ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและรายละเอียดค่าใช้จ่าย
การจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ จ้างบริการช่องทางสื่อสารข้อมูลระบบอินเทอร์เน็ตของ รฟม. ประจำปีงบประมาณ 2566
2. หน่วยงานเจ้าของโครงการ ฝ่ายเทคโนโลยีสารสนเทศ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
3. วงเงินงบประมาณที่ได้รับจัดสรร 17,710,000.00 บาท (สิบเจ็ดล้านเจ็ดแสนหนึ่งหมื่นบาทถ้วน) รวมภาษีมูลค่าเพิ่ม
4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) ณ วันที่ 24 กุมภาพันธ์ 2565
   เป็นเงินทั้งสิ้น 17,706,360.00 บาท (สิบเจ็ดล้านเจ็ดแสนหกพันสามร้อยหกสิบบาทถ้วน) รวมภาษีมูลค่าเพิ่ม
5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง) สืบราคาจากท้องตลาด 3 ราย ดังนี้
   5.1 บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
   5.2 บริษัท เค เอส ซี คอมเมอร์เชียล อินเตอร์เนต จำกัด
   5.3 บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด
6. รายชื่อผู้รับผิดชอบกำหนดราคากลาง
   6.1 นายอานันท์ หวังกุหลำ ประธานกรรมการ
   6.2 นางสาวณัชชา สินประเสริฐรัตน์ กรรมการ
   6.3 นางสาวยูถิกา จันทวงศ์ กรรมการ
   6.4 นางสาวนันทพร ว่องไวพาณิชย์ กรรมการ
   6.5 นายกฤษฎ์ธิวัฒน์ ขจรพันธ์ กรรมการและเลขานุการ

ขอบเขตของงานจ้างบริการช่องทางสื่อสารข้อมูล
ระบบอินเทอร์เน็ตของ รฟม. ประจำปีงบประมาณ 2566

1. ความเป็นมา

โครงการจัดหาบริการช่องทางสื่อสารข้อมูลระบบอินเทอร์เน็ตของ รฟม. มีวัตถุประสงค์เพื่อจัดหาบริการช่องทางสื่อสารข้อมูลระบบอินเทอร์เน็ตของ รฟม. ซึ่งเป็นโครงการที่ต้องดำเนินการทุกปี เพื่อให้เกิดความต่อเนื่องในการปฏิบัติงาน รวมถึงเตรียมความพร้อมหากการให้บริการระบบสื่อสารและโทรคมนาคมของ รฟม. ประจำปีงบประมาณ 2565 สิ้นสุดลง ดังนั้น รฟม. จึงมีความจำเป็นต้องจัดหาผู้รับจ้างบริการช่องทางสื่อสารข้อมูลและอินเทอร์เน็ตของ รฟม. ประจำปีงบประมาณ 2566 ตามลำดับ

2. วัตถุประสงค์

เพื่อให้ รฟม. มีบริการช่องทางสื่อสารข้อมูลและอินเทอร์เน็ตของ รฟม. ประจำปีงบประมาณ 2566 สำหรับใช้ในการปฏิบัติงานและสนับสนุนการปฏิบัติงานที่เกี่ยวข้องกับการให้บริการรถไฟฟ้าได้อย่างมีประสิทธิภาพและต่อเนื่อง รวมถึงใช้เป็นช่องทางการติดต่อสื่อสาร การเผยแพร่ข้อมูลข่าวสารต่างๆ ให้กับส่วนงานภายใน รฟม. ประชาชน ผู้มีส่วนเกี่ยวข้องต่างๆ และสนับสนุนการปฏิบัติงานที่เกี่ยวข้องกับการให้บริการรถไฟฟ้าสายต่างๆ ในปัจจุบัน

3. ขอบเขตการดำเนินงาน

ผู้ยื่นข้อเสนอต้องจัดหา ติดตั้ง และจัดให้มีบริการตามรายการ ดังนี้

3.1 บริการช่องทางสื่อสารข้อมูลระบบอินเทอร์เน็ตทั้งวงจรหลักและวงจรสำรอง

3.2 บริการเชื่อมโยงระบบเครือข่ายระหว่างสำนักงานใหญ่กับสำนักงานย่อย

3.3 บริการเชื่อมโยงระบบเครือข่ายสำหรับระบบรายงานจำนวนที่จอดรถว่างแบบ Real Time

3.4 บริการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์และการเฝ้าระวังรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

3.5 บริการพื้นที่ศูนย์คอมพิวเตอร์สำรอง (DR-Site) ของ รฟม.

โดยมีรายละเอียดคุณลักษณะเฉพาะตามภาคผนวก ก

4. คุณสมบัติของผู้ยื่นข้อเสนอ

4.1 มีความสามารถตามกฎหมาย

4.2 ไม่เป็นบุคคลล้มละลาย

4.3 ไม่อยู่ระหว่างเลิกกิจการ

4.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

/4.5 ไม่เป็น...

4.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วน ผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

4.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

4.7 เป็นนิติบุคคล ผู้ประกอบกิจการในด้านการให้บริการอินเทอร์เน็ต และการให้บริการระบบสื่อสารหรือระบบโทรคมนาคม หรือเป็นนิติบุคคล ผู้ประกอบการกิจการในด้านการให้บริการอินเทอร์เน็ตและการให้บริการระบบสื่อสารหรือระบบโทรคมนาคมที่ได้ขึ้นทะเบียนผู้ประกอบการวิสาหกิจขนาดกลางและขนาดย่อม (SMEs)

4.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่น หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรม

4.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกันซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่ รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

4.10 ผู้ยื่นข้อเสนอต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e-GP) ของกรมบัญชีกลาง

4.11 ผู้ยื่นข้อเสนอต้องมีผลงานในการให้บริการช่องทางสื่อสารข้อมูลระบบอินเทอร์เน็ตให้กับส่วนราชการ หน่วยงานตามกฎหมายว่าด้วยระเบียบราชการส่วนท้องถิ่น หน่วยงานของรัฐ รัฐวิสาหกิจ หรือหน่วยงานเอกชนที่ รฟม. เชื่อถือได้ ที่ได้ดำเนินการแล้วเสร็จภายในระยะเวลาไม่เกิน 5 ปี นับถึงวันที่ยื่นข้อเสนอประกวดราคา โดยมีมูลค่าสัญญาไม่น้อยกว่า 7,084,000 บาท (เจ็ดล้านแปดหมื่นสี่พันบาทถ้วน) จำนวนอย่างน้อย 1 สัญญา โดยผู้ยื่นข้อเสนอจะต้องแนบสำเนาหนังสือรับรองผลงานหรือสำเนาสัญญามาพร้อมกับการยื่นข้อเสนอ

5. หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

ในการพิจารณาผลการยื่นข้อเสนอครั้งนี้ รฟม. จะพิจารณาจากเกณฑ์ราคาที่เป็นราคาต่ำสุด อยู่ในวงเงินงบประมาณ รวมทั้งยอมรับเงื่อนไขการจ้างของ รฟม.

6. เงื่อนไขและข้อกำหนดทั่วไป

6.1 ผู้ยื่นข้อเสนอต้องมีวงจรสื่อสารเชื่อมโยงสำหรับการใช้งานระบบเครือข่ายอินเทอร์เน็ตภายในประเทศ (National Internet Exchange: NIX) อย่างน้อย 2 แห่ง ความเร็วรวมกันไม่น้อยกว่า 600 Gbps โดยต้องแสดงแผนผังการเชื่อมต่อตาม Map of Internet Connectivities in Thailand ซึ่งจัดทำโดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) ฉบับล่าสุด ในวันที่ยื่นข้อเสนอนี้

6.2 ผู้ยื่นข้อเสนอต้องมีวงจรสื่อสารเชื่อมโยงสำหรับการใช้งานระบบเครือข่ายอินเทอร์เน็ตต่างประเทศ (International Internet Gateway : IIG) อย่างน้อย 2 แห่ง ความเร็วรวมกันไม่น้อยกว่า 200 Gbps โดยต้องแสดงแผนผังการเชื่อมต่อตาม Map of Internet Connectivities in Thailand ซึ่งจัดทำโดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) ฉบับล่าสุด ในวันที่ยื่นข้อเสนอนี้

6.3 ผู้ยื่นข้อเสนอต้องมีบุคลากรที่มีความรู้ ความเชี่ยวชาญในการเฝ้าระวังความปลอดภัยเทคโนโลยีสารสนเทศ ตามข้อ 3.4 พร้อมทั้งมีใบรับรอง (Certificate) ในด้านที่เกี่ยวข้อง ทั้งนี้ ผู้ยื่นข้อเสนอจะต้องแนบ

/สำเนา...

สำเนาใบรับรอง (Certificate) ดังกล่าว มาพร้อมกับการยื่นข้อเสนอในครั้งนี้ โดยรายละเอียดของใบรับรอง (Certificate) มีดังนี้

6.3.1 การตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ Information Security Management Systems (ISMS) Auditor/Lead Auditor (In Accordance with ISO 27001:2013) อย่างน้อย 1 คน

6.3.2 การเจาะระบบอย่างมีจรรยาบรรณ Certified Ethical Hacker (CEH) อย่างน้อย 1 คน

6.3.3 ความรู้ด้าน Security ตามมาตรฐาน CompTIA (CompTIA Security+) อย่างน้อย 1 คน

6.3.4 ความรู้ด้านบริหารจัดการความมั่นคงปลอดภัยบนระบบ Cloud (Process Cloud Security Manager (PCS)) อย่างน้อย 1 คน

รายการ 6.3.1-6.3.4 สามารถเป็นบุคคลเดียวกันได้

6.4 อุปกรณ์ที่นำมาติดตั้งให้กับ รฟม. ต้องเป็นของแท้ อยู่ในสภาพที่ใช้งานได้ดี เป็นรุ่นที่ยังอยู่ในสายการผลิต (Production Line) และต้องไม่ถูกนำมาปรับปรุงสภาพใหม่ (Reconditioned หรือ Rebuilt)

6.5 ราคาจ้างบริการที่เสนอตามรายการข้อ 3.1 - 3.5 ให้รวมถึง ฮาร์ดแวร์ ซอฟต์แวร์ และค่าใช้จ่ายในการติดตั้ง ซ่อมแซมแก้ไข การให้คำปรึกษา การวิเคราะห์ปัญหา การเคลื่อนย้าย และการเปลี่ยนแปลงค่า (Re-Config) ของอุปกรณ์ที่ได้ติดตั้ง และเกี่ยวข้องตามสัญญานี้ รวมถึงอุปกรณ์อื่นใดที่ไม่ได้กล่าวถึง ซึ่งจำเป็นต้องมี เพื่อให้สามารถใช้งานร่วมกับระบบสื่อสารข้อมูลของ รฟม. ที่มีและใช้งานอยู่ได้อย่างมีประสิทธิภาพ โดย รฟม. มีสิทธิที่จะแจ้งให้ผู้ยื่นข้อเสนอมาดำเนินการให้ รฟม. ได้ตลอดอายุสัญญาโดยไม่มีการคิดค่าใช้จ่ายใดๆ เพิ่มเติมทั้งสิ้น

6.6 อุปกรณ์ต่างๆ ที่นำมาใช้เพื่อให้บริการ ต้องสามารถใช้งานกับระบบไฟฟ้า 220V AC 50Hz โดยไม่ต้องใช้อุปกรณ์แปลงระบบไฟฟ้า และปลั๊กไฟฟ้าของอุปกรณ์จะต้องเป็นชนิด 3 ขา (มีขาสำหรับสายดิน)

6.7 กรณีที่มีการเดินสายสัญญาณเพิ่มเติม ต้องไม่มีการต่อเชื่อมสายใดๆ ในท่อหรือรางร้อยสาย รวมทั้งต้องแยกสายสัญญาณออกจากท่อ หรือรางร้อยสายของระบบไฟฟ้าต่างๆ หรือตามที่ รฟม. กำหนด

6.8 ผู้ยื่นข้อเสนอต้องมีศูนย์ Call Center ที่ได้รับมาตรฐาน ISO9001 เป็นอย่างน้อย

7. ระยะเวลาใช้บริการ

ระยะเวลาการใช้บริการตั้งแต่วันที่ 1 ตุลาคม 2565 ถึงวันที่ 30 กันยายน 2566

8. การติดตั้งและส่งมอบ

8.1 ผู้รับจ้างต้องจัดหา ติดตั้งและให้บริการระบบสื่อสารและโทรคมนาคม ที่มีคุณลักษณะเฉพาะตามข้อ 3.1 - 3.5 โดยต้องทำการติดตั้งและทดสอบความพร้อมการใช้งานให้แล้วเสร็จ ก่อนวันที่ 1 ตุลาคม 2565 อีกทั้งต้องสามารถใช้งานได้ดี และมีประสิทธิภาพไปจนสิ้นสุดสัญญา

8.2 ผู้รับจ้างต้องจัดให้มีการประชุมเริ่มงาน (Kickoff Meeting) เพื่อทำความเข้าใจ และนำเสนอผลการดำเนินงาน ภายใน 15 วัน นับถัดจากวันที่ลงนามในสัญญา

8.3 ผู้รับจ้างต้องจัดให้มีการจัดอบรมเจ้าหน้าที่ผู้ดูแลระบบ เพื่อให้ความรู้ และเสริมสร้างทักษะในการปฏิบัติหน้าที่ที่เกี่ยวข้องกับการให้บริการในข้อ 3. อย่างน้อย 1 หลักสูตร โดยในการฝึกอบรม ผู้รับจ้างต้องเตรียมสถานที่ วิทยากร เอกสารการฝึกอบรม และอื่นๆ ตามที่เหมาะสม ให้กับเจ้าหน้าที่ทุกคนที่เข้าร่วม โดยจำนวนผู้เข้าฝึกอบรมเป็นไปตามที่ รฟม. กำหนด

/8.4 ผู้รับจ้าง...

8.4 ผู้รับจ้างจะต้องจัดทำรายละเอียดผลการดำเนินงานตามคุณลักษณะเฉพาะข้อ 3.1 - 3.5 ตามสัญญา โดยทำเป็นหนังสือยื่นต่อคณะกรรมการตรวจรับพัสดุ ก่อนวันที่ 15 ตุลาคม 2565

9. วงเงินงบประมาณ

17,710,000 บาท (สิบเจ็ดล้านเจ็ดแสนหนึ่งหมื่นบาทถ้วน) (รวมภาษีมูลค่าเพิ่ม)

10. การชำระค่าบริการ

10.1 การชำระค่าจ้างบริการตามสัญญานี้ เป็นการจ้างแบบมีกำหนดระยะเวลา โดย รฟม. จะชำระค่าจ้างเป็นรายงวด แบ่งออกเป็น 4 งวด ซึ่งเป็นราคารวมภาษีมูลค่าเพิ่มตลอดจนภาษีอากรอื่นๆ และค่าใช้จ่ายทั้งปวงด้วยแล้ว มีรายละเอียดดังนี้

10.1.1 งวดที่ 1 รฟม. จะชำระเงินค่าจ้าง เมื่อผู้รับจ้างได้ดำเนินการตามขอบเขตของงานฯ เป็นเวลา 3 เดือน นับตั้งแต่วันที่ 1 ตุลาคม 2565 ถึงวันที่ 31 ธันวาคม 2565 และคณะกรรมการตรวจรับพัสดุฯ ได้ตรวจรับงานถูกต้องครบถ้วนแล้ว

10.1.2 งวดที่ 2 รฟม. จะชำระเงินค่าจ้าง เมื่อผู้รับจ้างได้ดำเนินการตามขอบเขตของงานฯ เป็นเวลา 3 เดือน นับตั้งแต่วันที่ 1 มกราคม 2566 ถึงวันที่ 31 มีนาคม 2566 และคณะกรรมการตรวจรับพัสดุฯ ได้ตรวจรับงานถูกต้องครบถ้วนแล้ว

10.1.3 งวดที่ 3 รฟม. จะชำระเงินค่าจ้าง เมื่อผู้รับจ้างได้ดำเนินการตามขอบเขตของงานฯ เป็นเวลา 3 เดือน นับตั้งแต่วันที่ 1 เมษายน 2566 ถึงวันที่ 30 มิถุนายน 2566 และคณะกรรมการตรวจรับพัสดุฯ ได้ตรวจรับงานถูกต้องครบถ้วนแล้ว

10.1.4 งวดที่ 4 รฟม. จะชำระเงินค่าจ้าง เมื่อผู้รับจ้างได้ดำเนินการตามขอบเขตของงานฯ เป็นเวลา 3 เดือน นับตั้งแต่วันที่ 1 กรกฎาคม 2566 ถึงวันที่ 30 กันยายน 2566 และคณะกรรมการตรวจรับพัสดุฯ ได้ตรวจรับงานถูกต้องครบถ้วนแล้ว

10.2 หากการบริการในเดือนแรกไม่ครบเดือนนั้น ให้คำนวณค่าบริการเริ่มตั้งแต่วันถัดจากวันที่ รฟม. รับมอบงานจากผู้รับจ้าง จนถึงวันสุดท้ายของเดือนนั้น ส่วนการจ้างเดือนสุดท้าย ให้คำนวณค่าจ้างตั้งแต่วันแรกของเดือนนั้นจนถึงวันสิ้นสุดสัญญา

ทั้งนี้ การคำนวณค่าจ้างบริการเป็นรายวัน ให้คิดจากอัตราค่าจ้างต่อเดือนหารด้วย 30 ซึ่งรวมภาษีมูลค่าเพิ่มแล้ว

11. เงื่อนไขด้านการบริการ

11.1 ผู้รับจ้างจะต้องจัดเตรียมเจ้าหน้าที่ผู้เชี่ยวชาญด้านเครือข่ายคอมพิวเตอร์ และ Dedicated Web Server ไว้คอยให้คำปรึกษา รวมถึงคำแนะนำด้านการใช้งาน พร้อมทั้งแก้ปัญหาอื่นๆ ที่เกี่ยวข้องในการใช้บริการของผู้รับจ้าง โดยผู้รับจ้างจะต้องประสานงานกับหน่วยงาน หรือผู้ให้บริการอื่นๆ ที่เกี่ยวข้องในการใช้งานเครือข่ายจนสามารถใช้งานได้ตามปกติ ทุกวันตลอด 24 ชั่วโมง ตลอดระยะเวลาที่ให้บริการตามสัญญา

11.2 ผู้รับจ้างจะต้องมีระบบรับแจ้งข้อมูลปัญหาการใช้งานตลอด 24 ชั่วโมง ทางโทรศัพท์ โทรศัพท์เคลื่อนที่ หรือ E-Mail ตลอดระยะเวลาที่ให้บริการตามสัญญา สำหรับในกรณีเกิดปัญหาหรือเหตุขัดข้องจนเป็นเหตุให้ รฟม.

/ไม่สามารถ...

ไม่สามารถใช้งานบริการได้ ผู้รับจ้างจะต้องมีระบบแจ้งปัญหาหรือเหตุขัดข้องนั้นให้ รฟม. ทราบทาง E-Mail และ SMS ไปยังเบอร์โทรศัพท์มือถือของเจ้าหน้าที่ รฟม. ได้ ตลอดระยะเวลาที่ใช้บริการโดยอัตโนมัติในทันที

11.3 ผู้รับจ้างจะต้องตอบรับทราบปัญหาหรือเหตุขัดข้องทันทีที่ได้รับแจ้งเหตุจาก รฟม. ภายใน 1 ชั่วโมง หลังจากได้รับแจ้งเหตุด้วยโทรศัพท์ โทรศัพท์เคลื่อนที่ หรือ E-Mail รวมถึงช่องทางการสื่อสารอื่นๆ ตามที่ รฟม. กำหนด และจะต้องดำเนินการแก้ไขให้วงจรสื่อสารกลับสู่สภาพปกติที่สามารถใช้งานได้โดยเร็วที่สุด

11.4 เมื่อมีการตรวจสอบ และ/หรือ ดำเนินการแก้ไขปัญหาขัดข้องใดๆ เสร็จสิ้น ผู้รับจ้างต้องแจ้งรายงานผลการดำเนินการดังกล่าวให้แก่ รฟม. ทราบหลังจากที่แก้ไขปัญหาแล้วเสร็จ และระหว่างที่ยังคงดำเนินการแก้ไขปัญหาไม่เสร็จสิ้น ผู้รับจ้างจะต้องแจ้งรายงานผลความคืบหน้าให้ รฟม. ทราบเป็นระยะๆ

11.5 กรณีอุปกรณ์ที่นำมาติดตั้งให้กับ รฟม. เกิดการชำรุดบกพร่องขึ้น อุปกรณ์ที่ใช้ในการแก้ไขซ่อมแซมหรือทดแทนอุปกรณ์ที่ชำรุด จะต้องเป็นอุปกรณ์ของแท้ ที่สามารถใช้งานได้ดี เป็นรุ่นที่ยังอยู่ในสายการผลิต (Production Line) และต้องไม่ถูกนำมาปรับปรุงสภาพใหม่ (Reconditioned หรือ Rebuilt)

12. อัตราค่าปรับ

12.1 กรณีที่ผู้รับจ้างไม่สามารถติดตั้งและส่งมอบงานได้แล้วเสร็จตามกำหนด ผู้รับจ้างยินยอมให้ รฟม. ปรับในอัตราร้อยละ 0.1 (ศูนย์จุดหนึ่ง) ของวงเงินค่าจ้างทั้งหมดตามสัญญาเป็นรายวัน (เศษของวันให้นับเป็นหนึ่งวัน) โดยค่าปรับข้างต้นผู้รับจ้างยินยอมให้ รฟม. หักจากค่าจ้างบริการรายเดือนที่รวมภาษีมูลค่าเพิ่มหรือเงินอื่นๆ ที่ค้างจ่ายได้ทันที โดย รฟม. ไม่ต้องบอกสงวนสิทธิ์แต่อย่างใด

12.2 อุปกรณ์ใดๆ ที่ใช้ในการซ่อมแซมหรือทดแทนอุปกรณ์ที่ชำรุด จะต้องเป็นอุปกรณ์ที่สามารถใช้งานได้ดีโดยไม่เกิดปัญหาใดๆ จากอุปกรณ์นั้นๆ หากความเสียหายที่เกิดจากเหตุขัดข้องทางเทคนิคที่พิสูจน์ได้ว่าเกิดจากเครือข่ายหรืออุปกรณ์ของผู้ให้บริการเป็นเหตุให้ รฟม. ไม่สามารถใช้งานได้ ผู้ให้บริการตกลงยินยอมชดเชยค่าใช้บริการให้ รฟม. โดยต้องมีการรับประกันคุณภาพการให้บริการ (Service Level Agreement : SLA) ไม่ต่ำกว่า 99.6% โดยรับประกันการใช้งานได้ของวงจรในแต่ละเดือน เมื่อนับจำนวนนาทีที่วงจรขัดข้องรวมกันแล้วเป็นจำนวนมากกว่า 172 นาที (หรือ 2 ชั่วโมง 52 นาที) หากเกินจำนวนที่รับประกันไว้ ผู้ให้บริการจะชดเชยค่าใช้บริการ ให้ตามจำนวนชั่วโมงที่วงจรขัดข้อง และเศษของชั่วโมงให้นับเป็นหนึ่งชั่วโมง โดยให้คำนวณดังนี้

$$\frac{\text{ชั่วโมงที่เสีย X ค่าใช้บริการรายเดือน (รวมภาษีมูลค่าเพิ่ม)}}{720}$$

13. ข้อสงวนสิทธิ์

ผู้รับจ้าง และ/หรือเจ้าหน้าที่ของผู้รับจ้าง ที่เข้าถึงระบบเทคโนโลยีสารสนเทศของ รฟม. ต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของ รฟม. ปรากฏดังภาคผนวก ข และจะต้องรักษาความลับต่างๆ ที่ได้จากการปฏิบัติงาน โดยห้ามมิให้ผู้รับจ้าง และ/หรือเจ้าหน้าที่ของผู้รับจ้างนำข้อมูลส่วนหนึ่งส่วนใดหรือทั้งหมดที่ได้จากการปฏิบัติงานใน รฟม. ไปทำซ้ำ เผยแพร่ หรือวิเคราะห์ประมวลผลเพื่อการอื่นใด ไม่ว่าการกระทำดังกล่าวจะเป็นการหาผลประโยชน์หรือไม่ก็ตาม หาก รฟม. ตรวจพบผู้รับจ้างต้องชดใช้ค่าเสียหายเป็นจำนวนเงินไม่น้อยกว่าค่าเช่าทั้งหมดที่กำหนดไว้ในสัญญา ทั้งนี้ ผู้รับจ้าง และ/หรือเจ้าหน้าที่ของผู้รับจ้างต้องลงนามในสัญญาการเก็บรักษาข้อมูลไว้เป็นความลับ (Non-Disclosure Agreement) ก่อนเริ่มปฏิบัติงาน ตามรูปแบบที่ รฟม. กำหนด

/ภาคผนวก...

ภาคผนวก ก

รายละเอียดคุณลักษณะเฉพาะ

1. บริการช่องทางสื่อสารข้อมูลระบบอินเทอร์เน็ต มีรายละเอียดดังนี้

1.1 ผู้รับจ้างต้องจัดหาวงจรสื่อสารข้อมูลสำหรับใช้เป็นช่องทางสื่อสารข้อมูลระบบเครือข่ายอินเทอร์เน็ต เชื่อมโยงระหว่าง รฟม. ณ ศูนย์คอมพิวเตอร์ อาคาร 1 ชั้น 5 (ต้นทาง) กับผู้ให้บริการอินเทอร์เน็ต (ISP) (ปลายทาง) จำนวน 2 วงจร (วงจรหลักและวงจรสำรอง) โดยมีรายละเอียดของวงจรดังนี้

1.1.1 เป็นวงจรสื่อสารความเร็วสูงผ่านโครงข่ายใยแก้วนำแสง (Fiber Optic)

1.1.2 วงจรหลักสามารถให้บริการอินเทอร์เน็ตภายในประเทศ (Domestic) ความเร็วไม่ต่ำกว่า 300 Mbps และบริการอินเทอร์เน็ตต่างประเทศ (International) ความเร็วไม่ต่ำกว่า 300 Mbps

1.1.3 วงจรสำรองสามารถให้บริการอินเทอร์เน็ตภายในประเทศ (Domestic) และบริการอินเทอร์เน็ตต่างประเทศ (International) ที่มีความเร็วเท่ากับวงจรหลัก ทั้งนี้วงจรสำรองจะต้องเป็นผู้ให้บริการ (ISP) ที่มี AS Number แตกต่างจากผู้ให้บริการหลัก และต้องมีคุณสมบัติตามข้อ 6.1 และ 6.2 ในข้อกำหนดทั่วไป เพื่อให้การใช้งานอินเทอร์เน็ตของ รฟม. มีประสิทธิภาพในการใช้งานได้อย่างต่อเนื่อง

1.1.4 วงจรหลักและวงจรสำรองสามารถใช้บริการได้พร้อมกันทั้ง 2 วงจร ซึ่งมีเส้นทางที่เป็นของตนเองแยกกันชัดเจน หากวงจรใดวงจรหนึ่งไม่สามารถใช้งานได้ ระบบต้องสามารถสลับวงจรไปใช้งานอีกวงจรที่ทำงานอยู่ และต้องทำการเพิ่มความเร็วในการให้บริการอินเทอร์เน็ตให้กับวงจรที่ใช้งานได้อย่างต่อเนื่อง เพื่อชดเชยการให้บริการอินเทอร์เน็ตของวงจรที่ไม่สามารถใช้งานได้ โดยมีความเร็ว ไม่ต่ำกว่า 600 Mbps สำหรับบริการอินเทอร์เน็ตภายในประเทศ (Domestic) และมีความเร็วไม่ต่ำกว่า 600 Mbps สำหรับบริการอินเทอร์เน็ตต่างประเทศ (International) หรือตามที่ รฟม. ร้องขอ ทั้งนี้ ต้องสามารถใช้งานทั้งการรับ-ส่งข้อมูลได้ ทุกประเภท โดยไม่จำกัดปริมาณของข้อมูล ชั่วโมงการใช้งาน และจำนวนผู้ใช้งาน ได้ตลอดระยะเวลาที่ใช้บริการ

1.1.5 วงจรหลักและวงจรสำรองต้องมีช่องทางสื่อสารเชื่อมโยงข้อมูลระบบเครือข่ายอินเทอร์เน็ตภายใน ประเทศ (National Internet Exchange: NIX) และช่องทางสื่อสารข้อมูลระบบเครือข่ายอินเทอร์เน็ตต่างประเทศ (International Internet Gateway : IIG) ที่เป็นของตนเองแยกกันชัดเจน

1.1.6 ผู้รับจ้างต้องจัดหาเส้นทางเชื่อมโยงโครงข่ายใยแก้วนำแสง (Fiber Optic) จำนวน 2 เส้นมาที่ศูนย์คอมพิวเตอร์หลัก ชั้น 5 อาคาร 1 รฟม. โดยแต่ละเส้นทางต้องแยกชุมสาย (Node) อิสระต่อกัน โดยแสดงเส้นทางเชื่อมโยงในวันที่ยื่นข้อเสนอ

1.1.7 ผู้รับจ้างต้องจัดหาวงจรสำรองให้บริการอินเทอร์เน็ตภายในประเทศ (Domestic) และบริการอินเทอร์เน็ตต่างประเทศ (International) ในการเชื่อมโยงโครงข่ายใยแก้วนำแสงแยกเส้นทางและแยกชุมสาย (Node) จากข้อ 1.1.6 โดยแสดงเส้นทางเชื่อมโยงในวันที่ยื่นข้อเสนอ

1.2 ผู้รับจ้างต้องจัดหา IP Address Version 4 (IPv4) จำนวน 2 Class C โดยให้จัดหาวงจรละ 1 Class C ที่มี IP เรียงต่อเนื่องกัน (/24)

1.3 ผู้รับจ้างต้องจัดหา IP Address Version 6 (IPv6) จำนวน 2 Class โดยให้จัดหาวงจรละ 1 Class (/48)

1.4 ผู้รับจ้างต้องดำเนินการต่อทะเบียน Public AS Number แบบสมาชิก ตลอดระยะเวลาที่ใช้บริการ พร้อมทั้ง Public IP Address ไม่น้อยกว่า 1 Class C โดยให้เป็นสิทธิ์ถือครองของ รฟม. ซึ่งสามารถเข้าถึงได้จากเครือข่ายอินเทอร์เน็ตทั่วโลกตามการใช้งานจริง และจดทะเบียนให้อยู่ภายใต้ Public AS Number ของ รฟม.

/1.5 ผู้รับจ้าง...

1.5 ผู้รับจ้างต้องดำเนินการจดทะเบียนหรือต่ออายุโดเมน (www.mrta.co.th) โดยให้สิทธิ์การถือครองเป็นของ รฟม. ตลอดระยะเวลาที่ใช้บริการ

1.6 ผู้รับจ้างต้องดำเนินการจดทะเบียนใบรับรองความปลอดภัยทางอิเล็กทรอนิกส์ ที่ออกหรืออนุมัติโดย CA (Certificate Authority) แบบ Wildcard ในการรับรองด้านความปลอดภัย เพื่อยืนยันการมีตัวตนของเจ้าของเว็บไซต์ หรือ E-Mail และยืนยันความสมบูรณ์ของการเข้ารหัสข้อมูลทางอิเล็กทรอนิกส์ผ่าน Secure Socket Layer (SSL) แบบ Organization ภายใต้โดเมนเนม (mrta.co.th) ซึ่งสามารถเข้าถึงได้จากเครือข่ายอินเทอร์เน็ตทั่วโลกตามการใช้งานจริง โดยให้สิทธิ์การถือครองเป็นของ รฟม. ตลอดระยะเวลาที่ใช้บริการ

1.7 ผู้รับจ้างต้องจัดหา ติดตั้ง และปรับแต่งค่า (Configuration) อุปกรณ์ค้นหาเส้นทาง (Router) อุปกรณ์กระจายสัญญาณ (Layer 2 Switch) และอุปกรณ์อื่นๆ ที่จำเป็น โดยมีจำนวนอุปกรณ์และมีประสิทธิภาพเพียงพอในการให้บริการอินเทอร์เน็ตทั้ง 2 วงจร ตลอดอายุสัญญา ซึ่งสามารถค้นหาเส้นทางเข้าสู่เครือข่ายอินเทอร์เน็ตผ่านโปรโตคอล BGP โดยระบบต้องสามารถสลับวงจรไปใช้งานอีกวงจรที่ทำงานอยู่ได้ในทันที หากวงจรใดวงจรหนึ่งไม่สามารถใช้งานได้

1.8 ผู้รับจ้างต้องมีระบบตรวจสอบสถิติการใช้งาน Internet แบบ Real Time แสดงผลในรูปแบบกราฟ Multi Router Traffic Grapher (MRTG) ซึ่งระบบต้องทำการแยกวงจรระหว่างวงจรสื่อสารภายใน ประเทศ (Domestic) และต่างประเทศ (International) โดยแยกรายละเอียดข้อมูลการใช้งานของแต่ละวงจรได้อย่างชัดเจน

1.9 ผู้รับจ้างต้องจัดหาระบบ Web Server และระบบ Database Server โดยมีรายละเอียดดังนี้

1.9.1 ผู้รับจ้างต้องจัดหาระบบ Web Server จำนวน 2 เครื่อง สำหรับการใช้งานเว็บไซต์ (www.mrta.co.th) และการใช้งาน Back-Office ของ Application รฟม. โดยแต่ละ Server ต้องมีคุณสมบัติเป็นอย่างน้อยดังนี้

1.9.1.1 สามารถทำงานในรูปแบบของ Enterprise Virtual Private Server (VPS) หรือ Dedicated Web Server หรือดีกว่า มีหน่วยประมวลผลกลาง (CPU) ที่มีแกนประมวลผล (Core) รวมไม่น้อยกว่า 12 แกน และมีหน่วยความจำภายในเครื่อง (RAM) ไม่น้อยกว่า 32 GB

1.9.1.2 มีพื้นที่สำหรับ Content ไม่น้อยกว่า 500 GB โดย รฟม. สามารถจัดการเพิ่ม/ลบ/เปลี่ยนแปลง Content ได้ตลอดระยะเวลาที่ใช้บริการ

1.9.1.3 มีการติดตั้ง Software Nginx, Apache HTTPD, Internet Information Service (IIS) หรืออื่น ๆ ที่รองรับรองรับการทำงานของภาษา PHP, ASP.NET พร้อมโปรโตคอล http, https และ sftp

1.9.1.4 มีการรองรับการทำงานในรูปแบบ Shell Script

1.9.1.5 มีระบบที่สามารถบริหารจัดการ (Control Panel) เช่น Plesk, Cpanel และ WHM

1.9.1.6 รองรับการทำงานตามมาตรฐานเว็บไซต์ภาครัฐ ของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) : สพร.

1.9.1.7 มีเครื่องมือสำหรับเก็บข้อมูล (Web Analytic) การเยี่ยมชมเว็บไซต์ของ รฟม. เช่น จำนวนครั้ง จำนวนหน้า ระยะเวลาการใช้งาน เป็นต้น

1.9.1.8 มีการเข้ารหัสข้อมูล (Encryption) เพื่อเพิ่มความปลอดภัยในการสื่อสารหรือส่งข้อมูลผ่านเครือข่ายอินเทอร์เน็ต แบบ Secure Socket Layer (SSL) หรือ (https) ตลอดระยะเวลาที่ใช้บริการ

/1.9.2 ผู้รับจ้าง...

1.9.2 ผู้รับจ้างต้องจัดหาระบบ Database Server จำนวน 2 ระบบ สำหรับการใช้งานเว็บไซต์ รฟม. (www.mrta.co.th) และการใช้งาน Back-Office ของ Application ให้ข้อมูลบริการรถไฟฟ้า MRT โดยแต่ละ Server ต้องมีคุณสมบัติเป็นอย่างน้อยดังนี้

1.9.2.1 สามารถทำงานในรูปแบบของ Enterprise Virtual Private Server (VPS) หรือ Dedicated Web Server หรือดีกว่า มีหน่วยประมวลผลกลาง (CPU) ที่มีแกนประมวลผล (Core) รวมไม่น้อยกว่า 12 แกน และมีหน่วยความจำภายในเครื่อง (RAM) ไม่น้อยกว่า 32 GB

1.9.2.2 มีพื้นที่สำหรับบริหารจัดการ Database ไม่น้อยกว่า 500 GB โดย รฟม. สามารถจัดการเพิ่ม/ลบ/เปลี่ยนแปลงฐานข้อมูลได้ตลอดระยะเวลาที่ใช้บริการ และรองรับการทำงานได้ในอนาคต ตามที่ รฟม. ต้องการ

1.9.2.3 สามารถทำงานในรูปแบบของฐานข้อมูล Microsoft SQL Server 2019 ขึ้นไป และ MySQL Version 8 ขึ้นไป

1.9.3 มีการจัดเก็บ Log File ที่ถูกต้องตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 (หรือฉบับที่มีผลบังคับใช้)

1.9.4 สามารถใช้งานผ่านเครือข่าย Internet Protocol Version 6 (IPv6) ได้

1.9.5 มีระบบการ Monitoring โดยสามารถตรวจสอบสถานะการทำงานได้ เช่น Monitor Host Server ในการตรวจสอบสถานะ Uptime และ Monitor Services เพื่อใช้ในการตรวจสอบ HTTP (TCP/port 80), HTTPS (TCP/port 443) โดยเมื่อพบปัญหาหรือเหตุขัดข้องจนเป็นเหตุให้ รฟม. ไม่สามารถใช้งานได้ ระบบต้องส่ง Alert เป็น E-Mail และ SMS ไปยังเบอร์โทรศัพท์มือถือของเจ้าหน้าที่ รฟม. ได้ ตลอดระยะเวลาที่ใช้บริการ

1.10 ผู้รับจ้างต้องจัดหาระบบป้องกันการโจมตีเว็บไซต์ Web Application Firewall (WAF) และ Web Application Firewall Support for SSL Websites รวมถึงการป้องกันภัยคุกคามจากการโจมตีเว็บไซต์ (www.mrta.co.th) ของ รฟม. โดยสามารถป้องกันภัยคุกคามได้อย่างน้อย ดังต่อไปนี้

1.10.1 ป้องกันเว็บไซต์ขั้นพื้นฐาน คือ SQL injection, XSS javascript, หรือ CMS เช่น WordPress, Magento, Drupal, PHP, Joomla

1.10.2 ป้องกันเว็บไซต์ระดับสูงสุด คือ OWASP (Open Web Application Security Project) 10 อันดับช่องโหว่ที่ส่งผลกระทบรุนแรงต่อเว็บแอปพลิเคชัน

1.10.3 ป้องกันเว็บไซต์ DDoS Attacks ในระดับ Application DDoS

1.10.4 โดยผู้รับจ้างจะต้องจัดทำ Policy Configuration หรือปรับเปลี่ยน Policy ตามที่ รฟม. กำหนด

1.10.5 หากเกิดการโจมตีเว็บไซต์เกิดขึ้น จะต้องแจ้งเตือน รฟม. ทราบทาง E-Mail หรือ โทรศัพท์ หรือ SMS ไปยังเบอร์โทรศัพท์มือถือของเจ้าหน้าที่ รฟม. ทันทีที่เกิดเหตุการณ์ขึ้น และจัดทำรายงานแจ้งเหตุที่เกิดจากการโจมตี

1.11 ผู้รับจ้างต้องมีการตรวจสอบ DNS Security ให้กับโดเมนของ รฟม. (mrta.co.th) ตลอดระยะเวลาที่ใช้บริการ

/1.12 ผู้รับจ้าง...

1.12 ผู้รับจ้างต้องจัดหาระบบ E-Mail Security (E-Mail Firewall, Zero-Hour Antivirus, Spam Detection และ Virus Protection) สำหรับใช้ป้องกันระบบ E-Mail (Mail Gateway) ทั้งขาเข้าและขาออก ก่อนส่งมายัง Mail Server ของ รฟม. โดยสามารถป้องกัน Mail Box ของ รฟม. ได้ไม่น้อยกว่า 600 Accounts พร้อมทั้งจัดส่งรายงานสรุปผลเป็น PDF File ให้กับ รฟม. ทางจดหมายอิเล็กทรอนิกส์และจัดทำรายงานสรุปเป็นเอกสารสีนำเสนอต่อคณะกรรมการตรวจรับพัสดุ เป็นประจำทุกเดือนตลอดระยะเวลาที่ใช้บริการ โดยจัดส่งภายในวันที่ 15 ของเดือนถัดไป

1.13 ผู้รับจ้างต้องจัดหาซิมการ์ด (SIM Card) เพื่อส่งข้อความไปยังโทรศัพท์มือถือได้ทุกระบบที่ให้บริการในประเทศไทย โดยสามารถส่งข้อความสั้น (SMS) ได้ไม่น้อยกว่า 12,000 ข้อความ/ปี

1.14 ผู้รับจ้างต้องจัดหาอุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย (Pocket WIFI) พร้อมซิมการ์ด (SIM Card) โดยสามารถใช้งานอินเทอร์เน็ตได้ไม่จำกัดปริมาณการใช้งาน จำนวนไม่น้อยกว่า 3 ชุด

2. บริการเชื่อมโยงระบบเครือข่ายระหว่างสำนักงานใหญ่กับสำนักงานย่อย มีรายละเอียดดังนี้

2.1 ผู้รับจ้างต้องจัดหาวงจรสื่อสารข้อมูลสำหรับใช้เป็นช่องทางสื่อสารข้อมูลระบบเครือข่ายคอมพิวเตอร์ของ รฟม. ด้วยเทคโนโลยี Multi Protocol Label Switching (MPLS) แบบ Point-to-Multipoint ผ่านวงจรสื่อสารความเร็วสูงผ่านโครงข่ายใยแก้วนำแสง (Fiber Optic) จำนวน 15 วงจร กำหนดต้นทางที่ศูนย์คอมพิวเตอร์หลัก ชั้น 5 อาคาร 1 รฟม. โดยมีรายละเอียดปลายทาง ความเร็ว และพอร์ตเชื่อมต่อ ดังตารางต่อไปนี้

ลำดับ	รายละเอียด		
	ปลายทาง	ความเร็ว	พอร์ตเชื่อมต่อ
1	ห้องทำงานฝ่ายปฏิบัติการ (ฝปก.) ชั้น M อาคาร BEM	100 Mbps	Fast Ethernet
2	อาคารเก็บสุนัข K9 ฝ่ายรักษาความปลอดภัยและกู้ภัย (ฝรภ.) บริเวณประตูทางเข้า – ออก รฟม. ทางด้านถนนวัฒนธรรม	3 Mbps	Fast Ethernet
รถไฟฟ้ามหานคร สายเฉลิมรัชมงคล			
3	ห้องทำงานฝ่ายรักษาความปลอดภัยและกู้ภัย (ฝรภ.) ชั้น 1 อาคารจอดรถ สถานีศูนย์วัฒนธรรมแห่งประเทศไทย	30 Mbps	Fast Ethernet
4	ห้องวิทยุฝ่ายรักษาความปลอดภัยและกู้ภัย (ฝรภ.) ชั้น 3 อาคารจอดรถสถานีลาดพร้าว	30 Mbps	Fast Ethernet
5	ห้องทำงานฝ่ายรักษาความปลอดภัยและกู้ภัย (ฝรภ.) ชั้น 2 สถานีกำแพงเพชรทางออกที่ 1 ถนนกำแพงเพชร	30 Mbps	Fast Ethernet
รถไฟฟ้ามหานคร สายเฉลิมรัชมงคล (ส่วนต่อขยาย)			
6	ห้องควบคุมฝ่ายปฏิบัติการ อาคารจอดรถ 10 ชั้น ซอยเพชรเกษม 80 สถานีหลักสอง	20 Mbps	Fast Ethernet
7	ห้องควบคุมฝ่ายปฏิบัติการ อาคารจอดรถ 8 ชั้น ซอยเพชรเกษม 47 สถานีหลักสอง	20 Mbps	Fast Ethernet

/ลำดับ...

ลำดับ	รายละเอียด		
	ปลายทาง	ความเร็ว	พอร์ตเชื่อมต่อ
รถไฟฟ้ามหานคร สายฉลองรัชธรรม			
8	ห้องทำงานฝ่ายปฏิบัติการ (ฝปก.) ชั้น 2 อาคารตึก Admin ศูนย์ซ่อมบำรุง รักษาโครงการรถไฟฟ้าสายสีม่วง ช่วงบางใหญ่ - บางซื่อ	30 Mbps	Fast Ethernet
9	ห้องทำงานฝ่ายปฏิบัติการ (ฝปก.) อาคารจอดรถสถานีสามแยกบางใหญ่ โครงการรถไฟฟ้าสายสีม่วง ช่วงบางใหญ่ - บางซื่อ ถนนรัตนาธิเบศร์	30 Mbps	Fast Ethernet
10	ห้องทำงานฝ่ายปฏิบัติการ (ฝปก.) อาคารจอดรถสถานีแยกนนทบุรี 1 ถนนรัตนาธิเบศร์	30 Mbps	Fast Ethernet
11	ห้องทำงานฝ่ายปฏิบัติการ (ฝปก.) อาคารจอดรถสถานีบางรักน้อย - ท่าอิฐ ถนนรัตนาธิเบศร์	30 Mbps	Fast Ethernet
12	ห้องควบคุมฝ่ายปฏิบัติการ ท่าเรือสถานีสะพานพระนั่งเกล้า	60 Mbps	Fast Ethernet
โครงการรถไฟฟ้าสายสีเขียว ช่วงหมอชิต – สะพานใหม่ - คูคต			
13	ห้องควบคุมอาคารจอดรถสถานีคูคต ใกล้สถานีตำรวจภูธรคูคต ถนนลำลูกกา	20 Mbps	Fast Ethernet
14	ห้องควบคุมอาคารจอดรถ สถานี กม.25 ใกล้แยก คปอ. ถนนพหลโยธิน	20 Mbps	Fast Ethernet
โครงการรถไฟฟ้าสายสีเขียว ช่วงแบริ่ง – สมุทรปราการ			
15	ห้องควบคุมลานจอดรถสถานีการเคหะฯ ถนนศรีนครินทร์	20 Mbps	Fast Ethernet

2.2 ผู้รับจ้างต้องจัดหา ติดตั้ง ปรับแต่งค่า (Configuration) อุปกรณ์ค้นหาเส้นทาง (Router) อุปกรณ์กระจายสัญญาณไม่น้อยกว่า (Layer 2 Switch) และอุปกรณ์อื่นๆ ที่จำเป็น โดยมีจำนวนอุปกรณ์และมีประสิทธิภาพเพียงพอในการให้บริการทุกจุด สำหรับเชื่อมโยงระบบทั้งฝั่งต้นทางและปลายทาง ให้สามารถใช้งานร่วมกับระบบเครือข่ายคอมพิวเตอร์ภายในของ รฟม. ได้อย่างมีประสิทธิภาพ ทั้งนี้ รฟม. สามารถใช้งานทั้งการรับ-ส่งข้อมูลได้ทุกประเภทโดยไม่จำกัดปริมาณของข้อมูล ชั่วโมงการใช้งาน และจำนวนผู้ใช้งาน สามารถใช้งานได้ตลอดระยะเวลาที่ใช้บริการตามสัญญา อนึ่ง ผู้รับจ้างจะต้องประสานงานกับผู้ดูแลอาคารสถานที่ และปฏิบัติตามระเบียบข้อกำหนด จนสามารถเดินสายภายในอาคารให้แล้วเสร็จ ตามที่ รฟม. กำหนด

2.3 รฟม. มีสิทธิร้องขอผู้รับจ้างให้จัดหาวงจรสื่อสารข้อมูลที่มีคุณสมบัติและความเร็วในการใช้งานตามข้อ 2.2 เพิ่มเติมได้ในอนาคต เพื่อเชื่อมโยงระบบเครือข่ายคอมพิวเตอร์ระหว่างศูนย์คอมพิวเตอร์ ฝ่ายเทคโนโลยีสารสนเทศ รฟม. ไปยังจุดติดตั้งตามที่ รฟม. กำหนด (ปลายทาง) จำนวนไม่น้อยกว่า 2 วงจร ที่มีความเร็วแต่ละวงจรไม่น้อยกว่า 30 Mbps โดย รฟม. ไม่ต้องเสียค่าใช้บริการใดๆ เพิ่มเติมทั้งสิ้นตลอดระยะเวลาที่ใช้บริการตามสัญญา

/3. บริการ...

3. บริการเชื่อมโยงระบบเครือข่ายสำหรับระบบรายงานจำนวนที่จอดรถว่างแบบ Real Time มีรายละเอียดดังนี้

3.1 ผู้รับจ้างต้องจัดหาวงจรสื่อสารข้อมูลสำหรับใช้เป็นช่องทางสื่อสารข้อมูลระบบเครือข่ายคอมพิวเตอร์ของ รฟม. ด้วยเทคโนโลยี Multi Protocol Label Switching (MPLS) แบบ Point-to-Multipoint ผ่านวงจรสื่อสารความเร็วสูงผ่านโครงข่ายใยแก้วนำแสง (Fiber Optic) กำหนดต้นทางที่ศูนย์คอมพิวเตอร์หลัก ชั้น 5 อาคาร 1 รฟม. ไปยังปลายทาง ด้วยเทคโนโลยีการเชื่อมต่อ VPN แบบ 3G หรือดีกว่า จำนวน 12 วงจร ดังตารางต่อไปนี้

ลำดับ	สถานที่ติดตั้ง	
	ปลายทาง	ความเร็ว
1	ตู้เก็บเงินค่าบริการจอดรถบริเวณทางเข้า-ออกที่ 4 ลานจอดรถสถานีรัชดาภิเษก (ซอยรัชดาภิเษก 28)	2 Mbps
2	ตู้เก็บเงินค่าบริการจอดรถบริเวณทางเข้า-ออก ที่ 1 ลานจอดรถสถานีห้วยขวาง (ใกล้สี่แยกห้วยขวาง)	2 Mbps
3	ตู้เก็บเงินค่าบริการจอดรถบริเวณทางเข้า-ออก ที่ 1 ลานจอดรถสถานีศูนย์วัฒนธรรมแห่งประเทศไทย (ใกล้แยกเทียมร่วมมิตร)	2 Mbps
4	ตู้เก็บเงินค่าบริการจอดรถบริเวณทางเข้า-ออกที่ 2 ลานจอดรถสถานีศูนย์วัฒนธรรมแห่งประเทศไทย (ซอยรัชดาภิเษก 6)	2 Mbps
5	ตู้เก็บเงินค่าบริการจอดรถบริเวณทางเข้า-ออกที่ 1 ลานจอดรถสถานีเพชรบุรี (ใกล้แยกอโศก - เพชรบุรี)	2 Mbps
6	ตู้เก็บเงินค่าบริการจอดรถบริเวณทางเข้า-ออกที่ 2 ลานจอดรถสถานีศูนย์การประชุมแห่งชาติสิริกิติ์ ด้านถนนรัชดาภิเษก บริเวณสี่แยกคลองเตย	2 Mbps
7	ตู้เก็บเงินค่าบริการจอดรถบริเวณทางเข้า-ออกที่ 1 ลานจอดรถสถานีสามย่าน ด้านหน้าวัดหัวลำโพง	2 Mbps
8	ตู้เก็บเงินค่าบริการจอดรถ บริเวณทางเข้า-ออกที่ 2 ลานจอดรถสถานีพระรามเก้า (ซอยรัชดาภิเษก 2)	2 Mbps
9	ตู้เก็บเงินค่าบริการจอดรถบริเวณอาคารจอดรถสถานีคลองบางไผ่ ถนนกาญจนาภิเษก	2 Mbps
10	ตู้เก็บเงินค่าบริการจอดรถบริเวณอาคารจอดรถสถานีสามแยกบางใหญ่ ถนนรัตนาธิเบศร์	2 Mbps
11	ตู้เก็บเงินค่าบริการจอดรถบริเวณอาคารจอดรถ สถานีแยกนนทบุรี 1 ถนนรัตนาธิเบศร์	2 Mbps
12	ตู้เก็บเงินค่าบริการจอดรถบริเวณอาคารจอดรถสถานีบางรักน้อย-ท่าอิฐ ถนนรัตนาธิเบศร์	2 Mbps

3.2 ผู้รับจ้างต้องจัดหา ติดตั้ง ปรับแต่งค่า (Configuration) อุปกรณ์ค้นหาเส้นทาง (Router) และอุปกรณ์อื่นๆ ที่จำเป็น ที่มีจำนวนอุปกรณ์และมีประสิทธิภาพเพียงพอในการให้บริการทุกจุด สำหรับเชื่อมโยงระบบทั้งฝั่งต้นทางและปลายทาง ให้สามารถใช้งานร่วมกับระบบเครือข่ายคอมพิวเตอร์ภายในของ รฟม. ได้อย่างมีประสิทธิภาพ ทั้งนี้ รฟม. สามารถใช้งานทั้งการรับ-ส่งข้อมูลได้ ทุกประเภทโดยไม่จำกัดปริมาณของข้อมูลชั่วโมงการใช้งาน และจำนวนผู้ใช้งานสามารถใช้งานได้ตลอดระยะเวลาที่ใช้บริการตามสัญญา

/3.3 รฟม....

3.3 รฟม. มีสิทธิ์ร้องขอผู้รับจ้างให้จัดหาวงจรสื่อสารข้อมูลที่มีคุณสมบัติและความเร็วในการใช้งานตามข้อ 3.1 เพิ่มเติมได้ในอนาคต เพื่อเชื่อมโยงระบบเครือข่ายคอมพิวเตอร์ สำหรับใช้งานกับระบบรายงานจำนวนที่จอดรถว่างแบบ Real Time ระหว่างศูนย์คอมพิวเตอร์ ฝ่ายเทคโนโลยีสารสนเทศ รฟม. ไปยังจุดติดตั้งตามที่ รฟม. กำหนด (ปลายทาง) จำนวนไม่น้อยกว่า 10 วงจร โดย รฟม. ไม่ต้องเสียค่าใช้บริการใดๆ เพิ่มเติมทั้งสิ้นตลอดระยะเวลาที่ใช้บริการตามสัญญา

4. บริการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์และการเฝ้าระวังรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ มีรายละเอียดดังนี้

4.1 ผู้รับจ้างต้องทำการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log File Collection) เฝ้าระวังความปลอดภัยเทคโนโลยีสารสนเทศ (Security Monitoring) การประเมินความเสี่ยงให้กับระบบและอุปกรณ์ต่างๆ ของ รฟม. ตามที่กำหนด โดยมีรายละเอียดดังตารางต่อไปนี้

ลำดับ	รายการอุปกรณ์	รายละเอียดของบริการ	
		Log File Collection	Security Monitoring
1	Active Directory (No.1)	✓	✓
2	Active Directory (No.2)	✓	✓
3	Active Directory (No.3)	✓	✓
4	Mail Server (No.1)	✓	✓
5	Mail Server (No.2)	✓	✓
6	Mail Server (No.3)	✓	✓
7	Advance Persistent Threat (APT) Appliance	✓	✓
8	Network Firewall Appliance	✓	✓
9	Network Load Balancer Appliance	✓	✓
10	Intrusion Prevention System (IPS) Appliance	✓	✓
11	Identity Service	✓	✓
12	Wireless Controller Appliance	✓	✓
13	KM Server	✓	✓
14	E-DOC Server	✓	✓
15	CRM Website	✓	✓
16	CRM System & Social Listening	✓	✓

ทั้งนี้ รฟม. มีสิทธิ์ในการเปลี่ยนแปลงรายการอุปกรณ์ในตารางตามที่ รฟม. กำหนด และมีสิทธิ์ร้องขอในการเพิ่มเติมจากรายการอุปกรณ์ จำนวนไม่น้อยกว่า 2 รายการอุปกรณ์ โดย รฟม. ไม่ต้องเสียค่าใช้บริการใดๆ เพิ่มเติมทั้งสิ้นตลอดระยะเวลาที่ใช้บริการตามสัญญา

/4.2 ผู้รับจ้าง...

4.2 ผู้รับจ้างต้องให้บริการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log File) และเฝ้าระวังความปลอดภัยเทคโนโลยีสารสนเทศ (Security Monitoring) โดยมีรายละเอียดดังนี้

4.2.1 ต้องมีศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามระบบเทคโนโลยีสารสนเทศ (Security Operations Center : SOC) จัดตั้งอยู่ในประเทศไทย ที่มีระบบบริหารจัดการความปลอดภัยสารสนเทศ (Information Security Management Service : ISMS) ที่ได้รับมาตรฐาน ISO27001:2013 เพื่อให้บริการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log File) และเฝ้าระวังความปลอดภัยเทคโนโลยีสารสนเทศ (Security Monitoring) ให้กับระบบและอุปกรณ์ต่างๆ ตามที่ รฟม. กำหนดตามตารางในข้อ 4.1

4.2.2 ต้องสามารถทำการเก็บรวบรวม Log File (Collection) ได้ถูกต้องตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ฉบับที่มีผลบังคับใช้

4.2.3 สามารถทำการคัดกรองเฉพาะ Log File ที่มีความสำคัญ (Filtering) การรวบรวม Log File จากอุปกรณ์หลายประเภท (Aggregation) โดยการจัดเก็บ Log File ให้อยู่ในรูปแบบเดียวกัน (Normalization) การจัดลำดับความสำคัญของเหตุการณ์ที่ตรวจพบจาก Log File (Prioritization) และทำการวิเคราะห์เพื่อหาสาเหตุของเหตุการณ์ที่เกิดขึ้น (Correlation) จาก Event Log ได้แบบ Real-time

4.2.4 ต้องทำการวิเคราะห์เหตุการณ์ และแสดงผลแบบ Real Time เพื่อบอกลำดับเหตุการณ์ต่างๆ ที่เกี่ยวกับความปลอดภัย (Incidents) โดยสามารถจำแนกระดับของความรุนแรง (Severity) และความสำคัญ (Priority) ของเหตุการณ์ความเสี่ยงที่เกิดขึ้นได้ 5 ระดับ เป็นอย่างน้อย

4.2.5 ต้องจัดเก็บรายละเอียดและกำหนดระดับความสำคัญของอุปกรณ์แต่ละรายการตามข้อ 4.1 โดยใช้เกณฑ์การจัดลำดับความสำคัญที่สอดคล้องกับผลกระทบทางธุรกิจ (Business Assets Value หรือค่า Confidentiality – Integrity – Availability : C-I-A)

4.2.6 ต้องทำการป้องกันการเปลี่ยนแปลงข้อมูลและทำการเข้ารหัสข้อมูล (Encryption) เพื่อป้องกันและรักษาความปลอดภัยของข้อมูล Log File

4.2.7 ต้องทำการแจ้งเตือนเจ้าหน้าที่ รฟม. ในทันที เมื่อมีเหตุการณ์เสี่ยงภัยหรือเหตุการณ์การบุกรุกระบบที่มีระดับความสำคัญหรือความรุนแรงสูง ผ่านทางโทรศัพท์ หรือ E-Mail

4.2.8 ต้องมีทีม CSIRT (Computer Security Incident Response Team) พร้อมที่จะปฏิบัติหน้าที่ในการตอบสนองต่อเหตุการณ์การบุกรุกระบบได้จำนวนอย่างน้อย 4 ครั้ง โดยเมื่อเกิดเหตุการณ์การบุกรุกระบบเครือข่ายคอมพิวเตอร์ของ รฟม. และ/หรือ รฟม. ต้องการความช่วยเหลือผู้รับจ้างต้องเข้าดำเนินการ ณ สถานที่ของ รฟม. ภายใน 4 ชั่วโมง นับตั้งแต่ รฟม. ได้แจ้งให้ผู้รับจ้างทราบทางโทรศัพท์ โทรศัพท์เคลื่อนที่ โทรสาร หรือ E-Mail รวมถึงช่องทางการสื่อสารอื่นๆ ตามที่ รฟม. กำหนดได้ทุกวัน ไม่เว้นวันหยุด

4.2.9 ผู้รับจ้างต้องจัดให้มีเจ้าหน้าที่ทำหน้าที่ในการประสานงาน (Helpdesk Support) ให้กับเจ้าหน้าที่ รฟม. ตลอด 24 ชั่วโมง

4.2.10 ผู้รับจ้างต้องจัดทำรายงานประจำเดือน เพื่อรายงานการเฝ้าระวังความปลอดภัยเทคโนโลยีสารสนเทศ (Security Monitoring) โดยมีรายละเอียดที่ต้องจัดส่งให้ รฟม. ดังต่อไปนี้

- สรุปจำนวนเหตุการณ์ผิดปกติที่เกิดขึ้นทั้งหมด
- สรุปจำนวนเหตุการณ์ที่เป็น Critical

/- สรุปจำนวน...

- สรุปจำนวนเหตุการณ์ทั้งหมดที่คุกคามระบบ โดยจำแนกตามสถานะ ความเร่งด่วน (Critical, High, Medium, Low, Very Low)
- สรุปจำนวนเหตุการณ์ที่เกิดขึ้นในแต่ละวัน โดยจำแนกตามสถานะความเร่งด่วน (Critical, High, Medium, Low, Very Low)
- สรุป Signature ที่เป็นสาเหตุในการเกิดเหตุการณ์ผิดปกติ ที่เกิดขึ้นมากที่สุด 10 อันดับ
- สรุปรายการอุปกรณ์ของ รฟม. ที่เฝ้าระวังภัยคุกคาม
- สรุปจำนวน Ticket ที่เกิดขึ้นในรอบเดือน โดยจำแนกตามสถานะของ Ticket
- สรุปรายละเอียดการทำงาน การวิเคราะห์เหตุการณ์ ของแต่ละ Ticket
- สรุปการเรียกใช้ทีม CSIRT (ถ้ามี)
- สรุปเหตุการณ์ที่เกิดขึ้นมากที่สุด 10 อันดับแรก จำแนกตามหัวข้อต่างๆ เช่น Rule Name, Source IP Address, Source Port, Target IP Address, Target Port

ทั้งนี้ ต้องจัดส่งรายงานดังกล่าวเป็น PDF File ให้กับ รฟม. ทาง E-Mail และจัดทำรายงานสรุปเป็นเอกสารสีนำเสนอต่อคณะกรรมการตรวจรับพัสดุ รฟม. เป็นประจำทุกเดือน โดยจัดส่งภายในวันที่ 15 ของเดือนถัดไป

4.3 ผู้รับจ้างต้องมีระบบแสดงสถานะการให้บริการผ่านทาง Web Portal โดยมีข้อมูลสถานะของการเปิดและปิด Tickets และสถานะของ Incidents ที่เกิดขึ้นได้

4.4 ผู้รับจ้างต้องทำการทดสอบการเจาะระบบ (Penetration Testing และ Re-Penetration Testing) ตามที่ รฟม. กำหนด โดยมีจำนวน IP Address ที่ใช้ทดสอบไม่น้อยกว่า 20 IP Address เพื่อนำรายละเอียดของช่องโหว่จากการทดสอบระบบงานดังกล่าวมาประกอบการวิเคราะห์เหตุการณ์บุกรุก รวมถึงผลกระทบในการเฝ้าระวังความปลอดภัย พร้อมทั้งให้คำแนะนำในการปิดช่องโหว่ที่ตรวจพบ โดยจัดทำรายงานเป็นเอกสารสีจำนวน 2 ชุด และไฟล์เอกสารโดยจัดเก็บลงใน Flash Drive แบบ USB จำนวน 3 ชุด ส่งให้กับคณะกรรมการตรวจรับพัสดุภายใน 30 วัน หลังจากดำเนินการแล้วเสร็จ ภายในระยะเวลาที่ใช้บริการตามสัญญา

4.5 ผู้รับจ้างต้องจัดหาซอฟต์แวร์สำหรับตรวจสอบช่องโหว่ (Vulnerability Assessment) และตรวจสอบการปฏิบัติตามข้อกฎหมาย ระเบียบ ข้อบังคับ หรือมาตรฐานสากลต่าง ๆ (Compliance Assessment) ของ รฟม. พร้อมสิทธิการใช้งานจำนวน 1 สิทธิ โดยต้องเป็นโปรแกรมที่ได้รับความนิยมในการนำมาใช้งานโดยต้องมีคุณลักษณะอย่างน้อยหรือดีกว่า ดังต่อไปนี้

4.5.1 เป็นโปรแกรมในลักษณะของ Commercial ware

4.5.2 สามารถตรวจสอบช่องโหวครอบคลุม ดังนี้

- ช่องโหว่จากข้อบกพร่องของโปรแกรม (Software Flaws)
- ช่องโหว่ที่อาจทำให้เกิดการบุกรุกจาก Malware และ Botnets
- ช่องโหว่จากการกำหนดค่าต่าง ๆ (Configuration)
- ช่องโหว่ของเครื่องแม่ข่ายที่เป็น Physical, Virtual และ Cloud

4.5.3 มีความสามารถในการตรวจสอบช่องโหว่ ดังนี้

- Operating Systems
- Network Devices
- Web Servers

/- Hypervisors...

- Hypervisors
- Databases
- Threats & Compliance Violations

4.5.4 สามารถสแกนหาช่องโหว่ได้ทั้ง IPv4 IPv6 หรือ Hybrid Networks

4.5.5 สามารถย้ายสิทธิการใช้งานระหว่างเครื่องคอมพิวเตอร์ได้

4.5.6 สามารถตรวจสอบการปฏิบัติตามข้อกฎหมาย ระเบียบ ข้อบังคับ หรือ มาตรฐานสากลต่างๆ (Compliance Assessment) ของ รฟม. ได้

4.5.7 สามารถจัดลำดับความรุนแรง (Severity) ของช่องโหว่ได้

4.5.8 สามารถให้คำแนะนำหรือแนวทางการปิดช่องโหว่ได้ (Hardening)

4.5.9 สามารถตรวจสอบช่องโหว่ได้โดยไม่จำกัดจำนวนหมายเลขไอพีและสามารถตรวจสอบช่องโหว่พร้อมกันได้ครั้งละไม่น้อยกว่า 128 IP Address

4.5.10 สามารถออกรายงานสรุปผลการตรวจสอบช่องโหว่ได้ ดังนี้

- สามารถใส่ตราสัญลักษณ์ของ รฟม. ในรายงานได้
- สามารถออกรายงานในรูปแบบของ XML PDF HTML และ CSV ได้
- สามารถส่งรายงานผลการตรวจสอบช่องโหว่แก่ผู้ที่เกี่ยวข้องผ่านทางระบบอีเมลได้

5. บริการพื้นที่ศูนย์คอมพิวเตอร์สำรอง (DR-Site) มีรายละเอียดดังนี้

ผู้รับจ้างต้องมีสถานที่เพื่อให้ รฟม. ใช้จัดตั้งเป็นศูนย์คอมพิวเตอร์สำรอง (DR-Site) โดยเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์กับ ศูนย์คอมพิวเตอร์หลัก ฝ่ายเทคโนโลยีสารสนเทศ รฟม. ตลอดระยะเวลาที่ใช้บริการ โดยมีคุณสมบัติดังนี้

5.1 ต้องมีทำเลที่ตั้งของตัวอาคารที่ใช้เป็นศูนย์คอมพิวเตอร์สำรองของ รฟม. ที่ได้ตามมาตรฐาน อยู่ในทำเลที่เหมาะสม ไม่อยู่ใกล้พื้นที่เสี่ยงต่อการชุมนุมประท้วง เช่น สถานทูต สถานที่ราชการ ที่ทำการพรรคการเมือง หรือไม่ควรอยู่ใกล้พื้นที่ๆ มีความเสี่ยงด้านภัยพิบัติทางธรรมชาติ เช่น น้ำท่วม หรือระบบสาธารณูปโภค และระบบสื่อสารข้อมูลขัดข้องบ่อยครั้ง รวมทั้งตัวอาคารไม่มีประวัติการเกิดเพลิงไหม้หรือมีการก่อวินาศกรรมบ่อยครั้ง

5.2 ต้องมีศูนย์คอมพิวเตอร์สำรอง (DR-Site) โดยมีระยะห่างจาก รฟม. (เลขที่ 175 ถนนพระรามเก้า แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร) เป็นระยะทางไม่น้อยกว่า 15 กิโลเมตร และสามารถเดินทางสะดวก เข้าถึงได้จากถนนสายหลัก

5.3 ต้องมีพื้นที่จอดรถให้กับเจ้าหน้าที่ รฟม. ไม่น้อยกว่า 10 คัน โดยไม่มีค่าใช้จ่าย ค่าที่จอดรถตลอดระยะเวลาที่ใช้บริการ

5.4 ต้องมีเจ้าหน้าที่รักษาความปลอดภัยภายในอาคาร พร้อมติดตั้งกล้องวงจรปิดที่มีการทำงานตลอด 24 ชั่วโมง

5.5 ต้องมีศูนย์ Data Center ด้าน Co-Location ที่ผ่านการรับรองมาตรฐาน Tier 3 และได้รับมาตรฐาน ISO 27001:2013

5.6 ต้องมีบริการ Co-Location ให้ รฟม. ติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย (Server) พร้อมอุปกรณ์ต่อพ่วงต่างๆ ภายในตู้ Rack ที่มีพื้นที่ในการติดตั้งอุปกรณ์ไม่น้อยกว่า 42U และมีวงจรสื่อสารความเร็วสูงผ่านโครงข่าย

/ใยแก้ว...

ใยแก้วนำแสง (Fiber Optic) ความเร็วไม่น้อยกว่า 1 Gbps เพื่อเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์กับศูนย์คอมพิวเตอร์หลัก รฟม. โดยผู้รับจ้างต้องมีเจ้าหน้าที่ให้ความช่วยเหลือและสนับสนุน ในกรณีที่ รฟม. มีการติดตั้งอุปกรณ์

5.7 ผู้รับจ้างต้องมีอุปกรณ์ Appliance Firewall เพื่อใช้ป้องกันให้กับเครื่องคอมพิวเตอร์แม่ข่าย (Server) และอุปกรณ์ต่อพ่วงต่างๆ ของ รฟม. ตลอดระยะเวลาที่ใช้บริการ โดยคุณสมบัติดังต่อไปนี้

- มี Interface Port แบบ RJ45 จำนวนไม่น้อยกว่า 12 Ports
- มี Interface Port แบบ RJ45 รองรับการเชื่อมต่อ DMZ/HA จำนวนไม่น้อยกว่า 2 Ports
- รองรับ Firewall Throughput รวม ไม่น้อยกว่า 4 Gbps
- รองรับ SSL VPN Throughput ไม่น้อยกว่า 200 Mbps
- รองรับ Concurrent SSL ไม่น้อยกว่า 200 Users
- รองรับ Intrusion Protection System (IPS) Throughput ไม่น้อยกว่า 450 Mbps

5.8 ต้องมีเจ้าหน้าที่ Network Operation Center (NOC) คอยเฝ้าระวังอยู่ตลอด 24 ชั่วโมง เพื่อคอยให้บริการลูกค้า เช่น การ Reboot เครื่องคอมพิวเตอร์แม่ข่าย (Server) การเปลี่ยนใส่เทปเพื่อการสำรองข้อมูลประจำวัน การปิดเปิดอุปกรณ์ต่างๆ หรือช่วยตรวจดูไฟสถานะต่างๆ ของอุปกรณ์ภายในตู้อุปกรณ์ เป็นต้น

5.9 ต้องมีสำนักงานชั่วคราวภายในศูนย์คอมพิวเตอร์สำรอง โดยมีคุณสมบัติอย่างน้อย ดังนี้

5.9.1 เป็นสำนักงานชั่วคราวที่ รฟม. สามารถใช้งานได้ไม่น้อยกว่า 30 วัน

5.9.2 ต้องมีระบบเครือข่าย LAN เชื่อมต่อแบบ Gigabit Ethernet Port 10/100/1000 จำนวนไม่น้อยกว่า 8 พอร์ต และระบบเครือข่าย Wi-Fi ที่เชื่อมต่อกับเครื่องคอมพิวเตอร์แม่ข่าย (Server) และอุปกรณ์คอมพิวเตอร์ของ รฟม. ภายในศูนย์ Data Center ได้ รวมทั้งต้องสามารถใช้งานอินเทอร์เน็ตได้

5.9.3 ต้องมีอุปกรณ์สำนักงานที่สามารถรองรับผู้ใช้งานได้จำนวนอย่างน้อย 20 คน ซึ่งประกอบด้วยอุปกรณ์ ดังนี้

5.9.3.1 เครื่องคอมพิวเตอร์โน้ตบุ๊ก จำนวนอย่างน้อย 12 เครื่อง

5.9.3.2 เครื่องมัลติฟังก์ชัน (Copy/Scanner) จำนวนอย่างน้อย 2 เครื่อง

5.9.3.3 โทรศัพท์ จำนวนอย่างน้อย 2 คู่สาย

5.9.3.4 อุปกรณ์โปรเจคเตอร์ จำนวนอย่างน้อย 1 ชุด

5.9.3.5 อุปกรณ์เครือข่ายอื่นๆ ที่จำเป็น ได้แก่ อุปกรณ์ Layer 2 Switch ที่มี Port แบบ Gigabit Ethernet 10/100/1000 จำนวนไม่น้อยกว่า 24 Ports พร้อมสายสัญญาณ UTP และอุปกรณ์ต่อพ่วงไฟฟ้า เป็นต้น

/ภาคผนวก...

ภาคผนวก ข

การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
MASS RAPID TRANSIT AUTHORITY OF THAILAND
รัฐวิสาหกิจภายใต้กำกับของรัฐมนตรีว่าการกระทรวงคมนาคม
A STATE ENTERPRISE UNDER SUPERVISION OF MINISTER OF TRANSPORT

ประกาศการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (ฉบับปรับปรุงครั้งที่ 10)

ด้วยพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 มาตรา 5 กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ จึงส่งผลให้ระบบเทคโนโลยีสารสนเทศของการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย (รฟม.) ต้องมีการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศอย่างครบถ้วนเพื่อธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (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 มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาและลดผลกระทบจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องหรือจากการถูกคุกคามจากภัยต่าง ๆ จึงได้กำหนดนโยบายเพื่อควบคุมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ดังนี้

1.1 การเข้าถึงหรือควบคุมการใช้งานสารสนเทศครอบคลุม 4 ด้าน คือ

1.1.1 การเข้าถึงระบบสารสนเทศ (Access Control) ต้องตรวจสอบการอนุมัติสิทธิ์การเข้าถึงระบบและกำหนดรหัสผ่าน การลงทะเบียนผู้ใช้งานเพื่อให้ผู้ใช้ที่มีสิทธิ์ (User Authentication) เท่านั้นที่สามารถ

/เข้าถึง ...

เข้าถึงระบบได้ รวมถึงมีการเก็บบันทึกข้อมูลการเข้าถึงระบบ (Access Log) และข้อมูลจราจรทางคอมพิวเตอร์ ทั้งนี้ การให้สิทธิ์การใช้งานระบบสารสนเทศนั้นต้องให้สิทธิ์อย่างเหมาะสมและเพียงพอ (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) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยกำหนดให้มีการยืนยันตัวตนเพื่อระบุถึงตัวตนของผู้ใช้งาน รวมทั้งกำหนดให้มีการจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น

1.1.4 การเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control) ต้องกำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศ โดยให้สิทธิ์เฉพาะระบบงานสารสนเทศที่ต้องปฏิบัติตามหน้าที่เท่านั้น รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานระบบสารสนเทศอย่างสม่ำเสมอ

1.2 มีระบบสารสนเทศและระบบสำรองที่อยู่ในสภาพพร้อมใช้งาน รวมทั้งมีแผนเตรียมพร้อมในกรณีฉุกเฉินหรือกรณีที่ไม่สามารถดำเนินการตามวิธีการทางอิเล็กทรอนิกส์ได้ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

1.3 ตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศอย่างสม่ำเสมอ

2. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รฟม.

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รฟม. ใช้แนวทางและกระบวนการอ้างอิงตาม 1) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานรัฐ พ.ศ. 2553 2) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555 และ 3) มาตรฐาน ISO/IEC 27001:2013 โดยแบ่งแนวปฏิบัติออกเป็น 15 ส่วนตามเอกสารแนบท้ายประกาศดังต่อไปนี้

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 รฟม. (ส่วนที่ 9)

/2.10 การใช้งาน

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)

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศตามข้อ 2. จัดเป็นมาตรฐานด้านความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. ซึ่งพนักงานและลูกจ้างของ รฟม. รวมทั้งหน่วยงานภายนอกที่เกี่ยวข้องจะต้องปฏิบัติตามอย่างเคร่งครัด

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

นโยบายนี้ให้ใช้บังคับเมื่อพ้นกำหนด 7 วัน นับแต่วันที่ผู้มีอำนาจลงนาม

ประกาศ ณ วันที่ 7 กันยายน พ.ศ. 2564

(นายภคพงศ์ ศิริกันทรมาศ)
ผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

เอกสารแนบท้ายประกาศ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ของ รฟม.

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

1. รฟม. หมายถึง การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
2. ฝทท. หมายถึง ฝ่ายเทคโนโลยีสารสนเทศ
3. ผู้บริหารระดับสูงสุด หมายถึง ผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
4. ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของ รฟม.
5. ผู้ใช้งาน หมายถึง บุคคลที่ได้รับอนุญาตให้สามารถเข้าใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. ดังนี้
   - พนักงาน ลูกจ้าง ของ รฟม.
   - บุคคลภายนอกที่ รฟม. อนุญาตให้เข้ามาใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. ได้ชั่วคราว เพื่อประโยชน์ในการดำเนินการของ รฟม. ได้แก่ พนักงานหรือลูกจ้างบริษัทภายนอกที่เข้ามาติดตั้งหรือดูแลรักษาระบบให้กับ รฟม. หรือที่ปรึกษา หรือผู้ปฏิบัติงานตามสัญญา หรือนิสิตนักศึกษาฝึกงาน
6. หน่วยงานภายนอก หมายถึง องค์กร ซึ่ง รฟม. อนุญาตให้มีสิทธิ์ในการเข้าถึง หรือใช้ข้อมูล หรือสินทรัพย์ต่าง ๆ ของ รฟม. โดยจะได้รับสิทธิ์ในการใช้ระบบตามประเภทงานตามอำนาจและต้องรับผิดชอบในการรักษาความลับของข้อมูล
7. ผู้ดูแลระบบ หมายถึง พนักงานที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบสารสนเทศ
8. เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
9. มาตรฐาน หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย
10. ขั้นตอนปฏิบัติ หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานตามที่ได้กำหนดไว้ตามวัตถุประสงค์
11. แนวปฏิบัติ หมายถึง แนวทางที่ต้องปฏิบัติตามเพื่อให้สามารถบรรลุวัตถุประสงค์หรือเป้าหมายได้ง่ายขึ้น
12. ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงานของ รฟม. ที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายสื่อสารข้อมูลมาช่วยในการสร้างสารสนเทศที่ รฟม. สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุน การให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ ได้แก่ ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลและสารสนเทศ เป็นต้น
13. ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด ที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

14. ข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Log) หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เวลา วันที่ ปริมาณ ระยะเวลา หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น
15. สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งข้อมูลอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิกให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ
16. ระบบคอมพิวเตอร์ (Computer System) หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่งหรือสิ่งอื่นใด และแนวปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
17. ระบบเครือข่ายสื่อสารข้อมูล (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของ รฟม. เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น
18. สิทธิ์ของผู้ใช้งาน หมายถึง สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิพิเศษ และสิทธิ์อื่นใด ที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน
19. ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)
20. เหตุการณ์ด้านความมั่นคงปลอดภัย หมายถึง เหตุการณ์ที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย มาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
21. สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม
22. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้
23. สินทรัพย์ (Assets) หมายถึง สินทรัพย์ด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารของ รฟม. เช่น อุปกรณ์คอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีค่าลิขสิทธิ์ ข้อมูล ระบบข้อมูล ฯลฯ
24. จดหมายอิเล็กทรอนิกส์ (e-mail) หมายถึง ระบบที่บุคคลใช้ในการรับ - ส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหวและเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ โดยข่าวสารที่ส่งนั้นจะถูกเก็บไว้ในตู้จดหมาย (Mail Box) ที่กำหนดไว้สำหรับผู้ใช้งาน ผู้รับสามารถเปิดอ่าน พิมพ์ลงกระดาษ หรือจะลบทิ้งก็ได้

25. ชุดคำสั่งไม่พึงประสงค์ (Malicious Code) หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
26. เครื่องคอมพิวเตอร์ หมายถึง เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ และเครื่องคอมพิวเตอร์แบบพกพา
27. อุปกรณ์เคลื่อนที่ (Mobile Device) หมายถึง อุปกรณ์พกพาที่ทำงานได้เหมือนกับเครื่องคอมพิวเตอร์ เช่น Tablet, Smart Phone

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 แผนการอบรมทางด้านความมั่นคงปลอดภัยประจำปีซึ่งรวมถึงการสร้างความตระหนัก
   1.9 ผลการทดสอบแผนกู้คืนในปีที่ผ่านมา
   1.10 ข้อมูลภัยคุกคามต่าง ๆ ที่เคยเกิดขึ้นในอดีตและปัจจุบัน รวมทั้งภัยคุกคามที่ได้รับแจ้งจากหน่วยงานภายนอก
   1.11 ผลการตรวจสอบการปฏิบัติตามนโยบายความมั่นคงปลอดภัยโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก
2. จัดให้มีทรัพยากรด้านบุคลากร งบประมาณ การบริหารจัดการ และวัตถุดิบที่เพียงพอต่อการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศในแต่ละปีงบประมาณ
3. จัดให้มีบุคลากรดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศและกำหนดหน้าที่ความรับผิดชอบรวมทั้งปรับปรุงโครงสร้างดังกล่าวตามความจำเป็น
4. แสดงเจตนารมณ์หรือสื่อสารอย่างสม่ำเสมอเพื่อให้ผู้ใช้งานทั้งหมดได้เห็นถึงความสำคัญของการปฏิบัติตามนโยบายความมั่นคงปลอดภัยและนโยบายสนับสนุนต่าง ๆ โดยเคร่งครัดและเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับสารสนเทศขององค์กร รวมถึงสร้างความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

ส่วนที่ 2
ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร

วัตถุประสงค์

☐ เพื่อให้ผู้ใช้งานเข้าใจถึงบทบาท หน้าที่ความรับผิดชอบ ทั้งก่อนการจ้างงาน ระหว่างการจ้างงาน และสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน ตลอดจนตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศเพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง การใช้งานระบบเทคโนโลยีสารสนเทศผิดวัตถุประสงค์และความผิดพลาดในการปฏิบัติหน้าที่ ซึ่งอาจส่งผลกระทบหรือทำให้ รฟม. 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 รฟม. ไปใช้ในทางที่ไม่เหมาะสม รวมทั้งเพื่อให้ผู้ใช้งานเข้าใจในหน้าที่ความรับผิดชอบของตนเอง

   1.1 การตรวจสอบคุณสมบัติของผู้สมัคร (Screening)

   ฝ่ายทรัพยากรบุคคล หรือฝ่าย/สำนัก ที่กำกับดูแลงานที่มีการว่าจ้างหน่วยงานภายนอกต้องตรวจสอบคุณสมบัติของผู้สมัคร (ทั้งกรณีการจ้างเป็นพนักงาน ลูกจ้าง การว่าจ้างหน่วยงานภายนอกเพื่อปฏิบัติงานให้ รฟม. รวมทั้งนิสิตนักศึกษาฝึกงาน) โดยผู้สมัครต้องไม่เคยกระทำผิดกฎหมาย ระเบียบ ข้อบังคับ หรือจริยธรรม รวมทั้งไม่มีประวัติในการบุกรุก แก้ไข ทำลาย หรือโจรกรรมข้อมูลในระบบเทคโนโลยีสารสนเทศมาก่อน และมีคุณสมบัติตามที่ รฟม. กำหนด

   1.2 การกำหนดเงื่อนไขการจ้างงาน (Terms and conditions of employment) การว่าจ้างให้มีเงื่อนไขการจ้างงานให้ครอบคลุมในเรื่องดังต่อไปนี้

      1.2.1 กำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศอย่างเป็นลายลักษณ์อักษร (Information security roles and responsibilities) แก่ผู้ใช้งาน โดยกำหนดให้สอดคล้องกับนโยบายความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของ รฟม.

      1.2.2 กำหนดให้มีการลงนามในสัญญาว่าจะไม่เปิดเผยความลับของ รฟม. (Non-Disclosure Agreement : NDA)

      1.2.3 ระบบเทคโนโลยีสารสนเทศที่สร้างหรือพัฒนาโดยผู้ใช้งานในระหว่างการว่าจ้างถือเป็นสินทรัพย์ของ รฟม.

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 ไวรัสคอมพิวเตอร์ เทคนิคการหลอกล่อทางจิตวิทยา (Social Engineering) และช่องโหว่ทางเทคนิค เป็นต้น

2.2.2 ฝทท. ต้องดำเนินการฝึกอบรม หรือประชาสัมพันธ์เพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศแก่ผู้ใช้งานเป็นประจำทุกปี

2.2.3 ฝทท. 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 ฝทท. จะเพิกถอนสิทธิ์การใช้งานและอาจเป็นความผิดทางวินัย หรือความผิดตามกฎหมายที่เกี่ยวข้อง

1) พนักงาน/ลูกจ้างที่ฝ่าฝืนหรือละเมิดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รฟม. ต้องถูกลงโทษตามกระบวนการทางวินัยของ รฟม. รวมถึงกฎหมายที่เกี่ยวข้อง

2) หน่วยงานภายนอกที่กระทำความผิด จะมีโทษตามที่ระบุไว้ในสัญญาหรือถูกเพิกถอนสิทธิ์การใช้งาน รวมถึงดำเนินการตามกฎหมายที่เกี่ยวข้อง

3. การสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน (Termination and change of employment)

เพื่อกำหนดหน้าที่ความรับผิดชอบเมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน ซึ่งรวมไปถึงการคืนทรัพย์สินและการถอดถอนสิทธิ์ในการเข้าถึง

3.1 การแจ้งการสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน

3.1.1 ฝ่ายทรัพยากรบุคคลต้องแจ้งให้ฝ่ายเทคโนโลยีสารสนเทศทราบทันทีหากพนักงานมีการลาออก โยกย้าย เกษียณ หรือเสียชีวิต เพื่อฝ่ายเทคโนโลยีสารสนเทศจะได้ตรวจสอบและบริหารจัดการสิทธิ์ในการเข้าถึงระบบเทคโนโลยีสารสนเทศ

3.1.2 ฝ่าย/สำนัก ที่กำกับดูแลงานที่มีการว่าจ้างหน่วยงานภายนอก ต้องแจ้งให้ฝ่ายเทคโนโลยีสารสนเทศทราบทันทีในกรณีที่ผู้รับจ้างภายนอกสิ้นสุดสัญญาจ้างหรือมีการยกเลิกสัญญาจ้าง เพื่อให้ ฝทท. ตรวจสอบการใช้งานระบบสารสนเทศและถอดถอนสิทธิ์ในการเข้าถึงระบบสารสนเทศของ รฟม.

3.2 การคืนสินทรัพย์ของ รฟม.

ผู้ดูแลระบบต้องตรวจสอบเพื่อเรียกคืนสินทรัพย์ของ รฟม. จากผู้ใช้งาน เมื่อการสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน

3.3 การถอดถอนสิทธิ์ในการเข้าถึง

3.3.1 ผู้ดูแลระบบต้องถอดถอนสิทธิ์ในการเข้าถึงของผู้ใช้งาน เมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน

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

3.3.3 ในกรณีที่ผู้ใช้งานที่สิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน มีการใช้บัญชีผู้ใช้งานร่วมกัน (Shared User ID) กับผู้ใช้งานอื่น ผู้บังคับบัญชาต้องเปลี่ยนรหัสผ่านทันทีหลังจากสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน

ส่วนที่ 3
การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

วัตถุประสงค์

☐ เพื่อควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าถึงอาคารสถานที่ และพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area)

ผู้รับผิดชอบ

☐ ผู้ดูแลระบบ

☐ ผู้อำนวยการฝ่ายจัดซื้อและบริการ

อ้างอิงมาตรฐาน

☐ หมวดที่ 7 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security)

แนวปฏิบัติ

1. ผู้ดูแลระบบ ต้องออกแบบ และติดตั้งอุปกรณ์หรือระบบสนับสนุน (Facilities) เพื่อป้องกันความมั่นคงปลอดภัยด้านกายภาพ เช่น อุปกรณ์ดับเพลิง ระบบสำรองไฟฟ้า เครื่องกำเนิดไฟฟ้า ระบบปรับอากาศและควบคุมความชื้น ระบบเตือนภัยน้ำรั่ว และต้องมีการบำรุงรักษาอย่างสม่ำเสมอ
2. ผู้ดูแลระบบต้องติดตั้งอุปกรณ์สารสนเทศในตู้แร็ก (Rack) หรือสถานที่ที่มีความมั่นคงปลอดภัยและมีการปิดล็อค
3. ผู้ดูแลระบบ ต้องมีการป้องกันสายเคเบิลที่ใช้เพื่อการสื่อสารหรือสายไฟ มิให้มีการดักรับสัญญาณ (Interception) หรือมีความเสียหายเกิดขึ้น โดยจะต้องเดินสายเคเบิลผ่านท่อร้อยสายหรือทางเดินสายที่มั่นคงปลอดภัยจากการเข้าถึง 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 กำหนดสิทธิ์ของผู้ใช้งานและหน่วยงานภายนอกในการเข้าถึงสถานที่ โดยแบ่งแยกได้ ดังนี้
      5.1.1 ผู้ดูแลระบบต้องกำหนดสิทธิ์แก่ผู้ใช้งานที่มีสิทธิ์เข้า - ออก และกำหนดช่วงระยะเวลาที่มีสิทธิ์ในการเข้า - ออกแต่ละพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศอย่างชัดเจน
      5.1.2 เจ้าหน้าที่รักษาความปลอดภัย (รปภ.) จะต้องให้หน่วยงานภายนอกหรือบุคคลภายนอกแลกบัตรที่สามารถระบุตัวตนของบุคคลนั้น ๆ ก่อนเข้าถึงอาคารของ รฟม. เช่น บัตรประจำตัวประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วบันทึกข้อมูลบัตรในสมุดบันทึกหรือระบบงานสารสนเทศ

5.1.3 หน่วยงานภายนอกที่มาติดต่อต้องติดบัตรผู้ติดต่อ (Visitor) ตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ใน รฟม. และคืนบัตรผู้ติดต่อ (Visitor) ก่อนออกจากอาคารของ รฟม.

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 รฟม. กำหนด

ส่วนที่ 4
การจัดการทรัพย์สิน

วัตถุประสงค์

☐ เพื่อบริหารจัดการทรัพย์สินสารสนเทศ ตั้งแต่การจัดหา 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 รฟม. อย่างระมัดระวัง และใช้เพื่อปฏิบัติงานของ รฟม. เท่านั้น รวมทั้งต้องปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ และนโยบาย ของ รฟม.
2. การจำแนกประเภทของทรัพย์สินสารสนเทศ (Asset classification)
   - 2.1 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจำแนกประเภททรัพย์สินตามขั้นตอนที่ รฟม. กำหนด และทบทวนการจำแนกดังกล่าวอย่างสม่ำเสมอ
   - 2.2 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจัดทำป้ายชื่อทรัพย์สินสารสนเทศ (Labeling) ให้ชัดเจน พร้อมทั้งจัดให้มีมาตรการดูแลการรักษาความมั่นคงปลอดภัยสารสนเทศที่สอดคล้องกับประเภททรัพย์สินตามระดับชั้นความลับที่ รฟม. กำหนด
3. การจัดการสื่อบันทึกข้อมูล (Media Handling)
   - 3.1 เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ใช้งานต้องควบคุมการใช้งานและจัดเก็บสื่อบันทึกแบบถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้ (Removable media) ตามที่ รฟม. กำหนด
   - 3.2 เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูล ตามขั้นตอนที่ รฟม. กำหนด โดยไม่สามารถกู้คืนข้อมูลกลับมาได้อีกก่อนจะกำจัดอุปกรณ์ดังกล่าวหรือ

ก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลที่สำคัญได้ 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 รวมถึงป้องกันสื่อบันทึกข้อมูลไม่ให้ได้รับความเสียหาย โดยรักษาความปลอดภัยสารสนเทศตามขั้นตอนที่ รฟม. กำหนด

ส่วนที่ 5

การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

วัตถุประสงค์

☐ เพื่อควบคุมการจัดหา พัฒนา และบำรุงรักษาระบบสารสนเทศ ให้มีการกำหนดมาตรการการรักษาความมั่นคงปลอดภัย เพื่อป้องกันความผิดพลาด สูญหาย และการเปลี่ยนแปลงแก้ไขระบบ

ผู้รับผิดชอบ

☐ ผู้บังคับบัญชา

☐ ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

☐ หมวดที่ 10 โครงสร้างการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (System acquisition, development and maintenance)

☐ หมวดที่ 11 ความสัมพันธ์กับหน่วยงานภายนอก (Supplier Relationships)

แนวปฏิบัติ

1. ผู้บังคับบัญชา ต้องควบคุมให้มีการกำหนดข้อตกลงและความรับผิดชอบที่เกี่ยวข้องกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศลงในสัญญากับผู้ให้บริการภายนอก โดยให้ครอบคลุมรวมถึงผู้รับจ้างช่วงด้วย
2. ผู้ดูแลระบบ ต้องจัดทำข้อกำหนดโดยระบุถึงการควบคุมความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร เช่น วิธีการแบบปลอดภัยในการพัฒนาโปรแกรมตามมาตรฐาน OWASP (Open Web Application Security Project) Top 10 หรือมาตรฐาน CWE (Common Weakness Enumeration) Top 25 หรือมาตรฐานที่ยอมรับในสากลหรือกำหนดซอฟต์แวร์ให้เป็นเวอร์ชันล่าสุดที่ได้รับการอัปเดตแล้ว
3. ผู้ดูแลระบบ ต้องมีการออกแบบระบบเพื่อตรวจสอบข้อมูลที่จะรับเข้าสู่แอปพลิเคชัน ข้อมูลที่เกิดจากการประมวลผล และข้อมูลที่อยู่ระหว่างการประมวลผล เพื่อตรวจหาและป้องกันความไม่ถูกต้องที่เกิดขึ้นกับข้อมูล เช่น หน่วยความจำล้น (Buffer overflows) การใช้ตัวแปรผิดประเภท และต้องมีมาตรการป้องกันหรือควบคุมความล้มเหลวระหว่างการประมวลผล (Rollback)
4. ผู้ดูแลระบบต้องมีการควบคุมการเข้าถึงและควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบตามขั้นตอนที่ รฟม. กำหนด เพื่อควบคุมผลกระทบที่เกิดขึ้น
5. ผู้ดูแลระบบต้องจำกัดให้มีการเปลี่ยนแปลงใด ๆ ต่อซอฟต์แวร์ที่ใช้งาน (Software Package) โดยเปลี่ยนแปลงเฉพาะที่จำเป็นเท่านั้น และควบคุมทุก ๆ การเปลี่ยนแปลงอย่างเข้มงวดตามขั้นตอนที่ รฟม. กำหนด
6. ผู้ดูแลระบบต้องจำกัดการเข้าถึง Sourcecode ให้เข้าถึงได้เฉพาะผู้ที่มีสิทธิ์เท่านั้น
7. ผู้ดูแลระบบต้องควบคุมข้อมูลที่นำมาใช้ในการทดสอบระบบ (Test Data) อย่างเหมาะสม โดยไม่นำข้อมูลจริงมาทดสอบ กรณีจำเป็นต้องใช้ข้อมูลจริงต้องได้รับอนุญาตข้อมูลจากเจ้าของก่อนนำมาใช้งาน และทำลายข้อมูลอย่างเหมาะสมตามขั้นตอนที่ รฟม. กำหนด

8. ผู้ดูแลระบบต้องแยกระบบสารสนเทศสำหรับการพัฒนา ทดสอบ และใช้งานจริงออกจากกันเพื่อลดความเสี่ยงที่เกิดจากการเปลี่ยนแปลงระบบสารสนเทศโดยไม่ได้รับอนุญาต และต้องมีการกำหนดสิทธิ์การเข้าถึงระบบสารสนเทศที่พัฒนา ทดสอบ หรือใช้งานจริง ทั้งระบบสารสนเทศใหม่ และการปรับปรุงแก้ไขระบบสารสนเทศเดิม
9. ผู้ดูแลระบบต้องมีการกำหนดขั้นตอนการทดสอบระบบสารสนเทศก่อนนำไปใช้งานจริง ทั้งในกรณีปรับปรุงระบบสารสนเทศเดิมและการพัฒนาระบบสารสนเทศใหม่
10. ผู้ดูแลระบบต้องติดตั้งซอฟต์แวร์บนระบบสารสนเทศที่ให้บริการ (Production) ตามขั้นตอนที่ รฟม. กำหนด และจำกัดสิทธิ์การติดตั้งซอฟต์แวร์เพื่อให้ระบบสารสนเทศต่าง ๆ มีความถูกต้องครบถ้วนและน่าเชื่อถือ
11. ผู้ดูแลระบบต้องนำซอฟต์แวร์ที่ไม่ละเมิดลิขสิทธิ์มาติดตั้งบนระบบสารสนเทศที่ให้บริการ (Production)
12. ผู้ดูแลระบบต้องกำกับดูแลให้ผู้รับจ้างปฏิบัติตามสัญญาหรือข้อตกลงการให้บริการที่ระบุไว้ โดยครอบคลุมถึงด้านความมั่นคงปลอดภัยสารสนเทศ และการปฏิบัติตามขั้นตอนที่เกี่ยวข้องต่าง ๆ ที่ รฟม. กำหนดไว้
13. ผู้ดูแลระบบ ต้องติดตาม ตรวจสอบรายงาน หรือบันทึกการให้บริการของบุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามสัญญาว่าจ้างอย่างสม่ำเสมอ
14. ผู้ดูแลระบบ ต้องดูแลให้ทรัพย์สินสารสนเทศได้รับการบำรุงรักษาและซ่อมแซมตามความต้องการ รวมทั้งต้องมีการบันทึกประวัติการทำงานผิดปกติ การบำรุงรักษา และการซ่อมแซมอุปกรณ์นั้น ๆ อย่างสม่ำเสมอ

ส่วนที่ 6
การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

☐ เพื่อควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศตั้งแต่การกำหนดสิทธิ์ กำหนดประเภทของข้อมูล จัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ระดับชั้นการเข้าถึง เวลาที่เข้าถึงได้ และช่องทางการเข้าถึง ทั้งนี้ เพื่อควบคุมและป้องกันการเข้าถึง การล่วงรู้ และการแก้ไขระบบสารสนเทศของ รฟม. 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 มีการแบ่งแยกหน้าที่ระหว่างการแจ้งความประสงค์การเข้าถึงและการอนุมัติการเข้าถึง เป็นต้น
   1.4 ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล
   เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ใช้งาน ต้องปฏิบัติ ดังนี้
   1.4.1 แบ่งประเภทข้อมูล ดังนี้
      1) ข้อมูลและสารสนเทศสำหรับสนับสนุนการตัดสินใจของผู้บริหาร ได้แก่ ข้อมูลสารสนเทศที่มีความสำคัญหรือมีความจำเป็นเร่งด่วนที่ต้องติดตามอย่างใกล้ชิดเพื่อประกอบการตัดสินใจเชิงนโยบาย กำหนดนโยบาย และการวางแผนของผู้บริหารระดับสูง
      2) ข้อมูลและสารสนเทศสนับสนุนเชิงยุทธศาสตร์ (Strategy Data) ได้แก่ ข้อมูลและสารสนเทศเชิงวิชาการเพื่อสนับสนุนการดำเนินงานตามพันธกิจและยุทธศาสตร์ของ รฟม. ให้บรรลุเป้าหมาย รวมทั้งข้อมูลที่เผยแพร่แก่ผู้รับบริการภายนอก

3) ข้อมูลและสารสนเทศที่สนับสนุนการปฏิบัติงานประจำ (Operation Data) ได้แก่ ข้อมูลที่สนับสนุนการทำงานทั่วไปของ รฟม.

1.4.2 จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น 3 ระดับ คือ

1) ข้อมูลที่มีระดับความสำคัญมาก หมายถึง ข้อมูลที่ใช้สำหรับสนับสนุนการตัดสินใจของผู้บริหาร

2) ข้อมูลที่มีระดับความสำคัญปานกลาง หมายถึง ข้อมูลที่ใช้ปฏิบัติงานเฉพาะกลุ่มงาน แผนก กอง หรือฝ่ายภายในองค์กร

3) ข้อมูลที่มีระดับความสำคัญน้อย หมายถึง ข้อมูลที่พนักงาน/ลูกจ้างภายใน รฟม. สามารถเข้าถึงร่วมกันได้หรือสามารถเผยแพร่ได้

1.4.3 จัดแบ่งลำดับชั้นความลับของข้อมูลตามที่ รฟม. กำหนด

1.4.4 จัดแบ่งระดับชั้นการเข้าถึง

1) ระดับชั้นสำหรับผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และภารกิจที่ได้รับมอบหมาย

2) ระดับชั้นสำหรับผู้ปฏิบัติงานทั่วไป เข้าถึงข้อมูลที่ได้รับมอบหมายตามอำนาจหน้าที่

3) ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย มีสิทธิ์ในการบริหารจัดการระบบและเข้าถึงข้อมูลที่ได้รับมอบหมายตามอำนาจหน้าที่

1.5 เจ้าของข้อมูลและผู้ดูแลระบบต้องกำหนดเวลาการเข้าถึงระบบสารสนเทศ

1.6 ผู้ดูแลระบบต้องจำกัดช่องทางการเข้าถึงระบบเทคโนโลยีสารสนเทศตามช่องทาง ดังนี้

1) เครือข่ายภายในของ รฟม.

2) เครือข่ายภายนอก รฟม.

3) เครือข่ายอื่นที่จัดไว้ให้ เช่น ระบบเครือข่ายสื่อสารข้อมูล GIN

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

1.8 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องพิจารณาข้อกำหนดต่าง ๆ ที่มีผลทางกฎหมายซึ่งเกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศของ รฟม. เช่น พระราชบัญญัติ ข้อกำหนดทางกฎหมาย ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่น ๆ เป็นต้น เพื่อกำหนดสิทธิ์การเข้าถึงสารสนเทศและระบบเทคโนโลยีสารสนเทศของ รฟม.

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 รฟม. ให้กำหนดชื่อผู้ใช้งาน (Username) ตามมาตรฐานจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ใช้ในองค์กร

2.1.2 เจ้าของข้อมูลต้องเป็นผู้อนุมัติการสร้างบัญชีผู้ใช้งานชั่วคราว (Temporary User) และต้องจำกัดช่วงเวลาการใช้งานเท่าที่จำเป็น

2.2 การบริหารจัดการรหัสผ่านผู้ใช้งาน (User Password Management)

2.2.1 ผู้ดูแลระบบกำหนดรหัสผ่านของผู้ใช้งานแบบชั่วคราวโดยใช้วิธีการสุ่ม และบังคับให้มีการเปลี่ยนรหัสผ่านเมื่อผู้ใช้งานเข้าใช้งานระบบในครั้งแรก

2.2.2 ผู้ดูแลระบบ ต้องกำหนดให้มีการเข้ารหัสข้อมูลรหัสผ่านในระบบ

2.2.3 ผู้ดูแลระบบ ต้องจัดให้มีการควบคุมรหัสผ่านอย่างเข้มงวด

2.2.4 ผู้ดูแลระบบต้องจัดส่งบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) แก่ผู้ใช้งานด้วยวิธีการที่ปลอดภัย

2.2.5 ผู้ดูแลระบบต้องควบคุมดูแลระบบปฏิบัติการ ฐานข้อมูล และระบบงานสารสนเทศ (Application) ที่จัดเก็บบัญชีผู้ใช้งานและรหัสผ่านอย่างเข้มงวด โดยให้เข้าถึงได้เฉพาะผู้ดูแลระบบที่ได้รับอนุญาตเท่านั้น

2.2.6 ผู้ดูแลระบบต้องกำหนดวิธีการหรือกระบวนการยืนยันตัวตนกรณีที่ลืมรหัสผ่าน

2.2.7 ผู้ใช้งาน ต้องใช้รหัสผ่านอย่างมั่นคงปลอดภัย ดังนี้

1) กำหนดรหัสผ่านต้องยาวอย่างน้อย 8 หลัก ซึ่งประกอบด้วย ตัวอักษร ตัวเลข และอักขระพิเศษ เช่น (a-Z) (0-9) (@ , # , & , “ , ‘ , *, =, < , > , % , $, + , ?) เป็นต้น

2) กำหนดรหัสผ่านที่ง่ายต่อการจดจำ แต่ต้องไม่เป็นคำที่สามารถคาดเดาได้ง่าย เช่น คำที่อยู่ในพจนานุกรม “qwerty” “abcde” “12345” ชื่อ-นามสกุล วันเดือนปีเกิด ที่อยู่หรือเบอร์โทรศัพท์ เป็นต้น

3) ต้องไม่ใช้งานรหัสผ่านโดยกระบวนการเข้าใช้งานโดยอัตโนมัติ ได้แก่ การกำหนดค่า “Remember Password” เป็นต้น

4) ต้องเก็บรหัสผ่านไว้เป็นความลับเฉพาะบุคคล ไม่เปิดเผยให้ผู้อื่นรับทราบ และผู้ใช้งานต้องไม่พิมพ์รหัสผ่านในลักษณะเปิดเผย เช่น พิมพ์รหัสผ่านต่อหน้าผู้ใช้งานคนอื่น เป็นต้น

5) ต้องไม่ใช้บัญชีชื่อผู้ใช้งานและรหัสผ่านร่วมกันกับผู้อื่น แม้ว่าบัญชีชื่อผู้ใช้งานจะได้รับการอนุญาตจากเจ้าของชื่อผู้ใช้งานบุคคลนั้นก็ตาม

6) ต้องเปลี่ยนแปลงรหัสผ่านเป็นประจำอย่างน้อยทุก 6 เดือน

7) ต้องเปลี่ยนแปลงรหัสผ่านเมื่อมีการแจ้งเตือนจากระบบ หรือสงสัยว่ารหัสผ่านล่วงรู้โดยบุคคลอื่น

2.3 การบริหารจัดการสิทธิ์ (Privilege Management)

2.3.1 ผู้บังคับบัญชาต้องกำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียน การเพิกถอนสิทธิ์ การเปลี่ยนแปลงสิทธิ์ และการทบทวนสิทธิ์ของผู้ใช้งานอย่างเป็นลายลักษณ์อักษร

2.3.2 กำหนดสิทธิ์ที่เหมาะสมกับผู้ใช้งานตามความจำเป็นและสอดคล้องกับหน้าที่ความรับผิดชอบ และจัดเก็บประวัติ (Log) การลงทะเบียน การเพิกถอนสิทธิ์ และการเปลี่ยนแปลงสิทธิ์ของผู้ใช้งาน

2.3.3 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจัดให้มีการควบคุมและจำกัดสิทธิ์ในการใช้งานระบบตามความจำเป็นในการใช้งานเท่านั้น

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 ต้องจำกัดจำนวนผู้ใช้งานที่ทำหน้าที่เป็นผู้ให้สิทธิ์กับผู้ใช้งานให้น้อยที่สุดตามความเหมาะสม

2.3.6 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจำกัดระยะเวลาการใช้งานในระบบเทคโนโลยีสารสนเทศของ รฟม. แก่หน่วยงานภายนอกที่เข้ามาปฏิบัติงานร่วมกับ รฟม.

2.3.7 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจัดให้มีการถอดถอนหรือเปลี่ยนแปลงสิทธิ์การเข้าถึงทันทีเมื่อผู้ใช้งานเกษียณ เปลี่ยนแปลงหน้าที่ความรับผิดชอบ เปลี่ยนแปลงการจ้างงาน หรือไม่มีความจำเป็นในการใช้งานระบบเทคโนโลยีสารสนเทศ

2.3.8 ผู้ดูแลระบบ ต้องลบหรือระงับการใช้งานสิทธิ์ของผู้ใช้งานที่มากับระบบ (Default User) ในกรณีที่มีความจำเป็นต้องใช้งานต้องกำหนดรหัสผ่านอย่างมั่นคงปลอดภัย

2.4 การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

2.4.1 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องมีการสอบทานสิทธิ์การเข้าถึงของผู้ใช้งานระบบเมื่อ รฟม. มีการเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศหรือโครงสร้างองค์กร

2.4.2 ผู้ดูแลระบบ ต้องมีการสอบทานและระงับการใช้งานบัญชีผู้ใช้งานที่ไม่ได้ใช้งานเกิน 180 วัน หากผู้ใช้งานต้องการกลับมาใช้งานจะต้องยืนยันตัวตนให้ ฝทท. ทราบ ทั้งนี้ ระยะเวลาที่ไม่ได้ใช้งานของบัญชีผู้ใช้งานอาจจะขึ้นอยู่กับแต่ละระบบสารสนเทศ

3. การป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล และการควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย

3.1 การป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล (Unattended User Equipment)

3.1.1 ผู้ดูแลระบบต้องจัดให้มีมาตรการสำหรับป้องกันระบบคอมพิวเตอร์ ระบบเครือข่ายสื่อสารข้อมูล และระบบเทคโนโลยีสารสนเทศ โดยการกำหนดค่าของระบบ (Configuration) ให้มีการล็อกหน้าจอสำหรับอุปกรณ์ที่ไม่มีพนักงานดูแล หรือล็อกอุปกรณ์อยู่เสมอ

3.1.2 ผู้ใช้งานและหน่วยงานภายนอก ต้องล็อกหน้าจออัตโนมัติเมื่อไม่มีการใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. ตามระยะเวลาที่กำหนด โดยต้องพักหน้าจอ (Screen Saver) อัตโนมัติ หลังจากที่ไม่มีการใช้งานคอมพิวเตอร์เป็นระยะเวลานานกว่า 15 นาที ผู้ใช้งานและหน่วยงานภายนอกจะใช้งานต่อได้เมื่อมีการใส่รหัสผ่านที่ถูกต้อง

3.1.3 ผู้ใช้งานต้อง Log Out ออกจากเครื่องคอมพิวเตอร์เมื่อมีความจำเป็นต้องละทิ้งเครื่องคอมพิวเตอร์

3.1.4 ผู้ใช้งานต้องป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ เช่น กล้องดิจิทัล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสารโดยไม่ได้รับอนุญาต

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 รฟม. 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 ชื่อระบบ และชื่ออุปกรณ์สารสนเทศแก่ผู้ที่ไม่ได้รับอนุญาตหรือหน่วยงานภายนอก

4.1.2 ผู้ดูแลระบบต้องควบคุมการใช้งานระบบเครือข่ายสื่อสารข้อมูล เพื่อป้องกันการเข้าถึงระบบเครือข่ายสื่อสารข้อมูลและบริการของระบบเครือข่ายสื่อสารข้อมูลโดยไม่ได้รับอนุญาต

4.1.3 ผู้ดูแลระบบต้องควบคุมการเชื่อมต่อเครือข่ายภายนอก เพื่อใช้งานอินเทอร์เน็ต ซึ่งอาจเป็นช่องทางให้หน่วยงานภายนอกเข้าถึงสารสนเทศหรือระบบเทคโนโลยีสารสนเทศของ รฟม. โดยมิได้รับอนุญาต

4.1.4 ผู้ใช้งานต้องแจ้งความประสงค์ในการขอใช้งานบริการเครือข่ายแก่ ฝทท. และสามารถใช้บริการเครือข่ายได้หลังจากได้รับการอนุมัติจาก ฝทท. แล้ว

4.1.5 ผู้ใช้งาน ต้องไม่ใช้ระบบเครือข่ายสื่อสารข้อมูลเพื่อเป็นช่องทางในการเจาะระบบ (Hacking) หรือการสแกนช่องโหว่ของระบบโดยมิได้รับอนุญาต

4.2 การพิสูจน์ตัวตนของผู้ใช้งานที่อยู่ภายนอก รฟม. (User Authentication for External Connections)
ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนผ่านระบบ Active Directory ของ รฟม. ก่อนอนุญาตให้ผู้ใช้งานที่อยู่ภายนอก รฟม. เข้าใช้งานเครือข่ายและระบบสารสนเทศของ รฟม.

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 (Instrusion Prevention System/ Instrusion Detection System) ของระบบเครือข่าย

4.6 การแบ่งแยกเครือข่าย (Segregation in Networks)

4.6.1 ผู้ดูแลระบบต้องจัดให้มีการแบ่งแยกเครือข่ายตามกลุ่มของผู้ใช้งาน หรือกลุ่มของระบบเทคโนโลยีสารสนเทศ เพื่อควบคุมการใช้งานในแต่ละเครือข่ายย่อยอย่างเหมาะสม โดยพิจารณาจากความต้องการในการเข้าถึงข้อมูล ระดับความสำคัญของข้อมูล รวมถึงการพิจารณาด้านราคา ประสิทธิภาพ และผลกระทบทางด้านความปลอดภัยดังต่อไปนี้

1) เครือข่ายที่อนุญาตให้เข้าถึงจากภายนอกและเครือข่ายที่ใช้ภายใน รฟม.
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 รฟม. เช่น Router หรือ Firewall เป็นต้น พร้อมทั้งติดตั้งระบบควบคุมเพื่อกลั่นกรองข้อมูลที่รับ - ส่ง เช่น Web Filtering, Email Filtering เป็นต้น เพื่อทำให้การเชื่อมต่อมีความปลอดภัย

4.7.2 ผู้ดูแลระบบต้องติดตั้ง Firewall ระหว่างเครือข่ายของ รฟม. กับเครือข่ายภายนอก ทั้งนี้ การติดตั้ง Firewall ต้องพิจารณาเรื่องดังต่อไปนี้

1) การป้องกันการจราจรจากภายนอก ต้องถูกกำหนดให้ใช้เส้นทางที่ผ่าน First Tier Firewall ที่มีความมั่นคงปลอดภัยเพื่อป้องกันทรัพย์สินสารสนเทศของ รฟม. และโครงสร้างพื้นฐานที่มีความสำคัญจากการเข้าถึงที่ไม่ได้รับอนุญาต
2) Firewall ต้องระบุตัวตนและพิสูจน์ตัวตนของผู้ใช้งานก่อนที่จะให้สิทธิ์การเข้าถึงอินเทอร์เฟส (Interface) เพื่อการบริหารจัดการ Firewall
3) Firewall ต้องตั้งค่าให้ระงับบัญชีผู้ใช้งานหลังจากมีความพยายามที่จะเข้าสู่ระบบไม่สำเร็จ 5 ครั้ง การยกเลิกการระงับต้องดำเนินการโดย ฝทท.
4) ไม่อนุญาตให้พิสูจน์ตัวตนผ่านทางอินเทอร์เฟส (Interface) การจัดการ Firewall จากระยะไกล (Remote)
5) ผู้ที่ได้รับการมอบหมายจาก ฝทท. เท่านั้นที่มีสิทธิ์ที่จะเปลี่ยนการตั้งค่าด้านความปลอดภัยบน Firewall
6) Firewall ต้องตั้งค่าให้บันทึกเหตุการณ์ด้านความมั่นคงปลอดภัย
7) Firewall ต้องได้รับการสอบทาน ทดสอบ และตรวจสอบอย่างสม่ำเสมอ
8) Firewall ต้องถูกบริหารจัดการผ่านทางการติดต่อสื่อสารที่มีการเข้ารหัส
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 และแพ็ตช์ (Patch) ที่จำเป็น และต้องติดตั้งแพ็ตช์ (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 ไม่แสดงข้อความว่าบัญชีผู้ใช้งานผิด 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 และต้องใช้ระบบเทคโนโลยีสารสนเทศพิสูจน์ตัวตนผู้ใช้งานในการเข้าถึงระบบปฏิบัติการโดยผ่านระบบ Active Directory หรือ Lightweight Derectory Access Protocol 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 ต้องตั้งค่าให้มีโปรแกรมพักหน้าจอที่ต้องใส่รหัสผ่านสำหรับเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์แบบพกพา และเครื่องคอมพิวเตอร์แม่ข่าย ทั้งนี้ โปรแกรมพักหน้าจอกำหนดให้ป้อนรหัสผ่านหลังจากที่มีการทิ้งเครื่องดังกล่าวไว้โดยไม่มีการใช้งานเป็นเวลา 15 นาที

5.5 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time)

5.5.1 ผู้ดูแลระบบ ต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง โดยต้องคำถึงระยะเวลาที่จำเป็นในกระบวนการดำเนินงานทางธุรกิจ ได้แก่ กำหนดให้เข้าใช้งานได้ในช่วงเวลาทำการของ รฟม. 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 รฟม. (Teleworking)

7.1 ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนการใช้งาน และเชื่อมต่อผ่านช่องทางที่มีความปลอดภัยที่มีเทคโนโลยีเข้ารหัสป้องกัน

7.2 ผู้ดูแลระบบต้องทำการถอดถอนสิทธิ์ในการเข้าถึงของผู้ใช้งานจากภายนอกสำนักงาน เมื่อครบกำหนดระยะเวลาที่ขออนุญาต

7.3 ผู้ใช้งาน หากจำเป็นต้องมีการปฏิบัติงานจากภายนอกสำนักงานของ รฟม. ต้องได้รับการอนุญาตจากผู้บังคับบัญชาอย่างเป็นลายลักษณ์อักษร ในกรณีเร่งด่วนสามารถดำเนินการก่อน โดยแจ้งให้ผู้บังคับบัญชารับทราบด้วย โดยผู้บังคับบัญชาต้องพิจารณาเงื่อนไขในการเตรียมการ ดังต่อไปนี้

1) ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมของการปฏิบัติงานจากภายนอก รฟม.

2) ความมั่นคงปลอดภัยทางการสื่อสาร โดยยึดจากระดับความสำคัญ (Sensitivity) ของข้อมูลที่จะถูกเข้าถึงและส่งผ่านช่องทางการเชื่อมต่อสื่อสาร (Communication Link) รวมถึงระดับความสำคัญ (Sensitivity) ของระบบภายใน รฟม.

7.4 ผู้ใช้งานต้องจัดเก็บเอกสารที่เป็นความลับในอุปกรณ์ที่ล็อกได้และมีการควบคุมการเข้าถึง โดยใช้หลักเกณฑ์การรักษาความลับเช่นเดียวกับสารสนเทศที่อยู่ในสำนักงานของ รฟม.

7.5 ผู้ใช้งาน ต้องติดตั้งโปรแกรมป้องกันไวรัสและ Personal Firewall สำหรับอุปกรณ์ส่วนตัวที่ใช้เชื่อมต่อเครือข่ายของ รฟม. จากภายนอก

8. ผู้บังคับบัญชา ต้องควบคุมการใช้งานข้อมูลส่วนบุคคลให้มีการใช้งานที่สอดคล้องกับกฎหมาย พระราชบัญญัติกฎระเบียบ ข้อบังคับที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ส่วนที่ 7
การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

วัตถุประสงค์

- ☐ เพื่อกำหนดมาตรการในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ของ รฟม. โดยการกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ
- ☐ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

ผู้รับผิดชอบ

- ☐ ผู้ดูแลระบบ
- ☐ ผู้ใช้งาน

อ้างอิงมาตรฐาน

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

แนวปฏิบัติ

1. ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของ รฟม. ต้องลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับการอนุญาตจาก ฝทท. อย่างเป็นลายลักษณ์อักษร
2. ผู้ดูแลระบบต้องลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ
3. ผู้ดูแลระบบต้องลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย
4. ผู้ดูแลระบบ ต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีใช้ Access Point (AP) ของ รฟม. รับ - ส่งสัญญาณได้
5. ผู้ดูแลระบบต้องเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและต้องสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณอาจช่วยลดการรั่วไหลของสัญญาณให้ดีขึ้น
6. ผู้ดูแลระบบต้องเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำ Access Point (AP) มาใช้งาน
7. ผู้ดูแลระบบต้องเปลี่ยนค่าชื่อ Login และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบต้องเลือกใช้ชื่อ Login และรหัสผ่านที่มีความคาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย
8. ผู้ดูแลระบบต้องควบคุม MAC Address ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยอนุญาตเฉพาะผู้ใช้งานที่ได้รับอนุญาตให้เข้าใช้เครือข่ายไร้สายได้อย่างถูกต้องเท่านั้น
9. ผู้ดูแลระบบต้องตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ และบันทึกเหตุการณ์น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สายตามขั้นตอนที่ รฟม. กำหนด

ส่วนที่ 8
การควบคุมหน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) เข้าถึงระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

☐ เพื่อควบคุมหน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) ที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. ให้เป็นไปอย่างมั่นคงปลอดภัย

ผู้รับผิดชอบ

☐ ผู้ดูแลระบบ

☐ ผู้บังคับบัญชา

☐ หน่วยงานภายนอก

☐ ผู้ใช้งาน (บุคคลภายนอก)

อ้างอิงมาตรฐาน

☐ หมวดที่ 5 การควบคุมการเข้าถึง (Access control)

☐ หมวดที่ 7 ความมั่นคงปลอดภัยทางภายภาพและสิ่งแวดล้อม (Physical and environment security)

☐ หมวดที่ 11 ความสัมพันธ์กับผู้ขาย ผู้ให้บริการภายนอก (Supplier relationships)

แนวปฏิบัติ

1. ผู้ดูแลระบบต้องประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศของ รฟม.
2. การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก)
   - 2.1 เจ้าของข้อมูลต้องเป็นผู้อนุญาตการให้สิทธิ์แก่หน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) ที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของ รฟม. อย่างเป็นลายลักษณ์อักษร
   - 2.2 ผู้บังคับบัญชาต้องกำหนดให้มีการลงนามการไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของ รฟม.
   - 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 เพื่อใช้สำหรับควบคุมหรือตรวจสอบการทำงานและเพื่อให้มั่นใจว่าการปฏิบัติงานเป็นไปตามขอบเขตที่ได้กำหนดไว้

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. ผู้ดูแลระบบต้องควบคุมการเปลี่ยนแปลงของหน่วยงานภายนอกที่ส่งผลกระทบต่อการให้บริการขององค์กรและต้องประเมินความเสี่ยงอย่างเหมาะสมเพื่อควบคุมผลกระทบอันเนื่องมาจากการเปลี่ยนแปลงนั้น
9. หน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) ต้องใช้งานทรัพย์สินสารสนเทศของ รฟม. ด้วยความระมัดระวัง และรักษาความลับของ รฟม. ไม่นำไปเปิดเผย และต้องขออนุญาตพร้อมทั้งปฏิบัติตามเงื่อนไขในการเข้าถึงระบบสารสนเทศของ รฟม. ทุกครั้ง
10. การควบคุมการนำอุปกรณ์ส่วนตัว (Bring Your Own Device: BYOD) มาเชื่อมต่อกับระบบเครือข่ายของ รฟม. เพื่อบริหารจัดการระบบงานสารสนเทศ

10.1 ผู้ดูแลระบบต้องอนุญาตการนำอุปกรณ์ส่วนตัวมาเชื่อมต่อกับระบบเครือข่ายของ รฟม. เพื่อเข้าถึงระบบงานสารสนเทศต่าง ๆ อย่างเป็นลายลักษณ์อักษร

10.2 ผู้ดูแลระบบต้องตรวจสอบการติดตั้งโปรแกรมป้องกันมัลแวร์ที่อุปกรณ์ส่วนตัวของผู้ใช้งานว่าต้องอัปเดตเป็นเวอร์ชันล่าสุด

10.3 ผู้ดูแลระบบต้องตรวจสอบการอัปเดต Patch ของระบบปฏิบัติการที่อุปกรณ์ส่วนตัวของผู้ใช้งานว่าต้องอัปเดตเป็นเวอร์ชันล่าสุด

10.4 ผู้ดูแลระบบต้องตรวจสอบผลการสแกนมัลแวร์ที่อุปกรณ์ส่วนตัวของผู้ใช้งาน โดยต้องมีผลการสแกนมัลแวร์ไม่เกิน 1 วัน

ส่วนที่ 9
การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ ของ รฟม.

วัตถุประสงค์

☐ เพื่อควบคุมการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ ที่ รฟม. จัดไว้ให้ใช้อย่างเหมาะสม ทั้งนี้ เพื่อป้องกันการสูญหาย เสียหาย หรือถูกเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ผู้รับผิดชอบ

☐ ผู้ดูแลระบบ

☐ ผู้ใช้งาน

อ้างอิงมาตรฐาน

☐ 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 รฟม.
   - 1.4 ผู้ใช้งานต้องไม่ติดตั้งโปรแกรมที่ละเมิดลิขสิทธิ์บนเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ของ รฟม.
   - 1.5 ผู้ใช้งานต้องขอนุญาตติดตั้งโปรแกรมในเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ตามขั้นตอนที่ รฟม. กำหนด
   - 1.6 ผู้ใช้งานต้องไม่ติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ของ รฟม. การดำเนินการดังกล่าวต้องดำเนินการโดยผู้ดูแลระบบเท่านั้น
   - 1.7 ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่อย่างละเอียด เพื่อให้สามารถใช้งานอย่างปลอดภัยและมีประสิทธิภาพ
   - 1.8 ผู้ใช้งานต้องไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ และรักษาให้มีสภาพเดิม
   - 1.9 ผู้ใช้งานต้องแจ้งซ่อมเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่เพื่อให้ ฝทท. เป็นผู้ดำเนินการเท่านั้น
   - 1.10 ผู้ใช้งานต้องไม่สร้าง Shortcut ไว้บน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของ รฟม.
   - 1.11 กรณีเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์เคลื่อนที่

     ผู้ใช้งาน ต้องปฏิบัติ ดังนี้

     - 1.11.1 ในกรณีที่มีการใช้งานอุปกรณ์ประเภทพกพาในที่สาธารณะ ห้องประชุม และพื้นที่ภายนอก อื่น ๆ ที่ไม่มีการป้องกัน หรือไม่ได้อยู่ในบริเวณของ รฟม. ให้ป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต เช่น ไม่เปิดการเชื่อมต่อแบบไร้สายโดยไม่มีการเข้ารหัสข้อมูล เป็นต้น

1.11.2 ต้องระมัดระวังการเคลื่อนย้าย โดยต้องใส่กระเป๋าเพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงานหรือหลุดมือ เป็นต้น

1.11.3 ไม่ใส่ในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับหรืออาจถูกจับโยนได้

1.11.4 การใช้งานเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัดต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

1.11.5 หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอย ขีดข่วน หรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

1.11.6 ไม่วางของทับบนหน้าจอและแป้นพิมพ์

1.11.7 การเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

1.11.8 ไม่คลื่อนย้ายเครื่องในขณะที่ Harddisk กำลังทำงาน

1.11.9 ไม่ใช้หรือวางใกล้สิ่งที่เป็นของเหลว 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 เพราะจำทำให้หน้าจอมีรอยขีดข่วนได้

1.11.13 รับผิดชอบในการป้องกันการสูญหาย เช่น ต้องล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

1.11.14 นำติดตัวไปด้วยเสมอ เช่น ไม่ละทิ้ง อุปกรณ์ประมวลผลประเภทพกพาในรถยนต์ ห้องพักในโรงแรม หรือห้องประชุม เป็นต้น ในกรณีที่มีความจำเป็นต้องละทิ้งให้จัดเก็บไว้ในสถานที่มั่นคงปลอดภัย

1.11.15 ไม่เก็บหรือใช้งานในสถานที่ที่มีความร้อน ความชื้นหรือฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

1.11.16 ไม่เปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Component) ที่ติดตั้งอยู่ภายใน เช่น แบตเตอรี่ หน่วยความจำ

2. แนวปฏิบัติในการใช้รหัสผ่าน
ให้ผู้ใช้งานปฏิบัติตามการใช้งานรหัสผ่าน (Password Use) (ส่วนที่ 6 ข้อ 2.2.7)

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 Floppy Disk, Thumb Drive และ Data Storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์ของ รฟม.

3.5 ผู้ใช้งาน หากพบหรือสงสัยว่าเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ติดชุดคำสั่งไม่พึงประสงค์ ให้รีบยกเลิกเชื่อมต่อเครื่องเข้ากับระบบเครือข่ายสื่อสารข้อมูลเพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่น ๆ ได้ และแจ้ง ฝทท. ทราบทันที

4. การสำรองข้อมูลและการกู้คืน

4.1 ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ไว้บนสื่อบันทึกอื่น ๆ เช่น ระบบ File Sharing, CD, DVD, External Harddisk เป็นต้น

4.2 ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

5. ผู้ดูแลระบบ ต้องควบคุมให้เครื่องคอมพิวเตอร์ได้รับการปรับตั้งค่าอย่างเหมาะสม เพื่อป้องกันการใช้งานหรือติดตั้ง Mobile code เช่น Active X, Java จากแหล่งที่ไม่น่าเชื่อถือ

ส่วนที่ 10
การใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์

วัตถุประสงค์

☐ เพื่อควบคุมการใช้งานอินเทอร์เน็ตและการใช้งานสื่อสังคมออนไลน์ (Social Network) ของ รฟม. ให้มีความปลอดภัยและป้องกันการละเมิดพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ จนส่งผลกระทบต่อ รฟม.

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 ในกรณีที่จำเป็นต้องได้รับการอนุญาตจากผู้บังคับบัญชาก่อนเท่านั้น
   2) ผู้ดูแลระบบต้องจำกัดการใช้งานอินเทอร์เน็ตเพื่อเรื่องส่วนตัวหรือที่ไม่ใช่การดำเนินงานของ รฟม. ให้น้อยที่สุดเท่าที่เป็นไปได้ เช่น การระงับการเข้าถึง Website ที่ไม่จำเป็น การระงับการเข้าถึง Website ที่มีเนื้อหาต้องห้ามตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
   3) ผู้ดูแลระบบต้องป้องกันไม่ให้มีการรับส่งข้อมูลที่ไม่เหมาะสมจากภายนอก รฟม. เช่น
      (ก) Executable เช่น .EXE .COM เป็นต้น
      (ข) ไฟล์ (File) เสียง เช่น AUD .WAV และ.MP3 เป็นต้น
      (ค) ไฟล์ (File) วีดิทัศน์ เช่น .MPG .MPEG .MOV และ .AVI เป็นต้น
      (ง) Peer to Peer เช่น .torrent เป็นต้น

      ในกรณีที่มีความจำเป็นต้องได้รับอนุญาตจากผู้บังคับบัญชา และ ฝทท.
   4) ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่ รฟม. จัดสรรไว้เท่านั้น เช่น Proxy, Firewall เป็นต้น ห้ามผู้ใช้งานเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นมีความจำเป็นและขออนุญาตจาก ฝทท. เป็นลายลักษณ์อักษรแล้ว
   5) ผู้ดูแลระบบต้องทดสอบเส้นทางสำหรับการเชื่อมต่ออินเทอร์เน็ตขององค์กรระหว่างเส้นทางที่ใช้งานจริงและเส้นทางสำรองอย่างน้อยปีละ 2 ครั้ง

6) 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. ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของ รฟม. เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น
6. ผู้ใช้งานจะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของ รฟม.
7. ผู้ใช้งานต้องหลีกเลี่ยงการกระทำที่สิ้นเปลืองทรัพยากรของเครือข่ายอินเทอร์เน็ต ดังนี้
   (ก) ส่งจดหมายอิเล็กทรอนิกส์ที่มีขนาดใหญ่หรือจดหมายอิเล็กทรอนิกส์ลูกโซ่
   (ข) ใช้เวลาในการเข้าถึงอินเทอร์เน็ตเกินความจำเป็น
   (ค) เล่นเกม Online
   (ง) เข้าห้องพูดคุย Online
8. ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับ รฟม.
9. ผู้ใช้งานต้องไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของ รฟม.
10. ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต
11. ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ที่จะทำให้ผู้อื่นเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย
12. ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน
13. ผู้ใช้งานต้องคำนึงว่าข้อมูลจากอินเทอร์เน็ตอาจไม่มีความทันสมัยหรือไม่มีความถูกต้อง ผู้ใช้งานต้องตรวจสอบความถูกต้องของข้อมูลจากแหล่งที่น่าเชื่อถือก่อนที่จะเผยแพร่ข้อมูลดังกล่าว
14. ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา
15. ผู้ใช้งานต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้ายในการเสนอความคิดเห็นที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของ รฟม. 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 รฟม.
    19.2 ผู้ใช้งานต้องระมัดระวังในการใช้สื่อสังคมออนไลน์ เนื่องจากพื้นที่บนสื่อสังคมออนไลน์เป็นพื้นที่สาธารณะไม่ใช่พื้นที่ส่วนบุคคล ซึ่งข้อมูลการใช้งานต่าง ๆ จะถูกบันทึกไว้และอาจมีผลทางกฎหมาย ถึงแม้จะเป็นการแสดงความคิดเห็นในนามชื่อบัญชีส่วนตัว และพึงตระหนักถึงผลกระทบที่อาจเกิดขึ้นกับ รฟม. ได้
    19.3 ผู้ใช้งานที่ใช้สื่อสังคมออนไลน์เป็นเครื่องมือสื่อสารข้อมูลในกิจการของ รฟม. 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 รฟม.
    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 ที่ผู้ใช้งานเผยแพร่ไว้บนบริการสื่อสังคมออนไลน์นั้นคงอยู่ถาวรและผู้อื่นอาจเข้าถึงและเผยแพร่ข้อมูลเหล่านั้นได้

19.11 ผู้ใช้งานต้องมีข้อพิจารณาในการรับเพื่อนเข้ากลุ่มที่ชัดเจน และควรประกาศข้อความปฏิเสธความรับผิดชอบที่เกี่ยวกับเนื้อหาหรือข้อความแสดงความคิดเห็นซึ่งถูกโพสต์จากเพื่อนในกลุ่มที่อาจปรากฏในเว็บไซต์ประเภท Social Network ของผู้ใช้งานเอง

19.12 ผู้ใช้งานต้องติดตั้งซอฟต์แวร์ป้องกันไวรัส และอัปเดตฐานข้อมูลไวรัสของโปรแกรมอยู่เสมอ และต้องหลีกเลี่ยงการใช้โปรแกรมที่ละเมิดลิขสิทธิ์เพราะอาจจะมีโปรแกรมประสงค์ร้ายแฝงตัวอยู่ภายในเพื่อลักลอบ ปลอมแปลง หรือขโมยข้อมูลสำคัญของผู้ใช้งานได้

19.13 ผู้ใช้งานต้องระมัดระวังการใช้ถ้อยคำและภาษาที่อาจเป็นการดูหมิ่น ยุยง ท้าทาย หรือเป็นการละเมิดต่อบุคคลอื่น กรณีบุคคลอื่นมีความคิดเห็นที่แตกต่างพึงงดเว้นการโต้ตอบด้วยถ้อยคำรุนแรง

19.14 ผู้ใช้งานต้องระมัดระวังกระบวนการหาข่าว หรือภาพจากสื่อสังคมออนไลน์ โดยมีการตรวจสอบอย่างถี่ถ้วนรอบด้านและต้องอ้างอิงแหล่งที่มาเมื่อนำเสนอ เว้นแต่สามารถตรวจสอบและอ้างอิงจากแหล่งข่าวได้โดยตรง

19.15 หากผู้ใช้งานต้องการใช้สื่อสังคมออนไลน์เป็นเครื่องมือในการรายงานข่าวในนามของบุคคลธรรมดาต้องแสดงให้ชัดเจนว่า 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 และระมัดระวังการถูกนำข้อมูลจากชื่อบัญชีไปใช้โดยไม่เหมาะสม ผิดวัตถุประสงค์ และลักษณะการแอบอ้างโดยบุคคลอื่น

20. ผู้ใช้งานต้องใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์โดยตระหนักถึงพระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่บังคับใช้อยู่เสมอ

ส่วนที่ 11
การใช้งานจดหมายอิเล็กทรอนิกส์

วัตถุประสงค์

☐ เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ของ รฟม. ให้มีความปลอดภัยและมีประสิทธิภาพ

ผู้รับผิดชอบ

☐ ผู้ดูแลระบบ

☐ ผู้ใช้งาน

อ้างอิงมาตรฐาน

☐ หมวดที่ 5 การควบคุมการเข้าถึง (Access control)

☐ หมวดที่ 8 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations security)

แนวปฏิบัติ

1. ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของ รฟม. ให้เหมาะสมกับหน้าที่ความรับผิดชอบของผู้ใช้งาน รวมทั้งทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ
2. ผู้ดูแลระบบต้องกำหนดบัญชีผู้ใช้งานตามมาตรฐานจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ใช้ในองค์กร
3. ผู้ใช้งานต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ไม่ให้เกิดความเสียหายต่อ รฟม. ละเมิดลิขสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น ผิดกฎหมาย ละเมิดศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ของ รฟม.
4. ผู้ใช้งานต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail Address) ของผู้อื่นเพื่ออ่าน รับ - ส่งข้อความ ยกเว้นได้รับการยินยอมจากเจ้าของบัญชีและให้ถือว่าเจ้าของบัญชีจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน
5. ผู้ใช้งานต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของ รฟม. เพื่อปฏิบัติงาน ติดต่อ และประสานงานของ รฟม. เท่านั้น
6. ผู้ใช้งานต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ฟรีของเอกชนในการปฏิบัติงาน ติดต่อ และประสานงานของ รฟม.
7. ผู้ใช้งานต้อง Logout ออกจากระบบทุกครั้ง หลังจากใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้นเพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์
8. ผู้ใช้งานต้องตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนเปิดอ่าน โดยใช้โปรแกรมป้องกันไวรัสเพื่อตรวจสอบมัลแวร์ต่าง ๆ
9. ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์ที่ได้รับจากผู้ส่งที่ไม่รู้จัก
10. ผู้ใช้งานต้องใช้ข้อความที่สุภาพในการรับ – ส่งจดหมายอิเล็กทรอนิกส์ และไม่จัดส่งจดหมายที่มีเนื้อหาอาจทำให้ รฟม. เสียชื่อเสียงหรือทำให้เกิดความแตกแยกภายใน รฟม.
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 ความถี่ในการดำเนินการสำรองข้อมูลและขั้นตอนการสำรองข้อมูลระบบแม่ข่ายเป็นความรับผิดชอบของ ฝทท. โดยมีแนวปฏิบัติ ดังนี้

   1.1 ผู้บังคับบัญชากำหนดผู้รับผิดชอบในการสำรองข้อมูล

   1.2 ผู้ดูแลระบบต้องกำหนดชนิดของข้อมูลของระบบที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้ เช่น ข้อมูลค่าคอนฟิกกูเรชัน (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 ความถี่ในการสำรองข้อมูลขึ้นอยู่กับความถี่ของการเปลี่ยนแปลงของข้อมูลและระดับความสำคัญของข้อมูลหากเกิดการสูญหาย

3. การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์

เพื่อให้สามารถระบุตัวบุคคลผู้ใช้งานได้อย่างถูกต้อง ผู้ดูแลระบบต้องดำเนินการดังนี้

3.1 ตั้งนาฬิกาของอุปกรณ์ที่ให้บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล Stratum - 1 เก็บรักษาข้อมูลจราจรคอมพิวเตอร์ โดยระยะเวลาในการเก็บตามประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 (90 วัน)

3.2 เก็บรักษาข้อมูลจราจรคอมพิวเตอร์ในสื่อที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง มีการเก็บรักษาความลับของข้อมูลตามระดับชั้นความลับในการเข้าถึงตามที่ รฟม. กำหนด โดยระบุตัวบุคคลที่สามารถเข้าถึงสื่อดังกล่าวได้

3.3 ประเภทของสารสนเทศที่เก็บรักษา แสดงตามตาราง

ประเภทของสารสนเทศ	กฎหมายที่เกี่ยวข้อง	ระยะเวลาการจัดเก็บรักษา (ปี)
Authentication Server Logs (RADIUS, TACACS)	1) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 2) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 3) ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550	1
Email Server Logs		1
Web Application Server Logs		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 รฟม.
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 เพื่อมิให้เกิดการใช้งานผิดประเภทหรือถูกละเมิดการใช้งาน (Compromise) โดยควบคุมการเข้าถึง และตรวจสอบการนำเครื่องมือไปใช้งานอย่างสม่ำเสมอ
9. ผู้ดูแลระบบต้องประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
10. ผู้ดูแลระบบต้องประเมินความเสี่ยงแล้วจัดลำดับความสำคัญของความเสี่ยงนั้นและค้นหาวิธีการเพื่อลดความเสี่ยงตามขั้นตอนที่ รฟม. กำหนด พร้อมทั้งพิจารณาข้อดีข้อเสียของวิธีการเหล่านั้นเพื่อให้ผู้บริหารของ รฟม. ตัดสินใจเลือกวิธีการเพื่อลดความเสี่ยงหรือยอมรับความเสี่ยง เมื่อเลือกวิธีการลดความเสี่ยงแล้วผู้บริหารต้องจัดสรรทรัพยากรอย่างเพียงพอเพื่อดำเนินการ แนวทางการลดความเสี่ยง แบ่งได้เป็น 3 รูปแบบ ได้แก่
    10.1 การเลือกใช้เทคโนโลยี เพื่อใช้ในการลดความเสี่ยงและเพิ่มความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รฟม. เป็นวิธีที่จำเป็นต้องใช้งบประมาณและทรัพยากรอย่างเพียงพอในการดำเนินการ เช่น การเลือกใช้อุปกรณ์ Firewall มากกว่าหนึ่งผลิตภัณฑ์ในการป้องกันการเข้าถึงเครือข่ายที่สำคัญ การใช้อุปกรณ์สมาร์ทการ์ด หรือ USB Token ในการตรวจสอบยืนยันตัวตนในการเข้าใช้งานระบบจากภายนอก รฟม. เป็นต้น
    10.2 การปรับเปลี่ยนขั้นตอนปฏิบัติ ต้องออกแบบขั้นตอนปฏิบัติใหม่ที่รัดกุมและสามารถรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รฟม. ได้ดีขึ้น เมื่อออกแบบขั้นตอนปฏิบัติใหม่แล้วต้องมีการพิจารณาหารือความเหมาะสม ความเป็นไปได้ และผู้บริหารต้องเป็นผู้อนุมัติให้มีการบังคับใช้ขั้นตอนปฏิบัติใหม่นั้น
    10.3 ผู้ดูแลระบบต้องแจ้งขั้นตอนปฏิบัติให้ผู้เกี่ยวข้องรับรู้อย่างทั่วถึง รวมทั้งต้องจัดฝึกอบรมผู้ใช้งานที่เกี่ยวข้องเพื่อให้สามารถปฏิบัติตามขั้นตอนปฏิบัติใหม่ได้อย่างราบรื่นและมีประสิทธิภาพ
11. การตรวจสอบความปลอดภัยของระบบสารสนเทศ
    11.1 ผู้ดูแลระบบ ต้องวางแผนการตรวจสอบและประเมินช่องโหว่หรือจุดอ่อนด้านความมั่นคงปลอดภัยสารสนเทศ และแจ้งผู้ที่เกี่ยวข้องเพื่อแก้ไขในกรณีที่พบว่าช่องโหว่หรือจุดอ่อนนั้นอาจเป็นเหตุการณ์ด้านความมั่นคงปลอดภัย อย่างน้อยปีละ 1 ครั้ง
    11.2 ผู้ดูแลระบบต้องตรวจสอบระบบสารสนเทศที่จะต้องมีการปรับปรุงเมื่อมีเวอร์ชันใหม่ (Patch) รวมทั้งข้อมูลที่เกี่ยวข้องกับช่องโหว่ด้านเทคนิคอย่างสม่ำเสมอเพื่อให้ทราบถึงภัยคุกคามและความเสี่ยง รวมถึงหาวิธีป้องกันและแก้ไขที่เหมาะสมกับช่องโหว่นั้น
    11.3 ผู้ใช้งาน ผู้ดูแลระบบ และหน่วยงานภายนอก ต้องบันทึกและรายงานช่องโหว่หรือจุดอ่อนใด ๆ ด้านความมั่นคงปลอดภัยสารสนเทศ ที่อาจสังเกตพบระหว่างการติดตามการใช้งานระบบสารสนเทศ ผ่านช่องทางบริหารจัดการที่กำหนดไว้อย่างเหมาะสม และต้องดำเนินการปิดช่องโหว่ที่มีการตรวจพบหรือได้รับแจ้ง
12. ผู้ดูแลระบบต้องมีการบริหารจัดการการเปลี่ยนแปลงเกี่ยวกับการจัดเตรียมการให้บริการ การดูแลปรับปรุงนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ขั้นตอนปฏิบัติงาน หรือการควบคุมเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ โดยคำนึงถึงระดับความสำคัญของการดำเนินธุรกิจที่เกี่ยวข้องและการประเมินความเสี่ยงอย่างต่อเนื่อง

ส่วนที่ 14
การถ่ายโอน และแลกเปลี่ยนข้อมูลสารสนเทศ

วัตถุประสงค์

☐ เพื่อให้มีการควบคุมการถ่ายโอนและแลกเปลี่ยนข้อมูลสารสนเทศ ป้องกันการรั่วไหล หรือมีการแก้ไขข้อมูลโดยที่ไม่ได้รับอนุญาต รวมถึงการป้องกันสื่อบันทึกข้อมูลให้มีความปลอดภัยเป็นไปตามข้อกำหนด

ผู้รับผิดชอบ

☐ ผู้บังคับบัญชา

☐ เจ้าของข้อมูล

☐ ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

☐ หมวดที่ 9 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)

แนวปฏิบัติ

1. ผู้บังคับบัญชา ต้องควบคุมให้มีการจัดทำนโยบาย และขั้นตอนการปฏิบัติเพื่อป้องกันข้อมูลสารสนเทศที่มีการสื่อสาร หรือแลกเปลี่ยนผ่านระบบสารสนเทศให้เหมาะสมตามระดับชั้นความลับข้อมูลสารสนเทศตามขั้นตอนที่ รฟม. 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 การเปลี่ยนแปลงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต
   - 6.4 การเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต
   - 6.5 การเข้าถึงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต
   - 6.6 การนำข้อมูลสารสนเทศกลับมาใช้ใหม่โดยไม่ได้รับอนุญาต
7. เจ้าของข้อมูล และผู้ดูแลระบบ ต้องมีการป้องกันข้อมูลสารสนเทศที่มีการเผยแพร่ต่อสาธารณชนมิให้มีการแก้ไขเปลี่ยนแปลงโดยมิได้รับอนุญาต เพื่อรักษาความถูกต้องครบถ้วนของข้อมูลสารสนเทศ

ส่วนที่ 15
การควบคุมการเข้ารหัส

วัตถุประสงค์

☐เพื่อให้มีการเข้ารหัสข้อมูลอย่างเหมาะสมและมีประสิทธิผลในการปกป้องความลับ ป้องกัน การปลอมแปลงข้อมูล และควบคุมความถูกต้องของข้อมูล

ผู้รับผิดชอบ

☐ผู้ดูแลระบบ

☐เจ้าของข้อมูล

☐ผู้ใช้งาน

อ้างอิงมาตรฐาน

☐ หมวดที่ 6 การเข้ารหัสข้อมูล (Cryptography)

แนวปฏิบัติ

1. เจ้าของข้อมูล ต้องเข้ารหัส หรือการใส่รหัสผ่านข้อมูลอิเล็กทรอนิกส์ขององค์กรตามระดับชั้นความลับเพื่อป้องกันผู้ไม่มีสิทธิเข้าถึง ตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และตามขั้นตอนที่ รฟม. 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	AES	128 bits
กุญแจแบบอสมมาตร	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) ควรส่งมอบให้กับเจ้าของกุญแจโดยตรงโดยวิธีการที่ปลอดภัย
   - 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 รฟม. กำหนด