

ขอบเขตของงานซื้ออุปกรณ์รักษาความปลอดภัยขั้นสูง  
(Advanced Persistent Threat : APT)

1. ความเป็นมา

การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย (รฟม.) ได้มีการใช้งานเครือข่ายสื่อสารในการ ปฏิบัติงานของ รฟม. และงานในโครงการรถไฟฟ้าที่อยู่ในความรับผิดชอบของ รฟม. ซึ่งในปัจจุบันพบว่าการโจมตีระบบรักษาความปลอดภัยมีรูปแบบใหม่และมีความหลากหลายมากขึ้น เช่น มีการใช้มัลแวร์เข้ามาทำการขโมยข้อมูลหรือทำการเรียกค่าไถ่ข้อมูลที่สำคัญมากขึ้น จึงมีความจำเป็นต้องจัดหาระบบป้องกันภัยคุกคามขั้นสูง เพื่อสามารถป้องกันภัยจากการโจมตีรูปแบบใหม่ๆ ได้

2. วัตถุประสงค์

- 2.1. จัดซื้อและติดตั้งระบบป้องกันภัยคุกคามขั้นสูงเพื่อปรับปรุงระดับการรักษาความปลอดภัยของข้อมูลภายในให้สูงขึ้น และช่วยป้องกันการสูญหาย รั่วไหลของข้อมูลสำคัญของ รฟม. โดยระบบจะต้องมีความสามารถป้องกันภัยคุกคามทางไซเบอร์ทั้งแบบ Signature ,Signature less และ Unknown Threat ได้
- 2.2. เพื่อเพิ่มประสิทธิภาพการวิเคราะห์ เชื่อมโยงข้อมูลและพฤติกรรมที่ผิดปกติของการรับส่งข้อมูลผ่านระบบเครือข่าย และสามารถตอบสนองต่อเหตุการณ์ที่เป็นอันตรายได้อย่างรวดเร็วโดยการปิดกั้นการเข้าถึง Website หรือกระบวนการที่เป็นอันตรายรวมถึงสามารถแยกอุปกรณ์ที่ถูกโจมตีออกจากระบบเพื่อลดผลกระทบจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

3. คุณสมบัติของผู้ยื่นข้อเสนอ

- 3.1 มีความสามารถตามกฎหมาย
- 3.2 ไม่เป็นบุคคลล้มละลาย
- 3.3 ไม่อยู่ระหว่างเลิกกิจการ
- 3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง
- 3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทำงานและได้แจ้งเวียนชื่อให้เป็นผู้ทำงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทำงานเป็นหุ้นส่วน ผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย
- 3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา
- 3.7 เป็นนิติบุคคลผู้มีอาชีพรับจ้างหรือขายงานที่ประกวดราคาอิเล็กทรอนิกส์หรือเป็นนิติบุคคลผู้มีอาชีพรับจ้างหรือขายงานที่ได้ขึ้นทะเบียนผู้ประกอบการวิสาหกิจขนาดกลางและขนาดย่อม (SMEs)
- 3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้
- 3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกันซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่ รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นนั้น

   
/3.10 ผู้ยื่นข้อ...  
หน้า... ๐๖๖๖ ๖

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

3.11 ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการเป็นไปตามเงื่อนไขข้อ 1.1 – 1.2 ของหนังสือคณะกรรมการวินิจฉัยปัญหาการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ กรมบัญชีกลาง ด่วนที่สุดที่ กค (กวจ) 0405.2/ว124 ลงวันที่ 1 มีนาคม 2566 เรื่องแนวทางปฏิบัติในการเร่งรัดการปฏิบัติงานตามสัญญา และการกำหนดคุณสมบัติของผู้มีสิทธิยื่นข้อเสนอ

3.12 ผู้ยื่นข้อเสนอที่เสนอราคาในรูปแบบของ “กิจการร่วมค้า” ต้องมีคุณสมบัติดังนี้  
กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงฯ จะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลักกิจกรรมร่วมค่านั้น ต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

3.13 ผู้ยื่นข้อเสนอต้องมีหนังสือแต่งตั้งการเป็นตัวแทนจำหน่ายและให้บริการเกี่ยวกับอุปกรณ์ที่เสนอทุกรายการที่เป็นต้นฉบับจากผู้ผลิต หรือจากสาขาของผู้ผลิตในประเทศไทย หรือจากตัวแทนจำหน่ายในประเทศไทย โดยต้องออกให้เพื่อมายื่นเอกสารประกวดราคาซื้อด้วยวิธีการทางอิเล็กทรอนิกส์นี้ และหนังสือนั้นต้องมีอายุไม่เกิน 90 วัน (เก้าสิบวัน) นับถัดจากวันที่ออกจนถึงวันที่ยื่นเอกสารประกวดราคา ทั้งนี้หากเป็นหนังสือจากตัวแทนจำหน่ายในประเทศไทยต้องแนบสำเนาเอกสารแต่งตั้งการเป็นตัวแทนจำหน่ายจากผู้ผลิตด้วย

#### 4. รายละเอียดคุณสมบัติเฉพาะของพัสดุ

##### 4.1 เงื่อนไขและข้อกำหนดทั่วไป

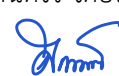
4.1.1 แต่ละผลิตภัณฑ์ที่นำเสนอต้องมีสำนักงานสาขาหรือตัวแทนจำหน่ายในประเทศไทยเพื่อสนับสนุนการให้บริการ

4.1.2 อุปกรณ์ในระบบดังกล่าวต้องเป็นของแท้ อยู่ในสภาพที่ใช้งานได้ดี เป็นรุ่นที่ยังอยู่ในสายการผลิต (Product Line) และต้องเป็นของใหม่ที่ไม่เคยถูกใช้งานมาก่อน

4.1.3 อุปกรณ์ที่เสนอต้องมีคุณสมบัติตรงตาม Catalog หรือ Brochure ของบริษัทผู้ผลิตที่เสนอขายตามท้องตลาด โดยมีระบบหลัก และ/หรือองค์ประกอบหลัก ที่ไม่ได้ประกอบ และ/หรือดัดแปลง เพื่อใช้เฉพาะการประกวดราคาครั้งนี้ โดยผู้ยื่นข้อเสนอจะต้องระบุยี่ห้อและรุ่นของผลิตภัณฑ์ที่เสนอ พร้อมทั้งต้องมี Catalog หรือ Brochure ที่ชัดเจนได้ ทำเครื่องหมาย หรือระบายสี พร้อมหัวข้อกำกับอุปกรณ์ที่เสนอไว้อย่างชัดเจน

4.1.4 อุปกรณ์ที่นำเสนอต้องสามารถใช้งานกับระบบไฟฟ้า 220V AC 50Hz ตามมาตรฐานของประเทศไทยได้โดยไม่ต้องใช้อุปกรณ์แปลงระบบไฟฟ้า และปลั๊กไฟฟ้าของอุปกรณ์ทุกรายการจะต้องเป็นชนิด 3 ขา (มีขาสำหรับสายดิน)

4.1.5 กรณีมีรายการใด ประสิทธิภาพการผลิต หรือตกหล่น ในส่วนของอุปกรณ์ควบใดๆ ส่งผลให้อุปกรณ์นั้น หรือระบบโดยรวม ไม่สามารถทำงานได้ตามความต้องการของ รพม. ให้ถือเป็นความรับผิดชอบของผู้ขายจัดหาเพิ่มเติม เพื่อให้ระบบสามารถทำงานได้ตามที่ทาง รพม. ได้กำหนดไว้ โดยไม่คิดค่าใช้จ่ายอื่นใดเพิ่มเติม

 นพ.วิวัฒน์

/4.1.6 ผู้ขาย...

  
นพ.วิวัฒน์

4.1.6 ผู้ขายต้องจัดฝึกอบรมเจ้าหน้าที่ผู้ดูแลระบบอย่างน้อย 4 คน โดยต้องเสนอหัวข้อการอบรมเชิงปฏิบัติการ พร้อมเอกสารที่จะใช้ฝึกอบรมที่เป็นภาษาไทย โดยเนื้อหาการฝึกอบรมต้องเป็นไปตามมาตรฐานของผลิตภัณฑ์ที่เสนอซึ่งต้องครอบคลุมเนื้อหาที่เกี่ยวข้องกับ การติดตั้ง กำหนดค่า บริหารจัดการ และการแก้ปัญหา ให้คณะกรรมการตรวจรับพัสดุพิจารณาและต้องได้รับการเห็นชอบก่อนทำการฝึกอบรม โดยต้องฝึกอบรมให้แล้วเสร็จก่อนการส่งมอบระบบทั้งหมด

4.1.7 คณะกรรมการตรวจรับพัสดุฯ จะทดสอบ ตรวจรับผลิตภัณฑ์ที่เสนอตามสัญญาฯ ต่อเมื่อคณะกรรมการตรวจรับพัสดุฯ ได้รับหนังสือแจ้งจากผู้ขายว่าได้ติดตั้งผลิตภัณฑ์ทั้งหมดเสร็จเรียบร้อยแล้วพร้อมที่จะส่งมอบแล้ว

4.1.8 อุปกรณ์ที่เสนอต้องมีคุณสมบัติเฉพาะอย่างน้อยตาม ภาคผนวก ก.

#### 4.2 ขอบเขตของงาน

4.2.1 จัดให้มีการประชุมเริ่มงาน (Kick off Meeting) เพื่อนำเสนอแผนการดำเนินงานในการออกแบบ ติดตั้งและทดสอบ ให้พิจารณาก่อนการดำเนินงานติดตั้งจริงภายใน 15 วัน (สิบห้าวัน) นับถัดจากวันที่ลงนามในสัญญา

4.2.2 ผู้ขายต้องดำเนินการออกแบบ ติดตั้งระบบที่เสนอให้สามารถใช้งานร่วมกับระบบเครือข่ายและระบบคอมพิวเตอร์ของ รพม. ได้อย่างมีประสิทธิภาพ

4.2.3 หลังจากที่ผู้ขายได้ดำเนินงานต่างๆ เรียบร้อยแล้ว ผู้ขายต้องจัดส่งรายงานผลการดำเนินงาน และเอกสารอื่นๆ ที่เกี่ยวข้องในรูปแบบ Digital Files ที่สามารถแก้ไขปรับปรุงได้ เช่น .docx, .xlsx, .vsdx เป็นต้นและในรูปแบบ pdf บรรจุลงใน USB Flash Drive จำนวน 5 ชุด โดยรายงานต้องมีรายละเอียดครอบคลุมดังนี้

(1) สรุปผลการดำเนินงานออกแบบ ติดตั้งระบบป้องกันภัยคุกคามขั้นสูงของ รพม. ที่เป็นไปตามเงื่อนไขต่างๆ ตามข้อ 4.2.2

(2) แผนผังระบบเครือข่ายสื่อสารข้อมูล (Network Diagram) และแผนผังอุปกรณ์ที่ได้ติดตั้ง

(3) เอกสารประกอบการฝึกอบรมเชิงปฏิบัติการ ตามข้อ 4.1.6

#### 5. กำหนดเวลาส่งมอบพัสดุ

ผู้ขายต้องดำเนินการจัดหา ออกแบบ ติดตั้ง และทดสอบระบบตาม ภาคผนวก ก. พร้อมทั้งจัดการฝึกอบรมให้แก่เจ้าหน้าที่ของ รพม. ให้แล้วเสร็จ พร้อมส่งมอบภายใน 90 วัน (เก้าสิบวัน) นับถัดจากวันลงนามในสัญญา โดยผู้ขายต้องทำหนังสือแจ้งให้คณะกรรมการตรวจรับพัสดุฯ รับทราบก่อนวันส่งมอบและตรวจรับไม่น้อยกว่า 3 วัน (สามวัน) ทำการของ รพม.

#### 6. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

ในการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ รพม. จะพิจารณาตัดสินโดยใช้หลักเกณฑ์ราคา

#### 7. วงเงินงบประมาณ/วงเงินที่ได้รับจัดสรร

10,000,000 บาท (สิบล้านบาทถ้วน) (รวมภาษีมูลค่าเพิ่มแล้ว)

นายวิวัฒน์

/8. จวตงาน...

จวต.

อ.จ.จ

## 8. งวดงานและการจ่ายเงิน

รพม. จะจ่ายค่าพัสดุซึ่งได้รวมภาษีมูลค่าเพิ่มตลอดจนภาษีอากรอื่นๆ และค่าใช้จ่ายทั้งปวงแล้วให้แก่ผู้ขาย เมื่อผู้ขายได้ส่งมอบพัสดุได้ครบถ้วนตามสัญญาแล้ว โดย รพม. จะจ่ายเงินภายใน 30 วัน (สามสิบวัน) นับถัดจากได้ตรวจรับมอบงานเรียบร้อยแล้ว

## 9. อัตราค่าปรับ

9.1 กรณีส่งมอบระบบ และ/หรือ อุปกรณ์ ที่ได้ติดตั้งตามสัญญาล่าช้าเกินกว่ากำหนดในสัญญา บางรายการหรือทั้งหมด หรือมีคุณสมบัติไม่ถูกต้องตามรายละเอียดและคุณลักษณะที่กำหนด หรือส่งมอบแล้วแต่ยังไม่สามารถใช้งานได้ หรือจัดฝึกอบรมให้แก่เจ้าหน้าที่ รพม. ล่าช้าเกินกว่ากำหนดในสัญญา รพม. มีสิทธิบอกเลิกสัญญาได้ ในกรณีที่ รพม. ไม่ใช้สิทธิบอกเลิกสัญญา ผู้ขายยินยอมให้ รพม. ปรับเป็นรายวัน ในอัตรา 10,000 บาท (หนึ่งหมื่นบาทถ้วน) โดยเศษของวันให้คิดเป็นหนึ่งวัน นับถัดจากวันครบกำหนดส่งมอบตามสัญญาจนถึงวันที่ผู้ขายได้ติดตั้ง จัดฝึกอบรมและส่งมอบระบบรวมทั้งอุปกรณ์ ที่ได้มาตามสัญญาให้แก่ รพม. จนถูกต้องครบถ้วน

9.2 กรณีที่ผู้ขายไม่เริ่มดำเนินการซ่อมแซมแก้ไขภายในเวลา 4 ชั่วโมง นับแต่เวลาที่ รพม. ได้แจ้งความชำรุดบกพร่องดังกล่าว ผู้ขายยินยอมให้ รพม. ปรับเป็นรายชั่วโมง ในอัตราชั่วโมงละ 1,000 บาท (หนึ่งพันบาทถ้วน) โดยเศษของชั่วโมงให้คิดเป็นหนึ่งชั่วโมง นับตั้งแต่ครบกำหนดเวลาดังกล่าวจนกว่าผู้ขายจะเริ่มดำเนินการซ่อมแซมแก้ไขแล้วเสร็จ

9.3 กรณีที่ผู้ขายไม่สามารถดำเนินการได้ตามข้อ 10.การรับประกันความชำรุดบกพร่อง ผู้ขายยินยอมให้ รพม. ปรับเป็นรายวัน ในอัตราร้อยละ 0.1 ตามมูลค่าของสัญญา โดยเศษของวันให้คิดเป็นหนึ่งวัน นับตั้งแต่ครบกำหนดเวลาดังกล่าวจนถึงวันที่ผู้ขายได้ดำเนินการซ่อมแซมแก้ไขหรือเปลี่ยนอุปกรณ์ให้แล้วเสร็จ และสามารถใช้งานได้ติดตั้งเดิมเรียบร้อยแล้ว

9.4 กรณีที่ รพม. ใช้สิทธิบอกเลิกสัญญา นอกจากยินยอมให้ รพม. คิดค่าปรับตามข้อ 9.1 นับแต่วันผิดสัญญาจนถึงวันบอกเลิกสัญญาแล้ว ผู้ขายยินยอมให้ รพม. รับหลักประกันสัญญาเป็นจำนวนทั้งหมด หรือแต่บางส่วนก็ได้ แล้วแต่ รพม. จะเห็นสมควร

## 10. การรับประกันความชำรุดบกพร่อง

10.1 ผู้ขายจะต้องรับประกันความชำรุดบกพร่องของงานจ้างที่เกิดขึ้นภายในระยะเวลาไม่น้อยกว่า 2 ปี นับถัดจากวันที่คณะกรรมการตรวจรับพัสดุได้รับมอบงานครบถ้วนถูกต้อง โดยต้องบริหารจัดการซ่อมแซมแก้ไขให้ใช้งานได้ติดตั้งเดิมภายใน 1 วัน นับถัดจากวันที่ได้รับแจ้งความชำรุดบกพร่อง ผู้ขายจะต้องจัดให้มีเจ้าหน้าที่ที่มีความเชี่ยวชาญและมีประสบการณ์เพื่อเริ่มดำเนินการภายใน 4 ชั่วโมง นับตั้งแต่เวลาที่ รพม. ได้แจ้งความชำรุดบกพร่องให้ผู้ขายทราบทางโทรศัพท์ โทรศัพท์เคลื่อนที่ โทรสาร หรือจดหมายอิเล็กทรอนิกส์ (E-mail) โดยอะไหล่หรือวัสดุอุปกรณ์ที่ใช้ในการซ่อมแซมแก้ไข หรือให้ใช้เป็นการชั่วคราวหรือที่นำมาเปลี่ยนให้ใหม่นั้น จะต้องมีความสมบัติไม่ต่ำกว่าของเดิม สำหรับกรณีการเปลี่ยนวัสดุอุปกรณ์ให้ใหม่ วัสดุอุปกรณ์นั้นจะต้องเป็นของใหม่ที่ไม่เคยถูกใช้งานมาก่อนและไม่เป็นของเก่าเก็บ

10.2 กรณีที่มีการเคลื่อนย้าย หรือเปลี่ยนแปลงค่า (Re-config) หรือติดตั้งใหม่ (New Install) ของระบบและ/หรืออุปกรณ์ ที่ได้ติดตั้งตามสัญญานี้ รพม. มีสิทธิ์ที่จะแจ้งให้ผู้ขายมาดำเนินการให้แล้วเสร็จตามระยะเวลาที่ รพม. กำหนด ได้ตลอดอายุสัญญา โดย รพม. ไม่เสียค่าใช้จ่ายใดๆ เพิ่มเติมทั้งสิ้น

## 11. ข้อสงวนสิทธิ์ในการยื่นข้อเสนอและอื่นๆ

11.1 ผู้ขายและ/หรือเจ้าหน้าที่ของผู้ขายที่เข้าถึงระบบเทคโนโลยีสารสนเทศของ รพม. ต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของ รพม. ปรากฏดัง ภาคผนวก ข และจะต้องรักษาความลับต่างๆ ที่ได้จากการปฏิบัติงานโดยห้ามมิให้ผู้ขายและ/หรือเจ้าหน้าที่ของผู้ขายนำข้อมูลส่วนหนึ่งส่วนใดหรือทั้งหมดที่ได้จากการปฏิบัติงานใน รพม. ไปทำซ้ำ เผยแพร่ หรือวิเคราะห์ประมวลผลเพื่อการอื่นใด ไม่ว่าการกระทำดังกล่าวจะเป็นการหาผลประโยชน์หรือไม่ก็ตาม หาก รพม. ตรวจพบผู้ขายจะต้องชดเชยค่าเสียหายเป็นจำนวนเงินไม่น้อยกว่ามูลค่าทั้งหมดที่กำหนดไว้ในสัญญา ทั้งนี้ ผู้ขายและ/หรือเจ้าหน้าที่ของผู้ขายต้องลงนามในสัญญาการเก็บรักษาข้อมูลไว้เป็นความลับ (Non-Disclosure Agreement) ก่อนเริ่มปฏิบัติงาน ตามรูปแบบที่ รพม. กำหนด

11.2 ระบบปฏิบัติการและซอฟต์แวร์ที่ผู้ขายจัดหาเพื่อใช้ในโครงการนี้ทั้งหมด รพม. ต้องได้รับเอกสารสิทธิ (Software License) และ/หรือ สิทธิการใช้งานได้อย่างถูกต้องตามกฎหมาย โดยเอกสารสิทธิดังกล่าว รพม. จะเป็นเจ้าของเอกสารสิทธิทั้งหมด

11.3 ผู้ขายต้องส่งบุคลากรเข้าร่วมการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness) เพื่อสร้างความตระหนักที่เหมาะสม ทบทวนนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และขั้นตอนปฏิบัติของ รพม. ตามที่ รพม. กำหนด

  
นายธีรวัฒน์  
นพ. ธีรวัฒน์  
๐๖๖๖

ภาคผนวก ก.  
คุณลักษณะเฉพาะ

  
นายวิชาญ ใจเย็น  นส. 

**1. ระบบตรวจจับความปลอดภัยและตอบสนองในระบบเครือข่าย (Network Detection and Response : NDR) พร้อมติดตั้งจำนวน 1 ระบบ มีคุณลักษณะอย่างน้อย ดังนี้**

- 1.1 เป็นอุปกรณ์แบบ Appliance ที่ออกแบบมาทำหน้าที่วิเคราะห์ ตรวจสอบความผิดปกติของเครือข่ายโดยเฉพาะ
- 1.2 สามารถวิเคราะห์ข้อมูลผ่านระบบเครือข่ายได้ไม่น้อยกว่า 5 Gbps
- 1.3 สามารถวิเคราะห์ข้อมูลผ่าน IP Address ที่ รพม. สนใจได้จำนวนไม่น้อยกว่า 6,000 IP
- 1.4 มี Interface ที่ใช้ในการตรวจสอบและป้องกันหรือบริหารจัดการแบบ Ethernet 10/100/1000 ไม่น้อยกว่า 2 interfaces
- 1.5 มี Interface ที่ใช้ในการตรวจสอบและป้องกันแบบ 10Gigabit Ethernet SFP+ หรือ 10G Base-T ไม่น้อยกว่า 2 interfaces
- 1.6 มี Power Supply แบบ Dual Power Supply หรือ Redundant Power Supply
- 1.7 สามารถรวบรวมข้อมูลภายในระบบเครือข่ายด้วยวิธีการ SPAN หรือ Mirrored ได้
- 1.8 สามารถตรวจสอบประเภทของไฟล์ที่ใช้ผ่านเครือข่ายภายในได้หลายประเภท เช่น PDF, DOC, DOCX, XLS, XLSX, PPT, PPTX, ZIP, RAR, EXE เป็นต้น
- 1.9 สามารถตรวจจับ ค้นหา แจ้งเตือน และรายงานอันตรายจากภัยต่าง ๆ (Threats) ใน ระบบเครือข่ายให้กับผู้ดูแลระบบได้ตามเวลาจริงที่เกิดขึ้น (Real-Time) เมื่อมีการตรวจพบไฟล์หรือกระแสข้อมูลที่ไม่ปลอดภัย ในการส่งข้อมูลทั้งขาเข้าและออกจากระบบเครือข่ายคอมพิวเตอร์
- 1.10 สามารถตรวจเนื้อหา การเชื่อมต่อ และพฤติกรรม ที่ไม่ปลอดภัยหรือการโจมตีภายใน กระแสข้อมูล (Traffic) ของระบบเครือข่ายคอมพิวเตอร์และสามารถป้องกันการติดต่อระหว่างเครื่องของผู้ใช้งานไปยัง Command and Control Servers หรือที่เรียกว่า Callback ได้ หรือสามารถทำงานร่วมกับอุปกรณ์เดิมของ รพม. (Integrate) เพื่อป้องกันการติดต่อดังกล่าวได้
- 1.11 มีความสามารถในการตรวจจับภัยคุกคามทางด้านไซเบอร์แบบเชิงรุกหรือสืบค้นต้นตอของเหตุการณ์ (Threat Hunting)
- 1.12 สามารถแสดงข้อมูลที่มาของการโจมตี เช่น URL ต้นทาง ของมัลแวร์หรือแสดงข้อมูล Traffic ในรูปแบบของ PCAP ได้
- 1.13 รองรับโปรโตคอล HTTP, HTTPS, SSH, SMB และ SMTP ได้เป็นอย่างดี
- 1.14 สามารถส่ง Syslog หรือ Export เพื่อสำรองข้อมูลไปยังเครื่องภายนอก (Remote Server) ได้
- 1.15 สามารถกำหนดสิทธิการเข้าใช้งานของผู้ใช้งาน (Role-base Administrator) ได้เพื่อการควบคุมจำกัดสิทธิใน การเข้าถึงอุปกรณ์
- 1.16 สามารถเข้าบริหารจัดการผ่าน Web Browser เช่น Microsoft edge, Firefox หรือ Google Chrome เป็นต้น โดยที่ไม่ต้องลงส่วนเสริม (Extension) ได้
- 1.17 เป็นผลิตภัณฑ์ที่ประกอบจากโรงงานที่ได้รับรองมาตรฐาน ISO 9000 Series หรือได้รับการรับรองตามมาตรฐาน UL 60950, EN 60950, IEC 60950 หรือเทียบเท่า
- 1.18 เป็นผลิตภัณฑ์ที่ได้รับรองมาตรฐานด้านสิ่งแวดล้อม FCC หรือ CE หรือ RoHS หรือเทียบเท่า

**2. ระบบป้องกัน ตรวจจับ และตอบสนองอัตโนมัติเครื่องผู้ใช้ปลายทาง (Endpoint Detection and Response : EDR) พร้อมติดตั้งจำนวน 1 ระบบ มีคุณลักษณะอย่างน้อย ดังนี้**

- 2.1 สามารถติดตั้งบนระบบปฏิบัติการคอมพิวเตอร์ได้อย่างน้อยดังนี้
  - Windows 10
  - Windows 11
  - Mac OS
- 2.2 เป็นซอฟต์แวร์สำหรับป้องกัน และตอบสนองต่อเหตุการณ์แบบเรียลไทม์ ที่สามารถติดตั้งบนคอมพิวเตอร์ของ รพม. ได้ โดยต้องส่งมอบสิทธิ์การใช้งานแก่ รพม. ไม่น้อยกว่า 50 สิทธิ์
- 2.3 สามารถป้องกันคอมพิวเตอร์ได้แม้คอมพิวเตอร์เครื่องดังกล่าวจะอยู่ในสถานะออฟไลน์
- 2.4 สามารถป้องกันการใช้งานแอปพลิเคชันที่ไม่ต้องการได้ (Application Block)
- 2.5 สามารถป้องกันการเชื่อมต่อไปยังปลายทางที่เป็นอันตรายเช่น C2 (C&C), Malicious Website หรือ Block process ที่มีความเสี่ยง สำหรับการเชื่อมต่อไปยังภายนอกได้เป็นอย่างดี
- 2.6 สามารถอัปเดตฐานข้อมูล Threat Intelligence จากเจ้าของผลิตภัณฑ์ได้ตลอดอายุสัญญา
- 2.7 สามารถกำหนดเงื่อนไขในการแก้ปัญหาเมื่อตรวจพบมัลแวร์ได้อย่างน้อย ดังนี้
  - Terminate Process
  - Delete File
  - Quarantine File หรือ Clean Persistent Data
- 2.8 สามารถระบุและตรวจสอบ Application ที่ใช้งานภายในองค์กร ตามรายการช่องโหว่ใน Common Vulnerability Scoring System (CVSS) หรือ Common Vulnerabilities and Exposures (CVE) ได้
- 2.9 สามารถวิเคราะห์สิ่งผิดปกติจากพฤติกรรมของผู้ใช้งาน (User Behavior Analytics (UBA) หรือ User and Entity Behavior Analytics (UEBA)) และวิเคราะห์สาเหตุที่แท้จริงของปัญหาที่เกิดขึ้น (Root Cause Analysis) หรือสามารถวิเคราะห์พฤติกรรมที่ผิดปกติโดยอ้างอิงจากเว็บไซต์ MITRE ATT&CK ผ่านตัวบ่งชี้ Indicators of attack (IOA) รวมถึงสร้างภาพเหตุการณ์ที่เกิดขึ้น (visualization and reporting) ได้ หรือแสดง Timeline ของเหตุการณ์ที่เกิดขึ้น (Timeline analysis of alerts) ได้
- 2.10 ซอฟต์แวร์ที่เสนอจะต้องมีระบบบริหารจัดการกลางจากส่วนกลาง โดยระบบต้องมีความสามารถอย่างน้อย ดังนี้
  - สามารถเข้าบริหารจัดการผ่าน Web Browser เช่น Microsoft edge, Firefox หรือ Google Chrome เป็นต้น โดยที่ไม่ต้องลงส่วนเสริม (Extension) ได้
  - มีหน้าจอสำหรับแสดงภาพรวมการตรวจจับภัยคุกคามด้านไซเบอร์ที่เกิดขึ้น
  - สามารถออกรายงานภัยคุกคามทางไซเบอร์ในรูปแบบของ PDF หรือ XML ได้เป็นอย่างดี
  - สามารถพิสูจน์ตัวตน (Authentication) และกำหนดสิทธิ์ (Authorization) สำหรับผู้ดูแลระบบได้ โดยทำงานร่วมกับฐานข้อมูลแบบ Local และ LDAP หรือ Domain ได้เป็นอย่างดี
  - สามารถส่ง Syslog ไปยังอุปกรณ์ภายนอก เช่น ระบบ SIEM ได้เป็นอย่างดี
  - สามารถเข้าถึงเครื่องคอมพิวเตอร์ที่ติดตั้งซอฟต์แวร์ข้างต้นได้โดยตรงเพื่อตรวจสอบและรวบรวมข้อมูลผ่านทาง Remote Shell หรือ Threat Hunting ได้เป็นอย่างดี

**3. ระบบตรวจจับและตอบสนองต่อภัยคุกคามแบบเจาะจง (Extended Detection and Response : XDR) พร้อมติดตั้งจำนวน 1 ระบบ มีคุณลักษณะอย่างน้อย ดังนี้**

3.1 สามารถรองรับการติดตั้งทั้งในรูปแบบ Hardware Appliance หรือแบบ Virtualize Deployment

3.2 สามารถรับข้อมูลจากระบบ NDR ที่เสนอมาในโครงการและรับข้อมูลจากอุปกรณ์ภายนอก เช่น IPS, WAF, Firewall เพื่อตรวจสอบภัยคุกคามได้อย่างน้อย ดังนี้

- Vulnerability risks
- Access risks
- Website attacks
- Attack exploitation
- Access to malicious files

3.3 สามารถรับข้อมูลจากระบบ EDR ที่เสนอมาในโครงการ เพื่อตรวจสอบภัยคุกคามได้อย่างน้อย ดังนี้

- Process Create, Process Destruction หรือ Process Termination
- DNS query
- File creation
- Port monitoring
- Scheduled task creation
- Service creation
- Service deletion

3.4 สามารถทำ Incident Response เพื่อตอบสนองต่อภัยคุกคามทั้งแบบ Manual และ Automation ไปยังอุปกรณ์ Network, Security หรือ Endpoint ได้โดยมีชุดข้อมูลแบบ Pre-defined มาให้ในระบบ และสามารถแก้ไขเพิ่มเติมได้ (Customization)

3.5 สามารถแจ้งเหตุการณ์การโจมตี โดยบอกรายละเอียดของภัยคุกคามที่เกิดขึ้น รวมไปถึงสามารถบอกกระบวนการของภัยคุกคามตั้งแต่เริ่มต้นจนถึงปัจจุบันบนหน้าจอ Dashboard ได้

3.6 สามารถเชื่อมต่อไปยังอุปกรณ์ EDR ที่เสนอมาในโครงการ เพื่อสั่ง Scan Virus หรือนำเครื่องออกจากระบบ (Isolate) เมื่อมีเหตุการณ์ผิดปกติเกิดขึ้น

3.7 สามารถตรวจสอบความเสี่ยง หรือช่องโหว่ในระบบได้ (Vulnerability) โดยมีข้อมูลประกอบ เช่น Vulnerability name หรือ Vulnerability Level, , Discovery time, CVE-ID หรือ MITRE ATT&CK Stage เป็นต้น

3.8 สามารถสรุปรายละเอียดของภัยคุกคามโดยเปรียบเทียบกับเทคนิคการโจมตีในมาตรฐานของ MITRE ATT&CK Framework ได้

3.9 สามารถพิสูจน์ตัวตน (Authentication) และกำหนดสิทธิ์การใช้งาน (Authorization) สำหรับผู้ดูแลระบบได้ โดยทำงานร่วมกับฐานข้อมูลแบบ Local และ LDAP ได้เป็นอย่างน้อย

3.10 สามารถส่ง Syslog เพื่อสำรองข้อมูลไปยังเครื่องภายนอก (Remote Server) ได้

3.11 อุปกรณ์ที่นำเสนอมีการเชื่อมต่อกับระบบเน็ตเวิร์คของเจ้าของผลิตภัณฑ์หรือ Call Home เพื่อแบ่งปันข้อมูลของ Advanced Malware หรือ Zero Threats ใหม่ ๆ ที่เกิดขึ้นได้

3.12 สามารถเก็บ Log ได้ไม่น้อยกว่า 100 GB ต่อวัน หรือไม่น้อยกว่า 1,000,000 event ต่อวันที่

3.13 สามารถค้นหา Logs แบบกำหนดเงื่อนไข เช่น ชนิดของการตรวจสอบ (Detection Type), IP Address ได้เป็นอย่างน้อย และค้นหา Logs แบบกำหนดเวลาได้

3.14 สามารถสร้างรายงาน (Report) ได้ ทั้งแบบ On-Demand และ Scheduled ในการสร้างรายงานแบบรายวัน รายสัปดาห์ และรายเดือน

**4. อุปกรณ์รักษาความปลอดภัย (Firewall) พร้อมติดตั้งจำนวน 2 ชุด มีคุณลักษณะอย่างน้อย ดังนี้**

4.1 เป็นอุปกรณ์รักษาความปลอดภัย (Firewall) ประเภท Appliance ซึ่ง Hardware ถูกออกแบบให้มีโครงสร้างสถาปัตยกรรมแบบ Single Pass Security Services enforcement หรือ Single-pass inspection มาเพื่อทำหน้าที่รักษาความปลอดภัยของเครือข่ายโดยเฉพาะ

4.2 เป็นอุปกรณ์รักษาความปลอดภัยประเภท Next Generation Firewall (NGFW)

4.3 มี Firewall Throughput Layer 7 ไม่ต่ำกว่า 10 Gbps

4.4 รองรับการเชื่อมต่อใหม่ (New Connections per Second) ได้ไม่น้อยกว่า 68,000 การเชื่อมต่อ

4.5 มี Interface แบบ Ethernet 10/100/1000 ไม่น้อยกว่า 8 interfaces

4.6 มี Interface แบบ 10Gigabit Ethernet SFP+ หรือ 10G Base-T ไม่น้อยกว่า 4 interfaces

4.7 มีพอร์ต Gigabit Ethernet ไว้สำหรับ Management แบบ Out-of-Band ไม่น้อยกว่า 1 พอร์ต

4.8 มี Storage ไม่น้อยกว่า 200 GB

4.9 รองรับการเชื่อมต่อในแบบ Active/Standby ได้

4.10 รองรับการทำงาน VLANs ไม่น้อยกว่า 512 VLANs

4.11 สามารถเข้าบริหารจัดการผ่าน Web Browser เช่น Microsoft edge, Firefox หรือ Google Chrome เป็นต้น โดยที่ไม่ต้องลงส่วนเสริม (Extension) ผ่านการเข้ารหัสแบบ TLS1.2 หรือ SSL3.0 ได้เป็นอย่างน้อย

4.12 สามารถทำงานแบบ URL Filtering บนตัวอุปกรณ์ได้ โดยมีการแบ่งเว็บไซต์ออกเป็นกลุ่ม (Categories) และสามารถกำหนด whitelist และ Blacklist ได้

4.13 มี Power Supply แบบ Dual Power Supply หรือ Redundant Power Supply

4.14 สามารถพิสูจน์ตัวตน (Authentication) และกำหนดสิทธิ์การใช้งาน (Authorization) สำหรับผู้ดูแลระบบได้ โดยทำงานร่วมกับฐานข้อมูลแบบ Local และ LDAP ได้เป็นอย่างน้อย

4.15 เป็นผลิตภัณฑ์ที่ประกอบจากโรงงานที่ได้รับรองมาตรฐาน ISO 9000 Series หรือเทียบเท่า

4.16 เป็นผลิตภัณฑ์ที่ได้รับรองมาตรฐานด้านสิ่งแวดล้อม FCC หรือ CE หรือ RoHS หรือเทียบเท่า

ภาคผนวก ข.

นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของ รฟม.

  
ประธานกรรมการ  
  
ผู้จัดการ  
๐๕๖๖



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 กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ จึงส่งผลให้ระบบเทคโนโลยีสารสนเทศของการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย (รฟม.) ต้องมีการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศอย่างครบถ้วนเพื่อธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) และความน่าเชื่อถือ (Reliability)

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

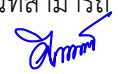
อาศัยอำนาจตามความในมาตรา 25 แห่งพระราชบัญญัติการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย พ.ศ. 2543 ผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย จึงออกประกาศการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ดังต่อไปนี้

1. วัตถุประสงค์และขอบเขต

เพื่อให้การใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาและลดผลกระทบจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องหรือจากการถูกคุกคามจากภัยต่าง ๆ จึงได้กำหนดนโยบายเพื่อควบคุมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ดังนี้

1.1 การเข้าถึงหรือควบคุมการใช้งานสารสนเทศครอบคลุม 4 ด้าน คือ

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

  
/เข้าถึง...

เข้าถึงระบบได้ รวมถึงมีการเก็บบันทึกข้อมูลการเข้าถึงระบบ (Access log) และข้อมูลจราจรทางคอมพิวเตอร์ ทั้งนี้ การให้สิทธิ์การใช้งานระบบสารสนเทศนั้นต้องให้สิทธิ์ที่เหมาะสมและเพียงพอ (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 เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคง 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 การใช้งาน...

- 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 รวมถึงผู้ให้บริการระบบสารสนเทศของ รฟม. ที่เกี่ยวข้องจะต้องปฏิบัติตามอย่างเคร่งครัด

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

นโยบายนี้ให้ใช้บังคับเมื่อพ้นกำหนด 7 วัน นับแต่วันที่ผู้มีอำนาจลงนาม

ประกาศ ณ วันที่ 28 กันยายน พ.ศ. 2566



(นายภคพงศ์ ศิริกันทรมาศ)

ผู้ว่าการการรถไฟฟ้ามหานครแห่งประเทศไทย



## สารบัญ

| เรื่อง                                                                                | หน้า |
|---------------------------------------------------------------------------------------|------|
| คำนิยาม .....                                                                         | 1    |
| ส่วนที่ 1 นโยบายการบริหารจัดการความมั่นคงปลอดภัยสำหรับผู้บริหาร .....                 | 4    |
| ส่วนที่ 2 ความมั่นคงปลอดภัยเกี่ยวกับบุคลากร.....                                      | 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. ฝทท. หมายถึง 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 บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย
11. ขั้นตอนปฏิบัติ หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานตามที่ได้กำหนดไว้ตามวัตถุประสงค์
12. แนวปฏิบัติ หมายถึง แนวทางที่ต้องปฏิบัติตามเพื่อให้สามารถบรรลุวัตถุประสงค์หรือเป้าหมายได้ง่ายขึ้น
13. ระบบเทคโนโลยีสารสนเทศ (Information technology system) หมายถึง ระบบงานของ รฟม. ที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายสื่อสารข้อมูลมาช่วยในการสร้างสารสนเทศที่ รฟม. สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุน การให้บริการ 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 ที่เกี่ยวข้องกัระบบสารสนเทศของหน่วยงาน
20. ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) และความน่าเชื่อถือ (Reliability)
21. เหตุการณ์ด้านความมั่นคงปลอดภัย หมายถึง เหตุการณ์ที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย มาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
22. สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม
23. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้
24. สินทรัพย์ (Assets) หมายถึง สินทรัพย์ด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารของ รพม. เช่น อุปกรณ์คอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีค่าลิขสิทธิ์ ข้อมูล ระบบข้อมูล ฯลฯ
25. จดหมายอิเล็กทรอนิกส์ (e-mail) หมายถึง ระบบที่บุคคลใช้ในการรับ - ส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ โดยข่าวสารที่ส่งนั้นจะถูกเก็บไว้ในตู้จดหมาย (Mail box) ที่กำหนดไว้สำหรับผู้ใช้งาน ผู้รับสามารถเปิดอ่าน พิมพ์ลงกระดาษ หรือจะลบทิ้งก็ได้

26. ชุดคำสั่งไม่พึงประสงค์ (Malicious code) หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ชัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
27. เครื่องคอมพิวเตอร์ หมายถึง เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ และเครื่องคอมพิวเตอร์แบบพกพา
28. อุปกรณ์เคลื่อนที่ (Mobile device) หมายถึง อุปกรณ์อิเล็กทรอนิกส์แบบพกพา ซึ่งมีความสามารถในการเชื่อมต่อกับอุปกรณ์อื่นเพื่อรับส่งข้อมูลผ่านระบบเครือข่ายโทรคมนาคมไร้สายหรือโดยอาศัยคลื่นแม่เหล็กไฟฟ้าเป็นสื่อกลาง เช่น Tablet, Smart Phone
29. ทรัพย์สินของ รฟม. หมายถึง ครุภัณฑ์ รฟม. และทรัพย์สินที่ไม่มีการขึ้นทะเบียนครุภัณฑ์ที่ รฟม. จัดสรรงบประมาณเพื่อเป็นค่าใช้จ่ายให้ทั้งหมดหรือบางส่วน
30. อุปกรณ์ส่วนตัว หมายถึง อุปกรณ์ที่ไม่ใช่ทรัพย์สินของ รฟม. ที่ผู้ใช้งานนำมาเชื่อมต่อกับระบบสารสนเทศของ รฟม. 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

### ความมั่นคงปลอดภัยเกี่ยวกับบุคลากร

#### วัตถุประสงค์

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

#### ผู้รับผิดชอบ

- ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ ผู้อำนวยการฝ่ายทรัพยากรบุคคล ผู้อำนวยการฝ่าย/สำนัก ที่กำกับดูแลงานที่มี การว่าจ้างหน่วยงานภายนอก

#### 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 หรือ จริยธรรม รวมทั้งไม่มีประวัติในการบุกรุก แก๊ง ทำลาย หรือโจรกรรมข้อมูลในระบบเทคโนโลยีสารสนเทศมาก่อน และมีคุณสมบัติตามที่ รพม. กำหนด
  - 1.2 การกำหนดเงื่อนไขการจ้างงาน (Terms and conditions of employment) การว่าจ้างให้มีเงื่อนไขการจ้างงานให้ครอบคลุมในเรื่องดังต่อไปนี้
    - 1.2.1 กำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศอย่างเป็นลายลักษณ์อักษร (Information security roles and responsibilities) แก่ผู้ใช้งาน โดยกำหนดให้สอดคล้องกับนโยบายความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของ รพม.
    - 1.2.2 กำหนดให้มีการลงนามในสัญญาว่าจะไม่เปิดเผยความลับของ รพม. (Non-Disclosure Agreement: NDA)

- 1.2.3 ระบบเทคโนโลยีสารสนเทศที่สร้างหรือพัฒนาโดยผู้ใช้งานในระหว่างการว่าจ้างถือเป็นสินทรัพย์ของ รพม.
- 1.2.4 กำหนดความรับผิดชอบหรือบทลงโทษ หากผู้ใช้งานไม่ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รพม. รวมทั้ง กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
2. การสร้างความมั่นคงปลอดภัยในระหว่างการจ้างงาน (During employment) เพื่อสร้างความตระหนักแก่ผู้ใช้งานเกี่ยวกับภัยที่เกี่ยวข้องกับการปฏิบัติงานสารสนเทศ รวมถึงให้ความรู้เพื่อให้สามารถป้องกันภัยดังกล่าวได้
  - 2.1 หน้าที่ในการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management responsibilities)
 

ผู้บริหาร รพม. ทุกระดับชั้นมีหน้าที่สนับสนุนและส่งเสริมเรื่องดังต่อไปนี้ แก่ผู้ใช้งาน

    - 2.1.1 ประกาศนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ รพม. เป็นลายลักษณ์อักษรให้ทุกคนรับทราบและปฏิบัติตาม
    - 2.1.2 จูงใจให้ผู้ใช้งานปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ รพม.
    - 2.1.3 สร้างความตระหนักถึงความมั่นคงปลอดภัยด้านสารสนเทศที่เกี่ยวข้องกับหน้าที่ความรับผิดชอบของตนเองและของ รพม.
  - 2.2 การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่ผู้ใช้งาน (Information security awareness, education and training) การสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยอย่างสม่ำเสมอ
    - 2.2.1 ผู้ดูแลระบบต้องแจ้งเตือนภัยคุกคาม และช่องโหว่ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศแก่ผู้ใช้งานที่เกี่ยวข้อง นอกจากนี้ต้องแจ้งเตือนให้ผู้ใช้งานเพิ่มความรู้ความระวังความเสี่ยงต่าง ๆ เช่น ไวรัสมัลแวร์ เทคนิคการหลอกล่อทางจิตวิทยา (Social engineering) และช่องโหว่ทางเทคนิค เป็นต้น
    - 2.2.2 ฝทท. ต้องดำเนินการฝึกอบรม หรือประชาสัมพันธ์เพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศแก่ผู้ใช้งานเป็นประจำทุกปี
    - 2.2.3 ฝทท. ต้องแจ้งผู้ใช้งานให้ทราบ เมื่อมีการเปลี่ยนแปลงนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศของ รพม. รวมทั้งอธิบายผลกระทบจากการเปลี่ยนแปลงดังกล่าว
  - 2.3 การแจ้งเหตุการณ์ไม่ปกติ
 

ผู้ใช้งานต้องแจ้งเหตุการณ์ไม่ปกติด้านเทคโนโลยีสารสนเทศที่พบผ่านช่องทางที่ รพม. กำหนดโดยเร็วที่สุด
  - 2.4 การกำหนดบทลงโทษ
    - 2.4.1 ความรับผิดชอบตามกฎหมาย
 

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ไม่ได้ก่อให้เกิดสิทธิทางกฎหมายที่ทำให้ผู้ใช้งานพ้นผิดแม้จะได้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ และผู้ใช้งานตกลงยินยอมที่จะไม่ดำเนินการใด ๆ ทางกฎหมายต่อ รพม. ซึ่งได้ปฏิบัติตามระเบียบนี้ แต่อย่างไรก็ตามหากผู้ใช้งานกระทำการละเมิดหรือกระทำผิดตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ อาจเป็นความผิดทางวินัยและเป็นเหตุ

ให้ถูกลงโทษทางวินัยได้ รฟม. ไม่มีส่วนรับผิดชอบต่อการละเมิดทรัพย์สินทางปัญญาที่เกิดจากการใช้ระบบคอมพิวเตอร์

#### 2.4.2 การพิจารณาโทษผู้กระทำผิด

ผู้ใช้งานที่กระทำความผิด ฝ่าท. จะเพิกถอนสิทธิการใช้งานและอาจเป็นความผิดทางวินัย หรือความผิดตามกฎหมายที่เกี่ยวข้อง

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

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

เพื่อกำหนดหน้าที่ความรับผิดชอบเมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน ซึ่งรวมไปถึงการคืนทรัพย์สินและการถอดถอนสิทธิในการเข้าถึง

#### 3.1 การแจ้งการสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน

- 3.1.1 ฝ่ายทรัพยากรบุคคลต้องแจ้งให้ฝ่ายเทคโนโลยีสารสนเทศทราบทันทีหากพนักงานมีการลาออก โยกย้าย เกษียณ หรือเสียชีวิต เพื่อฝ่ายเทคโนโลยีสารสนเทศจะได้ตรวจสอบและบริหารจัดการสิทธิในการเข้าถึงระบบเทคโนโลยีสารสนเทศ
- 3.1.2 ฝ่าย/สำนัก ที่กำกับดูแลงานที่มีการว่าจ้างหน่วยงานภายนอก ต้องแจ้งให้ฝ่ายเทคโนโลยีสารสนเทศทราบทันทีในกรณีที่ผู้รับจ้างภายนอกสิ้นสุดสัญญาจ้างหรือมีการยกเลิกสัญญาจ้าง เพื่อให้ ฝ่าท. ตรวจสอบการใช้งานระบบสารสนเทศและถอดถอนสิทธิในการเข้าถึงระบบสารสนเทศของ รฟม.

#### 3.2 การคืนสินทรัพย์ของ รฟม.

ผู้ดูแลระบบต้องตรวจสอบเพื่อเรียกคืนสินทรัพย์ของ รฟม. จากผู้ใช้งาน เมื่อการสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน

#### 3.3 การถอดถอนสิทธิในการเข้าถึง

- 3.3.1 ผู้ดูแลระบบต้องถอดถอนสิทธิในการเข้าถึงของผู้ใช้งาน เมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน
- 3.3.2 การถอดถอนสิทธิในการเข้าถึงหมายถึงรวมถึง 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 กำหนดสิทธิของผู้ใช้งานและหน่วยงานภายนอกในการเข้าถึงสถานที่ โดยแบ่งแยกได้ ดังนี้
    - 5.1.1 ผู้ดูแลระบบต้องกำหนดสิทธิแก่ผู้ใช้งานที่มีสิทธิเข้า - ออก และกำหนดช่วงระยะเวลาที่มีสิทธิในการเข้า - 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 ตั้งแต่การจัดหา 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<br>2) ใช้วิธีทุบหรือบดให้เสียหาย |
| แผ่น CD/DVD            | ให้หันด้วยเครื่องทำลายเอกสาร                                                                                                                           |
| เทป                    | ใช้วิธีทุบหรือบดให้เสียหายหรือเผาทำลาย                                                                                                                 |
| ฮาร์ดดิสก์             | 1) ทำลายข้อมูลบนฮาร์ดดิสก์ตามมาตรฐาน DOD5220.22M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นการเขียนทับข้อมูลเดิมหลายรอบ<br>2) ใช้วิธีทุบหรือบดให้เสียหาย    |

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

## ส่วนที่ 5

### การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

#### วัตถุประสงค์

- เพื่อควบคุมการจัดหา พัฒนา และบำรุงรักษาระบบสารสนเทศ ให้มีการกำหนดมาตรการการรักษาความมั่นคงปลอดภัย เพื่อป้องกันความผิดพลาด สูญหาย และการเปลี่ยนแปลงแก้ไขระบบ

#### ผู้รับผิดชอบ

- ผู้บังคับบัญชา
- ผู้ดูแลระบบ

#### อ้างอิงมาตรฐาน

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

#### แนวปฏิบัติ

1. ผู้บังคับบัญชา ต้องควบคุมให้มีการกำหนดข้อตกลงและความรับผิดชอบที่เกี่ยวข้องกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศลงในสัญญากับผู้ให้บริการภายนอก โดยให้ครอบคลุมรวมถึงผู้รับจ้างช่วงด้วย
2. 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 และต้องมีการกำหนดสิทธ์การเข้าถึงระบบสารสนเทศที่พัฒนา ทดสอบ หรือใช้งานจริง ทั้งระบบสารสนเทศใหม่ และการปรับปรุงแก้ไขระบบสารสนเทศเดิม
16. ผู้ดูแลระบบต้องมีการกำหนดขั้นตอนการทดสอบระบบสารสนเทศก่อนนำไปใช้งานจริง ทั้งในกรณีปรับปรุงระบบสารสนเทศเดิมและการพัฒนาระบบสารสนเทศใหม่
17. ผู้ดูแลระบบต้องติดตั้งซอฟต์แวร์บนระบบสารสนเทศที่ให้บริการ (Production) ตามขั้นตอนที่ รพม. กำหนด และจำกัดสิทธ์การติดตั้งซอฟต์แวร์เพื่อให้ระบบสารสนเทศต่าง 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 ต้องมีการสอบทานสิทธิ์ในการเข้าถึงระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ พร้อมทั้งเพิกถอนสิทธิ์เมื่อพบเห็นสิทธิ์ที่ไม่ถูกต้องตามสิทธิ์ในการเข้าถึง (Authorization matrix)
2. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)
 

ให้มีการควบคุมการลงทะเบียนผู้ใช้งาน การบริหารจัดการรหัสผ่าน การบริหารจัดการสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศ และการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน

  - 2.1 การลงทะเบียนผู้ใช้งาน (User registration)
    - 2.1.1 ผู้ดูแลระบบต้องบริหารจัดการและควบคุมบัญชีชื่อผู้ใช้งาน (Username) มิให้มีการใช้งานบัญชีชื่อผู้ใช้งานซ้ำกัน ทั้งนี้ ในส่วนของพนักงาน/ลูกจ้าง รพม. ให้กำหนดชื่อผู้ใช้งาน (Username) ตามมาตรฐานจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ใช้ในองค์กร
    - 2.1.2 เจ้าของข้อมูลต้องเป็นผู้อนุมัติการสร้างบัญชีผู้ใช้งานชั่วคราว (Temporary user) และต้องจำกัดช่วงเวลาการใช้งานเท่าที่จำเป็น
  - 2.2 การบริหารจัดการรหัสผ่าน (User password management)
    - 2.2.1 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

#### กรณีแอปพลิเคชันที่ใช้ผ่านอุปกรณ์เคลื่อนที่ (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) ต้องไม่ใช้การรหัสผ่านโดยกระบวนการเข้าใช้งานโดยอัตโนมัติ ได้แก่ การกำหนดค่า “Remember Password” เป็นต้น
- 3) ต้องเก็บรหัสผ่านไว้เป็นความลับเฉพาะบุคคล ไม่เปิดเผยให้ผู้อื่นรับทราบ และไม่พิมพ์รหัสผ่านในลักษณะเปิดเผย เช่น พิมพ์รหัสผ่านต่อหน้าผู้ใช้งานคนอื่น เป็นต้น
- 4) ต้องไม่ใช้บัญชีชื่อผู้ใช้งานและรหัสผ่านร่วมกันกับผู้อื่น แม้ว่าบัญชีชื่อผู้ใช้งานจะได้รับการอนุญาตจากเจ้าของชื่อผู้ใช้งานบุคคลนั้นก็ตาม
- 5) ต้องเปลี่ยนแปลงรหัสผ่านเมื่อมีการแจ้งเตือนจากระบบ หรือสงสัยว่ารหัสผ่านลั่วงรู้โดยบุคคลอื่น

## 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) สิทธิ์ในการมอบหมายสิทธิ์ในการดำเนินการแทน (Assign)
  - 6) สิทธิ์ในการรับรองความถูกต้องครบถ้วนของข้อมูล (Approve/Authenticate)
  - 7) ไม่มีสิทธิ์
- 2.3.4 เจ้าของข้อมูลและผู้ดูแลระบบต้องเป็นผู้อนุมัติการให้สิทธิ์เพื่อเข้าถึงสารสนเทศหรือระบบเทคโนโลยีสารสนเทศใด 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 และการควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย
- 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 ออกจากเครื่องคอมพิวเตอร์เมื่อมีความจำเป็นต้องละทิ้งเครื่องคอมพิวเตอร์
- 3.1.4 ผู้ใช้งานต้องป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ เช่น กล้องดิจิทัล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสารโดยไม่ได้รับอนุญาต
- 3.2 การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear desk and clear screen control)
- 3.2.1 ผู้บังคับบัญชาต้องกำหนดให้มีผู้รับผิดชอบในการดูแลสถานที่ที่มีการรับ - ส่งแฟกซ์ หรือจดหมายเข้า - ออก
- 3.2.2 ผู้ใช้งานต้องออกจากระบบคอมพิวเตอร์ (Log out) ทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล

- 3.2.3 ผู้ใช้งานต้องจัดเก็บข้อมูลสำคัญแยกต่างหาก และป้องกันให้มีความปลอดภัยอย่างพอเพียง
  - 3.2.4 ผู้ใช้งานต้องนำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ
4. การควบคุมการเข้าถึงเครือข่าย (Network access control)
- ให้มีการควบคุมการใช้งานบริการเครือข่าย การควบคุมการพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอก 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 ฝพท.
- 4) ไม่อนุญาตให้พิสูจน์ตัวตนผ่านทางอินเทอร์เน็ต (Interface) การจัดการ Firewall จากระยะไกล (Remote)
- 5) ผู้ที่ได้รับการมอบหมายจาก ฝพท. เท่านั้นที่มีสิทธิ์ที่จะเปลี่ยนการตั้งค่าด้านความปลอดภัยบน Firewall
- 6) Firewall ต้องตั้งค่าให้บันทึกเหตุการณ์ด้านความมั่นคงปลอดภัย
- 7) Firewall ต้องได้รับการสอบทาน ทดสอบ และตรวจสอบอย่างสม่ำเสมอ
- 8) Firewall ต้องถูกบริหารจัดการผ่านทาง การติดต่อสื่อสารที่มีการเข้ารหัส
- 9) ต้องปิดบริการและพอร์ต (Port) ที่ไม่จำเป็นต้องใช้บน Firewall

- 10) Firewall ประเภทซอฟต์แวร์ (Software) ต้องติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายแยกต่างหาก
- 11) Firewall ต้องสามารถป้องกันตัวเองจากการโจมตี DOS (Denial of service) ได้อย่างเช่น Ping, Sweeps หรือ TCP SYN Floods เป็นต้น
- 12) ต้องใช้เวอร์ชันของซอฟต์แวร์ (Software) Firewall และระบบปฏิบัติการที่เจ้าของผลิตภัณฑ์ยังให้การสนับสนุน
- 13) ผู้ดูแล Firewall ต้องติดตามข้อมูลช่องโหว่จากผู้ให้บริการ (Vendor) 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 และกำหนดสิทธิ์ในการใช้งานโปรแกรมประเภทยูทิลิตี้เฉพาะกลุ่มคนที่มิหน้าที่รับผิดชอบ
  - 5.3.4 มีการบันทึกเหตุการณ์ (Log) การใช้งานโปรแกรมประเภทยูทิลิตี้ และต้องสอบทานจากผู้ดูแลระบบอย่างสม่ำเสมอ
  - 5.3.5 ต้องทำการเพิกถอนหรือระงับโปรแกรมประเภทยูทิลิตี้ที่ไม่จำเป็น
- 5.4 การหมดเวลาการใช้งานระบบสารสนเทศ (Session time-out)
- 5.4.1 ผู้ดูแลระบบต้องกำหนด Session time-out ของระบบเทคโนโลยีสารสนเทศที่ไม่มีการใช้งานภายในระยะเวลา 15 นาที ทั้งนี้ ถ้าระบบที่ไม่สามารถตัดการเชื่อมต่อแบบอัตโนมัติได้ กำหนดให้ใช้โปรแกรมพักหน้าจอที่ต้องใส่รหัสผ่านหรือกำหนดให้มีการล็อกหน้าจอ
  - 5.4.2 ผู้ดูแลระบบ และผู้ใช้งาน ต้องตั้งค่าให้มีโปรแกรมพักหน้าจอที่ต้องใส่รหัสผ่านสำหรับเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์แบบพกพา และเครื่องคอมพิวเตอร์แม่ข่าย ทั้งนี้

โปรแกรมพักหน้าจอกำหนดให้ป้อนรหัสผ่านหลังจากที่มีการทิ้งเครื่องดังกล่าวไว้โดยไม่มีการใช้งานเป็นเวลา 15 นาที

- 5.5 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)
  - 5.5.1 ผู้ดูแลระบบ ต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง 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 พระราชบัญญัติกฏระเบียบ ข้อบังคับที่เกี่ยวข้อง เช่น 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. ผู้ดูแลระบบต้องลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย
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 และรหัสผ่านที่มีความคาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ไม่สามารถเดาหรือเจาะรหัสได้โดยง่าย
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. อย่างเป็นลายลักษณ์อักษร
  - 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 ตรวจสอบรายงานหรือบันทึกการให้บริการของหน่วยงานภายนอกตามที่แจ้งอย่าง  
สม่ำเสมอตามสัญญาว่าจ้าง
6. ผู้ดูแลระบบ ต้องกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีหน้าที่ในการกำกับดูแล หรือ  
หน่วยงานที่เกี่ยวข้องกับการบังคับใช้กฎหมาย รวมทั้งหน่วยงานที่ควบคุมดูแลสถานการณ์ฉุกเฉินภายใต้  
สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน
7. ผู้ดูแลระบบ ต้องมีขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีความเชี่ยวชาญเฉพาะด้านหรือ  
หน่วยงานที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน
8. ผู้ดูแลระบบต้องควบคุมการเปลี่ยนแปลงของหน่วยงานภายนอกที่ส่งผลกระทบต่อการทำงานขององค์กร และ  
ต้องประเมินความเสี่ยงอย่างเหมาะสมเพื่อควบคุมผลกระทบอันเนื่องมาจากการเปลี่ยนแปลงนั้น
9. หน่วยงานภายนอกและผู้ใช้งานภายนอก ต้องใช้งานทรัพย์สินสารสนเทศของ รฟม. ด้วยความระมัดระวัง และ  
รักษาความลับของ รฟม. ไม่นำไปเปิดเผย และต้องขออนุญาตพร้อมทั้งปฏิบัติตามเงื่อนไขในการเข้าถึงระบบ  
สารสนเทศของ รฟม. ทุกครั้ง
10. หน่วยงานภายนอกและผู้ใช้งานภายนอกต้องแจ้งเหตุการณ์ไม่ปกติต่าง ๆ ด้านเทคโนโลยีสารสนเทศที่พบผ่าน  
ช่องทางที่ รฟม. กำหนดโดยเร็วที่สุด
11. หน่วยงานภายนอกและผู้ใช้งานภายนอกต้องจัดเก็บบัญชีผู้ใช้งานที่ รฟม. 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 ขีดข่วนหรือทำให้จอ 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 การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบาที่สุด 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 ในกรณีที่จำเป็นต้องได้รับการอนุญาตจากผู้บังคับบัญชาก่อนเท่านั้น
  - 2) ผู้ดูแลระบบต้องจำกัดการใช้งานอินเทอร์เน็ตเพื่อเรื่องส่วนตัวหรือที่ไม่ใช่การดำเนินงานของ รพม. ให้น้อยที่สุดเท่าที่เป็นไปได้ เช่น การระงับการเข้าถึง Website ที่ไม่จำเป็น การระงับการเข้าถึง Website ที่มีเนื้อหาต้องห้ามตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
  - 3) ผู้ดูแลระบบต้องป้องกันไม่ให้มีการรับส่งข้อมูลที่ไม่เหมาะสมจากภายนอก รพม. เช่น
    - (ก) Executable เช่น .EXE .COM เป็นต้น
    - (ข) ไฟล์ (File) เสียง เช่น AUD .WAV และ.MP3 เป็นต้น
    - (ค) ไฟล์ (File) วิดีทัศน์ 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) ผู้ดูแลระบบต้องทดสอบเส้นทางการเชื่อมต่ออินเทอร์เน็ตขององค์กรระหว่างเส้นทางที่ใช้จริงและเส้นทางสำรองอย่างน้อยปีละ 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) ส่งจดหมายอิเล็กทรอนิกส์ลวกๆ
  - (ข) ใช้เวลาในการเข้าถึงอินเทอร์เน็ตเกินความจำเป็นยกเว้นเพื่อปฏิบัติงานให้ รฟม.
  - (ค) เล่นเกม Online
  - (ง) เข้าห้องพูดคุย Online ที่ไม่ได้มีวัตถุประสงค์เพื่อปฏิบัติงานให้ รฟม.
8. ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม 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. ผู้ใช้งานต้องไม่ใช่ข้อมูลที่ชั่วร้ายในการเสนอความคิดเห็นที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของ 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 ถึงแม้จะเป็นการแสดงความคิดเห็นในนามชื่อบุคคลส่วนตัว และพึงตระหนักถึงผลกระทบที่อาจเกิดขึ้นกับ รพม. ได้
  - 19.3 ผู้ใช้งานที่ใช้สื่อสังคมออนไลน์เป็นเครื่องมือสื่อสารข้อมูลในกิจการของ รพม. หรือชื่อบุคคลที่ทำให้เข้าใจได้ว่าเป็นบุคคลในสังกัด ต้องแสดงภาพ และข้อมูลให้ถูกต้องชัดเจนในข้อมูล โปรไฟล์ (Profile) และพึงใช้ด้วยความสุภาพและมีวิจารณญาณ
  - 19.4 ผู้ใช้งานควรตั้งคำถามที่ใช้ในกรณีกู้คืนบัญชีผู้ใช้งานหรือกู้คืนรหัสผ่าน (Forgot your password) ควรเลือกใช้ข้อมูลหรือคำถามที่เป็นส่วนบุคคลและเป็นข้อมูลที่ผู้อื่นคาดเดาได้ยากเพื่อป้องกันการสุ่มคำถามจากผู้ประสงค์ร้าย
  - 19.5 ผู้ใช้งานต้องไม่ใช้ระบบอีเมลของเว็บไซต์ประเภทสื่อสังคมออนไลน์ หากจำเป็นต้องใช้จะต้องระมัดระวังในการคลิกลิงก์ที่น่าสงสัย โดยเฉพาะอีเมลแจ้งเตือนจากเว็บไซต์ต่าง ๆ ในลักษณะเชิญให้คลิกลิงก์ที่แนบมาในอีเมล ผู้ใช้งานต้องสงสัยว่าลิงก์ดังกล่าวเป็นลิงก์ที่ไม่ปลอดภัย (ลิงก์ที่ถูกสร้างมาเพื่อใช้ขโมยข้อมูลส่วนบุคคล 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 ยุยง 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 หรือส่งผลเสียให้กับบุคคล สังคม หรือ รพม.
  - 19.16.2 ผู้ใช้งานต้องไม่ส่งต่อหรือเผยแพร่ข้อมูลเรื่องบุคคลเสียชีวิต เด็กและเยาวชน ผู้สูญหาย ผู้ต้องหา เว้นเสียแต่ตรวจสอบข้อเท็จจริงแล้วและเห็นว่าเป็นประโยชน์ต่อสาธารณะ
  - 19.16.3 ผู้ใช้งานต้องไม่ส่งต่อหรือเผยแพร่ข้อมูลที่กระทบต่อสิทธิความเป็นส่วนตัว และศักดิ์ศรีความเป็นมนุษย์
- 19.17 ผู้ใช้งานต้องตั้งคำถามปอดภัยของการใช้งานสื่อสังคมออนไลน์ และระมัดระวังการถูกนำข้อมูลจากข้อบัญชีไปใช้โดยไม่เหมาะสม ผิดวัตถุประสงค์ และลักษณะการแอบอ้างโดยบุคคลอื่น
20. ผู้ใช้งานต้องใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์โดยตระหนักถึงพระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่บังคับใช้อยู่เสมอ

## ส่วนที่ 11

### การใช้งานจดหมายอิเล็กทรอนิกส์

#### วัตถุประสงค์

- เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ของ รพม. ให้มีความปลอดภัยและมีประสิทธิภาพ

#### ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

#### อ้างอิงมาตรฐาน

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

#### แนวปฏิบัติ

1. ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของ รพม. ให้เหมาะสมกับหน้าที่ความรับผิดชอบของผู้ใช้งาน รวมทั้งทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ
2. ผู้ดูแลระบบต้องกำหนดบัญชีผู้ใช้งานตามมาตรฐานจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ใช้ในองค์กร
3. ผู้ใช้งานต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ไม่ให้เกิดความเสียหายต่อ รพม. ละเมิดลิขสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น ผิดกฎหมาย ละเมิดศีลธรรม และไม่แสวงหาประโยชน์ 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<br>2) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560<br>3) ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564 | 1                         |
| Email server logs                           |                                                                                                                                                                                                                                                                                         | 1                         |
| Web application server logs                 |                                                                                                                                                                                                                                                                                         | 1                         |
| NTP server logs                             |                                                                                                                                                                                                                                                                                         | 1                         |
| DHCP server logs                            |                                                                                                                                                                                                                                                                                         | 1                         |
| IPS logs                                    |                                                                                                                                                                                                                                                                                         | 1                         |
| Firewalls logs                              |                                                                                                                                                                                                                                                                                         | 1                         |
| Routers & Switches logs                     |                                                                                                                                                                                                                                                                                         | 1                         |
| Active directory logs                       |                                                                                                                                                                                                                                                                                         | 1                         |

4. การจัดเก็บบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and monitoring)
  - 4.1 ผู้ดูแลระบบต้องมีการจัดเก็บบันทึกเหตุการณ์ (Event logs) การใช้งานระบบสารสนเทศ
  - 4.2 ผู้ดูแลระบบต้องเก็บบันทึกข้อมูล Audit log ซึ่งบันทึกกิจกรรมการใช้งานของผู้ใช้งานระบบสารสนเทศและเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยต่าง ๆ เพื่อประโยชน์ในการสืบสวน สอบสวน และเพื่อการติดตามการควบคุมการเข้าถึง

- 4.3 ผู้ดูแลระบบต้องมีการตรวจสอบข้อมูลบันทึกเหตุการณ์อย่างสม่ำเสมอ (Log review)
- 4.4 ผู้ดูแลระบบต้องไม่ลบข้อมูลล็อก (Log) หรือปิดการใช้งานการบันทึกข้อมูลล็อก (Log)
- 4.5 ผู้ดูแลระบบต้องป้องกันระบบสารสนเทศที่จัดเก็บล็อก (Log) และข้อมูลล็อก (Log) เพื่อป้องกันการเข้าถึงหรือแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต
5. การเตรียมความพร้อมกรณีฉุกเฉิน
 

เพื่อให้มีการบริหารจัดการความต่อเนื่องให้กับกระบวนการทางธุรกิจที่สำคัญขององค์กร เมื่อมีเหตุการณ์ที่ทำให้เกิดการหยุดชะงักหรือติดขัดต่อกระบวนการดังกล่าว โดยมีแนวปฏิบัติ ดังนี้

  - 5.1 ผู้ดูแลระบบต้องกำหนดระบบที่มีความสำคัญทั้งหมดขององค์กร 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 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 รฟม. 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 การเปลี่ยนแปลงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

- 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 ตู้निรภัย หรือสื่อบันทึกที่ปลอดภัย และไม่มีใครสามารถเข้าถึงได้

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

## ส่วนที่ 16

### การนำอุปกรณ์ส่วนตัวมาใช้งาน (Bring your own device)

#### วัตถุประสงค์

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

#### ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

#### อ้างอิงมาตรฐาน

- หมวดที่ 2 อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากระยะไกล (Mobile devices and teleworking)

#### แนวปฏิบัติ

1. ผู้ดูแลระบบต้องกำหนดคุณสมบัติของระบบปฏิบัติการของอุปกรณ์ส่วนตัวที่อนุญาตให้นำมาเชื่อมต่อหรือเข้าถึงระบบงานสารสนเทศของ รพม. ได้ โดยต้องเป็นระบบปฏิบัติการที่ไม่ล้าสมัย (Obsolete operating system) และยังได้รับการสนับสนุนการใช้งานจากเจ้าของผลิตภัณฑ์
2. ผู้ดูแลระบบต้องตัดการเชื่อมต่อหากระบบปฏิบัติการของอุปกรณ์ส่วนตัวที่อนุญาตให้นำมาเชื่อมต่อหรือเข้าถึงระบบงานสารสนเทศของ รพม. เกิดการล้าสมัย (Obsolete operating system) หรือเจ้าของผลิตภัณฑ์ไม่สนับสนุนการใช้งานแล้ว
3. ผู้ดูแลระบบต้องมีมาตรการป้องกันมัลแวร์ และตรวจสอบการอัปเดต Patch เวอร์ชันของระบบปฏิบัติการที่เจ้าของผลิตภัณฑ์ยังให้การสนับสนุนการใช้งาน
4. ผู้ดูแลระบบต้องไม่อนุญาตให้อุปกรณ์ที่มีการปรับแต่งการเข้าถึงระบบปฏิบัติการ (rooted/jailbroken) มาเชื่อมต่อหรือเข้าถึงระบบสารสนเทศของ รพม.
5. ผู้ดูแลระบบต้องแบ่งแยกเครือข่ายของอุปกรณ์ส่วนตัวที่นำมาเชื่อมต่อหรือเข้าถึงระบบสารสนเทศของ รพม.
6. 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