกระทำในสถานที่ที่มีมาตรการป้องกันความปลอดภัย
 - 5.2 เมื่อมีการสร้างกุญแจรหัสที่เป็นกุญแจลับ (Private key) ควรส่งมอบให้กับเจ้าของกุญแจโดยตรง โดยวิธีการที่ปลอดภัย
 - 5.3 ควรจัดให้มีการเก็บบันทึก Log เพื่อการตรวจสอบสำหรับกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับการจัดการกุญแจรหัส

6. ผู้ใช้งาน ควรรักษาความปลอดภัยในการใช้งานกุญแจ ดังนี้
 - 6.1 เก็บกุญแจรหัสในสถานที่ที่ปลอดภัย เช่น ตู้นิรภัย หรือสื่อบันทึกที่ปลอดภัย และไม่มีใครสามารถเข้าถึงได้
 - 6.2 เมื่อมีการรับกุญแจสาธารณะ (Public key) มาใช้ ก่อนใช้งานจะต้องพิสูจน์ความถูกต้องของกุญแจสาธารณะ โดยสอบถามกับผู้ส่งหรือตรวจสอบกับผู้แทนในการรับรองความถูกต้องของกุญแจสาธารณะ (Certificate authority) ที่เชื่อถือได้เท่านั้น
 - 6.3 ควบคุมการใช้งานและจัดเก็บกุญแจให้สอดคล้องกับการรักษาความลับข้อมูลตามที่ รพม. กำหนด

ส่วนที่ 16

การนำอุปกรณ์ส่วนตัวมาใช้งาน (Bring your own device)

วัตถุประสงค์

- เพื่อควบคุมการนำอุปกรณ์ส่วนตัวมาเชื่อมต่อหรือเข้าถึงระบบสารสนเทศของ รพม. ที่ใช้ในการบริหารจัดการระบบสารสนเทศของ รพม. หรือปฏิบัติงานให้ รพม. ทั้งนี้เพื่อป้องกันภัยคุกคามที่อาจเกิดขึ้นกับระบบสารสนเทศของ รพม. รวมถึงเพื่อป้องกันไม่ให้ข้อมูลของ รพม. เกิดการรั่วไหล

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 2 อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากระยะไกล (Mobile devices and teleworking)

แนวปฏิบัติ

1. ผู้ดูแลระบบต้องกำหนดคุณสมบัติของระบบปฏิบัติการของอุปกรณ์ส่วนตัวที่อนุญาตให้นำมาเชื่อมต่อหรือเข้าถึงระบบงานสารสนเทศของ รพม. ได้ โดยต้องเป็นระบบปฏิบัติการที่ไม่ล้าสมัย (Obsolete operating system) และยังได้รับการสนับสนุนการใช้งานจากเจ้าของผลิตภัณฑ์
2. ผู้ดูแลระบบต้องตัดการเชื่อมต่อหากระบบปฏิบัติการของอุปกรณ์ส่วนตัวที่อนุญาตให้นำมาเชื่อมต่อหรือเข้าถึงระบบงานสารสนเทศของ รพม. เกิดการล้าสมัย (Obsolete operating system) หรือเจ้าของผลิตภัณฑ์ไม่สนับสนุนการใช้งานแล้ว
3. ผู้ดูแลระบบต้องมีมาตรการป้องกันมัลแวร์ และตรวจสอบการอัปเดต Patch เวอร์ชันของระบบปฏิบัติการที่เจ้าของผลิตภัณฑ์ยังให้การสนับสนุนการใช้งาน
4. ผู้ดูแลระบบต้องไม่อนุญาตให้อุปกรณ์ที่มีการปรับแต่งการเข้าถึงระบบปฏิบัติการ (rooted/jailbroken) มาเชื่อมต่อหรือเข้าถึงระบบสารสนเทศของ รพม.
5. ผู้ดูแลระบบต้องแบ่งแยกเครือข่ายของอุปกรณ์ส่วนตัวที่นำมาเชื่อมต่อหรือเข้าถึงระบบสารสนเทศของ รพม.
6. ผู้ใช้งานต้องไม่นำอุปกรณ์ส่วนตัวที่ติดตั้งแอปพลิเคชันนอก Official store มาเชื่อมต่อหรือเข้าถึงระบบงานสารสนเทศของ รพม.
7. ผู้ใช้งานต้องไม่นำอุปกรณ์ส่วนตัวที่ติดตั้งโปรแกรมละเมิดลิขสิทธิ์มาเชื่อมต่อหรือเข้าถึงระบบงานสารสนเทศของ รพม.
8. ผู้ใช้งานต้องอัปเดต Patch ของระบบปฏิบัติการที่อุปกรณ์ส่วนตัวให้เป็นเวอร์ชันล่าสุด รวมถึงต้องเป็นระบบปฏิบัติการที่เจ้าของผลิตภัณฑ์ยังให้การสนับสนุนการใช้งาน
9. ผู้ใช้งานต้องยืนยันตัวตนก่อนเข้าถึงระบบสารสนเทศของ รพม. ทุกครั้ง
10. ผู้ใช้งานต้องติดตั้ง Network Access Control agent (NAC agent) หรือ Mobile Device Management agent (MDM agent) ตามที่ รพม. กำหนด เพื่อควบคุมการใช้งานเครือข่ายและการเข้าถึงระบบสารสนเทศของ รพม.
11. กรณีอุปกรณ์ส่วนตัวสูญหายหรือถูกขโมยผู้ใช้งานต้องแจ้งผู้ดูแลระบบโดยเร็วที่สุด เพื่อจัดการข้อมูลที่จัดเก็บอยู่ในอุปกรณ์ส่วนตัวของผู้ใช้งาน

ภาคผนวก ข.

รายงานผลการบำรุงรักษา
ระบบติดตามความก้าวหน้าโครงการ (PPMS)
ประจำไตรมาสที่ (.....-.....)

สัญญาเลขที่

จัดทำโดย

บริษัท

รายงานผลการตรวจสอบระบบติดตามความก้าวหน้าโครงการ (PPMS)

วันที่ เดือน ปี พ.ศ.

PPMS Web Server (Server Name :

1. ตรวจสอบการทำงานของเครื่องเซิร์ฟเวอร์ (PPMS Web Server)

1.1 ตรวจสอบเวอร์ชันของระบบปฏิบัติการ

1.1.1 Windows Version

----- รูป -----

1.1.2 Windows Update

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

1.2 ตรวจสอบการใช้งานของ CPU

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

1.3 ตรวจสอบการใช้งานของ Memory

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

1.4 ตรวจสอบพื้นที่การใช้งานของ Hard disk

	4/2566	1/2567	2/2567	3/2567	4/2567
Drive C					
Drive D					

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

ศพธธ

1.5 ตรวจสอบรายละเอียดการเชื่อมต่อเครือข่าย

1.5.1 ตรวจสอบ IP address ของเครื่องคอมพิวเตอร์

----- รูป -----

1.5.2 ทดสอบการเชื่อมต่อเครือข่ายกับเครื่อง PPMS Database Server

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

1.6 ตรวจสอบ Log ของเครื่องเซิร์ฟเวอร์

1.6.1 Application log

----- รูป -----

1.6.2 Security log

----- รูป -----

1.6.3 System log

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

1.7 ตรวจสอบวันที่และเวลาของเครื่อง

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

2. ตรวจสอบการทำงานของ PPMS Application

2.1 ตรวจสอบการทำงานของ Service ของ Web server

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

2.2 ตรวจสอบ Version ของ PPMS Application

2.2.1 PPMS Production

Path ที่จัดเก็บ :

	4/2566	1/2567	2/2567	3/2567	4/2567
version					

----- รูป -----

2.2.2 PPMS Test

Path ที่จัดเก็บ :

	4/2566	1/2567	2/2567	3/2567	4/2567
version					

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

2.3 ตรวจสอบการสำรองข้อมูลของ PPMS Application

Path ที่จัดเก็บ :

	4/2566	1/2567	2/2567	3/2567	4/2567
Folder Size					

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

2.4 ตรวจสอบ Log ของ PPMS Application

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

ศุภรณมา

PPMS Database Server (Server Name :)

3. ตรวจสอบการทำงานของเครื่องเซิร์ฟเวอร์ (PPMS Database Server)

3.1 ตรวจสอบเวอร์ชันของระบบปฏิบัติการ

3.1.1 Windows Version

----- รูป -----

3.1.2 Windows Update

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

3.2 ตรวจสอบการใช้งานของ CPU

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

3.3 ตรวจสอบการใช้งานของ Memory

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

3.4 ตรวจสอบพื้นที่การใช้งานของ Hard disk

	4/2566	1/2567	2/2567	3/2567	4/2567
Drive C					
Drive D					

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

3.5 ตรวจสอบรายละเอียดการเชื่อมต่อเครือข่าย

3.5.1 ตรวจสอบ IP address ของเครื่องคอมพิวเตอร์

----- รูป -----

3.5.2 ทดสอบการเชื่อมต่อเครือข่ายกับเครื่อง PPMS Web Server

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

3.6 ตรวจสอบ Log ของเครื่องเซิร์ฟเวอร์

3.6.1 Application log

----- รูป -----

3.6.2 Security log

----- รูป -----

3.6.3 System log

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

3.7 ตรวจสอบวันที่และเวลาของเครื่อง

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

4. ตรวจสอบการทำงานของ PPMS Database

4.1 ตรวจสอบการทำงานของ Service ของ PPMS Database

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

4.2 ตรวจสอบการใช้พื้นที่ของฐานข้อมูล

4.2.1 PPMS Production

Database file name :

Database log name :

	4/2566	1/2567	2/2567	3/2567	4/2567
Database file size					
Database log size					

----- รูป -----

4.2.2 PPMS Test

Database file name :

Database log name :

	4/2566	1/2567	2/2567	3/2567	4/2567
Database file size					
Database log size					

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

4.3 ตรวจสอบการสำรองข้อมูลของ PPMS Database

Path ที่จัดเก็บ :

	4/2566	1/2567	2/2567	3/2567	4/2567
File size					

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

4.4 ตรวจสอบการทำงานของ JOB

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

5. ตรวจสอบการทำงานของระบบติดตามความก้าวหน้าโครงการ (PPMS)

5.1 ตรวจสอบการเข้าใช้งาน (Authentication Testing)

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

5.2 ตรวจสอบประสิทธิภาพการให้บริการในการตอบสนองการเรียกใช้งาน (Response Time) *

หมายเหตุ:

* ตรวจสอบระยะเวลาในการตอบสนองการเรียกใช้งานไม่ควรเกิน 4 วินาที (อย่างน้อย 3 หน้าจอ)

----- รูป -----

Response Time วินาที

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

5.3 ตรวจสอบการหมดเวลาใช้งานระบบสารสนเทศ (Session Time - Out)

ระบบติดตามความก้าวหน้าโครงการ (PPMS) (15 นาที หรือตามที่ระบบฯ กำหนด)

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

5.4 ตรวจสอบการออกรายงาน

----- รูป -----

สรุปผลการตรวจสอบ ปกติ ไม่ปกติ

ลงชื่อ ผู้ตรวจสอบ

()

วันที่

ศพมจว

รายงานการตรวจสอบสิทธิการเข้าถึงระบบ (Role Matrix) ระบบติดตามความก้าวหน้าโครงการ (PPMS)

การรถไฟแห่งประเทศไทย

ประจำไตรมาสที่ (ตั้งแต่วันที่ ถึงวันที่

ที่	ชื่อ - สกุล	Application Server				Database Server				Application				DBMS			
		Super Administrator	Administrator	Super User	User	การเข้าถึงเอกสาร (F/C/R/U/D)	Super Administrator	Administrator	Super User	User	การเข้าถึงเอกสาร (F/C/R/U/D)	Super Administrator	Administrator	Super User	User	การเข้าถึงเอกสาร (F/C/R/U/D)	

หมายเหตุ : การเข้าถึงเอกสาร F : Full, C : Create, R : Read, U : Update, D : Delete

* Super Administrator : ผู้มีสิทธิ์สามารถกำหนดสิทธิ์ และบริหารจัดการข้อมูลเครื่องเซิร์ฟเวอร์ ภายใต้ Domain ได้ (Domain Admin)

* Administrator : ผู้มีสิทธิ์สามารถกำหนดสิทธิ์ และบริหารจัดการข้อมูลเครื่องเซิร์ฟเวอร์ที่มีสิทธิ์ได้ (Local Admin) รวมทั้งกำหนดสิทธิ์ให้กับผู้ใช้งานระบบสารสนเทศต่าง ๆ ได้

* Super User : ผู้มีสิทธิ์สามารถจัดการข้อมูลภายในระบบสารสนเทศต่าง ๆ ได้

* User : ผู้ใช้งานทั่วไป เข้าถึง เรียกดูข้อมูลภายในระบบงานสารสนเทศต่าง ๆ ได้

รายงานผลการปิดช่องโหว่ระบบติดตามความก้าวหน้าโครงการ (PPMS)

การรถไฟฟ้ามหานครแห่งประเทศไทย

ประจำไตรมาสที่ (ตั้งแต่วันที่ ถึงวันที่

ลำดับ	วันที่พบ ช่องโหว่	หมายเลข ช่องโหว่	ชื่อช่องโหว่	รายละเอียด	ผลการดำเนินการ/ การแก้ไข/ ผลกระทบ	ผู้ดำเนินการแก้ไข	วันที่ ดำเนินการ แล้วเสร็จ	สถานะ

รายงานทะเบียนทรัพย์สิน (Asset Inventory) ระบบติดตามความก้าวหน้าโครงการ (PPMS)

การรถไฟฯขนส่งมวลชนแห่งประเทศไทย

ประจำไตรมาสที่ (ตั้งแต่วันที่ ถึงวันที่

ลำดับ	รายการทรัพย์สิน	End of Support	End of Life	กลุ่มทรัพย์สิน	ประเภททรัพย์สิน	Firmware/ Patch Version	สถานที่จัดเก็บ	ผู้บันทึก

PPMS

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและรายละเอียดค่าใช้จ่าย
การจัดซื้อจัดจ้างที่มีใ้ใช้งานก่อสร้าง

ชื่อโครงการ	จ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (PPMS) ประจำปีงบประมาณ 2567
1. หน่วยงานเจ้าของโครงการ	ฝ่ายเทคโนโลยีสารสนเทศ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
2. วงเงินงบประมาณที่ได้รับจัดสรร	1,350,000.00 บาท (หนึ่งล้านสามแสนห้าหมื่นบาทถ้วน)
3. วันที่กำหนดราคากลาง (ราคาอ้างอิง) ณ วันที่ เป็นเงิน	23 มิถุนายน 2566 650,000.00 บาท (หกแสนห้าหมื่นบาทถ้วน) (รวมภาษีมูลค่าเพิ่ม)
4. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)	ราคาที่ได้มาจากการสืบราคาจากท้องตลาด โดยสืบราคาจากผู้รับจ้างรายเดิม (บริษัท เอทูพี โซลูชั่น จำกัด)
5. รายชื่อผู้รับผิดชอบกำหนดราคากลาง	นางสาวสุพรรณษา นิลสมบูรณ์ โปรแกรมเมอร์ ระดับ 7

สุพรรณษา



คำสั่ง การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

ที่ ๒๓๓๘/๒๕๖๖

เรื่อง แต่งตั้ง คณะกรรมการจ้างโดยวิธีเฉพาะเจาะจง และคณะกรรมการตรวจรับพัสดุ
สำหรับการจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (Project Progress Monitoring System:
PPMS) ประจำปีงบประมาณ ๒๕๖๗ โดยวิธีเฉพาะเจาะจง

ด้วย การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย (รฟม.) มีความประสงค์จะจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (Project Progress Monitoring System: PPMS) ประจำปีงบประมาณ ๒๕๖๗ โดยวิธีเฉพาะเจาะจง และเพื่อให้เป็นไปตามระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐ จึงขอแต่งตั้งพนักงานรายชื่อต่อไปนี้ เป็นคณะกรรมการจ้างโดยวิธีเฉพาะเจาะจง และคณะกรรมการตรวจรับพัสดุ สำหรับการจ้างบำรุงรักษาระบบติดตามความก้าวหน้าโครงการ (Project Progress Monitoring System: PPMS) ประจำปีงบประมาณ ๒๕๖๗ โดยวิธีเฉพาะเจาะจง

คณะกรรมการจ้างโดยวิธีเฉพาะเจาะจง

๑. นางสาวศิริลี เกตุคง

ประธานกรรมการ

หัวหน้าแผนกแผนงานและบริหารเอกสาร ๒-๓

กองแผนงานและบริหารเอกสาร ๒

ฝ่ายบริหารงานก่อสร้าง ๒

๒. นางสาววิสุตา ชลายนเดชะ

กรรมการ

หัวหน้าแผนกแผนงานและบริหารเอกสาร ๑-๓

กองแผนงานและบริหารเอกสาร ๑

ฝ่ายบริหารงานก่อสร้าง ๑

๓. นางสาวปวีณา เปล่งเสียง

กรรมการ

พนักงานวิเคราะห์ระบบ ระดับ ๗

แผนกพัฒนาระบบงานคอมพิวเตอร์

กองระบบงานคอมพิวเตอร์

ฝ่ายเทคโนโลยีสารสนเทศ

/๔. นางสาว...

๔. นางสาวไพลิน ปันจยีสีห์ กรรมการและเลขานุการ
พนักงานบริหารพัสดุ ระดับ ๖
แผนกจัดหาพัสดุทั่วไป ๑
กองจัดหาพัสดุทั่วไป
ฝ่ายจัดซื้อและบริการ

อำนาจและหน้าที่

๑. พิจารณาคุณสมบัติของผู้ประกอบการที่ยื่นข้อเสนอให้เป็นไปตามเงื่อนไขที่กำหนดในหนังสือ

เชิญชวน

๒. พิจารณาคัดเลือกผู้ประกอบการตามหลักเกณฑ์การพิจารณาข้อเสนอให้เป็นไปตามเงื่อนไขที่กำหนดไว้ในหนังสือเชิญชวน

๓. รายงานผลการพิจารณาและเสนอความเห็นต่อหัวหน้าหน่วยงานของรัฐ

การกำหนดระยะเวลาในการพิจารณาผลการเสนอราคา

กำหนดระยะเวลาในการพิจารณาผลการเสนอราคาให้แล้วเสร็จภายใน ๑๕ วัน นับถัดจากวันเสนอ

ราคา

คณะกรรมการตรวจรับพัสดุ

๑. นางสาวสิริพร อุษาสาธิต ประธานกรรมการ

หัวหน้าแผนกออาวุโส

แผนกข้อมูลและบริหารงานเอกสาร ฝ่ายวิศวกรรมและสถาปัตยกรรม ๑ ระดับ ๑๐

ฝ่ายวิศวกรรมและสถาปัตยกรรม

๒. นางสาวจตุรพร จารุวัจนกุล กรรมการ

หัวหน้าแผนกประเมินผลโครงการรถไฟฟ้า

กองวางแผนโครงการรถไฟฟ้า

ฝ่ายพัฒนาโครงการรถไฟฟ้า

๓. นางสาวสุพรรณษา นิลสมบุรณ์ กรรมการและเลขานุการ

โปรแกรมเมอร์ ระดับ ๗

แผนกสนับสนุนระบบงานคอมพิวเตอร์

กองระบบงานคอมพิวเตอร์

ฝ่ายเทคโนโลยีสารสนเทศ

/๔. นางสาว...

๔. นางสาวไพลิน ปันจัยสีห์

ผู้ช่วยเลขานุการ

พนักงานบริหารพัสดุ ระดับ ๖

แผนกจัดหาพัสดุทั่วไป ๑

กองจัดหาพัสดุทั่วไป

ฝ่ายจัดซื้อและบริการ

อำนาจและหน้าที่

ทำการตรวจรับงานจ้างให้เป็นไปตามเงื่อนไขของสัญญาหรือข้อตกลงนั้น และบริหารสัญญา

สั่ง ณ วันที่ ๒๐ กรกฎาคม พ.ศ. ๒๕๖๖



(นายทวิช พึ่งตน)

ผู้อำนวยการฝ่ายจัดซื้อและบริการ

ปฏิบัติการแทน ผู้อำนวยการรถไฟฟ้ามหานครแห่งประเทศไทย