



การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

MASS RAPID TRANSIT AUTHORITY OF THAILAND

ร่างขอบเขตของงาน, ร่างประกาศและร่างเอกสารประกวดราคา

เช่าเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์

ประจำปีงบประมาณ 2568 - 2570

ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e - bidding)

(ฉบับแรก)

ผู้สนใจสามารถแนะนำ วิจารณ์ หรือส่งความเห็นมาได้ที่

[procure@mrta.co.th](mailto:procure@mrta.co.th)

ภายในวันที่ 18 มิถุนายน 2567

การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

13 มิถุนายน 2567

---

**ขอบเขตของงานเช่าเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์**  
**ประจำปีงบประมาณ 2568 - 2570**

**1. ความเป็นมา**

การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย (รฟม.) ได้มีการจัดหาเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ เพื่อสนับสนุนการปฏิบัติงานของ รฟม. ระหว่างปีงบประมาณ 2565 - 2567 ด้วยวิธีการเช่า โดยจะหมดสัญญาเช่า ในวันที่ 30 กันยายน 2567 เพื่อสนับสนุนส่วนงานต่าง ๆ ที่ได้มีการร้องขอเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ เพิ่มเติม ดังนั้น รฟม. จึงมีความจำเป็นต้องจัดหาเพื่อทดแทนและเพิ่มเติมให้เพียงพอต่อการใช้งานทั้งในปัจจุบันและอนาคต

**2. วัตถุประสงค์**

เพื่อเช่าเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ (ซึ่งต่อไปนี้เรียกว่า “คอมพิวเตอร์”) ทดแทนของเดิม ที่หมดสัญญาเช่าและเช่าคอมพิวเตอร์เพิ่มเติมให้เพียงพอต่อการปฏิบัติงาน โดยมีรายการและจำนวน ดังนี้

2.1 เครื่องคอมพิวเตอร์ สำหรับงานสำนักงาน	จำนวน	330	ชุด
2.2 เครื่องคอมพิวเตอร์ สำหรับงานกราฟิก	จำนวน	27	ชุด
2.3 เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงาน แบบที่ 1	จำนวน	83	ชุด
2.4 เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงาน แบบที่ 2	จำนวน	102	ชุด
2.5 เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานกราฟิก	จำนวน	2	ชุด
2.6 เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานประมวลผล	จำนวน	3	ชุด
2.7 เครื่องคอมพิวเตอร์แท็บเล็ต แบบที่ 1	จำนวน	16	ชุด
2.8 เครื่องคอมพิวเตอร์แท็บเล็ต แบบที่ 2	จำนวน	30	ชุด
2.9 เครื่องสำรองไฟฟ้า	จำนวน	357	ชุด
2.10 ซอฟต์แวร์ป้องกันไวรัส	จำนวน	547	ชุด

**3. คุณสมบัติของผู้ยื่นข้อเสนอ**

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจาก เป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลัง กำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทำงานและได้แจ้งเวียนชื่อให้เป็นผู้ทำงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทำงานเป็นหุ้นส่วน ผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย







/3.6 มีคุณสมบัติ...

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นนิติบุคคลผู้มีอาชีพขายหรือให้เช่าพัสดุที่ประกวดราคาเช่าด้วยวิธีประกวดราคาอิเล็กทรอนิกส์

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ รพม. ณ วัน ประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นนั้น

3.10 ผู้ยื่นข้อเสนอที่เสนอราคาในรูปแบบของ “กิจการร่วมค้า” ต้องมีคุณสมบัติดังนี้

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค่างำหนดให้ผู้เข้าร่วมค้ำรายใดรายหนึ่งเป็นผู้เข้าร่วมค้ำหลัก ข้อตกลงระหว่างผู้เข้าร่วมค้ำจะต้องมีการกำหนดสัดส่วนหน้าที่และความรับผิดชอบในปริมาณงาน สิ่งของหรือมูลค่าตามสัญญาของผู้เข้าร่วมค้ำหลักมากกว่าผู้เข้าร่วมค้ำรายอื่นทุกราย

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค่างำหนดให้ผู้เข้าร่วมค้ำรายใดรายหนึ่งเป็นผู้เข้าร่วมค้ำหลัก กิจการร่วมค้ำนั้นต้องใช้ผลงานของผู้เข้าร่วมค้ำหลักรายเดียวเป็นผลงานของกิจการร่วมค้ำที่ยื่นข้อเสนอ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้ำที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ำรายใดเป็นผู้เข้าร่วมค้ำหลัก ผู้เข้าร่วมค้ำทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค่างำหนดให้มีการมอบหมายผู้เข้าร่วมค้ำรายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้ำ การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

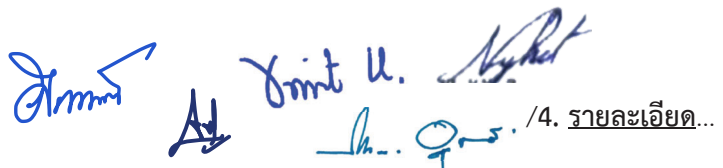
สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้ำที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ำรายใดเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้ำทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ำรายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้ำ

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

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

3.13 ผู้ยื่นข้อเสนอต้องมีหนังสือรับรองการเป็นตัวแทนจำหน่ายผลิตภัณฑ์ที่มีอายุไม่เกิน 90 วันนับจากวันที่ออกหนังสือจนถึงวันที่ยื่นข้อเสนอนี้ จากบริษัทผู้ผลิต หรือบริษัทสาขาของผู้ผลิตในต่างประเทศ หรือบริษัทสาขาของผู้ผลิตในประเทศไทย หรือตัวแทนจำหน่ายในประเทศไทย โดยต้องออกให้เพื่อมายื่นข้อเสนอนี้ ทั้งนี้ ผู้ยื่นข้อเสนอจะต้องแนบหนังสือรับรองดังกล่าวเพื่อประกอบการพิจารณา เฉพาะรายการดังต่อไปนี้

- 1) เครื่องคอมพิวเตอร์ สำหรับงานสำนักงาน
- 2) เครื่องคอมพิวเตอร์ สำหรับงานกราฟิก
- 3) เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานสำนักงาน แบบที่ 1
- 4) เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานสำนักงาน แบบที่ 2
- 5) เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานประมวลผล
- 6) เครื่องสำรองไฟฟ้า

 /4. รายละเอียด...

#### 4. รายละเอียดคุณลักษณะเฉพาะของพัสดุที่จะดำเนินการเช่า

4.1 คอมพิวเตอร์ที่เสนอต้องเป็นของแท้ อยู่ในสภาพที่ใช้งานได้ดี เป็นรุ่นที่ยังอยู่ในสายการผลิต (Production Line) และต้องเป็นของใหม่ที่ยังมิได้ถูกติดตั้งใช้งาน ณ ที่ใดมาก่อน รวมทั้งต้องไม่ถูกนำมาปรับปรุงสภาพใหม่ (Reconditioned หรือ Rebuilt)

4.2 คอมพิวเตอร์ที่เสนอต้องมีคุณสมบัติตรงตาม Catalog หรือ Brochure ของบริษัทผู้ผลิตที่เสนอขายตามท้องตลาด โดยมีระบบหลักและ/หรือองค์ประกอบหลักที่มีได้ประกอบและ/หรือตัดแปลงเพื่อใช้เฉพาะการยื่นข้อเสนอ โดยผู้ยื่นข้อเสนอจะต้องระบุยี่ห้อและรุ่นของผลิตภัณฑ์ที่เสนอ พร้อมทั้งต้องมี Catalog หรือ Brochure ที่ชัดเจนได้ และทำเครื่องหมาย พร้อมหัวข้อกำกับอุปกรณ์ที่เสนอไว้อย่างชัดเจน

4.3 คอมพิวเตอร์ที่เสนอต้องสามารถใช้งานกับระบบไฟฟ้า 220V AC 50Hz ตามมาตรฐานของประเทศไทยได้ โดยไม่ต้องใช้อุปกรณ์แปลงระบบไฟฟ้า และปลั๊กไฟของอุปกรณ์ทุกรายการจะต้องเป็นชนิด 3 ขา (มีขาสำหรับสายดิน)

4.4 ในกรณีที่มีการส่งมอบคอมพิวเตอร์ต่างไปจากที่กำหนดไว้หรือที่เสนอมา จะต้องมียกข้อยกเว้นจากบริษัทผู้ผลิต หรือจากบริษัทสาขาของผู้ผลิตในต่างประเทศ หรือจากบริษัทสาขาของผู้ผลิตในประเทศไทย หรือตัวแทนจำหน่ายในประเทศไทย ว่าเป็นรุ่นใหม่และจะต้องมีคุณสมบัติไม่ต่ำกว่าที่กำหนดไว้หรือที่เสนอมา ทั้งนี้ รพม. สงวนสิทธิ์ที่จะรับมอบหรือไม่ก็ได้

4.5 กรณีฮาร์ดดิสก์ของคอมพิวเตอร์ตามข้อ 2.1 - 2.6 เสียในส่วนของฮาร์ดแวร์ ผู้ให้เช่าจะต้องมีบริการกู้ข้อมูลที่สูญหายตามการร้องขอของ รพม. รวมทั้งต้องจัดเตรียมฮาร์ดดิสก์ชุดใหม่เพื่อทดแทนชุดเดิมที่เสียหายภายหลังการกู้ข้อมูลกลับมาแล้ว ทั้งนี้การกู้ข้อมูลต้องกระทำโดยบริษัทที่มีห้องปฏิบัติการมาตรฐาน (Clean Room) และมีการรับรองมาตรฐาน ISO 9000 Series หรือเทียบเท่า ซึ่งผู้ให้เช่าต้องแจ้งชื่อบริษัทดังกล่าวให้ รพม. พิจารณาทุกครั้งก่อนการดำเนินการ โดยไม่มีการคิดค่าใช้จ่ายใด ๆ เพิ่มเติม

4.6 กรณีที่มีการเคลื่อนย้ายคอมพิวเตอร์และอุปกรณ์ที่ได้ติดตั้งตามสัญญาฯ นี้ รพม. มีสิทธิ์ที่จะแจ้งให้ผู้ให้เช่ามาดำเนินการให้ รพม. ได้ตลอดอายุสัญญา โดยไม่มีการคิดค่าใช้จ่ายใด ๆ เพิ่มเติม

4.7 คอมพิวเตอร์ที่เสนอต้องมีคุณลักษณะเฉพาะอย่างน้อยตาม ภาคผนวก ก.

#### 5. ขอบเขตของงานที่จะดำเนินการเช่า

5.1 ผู้ให้เช่าจะต้องส่งมอบและติดตั้งเครื่องคอมพิวเตอร์ ณ อาคารสำนักงานของ รพม. ได้แก่ อาคาร 1 อาคาร 2 อาคาร 4 และสถานีรถไฟฯ ซึ่งอยู่ในเขตกรุงเทพมหานครและปริมณฑล รายละเอียดตาม ภาคผนวก ข.

5.2 ผู้ให้เช่าจะต้องจัดให้มีการประชุมเริ่มงาน (Kickoff Meeting) เพื่อทำความเข้าใจ และนำเสนอแผนการดำเนินงานในการติดตั้ง ให้พิจารณาก่อนการดำเนินการติดตั้งจริงภายใน 15 วัน นับถัดจากวันที่ลงนามในสัญญา

5.3 ผู้ให้เช่าต้องเข้ามาสำรวจคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ทั้งหมดของ รพม. เพื่อจัดทำ Asset Inventory โดยบันทึกรายละเอียดที่ระบุชื่อผู้ใช้งาน สังกัด สถานที่ติดตั้ง และ MAC Address เป็นอย่างน้อย และส่งเป็นเอกสารอิเล็กทรอนิกส์ให้แก่ผู้ควบคุมงานของฝ่ายเทคโนโลยีสารสนเทศ (ฟทท.) ภายใน 30 วัน นับถัดจากวันที่การตรวจรับเสร็จสิ้น

 /5.4 ผู้ให้เช่า...

5.4 ผู้ให้เช่าต้องจัดเตรียมเครื่องคอมพิวเตอร์ตามข้อ 2.1 - 2.3 และข้อ 2.6 พร้อมติดตั้งระบบปฏิบัติการและซอฟต์แวร์ที่เกี่ยวข้องรายการละ 2 เครื่อง โดยนำส่งและติดตั้งที่ ฝพท. เพื่อให้ส่วนงานที่เกี่ยวข้องกับการพัฒนาระบบได้ทำการทดสอบการใช้งานร่วมกับระบบสารสนเทศของ รพม. ที่มีและใช้งานอยู่

5.5 ผู้ให้เช่าต้องจัดเตรียมเครื่องคอมพิวเตอร์ตามข้อ 2.1 - 2.3 และข้อ 2.6 พร้อมติดตั้งระบบปฏิบัติการและซอฟต์แวร์ที่เกี่ยวข้องรายการละ 1 เครื่อง โดยนำส่งและติดตั้งที่ ฝพท. เพื่อจัดทำเครื่องต้นแบบ (Master)

5.6 ผู้ให้เช่าต้องจัดให้มีการตรวจสอบรายละเอียดคุณลักษณะเฉพาะ (Specification) ของเครื่องคอมพิวเตอร์ที่เสนอ โดยแจ้งกำหนดการตรวจสอบรายละเอียดดังกล่าวล่วงหน้าอย่างน้อย 1 วัน และผู้ให้เช่าต้องจัดเตรียมสถานที่ รองรับสิ่งอำนวยความสะดวกและอุปกรณ์ต่าง ๆ ที่เกี่ยวข้องสำหรับการตรวจสอบรายละเอียดคุณลักษณะเฉพาะก่อนนำเครื่องคอมพิวเตอร์มาติดตั้งตามสถานที่ที่ รพม. กำหนด โดยเป็นค่าใช้จ่ายของผู้ให้เช่าเอง

5.7 ผู้ให้เช่าต้องดำเนินการติดตั้ง กำหนดค่าต่าง ๆ พร้อมทั้งโอนย้ายข้อมูลระหว่างเครื่องคอมพิวเตอร์ของพนักงานที่ใช้งานอยู่เดิมไปยังเครื่องคอมพิวเตอร์ใหม่ที่ได้มาตามสัญญา

5.8 ผู้ให้เช่าต้องจัดทำสติกเกอร์ที่ระบุชื่อบริษัทผู้ให้เช่า เลขที่สัญญา ระยะเวลาการรับประกัน หมายเลขโทรศัพท์สำหรับการแจ้งปัญหา และหมายเลขของเครื่องติดให้กับคอมพิวเตอร์ทุกรายการให้ชัดเจน

5.9 ผู้ให้เช่าจะต้องส่งมอบ Master Image ให้กับ รพม. โดยจัดเก็บลงใน External Drive แบบ USB ความจุไม่น้อยกว่า 2 TB จำนวน 3 ชุด

5.10 ผู้ให้เช่าต้องจัดหาอุปกรณ์แปลงสัญญาณ USB-C เป็น VGA สำหรับสำรองใช้งาน จำนวน 20 ชุด

5.11 ผู้ให้เช่าต้องจัดหา Media Card Reader ที่สามารถใช้งานกับ Memory Card แบบ Secure Digital (SD) หรือ microSD หรือดีกว่า สำหรับสำรองใช้งาน จำนวน 20 ชุด




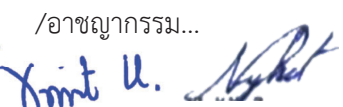
5.12 ภายหลังจากติดตั้ง ผู้ให้เช่าต้องจัดทำเอกสารการติดตั้งคอมพิวเตอร์ทุกรายการ ที่ระบุรายละเอียดต่าง ๆ เช่น ยี่ห้อ/ ประเภทของอุปกรณ์/ รุ่น/ หมายเลขของเครื่อง/ สถานที่ติดตั้ง/ MAC Address ฯลฯ ส่งมอบให้ รพม. จำนวน 1 ชุด (พร้อมส่งมอบเป็น Microsoft Excel File) ภายใน 15 วัน นับถัดจากวันที่การตรวจรับเสร็จสิ้น

5.13 ผู้ให้เช่าจะต้องจัดส่งเจ้าหน้าที่ที่มีความรู้ความสามารถด้านการซ่อมแซม แก๊ซ และบำรุงรักษาเครื่องคอมพิวเตอร์หรือมีความรู้อื่นที่เกี่ยวข้องมาประจำที่สำนักงานใหญ่ของ รพม. ตลอดอายุสัญญา จำนวนไม่น้อยกว่า 2 คน ด้วยค่าใช้จ่ายของผู้ให้เช่าเอง โดยไม่คิดค่าใช้จ่ายใด ๆ เพิ่มเติมจากสัญญาเช่าทั้งสิ้น โดยมีข้อกำหนด ดังนี้

5.13.1 เจ้าหน้าที่จะต้องมีวุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรี โดยผู้ให้เช่าจะต้องแจ้งชื่อ-นามสกุล ประวัติการทำงาน และวุฒิการศึกษาของเจ้าหน้าที่ดังกล่าว ให้ รพม. พิจารณาภายในวันตรวจรับ โดยกรอกรายละเอียดตาม ภาคผนวก ค. และจะต้องเริ่มปฏิบัติงานตั้งแต่วันที่ถัดจากวันที่การตรวจรับเสร็จสิ้น

5.13.2 ผู้ให้เช่าจะต้องดำเนินการให้สำนักงานตำรวจแห่งชาติตรวจประวัติอาชญากรรมด้วยลายนิ้วมือของเจ้าหน้าที่หลักที่จะเข้ามาปฏิบัติงานที่ รพม. ด้วยค่าใช้จ่ายของผู้ให้เช่าเอง และแสดงหลักฐานการดำเนินการดังกล่าวให้ รพม. ทราบภายใน 30 วัน นับถัดจากวันที่การตรวจรับเสร็จสิ้น

เจ้าหน้าที่ของผู้ให้เช่าจะต้องไม่มีประวัติอาชญากรรมเกี่ยวกับความผิดทางอาญา เว้นแต่โทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ ทั้งนี้ รพม. ไม่อนุญาตให้เจ้าหน้าที่ที่มีประวัติ

  
/อาชญากรรม...  
  

อาชญากรรมเกี่ยวกับความผิดอาญาดังกล่าวเข้าทำงาน หากพบว่าเจ้าหน้าที่ของผู้ให้เข้ามีประวัติอาชญากรรมดังกล่าว ผู้ให้เข้าจะต้องเปลี่ยนตัวเจ้าหน้าที่คนดังกล่าว แล้วจัดหาเจ้าหน้าที่มาปฏิบัติงานแทน ภายใน 10 วันทำการ

5.13.3 เจ้าหน้าที่จะต้องปฏิบัติงานในวันจันทร์ - วันศุกร์ ตั้งแต่เวลา 08.00 - 17.00 น. (ระหว่างเวลา 12.00 - 13.00 น. เป็นเวลาพักรับประทานอาหารกลางวัน) เว้นวันหยุดที่ รฟม. กำหนดไว้ รวมเวลาทำงานวันละ 8 ชั่วโมง

5.13.4 เจ้าหน้าที่จะต้องจัดทำรายงานสรุปเวลาเข้า-ออกการปฏิบัติงาน ด้วยวิธีการลงเวลาตามแบบฟอร์มของผู้ให้เข้าเองหรือตามที่ รฟม. กำหนด เป็นประจำทุกเดือนแล้วจัดส่งให้ผู้ควบคุมงานของ ผทท. ภายในวันที่ 15 ของเดือนถัดไป

5.13.5 เจ้าหน้าที่จะต้องจัดทำรายงานการปฏิบัติงานตามสัญญา ประจำเดือน ส่งให้ผู้ควบคุมงานของ ผทท. ภายในวันที่ 15 ของเดือนถัดไป

5.13.6 ผู้ให้เข้าจะต้องจัดหาอุปกรณ์ และเครื่องมือสำหรับการปฏิบัติงาน ซ่อมแซม แก้ไขและบำรุงรักษา เครื่องคอมพิวเตอร์ รวมทั้งอุปกรณ์ที่เกี่ยวข้องให้แก่เจ้าหน้าที่ที่มาปฏิบัติงานตามความเหมาะสม

5.13.7 ผู้ให้เข้าต้องจัดหาบัตรน้ำมันเชื้อเพลิงมูลค่าไม่น้อยกว่า 3,600 บาทต่อเดือน สำหรับใช้เติมน้ำมันพาหนะ เพื่อใช้ในการปฏิบัติงานของ รฟม. โดยบัตรดังกล่าวต้องสามารถสะสมยอดเงินคงเหลือในแต่ละเดือนได้

5.13.8 กรณีผู้ให้เข้าต้องการเปลี่ยนตัวเจ้าหน้าที่หลัก จะต้องกรอกรายละเอียดตาม ภาคผนวก ค. และทำเป็นหนังสือยื่นต่อคณะกรรมการตรวจรับพัสดุฯ เพื่อพิจารณาก่อนการเปลี่ยนตัวเจ้าหน้าที่หลักดังกล่าว

5.13.9 รฟม. มีสิทธิ์ขอเปลี่ยนตัวเจ้าหน้าที่ของผู้ให้เข้าได้ตลอดอายุสัญญา เมื่อ รฟม. เห็นว่าไม่มีความเหมาะสมที่จะปฏิบัติหน้าที่ ซึ่งผู้ให้เข้าจะต้องหาเจ้าหน้าที่มาทดแทนภายใน 10 วันทำการ โดยระหว่างการจัดหาเจ้าหน้าที่มาทดแทนนั้น ผู้ให้เข้าจะต้องจัดให้มีเจ้าหน้าที่สำรองเข้ามาปฏิบัติงานที่ รฟม. จนกว่าผู้ให้เข้าจะสามารถจัดหาเจ้าหน้าที่มาทดแทนได้

5.13.10 กรณีเจ้าหน้าที่ปฏิบัติงานไม่ครบชั่วโมงการทำงาน ผู้ให้เข้ายินยอมให้ปรับในอัตรา 125 บาท ต่อชั่วโมง (เศษของชั่วโมงให้นับเป็นหนึ่งชั่วโมง) โดยค่าปรับข้างต้นผู้ให้เข้ายินยอมให้ รฟม. หักจากค่าเช่าหรือเงินอื่น ๆ ที่ค้างจ่ายได้ทันที โดย รฟม. ไม่ต้องบอกสงวนสิทธิ์แต่อย่างใด

5.13.11 กรณีเจ้าหน้าที่ไม่มาปฏิบัติงาน หรือมีความจำเป็นต้องหยุดงาน หรือไม่สามารถมาปฏิบัติงานได้ ผู้ให้เข้าต้องจัดส่งเจ้าหน้าที่ที่มีความรู้ความสามารถตามที่ รฟม. กำหนดไว้มาปฏิบัติงานแทนภายในเวลาไม่เกิน 08.00 น. ของวันทำการนั้น โดยจะต้องแจ้งให้ผู้ควบคุมงานของ ผทท. ทราบล่วงหน้าก่อนเจ้าหน้าที่จะเข้ามาปฏิบัติงานทดแทน หากผู้ให้เข้าไม่สามารถจัดหาเจ้าหน้าที่มาปฏิบัติงานทดแทนได้ หรือมาแล้วแต่ไม่สามารถปฏิบัติงานได้ ผู้ให้เข้ายินยอมให้ปรับในอัตรา 1,000 บาทต่อวัน โดยค่าปรับข้างต้นผู้ให้เข้ายินยอมให้ รฟม. หักจากค่าเช่าหรือเงินอื่น ๆ ที่ค้างจ่ายได้ทันที โดย รฟม. ไม่ต้องบอกสงวนสิทธิ์แต่อย่างใด

5.14 ราคาเช่าที่เสนอให้รวมถึง ค่าเช่าใช้ทั้งฮาร์ดแวร์ ซอฟต์แวร์ ค่าการให้คำปรึกษา ค่าใช้จ่ายในการบำรุงรักษา และซ่อมแซมแก้ไข ค่าบริการ ค่าดำเนินการติดตั้ง ค่าขนย้าย ค่าเก็บรักษาทั้งก่อนและหลังการติดตั้ง (โกดังและ/หรือคลังสินค้า) และอุปกรณ์อื่นใดที่ไม่ได้กล่าวถึง ซึ่งจำเป็นต้องมี เพื่อให้สามารถใช้งานเข้ากับระบบคอมพิวเตอร์และระบบเครือข่ายสื่อสารข้อมูลของ รฟม. ที่มีและใช้งานอยู่ได้อย่างมีประสิทธิภาพ โดยไม่มีการคิดค่าใช้จ่ายใดๆ เพิ่มเติมทั้งสิ้น

/6. กำหนดเวลา...

Joint U.

**6. กำหนดเวลาส่งมอบพัสดุ**

ผู้ให้เช่าต้องติดตั้งคอมพิวเตอร์ตามสถานที่ที่กำหนดให้แล้วเสร็จและมีหนังสือส่งมอบงานให้ รพม. ภายใน 60 วัน นับถัดจากวันที่ลงนามในสัญญา (ผู้ให้เช่าต้องเป็นผู้จัดหาบุคลากรและอุปกรณ์ประกอบ พร้อมทั้งเครื่องมือที่จำเป็น ในการดำเนินการต่าง ๆ ที่เกี่ยวข้อง โดยผู้ให้เช่าเป็นผู้ออกค่าใช้จ่ายเองทั้งสิ้น)

**7. ระยะเวลาการเช่า**

ระยะเวลาเช่าทั้งสิ้น 36 เดือน นับถัดจากวันคณะกรรมการตรวจรับพัสดุฯ ได้รับมอบพัสดุทั้งหมดหรือบางส่วน หรือบางรายการจากผู้ให้เช่าเรียบร้อยแล้ว

**8. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ**

ในการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ รพม. จะพิจารณาตัดสินโดยใช้หลักเกณฑ์ราคา

**9. วงเงินงบประมาณ/วงเงินที่ได้รับจัดสรร**

27,165,600 บาท (ยี่สิบเจ็ดล้านหนึ่งแสนหกหมื่นห้าพันหกร้อยบาทถ้วน) (รวมภาษีมูลค่าเพิ่ม)

**10. งวดงานและการจ่ายเงิน**

การชำระค่าเช่าคอมพิวเตอร์ตามสัญญานี้ รพม. จะชำระค่าเช่าเป็นรายเดือน ซึ่งเป็นค่าเช่าที่รวมภาษีมูลค่าเพิ่ม ตลอดจนภาษีอากรอื่น ๆ และค่าใช้จ่ายทั้งปวงแล้วเมื่อผู้ให้เช่าได้ส่งมอบเครื่องคอมพิวเตอร์ทั้งหมดหรือบางส่วนหรือ บางรายการและคณะกรรมการตรวจรับพัสดุฯ ได้รับมอบพัสดุฯ ดังกล่าวเรียบร้อยแล้ว

การคิดค่าเช่าในเดือนแรกหรือเดือนอื่น ๆ ที่มีการเช่าไม่ครบเดือน ให้คำนวณค่าเช่าเริ่มตั้งแต่วันที่ถัดจากวันที่ รพม. ได้รับมอบเครื่องคอมพิวเตอร์ทั้งหมด หรือบางส่วน หรือบางรายการจากผู้ให้เช่า จนถึงวันสุดท้ายของเดือนนั้น โดยให้ คำนวณค่าเช่าเป็นรายวัน ซึ่งรวมภาษีมูลค่าเพิ่มแล้วหารด้วยจำนวน 30 วัน

**11. การฝึกอบรม**

11.1 ผู้ให้เช่าต้องจัดฝึกอบรม/สัมมนาให้แก่เจ้าหน้าที่ของ รพม. จำนวน 2 หลักสูตร โดยจะต้องดำเนินการ ภายใน 180 วัน นับถัดจากวันที่ตรวจรับแล้วเสร็จ ดังนี้

11.1.1 หลักสูตรสำหรับผู้ใช้งาน จำนวน 1 หลักสูตร จำนวนไม่น้อยกว่า 100 คน และเป็นเวลาไม่น้อยกว่า 0.5 วัน โดยมีเนื้อหาเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์ หรือการใช้งานซอฟต์แวร์สำนักงานเบื้องต้น

11.1.2 หลักสูตรสำหรับผู้ดูแลระบบ จำนวน 1 หลักสูตร จำนวนไม่น้อยกว่า 5 คน และเป็นเวลาไม่น้อยกว่า 1 วัน โดยมีเนื้อหาเกี่ยวกับการแก้ไขปัญหาการใช้งานเครื่องคอมพิวเตอร์ หรือการแก้ไขปัญหาการใช้งานซอฟต์แวร์ สำนักงาน

11.2 ผู้ให้เช่าต้องเป็นผู้รับผิดชอบและจัดเตรียมวิทยากร เอกสาร อาหารว่าง เครื่องดื่ม อาหารกลางวัน และ อุปกรณ์ที่จำเป็นในการฝึกอบรม/สัมมนา จำนวนไม่น้อยกว่าผู้เข้าร่วมอบรม ทั้งนี้ เอกสารจะต้องเป็นภาษาไทยเว้นแต่ กรณีที่ต้องการอธิบายด้วยภาษาทางเทคนิคหรือภาษาเฉพาะให้ใช้ภาษาอังกฤษได้

 The bottom of the page contains several handwritten signatures and stamps. On the left, there is a signature that appears to be 'Asat A.'. In the center, there is a signature that appears to be 'Jint U. Jint'. On the right, there is a signature that appears to be 'Jint U. Jint' and a stamp that says '/12.อัตราค่าปรับ...'. There are also some other illegible signatures and marks.

## 12. อัตราค่าปรับ

12.1 ในกรณีผู้ให้เช่าไม่สามารถปฏิบัติตามเงื่อนไขการติดตั้งและส่งมอบ หรือการส่งมอบคอมพิวเตอร์ล่าช้ากว่าที่กำหนดไว้ในสัญญาในบางรายการหรือทั้งหมด หรือส่งมอบแล้วแต่มีคุณสมบัติไม่ถูกต้องตามรายละเอียดและคุณลักษณะเฉพาะที่กำหนด หรือยังไม่สามารถใช้งานได้ รพม. มีสิทธิ์บอกเลิกสัญญาได้ ในกรณีที่ รพม. ไม่ใช้สิทธิ์บอกเลิกสัญญา ผู้ให้เช่ายินยอมให้ รพม. ปรับในอัตราร้อยละ 0.20 (ศูนย์จุดสองศูนย์) ของราคาค่าเช่าตลอดอายุของสัญญาต่อคอมพิวเตอร์ที่ยังไม่ได้ส่งมอบนั้น ๆ เป็นรายวัน (เศษของวันให้นับเป็นหนึ่งวัน) โดยการปรับจะนับถัดจากวันครบกำหนดส่งมอบตามสัญญาจนถึงวันที่ผู้ให้เช่าได้นำคอมพิวเตอร์มาติดตั้งและส่งมอบให้แก่ รพม. จนถูกต้องครบถ้วนแล้ว ทั้งนี้ ค่าปรับข้างต้นผู้ให้เช่ายินยอมให้ รพม. หักจากค่าเช่าหรือเงินอื่น ๆ (รวมภาษีมูลค่าเพิ่ม) ที่ค้างจ่ายได้ทันที โดย รพม. ไม่ต้องบอกสงวนสิทธิ์แต่อย่างใด

12.2 ในกรณีที่ รพม. ใช้สิทธิ์บอกเลิกสัญญาผู้ให้เช่ายินยอมให้ รพม. คิดค่าปรับตามข้อ 12.1 โดยนับถัดจากวันครบกำหนดส่งมอบตามสัญญาจนถึงวันบอกเลิกสัญญาและผู้ให้เช่ายินยอมให้ รพม. รับผิดชอบประกันสัญญาเป็นจำนวนทั้งหมดหรือแต่บางส่วนก็ได้ แล้วแต่ รพม. จะเห็นสมควร

12.3 ในกรณีผู้ให้เช่าไม่สามารถปฏิบัติตามเงื่อนไขตามข้อ 13.1 ผู้ให้เช่ายินยอมให้ รพม. ปรับเป็นในอัตรา 27,200 บาท (สองหมื่นเจ็ดพันสองร้อยบาทถ้วน) เป็นรายวัน (เศษของวันให้นับเป็นหนึ่งวัน) โดยค่าปรับข้างต้นผู้ให้เช่ายินยอมให้ รพม. หักจากค่าเช่าหรือเงินอื่น ๆ (รวมภาษีมูลค่าเพิ่ม) ที่ค้างจ่ายได้ทันที โดย รพม. ไม่ต้องบอกสงวนสิทธิ์แต่อย่างใด

12.4 ในกรณีผู้ให้เช่าไม่สามารถปฏิบัติตามเงื่อนไขตามข้อ 13.2 - 13.3 ผู้ให้เช่ายินยอมให้ รพม. ปรับในอัตรา 3,000 บาท (สามพันบาทถ้วน) ต่อเหตุการณ์นั้น ๆ เป็นรายวัน (เศษของวันให้นับเป็นหนึ่งวัน) นับตั้งแต่วันที่เจ้าหน้าที่ของ รพม. ได้แจ้งให้ผู้ให้เช่ารับทราบถึงความชำรุดบกพร่อง จนกว่าผู้ให้เช่าจะดำเนินการดังกล่าวแล้วเสร็จหรือจนกว่า รพม. เห็นว่าผู้ให้เช่าไม่อาจจัดหาคอมพิวเตอร์อื่นแทนได้และบอกเลิกสัญญา โดยค่าปรับข้างต้นผู้ให้เช่ายินยอมให้ รพม. หักจากค่าเช่าหรือเงินอื่น ๆ (รวมภาษีมูลค่าเพิ่ม) ที่ค้างจ่ายได้ทันที โดย รพม. ไม่ต้องบอกสงวนสิทธิ์แต่อย่างใด

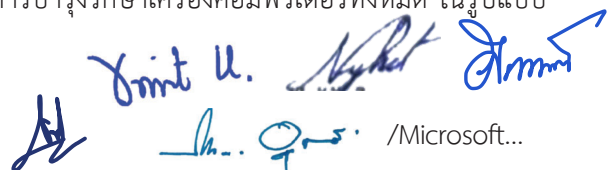
12.5 กรณีผู้ให้เช่าไปเช่าช่วงหรือจ้างช่วงงานแต่บางส่วนโดยฝ่าฝืนความตามข้อ 14.11 ผู้ให้เช่ายินยอมให้ รพม. ปรับในอัตราร้อยละ 10 (สิบ) ของวงเงินค่าเช่าตามสัญญา ทั้งนี้ ไม่ตัดสิทธิ์ รพม. ในการบอกเลิกสัญญา โดยค่าปรับข้างต้นผู้ให้เช่ายินยอมให้ รพม. หักจากค่าเช่าหรือเงินอื่น ๆ (รวมภาษีมูลค่าเพิ่ม) ที่ค้างจ่ายได้ทันที โดย รพม. ไม่ต้องบอกสงวนสิทธิ์แต่อย่างใด

## 13. การกำหนดระยะเวลารับประกันความชำรุดบกพร่อง

### 13.1 การบำรุงรักษา

13.1.1 ผู้ให้เช่าจะต้องรับผิดชอบการบำรุงรักษาเครื่องคอมพิวเตอร์ตลอดระยะเวลาของสัญญา จำนวน 3 ครั้ง เป็นอย่างน้อย ซึ่งแต่ละครั้งต้องมีระยะเวลาห่างกันอย่างเหมาะสม โดยผู้ให้เช่าจะต้องเสนอแผนการบำรุงรักษาให้คณะกรรมการตรวจรับพัสดุฯ พิจารณาในที่ประชุมเริ่มงาน (Kickoff Meeting) ตามข้อ 5.2 ทั้งนี้ แผนดังกล่าวคณะกรรมการตรวจรับพัสดุฯ สามารถปรับเปลี่ยนได้ตามความเหมาะสมตลอดอายุสัญญา

13.1.2 ผู้ให้เช่าต้องส่งตารางเวลาการบำรุงรักษาตามข้อ 13.1.1 มาให้คณะกรรมการตรวจรับพัสดุฯ พิจารณาก่อนดำเนินการ 5 วันทำการ พร้อมทั้งส่งรายงานผลการบำรุงรักษาเครื่องคอมพิวเตอร์ทั้งหมด ในรูปแบบ

 Jint U. /Microsoft...



Microsoft Excel File โดยจัดเก็บลงในระบบจัดเก็บข้อมูลที่ รพม. กำหนด ภายใน 10 วันทำการ หลังจากที่ผู้ให้เข้าได้ทำการบำรุงรักษาเสร็จเรียบร้อยแล้ว โดย รพม. ไม่เสียค่าใช้จ่ายใด ๆ เพิ่มเติมทั้งสิ้น

### 13.1.3 การบำรุงรักษาจะต้องตรวจสอบอย่างน้อยตามรายการต่อไปนี้

- (1) ทำความสะอาดโดยการดูดฝุ่นเครื่องคอมพิวเตอร์
- (2) ตรวจสอบอุปกรณ์ ความเรียบร้อย ความครบถ้วนของเครื่องคอมพิวเตอร์ หากมีการชำรุดเสียหาย หรือสูญหาย ผู้ให้เข้าจะต้องทำรายงานให้ รพม. ทราบทันทีที่มิฉะนั้น รพม. ถือว่าผู้ให้เข้าไม่ตั้งใจที่จะเรียกจ่ายค่าเสียหายใด ๆ เพิ่มเติมทั้งสิ้น
- (3) ตรวจสอบจำนวนเครื่องคอมพิวเตอร์ ผู้ครอบครอง สถานที่ติดตั้ง (ล่าสุด) และตรวจสอบการติดตั้งโปรแกรมอื่น ๆ ตามที่ รพม. กำหนด

### 13.2 การซ่อมแซมแก้ไข

ผู้ให้เข้ายอมรับประกันความชำรุดบกพร่องหรือขัดข้องของคอมพิวเตอร์ รวมทั้งซอฟต์แวร์ป้องกันไวรัสตามสัญญาที่ ตลอดจนอายุสัญญานับถัดจากวันที่ รพม. ดำเนินการตรวจรับเรียบร้อยแล้วไปจนถึงสิ้นสุดระยะเวลาตามสัญญา ถ้าภายในระยะเวลาดังกล่าว คอมพิวเตอร์ รวมทั้งซอฟต์แวร์ป้องกันไวรัสชำรุดบกพร่อง หรือใช้งานไม่ได้ทั้งหมดหรือแต่บางส่วน และความชำรุดบกพร่องดังกล่าวมิใช่ความผิดของ รพม. ผู้ให้เข้าจะต้องจัดให้เจ้าหน้าที่ที่มีความรู้ ความชำนาญมาดำเนินการซ่อมแซมแก้ไขให้แล้วเสร็จสามารถใช้งานได้ติดตั้งเดิมภายในวันทำการถัดไป นับแต่วันที่ รพม. ได้แจ้ง ผู้ให้เข้ารับทราบทางโทรศัพท์ โทรศัพท์เคลื่อนที่ โทรสาร จดหมายอิเล็กทรอนิกส์ (E-mail) หรือช่องทางอื่น ๆ ที่ รพม. กำหนด

### 13.3 ความรับผิดชอบต่อความเสียหาย

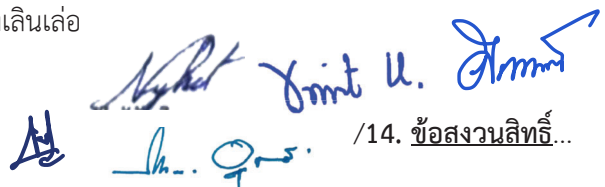
13.3.1 ในกรณีที่ไม่สามารถซ่อมแซมคอมพิวเตอร์ให้แล้วเสร็จภายในกำหนดระยะเวลาตามข้อ 13.2 ผู้ให้เข้าต้องจัดหาคอมพิวเตอร์ที่มีคุณสมบัติไม่ต่ำกว่าของเดิมหรือดีกว่าและมีสภาพดี มาให้ รพม. ใช้งานทดแทนจนกว่าจะซ่อมแซมคอมพิวเตอร์ที่ชำรุดแล้วเสร็จสามารถใช้งานได้ติดตั้งเดิม ในกรณีที่ผู้ให้เข้าต้องนำคอมพิวเตอร์ที่เสียหรือชำรุดไปซ่อมแซมแก้ไขภายนอก ผู้ให้เข้าต้องนำคอมพิวเตอร์ดังกล่าวกลับมาคืนภายใน 10 วันทำการ โดยอะไหล่หรือวัสดุอุปกรณ์ที่นำมาใช้ในการซ่อมแซมแก้ไข หรือให้ใช้เป็นการชั่วคราว หรือที่นำมาเปลี่ยนให้ใหม่นั้น จะต้องมียุทธศาสตร์ที่ต่ำกว่าของเดิม สำหรับกรณีการเปลี่ยนวัสดุอุปกรณ์ให้ใหม่ วัสดุอุปกรณ์นั้นจะต้องเป็นของใหม่ที่ไม่เคยถูกใช้งานมาก่อนและไม่เป็นของเก่าเก็บ

13.3.2 ในกรณีคอมพิวเตอร์ชำรุดจนไม่สามารถซ่อมแซมได้ หรือชำรุดบกพร่องในปัญหาเดิมซ้ำเป็นจำนวน 3 ครั้ง ภายในระยะเวลา 1 เดือน ผู้ให้เข้าจะต้องจัดหาคอมพิวเตอร์ที่มีคุณสมบัติไม่ต่ำกว่าของเดิมหรือดีกว่า และมีสภาพดีมาเปลี่ยนทดแทนอย่างถาวรภายใน 10 วันทำการ โดยผู้ให้เข้าต้องทำหนังสือแจ้งขอเปลี่ยนคอมพิวเตอร์เป็นลายลักษณ์อักษรเพื่อให้ รพม. พิจารณาและต้องได้รับการเห็นชอบก่อนการเปลี่ยนคอมพิวเตอร์ดังกล่าว

13.3.3 ความเสียหายต่อเครื่องคอมพิวเตอร์ในข้อ 2.3 - 2.8 ให้ครอบคลุมถึงความเสียหายทุกชนิดดังต่อไปนี้

- ความเสียหายอันเกิดจากภัยธรรมชาติต่างๆ เช่น ไฟฟ้า น้ำท่วม เป็นต้น
- ความเสียหายอันเกิดจากไฟไหม้ ไฟฟ้าลัดวงจร ระเบิด
- ความเสียหายอันเกิดจากอุบัติเหตุ เครื่องตกหล่น หรือกระแทก
- ความเสียหายอันเกิดจากเครื่องโดนน้ำ หรือของเหลวหกใส่
- เครื่องสูญหายเนื่องจากการโจรกรรมแบบมีหลักฐานพิสูจน์ได้

ยกเว้น กรณีเหตุที่เกิดจากความประมาทเลินเล่อ

 /14. ข้อสงวนสิทธิ์...

#### 14. ข้อสงวนสิทธิ์

14.1 เมื่อสิ้นสุดสัญญาเช่าหากการจัดหาหรือติดตั้งเครื่องใหม่ของ รพม. ยังดำเนินการไม่แล้วเสร็จ รพม. มีสิทธิ์ใช้คอมพิวเตอร์ทั้งหมด รวมถึงเจ้าหน้าที่ตามข้อ 5.13 จะต้องปฏิบัติงานต่อไปอีก 2 เดือน นับจากวันที่สัญญาสิ้นสุดลง โดย รพม. ไม่เสียค่าใช้จ่ายใด ๆ เพิ่มเติมทั้งสิ้น

14.2 หากพ้นระยะเวลาตามข้อ 14.1 ในกรณีที่ รพม. มีความจำเป็นต้องเช่าคอมพิวเตอร์ทั้งหมด หรือบางส่วน หรือบางรายการต่อเมื่อสิ้นสุดสัญญา ผู้ให้เช่ายินยอมให้เช่าต่อโดยใช้ราคาอ้างอิงจากสัญญาเช่าเดิม ทั้งนี้ ราคาเช่าดังกล่าวจะไม่เกินร้อยละ 50 ของราคาเช่าเดิม

14.3 กรณีผู้ให้เช่าประสงค์ที่จะขายคอมพิวเตอร์ตามข้อ 2.1 - 2.6 ผู้ให้เช่ายินยอมให้สิทธิ์ รพม. หรือพนักงาน/ลูกจ้าง ของ รพม. ซื้อคอมพิวเตอร์ดังกล่าว (ทั้งชุด) พร้อมเครื่องสำรองไฟฟ้า โดยราคารวมภาษีมูลค่าเพิ่มแล้วเป็นจำนวนเงิน 1,500 บาท (หนึ่งพันห้าร้อยบาทถ้วน)

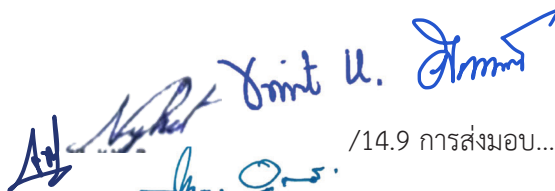
14.4 กรณีผู้ให้เช่าประสงค์ที่จะขายคอมพิวเตอร์ตามข้อ 2.7 - 2.8 ผู้ให้เช่ายินยอมให้สิทธิ์ รพม. หรือพนักงาน/ลูกจ้าง ของ รพม. ซื้อคอมพิวเตอร์ดังกล่าว (ทั้งชุด) โดยราคารวมภาษีมูลค่าเพิ่มแล้วเป็นจำนวนเงิน 500 บาท (ห้าร้อยบาทถ้วน)

14.5 ผู้ให้เช่าจะต้องทำลายข้อมูลที่อยู่ภายในหน่วยเก็บข้อมูล (Hard disk) ของเครื่องคอมพิวเตอร์จนไม่สามารถกู้ข้อมูลกลับมาได้ โดยต้องดำเนินการให้เป็นไปตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของ รพม.

14.6 ภายหลังจากที่ผู้ให้เช่าได้ดำเนินการตามข้อ 14.1 - 14.5 เรียบร้อยแล้ว ผู้ให้เช่าจะต้องขนย้ายคอมพิวเตอร์กลับคืนไปภายใน 60 วัน นับถัดจากวันที่ รพม. ได้แจ้ง ผู้ให้เช่ารับทราบทางโทรศัพท์ โทรศัพท์เคลื่อนที่ โทรสาร จดหมายอิเล็กทรอนิกส์ (E-mail) หรือช่องทางอื่น ๆ ที่ รพม. กำหนด โดยในระยะเวลาดังกล่าว รพม. จะไม่รับผิดชอบต่อความเสียหายหรือการสูญหายที่อาจเกิดขึ้นกับเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ทั้งหมด ทั้งนี้ ผู้ให้เช่าจะต้องรับผิดชอบต่อค่าใช้จ่ายในการขนย้ายด้วย

14.7 ผู้ให้เช่าและ/หรือเจ้าหน้าที่ของผู้ให้เช่า ที่เข้าถึงระบบเทคโนโลยีสารสนเทศของ รพม. ต้องรับทราบและปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของ รพม. ตาม ภาคผนวก ง. และจะต้องรักษาความลับต่าง ๆ ที่ได้จากการปฏิบัติงาน โดยห้ามมิให้ผู้ให้เช่า และ/หรือเจ้าหน้าที่ของผู้ให้เช่านำข้อมูลส่วนหนึ่งส่วนใดหรือทั้งหมดที่ได้จากการปฏิบัติงานใน รพม. ไปทำซ้ำ เผยแพร่ หรือวิเคราะห์ประมวลผลเพื่อการอื่นใด ไม่ว่าการกระทำดังกล่าวจะเป็นการหาผลประโยชน์หรือไม่ก็ตาม หาก รพม. ตรวจสอบผู้ให้เช่าต้องชดเชยค่าเสียหายเป็นจำนวนเงินไม่น้อยกว่าค่าเช่าทั้งหมดที่กำหนดไว้ในสัญญา ทั้งนี้ ผู้ให้เช่าและ/หรือเจ้าหน้าที่ของผู้ให้เช่าต้องลงนามในสัญญาการเก็บรักษาข้อมูลไว้เป็นความลับ (Non-Disclosure Agreement) ตาม ภาคผนวก จ. ก่อนเริ่มปฏิบัติงานตามรูปแบบที่ รพม. กำหนด

14.8 การใช้ประโยชน์ในเครื่องเช่าตามสัญญานี้ ผู้ให้เช่ายินยอมให้อยู่ภายใต้การจัดการและการควบคุมดูแลของ รพม. โดยสิ้นเชิง นอกจาก รพม. จะใช้ในการปฏิบัติงานของ รพม. เองแล้ว รพม. อาจให้ผู้อื่นมาใช้เครื่องเช่านี้ได้โดยอยู่ภายใต้การควบคุมดูแลของ รพม.

  
/14.9 การส่งมอบ...

14.9 การส่งมอบคอมพิวเตอร์ที่ไม่ตรงตามสัญญา รฟม. ทรงไว้ซึ่งสิทธิ์ที่จะไม่รับคอมพิวเตอร์นั้น ในกรณีนี้ ผู้ให้เช่าต้องรับนำกลับคืนไปแก้ไขให้ถูกต้องตามสัญญาและนำมาส่งมอบให้ใหม่ด้วยค่าใช้จ่ายของผู้ให้เช่าเอง และระยะเวลาที่เสียไปเพราะเหตุดังกล่าว ผู้ให้เช่าจะนำมาอ้างเพื่อขอตหรือลดค่าปรับ หรือขอขยายเวลาในภายหลังไม่ได้

14.10 ผู้ให้เช่าจะต้องส่งบุคลากรเข้าร่วมการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness) เพื่อสร้างความตระหนักที่เหมาะสม ทบทวนนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และขั้นตอนปฏิบัติของ รฟม. ตามที่ รฟม. กำหนด

14.11 ผู้ให้เช่าจะต้องไม่เอางานทั้งหมดหรือแต่บางส่วนไปเช่าช่วงหรือจ้างช่วงอีกทอดหนึ่ง เว้นแต่การเช่าช่วงหรือจ้างช่วงงานแต่บางส่วนที่ได้รับอนุญาตเป็นหนังสือจากคณะกรรมการตรวจรับพัสดุฯ แล้ว การที่ รฟม. ได้อนุญาตให้เช่าช่วงหรือจ้างช่วงงานแต่บางส่วนดังกล่าวนี้ ไม่เป็นเหตุให้ผู้ให้เช่าหลุดพ้นจากความรับผิดหรือพ้นหน้าที่ และผู้ให้เช่าจะยังคงต้องรับผิดในความผิดและความประมาทเลินเล่อของผู้ให้เช่าช่วง หรือของตัวแทนหรือลูกจ้างของผู้ให้เช่าช่วงนั้นทุกประการ (หากมี)

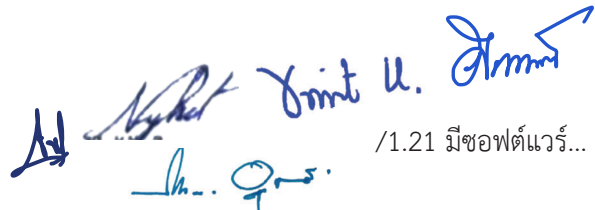
*Joint U. [Signature]*  
*[Signature]*

ภาคผนวก ก.  
รายละเอียดคุณลักษณะเฉพาะ

At Joint U. Stmmt  
K. S. - In. Q. S.

**1. เครื่องคอมพิวเตอร์ สำหรับงานสำนักงาน มีคุณสมบัติอย่างน้อยดังนี้**

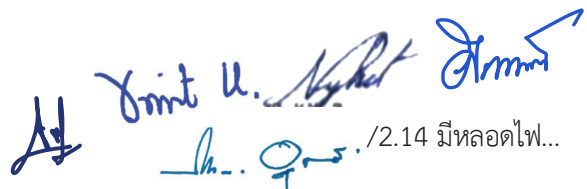
- 1.1 มีหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า 4 Core และ 8 Tread รุ่นล่าสุดที่มีในท้องตลาด และมีเทคโนโลยีเพิ่มสัญญาณนาฬิกาได้ในกรณีที่ต้องใช้ความสามารถในการประมวลผลสูง (Turbo Boost หรือ Max Boost) โดยมีความเร็วสัญญาณนาฬิกาสูงสุด ไม่น้อยกว่า 4.5 GHz
- 1.2 หน่วยประมวลผลกลาง (CPU) มีหน่วยความจำแบบ Cache Memory ขนาดไม่น้อยกว่า 12 MB
- 1.3 มีหน่วยความจำหลักแบบ DDR5 หรือดีกว่า ขนาดไม่น้อยกว่า 8 GB จำนวน 1 หน่วย
- 1.4 มี Hard Disk ชนิด M.2 SSD ที่มี Interface แบบ PCIe NVMe ความจุไม่น้อยกว่า 1TB
- 1.5 มีหน่วยควบคุมการแสดงผลแบบ Integrated HD Graphics หรือดีกว่าโดยใช้หน่วยความจำ ร่วมกับหน่วยความจำหลักได้
- 1.6 มีช่องเชื่อมต่อแบบ VGA และ/หรือ Display Port และ/หรือ HDMI จำนวนรวมไม่น้อยกว่า 2 ช่อง
- 1.7 มีช่องเชื่อมต่อระบบเครือข่าย Gigabit Ethernet จำนวน 1 หน่วย
- 1.8 มีช่องเชื่อมต่อตามมาตรฐาน USB 2.0 USB 3.0 และ USB-C จำนวนรวมไม่น้อยกว่า 6 ช่อง
- 1.9 มีระบบเครือข่ายไร้สายแบบติดตั้งภายใน และรองรับมาตรฐาน IEEE802.11ax (WIFI-6E) หรือดีกว่า
- 1.10 มี Bluetooth 5.2 หรือดีกว่า ติดตั้งภายในเครื่อง
- 1.11 มีระบบเสียงพร้อมลำโพงติดตั้งภายในเครื่อง
- 1.12 ตัวเครื่องเป็นแบบ Ultra Small PC หรือ Mini PC หรือ micro PC หรือเทียบเท่า ที่มีระบบเตือนการเปิดฝาเครื่อง (Intrusion switch)
- 1.13 มีอุปกรณ์แปลงไฟฟ้า (Adapter) ขนาดไม่น้อยกว่า 65 Watt สำหรับต่อใช้งานกับไฟฟ้า 220V
- 1.14 มีอุปกรณ์สำหรับติดตั้งตัวเครื่องบริเวณด้านหลังจอภาพ (VESA Mount) หรือมีฐานวางตัวเครื่องแนวตั้ง (Vertical Stand)
- 1.15 มีหลอดไฟแบบ LED ด้านหน้าเครื่องสำหรับแสดงสถานะการเปิด/ปิดเครื่อง และการทำงานของ Hard Disk ได้เป็นอย่างดี
- 1.16 มี Security Chip ตามมาตรฐาน TPM 2.0 (Trusted Platform Module) หรือดีกว่า
- 1.17 เครื่องคอมพิวเตอร์ที่เสนอต้องมีระบบ Online Support ที่ให้บริการ Download Driver ผ่านช่องทาง Internet จากผู้ผลิต
- 1.18 มีจอภาพแบบ LED (Wide Screen) ขนาดไม่น้อยกว่า 23 นิ้ว ที่มีลำโพงติดตั้งอยู่ภายในและมีช่องเชื่อมต่อแบบ VGA หรือ Display Port หรือ HDMI ที่ความละเอียดสูงสุดไม่น้อยกว่า 1920 x 1080 Pixels โดยขาตั้งสามารถปรับระดับสูง-ต่ำได้
- 1.19 มีแป้นพิมพ์ ที่มีตัวอักษรภาษาไทยและภาษาอังกฤษติดบนปุ่มกดอย่างถาวร เชื่อมต่อแบบ USB 2.0 หรือดีกว่า โดยเป็นยี่ห้อเดียวกับผลิตภัณฑ์ที่เสนอ
- 1.20 มี Laser Mouse เชื่อมต่อแบบ USB 2.0 หรือดีกว่า โดยเป็นยี่ห้อเดียวกับผลิตภัณฑ์ที่เสนอ พร้อมแผ่นรอง

  
/1.21 มีซอฟต์แวร์...

- 1.21 มีซอฟต์แวร์ระบบปฏิบัติการ Windows 11 Professional 64bit แบบ OEM License ที่สามารถดาวน์โหลดมาเป็น Windows 10 Professional 64bit ได้ โดยจะต้องมีลิขสิทธิ์ถูกต้องตามกฎหมายจากเจ้าของผลิตภัณฑ์และเป็นสิทธิ์การใช้งานของ รพม.
- 1.22 มีการรับประกันความชำรุดบกพร่องของเครื่องคอมพิวเตอร์และอุปกรณ์ทุกชิ้นส่วนทั้งค่าแรง อะไหล่ โดยเข้ามาทำการแก้ไข/ซ่อมแซม ณ ที่ติดตั้งเครื่อง (On-Site Service) จากบริษัทผู้ผลิต ภายในวันทำการถัดไป (Next Business Day)
- 1.23 มีเอกสารการรับรองคุณภาพเครื่องคอมพิวเตอร์ตามมาตรฐานที่เกี่ยวข้องกับผลิตภัณฑ์ ด้านต่าง ๆ ดังต่อไปนี้
  - 1) มาตรฐานด้านระบบคุณภาพ ISO 9001 และ ISO 14001 Series
  - 2) มาตรฐานด้านการประหยัดพลังงาน Energy Star และ EPEAT ระดับ Gold
  - 3) มาตรฐานด้านความปลอดภัย UL และ CE
  - 4) มาตรฐานด้านสิ่งแวดล้อม RoHS และ TCO
  - 5) มาตรฐานด้านการแพร่กระจายคลื่นแม่เหล็กไฟฟ้า FCC

## **2. เครื่องคอมพิวเตอร์ สำหรับงานกราฟิก มีคุณสมบัติอย่างน้อยดังนี้**

- 2.1 มีหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า 14 Core และ 20 Tread รุ่นล่าสุดที่มีในท้องตลาด และมีเทคโนโลยีเพิ่มสัญญาณนาฬิกาได้ในกรณีที่ต้องใช้ความสามารถในการประมวลผลสูง (Turbo Boost หรือ Max Boost) โดยมีความเร็วสัญญาณนาฬิกาสูงสุด ไม่น้อยกว่า 5.0 GHz
- 2.2 หน่วยประมวลผลกลาง (CPU) มีหน่วยความจำแบบ Cache Memory ขนาดไม่น้อยกว่า 24 MB
- 2.3 มีหน่วยความจำหลักแบบ DDR5 หรือดีกว่า ขนาดไม่น้อยกว่า 16 GB
- 2.4 มี Hard Disk ชนิด M.2 SSD ที่มี Interface แบบ PCIe NVMe ความจุไม่น้อยกว่า 1TB
- 2.5 มีหน่วยควบคุมการแสดงผลแบบ GDDR6 ที่มีหน่วยความจำไม่น้อยกว่า 4 GB (แยกจากหน่วยความจำหลัก) โดยรองรับการเชื่อมต่อแบบ Display port หรือ mini-Display Port หรือ HDMI เป็นอย่างน้อย
- 2.6 มี DVD +/- RW แบบติดตั้งภายในหรือภายนอกเครื่อง จำนวน 1 หน่วย
- 2.7 มีช่องเชื่อมต่อระบบเครือข่าย Gigabit Ethernet จำนวน 1 หน่วย
- 2.8 มีช่องเชื่อมต่อตามมาตรฐาน USB 2.0 USB 3.0 และ USB-C จำนวนรวมไม่น้อยกว่า 6 ช่อง
- 2.9 มีระบบเครือข่ายไร้สายแบบติดตั้งภายใน และรองรับมาตรฐาน IEEE802.11ax (WIFI-6E) หรือดีกว่า
- 2.10 มี Bluetooth 5.2 หรือดีกว่า ติดตั้งภายในเครื่อง
- 2.11 มีระบบเสียงพร้อมลำโพงติดตั้งภายในเครื่อง
- 2.12 ตัวเครื่องเป็นแบบ Small Form Factor (SFF) หรือเทียบเท่า ที่มีระบบเตือนการเปิดฝาเครื่อง (Intrusion switch)
- 2.13 มีระบบจ่ายกำลังไฟฟ้าแบบติดตั้งภายในตัวเครื่อง ขนาดไม่น้อยกว่า 180 Watt

  
/2.14 มีหลอดไฟ...

- 2.14 มีหลอดไฟแบบ LED ด้านหน้าเครื่องสำหรับแสดงสถานะการเปิด/ปิดเครื่อง และการทำงานของ Hard Disk ได้เป็นอย่างดี
- 2.15 มี Security Chip ตามมาตรฐาน TPM 2.0 (Trusted Platform Module) หรือดีกว่า
- 2.16 เครื่องคอมพิวเตอร์ที่เสนอต้องมีระบบ Online Support ที่ให้บริการ Download Driver ผ่านช่องทาง Internet จากผู้ผลิต
- 2.17 มีจอภาพแบบ LED (Wide Screen) ขนาดไม่น้อยกว่า 23 นิ้ว ที่มีลำโพงติดตั้งอยู่ภายในและมีช่องเชื่อมต่อแบบ VGA หรือ Display Port หรือ HDMI ที่ความละเอียดสูงสุดไม่น้อยกว่า 1920 x 1080 Pixels โดยขาตั้งสามารถปรับระดับสูง-ต่ำได้
- 2.18 มีแป้นพิมพ์ ที่มีตัวอักษรภาษาไทยและภาษาอังกฤษติดบนปุ่มกดอย่างถาวร เชื่อมต่อแบบ USB 2.0 หรือดีกว่า โดยเป็นยี่ห้อเดียวกับผลิตภัณฑ์ที่เสนอ
- 2.19 มี Laser Mouse เชื่อมต่อแบบ USB 2.0 หรือดีกว่า โดยเป็นยี่ห้อเดียวกับผลิตภัณฑ์ที่เสนอ พร้อมแผ่นรอง
- 2.20 มีซอฟต์แวร์ระบบปฏิบัติการ Windows 11 Professional 64bit แบบ OEM License ที่สามารถดาวน์โหลดเป็น Windows 10 Professional 64bit ได้ โดยจะต้องมีลิขสิทธิ์ถูกต้องตามกฎหมายจากเจ้าของผลิตภัณฑ์และเป็นสิทธิ์การใช้งานของ รพม.
- 2.21 มีการรับประกันความชำรุดบกพร่องของเครื่องคอมพิวเตอร์และอุปกรณ์ทุกชิ้นส่วนทั้งค่าแรง อะไหล่ โดยเข้ามาทำการแก้ไข/ซ่อมแซม ณ ที่ติดตั้งเครื่อง (On-Site Service) จากบริษัทผู้ผลิต ภายในวันทำการถัดไป (Next Business Day)
- 2.22 มีเอกสารการรับรองคุณภาพเครื่องคอมพิวเตอร์ตามมาตรฐานที่เกี่ยวข้องกับผลิตภัณฑ์ ด้านต่าง ๆ ดังต่อไปนี้
  - 1) มาตรฐานด้านระบบคุณภาพ ISO 9001 และ ISO 14001 Series
  - 2) มาตรฐานด้านการประหยัดพลังงาน Energy Star และ EPEAT ระดับ Gold
  - 3) มาตรฐานด้านความปลอดภัย UL และ CE
  - 4) มาตรฐานด้านสิ่งแวดล้อม RoHS และ TCO
  - 5) มาตรฐานด้านการแพร่กระจายคลื่นแม่เหล็กไฟฟ้า FCC

### 3. เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานสำนักงาน แบบที่ 1 มีคุณสมบัติอย่างน้อยดังนี้

- 3.1 มีหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า 12 Core และ 16 Tread รุ่นล่าสุดที่มีในท้องตลาด และมีเทคโนโลยีเพิ่มสัญญาณนาฬิกาได้ในกรณีที่ต้องใช้ความสามารถในการประมวลผลสูง (Turbo Boost หรือ Max Boost) โดยมีความเร็วสัญญาณนาฬิกาสูงสุด ไม่น้อยกว่า 4.7 GHz
- 3.2 หน่วยประมวลผลกลาง (CPU) มีหน่วยความจำแบบ Cache Memory ขนาดไม่น้อยกว่า 12 MB
- 3.3 มีจอภาพขนาดไม่เกิน 14 นิ้ว แบบ FHD Anti-Glare ที่ความสว่าง 400 nits และมีความละเอียดสูงสุด ไม่น้อยกว่า 1920 x 1080 Pixels
- 3.4 มีหน่วยความจำหลักแบบ DDR5 หรือดีกว่า ขนาดไม่น้อยกว่า 16 GB



Joint U. 

/3.5 มี Hard Disk...

- 3.5 มี Hard Disk ชนิด M.2 SSD ที่มี Interface แบบ PCIe NVMe ความจุไม่น้อยกว่า 1 TB
- 3.6 มีหน่วยควบคุมการแสดงผลแบบ GDDR6 หรือดีกว่า ที่มีหน่วยความจำไม่น้อยกว่า 2 GB โดยแยกจากหน่วยความจำหลัก
- 3.7 มีระบบเสียงพร้อมลำโพงติดตั้งภายในเครื่อง
- 3.8 มีกล้อง Webcam แบบ FHD ที่สามารถใช้ยืนยันตัวบุคคลได้ โดยติดตั้งภายในตัวเครื่อง พร้อมแผ่นเลื่อนเพื่อปิดกล้องเมื่อไม่ใช้งาน
- 3.9 มีเซ็นเซอร์ยืนยันตัวบุคคลด้วยลายนิ้วมือ (Fingerprint Reader)
- 3.10 มีช่องเชื่อมต่อระบบเครือข่าย Gigabit Ethernet จำนวน 1 ช่อง
- 3.11 มีระบบเครือข่ายไร้สายแบบติดตั้งภายใน และรองรับมาตรฐาน IEEE802.11ax (WIFI-6E) หรือดีกว่า
- 3.12 มีช่องเชื่อมต่อตามมาตรฐาน USB 2.0 USB 3.0 และ USB-C จำนวนรวมไม่น้อยกว่า 3 ช่อง
- 3.13 มีช่องเชื่อมต่อแบบ HDMI
- 3.14 มีแป้นพิมพ์ ที่มีตัวอักษรภาษาไทยและภาษาอังกฤษติดบนปุ่มกดอย่างถาวร
- 3.15 มี Mouse ไร้สายที่ใช้ตัวรับสัญญาณขนาดเล็ก (Unifying) โดยเป็นยี่ห้อเดียวกับผลิตภัณฑ์ที่เสนอ พร้อมแผ่นรอง
- 3.16 มีแบตเตอรี่แบบ Li-Polymer ขนาดไม่น้อยกว่า 50 Whr พร้อมซอฟต์แวร์ที่สามารถตรวจสอบประสิทธิภาพของแบตเตอรี่ได้และเป็นยี่ห้อเดียวกับผลิตภัณฑ์ที่เสนอ
- 3.17 มีอุปกรณ์แปลงไฟฟ้า (Adapter) แบบ USB-C สำหรับต่อใช้งานกับไฟฟ้า 220V
- 3.18 มีน้ำหนักของเครื่องไม่เกิน 1.8 กิโลกรัม โดยไม่รวมน้ำหนักของแบตเตอรี่
- 3.19 มี Security Chip หรือ Firmware ตามมาตรฐาน TPM 2.0 (Trusted Platform Module) หรือดีกว่า
- 3.20 เครื่องคอมพิวเตอร์ที่เสนอต้องมีระบบ Online Support ที่ให้บริการ Download Driver ผ่านช่องทาง Internet จากผู้ผลิต
- 3.21 มีกระเป๋าสำหรับใส่เครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ แบบสะพายหลัง
- 3.22 มีซอฟต์แวร์ระบบปฏิบัติการ Windows 11 Professional 64bit แบบ OEM License ที่สามารถดาวน์โหลดเป็น Windows 10 Professional 64bit ได้ โดยจะต้องมีลิขสิทธิ์ถูกต้องตามกฎหมายจากเจ้าของผลิตภัณฑ์และเป็นสิทธิ์การใช้งานของ รพม.
- 3.23 มีการรับประกันความชำรุดบกพร่องของเครื่องคอมพิวเตอร์และอุปกรณ์ทุกชิ้นส่วนทั้งค่าแรง อะไหล่โดยเข้ามาทำการแก้ไข/ซ่อมแซม ณ ที่ติดตั้งเครื่อง (On-Site Service) จากบริษัทผู้ผลิต ภายในวันทำการถัดไป (Next Business Day)
- 3.24 มีเอกสารการรับรองคุณภาพเครื่องคอมพิวเตอร์ตามมาตรฐานที่เกี่ยวข้องกับผลิตภัณฑ์ ด้านต่าง ๆ ดังต่อไปนี้
  - 1) มาตรฐานด้านระบบคุณภาพ ISO 9001 และ ISO 14001 Series
  - 2) มาตรฐานด้านการประหยัดพลังงาน Energy Star และ EPEAT ระดับ Gold
  - 3) มาตรฐานด้านความปลอดภัย UL และ CE





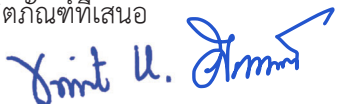
/4) มาตรฐาน...



- 4) มาตรฐานด้านสิ่งแวดล้อม RoHS และ TCO
- 5) มาตรฐานด้านการแพร่กระจายคลื่นแม่เหล็กไฟฟ้า FCC
- 6) มาตรฐานด้านความทนทาน MIL-STD 810H

**4. เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานสำนักงาน แบบที่ 2 มีคุณสมบัติอย่างน้อยดังนี้**

- 4.1 มีหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า 12 Core และ 16 Tread รุ่นล่าสุดที่มีในท้องตลาด และมีเทคโนโลยีเพิ่มสัญญาณนาฬิกาได้ในกรณีที่ต้องใช้ความสามารถในการประมวลผลสูง (Turbo Boost หรือ Max Boost) โดยมีความเร็วสัญญาณนาฬิกาสูงสุด ไม่น้อยกว่า 4.7 GHz
- 4.2 หน่วยประมวลผลกลาง (CPU) มีหน่วยความจำแบบ Cache Memory ขนาดไม่น้อยกว่า 12 MB
- 4.3 มีจอภาพขนาดไม่เกิน 14 นิ้ว แบบ FHD Anti-Glare ที่ความสว่าง 400 nits และมีความละเอียดสูงสุด ไม่น้อยกว่า 1920 x 1080 Pixels
- 4.4 มีหน่วยความจำหลักแบบ DDR5 หรือดีกว่า ขนาดไม่น้อยกว่า 16 GB
- 4.5 มี Hard Disk ชนิด M.2 SSD ที่มี Interface แบบ PCIe NVMe ความจุไม่น้อยกว่า 1 TB
- 4.6 มีหน่วยควบคุมการแสดงผลแบบ GDDR6 หรือดีกว่า ที่มีหน่วยความจำไม่น้อยกว่า 2 GB โดยแยกจากหน่วยความจำหลัก
- 4.7 มีระบบเสียงพร้อมลำโพงติดตั้งภายในเครื่อง
- 4.8 มีกล้อง Webcam แบบ FHD ที่สามารถใช้ยืนยันตัวบุคคลได้ โดยติดตั้งภายในตัวเครื่อง พร้อมแผ่นเลื่อนเพื่อปิดกล้องเมื่อไม่ใช้งาน
- 4.9 มีเซ็นเซอร์ยืนยันตัวบุคคลด้วยลายนิ้วมือ (Fingerprint Reader)
- 4.10 มีช่องเชื่อมต่อระบบเครือข่าย Gigabit Ethernet จำนวน 1 ช่อง
- 4.11 มีระบบเครือข่ายไร้สายแบบติดตั้งภายใน และรองรับมาตรฐาน IEEE802.11ax (WIFI-6E) หรือดีกว่า
- 4.12 มีช่องเชื่อมต่อตามมาตรฐาน USB 2.0 USB 3.0 และ USB-C จำนวนรวมไม่น้อยกว่า 3 ช่อง
- 4.13 มีช่องเชื่อมต่อแบบ HDMI
- 4.14 มีแป้นพิมพ์ ที่มีตัวอักษรภาษาไทยและภาษาอังกฤษติดบนปุ่มกดอย่างถาวร
- 4.15 มีแบตเตอรี่แบบ Li-Polymer ขนาดไม่น้อยกว่า 50 Whr พร้อมซอฟต์แวร์ที่สามารถตรวจสอบประสิทธิภาพของแบตเตอรี่ได้และเป็นยี่ห้อเดียวกับผลิตภัณฑ์ที่เสนอ
- 4.16 มีอุปกรณ์แปลงไฟฟ้า (Adapter) แบบ USB-C สำหรับต่อใช้งานกับไฟฟ้า 220V
- 4.17 มีน้ำหนักของเครื่องไม่เกิน 1.8 กิโลกรัม โดยไม่รวมน้ำหนักของแบตเตอรี่
- 4.18 มี Security Chip หรือ Firmware ตามมาตรฐาน TPM 2.0 (Trusted Platform Module) หรือดีกว่า
- 4.19 เครื่องคอมพิวเตอร์ที่เสนอต้องมีระบบ Online Support ที่ให้บริการ Download Driver ผ่านช่องทาง Internet จากผู้ผลิต
- 4.20 มี Mouse และ Keyboard ไร้สายที่มีตัวอักษรภาษาไทยและภาษาอังกฤษติดบนปุ่มกดอย่างถาวร โดยใช้ตัวรับสัญญาณขนาดเล็ก (Unifying) ร่วมกัน ทั้งนี้ ต้องเป็นยี่ห้อเดียวกับผลิตภัณฑ์ที่เสนอ

    
/4.21 มีจอภาพ...

- 4.21 มีจอภาพแบบ LED (Wide Screen) ขนาดไม่น้อยกว่า 23 นิ้ว ที่มีลำโพงติดตั้งอยู่ภายในและมีช่องเชื่อมต่อแบบ VGA หรือ Display Port หรือ HDMI ที่ความละเอียดสูงสุดไม่น้อยกว่า 1920 x 1080 Pixels โดยขาตั้งสามารถปรับระดับสูง-ต่ำได้
- 4.22 มีกระเป๋าสำหรับใส่เครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ แบบสะพายหลัง
- 4.23 มีซอฟต์แวร์ระบบปฏิบัติการ Windows 11 Professional 64bit แบบ OEM License ที่สามารถดาวน์โหลดเป็น Windows 10 Professional 64bit ได้ โดยจะต้องมีลิขสิทธิ์ถูกต้องตามกฎหมายจากเจ้าของผลิตภัณฑ์และเป็นสิทธิ์การใช้งานของ รพม.
- 4.24 มีการรับประกันความชำรุดบกพร่องของเครื่องคอมพิวเตอร์และอุปกรณ์ทุกชิ้นส่วนทั้งค่าแรง อะไหล่โดยเข้ามาทำการแก้ไข/ซ่อมแซม ณ ที่ติดตั้งเครื่อง (On-Site Service) จากบริษัทผู้ผลิต ภายในวันทำการถัดไป (Next Business Day)
- 4.25 มีเอกสารการรับรองคุณภาพเครื่องคอมพิวเตอร์ตามมาตรฐานที่เกี่ยวข้องกับผลิตภัณฑ์ ด้านต่าง ๆ ดังต่อไปนี้
  - 1) มาตรฐานด้านระบบคุณภาพ ISO 9001 และ ISO 14001 Series
  - 2) มาตรฐานด้านการประหยัดพลังงาน Energy Star และ EPEAT ระดับ Gold
  - 3) มาตรฐานด้านความปลอดภัย UL และ CE
  - 4) มาตรฐานด้านสิ่งแวดล้อม RoHS และ TCO
  - 5) มาตรฐานด้านการแพร่กระจายคลื่นแม่เหล็กไฟฟ้า FCC
  - 6) มาตรฐานด้านความทนทาน MIL-STD 810H

**5. เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานกราฟิก มีคุณสมบัติอย่างน้อยดังนี้**

- 5.1 มีหน่วยประมวลผลกลาง (CPU) ซีพียู M3 แบบ 8 Core หรือดีกว่า
- 5.2 มีหน่วยความจำหลัก ขนาดรวมไม่น้อยกว่า 16 GB
- 5.3 มี Hard Disk ชนิด Solid State Drive (SSD) ความจุไม่น้อยกว่า 1 TB หรือดีกว่า จำนวน 1 หน่วย
- 5.4 มีหน่วยควบคุมการแสดงผล Graphics (GPU) แบบ 10 core
- 5.5 มีระบบเสียงพร้อมลำโพงติดตั้งภายในเครื่อง
- 5.6 มีระบบเครือข่ายไร้สายแบบติดตั้งภายใน และรองรับมาตรฐาน IEEE802.11ax (WIFI-6E) หรือดีกว่า
- 5.7 มีช่องเชื่อมต่อตามมาตรฐาน Thunderbolt/ USB 4.0 หรือดีกว่า จำนวนรวมไม่น้อยกว่า 2 ช่อง
- 5.8 มีจอภาพขนาดไม่น้อยกว่า 15 นิ้ว มีความละเอียดสูงสุดไม่น้อยกว่า 2880 x 1864 Pixels
- 5.9 มีกล้องแบบ HD ความละเอียด 1080p
- 5.10 มีแท็คแพดแบบ Force Touch และสามารถใช้งานแบบ Multi-Touch ได้
- 5.11 มีแบตเตอรี่แบบ Li-Polymer ขนาดไม่น้อยกว่า 60 Whr
- 5.12 มีอุปกรณ์แปลงไฟฟ้า (Adapter) สำหรับต่อใช้งานกับไฟฟ้า 220V พร้อมสายชาร์จแบบ MagSafe
- 5.13 มีแป้นพิมพ์ ที่มีตัวอักษรภาษาไทยและภาษาอังกฤษติดบนปุ่มกดอย่างถาวร



/5.14 มี Mouse ...




- 5.14 มี Mouse ไร้สายที่เป็นยี่ห้อเดียวกับผลิตภัณฑ์ที่เสนอ
- 5.15 มีอุปกรณ์แปลงสัญญาณ (Adapter) แบบ USB-C เป็น Gigabit Ethernet
- 5.16 มีอุปกรณ์แปลงสัญญาณ (Adapter) แบบ USB-C เป็น HDMI และ USB
- 5.17 มีกระเป๋าสำหรับใส่เครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ แบบสะพายหลัง
- 5.18 มีซอฟต์แวร์ระบบปฏิบัติการ MacOS โดยซอฟต์แวร์จะต้องมีลิขสิทธิ์ถูกต้องตามกฎหมาย
- 5.19 เครื่องคอมพิวเตอร์ที่เสนอต้องมีระบบ Online Support ที่ให้บริการ Download Driver ผ่านช่องทาง Internet จากผู้ผลิต
- 5.20 มีการรับประกันความชำรุดบกพร่องของเครื่องคอมพิวเตอร์และอุปกรณ์ทุกชิ้นส่วนทั้งค่าแรง อะไหล่ โดยเข้ามาทำการแก้ไข/ซ่อมแซม ณ ที่ติดตั้งเครื่อง (On-Site Service) จากบริษัทผู้ผลิตและ/หรือผู้ให้เช่า ภายในวันทำการถัดไป (Next Business Day)

## 6. เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานประมวลผล มีคุณสมบัติอย่างน้อยดังนี้

- 6.1 มีหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า 14 Core และ 20 Tread รุ่นล่าสุดที่มีในท้องตลาด และมีเทคโนโลยีเพิ่มสัญญาณนาฬิกาได้ในกรณีที่ต้องใช้ความสามารถในการประมวลผลสูง (Turbo Boost หรือ Max Boost) โดยมีความเร็วสัญญาณนาฬิกาสูงสุด ไม่น้อยกว่า 5.2 GHz
- 6.2 หน่วยประมวลผลกลาง (CPU) มีหน่วยความจำแบบ Cache Memory ขนาดไม่น้อยกว่า 24 MB
- 6.3 มีจอภาพขนาดไม่เกิน 15.6 นิ้ว แบบ FHD Anti-Glare ที่ความสว่าง 400 nits และมีความละเอียดสูงสุดไม่น้อยกว่า 1920 x 1080 Pixels
- 6.4 มีหน่วยความจำหลักแบบ DDR5 หรือดีกว่า ขนาดไม่น้อยกว่า 32 GB
- 6.5 มี Hard Disk ชนิด M.2 SSD ที่มี Interface แบบ PCIe NVMe ความจุไม่น้อยกว่า 1 TB
- 6.6 มีหน่วยควบคุมการแสดงผลแบบ GDDR6 หรือดีกว่า ที่มีหน่วยความจำไม่น้อยกว่า 4 GB โดยแยกจากหน่วยความจำหลัก
- 6.7 มีระบบเสียงพร้อมลำโพงติดตั้งภายในเครื่อง
- 6.8 มีกล้อง Webcam แบบ FHD ที่สามารถใช้ยืนยันตัวบุคคลได้ โดยติดตั้งภายในตัวเครื่อง พร้อมแผ่นเลื่อนเพื่อปิดกล้องเมื่อไม่ใช้งาน
- 6.9 มีเซ็นเซอร์ยืนยันตัวบุคคลด้วยลายนิ้วมือ (Fingerprint Reader)
- 6.10 มีช่องเชื่อมต่อระบบเครือข่าย Gigabit Ethernet จำนวน 1 ช่อง
- 6.11 มีระบบเครือข่ายไร้สายแบบติดตั้งภายใน และรองรับมาตรฐาน IEEE802.11ax (WIFI-6E) หรือดีกว่า
- 6.12 มีช่องเชื่อมต่อตามมาตรฐาน USB 2.0 USB 3.0 และ USB-C จำนวนรวมไม่น้อยกว่า 3 ช่อง
- 6.13 มีช่องเชื่อมต่อแบบ HDMI
- 6.14 มีแป้นพิมพ์ ที่มีตัวอักษรภาษาไทยและภาษาอังกฤษติดบนปุ่มกดอย่างถาวร
- 6.15 มีแบตเตอรี่แบบ Li-Polymer ขนาดไม่น้อยกว่า 50 Whr พร้อมซอฟต์แวร์ที่สามารถตรวจสอบประสิทธิภาพของแบตเตอรี่ได้และเป็นยี่ห้อเดียวกับผลิตภัณฑ์ที่เสนอ



Print U.   
/6.16 มีอุปกรณ์...

- 6.16 มีอุปกรณ์แปลงไฟฟ้า (Adapter) แบบ USB-C สำหรับต่อใช้งานกับไฟฟ้า 220V
- 6.17 มีน้ำหนักของเครื่องไม่เกิน 1.8 กิโลกรัม โดยไม่รวมน้ำหนักของแบตเตอรี่
- 6.18 มี Security Chip หรือ Firmware ตามมาตรฐาน TPM 2.0 (Trusted Platform Module) หรือดีกว่า
- 6.19 เครื่องคอมพิวเตอร์ที่เสนอต้องมีระบบ Online Support ที่ให้บริการ Download Driver ผ่านช่องทาง Internet จากผู้ผลิต
- 6.20 มี Mouse และ Keyboard ไร้สายที่มีตัวอักษรภาษาไทยและภาษาอังกฤษติดบนปุ่มกดอย่างถาวร โดยใช้ตัวรับสัญญาณขนาดเล็ก (Unifying) ร่วมกัน ทั้งนี้ ต้องเป็นยี่ห้อเดียวกับผลิตภัณฑ์ที่เสนอ
- 6.21 มีจอภาพแบบ LED (Wide Screen) ขนาดไม่น้อยกว่า 23 นิ้ว ที่มีลำโพงติดตั้งอยู่ภายในและมีช่องเชื่อมต่อแบบ VGA หรือ Display Port หรือ HDMI ที่ความละเอียดสูงสุดไม่น้อยกว่า 1920 x 1080 Pixels โดยขาตั้งสามารถปรับระดับสูง-ต่ำได้
- 6.22 มีกระเป๋าสำหรับใส่เครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ แบบสะพายหลัง
- 6.23 มีซอฟต์แวร์ระบบปฏิบัติการ Windows 11 Professional 64bit แบบ OEM License ที่สามารถดาวน์โหลดเป็น Windows 10 Professional 64bit ได้ โดยจะต้องมีลิขสิทธิ์ถูกต้องตามกฎหมายจากเจ้าของผลิตภัณฑ์และเป็นสิทธิ์การใช้งานของ รพม.
- 6.24 มีการรับประกันความชำรุดบกพร่องของเครื่องคอมพิวเตอร์และอุปกรณ์ทุกชิ้นส่วนทั้งค่าแรง อะไหล่โดยเข้ามาทำการแก้ไข/ซ่อมแซม ณ ที่ติดตั้งเครื่อง (On-Site Service) จากบริษัทผู้ผลิต ภายในวันทำการถัดไป (Next Business Day)
- 6.25 มีเอกสารการรับรองคุณภาพเครื่องคอมพิวเตอร์ตามมาตรฐานที่เกี่ยวข้องกับผลิตภัณฑ์ ด้านต่าง ๆ ดังต่อไปนี้
  - 1) มาตรฐานด้านระบบคุณภาพ ISO 9001 และ ISO 14001 Series
  - 2) มาตรฐานด้านการประหยัดพลังงาน Energy Star และ EPEAT ระดับ Gold
  - 3) มาตรฐานด้านความปลอดภัย UL และ CE
  - 4) มาตรฐานด้านสิ่งแวดล้อม RoHS และ TCO
  - 5) มาตรฐานด้านการแพร่กระจายคลื่นแม่เหล็กไฟฟ้า FCC
  - 6) มาตรฐานด้านความทนทาน MIL-STD 810H

**7. เครื่องคอมพิวเตอร์แท็บเล็ต แบบที่ 1 มีคุณสมบัติอย่างน้อยดังนี้**

- 7.1 เป็นเครื่องคอมพิวเตอร์พกพาแบบหน้าจอสัมผัส พร้อมติดตั้งระบบปฏิบัติการ (OS) เวอร์ชันล่าสุด
- 7.2 มีหน่วยประมวลผลกลาง (CPU) ชิพ A14 แบบ 6 Core หรือดีกว่า
- 7.3 หน่วยควบคุมการแสดงผล Graphics (GPU) แบบ 4 Core
- 7.4 มีหน่วยจัดเก็บข้อมูล (Internal Storage) ความจุไม่น้อยกว่า 64 GB
- 7.5 มีเซ็นเซอร์ยืนยันตัวตนบุคคลด้วยลายนิ้วมือ (Touch ID) หรือดีกว่า
- 7.6 มีระบบเสียงพร้อมลำโพงติดตั้งภายในเครื่อง

 Joint U.   
/7.7 มีระบบ...

- 7.7 มีระบบเครือข่ายไร้สายที่รองรับมาตรฐาน IEEE 802.11ax (WIFI-6) หรือดีกว่า
- 7.8 รองรับ SIM card แบบ Nano-SIM หรือดีกว่า
- 7.9 มีจอภาพขนาดไม่น้อยกว่า 10.9 นิ้ว ชนิด Liquid Retina แบบ LED-Backlit Multi-Touch และมีความละเอียดสูงสุดไม่น้อยกว่า 2360 x 1640 Pixels เคลือบสารกันรอยนิ้วมือ และรองรับ Pencil
- 7.10 มีแบตเตอรี่แบบ Li-Polymer ความจุไม่น้อยกว่า 28 Whr และอุปกรณ์แปลงไฟฟ้า (Adapter) สำหรับต่อใช้งานกับไฟฟ้า 220V
- 7.11 มีปากกาหรือดินสอที่มีแบตเตอรี่ในตัวสามารถชาร์จไฟฟ้าผ่านสาย USB-C ได้ และเป็นยี่ห้อเดียวกับผลิตภัณฑ์ที่เสนอ
- 7.12 มี Smart Cover ที่สามารถใส่ปากกาหรือดินสอที่เสนอได้
- 7.13 มีฟิล์มกันรอยแบบกระจก ที่สามารถใช้งานกับผลิตภัณฑ์ที่เสนอได้
- 7.14 มีสายสัญญาณ USB-C หรือดีกว่า สำหรับรับ-ส่งข้อมูล และชาร์จไฟฟ้าได้ ความยาวไม่น้อยกว่า 1 เมตร
- 7.15 มีการรับประกันความชำรุดบกพร่องของเครื่องคอมพิวเตอร์และอุปกรณ์ทุกชิ้นส่วนทั้งค่าแรง อะไหล่ โดยเข้ามาทำการแก้ไข/ซ่อมแซม ณ ที่ติดตั้งเครื่อง (On-Site Service) จากบริษัทผู้ผลิตและ/หรือผู้ให้เช่า ภายในวันทำการถัดไป (Next Business Day)
- 7.16 มีการรับรองคุณภาพตามมาตรฐานด้านการประหยัดพลังงาน Energy Star

**8. เครื่องคอมพิวเตอร์แท็บเล็ต แบบที่ 2 มีคุณสมบัติอย่างน้อยดังนี้**

- 8.1 เป็นเครื่องคอมพิวเตอร์พกพาแบบหน้าจอสัมผัส พร้อมติดตั้งระบบปฏิบัติการ (OS) เวอร์ชันล่าสุด
- 8.2 มีหน่วยประมวลผลกลาง (CPU) ชิพ M2 แบบ 8 Core หรือดีกว่า
- 8.3 หน่วยควบคุมการแสดงผล Graphics (GPU) แบบ 10 Core
- 8.4 มีหน่วยความจำหลัก ขนาดรวมไม่น้อยกว่า 8 GB
- 8.5 มีหน่วยจัดเก็บข้อมูล (Internal Storage) ความจุไม่น้อยกว่า 256 GB
- 8.6 มีเซ็นเซอร์ยืนยันตัวตนบุคคลด้วยลายนิ้วมือ (Touch ID) หรือดีกว่า
- 8.7 มีระบบเสียงพร้อมลำโพงติดตั้งภายในเครื่อง
- 8.8 มีระบบเครือข่ายไร้สายที่รองรับมาตรฐาน IEEE 802.11ax (WI-FI 6E) หรือดีกว่า
- 8.9 รองรับการใช้งานเซลลูลาร์แบบ 5G และเทคโนโลยี eSIM
- 8.10 มีจอภาพขนาดไม่น้อยกว่า 11 นิ้ว ชนิด Liquid Retina แบบ LED-Backlit Multi-Touch และมีความละเอียดสูงสุดไม่น้อยกว่า 2360 x 1640 Pixels เคลือบสารกันรอยนิ้วมือ และรองรับ Pencil
- 8.11 มีแบตเตอรี่แบบ Li-Polymer ความจุไม่น้อยกว่า 28 Whr
- 8.12 มีปากกาหรือดินสอที่มีแบตเตอรี่ในตัวสามารถชาร์จไฟฟ้าแบบไร้สายเมื่อเชื่อมต่อกับคอมพิวเตอร์ที่เสนอได้ และเป็นยี่ห้อเดียวกับผลิตภัณฑ์ที่เสนอ
- 8.13 มี Smart Cover ที่สามารถใส่ปากกาหรือดินสอที่เสนอได้
- 8.14 มีฟิล์มกันรอยแบบกระจก ที่สามารถใช้งานกับผลิตภัณฑ์ที่เสนอได้

  /8.15 มีสายสัญญาณ...  

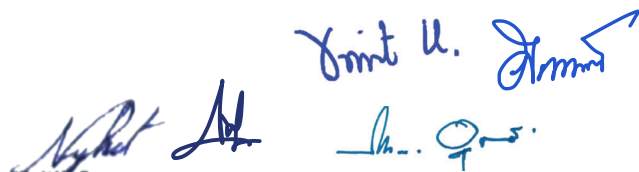

- 8.15 มีสายสัญญาณ USB-C หรือดีกว่า สำหรับรับ-ส่งข้อมูล และชาร์จไฟฟ้าได้ ความยาวไม่น้อยกว่า 1 เมตร
- 8.16 มีอุปกรณ์แปลงไฟฟ้า (Adapter) สำหรับต่อใช้งานกับไฟฟ้า 220V แบบ USB-C ขนาดไม่น้อยกว่า 20 วัตต์
- 8.17 มีหูฟังที่สามารถใช้งานกับผลิตภัณฑ์ที่เสนอได้
- 8.18 มีการรับประกันความชำรุดบกพร่องของเครื่องคอมพิวเตอร์และอุปกรณ์ทุกชิ้นส่วนทั้งค่าแรง อะไหล่ โดยเข้ามาทำการแก้ไข/ซ่อมแซม ณ ที่ติดตั้งเครื่อง (On-Site Service) จากบริษัทผู้ผลิตและ/หรือผู้ให้เช่า ภายในวันทำการถัดไป (Next Business Day)
- 8.19 มีการรับรองคุณภาพตามมาตรฐานด้านการประหยัดพลังงาน Energy Star

**9. เครื่องสำรองไฟฟ้า มีคุณสมบัติอย่างน้อยดังนี้**

- 9.1 เป็นเครื่องสำรองไฟฟ้า (UPS) แบบ Line Interactive ที่มีขนาดไม่น้อยกว่า 800VA/320W
- 9.2 มีช่องเสียบปลั๊กไฟฟ้า จำนวนไม่น้อยกว่า 3 ช่อง
- 9.3 มีระบบป้องกันแรงดันไฟตก (Under Voltage)
- 9.4 มีระบบป้องกันไฟเกิน (Over Voltage)
- 9.5 มีระบบป้องกันไฟกระชาก (Stabilizer)
- 9.6 มีระบบหยุดการทำงานแบตเตอรี่อัตโนมัติ (Low Voltage cut-off)
- 9.7 สามารถจ่ายไฟฟ้าสำรองได้ไม่น้อยกว่า 20 นาที
- 9.8 มีการรับประกันความชำรุดบกพร่องของเครื่องคอมพิวเตอร์และอุปกรณ์ทุกชิ้นส่วนทั้งค่าแรง อะไหล่ โดยเข้ามาทำการแก้ไข/ซ่อมแซม ณ ที่ติดตั้งเครื่อง (On-Site Service) จากบริษัทผู้ผลิต ภายในวันทำการถัดไป (Next Business Day)



**10. ซอฟต์แวร์ป้องกันไวรัส มีคุณสมบัติอย่างน้อยดังนี้**

- 10.1 เป็นซอฟต์แวร์ป้องกันไวรัส Kaspersky Endpoint Security for Business Select หรือดีกว่า
- 10.2 สามารถ Update Engine และ Virus Signature ผ่านช่องทาง Internet
- 10.3 สามารถบริหารจัดการผ่านช่องทางซอฟต์แวร์ Management ที่ติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายของ รพม. ได้โดยอัตโนมัติตลอดระยะเวลาของสัญญาเช่า



ภาคผนวก ข.

รายละเอียด สถานที่ติดตั้งนอกพื้นที่สำนักงาน รพม.

 Joint U.   


ภาคผนวก ข.

รายละเอียด สถานที่ติดตั้งนอกพื้นที่สำนักงาน รพม.

เครื่องคอมพิวเตอร์สำหรับงานสำนักงาน

ลำดับ	อาคารสำนักงาน/สถานี	จำนวน
1	อาคาร บริษัททางด่วนและรถไฟฟ้ากรุงเทพจำกัด (มหาชน) (อาคาร BEM)	13
2	สถานีรถไฟฟ้า สายเฉลิมรัชมงคล (สายสีน้ำเงิน) สถานีศูนย์วัฒนธรรมแห่งประเทศไทย	6
3	สถานีรถไฟฟ้า สายเฉลิมรัชมงคล (สายสีน้ำเงิน) สถานีลาดพร้าว	1
4	สถานีรถไฟฟ้า สายฉลองรัชธรรม (สายสีม่วง) สถานีคลองบางไผ่	13

เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานสำนักงาน แบบที่ 1

ลำดับ	อาคารสำนักงาน/สถานี	จำนวน
1	อาคาร บริษัททางด่วนและรถไฟฟ้ากรุงเทพจำกัด (มหาชน) (อาคาร BEM)	1

*Yint U. Thammak*  
*๒๕๖๕*



ภาคผนวก ค.

แบบฟอร์มรายละเอียดคุณสมบัติและประสบการณ์การทำงานของเจ้าหน้าที่

   
In. ๑๐๕.

### รายละเอียดคุณสมบัติและประสบการณ์การทำงานของผู้สมัคร

การเก็บรวบรวมข้อมูลส่วนบุคคลในเอกสารนี้ จัดทำขึ้นภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ด้วยวัตถุประสงค์เพื่อตรวจสอบข้อมูลของผู้สมัครที่เข้ามาปฏิบัติงานให้ รพม. ซึ่งเป็นการประมวลผลข้อมูลส่วนบุคคลเพื่อปฏิบัติตามสัญญา โดยเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็นจากเจ้าของข้อมูลส่วนบุคคล ซึ่ง รพม. จะจัดเก็บข้อมูลส่วนบุคคลจนกว่าจะสิ้นสุดข้อผูกพันตามสัญญา ทั้งนี้ หากมีข้อสอบถามหรือขอใช้สิทธิ์ของผู้สมัครสามารถติดต่อได้ที่ การรถไฟฯขนส่งมวลชนแห่งประเทศไทย สำนักงานใหญ่ เว็บไซต์ [www.mrta.co.th](http://www.mrta.co.th) โทรศัพท์ 0 2716 4000

ชื่อภาษาไทย (คำนำหน้าชื่อ ชื่อ นามสกุล) \_\_\_\_\_ วัน/เดือน/ปี เกิด (วันที่/เดือน/ปี พ.ศ.) \_\_\_\_\_ อายุ (ปี) \_\_\_\_\_ ถิ่นพำนักปัจจุบัน (กรุงเทพมหานคร ประเทศไทย)  
การศึกษา

ประกาศนียบัตรวิชาชีพชั้นสูง (ปวส.) (สาขาวิชา) \_\_\_\_\_ สถานศึกษา (วิทยาลัย / มหาวิทยาลัย / ฯลฯ ประเทศไทย) ปีที่จบการศึกษา (พ.ศ.)

ปริญญาตรี (สาขาวิชา) \_\_\_\_\_ สถานศึกษา (วิทยาลัย / มหาวิทยาลัย / ฯลฯ ประเทศไทย) ปีที่จบการศึกษา (พ.ศ.)

#### สถานะการทำงานในปัจจุบัน

สถานที่ (ชื่อหน่วยงาน) \_\_\_\_\_ ลักษณะการจ้าง (อาชีพอิสระ/พนักงานประจำ/อื่นๆ (โปรดระบุ))

ตำแหน่ง (ตำแหน่ง) \_\_\_\_\_ ช่วงเวลาที่ปฏิบัติงาน (วันที่/เดือน/ปี พ.ศ. - วันที่/เดือน/ปี พ.ศ.) \_\_\_\_\_ ระยะเวลาการทำงาน (ปี, เดือน) \_\_\_\_\_ (สำหรับพนักงานประจำเท่านั้น)

ผลการตรวจประวัติอาชญากรรมด้วยลายนิ้วมือ  ไม่มีประวัติอาชญากรรม

#### ประสบการณ์การทำงาน

##### ลำดับที่ 1

สถานที่ (ชื่อหน่วยงาน) \_\_\_\_\_ ลักษณะการจ้าง (อาชีพอิสระ/พนักงานประจำ/อื่นๆ (โปรดระบุ))

ตำแหน่ง (ตำแหน่ง) \_\_\_\_\_ ช่วงเวลาที่ปฏิบัติงาน (DD/MM/YYYY - DD/MM/YYYY) \_\_\_\_\_ ระยะเวลาการทำงาน (ปี, เดือน) \_\_\_\_\_ (สำหรับพนักงานประจำเท่านั้น)

ข้าพเจ้าขอรับรองว่ารายละเอียดคุณสมบัติและประสบการณ์การทำงานข้างต้นนี้ เป็นความจริงทุกประการ

ลงชื่อ (ลงนามผู้มีอำนาจจากบริษัท) \_\_\_\_\_

(.....)

ตำแหน่ง.....

บริษัท.....

วันที่...../...../.....

ลงชื่อ (ลงนามเจ้าหน้าที่) \_\_\_\_\_

(.....)

วันที่...../...../.....

#### หมายเหตุ

- แบบหลักฐานสำเนาหนังสือรับรองวุฒิการศึกษา หรือประกาศนียบัตร และผลการตรวจประวัติอาชญากรรมด้วยลายนิ้วมือ เพื่อประกอบการพิจารณา
- แบบหลักฐานการเปลี่ยนชื่อหรือนามสกุล (ถ้ามี) เพื่อประกอบการพิจารณา
- ข้อมูลป้อนให้แสดงเป็นพุทธศักราช



รูปถ่าย  
ไม่เกิน 6 เดือน

ภาคผนวก ง.

ประกาศการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย  
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

  
A  
  
Joint U.  




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

ประกาศการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย  
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (ฉบับปรับปรุงครั้งที่ 12)

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

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

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

1. วัตถุประสงค์และขอบเขต

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

1.1 การเข้าถึงหรือควบคุมการใช้งานสารสนเทศครอบคลุม 4 ด้าน คือ

- 1.1.1 การเข้าถึงระบบสารสนเทศ (Access control) ต้องตรวจสอบการอนุมัติสิทธิ์การเข้าถึงระบบและ กำหนดรหัสผ่าน 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 หรือการไหลเวียนข้อมูลหรือสารสนเทศจะต้องผ่านระบบการรักษาความปลอดภัยที่องค์กร จัดสรรไว้ เช่น Firewall IDS/IPS Proxy หรือการตรวจสอบไวรัสคอมพิวเตอร์ เป็นต้น เพื่อควบคุมและ ป้องกันภัยคุกคามอย่างเป็นระบบ
  - 1.1.3 การเข้าถึงระบบปฏิบัติการ (Operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการ โดยไม่ได้รับอนุญาต โดยกำหนดให้มีการยืนยันตัวตนเพื่อระบุถึงตัวตนของผู้ใช้งาน รวมทั้งกำหนดให้มี การจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น
  - 1.1.4 การเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information access control) ต้องกำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศ โดยให้สิทธิ์เฉพาะระบบงานสารสนเทศที่ ต้องปฏิบัติตามหน้าที่เท่านั้น รวมทั้งมีการทบทวนสิทธิ์การใช้งานระบบสารสนเทศอย่างสม่ำเสมอ
  - 1.2 มีระบบสารสนเทศและระบบสำรองที่อยู่ในสภาพพร้อมใช้งาน รวมทั้งมีแผนเตรียมพร้อมในกรณีฉุกเฉินหรือ กรณีที่ไม่สามารถดำเนินการตามวิธีการทางอิเล็กทรอนิกส์ได้ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติ อย่างต่อเนื่อง
  - 1.3 ตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศอย่างสม่ำเสมอ
2. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รพม.
- แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รพม. ใช้แนวทางและกระบวนการ อ้างอิงตาม 1) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศของหน่วยงานรัฐ พ.ศ. 2553 2) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐาน การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555 และ 3) มาตรฐาน ISO/IEC 27001:2013 โดยแบ่งแนวปฏิบัติออกเป็น 16 ส่วนตามเอกสารแนบท้ายประกาศ ดังต่อไปนี้
- 2.1 นโยบายการบริหารจัดการความมั่นคงปลอดภัยสำหรับผู้บริหาร (ส่วนที่ 1)
  - 2.2 ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร (ส่วนที่ 2)
  - 2.3 การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (ส่วนที่ 3)
  - 2.4 การจัดการทรัพย์สิน (ส่วนที่ 4)
  - 2.5 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (ส่วนที่ 5)
  - 2.6 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ (ส่วนที่ 6)
  - 2.7 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (ส่วนที่ 7)
  - 2.8 การควบคุมหน่วยงานภายนอกและผู้ใช้งาน (บุคคลภายนอก) เข้าถึงระบบเทคโนโลยีสารสนเทศ (ส่วนที่ 8)
  - 2.9 การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ของ รพม. (ส่วนที่ 9)
  - 2.10 การใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์ (ส่วนที่ 10)



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

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

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

นโยบายนี้ให้ใช้บังคับเมื่อพ้นกำหนด 7 วัน นับแต่วันที่ผู้มีอำนาจลงนาม

ประกาศ ณ วันที่ 28 กันยายน พ.ศ. 2566



(นายภคพงศ์ ศิริกันทรมาศ)

ผู้ว่าการการรถไฟฟ้ามหานครแห่งประเทศไทย



## สารบัญ

เรื่อง	หน้า
คำนิยาม .....	1
ส่วนที่ 1 นโยบายการบริหารจัดการความมั่นคงปลอดภัยสำหรับผู้บริหาร .....	4
ส่วนที่ 2 ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร .....	5
ส่วนที่ 3 การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม .....	8
ส่วนที่ 4 การจัดการทรัพย์สิน .....	10
ส่วนที่ 5 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ.....	12
ส่วนที่ 6 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ.....	15
ส่วนที่ 7 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย .....	26
ส่วนที่ 8 การควบคุมหน่วยงานภายนอกหรือผู้ใช้งานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ.....	27
ส่วนที่ 9 การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ ของ รฟม.....	29
ส่วนที่ 10 การใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์ .....	32
ส่วนที่ 11 การใช้งานจดหมายอิเล็กทรอนิกส์.....	36
ส่วนที่ 12 การสำรองข้อมูลและการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ .....	37
ส่วนที่ 13 การตรวจสอบและประเมินความเสี่ยง .....	40
ส่วนที่ 14 การถ่ายโอน และแลกเปลี่ยนข้อมูลสารสนเทศ.....	43
ส่วนที่ 15 การควบคุมการเข้ารหัส .....	45
ส่วนที่ 16 การนำอุปกรณ์ส่วนตัวมาใช้งาน (Bring your own device) .....	47

**เอกสารแนบท้ายประกาศ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย**  
**เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ**  
**แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ของ รฟม.**

**คำนิยาม**

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

1. รฟม. หมายถึง การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
2. ฝ่ายเทคโนโลยีสารสนเทศ
3. ผู้บริหารระดับสูงสุด หมายถึง ผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
4. ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของ รฟม.
5. ผู้ใช้งาน หมายถึง บุคคลที่ได้รับอนุญาตให้สามารถเข้าใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. เพื่อประโยชน์ในการดำเนินงานของ รฟม. ดังนี้
  - ผู้ใช้งานภายใน หมายถึง บุคลากรของ รฟม.
  - ผู้ใช้งานภายนอก หมายถึง บุคคลภายนอกที่ รฟม. อนุญาตให้เข้ามาใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. เช่น ที่ปรึกษา ผู้ปฏิบัติงานตามสัญญา หรือนิสิตนักศึกษาฝึกงาน เป็นต้น
6. ผู้ใช้บริการ หมายถึง ผู้ที่สมัครใช้บริการระบบงานสารสนเทศของ รฟม. ผ่านเครือข่ายสาธารณะ (Internet)
7. หน่วยงานภายนอก หมายถึง องค์กรต่าง ๆ รวมถึงผู้รับจ้าง ซึ่ง รฟม. อนุญาตให้มีสิทธิในการเข้าถึง หรือใช้ข้อมูลหรือสินทรัพย์ต่าง ๆ ของ รฟม. โดยจะได้รับสิทธิในการใช้ระบบตามประเภทงานตามอำนาจและต้องรับผิดชอบในการรักษาความลับของข้อมูล
8. ผู้ดูแลระบบ หมายถึง พนักงานที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบสารสนเทศ และพนักงานของผู้รับจ้างที่รับผิดชอบติดตั้งหรือบำรุงรักษาระบบสารสนเทศให้ รฟม.
9. เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
10. มาตรฐาน หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติภารกิจเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย
11. ขั้นตอนปฏิบัติ หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานตามที่ได้กำหนดไว้ตามวัตถุประสงค์
12. แนวปฏิบัติ หมายถึง แนวทางที่ต้องปฏิบัติตามเพื่อให้สามารถบรรลุวัตถุประสงค์หรือเป้าหมายได้ง่ายขึ้น
13. ระบบเทคโนโลยีสารสนเทศ (Information technology system) หมายถึง ระบบงานของ รฟม. ที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายสื่อสารข้อมูลมาช่วยในการสร้างสารสนเทศที่ รฟม. สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุน การให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสารซึ่งมีองค์ประกอบ ได้แก่ ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลและสารสนเทศ เป็นต้น
14. ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด ที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์



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

26. ชุดคำสั่งไม่พึงประสงค์ (Malicious code) หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ชัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
27. เครื่องคอมพิวเตอร์ หมายถึง เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ และเครื่องคอมพิวเตอร์แบบพกพา
28. อุปกรณ์เคลื่อนที่ (Mobile device) หมายถึง อุปกรณ์อิเล็กทรอนิกส์แบบพกพา ซึ่งมีความสามารถในการเชื่อมต่อกับอุปกรณ์อื่นเพื่อรับส่งข้อมูลผ่านระบบเครือข่ายโทรคมนาคมไร้สายหรือโดยอาศัยคลื่นแม่เหล็กไฟฟ้าเป็นสื่อกลาง เช่น Tablet, Smart Phone
29. ทรัพย์สินของ รพม. หมายถึง ครุภัณฑ์ รพม. และทรัพย์สินที่ไม่มีการขึ้นทะเบียนครุภัณฑ์ที่ รพม. จัดสรรงบประมาณเพื่อเป็นค่าใช้จ่ายให้ทั้งหมดหรือบางส่วน
30. อุปกรณ์ส่วนตัว หมายถึง อุปกรณ์ที่ไม่ใช่ทรัพย์สินของ รพม. ที่ผู้ใช้งานนำมาเชื่อมต่อกับระบบสารสนเทศของ รพม. เช่น เครื่องคอมพิวเตอร์ส่วนบุคคล (Personal computer) เครื่องคอมพิวเตอร์พกพา (Notebook) อุปกรณ์เคลื่อนที่ (Mobile device) Removable media หรืออุปกรณ์คอมพิวเตอร์ของโครงการรถไฟฟ้า เป็นต้น

## ส่วนที่ 1

### นโยบายการบริหารจัดการความมั่นคงปลอดภัยสำหรับผู้บริหาร

#### วัตถุประสงค์

- เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรมีความสอดคล้องกับมาตรฐานสากลและกฎหมายด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง

#### ผู้รับผิดชอบ

- ผู้บริหารสูงสุด

#### อ้างอิงมาตรฐาน

- หมวดที่ 1 นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information security policy)

#### แนวปฏิบัติ

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

## ส่วนที่ 2

### ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร

#### วัตถุประสงค์

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

#### ผู้รับผิดชอบ

- ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ ผู้อำนวยการฝ่ายทรัพยากรบุคคล ผู้อำนวยการฝ่าย/สำนัก ที่กำกับดูแลงานที่มีการว่าจ้างหน่วยงานภายนอก

#### อ้างอิงมาตรฐาน

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

#### แนวปฏิบัติ

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

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

- 1.2.3 ระบบเทคโนโลยีสารสนเทศที่สร้างหรือพัฒนาโดยผู้ใช้งานในระหว่างการว่าจ้างถือเป็นสินทรัพย์ของ 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)
    - 2.1.1 ผู้บริหาร รฟม. ทุกระดับชั้นมีหน้าที่สนับสนุนและส่งเสริมเรื่องดังต่อไปนี้ แก่ผู้ใช้งาน
      - 2.1.1.1 ประกาศนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ รฟม. เป็นลายลักษณ์อักษรให้ทุกคนรับทราบและปฏิบัติตาม
      - 2.1.1.2 จูงใจให้ผู้ใช้งานปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ รฟม.
      - 2.1.1.3 สร้างความตระหนักถึงความมั่นคงปลอดภัยด้านสารสนเทศที่เกี่ยวข้องกับหน้าที่ความรับผิดชอบของตนเองและของ รฟม.
  - 2.2 การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่ผู้ใช้งาน (Information security awareness, education and training) การสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยอย่างสม่ำเสมอ
    - 2.2.1 ผู้ดูแลระบบต้องแจ้งเตือนภัยคุกคาม และช่องโหว่ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศแก่ผู้ใช้งานที่เกี่ยวข้อง นอกจากนี้ต้องแจ้งเตือนให้ผู้ใช้งานเพิ่มความระมัดระวังความเสี่ยงต่าง ๆ เช่น ไวรัสมัลแวร์ เทคนิคการหลอกล่อทางจิตวิทยา (Social engineering) และช่องโหว่ทางเทคนิค เป็นต้น
    - 2.2.2 ผทท. ต้องดำเนินการฝึกอบรม หรือประชาสัมพันธ์เพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศแก่ผู้ใช้งานเป็นประจำทุกปี
    - 2.2.3 ผทท. ต้องแจ้งผู้ใช้งานให้ทราบ เมื่อมีการเปลี่ยนแปลงนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศของ รฟม. รวมทั้งอธิบายผลกระทบจากการเปลี่ยนแปลงดังกล่าว
  - 2.3 การแจ้งเหตุการณ์ไม่ปกติ
 

ผู้ใช้งานต้องแจ้งเหตุการณ์ไม่ปกติด้านเทคโนโลยีสารสนเทศที่พบผ่านช่องทางที่ รฟม. กำหนดโดยเร็วที่สุด
  - 2.4 การกำหนดบทลงโทษ
    - 2.4.1 ความรับผิดตามกฎหมาย
 

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ไม่ได้ก่อให้เกิดสิทธิทางกฎหมายที่ทำให้ผู้ใช้งานพ้นผิดแม้จะได้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ และผู้ใช้งานตกลงยินยอมที่จะไม่ดำเนินการใด ๆ ทางกฎหมายต่อ รฟม. ซึ่งได้ปฏิบัติตามระเบียบนี้ แต่อย่างไรก็ตามหากผู้ใช้งานกระทำการละเมิดหรือกระทำผิดตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ อาจเป็นความผิดทางวินัยและเป็นเหตุ

ให้ถูกลงโทษทางวินัยได้ รฟม. ไม่มีส่วนรับผิดชอบต่อการละเมิดทรัพย์สินทางปัญญาที่เกิดจากการใช้ระบบคอมพิวเตอร์

#### 2.4.2 การพิจารณาโทษผู้กระทำผิด

ผู้ใช้งานที่กระทำความผิด ผทท. จะเพิกถอนสิทธิ์การใช้งานและอาจเป็นความผิดทางวินัย หรือความผิดตามกฎหมายที่เกี่ยวข้อง

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

### 3. การสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน (Termination and change of employment)

เพื่อกำหนดหน้าที่ความรับผิดชอบเมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน ซึ่งรวมถึงการคืนทรัพย์สินและการถอดถอนสิทธิ์ในการเข้าถึง

#### 3.1 การแจ้งการสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน

3.1.1 ฝ่ายทรัพยากรบุคคลต้องแจ้งให้ฝ่ายเทคโนโลยีสารสนเทศทราบทันทีหากพนักงานมีการลาออก โยกย้าย เกษียณ หรือเสียชีวิต เพื่อฝ่ายเทคโนโลยีสารสนเทศจะได้ตรวจสอบและบริหารจัดการสิทธิ์ในการเข้าถึงระบบเทคโนโลยีสารสนเทศ

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

#### 3.2 การคืนทรัพย์สินของ รฟม.

ผู้ดูแลระบบต้องตรวจสอบเพื่อเรียกคืนทรัพย์สินของ รฟม. จากผู้ใช้งาน เมื่อการสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน

#### 3.3 การถอดถอนสิทธิ์ในการเข้าถึง

3.3.1 ผู้ดูแลระบบต้องถอดถอนสิทธิ์ในการเข้าถึงของผู้ใช้งาน เมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน

3.3.2 การถอดถอนสิทธิ์ในการเข้าถึงหมายถึงรวมถึง 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) หรือสถานที่ที่มีความมั่นคงปลอดภัยและมีการปิดล็อก
3. ผู้ดูแลระบบ ต้องมีการป้องกันสายเคเบิลที่ใช้เพื่อการสื่อสารหรือสายไฟ มิให้มีการดักจับสัญญาณ (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 รพม. เช่น บัตรประจำตัวประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วบันทึกข้อมูลบัตรในสมุดบันทึกหรือระบบงานสารสนเทศ

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



## ส่วนที่ 4

### การจัดการทรัพย์สิน

#### วัตถุประสงค์

- เพื่อบริหารจัดการทรัพย์สินสารสนเทศ ตั้งแต่การจัดการ การใช้งาน จนถึงการยกเลิกใช้งาน โดยมีการระบุ สิทธิ์ขององค์กรและกำหนดหน้าที่ความรับผิดชอบในการปกป้องทรัพย์สินสารสนเทศอย่างเหมาะสม

#### 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 เพื่อรับผิดชอบดูแล ความมั่นคงปลอดภัยสารสนเทศตลอดวงจรอายุการใช้งาน
  - 1.3 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องเรียกคืนทรัพย์สินสารสนเทศเมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน
  - 1.4 ผู้ใช้งานต้องใช้ทรัพย์สินสารสนเทศของ รพม. อย่างระมัดระวัง และใช้เพื่อปฏิบัติงานของ รพม. เท่านั้น รวมทั้งต้องปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ และนโยบาย ของ รพม.
2. การจำแนกประเภทของทรัพย์สินสารสนเทศ (Asset classification)
  - 2.1 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจำแนกประเภททรัพย์สินตามขั้นตอนที่ รพม. กำหนด และทบทวนการ จำแนกดังกล่าวอย่างสม่ำเสมอ
  - 2.2 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจัดทำป้ายชื่อทรัพย์สินสารสนเทศ (Labeling) ให้ชัดเจน พร้อมทั้งจัดให้มีมาตรการ ดูแลการรักษาความมั่นคงปลอดภัยสารสนเทศที่สอดคล้องกับประเภททรัพย์สินตามระดับชั้นความลับที่ รพม. กำหนด
3. การจัดการสื่อบันทึกข้อมูล (Media handling)
  - 3.1 เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ใช้งานต้องควบคุมการใช้งานและจัดเก็บสื่อบันทึกแบบถอดหรือต่อพ่วง กับเครื่องคอมพิวเตอร์ได้ (Removable media) ตามที่ รพม. กำหนด
  - 3.2 เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูล ตามขั้นตอนที่ รพม. กำหนด โดยไม่สามารถกู้คืนข้อมูลกลับมาได้อีกก่อนจะกำจัดอุปกรณ์ดังกล่าวหรือ

ก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อเพื่อป้องกันไม่ให้เกิดการเข้าถึงข้อมูลที่สำคัญได้ โดยพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

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

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

## ส่วนที่ 5

### การจัดทำ การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

#### วัตถุประสงค์

- เพื่อควบคุมการจัดทำ พัฒนา และบำรุงรักษาระบบสารสนเทศ ให้มีการกำหนดมาตรการการรักษาความมั่นคงปลอดภัย เพื่อป้องกันความผิดพลาด สูญหาย และการเปลี่ยนแปลงแก้ไขระบบ

#### ผู้รับผิดชอบ

- ผู้บังคับบัญชา
- ผู้ดูแลระบบ

#### อ้างอิงมาตรฐาน

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

#### แนวปฏิบัติ

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

10. ผู้ดูแลระบบต้องควบคุมการจัดส่ง Source code ผ่านช่องทางที่มั่นคงปลอดภัยและเป็นช่องทางที่ รพม. กำหนดให้ใช้งานเท่านั้น
11. ผู้ดูแลระบบต้องปิดบังข้อมูลส่วนบุคคล (Data Masking) ที่จัดเก็บอยู่ในระบบงานสารสนเทศด้วยวิธีการที่เหมาะสม
12. ผู้ดูแลระบบต้องแสดงข้อมูลของผู้ใช้งานอย่างรัดกุม เช่น การปิดบังข้อมูลสำคัญของผู้ใช้งาน (Sensitive data masking) เป็นต้น
13. กรณีของแอปพลิเคชันที่ใช้งานผ่านอุปกรณ์เคลื่อนที่ (Mobile device) ให้ผู้ดูแลระบบดำเนินการ ดังนี้
  - 13.1 ปิดบังหน้าจอเมื่อย่อแอปพลิเคชัน (Application blurring) เพื่อลดความเสี่ยงที่ข้อมูลสำคัญของผู้ใช้งานจะรั่วไหล
  - 13.2 ขอสสิทธ์เข้าถึงทรัพยากรหรือบริการโดยแอปพลิเคชัน (Application permission) บนอุปกรณ์เคลื่อนที่ของผู้ใช้งานเท่าที่จำเป็น และมีกระบวนการทบทวนการขอสสิทธ์เป็นประจำเพื่อป้องกันการละเมิดสิทธ์ความเป็นส่วนตัวของผู้ใช้งาน
14. ผู้ดูแลระบบต้องควบคุมข้อมูลที่นำมาใช้ในการทดสอบระบบ (Test data) อย่างเหมาะสม โดยไม่นำข้อมูลจริงมาทดสอบ กรณีจำเป็นต้องใช้ข้อมูลจริงต้องได้รับอนุญาตข้อมูลจากเจ้าของก่อนนำมาใช้งาน และทำลายข้อมูลอย่างเหมาะสมตามขั้นตอนที่ รพม. กำหนด
15. ผู้ดูแลระบบต้องแยกระบบสารสนเทศสำหรับการพัฒนา ทดสอบ และใช้งานจริงออกจากกันเพื่อลดความเสี่ยงที่เกิดจากการเปลี่ยนแปลงระบบสารสนเทศโดยไม่ได้รับอนุญาต และต้องมีการกำหนดสิทธิ์การเข้าถึงระบบสารสนเทศที่พัฒนา ทดสอบ หรือใช้งานจริง ทั้งระบบสารสนเทศใหม่ และการปรับปรุงแก้ไขระบบสารสนเทศเดิม
16. ผู้ดูแลระบบต้องมีการกำหนดขั้นตอนการทดสอบระบบสารสนเทศก่อนนำไปใช้งานจริง ทั้งในกรณีปรับปรุงระบบสารสนเทศเดิมและการพัฒนาระบบสารสนเทศใหม่
17. ผู้ดูแลระบบต้องติดตั้งซอฟต์แวร์บนระบบสารสนเทศที่ให้บริการ (Production) ตามขั้นตอนที่ รพม. กำหนด และจำกัดสิทธิ์การติดตั้งซอฟต์แวร์เพื่อให้ระบบสารสนเทศต่าง ๆ มีความถูกต้องครบถ้วนและน่าเชื่อถือ
18. ผู้ดูแลระบบต้องนำซอฟต์แวร์ที่ไม่ละเมิดลิขสิทธิ์มาติดตั้งบนระบบสารสนเทศที่ให้บริการ (Production)
19. ผู้ดูแลระบบต้องกำกับดูแลให้ผู้รับจ้างปฏิบัติตามสัญญาหรือข้อตกลงการให้บริการที่ระบุไว้ โดยครอบคลุมถึงด้านความมั่นคงปลอดภัยสารสนเทศ และการปฏิบัติตามขั้นตอนที่เกี่ยวข้องต่าง ๆ ที่ รพม. กำหนดไว้
20. ผู้ดูแลระบบ ต้องติดตาม ตรวจสอบรายงาน หรือบันทึกการให้บริการของบุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามสัญญาว่าจ้างอย่างสม่ำเสมอ
21. ผู้ดูแลระบบ ต้องดูแลให้ทรัพย์สินสารสนเทศได้รับการบำรุงรักษาและซ่อมแซมตามความต้องการ รวมทั้งต้องมีการบันทึกประวัติการทำงานผิดปกติ การบำรุงรักษา และการซ่อมแซมอุปกรณ์นั้น ๆ อย่างสม่ำเสมอ
22. ผู้ดูแลระบบจะต้องปิดช่องโหว่ของระบบสารสนเทศที่มีระดับความรุนแรงในระดับวิกฤติ (Critical) และระดับความรุนแรงระดับสูง (High) ทั้งหมดก่อนนำไปใช้งานจริง (Production) หรือก่อนเริ่ม Go live โดยเฉพาะระบบที่ให้บริการผ่านเครือข่ายอินเทอร์เน็ต (Internet facing) และระบบที่มีความสำคัญต่อการดำเนินงานของ รพม.
23. ผู้ดูแลระบบต้องพิจารณาเลือกใช้ Version ของ Software ดังนี้

- 23.1 กรณีนำ Software เดิมมาใช้ในการจัดหาหรือพัฒนาระบบ จะต้องนำผลการตรวจสอบช่องโหว่และผลการทดสอบเจาะระบบมาประกอบการพิจารณาคัดเลือกเวอร์ชันของ Software ด้วย เพื่อป้องกันไม่ให้เกิดช่องโหว่เดิมรวมถึงเพื่อลดภาระงานในการปิดช่องโหว่เดิมซ้ำ
- 23.2 กรณีเป็น Software ที่ไม่เคยนำมาใช้งานให้เลือกใช้ Software เวอร์ชันล่าสุด

## ส่วนที่ 6

### การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

#### วัตถุประสงค์

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

#### ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- เจ้าของข้อมูล
- ผู้ใช้งาน

#### อ้างอิงมาตรฐาน

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

#### แนวปฏิบัติ

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

## 1.5 ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ใช้งาน ต้องปฏิบัติ ดังนี้

### 1.5.1 แบ่งประเภทข้อมูล ดังนี้

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

### 1.5.2 จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น 3 ระดับ คือ

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

### 1.5.3 จัดแบ่งลำดับชั้นความลับของข้อมูลตามที่ รพม. กำหนด

### 1.5.4 จัดแบ่งระดับชั้นการเข้าถึง

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

## 1.6 เจ้าของข้อมูลและผู้ดูแลระบบต้องกำหนดเวลาการเข้าถึงระบบสารสนเทศ

## 1.7 ผู้ดูแลระบบต้องจำกัดช่องทางการเข้าถึงระบบเทคโนโลยีสารสนเทศตามช่องทาง ดังนี้

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

## 1.8 ผู้ดูแลระบบต้องกำกับดูแล Default permission ของไฟล์ (File) และ โฟลเดอร์ (Folder) ที่สร้างขึ้นให้มีการจำกัดสิทธิ์ในการเข้าถึง

## 1.9 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องพิจารณาข้อกำหนดต่าง ๆ ที่มีผลทางกฎหมายซึ่งเกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศของ รพม. เช่น พระราชบัญญัติ ข้อกำหนดทางกฎหมาย ข้อกำหนดในสัญญา

และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่น ๆ เป็นต้น เพื่อกำหนดสิทธิ์การเข้าถึงสารสนเทศและระบบเทคโนโลยีสารสนเทศของ รพม.

- 1.10 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องมีการสอบถามสิทธิ์ในการเข้าถึงระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ พร้อมทั้งเพิกถอนสิทธิ์เมื่อพบเห็นสิทธิ์ที่ไม่ถูกต้องตามสิทธิ์ในการเข้าถึง (Authorization matrix)
2. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)
 

ให้มีการควบคุมการลงทะเบียนผู้ใช้งาน การบริหารจัดการรหัสผ่าน การบริหารจัดการสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศ และการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน

  - 2.1 การลงทะเบียนผู้ใช้งาน (User registration)
    - 2.1.1 ผู้ดูแลระบบต้องบริหารจัดการและควบคุมบัญชีชื่อผู้ใช้งาน (Username) มิให้มีการใช้งานบัญชีชื่อผู้ใช้งานซ้ำกัน ทั้งนี้ ในส่วนของพนักงาน/ลูกจ้าง รพม. ให้กำหนดชื่อผู้ใช้งาน (Username) ตามมาตรฐานจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ใช้ในองค์กร
    - 2.1.2 เจ้าของข้อมูลต้องเป็นผู้อนุมัติการสร้างบัญชีผู้ใช้งานชั่วคราว (Temporary user) และต้องจำกัดช่วงเวลาการใช้งานเท่าที่จำเป็น
  - 2.2 การบริหารจัดการรหัสผ่าน (User password management)
    - 2.2.1 ผู้ดูแลระบบต้องกำหนดรหัสผ่านแบบชั่วคราวโดยใช้วิธีการสุ่ม และบังคับให้มีการเปลี่ยนรหัสผ่านเมื่อผู้ใช้งานเข้าใช้งานระบบในครั้งแรก
    - 2.2.2 ผู้ดูแลระบบต้องกำหนดความยาวของรหัสผ่าน ดังนี้
      - 1) ผู้ดูแลระบบมีความยาวอย่างน้อย 16 หลัก
      - 2) ผู้ใช้งานมีความยาวอย่างน้อย 12 หลัก
    - 2.2.3 ผู้ดูแลระบบต้องกำหนดให้มีการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication) ตามความเหมาะสม
    - 2.2.4 ผู้ดูแลระบบต้องกำหนดให้รหัสผ่านมีความซับซ้อน โดยประกอบด้วย ตัวอักษร ตัวเลข และอักขระพิเศษ เช่น (a-Z) (0-9) (@, #, &, “, ‘, \*, =, <, >, %, \$, +, ?) เป็นต้น
    - 2.2.5 ผู้ดูแลระบบต้องกำหนดให้มีการเปลี่ยนแปลงรหัสผ่าน ดังนี้
      - 1) ผู้ดูแลระบบต้องเปลี่ยนรหัสผ่านทุก ๆ 3 เดือน
      - 2) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทุก ๆ 6 เดือน
      - 3) ผู้ใช้งานเชิงระบบ (System account) ให้พิจารณาเปลี่ยนรหัสผ่านตามความเหมาะสม
    - 2.2.6 ผู้ดูแลระบบต้องกำหนดให้มีการเข้ารหัสข้อมูลรหัสผ่านในระบบ
    - 2.2.7 ผู้ดูแลระบบต้องจัดให้มีการควบคุมรหัสผ่านอย่างเข้มงวด
    - 2.2.8 ผู้ดูแลระบบต้องจัดส่งบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ด้วยวิธีการที่ปลอดภัย
    - 2.2.9 ผู้ดูแลระบบต้องควบคุมดูแลระบบปฏิบัติการ ระบบฐานข้อมูล และระบบงานสารสนเทศ (Application) ที่จัดเก็บบัญชีผู้ใช้งานและรหัสผ่านอย่างเข้มงวด โดยให้เข้าถึงได้เฉพาะผู้ดูแลระบบที่ได้รับอนุญาตเท่านั้น
    - 2.2.10 ผู้ดูแลระบบต้องกำหนดวิธีการหรือกระบวนการยืนยันตัวตนที่ปลอดภัย เช่น กรณีที่ลืมรหัสผ่าน



### 2.2.11 ผู้ดูแลระบบต้องกำหนดให้ผู้ให้บริการ ใช้รหัสผ่านอย่างมั่นคงปลอดภัย ดังนี้

#### กรณีแอปพลิเคชันทั่วไป

- 1) กำหนดความยาวรหัสผ่านอย่างน้อย 12 หลัก ซึ่งประกอบด้วย ตัวอักษร ตัวเลข และ อักขระพิเศษ เช่น (a-z) (0-9) (@ , # , & , “ , ‘ , \* , = , < , > , % , \$ , + , ?) เป็นต้น
- 2) รหัสผ่านต้องไม่เป็นคำที่คาดเดาได้ง่าย เช่น คำที่อยู่ในพจนานุกรม ชื่อ-นามสกุล วันเดือนปีเกิด ที่อยู่ หรือเบอร์โทรศัพท์ เป็นต้น
- 3) ไม่บังคับให้เปลี่ยนรหัสผ่าน ทั้งนี้ขึ้นอยู่กับความสมัครใจในการเปลี่ยนรหัสผ่าน และระบบ ต้องรองรับการเปลี่ยนรหัสผ่านในกรณีต่าง ๆ ด้วยวิธีการที่ปลอดภัย

#### กรณีแอปพลิเคชันที่ใช้งานผ่านอุปกรณ์เคลื่อนที่ (Mobile device)

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

### 2.2.12 ผู้ดูแลระบบและผู้ใช้งานต้องใช้รหัสผ่านอย่างปลอดภัย ดังนี้

- 1) ต้องกำหนดรหัสผ่านที่ไม่สามารถคาดเดาได้ง่าย เช่น คำที่อยู่ในพจนานุกรม “qwerty” “abcde” “12345” ชื่อ-นามสกุล วันเดือนปีเกิด ที่อยู่ หรือเบอร์โทรศัพท์ เป็นต้น
- 2) ต้องไม่ใช้งานรหัสผ่านโดยกระบวนการเข้าใช้งานโดยอัตโนมัติ ได้แก่ การกำหนดค่า “Remember Password” เป็นต้น
- 3) ต้องเก็บรหัสผ่านไว้เป็นความลับเฉพาะบุคคล ไม่เปิดเผยให้ผู้อื่นรับทราบ และไม่พิมพ์รหัสผ่านในลักษณะเปิดเผย เช่น พิมพ์รหัสผ่านต่อหน้าผู้ใช้งานคนอื่น เป็นต้น
- 4) ต้องไม่ใช้บัญชีชื่อผู้ใช้งานและรหัสผ่านร่วมกันกับผู้อื่น แม้ว่าบัญชีชื่อผู้ใช้งานจะได้รับการอนุญาตจากเจ้าของชื่อผู้ใช้งานบุคคลนั้นก็ตาม
- 5) ต้องเปลี่ยนแปลงรหัสผ่านเมื่อมีการแจ้งเตือนจากระบบ หรือสงสัยว่ารหัสผ่านลวงรู้โดยบุคคลอื่น

## 2.3 การบริหารจัดการสิทธิ์ (Privilege management)

### 2.3.1 ผู้บังคับบัญชาต้องกำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียน การเพิกถอนสิทธิ์ การเปลี่ยนแปลงสิทธิ์ และการทบทวนสิทธิ์ของผู้ใช้งานอย่างเป็นลายลักษณ์อักษร

### 2.3.2 กำหนดสิทธิ์ที่เหมาะสมกับผู้ใช้งานตามความจำเป็นและสอดคล้องกับหน้าที่ความรับผิดชอบและจัดเก็บประวัติ (Log) การลงทะเบียน การเพิกถอนสิทธิ์ และการเปลี่ยนแปลงสิทธิ์ของผู้ใช้งาน

### 2.3.3 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจัดให้มีการควบคุมและจำกัดสิทธิ์ในการใช้งานระบบตามความจำเป็นในการใช้งานเท่านั้น

- 1) สิทธิ์ในการสร้างข้อมูล (Create)
- 2) สิทธิ์ในการอ่านข้อมูลหรือเรียกดูข้อมูล (READ)
- 3) สิทธิ์ในการปรับปรุงข้อมูล (Modify / Update)
- 4) สิทธิ์ในการลบข้อมูล (Delete)

- 5) สิทธิในการมอบหมายสิทธิในการดำเนินการแทน (Assign)
  - 6) สิทธิในการรับรองความถูกต้องครบถ้วนของข้อมูล (Approve/Authenticate)
  - 7) ไม่มีสิทธิ
- 2.3.4 เจ้าของข้อมูลและผู้ดูแลระบบต้องเป็นผู้อนุมัติการให้สิทธิเพื่อเข้าถึงสารสนเทศหรือระบบเทคโนโลยีสารสนเทศใด ๆ อย่างเป็นลายลักษณ์อักษร
- 2.3.5 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจำกัดจำนวนผู้ใช้งานที่ทำหน้าที่เป็นผู้ให้สิทธิ์กับผู้ใช้งานให้น้อยที่สุดตามความเหมาะสม
- 2.3.6 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจำกัดระยะเวลาการใช้งานระบบเทคโนโลยีสารสนเทศของ รพม. แก่หน่วยงานภายนอกที่เข้ามาปฏิบัติงานร่วมกับ รพม.
- 2.3.7 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจัดให้มีการถอดถอนหรือเปลี่ยนแปลงสิทธิ์การเข้าถึงทันที เมื่อผู้ใช้งานเกษียณ เปลี่ยนแปลงหน้าที่ความรับผิดชอบ เปลี่ยนแปลงการจ้างงาน หรือไม่มีความจำเป็นในการใช้งานระบบเทคโนโลยีสารสนเทศ
- 2.3.8 ผู้ดูแลระบบต้องลบหรือระงับการใช้งานสิทธิ์ของผู้ใช้งานที่มาจากระบบ (Default user) ในกรณีที่มีความจำเป็นต้องใช้งานต้องกำหนดรหัสผ่านอย่างมั่นคงปลอดภัย
- 2.4 การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of user access rights)
- 2.4.1 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องมีการสอบทานสิทธิ์การเข้าถึงของผู้ใช้งานระบบเมื่อ รพม. มีการเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศหรือโครงสร้างองค์กร
- 2.4.2 ผู้ดูแลระบบ ต้องมีการสอบทานและระงับการใช้งานบัญชีผู้ใช้งานที่ไม่ได้ใช้งานเกิน 180 วัน หากผู้ใช้งานต้องการกลับมาใช้งานจะต้องยืนยันตัวตนให้ ผทท. ทราบ ทั้งนี้ ระยะเวลาที่ไม่ได้ใช้งานของบัญชีผู้ใช้งานอาจจะขึ้นอยู่กับแต่ละระบบสารสนเทศ
3. การป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล และการควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ไม่ปลอดภัย
- 3.1 การป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล (Unattended user equipment)
- 3.1.1 ผู้ดูแลระบบต้องจัดให้มีมาตรการสำหรับป้องกันระบบคอมพิวเตอร์ ระบบเครือข่ายสื่อสารข้อมูล และระบบเทคโนโลยีสารสนเทศ โดยการกำหนดค่าของระบบ (Configuration) ให้มีการล็อกหน้าจอสำหรับอุปกรณ์ที่ไม่มีพนักงานดูแล หรือล็อกอุปกรณ์อยู่เสมอ
- 3.1.2 ผู้ใช้งานและหน่วยงานภายนอก ต้องล็อกหน้าจออัตโนมัติเมื่อไม่มีการใช้งานระบบเทคโนโลยีสารสนเทศของ รพม. ตามระยะเวลาที่กำหนด โดยต้องพักหน้าจอ (Screen saver) อัตโนมัติหลังจากที่ไม่มีการใช้งานคอมพิวเตอร์เป็นระยะเวลานานกว่า 15 นาที ผู้ใช้งานและหน่วยงานภายนอกจะใช้งานต่อได้เมื่อมีการใส่รหัสผ่านที่ถูกต้อง
- 3.1.3 ผู้ใช้งานต้อง Log out ออกจากเครื่องคอมพิวเตอร์เมื่อมีความจำเป็นต้องทิ้งเครื่องคอมพิวเตอร์
- 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 รพม. การควบคุมการพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย การป้องกันพอร์ต (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ การแบ่งแยกเครือข่าย (Segregation in networks) อย่างเหมาะสม การควบคุมการเชื่อมต่อทางเครือข่าย และการควบคุมการกำหนดเส้นทางบนเครือข่าย

##### 4.1 การใช้งานบริการเครือข่าย (Use of network services)

4.1.1 ผู้ดูแลระบบต้องควบคุมการเผยแพร่แผนผังระบบเครือข่ายสื่อสารข้อมูล (Network diagram) รวมถึงโครงสร้าง IP address ชื่อระบบ และชื่ออุปกรณ์สารสนเทศแก่ผู้ที่ไม่ได้รับอนุญาตหรือหน่วยงานภายนอก

4.1.2 ผู้ดูแลระบบต้องควบคุมการใช้งานระบบเครือข่ายสื่อสารข้อมูล เพื่อป้องกันการเข้าถึงระบบเครือข่ายสื่อสารข้อมูลและบริการของระบบเครือข่ายสื่อสารข้อมูลโดยไม่ได้รับอนุญาต

4.1.3 ผู้ดูแลระบบต้องควบคุมการเชื่อมต่อเครือข่ายภายนอก เพื่อใช้งานอินเทอร์เน็ต ซึ่งอาจเป็นช่องทางให้หน่วยงานภายนอกเข้าถึงสารสนเทศหรือระบบเทคโนโลยีสารสนเทศของ รพม. โดยมิได้รับอนุญาต

4.1.4 ผู้ใช้งานต้องแจ้งความประสงค์ในการขอใช้งานบริการเครือข่ายแก่ ผทท. และสามารถใช้บริการเครือข่ายได้หลังจากได้รับการอนุมัติจาก ผทท. แล้ว

4.1.5 ผู้ใช้งาน ต้องไม่ใช้ระบบเครือข่ายสื่อสารข้อมูลเพื่อเป็นช่องทางในการเจาะระบบ (Hacking) หรือการสแกนช่องโหว่ของระบบโดยมิได้รับอนุญาต

##### 4.2 การพิสูจน์ตัวตนของผู้ใช้งานที่อยู่ภายนอก รพม. (User authentication for external connections)

ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนผ่านระบบ Active directory ของ รพม. ก่อนอนุญาตให้ผู้ใช้งานที่อยู่ภายนอก รพม. เข้าใช้งานเครือข่ายและระบบสารสนเทศของ รพม.

##### 4.3 การพิสูจน์ตัวตนของอุปกรณ์ในระบบเครือข่ายสื่อสารข้อมูล (Equipment identification in networks)

ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนของอุปกรณ์ในระบบเครือข่ายสื่อสารข้อมูล ได้แก่ การตรวจสอบ MAC address

##### 4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection)

ผู้ดูแลระบบต้องระงับบริการและพอร์ต (Port) ที่ไม่มีความจำเป็นต้องใช้บนเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่าย

##### 4.5 ผู้ดูแลระบบต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion prevention system/ intrusion detection system) ของระบบเครือข่าย

##### 4.6 การแบ่งแยกเครือข่าย (Segregation in networks)

4.6.1 ผู้ดูแลระบบต้องจัดให้มีการแบ่งแยกเครือข่ายตามกลุ่มของผู้ใช้งาน หรือกลุ่มของระบบเทคโนโลยีสารสนเทศ เพื่อควบคุมการใช้งานในแต่ละเครือข่ายอย่างเหมาะสม โดยพิจารณาจากความ

ต้องการในการเข้าถึงข้อมูล ระดับความสำคัญของข้อมูล รวมถึงการพิจารณาด้านราคา ประสิทธิภาพ และผลกระทบทางด้านความปลอดภัยดังต่อไปนี้

- 1) เครือข่ายที่อนุญาตให้เข้าถึงจากภายนอกและเครือข่ายที่ใช้ภายใน รพม.
  - 2) เครือข่ายแอปพลิเคชัน (Application) ที่มีความสำคัญกับเครือข่ายอื่น ๆ ที่มีความสำคัญน้อยกว่า
  - 3) เครือข่ายสำหรับเครื่องให้บริการ (Server farm) กับเครือข่ายของผู้ใช้งาน ควรมีการติดตั้งอุปกรณ์ที่สามารถแบ่งแยกเครือข่ายได้ เช่น Firewall หรือ Switch ที่สามารถแบ่ง VLAN ได้ เป็นต้น
- 4.6.2 ผู้ดูแลระบบจะกำหนดเส้นทางบนเครือข่ายที่เข้มงวด เพื่อจำกัดการเข้าถึงระยะไกลไปเฉพาะเครือข่ายที่กำหนดเท่านั้น
- 4.6.3 ผู้ดูแลระบบต้องตั้งค่า (Configuration) อุปกรณ์เครือข่าย เช่น Firewall หรือ Router มิให้สามารถบริหารจัดการจากภายนอกเครือข่ายได้ เว้นแต่ในกรณีฉุกเฉินซึ่งต้องได้รับการอนุญาตจากผู้ดูแลระบบเท่านั้น
- 4.7 การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control)
- 4.7.1 ผู้ดูแลระบบต้องจำกัดการใช้งานเครือข่ายของผู้ใช้งานในการเชื่อมต่อกับเครือข่ายของ รพม. เช่น Router หรือ Firewall เป็นต้น พร้อมทั้งติดตั้งระบบควบคุมเพื่อกั้นกรองข้อมูลที่รับ - ส่ง เช่น Web filtering, E-mail filtering เป็นต้น เพื่อทำให้การเชื่อมต่อมีความปลอดภัย
- 4.7.2 ผู้ดูแลระบบต้องติดตั้ง Firewall ระหว่างเครือข่ายของ รพม. กับเครือข่ายภายนอก ทั้งนี้ การติดตั้ง Firewall ต้องพิจารณาเรื่องดังต่อไปนี้
- 1) การป้องกันการจราจรจากภายนอก ต้องถูกกำหนดให้ใช้เส้นทางที่ผ่าน First tier firewall ที่มีความมั่นคงปลอดภัยเพื่อป้องกันการรั่วไหลของข้อมูลของ รพม. และโครงสร้างพื้นฐานที่มีความสำคัญจากการเข้าถึงที่ไม่ได้รับอนุญาต
  - 2) Firewall ต้องระบุตัวตนและพิสูจน์ตัวตนของผู้ใช้งานก่อนที่จะให้สิทธิ์การเข้าถึงอินเทอร์เน็ต (Interface) เพื่อการบริหารจัดการ Firewall
  - 3) Firewall ต้องตั้งค่าให้ระงับบัญชีผู้ใช้งานหลังจากมีความพยายามที่จะเข้าสู่ระบบไม่สำเร็จ 5 ครั้ง การยกเลิกการระงับต้องดำเนินการโดย ผทท.
  - 4) ไม่อนุญาตให้พิสูจน์ตัวตนผ่านทางอินเทอร์เน็ต (Interface) การจัดการ Firewall จากระยะไกล (Remote)
  - 5) ผู้ที่ได้รับการมอบหมายจาก ผทท. เท่านั้นที่มีสิทธิ์ที่จะเปลี่ยนการตั้งค่าด้านความปลอดภัยบน Firewall
  - 6) Firewall ต้องตั้งค่าให้บันทึกเหตุการณ์ด้านความมั่นคงปลอดภัย
  - 7) Firewall ต้องได้รับการสอบทาน ทดสอบ และตรวจสอบอย่างสม่ำเสมอ
  - 8) Firewall ต้องถูกบริหารจัดการผ่านทาง การติดต่อสื่อสารที่มีการเข้ารหัส
  - 9) ต้องปิดบริการและพอร์ต (Port) ที่ไม่จำเป็นต้องใช้บน Firewall

- 10) Firewall ประเภทซอฟต์แวร์ (Software) ต้องติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายแยกต่างหาก
- 11) Firewall ต้องสามารถป้องกันตัวเองจากการโจมตี DOS (Denial of service) ได้ อย่างเช่น Ping, Sweeps หรือ TCP SYN Floods เป็นต้น
- 12) ต้องใช้เวอร์ชันของซอฟต์แวร์ (Software) Firewall และระบบปฏิบัติการที่เจ้าของผลิตภัณฑ์ยังให้การสนับสนุน
- 13) ผู้ดูแล Firewall ต้องติดตามข้อมูลช่องโหว่จากผู้ให้บริการ (Vendor) เพื่อรับทราบข่าวสาร การ Upgrade และแพตช์ (Patch) ที่จำเป็น และต้องติดตั้งแพตช์ (Patch) ทั้งหมดที่เกี่ยวข้อง

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

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

4.8 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control)

ผู้ดูแลระบบต้องควบคุมการกำหนดเส้นทางบนเครือข่ายเพื่อให้มั่นใจว่าการเชื่อมต่อเครื่องคอมพิวเตอร์ และการไหลเวียนของสารสนเทศบนเครือข่าย โดยมีกลไกในการตรวจสอบที่อยู่ปลายทางและต้นทางของการเชื่อมต่อ เช่น การควบคุมโดย Firewall หรือ Proxy เป็นต้น

5. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)

ให้มีการควบคุมการเข้าถึงระบบปฏิบัติการอย่างมั่นคงปลอดภัย การควบคุมการระบุและพิสูจน์ตัวตนของผู้ใช้งาน การควบคุมระบบบริหารจัดการรหัสผ่าน การควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ (System utilities) การควบคุมการหมดเวลาการใช้งานระบบเทคโนโลยีสารสนเทศ และควบคุมการจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ

5.1 ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on procedures)

5.1.1 ผู้ดูแลระบบ ต้องจัดให้มีการควบคุมการเข้าถึงระบบปฏิบัติการอย่างมั่นคงปลอดภัยโดยขั้นตอนการเข้าสู่ระบบต้องเปิดเผยข้อมูลเกี่ยวกับระบบให้น้อยที่สุดเพื่อหลีกเลี่ยงผู้ใช้งานที่ไม่ได้รับอนุญาต ซึ่งขั้นตอนการ Log-on ต้องพิจารณา ดังนี้

- 1) หากกระบวนการเข้าสู่ระบบไม่สำเร็จ ระบบต้องไม่แสดงข้อมูลของระบบหรือแอปพลิเคชัน (Application) ที่ใช้งานอยู่
- 2) ระบบต้องแสดงข้อความเตือนผู้ใช้งานว่าสามารถเข้าใช้งานเครื่องคอมพิวเตอร์ได้เฉพาะผู้ที่มีสิทธิ์เท่านั้น
- 3) หากกระบวนการเข้าสู่ระบบไม่สำเร็จ ระบบต้องไม่แสดงข้อมูลที่สามารถระบุตัวตนของระบบ เช่น เครือข่ายที่ใช้งาน สถานที่ตั้งของระบบ หรือชื่อเครื่องคอมพิวเตอร์แม่ข่าย เป็นต้น

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

โปรแกรมพักหน้าจอกำหนดให้ป้อนรหัสผ่านหลังจากที่มีการทิ้งเครื่องดังกล่าวไว้โดยไม่มีการใช้งาน เป็นเวลา 15 นาที

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

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



## ส่วนที่ 7

### การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

#### วัตถุประสงค์

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

#### ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

#### อ้างอิงมาตรฐาน

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

#### แนวปฏิบัติ

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

## ส่วนที่ 8

### การควบคุมหน่วยงานภายนอกและผู้ใช้งานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ

#### วัตถุประสงค์

- เพื่อควบคุมหน่วยงานภายนอกและผู้ใช้งานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. ให้เป็นไปอย่างมั่นคงปลอดภัย

#### ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้บังคับบัญชา
- หน่วยงานภายนอก
- ผู้ใช้งาน (บุคคลภายนอก)

#### อ้างอิงมาตรฐาน

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

#### แนวปฏิบัติ

1. ผู้ดูแลระบบต้องประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผล โดยหน่วยงานภายนอกและผู้ใช้งานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศของ รฟม.
2. การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอกและผู้ใช้งานภายนอก
  - 2.1 เจ้าของข้อมูลต้องเป็นผู้อนุญาตการให้สิทธิ์แก่หน่วยงานภายนอกและผู้ใช้งานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของ รฟม. อย่างเป็นทางการลายลักษณ์อักษร
  - 2.2 ผู้บังคับบัญชาต้องกำหนดให้มีการลงนามการไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของ รฟม.
  - 2.3 ผู้บังคับบัญชา ต้องควบคุมให้มีการกำหนดข้อตกลงและความรับผิดชอบที่เกี่ยวข้องกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศลงในสัญญา กับหน่วยงานภายนอกที่ให้บริการด้านสารสนเทศและบริการด้านการสื่อสาร โดยให้ครอบคลุมรวมถึงผู้รับจ้างช่วง
  - 2.4 ผู้บังคับบัญชาต้องกำหนดให้จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกและผู้ใช้งานภายนอกระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศ ซึ่งมีรายละเอียด ดังนี้
    - 2.4.1 เหตุผลในการขอใช้
    - 2.4.2 ระยะเวลาในการใช้
    - 2.4.3 การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย
    - 2.4.4 การตรวจสอบ MAC address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

- 2.5 ผู้ดูแลระบบมีสิทธิ์ในการตรวจสอบการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอกและ  
ผู้ใช้งานภายนอก เพื่อควบคุมการใช้งานได้อย่างมั่นคงปลอดภัยตามสัญญา
- 2.6 ผู้ดูแลระบบต้องควบคุมให้หน่วยงานภายนอกจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงานและเอกสารที่  
เกี่ยวข้อง รวมทั้งต้องปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อใช้สำหรับควบคุมหรือตรวจสอบการทำงาน และ  
เพื่อให้มั่นใจว่าการปฏิบัติงานเป็นไปตามขอบเขตที่ได้กำหนดไว้
3. ผู้ดูแลระบบต้องแจ้งแนวปฏิบัติต่าง ๆ ที่เกี่ยวข้องแก่หน่วยงานภายนอกและผู้ใช้งานภายนอกเพื่อให้ปฏิบัติตาม
4. ผู้ดูแลระบบ ต้องกำกับดูแลหน่วยงานภายนอกและผู้ใช้งานภายนอกให้ปฏิบัติตามสัญญาหรือข้อตกลงการ  
ให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงด้านความมั่นคงปลอดภัย
5. ผู้ดูแลระบบ ต้องติดตาม ตรวจสอบรายงานหรือบันทึกการให้บริการของหน่วยงานภายนอกตามที่อ้างอิงอย่าง  
สม่ำเสมอตามสัญญาว่าจ้าง
6. ผู้ดูแลระบบ ต้องกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีหน้าที่ในการกำกับดูแล หรือ  
หน่วยงานที่เกี่ยวข้องกับการบังคับใช้กฎหมาย รวมทั้งหน่วยงานที่ควบคุมดูแลสถานการณ์ฉุกเฉินภายใต้  
สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน
7. ผู้ดูแลระบบ ต้องมีขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีความเชี่ยวชาญเฉพาะด้านหรือ  
หน่วยงานที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน
8. ผู้ดูแลระบบต้องควบคุมการเปลี่ยนแปลงของหน่วยงานภายนอกที่ส่งผลกระทบต่อการทำงานขององค์กร และ  
ต้องประเมินความเสี่ยงอย่างเหมาะสมเพื่อควบคุมผลกระทบอันเนื่องมาจากการเปลี่ยนแปลงนั้น
9. หน่วยงานภายนอกและผู้ใช้งานภายนอก ต้องใช้งานทรัพย์สินสารสนเทศของ รพม. ด้วยความระมัดระวัง และ  
รักษาความลับของ รพม. ไม่นำไปเปิดเผย และต้องขออนุญาตพร้อมทั้งปฏิบัติตามเงื่อนไขในการเข้าถึงระบบ  
สารสนเทศของ รพม. ทุกครั้ง
10. หน่วยงานภายนอกและผู้ใช้งานภายนอกต้องแจ้งเหตุการณ์ไม่ปกติต่าง ๆ ด้านเทคโนโลยีสารสนเทศที่พบผ่าน  
ช่องทางที่ รพม. กำหนดโดยเร็วที่สุด
11. หน่วยงานภายนอกและผู้ใช้งานภายนอกต้องจัดเก็บบัญชีผู้ใช้งานที่ รพม. จัดทำไว้ให้ใช้งานเป็นความลับ เฉพาะ  
บุคคล ไม่เปิดเผยให้ผู้อื่นรับทราบ

## ส่วนที่ 9

### การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ ของ รพม.

#### วัตถุประสงค์

- เพื่อควบคุมการใช้งานทรัพย์สินของ รพม. ประเภทเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ที่เหมาะสม ทั้งนี้ เพื่อป้องกันการสูญหาย เสียหาย หรือถูกเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

#### ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

#### อ้างอิงมาตรฐาน

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

#### แนวปฏิบัติ

##### 1. การใช้งานทั่วไป

- 1.1 ผู้ดูแลระบบต้องกำหนดบัญชีซอฟต์แวร์มาตรฐาน (Software standard) ที่อนุญาตให้ติดตั้งบนเครื่องคอมพิวเตอร์ของผู้ใช้งาน และปรับปรุงให้เป็นปัจจุบันเสมอ
- 1.2 ผู้ดูแลระบบต้องเป็นผู้กำหนดการตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) เท่านั้น
- 1.3 ผู้ใช้งานต้องติดตั้งโปรแกรมสำหรับควบคุมการใช้งานอุปกรณ์เคลื่อนที่ (Mobile Device Management: MDM) รวมถึงอุปกรณ์อื่น ๆ ที่ รพม. ไม่สามารถควบคุมการใช้งานผ่านระบบ Active Directory ได้
- 1.4 ผู้ใช้งานต้องใช้งานอย่างมีประสิทธิภาพเพื่องานของ รพม.
- 1.5 ผู้ใช้งานต้องไม่ติดตั้งโปรแกรมที่ละเมิดลิขสิทธิ์บนเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ของ รพม.
- 1.6 ผู้ใช้งานต้องขออนุญาตติดตั้งโปรแกรมในเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ตามขั้นตอนที่ รพม. กำหนด
- 1.7 ผู้ใช้งานต้องไม่ติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ของ รพม. การดำเนินการดังกล่าวต้องดำเนินการโดยผู้ดูแลระบบเท่านั้น
- 1.8 ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่อย่างละเอียด เพื่อให้สามารถใช้งานอย่างปลอดภัยและมีประสิทธิภาพ
- 1.9 ผู้ใช้งานต้องไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ และรักษาให้มีสภาพเดิม
- 1.10 ผู้ใช้งานต้องแจ้งซ่อมเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ที่อยู่ในความรับผิดชอบของ ผทท. ให้ ผทท. เป็นผู้ดำเนินการเท่านั้น
- 1.11 ผู้ใช้งานต้องอัปเดต Patch และระบบปฏิบัติการให้ทันสมัยอยู่เสมอ
- 1.12 ผู้ใช้งานต้องไม่สร้าง Shortcut ไว้บน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของ รพม.

- 1.13 กรณีเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์เคลื่อนที่ ผู้ใช้งานต้องปฏิบัติเพิ่มเติม ดังนี้
  - 1.13.1 ต้องติดตั้ง Application จาก Official Store หรือเว็บไซต์ที่ให้บริการผ่านโปรโตคอล https
  - 1.13.2 ไม่ปรับแต่งการเข้าถึงระบบปฏิบัติการ (rooted/jailbroken)
  - 1.13.3 ในกรณีที่มีการใช้งานอุปกรณ์ประเภทพกพาในที่สาธารณะ ห้องประชุม และพื้นที่ภายนอก อื่น ๆ ที่ไม่มีการป้องกัน หรือไม่ได้อยู่ในบริเวณของ รพม. ให้ป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต เช่น ไม่เปิดการเชื่อมต่อแบบไร้สายโดยไม่มีการเข้ารหัสข้อมูล เป็นต้น
  - 1.13.4 ต้องระมัดระวังการเคลื่อนย้าย โดยต้องใส่กระเป๋าเพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงานหรือหลุดมือ เป็นต้น
  - 1.13.5 ไม่ใส่ในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับหรืออาจถูกจับโยนได้
  - 1.13.6 การใช้งานเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัดต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง
  - 1.13.7 หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอย ชีตข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้
  - 1.13.8 ไม่วางของทับบนหน้าจอและแป้นพิมพ์
  - 1.13.9 การเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น
  - 1.13.10 ไม่เคลื่อนย้ายเครื่องในขณะที่ Harddisk กำลังทำงาน
  - 1.13.11 ไม่ใช้หรือวางใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่าง ๆ เป็นต้น
  - 1.13.12 ไม่วางใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูง เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น
  - 1.13.13 ไม่ติดตั้งหรือวางในที่ที่มีการสั่นสะเทือน เช่น ในยานพาหนะที่กำลังเคลื่อนที่
  - 1.13.14 การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้
  - 1.13.15 รับผิดชอบในการป้องกันการสูญหาย เช่น ต้องล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย
  - 1.13.16 นำติดตัวไปด้วยเสมอ เช่น ไม่ละทิ้ง อุปกรณ์ประมวลผลประเภทพกพาในรถยนต์ ห้องพักในโรงแรม หรือห้องประชุม เป็นต้น ในกรณีที่มีความจำเป็นต้องละทิ้งให้จัดเก็บไว้ในสถานที่ที่มั่นคงปลอดภัย
  - 1.13.17 ไม่เก็บหรือใช้งานในสถานที่ที่มีความร้อน ความชื้นหรือฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ
  - 1.13.18 ไม่เปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub component) ที่ติดตั้งอยู่ภายใน เช่น แบตเตอรี่ หน่วยความจำ
2. แนวปฏิบัติในการใช้รหัสผ่าน
  - ให้ผู้ใช้งานปฏิบัติตามการใช้งานรหัสผ่าน (Password Use) (ส่วนที่ 6)
3. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malicious code)

- 3.1 ผู้ดูแลระบบต้องควบคุมการ Update ระบบปฏิบัติการ เว็บเบราว์เซอร์ และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ
  - 3.2 ผู้ดูแลระบบต้องติดตั้งและปรับปรุงโปรแกรมป้องกันไวรัสให้ทันสมัยอยู่เสมอ
  - 3.3 ผู้ใช้งานต้องไม่ปิดหรือยกเลิกระบบการป้องกันไวรัสที่ติดตั้งอยู่
  - 3.4 ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อบันทึกต่าง ๆ เช่น Thumb drive และ Data storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์ของ รพม.
  - 3.5 ผู้ใช้งาน หากพบหรือสงสัยว่าเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ติดชุดคำสั่งไม่พึงประสงค์ ให้รีบยกเลิกเชื่อมต่อเครื่องเข้ากับระบบเครือข่ายสื่อสารข้อมูลเพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่น ๆ ได้ และแจ้ง ผทท. ทราบทันที
4. การสำรองข้อมูลและการกู้คืน
    - 4.1 ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ไว้บนสื่อบันทึกอื่น ๆ เช่น ระบบ File Sharing, CD, DVD, External harddisk เป็นต้น
    - 4.2 ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ
  5. ผู้ดูแลระบบ ต้องควบคุมให้เครื่องคอมพิวเตอร์ได้รับการปรับตั้งค่าอย่างเหมาะสม เพื่อป้องกันการใช้งานหรือติดตั้ง Mobile code เช่น Active x, Java จากแหล่งที่ไม่น่าเชื่อถือ

## ส่วนที่ 10

### การใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์

#### วัตถุประสงค์

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

#### ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

#### อ้างอิงมาตรฐาน

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

#### แนวปฏิบัติ

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

2. ผู้ใช้งานต้องไม่มีเจตนาปิดบังหรือบิดเบือนตัวตนเมื่อมีการใช้งานอินเทอร์เน็ต
3. ผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัส พร้อมทั้งต้องปรับปรุง Virus signature ที่เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพาให้มีความทันสมัยอยู่เสมอ ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web browser) และต้องปิดช่องโหว่ของระบบปฏิบัติการที่เว็บเบราว์เซอร์ติดตั้งอยู่
4. ผู้ใช้งานจะต้องตรวจสอบไวรัส (Virus scanning) ก่อนการรับ - ส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ต
5. ผู้ใช้งานต้องไม่ใช่เครือข่ายอินเทอร์เน็ตของ รฟม. เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น
6. ผู้ใช้งานจะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของ รฟม.
7. ผู้ใช้งานต้องหลีกเลี่ยงการกระทำที่สิ้นเปลืองทรัพยากรของเครือข่ายอินเทอร์เน็ต ดังนี้
  - (ก) ส่งจดหมายอิเล็กทรอนิกส์ลูกโซ่
  - (ข) ใช้เวลาในการเข้าถึงอินเทอร์เน็ตเกินความจำเป็นยกเว้นเพื่อปฏิบัติงานให้ รฟม.
  - (ค) เล่นเกม Online
  - (ง) เข้าห้องพูดคุย Online ที่ไม่ได้มีวัตถุประสงค์เพื่อปฏิบัติงานให้ รฟม.
8. ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เป็นการทำประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับ รฟม.
9. ผู้ใช้งานต้องไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของ รฟม.
10. ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต
11. ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ที่จะทำให้อื่นเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย
12. ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน
13. ผู้ใช้งานต้องคำนึงว่าข้อมูลจากอินเทอร์เน็ตอาจไม่มีความทันสมัยหรือไม่มีความถูกต้อง ผู้ใช้งานต้องตรวจสอบความถูกต้องของข้อมูลจากแหล่งที่น่าเชื่อถือก่อนที่จะเผยแพร่ข้อมูลดังกล่าว
14. ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา
15. ผู้ใช้งานต้องไม่ใช่ข้อมูลที่ช่วยุให้ร้ายในการเสนอความคิดเห็นที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของ 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 รพม.
  - 19.2 ผู้ใช้งานต้องระมัดระวังในการใช้สื่อสังคมออนไลน์ เนื่องจากพื้นที่บนสื่อสังคมออนไลน์เป็นพื้นที่สาธารณะไม่ใช่พื้นที่ส่วนบุคคล ซึ่งข้อมูลการใช้งานต่าง ๆ จะถูกบันทึกไว้และอาจมีผลทางกฎหมาย ถึงแม้จะเป็นการแสดงความคิดเห็นในนามชื่อบัญชีส่วนตัว และพึงตระหนักถึงผลกระทบที่อาจเกิดขึ้นกับ รพม. ได้
  - 19.3 ผู้ใช้งานที่ใช้สื่อสังคมออนไลน์เป็นเครื่องมือสื่อสารข้อมูลในกิจการของ รพม. หรือชื่อบุคคลที่ทำให้เข้าใจได้ว่าเป็นบุคคลในสังกัด ต้องแสดงภาพ และข้อมูลที่ถูกต้องชัดเจนในข้อมูล โปรไฟล์ (Profile) และพึงใช้ด้วยความสุภาพและมีวิจารณญาณ
  - 19.4 ผู้ใช้งานควรตั้งคำถามที่ใช้ในกรณีกู้คืนบัญชีผู้ใช้งานหรือกู้คืนรหัสผ่าน (Forgot your password) ควรหลีกเลี่ยงข้อมูลหรือคำถามที่เป็นส่วนบุคคลและเป็นข้อมูลที่ผู้อื่นคาดเดาได้ยากเพื่อป้องกันการสุ่มคำถามจากผู้ประสงค์ร้าย
  - 19.5 ผู้ใช้งานต้องไม่ใช้ระบบอีเมลของเว็บไซต์ประเภทสื่อสังคมออนไลน์ หากจำเป็นต้องใช้จะต้องระมัดระวังในการคลิกลิงก์ที่น่าสงสัย โดยเฉพาะอีเมลแจ้งเตือนจากเว็บไซต์ต่าง ๆ ในลักษณะเชิญให้คลิกลิงก์ที่แนบมาในอีเมล ผู้ใช้งานต้องสงสัยว่าลิงก์ดังกล่าวเป็นลิงก์ที่ไม่ปลอดภัย (ลิงก์ที่ถูกสร้างมาเพื่อใช้ขโมยข้อมูลส่วนบุคคล ด้วยการนำไปสู่เว็บไซต์ที่ดูน่าเชื่อถือที่ผู้ประสงค์ร้ายสร้างไว้เพื่อให้ผู้ใช้งานกรอกข้อมูลส่วนตัว เช่น รหัสผ่าน เป็นต้น)
  - 19.6 ผู้ใช้งานต้องศึกษาการตั้งค่าความเป็นส่วนตัวหรือ “Privacy settings” ให้เข้าใจเป็นอย่างดีและปรับแต่งการตั้งค่าความเป็นส่วนตัวให้เหมาะสมเพื่อป้องกันการถูกละเมิดความเป็นส่วนตัวซึ่งอาจจะส่งผลกระทบต่อตนเองหรือ รพม.
  - 19.7 ผู้ใช้งานต้องใช้งานสื่อสังคมออนไลน์อย่างเหมาะสม โดยไม่ละเมิดกฎหมายและไม่ก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานขององค์กร
  - 19.8 ผู้ใช้งานควรปิดการใช้งานระบบโพสต์ข้อความสาธารณะทุก ๆ ส่วนของเว็บไซต์ประเภท Social network หากจำเป็นต้องใช้งานต้องปรับค่าให้มีการตรวจสอบข้อความก่อนเพื่อหลีกเลี่ยงโอกาสแพร่กระจายลิงก์ที่ไม่ปลอดภัยจากผู้ประสงค์ร้าย ซึ่งเป็นหนึ่งในเทคนิคที่ใช้ในการโจมตีประเภท Spear-phishing
  - 19.9 ผู้ใช้งานต้องตรวจสอบก่อนจะรับเพื่อนเข้ากลุ่มในเว็บไซต์ประเภท Social network โดยต้องแน่ใจว่าข้อมูลส่วนตัวของเพื่อนคนนั้น เช่น รูปถ่ายและประวัติส่วนตัวไม่ถูกแก้ไขเพื่อปลอมแปลงตัวตนจากผู้ประสงค์ร้ายที่หวังแอบอ้างเพื่อคุกคามเป้าหมาย

- 19.10 ผู้ใช้งานต้องตระหนักไว้เสมอว่าข้อมูลต่าง ๆ ที่ผู้ใช้งานเผยแพร่ไว้บนบริการสื่อสังคมออนไลน์นั้นคงอยู่ถาวรและผู้อื่นอาจเข้าถึงและเผยแพร่ข้อมูลเหล่านั้นได้
- 19.11 ผู้ใช้งานต้องมีข้อพิจารณาในการรับเพื่อนเข้ากลุ่มที่ชัดเจน และควรประกาศข้อความปฏิเสธความรับผิดชอบที่เกี่ยวกับเนื้อหาหรือข้อความแสดงความคิดเห็นซึ่งถูกโพสต์จากเพื่อนในกลุ่มที่อาจปรากฏในเว็บไซต์ประเภท Social network ของผู้ใช้งานเอง
- 19.12 ผู้ใช้งานต้องติดตั้งซอฟต์แวร์ป้องกันไวรัส และอัปเดตฐานข้อมูลไวรัสของโปรแกรมอยู่เสมอ และต้องหลีกเลี่ยงการใช้โปรแกรมที่ละเมิดลิขสิทธิ์เพราะอาจจะมีโปรแกรมประสงค์ร้ายแฝงตัวอยู่ภายในเพื่อลักลอบ ปลอมแปลง หรือขโมยข้อมูลสำคัญของผู้ใช้งานได้
- 19.13 ผู้ใช้งานต้องระมัดระวังการใช้ถ้อยคำและภาษาที่อาจเป็นการดูหมิ่น ยุ้ง ทำร้าย หรือเป็นการละเมิดต่อบุคคลอื่น กรณีบุคคลอื่นมีความคิดเห็นที่แตกต่างพึงงดเว้นการโต้ตอบด้วยถ้อยคำรุนแรง
- 19.14 ผู้ใช้งานต้องระมัดระวังกระบวนการหาข่าว หรือภาพจากสื่อสังคมออนไลน์ โดยมีการตรวจสอบอย่างถี่ถ้วนรอบด้านและต้องอ้างอิงแหล่งที่มาเมื่อนำเสนอ เว้นแต่สามารถตรวจสอบและอ้างอิงจากแหล่งข่าวได้โดยตรง
- 19.15 หากผู้ใช้งานต้องการใช้สื่อสังคมออนไลน์เป็นเครื่องมือในการรายงานข่าวในนามของบุคคลธรรมดาต้องแสดงให้เห็นชัดเจนว่า ข้อความใดเป็น "ข่าว" ข้อความใดเป็น "ความคิดเห็นส่วนตัว"
- 19.16 การส่งต่อหรือเผยแพร่ข้อมูลในสื่อสังคมออนไลน์ (Social media)
- 19.16.1 ผู้ใช้งานต้องไม่ส่งต่อหรือเผยแพร่ข้อมูลที่เป็นเท็จ ข่าวลือ ข่าวไม่ปรากฏที่มา เป็นเพียงการคาดเดา หรือส่งผลเสียหายกับบุคคล สังคม หรือ รพม.
- 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 รพม. ให้มีความปลอดภัยและมีประสิทธิภาพ

#### ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

#### อ้างอิงมาตรฐาน

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

#### แนวปฏิบัติ

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

## ส่วนที่ 12

### การสำรองข้อมูลและการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

#### วัตถุประสงค์

- เพื่อให้มีข้อมูลสำรองไว้ใช้งานในกรณีที่ข้อมูลหลักเกิดความเสียหายไม่สามารถใช้งานหรือเข้าถึงได้ หรือเมื่อเกิดภาวะฉุกเฉินต่าง ๆ
- เพื่อให้มีการปฏิบัติที่สอดคล้องกับกฎหมาย พระราชบัญญัติ หรือข้อบังคับภายนอกอื่น ๆ

#### ผู้รับผิดชอบ

- ผู้บังคับบัญชา
- ผู้ดูแลระบบ
- เจ้าของข้อมูล
- ผู้ใช้งาน

#### อ้างอิงมาตรฐาน

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

#### แนวปฏิบัติ

##### 1. การสำรองข้อมูลระบบแม่ข่าย

ข้อมูลระบบแม่ข่ายและข้อมูลสำคัญซึ่งเป็นความลับของ รพม. ต้องได้รับการเก็บรักษาไว้ที่ระบบเก็บข้อมูลส่วนกลาง และสำรองข้อมูลไว้อย่างสม่ำเสมอ เพื่อให้มีข้อมูลสำรองไว้ใช้ ในกรณีที่ข้อมูลหลักเกิดความเสียหายหรือไม่สามารถใช้งาน ความถี่ในการดำเนินการสำรองข้อมูลและขั้นตอนการสำรองข้อมูลระบบแม่ข่ายเป็นความรับผิดชอบของ ผทท. โดยมีแนวปฏิบัติ ดังนี้

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

2. การสำรองข้อมูลคอมพิวเตอร์ส่วนบุคคล  
ผู้ใช้งานจะต้องสำรองข้อมูลสำคัญที่เก็บรักษาไว้ในเครื่องคอมพิวเตอร์ส่วนบุคคลหรือคอมพิวเตอร์ หรืออุปกรณ์พกพาอื่น ๆ อย่างสม่ำเสมอ ความถี่ในการสำรองข้อมูลขึ้นอยู่กับความถี่ของการเปลี่ยนแปลงของข้อมูลและระดับความสำคัญของข้อมูลหากเกิดการสูญหาย
3. การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์  
เพื่อให้สามารถระบุตัวบุคคลผู้ใช้งานได้อย่างถูกต้อง ผู้ดูแลระบบต้องดำเนินการดังนี้
  - 3.1 เลือกใช้นาฬิกาจากแหล่งที่น่าเชื่อถือที่มีการเชื่อมต่อในลำดับชั้น Stratum 0 โดยนาฬิกาจากแหล่งดังกล่าวจะต้องได้รับการอนุมัติให้ใช้งาน
  - 3.2 ตั้งนาฬิกาของอุปกรณ์ที่ให้บริการทุกชนิดจาก NTP Server ของ รฟม. เท่านั้น
  - 3.3 ต้องทบทวนนาฬิกาที่ NTP Server อย่างน้อยสัปดาห์ละ 1 ครั้ง
  - 3.4 ต้องจัดเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ โดยระยะเวลาในการเก็บตามประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 (อย่างน้อย 90 วัน)
  - 3.5 เก็บรักษาข้อมูลจราจรคอมพิวเตอร์ในสื่อที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง มีการเก็บรักษาความลับของข้อมูลตามระดับชั้นความลับในการเข้าถึงตามที่ รฟม. กำหนด
  - 3.6 ประเภทของสารสนเทศที่เก็บรักษา แสดงตามตาราง

ประเภทของสารสนเทศ	กฎหมายที่เกี่ยวข้อง	ระยะเวลาการเก็บรักษา (ปี)
Authentication server logs (RADIUS, TACACS)	1) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	1
Email server logs	2) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560	1
Web application server logs	3) ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม	1
NTP server logs	เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564	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 และจัดทำเป็นบัญชีรายชื่อระบบดังกล่าว รวมทั้งปรับปรุงรายชื่อระบบสำคัญและบัญชีฯ 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 ลิขสิทธิ์ในเอกสารหรือซอฟต์แวร์ เครื่องหมายการค้า สิทธิบัตร และใบอนุญาตการใช้งานซอร์สโค้ด หรือการใช้งานซอฟต์แวร์ เพื่อให้การดำเนินงานเป็นไปตามข้อกำหนดทั้งในแง่ของข้อสัญญา และด้านกฎหมาย พระราชบัญญัติ กฎระเบียบ ข้อบังคับด้านสินทรัพย์ทางปัญญาที่เกี่ยวข้อง
3. ผู้บังคับบัญชา ต้องควบคุมให้มีการคุ้มครองข้อมูลส่วนบุคคลโดยให้สอดคล้องกับกฎหมาย พระราชบัญญัติ กฎระเบียบ ข้อบังคับที่เกี่ยวข้อง
4. ผู้บังคับบัญชา ต้องกำกับดูแล และควบคุมการปฏิบัติงานของผู้ที่อยู่ใต้การบังคับบัญชา เพื่อป้องกันการใช้งานระบบสารสนเทศผิดวัตถุประสงค์ หรือละเมิดต่อนโยบายและแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของ รพม.
5. ผู้บังคับบัญชา ต้องควบคุมให้มีการป้องกันข้อมูลสำคัญขององค์กร ข้อมูลสำคัญที่เกี่ยวข้องกับข้อกำหนดทางกฎหมาย ระเบียบ ข้อบังคับ สัญญา ควรได้รับการป้องกันจากการสูญหาย ถูกทำลาย และปลอมแปลง

6. ผู้บังคับบัญชาต้องจัดให้มีการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยผู้ตรวจสอบภายใน (Internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External auditor) ตามระยะเวลาอย่างน้อยปีละ 1 ครั้ง
7. ผู้ดูแลระบบต้องกำหนดกระบวนการตรวจสอบและการแจ้งเตือนเมื่อเกิดเหตุผิดปกติเกี่ยวกับการใช้งานทรัพยากร (Capacity) กำหนดเกณฑ์การใช้งานทรัพยากรและวางแผนด้านทรัพยากรสารสนเทศให้รองรับการปฏิบัติงานในอนาคตอย่างเหมาะสม รวมถึงต้องติดตามผลการใช้งานทรัพยากรสารสนเทศ
8. ผู้ดูแลระบบต้องมีการตรวจสอบการทำงาน (Monitor) ของระบบรักษาความปลอดภัยและระบบปฏิบัติการอย่างสม่ำเสมอ
9. ผู้ดูแลระบบ ต้องป้องกันการเข้าใช้งานเครื่องมือที่ใช้เพื่อการตรวจสอบ เพื่อมิให้เกิดการใช้งานผิดประเภทหรือถูกละเมิดการใช้งาน (Compromise) โดยควบคุมการเข้าถึง และตรวจสอบการนำเครื่องมือไปใช้งานอย่างสม่ำเสมอ
10. ผู้ดูแลระบบต้องประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
11. ผู้บังคับบัญชาต้องติดตามผลการดำเนินการตามแผนบริหารจัดการความเสี่ยง (Risk treatment plan) เป็นประจำทุกไตรมาส
12. ผู้ดูแลระบบต้องประเมินความเสี่ยงแล้วจัดลำดับความสำคัญของความเสี่ยงนั้นและค้นหาวิธีการเพื่อลดความเสี่ยงตามขั้นตอนที่ รพม. กำหนด พร้อมทั้งพิจารณาข้อดีข้อเสียของวิธีการเหล่านั้นเพื่อให้ผู้บริหารของ รพม. ตัดสินใจเลือกวิธีการเพื่อลดความเสี่ยงหรือยอมรับความเสี่ยง เมื่อเลือกวิธีการลดความเสี่ยงแล้วผู้บริหารต้องจัดสรรทรัพยากรอย่างเพียงพอเพื่อดำเนินการ แนวทางการลดความเสี่ยง แบ่งได้เป็น 3 รูปแบบ ได้แก่
  - 12.1 การเลือกใช้เทคโนโลยี เพื่อใช้ในการลดความเสี่ยงและเพิ่มความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รพม. เป็นวิธีที่จำเป็นต้องใช้งบประมาณและทรัพยากรอย่างเพียงพอในการดำเนินการ เช่น การเลือกใช้อุปกรณ์ Firewall มากกว่าหนึ่งผลิตภัณฑ์ในการป้องกันการเข้าถึงเครือข่ายที่สำคัญ การใช้อุปกรณ์สมาร์ตการ์ด หรือ USB Token ในการตรวจสอบยืนยันตัวตนในการเข้าใช้งานระบบจากภายนอก รพม. เป็นต้น
  - 12.2 การปรับเปลี่ยนขั้นตอนปฏิบัติ ต้องออกแบบขั้นตอนปฏิบัติใหม่ที่รัดกุมและสามารถรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รพม. ได้ดีขึ้น เมื่อกำหนดขั้นตอนปฏิบัติใหม่แล้วต้องมีการพิจารณาหาหรือความเหมาะสม ความเป็นไปได้ และผู้บริหารต้องเป็นผู้อนุมัติให้มีการบังคับใช้ขั้นตอนปฏิบัติใหม่นั้น
  - 12.3 ผู้ดูแลระบบต้องแจ้งขั้นตอนปฏิบัติให้ผู้เกี่ยวข้องรับรู้อย่างทั่วถึง รวมทั้งต้องจัดฝึกอบรมผู้ใช้งานที่เกี่ยวข้องเพื่อให้สามารถปฏิบัติตามขั้นตอนปฏิบัติใหม่ได้อย่างราบรื่นและมีประสิทธิภาพ
13. การตรวจสอบความปลอดภัยของระบบสารสนเทศ
  - 13.1 ผู้ดูแลระบบ ต้องวางแผนการตรวจสอบและประเมินช่องโหว่หรือจุดอ่อนด้านความมั่นคงปลอดภัยสารสนเทศ และแจ้งผู้ที่เกี่ยวข้องเพื่อแก้ไขในกรณีที่พบว่าช่องโหว่หรือจุดอ่อนนั้นอาจเป็นเหตุการณ์ด้านความมั่นคงปลอดภัย อย่างน้อยปีละ 1 ครั้ง
  - 13.2 ผู้ดูแลระบบต้องตรวจสอบระบบสารสนเทศที่จะต้องมีการปรับปรุงเมื่อมีเวอร์ชันใหม่ (Patch) รวมทั้งข้อมูลที่เกี่ยวข้องกับช่องโหว่ด้านเทคนิคอย่างสม่ำเสมอเพื่อให้ทราบถึงภัยคุกคามและความเสี่ยง รวมถึงหาวิธีป้องกันและแก้ไขที่เหมาะสมกับช่องโหว่นั้น
  - 13.3 ผู้ใช้งาน ผู้ดูแลระบบ และหน่วยงานภายนอก ต้องบันทึกและรายงานช่องโหว่หรือจุดอ่อนใด ๆ ด้านความมั่นคงปลอดภัยสารสนเทศ ที่อาจสังเกตพบระหว่างการติดตามการใช้งานระบบสารสนเทศ ผ่านช่องทางบริหารจัดการที่กำหนดไว้อย่างเหมาะสม และต้องดำเนินการปิดช่องโหว่ที่มีการตรวจพบหรือได้รับแจ้ง



14. 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 หรือแลกเปลี่ยนผ่านระบบสารสนเทศให้เหมาะสมตามระดับชั้นความลับข้อมูลสารสนเทศ ตามขั้นตอนที่ รพม. กำหนด
2. ผู้บังคับบัญชา และเจ้าของข้อมูล ต้องควบคุมให้มีการจัดทำข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศระหว่างองค์กรกับบุคคลหรือหน่วยงานภายนอก
3. ผู้ดูแลระบบต้องแลกเปลี่ยนข้อมูลสารสนเทศต้องแลกเปลี่ยนผ่านช่องทางที่ปลอดภัย เช่น Web Service ที่ใช้งานผ่านโปรโตคอล https
4. ผู้ดูแลระบบ ต้องมีการป้องกันข้อมูลสารสนเทศที่มีการสื่อสารกันผ่านข้อมูลอิเล็กทรอนิกส์ (Electronic messaging) เช่น จดหมายอิเล็กทรอนิกส์ (E-mail) หรือ Instant messaging ด้วยวิธีการหรือมาตรการที่เหมาะสม
5. ผู้ดูแลระบบ ต้องป้องกันข้อมูลสารสนเทศที่มีการแลกเปลี่ยนในการทำพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce) ผ่านเครือข่ายคอมพิวเตอร์สาธารณะ เพื่อมิให้มีการฉ้อโกง ละเมิดสัญญา หรือมีการรั่วไหล หรือข้อมูลสารสนเทศถูกแก้ไขโดยมิได้รับอนุญาต
6. ผู้ดูแลระบบ ต้องป้องกันข้อมูลสารสนเทศที่มีการสื่อสาร หรือแลกเปลี่ยนในการทำธุรกรรมทางออนไลน์ (Online transaction) เพื่อมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ ส่งข้อมูลไปผิดที่ การรั่วไหลของข้อมูล ข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ หรือถูกส่งซ้ำโดยมิได้รับอนุญาต
7. ผู้ดูแลระบบ ต้องควบคุมการรับส่งข้อมูลสารสนเทศเพื่อป้องกันความผิดพลาด ดังนี้
  - 7.1 ความไม่สมบูรณ์ของข้อมูลสารสนเทศที่รับ-ส่ง
  - 7.2 การส่งข้อมูลสารสนเทศผิดจุดหมายปลายทาง
  - 7.3 การเปลี่ยนแปลงข้อมูลสารสนเทศโดยมิได้รับอนุญาต

- 7.4 การเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต
  - 7.5 การเข้าถึงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต
  - 7.6 การนำข้อมูลสารสนเทศกลับมาใช้ใหม่โดยไม่ได้รับอนุญาต
8. เจ้าของข้อมูล และผู้ดูแลระบบ ต้องมีการป้องกันข้อมูลสารสนเทศที่มีการเผยแพร่ต่อสาธารณชน มิให้มีการแก้ไขเปลี่ยนแปลงโดยมิได้รับอนุญาต เพื่อรักษาความถูกต้องครบถ้วนของข้อมูลสารสนเทศ

## ส่วนที่ 15

### การควบคุมการเข้ารหัส

#### วัตถุประสงค์

- เพื่อให้มีการเข้ารหัสข้อมูลอย่างเหมาะสมและมีประสิทธิภาพในการปกป้องความลับ ป้องกัน การปลอมแปลงข้อมูล และควบคุมความถูกต้องของข้อมูล

#### ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- เจ้าของข้อมูล
- ผู้ใช้งาน

#### อ้างอิงมาตรฐาน

- หมวดที่ 6 การเข้ารหัสข้อมูล (Cryptography)

#### แนวปฏิบัติ

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

ประเภทกุญแจ / วิธีการเข้ารหัส	เกณฑ์ขั้นต่ำ	ความยาวกุญแจ (อย่างน้อย)
กุญแจแบบสมมาตร (Symmetric)	AES	256 bits
กุญแจแบบอสมมาตร (Asymmetric)	RSA	1024 bits
การ Hashing	BCrypt	Cost Factor 10 ขึ้นไป

4. ผู้ดูแลระบบ ต้องมีการทบทวนขั้นตอนวิธี (Algorithm) และความยาวของกุญแจที่เข้ารหัสอย่างน้อยปีละ 1 ครั้ง เพื่อให้ยังสามารถรักษาไว้ซึ่งความมั่นคงปลอดภัย
5. ผู้ดูแลระบบ ต้องกำหนดให้มีการบริหารจัดการกุญแจที่ใช้ในการเข้ารหัส ดังนี้
  - 5.1 การสร้างกุญแจรหัสควรกระทำในสถานที่ที่มีมาตรการป้องกันความปลอดภัย
  - 5.2 เมื่อมีการสร้างกุญแจรหัสที่เป็นกุญแจลับ (Private key) ควรส่งมอบให้กับเจ้าของกุญแจโดยตรง โดยวิธีการที่ปลอดภัย
  - 5.3 ควรจัดให้มีการเก็บบันทึก Log เพื่อการตรวจสอบสำหรับกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับการจัดการกุญแจรหัส
6. ผู้ใช้งาน ควรรักษาความปลอดภัยในการใช้งานกุญแจ ดังนี้
  - 6.1 เก็บกุญแจรหัสในสถานที่ที่ปลอดภัย เช่น ตู้นิรภัย หรือสื่อบันทึกที่ปลอดภัย และไม่มีใครสามารถเข้าถึงได้

- 6.2 เมื่อมีการรับกุญแจสาธารณะ (Public key) มาใช้ ก่อนใช้งานจะต้องพิสูจน์ความถูกต้องของกุญแจสาธารณะ โดยสอบถามกับผู้ส่งหรือตรวจสอบกับผู้แทนในการรับรองความถูกต้องของกุญแจสาธารณะ (Certificate authority) ที่เชื่อถือได้เท่านั้น
- 6.3 ควบคุมการใช้งานและจัดเก็บกุญแจให้สอดคล้องกับการรักษาความลับข้อมูลตามที่ รฟม. กำหนด

## ส่วนที่ 16

### การนำอุปกรณ์ส่วนตัวมาใช้งาน (Bring your own device)

#### วัตถุประสงค์

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

#### ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

#### อ้างอิงมาตรฐาน

- หมวดที่ 2 อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากระยะไกล (Mobile devices and teleworking)

#### แนวปฏิบัติ

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

12. กรณีอุปกรณ์ส่วนตัวสูญหายหรือถูกขโมยผู้ใช้งานต้องแจ้งผู้ดูแลระบบโดยเร็วที่สุด เพื่อจัดการข้อมูลที่จัดเก็บอยู่ในอุปกรณ์ส่วนตัวของผู้ใช้งาน
13. ผู้ใช้งานต้องเข้าถึงระบบสารสนเทศของ รพม. ผ่านช่องทางที่ รพม. กำหนด เช่น VPN

ภาคผนวก จ.

สัญญาการเก็บรักษาข้อมูลไว้เป็นความลับ (Non-Disclosure Agreement)

 At Joint U.   
h. 9.5.





## สัญญาการเก็บรักษาข้อมูลไว้เป็นความลับ

สัญญาฉบับนี้ทำขึ้น ณ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย เลขที่ 175 ถนนพระราม 9  
แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร เมื่อวันที่ ..... ระหว่าง

การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย สำนักงานตั้งอยู่เลขที่ 175 ถนนพระราม 9  
แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร โดย .....  
.....ซึ่งต่อไปในสัญญานี้เรียกว่า “รฟม.” ฝ่ายหนึ่ง กับ

นาย/นาง/นางสาว/ ..... เลขที่บัตรประชาชน .....  
ซึ่งต่อไปในสัญญานี้เรียกว่า “ผู้รับข้อมูล” อีกฝ่ายหนึ่ง

ตามที่ ..... (คู่สัญญา เช่น กลุ่มบริษัท/บริษัท/มหาวิทยาลัย/ฯลฯ)  
..... ได้ตกลงทำสัญญา ..... เลขที่ .....  
เมื่อวันที่ ..... กับ รฟม. ซึ่งต่อไปในสัญญานี้เรียกว่า “สัญญาโครงการ” โดย .....  
(คู่สัญญา) ..... จะได้รับข้อมูลจาก รฟม. เพื่อใช้ในการปฏิบัติงาน ซึ่งในการ  
ดำเนินงานดังกล่าว ..... (คู่สัญญา) ..... ได้มอบหมายให้ผู้รับ  
ข้อมูลประสานขอข้อมูลจาก รฟม. เพื่อนำไปประกอบการปฏิบัติงานที่เกี่ยวข้องสำหรับการดำเนินโครงการ  
..... นั้น

ทั้งสองฝ่ายจึงตกลงทำสัญญากัน ดังมีข้อความต่อไปนี้

1. ในสัญญาฉบับนี้ “ข้อมูล” หมายถึง สิ่งที่มีชื่อความหมายให้รู้เรื่องราวข้อเท็จจริง ข้อมูล  
หรือสิ่งใด ๆ ไม่ว่าจะการสื่อความหมายนั้นจะทำได้โดยสภาพสิ่งของนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่า  
จะได้จัดทำไว้ในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผ่นผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การ  
บันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดในระบบ  
คอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์  
ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

2. ผู้รับข้อมูลให้สัญญาแก่ รฟม. ว่าข้อมูลที่รับจาก รฟม. หรือในนามของ รฟม. ผู้รับข้อมูล  
จะใช้เพื่อประกอบการปฏิบัติงานที่เกี่ยวข้องสำหรับดำเนินโครงการ .....  
ตามสัญญาโครงการเท่านั้น และจะไม่นำไปใช้เพื่อวัตถุประสงค์อื่น เช่น ใช้เพื่อวัตถุประสงค์ในเชิงพาณิชย์  
การพัฒนาเป็นผลิตภัณฑ์หรือเทคโนโลยีอื่น การใช้หรือพยายามใช้ข้อมูลเพื่อการอื่น การอ้างอิงหรือรวมเข้า  
ไปเป็นส่วนหนึ่งของการประดิษฐ์ใด ๆ การรับขอความคุ้มครองจากทรัพย์สินทางปัญญาใด ๆ ของผู้รับข้อมูล  
เว้นแต่ได้รับการอนุญาตจาก รฟม. เป็นลายลักษณ์อักษรก่อน

3. ผู้รับข้อมูลจะต้องปกปิดข้อมูลทั้งหมดที่ได้มีการเปิดเผยภายใต้สัญญาโครงการนี้ไว้เป็น  
ความลับอย่างเคร่งครัด

4. ถ้าข้อกำหนดใด ๆ ตามสัญญาฉบับนี้ตกเป็นโมฆะ ให้ข้อสัญญาที่เหลืออยู่ในสัญญาฉบับนี้  
คงใช้บังคับและมีผลอยู่อย่างสมบูรณ์

/5. หากผู้รับ ...

5. หากผู้รับข้อมูลไม่ปฏิบัติตามกฎหมาย หรือฝ่าฝืนสัญญาไม่ว่าข้อใดข้อหนึ่ง ผู้รับข้อมูล ยินยอมชดใช้ค่าเสียหายใด ๆ ที่เกิดขึ้นหรือที่เกี่ยวข้องเนื่องแก่ รพม. ทั้งสิ้น

สัญญาฉบับนี้ทำขึ้นเป็นสองฉบับมีข้อความถูกต้องตรงกัน คู่สัญญาได้อ่านและเข้าใจข้อความ ในสัญญานี้แล้ว เห็นว่าถูกต้องตรงตามเจตนาของตน จึงได้ลงนามและประทับตรา (ถ้ามี) ไว้ต่อหน้าพยานและ ยึดถือไว้ฝ่ายละหนึ่งฉบับ


การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

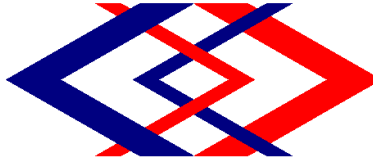
ลงชื่อ .....  
(.....)  
ตำแหน่ง ผู้อำนวยการฝ่าย/สำนัก.....  
วันที่ ...../...../.....

ลงชื่อ ..... ผู้รับข้อมูล  
(.....)  
วันที่ ...../...../.....

ลงชื่อ ..... พยาน  
(.....)  
ตำแหน่ง .....  
วันที่ ...../...../.....

ลงชื่อ ..... พยาน  
(.....)  
วันที่ ...../...../.....

  
Joint U.



## ประกาศการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

เรื่อง ประกวดราคาเช่าเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ ประจำปีงบประมาณ ๒๕๖๘ - ๒๕๗๐

ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding)

การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย มีความประสงค์จะประกวดราคาเช่าเครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์ ประจำปีงบประมาณ ๒๕๖๘ - ๒๕๗๐ ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding) ราคากลางของงานเช่า ในการประกวดราคาครั้งนี้ เป็นเงินทั้งสิ้น ๒๗,๑๔๒,๙๒๐.๐๐ บาท (ยี่สิบเจ็ดล้านหนึ่งแสนสี่หมื่นสองพันเก้าร้อยยี่สิบบาทถ้วน) ตามรายการ ดังนี้

เช่าเครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์ จำนวน ๑ งาน  
ประจำปีงบประมาณ ๒๕๖๘ - ๒๕๗๐

ผู้ยื่นข้อเสนอจะต้องมีคุณสมบัติ ดังต่อไปนี้

๑. มีความสามารถตามกฎหมาย
๒. ไม่เป็นบุคคลล้มละลาย
๓. ไม่อยู่ระหว่างเลิกกิจการ
๔. ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง
๕. ไม่เป็นบุคคลซึ่งถูกระงับชื่อไว้ในบัญชีรายชื่อผู้ทำงานและได้แจ้งเวียนชื่อให้เป็นผู้ทำงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทำงานเป็นหุ้นส่วน ผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย
๖. มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา
๗. เป็นนิติบุคคลผู้มีอาชีพขายหรือให้เช่าพัสดุที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว
๘. ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรม ในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้
๙. ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งสละเอกสิทธิ์และความคุ้มกันเช่นนั้น
๑๐. ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ต้องมีคุณสมบัติดังนี้  
กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค่างำหนดให้ผู้เข้าร่วมค้ำรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงระหว่างผู้เข้าร่วมค้าจะต้องมีการกำหนดสัดส่วนหน้าที่และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ำรายอื่นทุกราย

/กรณีที...

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมคำกำหนดให้ผู้เข้าร่วมคำรายใดรายหนึ่งเป็นผู้เข้าร่วมคำหลัก  
กิจการร่วมค่านั้นต้องใช้ผลงานของผู้เข้าร่วมคำหลักรายเดียวเป็นผลงานของกิจการร่วมคำที่ยื่นข้อเสนอ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมคำที่ไม่ได้กำหนดให้ผู้เข้าร่วมคำรายใดเป็นผู้เข้าร่วมคำหลัก  
ผู้เข้าร่วมคำทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมคำกำหนดให้มีการมอบหมายผู้เข้าร่วมคำรายใดรายหนึ่ง  
เป็นผู้ยื่นข้อเสนอ ในนามกิจการร่วมคำ การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมคำที่ไม่ได้กำหนดให้ผู้เข้าร่วมคำรายใดเป็นผู้ยื่นข้อเสนอ  
ผู้เข้าร่วมคำทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมคำรายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอใน  
นามกิจการร่วมคำ

๑๑. ผู้ยื่นข้อเสนอต้องลงทะเบียนที่มีข้อมูลถูกต้องครบถ้วนในระบบจัดซื้อจัดจ้างภาครัฐด้วย  
อิเล็กทรอนิกส์ (Electronic Government Procurement : e-GP) ของกรมบัญชีกลาง

๑๒. ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

(๑) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า ๑ ปี  
ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิ ที่ปรากฏในงบแสดงฐานะการเงิน  
ที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ

(๒) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีงบแสดง  
ฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้อง  
มีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ไม่ต่ำกว่า ๘ ล้านบาท

(๓) สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเงินเกิน ๕๐๐,๐๐๐ บาทขึ้นไป กรณีผู้ยื่นข้อเสนอ  
เป็นบุคคลธรรมดา โดยพิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน ๙๐ วัน ก่อนวันยื่นข้อเสนอ โดยต้องมีเงิน  
ฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอ  
ในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชี  
เงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

(๔) กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะ  
เข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่างบประมาณของ  
โครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง (สินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัท  
เงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้าประกันตาม  
ประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบโดย  
พิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบ  
อำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน ๙๐ วัน)

/(๕) กรณีตาม...

(๕) กรณีตาม (๑) - (๔) ยกเว้นสำหรับกรณีดังต่อไปนี้

(๕.๑) กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ

(๕.๒) นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติ

ล้มละลาย (ฉบับที่ ๑๐) พ.ศ. ๒๕๖๑

๑๓. ผู้ยื่นข้อเสนอต้องมีหนังสือรับรองการเป็นตัวแทนจำหน่ายผลิตภัณฑ์ที่มีอายุไม่เกิน ๙๐ วัน นับจากวันที่ออกหนังสือจนถึงวันที่ยื่นข้อเสนอนี้ จากบริษัทผู้ผลิต หรือบริษัทสาขาของผู้ผลิตในต่างประเทศ หรือ บริษัทสาขาของผู้ผลิตในประเทศไทย หรือตัวแทนจำหน่ายในประเทศไทย โดยต้องออกให้เพื่อยืนยันข้อเสนอนี้ ทั้งนี้ ผู้ยื่นข้อเสนอจะต้องแนบหนังสือรับรองดังกล่าวเพื่อประกอบการพิจารณา เฉพาะรายการดังต่อไปนี้

๑๓.๑ เครื่องคอมพิวเตอร์ สำหรับงานสำนักงาน

๑๓.๒ เครื่องคอมพิวเตอร์ สำหรับงานกราฟิก

๑๓.๓ เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานสำนักงาน แบบที่ ๑

๑๓.๔ เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานสำนักงาน แบบที่ ๒

๑๓.๕ เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานประมวลผล

๑๓.๖ เครื่องสำรองไฟฟ้า

ผู้ยื่นข้อเสนอต้องยื่นข้อเสนอและเสนอราคาทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ในวันที่ .....ระหว่างเวลา.....น. ถึง.....น.

ผู้สนใจสามารถขอรับเอกสารประกวดราคาอิเล็กทรอนิกส์ โดยดาวน์โหลดเอกสารทางระบบจัดซื้อจัดจ้าง ภาครัฐด้วยอิเล็กทรอนิกส์ หัวข้อ ค้นหาประกาศจัดซื้อจัดจ้างได้ตั้งแต่วันที่ประกาศจนถึงวันเสนอราคา

ผู้ยื่นข้อเสนอสามารถเตรียมเอกสารข้อเสนอได้ตั้งแต่วันที่ประกาศจนถึงวันเสนอราคา

ผู้สนใจสามารถดูรายละเอียดได้ที่เว็บไซต์ [www.mrta.co.th](http://www.mrta.co.th) หรือ [www.gprocurement.go.th](http://www.gprocurement.go.th) หรือสอบถามทางโทรศัพท์หมายเลข ๐ ๒๗๑๖ ๔๐๐๐ ต่อ ๑๖๗๕ ในวันและเวลาราชการ

ประกาศ ณ วันที่ ๑๓ มิถุนายน พ.ศ. ๒๕๖๗



(นายพัฒนพงษ์ พงศ์ศุภสมิทธิ)

รองผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย (บริหาร)  
ปฏิบัติการแทน ผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย



เอกสารประกวดราคาเช่าด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding)

เลขที่

ประกวดราคาเช่าเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ ประจำปีงบประมาณ ๒๕๖๘ - ๒๕๗๐

ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding)

ตามประกาศ การรถไฟฟ้ายานขนส่งมวลชนแห่งประเทศไทย

ลงวันที่ มิถุนายน ๒๕๖๗

การรถไฟฟ้ายานขนส่งมวลชนแห่งประเทศไทย ซึ่งต่อไปนี้จะเรียกว่า "รฟม." มีความประสงค์จะประกวดราคาเช่าด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ ตามรายการ ดังนี้

เช่าเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ จำนวน ๑ งาน  
ประจำปีงบประมาณ ๒๕๖๘ - ๒๕๗๐

พัสดุที่จะเช่านี้ต้องเป็นของแท้ ของใหม่ ไม่เคยใช้งานมาก่อน ไม่เป็นของเก่าเก็บ อยู่ในสภาพที่จะใช้งานได้ทันที และมีคุณลักษณะเฉพาะตรงตามที่กำหนดไว้ในเอกสารประกวดราคาเช่าด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ฉบับนี้ โดยมีข้อแนะนำและข้อกำหนด ดังต่อไปนี้

๑. เอกสารแนบท้ายเอกสารประกวดราคาอิเล็กทรอนิกส์

- ๑.๑ ร่างรายละเอียดขอบเขตของงานทั้งโครงการ (Terms of Reference : TOR)
- ๑.๒ แบบใบเสนอราคาที่กำหนดไว้ในระบบการจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์
- ๑.๓ แบบสัญญาเช่าคอมพิวเตอร์
- ๑.๔ แบบหนังสือค้ำประกัน
  - (๑) หลักประกันการเสนอราคา
  - (๒) หลักประกันสัญญา
- ๑.๕ บทนิยาม
  - (๑) ผู้ที่มีผลประโยชน์ร่วมกัน
  - (๒) การขัดขวางการแข่งขันอย่างเป็นธรรม
- ๑.๖ แบบบัญชีเอกสารที่กำหนดไว้ในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์
  - (๑) บัญชีเอกสารส่วนที่ ๑
  - (๒) บัญชีเอกสารส่วนที่ ๒
- ๑.๗ แผนการทำงาน

## ๒. คุณสมบัติของผู้ยื่นข้อเสนอ

๒.๑ มีความสามารถตามกฎหมาย

๒.๒ ไม่เป็นบุคคลล้มละลาย

๒.๓ ไม่อยู่ระหว่างเลิกกิจการ

๒.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๒.๕ ไม่เป็นบุคคลซึ่งถูกระงับชื่อไว้ในบัญชีรายชื่อผู้ทำงานและได้แจ้งเวียนชื่อให้เป็นผู้ทำงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทำงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๒.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๒.๗ เป็นนิติบุคคลผู้มีอาชีพขายหรือให้เช่าพัสดุที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

๒.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ รพม. ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวาง การแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๒.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาล ของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นนั้น

๒.๑๐ ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ต้องมีคุณสมบัติดังนี้

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงระหว่างผู้เข้าร่วมค้าจะต้องมีการกำหนดสัดส่วนหน้าที่และความรับผิดชอบในปริมาณงาน สิ่งของหรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค่านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอ ในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

๒.๑๑ ยื่นข้อเสนอต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement: e - GP) ของกรมบัญชีกลาง

๒.๑๒ ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

(๑) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า ๑ ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ

(๒) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งยังไม่มีงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ไม่ต่ำกว่า ๘ ล้านบาท

(๓) สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเงินเกิน ๕๐๐,๐๐๐ บาทขึ้นไป กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดา โดยพิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน ๙๐ วัน ก่อนวันยื่นข้อเสนอ โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

(๔) กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียนหรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง (สินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้าประกัน ตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน ๙๐ วัน)

(๕) กรณีตาม (๑) - (๔) ยกเว้นสำหรับกรณีดังต่อไปนี้

(๕.๑) กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ

(๕.๒) นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตาม

พระราชบัญญัติล้มละลาย (ฉบับที่ ๑๐) พ.ศ. ๒๕๖๑

๒.๑๓ ผู้ยื่นข้อเสนอต้องมีหนังสือรับรองการเป็นตัวแทนจำหน่ายผลิตภัณฑ์ที่มีอายุไม่เกิน ๙๐ วันนับจากวันที่ออกหนังสือจนถึงวันที่ยื่นข้อเสนอนี้ จากบริษัทผู้ผลิต หรือบริษัทสาขาของผู้ผลิตในต่างประเทศ หรือบริษัทสาขาของผู้ผลิตในประเทศไทย หรือตัวแทนจำหน่ายในประเทศไทย โดยต้องออกให้เพื่อยื่นข้อเสนอนี้ ทั้งนี้ ผู้ยื่นข้อเสนอจะต้องแนบหนังสือรับรองดังกล่าวเพื่อประกอบการพิจารณา เฉพาะรายการดังต่อไปนี้

๒.๑๓.๑ เครื่องคอมพิวเตอร์ สำหรับงานสำนักงาน

๒.๑๓.๒ เครื่องคอมพิวเตอร์ สำหรับงานกราฟิก

๒.๑๓.๓ เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานสำนักงาน แบบที่ ๑

๒.๑๓.๔ เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานสำนักงาน แบบที่ ๒

๒.๑๓.๕ เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานประมวลผล

๒.๑๓.๖ เครื่องสำรองไฟฟ้า



### ๓. หลักฐานการยื่นข้อเสนอ

ผู้ยื่นข้อเสนอจะต้องเสนอเอกสารหลักฐานทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ โดยแยกเป็น ๒ ส่วน คือ

#### ๓.๑ ส่วนที่ ๑ อย่างน้อยต้องมีเอกสารดังต่อไปนี้

(๑) ในกรณีผู้ยื่นข้อเสนอเป็นนิติบุคคล

(ก) ห้างหุ้นส่วนสามัญหรือห้างหุ้นส่วนจำกัด ให้ยื่นสำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล บัญชีรายชื่อหุ้นส่วนผู้จัดการ ผู้มีอำนาจควบคุม (ถ้ามี)

(ข) บริษัทจำกัดหรือบริษัทมหาชนจำกัด ให้ยื่นสำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล หนังสือบริคณห์สนธิ บัญชีรายชื่อกรรมการผู้จัดการ ผู้มีอำนาจควบคุม (ถ้ามี) และบัญชีผู้ถือหุ้นรายใหญ่ (ถ้ามี)

(๒) ในกรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดาหรือคณะบุคคลที่ไม่มีนิติบุคคล ให้ยื่นสำเนาบัตรประจำตัวประชาชนของผู้ยื่น ข้อเสนอข้อตกลงที่แสดงถึงการเข้าเป็นหุ้นส่วน (ถ้ามี) สำเนาบัตรประจำตัวประชาชนของผู้เป็นหุ้นส่วน หรือสำเนาหนังสือเดินทางของผู้เป็นหุ้นส่วนที่ได้ถือสัญชาติไทย

(๓) ในกรณีผู้ยื่นข้อเสนอเป็นผู้ยื่นข้อเสนอร่วมกันในฐานะเป็นผู้ร่วมค้า ให้ยื่นสำเนาสัญญาของการเข้าร่วมค้า และเอกสารตามที่ระบุไว้ใน (๑) หรือ (๒) ของผู้ร่วมค้า แล้วแต่กรณี

(๔) ผู้ยื่นข้อเสนอต้องแสดงหลักฐานเกี่ยวกับมูลค่าสุทธิของกิจการ ดังนี้

(๔.๑) ในกรณีผู้ยื่นข้อเสนอเป็นนิติบุคคล ให้ยื่นงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ โดยให้ยื่นขณะเข้าเสนอราคา

(๔.๒) ในกรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดา ให้ยื่นหนังสือรับรองบัญชีเงินฝากไม่เกิน ๙๐ วันก่อนวันยื่นข้อเสนอ โดยให้ยื่นขณะเข้าเสนอราคา และจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

(๔.๓) กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการและทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ ให้ยื่นสำเนาหนังสือรับรองวงเงินสินเชื่อ (สินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้าประกัน ตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรองหรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน ๙๐ วัน)

(๕) สำเนาใบสำคัญแสดงการจดทะเบียนห้างหุ้นส่วนบริษัท

(๖) สำเนาหนังสือรับรองบริษัท

(๗) สำเนาใบทะเบียนภาษีมูลค่าเพิ่ม (ภ.พ.๒๐) (ถ้ามี)

(๘) บัญชีเอกสารส่วนที่ ๑ ทั้งหมดที่ได้ยื่นพร้อมกับการเสนอราคาทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ ตามแบบในข้อ ๑.๖ (๑) โดยไม่ต้องแนบในรูปแบบ PDF File (Portable Document Format)

ทั้งนี้ เมื่อผู้ยื่นข้อเสนอดำเนินการแนบไฟล์เอกสารตามบัญชีเอกสารส่วนที่ ๑ ครบถ้วน ถูกต้องแล้ว ระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์จะสร้างบัญชีเอกสารส่วนที่ ๑ ตามแบบ ในข้อ ๑.๖ (๑) ให้โดยผู้ยื่นข้อเสนอไม่ต้องแนบบัญชีเอกสารส่วนที่ ๑ ดังกล่าวในรูปแบบ PDF File (Portable Document Format)

### ๓.๒ ส่วนที่ ๒ อย่างน้อยต้องมีเอกสารดังต่อไปนี้

(๑) ในกรณีที่ผู้ยื่นข้อเสนอมอบอำนาจให้บุคคลอื่นกระทำการแทนให้แนบหนังสือมอบอำนาจซึ่งติดอากรแสตมป์ตามกฎหมาย โดยมีหลักฐานแสดงตัวตนของผู้มอบอำนาจและผู้รับมอบอำนาจ ทั้งนี้ หากผู้รับมอบอำนาจเป็นบุคคลธรรมดาต้องเป็นผู้ที่บรรลุนิติภาวะตามกฎหมายแล้วเท่านั้น

(๒) แคตตาล็อกและ/หรือรายละเอียดคุณลักษณะเฉพาะ ตามข้อ ๔.๔

(๓) หลักประกันการเสนอราคา ตามข้อ ๕

(๔) สำเนาหนังสือรับรองสินค้า Made In Thailand ของสภาอุตสาหกรรมแห่งประเทศไทย (ถ้ามี)

(๕) สำเนาใบขึ้นทะเบียนผู้ประกอบการวิสาหกิจขนาดกลางและขนาดย่อม (SMEs) (ถ้ามี)

(๖) หนังสือรับรองการเป็นตัวแทนจำหน่ายผลิตภัณฑ์ที่มีอายุไม่เกิน ๙๐ วันนับจากวันที่ออกหนังสือจนถึงวันที่ยื่นข้อเสนอนี้ จากบริษัทผู้ผลิต หรือบริษัทสาขาของผู้ผลิตในต่างประเทศ หรือบริษัทสาขาของผู้ผลิตในประเทศไทย หรือตัวแทนจำหน่ายในประเทศไทย โดยต้องออกให้เพื่อยืนยันข้อเสนอนี้ ทั้งนี้ ผู้ยื่นข้อเสนอจะต้องแนบหนังสือรับรองดังกล่าวเพื่อประกอบการพิจารณา เฉพาะรายการดังต่อไปนี้

- เครื่องคอมพิวเตอร์ สำหรับงานสำนักงาน
- เครื่องคอมพิวเตอร์ สำหรับงานกราฟิก
- เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานสำนักงาน แบบที่ ๑
- เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานสำนักงาน แบบที่ ๒
- เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานประมวลผล
- เครื่องสำรองไฟฟ้า

(๗) บัญชีเอกสารส่วนที่ ๒ ทั้งหมดที่ได้ยื่นพร้อมกับการเสนอราคาทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ ตามแบบในข้อ ๑.๖ (๒) โดยไม่ต้องแนบในรูปแบบ PDF File (Portable Document Format)

ทั้งนี้ เมื่อผู้ยื่นข้อเสนอดำเนินการแนบไฟล์เอกสารตามบัญชีเอกสารส่วนที่ ๒ ครบถ้วน ถูกต้องแล้ว ระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์จะสร้างบัญชีเอกสารส่วนที่ ๒ ตามแบบ ในข้อ ๑.๖ (๒) ให้โดยผู้ยื่นข้อเสนอไม่ต้องแนบบัญชีเอกสารส่วนที่ ๒ ดังกล่าวในรูปแบบ PDF File (Portable Document Format)

### ๔. การเสนอราคา

๔.๑ ผู้ยื่นข้อเสนอต้องยื่นข้อเสนอและเสนอราคาทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ตามที่กำหนดไว้ในเอกสารประกวดราคาอิเล็กทรอนิกส์นี้ โดยไม่มีเงื่อนไขใด ๆ ทั้งสิ้น และจะต้องกรอกข้อความ ให้ถูกต้องครบถ้วน พร้อมทั้งหลักฐานแสดงตัวตนและทำการยืนยันตัวตนของผู้ยื่นข้อเสนอโดยไม่ต้องแนบบใบเสนอราคาในรูปแบบ PDF File (Portable Document Format)

๔.๒ ในการเสนอราคาให้เสนอราคาเป็นเงินบาท และเสนอราคาได้เพียงครั้งเดียวและราคาเดียว โดยเสนอราคารวม และหรือราคาต่อหน่วย และหรือต่อรายการ ตามเงื่อนไขที่ระบุไว้ท้ายใบเสนอราคา ให้ถูกต้อง ทั้งนี้ ราคารวมที่เสนอจะต้องตรงกันทั้งตัวเลขและตัวหนังสือ ถ้าตัวเลขและตัวหนังสือไม่ตรงกัน ให้ถือตัวหนังสือเป็นสำคัญ โดยคิดราคารวมทั้งสิ้นซึ่งรวมค่าภาษีมูลค่าเพิ่ม ภาษีอากรอื่น ค่าขนส่ง ค่าจดทะเบียน และค่าใช้จ่ายอื่น ๆ ทั้งปวงไว้แล้ว จนกระทั่งส่งมอบพัสดุให้ ณ การรถไฟฯขนส่งมวลชนแห่งประเทศไทย

ราคาที่เสนอจะต้องเสนอกำหนดยื่นราคาไม่น้อยกว่า ๑๒๐ วัน ตั้งแต่วันเสนอราคาโดยภายในกำหนดยื่นราคา ผู้ยื่นข้อเสนอต้องรับผิดชอบราคาที่ตนได้เสนอไว้ และจะถอนการเสนอราคามีได้

๔.๓ ผู้ยื่นข้อเสนอจะต้องเสนอกำหนดเวลาการส่งมอบและติดตั้งพัสดุภายใน ๖๐ วัน (หกสิบวัน) นับถัดจากวันลงนามในสัญญา และมีระยะเวลาเช่าทั้งสิ้น ๓๖ เดือน นับถัดจากวันคณะกรรมการตรวจรับพัสดุ ได้รับมอบพัสดุทั้งหมดหรือบางส่วนหรือบางรายการจากผู้ให้เช่าเรียบร้อยแล้ว ทั้งนี้ระยะเวลาการคำนวณค่าเช่า ไม่นับรวมระยะเวลาติดตั้งและส่งมอบ

๔.๔ ผู้ยื่นข้อเสนอจะต้องส่งแคตตาล็อก และหรือรายละเอียดคุณลักษณะเฉพาะของเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ ไปพร้อมการเสนอราคาทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ เพื่อประกอบการพิจารณา หลักฐานดังกล่าวนี้ รฟม. จะยึดไว้เป็นเอกสารของทางราชการ

๔.๕ ก่อนเสนอราคา ผู้ยื่นข้อเสนอควรตรวจดูร่างสัญญา ร่างรายละเอียดขอบเขตของงาน ทั้งโครงการ (Terms of Reference : TOR) ให้ถี่ถ้วนและเข้าใจเอกสารประกวดราคาอิเล็กทรอนิกส์ทั้งหมด เสียก่อนที่จะตกลงยื่นข้อเสนอตามเงื่อนไข ในเอกสารประกวดราคาเช่าอิเล็กทรอนิกส์

๔.๖ ผู้ยื่นข้อเสนอจะต้องยื่นเสนอราคาทางระบบจัดซื้อจัดจ้างภาครัฐ ด้วยอิเล็กทรอนิกส์ ในวันที่                   ระหว่างเวลา                   น. ถึง                   น. และเวลาในการเสนอราคาให้ถือตามเวลาของระบบการจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์เป็นเกณฑ์

เมื่อพ้นกำหนดเวลายื่นข้อเสนอและเสนอราคาแล้ว จะไม่รับเอกสารการยื่นข้อเสนอ และการเสนอราคาใด ๆ โดยเด็ดขาด

๔.๗ ผู้ยื่นข้อเสนอต้องจัดทำเอกสารสำหรับใช้ในการยื่นเอกสารข้อเสนอในรูปแบบไฟล์ เอกสารประเภท PDF File (Portable Document Format) โดยผู้ยื่นข้อเสนอต้องเป็นผู้รับผิดชอบตรวจสอบความครบถ้วน ถูกต้อง และชัดเจนของเอกสาร PDF File ก่อนที่จะยืนยันการยื่นเอกสารข้อเสนอ แล้วจึงส่งข้อมูล (Upload) เพื่อเป็นการยื่นเอกสารข้อเสนอให้แก่ รฟม. ผ่านทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์

๔.๘ คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์ จะดำเนินการตรวจสอบคุณสมบัติของผู้ยื่นข้อเสนอแต่ละรายว่า เป็นผู้ยื่นข้อเสนอที่มีผลประโยชน์ร่วมกันกับผู้ยื่นเสนอรายอื่น ตามข้อ ๑.๕ (๑) หรือไม่ หากปรากฏว่าผู้ยื่นเสนอรายใดเป็นผู้ยื่นข้อเสนอที่มีผลประโยชน์ร่วมกันกับผู้ยื่นเสนอรายอื่น คณะกรรมการฯ จะตัดรายชื่อผู้ยื่นข้อเสนอที่มีผลประโยชน์ร่วมกันนั้นออกจากการเป็นผู้ยื่นข้อเสนอ

หากปรากฏต่อคณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์ว่า ก่อนหรือในขณะที่มีการพิจารณาข้อเสนอ มีผู้ยื่นเสนอรายใดกระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรม ตามข้อ ๑.๕ (๒) และคณะกรรมการฯ เชื่อว่ามีการกระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรม คณะกรรมการฯ จะตัดรายชื่อผู้ยื่นเสนอรายนั้นออกจากการเป็นผู้ยื่นข้อเสนอ และ รฟม. จะพิจารณาลงโทษผู้ยื่นเสนอดังกล่าว เป็นผู้ทำงาน เว้นแต่ รฟม. จะพิจารณาเห็นว่า ผู้ยื่นเสนอรายนั้นมิใช่เป็นผู้ริเริ่มให้มีการกระทำดังกล่าวและได้ให้ความร่วมมือเป็นประโยชน์ ต่อการพิจารณาของ รฟม.

๔.๙ ผู้ยื่นข้อเสนอจะต้องปฏิบัติ ดังนี้

- (๑) ปฏิบัติตามเงื่อนไขที่ระบุไว้ในเอกสารประกวดราคาอิเล็กทรอนิกส์
- (๒) ราคาที่เสนอจะต้องเป็นราคาที่รวมภาษีมูลค่าเพิ่ม และภาษีอื่น ๆ (ถ้ามี) รวม

ค่าใช้จ่ายที่ส่งไปเรียบร้อยแล้ว

(๓) ผู้ยื่นข้อเสนอจะต้องลงทะเบียนเพื่อเข้าสู่กระบวนการเสนอราคา ตามวัน เวลา ที่กำหนด

(๔) ผู้ยื่นข้อเสนอจะถอนการเสนอราคาที่เสนอแล้วไม่ได้

(๕) ผู้ยื่นข้อเสนอต้องศึกษาและทำความเข้าใจในระบบและวิธีการเสนอราคา ด้วยวิธี ประกวดราคาอิเล็กทรอนิกส์ ของกรมบัญชีกลางที่แสดงไว้ในเว็บไซต์ [www.gprocurement.go.th](http://www.gprocurement.go.th)

๔.๑๐ คู่สัญญาต้องจัดทำแผนการทำงานมาให้ภายใน ๖๐ วัน นับถัดจากวันลงนามในสัญญา โดยจัดทำแผนการทำงานตามเอกสารแนบท้ายเอกสารประกวดราคาอิเล็กทรอนิกส์ เว้นแต่เป็นกรณีสัญญาที่มี วงเงินไม่เกิน ๕๐๐,๐๐๐ บาท ทั้งนี้ แผนการทำงานให้ถือเป็นเอกสารส่วนหนึ่งของสัญญา

## ๕ หลักประกันการเสนอราคา

ผู้ยื่นข้อเสนอต้องวางหลักประกันการเสนอราคาพร้อมกับการเสนอราคาทางระบบการจัดซื้อ จัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ โดยใช้หลักประกันอย่างหนึ่งอย่างใดดังต่อไปนี้ จำนวน ๑,๓๕๘,๒๘๐.๐๐ บาท (หนึ่งล้านสามแสนห้าหมื่นแปดพันสองร้อยแปดสิบบาทถ้วน)

๕.๑ เช็คหรือตราพท์ที่ธนาคารเซ็นส่งจ่าย ซึ่งเป็นเช็คหรือตราพท์ลงวันที่ที่ใช้เช็คหรือตราพท์ นั้นชำระต่อเจ้าหน้าที่ในวันที่ยื่นข้อเสนอ หรือก่อนวันนั้นไม่เกิน ๓ วันทำการ

๕.๒ หนังสือค้ำประกันอิเล็กทรอนิกส์ของธนาคารภายในประเทศตามแบบที่ คณะกรรมการนโยบายกำหนด

๕.๓ พันธบัตรรัฐบาลไทย

๕.๔ หนังสือค้ำประกันของบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยอนุโลมให้ใช้ตามตัวอย่างหนังสือค้ำประกัน ของธนาคารที่คณะกรรมการนโยบายกำหนด

กรณีที่ผู้ยื่นข้อเสนอ นำเช็คหรือตราพท์ที่ธนาคารส่งจ่ายหรือพันธบัตรรัฐบาลไทยหรือ หนังสือค้ำประกันของบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ มาวางเป็นหลักประกันการเสนอราคาจะต้อง ส่งต้นฉบับเอกสารดังกล่าวมาให้ รพม. ตรวจสอบความถูกต้องในวันที่ ระหว่างเวลา น. ถึง น.

กรณีที่ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ประสงค์จะใช้หนังสือ ค้ำประกันอิเล็กทรอนิกส์ของธนาคารในประเทศเป็นหลักประกันการเสนอราคาให้ระบุชื่อผู้เข้าร่วมค้ารายที่สัญญา ร่วมค้ากำหนดให้เป็นผู้เข้ายื่นข้อเสนอกับหน่วยงานของรัฐเป็นผู้ยื่นข้อเสนอ

หลักประกันการเสนอราคาตามข้อนี้ รพม. จะคืนให้ผู้ยื่นข้อเสนอหรือผู้ค้ำประกันภายใน ๑๕ วัน นับถัดจากวันที่ รพม. ได้พิจารณาเห็นชอบรายงานผลคัดเลือกผู้ชนะการประกวดราคาเรียบร้อยแล้ว เว้นแต่ ผู้ยื่นข้อเสนอรายที่คัดเลือกไว้ซึ่งเสนอราคาต่ำสุดหรือได้คะแนนรวมสูงสุดไม่เกิน ๓ ราย ให้คืนได้ต่อเมื่อ ได้ทำสัญญาหรือข้อตกลง หรือผู้ยื่นข้อเสนอได้พ้นจากข้อผูกพันแล้ว

การคืนหลักประกันการเสนอราคา ไม่ว่าในกรณีใด ๆ จะคืนให้โดยไม่มีดอกเบี้ย

## ๖. หลักเกณฑ์และสิทธิในการพิจารณา

๖.๑ ในการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ รพม. จะพิจารณา ตัดสินโดยใช้หลักเกณฑ์ ราคา

๖.๒ การพิจารณาผู้ชนะการยื่นข้อเสนอ

กรณีใช้หลักเกณฑ์ราคาในการพิจารณาผู้ชนะการยื่นข้อเสนอ รฟม. จะพิจารณาจากราคารวม

๖.๓ หากผู้ยื่นข้อเสนอรายใดมีคุณสมบัติไม่ถูกต้องตามข้อ ๒ หรือยื่นหลักฐานการยื่นข้อเสนอไม่ถูกต้อง หรือไม่ครบถ้วนตามข้อ ๓ หรือยื่นข้อเสนอไม่ถูกต้องตามข้อ ๔ คณะกรรมการพิจารณาผล การประกวดราคาอิเล็กทรอนิกส์จะไม่รับพิจารณาข้อเสนอของผู้ยื่นข้อเสนอรายนั้น เว้นแต่ ผู้ยื่นข้อเสนอรายใด เสนอเอกสารทางเทคนิคหรือรายละเอียดคุณลักษณะเฉพาะของพัสดุที่ให้เข้าไม่ครบถ้วน หรือเสนอรายละเอียดแตกต่างไปจากเงื่อนไขที่ รฟม. กำหนดไว้ในประกาศและเอกสารประกวดราคาอิเล็กทรอนิกส์ ในส่วนที่มีสาระสำคัญและความแตกต่างนั้นไม่มีผลทำให้เกิดการได้เปรียบเสียเปรียบ ต่อผู้ยื่นข้อเสนอรายอื่น หรือเป็นการผิดพลาดเล็กน้อย คณะกรรมการฯ อาจพิจารณาผ่อนปรนการตัดสิทธิ ผู้ยื่นข้อเสนอรายนั้น

๖.๔ รฟม. สงวนสิทธิ์ไม่พิจารณาข้อเสนอของผู้ยื่นข้อเสนอโดยไม่มีการผ่อนผัน ในกรณีดังต่อไปนี้

(๑) ไม่กรอกชื่อผู้ยื่นข้อเสนอในการเสนอราคาทางระบบจัดซื้อจัดจ้างด้วยอิเล็กทรอนิกส์

(๒) เสนอรายละเอียดแตกต่างไปจากเงื่อนไขที่กำหนดในเอกสารประกวดราคาอิเล็กทรอนิกส์ที่เป็นสาระสำคัญ หรือมีผลทำให้เกิดความได้เปรียบเสียเปรียบแก่ผู้ยื่นข้อเสนอรายอื่น

๖.๕ ในการตัดสินใจการประกวดราคาอิเล็กทรอนิกส์หรือในการทำสัญญา คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์หรือ รฟม. มีสิทธิให้ผู้ยื่นข้อเสนอดีขึ้นชี้แจงข้อเท็จจริงเพิ่มเติมได้ รฟม. มีสิทธิที่จะไม่รับข้อเสนอ ไม่รับราคา หรือไม่ทำสัญญา หากข้อเท็จจริงดังกล่าว ไม่เหมาะสมหรือไม่ถูกต้อง

๖.๖ รฟม. ทรงไว้ซึ่งสิทธิที่จะไม่รับราคาต่ำสุด หรือราคาหนึ่งราคาใด หรือราคาที่เสนอทั้งหมดก็ได้ และอาจพิจารณาเลือกเข้าในจำนวน หรือขนาด หรือเฉพาะรายการหนึ่งรายการใด หรืออาจจะยกเลิกการประกวดราคาอิเล็กทรอนิกส์โดยไม่พิจารณาเข้าเลยก็ได้ สุดแต่จะพิจารณา ทั้งนี้ เพื่อประโยชน์ของทางราชการเป็นสำคัญ และให้ถือว่าการตัดสินใจของ รฟม. เป็นเด็ดขาด ผู้ยื่นข้อเสนอจะเรียกร้องค่าใช้จ่าย หรือค่าเสียหายใด ๆ มิได้ รวมทั้ง รฟม. จะพิจารณายกเลิกการประกวดราคาอิเล็กทรอนิกส์และลงโทษผู้ยื่นข้อเสนอเป็นผู้ทำงาน ไม่ว่าจะเป็นผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกหรือไม่ก็ตาม หากมีเหตุที่เชื่อถือได้ว่าการยื่นข้อเสนอกระทำการโดยไม่สุจริต เช่น การเสนอเอกสารอันเป็นเท็จ หรือใช้ข้อมูลคลาดเคลื่อนมาเสนอราคาแทน เป็นต้น

ในกรณีที่ผู้ยื่นข้อเสนอรายที่เสนอราคาต่ำสุด เสนอราคาต่ำจนคาดหมายได้ว่าไม่อาจดำเนินงานตามเอกสารประกวดราคาอิเล็กทรอนิกส์ได้ คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์หรือ รฟม. จะให้ผู้ยื่นข้อเสนอนั้นชี้แจงและแสดงหลักฐานที่ทำให้เชื่อได้ว่า ผู้ยื่นข้อเสนอสามารถดำเนินการตามเอกสารประกวดราคาอิเล็กทรอนิกส์ให้เสร็จสมบูรณ์ หากคำชี้แจงไม่เป็นที่รับฟังได้ รฟม. มีสิทธิที่จะไม่รับข้อเสนอ หรือไม่รับราคาของผู้ยื่นข้อเสนอรายนั้น ทั้งนี้ ผู้ยื่นข้อเสนอดังกล่าวไม่มีสิทธิเรียกร้องค่าใช้จ่ายหรือค่าเสียหายใด ๆ จาก รฟม.

๖.๗ ก่อนลงนามในสัญญา รฟม. อาจประกาศยกเลิกการประกวดราคาอิเล็กทรอนิกส์ หากปรากฏว่ามีการกระทำที่เข้าลักษณะผู้ยื่นข้อเสนอที่ชนะการประกวดราคาหรือที่ได้รับการคัดเลือกมีผลประโยชน์ร่วมกัน หรือมีส่วนได้เสียกับผู้ยื่นข้อเสนอรายอื่น หรือขัดขวางการแข่งขันอย่างเป็นธรรม หรือสมยอมกันกับผู้ยื่นข้อเสนอรายอื่น หรือเจ้าหน้าที่ในการเสนอราคา หรือสื่อว่ากระทำการทุจริตอื่นใดในการเสนอราคา

๖.๘ หากผู้ยื่นข้อเสนอซึ่งเป็นผู้ประกอบการ SMEs เสนอราคาสูงกว่าราคาต่ำสุดของผู้ยื่นข้อเสนอรายอื่นที่ไม่เกินร้อยละ ๑๐ ให้หน่วยงานของรัฐจัดซื้อจัดจ้างจากผู้ประกอบการ SMEs ดังกล่าว โดยจัดเรียงลำดับผู้ยื่นข้อเสนอซึ่งเป็นผู้ประกอบการ SMEs ซึ่งเสนอราคาสูงกว่าราคาต่ำสุดของผู้ยื่นข้อเสนอรายอื่นไม่เกินร้อยละ ๑๐ ที่จะเรียกมาทำสัญญาไม่เกิน ๓ ราย

ผู้ยื่นข้อเสนอที่เป็นกิจการร่วมค้าที่จะได้สิทธิตามวรรคหนึ่ง ผู้เข้าร่วมค้าทุกรายจะต้องเป็นผู้ประกอบการ SMEs

ทั้งนี้ ผู้ประกอบการ SMEs ที่จะได้แต้มต่อด้านราคาตามวรรคหนึ่ง จะต้องมีวงเงินสัญญาสะสมตามปีปฏิทินรวมกับราคาที่เสนอในครั้งนี้อันแล้ว มีมูลค่ารวมกันไม่เกินมูลค่าของรายได้ตามขนาดที่ขึ้นทะเบียนไว้กับ สสว.

๖.๙ หากผู้ยื่นข้อเสนอได้เสนอพัสดุที่ได้รับการรับรองและออกเครื่องหมายสินค้าที่ผลิตภายในประเทศไทย (Made in Thailand) จากสภาอุตสาหกรรมแห่งประเทศไทย เสนอราคาสูงกว่าราคาต่ำสุดของผู้เสนอราคารายอื่น ไม่เกินร้อยละ ๕ ให้จัดซื้อจัดจ้างจากผู้ยื่นข้อเสนอที่เสนอพัสดุที่ได้รับการรับรองและออกเครื่องหมายสินค้าที่ผลิตภายในประเทศไทย (Made in Thailand) จากสภาอุตสาหกรรมแห่งประเทศไทย

อนึ่ง หากในการเสนอราคาครั้งนั้น ผู้ยื่นข้อเสนอรายใดมีคุณสมบัติทั้งข้อ ๖.๘ และข้อ ๖.๙ ให้ผู้เสนอราคารายนั้นได้แต้มต่อในการเสนอราคาสูงกว่าผู้ประกอบการรายอื่นไม่เกินร้อยละ ๑๕

๖.๑๐ หากผู้ยื่นข้อเสนอซึ่งมิใช่ผู้ประกอบการ SMEs แต่เป็นบุคคลธรรมดาที่ถือสัญชาติไทยหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยเสนอราคาสูงกว่าราคาต่ำสุดของผู้ยื่นข้อเสนอซึ่งเป็นบุคคลธรรมดาที่มิได้ถือสัญชาติไทยหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายของต่างประเทศไม่เกินร้อยละ ๓ ให้จัดซื้อจัดจ้างกับบุคคลธรรมดาที่ถือสัญชาติไทยหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยดังกล่าว

ผู้ยื่นข้อเสนอที่เป็นกิจการร่วมค้าที่จะได้สิทธิตามวรรคหนึ่ง ผู้เข้าร่วมค้าทุกรายจะต้องเป็นบุคคลธรรมดาที่ถือสัญชาติไทยหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย

## ๗. การทำสัญญาเช่า

๗.๑ ในกรณีที่ผู้ชนะการประกวดราคาอิเล็กทรอนิกส์ สามารถส่งมอบพัสดุที่ให้เช่าได้ครบถ้วนภายใน ๕ วันทำการ นับแต่วันที่ทำข้อตกลงเช่า รพม. จะพิจารณาจัดทำข้อตกลงเป็นหนังสือแทน การทำสัญญาตามแบบสัญญาดังระบุ ในข้อ ๑.๓ ก็ได้

๗.๒ ในกรณีที่ผู้ชนะการประกวดราคาอิเล็กทรอนิกส์ไม่สามารถส่งมอบสิ่งของได้ครบถ้วนภายใน ๕ วันทำการ หรือ รพม. เห็นว่าไม่สมควรจัดทำข้อตกลงเป็นหนังสือ ตามข้อ ๗.๑ ผู้ชนะการประกวดราคาอิเล็กทรอนิกส์จะต้องทำสัญญาเช่าตามแบบสัญญาดังระบุในข้อ ๑.๓ หรือทำข้อตกลงเป็นหนังสือ กับ รพม. ภายใน ๗ วัน นับถัดจากวันที่ได้รับแจ้ง และจะต้องวางหลักประกันสัญญาเป็นจำนวนเงินเท่ากับร้อยละ ๕ ของราคาค่าพัสดุที่ให้เช่าที่ประกวดราคาอิเล็กทรอนิกส์ให้ รพม. ยึดถือไว้ในขณะทำสัญญา โดยใช้หลักประกันอย่างหนึ่งอย่างใดดังต่อไปนี้

(๑) เงินสด

(๒) เช็คหรือตราพท์ที่ธนาคารเซ็นสั่งจ่าย ซึ่งเป็นเช็คหรือตราพท์ลงวันที่ที่ใช้เช็ค หรือตราพท์นั้นชำระต่อเจ้าหน้าที่ในวันทำสัญญา หรือก่อนวันนั้นไม่เกิน ๓ วันทำการ

(๓) หนังสือค้ำประกันของธนาคารภายในประเทศ ตามตัวอย่างที่คณะกรรมการนโยบายกำหนด ดังระบุในข้อ ๑.๔ (๒) หรือจะเป็นหนังสือค้ำประกันอิเล็กทรอนิกส์ตามวิธีการที่กรมบัญชีกลางกำหนด

(๔) หนังสือค้ำประกันของบริษัทเงินทุน หรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยอนุโลมให้ใช้ตามตัวอย่างหนังสือค้ำประกันของธนาคารที่คณะกรรมการนโยบายกำหนด ดังระบุในข้อ ๑.๔ (๒)

(๕) พันธบัตรรัฐบาลไทย

หลักประกันนี้จะคืนให้ โดยไม่มีดอกเบี้ยภายใน ๑๕ วัน นับถัดจากวันที่ผู้ชนะการประกวดราคาอิเล็กทรอนิกส์ (ผู้ให้เช่า) พันจากข้อผูกพันตามสัญญาเช่าแล้ว

หลักประกันนี้จะคืนให้ โดยไม่มีดอกเบี้ย ตามอัตราส่วนของพัสดุที่ให้เช่าซึ่ง รพม. ได้รับมอบไว้แล้ว

#### ๘. ค่าจ้างและการจ่ายเงิน

รายละเอียดตามขอบเขตของงานเช่าเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ประจำปีงบประมาณ ๒๕๖๘ - ๒๕๗๐

#### ๙. อัตราค่าปรับ

รายละเอียดตามขอบเขตของงานเช่าเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ประจำปีงบประมาณ ๒๕๖๘ - ๒๕๗๐

#### ๑๐. การรับประกันความชำรุดบกพร่อง

รายละเอียดตามขอบเขตของงานเช่าเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ประจำปีงบประมาณ ๒๕๖๘ - ๒๕๗๐

#### ๑๑. ข้อสงวนสิทธิ์ในการยื่นข้อเสนอและอื่น ๆ

๑๑.๑ เงินค่าพัสดุสำหรับการเช่าครั้งนี้ ได้มาจากเงินงบประมาณประจำปี พ.ศ. ๒๕๖๘

การลงนามในสัญญาจะกระทำได้ ต่อเมื่อ รพม. ได้รับอนุมัติเงินค่าพัสดุจากเงินงบประมาณประจำปี พ.ศ. ๒๕๖๘ แล้วเท่านั้น

๑๑.๒ เมื่อ รพม. ได้คัดเลือกผู้ยื่นข้อเสนอรายใดให้เป็นผู้ให้เช่า และได้ตกลงเช่าพัสดุตามการประกวดราคาอิเล็กทรอนิกส์แล้ว ถ้าผู้ให้เช่าจะต้องส่งหรือนำพัสดุที่ให้เช่าดังกล่าวเข้ามาจากต่างประเทศและของนั้นต้องนำเข้ามาโดยทางเรือในเส้นทางที่มีเรือไทยเดินอยู่ และสามารถให้บริการรับขนได้ตามที่รัฐมนตรีว่าการกระทรวงคมนาคมประกาศกำหนด ผู้ยื่นข้อเสนอซึ่งเป็นผู้ให้เช่าจะต้องปฏิบัติตามกฎหมายว่าด้วยการส่งเสริมการพาณิชย์นาวี ดังนี้

(๑) แจ้งการส่งหรือนำพัสดุที่ให้เช่าที่เช่าดังกล่าวเข้ามาจากต่างประเทศต่อกรมเจ้าท่า ภายใน ๗ วัน นับตั้งแต่วันที่ผู้ให้เช่าส่ง หรือเช่าของจากต่างประเทศ เว้นแต่เป็นของที่รัฐมนตรีว่าการกระทรวงคมนาคมประกาศยกเว้นให้บรรทุกโดยเรืออื่นได้

(๒) จัดการให้สิ่งของที่เช่าดังกล่าวบรรทุกโดยเรือไทย หรือเรือที่มีสิทธิเช่นเดียวกับเรือไทย จากต่างประเทศมายังประเทศไทย เว้นแต่จะได้รับอนุญาตจากกรมเจ้าท่า ให้บรรทุกสิ่งของนั้นโดยเรืออื่นที่มีใช้เรือไทย ซึ่งจะต้องได้รับอนุญาตเช่นนั้นก่อนบรรทุกของลงเรืออื่น หรือเป็นของที่รัฐมนตรีว่าการกระทรวงคมนาคมประกาศยกเว้นให้บรรทุกโดยเรืออื่น

(๓) ในกรณีที่ไปปฏิบัติตาม (๑) หรือ (๒) ผู้ให้เช่าจะต้องรับผิดชอบตามกฎหมายว่าด้วยการส่งเสริมการพาณิชย์นาวี

๑๑.๓ ผู้ยื่นข้อเสนอซึ่ง รพม. ได้คัดเลือกแล้ว ไม่ไปทำสัญญาหรือข้อตกลงเช่า เป็นหนังสือภายในเวลาที่กำหนด ดังระบุไว้ในข้อ ๗ รพม. จะริบหลักประกันการยื่นข้อเสนอ หรือเรียกประกันจากผู้ออกหนังสือค้ำประกันการยื่นข้อเสนอทันที และอาจพิจารณาเรียกชดเชยความเสียหายอื่น (ถ้ามี) รวมทั้งจะพิจารณาให้เป็นผู้ทำงาน ตามระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและ การบริหารพัสดุภาครัฐ

๑๑.๔ รฟม. สงวนสิทธิ์ที่จะแก้ไขเพิ่มเติมเงื่อนไข หรือข้อกำหนดในแบบสัญญาหรือข้อตกลงเช่าเป็นหนังสือ ให้เป็นไปตามความเห็นของสำนักงานอัยการสูงสุด (ถ้ามี)

๑๑.๕ ในกรณีที่เอกสารแนบท้ายเอกสารประกวดราคาอิเล็กทรอนิกส์นี้ มีความขัดหรือแย้งกัน ผู้ยื่นข้อเสนอจะต้องปฏิบัติตามคำวินิจฉัยของ รฟม. คำวินิจฉัยดังกล่าวให้ถือเป็นที่สุด และผู้ยื่นข้อเสนอไม่มีสิทธิเรียกร้องค่าใช้จ่ายใด ๆ เพิ่มเติม

๑๑.๖ รฟม. อาจประกาศยกเลิกการเช่าในกรณีต่อไปนี้ได้ โดยที่ผู้ยื่นข้อเสนอ จะเรียกร้องค่าเสียหายใด ๆ จาก รฟม. ไม่ได้

(๑) รฟม. ไม่ได้รับการจัดสรรเงินที่จะใช้ในการเช่าหรือที่ได้รับจัดสรรแต่ไม่เพียงพอที่จะทำการเช่าครั้งนี้ต่อไป

(๒) มีการกระทำที่เข้าลักษณะผู้ยื่นข้อเสนอที่ชนะการเช่าหรือที่ได้รับการคัดเลือก มีผลประโยชน์ร่วมกัน หรือมีส่วนได้เสียกับผู้ยื่นข้อเสนอรายอื่น หรือขัดขวางการแข่งขันอย่างเป็นธรรม หรือสมยอมกันกับผู้ยื่นข้อเสนอรายอื่น หรือเจ้าหน้าที่ในการเสนอราคา หรือกล่าวว่าการทุจริตอื่นใดในการเสนอราคา

(๓) การทำการเช่าครั้งนี้ต่อไปอาจก่อให้เกิดความเสียหายแก่ รฟม. หรือกระทบต่อประโยชน์สาธารณะ

(๔) กรณีอื่นในทำนองเดียวกับ (๑) (๒) หรือ (๓) ตามที่กำหนดในกฎกระทรวง ซึ่งออกตามความในกฎหมายว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ

## ๑๒. การปฏิบัติตามกฎหมายและระเบียบ

ในระหว่างระยะเวลาการเช่า ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้ให้เช่าต้องปฏิบัติตามหลักเกณฑ์ที่กฎหมายและระเบียบได้กำหนดไว้โดยเคร่งครัด

## ๑๓. การประเมินผลการปฏิบัติงานของผู้ประกอบการ

รฟม. สามารถนำผลการปฏิบัติงานแล้วเสร็จตามสัญญาของผู้ยื่นข้อเสนอที่ได้รับ การคัดเลือกให้เป็นผู้ให้เช่าเพื่อนำมาประเมินผลการปฏิบัติงานของผู้ประกอบการ

ทั้งนี้ หากผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกไม่ผ่านเกณฑ์ที่กำหนดจะถูกระงับการยื่นข้อเสนอหรือทำสัญญากับ รฟม. ไว้ชั่วคราว

การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

มิถุนายน ๒๕๖๗



**ขอบเขตของงานเช่าเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์**  
**ประจำปีงบประมาณ 2568 - 2570**

**1. ความเป็นมา**

การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย (รฟม.) ได้มีการจัดหาเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ เพื่อสนับสนุนการปฏิบัติงานของ รฟม. ระหว่างปีงบประมาณ 2565 - 2567 ด้วยวิธีการเช่า โดยจะหมดสัญญาเช่า ในวันที่ 30 กันยายน 2567 เพื่อสนับสนุนส่วนงานต่าง ๆ ที่ได้มีการร้องขอเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ เพิ่มเติม ดังนั้น รฟม. จึงมีความจำเป็นต้องจัดหาเพื่อทดแทนและเพิ่มเติมให้เพียงพอต่อการใช้งานทั้งในปัจจุบันและอนาคต

**2. วัตถุประสงค์**

เพื่อเช่าเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ (ซึ่งต่อไปนี้จะเรียกว่า “คอมพิวเตอร์”) ทดแทนของเดิมที่หมดสัญญาเช่าและเช่าคอมพิวเตอร์เพิ่มเติมให้เพียงพอต่อการปฏิบัติงาน โดยมีรายการและจำนวน ดังนี้

2.1 เครื่องคอมพิวเตอร์ สำหรับงานสำนักงาน	จำนวน	330	ชุด
2.2 เครื่องคอมพิวเตอร์ สำหรับงานกราฟิก	จำนวน	27	ชุด
2.3 เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงาน แบบที่ 1	จำนวน	83	ชุด
2.4 เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงาน แบบที่ 2	จำนวน	102	ชุด
2.5 เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานกราฟิก	จำนวน	2	ชุด
2.6 เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานประมวลผล	จำนวน	3	ชุด
2.7 เครื่องคอมพิวเตอร์แท็บเล็ต แบบที่ 1	จำนวน	16	ชุด
2.8 เครื่องคอมพิวเตอร์แท็บเล็ต แบบที่ 2	จำนวน	30	ชุด
2.9 เครื่องสำรองไฟฟ้า	จำนวน	357	ชุด
2.10 ซอฟต์แวร์ป้องกันไวรัส	จำนวน	547	ชุด

**3. คุณสมบัติของผู้ยื่นข้อเสนอ**

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลัง กำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทำงานและได้แจ้งเวียนชื่อให้เป็นผู้ทำงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทำงานเป็นหุ้นส่วน ผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย







/3.6 มีคุณสมบัติ...

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นนิติบุคคลผู้มีอาชีพขายหรือให้เช่าพัสดุที่ประกวดราคาเช่าด้วยวิธีประกวดราคาอิเล็กทรอนิกส์

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ รพม. ณ วัน ประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นนั้น

3.10 ผู้ยื่นข้อเสนอที่เสนอราคาในรูปแบบของ “กิจการร่วมค้า” ต้องมีคุณสมบัติดังนี้

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค่างำหนดให้ผู้เข้าร่วมค้ำรายใดรายหนึ่งเป็นผู้เข้าร่วมค้ำหลัก ข้อตกลงระหว่างผู้เข้าร่วมค้ำจะต้องมีการกำหนดสัดส่วนหน้าที่และความรับผิดชอบในปริมาณงาน สิ่งของหรือมูลค่าตามสัญญาของผู้เข้าร่วมค้ำหลักมากกว่าผู้เข้าร่วมค้ำรายอื่นทุกราย

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค่างำหนดให้ผู้เข้าร่วมค้ำรายใดรายหนึ่งเป็นผู้เข้าร่วมค้ำหลัก กิจการร่วมค้ำนั้นต้องใช้ผลงานของผู้เข้าร่วมค้ำหลักรายเดียวเป็นผลงานของกิจการร่วมค้ำที่ยื่นข้อเสนอ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้ำที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ำรายใดเป็นผู้เข้าร่วมค้ำหลัก ผู้เข้าร่วมค้ำทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค่างำหนดให้มีการมอบหมายผู้เข้าร่วมค้ำรายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้ำ การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ




สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้ำที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ำรายใดเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้ำทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ำรายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้ำ

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

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

3.13 ผู้ยื่นข้อเสนอต้องมีหนังสือรับรองการเป็นตัวแทนจำหน่ายผลิตภัณฑ์ที่มีอายุไม่เกิน 90 วันนับจากวันที่ออกหนังสือจนถึงวันที่ยื่นข้อเสนอนี้ จากบริษัทผู้ผลิต หรือบริษัทสาขาของผู้ผลิตในต่างประเทศ หรือบริษัทสาขาของผู้ผลิตในประเทศไทย หรือตัวแทนจำหน่ายในประเทศไทย โดยต้องออกให้เพื่อยื่นข้อเสนอนี้ ทั้งนี้ ผู้ยื่นข้อเสนอจะต้องแนบหนังสือรับรองดังกล่าวเพื่อประกอบการพิจารณา เฉพาะรายการดังต่อไปนี้

- 1) เครื่องคอมพิวเตอร์ สำหรับงานสำนักงาน
- 2) เครื่องคอมพิวเตอร์ สำหรับงานกราฟิก
- 3) เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานสำนักงาน แบบที่ 1
- 4) เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานสำนักงาน แบบที่ 2
- 5) เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานประมวลผล
- 6) เครื่องสำรองไฟฟ้า

  Joint U.   
/4. รายละเอียด...

#### 4. รายละเอียดคุณลักษณะเฉพาะของพัสดุที่จะดำเนินการเช่า

4.1 คอมพิวเตอร์ที่เสนอต้องเป็นของแท้ อยู่ในสภาพที่ใช้งานได้ดี เป็นรุ่นที่ยังอยู่ในสายการผลิต (Production Line) และต้องเป็นของใหม่ที่ยังมิได้ถูกติดตั้งใช้งาน ณ ที่ใดมาก่อน รวมทั้งต้องไม่ถูกนำมาปรับปรุงสภาพใหม่ (Reconditioned หรือ Rebuilt)

4.2 คอมพิวเตอร์ที่เสนอต้องมีคุณสมบัติตรงตาม Catalog หรือ Brochure ของบริษัทผู้ผลิตที่เสนอขายตามท้องตลาด โดยมีระบบหลักและ/หรือองค์ประกอบหลักที่มีได้ประกอบและ/หรือตัดแปลงเพื่อใช้เฉพาะการยื่นข้อเสนอ โดยผู้ยื่นข้อเสนอจะต้องระบุยี่ห้อและรุ่นของผลิตภัณฑ์ที่เสนอ พร้อมทั้งต้องมี Catalog หรือ Brochure ที่ชัดเจนได้ และทำเครื่องหมาย พร้อมหัวข้อกำกับอุปกรณ์ที่เสนอไว้อย่างชัดเจน

4.3 คอมพิวเตอร์ที่เสนอต้องสามารถใช้งานกับระบบไฟฟ้า 220V AC 50Hz ตามมาตรฐานของประเทศไทยได้ โดยไม่ต้องใช้อุปกรณ์แปลงระบบไฟฟ้า และปลั๊กไฟของอุปกรณ์ทุกรายการจะต้องเป็นชนิด 3 ขา (มีขาสำหรับสายดิน)

4.4 ในกรณีที่มีการส่งมอบคอมพิวเตอร์ต่างไปจากที่กำหนดไว้หรือที่เสนอมา จะต้องมียกข้อยกเว้นจากบริษัทผู้ผลิต หรือจากบริษัทสาขาของผู้ผลิตในต่างประเทศ หรือจากบริษัทสาขาของผู้ผลิตในประเทศไทย หรือตัวแทนจำหน่ายในประเทศไทย ว่าเป็นรุ่นใหม่และจะต้องมีคุณสมบัติไม่ต่ำกว่าที่กำหนดไว้หรือที่เสนอมา ทั้งนี้ รพม. สงวนสิทธิ์ที่จะรับมอบหรือไม่ก็ได้

4.5 กรณีฮาร์ดดิสก์ของคอมพิวเตอร์ตามข้อ 2.1 - 2.6 เสียในส่วนของฮาร์ดแวร์ ผู้ให้เช่าจะต้องมีบริการกู้ข้อมูลที่สูญหายตามการร้องขอของ รพม. รวมทั้งต้องจัดเตรียมฮาร์ดดิสก์ชุดใหม่เพื่อทดแทนชุดเดิมที่เสียหายภายหลังการกู้ข้อมูลกลับมาแล้ว ทั้งนี้การกู้ข้อมูลต้องกระทำโดยบริษัทที่มีห้องปฏิบัติการมาตรฐาน (Clean Room) และมีการรับรองมาตรฐาน ISO 9000 Series หรือเทียบเท่า ซึ่งผู้ให้เช่าต้องแจ้งชื่อบริษัทดังกล่าวให้ รพม. พิจารณาทุกครั้งก่อนการดำเนินการ โดยไม่มีการคิดค่าใช้จ่ายใด ๆ เพิ่มเติม

4.6 กรณีที่มีการเคลื่อนย้ายคอมพิวเตอร์และอุปกรณ์ที่ได้ติดตั้งตามสัญญาฯ นี้ รพม. มีสิทธิ์ที่จะแจ้งให้ผู้ให้เช่ามาดำเนินการให้ รพม. ได้ตลอดอายุสัญญา โดยไม่มีการคิดค่าใช้จ่ายใด ๆ เพิ่มเติม

4.7 คอมพิวเตอร์ที่เสนอต้องมีคุณลักษณะเฉพาะอย่างน้อยตาม ภาคผนวก ก.

#### 5. ขอบเขตของงานที่จะดำเนินการเช่า

5.1 ผู้ให้เช่าจะต้องส่งมอบและติดตั้งเครื่องคอมพิวเตอร์ ณ อาคารสำนักงานของ รพม. ได้แก่ อาคาร 1 อาคาร 2 อาคาร 4 และสถานีรถไฟฟ้ามหานคร ซึ่งอยู่ในเขตกรุงเทพมหานครและปริมณฑล รายละเอียดตาม ภาคผนวก ข.

5.2 ผู้ให้เช่าจะต้องจัดให้มีการประชุมเริ่มงาน (Kickoff Meeting) เพื่อทำความเข้าใจ และนำเสนอแผนการดำเนินงานในการติดตั้ง ให้พิจารณาก่อนการดำเนินการติดตั้งจริงภายใน 15 วัน นับถัดจากวันที่ลงนามในสัญญา

5.3 ผู้ให้เช่าต้องเข้ามาสำรวจคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ทั้งหมดของ รพม. เพื่อจัดทำ Asset Inventory โดยบันทึกรายละเอียดที่ระบุชื่อผู้ใช้งาน สังกัด สถานที่ติดตั้ง และ MAC Address เป็นอย่างน้อย และส่งเป็นเอกสารอิเล็กทรอนิกส์ให้แก่ผู้ควบคุมงานของฝ่ายเทคโนโลยีสารสนเทศ (ฟทท.) ภายใน 30 วัน นับถัดจากวันที่การตรวจรับเสร็จสิ้น

 /5.4 ผู้ให้เช่า...

5.4 ผู้ให้เช่าต้องจัดเตรียมเครื่องคอมพิวเตอร์ตามข้อ 2.1 - 2.3 และข้อ 2.6 พร้อมติดตั้งระบบปฏิบัติการและซอฟต์แวร์ที่เกี่ยวข้องรายการละ 2 เครื่อง โดยนำส่งและติดตั้งที่ ฝพท. เพื่อให้ส่วนงานที่เกี่ยวข้องกับการพัฒนาระบบได้ทำการทดสอบการใช้งานร่วมกับระบบสารสนเทศของ รพม. ที่มีและใช้งานอยู่

5.5 ผู้ให้เช่าต้องจัดเตรียมเครื่องคอมพิวเตอร์ตามข้อ 2.1 - 2.3 และข้อ 2.6 พร้อมติดตั้งระบบปฏิบัติการและซอฟต์แวร์ที่เกี่ยวข้องรายการละ 1 เครื่อง โดยนำส่งและติดตั้งที่ ฝพท. เพื่อจัดทำเครื่องต้นแบบ (Master)

5.6 ผู้ให้เช่าต้องจัดให้มีการตรวจสอบรายละเอียดคุณลักษณะเฉพาะ (Specification) ของเครื่องคอมพิวเตอร์ที่เสนอ โดยแจ้งกำหนดการตรวจสอบรายละเอียดดังกล่าวล่วงหน้าอย่างน้อย 1 วัน และผู้ให้เช่าต้องจัดเตรียมสถานที่ รองรับสิ่งอำนวยความสะดวกและอุปกรณ์ต่าง ๆ ที่เกี่ยวข้องสำหรับการตรวจสอบรายละเอียดคุณลักษณะเฉพาะก่อนนำเครื่องคอมพิวเตอร์มาติดตั้งตามสถานที่ที่ รพม. กำหนด โดยเป็นค่าใช้จ่ายของผู้ให้เช่าเอง

5.7 ผู้ให้เช่าต้องดำเนินการติดตั้ง กำหนดค่าต่าง ๆ พร้อมทั้งโอนย้ายข้อมูลระหว่างเครื่องคอมพิวเตอร์ของพนักงานที่ใช้งานอยู่เดิมไปยังเครื่องคอมพิวเตอร์ใหม่ที่ได้มาตามสัญญา

5.8 ผู้ให้เช่าต้องจัดทำสติกเกอร์ที่ระบุชื่อบริษัทผู้ให้เช่า เลขที่สัญญา ระยะเวลาการรับประกัน หมายเลขโทรศัพท์สำหรับการแจ้งปัญหา และหมายเลขของเครื่องติดให้กับคอมพิวเตอร์ทุกรายการให้ชัดเจน

5.9 ผู้ให้เช่าจะต้องส่งมอบ Master Image ให้กับ รพม. โดยจัดเก็บลงใน External Drive แบบ USB ความจุไม่น้อยกว่า 2 TB จำนวน 3 ชุด

5.10 ผู้ให้เช่าต้องจัดหาอุปกรณ์แปลงสัญญาณ USB-C เป็น VGA สำหรับสำรองใช้งาน จำนวน 20 ชุด

5.11 ผู้ให้เช่าต้องจัดหา Media Card Reader ที่สามารถใช้งานกับ Memory Card แบบ Secure Digital (SD) หรือ microSD หรือดีกว่า สำหรับสำรองใช้งาน จำนวน 20 ชุด




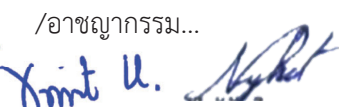
5.12 ภายหลังจากติดตั้ง ผู้ให้เช่าต้องจัดทำเอกสารการติดตั้งคอมพิวเตอร์ทุกรายการ ที่ระบุรายละเอียดต่าง ๆ เช่น ยี่ห้อ/ ประเภทของอุปกรณ์/ รุ่น/ หมายเลขของเครื่อง/ สถานที่ติดตั้ง/ MAC Address ฯลฯ ส่งมอบให้ รพม. จำนวน 1 ชุด (พร้อมส่งมอบเป็น Microsoft Excel File) ภายใน 15 วัน นับถัดจากวันที่การตรวจรับเสร็จสิ้น

5.13 ผู้ให้เช่าจะต้องจัดส่งเจ้าหน้าที่ที่มีความรู้ความสามารถด้านการซ่อมแซม แก๊ซ และบำรุงรักษาเครื่องคอมพิวเตอร์หรือมีความรู้อื่นที่เกี่ยวข้องมาประจำที่สำนักงานใหญ่ของ รพม. ตลอดอายุสัญญา จำนวนไม่น้อยกว่า 2 คน ด้วยค่าใช้จ่ายของผู้ให้เช่าเอง โดยไม่คิดค่าใช้จ่ายใด ๆ เพิ่มเติมจากสัญญาเช่าทั้งสิ้น โดยมีข้อกำหนด ดังนี้

5.13.1 เจ้าหน้าที่จะต้องมีวุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรี โดยผู้ให้เช่าจะต้องแจ้งชื่อ-นามสกุล ประวัติการทำงาน และวุฒิการศึกษาของเจ้าหน้าที่ดังกล่าว ให้ รพม. พิจารณาภายในวันตรวจรับ โดยกรอกรายละเอียดตาม ภาคผนวก ค. และจะต้องเริ่มปฏิบัติงานตั้งแต่วันถัดจากวันที่การตรวจรับเสร็จสิ้น

5.13.2 ผู้ให้เช่าจะต้องดำเนินการให้สำนักงานตำรวจแห่งชาติตรวจประวัติอาชญากรรมด้วยลายนิ้วมือของเจ้าหน้าที่หลักที่จะเข้ามาปฏิบัติงานที่ รพม. ด้วยค่าใช้จ่ายของผู้ให้เช่าเอง และแสดงหลักฐานการดำเนินการดังกล่าวให้ รพม. ทราบภายใน 30 วัน นับถัดจากวันที่การตรวจรับเสร็จสิ้น

เจ้าหน้าที่ของผู้ให้เช่าจะต้องไม่มีประวัติอาชญากรรมเกี่ยวกับความผิดทางอาญา เว้นแต่โทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ ทั้งนี้ รพม. ไม่อนุญาตให้เจ้าหน้าที่ที่มีประวัติ

  
/อาชญากรรม...  
  

อาชญากรรมเกี่ยวกับความผิดอาญาดังกล่าวเข้าทำงาน หากพบว่าเจ้าหน้าที่ของผู้ให้เข้ามีประวัติอาชญากรรมดังกล่าว ผู้ให้เข้าจะต้องเปลี่ยนตัวเจ้าหน้าที่คนดังกล่าว แล้วจัดหาเจ้าหน้าที่มาปฏิบัติงานแทน ภายใน 10 วันทำการ

5.13.3 เจ้าหน้าที่จะต้องปฏิบัติงานในวันจันทร์ - วันศุกร์ ตั้งแต่เวลา 08.00 - 17.00 น. (ระหว่างเวลา 12.00 - 13.00 น. เป็นเวลาพักรับประทานอาหารกลางวัน) เว้นวันหยุดที่ รฟม. กำหนดไว้ รวมเวลาทำงานวันละ 8 ชั่วโมง

5.13.4 เจ้าหน้าที่จะต้องจัดทำรายงานสรุปเวลาเข้า-ออกการปฏิบัติงาน ด้วยวิธีการลงเวลาตามแบบฟอร์มของผู้ให้เข้าเองหรือตามที่ รฟม. กำหนด เป็นประจำทุกเดือนแล้วจัดส่งให้ผู้ควบคุมงานของ ผทท. ภายในวันที่ 15 ของเดือนถัดไป

5.13.5 เจ้าหน้าที่จะต้องจัดทำรายงานการปฏิบัติงานตามสัญญา ประจำเดือน ส่งให้ผู้ควบคุมงานของ ผทท. ภายในวันที่ 15 ของเดือนถัดไป

5.13.6 ผู้ให้เข้าจะต้องจัดหาอุปกรณ์ และเครื่องมือสำหรับการปฏิบัติงาน ซ่อมแซม แก้ไขและบำรุงรักษา เครื่องคอมพิวเตอร์ รวมทั้งอุปกรณ์ที่เกี่ยวข้องให้แก่เจ้าหน้าที่ที่มาปฏิบัติงานตามความเหมาะสม

5.13.7 ผู้ให้เข้าต้องจัดหาบัตรน้ำมันเชื้อเพลิงมูลค่าไม่น้อยกว่า 3,600 บาทต่อเดือน สำหรับใช้เติมน้ำมันยานพาหนะ เพื่อใช้ในการปฏิบัติงานของ รฟม. โดยบัตรดังกล่าวต้องสามารถสะสมยอดเงินคงเหลือในแต่ละเดือนได้

5.13.8 กรณีผู้ให้เข้าต้องการเปลี่ยนตัวเจ้าหน้าที่หลัก จะต้องกรอกรายละเอียดตาม ภาคผนวก ค. และทำเป็นหนังสือยื่นต่อคณะกรรมการตรวจรับพัสดุฯ เพื่อพิจารณาก่อนการเปลี่ยนตัวเจ้าหน้าที่หลักดังกล่าว

5.13.9 รฟม. มีสิทธิ์ขอเปลี่ยนตัวเจ้าหน้าที่ของผู้ให้เข้าได้ตลอดอายุสัญญา เมื่อ รฟม. เห็นว่าไม่มีความเหมาะสมที่จะปฏิบัติหน้าที่ ซึ่งผู้ให้เข้าจะต้องหาเจ้าหน้าที่มาทดแทนภายใน 10 วันทำการ โดยระหว่างการจัดหาเจ้าหน้าที่มาทดแทนนั้น ผู้ให้เข้าจะต้องจัดให้มีเจ้าหน้าที่สำรองเข้ามาปฏิบัติงานที่ รฟม. จนกว่าผู้ให้เข้าจะสามารถจัดหาเจ้าหน้าที่มาทดแทนได้

5.13.10 กรณีเจ้าหน้าที่ปฏิบัติงานไม่ครบชั่วโมงการทำงาน ผู้ให้เข้ายินยอมให้ปรับในอัตรา 125 บาท ต่อชั่วโมง (เศษของชั่วโมงให้นับเป็นหนึ่งชั่วโมง) โดยค่าปรับข้างต้นผู้ให้เข้ายินยอมให้ รฟม. หักจากค่าเช่าหรือเงินอื่น ๆ ที่ค้างจ่ายได้ทันที โดย รฟม. ไม่ต้องบอกสงวนสิทธิ์แต่อย่างใด

5.13.11 กรณีเจ้าหน้าที่ไม่มาปฏิบัติงาน หรือมีความจำเป็นต้องหยุดงาน หรือไม่สามารถมาปฏิบัติงานได้ ผู้ให้เข้าต้องจัดส่งเจ้าหน้าที่ที่มีความรู้ความสามารถตามที่ รฟม. กำหนดไว้มาปฏิบัติงานแทนภายในเวลาไม่เกิน 08.00 น. ของวันทำการนั้น โดยจะต้องแจ้งให้ผู้ควบคุมงานของ ผทท. ทราบล่วงหน้าก่อนเจ้าหน้าที่จะเข้ามาปฏิบัติงานทดแทน หากผู้ให้เข้าไม่สามารถจัดหาเจ้าหน้าที่มาปฏิบัติงานทดแทนได้ หรือมาแล้วแต่ไม่สามารถปฏิบัติงานได้ ผู้ให้เข้ายินยอมให้ปรับในอัตรา 1,000 บาทต่อวัน โดยค่าปรับข้างต้นผู้ให้เข้ายินยอมให้ รฟม. หักจากค่าเช่าหรือเงินอื่น ๆ ที่ค้างจ่ายได้ทันที โดย รฟม. ไม่ต้องบอกสงวนสิทธิ์แต่อย่างใด

5.14 ราคาเช่าที่เสนอให้รวมถึง ค่าเช่าใช้ทั้งฮาร์ดแวร์ ซอฟต์แวร์ ค่าการให้คำปรึกษา ค่าใช้จ่ายในการบำรุงรักษา และซ่อมแซมแก้ไข ค่าบริการ ค่าดำเนินการติดตั้ง ค่าขนย้าย ค่าเก็บรักษาทั้งก่อนและหลังการติดตั้ง (โกดังและ/หรือคลังสินค้า) และอุปกรณ์อื่นใดที่ไม่ได้กล่าวถึง ซึ่งจำเป็นต้องมี เพื่อให้สามารถใช้งานเข้ากับระบบคอมพิวเตอร์และระบบเครือข่ายสื่อสารข้อมูลของ รฟม. ที่มีและใช้งานอยู่ได้อย่างมีประสิทธิภาพ โดยไม่มีการคิดค่าใช้จ่ายใดๆ เพิ่มเติมทั้งสิ้น

/6. กำหนดเวลา...

Joint U.

**6. กำหนดเวลาส่งมอบพัสดุ**

ผู้ให้เช่าต้องติดตั้งคอมพิวเตอร์ตามสถานที่ที่กำหนดให้แล้วเสร็จและมีหนังสือส่งมอบงานให้ รพม. ภายใน 60 วัน นับถัดจากวันที่ลงนามในสัญญา (ผู้ให้เช่าต้องเป็นผู้จัดหาบุคลากรและอุปกรณ์ประกอบ พร้อมทั้งเครื่องมือที่จำเป็น ในการดำเนินการต่าง ๆ ที่เกี่ยวข้อง โดยผู้ให้เช่าเป็นผู้ออกค่าใช้จ่ายเองทั้งสิ้น)

**7. ระยะเวลาการเช่า**

ระยะเวลาเช่าทั้งสิ้น 36 เดือน นับถัดจากวันคณะกรรมการตรวจรับพัสดุฯ ได้รับมอบพัสดุทั้งหมดหรือบางส่วน หรือบางรายการจากผู้ให้เช่าเรียบร้อยแล้ว

**8. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ**

ในการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ รพม. จะพิจารณาตัดสินโดยใช้หลักเกณฑ์ราคา

**9. วงเงินงบประมาณ/วงเงินที่ได้รับจัดสรร**

27,165,600 บาท (ยี่สิบเจ็ดล้านหนึ่งแสนหกหมื่นห้าพันหกร้อยบาทถ้วน) (รวมภาษีมูลค่าเพิ่ม)

**10. งวดงานและการจ่ายเงิน**

การชำระค่าเช่าคอมพิวเตอร์ตามสัญญานี้ รพม. จะชำระค่าเช่าเป็นรายเดือน ซึ่งเป็นค่าเช่าที่รวมภาษีมูลค่าเพิ่ม ตลอดจนภาษีอากรอื่น ๆ และค่าใช้จ่ายทั้งปวงแล้วเมื่อผู้ให้เช่าได้ส่งมอบเครื่องคอมพิวเตอร์ทั้งหมดหรือบางส่วนหรือ บางรายการและคณะกรรมการตรวจรับพัสดุฯ ได้รับมอบพัสดุฯ ดังกล่าวเรียบร้อยแล้ว

การคิดค่าเช่าในเดือนแรกหรือเดือนอื่น ๆ ที่มีการเช่าไม่ครบเดือน ให้คำนวณค่าเช่าเริ่มตั้งแต่วันที่ถัดจากวันที่ รพม. ได้รับมอบเครื่องคอมพิวเตอร์ทั้งหมด หรือบางส่วน หรือบางรายการจากผู้ให้เช่า จนถึงวันสุดท้ายของเดือนนั้น โดยให้ คำนวณค่าเช่าเป็นรายวัน ซึ่งรวมภาษีมูลค่าเพิ่มแล้วหารด้วยจำนวน 30 วัน

**11. การฝึกอบรม**

11.1 ผู้ให้เช่าต้องจัดฝึกอบรม/สัมมนาให้แก่เจ้าหน้าที่ของ รพม. จำนวน 2 หลักสูตร โดยจะต้องดำเนินการ ภายใน 180 วัน นับถัดจากวันที่ตรวจรับแล้วเสร็จ ดังนี้

11.1.1 หลักสูตรสำหรับผู้ใช้งาน จำนวน 1 หลักสูตร จำนวนไม่น้อยกว่า 100 คน และเป็นเวลาไม่น้อยกว่า 0.5 วัน โดยมีเนื้อหาเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์ หรือการใช้งานซอฟต์แวร์สำนักงานเบื้องต้น

11.1.2 หลักสูตรสำหรับผู้ดูแลระบบ จำนวน 1 หลักสูตร จำนวนไม่น้อยกว่า 5 คน และเป็นเวลาไม่น้อยกว่า 1 วัน โดยมีเนื้อหาเกี่ยวกับการแก้ไขปัญหาการใช้งานเครื่องคอมพิวเตอร์ หรือการแก้ไขปัญหาการใช้งานซอฟต์แวร์ สำนักงาน

11.2 ผู้ให้เช่าต้องเป็นผู้รับผิดชอบและจัดเตรียมวิทยากร เอกสาร อาหารว่าง เครื่องดื่ม อาหารกลางวัน และ อุปกรณ์ที่จำเป็นในการฝึกอบรม/สัมมนา จำนวนไม่น้อยกว่าผู้เข้าร่วมอบรม ทั้งนี้ เอกสารจะต้องเป็นภาษาไทยเว้นแต่ กรณีที่ต้องการอธิบายด้วยภาษาทางเทคนิคหรือภาษาเฉพาะให้ใช้ภาษาอังกฤษได้

 The bottom of the page contains several handwritten signatures and stamps. On the left, there is a signature that appears to be 'Asat A.'. In the center, there is a signature that appears to be 'Jint U. Jint'. On the right, there is a signature that appears to be 'Jint U. Jint' and a stamp that says '/12.อัตราค่าปรับ...'. There are also some other illegible signatures and marks.

## 12. อัตราค่าปรับ

12.1 ในกรณีผู้ให้เช่าไม่สามารถปฏิบัติตามเงื่อนไขการติดตั้งและส่งมอบ หรือการส่งมอบคอมพิวเตอร์ล่าช้ากว่าที่กำหนดไว้ในสัญญาในบางรายการหรือทั้งหมด หรือส่งมอบแล้วแต่มีคุณสมบัติไม่ถูกต้องตามรายละเอียดและคุณลักษณะเฉพาะที่กำหนด หรือยังไม่สามารถใช้งานได้ รพม. มีสิทธิ์บอกเลิกสัญญาได้ ในกรณีที่ รพม. ไม่ใช้สิทธิ์บอกเลิกสัญญา ผู้ให้เช่ายินยอมให้ รพม. ปรับในอัตราร้อยละ 0.20 (ศูนย์จุดสองศูนย์) ของราคาค่าเช่าตลอดอายุของสัญญาต่อคอมพิวเตอร์ที่ยังไม่ได้ส่งมอบนั้น ๆ เป็นรายวัน (เศษของวันให้นับเป็นหนึ่งวัน) โดยการปรับจะนับถัดจากวันครบกำหนดส่งมอบตามสัญญาจนถึงวันที่ผู้ให้เช่าได้นำคอมพิวเตอร์มาติดตั้งและส่งมอบให้แก่ รพม. จนถูกต้องครบถ้วนแล้ว ทั้งนี้ ค่าปรับข้างต้นผู้ให้เช่ายินยอมให้ รพม. หักจากค่าเช่าหรือเงินอื่น ๆ (รวมภาษีมูลค่าเพิ่ม) ที่ค้างจ่ายได้ทันที โดย รพม. ไม่ต้องบอกสงวนสิทธิ์แต่อย่างใด

12.2 ในกรณีที่ รพม. ใช้สิทธิ์บอกเลิกสัญญาผู้ให้เช่ายินยอมให้ รพม. คิดค่าปรับตามข้อ 12.1 โดยนับถัดจากวันครบกำหนดส่งมอบตามสัญญาจนถึงวันบอกเลิกสัญญาและผู้ให้เช่ายินยอมให้ รพม. รับผิดชอบประกันสัญญาเป็นจำนวนทั้งหมดหรือแต่บางส่วนก็ได้ แล้วแต่ รพม. จะเห็นสมควร

12.3 ในกรณีผู้ให้เช่าไม่สามารถปฏิบัติตามเงื่อนไขตามข้อ 13.1 ผู้ให้เช่ายินยอมให้ รพม. ปรับเป็นในอัตรา 27,200 บาท (สองหมื่นเจ็ดพันสองร้อยบาทถ้วน) เป็นรายวัน (เศษของวันให้นับเป็นหนึ่งวัน) โดยค่าปรับข้างต้นผู้ให้เช่ายินยอมให้ รพม. หักจากค่าเช่าหรือเงินอื่น ๆ (รวมภาษีมูลค่าเพิ่ม) ที่ค้างจ่ายได้ทันที โดย รพม. ไม่ต้องบอกสงวนสิทธิ์แต่อย่างใด

12.4 ในกรณีผู้ให้เช่าไม่สามารถปฏิบัติตามเงื่อนไขตามข้อ 13.2 - 13.3 ผู้ให้เช่ายินยอมให้ รพม. ปรับในอัตรา 3,000 บาท (สามพันบาทถ้วน) ต่อเหตุการณ์นั้น ๆ เป็นรายวัน (เศษของวันให้นับเป็นหนึ่งวัน) นับตั้งแต่วันที่เจ้าหน้าที่ของ รพม. ได้แจ้งให้ผู้ให้เช่ารับทราบถึงความชำรุดบกพร่อง จนกว่าผู้ให้เช่าจะดำเนินการดังกล่าวแล้วเสร็จหรือจนกว่า รพม. เห็นว่าผู้ให้เช่าไม่อาจจัดหาคอมพิวเตอร์อื่นแทนได้และบอกเลิกสัญญา โดยค่าปรับข้างต้นผู้ให้เช่ายินยอมให้ รพม. หักจากค่าเช่าหรือเงินอื่น ๆ (รวมภาษีมูลค่าเพิ่ม) ที่ค้างจ่ายได้ทันที โดย รพม. ไม่ต้องบอกสงวนสิทธิ์แต่อย่างใด

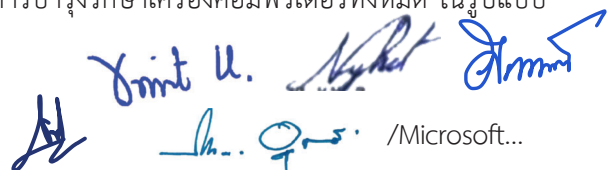
12.5 กรณีผู้ให้เช่าไปเช่าช่วงหรือจ้างช่วงงานแต่บางส่วนโดยฝ่าฝืนความตามข้อ 14.11 ผู้ให้เช่ายินยอมให้ รพม. ปรับในอัตราร้อยละ 10 (สิบ) ของวงเงินค่าเช่าตามสัญญา ทั้งนี้ ไม่ตัดสิทธิ์ รพม. ในการบอกเลิกสัญญา โดยค่าปรับข้างต้นผู้ให้เช่ายินยอมให้ รพม. หักจากค่าเช่าหรือเงินอื่น ๆ (รวมภาษีมูลค่าเพิ่ม) ที่ค้างจ่ายได้ทันที โดย รพม. ไม่ต้องบอกสงวนสิทธิ์แต่อย่างใด

## 13. การกำหนดระยะเวลารับประกันความชำรุดบกพร่อง

### 13.1 การบำรุงรักษา

13.1.1 ผู้ให้เช่าจะต้องรับผิดชอบการบำรุงรักษาเครื่องคอมพิวเตอร์ตลอดระยะเวลาของสัญญา จำนวน 3 ครั้ง เป็นอย่างน้อย ซึ่งแต่ละครั้งต้องมีระยะเวลาห่างกันอย่างเหมาะสม โดยผู้ให้เช่าจะต้องเสนอแผนการบำรุงรักษาให้คณะกรรมการตรวจรับพัสดุฯ พิจารณาในที่ประชุมเริ่มงาน (Kickoff Meeting) ตามข้อ 5.2 ทั้งนี้ แผนดังกล่าวคณะกรรมการตรวจรับพัสดุฯ สามารถปรับเปลี่ยนได้ตามความเหมาะสมตลอดอายุสัญญา

13.1.2 ผู้ให้เช่าต้องส่งตารางเวลาการบำรุงรักษาตามข้อ 13.1.1 มาให้คณะกรรมการตรวจรับพัสดุฯ พิจารณาก่อนดำเนินการ 5 วันทำการ พร้อมทั้งส่งรายงานผลการบำรุงรักษาเครื่องคอมพิวเตอร์ทั้งหมด ในรูปแบบ

  
/Microsoft...

Microsoft Excel File โดยจัดเก็บลงในระบบจัดเก็บข้อมูลที่ รพม. กำหนด ภายใน 10 วันทำการ หลังจากที่ผู้ให้เข้าได้ทำการบำรุงรักษาเสร็จเรียบร้อยแล้ว โดย รพม. ไม่เสียค่าใช้จ่ายใด ๆ เพิ่มเติมทั้งสิ้น

### 13.1.3 การบำรุงรักษาจะต้องตรวจสอบอย่างน้อยตามรายการต่อไปนี้

- (1) ทำความสะอาดโดยการดูดฝุ่นเครื่องคอมพิวเตอร์
- (2) ตรวจสอบอุปกรณ์ ความเรียบร้อย ความครบถ้วนของเครื่องคอมพิวเตอร์ หากมีการชำรุดเสียหาย หรือสูญหาย ผู้ให้เข้าจะต้องทำรายงานให้ รพม. ทราบทันทีที่มิฉะนั้น รพม. ถือว่าผู้ให้เข้าไม่ตั้งใจที่จะเรียกจ่ายค่าเสียหายใด ๆ เพิ่มเติมทั้งสิ้น
- (3) ตรวจสอบจำนวนเครื่องคอมพิวเตอร์ ผู้ครอบครอง สถานที่ติดตั้ง (ล่าสุด) และตรวจสอบการติดตั้งโปรแกรมอื่น ๆ ตามที่ รพม. กำหนด

### 13.2 การซ่อมแซมแก้ไข

ผู้ให้เข้ายอมรับประกันความชำรุดบกพร่องหรือขัดข้องของคอมพิวเตอร์ รวมทั้งซอฟต์แวร์ป้องกันไวรัสตามสัญญาที่ ตลอดจนอายุสัญญานับถัดจากวันที่ รพม. ดำเนินการตรวจรับเรียบร้อยแล้วไปจนถึงสิ้นสุดระยะเวลาตามสัญญา ถ้าภายในระยะเวลาดังกล่าว คอมพิวเตอร์ รวมทั้งซอฟต์แวร์ป้องกันไวรัสชำรุดบกพร่อง หรือใช้งานไม่ได้ทั้งหมดหรือแต่บางส่วน และความชำรุดบกพร่องดังกล่าวมิใช่ความผิดของ รพม. ผู้ให้เข้าจะต้องจัดให้เจ้าหน้าที่ที่มีความรู้ ความชำนาญมาดำเนินการซ่อมแซมแก้ไขให้แล้วเสร็จสามารถใช้งานได้ติดตั้งเดิมภายในวันทำการถัดไป นับแต่วันที่ รพม. ได้แจ้ง ผู้ให้เข้ารับทราบทางโทรศัพท์ โทรศัพท์เคลื่อนที่ โทรสาร จดหมายอิเล็กทรอนิกส์ (E-mail) หรือช่องทางอื่น ๆ ที่ รพม. กำหนด

### 13.3 ความรับผิดชอบต่อความเสียหาย



13.3.1 ในกรณีที่ไม่สามารถซ่อมแซมคอมพิวเตอร์ให้แล้วเสร็จภายในกำหนดระยะเวลาตามข้อ 13.2 ผู้ให้เข้าต้องจัดหาคอมพิวเตอร์ที่มีคุณสมบัติไม่ต่ำกว่าของเดิมหรือดีกว่าและมีสภาพดี มาให้ รพม. ใช้งานทดแทนจนกว่าจะซ่อมแซมคอมพิวเตอร์ที่ชำรุดแล้วเสร็จสามารถใช้งานได้ติดตั้งเดิม ในกรณีที่ผู้ให้เข้าต้องนำคอมพิวเตอร์ที่เสียหรือชำรุดไปซ่อมแซมแก้ไขภายนอก ผู้ให้เข้าต้องนำคอมพิวเตอร์ดังกล่าวกลับมาคืนภายใน 10 วันทำการ โดยอะไหล่หรือวัสดุอุปกรณ์ที่นำมาใช้ในการซ่อมแซมแก้ไข หรือให้ใช้เป็นการชั่วคราว หรือที่นำมาเปลี่ยนให้ใหม่นั้น จะต้องมียุทธศาสตร์ที่ต่ำกว่าของเดิม สำหรับกรณีการเปลี่ยนวัสดุอุปกรณ์ให้ใหม่ วัสดุอุปกรณ์นั้นจะต้องเป็นของใหม่ที่ไม่เคยถูกใช้งานมาก่อนและไม่เป็นของเก่าเก็บ

13.3.2 ในกรณีคอมพิวเตอร์ชำรุดจนไม่สามารถซ่อมแซมได้ หรือชำรุดบกพร่องในปัญหาเดิมซ้ำเป็นจำนวน 3 ครั้ง ภายในระยะเวลา 1 เดือน ผู้ให้เข้าจะต้องจัดหาคอมพิวเตอร์ที่มีคุณสมบัติไม่ต่ำกว่าของเดิมหรือดีกว่า และมีสภาพดีมาเปลี่ยนทดแทนอย่างถาวรภายใน 10 วันทำการ โดยผู้ให้เข้าต้องทำหนังสือแจ้งขอเปลี่ยนคอมพิวเตอร์เป็นลายลักษณ์อักษรเพื่อให้ รพม. พิจารณาและต้องได้รับการเห็นชอบก่อนการเปลี่ยนคอมพิวเตอร์ดังกล่าว

13.3.3 ความเสียหายต่อเครื่องคอมพิวเตอร์ในข้อ 2.3 - 2.8 ให้ครอบคลุมถึงความเสียหายทุกชนิดดังต่อไปนี้

- ความเสียหายอันเกิดจากภัยธรรมชาติต่างๆ เช่น ไฟฟ้า น้ำท่วม เป็นต้น
- ความเสียหายอันเกิดจากไฟไหม้ ไฟฟ้าลัดวงจร ระเบิด
- ความเสียหายอันเกิดจากอุบัติเหตุ เครื่องตกหล่น หรือกระแทก
- ความเสียหายอันเกิดจากเครื่องโดนน้ำ หรือของเหลวหกใส่
- เครื่องสูญหายเนื่องจากการโจรกรรมแบบมีหลักฐานพิสูจน์ได้

ยกเว้น กรณีเหตุที่เกิดจากความประมาทเลินเล่อ

    
 /14. ข้อสงวนสิทธิ์...



#### 14. ข้อสงวนสิทธิ์

14.1 เมื่อสิ้นสุดสัญญาเช่าหากการจัดหาหรือติดตั้งเครื่องใหม่ของ รพม. ยังดำเนินการไม่แล้วเสร็จ รพม. มีสิทธิ์ใช้คอมพิวเตอร์ทั้งหมด รวมถึงเจ้าหน้าที่ตามข้อ 5.13 จะต้องปฏิบัติงานต่อไปอีก 2 เดือน นับจากวันที่สัญญาสิ้นสุดลง โดย รพม. ไม่เสียค่าใช้จ่ายใด ๆ เพิ่มเติมทั้งสิ้น

14.2 หากพ้นระยะเวลาตามข้อ 14.1 ในกรณีที่ รพม. มีความจำเป็นต้องเช่าคอมพิวเตอร์ทั้งหมด หรือบางส่วน หรือบางรายการต่อเมื่อสิ้นสุดสัญญา ผู้ให้เช่ายินยอมให้เช่าต่อโดยใช้ราคาอ้างอิงจากสัญญาเช่าเดิม ทั้งนี้ ราคาเช่าดังกล่าวจะไม่เกินร้อยละ 50 ของราคาเช่าเดิม

14.3 กรณีผู้ให้เช่าประสงค์ที่จะขายคอมพิวเตอร์ตามข้อ 2.1 - 2.6 ผู้ให้เช่ายินยอมให้สิทธิ์ รพม. หรือพนักงาน/ลูกจ้าง ของ รพม. ซื้อคอมพิวเตอร์ดังกล่าว (ทั้งชุด) พร้อมเครื่องสำรองไฟฟ้า โดยราคารวมภาษีมูลค่าเพิ่มแล้วเป็นจำนวนเงิน 1,500 บาท (หนึ่งพันห้าร้อยบาทถ้วน)

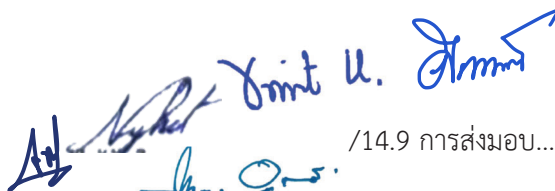
14.4 กรณีผู้ให้เช่าประสงค์ที่จะขายคอมพิวเตอร์ตามข้อ 2.7 - 2.8 ผู้ให้เช่ายินยอมให้สิทธิ์ รพม. หรือพนักงาน/ลูกจ้าง ของ รพม. ซื้อคอมพิวเตอร์ดังกล่าว (ทั้งชุด) โดยราคารวมภาษีมูลค่าเพิ่มแล้วเป็นจำนวนเงิน 500 บาท (ห้าร้อยบาทถ้วน)

14.5 ผู้ให้เช่าจะต้องทำลายข้อมูลที่อยู่ภายในหน่วยเก็บข้อมูล (Hard disk) ของเครื่องคอมพิวเตอร์จนไม่สามารถกู้ข้อมูลกลับมาได้ โดยต้องดำเนินการให้เป็นไปตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของ รพม.

14.6 ภายหลังจากที่ผู้ให้เช่าได้ดำเนินการตามข้อ 14.1 - 14.5 เรียบร้อยแล้ว ผู้ให้เช่าจะต้องขนย้ายคอมพิวเตอร์กลับคืนไปภายใน 60 วัน นับถัดจากวันที่ รพม. ได้แจ้ง ผู้ให้เช่ารับทราบทางโทรศัพท์ โทรศัพท์เคลื่อนที่ โทรสาร จดหมายอิเล็กทรอนิกส์ (E-mail) หรือช่องทางอื่น ๆ ที่ รพม. กำหนด โดยในระยะเวลาดังกล่าว รพม. จะไม่รับผิดชอบต่อความเสียหายหรือการสูญหายที่อาจเกิดขึ้นกับเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ทั้งหมด ทั้งนี้ ผู้ให้เช่าจะต้องรับผิดชอบต่อค่าใช้จ่ายในการขนย้ายด้วย

14.7 ผู้ให้เช่าและ/หรือเจ้าหน้าที่ของผู้ให้เช่า ที่เข้าถึงระบบเทคโนโลยีสารสนเทศของ รพม. ต้องรับทราบและปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของ รพม. ตาม ภาคผนวก ง. และจะต้องรักษาความลับต่าง ๆ ที่ได้จากการปฏิบัติงาน โดยห้ามมิให้ผู้ให้เช่า และ/หรือเจ้าหน้าที่ของผู้ให้เช่านำข้อมูลส่วนหนึ่งส่วนใดหรือทั้งหมดที่ได้จากการปฏิบัติงานใน รพม. ไปทำซ้ำ เผยแพร่ หรือวิเคราะห์ประมวลผลเพื่อการอื่นใด ไม่ว่าการกระทำดังกล่าวจะเป็นการหาผลประโยชน์หรือไม่ก็ตาม หาก รพม. ตรวจสอบผู้ให้เช่าต้องชดเชยค่าเสียหายเป็นจำนวนเงินไม่น้อยกว่าค่าเช่าทั้งหมดที่กำหนดไว้ในสัญญา ทั้งนี้ ผู้ให้เช่าและ/หรือเจ้าหน้าที่ของผู้ให้เช่าต้องลงนามในสัญญาการเก็บรักษาข้อมูลไว้เป็นความลับ (Non-Disclosure Agreement) ตาม ภาคผนวก จ. ก่อนเริ่มปฏิบัติงานตามรูปแบบที่ รพม. กำหนด

14.8 การใช้ประโยชน์ในเครื่องเช่าตามสัญญานี้ ผู้ให้เช่ายินยอมให้อยู่ภายใต้การจัดการและการควบคุมดูแลของ รพม. โดยสิ้นเชิง นอกจาก รพม. จะใช้ในการปฏิบัติงานของ รพม. เองแล้ว รพม. อาจให้ผู้อื่นมาใช้เครื่องเช่านี้ได้โดยอยู่ภายใต้การควบคุมดูแลของ รพม.

  
/14.9 การส่งมอบ...

14.9 การส่งมอบคอมพิวเตอร์ที่ไม่ตรงตามสัญญา รฟม. ทรงไว้ซึ่งสิทธิ์ที่จะไม่รับคอมพิวเตอร์นั้น ในกรณีนี้ ผู้ให้เช่าต้องรับนำกลับคืนไปแก้ไขให้ถูกต้องตามสัญญาและนำมาส่งมอบให้ใหม่ด้วยค่าใช้จ่ายของผู้ให้เช่าเอง และระยะเวลาที่เสียไปเพราะเหตุดังกล่าว ผู้ให้เช่าจะนำมาอ้างเพื่อขอตหรือลดค่าปรับ หรือขอขยายเวลาในภายหลังไม่ได้

14.10 ผู้ให้เช่าจะต้องส่งบุคลากรเข้าร่วมการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness) เพื่อสร้างความตระหนักที่เหมาะสม ทบทวนนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และขั้นตอนปฏิบัติของ รฟม. ตามที่ รฟม. กำหนด

14.11 ผู้ให้เช่าจะต้องไม่เอางานทั้งหมดหรือแต่บางส่วนไปเช่าช่วงหรือจ้างช่วงอีกทอดหนึ่ง เว้นแต่การเช่าช่วงหรือจ้างช่วงงานแต่บางส่วนที่ได้รับอนุญาตเป็นหนังสือจากคณะกรรมการตรวจรับพัสดุฯ แล้ว การที่ รฟม. ได้อนุญาตให้เช่าช่วงหรือจ้างช่วงงานแต่บางส่วนดังกล่าวนี้ ไม่เป็นเหตุให้ผู้ให้เช่าหลุดพ้นจากความรับผิดชอบหรือพ้นหน้าที่ และผู้ให้เช่าจะยังคงต้องรับผิดชอบในความผิดและความประมาทเลินเล่อของผู้ให้เช่าช่วง หรือของตัวแทนหรือลูกจ้างของผู้ให้เช่าช่วงนั้นทุกประการ (หากมี)

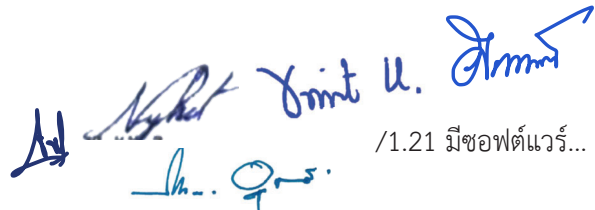
*Joint U. [Signature]*  
*[Signature]*

ภาคผนวก ก.  
รายละเอียดคุณลักษณะเฉพาะ

At Joint U. Stmmt  
K. S. - In. Q. S.

**1. เครื่องคอมพิวเตอร์ สำหรับงานสำนักงาน มีคุณสมบัติอย่างน้อยดังนี้**

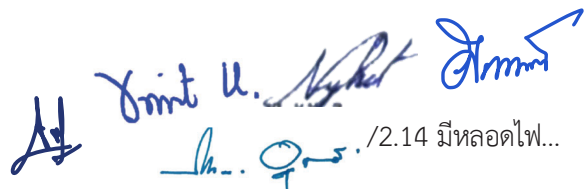
- 1.1 มีหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า 4 Core และ 8 Tread รุ่นล่าสุดที่มีในท้องตลาด และมีเทคโนโลยีเพิ่มสัญญาณนาฬิกาได้ในกรณีที่ต้องใช้ความสามารถในการประมวลผลสูง (Turbo Boost หรือ Max Boost) โดยมีความเร็วสัญญาณนาฬิกาสูงสุด ไม่น้อยกว่า 4.5 GHz
- 1.2 หน่วยประมวลผลกลาง (CPU) มีหน่วยความจำแบบ Cache Memory ขนาดไม่น้อยกว่า 12 MB
- 1.3 มีหน่วยความจำหลักแบบ DDR5 หรือดีกว่า ขนาดไม่น้อยกว่า 8 GB จำนวน 1 หน่วย
- 1.4 มี Hard Disk ชนิด M.2 SSD ที่มี Interface แบบ PCIe NVMe ความจุไม่น้อยกว่า 1TB
- 1.5 มีหน่วยควบคุมการแสดงผลแบบ Integrated HD Graphics หรือดีกว่าโดยใช้หน่วยความจำ ร่วมกับหน่วยความจำหลักได้
- 1.6 มีช่องเชื่อมต่อแบบ VGA และ/หรือ Display Port และ/หรือ HDMI จำนวนรวมไม่น้อยกว่า 2 ช่อง
- 1.7 มีช่องเชื่อมต่อระบบเครือข่าย Gigabit Ethernet จำนวน 1 หน่วย
- 1.8 มีช่องเชื่อมต่อตามมาตรฐาน USB 2.0 USB 3.0 และ USB-C จำนวนรวมไม่น้อยกว่า 6 ช่อง
- 1.9 มีระบบเครือข่ายไร้สายแบบติดตั้งภายใน และรองรับมาตรฐาน IEEE802.11ax (WIFI-6E) หรือดีกว่า
- 1.10 มี Bluetooth 5.2 หรือดีกว่า ติดตั้งภายในเครื่อง
- 1.11 มีระบบเสียงพร้อมลำโพงติดตั้งภายในเครื่อง
- 1.12 ตัวเครื่องเป็นแบบ Ultra Small PC หรือ Mini PC หรือ micro PC หรือเทียบเท่า ที่มีระบบเตือนการเปิดฝาเครื่อง (Intrusion switch)
- 1.13 มีอุปกรณ์แปลงไฟฟ้า (Adapter) ขนาดไม่น้อยกว่า 65 Watt สำหรับต่อใช้งานกับไฟฟ้า 220V
- 1.14 มีอุปกรณ์สำหรับติดตั้งตัวเครื่องบริเวณด้านหลังจอภาพ (VESA Mount) หรือมีฐานวางตัวเครื่องแนวตั้ง (Vertical Stand)
- 1.15 มีหลอดไฟแบบ LED ด้านหน้าเครื่องสำหรับแสดงสถานะการเปิด/ปิดเครื่อง และการทำงานของ Hard Disk ได้เป็นอย่างดี
- 1.16 มี Security Chip ตามมาตรฐาน TPM 2.0 (Trusted Platform Module) หรือดีกว่า
- 1.17 เครื่องคอมพิวเตอร์ที่เสนอต้องมีระบบ Online Support ที่ให้บริการ Download Driver ผ่านช่องทาง Internet จากผู้ผลิต
- 1.18 มีจอภาพแบบ LED (Wide Screen) ขนาดไม่น้อยกว่า 23 นิ้ว ที่มีลำโพงติดตั้งอยู่ภายในและมีช่องเชื่อมต่อแบบ VGA หรือ Display Port หรือ HDMI ที่ความละเอียดสูงสุดไม่น้อยกว่า 1920 x 1080 Pixels โดยขาตั้งสามารถปรับระดับสูง-ต่ำได้
- 1.19 มีแป้นพิมพ์ ที่มีตัวอักษรภาษาไทยและภาษาอังกฤษติดบนปุ่มกดอย่างถาวร เชื่อมต่อแบบ USB 2.0 หรือดีกว่า โดยเป็นยี่ห้อเดียวกับผลิตภัณฑ์ที่เสนอ
- 1.20 มี Laser Mouse เชื่อมต่อแบบ USB 2.0 หรือดีกว่า โดยเป็นยี่ห้อเดียวกับผลิตภัณฑ์ที่เสนอ พร้อมแผ่นรอง

  
/1.21 มีซอฟต์แวร์...

- 1.21 มีซอฟต์แวร์ระบบปฏิบัติการ Windows 11 Professional 64bit แบบ OEM License ที่สามารถดาวน์โหลดมาเป็น Windows 10 Professional 64bit ได้ โดยจะต้องมีลิขสิทธิ์ถูกต้องตามกฎหมายจากเจ้าของผลิตภัณฑ์และเป็นสิทธิ์การใช้งานของ รพม.
- 1.22 มีการรับประกันความชำรุดบกพร่องของเครื่องคอมพิวเตอร์และอุปกรณ์ทุกชิ้นส่วนทั้งค่าแรง อะไหล่ โดยเข้ามาทำการแก้ไข/ซ่อมแซม ณ ที่ติดตั้งเครื่อง (On-Site Service) จากบริษัทผู้ผลิต ภายในวันทำการถัดไป (Next Business Day)
- 1.23 มีเอกสารการรับรองคุณภาพเครื่องคอมพิวเตอร์ตามมาตรฐานที่เกี่ยวข้องกับผลิตภัณฑ์ ด้านต่าง ๆ ดังต่อไปนี้
  - 1) มาตรฐานด้านระบบคุณภาพ ISO 9001 และ ISO 14001 Series
  - 2) มาตรฐานด้านการประหยัดพลังงาน Energy Star และ EPEAT ระดับ Gold
  - 3) มาตรฐานด้านความปลอดภัย UL และ CE
  - 4) มาตรฐานด้านสิ่งแวดล้อม RoHS และ TCO
  - 5) มาตรฐานด้านการแพร่กระจายคลื่นแม่เหล็กไฟฟ้า FCC

## **2. เครื่องคอมพิวเตอร์ สำหรับงานกราฟิก มีคุณสมบัติอย่างน้อยดังนี้**

- 2.1 มีหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า 14 Core และ 20 Tread รุ่นล่าสุดที่มีในท้องตลาด และมีเทคโนโลยีเพิ่มสัญญาณนาฬิกาได้ในกรณีที่ต้องใช้ความสามารถในการประมวลผลสูง (Turbo Boost หรือ Max Boost) โดยมีความเร็วสัญญาณนาฬิกาสูงสุด ไม่น้อยกว่า 5.0 GHz
- 2.2 หน่วยประมวลผลกลาง (CPU) มีหน่วยความจำแบบ Cache Memory ขนาดไม่น้อยกว่า 24 MB
- 2.3 มีหน่วยความจำหลักแบบ DDR5 หรือดีกว่า ขนาดไม่น้อยกว่า 16 GB
- 2.4 มี Hard Disk ชนิด M.2 SSD ที่มี Interface แบบ PCIe NVMe ความจุไม่น้อยกว่า 1TB
- 2.5 มีหน่วยควบคุมการแสดงผลแบบ GDDR6 ที่มีหน่วยความจำไม่น้อยกว่า 4 GB (แยกจากหน่วยความจำหลัก) โดยรองรับการเชื่อมต่อแบบ Display port หรือ mini-Display Port หรือ HDMI เป็นอย่างน้อย
- 2.6 มี DVD +/- RW แบบติดตั้งภายในหรือภายนอกเครื่อง จำนวน 1 หน่วย
- 2.7 มีช่องเชื่อมต่อระบบเครือข่าย Gigabit Ethernet จำนวน 1 หน่วย
- 2.8 มีช่องเชื่อมต่อตามมาตรฐาน USB 2.0 USB 3.0 และ USB-C จำนวนรวมไม่น้อยกว่า 6 ช่อง
- 2.9 มีระบบเครือข่ายไร้สายแบบติดตั้งภายใน และรองรับมาตรฐาน IEEE802.11ax (WIFI-6E) หรือดีกว่า
- 2.10 มี Bluetooth 5.2 หรือดีกว่า ติดตั้งภายในเครื่อง
- 2.11 มีระบบเสียงพร้อมลำโพงติดตั้งภายในเครื่อง
- 2.12 ตัวเครื่องเป็นแบบ Small Form Factor (SFF) หรือเทียบเท่า ที่มีระบบเตือนการเปิดฝาเครื่อง (Intrusion switch)
- 2.13 มีระบบจ่ายกำลังไฟฟ้าแบบติดตั้งภายในตัวเครื่อง ขนาดไม่น้อยกว่า 180 Watt

 /2.14 มีหลอดไฟ...

- 2.14 มีหลอดไฟแบบ LED ด้านหน้าเครื่องสำหรับแสดงสถานะการเปิด/ปิดเครื่อง และการทำงานของ Hard Disk ได้เป็นอย่างดี
- 2.15 มี Security Chip ตามมาตรฐาน TPM 2.0 (Trusted Platform Module) หรือดีกว่า
- 2.16 เครื่องคอมพิวเตอร์ที่เสนอต้องมีระบบ Online Support ที่ให้บริการ Download Driver ผ่านช่องทาง Internet จากผู้ผลิต
- 2.17 มีจอภาพแบบ LED (Wide Screen) ขนาดไม่น้อยกว่า 23 นิ้ว ที่มีลำโพงติดตั้งอยู่ภายในและมีช่องเชื่อมต่อแบบ VGA หรือ Display Port หรือ HDMI ที่ความละเอียดสูงสุดไม่น้อยกว่า 1920 x 1080 Pixels โดยขาตั้งสามารถปรับระดับสูง-ต่ำได้
- 2.18 มีแป้นพิมพ์ ที่มีตัวอักษรภาษาไทยและภาษาอังกฤษติดบนปุ่มกดอย่างถาวร เชื่อมต่อแบบ USB 2.0 หรือดีกว่า โดยเป็นยี่ห้อเดียวกับผลิตภัณฑ์ที่เสนอ
- 2.19 มี Laser Mouse เชื่อมต่อแบบ USB 2.0 หรือดีกว่า โดยเป็นยี่ห้อเดียวกับผลิตภัณฑ์ที่เสนอ พร้อมแผ่นรอง
- 2.20 มีซอฟต์แวร์ระบบปฏิบัติการ Windows 11 Professional 64bit แบบ OEM License ที่สามารถดาวน์โหลดเป็น Windows 10 Professional 64bit ได้ โดยจะต้องมีลิขสิทธิ์ถูกต้องตามกฎหมายจากเจ้าของผลิตภัณฑ์และเป็นสิทธิ์การใช้งานของ รพม.
- 2.21 มีการรับประกันความชำรุดบกพร่องของเครื่องคอมพิวเตอร์และอุปกรณ์ทุกชิ้นส่วนทั้งค่าแรง อะไหล่ โดยเข้ามาทำการแก้ไข/ซ่อมแซม ณ ที่ติดตั้งเครื่อง (On-Site Service) จากบริษัทผู้ผลิต ภายในวันทำการถัดไป (Next Business Day)
- 2.22 มีเอกสารการรับรองคุณภาพเครื่องคอมพิวเตอร์ตามมาตรฐานที่เกี่ยวข้องกับผลิตภัณฑ์ ด้านต่าง ๆ ดังต่อไปนี้
  - 1) มาตรฐานด้านระบบคุณภาพ ISO 9001 และ ISO 14001 Series
  - 2) มาตรฐานด้านการประหยัดพลังงาน Energy Star และ EPEAT ระดับ Gold
  - 3) มาตรฐานด้านความปลอดภัย UL และ CE
  - 4) มาตรฐานด้านสิ่งแวดล้อม RoHS และ TCO
  - 5) มาตรฐานด้านการแพร่กระจายคลื่นแม่เหล็กไฟฟ้า FCC

### 3. เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานสำนักงาน แบบที่ 1 มีคุณสมบัติอย่างน้อยดังนี้

- 3.1 มีหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า 12 Core และ 16 Tread รุ่นล่าสุดที่มีในท้องตลาด และมีเทคโนโลยีเพิ่มสัญญาณนาฬิกาได้ในกรณีที่ต้องใช้ความสามารถในการประมวลผลสูง (Turbo Boost หรือ Max Boost) โดยมีความเร็วสัญญาณนาฬิกาสูงสุด ไม่น้อยกว่า 4.7 GHz
- 3.2 หน่วยประมวลผลกลาง (CPU) มีหน่วยความจำแบบ Cache Memory ขนาดไม่น้อยกว่า 12 MB
- 3.3 มีจอภาพขนาดไม่เกิน 14 นิ้ว แบบ FHD Anti-Glare ที่ความสว่าง 400 nits และมีความละเอียดสูงสุด ไม่น้อยกว่า 1920 x 1080 Pixels
- 3.4 มีหน่วยความจำหลักแบบ DDR5 หรือดีกว่า ขนาดไม่น้อยกว่า 16 GB



/3.5 มี Hard Disk...

- 3.5 มี Hard Disk ชนิด M.2 SSD ที่มี Interface แบบ PCIe NVMe ความจุไม่น้อยกว่า 1 TB
- 3.6 มีหน่วยควบคุมการแสดงผลแบบ GDDR6 หรือดีกว่า ที่มีหน่วยความจำไม่น้อยกว่า 2 GB โดยแยกจากหน่วยความจำหลัก
- 3.7 มีระบบเสียงพร้อมลำโพงติดตั้งภายในเครื่อง
- 3.8 มีกล้อง Webcam แบบ FHD ที่สามารถใช้ยืนยันตัวตนบุคคลได้ โดยติดตั้งภายในตัวเครื่อง พร้อมแผ่นเลื่อนเพื่อปิดกล้องเมื่อไม่ใช้งาน
- 3.9 มีเซ็นเซอร์ยืนยันตัวตนบุคคลด้วยลายนิ้วมือ (Fingerprint Reader)
- 3.10 มีช่องเชื่อมต่อระบบเครือข่าย Gigabit Ethernet จำนวน 1 ช่อง
- 3.11 มีระบบเครือข่ายไร้สายแบบติดตั้งภายใน และรองรับมาตรฐาน IEEE802.11ax (WIFI-6E) หรือดีกว่า
- 3.12 มีช่องเชื่อมต่อตามมาตรฐาน USB 2.0 USB 3.0 และ USB-C จำนวนรวมไม่น้อยกว่า 3 ช่อง
- 3.13 มีช่องเชื่อมต่อแบบ HDMI
- 3.14 มีแป้นพิมพ์ ที่มีตัวอักษรภาษาไทยและภาษาอังกฤษติดบนปุ่มกดอย่างถาวร
- 3.15 มี Mouse ไร้สายที่ใช้ตัวรับสัญญาณขนาดเล็ก (Unifying) โดยเป็นยี่ห้อเดียวกับผลิตภัณฑ์ที่เสนอ พร้อมแผ่นรอง
- 3.16 มีแบตเตอรี่แบบ Li-Polymer ขนาดไม่น้อยกว่า 50 Whr พร้อมซอฟต์แวร์ที่สามารถตรวจสอบประสิทธิภาพของแบตเตอรี่ได้และเป็นยี่ห้อเดียวกับผลิตภัณฑ์ที่เสนอ
- 3.17 มีอุปกรณ์แปลงไฟฟ้า (Adapter) แบบ USB-C สำหรับต่อใช้งานกับไฟฟ้า 220V
- 3.18 มีน้ำหนักของเครื่องไม่เกิน 1.8 กิโลกรัม โดยไม่รวมน้ำหนักของแบตเตอรี่
- 3.19 มี Security Chip หรือ Firmware ตามมาตรฐาน TPM 2.0 (Trusted Platform Module) หรือดีกว่า
- 3.20 เครื่องคอมพิวเตอร์ที่เสนอต้องมีระบบ Online Support ที่ให้บริการ Download Driver ผ่านช่องทาง Internet จากผู้ผลิต
- 3.21 มีกระเป๋าสำหรับใส่เครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ แบบสะพายหลัง
- 3.22 มีซอฟต์แวร์ระบบปฏิบัติการ Windows 11 Professional 64bit แบบ OEM License ที่สามารถดาวน์โหลดเป็น Windows 10 Professional 64bit ได้ โดยจะต้องมีลิขสิทธิ์ถูกต้องตามกฎหมายจากเจ้าของผลิตภัณฑ์และเป็นสิทธิ์การใช้งานของ รพม.
- 3.23 มีการรับประกันความชำรุดบกพร่องของเครื่องคอมพิวเตอร์และอุปกรณ์ทุกชิ้นส่วนทั้งค่าแรง อะไหล่โดยเข้ามาทำการแก้ไข/ซ่อมแซม ณ ที่ติดตั้งเครื่อง (On-Site Service) จากบริษัทผู้ผลิต ภายในวันทำการถัดไป (Next Business Day)
- 3.24 มีเอกสารการรับรองคุณภาพเครื่องคอมพิวเตอร์ตามมาตรฐานที่เกี่ยวข้องกับผลิตภัณฑ์ ด้านต่าง ๆ ดังต่อไปนี้
  - 1) มาตรฐานด้านระบบคุณภาพ ISO 9001 และ ISO 14001 Series
  - 2) มาตรฐานด้านการประหยัดพลังงาน Energy Star และ EPEAT ระดับ Gold
  - 3) มาตรฐานด้านความปลอดภัย UL และ CE



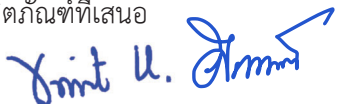


/4) มาตรฐาน...

- 4) มาตรฐานด้านสิ่งแวดล้อม RoHS และ TCO
- 5) มาตรฐานด้านการแพร่กระจายคลื่นแม่เหล็กไฟฟ้า FCC
- 6) มาตรฐานด้านความทนทาน MIL-STD 810H

**4. เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานสำนักงาน แบบที่ 2 มีคุณสมบัติอย่างน้อยดังนี้**

- 4.1 มีหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า 12 Core และ 16 Tread รุ่นล่าสุดที่มีในท้องตลาด และมีเทคโนโลยีเพิ่มสัญญาณนาฬิกาได้ในกรณีที่ต้องใช้ความสามารถในการประมวลผลสูง (Turbo Boost หรือ Max Boost) โดยมีความเร็วสัญญาณนาฬิกาสูงสุด ไม่น้อยกว่า 4.7 GHz
- 4.2 หน่วยประมวลผลกลาง (CPU) มีหน่วยความจำแบบ Cache Memory ขนาดไม่น้อยกว่า 12 MB
- 4.3 มีจอภาพขนาดไม่เกิน 14 นิ้ว แบบ FHD Anti-Glare ที่ความสว่าง 400 nits และมีความละเอียดสูงสุด ไม่น้อยกว่า 1920 x 1080 Pixels
- 4.4 มีหน่วยความจำหลักแบบ DDR5 หรือดีกว่า ขนาดไม่น้อยกว่า 16 GB
- 4.5 มี Hard Disk ชนิด M.2 SSD ที่มี Interface แบบ PCIe NVMe ความจุไม่น้อยกว่า 1 TB
- 4.6 มีหน่วยควบคุมการแสดงผลแบบ GDDR6 หรือดีกว่า ที่มีหน่วยความจำไม่น้อยกว่า 2 GB โดยแยกจากหน่วยความจำหลัก
- 4.7 มีระบบเสียงพร้อมลำโพงติดตั้งภายในเครื่อง
- 4.8 มีกล้อง Webcam แบบ FHD ที่สามารถใช้ยืนยันตัวบุคคลได้ โดยติดตั้งภายในตัวเครื่อง พร้อมแผ่นเลื่อนเพื่อปิดกล้องเมื่อไม่ใช้งาน
- 4.9 มีเซ็นเซอร์ยืนยันตัวบุคคลด้วยลายนิ้วมือ (Fingerprint Reader)
- 4.10 มีช่องเชื่อมต่อระบบเครือข่าย Gigabit Ethernet จำนวน 1 ช่อง
- 4.11 มีระบบเครือข่ายไร้สายแบบติดตั้งภายใน และรองรับมาตรฐาน IEEE802.11ax (WIFI-6E) หรือดีกว่า
- 4.12 มีช่องเชื่อมต่อตามมาตรฐาน USB 2.0 USB 3.0 และ USB-C จำนวนรวมไม่น้อยกว่า 3 ช่อง
- 4.13 มีช่องเชื่อมต่อแบบ HDMI
- 4.14 มีแป้นพิมพ์ ที่มีตัวอักษรภาษาไทยและภาษาอังกฤษติดบนปุ่มกดอย่างถาวร
- 4.15 มีแบตเตอรี่แบบ Li-Polymer ขนาดไม่น้อยกว่า 50 Whr พร้อมซอฟต์แวร์ที่สามารถตรวจสอบประสิทธิภาพของแบตเตอรี่ได้และเป็นยี่ห้อเดียวกับผลิตภัณฑ์ที่เสนอ
- 4.16 มีอุปกรณ์แปลงไฟฟ้า (Adapter) แบบ USB-C สำหรับต่อใช้งานกับไฟฟ้า 220V
- 4.17 มีน้ำหนักของเครื่องไม่เกิน 1.8 กิโลกรัม โดยไม่รวมน้ำหนักของแบตเตอรี่
- 4.18 มี Security Chip หรือ Firmware ตามมาตรฐาน TPM 2.0 (Trusted Platform Module) หรือดีกว่า
- 4.19 เครื่องคอมพิวเตอร์ที่เสนอต้องมีระบบ Online Support ที่ให้บริการ Download Driver ผ่านช่องทาง Internet จากผู้ผลิต
- 4.20 มี Mouse และ Keyboard ไร้สายที่มีตัวอักษรภาษาไทยและภาษาอังกฤษติดบนปุ่มกดอย่างถาวร โดยใช้ตัวรับสัญญาณขนาดเล็ก (Unifying) ร่วมกัน ทั้งนี้ ต้องเป็นยี่ห้อเดียวกับผลิตภัณฑ์ที่เสนอ

   /4.21 มีจอภาพ...



- 4.21 มีจอภาพแบบ LED (Wide Screen) ขนาดไม่น้อยกว่า 23 นิ้ว ที่มีลำโพงติดตั้งอยู่ภายในและมีช่องเชื่อมต่อแบบ VGA หรือ Display Port หรือ HDMI ที่ความละเอียดสูงสุดไม่น้อยกว่า 1920 x 1080 Pixels โดยขาตั้งสามารถปรับระดับสูง-ต่ำได้
- 4.22 มีกระเป๋าสำหรับใส่เครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ แบบสะพายหลัง
- 4.23 มีซอฟต์แวร์ระบบปฏิบัติการ Windows 11 Professional 64bit แบบ OEM License ที่สามารถดาวน์โหลดเป็น Windows 10 Professional 64bit ได้ โดยจะต้องมีลิขสิทธิ์ถูกต้องตามกฎหมายจากเจ้าของผลิตภัณฑ์และเป็นสิทธิ์การใช้งานของ รพม.
- 4.24 มีการรับประกันความชำรุดบกพร่องของเครื่องคอมพิวเตอร์และอุปกรณ์ทุกชิ้นส่วนทั้งค่าแรง อะไหล่โดยเข้ามาทำการแก้ไข/ซ่อมแซม ณ ที่ติดตั้งเครื่อง (On-Site Service) จากบริษัทผู้ผลิต ภายในวันทำการถัดไป (Next Business Day)
- 4.25 มีเอกสารการรับรองคุณภาพเครื่องคอมพิวเตอร์ตามมาตรฐานที่เกี่ยวข้องกับผลิตภัณฑ์ ด้านต่าง ๆ ดังต่อไปนี้
  - 1) มาตรฐานด้านระบบคุณภาพ ISO 9001 และ ISO 14001 Series
  - 2) มาตรฐานด้านการประหยัดพลังงาน Energy Star และ EPEAT ระดับ Gold
  - 3) มาตรฐานด้านความปลอดภัย UL และ CE
  - 4) มาตรฐานด้านสิ่งแวดล้อม RoHS และ TCO
  - 5) มาตรฐานด้านการแพร่กระจายคลื่นแม่เหล็กไฟฟ้า FCC
  - 6) มาตรฐานด้านความทนทาน MIL-STD 810H

**5. เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานกราฟิก มีคุณสมบัติอย่างน้อยดังนี้**

- 5.1 มีหน่วยประมวลผลกลาง (CPU) ซีพียู M3 แบบ 8 Core หรือดีกว่า
- 5.2 มีหน่วยความจำหลัก ขนาดรวมไม่น้อยกว่า 16 GB
- 5.3 มี Hard Disk ชนิด Solid State Drive (SSD) ความจุไม่น้อยกว่า 1 TB หรือดีกว่า จำนวน 1 หน่วย
- 5.4 มีหน่วยควบคุมการแสดงผล Graphics (GPU) แบบ 10 core
- 5.5 มีระบบเสียงพร้อมลำโพงติดตั้งภายในเครื่อง
- 5.6 มีระบบเครือข่ายไร้สายแบบติดตั้งภายใน และรองรับมาตรฐาน IEEE802.11ax (WIFI-6E) หรือดีกว่า
- 5.7 มีช่องเชื่อมต่อตามมาตรฐาน Thunderbolt/ USB 4.0 หรือดีกว่า จำนวนรวมไม่น้อยกว่า 2 ช่อง
- 5.8 มีจอภาพขนาดไม่น้อยกว่า 15 นิ้ว มีความละเอียดสูงสุดไม่น้อยกว่า 2880 x 1864 Pixels
- 5.9 มีกล้องแบบ HD ความละเอียด 1080p
- 5.10 มีแท็คแพดแบบ Force Touch และสามารถใช้งานแบบ Multi-Touch ได้
- 5.11 มีแบตเตอรี่แบบ Li-Polymer ขนาดไม่น้อยกว่า 60 Whr
- 5.12 มีอุปกรณ์แปลงไฟฟ้า (Adapter) สำหรับต่อใช้งานกับไฟฟ้า 220V พร้อมสายชาร์จแบบ MagSafe
- 5.13 มีแป้นพิมพ์ ที่มีตัวอักษรภาษาไทยและภาษาอังกฤษติดบนปุ่มกดอย่างถาวร



/5.14 มี Mouse ...




- 5.14 มี Mouse ไร้สายที่เป็นยี่ห้อเดียวกับผลิตภัณฑ์ที่เสนอ
- 5.15 มีอุปกรณ์แปลงสัญญาณ (Adapter) แบบ USB-C เป็น Gigabit Ethernet
- 5.16 มีอุปกรณ์แปลงสัญญาณ (Adapter) แบบ USB-C เป็น HDMI และ USB
- 5.17 มีกระเป๋าสำหรับใส่เครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ แบบสะพายหลัง
- 5.18 มีซอฟต์แวร์ระบบปฏิบัติการ MacOS โดยซอฟต์แวร์จะต้องมีลิขสิทธิ์ถูกต้องตามกฎหมาย
- 5.19 เครื่องคอมพิวเตอร์ที่เสนอต้องมีระบบ Online Support ที่ให้บริการ Download Driver ผ่านช่องทาง Internet จากผู้ผลิต
- 5.20 มีการรับประกันความชำรุดบกพร่องของเครื่องคอมพิวเตอร์และอุปกรณ์ทุกชิ้นส่วนทั้งค่าแรง อะไหล่ โดยเข้ามาทำการแก้ไข/ซ่อมแซม ณ ที่ติดตั้งเครื่อง (On-Site Service) จากบริษัทผู้ผลิตและ/หรือผู้ให้เช่า ภายในวันทำการถัดไป (Next Business Day)

## **6. เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานประมวลผล มีคุณสมบัติอย่างน้อยดังนี้**

- 6.1 มีหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า 14 Core และ 20 Tread รุ่นล่าสุดที่มีในท้องตลาด และมีเทคโนโลยีเพิ่มสัญญาณนาฬิกาได้ในกรณีที่ต้องใช้ความสามารถในการประมวลผลสูง (Turbo Boost หรือ Max Boost) โดยมีความเร็วสัญญาณนาฬิกาสูงสุด ไม่น้อยกว่า 5.2 GHz
- 6.2 หน่วยประมวลผลกลาง (CPU) มีหน่วยความจำแบบ Cache Memory ขนาดไม่น้อยกว่า 24 MB
- 6.3 มีจอภาพขนาดไม่เกิน 15.6 นิ้ว แบบ FHD Anti-Glare ที่ความสว่าง 400 nits และมีความละเอียดสูงสุดไม่น้อยกว่า 1920 x 1080 Pixels
- 6.4 มีหน่วยความจำหลักแบบ DDR5 หรือดีกว่า ขนาดไม่น้อยกว่า 32 GB
- 6.5 มี Hard Disk ชนิด M.2 SSD ที่มี Interface แบบ PCIe NVMe ความจุไม่น้อยกว่า 1 TB
- 6.6 มีหน่วยควบคุมการแสดงผลแบบ GDDR6 หรือดีกว่า ที่มีหน่วยความจำไม่น้อยกว่า 4 GB โดยแยกจากหน่วยความจำหลัก
- 6.7 มีระบบเสียงพร้อมลำโพงติดตั้งภายในเครื่อง
- 6.8 มีกล้อง Webcam แบบ FHD ที่สามารถใช้ยืนยันตัวบุคคลได้ โดยติดตั้งภายในตัวเครื่อง พร้อมแผ่นเลื่อนเพื่อปิดกล้องเมื่อไม่ใช้งาน
- 6.9 มีเซ็นเซอร์ยืนยันตัวบุคคลด้วยลายนิ้วมือ (Fingerprint Reader)
- 6.10 มีช่องเชื่อมต่อระบบเครือข่าย Gigabit Ethernet จำนวน 1 ช่อง
- 6.11 มีระบบเครือข่ายไร้สายแบบติดตั้งภายใน และรองรับมาตรฐาน IEEE802.11ax (WIFI-6E) หรือดีกว่า
- 6.12 มีช่องเชื่อมต่อตามมาตรฐาน USB 2.0 USB 3.0 และ USB-C จำนวนรวมไม่น้อยกว่า 3 ช่อง
- 6.13 มีช่องเชื่อมต่อแบบ HDMI
- 6.14 มีแป้นพิมพ์ ที่มีตัวอักษรภาษาไทยและภาษาอังกฤษติดบนปุ่มกดอย่างถาวร
- 6.15 มีแบตเตอรี่แบบ Li-Polymer ขนาดไม่น้อยกว่า 50 Whr พร้อมซอฟต์แวร์ที่สามารถตรวจสอบประสิทธิภาพของแบตเตอรี่ได้และเป็นยี่ห้อเดียวกับผลิตภัณฑ์ที่เสนอ



Print U.   
/6.16 มีอุปกรณ์...

- 6.16 มีอุปกรณ์แปลงไฟฟ้า (Adapter) แบบ USB-C สำหรับต่อใช้งานกับไฟฟ้า 220V
- 6.17 มีน้ำหนักของเครื่องไม่เกิน 1.8 กิโลกรัม โดยไม่รวมน้ำหนักของแบตเตอรี่
- 6.18 มี Security Chip หรือ Firmware ตามมาตรฐาน TPM 2.0 (Trusted Platform Module) หรือดีกว่า
- 6.19 เครื่องคอมพิวเตอร์ที่เสนอต้องมีระบบ Online Support ที่ให้บริการ Download Driver ผ่านช่องทาง Internet จากผู้ผลิต
- 6.20 มี Mouse และ Keyboard ไร้สายที่มีตัวอักษรภาษาไทยและภาษาอังกฤษติดบนปุ่มกดอย่างถาวร โดยใช้ตัวรับสัญญาณขนาดเล็ก (Unifying) ร่วมกัน ทั้งนี้ ต้องเป็นยี่ห้อเดียวกับผลิตภัณฑ์ที่เสนอ
- 6.21 มีจอภาพแบบ LED (Wide Screen) ขนาดไม่น้อยกว่า 23 นิ้ว ที่มีลำโพงติดตั้งอยู่ภายในและมีช่องเชื่อมต่อแบบ VGA หรือ Display Port หรือ HDMI ที่ความละเอียดสูงสุดไม่น้อยกว่า 1920 x 1080 Pixels โดยขาตั้งสามารถปรับระดับสูง-ต่ำได้
- 6.22 มีกระเป๋าสำหรับใส่เครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ แบบสะพายหลัง
- 6.23 มีซอฟต์แวร์ระบบปฏิบัติการ Windows 11 Professional 64bit แบบ OEM License ที่สามารถดาวน์โหลดเป็น Windows 10 Professional 64bit ได้ โดยจะต้องมีลิขสิทธิ์ถูกต้องตามกฎหมายจากเจ้าของผลิตภัณฑ์และเป็นสิทธิ์การใช้งานของ รพม.
- 6.24 มีการรับประกันความชำรุดบกพร่องของเครื่องคอมพิวเตอร์และอุปกรณ์ทุกชิ้นส่วนทั้งค่าแรง อะไหล่โดยเข้ามาทำการแก้ไข/ซ่อมแซม ณ ที่ติดตั้งเครื่อง (On-Site Service) จากบริษัทผู้ผลิต ภายในวันทำการถัดไป (Next Business Day)
- 6.25 มีเอกสารการรับรองคุณภาพเครื่องคอมพิวเตอร์ตามมาตรฐานที่เกี่ยวข้องกับผลิตภัณฑ์ ด้านต่าง ๆ ดังต่อไปนี้
  - 1) มาตรฐานด้านระบบคุณภาพ ISO 9001 และ ISO 14001 Series
  - 2) มาตรฐานด้านการประหยัดพลังงาน Energy Star และ EPEAT ระดับ Gold
  - 3) มาตรฐานด้านความปลอดภัย UL และ CE
  - 4) มาตรฐานด้านสิ่งแวดล้อม RoHS และ TCO
  - 5) มาตรฐานด้านการแพร่กระจายคลื่นแม่เหล็กไฟฟ้า FCC
  - 6) มาตรฐานด้านความทนทาน MIL-STD 810H

**7. เครื่องคอมพิวเตอร์แท็บเล็ต แบบที่ 1 มีคุณสมบัติอย่างน้อยดังนี้**

- 7.1 เป็นเครื่องคอมพิวเตอร์พกพาแบบหน้าจอสัมผัส พร้อมติดตั้งระบบปฏิบัติการ (OS) เวอร์ชันล่าสุด
- 7.2 มีหน่วยประมวลผลกลาง (CPU) ซีพียู A14 แบบ 6 Core หรือดีกว่า
- 7.3 หน่วยควบคุมการแสดงผล Graphics (GPU) แบบ 4 Core
- 7.4 มีหน่วยจัดเก็บข้อมูล (Internal Storage) ความจุไม่น้อยกว่า 64 GB
- 7.5 มีเซ็นเซอร์ยืนยันตัวตนบุคคลด้วยลายนิ้วมือ (Touch ID) หรือดีกว่า
- 7.6 มีระบบเสียงพร้อมลำโพงติดตั้งภายในเครื่อง

 Joint U.   
/7.7 มีระบบ...

- 7.7 มีระบบเครือข่ายไร้สายที่รองรับมาตรฐาน IEEE 802.11ax (WIFI-6) หรือดีกว่า
- 7.8 รองรับ SIM card แบบ Nano-SIM หรือดีกว่า
- 7.9 มีจอภาพขนาดไม่น้อยกว่า 10.9 นิ้ว ชนิด Liquid Retina แบบ LED-Backlit Multi-Touch และมีความละเอียดสูงสุดไม่น้อยกว่า 2360 x 1640 Pixels เคลือบสารกันรอยนิ้วมือ และรองรับ Pencil
- 7.10 มีแบตเตอรี่แบบ Li-Polymer ความจุไม่น้อยกว่า 28 Whr และอุปกรณ์แปลงไฟฟ้า (Adapter) สำหรับต่อใช้งานกับไฟฟ้า 220V
- 7.11 มีปากกาหรือดินสอที่มีแบตเตอรี่ในตัวสามารถชาร์จไฟฟ้าผ่านสาย USB-C ได้ และเป็นยี่ห้อเดียวกับผลิตภัณฑ์ที่เสนอ
- 7.12 มี Smart Cover ที่สามารถใส่ปากกาหรือดินสอที่เสนอได้
- 7.13 มีฟิล์มกันรอยแบบกระจก ที่สามารถใช้งานกับผลิตภัณฑ์ที่เสนอได้
- 7.14 มีสายสัญญาณ USB-C หรือดีกว่า สำหรับรับ-ส่งข้อมูล และชาร์จไฟฟ้าได้ ความยาวไม่น้อยกว่า 1 เมตร
- 7.15 มีการรับประกันความชำรุดบกพร่องของเครื่องคอมพิวเตอร์และอุปกรณ์ทุกชิ้นส่วนทั้งค่าแรง อะไหล่ โดยเข้ามาทำการแก้ไข/ซ่อมแซม ณ ที่ติดตั้งเครื่อง (On-Site Service) จากบริษัทผู้ผลิตและ/หรือผู้ให้เช่า ภายในวันทำการถัดไป (Next Business Day)
- 7.16 มีการรับรองคุณภาพตามมาตรฐานด้านการประหยัดพลังงาน Energy Star

**8. เครื่องคอมพิวเตอร์แท็บเล็ต แบบที่ 2 มีคุณสมบัติอย่างน้อยดังนี้**

- 8.1 เป็นเครื่องคอมพิวเตอร์พกพาแบบหน้าจอสัมผัส พร้อมติดตั้งระบบปฏิบัติการ (OS) เวอร์ชันล่าสุด
- 8.2 มีหน่วยประมวลผลกลาง (CPU) ชิพ M2 แบบ 8 Core หรือดีกว่า
- 8.3 หน่วยควบคุมการแสดงผล Graphics (GPU) แบบ 10 Core
- 8.4 มีหน่วยความจำหลัก ขนาดรวมไม่น้อยกว่า 8 GB
- 8.5 มีหน่วยจัดเก็บข้อมูล (Internal Storage) ความจุไม่น้อยกว่า 256 GB
- 8.6 มีเซ็นเซอร์ยืนยันตัวตนบุคคลด้วยลายนิ้วมือ (Touch ID) หรือดีกว่า
- 8.7 มีระบบเสียงพร้อมลำโพงติดตั้งภายในเครื่อง
- 8.8 มีระบบเครือข่ายไร้สายที่รองรับมาตรฐาน IEEE 802.11ax (WI-FI 6E) หรือดีกว่า
- 8.9 รองรับการใช้งานเซลลูลาร์แบบ 5G และเทคโนโลยี eSIM
- 8.10 มีจอภาพขนาดไม่น้อยกว่า 11 นิ้ว ชนิด Liquid Retina แบบ LED-Backlit Multi-Touch และมีความละเอียดสูงสุดไม่น้อยกว่า 2360 x 1640 Pixels เคลือบสารกันรอยนิ้วมือ และรองรับ Pencil
- 8.11 มีแบตเตอรี่แบบ Li-Polymer ความจุไม่น้อยกว่า 28 Whr
- 8.12 มีปากกาหรือดินสอที่มีแบตเตอรี่ในตัวสามารถชาร์จไฟฟ้าแบบไร้สายเมื่อเชื่อมต่อกับคอมพิวเตอร์ที่เสนอได้ และเป็นยี่ห้อเดียวกับผลิตภัณฑ์ที่เสนอ
- 8.13 มี Smart Cover ที่สามารถใส่ปากกาหรือดินสอที่เสนอได้
- 8.14 มีฟิล์มกันรอยแบบกระจก ที่สามารถใช้งานกับผลิตภัณฑ์ที่เสนอได้

  /8.15 มีสายสัญญาณ...  

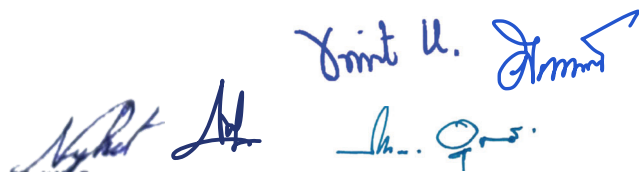

- 8.15 มีสายสัญญาณ USB-C หรือดีกว่า สำหรับรับ-ส่งข้อมูล และชาร์จไฟฟ้าได้ ความยาวไม่น้อยกว่า 1 เมตร
- 8.16 มีอุปกรณ์แปลงไฟฟ้า (Adapter) สำหรับต่อใช้งานกับไฟฟ้า 220V แบบ USB-C ขนาดไม่น้อยกว่า 20 วัตต์
- 8.17 มีหูฟังที่สามารถใช้งานกับผลิตภัณฑ์ที่เสนอได้
- 8.18 มีการรับประกันความชำรุดบกพร่องของเครื่องคอมพิวเตอร์และอุปกรณ์ทุกชิ้นส่วนทั้งค่าแรง อะไหล่ โดยเข้ามาทำการแก้ไข/ซ่อมแซม ณ ที่ติดตั้งเครื่อง (On-Site Service) จากบริษัทผู้ผลิตและ/หรือผู้ให้เช่า ภายในวันทำการถัดไป (Next Business Day)
- 8.19 มีการรับรองคุณภาพตามมาตรฐานด้านการประหยัดพลังงาน Energy Star

**9. เครื่องสำรองไฟฟ้า มีคุณสมบัติอย่างน้อยดังนี้**

- 9.1 เป็นเครื่องสำรองไฟฟ้า (UPS) แบบ Line Interactive ที่มีขนาดไม่น้อยกว่า 800VA/320W
- 9.2 มีช่องเสียบปลั๊กไฟฟ้า จำนวนไม่น้อยกว่า 3 ช่อง
- 9.3 มีระบบป้องกันแรงดันไฟตก (Under Voltage)
- 9.4 มีระบบป้องกันไฟเกิน (Over Voltage)
- 9.5 มีระบบป้องกันไฟกระชาก (Stabilizer)
- 9.6 มีระบบหยุดการทำงานแบตเตอรี่อัตโนมัติ (Low Voltage cut-off)
- 9.7 สามารถจ่ายไฟฟ้าสำรองได้ไม่น้อยกว่า 20 นาที
- 9.8 มีการรับประกันความชำรุดบกพร่องของเครื่องคอมพิวเตอร์และอุปกรณ์ทุกชิ้นส่วนทั้งค่าแรง อะไหล่ โดยเข้ามาทำการแก้ไข/ซ่อมแซม ณ ที่ติดตั้งเครื่อง (On-Site Service) จากบริษัทผู้ผลิต ภายในวันทำการถัดไป (Next Business Day)

**10. ซอฟต์แวร์ป้องกันไวรัส มีคุณสมบัติอย่างน้อยดังนี้**


- 10.1 เป็นซอฟต์แวร์ป้องกันไวรัส Kaspersky Endpoint Security for Business Select หรือดีกว่า
- 10.2 สามารถ Update Engine และ Virus Signature ผ่านช่องทาง Internet
- 10.3 สามารถบริหารจัดการผ่านช่องทางซอฟต์แวร์ Management ที่ติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายของ รพม. ได้โดยอัตโนมัติตลอดระยะเวลาของสัญญาเช่า



Handwritten signatures in blue ink, including the name "Joint U. ...".

ภาคผนวก ข.

รายละเอียด สถานที่ติดตั้งนอกพื้นที่สำนักงาน รพม.

 Joint U. Jomrat  
Ch. Jomrat

ภาคผนวก ข.

รายละเอียด สถานที่ติดตั้งนอกพื้นที่สำนักงาน รพม.

เครื่องคอมพิวเตอร์สำหรับงานสำนักงาน

ลำดับ	อาคารสำนักงาน/สถานี	จำนวน
1	อาคาร บริษัททางด่วนและรถไฟฟ้ากรุงเทพจำกัด (มหาชน) (อาคาร BEM)	13
2	สถานีรถไฟฟ้า สายเฉลิมรัชมงคล (สายสีน้ำเงิน) สถานีศูนย์วัฒนธรรมแห่งประเทศไทย	6
3	สถานีรถไฟฟ้า สายเฉลิมรัชมงคล (สายสีน้ำเงิน) สถานีลาดพร้าว	1
4	สถานีรถไฟฟ้า สายฉลองรัชธรรม (สายสีม่วง) สถานีคลองบางไผ่	13

เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานสำนักงาน แบบที่ 1

ลำดับ	อาคารสำนักงาน/สถานี	จำนวน
1	อาคาร บริษัททางด่วนและรถไฟฟ้ากรุงเทพจำกัด (มหาชน) (อาคาร BEM)	1

*Yint U. Amm*  
*๒๕๖๕*

ภาคผนวก ค.

แบบฟอร์มรายละเอียดคุณสมบัติและประสบการณ์การทำงานของเจ้าหน้าที่

   
In. ๑๖๕.



### รายละเอียดคุณสมบัติและประสบการณ์การทำงานของผู้สมัคร

การเก็บรวบรวมข้อมูลส่วนบุคคลในเอกสารนี้ จัดทำขึ้นภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ด้วยวัตถุประสงค์เพื่อตรวจสอบข้อมูลของผู้สมัครที่เข้ามาปฏิบัติงานให้ รพม. ซึ่งเป็นการประมวลผลข้อมูลส่วนบุคคลเพื่อปฏิบัติตามสัญญา โดยเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็นจากเจ้าของข้อมูลส่วนบุคคล ซึ่ง รพม. จะจัดเก็บข้อมูลส่วนบุคคลจนกว่าจะสิ้นสุดข้อผูกพันตามสัญญา ทั้งนี้ หากมีข้อสอบถามหรือขอใช้สิทธิ์ของผู้สมัครสามารถติดต่อได้ที่ การรถไฟฯขนส่งมวลชนแห่งประเทศไทย สำนักงานใหญ่ เว็บไซต์ [www.mrta.co.th](http://www.mrta.co.th) โทรศัพท์ 0 2716 4000

ชื่อภาษาไทย (คำนำหน้าชื่อ ชื่อ นามสกุล) \_\_\_\_\_ วัน/เดือน/ปี เกิด (วันที่/เดือน/ปี พ.ศ.) \_\_\_\_\_ อายุ (ปี) \_\_\_\_\_ ถิ่นพำนักปัจจุบัน (กรุงเทพมหานคร ประเทศไทย)  
**การศึกษา**  
ประกาศนียบัตรวิชาชีพชั้นสูง (ปวส.) (สาขาวิชา) \_\_\_\_\_ สถานศึกษา (วิทยาลัย / มหาวิทยาลัย / ฯลฯ ประเทศไทย) ปีที่จบการศึกษา (พ.ศ.) \_\_\_\_\_  
ปริญญาตรี (สาขาวิชา) \_\_\_\_\_ สถานศึกษา (วิทยาลัย / มหาวิทยาลัย / ฯลฯ ประเทศไทย) ปีที่จบการศึกษา (พ.ศ.) \_\_\_\_\_  
**สถานะการทำงานในปัจจุบัน**  
สถานที่ (ชื่อหน่วยงาน) \_\_\_\_\_ ลักษณะการจ้าง (อาชีพอิสระ/พนักงานประจำ/อื่นๆ (โปรดระบุ)) \_\_\_\_\_  
ตำแหน่ง (ตำแหน่ง) \_\_\_\_\_ ช่วงเวลาที่ปฏิบัติงาน (วันที่/เดือน/ปี พ.ศ. - วันที่/เดือน/ปี พ.ศ.) \_\_\_\_\_ ระยะเวลาการทำงาน (ปี, เดือน) \_\_\_\_\_ (สำหรับพนักงานประจำเท่านั้น)  
ผลการตรวจประวัติอาชญากรรมด้วยลายนิ้วมือ  ไม่มีประวัติอาชญากรรม

**ประสบการณ์การทำงาน**  
ลำดับที่ 1  
สถานที่ (ชื่อหน่วยงาน) \_\_\_\_\_ ลักษณะการจ้าง (อาชีพอิสระ/พนักงานประจำ/อื่นๆ (โปรดระบุ)) \_\_\_\_\_  
ตำแหน่ง (ตำแหน่ง) \_\_\_\_\_ ช่วงเวลาที่ปฏิบัติงาน (DD/MM/YYYY - DD/MM/YYYY) \_\_\_\_\_ ระยะเวลาการทำงาน (ปี, เดือน) \_\_\_\_\_ (สำหรับพนักงานประจำเท่านั้น)  
ข้าพเจ้าขอรับรองว่ารายละเอียดคุณสมบัติและประสบการณ์การทำงานข้างต้นนี้ เป็นความจริงทุกประการ

รูปถ่าย  
ไม่เกิน 6 เดือน

ลงชื่อ (ลงนามผู้มีอำนาจจากบริษัท) \_\_\_\_\_  
(.....)  
ตำแหน่ง.....  
บริษัท.....  
วันที่...../...../.....

ลงชื่อ (ลงนามเจ้าหน้าที่) \_\_\_\_\_  
(.....)  
วันที่...../...../.....

#### หมายเหตุ

- แบบหลักฐานสำเนาหนังสือรับรองวุฒิการศึกษา หรือประกาศนียบัตร และผลการตรวจประวัติอาชญากรรมด้วยลายนิ้วมือ เพื่อประกอบการพิจารณา
- แบบหลักฐานการเปลี่ยนชื่อหรือนามสกุล (ถ้ามี) เพื่อประกอบการพิจารณา
- ข้อมูลป้อนให้แสดงเป็นพุทธศักราช

*Amn Joint U.*  
*Sh. Q. S. Ad*

ภาคผนวก ง.

ประกาศการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย  
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

  
  
  
Joint U.  




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

ประกาศการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย  
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (ฉบับปรับปรุงครั้งที่ 12)

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

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ 2) พ.ศ. 2556 ข้อ 14 กำหนดให้หน่วยงานของรัฐต้องกำหนด ความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กรหรือ ผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศ ทั้งนี้ ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer: CEO) เป็นผู้รับผิดชอบ ต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

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

1. วัตถุประสงค์และขอบเขต

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

1.1 การเข้าถึงหรือควบคุมการใช้งานสารสนเทศครอบคลุม 4 ด้าน คือ

- 1.1.1 การเข้าถึงระบบสารสนเทศ (Access control) ต้องตรวจสอบการอนุมัติสิทธิ์การเข้าถึงระบบและ กำหนดรหัสผ่าน 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 หรือการไหลเวียนข้อมูลหรือสารสนเทศจะต้องผ่านระบบการรักษาความปลอดภัยที่องค์กร จัดสรรไว้ เช่น Firewall IDS/IPS Proxy หรือการตรวจสอบไวรัสคอมพิวเตอร์ เป็นต้น เพื่อควบคุมและ ป้องกันภัยคุกคามอย่างเป็นระบบ
  - 1.1.3 การเข้าถึงระบบปฏิบัติการ (Operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการ โดยไม่ได้รับอนุญาต โดยกำหนดให้มีการยืนยันตัวตนเพื่อระบุถึงตัวตนของผู้ใช้งาน รวมทั้งกำหนดให้มี การจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น
  - 1.1.4 การเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information access control) ต้องกำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศ โดยให้สิทธิ์เฉพาะระบบงานสารสนเทศที่ ต้องปฏิบัติตามหน้าที่เท่านั้น รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานระบบสารสนเทศอย่างสม่ำเสมอ
  - 1.2 มีระบบสารสนเทศและระบบสำรองที่อยู่ในสภาพพร้อมใช้งาน รวมทั้งมีแผนเตรียมพร้อมในกรณีฉุกเฉินหรือ กรณีที่ไม่สามารถดำเนินการตามวิธีการทางอิเล็กทรอนิกส์ได้ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติ อย่างต่อเนื่อง
  - 1.3 ตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศอย่างสม่ำเสมอ
2. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รพม.
- แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รพม. ใช้แนวทางและกระบวนการ อ้างอิงตาม 1) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศของหน่วยงานรัฐ พ.ศ. 2553 2) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐาน การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555 และ 3) มาตรฐาน ISO/IEC 27001:2013 โดยแบ่งแนวปฏิบัติออกเป็น 16 ส่วนตามเอกสารแนบท้ายประกาศ ดังต่อไปนี้
- 2.1 นโยบายการบริหารจัดการความมั่นคงปลอดภัยสำหรับผู้บริหาร (ส่วนที่ 1)
  - 2.2 ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร (ส่วนที่ 2)
  - 2.3 การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (ส่วนที่ 3)
  - 2.4 การจัดการทรัพย์สิน (ส่วนที่ 4)
  - 2.5 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (ส่วนที่ 5)
  - 2.6 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ (ส่วนที่ 6)
  - 2.7 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (ส่วนที่ 7)
  - 2.8 การควบคุมหน่วยงานภายนอกและผู้ใช้งาน (บุคคลภายนอก) เข้าถึงระบบเทคโนโลยีสารสนเทศ (ส่วนที่ 8)
  - 2.9 การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ของ รพม. (ส่วนที่ 9)
  - 2.10 การใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์ (ส่วนที่ 10)



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

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

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

นโยบายนี้ให้ใช้บังคับเมื่อพ้นกำหนด 7 วัน นับแต่วันที่ผู้มีอำนาจลงนาม

ประกาศ ณ วันที่ 28 กันยายน พ.ศ. 2566



(นายภคพงศ์ ศิริกันทรมาศ)

ผู้ว่าการการรถไฟฟ้ามหานครแห่งประเทศไทย



## สารบัญ

เรื่อง	หน้า
คำนิยาม .....	1
ส่วนที่ 1 นโยบายการบริหารจัดการความมั่นคงปลอดภัยสำหรับผู้บริหาร .....	4
ส่วนที่ 2 ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร .....	5
ส่วนที่ 3 การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม .....	8
ส่วนที่ 4 การจัดการทรัพย์สิน .....	10
ส่วนที่ 5 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ.....	12
ส่วนที่ 6 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ.....	15
ส่วนที่ 7 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย .....	26
ส่วนที่ 8 การควบคุมหน่วยงานภายนอกหรือผู้ใช้งานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ.....	27
ส่วนที่ 9 การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ ของ รฟม.....	29
ส่วนที่ 10 การใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์ .....	32
ส่วนที่ 11 การใช้งานจดหมายอิเล็กทรอนิกส์.....	36
ส่วนที่ 12 การสำรองข้อมูลและการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ .....	37
ส่วนที่ 13 การตรวจสอบและประเมินความเสี่ยง .....	40
ส่วนที่ 14 การถ่ายโอน และแลกเปลี่ยนข้อมูลสารสนเทศ.....	43
ส่วนที่ 15 การควบคุมการเข้ารหัส .....	45
ส่วนที่ 16 การนำอุปกรณ์ส่วนตัวมาใช้งาน (Bring your own device) .....	47

**เอกสารแนบท้ายประกาศ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย**  
**เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ**  
**แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ของ รฟม.**

**คำนิยาม**

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

1. รฟม. หมายถึง การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
2. ฝ่ายเทคโนโลยีสารสนเทศ
3. ผู้บริหารระดับสูงสุด หมายถึง ผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
4. ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของ รฟม.
5. ผู้ใช้งาน หมายถึง บุคคลที่ได้รับอนุญาตให้สามารถเข้าใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. เพื่อประโยชน์ในการดำเนินงานของ รฟม. ดังนี้
  - ผู้ใช้งานภายใน หมายถึง บุคลากรของ รฟม.
  - ผู้ใช้งานภายนอก หมายถึง บุคคลภายนอกที่ รฟม. อนุญาตให้เข้ามาใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. เช่น ที่ปรึกษา ผู้ปฏิบัติงานตามสัญญา หรือนิสิตนักศึกษาฝึกงาน เป็นต้น
6. ผู้ใช้บริการ หมายถึง ผู้ที่สมัครใช้บริการระบบงานสารสนเทศของ รฟม. ผ่านเครือข่ายสาธารณะ (Internet)
7. หน่วยงานภายนอก หมายถึง องค์กรต่าง ๆ รวมถึงผู้รับจ้าง ซึ่ง รฟม. อนุญาตให้มีสิทธิในการเข้าถึง หรือใช้ข้อมูลหรือสินทรัพย์ต่าง ๆ ของ รฟม. โดยจะได้รับสิทธิในการใช้ระบบตามประเภทงานตามอำนาจและต้องรับผิดชอบในการรักษาความลับของข้อมูล
8. ผู้ดูแลระบบ หมายถึง พนักงานที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบสารสนเทศ และพนักงานของผู้รับจ้างที่รับผิดชอบติดตั้งหรือบำรุงรักษาระบบสารสนเทศให้ รฟม.
9. เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
10. มาตรฐาน หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติภารกิจเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย
11. ขั้นตอนปฏิบัติ หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานตามที่ได้กำหนดไว้ตามวัตถุประสงค์
12. แนวปฏิบัติ หมายถึง แนวทางที่ต้องปฏิบัติตามเพื่อให้สามารถบรรลุวัตถุประสงค์หรือเป้าหมายได้ง่ายขึ้น
13. ระบบเทคโนโลยีสารสนเทศ (Information technology system) หมายถึง ระบบงานของ รฟม. ที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายสื่อสารข้อมูลมาช่วยในการสร้างสารสนเทศที่ รฟม. สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุน การให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสารซึ่งมีองค์ประกอบ ได้แก่ ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลและสารสนเทศ เป็นต้น
14. ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด ที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

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



26. ชุดคำสั่งไม่พึงประสงค์ (Malicious code) หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ชัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
27. เครื่องคอมพิวเตอร์ หมายถึง เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ และเครื่องคอมพิวเตอร์แบบพกพา
28. อุปกรณ์เคลื่อนที่ (Mobile device) หมายถึง อุปกรณ์อิเล็กทรอนิกส์แบบพกพา ซึ่งมีความสามารถในการเชื่อมต่อกับอุปกรณ์อื่นเพื่อรับส่งข้อมูลผ่านระบบเครือข่ายโทรคมนาคมไร้สายหรือโดยอาศัยคลื่นแม่เหล็กไฟฟ้าเป็นสื่อกลาง เช่น Tablet, Smart Phone
29. ทรัพย์สินของ รพม. หมายถึง ครุภัณฑ์ รพม. และทรัพย์สินที่ไม่มีการขึ้นทะเบียนครุภัณฑ์ที่ รพม. จัดสรรงบประมาณเพื่อเป็นค่าใช้จ่ายให้ทั้งหมดหรือบางส่วน
30. อุปกรณ์ส่วนตัว หมายถึง อุปกรณ์ที่ไม่ใช่ทรัพย์สินของ รพม. ที่ผู้ใช้งานนำมาเชื่อมต่อกับระบบสารสนเทศของ รพม. เช่น เครื่องคอมพิวเตอร์ส่วนบุคคล (Personal computer) เครื่องคอมพิวเตอร์พกพา (Notebook) อุปกรณ์เคลื่อนที่ (Mobile device) Removable media หรืออุปกรณ์คอมพิวเตอร์ของโครงการรถไฟฟ้า เป็นต้น

## ส่วนที่ 1

### นโยบายการบริหารจัดการความมั่นคงปลอดภัยสำหรับผู้บริหาร

#### วัตถุประสงค์

- เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรมีความสอดคล้องกับมาตรฐานสากลและกฎหมายด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง

#### ผู้รับผิดชอบ

- ผู้บริหารสูงสุด

#### อ้างอิงมาตรฐาน

- หมวดที่ 1 นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information security policy)

#### แนวปฏิบัติ

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

## ส่วนที่ 2

### ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร

#### วัตถุประสงค์

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

#### ผู้รับผิดชอบ

- ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ ผู้อำนวยการฝ่ายทรัพยากรบุคคล ผู้อำนวยการฝ่าย/สำนัก ที่กำกับดูแลงานที่มีการว่าจ้างหน่วยงานภายนอก

#### อ้างอิงมาตรฐาน

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

#### แนวปฏิบัติ

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

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

- 1.2.3 ระบบเทคโนโลยีสารสนเทศที่สร้างหรือพัฒนาโดยผู้ใช้งานในระหว่างการว่าจ้างถือเป็นสินทรัพย์ของ 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)
    - 2.1.1 ผู้บริหาร รฟม. ทุกระดับชั้นมีหน้าที่สนับสนุนและส่งเสริมเรื่องดังต่อไปนี้ แก่ผู้ใช้งาน
      - 2.1.1.1 ประกาศนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ รฟม. เป็นลายลักษณ์อักษรให้ทุกคนรับทราบและปฏิบัติตาม
      - 2.1.1.2 จูงใจให้ผู้ใช้งานปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ รฟม.
      - 2.1.1.3 สร้างความตระหนักถึงความมั่นคงปลอดภัยด้านสารสนเทศที่เกี่ยวข้องกับหน้าที่ความรับผิดชอบของตนเองและของ รฟม.
  - 2.2 การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่ผู้ใช้งาน (Information security awareness, education and training) การสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยอย่างสม่ำเสมอ
    - 2.2.1 ผู้ดูแลระบบต้องแจ้งเตือนภัยคุกคาม และช่องโหว่ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศแก่ผู้ใช้งานที่เกี่ยวข้อง นอกจากนี้ต้องแจ้งเตือนให้ผู้ใช้งานเพิ่มความระมัดระวังความเสี่ยงต่าง ๆ เช่น ไวรัสมัลแวร์ เทคนิคการหลอกล่อทางจิตวิทยา (Social engineering) และช่องโหว่ทางเทคนิค เป็นต้น
    - 2.2.2 ผทท. ต้องดำเนินการฝึกอบรม หรือประชาสัมพันธ์เพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศแก่ผู้ใช้งานเป็นประจำทุกปี
    - 2.2.3 ผทท. ต้องแจ้งผู้ใช้งานให้ทราบ เมื่อมีการเปลี่ยนแปลงนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศของ รฟม. รวมทั้งอธิบายผลกระทบจากการเปลี่ยนแปลงดังกล่าว
  - 2.3 การแจ้งเหตุการณ์ไม่ปกติ
 

ผู้ใช้งานต้องแจ้งเหตุการณ์ไม่ปกติด้านเทคโนโลยีสารสนเทศที่พบผ่านช่องทางที่ รฟม. กำหนดโดยเร็วที่สุด
  - 2.4 การกำหนดบทลงโทษ
    - 2.4.1 ความรับผิดตามกฎหมาย
 

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ไม่ได้ก่อให้เกิดสิทธิทางกฎหมายที่ทำให้ผู้ใช้งานพ้นผิดแม้จะได้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ และผู้ใช้งานตกลงยินยอมที่จะไม่ดำเนินการใด ๆ ทางกฎหมายต่อ รฟม. ซึ่งได้ปฏิบัติตามระเบียบนี้ แต่อย่างไรก็ตามหากผู้ใช้งานกระทำการละเมิดหรือกระทำผิดตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ อาจเป็นความผิดทางวินัยและเป็นเหตุ

ให้ถูกลงโทษทางวินัยได้ รฟม. ไม่มีส่วนรับผิดชอบต่อการละเมิดทรัพย์สินทางปัญญาที่เกิดจากการใช้ระบบคอมพิวเตอร์

#### 2.4.2 การพิจารณาโทษผู้กระทำผิด

ผู้ใช้งานที่กระทำความผิด ผทท. จะเพิกถอนสิทธิ์การใช้งานและอาจเป็นความผิดทางวินัย หรือความผิดตามกฎหมายที่เกี่ยวข้อง

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

### 3. การสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน (Termination and change of employment)

เพื่อกำหนดหน้าที่ความรับผิดชอบเมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน ซึ่งรวมถึงการคืนทรัพย์สินและการถอดถอนสิทธิ์ในการเข้าถึง

#### 3.1 การแจ้งการสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน

3.1.1 ฝ่ายทรัพยากรบุคคลต้องแจ้งให้ฝ่ายเทคโนโลยีสารสนเทศทราบทันทีหากพนักงานมีการลาออก โยกย้าย เกษียณ หรือเสียชีวิต เพื่อฝ่ายเทคโนโลยีสารสนเทศจะได้ตรวจสอบและบริหารจัดการสิทธิ์ในการเข้าถึงระบบเทคโนโลยีสารสนเทศ

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

#### 3.2 การคืนทรัพย์สินของ รฟม.

ผู้ดูแลระบบต้องตรวจสอบเพื่อเรียกคืนทรัพย์สินของ รฟม. จากผู้ใช้งาน เมื่อการสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน

#### 3.3 การถอดถอนสิทธิ์ในการเข้าถึง

3.3.1 ผู้ดูแลระบบต้องถอดถอนสิทธิ์ในการเข้าถึงของผู้ใช้งาน เมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน

3.3.2 การถอดถอนสิทธิ์ในการเข้าถึงหมายถึงรวมถึง 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) หรือสถานที่ที่มีความมั่นคงปลอดภัยและมีการปิดล็อก
3. ผู้ดูแลระบบ ต้องมีการป้องกันสายเคเบิลที่ใช้เพื่อการสื่อสารหรือสายไฟ มิให้มีการดักจับสัญญาณ (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 รพม. เช่น บัตรประจำตัวประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วบันทึกข้อมูลบัตรในสมุดบันทึกหรือระบบงานสารสนเทศ

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

## ส่วนที่ 4

### การจัดการทรัพย์สิน

#### วัตถุประสงค์

- เพื่อบริหารจัดการทรัพย์สินสารสนเทศ ตั้งแต่การจัดการ การใช้งาน จนถึงการยกเลิกใช้งาน โดยมีการระบุ สิทธิขององค์กรและกำหนดหน้าที่ความรับผิดชอบในการปกป้องทรัพย์สินสารสนเทศอย่างเหมาะสม

#### 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 เพื่อรับผิดชอบดูแล ความมั่นคงปลอดภัยสารสนเทศตลอดวงจรอายุการใช้งาน
  - 1.3 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องเรียกคืนทรัพย์สินสารสนเทศเมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน
  - 1.4 ผู้ใช้งานต้องใช้ทรัพย์สินสารสนเทศของ รพม. อย่างระมัดระวัง และใช้เพื่อปฏิบัติงานของ รพม. เท่านั้น รวมทั้งต้องปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ และนโยบาย ของ รพม.
2. การจำแนกประเภทของทรัพย์สินสารสนเทศ (Asset classification)
  - 2.1 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจำแนกประเภททรัพย์สินตามขั้นตอนที่ รพม. กำหนด และทบทวนการ จำแนกดังกล่าวอย่างสม่ำเสมอ
  - 2.2 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจัดทำป้ายชื่อทรัพย์สินสารสนเทศ (Labeling) ให้ชัดเจน พร้อมทั้งจัดให้มีมาตรการ ดูแลการรักษาความมั่นคงปลอดภัยสารสนเทศที่สอดคล้องกับประเภททรัพย์สินตามระดับชั้นความลับที่ รพม. กำหนด
3. การจัดการสื่อบันทึกข้อมูล (Media handling)
  - 3.1 เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ใช้งานต้องควบคุมการใช้งานและจัดเก็บสื่อบันทึกแบบถอดหรือต่อพ่วง กับเครื่องคอมพิวเตอร์ได้ (Removable media) ตามที่ รพม. กำหนด
  - 3.2 เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูล ตามขั้นตอนที่ รพม. กำหนด โดยไม่สามารถกู้คืนข้อมูลกลับมาได้อีกก่อนจะกำจัดอุปกรณ์ดังกล่าวหรือ



ก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อเพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลที่สำคัญได้ โดยพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

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

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

## ส่วนที่ 5

### การจัดทำ การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

#### วัตถุประสงค์

- เพื่อควบคุมการจัดทำ พัฒนา และบำรุงรักษาระบบสารสนเทศ ให้มีการกำหนดมาตรการการรักษาความมั่นคงปลอดภัย เพื่อป้องกันความผิดพลาด สูญหาย และการเปลี่ยนแปลงแก้ไขระบบ

#### ผู้รับผิดชอบ

- ผู้บังคับบัญชา
- ผู้ดูแลระบบ

#### อ้างอิงมาตรฐาน

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

#### แนวปฏิบัติ

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

10. ผู้ดูแลระบบต้องควบคุมการจัดส่ง Source code ผ่านช่องทางที่มั่นคงปลอดภัยและเป็นช่องทางที่ รพม. กำหนดให้ใช้งานเท่านั้น
11. ผู้ดูแลระบบต้องปิดบังข้อมูลส่วนบุคคล (Data Masking) ที่จัดเก็บอยู่ในระบบงานสารสนเทศด้วยวิธีการที่เหมาะสม
12. ผู้ดูแลระบบต้องแสดงข้อมูลของผู้ใช้งานอย่างรัดกุม เช่น การปิดบังข้อมูลสำคัญของผู้ใช้งาน (Sensitive data masking) เป็นต้น
13. กรณีของแอปพลิเคชันที่ใช้งานผ่านอุปกรณ์เคลื่อนที่ (Mobile device) ให้ผู้ดูแลระบบดำเนินการ ดังนี้
  - 13.1 ปิดบังหน้าจอเมื่อย่อแอปพลิเคชัน (Application blurring) เพื่อลดความเสี่ยงที่ข้อมูลสำคัญของผู้ใช้งานจะรั่วไหล
  - 13.2 ขอสสิทธ์เข้าถึงทรัพยากรหรือบริการโดยแอปพลิเคชัน (Application permission) บนอุปกรณ์เคลื่อนที่ของผู้ใช้งานเท่าที่จำเป็น และมีกระบวนการทบทวนการขอสสิทธ์เป็นประจำเพื่อป้องกันการละเมิดสิทธ์ความเป็นส่วนตัวของผู้ใช้งาน
14. ผู้ดูแลระบบต้องควบคุมข้อมูลที่นำมาใช้ในการทดสอบระบบ (Test data) อย่างเหมาะสม โดยไม่นำข้อมูลจริงมาทดสอบ กรณีจำเป็นต้องใช้ข้อมูลจริงต้องได้รับอนุญาตข้อมูลจากเจ้าของก่อนนำมาใช้งาน และทำลายข้อมูลอย่างเหมาะสมตามขั้นตอนที่ รพม. กำหนด
15. ผู้ดูแลระบบต้องแยกระบบสารสนเทศสำหรับการพัฒนา ทดสอบ และใช้งานจริงออกจากกันเพื่อลดความเสี่ยงที่เกิดจากการเปลี่ยนแปลงระบบสารสนเทศโดยไม่ได้รับอนุญาต และต้องมีการกำหนดสิทธิ์การเข้าถึงระบบสารสนเทศที่พัฒนา ทดสอบ หรือใช้งานจริง ทั้งระบบสารสนเทศใหม่ และการปรับปรุงแก้ไขระบบสารสนเทศเดิม
16. ผู้ดูแลระบบต้องมีการกำหนดขั้นตอนการทดสอบระบบสารสนเทศก่อนนำไปใช้งานจริง ทั้งในกรณีปรับปรุงระบบสารสนเทศเดิมและการพัฒนาระบบสารสนเทศใหม่
17. ผู้ดูแลระบบต้องติดตั้งซอฟต์แวร์บนระบบสารสนเทศที่ให้บริการ (Production) ตามขั้นตอนที่ รพม. กำหนด และจำกัดสิทธิ์การติดตั้งซอฟต์แวร์เพื่อให้ระบบสารสนเทศต่าง ๆ มีความถูกต้องครบถ้วนและน่าเชื่อถือ
18. ผู้ดูแลระบบต้องนำซอฟต์แวร์ที่ไม่ละเมิดลิขสิทธิ์มาติดตั้งบนระบบสารสนเทศที่ให้บริการ (Production)
19. ผู้ดูแลระบบต้องกำกับดูแลให้ผู้รับจ้างปฏิบัติตามสัญญาหรือข้อตกลงการให้บริการที่ระบุไว้ โดยครอบคลุมถึงด้านความมั่นคงปลอดภัยสารสนเทศ และการปฏิบัติตามขั้นตอนที่เกี่ยวข้องต่าง ๆ ที่ รพม. กำหนดไว้
20. ผู้ดูแลระบบ ต้องติดตาม ตรวจสอบรายงาน หรือบันทึกการให้บริการของบุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามสัญญาว่าจ้างอย่างสม่ำเสมอ
21. ผู้ดูแลระบบ ต้องดูแลให้ทรัพย์สินสารสนเทศได้รับการบำรุงรักษาและซ่อมแซมตามความต้องการ รวมทั้งต้องมีการบันทึกประวัติการทำงานผิดปกติ การบำรุงรักษา และการซ่อมแซมอุปกรณ์นั้น ๆ อย่างสม่ำเสมอ
22. ผู้ดูแลระบบจะต้องปิดช่องโหว่ของระบบสารสนเทศที่มีระดับความรุนแรงในระดับวิกฤติ (Critical) และระดับความรุนแรงระดับสูง (High) ทั้งหมดก่อนนำไปใช้งานจริง (Production) หรือก่อนเริ่ม Go live โดยเฉพาะระบบที่ให้บริการผ่านเครือข่ายอินเทอร์เน็ต (Internet facing) และระบบที่มีความสำคัญต่อการดำเนินงานของ รพม.
23. ผู้ดูแลระบบต้องพิจารณาเลือกใช้ Version ของ Software ดังนี้

- 23.1 กรณีนำ Software เดิมมาใช้ในการจัดหาหรือพัฒนาระบบ จะต้องนำผลการตรวจสอบช่องโหว่และผลการทดสอบเจาะระบบมาประกอบการพิจารณาคัดเลือกเวอร์ชันของ Software ด้วย เพื่อป้องกันไม่ให้เกิดช่องโหว่เดิมรวมถึงเพื่อลดภาระงานในการปิดช่องโหว่เดิมซ้ำ
- 23.2 กรณีเป็น Software ที่ไม่เคยนำมาใช้งานให้เลือกใช้ Software เวอร์ชันล่าสุด

## ส่วนที่ 6

### การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

#### วัตถุประสงค์

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

#### ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- เจ้าของข้อมูล
- ผู้ใช้งาน

#### อ้างอิงมาตรฐาน

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

#### แนวปฏิบัติ

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

## 1.5 ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ใช้งาน ต้องปฏิบัติ ดังนี้

### 1.5.1 แบ่งประเภทข้อมูล ดังนี้

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

### 1.5.2 จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น 3 ระดับ คือ

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

### 1.5.3 จัดแบ่งลำดับชั้นความลับของข้อมูลตามที่ รพม. กำหนด

### 1.5.4 จัดแบ่งระดับชั้นการเข้าถึง

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

## 1.6 เจ้าของข้อมูลและผู้ดูแลระบบต้องกำหนดเวลาการเข้าถึงระบบสารสนเทศ

## 1.7 ผู้ดูแลระบบต้องจำกัดช่องทางการเข้าถึงระบบเทคโนโลยีสารสนเทศตามช่องทาง ดังนี้

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

## 1.8 ผู้ดูแลระบบต้องกำกับดูแล Default permission ของไฟล์ (File) และ โฟลเดอร์ (Folder) ที่สร้างขึ้นให้มีการจำกัดสิทธิ์ในการเข้าถึง

## 1.9 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องพิจารณาข้อกำหนดต่าง ๆ ที่มีผลทางกฎหมายซึ่งเกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศของ รพม. เช่น พระราชบัญญัติ ข้อกำหนดทางกฎหมาย ข้อกำหนดในสัญญา

และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่น ๆ เป็นต้น เพื่อกำหนดสิทธิ์การเข้าถึงสารสนเทศและระบบเทคโนโลยีสารสนเทศของ รพม.

- 1.10 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องมีการสอบถามสิทธิ์ในการเข้าถึงระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ พร้อมทั้งเพิกถอนสิทธิ์เมื่อพบเห็นสิทธิ์ที่ไม่ถูกต้องตามสิทธิ์ในการเข้าถึง (Authorization matrix)
2. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)
 

ให้มีการควบคุมการลงทะเบียนผู้ใช้งาน การบริหารจัดการรหัสผ่าน การบริหารจัดการสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศ และการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน

  - 2.1 การลงทะเบียนผู้ใช้งาน (User registration)
    - 2.1.1 ผู้ดูแลระบบต้องบริหารจัดการและควบคุมบัญชีชื่อผู้ใช้งาน (Username) มิให้มีการใช้งานบัญชีชื่อผู้ใช้งานซ้ำกัน ทั้งนี้ ในส่วนของพนักงาน/ลูกจ้าง รพม. ให้กำหนดชื่อผู้ใช้งาน (Username) ตามมาตรฐานจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ใช้ในองค์กร
    - 2.1.2 เจ้าของข้อมูลต้องเป็นผู้อนุมัติการสร้างบัญชีผู้ใช้งานชั่วคราว (Temporary user) และต้องจำกัดช่วงเวลาการใช้งานเท่าที่จำเป็น
  - 2.2 การบริหารจัดการรหัสผ่าน (User password management)
    - 2.2.1 ผู้ดูแลระบบต้องกำหนดรหัสผ่านแบบชั่วคราวโดยใช้วิธีการสุ่ม และบังคับให้มีการเปลี่ยนรหัสผ่านเมื่อผู้ใช้งานเข้าใช้งานระบบในครั้งแรก
    - 2.2.2 ผู้ดูแลระบบต้องกำหนดความยาวของรหัสผ่าน ดังนี้
      - 1) ผู้ดูแลระบบมีความยาวอย่างน้อย 16 หลัก
      - 2) ผู้ใช้งานมีความยาวอย่างน้อย 12 หลัก
    - 2.2.3 ผู้ดูแลระบบต้องกำหนดให้มีการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication) ตามความเหมาะสม
    - 2.2.4 ผู้ดูแลระบบต้องกำหนดให้รหัสผ่านมีความซับซ้อน โดยประกอบด้วย ตัวอักษร ตัวเลข และอักขระพิเศษ เช่น (a-Z) (0-9) (@ , # , & , “ , ‘ , \* , = , < , > , % , \$ , + , ?) เป็นต้น
    - 2.2.5 ผู้ดูแลระบบต้องกำหนดให้มีการเปลี่ยนแปลงรหัสผ่าน ดังนี้
      - 1) ผู้ดูแลระบบต้องเปลี่ยนรหัสผ่านทุก ๆ 3 เดือน
      - 2) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทุก ๆ 6 เดือน
      - 3) ผู้ใช้งานเชิงระบบ (System account) ให้พิจารณาเปลี่ยนรหัสผ่านตามความเหมาะสม
    - 2.2.6 ผู้ดูแลระบบต้องกำหนดให้มีการเข้ารหัสข้อมูลรหัสผ่านในระบบ
    - 2.2.7 ผู้ดูแลระบบต้องจัดให้มีการควบคุมรหัสผ่านอย่างเข้มงวด
    - 2.2.8 ผู้ดูแลระบบต้องจัดส่งบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ด้วยวิธีการที่ปลอดภัย
    - 2.2.9 ผู้ดูแลระบบต้องควบคุมดูแลระบบปฏิบัติการ ระบบฐานข้อมูล และระบบงานสารสนเทศ (Application) ที่จัดเก็บบัญชีผู้ใช้งานและรหัสผ่านอย่างเข้มงวด โดยให้เข้าถึงได้เฉพาะผู้ดูแลระบบที่ได้รับอนุญาตเท่านั้น
    - 2.2.10 ผู้ดูแลระบบต้องกำหนดวิธีการหรือกระบวนการยืนยันตัวตนที่ปลอดภัย เช่น กรณีที่ลืมรหัสผ่าน

### 2.2.11 ผู้ดูแลระบบต้องกำหนดให้ผู้ให้บริการ ใช้รหัสผ่านอย่างมั่นคงปลอดภัย ดังนี้

#### กรณีแอปพลิเคชันทั่วไป

- 1) กำหนดความยาวรหัสผ่านอย่างน้อย 12 หลัก ซึ่งประกอบด้วย ตัวอักษร ตัวเลข และ อักขระพิเศษ เช่น (a-z) (0-9) (@ , # , & , “ , ‘ , \* , = , < , > , % , \$ , + , ?) เป็นต้น
- 2) รหัสผ่านต้องไม่เป็นคำที่คาดเดาได้ง่าย เช่น คำที่อยู่ในพจนานุกรม ชื่อ-นามสกุล วันเดือนปีเกิด ที่อยู่ หรือเบอร์โทรศัพท์ เป็นต้น
- 3) ไม่บังคับให้เปลี่ยนรหัสผ่าน ทั้งนี้ขึ้นอยู่กับความสมัครใจในการเปลี่ยนรหัสผ่าน และระบบ ต้องรองรับการเปลี่ยนรหัสผ่านในกรณีต่าง ๆ ด้วยวิธีการที่ปลอดภัย

#### กรณีแอปพลิเคชันที่ใช้งานผ่านอุปกรณ์เคลื่อนที่ (Mobile device)

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

### 2.2.12 ผู้ดูแลระบบและผู้ใช้งานต้องใช้รหัสผ่านอย่างปลอดภัย ดังนี้

- 1) ต้องกำหนดรหัสผ่านที่ไม่สามารถคาดเดาได้ง่าย เช่น คำที่อยู่ในพจนานุกรม “qwerty” “abcde” “12345” ชื่อ-นามสกุล วันเดือนปีเกิด ที่อยู่ หรือเบอร์โทรศัพท์ เป็นต้น
- 2) ต้องไม่ใช้งานรหัสผ่านโดยกระบวนการเข้าใช้งานโดยอัตโนมัติ ได้แก่ การกำหนดค่า “Remember Password” เป็นต้น
- 3) ต้องเก็บรหัสผ่านไว้เป็นความลับเฉพาะบุคคล ไม่เปิดเผยให้ผู้อื่นรับทราบ และไม่พิมพ์รหัสผ่านในลักษณะเปิดเผย เช่น พิมพ์รหัสผ่านต่อหน้าผู้ใช้งานคนอื่น เป็นต้น
- 4) ต้องไม่ใช้บัญชีชื่อผู้ใช้งานและรหัสผ่านร่วมกันกับผู้อื่น แม้ว่าบัญชีชื่อผู้ใช้งานจะได้รับการอนุญาตจากเจ้าของชื่อผู้ใช้งานบุคคลนั้นก็ตาม
- 5) ต้องเปลี่ยนแปลงรหัสผ่านเมื่อมีการแจ้งเตือนจากระบบ หรือสงสัยว่ารหัสผ่านลวงรู้โดยบุคคลอื่น

## 2.3 การบริหารจัดการสิทธิ์ (Privilege management)

### 2.3.1 ผู้บังคับบัญชาต้องกำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียน การเพิกถอนสิทธิ์ การเปลี่ยนแปลงสิทธิ์ และการทบทวนสิทธิ์ของผู้ใช้งานอย่างเป็นลายลักษณ์อักษร

### 2.3.2 กำหนดสิทธิ์ที่เหมาะสมกับผู้ใช้งานตามความจำเป็นและสอดคล้องกับหน้าที่ความรับผิดชอบและจัดเก็บประวัติ (Log) การลงทะเบียน การเพิกถอนสิทธิ์ และการเปลี่ยนแปลงสิทธิ์ของผู้ใช้งาน

### 2.3.3 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจัดให้มีการควบคุมและจำกัดสิทธิ์ในการใช้งานระบบตามความจำเป็นในการใช้งานเท่านั้น

- 1) สิทธิ์ในการสร้างข้อมูล (Create)
- 2) สิทธิ์ในการอ่านข้อมูลหรือเรียกดูข้อมูล (READ)
- 3) สิทธิ์ในการปรับปรุงข้อมูล (Modify / Update)
- 4) สิทธิ์ในการลบข้อมูล (Delete)



- 5) สิทธิในการมอบหมายสิทธิในการดำเนินการแทน (Assign)
  - 6) สิทธิในการรับรองความถูกต้องครบถ้วนของข้อมูล (Approve/Authenticate)
  - 7) ไม่มีสิทธิ
- 2.3.4 เจ้าของข้อมูลและผู้ดูแลระบบต้องเป็นผู้อนุมัติการให้สิทธิเพื่อเข้าถึงสารสนเทศหรือระบบเทคโนโลยีสารสนเทศใด ๆ อย่างเป็นลายลักษณ์อักษร
- 2.3.5 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจำกัดจำนวนผู้ใช้งานที่ทำหน้าที่เป็นผู้ให้สิทธิ์กับผู้ใช้งานให้น้อยที่สุดตามความเหมาะสม
- 2.3.6 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจำกัดระยะเวลาการใช้งานระบบเทคโนโลยีสารสนเทศของ รพม. แก่หน่วยงานภายนอกที่เข้ามาปฏิบัติงานร่วมกับ รพม.
- 2.3.7 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจัดให้มีการถอดถอนหรือเปลี่ยนแปลงสิทธิ์การเข้าถึงทันที เมื่อผู้ใช้งานเกษียณ เปลี่ยนแปลงหน้าที่ความรับผิดชอบ เปลี่ยนแปลงการจ้างงาน หรือไม่มีความจำเป็นในการใช้งานระบบเทคโนโลยีสารสนเทศ
- 2.3.8 ผู้ดูแลระบบต้องลบหรือระงับการใช้งานสิทธิ์ของผู้ใช้งานที่มาจากระบบ (Default user) ในกรณีที่มีความจำเป็นต้องใช้งานต้องกำหนดรหัสผ่านอย่างมั่นคงปลอดภัย
- 2.4 การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of user access rights)
- 2.4.1 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องมีการสอบทานสิทธิ์การเข้าถึงของผู้ใช้งานระบบเมื่อ รพม. มีการเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศหรือโครงสร้างองค์กร
- 2.4.2 ผู้ดูแลระบบ ต้องมีการสอบทานและระงับการใช้งานบัญชีผู้ใช้งานที่ไม่ได้ใช้งานเกิน 180 วัน หากผู้ใช้งานต้องการกลับมาใช้งานจะต้องยืนยันตัวตนให้ ผทท. ทราบ ทั้งนี้ ระยะเวลาที่ไม่ได้ใช้งานของบัญชีผู้ใช้งานอาจจะขึ้นอยู่กับแต่ละระบบสารสนเทศ
3. การป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล และการควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ไม่ปลอดภัย
- 3.1 การป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล (Unattended user equipment)
- 3.1.1 ผู้ดูแลระบบต้องจัดให้มีมาตรการสำหรับป้องกันระบบคอมพิวเตอร์ ระบบเครือข่ายสื่อสารข้อมูล และระบบเทคโนโลยีสารสนเทศ โดยการกำหนดค่าของระบบ (Configuration) ให้มีการล็อกหน้าจอสำหรับอุปกรณ์ที่ไม่มีพนักงานดูแล หรือล็อกอุปกรณ์อยู่เสมอ
- 3.1.2 ผู้ใช้งานและหน่วยงานภายนอก ต้องล็อกหน้าจออัตโนมัติเมื่อไม่มีการใช้งานระบบเทคโนโลยีสารสนเทศของ รพม. ตามระยะเวลาที่กำหนด โดยต้องพักหน้าจอ (Screen saver) อัตโนมัติหลังจากที่ไม่มีการใช้งานคอมพิวเตอร์เป็นระยะเวลานานกว่า 15 นาที ผู้ใช้งานและหน่วยงานภายนอกจะใช้งานต่อได้เมื่อมีการใส่รหัสผ่านที่ถูกต้อง
- 3.1.3 ผู้ใช้งานต้อง Log out ออกจากเครื่องคอมพิวเตอร์เมื่อมีความจำเป็นต้องทิ้งเครื่องคอมพิวเตอร์
- 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 รพม. การควบคุมการพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย การป้องกันพอร์ต (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ การแบ่งแยกเครือข่าย (Segregation in networks) อย่างเหมาะสม การควบคุมการเชื่อมต่อทางเครือข่าย และการควบคุมการกำหนดเส้นทางบนเครือข่าย

##### 4.1 การใช้งานบริการเครือข่าย (Use of network services)

4.1.1 ผู้ดูแลระบบต้องควบคุมการเผยแพร่แผนผังระบบเครือข่ายสื่อสารข้อมูล (Network diagram) รวมถึงโครงสร้าง IP address ชื่อระบบ และชื่ออุปกรณ์สารสนเทศแก่ผู้ที่ไม่ได้รับอนุญาตหรือหน่วยงานภายนอก

4.1.2 ผู้ดูแลระบบต้องควบคุมการใช้งานระบบเครือข่ายสื่อสารข้อมูล เพื่อป้องกันการเข้าถึงระบบเครือข่ายสื่อสารข้อมูลและบริการของระบบเครือข่ายสื่อสารข้อมูลโดยไม่ได้รับอนุญาต

4.1.3 ผู้ดูแลระบบต้องควบคุมการเชื่อมต่อเครือข่ายภายนอก เพื่อใช้งานอินเทอร์เน็ต ซึ่งอาจเป็นช่องทางให้หน่วยงานภายนอกเข้าถึงสารสนเทศหรือระบบเทคโนโลยีสารสนเทศของ รพม. โดยมิได้รับอนุญาต

4.1.4 ผู้ใช้งานต้องแจ้งความประสงค์ในการขอใช้งานบริการเครือข่ายแก่ ผทท. และสามารถใช้บริการเครือข่ายได้หลังจากได้รับการอนุมัติจาก ผทท. แล้ว

4.1.5 ผู้ใช้งาน ต้องไม่ใช้ระบบเครือข่ายสื่อสารข้อมูลเพื่อเป็นช่องทางในการเจาะระบบ (Hacking) หรือการสแกนช่องโหว่ของระบบโดยมิได้รับอนุญาต

##### 4.2 การพิสูจน์ตัวตนของผู้ใช้งานที่อยู่ภายนอก รพม. (User authentication for external connections)

ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนผ่านระบบ Active directory ของ รพม. ก่อนอนุญาตให้ผู้ใช้งานที่อยู่ภายนอก รพม. เข้าใช้งานเครือข่ายและระบบสารสนเทศของ รพม.

##### 4.3 การพิสูจน์ตัวตนของอุปกรณ์ในระบบเครือข่ายสื่อสารข้อมูล (Equipment identification in networks)

ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนของอุปกรณ์ในระบบเครือข่ายสื่อสารข้อมูล ได้แก่ การตรวจสอบ MAC address

##### 4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection)

ผู้ดูแลระบบต้องระงับบริการและพอร์ต (Port) ที่ไม่มีความจำเป็นต้องใช้บนเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่าย

##### 4.5 ผู้ดูแลระบบต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion prevention system/ intrusion detection system) ของระบบเครือข่าย

##### 4.6 การแบ่งแยกเครือข่าย (Segregation in networks)

4.6.1 ผู้ดูแลระบบต้องจัดให้มีการแบ่งแยกเครือข่ายตามกลุ่มของผู้ใช้งาน หรือกลุ่มของระบบเทคโนโลยีสารสนเทศ เพื่อควบคุมการใช้งานในแต่ละเครือข่ายอย่างเหมาะสม โดยพิจารณาจากความ

ต้องการในการเข้าถึงข้อมูล ระดับความสำคัญของข้อมูล รวมถึงการพิจารณาด้านราคา ประสิทธิภาพ และผลกระทบทางด้านความปลอดภัยดังต่อไปนี้

- 1) เครือข่ายที่อนุญาตให้เข้าถึงจากภายนอกและเครือข่ายที่ใช้ภายใน รพม.
  - 2) เครือข่ายแอปพลิเคชัน (Application) ที่มีความสำคัญกับเครือข่ายอื่น ๆ ที่มีความสำคัญน้อยกว่า
  - 3) เครือข่ายสำหรับเครื่องให้บริการ (Server farm) กับเครือข่ายของผู้ใช้งาน ควรมีการติดตั้งอุปกรณ์ที่สามารถแบ่งแยกเครือข่ายได้ เช่น Firewall หรือ Switch ที่สามารถแบ่ง VLAN ได้ เป็นต้น
- 4.6.2 ผู้ดูแลระบบจะกำหนดเส้นทางบนเครือข่ายที่เข้มงวด เพื่อจำกัดการเข้าถึงระยะไกลไปเฉพาะเครือข่ายที่กำหนดเท่านั้น
- 4.6.3 ผู้ดูแลระบบต้องตั้งค่า (Configuration) อุปกรณ์เครือข่าย เช่น Firewall หรือ Router มิให้สามารถบริหารจัดการจากภายนอกเครือข่ายได้ เว้นแต่ในกรณีฉุกเฉินซึ่งต้องได้รับการอนุญาตจากผู้ดูแลระบบเท่านั้น
- 4.7 การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control)
- 4.7.1 ผู้ดูแลระบบต้องจำกัดการใช้งานเครือข่ายของผู้ใช้งานในการเชื่อมต่อกับเครือข่ายของ รพม. เช่น Router หรือ Firewall เป็นต้น พร้อมทั้งติดตั้งระบบควบคุมเพื่อกลั่นกรองข้อมูลที่รับ - ส่ง เช่น Web filtering, E-mail filtering เป็นต้น เพื่อทำให้การเชื่อมต่อมีความปลอดภัย
- 4.7.2 ผู้ดูแลระบบต้องติดตั้ง Firewall ระหว่างเครือข่ายของ รพม. กับเครือข่ายภายนอก ทั้งนี้ การติดตั้ง Firewall ต้องพิจารณาเรื่องดังต่อไปนี้
- 1) การป้องกันการจราจรจากภายนอก ต้องถูกกำหนดให้ใช้เส้นทางที่ผ่าน First tier firewall ที่มีความมั่นคงปลอดภัยเพื่อป้องกันการรั่วไหลของข้อมูลของ รพม. และโครงสร้างพื้นฐานที่มีความสำคัญจากการเข้าถึงที่ไม่ได้รับอนุญาต
  - 2) Firewall ต้องระบุตัวตนและพิสูจน์ตัวตนของผู้ใช้งานก่อนที่จะให้สิทธิ์การเข้าถึงอินเทอร์เน็ต (Interface) เพื่อการบริหารจัดการ Firewall
  - 3) Firewall ต้องตั้งค่าให้ระงับบัญชีผู้ใช้งานหลังจากมีความพยายามที่จะเข้าสู่ระบบไม่สำเร็จ 5 ครั้ง การยกเลิกการระงับต้องดำเนินการโดย ผทท.
  - 4) ไม่อนุญาตให้พิสูจน์ตัวตนผ่านทางอินเทอร์เน็ต (Interface) การจัดการ Firewall จากระยะไกล (Remote)
  - 5) ผู้ที่ได้รับการมอบหมายจาก ผทท. เท่านั้นที่มีสิทธิ์ที่จะเปลี่ยนการตั้งค่าด้านความปลอดภัยบน Firewall
  - 6) Firewall ต้องตั้งค่าให้บันทึกเหตุการณ์ด้านความมั่นคงปลอดภัย
  - 7) Firewall ต้องได้รับการสอบทาน ทดสอบ และตรวจสอบอย่างสม่ำเสมอ
  - 8) Firewall ต้องถูกบริหารจัดการผ่านทาง การติดต่อสื่อสารที่มีการเข้ารหัส
  - 9) ต้องปิดบริการและพอร์ต (Port) ที่ไม่จำเป็นต้องใช้บน Firewall

- 10) Firewall ประเภทซอฟต์แวร์ (Software) ต้องติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายแยกต่างหาก
- 11) Firewall ต้องสามารถป้องกันตัวเองจากการโจมตี DOS (Denial of service) ได้ อย่างเช่น Ping, Sweeps หรือ TCP SYN Floods เป็นต้น
- 12) ต้องใช้เวอร์ชันของซอฟต์แวร์ (Software) Firewall และระบบปฏิบัติการที่เจ้าของผลิตภัณฑ์ยังให้การสนับสนุน
- 13) ผู้ดูแล Firewall ต้องติดตามข้อมูลช่องโหว่จากผู้ให้บริการ (Vendor) เพื่อรับทราบข่าวสาร การ Upgrade และแพตช์ (Patch) ที่จำเป็น และต้องติดตั้งแพตช์ (Patch) ทั้งหมดที่เกี่ยวข้อง

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

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

4.8 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control)

ผู้ดูแลระบบต้องควบคุมการกำหนดเส้นทางบนเครือข่ายเพื่อให้มั่นใจว่าการเชื่อมต่อเครื่องคอมพิวเตอร์และการไหลเวียนของสารสนเทศบนเครือข่าย โดยมีกลไกในการตรวจสอบที่อยู่ปลายทางและต้นทางของการเชื่อมต่อ เช่น การควบคุมโดย Firewall หรือ Proxy เป็นต้น

5. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)

ให้มีการควบคุมการเข้าถึงระบบปฏิบัติการอย่างมั่นคงปลอดภัย การควบคุมการระบุและพิสูจน์ตัวตนของผู้ใช้งาน การควบคุมระบบบริหารจัดการรหัสผ่าน การควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ (System utilities) การควบคุมการหมดเวลาการใช้งานระบบเทคโนโลยีสารสนเทศ และควบคุมการจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ

5.1 ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on procedures)

5.1.1 ผู้ดูแลระบบ ต้องจัดให้มีการควบคุมการเข้าถึงระบบปฏิบัติการอย่างมั่นคงปลอดภัยโดยขั้นตอนการเข้าสู่ระบบต้องเปิดเผยข้อมูลเกี่ยวกับระบบให้น้อยที่สุดเพื่อหลีกเลี่ยงผู้ใช้งานที่ไม่ได้รับอนุญาต ซึ่งขั้นตอนการ Log-on ต้องพิจารณา ดังนี้

- 1) หากกระบวนการเข้าสู่ระบบไม่สำเร็จ ระบบต้องไม่แสดงข้อมูลของระบบหรือแอปพลิเคชัน (Application) ที่ใช้งานอยู่
- 2) ระบบต้องแสดงข้อความเตือนผู้ใช้งานว่าสามารถเข้าใช้งานเครื่องคอมพิวเตอร์ได้เฉพาะผู้ที่มีสิทธิ์เท่านั้น
- 3) หากกระบวนการเข้าสู่ระบบไม่สำเร็จ ระบบต้องไม่แสดงข้อมูลที่สามารถระบุตัวตนของระบบ เช่น เครือข่ายที่ใช้งาน สถานที่ตั้งของระบบ หรือชื่อเครื่องคอมพิวเตอร์แม่ข่าย เป็นต้น

- 4) ระบบต้องไม่แสดงข้อความที่ชี้เฉพาะเหตุของการเข้าสู่ระบบไม่สำเร็จ เช่น ไม่แสดงข้อความว่า บัญชีผู้ใช้งานผิด หรือ รหัสผ่านผิด เป็นต้น
  - 5) ห้ามเข้าสู่ระบบจากบัญชีผู้ใช้งานส่วนบุคคลเดียวกันมากกว่าหนึ่ง Session ในระบบเดียวกัน
  - 6) ระบบต้องจำกัดจำนวนครั้งในการพยายามเข้าสู่ระบบที่ไม่สำเร็จ และต้องพิจารณาเงื่อนไขต่อไปนี้
    - (ก) การเก็บบันทึกผลการเข้าสู่ระบบทั้งที่สำเร็จและไม่สำเร็จ
    - (ข) หน่วงระยะเวลาในการเข้าใช้งานระบบครั้งต่อไป
    - (ค) การตัดการเชื่อมต่อ
    - (ง) การแสดงข้อความเตือนที่หน้าจอของผู้ดูแลระบบเมื่อมีการเข้าสู่ระบบเกินจำนวนครั้งที่จำกัดไว้
  - 7) ระบบต้องแสดงวัน เวลา ในการเข้าสู่ระบบที่สำเร็จในครั้งก่อน พร้อมทั้งบันทึกจำนวนครั้งที่พยายามเข้าไม่สำเร็จนับแต่การเข้าสู่ระบบที่สำเร็จในครั้งก่อนของผู้ใช้งาน
  - 8) ระบบต้องไม่ส่งรหัสผ่านแบบ Clear text ผ่านระบบเครือข่ายสื่อสารข้อมูล
  - 9) ผู้ดูแลระบบต้องกำหนดจำนวนครั้งที่ยอมให้ใส่รหัสผ่านผิดได้ไม่เกิน 5 ครั้ง
- 5.2 การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication)  
 ผู้ดูแลระบบ ต้องจัดให้ผู้ใช้งานมีบัญชีผู้ใช้งานของแต่ละบุคคลเพื่อใช้พิสูจน์ตัวตนในการเข้าถึงระบบเทคโนโลยีสารสนเทศ และต้องใช้ระบบเทคโนโลยีสารสนเทศพิสูจน์ตัวตนผู้ใช้งานในการเข้าถึงระบบปฏิบัติการ โดยผ่านระบบ Active directory หรือ Lightweight Directory Access Protocol (LDAP) ทุกครั้ง พร้อมทั้งบันทึกข้อมูลการเข้าถึง
- 5.3 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities)  
 ผู้ดูแลระบบ ต้องควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้บนระบบที่ใช้งานจริง (Production system) ดังนี้
- 5.3.1 ต้องจัดทำบัญชีโปรแกรมประเภทยูทิลิตี้ (System utilities) ที่นำมาใช้งาน
  - 5.3.2 กำหนดความรับผิดชอบในการใช้โปรแกรมประเภทยูทิลิตี้ (System utilities) แต่ละรายการอย่างชัดเจนและสื่อสารให้ผู้เกี่ยวข้องทราบเพื่อถือปฏิบัติ
  - 5.3.3 ให้มีการพิสูจน์ตัวตน และกำหนดสิทธิ์ในการใช้งานโปรแกรมประเภทยูทิลิตี้เฉพาะกลุ่มคนที่มีหน้าที่รับผิดชอบ
  - 5.3.4 มีการบันทึกเหตุการณ์ (Log) การใช้งานโปรแกรมประเภทยูทิลิตี้ และต้องสอบถามจากผู้ดูแลระบบอย่างสม่ำเสมอ
  - 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

โปรแกรมพักหน้าจอกำหนดให้ป้อนรหัสผ่านหลังจากที่มีการทิ้งเครื่องดังกล่าวไว้โดยไม่มีการใช้งาน เป็นเวลา 15 นาที

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

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

## ส่วนที่ 7

### การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

#### วัตถุประสงค์

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

#### ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

#### อ้างอิงมาตรฐาน

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

#### แนวปฏิบัติ

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



## ส่วนที่ 8

### การควบคุมหน่วยงานภายนอกและผู้ใช้งานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ

#### วัตถุประสงค์

- เพื่อควบคุมหน่วยงานภายนอกและผู้ใช้งานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. ให้เป็นไปอย่างมั่นคงปลอดภัย

#### ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้บังคับบัญชา
- หน่วยงานภายนอก
- ผู้ใช้งาน (บุคคลภายนอก)

#### อ้างอิงมาตรฐาน

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

#### แนวปฏิบัติ

1. ผู้ดูแลระบบต้องประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผล โดยหน่วยงานภายนอกและผู้ใช้งานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศของ รฟม.
2. การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอกและผู้ใช้งานภายนอก
  - 2.1 เจ้าของข้อมูลต้องเป็นผู้อนุญาตการให้สิทธิ์แก่หน่วยงานภายนอกและผู้ใช้งานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของ รฟม. อย่างเป็นทางการลายลักษณ์อักษร
  - 2.2 ผู้บังคับบัญชาต้องกำหนดให้มีการลงนามการไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของ รฟม.
  - 2.3 ผู้บังคับบัญชา ต้องควบคุมให้มีการกำหนดข้อตกลงและความรับผิดชอบที่เกี่ยวข้องกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศลงในสัญญา กับหน่วยงานภายนอกที่ให้บริการด้านสารสนเทศและบริการด้านการสื่อสาร โดยให้ครอบคลุมรวมถึงผู้รับจ้างช่วง
  - 2.4 ผู้บังคับบัญชาต้องกำหนดให้จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกและผู้ใช้งานภายนอก ระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศ ซึ่งมีรายละเอียด ดังนี้
    - 2.4.1 เหตุผลในการขอใช้
    - 2.4.2 ระยะเวลาในการใช้
    - 2.4.3 การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย
    - 2.4.4 การตรวจสอบ MAC address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

- 2.5 ผู้ดูแลระบบมีสิทธิ์ในการตรวจสอบการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอกและ  
ผู้ใช้งานภายนอก เพื่อควบคุมการใช้งานได้อย่างมั่นคงปลอดภัยตามสัญญา
- 2.6 ผู้ดูแลระบบต้องควบคุมให้หน่วยงานภายนอกจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงานและเอกสารที่  
เกี่ยวข้อง รวมทั้งต้องปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อใช้สำหรับควบคุมหรือตรวจสอบการทำงาน และ  
เพื่อให้มั่นใจว่าการปฏิบัติงานเป็นไปตามขอบเขตที่ได้กำหนดไว้
3. ผู้ดูแลระบบต้องแจ้งแนวปฏิบัติต่าง ๆ ที่เกี่ยวข้องแก่หน่วยงานภายนอกและผู้ใช้งานภายนอกเพื่อให้ปฏิบัติตาม
4. ผู้ดูแลระบบ ต้องกำกับดูแลหน่วยงานภายนอกและผู้ใช้งานภายนอกให้ปฏิบัติตามสัญญาหรือข้อตกลงการ  
ให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงด้านความมั่นคงปลอดภัย
5. ผู้ดูแลระบบ ต้องติดตาม ตรวจสอบรายงานหรือบันทึกการให้บริการของหน่วยงานภายนอกตามที่อ้างอิงอย่าง  
สม่ำเสมอตามสัญญาว่าจ้าง
6. ผู้ดูแลระบบ ต้องกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีหน้าที่ในการกำกับดูแล หรือ  
หน่วยงานที่เกี่ยวข้องกับการบังคับใช้กฎหมาย รวมทั้งหน่วยงานที่ควบคุมดูแลสถานการณ์ฉุกเฉินภายใต้  
สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน
7. ผู้ดูแลระบบ ต้องมีขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีความเชี่ยวชาญเฉพาะด้านหรือ  
หน่วยงานที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน
8. ผู้ดูแลระบบต้องควบคุมการเปลี่ยนแปลงของหน่วยงานภายนอกที่ส่งผลกระทบต่อการทำงานขององค์กร และ  
ต้องประเมินความเสี่ยงอย่างเหมาะสมเพื่อควบคุมผลกระทบอันเนื่องมาจากการเปลี่ยนแปลงนั้น
9. หน่วยงานภายนอกและผู้ใช้งานภายนอก ต้องใช้งานทรัพย์สินสารสนเทศของ รพม. ด้วยความระมัดระวัง และ  
รักษาความลับของ รพม. ไม่นำไปเปิดเผย และต้องขออนุญาตพร้อมทั้งปฏิบัติตามเงื่อนไขในการเข้าถึงระบบ  
สารสนเทศของ รพม. ทุกครั้ง
10. หน่วยงานภายนอกและผู้ใช้งานภายนอกต้องแจ้งเหตุการณ์ไม่ปกติต่าง ๆ ด้านเทคโนโลยีสารสนเทศที่พบผ่าน  
ช่องทางที่ รพม. กำหนดโดยเร็วที่สุด
11. หน่วยงานภายนอกและผู้ใช้งานภายนอกต้องจัดเก็บบัญชีผู้ใช้งานที่ รพม. จัดทำไว้ให้ใช้งานเป็นความลับ เฉพาะ  
บุคคล ไม่เปิดเผยให้ผู้อื่นรับทราบ

## ส่วนที่ 9

### การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ ของ รพม.

#### วัตถุประสงค์

- เพื่อควบคุมการใช้งานทรัพย์สินของ รพม. ประเภทเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ที่เหมาะสม ทั้งนี้ เพื่อป้องกันการสูญหาย เสียหาย หรือถูกเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

#### ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

#### อ้างอิงมาตรฐาน

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

#### แนวปฏิบัติ

##### 1. การใช้งานทั่วไป

- 1.1 ผู้ดูแลระบบต้องกำหนดบัญชีซอฟต์แวร์มาตรฐาน (Software standard) ที่อนุญาตให้ติดตั้งบนเครื่องคอมพิวเตอร์ของผู้ใช้งาน และปรับปรุงให้เป็นปัจจุบันเสมอ
- 1.2 ผู้ดูแลระบบต้องเป็นผู้กำหนดการตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) เท่านั้น
- 1.3 ผู้ใช้งานต้องติดตั้งโปรแกรมสำหรับควบคุมการใช้งานอุปกรณ์เคลื่อนที่ (Mobile Device Management: MDM) รวมถึงอุปกรณ์อื่น ๆ ที่ รพม. ไม่สามารถควบคุมการใช้งานผ่านระบบ Active Directory ได้
- 1.4 ผู้ใช้งานต้องใช้งานอย่างมีประสิทธิภาพเพื่องานของ รพม.
- 1.5 ผู้ใช้งานต้องไม่ติดตั้งโปรแกรมที่ละเมิดลิขสิทธิ์บนเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ของ รพม.
- 1.6 ผู้ใช้งานต้องขออนุญาตติดตั้งโปรแกรมในเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ตามขั้นตอนที่ รพม. กำหนด
- 1.7 ผู้ใช้งานต้องไม่ติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ของ รพม. การดำเนินการดังกล่าวต้องดำเนินการโดยผู้ดูแลระบบเท่านั้น
- 1.8 ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่อย่างละเอียด เพื่อให้สามารถใช้งานอย่างปลอดภัยและมีประสิทธิภาพ
- 1.9 ผู้ใช้งานต้องไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ และรักษาให้มีสภาพเดิม
- 1.10 ผู้ใช้งานต้องแจ้งซ่อมเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ที่อยู่ในความรับผิดชอบของ ผทท. ให้ ผทท. เป็นผู้ดำเนินการเท่านั้น
- 1.11 ผู้ใช้งานต้องอัปเดต Patch และระบบปฏิบัติการให้ทันสมัยอยู่เสมอ
- 1.12 ผู้ใช้งานต้องไม่สร้าง Shortcut ไว้บน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของ รพม.

- 1.13 กรณีเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์เคลื่อนที่ ผู้ใช้งานต้องปฏิบัติเพิ่มเติม ดังนี้
  - 1.13.1 ต้องติดตั้ง Application จาก Official Store หรือเว็บไซต์ที่ให้บริการผ่านโปรโตคอล https
  - 1.13.2 ไม่ปรับแต่งการเข้าถึงระบบปฏิบัติการ (rooted/jailbroken)
  - 1.13.3 ในกรณีที่มีการใช้งานอุปกรณ์ประเภทพกพาในที่สาธารณะ ห้องประชุม และพื้นที่ภายนอก อื่น ๆ ที่ไม่มีการป้องกัน หรือไม่ได้อยู่ในบริเวณของ รพม. ให้ป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต เช่น ไม่เปิดการเชื่อมต่อแบบไร้สายโดยไม่มีการเข้ารหัสข้อมูล เป็นต้น
  - 1.13.4 ต้องระมัดระวังการเคลื่อนย้าย โดยต้องใส่กระเป๋าเพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงานหรือหลุดมือ เป็นต้น
  - 1.13.5 ไม่ใส่ในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับหรืออาจถูกจับโยนได้
  - 1.13.6 การใช้งานเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัดต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง
  - 1.13.7 หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอย ชีตข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้
  - 1.13.8 ไม่วางของทับบนหน้าจอและแป้นพิมพ์
  - 1.13.9 การเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น
  - 1.13.10 ไม่เคลื่อนย้ายเครื่องในขณะที่ Harddisk กำลังทำงาน
  - 1.13.11 ไม่ใช้หรือวางใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่าง ๆ เป็นต้น
  - 1.13.12 ไม่วางใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูง เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น
  - 1.13.13 ไม่ติดตั้งหรือวางในที่ที่มีการสั่นสะเทือน เช่น ในยานพาหนะที่กำลังเคลื่อนที่
  - 1.13.14 การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้
  - 1.13.15 รับผิดชอบในการป้องกันการสูญหาย เช่น ต้องล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย
  - 1.13.16 นำติดตัวไปด้วยเสมอ เช่น ไม่ละทิ้ง อุปกรณ์ประมวลผลประเภทพกพาในรถยนต์ ห้องพักในโรงแรม หรือห้องประชุม เป็นต้น ในกรณีที่มีความจำเป็นต้องละทิ้งให้จัดเก็บไว้ในสถานที่ที่มั่นคงปลอดภัย
  - 1.13.17 ไม่เก็บหรือใช้งานในสถานที่ที่มีความร้อน ความชื้นหรือฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ
  - 1.13.18 ไม่เปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub component) ที่ติดตั้งอยู่ภายใน เช่น แบตเตอรี่ หน่วยความจำ
2. แนวปฏิบัติในการใช้รหัสผ่าน
  - ให้ผู้ใช้งานปฏิบัติตามการใช้งานรหัสผ่าน (Password Use) (ส่วนที่ 6)
3. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malicious code)

- 3.1 ผู้ดูแลระบบต้องควบคุมการ Update ระบบปฏิบัติการ เว็บเบราว์เซอร์ และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ
  - 3.2 ผู้ดูแลระบบต้องติดตั้งและปรับปรุงโปรแกรมป้องกันไวรัสให้ทันสมัยอยู่เสมอ
  - 3.3 ผู้ใช้งานต้องไม่ปิดหรือยกเลิกระบบการป้องกันไวรัสที่ติดตั้งอยู่
  - 3.4 ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อบันทึกต่าง ๆ เช่น Thumb drive และ Data storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์ของ รพม.
  - 3.5 ผู้ใช้งาน หากพบหรือสงสัยว่าเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ติดชุดคำสั่งไม่พึงประสงค์ ให้รีบยกเลิกเชื่อมต่อเครื่องเข้ากับระบบเครือข่ายสื่อสารข้อมูลเพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่น ๆ ได้ และแจ้ง ผทท. ทราบทันที
4. การสำรองข้อมูลและการกู้คืน
    - 4.1 ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ไว้บนสื่อบันทึกอื่น ๆ เช่น ระบบ File Sharing, CD, DVD, External harddisk เป็นต้น
    - 4.2 ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ
  5. ผู้ดูแลระบบ ต้องควบคุมให้เครื่องคอมพิวเตอร์ได้รับการปรับตั้งค่าอย่างเหมาะสม เพื่อป้องกันการใช้งานหรือติดตั้ง Mobile code เช่น Active x, Java จากแหล่งที่ไม่น่าเชื่อถือ

## ส่วนที่ 10

### การใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์

#### วัตถุประสงค์

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

#### ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

#### อ้างอิงมาตรฐาน

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

#### แนวปฏิบัติ

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

2. ผู้ใช้งานต้องไม่มีเจตนาปิดบังหรือบิดเบือนตัวตนเมื่อมีการใช้งานอินเทอร์เน็ต
3. ผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัส พร้อมทั้งต้องปรับปรุง Virus signature ที่เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพาให้มีความทันสมัยอยู่เสมอ ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web browser) และต้องปิดช่องโหว่ของระบบปฏิบัติการที่เว็บเบราว์เซอร์ติดตั้งอยู่
4. ผู้ใช้งานจะต้องตรวจสอบไวรัส (Virus scanning) ก่อนการรับ - ส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ต
5. ผู้ใช้งานต้องไม่ใช่เครือข่ายอินเทอร์เน็ตของ รฟม. เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น
6. ผู้ใช้งานจะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของ รฟม.
7. ผู้ใช้งานต้องหลีกเลี่ยงการกระทำที่สิ้นเปลืองทรัพยากรของเครือข่ายอินเทอร์เน็ต ดังนี้
  - (ก) ส่งจดหมายอิเล็กทรอนิกส์ลูกโซ่
  - (ข) ใช้เวลาในการเข้าถึงอินเทอร์เน็ตเกินความจำเป็นยกเว้นเพื่อปฏิบัติงานให้ รฟม.
  - (ค) เล่นเกม Online
  - (ง) เข้าห้องพูดคุย Online ที่ไม่ได้มีวัตถุประสงค์เพื่อปฏิบัติงานให้ รฟม.
8. ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เป็นการทำประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับ รฟม.
9. ผู้ใช้งานต้องไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของ รฟม.
10. ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต
11. ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ที่จะทำให้อื่นเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย
12. ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน
13. ผู้ใช้งานต้องคำนึงว่าข้อมูลจากอินเทอร์เน็ตอาจไม่มีความทันสมัยหรือไม่มีความถูกต้อง ผู้ใช้งานต้องตรวจสอบความถูกต้องของข้อมูลจากแหล่งที่น่าเชื่อถือก่อนที่จะเผยแพร่ข้อมูลดังกล่าว
14. ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา
15. ผู้ใช้งานต้องไม่ใช่ข้อมูลที่ช่วยุให้ร้ายในการเสนอความคิดเห็นที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของ 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 รพม.
  - 19.2 ผู้ใช้งานต้องระมัดระวังในการใช้สื่อสังคมออนไลน์ เนื่องจากพื้นที่บนสื่อสังคมออนไลน์เป็นพื้นที่สาธารณะไม่ใช่พื้นที่ส่วนบุคคล ซึ่งข้อมูลการใช้งานต่าง ๆ จะถูกบันทึกไว้และอาจมีผลทางกฎหมาย ถึงแม้จะเป็นการแสดงความคิดเห็นในนามชื่อบัญชีส่วนตัว และพึงตระหนักถึงผลกระทบที่อาจเกิดขึ้นกับ รพม. ได้
  - 19.3 ผู้ใช้งานที่ใช้สื่อสังคมออนไลน์เป็นเครื่องมือสื่อสารข้อมูลในกิจการของ รพม. หรือชื่อบุคคลที่ทำให้เข้าใจได้ว่าเป็นบุคคลในสังกัด ต้องแสดงภาพ และข้อมูลที่ถูกต้องชัดเจนในข้อมูล โปรไฟล์ (Profile) และพึงใช้ด้วยความสุภาพและมีวิจารณญาณ
  - 19.4 ผู้ใช้งานควรตั้งคำถามที่ใช้ในกรณีกู้คืนบัญชีผู้ใช้งานหรือกู้คืนรหัสผ่าน (Forgot your password) ควรหลีกเลี่ยงข้อมูลหรือคำถามที่เป็นส่วนบุคคลและเป็นข้อมูลที่ผู้อื่นคาดเดาได้ยากเพื่อป้องกันการสุ่มคำถามจากผู้ประสงค์ร้าย
  - 19.5 ผู้ใช้งานต้องไม่ใช้ระบบอีเมลของเว็บไซต์ประเภทสื่อสังคมออนไลน์ หากจำเป็นต้องใช้จะต้องระมัดระวังในการคลิกลิงก์ที่น่าสงสัย โดยเฉพาะอีเมลแจ้งเตือนจากเว็บไซต์ต่าง ๆ ในลักษณะเชิญให้คลิกลิงก์ที่แนบมาในอีเมล ผู้ใช้งานต้องสงสัยว่าลิงก์ดังกล่าวเป็นลิงก์ที่ไม่ปลอดภัย (ลิงก์ที่ถูกสร้างมาเพื่อใช้ขโมยข้อมูลส่วนบุคคล ด้วยการนำไปสู่เว็บไซต์ที่ดูน่าเชื่อถือที่ผู้ประสงค์ร้ายสร้างไว้เพื่อให้ผู้ใช้งานกรอกข้อมูลส่วนตัว เช่น รหัสผ่าน เป็นต้น)
  - 19.6 ผู้ใช้งานต้องศึกษาการตั้งค่าความเป็นส่วนตัวหรือ “Privacy settings” ให้เข้าใจเป็นอย่างดีและปรับแต่งการตั้งค่าความเป็นส่วนตัวให้เหมาะสมเพื่อป้องกันการถูกละเมิดความเป็นส่วนตัวซึ่งอาจจะส่งผลกระทบต่อตนเองหรือ รพม.
  - 19.7 ผู้ใช้งานต้องใช้งานสื่อสังคมออนไลน์อย่างเหมาะสม โดยไม่ละเมิดกฎหมายและไม่ก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานขององค์กร
  - 19.8 ผู้ใช้งานควรปิดการใช้งานระบบโพสต์ข้อความสาธารณะทุก ๆ ส่วนของเว็บไซต์ประเภท Social network หากจำเป็นต้องใช้งานต้องปรับค่าให้มีการตรวจสอบข้อความก่อนเพื่อหลีกเลี่ยงโอกาสแพร่กระจายลิงก์ที่ไม่ปลอดภัยจากผู้ประสงค์ร้าย ซึ่งเป็นหนึ่งในเทคนิคที่ใช้ในการโจมตีประเภท Spear-phishing
  - 19.9 ผู้ใช้งานต้องตรวจสอบก่อนจะรับเพื่อนเข้ากลุ่มในเว็บไซต์ประเภท Social network โดยต้องแน่ใจว่าข้อมูลส่วนตัวของเพื่อนคนนั้น เช่น รูปถ่ายและประวัติส่วนตัวไม่ถูกแก้ไขเพื่อปลอมแปลงตัวตนจากผู้ประสงค์ร้ายที่หวังแอบอ้างเพื่อคุกคามเป้าหมาย



- 19.10 ผู้ใช้งานต้องตระหนักไว้เสมอว่าข้อมูลต่าง ๆ ที่ผู้ใช้งานเผยแพร่ไว้บนบริการสื่อสังคมออนไลน์นั้นคงอยู่ถาวรและผู้อื่นอาจเข้าถึงและเผยแพร่ข้อมูลเหล่านั้นได้
- 19.11 ผู้ใช้งานต้องมีข้อพิจารณาในการรับเพื่อนเข้ากลุ่มที่ชัดเจน และควรประกาศข้อความปฏิเสธความรับผิดชอบที่เกี่ยวกับเนื้อหาหรือข้อความแสดงความคิดเห็นซึ่งถูกโพสต์จากเพื่อนในกลุ่มที่อาจปรากฏในเว็บไซต์ประเภท Social network ของผู้ใช้งานเอง
- 19.12 ผู้ใช้งานต้องติดตั้งซอฟต์แวร์ป้องกันไวรัส และอัปเดตฐานข้อมูลไวรัสของโปรแกรมอยู่เสมอ และต้องหลีกเลี่ยงการใช้โปรแกรมที่ละเมิดลิขสิทธิ์เพราะอาจจะมีโปรแกรมประสงค์ร้ายแฝงตัวอยู่ภายในเพื่อลักลอบ ปลอมแปลง หรือขโมยข้อมูลสำคัญของผู้ใช้งานได้
- 19.13 ผู้ใช้งานต้องระมัดระวังการใช้ถ้อยคำและภาษาที่อาจเป็นการดูหมิ่น ยุ้ง ทำร้าย หรือเป็นการละเมิดต่อบุคคลอื่น กรณีบุคคลอื่นมีความคิดเห็นที่แตกต่างพึงงดเว้นการโต้ตอบด้วยถ้อยคำรุนแรง
- 19.14 ผู้ใช้งานต้องระมัดระวังกระบวนการหาข่าว หรือภาพจากสื่อสังคมออนไลน์ โดยมีการตรวจสอบอย่างถี่ถ้วนรอบด้านและต้องอ้างอิงแหล่งที่มาเมื่อนำเสนอ เว้นแต่สามารถตรวจสอบและอ้างอิงจากแหล่งข่าวได้โดยตรง
- 19.15 หากผู้ใช้งานต้องการใช้สื่อสังคมออนไลน์เป็นเครื่องมือในการรายงานข่าวในนามของบุคคลธรรมดาต้องแสดงให้เห็นชัดเจนว่า ข้อความใดเป็น "ข่าว" ข้อความใดเป็น "ความคิดเห็นส่วนตัว"
- 19.16 การส่งต่อหรือเผยแพร่ข้อมูลในสื่อสังคมออนไลน์ (Social media)
- 19.16.1 ผู้ใช้งานต้องไม่ส่งต่อหรือเผยแพร่ข้อมูลที่เป็นเท็จ ข่าวลือ ข่าวไม่ปรากฏที่มา เป็นเพียงการคาดเดา หรือส่งผลเสียหายกับบุคคล สังคม หรือ รพม.
- 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 รพม. ให้มีความปลอดภัยและมีประสิทธิภาพ

#### ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

#### อ้างอิงมาตรฐาน

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

#### แนวปฏิบัติ

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

## ส่วนที่ 12

### การสำรองข้อมูลและการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

#### วัตถุประสงค์

- เพื่อให้มีข้อมูลสำรองไว้ใช้งานในกรณีที่ข้อมูลหลักเกิดความเสียหายไม่สามารถใช้งานหรือเข้าถึงได้ หรือเมื่อเกิดภาวะฉุกเฉินต่าง ๆ
- เพื่อให้มีการปฏิบัติที่สอดคล้องกับกฎหมาย พระราชบัญญัติ หรือข้อบังคับภายนอกอื่น ๆ

#### ผู้รับผิดชอบ

- ผู้บังคับบัญชา
- ผู้ดูแลระบบ
- เจ้าของข้อมูล
- ผู้ใช้งาน

#### อ้างอิงมาตรฐาน

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

#### แนวปฏิบัติ

##### 1. การสำรองข้อมูลระบบแม่ข่าย

ข้อมูลระบบแม่ข่ายและข้อมูลสำคัญซึ่งเป็นความลับของ รพม. ต้องได้รับการเก็บรักษาไว้ที่ระบบเก็บข้อมูลส่วนกลาง และสำรองข้อมูลไว้อย่างสม่ำเสมอ เพื่อให้มีข้อมูลสำรองไว้ใช้ ในกรณีที่ข้อมูลหลักเกิดความเสียหายหรือไม่สามารถใช้งาน ความถี่ในการดำเนินการสำรองข้อมูลและขั้นตอนการสำรองข้อมูลระบบแม่ข่ายเป็นความรับผิดชอบของ ผทท. โดยมีแนวปฏิบัติ ดังนี้

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

2. การสำรองข้อมูลคอมพิวเตอร์ส่วนบุคคล  
ผู้ใช้งานจะต้องสำรองข้อมูลสำคัญที่เก็บรักษาไว้ในเครื่องคอมพิวเตอร์ส่วนบุคคลหรือคอมพิวเตอร์ หรืออุปกรณ์พกพาอื่น ๆ อย่างสม่ำเสมอ ความถี่ในการสำรองข้อมูลขึ้นอยู่กับความถี่ของการเปลี่ยนแปลงของข้อมูลและระดับความสำคัญของข้อมูลหากเกิดการสูญหาย
3. การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์  
เพื่อให้สามารถระบุตัวบุคคลผู้ใช้งานได้อย่างถูกต้อง ผู้ดูแลระบบต้องดำเนินการดังนี้
  - 3.1 เลือกใช้นาฬิกาจากแหล่งที่นำเชื่อถือที่มีการเชื่อมต่อในลำดับชั้น Stratum 0 โดยนาฬิกาจากแหล่งดังกล่าวจะต้องได้รับการอนุมัติให้ใช้งาน
  - 3.2 ตั้งนาฬิกาของอุปกรณ์ที่ให้บริการทุกชนิดจาก NTP Server ของ รฟม. เท่านั้น
  - 3.3 ต้องทบทวนนาฬิกาที่ NTP Server อย่างน้อยสัปดาห์ละ 1 ครั้ง
  - 3.4 ต้องจัดเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ โดยระยะเวลาในการเก็บตามประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 (อย่างน้อย 90 วัน)
  - 3.5 เก็บรักษาข้อมูลจราจรคอมพิวเตอร์ในสื่อที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง มีการเก็บรักษาความลับของข้อมูลตามระดับชั้นความลับในการเข้าถึงตามที่ รฟม. กำหนด
  - 3.6 ประเภทของสารสนเทศที่เก็บรักษา แสดงตามตาราง

ประเภทของสารสนเทศ	กฎหมายที่เกี่ยวข้อง	ระยะเวลาการเก็บรักษา (ปี)
Authentication server logs (RADIUS, TACACS)	1) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	1
Email server logs	2) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560	1
Web application server logs	3) ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม	1
NTP server logs	เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564	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 และจัดทำเป็นบัญชีรายชื่อระบบดังกล่าว รวมทั้งปรับปรุงรายชื่อระบบสำคัญและบัญชีฯ 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 ลิขสิทธิ์ในเอกสารหรือซอฟต์แวร์ 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. ผู้ดูแลระบบต้องกำหนดกระบวนการตรวจสอบและการแจ้งเตือนเมื่อเกิดเหตุผิดปกติเกี่ยวกับการใช้งานทรัพยากร (Capacity) กำหนดเกณฑ์การใช้งานทรัพยากรและวางแผนด้านทรัพยากรสารสนเทศให้รองรับการปฏิบัติงานในอนาคตอย่างเหมาะสม รวมถึงต้องติดตามผลการใช้งานทรัพยากรสารสนเทศ
8. ผู้ดูแลระบบต้องมีการตรวจสอบการทำงาน (Monitor) ของระบบรักษาความปลอดภัยและระบบปฏิบัติการอย่างสม่ำเสมอ
9. ผู้ดูแลระบบ ต้องป้องกันการเข้าใช้งานเครื่องมือที่ใช้เพื่อการตรวจสอบ เพื่อมิให้เกิดการใช้งานผิดประเภทหรือถูกละเมิดการใช้งาน (Compromise) โดยควบคุมการเข้าถึง และตรวจสอบการนำเครื่องมือไปใช้งานอย่างสม่ำเสมอ
10. ผู้ดูแลระบบต้องประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
11. ผู้บังคับบัญชาต้องติดตามผลการดำเนินการตามแผนบริหารจัดการความเสี่ยง (Risk treatment plan) เป็นประจำทุกไตรมาส
12. ผู้ดูแลระบบต้องประเมินความเสี่ยงแล้วจัดลำดับความสำคัญของความเสี่ยงนั้นและค้นหาวิธีการเพื่อลดความเสี่ยงตามขั้นตอนที่ รพม. กำหนด พร้อมทั้งพิจารณาข้อดีข้อเสียของวิธีการเหล่านั้นเพื่อให้ผู้บริหารของ รพม. ตัดสินใจเลือกวิธีการเพื่อลดความเสี่ยงหรือยอมรับความเสี่ยง เมื่อเลือกวิธีการลดความเสี่ยงแล้วผู้บริหารต้องจัดสรรทรัพยากรอย่างเพียงพอเพื่อดำเนินการ แนวทางการลดความเสี่ยง แบ่งได้เป็น 3 รูปแบบ ได้แก่
  - 12.1 การเลือกใช้เทคโนโลยี เพื่อใช้ในการลดความเสี่ยงและเพิ่มความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รพม. เป็นวิธีที่จำเป็นต้องใช้งบประมาณและทรัพยากรอย่างเพียงพอในการดำเนินการ เช่น การเลือกใช้อุปกรณ์ Firewall มากกว่าหนึ่งผลิตภัณฑ์ในการป้องกันการเข้าถึงเครือข่ายที่สำคัญ การใช้อุปกรณ์สมาร์ตการ์ด หรือ USB Token ในการตรวจสอบยืนยันตัวตนในการเข้าใช้งานระบบจากภายนอก รพม. เป็นต้น
  - 12.2 การปรับเปลี่ยนขั้นตอนปฏิบัติ ต้องออกแบบขั้นตอนปฏิบัติใหม่ที่รัดกุมและสามารถรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รพม. ได้ดีขึ้น เมื่อออกแบบขั้นตอนปฏิบัติใหม่แล้วต้องมีการพิจารณาหาหรือความเหมาะสม ความเป็นไปได้ และผู้บริหารต้องเป็นผู้อนุมัติให้มีการบังคับใช้ขั้นตอนปฏิบัติใหม่นั้น
  - 12.3 ผู้ดูแลระบบต้องแจ้งขั้นตอนปฏิบัติให้ผู้เกี่ยวข้องรับรู้อย่างทั่วถึง รวมทั้งต้องจัดฝึกอบรมผู้ใช้งานที่เกี่ยวข้องเพื่อให้สามารถปฏิบัติตามขั้นตอนปฏิบัติใหม่ได้อย่างราบรื่นและมีประสิทธิภาพ
13. การตรวจสอบความปลอดภัยของระบบสารสนเทศ
  - 13.1 ผู้ดูแลระบบ ต้องวางแผนการตรวจสอบและประเมินช่องโหว่หรือจุดอ่อนด้านความมั่นคงปลอดภัยสารสนเทศ และแจ้งผู้ที่เกี่ยวข้องเพื่อแก้ไขในกรณีที่พบว่าช่องโหว่หรือจุดอ่อนนั้นอาจเป็นเหตุการณ์ด้านความมั่นคงปลอดภัย อย่างน้อยปีละ 1 ครั้ง
  - 13.2 ผู้ดูแลระบบต้องตรวจสอบระบบสารสนเทศที่จะต้องมีการปรับปรุงเมื่อมีเวอร์ชันใหม่ (Patch) รวมทั้งข้อมูลที่เกี่ยวข้องกับช่องโหว่ด้านเทคนิคอย่างสม่ำเสมอเพื่อให้ทราบถึงภัยคุกคามและความเสี่ยง รวมถึงหาวิธีป้องกันและแก้ไขที่เหมาะสมกับช่องโหว่นั้น
  - 13.3 ผู้ใช้งาน ผู้ดูแลระบบ และหน่วยงานภายนอก ต้องบันทึกและรายงานช่องโหว่หรือจุดอ่อนใด ๆ ด้านความมั่นคงปลอดภัยสารสนเทศ ที่อาจสังเกตพบระหว่างการติดตามการใช้งานระบบสารสนเทศ ผ่านช่องทางบริหารจัดการที่กำหนดไว้อย่างเหมาะสม และต้องดำเนินการปิดช่องโหว่ที่มีการตรวจพบหรือได้รับแจ้ง

14. 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 หรือแลกเปลี่ยนผ่านระบบสารสนเทศให้เหมาะสมตามระดับชั้นความลับข้อมูลสารสนเทศ ตามขั้นตอนที่ รพม. กำหนด
2. ผู้บังคับบัญชา และเจ้าของข้อมูล ต้องควบคุมให้มีการจัดทำข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศระหว่างองค์กรกับบุคคลหรือหน่วยงานภายนอก
3. ผู้ดูแลระบบต้องแลกเปลี่ยนข้อมูลสารสนเทศต้องแลกเปลี่ยนผ่านช่องทางที่ปลอดภัย เช่น Web Service ที่ใช้งานผ่านโปรโตคอล https
4. ผู้ดูแลระบบ ต้องมีการป้องกันข้อมูลสารสนเทศที่มีการสื่อสารกันผ่านข้อมูลอิเล็กทรอนิกส์ (Electronic messaging) เช่น จดหมายอิเล็กทรอนิกส์ (E-mail) หรือ Instant messaging ด้วยวิธีการหรือมาตรการที่เหมาะสม
5. ผู้ดูแลระบบ ต้องป้องกันข้อมูลสารสนเทศที่มีการแลกเปลี่ยนในการทำพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce) ผ่านเครือข่ายคอมพิวเตอร์สาธารณะ เพื่อมิให้มีการฉ้อโกง ละเมิดสัญญา หรือมีการรั่วไหล หรือข้อมูลสารสนเทศถูกแก้ไขโดยมิได้รับอนุญาต
6. ผู้ดูแลระบบ ต้องป้องกันข้อมูลสารสนเทศที่มีการสื่อสาร หรือแลกเปลี่ยนในการทำธุรกรรมทางออนไลน์ (Online transaction) เพื่อมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ ส่งข้อมูลไปผิดที่ การรั่วไหลของข้อมูล ข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ หรือถูกส่งซ้ำโดยมิได้รับอนุญาต
7. ผู้ดูแลระบบ ต้องควบคุมการรับส่งข้อมูลสารสนเทศเพื่อป้องกันความผิดพลาด ดังนี้
  - 7.1 ความไม่สมบูรณ์ของข้อมูลสารสนเทศที่รับ-ส่ง
  - 7.2 การส่งข้อมูลสารสนเทศผิดจุดหมายปลายทาง
  - 7.3 การเปลี่ยนแปลงข้อมูลสารสนเทศโดยมิได้รับอนุญาต

- 7.4 การเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต
  - 7.5 การเข้าถึงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต
  - 7.6 การนำข้อมูลสารสนเทศกลับมาใช้ใหม่โดยไม่ได้รับอนุญาต
8. เจ้าของข้อมูล และผู้ดูแลระบบ ต้องมีการป้องกันข้อมูลสารสนเทศที่มีการเผยแพร่ต่อสาธารณชน มิให้มีการแก้ไขเปลี่ยนแปลงโดยมิได้รับอนุญาต เพื่อรักษาความถูกต้องครบถ้วนของข้อมูลสารสนเทศ

## ส่วนที่ 15

### การควบคุมการเข้ารหัส

#### วัตถุประสงค์

- เพื่อให้มีการเข้ารหัสข้อมูลอย่างเหมาะสมและมีประสิทธิภาพในการปกป้องความลับ ป้องกัน การปลอมแปลงข้อมูล และควบคุมความถูกต้องของข้อมูล

#### ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- เจ้าของข้อมูล
- ผู้ใช้งาน

#### อ้างอิงมาตรฐาน

- หมวดที่ 6 การเข้ารหัสข้อมูล (Cryptography)

#### แนวปฏิบัติ

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

ประเภทกุญแจ / วิธีการเข้ารหัส	เกณฑ์ขั้นต่ำ	ความยาวกุญแจ (อย่างน้อย)
กุญแจแบบสมมาตร (Symmetric)	AES	256 bits
กุญแจแบบอสมมาตร (Asymmetric)	RSA	1024 bits
การ Hashing	BCrypt	Cost Factor 10 ขึ้นไป

4. ผู้ดูแลระบบ ต้องมีการทบทวนขั้นตอนวิธี (Algorithm) และความยาวของกุญแจที่เข้ารหัสอย่างน้อยปีละ 1 ครั้ง เพื่อให้ยังสามารถรักษาไว้ซึ่งความมั่นคงปลอดภัย
5. ผู้ดูแลระบบ ต้องกำหนดให้มีการบริหารจัดการกุญแจที่ใช้ในการเข้ารหัส ดังนี้
  - 5.1 การสร้างกุญแจรหัสควรกระทำในสถานที่ที่มีมาตรการป้องกันความปลอดภัย
  - 5.2 เมื่อมีการสร้างกุญแจรหัสที่เป็นกุญแจลับ (Private key) ควรส่งมอบให้กับเจ้าของกุญแจโดยตรง โดยวิธีการที่ปลอดภัย
  - 5.3 ควรจัดให้มีการเก็บบันทึก Log เพื่อการตรวจสอบสำหรับกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับการจัดการกุญแจรหัส
6. ผู้ใช้งาน ควรรักษาความปลอดภัยในการใช้งานกุญแจ ดังนี้
  - 6.1 เก็บกุญแจรหัสในสถานที่ที่ปลอดภัย เช่น ตู้นิรภัย หรือสื่อบันทึกที่ปลอดภัย และไม่มีใครสามารถเข้าถึงได้

- 6.2 เมื่อมีการรับกุญแจสาธารณะ (Public key) มาใช้ ก่อนใช้งานจะต้องพิสูจน์ความถูกต้องของกุญแจสาธารณะ โดยสอบถามกับผู้ส่งหรือตรวจสอบกับผู้แทนในการรับรองความถูกต้องของกุญแจสาธารณะ (Certificate authority) ที่เชื่อถือได้เท่านั้น
- 6.3 ควบคุมการใช้งานและจัดเก็บกุญแจให้สอดคล้องกับการรักษาความลับข้อมูลตามที่ รฟม. กำหนด

## ส่วนที่ 16

### การนำอุปกรณ์ส่วนตัวมาใช้งาน (Bring your own device)

#### วัตถุประสงค์

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

#### ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

#### อ้างอิงมาตรฐาน

- หมวดที่ 2 อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากระยะไกล (Mobile devices and teleworking)

#### แนวปฏิบัติ

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

12. กรณีอุปกรณ์ส่วนตัวสูญหายหรือถูกขโมยผู้ใช้งานต้องแจ้งผู้ดูแลระบบโดยเร็วที่สุด เพื่อจัดการข้อมูลที่จัดเก็บอยู่ในอุปกรณ์ส่วนตัวของผู้ใช้งาน
13. ผู้ใช้งานต้องเข้าถึงระบบสารสนเทศของ รพม. ผ่านช่องทางที่ รพม. กำหนด เช่น VPN

ภาคผนวก จ.

สัญญาการเก็บรักษาข้อมูลไว้เป็นความลับ (Non-Disclosure Agreement)

 At Joint U.   
h. 9.5.



## สัญญาการเก็บรักษาข้อมูลไว้เป็นความลับ

สัญญาฉบับนี้ทำขึ้น ณ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย เลขที่ 175 ถนนพระราม 9  
แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร เมื่อวันที่ ..... ระหว่าง

การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย สำนักงานตั้งอยู่เลขที่ 175 ถนนพระราม 9  
แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร โดย .....  
.....ซึ่งต่อไปในสัญญานี้เรียกว่า “รฟม.” ฝ่ายหนึ่ง กับ

นาย/นาง/นางสาว/ ..... เลขที่บัตรประชาชน .....  
ซึ่งต่อไปในสัญญานี้เรียกว่า “ผู้รับข้อมูล” อีกฝ่ายหนึ่ง

ตามที่ ..... (คู่สัญญา เช่น กลุ่มบริษัท/บริษัท/มหาวิทยาลัย/ฯลฯ)  
..... ได้ตกลงทำสัญญา ..... เลขที่ .....  
เมื่อวันที่ ..... กับ รฟม. ซึ่งต่อไปในสัญญานี้เรียกว่า “สัญญาโครงการ” โดย .....  
(คู่สัญญา) ..... จะได้รับข้อมูลจาก รฟม. เพื่อใช้ในการปฏิบัติงาน ซึ่งในการ  
ดำเนินงานดังกล่าว ..... (คู่สัญญา) ..... ได้มอบหมายให้ผู้รับ  
ข้อมูลประสานขอข้อมูลจาก รฟม. เพื่อนำไปประกอบการปฏิบัติงานที่เกี่ยวข้องสำหรับการดำเนินโครงการ  
..... นั้น

ทั้งสองฝ่ายจึงตกลงทำสัญญากัน ดังมีข้อความต่อไปนี้

1. ในสัญญาฉบับนี้ “ข้อมูล” หมายถึง สิ่งที่มีชื่อความหมายให้รู้เรื่องราวข้อเท็จจริง ข้อมูล  
หรือสิ่งใด ๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพสิ่งของนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่า  
จะได้จัดทำไว้ในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผ่นผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การ  
บันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดในระบบ  
คอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์  
ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

2. ผู้รับข้อมูลให้สัญญาแก่ รฟม. ว่าข้อมูลที่รับจาก รฟม. หรือในนามของ รฟม. ผู้รับข้อมูล  
จะใช้เพื่อประกอบการปฏิบัติงานที่เกี่ยวข้องสำหรับดำเนินโครงการ .....  
ตามสัญญาโครงการเท่านั้น และจะไม่นำไปใช้เพื่อวัตถุประสงค์อื่น เช่น ใช้เพื่อวัตถุประสงค์ในเชิงพาณิชย์  
การพัฒนาเป็นผลิตภัณฑ์หรือเทคโนโลยีอื่น การใช้หรือพยายามใช้ข้อมูลเพื่อการอื่น การอ้างอิงหรือรวมเข้า  
ไปเป็นส่วนหนึ่งของการประดิษฐ์ใด ๆ การรับขอความคุ้มครองจากทรัพย์สินทางปัญญาใด ๆ ของผู้รับข้อมูล  
เว้นแต่ได้รับการอนุญาตจาก รฟม. เป็นลายลักษณ์อักษรก่อน

3. ผู้รับข้อมูลจะต้องปกปิดข้อมูลทั้งหมดที่ได้มีการเปิดเผยภายใต้สัญญาโครงการนี้ไว้เป็น  
ความลับอย่างเคร่งครัด

4. ถ้าข้อกำหนดใด ๆ ตามสัญญาฉบับนี้ตกเป็นโมฆะ ให้ข้อสัญญาที่เหลืออยู่ในสัญญาฉบับนี้  
คงใช้บังคับและมีผลอยู่อย่างสมบูรณ์

/5. หากผู้รับ ...



5. หากผู้รับข้อมูลไม่ปฏิบัติตามกฎหมาย หรือฝ่าฝืนสัญญาไม่ว่าข้อใดข้อหนึ่ง ผู้รับข้อมูล ยินยอมชดใช้ค่าเสียหายใด ๆ ที่เกิดขึ้นหรือที่เกี่ยวข้องเนื่องแก่ รพม. ทั้งสิ้น

สัญญาฉบับนี้ทำขึ้นเป็นสองฉบับมีข้อความถูกต้องตรงกัน คู่สัญญาได้อ่านและเข้าใจข้อความ ในสัญญานี้แล้ว เห็นว่าถูกต้องตรงตามเจตนาของตน จึงได้ลงนามและประทับตรา (ถ้ามี) ไว้ต่อหน้าพยานและ ยึดถือไว้ฝ่ายละหนึ่งฉบับ

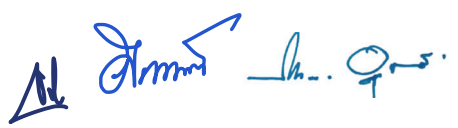
การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

ลงชื่อ .....  
(.....)  
ตำแหน่ง ผู้อำนวยการฝ่าย/สำนัก.....  
วันที่ ...../...../.....

ลงชื่อ ..... ผู้รับข้อมูล  
(.....)  
วันที่ ...../...../.....

ลงชื่อ ..... พยาน  
(.....)  
ตำแหน่ง .....  
วันที่ ...../...../.....

ลงชื่อ ..... พยาน  
(.....)  
วันที่ ...../...../.....

  
Joint U.



๕.๒ มอบหลักประกันการปฏิบัติตามสัญญา ตามที่ระบุไว้ในข้อ ๗ ของเอกสารเช่าด้วยวิธี  
ประกวดราคาอิเล็กทรอนิกส์ให้แก่.....<sup>๑</sup> ขณะที่ได้ลงนามในสัญญาเป็นจำนวนร้อยละ  
.....ของราคาตามสัญญาที่ได้ระบุไว้ในใบเสนอราคานี้เพื่อเป็นหลักประกันการปฏิบัติตาม  
สัญญาโดยถูกต้องและครบถ้วน

หากข้าพเจ้าไม่ปฏิบัติให้ครบถ้วนตามที่ระบุไว้ในข้อ ๕.๑ และ/หรือข้อ ๕.๒ ดังกล่าวข้างต้น  
ข้าพเจ้ายอมให้ .....<sup>๑</sup> รับผิดชอบการเสนอราคาหรือเรียกร้องจากผู้ออกหนังสือ  
ค้ำประกัน ข้าพเจ้ายอมชดใช้ค่าเสียหายใดๆ ที่อาจมีแก่.....<sup>๑</sup> และ .....<sup>๑</sup>  
มีสิทธิจะให้ผู้อื่นขอเสนอรายอื่นเป็นผู้ชนะการประกวดราคาอิเล็กทรอนิกส์ได้หรือ.....<sup>๑</sup>  
อาจดำเนินการเช่าการประกวดราคาอิเล็กทรอนิกส์ใหม่ก็ได้

๖. ข้าพเจ้ายอมรับว่า .....<sup>๑</sup>ไม่มีความผูกพันที่จะรับคำเสนอนี้ หรือใบเสนอราคาใดๆ  
รวมทั้งไม่ต้องรับผิดชอบในค่าใช้จ่ายใดๆ อันอาจเกิดขึ้นในการที่ข้าพเจ้าได้เข้ายื่นข้อเสนอกครั้งนี้

๗. บรรดาหลักฐานประกอบการพิจารณา เช่น ตัวอย่าง (sample) แคตตาล็อก รายละเอียด  
คุณลักษณะเฉพาะ (Specifications) พร้อมใบเสนอราคา ซึ่งข้าพเจ้าได้ลงไว้ในระบบการจัดซื้อจัดจ้างภาครัฐ  
ด้วยอิเล็กทรอนิกส์ ข้าพเจ้ายินยอมมอบให้ .....<sup>๑</sup> ไว้เป็นเอกสารและทรัพย์สิน  
ของ.....<sup>๑</sup>

สำหรับตัวอย่างที่เหลือหรือไม่ใช้แล้ว ซึ่ง.....<sup>๑</sup>ส่งคืนให้ ข้าพเจ้า  
จะไม่เรียกร้องค่าเสียหายใดๆ ที่เกิดขึ้นกับตัวอย่างนั้น

๘. เพื่อเป็นหลักประกันในการปฏิบัติโดยถูกต้อง ตามที่ได้ทำความเข้าใจและตามความผูกพัน  
แห่งคำเสนอนี้ ข้าพเจ้าขอมอบ..... เพื่อเป็นหลักประกันการเสนอราคาเป็นเงินจำนวน  
.....บาท (.....) มงพร้อมนี้

๙. ข้าพเจ้าได้ตรวจทานตัวเลขที่ได้ยื่นพร้อมใบเสนอราคานี้โดยละเอียดแล้ว และเข้าใจดีว่า  
.....<sup>๑</sup>ไม่ต้องรับผิดชอบใดๆ ในความผิดพลาดหรือตกหล่น

๑๐. ใบเสนอราคานี้ ได้ยื่นเสนอโดยบริสุทธิ์ยุติธรรม และปราศจากกลฉ้อฉลหรือการสมรู้ร่วมคิดกัน  
โดยไม่ชอบด้วยกฎหมายกับบุคคลใดบุคคลหนึ่ง หรือหลายบุคคล หรือกับห้างหุ้นส่วน บริษัทใดๆ ที่ได้ยื่น  
ข้อเสนอในคราวเดียวกัน

เสนอมา ณ วันที่..... เดือน..... พ.ศ. ....

ลงชื่อ .....

(.....)

ตำแหน่ง.....

หมายเหตุ

<sup>๑</sup> ให้ระบุชื่อย่อหน่วยงานของรัฐที่ดำเนินการจัดซื้อ เช่น กรม หรือจังหวัด หรือทีโอที เป็นต้น

แบบสัญญา  
สัญญาเช่าคอมพิวเตอร์

สัญญาเลขที่ .....(๑).....

สัญญาฉบับนี้ทำขึ้น ณ .....

ตำบล/แขวง.....อำเภอ/เขต.....

จังหวัด.....เมื่อวันที่.....เดือน.....พ.ศ.....

ระหว่าง.....(๒).....

โดย.....(๓).....

ซึ่งต่อไปในสัญญานี้เรียกว่า “ผู้เช่า” ฝ่ายหนึ่ง กับ.....(๔ ก).....

ซึ่งจดทะเบียนเป็นนิติบุคคล ณ .....

มีสำนักงานใหญ่อยู่เลขที่.....ถนน.....ตำบล/แขวง.....

อำเภอ/เขต.....จังหวัด.....โดย.....

ผู้มีอำนาจลงนามผูกพันนิติบุคคลปรากฏตามหนังสือรับรองของสำนักงานทะเบียนหุ้นส่วนบริษัท.....

ลงวันที่.....(๕) (และหนังสือมอบอำนาจลงวันที่.....) แนบท้ายสัญญานี้

(๖) (ในกรณีที่ผู้ให้เช่าเป็นบุคคลธรรมดาให้ใช้ข้อความว่า กับ.....(๕ ข).....

อยู่บ้านเลขที่.....ถนน.....ตำบล/แขวง.....

อำเภอ/เขต.....จังหวัด.....ผู้ถือบัตรประจำตัวประชาชน

เลขที่.....ตั้งปรากฏตามสำเนาบัตรประจำตัวประชาชนแนบท้ายสัญญานี้) ซึ่งต่อไปในสัญญานี้เรียกว่า

“ผู้ให้เช่า” อีกฝ่ายหนึ่ง

คู่สัญญาได้ตกลงกันมีข้อความดังต่อไปนี้

**ข้อ ๑ คำนิยาม**

“ค่าเช่า” หมายความรวมถึง ค่าบำรุงรักษาด้วย

“ค่าบำรุงรักษา” หมายความรวมถึง ค่าใช้จ่ายทั้งสิ้นในการบำรุงรักษาและซ่อมแซมแก้ไข

“การบำรุงรักษา” หมายความรวมถึง การตรวจสอบตามกำหนดเวลาตลอดจนการซ่อมแซมแก้ไขและเปลี่ยนแปลงส่วนประกอบที่เกี่ยวข้องกับคอมพิวเตอร์ที่เช่าเพื่อให้ใช้งานได้อย่างทันสมัยเป็นปกติและมีประสิทธิภาพตลอดระยะเวลาของการเช่า

“การซ่อมแซมแก้ไข” หมายความรวมถึง การซ่อมแซมแก้ไขไม่ว่าจะเป็นการซ่อมแซมแก้ไขเล็กน้อยหรือไม่

“การเช่าลักษณะที่ ๑” หมายถึง การเช่าที่ผู้เช่าสามารถใช้คอมพิวเตอร์โดยไม่จำกัดชั่วโมงการใช้งานในแต่ละเดือน ซึ่งรวมถึงค่าบำรุงรักษาในคาบเวลาที่ต้องการบำรุงรักษาที่กำหนดในเอกสารแนบท้ายสัญญาผนวก ๒

“การเช่าลักษณะที่ ๒” หมายถึง การเช่าที่มีการกำหนดอัตราค่าเช่าขั้นต่ำต่อเดือน ซึ่งรวมถึงค่าบำรุงรักษาในเวลาปกติ แบ่งออกเป็น ๒ กรณี คือ

กรณีที่ ๑ ได้แก่ กรณีที่ใช้คอมพิวเตอร์ไม่เกิน ๑๗๖ (หนึ่งร้อยเจ็ดสิบหก) ชั่วโมงในแต่ละเดือนผู้เช่าจะเสียค่าเช่าประจำเดือนของคอมพิวเตอร์หน่วยนั้นเท่ากับอัตราค่าเช่าต่อเดือนที่กำหนดในเอกสารแนบท้ายสัญญาผนวก ๒

กรณีที่ ๒ ได้แก่ กรณีที่ใช้คอมพิวเตอร์เกิน ๑๗๖ (หนึ่งร้อยเจ็ดสิบหก) ชั่วโมงในแต่ละเดือนผู้เช่าจะเสียค่าเช่าประจำเดือนของคอมพิวเตอร์หน่วยนั้นเท่ากับผลบวกระหว่างค่าเช่าต่อเดือนที่กำหนดในเอกสารแนบท้ายสัญญาผนวก ๒ กับค่าเช่าส่วนเพิ่มซึ่งคำนวณจากค่าเช่าต่อชั่วโมงของคอมพิวเตอร์

หน่วยนั้นตามที่กำหนดในเอกสารแนบท้ายสัญญาผนวก ๒ คูณกับจำนวนชั่วโมงที่เกินกว่า ๑๗๖ (หนึ่งร้อยเจ็ดสิบหก) ชั่วโมงในเดือนนั้น

“การเช่าลักษณะที่ ๓” หมายถึง การเช่าที่ผู้เช่าสามารถใช้คอมพิวเตอร์ โดยเสียค่าเช่าประจำเดือนตามจำนวนชั่วโมงที่ใช้จริงของรายการนั้น ในอัตราค่าเช่าต่อชั่วโมงที่กำหนดในเอกสารแนบท้ายสัญญาผนวก ๒ ซึ่งรวมถึงค่าบำรุงรักษา ในเวลาปกติแล้ว

“ในเวลาปกติ” หมายถึง ในช่วงเวลาระหว่าง ๐๘.๐๐ น. – ๑๗.๐๐ น. ของวันทำการของผู้เช่า  
“ค่าบำรุงรักษานอกเวลาปกติ” หมายถึง ค่าบำรุงรักษาเฉพาะส่วนที่เพิ่มเติมจากค่าบำรุงรักษา

ในเวลาปกติ

### ข้อ ๒ ข้อตกลงเช่า

ผู้เช่าตกลงเช่าและให้ผู้เช่าตกลงให้เช่าเครื่องคอมพิวเตอร์ (Hardware) ซอฟต์แวร์ (Software) อุปกรณ์ประมวลผลระบบคอมพิวเตอร์ โปรแกรมประยุกต์การให้บริการ อุปกรณ์ประกอบระบบ .....(๗)..... รวมทั้งส่วนประกอบอื่นๆ ที่สามารถรับโปรแกรม ข้อมูล ประมวลผลสื่อสาร เคลื่อนย้ายข้อมูล และแสดงผลลัพธ์ได้ ซึ่งเป็นผลิตภัณฑ์ของ.....(๘)..... ซึ่งต่อไปในสัญญานี้เรียกว่า “คอมพิวเตอร์” ตามเอกสารแนบท้ายสัญญาผนวก ๑

ในกรณีที่ผู้ให้เช่าประสงค์จะนำคอมพิวเตอร์รายการใดต่างไปจากรายละเอียดที่กำหนดไว้ในเอกสารแนบท้ายสัญญาผนวก ๑ มาติดตั้งให้ผู้เช่า ผู้ให้เช่าจะต้องได้รับความเห็นชอบเป็นหนังสือจากผู้เช่าก่อน และคอมพิวเตอร์รายการนั้นจะต้องมีคุณสมบัติไม่ต่ำกว่าที่กำหนดไว้ในเอกสารแนบท้ายสัญญาผนวก ๑

### ข้อ ๓ เอกสารอันเป็นส่วนหนึ่งของสัญญา

เอกสารแนบท้ายสัญญาต่อไปนี้ ให้ถือเป็นส่วนหนึ่งของสัญญานี้

๓.๑	ผนวก ๑	รายการคอมพิวเตอร์ที่เช่า	จำนวน.....(.....) หน้า
๓.๒	ผนวก ๒	รายการคอมพิวเตอร์ที่มีการเช่าลักษณะต่างๆ	จำนวน.....(.....) หน้า
๓.๓	ผนวก ๓	รายละเอียดการทดสอบการใช้งานของคอมพิวเตอร์	จำนวน.....(.....) หน้า
๓.๔	ผนวก ๔	การกำหนดตัวถังของคอมพิวเตอร์	จำนวน.....(.....) หน้า
๓.๕	ผนวก ๕	การอบรมวิชาการด้านคอมพิวเตอร์	จำนวน.....(.....) หน้า
๓.๖	ผนวก ๖	รายการเอกสารคู่มือการใช้คอมพิวเตอร์	จำนวน.....(.....) หน้า
๓.๗	ผนวก ๗	ข้อกำหนดการใช้โปรแกรม	จำนวน.....(.....) หน้า
๓.๘	ผนวก ๘	รายละเอียดการอนุญาตจากเจ้าของลิขสิทธิ์	จำนวน.....(.....) หน้า
		..... ฯลฯ.....	

ความใดในเอกสารแนบท้ายสัญญาที่ขัดหรือแย้งกับข้อความในสัญญานี้ ให้ใช้ข้อความในสัญญานี้บังคับ และในกรณีที่เอกสารแนบท้ายสัญญาขัดแย้งกันเอง ผู้ให้เช่าจะต้องปฏิบัติตามคำวินิจฉัยของผู้เช่า คำวินิจฉัยของผู้เช่าให้ถือเป็นที่สุด และผู้ให้เช่าไม่มีสิทธิเรียกร้องค่าเช่า ค่าเสียหาย หรือค่าใช้จ่ายใดๆ เพิ่มเติมจากผู้เช่าทั้งสิ้น

### ข้อ ๔ ระยะเวลาการเช่า

สัญญานี้มีผลบังคับตั้งแต่วันที่ลงนามในสัญญา แต่ระยะเวลาการคำนวณค่าเช่าคอมพิวเตอร์ตามสัญญานี้ให้มีกำหนด.....(.....) ปี นับถัดจากวันที่ผู้เช่ารับมอบคอมพิวเตอร์ถูกต้องครบถ้วนแล้ว

### ข้อ ๕ การชำระค่าเช่า

การเช่าคอมพิวเตอร์ตามสัญญาเป็นการเช่าแบบมีกำหนดระยะเวลา โดยผู้เช่าจะชำระค่าเช่าเป็นรายเดือนตามเดือนปฏิทิน ประกอบด้วย การเช่าลักษณะตามที่กำหนดในเอกสารแนบท้ายสัญญาผนวก ๒

กรณีการเช่าลักษณะที่ ๑ หรือลักษณะที่ ๒ หากการเช่าในเดือนแรกไม่ครบเดือนปฏิทินนั้น ให้คำนวณค่าเช่าเริ่มตั้งแต่วันที่ผู้เช่ารับมอบคอมพิวเตอร์จากผู้ให้เช่าตามข้อ ๘ จนถึงวันสุดท้ายแห่งเดือนปฏิทินนั้น ส่วนการเช่าเดือนสุดท้ายให้คำนวณค่าเช่าตั้งแต่วันที่แรกของเดือนปฏิทินนั้นจนถึงวันสิ้นสุดสัญญา

การคำนวณค่าเช่าตามวรรคสอง สำหรับการเช่าลักษณะที่ ๑ ให้คำนวณค่าเช่าต่อวันจากอัตราค่าเช่าต่อเดือนในเอกสารแนบท้ายสัญญาผนวก ๒ หาดด้วย ๓๐ ส่วนการเช่าลักษณะที่ ๒ ให้คำนวณค่าเช่าต่อวันจากอัตราค่าเช่าต่อเดือนในเอกสารแนบท้ายสัญญาผนวก ๒ หาดด้วย ๒๒

(๙) การจ่ายเงินตามเงื่อนไขแห่งสัญญา ผู้เช่าจะโอนเงินเข้าบัญชีเงินฝากธนาคารของผู้ให้เช่า ชื่อธนาคาร.....สาขา.....ชื่อบัญชี..... เลขที่บัญชี..... ทั้งนี้ ผู้ให้เช่าตกลงเป็นผู้รับภาระเงินค่าธรรมเนียม หรือค่าบริการอื่นใด เกี่ยวกับการโอน รวมทั้งค่าใช้จ่ายอื่นใด (ถ้ามี) ที่ธนาคารเรียกเก็บ และยินยอมให้มีการหักเงินดังกล่าวจากจำนวนเงินโอนในงวดนั้น ๆ (ความในวรรคนี้ใช้สำหรับกรณีที่หน่วยงานของรัฐจะจ่ายเงินตรงให้แก่ผู้ให้เช่า (ระบบ Direct Payment) โดยการโอนเงินเข้าบัญชีเงินฝากธนาคารของผู้ให้เช่าตามแนวทางที่กระทรวงการคลังหรือหน่วยงานของรัฐเจ้าของงบประมาณเป็นผู้กำหนด แล้วแต่กรณี)

### ข้อ ๖ การรับรองคุณภาพ

ผู้ให้เช่ารับรองว่าคอมพิวเตอร์ที่ให้เช่าตามสัญญา มีคุณสมบัติไม่ต่ำกว่าที่กำหนดไว้ในเอกสารแนบท้ายสัญญาผนวก ๑

### ข้อ ๗ การส่งมอบและติดตั้ง

ผู้ให้เช่าจะทำการส่งมอบและติดตั้งคอมพิวเตอร์ที่เช่าตามสัญญาให้ถูกต้องและครบถ้วนตามที่กำหนดไว้ในข้อ ๒ ในลักษณะพร้อมที่จะใช้งานอย่างมีประสิทธิภาพได้ทันทีตามรายละเอียดการทดสอบเอกสารแนบท้ายสัญญาในเอกสารแนบท้ายสัญญาผนวก ๓ ให้แก่ผู้เช่า ณ ..... และส่งมอบให้แก่ผู้เช่าภายใน.....(๑๐).....(.....) วัน นับถัดจากวันที่คู่สัญญาได้ลงนามในสัญญา ซึ่งผู้ให้เช่าต้องเป็นผู้จัดหาอุปกรณ์ประกอบพร้อมทั้งเครื่องมือที่จำเป็นในการติดตั้ง โดยผู้ให้เช่าเป็นผู้ออกค่าใช้จ่ายเองทั้งสิ้น

ผู้ให้เช่าจะต้องแจ้งกำหนดเวลาติดตั้งแล้วเสร็จพร้อมที่จะใช้งานและส่งมอบคอมพิวเตอร์ได้ โดยทำเป็นหนังสือต่อผู้เช่า ณ ..... ในวันและเวลาราชการ ก่อนวันกำหนดส่งมอบตามวรรคหนึ่ง ไม่น้อยกว่า.....(๑๑).....(.....) วันทำการ

ผู้ให้เช่าต้องออกแบบสถานที่ติดตั้งคอมพิวเตอร์ รวมทั้งระบบอื่นๆ ที่เกี่ยวข้องตามมาตรฐานของผู้ให้เช่าซึ่งได้รับความเห็นชอบจากผู้เช่าเป็นหนังสือแล้ว และผู้ให้เช่าต้องจัดหาเจ้าหน้าที่มาให้คำแนะนำและตรวจสอบความถูกต้องเหมาะสมของสถานที่ให้ทันต่อการติดตั้งคอมพิวเตอร์ภายใน.....(.....) วัน นับถัดจากวันที่ลงนามในสัญญา ทั้งนี้ โดยไม่คิดค่าใช้จ่ายใดๆ ทั้งสิ้นจากผู้เช่า

### ข้อ ๘ การตรวจรับ

เมื่อผู้เช่าได้ตรวจรับคอมพิวเตอร์ที่ส่งมอบและติดตั้งแล้วเห็นว่าถูกต้องครบถ้วนตามสัญญาแล้ว ผู้เช่าจะออกหลักฐานการรับมอบไว้เป็นหนังสือ เพื่อผู้ให้นำนามาใช้เป็นหลักฐานประกอบการขอรับเงินค่าเช่าคอมพิวเตอร์

ถ้าผลของการตรวจรับปรากฏว่าคอมพิวเตอร์ที่ผู้ให้เช่าส่งมอบไม่ตรงตามข้อ ๒ ผู้เช่าทรงไว้ซึ่งสิทธิที่จะไม่รับคอมพิวเตอร์นั้น ในกรณีเช่นนั้น ผู้ให้เช่าต้องรับนำคอมพิวเตอร์นั้นกลับคืนโดยเร็วที่สุดเท่าที่จะทำได้ และนำคอมพิวเตอร์มาส่งมอบให้ใหม่ หรือต้องทำการแก้ไขให้ถูกต้องตามสัญญาด้วยค่าใช้จ่ายของผู้ให้เช่าเอง และระยะเวลาที่เสียไปเพราะเหตุดังกล่าวผู้ให้เช่าจะนำมาอ้างเป็นเหตุขอขยายเวลาส่งมอบตามสัญญาหรือของดหรือลดค่าปรับไม่ได้

(๑๒) ในกรณีที่ผู้ให้เช่าส่งมอบคอมพิวเตอร์ถูกต้องแต่ไม่ครบจำนวน หรือส่งมอบครบจำนวนแต่ไม่ถูกต้องทั้งหมด ผู้เช่าจะตรวจรับเฉพาะส่วนที่ถูกต้อง โดยออกหลักฐานการตรวจรับเฉพาะส่วนนั้นก็ได้ (ความในวรรคนี้ จะไม่กำหนดไว้ในกรณีที่ผู้เช่าต้องการคอมพิวเตอร์ทั้งหมดในคราวเดียวกัน หรือการเช่าคอมพิวเตอร์ที่ประกอบเป็นชุดหรือหน่วย ถ้าขาดส่วนประกอบอย่างหนึ่งอย่างใดไปแล้ว จะไม่สามารถใช้งานได้โดยสมบูรณ์)

### ข้อ ๙ การบำรุงรักษา

ผู้ให้เช่ามีหน้าที่บำรุงรักษาคอมพิวเตอร์ให้อยู่ในสภาพใช้งานได้ดีอยู่เสมอ รวมทั้งปรับปรุงพัฒนาระบบคอมพิวเตอร์ให้ทันสมัยเป็นปัจจุบันและมีประสิทธิภาพตามความต้องการใช้งานของผู้เช่า ด้วยค่าใช้จ่ายของผู้ให้เช่า โดยต้องจัดหาและสำรองอุปกรณ์ให้เพียงพอต่อการใช้งานและการบำรุงรักษา ทั้งนี้ ผู้ให้เช่าต้องจัดหาช่างผู้มีความรู้ความชำนาญและมีฝีมือดีมาตรวจสอบบำรุงรักษาและซ่อมแซมแก้ไขคอมพิวเตอร์ที่ให้เช่า ตลอดอายุสัญญาเช่าอย่างน้อยเดือนละ.....(๑๓).....(.....) ครั้ง โดยให้มีระยะเวลาห่างกันไม่น้อยกว่า.....(.....) วัน

การใช้คอมพิวเตอร์ตามสัญญานี้ให้ถือว่าอยู่ในสภาพทันสมัยเป็นปัจจุบันใช้งานได้ดีตามปกติตามวรรคหนึ่ง โดยให้มีเวลาคอมพิวเตอร์ขัดข้องรวมตามเกณฑ์การคำนวณเวลาขัดข้องตามวรรคสามไม่เกินเดือนละ.....(.....) ชั่วโมง หรือร้อยละ.....(๑๔).....(.....) ของเวลาใช้งานทั้งหมดของคอมพิวเตอร์ของเดือนนั้น แล้วแต่ตัวเลขใดจะมากกว่ากัน มิฉะนั้น ผู้ให้เช่าต้องยอมให้ผู้เช่าคิดค่าปรับสำหรับเวลาที่ไม่สามารถใช้คอมพิวเตอร์ได้ในส่วนที่เกินกำหนดข้างต้นในอัตราชั่วโมงละ.....(.....) บาท โดยผู้ให้เช่ายินยอมให้ผู้เช่าหักค่าปรับดังกล่าวออกจากค่าเช่าประจำเดือน

เกณฑ์การคำนวณเวลาขัดข้องของคอมพิวเตอร์ตามวรรคสองให้เป็นดังนี้

- กรณีที่คอมพิวเตอร์ขัดข้องพร้อมกันหลายหน่วยให้นับเวลาขัดข้องของหน่วยที่มีตัวถ่วงมากที่สุด เพียงหน่วยเดียว

- กรณีความเสียหายอันสืบเนื่องมาจากความขัดข้องของคอมพิวเตอร์แตกต่างกัน เวลาที่ใช้ในการคำนวณค่าปรับจะเท่ากับเวลาขัดข้องของคอมพิวเตอร์หน่วยนั้นคูณด้วยตัวถ่วงซึ่งมีค่าต่างๆ ตามเอกสารแนบท้ายสัญญาผนวก ๔

เวลาคอมพิวเตอร์ขัดข้องในช่วงเวลานอกคาบเวลาบำรุงรักษาตามรายละเอียดในเอกสารแนบท้ายสัญญาผนวก ๒ และผู้เช่ามิได้แจ้งให้ผู้ให้เช่าทราบล่วงหน้าตามข้อ ๑๐ มิให้นำมานับรวมเพื่อคำนวณค่าปรับ

### ข้อ ๑๐ การซ่อมแซมแก้ไข

๑๐.๑ ในกรณีคอมพิวเตอร์ชำรุดบกพร่อง เสียหาย หรือขัดข้องใช้งานไม่ได้ทั้งหมดหรือแต่บางส่วน โดยมีใช้ความผิดของผู้เช่า ผู้ให้เช่าจะต้องจัดให้ช่างที่มีความรู้ ความชำนาญและมีฝีมือดีมาจัดการซ่อมแซมแก้ไขให้อยู่ในสภาพใช้งานได้ดีตามปกติด้วยค่าใช้จ่ายของผู้ให้เช่า โดยเริ่มดำเนินการ ดังนี้

(๑) กรณีคอมพิวเตอร์ชำรุดบกพร่องในเวลาปกติ ผู้ให้เช่าจะต้องเริ่มดำเนินการภายใน.....(.....) ชั่วโมง นับตั้งแต่เวลาที่ได้รับแจ้งจากผู้เช่าหรือผู้ที่ได้รับมอบหมายจากผู้เช่า

(๒) กรณีคอมพิวเตอร์ชำรุดบกพร่องนอกเวลาปกติ ผู้ให้เช่าจะต้องเริ่มดำเนินการภายใน.....(.....) ชั่วโมง นับตั้งแต่เวลาที่ได้รับแจ้งจากผู้เช่าหรือผู้ที่ได้รับมอบหมายจากผู้เช่า แต่ทั้งนี้ผู้เช่าหรือผู้ที่ได้รับมอบหมายจากผู้เช่า ได้แจ้งความประสงค์ในการใช้คอมพิวเตอร์นอกเวลาปกติให้ผู้ให้เช่าทราบล่วงหน้าในเวลาปกติแล้ว

การที่ผู้เช่าหรือผู้ที่ได้รับมอบหมายจากผู้เช่าแจ้งให้ผู้ให้เช่าหรือผู้ที่ได้รับมอบหมายจากผู้ให้เช่าทราบทางวาจา ทางโทรสาร หรือทางไปรษณีย์อิเล็กทรอนิกส์ (e-mail) หรือทางโทรศัพท์ ไม่ว่าจะวิธีใดวิธีหนึ่งให้ถือเป็นการแจ้งโดยชอบตามสัญญาแล้ว

ถ้าผู้ให้เช่าไม่สามารถปฏิบัติตามวรรคหนึ่ง ผู้ให้เช่ายอมให้ผู้เช่าปรับเป็นรายชั่วโมง ในอัตรา ชั่วโมงละ.....(๑๕).....บาท (.....) โดยยินยอมให้ผู้เช่าหักค่าปรับดังกล่าวออกจากค่าเช่าประจำเดือน สำหรับจำนวนชั่วโมงที่ใช้ในการคำนวณค่าปรับจะเริ่มนับตั้งแต่เวลาที่ผู้เช่าหรือผู้ที่ได้รับมอบหมายจากผู้เช่าได้แจ้งให้ผู้ให้เช่าทราบถึงความชำรุดบกพร่องจนถึงเวลาที่ผู้ให้เช่าเริ่มดำเนินการซ่อมแซมแก้ไข

๑๐.๒ ในกรณีที่คอมพิวเตอร์ที่เช่าในลักษณะที่ ๒ หรือลักษณะที่ ๓ ชำรุดบกพร่องและผู้เช่าหรือผู้ที่ได้รับมอบหมายจากผู้เช่าได้แจ้งให้ผู้ให้เช่าทราบในเวลาปกติถึงการชำรุดบกพร่องแล้ว ผู้ให้เช่าจะต้องซ่อมแซมแก้ไขคอมพิวเตอร์ที่ชำรุดบกพร่องนั้นให้แล้วเสร็จจนใช้งานได้ตามสภาพปกติ โดยไม่คิดค่าใช้จ่ายใดๆ ทั้งสิ้นจากผู้เช่า ไม่ว่าจะการซ่อมแซมแก้ไขจะกระทำในเวลาปกติหรือนอกเวลาปกติก็ตาม สำหรับกรณีที่ผู้เช่าแจ้งให้ผู้ให้เช่าทราบนอกเวลาปกติถึงการชำรุดบกพร่องของคอมพิวเตอร์และต้องการให้ผู้ให้เช่าซ่อมแซมแก้ไขในช่วงเวลาดังกล่าว ผู้เช่าจะต้องชำระค่าซ่อมแซมแก้ไขสำหรับช่วงเวลานั้นให้แก่ผู้ให้เช่าโดยคำนวณจากอัตราค่าบำรุงรักษานอกเวลาปกติที่ระบุในเอกสารแนบท้ายสัญญาผนวก ๒ คูณกับจำนวนชั่วโมงที่ใช้จริงในการบำรุงรักษานอกเวลาปกติ

๑๐.๓ ในกรณีที่คอมพิวเตอร์ขัดข้องใช้งานไม่ได้ตามปกติ และผู้เช่าเห็นว่าไม่อาจซ่อมแซมแก้ไขได้ ผู้เช่าจะแจ้งให้ผู้ให้เช่าทราบเป็นหนังสือให้จัดหาคอมพิวเตอร์ที่มีคุณภาพและความสามารถในการใช้งานไม่ต่ำกว่าของเดิม มาให้ผู้เช่าใช้แทนภายในเวลา.....(๑๖).....(.....) วัน นับถัดจากวันที่ได้รับหนังสือแจ้งจากผู้เช่าโดยไม่คิดค่าใช้จ่าย หากผู้ให้เช่าไม่สามารถจัดหาคอมพิวเตอร์ดังกล่าวมาให้ผู้เช่าใช้งานแทนได้ภายในเวลาที่กำหนด ผู้ให้เช่ายินยอมให้ผู้เช่าปรับเป็นรายวัน ในอัตราร้อยละ.....(๑๗).....(.....) ของราคาคอมพิวเตอร์ที่เช่าตามข้อ ๒ นับถัดจากวันครบกำหนดดังกล่าวจนกว่าผู้ให้เช่าจะดำเนินการแล้วเสร็จหรือจนกว่าผู้เช่าเห็นว่าผู้ให้เช่าไม่อาจจัดหาคอมพิวเตอร์อื่นแทนได้และบอกเลิกสัญญา ทั้งนี้ ผู้เช่าไม่จำเป็นต้องจ่ายค่าเช่าในระหว่างเวลาที่ผู้เช่าไม่สามารถใช้คอมพิวเตอร์ตามสัญญานี้ได้ นับตั้งแต่วันที่คอมพิวเตอร์ขัดข้องใช้งานไม่ได้ตามปกติจนถึงวันที่ผู้ให้เช่าดำเนินการดังกล่าวแล้วเสร็จหรือจนกว่าผู้เช่าบอกเลิกสัญญา แล้วแต่กรณี

#### ข้อ ๑๑ การใช้ประโยชน์

การใช้ประโยชน์ในคอมพิวเตอร์ตามสัญญานี้ ผู้ให้เช่ายินยอมให้อยู่ภายใต้การจัดการและการควบคุมดูแลของผู้เช่าโดยสิ้นเชิง นอกจากผู้เช่าจะใช้ในการปฏิบัติงานของผู้เช่าแล้ว ผู้เช่าอาจให้ผู้อื่นมาใช้คอมพิวเตอร์นี้ได้ โดยอยู่ภายใต้การควบคุมดูแลของผู้เช่า

#### ข้อ ๑๒ การจัดอบรม

ผู้ให้เช่าต้องจัดอบรมวิชาการด้านคอมพิวเตอร์ให้แก่เจ้าหน้าที่ของผู้เช่าให้มีความรู้ความเข้าใจและสามารถใช้ระบบคอมพิวเตอร์ได้เป็นอย่างดี โดยต้องดำเนินการฝึกอบรมให้แล้วเสร็จภายใน.....(.....) วัน นับถัดจากวันที่ผู้เช่าได้รับมอบคอมพิวเตอร์ โดยไม่คิดค่าใช้จ่ายใดๆ รายละเอียดของการฝึกอบรมให้เป็นไปตามเอกสารแนบท้ายสัญญาผนวก ๕



**ข้อ ๑๓ คู่มือการใช้คอมพิวเตอร์**

ผู้ให้เช่าต้องจัดหาและส่งมอบคู่มือการใช้คอมพิวเตอร์ที่ให้เช่าตามสัญญา นี้ ตามที่กำหนดไว้ในเอกสารแนบท้ายสัญญาผนวก ๖ จำนวน.....(.....) ชุด ให้กับผู้เช่าในวันที่ส่งมอบคอมพิวเตอร์ และต้องปรับปรุงคู่มือดังกล่าวให้ทันสมัยเป็นปัจจุบันตลอดอายุสัญญา นี้โดยไม่คิดมูลค่าใดๆ เพิ่มเติมจากผู้เช่าอีก

**ข้อ ๑๔ หลักประกันการปฏิบัติตามสัญญา**

ในขณะที่ทำสัญญา นี้ ผู้ให้เช่าได้นำหลักประกันเป็น.....(๑๘)..... เป็นจำนวนเงิน.....บาท (.....) ซึ่งเท่ากับร้อยละ.....(๑๙).....(.....) ของค่าเช่าคอมพิวเตอร์ทั้งหมดตามสัญญา มามอบไว้แก่ผู้เช่าเพื่อเป็นหลักประกันการปฏิบัติตามสัญญา นี้

(๒๐) กรณีผู้ให้เช่าใช้หนังสือค้ำประกันมาเป็นหลักประกันการปฏิบัติตามสัญญา หนังสือค้ำประกันดังกล่าวจะต้องออกโดยธนาคารที่ประกอบกิจการในประเทศไทย หรือโดยบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกัน ตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ ตามแบบที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนด หรืออาจเป็นหนังสือค้ำประกันอิเล็กทรอนิกส์ตามวิธีการที่กรมบัญชีกลางกำหนดก็ได้ และจะต้องมีอายุการค้ำประกันตลอดไปจนกว่าผู้ให้เช่าพ้นข้อผูกพันตามสัญญา นี้

หลักประกันที่นำมามอบให้ตามวรรคหนึ่ง จะต้องมีอายุครอบคลุมความรับผิดชอบของผู้ให้เช่าตลอดอายุสัญญา ถ้าหลักประกันที่ผู้ให้เช่านำมามอบให้ดังกล่าวลดลงหรือเสื่อมค่าลง หรือมีอายุไม่ครอบคลุมถึงความรับผิดชอบของผู้ให้เช่าตลอดอายุสัญญา ไม่ว่าด้วยเหตุใดๆ ก็ตาม รวมถึงกรณีผู้ให้เช่าส่งมอบและติดตั้งคอมพิวเตอร์ล่าช้าเป็นเหตุให้ระยะเวลาการเช่าตามสัญญาเปลี่ยนแปลงไป ผู้ให้เช่าต้องหาหลักประกันใหม่หรือหลักประกันเพิ่มเติมให้มีจำนวนครบถ้วนตามวรรคหนึ่งมามอบให้แก่ผู้เช่าภายใน.....(.....) วัน นับถัดจากวันที่ได้รับแจ้งเป็นหนังสือจากผู้เช่า

หลักประกันที่ผู้ให้เช่านำมามอบไว้ตามข้อนี้ ผู้เช่าจะคืนให้แก่ผู้ให้เช่าโดยไม่มีดอกเบี้ย เมื่อผู้ให้เช่าพ้นจากข้อผูกพันและความรับผิดชอบที่พึงปฏิบัติตามสัญญา นี้แล้ว

**ข้อ ๑๕ ข้อตกลงการใช้โปรแกรม**

ผู้ให้เช่ายินยอมปฏิบัติตามข้อตกลงการใช้โปรแกรมตามที่กำหนดไว้ในเอกสารแนบท้ายสัญญาผนวก ๗

(๒๑) ผู้ให้เช่าต้องดำเนินการให้ผู้เช่าและผู้ที่ได้รับมอบหมายจากผู้เช่าได้รับอนุญาต ตามกฎหมายจากเจ้าของลิขสิทธิ์ในการใช้และสร้างสรรค์โดยการดัดแปลง การรวบรวม หรือการประกอบกันเข้า จากโปรแกรมคอมพิวเตอร์ที่เช่าตามรายละเอียดในเอกสารแนบท้ายสัญญาผนวก ๘

(๒๒) บรรดาข้อมูลและสารสนเทศไม่ว่าในรูปแบบใดที่เก็บอยู่ในหรือที่สร้างขึ้นโดยระบบคอมพิวเตอร์ รวมทั้งงานโปรแกรมคอมพิวเตอร์ที่สร้างสรรค์ขึ้นโดยผู้ให้เช่า หรือลูกจ้าง พนักงาน และผู้ที่ได้รับมอบหมายจากผู้ให้เช่า ให้ถือว่าเป็นลิขสิทธิ์ของผู้เช่าทั้งสิ้น

(๒๓) ประโยชน์อันจะเกิดขึ้นในอนาคตจากการพัฒนา การแก้ไขเปลี่ยนแปลง การใช้งานซ้ำโปรแกรมคอมพิวเตอร์ อันเป็นงานสร้างสรรค์อันมีลิขสิทธิ์ใหม่ตามวรรคก่อน ซึ่งบางส่วนจะใช้ประโยชน์จากโปรแกรมคอมพิวเตอร์ที่เช่าอันเป็นงานสร้างสรรค์ที่ลิขสิทธิ์เดิมเป็นของผู้ให้เช่า ทั้งลิขสิทธิ์ที่มีอยู่หรือที่อาจจะเกิดขึ้นในภายหน้า ซึ่งรวมถึงในกรณีที่มีซอฟต์แวร์ที่ติดตั้งมาพร้อมกับส่วนอุปกรณ์ครั้งนี้ด้วย ผู้ให้เช่าไม่มีสิทธิเรียกร้องค่าใช้จ่ายใดๆ จากผู้เช่าทั้งสิ้น

ห้ามมิให้ผู้ให้เช่า ลูกจ้าง ตัวแทนหรือพนักงานของผู้ให้เช่าเอาไป เปิดเผยหรือใช้ข้อมูล และหรือสารสนเทศในระบบดังกล่าว หรือกระทำด้วยประการใดๆ ให้บุคคลอื่นเอาไป เปิดเผย หรือใช้ข้อมูล และหรือสารสนเทศในระบบดังกล่าว หรือเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์หรือล่องรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่จัดทำขึ้นเป็นการเฉพาะหรือกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อดักจับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้เช่าหรือผู้ที่เกี่ยวข้องกับผู้เช่าที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ โดยไม่ชอบด้วยกฎหมายหรือโดยไม่ได้รับความยินยอมเป็นหนังสือจากผู้เช่า หากมีการฝ่าฝืนผู้ให้เช่าต้องรับผิดชอบ ค่าเสียหายให้แก่ผู้เช่าจนเต็มจำนวน และให้นำความในข้อ ๑๘ และข้อ ๒๒ มาใช้บังคับโดยอนุโลม

#### ข้อ ๑๖ การรับประกันความเสียหาย

ในกรณีที่บุคคลภายนอกกล่าวอ้างหรือใช้สิทธิเรียกร้องใดๆ ว่ามีการละเมิดลิขสิทธิ์ สิทธิบัตร หรือสิทธิในทรัพย์สินทางปัญญาใดๆ อันเกี่ยวกับคอมพิวเตอร์ตามสัญญาฯ นี้ โดยผู้เช่ามิได้แก้ไขตัดแปลงไปจากเดิม ผู้ให้เช่าจะต้องดำเนินการทั้งปวงเพื่อให้การกล่าวอ้างหรือการเรียกร้องดังกล่าวระงับสิ้นไปโดยเร็ว หากผู้เช่าต้องรับผิดชอบต่อค่าเสียหายต่อบุคคลภายนอก เนื่องจากผลแห่งการละเมิดลิขสิทธิ์ สิทธิบัตร หรือสิทธิในทรัพย์สินทางปัญญาดังกล่าว ผู้ให้เช่าต้องเป็นผู้ชำระค่าเสียหายและค่าใช้จ่ายรวมทั้งค่าฤชาธรรมเนียมและค่าทนายความ แทนผู้เช่า ทั้งนี้ ผู้เช่าต้องแจ้งให้ผู้ให้เช่าทราบเป็นหนังสือในเมื่อได้มีการกล่าวอ้างหรือใช้สิทธิเรียกร้องดังกล่าว โดยไม่ชักช้า

#### ข้อ ๑๗ ความรับผิดชอบต่อความเสียหาย

ผู้เช่าไม่ต้องรับผิดชอบต่อการสูญหายหรือเสียหายใดๆ ที่เกิดขึ้นแก่คอมพิวเตอร์อันไม่ใช่ ความผิดของผู้เช่าตลอดระยะเวลาที่คอมพิวเตอร์อยู่ในความครอบครองของผู้เช่า

ถ้าเกิดความเสียหายขึ้นแก่คอมพิวเตอร์หรือส่วนใดส่วนหนึ่งของคอมพิวเตอร์ที่อยู่ในความครอบครองของผู้เช่าตามวรรคหนึ่ง ผู้ให้เช่าต้องดำเนินการทุกประการตามที่จำเป็นเพื่อให้คอมพิวเตอร์ กลับคืนสภาพที่ใช้งานได้ดีดังเดิมโดยเร็วที่สุด และในกรณีที่ไมอาจดำเนินการให้คอมพิวเตอร์คืนสู่สภาพที่ใช้งาน ได้ดีดังเดิมได้ หรือในกรณีที่คอมพิวเตอร์สูญหาย ผู้ให้เช่าต้องนำคอมพิวเตอร์เครื่องใหม่ที่มีคุณภาพ ประสิทธิภาพ และความสามารถใช้งานไม่ต่ำกว่าคอมพิวเตอร์เดิมมาติดตั้งให้แก่ผู้เช่าแทนภายใน.....(.....) วัน นับถัดจากวันที่ผู้ให้เช่าได้รับแจ้งจากผู้เช่า คอมพิวเตอร์ที่นำมาติดตั้งแทนนี้ให้ถือเป็นคอมพิวเตอร์ตามนัยข้อ ๒ แห่งสัญญานี้ด้วย ทั้งนี้ ในการปฏิบัติตามสัญญาข้อนี้ผู้ให้เช่าเป็นผู้ออกค่าใช้จ่ายเองทั้งสิ้น

#### ข้อ ๑๘ การบอกเลิกสัญญา

เมื่อครบกำหนดติดตั้งและส่งมอบคอมพิวเตอร์ตามสัญญาแล้ว ถ้าผู้ให้เช่าไม่ส่งมอบ และติดตั้งคอมพิวเตอร์บางรายการหรือทั้งหมดให้แก่ผู้เช่าภายในกำหนดเวลาตามสัญญา หรือส่งมอบคอมพิวเตอร์ ไม่ตรงตามสัญญา หรือมีคุณสมบัติไม่ถูกต้องตามสัญญา หรือส่งมอบและติดตั้งแล้วเสร็จภายในกำหนด แต่ไม่สามารถใช้งานได้โดยมีประสิทธิภาพ หรือใช้งานได้ไม่ครบถ้วนตามสัญญา หรือผู้ให้เช่าไม่ปฏิบัติตามสัญญา ข้อใดข้อหนึ่ง ผู้เช่ามีสิทธิบอกเลิกสัญญาทั้งหมดหรือแต่บางส่วนได้ การใช้สิทธิบอกเลิกสัญญานั้นไม่กระทบสิทธิ ของผู้เช่าที่จะเรียกร้องค่าเสียหายจากผู้ให้เช่า

ในกรณีที่ผู้เช่าใช้สิทธิบอกเลิกสัญญา ผู้เช่ามีสิทธิรับหรือบังคับจากหลักประกัน ตามข้อ ๑๔ เป็นจำนวนเงินทั้งหมดหรือแต่บางส่วนก็ได้ แล้วแต่ผู้เช่าจะเห็นสมควร และถ้าผู้เช่าต้องเช่า คอมพิวเตอร์จากบุคคลอื่นทั้งหมด หรือแต่บางส่วนภายในกำหนด.....(๒๔).....(.....) เดือน นับถัดจาก วันบอกเลิกสัญญา ผู้ให้เช่ายอมรับผิดค่าใช้จ่ายที่เพิ่มขึ้นจากค่าเช่าที่กำหนดไว้ในสัญญานี้รวมทั้งค่าใช้จ่ายใดๆ ที่ผู้เช่าต้องใช้จ่ายในการจัดหาผู้ให้เช่าคอมพิวเตอร์รายใหม่ดังกล่าวด้วย

### ข้อ ๑๙ ค่าปรับ

ในกรณีที่ผู้เช่าไม่ใช้สิทธิบอกเลิกสัญญาตามข้อ ๑๘ ผู้ให้เช่าจะต้องชำระค่าปรับให้ผู้เช่าเป็นรายวันสำหรับคอมพิวเตอร์ที่ยังไม่ได้ส่งมอบให้ถูกต้องครบถ้วนตามสัญญา ในอัตราวันละ.....(๒๕).....บาท (.....) ต่อเครื่อง นับถัดจากวันครบกำหนดส่งมอบตามสัญญาจนถึงวันที่ผู้ให้เช่าได้นำคอมพิวเตอร์มาส่งมอบและติดตั้งให้แก่ผู้เช่าจนถูกต้องครบถ้วน

การคิดค่าปรับในกรณีคอมพิวเตอร์ที่ตกลงเช่าเป็นระบบ ถ้าผู้ให้เช่าส่งมอบเพียงบางส่วนหรือขาดส่วนประกอบส่วนหนึ่งส่วนใดไป หรือส่งมอบและติดตั้งทั้งหมดแล้ว แต่มีคุณสมบัติไม่ครบถ้วนหรือใช้งานไม่ได้ อย่างมีประสิทธิภาพหรือไม่ถูกต้องครบถ้วนตามเอกสารแนบท้ายสัญญาผนวก ๓ ให้ถือว่ายังไม่ได้ส่งมอบคอมพิวเตอร์นั้นเลย และให้คิดค่าปรับเป็นรายวันจากราคาคอมพิวเตอร์ทั้งระบบ

ในระหว่างที่ผู้เช่ายังมีได้ใช้สิทธิบอกเลิกสัญญานั้น ถ้าผู้เช่าเห็นว่าผู้ให้เช่าไม่อาจปฏิบัติตามสัญญาต่อไปได้ ผู้เช่าจะใช้สิทธิบอกเลิกสัญญา และริบหรือบังคับจากหลักประกันตามข้อ ๑๔ กับเรียกร้องให้ชดใช้ค่าเช่าที่เพิ่มขึ้นตามที่กำหนดไว้ในข้อ ๑๘ วรรคสอง ก็ได้ และถ้าผู้เช่าได้แจ้งข้อเรียกร้องให้ชำระค่าปรับไปยังผู้ให้เช่าเมื่อครบกำหนดส่งมอบแล้ว ผู้เช่ามีสิทธิที่จะปรับผู้ให้เช่าจนถึงวันบอกเลิกสัญญาได้อีกด้วย

### ข้อ ๒๐ การนำคอมพิวเตอร์กลับคืนไป

เมื่อสัญญาสิ้นสุดลงไม่ว่าจะโดยการบอกเลิกสัญญา หรือครบอายุสัญญา ผู้ให้เช่าต้องนำคอมพิวเตอร์กลับคืนไปภายใน.....(.....) วัน นับถัดจากวันที่สัญญาสิ้นสุดลง โดยผู้ให้เช่าเป็นผู้เสียค่าใช้จ่ายเองทั้งสิ้น

(๒๖) ถ้าผู้ให้เช่าไม่นำคอมพิวเตอร์กลับคืนไปภายในกำหนดเวลาตามวรรคหนึ่ง ผู้เช่าจะกำหนดเวลาให้ผู้ให้เช่านำคอมพิวเตอร์กลับคืนไปอีกครั้งหนึ่ง หากพ้นกำหนดเวลาดังกล่าวแล้ว ผู้ให้เช่ายังไม่นำคอมพิวเตอร์กลับคืนไปอีก ผู้เช่ามีสิทธินำคอมพิวเตอร์ออกขายทอดตลาดได้ทันที โดยเงินที่ได้จากการขายทอดตลาด ผู้ให้เช่าตกลงยินยอมให้ผู้เช่าหักเป็นค่าปรับ ค่าเสียหาย และค่าใช้จ่ายต่างๆ ซึ่งรวมถึงค่าใช้จ่ายที่ผู้เช่าได้เสียไปในการดำเนินการขายทอดตลาดคอมพิวเตอร์ดังกล่าว และค่าใช้จ่ายในการทำสถานที่ที่เรือถอนคอมพิวเตอร์ออกไปให้มีสภาพตั้งที่เป็นอยู่เดิมก่อนทำสัญญานี้ เงินที่เหลือจากการหักค่าปรับ ค่าใช้จ่าย หรือค่าเสียหายแล้ว ผู้เช่าจะคืนให้แก่ผู้ให้เช่า แต่หากขายทอดตลาดไม่ได้หรือขายได้แต่ได้เงินไม่เพียงพอที่จะชดใช้เป็นค่าปรับ ค่าใช้จ่าย หรือค่าเสียหายดังกล่าว ผู้ให้เช่ายังคงต้องรับผิดชอบชดใช้ให้แก่ผู้เช่าจนครบถ้วน

เมื่อสัญญาสิ้นสุดลงไม่ว่าด้วยเหตุใดๆ ผู้เช่าไม่ต้องรับผิดชอบในความเสียหายใดๆ ทั้งสิ้น อันเกิดแก่คอมพิวเตอร์ซึ่งอยู่ในความครอบครองของผู้เช่า

### ข้อ ๒๑ การโอนกรรมสิทธิ์ให้บุคคลอื่น

ในระหว่างอายุสัญญาเช่า ผู้ให้เช่าจะไม่โอนกรรมสิทธิ์ในคอมพิวเตอร์ที่ให้เช่าแก่บุคคลอื่น หากผู้ให้เช่าฝ่าฝืน ผู้ให้เช่ายินยอมชดใช้ค่าเสียหายให้แก่ผู้เช่า

### ข้อ ๒๒ การบังคับค่าปรับ ค่าเสียหาย และค่าใช้จ่าย

ในกรณีที่ผู้ให้เช่าไม่ปฏิบัติตามสัญญาข้อใดข้อหนึ่งด้วยเหตุใดๆ ก็ตาม จนเป็นเหตุให้เกิดค่าปรับ ค่าเสียหาย หรือค่าใช้จ่ายแก่ผู้เช่า ผู้ให้เช่าต้องชดใช้ค่าปรับ ค่าเสียหาย หรือค่าใช้จ่ายดังกล่าวให้แก่ผู้เช่า โดยสิ้นเชิงภายในกำหนด.....(.....) วัน นับถัดจากวันที่ได้รับแจ้งเป็นหนังสือจากผู้เช่า หากผู้ให้เช่าไม่ชดใช้ให้ถูกต้องครบถ้วนภายในระยะเวลาดังกล่าวให้ผู้เช่ามีสิทธิที่จะหักเอาจากค่าเช่าที่ต้องชำระ หรือบังคับจากหลักประกันการปฏิบัติตามสัญญาได้ทันที

หากค่าปรับ ค่าเสียหาย หรือค่าใช้จ่ายที่บังคับจากค่าเช่าที่ต้องชำระ หรือหลักประกัน การปฏิบัติตามสัญญาแล้วยังไม่เพียงพอ ผู้ให้เช่ายินยอมชำระส่วนที่เหลือที่ยังขาดอยู่จนครบถ้วนตามจำนวน ค่าปรับ ค่าเสียหาย หรือค่าใช้จ่ายนั้น ภายในกำหนด.....(.....) วัน นับถัดจากวันที่ได้รับแจ้ง เป็นหนังสือจากผู้เช่า

**ข้อ ๒๓ การงดหรือลดค่าปรับ หรือขยายเวลาในการปฏิบัติตามสัญญา**

ในกรณีที่มีเหตุสุดวิสัย หรือเหตุใดๆ อันเนื่องมาจากความผิดหรือความบกพร่องของฝ่ายผู้เช่า หรือจากพฤติการณ์อันหนึ่งอันใดที่ผู้ให้เช่าไม่ต้องรับผิดชอบตามกฎหมาย หรือเหตุอื่นตามที่กำหนดในกฎกระทรวง ซึ่งออกตามความในกฎหมายว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ ทำให้ผู้ให้เช่าไม่สามารถส่งมอบ คอมพิวเตอร์ตามเงื่อนไขและกำหนดเวลาในข้อ ๗ แห่งสัญญานี้ได้ หรือไม่สามารถซ่อมแซมคอมพิวเตอร์หรือจัดหา คอมพิวเตอร์ให้ผู้เช่าใช้แทนตามเงื่อนไขและกำหนดเวลาในข้อ ๑๐ ได้ ผู้ให้เช่ามีสิทธิของงดหรือลดค่าปรับหรือขยาย เวลาตามสัญญาได้โดยจะต้องแจ้งเหตุหรือพฤติการณ์ดังกล่าว พร้อมหลักฐานเป็นหนังสือให้ผู้เช่าทราบภายใน ๑๕ (สิบห้า) วัน นับถัดจากวันที่เหตุอันสิ้นสุดลง หรือตามที่กำหนดในกฎกระทรวงดังกล่าว

ถ้าผู้ให้เช่าไม่ปฏิบัติให้เป็นไปตามความในวรรคหนึ่ง ให้ถือว่าผู้ให้เช่าได้ละสิทธิเรียกร้อง ในการที่จะงดหรือลดค่าปรับหรือขยายเวลาตามสัญญา โดยไม่มีเงื่อนไขใดๆ ทั้งสิ้น เว้นแต่กรณีเหตุเกิดจาก ความผิดหรือความบกพร่องของฝ่ายผู้เช่าซึ่งมีหลักฐานชัดเจน หรือผู้เช่าทราบที่อยู่แล้วตั้งแต่ต้น

การงดหรือลดค่าปรับหรือขยายเวลาตามสัญญาตามวรรคหนึ่ง อยู่ในดุลพินิจของผู้เช่าที่จะ พิจารณาตามที่เห็นสมควร

**ข้อ ๒๔ การโอนสิทธิและหน้าที่ตามสัญญา**

ผู้ให้เช่าจะไม่โอนสิทธิและหน้าที่ที่มีต่อผู้เช่าตามสัญญานี้ให้แก่บุคคลอื่นโดยไม่ได้รับความ เห็นชอบเป็นหนังสือจากผู้เช่าก่อน

สัญญานี้ทำขึ้นสองฉบับ มีข้อความถูกต้องตรงกัน คู่สัญญาได้อ่านและเข้าใจข้อความโดยละเอียด ตลอดแล้ว จึงได้ลงลายมือชื่อพร้อมทั้งประทับตรา (ถ้ามี) ไว้เป็นสำคัญต่อหน้าพยานและคู่สัญญาต่างยึดถือไว้ ฝ่ายละหนึ่งฉบับ

(ลงชื่อ).....ผู้เช่า  
(.....)

(ลงชื่อ).....ผู้ให้เช่า  
(.....)

(ลงชื่อ).....พยาน  
(.....)

(ลงชื่อ).....พยาน  
(.....)

### วิธีปฏิบัติเกี่ยวกับสัญญาเช่าคอมพิวเตอร์

- (๑) ให้ระบุเลขที่สัญญาในปีกงบประมาณหนึ่งๆ ตามลำดับ
- (๒) ให้ระบุชื่อของหน่วยงานของรัฐที่เป็นนิติบุคคล เช่น กรม ก. หรือรัฐวิสาหกิจ ข. เป็นต้น
- (๓) ให้ระบุชื่อและตำแหน่งของหัวหน้าหน่วยงานของรัฐที่เป็นนิติบุคคลนั้น หรือผู้ที่ได้รับมอบอำนาจ เช่น นาย ก. อธิบดีกรม..... หรือ นาย ข. ผู้ได้รับมอบอำนาจจากอธิบดีกรม.....
- (๔) ให้ระบุชื่อผู้ให้เช่า
  - ก. กรณีนิติบุคคล เช่น ห้างหุ้นส่วนสามัญจดทะเบียน ห้างหุ้นส่วนจำกัด บริษัทจำกัด
  - ข. กรณีบุคคลธรรมดา ให้ระบุชื่อและที่อยู่
- (๕) เป็นข้อความหรือเงื่อนไขเพิ่มเติม ซึ่งหน่วยงานของรัฐผู้ทำสัญญาอาจเลือกใช้หรือตัดออกได้ตามข้อเท็จจริง
- (๖) เป็นข้อความหรือเงื่อนไขเพิ่มเติม ซึ่งหน่วยงานของรัฐผู้ทำสัญญาอาจเลือกใช้หรือตัดออกได้ตามข้อเท็จจริง
- (๗) ให้ระบุจำนวนลักษณะของการเช่าที่ต้องการเช่า ซึ่งจะต้องระบุไว้ในเอกสารเชิญชวน
- (๘) ให้ระบุยี่ห้อคอมพิวเตอร์ที่เช่า รุ่นคอมพิวเตอร์
- (๙) เป็นข้อความหรือเงื่อนไขเพิ่มเติม ซึ่งหน่วยงานของรัฐผู้ทำสัญญาอาจเลือกใช้หรือตัดออกได้ตามข้อเท็จจริง
- (๑๐) กำหนดวันส่งมอบ อาจระบุ วันที่.....พ.ศ. ....

การกำหนดเวลาส่งมอบจะแจ้งล่วงหน้ากี่วัน ให้อยู่ในดุลพินิจของผู้เช่าโดยตกลงกับผู้ให้เช่า โดยปกติควรจะกำหนดไว้ประมาณ ๓ วันทำการ เพื่อที่ผู้เช่าจะได้จัดเตรียมเจ้าหน้าที่ไว้ตรวจรับของนั้น

ในกรณีที่มีการส่งมอบหลายครั้ง ให้ระบุวันเวลาที่ส่งมอบแต่ละครั้งไว้ด้วย
- (๑๑) กำหนดวันส่งมอบ อาจระบุ วันที่.....พ.ศ. ....

การกำหนดเวลาส่งมอบจะแจ้งล่วงหน้ากี่วัน ให้อยู่ในดุลพินิจของผู้เช่าโดยตกลงกับผู้ให้เช่า โดยปกติควรจะกำหนดไว้ประมาณ ๓ วันทำการ เพื่อที่ผู้เช่าจะได้จัดเตรียมเจ้าหน้าที่ไว้ตรวจรับของนั้น

ในกรณีที่มีการส่งมอบหลายครั้ง ให้ระบุวันเวลาที่ส่งมอบแต่ละครั้งไว้ด้วย
- (๑๒) เป็นข้อความหรือเงื่อนไขเพิ่มเติม ซึ่งหน่วยงานของรัฐผู้ทำสัญญาอาจเลือกใช้หรือตัดออกได้ตามข้อเท็จจริง
- (๑๓) กำหนดระยะเวลาการตรวจสอบบำรุงรักษาเท่าที่จำเป็น โดยปกติกำหนดเดือนละ ๑ ครั้ง
- (๑๔) เวลาหรือร้อยละของเวลาใช้งานทั้งหมดของคอมพิวเตอร์ในเดือนนั้น (total elapsed time) ให้กำหนดโดยคำนึงถึงสถานที่ติดตั้ง ลักษณะหรือขนาดของคอมพิวเตอร์ โดยปกติให้ใช้เกณฑ์กำหนดเวลาที่ใช้งานไม่ได้ (downtime) ไม่น้อยกว่าร้อยละ ๕ และไม่เกินร้อยละ ๒๐ กรณีที่สถานที่ติดตั้งอยู่ในกรุงเทพมหานคร ควรกำหนดไม่เกินเดือนละ ๙ ชั่วโมง (คำนวณจากร้อยละ ๕ ของเกณฑ์การทำงานปกติ ๘ ชั่วโมงต่อวัน และ ๒๒ วันต่อเดือน) แต่ถ้ามีการใช้งานต่อเดือนมากกว่านี้ควรกำหนดไว้ไม่เกินร้อยละ ๕ ของเวลาใช้งานทั้งหมดของคอมพิวเตอร์ซึ่งเป็นตัวเลขที่มากกว่า
- เวลาหรือร้อยละที่ใช้งานข้างต้น ให้กำหนดไว้ในเอกสารเชิญชวนด้วย
- (๑๕) กำหนดในอัตราระหว่างร้อยละ ๐.๐๒๕ - ๐.๐๓๕ ของราคาตามสัญญาต่อชั่วโมง
- (๑๖) ระยะเวลารับประกันและระยะเวลาแก้ไขซ่อมแซมจะกำหนดเท่าใด แล้วแต่ลักษณะของสิ่งของที่เช่าคอมพิวเตอร์กัน โดยให้อยู่ในดุลพินิจของผู้เช่า ทั้งนี้ จะต้องประกาศให้ทราบในเอกสารเชิญชวนด้วย

(๑๗) อัตราค่าปรับตามสัญญาข้อ ๑๙ ให้กำหนดเป็นรายวันในอัตราตายตัวระหว่างร้อยละ ๐.๐๑ - ๐.๒๐ ของราคาพัสดุที่ยังไม่ได้ส่งมอบ ตามระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐ ข้อ ๑๖๒ ส่วนกรณีจะปรับร้อยละเท่าใด ให้อยู่ในดุลพินิจของหน่วยงานของรัฐผู้เช่าที่จะพิจารณา โดยคำนึงถึงราคาและลักษณะของพัสดุที่เช่า ซึ่งอาจมีผลกระทบต่อการใช้เช่าจะหลีกเลี่ยงไม่ปฏิบัติตามสัญญา แต่ทั้งนี้ การที่จะกำหนดค่าปรับเป็นร้อยละเท่าใดจะต้องกำหนดไว้ในเอกสารเชิญชวนด้วย

(๑๘) “หลักประกัน” หมายถึง หลักประกันที่ผู้รับจ้างนำมามอบไว้แก่หน่วยงานของรัฐเมื่อลงนามในสัญญาเพื่อประกันความเสียหายที่อาจเกิดขึ้นจากการปฏิบัติตามสัญญา ดังนี้

(๑) เงินสด

(๒) เช็คหรือตราพท์ที่ธนาคารเซ็นสั่งจ่าย ซึ่งเป็นเช็คหรือตราพท์ลงวันที่ที่ใช้เช็คหรือตราพท์นั้นชำระต่อเจ้าหน้าที่ หรือก่อนวันนั้นไม่เกิน ๓ วันทำการ

(๓) หนังสือค้ำประกันของธนาคารภายในประเทศตามตัวอย่างที่คณะกรรมการนโยบายกำหนด โดยอาจเป็นหนังสือค้ำประกันอิเล็กทรอนิกส์ตามวิธีการที่กรมบัญชีกลางกำหนดก็ได้

(๔) หนังสือค้ำประกันของบริษัทเงินทุนหรือบริษัทหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยอนุโลมให้ใช้ตามตัวอย่างหนังสือค้ำประกันของธนาคารที่คณะกรรมการนโยบายกำหนด

(๕) พันธบัตรรัฐบาลไทย

(๑๙) ให้กำหนดจำนวนเงินหลักประกันการปฏิบัติตามสัญญาตามระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐ ข้อ ๑๖๘

(๒๐) เป็นข้อความหรือเงื่อนไขเพิ่มเติม ซึ่งหน่วยงานของรัฐผู้ทำสัญญาอาจเลือกใช้หรือตัดออกได้ตามข้อเท็จจริง

(๒๑) เป็นข้อความหรือเงื่อนไขเพิ่มเติม ซึ่งหน่วยงานของรัฐผู้ทำสัญญาอาจเลือกใช้หรือตัดออกได้ตามข้อเท็จจริง

(๒๒) เป็นข้อความหรือเงื่อนไขเพิ่มเติม ซึ่งหน่วยงานของรัฐผู้ทำสัญญาอาจเลือกใช้หรือตัดออกได้ตามข้อเท็จจริง

(๒๓) เป็นข้อความหรือเงื่อนไขเพิ่มเติม ซึ่งหน่วยงานของรัฐผู้ทำสัญญาอาจเลือกใช้หรือตัดออกได้ตามข้อเท็จจริง

(๒๔) กำหนดเวลาที่ผู้เช่าจะเช่าคอมพิวเตอร์จากแหล่งอื่นเมื่อบอกเลิกสัญญาและมีสิทธิเรียกเงินในส่วนที่เพิ่มขึ้นจากราคาที่กำหนดไว้ในสัญญานั้น ให้อยู่ในดุลพินิจของผู้เช่าโดยตกลงกับผู้ให้เช่า

(๒๕) อัตราค่าปรับตามสัญญาข้อ ๑๙ ให้กำหนดเป็นรายวันในอัตราตายตัวระหว่างร้อยละ ๐.๐๑ - ๐.๒๐ ของราคาพัสดุที่ยังไม่ได้ส่งมอบ ตามระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐ ข้อ ๑๖๒ ส่วนกรณีจะปรับร้อยละเท่าใด ให้อยู่ในดุลพินิจของหน่วยงานของรัฐผู้เช่าที่จะพิจารณา โดยคำนึงถึงราคาและลักษณะของพัสดุที่เช่า ซึ่งอาจมีผลกระทบต่อการใช้เช่าจะหลีกเลี่ยงไม่ปฏิบัติตามสัญญา แต่ทั้งนี้ การที่จะกำหนดค่าปรับเป็นร้อยละเท่าใดจะต้องกำหนดไว้ในเอกสารเชิญชวนด้วย

(๒๖) อาจแก้ไขเปลี่ยนแปลงได้ตามความเหมาะสมถ้าหน่วยงานของรัฐผู้ทำสัญญา สามารถกำหนดมาตรการอื่นใดในสัญญา หรือกำหนดทางปฏิบัติเพื่อแก้ไขปัญหา ที่ผู้ให้เช่าไม่ยอมนำคอมพิวเตอร์กลับคืนไปได้

## แบบหนังสือค้ำประกัน

(หลักประกันการเสนอราคาการซื้อ)

เลขที่.....

วันที่.....

ข้าพเจ้า.....(ชื่อธนาคาร/บริษัทเงินทุน).....สำนักงานตั้งอยู่เลขที่..... ถนน..... ตำบล/แขวง..... อำเภอ/เขต..... จังหวัด..... โดย.....ผู้มีอำนาจลงนามผูกพันธนาคาร/บริษัทเงินทุน ขอทำหนังสือค้ำประกันฉบับนี้ให้ไว้ต่อ.....(ชื่อหน่วยงานของรัฐผู้ประกวดราคา)..... ดังมีข้อความต่อไปนี้

๑. ตามที่.....(ชื่อผู้เสนอราคา).....ได้ยื่นซองประกวดราคาสำหรับการจัดซื้อ..... ตามเอกสารประกวดราคาเลขที่..... ซึ่งต้องวางหลักประกันของตามเงื่อนไขการประกวดราคา ต่อ.....(ชื่อหน่วยงานของรัฐผู้ประกวดราคา)..... เป็นจำนวนเงิน.....บาท (.....) นั้น

ข้าพเจ้ายินยอมผูกพันตนโดยไม่มีเงื่อนไขที่จะค้ำประกันการชำระเงินตามสิทธิเรียกร้องของ.....(ชื่อหน่วยงานของรัฐผู้ประกวดราคา)..... จำนวนไม่เกิน.....บาท (.....) ในฐานะเป็นลูกหนี้ร่วม ในกรณี.....(ชื่อผู้ยื่นข้อเสนอ).....ไม่ปฏิบัติตามเงื่อนไขในการประกวดราคา อันเป็นเหตุให้.....(ชื่อหน่วยงานของรัฐผู้ประกวดราคา).....มีสิทธิริบหลักประกันของประกวดราคา หรือชดใช้ค่าเสียหายใด ๆ รวมทั้งกรณีที่.....(ชื่อผู้ยื่นข้อเสนอ).....ได้ถอนใบเสนอราคาของตน ภายในระยะเวลาที่ใบเสนอราคายังมีผลอยู่ หรือมิได้ไปลงนามในสัญญาเมื่อได้รับแจ้งไปทำสัญญาหรือมิได้วางหลักประกันสัญญาภายในระยะเวลาที่กำหนดในเอกสารประกวดราคา โดย.....(ชื่อหน่วยงานของรัฐผู้ประกวดราคา).....ไม่จำเป็นต้องเรียกร้องให้.....(ชื่อผู้ยื่นข้อเสนอ).....ชำระหนี้ก่อน

๒. หนังสือค้ำประกันนี้มีผลใช้บังคับตั้งแต่วันที่..... เดือน..... พ.ศ. .... ถึงวันที่..... เดือน..... พ.ศ. .... และข้าพเจ้าจะไม่เพิกถอนการค้ำประกันนี้ภายในระยะเวลาที่กำหนดไว้

๓. ถ้า.....(ชื่อผู้ยื่นข้อเสนอ).....ขยายกำหนดเวลายื่นราคาของการเสนอราคาออกไป ข้าพเจ้ายินยอมที่จะขยายกำหนดระยะเวลาการค้ำประกันนี้ออกไปตลอดระยะเวลาที่ยื่นราคาที่ได้ขยายออกไปดังกล่าว

ข้าพเจ้าได้ลงนามและประทับตราไว้ต่อหน้าพยานเป็นสำคัญ

ลงชื่อ.....ผู้ค้ำประกัน

(.....)

ตำแหน่ง.....

ลงชื่อ.....พยาน

(.....)

ลงชื่อ.....พยาน

(.....)

## แบบหนังสือค้ำประกัน

(หลักประกันสัญญาซื้อ)

(กรณีปกติ)

เลขที่.....

วันที่.....

ข้าพเจ้า.....(ชื่อธนาคาร).....สำนักงานตั้งอยู่เลขที่..... ถนน..... ตำบล/แขวง..... อำเภอ/เขต..... จังหวัด..... โดย..... ผู้มีอำนาจลงนามผูกพันธนาคาร ขอทำหนังสือค้ำประกันฉบับนี้ไว้ต่อ.....(ชื่อหน่วยงานของรัฐ ผู้ประกวดราคา).....ซึ่งต่อไปนี้เรียกว่า “ผู้ซื้อ” ดังมีข้อความต่อไปนี้

๑. ตามที่.....(ชื่อผู้ขาย).....ซึ่งต่อไปนี้เรียกว่า “ผู้ขาย” ได้ทำสัญญาซื้อขาย.....กับผู้ซื้อ ตามสัญญาเลขที่.....ลงวันที่..... เดือน..... พ.ศ. .... ซึ่งผู้ขายต้องวางหลักประกัน การปฏิบัติตามสัญญาต่อผู้ซื้อ เป็นจำนวนเงิน.....บาท (.....) ซึ่งเท่ากับร้อยละ..... (.....) ของมูลค่า ทั้งหมดของสัญญา

ข้าพเจ้ายินยอมผูกพันตนโดยไม่มีเงื่อนไขที่จะค้ำประกันในการชำระเงินให้ตามสิทธิเรียกร้องของผู้ซื้อ จำนวนไม่เกิน.....บาท (.....) ในฐานะเป็นลูกหนี้ร่วม ในกรณีที่ผู้ขายก่อให้เกิด ความเสียหายใด ๆ หรือต้องชำระค่าปรับ หรือค่าใช้จ่ายใด ๆ หรือผู้ขายมิได้ปฏิบัติตามภาระหน้าที่ใด ๆ ที่กำหนด ในสัญญาดังกล่าวข้างต้น ทั้งนี้ โดยผู้ซื้อไม่จำเป็นต้องเรียกร้องให้ผู้ขายชำระหนี้ก่อน

๒. หนังสือค้ำประกันนี้มีผลใช้บังคับตั้งแต่ \*วันที่..... เดือน..... พ.ศ. .... ถึงวันที่..... เดือน..... พ.ศ. .... และข้าพเจ้าจะไม่เพิกถอนการค้ำประกันนี้ภายในระยะเวลาที่กำหนดไว้

๓. หากผู้ซื้อได้ขยายระยะเวลาให้แก่ผู้ขาย ให้ถือว่าข้าพเจ้ายินยอมในกรณีนั้น ๆ ด้วย โดยให้ขยาย ระยะเวลาการค้ำประกันนี้ออกไปตลอดระยะเวลาที่ผู้ซื้อได้ขยายระยะเวลาให้แก่ผู้ขายดังกล่าวข้างต้น

ข้าพเจ้าได้ลงนามและประทับตราไว้ต่อหน้าพยานเป็นสำคัญ

ลงชื่อ.....ผู้ค้ำประกัน

(.....)

ตำแหน่ง.....

ลงชื่อ.....พยาน

(.....)

ลงชื่อ.....พยาน

(.....)

\* หมายเหตุ : กรณีลงนามในสัญญาซื้อตามปกติ ให้หน่วยงานของรัฐระบุวันที่หนังสือค้ำประกันเริ่มมีผล ใช้บังคับให้มีผลตั้งแต่วันที่ทำสัญญาซื้อ



## แบบหนังสือค้ำประกัน

(หลักประกันสัญญาซื้อ)  
(กรณีสัญญาซื้อมีผลย้อนหลัง)

เลขที่.....

วันที่.....

ข้าพเจ้า.....(ชื่อธนาคาร).....สำนักงานตั้งอยู่เลขที่..... ถนน.....  
ตำบล/แขวง..... อำเภอ/เขต..... จังหวัด..... โดย.....  
ผู้มีอำนาจลงนามผูกพันธนาคาร ขอทำหนังสือค้ำประกันฉบับนี้ไว้ต่อ.....(ชื่อหน่วยงานของรัฐ  
ผู้ประกวดราคา).....ซึ่งต่อไปนี้เรียกว่า “ผู้ซื้อ” ดังมีข้อความต่อไปนี้

๑. ตามที่.....(ชื่อผู้ขาย).....ซึ่งต่อไปนี้เรียกว่า “ผู้ขาย” ได้ทำสัญญาซื้อขาย.....กับผู้ซื้อ  
ตามสัญญาเลขที่.....ลงวันที่..... เดือน..... พ.ศ. .... โดยให้มีผลย้อนหลังไปจนถึง  
วันที่.....เดือน.....พ.ศ. .... ซึ่งผู้ขายต้องวางหลักประกันการปฏิบัติตามสัญญาต่อผู้ซื้อ  
เป็นจำนวนเงิน.....บาท (.....) ซึ่งเท่ากับร้อยละ..... (.....) ของมูลค่าทั้งหมดของสัญญา

ข้าพเจ้ายินยอมผูกพันตนโดยไม่มีเงื่อนไขที่จะค้ำประกันในการชำระเงินให้ตามสิทธิเรียกร้องของผู้ซื้อ  
จำนวนไม่เกิน.....บาท (.....) ในฐานะเป็นลูกหนี้ร่วม ในกรณีที่ผู้ขายก่อให้เกิด  
ความเสียหายใด ๆ หรือต้องชำระค่าปรับ หรือค่าใช้จ่ายใด ๆ หรือผู้ขายมิได้ปฏิบัติตามภาระหน้าที่ใด ๆ ที่กำหนด  
ในสัญญาดังกล่าวข้างต้น ทั้งนี้ โดยผู้ซื้อไม่จำเป็นต้องเรียกร้องให้ผู้ขายชำระหนี้ดังกล่าวก่อน

๒. หนังสือค้ำประกันนี้มีผลใช้บังคับตั้งแต่ \*วันที่..... เดือน..... พ.ศ. .... ถึงวันที่.....  
เดือน..... พ.ศ. .... และข้าพเจ้าจะไม่เพิกถอนการค้ำประกันนี้ภายในระยะเวลาที่กำหนดไว้

๓. หากผู้ซื้อได้ขยายระยะเวลาให้แก่ผู้ขาย ให้ถือว่าข้าพเจ้ายินยอมในกรณีนั้น ๆ ด้วย โดยให้ขยาย  
ระยะเวลาการค้ำประกันนี้ออกไปตลอดระยะเวลาที่ผู้ซื้อได้ขยายระยะเวลาให้แก่ผู้ขายดังกล่าวข้างต้น

ข้าพเจ้าได้ลงนามและประทับตราไว้ต่อหน้าพยานเป็นสำคัญ

ลงชื่อ.....ผู้ค้ำประกัน

(.....)

ตำแหน่ง.....

ลงชื่อ.....พยาน

(.....)

ลงชื่อ.....พยาน

(.....)

\* หมายเหตุ : กรณีที่หน่วยงานของรัฐได้รับการอนุมัติยกเว้นหรือผ่อนผันจากคณะกรรมการวินิจฉัยปัญหา  
การจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐให้สัญญาซื้อมีผลใช้บังคับย้อนหลังไปจนถึงวันที่เริ่มต้น  
ปีงบประมาณ หรือวันที่มีการซื้อจริง ให้หน่วยงานของรัฐระบุวันที่หนังสือค้ำประกันเริ่มมีผล  
ใช้บังคับให้มีผลไปถึงวันดังกล่าว

## บทนิยาม

“**ผู้เสนอราคาที่มีผลประโยชน์ร่วมกัน**” หมายความว่า บุคคลธรรมดาหรือนิติบุคคลที่เข้าเสนอราคาขายในการประกวดราคาซื้อของกรม เป็นผู้มีส่วนได้เสียไม่ว่าโดยทางตรงหรือทางอ้อมในกิจการของบุคคลธรรมดาหรือนิติบุคคลอื่นที่เข้าเสนอราคาขายในการประกวดราคาซื้อของกรมในคราวเดียวกัน

การมีส่วนได้เสียไม่ว่าโดยทางตรงหรือทางอ้อมของบุคคลธรรมดาหรือนิติบุคคลดังกล่าวข้างต้น ได้แก่การที่บุคคลธรรมดาหรือนิติบุคคลดังกล่าวมีความสัมพันธ์กันในลักษณะดังต่อไปนี้

(๑) มีความสัมพันธ์กันในเชิงบริหาร โดยผู้จัดการ หุ่นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร หรือผู้มีอำนาจในการดำเนินงานในกิจการของบุคคลธรรมดาหรือของนิติบุคคลรายหนึ่ง มีอำนาจหรือสามารถใช้อำนาจในการบริหารจัดการกิจการของบุคคลธรรมดาหรือของนิติบุคคลอีกรายหนึ่งหรือหลายราย มีอำนาจหรือสามารถใช้อำนาจในการบริหารจัดการกิจการของบุคคลธรรมดาหรือของนิติบุคคลอีกรายหนึ่งหรือหลายราย ที่เสนอราคาให้แก่กรมในการประกวดราคาซื้อครั้งนี้

(๒) มีความสัมพันธ์กันในเชิงทุน โดยผู้เป็นหุ้นส่วนในห้างหุ้นส่วนสามัญ หรือผู้เป็นหุ้นส่วนไม่จำกัดความรับผิดในห้างหุ้นส่วนจำกัด หรือผู้ถือหุ้นรายใหญ่ในบริษัทจำกัดหรือบริษัทมหาชนจำกัด เป็นหุ้นส่วนในห้างหุ้นส่วนสามัญหรือห้างหุ้นส่วนจำกัด หรือเป็นผู้ถือหุ้นรายใหญ่ในบริษัทจำกัดหรือบริษัทมหาชนจำกัด อีกรายหนึ่งหรือหลายรายที่เสนอราคาให้แก่กรมในการประกวดราคาซื้อครั้งนี้

คำว่า “ผู้ถือหุ้นรายใหญ่” หมายความว่า ผู้ถือหุ้นซึ่งถือหุ้นเกินกว่าร้อยละสิบห้าในกิจการนั้น หรือในอัตราอื่นตามที่คณะกรรมการว่าด้วยการพัสดุเห็นสมควรประกาศกำหนดสำหรับกิจการบางประเภทหรือบางขนาด

(๓) มีความสัมพันธ์กันในลักษณะไขว้กันระหว่าง (๑) และ (๒) โดยผู้จัดการ หุ่นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร หรือผู้มีอำนาจในการดำเนินงานในกิจการของบุคคลธรรมดาหรือของนิติบุคคลรายหนึ่ง เป็นหุ้นส่วนในห้างหุ้นส่วนสามัญหรือห้างหุ้นส่วนจำกัด หรือเป็นผู้ถือหุ้นรายใหญ่ในบริษัทจำกัดหรือบริษัทมหาชนจำกัด อีกรายหนึ่งหรือหลายรายที่เข้าเสนอราคาให้แก่กรมในการประกวดราคาซื้อครั้งนี้ หรือในนัยกลับกัน

การดำรงตำแหน่ง การเป็นหุ้นส่วน หรือเข้าถือหุ้นดังกล่าวข้างต้นของคู่สมรส หรือบุตรที่ยังไม่บรรลุนิติภาวะของบุคคลใน (๑) (๒) หรือ (๓) ให้ถือว่าเป็นการดำรงตำแหน่ง การเป็นหุ้นส่วน หรือการถือหุ้นของบุคคลดังกล่าว

ในกรณีบุคคลใดใช้ชื่อบุคคลอื่นเป็นผู้จัดการ หุ่นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้เป็นหุ้นส่วนหรือผู้ถือหุ้นโดยที่ตนเองเป็นผู้ใช้อำนาจในการบริหารที่แท้จริง หรือเป็นผู้ถือหุ้นหรือผู้ถือหุ้นที่แท้จริงของห้างหุ้นส่วน หรือบริษัทจำกัด หรือบริษัทมหาชนจำกัด แล้วแต่กรณี และห้างหุ้นส่วน หรือบริษัทจำกัดหรือบริษัทมหาชนจำกัดที่เกี่ยวข้อง ได้เสนอราคาให้แก่กรมในการประกวดราคาซื้อคราวเดียวกัน ให้ถือว่าผู้เสนอราคาหรือผู้เสนองานนั้นมีความสัมพันธ์กันตาม (๑) (๒) หรือ (๓) แล้วแต่กรณี

## บทนิยาม

“การขัดขวางการแข่งขันราคาอย่างเป็นธรรม” หมายความว่า การที่ผู้ยื่นข้อเสนอรายหนึ่งหรือหลายราย กระทำการอย่างใด ๆ อันเป็นการขัดขวาง หรือเป็นอุปสรรค หรือไม่เปิดโอกาสให้มีการแข่งขันอย่างเป็นธรรม ในการเสนอราคาหรือยื่นข้อเสนอต่อหน่วยงานของรัฐ ไม่ว่าจะกระทำโดยการสมยอมกัน หรือโดยการให้ ขอให้ หรือรับว่าจะให้ เรียก รับ หรือยอมจะรับเงิน หรือทรัพย์สิน หรือประโยชน์อื่นใด หรือใช้กำลังประทุษร้าย หรือข่มขู่ว่าจะใช้กำลังประทุษร้าย หรือแสดงเอกสารอันเป็นเท็จ หรือส่อว่ากระทำการทุจริตอื่นใดในการเสนอราคา ทั้งนี้ โดยมีวัตถุประสงค์ที่จะแสวงหาประโยชน์ในระหว่างผู้ยื่นข้อเสนอด້วยกัน หรือเพื่อให้ประโยชน์แก่ผู้ยื่นข้อเสนอรายหนึ่งรายใดเป็นผู้มีสิทธิทำสัญญากับหน่วยงานของรัฐนั้น หรือเพื่อหลีกเลี่ยงการแข่งขันอย่างเป็นธรรม หรือเพื่อให้เกิดความได้เปรียบหน่วยงานของรัฐโดยมิใช่เป็นไปในทางประกอบธุรกิจปกติ

## บัญชีเอกสารส่วนที่ ๑

### ๑. ในกรณีผู้ยื่นข้อเสนอเป็นนิติบุคคล

#### (ก) ห้างหุ้นส่วนสามัญหรือห้างหุ้นส่วนจำกัด

- สำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล

ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น

- บัญชีรายชื่อหุ้นส่วนผู้จัดการ

ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น

- ผู้มีอำนาจควบคุม (ถ้ามี)

ไม่มีผู้มีอำนาจควบคุม

มีผู้มีอำนาจควบคุม

ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น

#### (ข) บริษัทจำกัดหรือบริษัทมหาชนจำกัด

- สำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล

ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น

- สำเนาหนังสือบริคณห์สนธิ

ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น

- บัญชีรายชื่อกรรมการผู้จัดการ

ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น

บัญชีผู้ถือหุ้นรายใหญ่ (ถ้ามี)

ไม่มีผู้ถือหุ้นรายใหญ่

มีผู้ถือหุ้นรายใหญ่

ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น

- ผู้มีอำนาจควบคุม (ถ้ามี)

ไม่มีผู้มีอำนาจควบคุม

มีผู้มีอำนาจควบคุม

ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น

### ๒. ในกรณีผู้ยื่นข้อเสนอไม่เป็นนิติบุคคล

#### (ก) บุคคลธรรมดา

- สำเนาบัตรประจำตัวประชาชนของผู้ยื่น

ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น

#### (ข) คณะบุคคล

- สำเนาข้อตกลงที่แสดงถึงการเข้าเป็นหุ้นส่วน

ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น

- สำเนาบัตรประจำตัวประชาชนของผู้เป็นหุ้นส่วน

ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น

๓. ในกรณีผู้ยื่นข้อเสนอเป็นผู้ยื่นข้อเสนอร่วมกันในฐานะเป็นผู้ร่วมค้า
- สำเนาสัญญาของการเข้าร่วมค้า  
ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น
  - (ก) ในกรณีผู้ร่วมค้าเป็นบุคคลธรรมดา
    - บุคคลสัญชาติไทย  
สำเนาบัตรประจำตัวประชาชน  
ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น
    - บุคคลที่มีใช้สัญชาติไทย  
สำเนาหนังสือเดินทาง  
ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น
  - (ข) ในกรณีผู้ร่วมค้าเป็นนิติบุคคล
    - ห้างหุ้นส่วนสามัญหรือห้างหุ้นส่วนจำกัด  
สำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล  
ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น
    - บัญชีรายชื่อหุ้นส่วนผู้จัดการ  
ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น
    - ผู้มีอำนาจควบคุม (ถ้ามี)
      - ไม่มีผู้ควบคุม
      - มีผู้ควบคุม  
ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น
    - บริษัทจำกัดหรือบริษัทมหาชนจำกัด  
สำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล  
ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น
    - สำนักงานหรือบริษัทอื่น  
ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น
    - บัญชีรายชื่อกรรมการผู้จัดการ  
ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น
    - บัญชีผู้ถือหุ้นรายใหญ่ (ถ้ามี)
      - ไม่มีผู้ถือหุ้นรายใหญ่
      - มีผู้ถือหุ้นรายใหญ่  
ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น
    - ผู้มีอำนาจควบคุม (ถ้ามี)
      - ไม่มีผู้มีอำนาจควบคุม
      - มีผู้มีอำนาจควบคุม  
ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น

๔. อื่น ๆ (ถ้ามี)

ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น

ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น

ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น

ข้าพเจ้าขอรับรองว่า เอกสารหลักฐานที่ข้าพเจ้ายื่นในการเสนอราคาทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ถูกต้องและเป็นความจริงทุกประการ

เพื่อเป็นหลักประกันในการปฏิบัติโดยถูกต้องตามที่ได้ทำความเข้าใจและตามความผูกพันแห่งคำเสนอนี้ ข้าพเจ้าขอมอบ.....เพื่อเป็นหลักประกันการเสนอราคาเป็นเงินจำนวน.....บาท (.....) มาพร้อมนี้

ข้าพเจ้าได้ตรวจสอบเอกสารต่าง ๆ ที่ได้ยื่นตามรายละเอียดการยื่นเอกสารการเสนอราคานี้โดยละเอียดแล้ว และเข้าใจดีว่า.....(หน่วยงาน).....ไม่ต้องรับผิดชอบใด ๆ ในความผิดพลาดหรือตกหล่น

ลงชื่อ.....ผู้ยื่นข้อเสนอ  
(.....)

.....

เอกสารฉบับนี้ต้องจัดทำเพื่อระบบจัดจ้างภาครัฐ

## บัญชีเอกสารส่วนที่ ๒

๑. แค็ตตาล็อกและหรือแบบรูปรายละเอียดคุณลักษณะเฉพาะ
- ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น
๒. หนังสือมอบอำนาจซึ่งปิดอากรแสตมป์ตามกฎหมายในกรณีที่ผู้ยื่นข้อเสนอมอบอำนาจให้บุคคลอื่นลงนามในใบเสนอราคาแทน
- ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น
๓. หลักประกันการเสนอราคา
- ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น
๔. สำเนาใบขึ้นทะเบียนผู้ประกอบการวิสาหกิจขนาดกลางและขนาดย่อม (SMEs) (ถ้ามี)
๕. สรุปรายละเอียดประกอบการอธิบายเอกสารตามที่หน่วยงานของรัฐกำหนดให้จัดส่งภายหลังวันเสนอราคา เพื่อใช้ในการประกอบการพิจารณา (ถ้ามี) ดังนี้
- ๕.๑ .....
- ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น
- ๕.๒ .....
- ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น
๖. อื่นๆ (ถ้ามี)
- ๖.๑.....
- ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น
- ๖.๒.....
- ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น
- ๖.๓.....
- ไฟล์ข้อมูล.....ขนาดไฟล์..... จำนวน .....แผ่น

ข้าพเจ้าขอรับรองว่าเอกสารหลักฐานที่ข้าพเจ้าได้ยื่นในการเสนอราคาทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ถูกต้องและเป็นความจริงทุกประการ

เพื่อเป็นหลักประกันในการปฏิบัติโดยถูกต้องตามที่ได้ทำความเข้าใจและตามความผูกพันแห่งคำเสนอนี้ ข้าพเจ้าขอมอบ.....เพื่อเป็นหลักประกันการเสนอราคาเป็นเงินจำนวน.....บาท (.....) มาพร้อมนี้

ข้าพเจ้าได้ตรวจสอบเอกสารต่าง ๆ ที่ได้ยื่นตามรายละเอียดการยื่นเอกสารการเสนอราคานี้โดยละเอียดแล้วและเข้าใจดีว่า.....(หน่วยงาน).....ไม่ต้องรับผิดชอบใด ๆ ในความผิดพลาดหรือตกหล่น

ลงชื่อ.....ผู้ยื่นข้อเสนอ  
(.....)

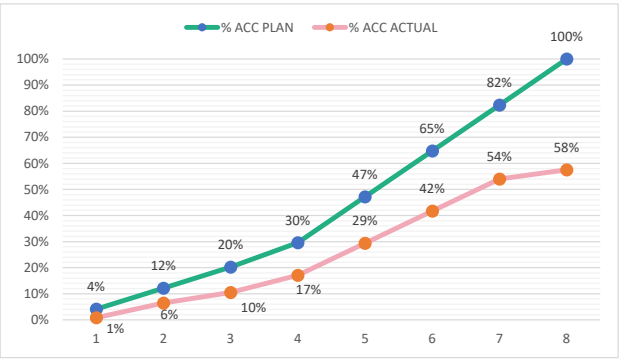
ตัวอย่างการคำนวณและการประเมินการดำเนินการตามแผนการทำงาน

ที่	รายการ	หน่วย	ปริมาณงาน	ราคาต่อหน่วย	เป็นเงิน	%
1	งานหรือโครงสร้างเดิม					
	a1	ลบ.ม.	100	5,000	500,000	16%
	a2	ลบ.ม.	120	2,000	240,000	8%
2	งานผิวทาง					
	b1	ตร.ม.	400	2,000	800,000	26%
	b2	ตร.ม.	300	5,000	1,500,000	49%
	รวม				3,040,000	100%

	1	2	3	4	5	6	7	8
	ตค	พย	ธค	มค	กพ	มีค	เมย	พค
Money	25	25	25	25				
AccMoney		50	50					
% PLAN				20	20	20	20	20
% ACC PLAN					25	25	25	25
% ACTUAL								
% ACC ACTUAL								
% ACC DIFF								
% PLAN/2								
% PLAN/2 DIFF								

$$\frac{(500,000 \times 25)}{100} = 125,000$$

$$\frac{125,000}{3,040,000} \times 100 = 4.1\%$$



- หมายเหตุ:
- กรณีตัวอย่าง กำหนดระยะเวลาการก่อสร้างตามแผนดำเนินงานทั้งสัญญา จำนวน 8 เดือน
  - หมายถึง ระยะเวลาการก่อสร้างตามแผนดำเนินงานของแต่ละรายการก่อสร้าง เช่น งานหรือโครงสร้างเดิม กำหนดระยะเวลาการก่อสร้าง จำนวน 4 เดือน (ไม่รวมระยะเวลาการก่อสร้างผิวทาง)
  - 25 หมายถึง ร้อยละของงานที่ผู้รับจ้างต้องดำเนินการก่อสร้างตามแผนงานประจำเดือนของแต่ละรายการก่อสร้าง (แต่ละรายการก่อสร้าง รวมกัน 100 %)
  - Money มูลค่างานแต่ละรายการ จำนวนจากร้อยละตามแผนงานเทียบกับมูลค่างานของแต่ละรายการ
  - % PLAN ร้อยละของแผนดำเนินงาน จำนวนจากมูลค่าของงานตามแผนดำเนินการ เมื่อเทียบกับมูลค่าของงานทั้งโครงการ



ตัวอย่างวิธีการจัดทำแผนการทำงาน

ที่	รายการ	หน่วย	ปริมาณงาน	ราคาต่อหน่วย	เป็นเงิน	%	1	2	3	4	5	6	7	8
							ตค	พย	ธค	มค	กพ	มีค	เมย	พค
1	งานรื้อโครงสร้างเดิม													
	a1	ลบ.ม.	100	5,000	500,000	16%	25	25	25	25				
	a2	ลบ.ม.	120	2,000	240,000	8%		50	50					
2	งานผิวทาง				-									
	b1	ตร.ม.	400	2,000	800,000	26%				20	20	20	20	20
	b2	ตร.ม.	300	5,000	1,500,000	49%					25	25	25	25
	รวม				3,040,000	100%								
	Money													
	AccMoney													
	% PLAN													
	% ACC PLAN													
	% ACTUAL													
	% ACC ACTUAL													
	% ACC DIFF													
	% PLAN/2													
	% PLAN/2 DIFF													

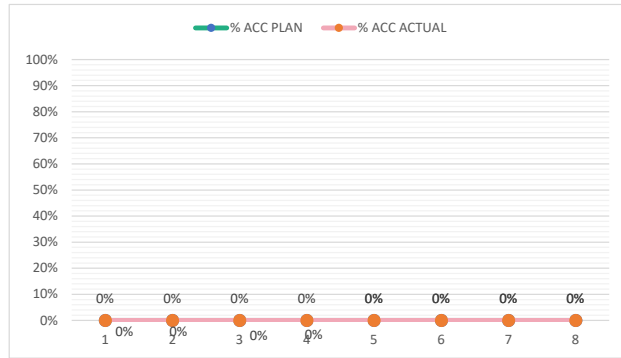
หมายเหตุ:

- กรณีตัวอย่าง กำหนดระยะเวลาการก่อสร้างตามแผนดำเนินงานทั้งสัญญา จำนวน 8 เดือน
- หมายถึง ระยะเวลาการก่อสร้างตามแผนดำเนินงานของแต่ละรายการก่อสร้าง เช่น 1. งานรื้อโครงสร้างเดิม กำหนดระยะเวลาการก่อสร้าง จำนวน 4 เดือน 2. งานก่อสร้างผิวทาง กำหนดระยะเวลาการก่อสร้าง 5 เดือน
- 25 หมายถึง ร้อยละของงานที่ผู้รับจ้างต้องดำเนินการก่อสร้างตามแผนงานประจำเดือนของแต่ละรายการก่อสร้าง ซึ่งแต่ละรายการก่อสร้าง คิดเป็นร้อยละ 100 ตามตัวอย่าง งานรื้อโครงสร้างเดิม ถือเป็นร้อยละ 100 ของรายการนี้
- Money มูลค่างานแต่ละรายการ คำนวณจากร้อยละตามแผนงานเทียบกับมูลค่างานของแต่ละรายการ
- % PLAN ร้อยละของแผนดำเนินงาน คำนวณจากมูลค่าของงานตามแผนดำเนินงาน เมื่อเทียบกับมูลค่าของงานทั้งโครงการ

ตัวอย่างแบบการจัดทำแผนการทำงาน

ที่	รายการ	หน่วย	ปริมาณงาน	ราคาต่อหน่วย	เป็นเงิน	%
1	งานรื้อโครงสร้างเดิม					
	รายการ...	ลบ.ม.				
	รายการ...	ลบ.ม.				
2	งานผิวทาง					
	รายการ...	ตร.ม.				
	รายการ...	ตร.ม.				
รวม					-	0%

1	2	3	4	5	6	7	8
เดือน...	เดือน...	เดือน...	เดือน...	เดือน...	เดือน...	เดือน...	เดือน...



Money								
AccMoney								
% PLAN								
% ACC PLAN								
% ACTUAL								
% ACC ACTUAL								
% ACC DIFF								
% PLAN/2								
% PLAN/2 DIFF								

หมายเหตุ:

- กรณีตัวอย่าง กำหนดระยะเวลาการก่อสร้างตามแผนดำเนินงานทั้งสัญญา จำนวน 8 เดือน
- หมายถึง ระยะเวลาการก่อสร้างตามแผนดำเนินงานของแต่ละรายการก่อสร้าง เช่น งานรื้อโครงสร้างเดิม กำหนดระยะเวลาการก่อสร้าง จำนวน 4 เดือน (ไม่รวมระยะเวลาการก่อสร้างผิวทาง)
- 25 หมายถึง ร้อยละของงานที่ผู้รับจ้างต้องดำเนินการก่อสร้างตามแผนงานประจำเดือนของแต่ละรายการก่อสร้าง ซึ่งแต่ละรายการก่อสร้าง คิดเป็น 100 %
- Money มูลค่างานแต่ละรายการ คำนวณจากร้อยละตามแผนงานเทียบกับมูลค่างานของแต่ละรายการ
- % PLAN ร้อยละของแผนดำเนินงาน คำนวณจากมูลค่าของงานตามแผนดำเนินการ เมื่อเทียบกับมูลค่าของงานทั้งโครงการ