แบบ บก.๐๖

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและรายละเอียดค่าใช้จ่าย
การจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ ซื้อระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA

2. หน่วยงานเจ้าของโครงการ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

3. วงเงินงบประมาณที่ได้รับจัดสรร 4,000,000.00 บาท (สี่ล้านบาทถ้วน) รวมภาษีมูลค่าเพิ่ม

4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) ณ วันที่ 27 พฤษภาคม 2567
เป็นเงิน 3,902,887.75 บาท (สามล้านเก้าแสนสองพันแปดร้อยแปดสิบเจ็ดบาทเจ็ดสิบห้าสตางค์) รวมภาษีมูลค่าเพิ่ม

5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)
   5.1 บริษัท ไฮเท็คซ์ อินเตอร์แอคทีฟ จำกัด
   5.2 บริษัท บุ๊คโดส จำกัด
   5.3 บริษัท ทรินนิเทค จำกัด

6. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง)
   นายสว่างพงษ์ จันทพร โปรแกรมเมอร์ ระดับ 7

ขอบเขตของงานซื้อระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA

1. <u>ความเป็นมา</u>

การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย (รฟม.) เป็นหน่วยงานภาครัฐที่มีหน้าที่บริการประชาชน ซึ่งปัจจุบันห้องสมุดของ รฟม. ยังใช้เทคโนโลยีแบบเดิมที่ไม่ทันสมัยและตอบรับด้านบริการไม่สะดวกต่อผู้ใช้บริการ ดังนั้นเพื่อให้การบริการของห้องสมุดครอบคลุมในทุก ๆ ด้าน จึงต้องพัฒนาห้องสมุดอัตโนมัติเพื่ออำนวยความสะดวกต่อการให้บริการทั้งบุคคลภายในและบุคคลภายนอก รวมถึงการจัดเก็บข้อมูลบรรณานุกรม การให้บริการยืมคืน และบริการสืบค้นผ่านเครือข่ายอินเตอร์เน็ต ตลอดจนเพิ่มความสะดวกรวดเร็วและอำนวยประโยชน์ต่อผู้ใช้บริการ รฟม.

2. <u>วัตถุประสงค์</u>

2.1 เพื่อปรับปรุงระบบห้องสมุดการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย (รฟม.) ให้เป็นมาตรฐานเดียวกับห้องสมุดชั้นนำในปัจจุบัน

2.2 เพื่อให้สามารถอ่านหนังสือหรือสิ่งพิมพ์ต่าง ๆ ในห้องสมุด ผ่านอุปกรณ์เคลื่อนที่ (smart device) ในรูปแบบสื่ออิเล็กทรอนิกส์ ที่สามารถเรียกดูข้อมูลได้โดยไม่จำกัดเวลาและสถานที่ โดยให้ผู้ใช้สามารถเข้าถึงสารสนเทศได้สะดวก รวดเร็ว ลดปัญหาและอุปสรรคในการเข้าถึงแหล่งสารสนเทศ

2.3 เพื่อเป็นแหล่งความรู้ ข้อมูลอ้างอิงด้านสถิติและข้อมูลที่สำคัญและจำเป็นต่อการให้บริการแก่ประชาชนทั่วไป และหน่วยงานที่เกี่ยวข้อง

2.4 เพื่ออำนวยความสะดวกในการให้บริการแก่ผู้บริหาร พนักงาน และผู้ปฏิบัติงานให้แก่ รฟม. ที่ปฏิบัติงานอยู่ในสถานที่ต่าง ๆ สามารถใช้บริการห้องสมุดได้อย่างทั่วถึง

2.5 เพื่อให้การบริหารงานห้องสมุด มีประสิทธิภาพมากยิ่งขึ้น

3. <u>คุณสมบัติของผู้ยื่นข้อเสนอ</u>

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วน ผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

/3.7 เป็นนิติบุคคล...

3.7 เป็นนิติบุคคล ผู้มีอาชีพขายพัสดุที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ รฟม. ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

3.10 ผู้ยื่นข้อเสนอที่เสนอราคาในรูปแบบของ “กิจการร่วมค้า” ต้องมีคุณสมบัติ ดังนี้

กิจการร่วมค้าที่ผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน เว้นแต่ในกรณีกิจการร่วมค้าที่มีข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นสามารถใช้ผลงานของผู้เข้าร่วมค้ารายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงดังกล่าวจะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญามากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

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

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

3.13 ผู้ยื่นข้อเสนอจะต้องมีผลงานในประเทศไทยในลักษณะซอฟต์แวร์สำเร็จรูป (Software Package) ประเภทเดียวกันกับงานที่ประกวดราคาอิเล็กทรอนิกส์นี้ <u>โดยมีผลงานอย่างน้อย 1 สัญญา วงเงินต่อสัญญาไม่น้อยกว่า 1,000,000 บาท (หนึ่งล้านบาทถ้วน) ทั้งนี้ ต้องเป็นผลงานที่ตรวจรับสมบูรณ์แล้ว ในช่วง 5 ปีที่ผ่านมา</u> นับถึงวันยื่นเอกสารประกวดราคา และเป็นผลงานที่ผู้ยื่นข้อเสนอเป็นคู่สัญญากับส่วนราชการ/หน่วยงานตามกฎหมายว่าด้วยระเบียบบริหารราชการส่วนท้องถิ่น รัฐวิสาหกิจ หรือหน่วยงานเอกชน <u>โดยแต่ละผลงานที่ยื่นต้องมีเอกสารดังนี้</u>

1. หนังสือรับรองผลงานจากผู้ว่าจ้างที่ลงนามโดยผู้มีอำนาจ
2. ข้อกำหนดหรือขอบเขตของงาน
3. สำเนาสัญญาหรือใบสั่งซื้อ/ ใบสั่งจ้าง (ถ้ามี)

ทั้งนี้ รฟม.ขอสงวนสิทธิ์ที่จะตรวจสอบข้อเท็จจริงที่เสนอ

/4. <u>ขอบเขตการ</u>...

4. <u>ขอบเขตการดำเนินงาน</u>

4.1 ผู้ขายต้องมีทีมงานที่มีประสบการณ์ด้านการศึกษา ออกแบบ และพัฒนาระบบงาน อย่างน้อย ประกอบด้วยบุคลากรหลัก ดังนี้

4.1.1 ผู้จัดการโครงการ (Project Manager)

4.1.2 นักวิเคราะห์ระบบ (System Analyst)

4.1.3 นักพัฒนาระบบ (Developer/ Programmer/ Technical)

4.1.4 วิศวกรระบบคอมพิวเตอร์ (System Engineer)

4.1.5 นักทดสอบระบบ (Implementer/ Tester)

4.1.6 ผู้ประสานงานโครงการ (Project Coordinator)

4.2 ผู้ขายต้องศึกษา วิเคราะห์รายละเอียดความต้องการของระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA เพื่อนำมาใช้ออกแบบและพัฒนาระบบให้สอดคล้องกับความต้องการและสภาพการดำเนินงานของ รฟม. พร้อมทั้งวางแผนรายละเอียดการดำเนินงาน นำเสนอเชิงแนวคิด (Conceptual) และรายละเอียด (Detailed)

4.3 ผู้ขายต้องศึกษา วิเคราะห์ ออกแบบ กระบวนการทำงานระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA พร้อมทั้งให้คำแนะนำและข้อเสนอแนะที่มีประโยชน์ รวมถึงพัฒนาระบบสารสนเทศเพื่อสนับสนุนการปฏิบัติงานของสำนักผู้ว่าการ ตามขั้นตอนการปฏิบัติงานของงานห้องสมุด

4.4 ผู้ขายต้องจัดหาหรือพัฒนาระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA ตามผลการศึกษาวิเคราะห์รายละเอียดความต้องการของระบบฯ ตามข้อ 4.2 บนระบบเว็บไซต์ (Web Application) และแอปพลิเคชันบน Smart Device (Mobile Application)

4.5 ผู้ขายต้องจัดหา ติดตั้งและส่งมอบซอฟต์แวร์ระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA ที่สามารถปรับแต่งระบบฯ ให้สามารถทำงานได้อย่างสอดคล้องกับคุณสมบัติตามข้อกำหนดและผลการศึกษาวิเคราะห์รายละเอียดความต้องการของระบบฯ ตามข้อ 5. รวมถึงติดตั้งและส่งมอบซอฟต์แวร์อื่น ๆ ที่เกี่ยวข้องทั้งหมดของระบบฯ ดังกล่าว ตามข้อ 7. ที่มีลิขสิทธิ์ถูกต้องตามกฎหมายและมอบให้เป็นสิทธิ์การใช้งานของ รฟม.

4.6 หากมีการพัฒนาระบบเพิ่มเติมจากซอฟต์แวร์สำเร็จรูปที่จัดหา Source code ที่ได้มีการพัฒนาขึ้นเพิ่มเติมโดยเฉพาะสำหรับ รฟม. เช่น พัฒนา API เพิ่มเติมเพื่อเชื่อมโยงข้อมูลกันระหว่างระบบงาน เป็นต้น ซึ่งไม่นับรวม Source code ที่เป็นส่วนหนึ่งของระบบงาน e-Library ของผู้ขาย ส่วนที่ได้พัฒนาเพิ่มเติมนั้น รวมทั้งรายงานหรือเอกสารใด ๆ ที่ผู้ขายได้ทำขึ้นอันเนื่องมาจากการปฏิบัติงานตามสัญญานี้ ให้ตกเป็นกรรมสิทธิ์และลิขสิทธิ์ของ รฟม. ทั้งหมด อย่างไรก็ตาม ผู้ขายอาจเก็บสำเนารายงานและเอกสารอื่นดังกล่าวไว้เพื่อเป็นประวัติการทำงานของผู้ขายเองได้

4.7 ผู้ขายต้องศึกษา วิเคราะห์ ขั้นตอนกระบวนงาน เอกสาร และข้อมูลที่เกี่ยวข้องกับงานเชื่อมโยงข้อมูลของระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA โดยให้จัดทำรายงานอย่างน้อย 2 ส่วน ดังนี้

4.7.1 รายงานภาพรวมการเชื่อมโยงของแต่ละกระบวนงาน และรายงานอธิบายของกระบวนงาน (Business Architecture) เช่น ชื่อกระบวนการ (Business Process Name) ผู้เกี่ยวข้องในแต่ละงาน (Who) เอกสารและข้อมูลที่ใช้ในแต่ละกระบวนงาน (Input/ Output) วิธีการและเครื่องมือที่ใช้ (Method and Tools) เป็นต้น และถ้ากระบวนการนั้นสามารถแตกย่อยได้ให้แตกกระบวนการย่อยให้ชัดเจน

/4.7.2 รายงาน...

4.7.2 รายงานอธิบายข้อมูล (Data Architecture) เช่น ชื่อข้อมูล คุณลักษณะข้อมูล ชนิดของข้อมูล ประเภทข้อมูล และถ้าข้อมูลนั้นสามารถแตกย่อยได้ ให้แตกย่อยรายละเอียดข้อมูลให้ชัดเจน ทั้งนี้ การตั้งชื่อและการอธิบายความ ต้องใช้ภาษาที่ผู้เกี่ยวข้องที่ไม่มีความรู้ด้านไอซีทีสามารถเข้าใจได้ (Non - IT staff understandable)

4.8 ผู้ขายต้องพัฒนาโดยเชื่อมโยงข้อมูลระหว่างระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA กับระบบสารสนเทศของ รฟม. ทั้งที่ใช้งานอยู่ในปัจจุบันและรองรับการเชื่อมโยงข้อมูลกับระบบของ รฟม. ที่จะเกิดขึ้นในอนาคต เพื่อให้สามารถเชื่อมโยงข้อมูลสารสนเทศระหว่างระบบได้โดยอัตโนมัติ เมื่อระบบมีการร้องขอข้อมูลสารสนเทศที่เกี่ยวข้อง

4.9 ผู้ขายต้องดำเนินการโอนย้ายหรือนำเข้าข้อมูลที่เกี่ยวข้องเข้าสู่ฐานข้อมูลของระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA

4.10 ผู้ขายต้องทดสอบ ตรวจสอบคุณภาพการทำงาน รวมถึงปรับแต่งการทำงานและเงื่อนไขต่าง ๆ ของระบบฯ ให้สอดคล้องกับภารกิจบทบาทหน้าที่ และแนวทางการปฏิบัติของ รฟม. และระบบอื่น ๆ ที่เกี่ยวข้องได้เป็นอย่างดี โดยหากพบว่าระบบทำงานได้ไม่สมบูรณ์ ต้องปรับปรุงระบบ เพื่อให้ระบบสามารถทำงานได้อย่างสมบูรณ์ โดยไม่คิดค่าใช้จ่ายเพิ่มเติม

4.11 ผู้ขายต้องออกแบบ พัฒนา ติดตั้ง และทดสอบระบบที่เสนอ เพื่อให้ระบบ Firewall ระบบ Antivirus ระบบ Backup Data และระบบอื่น ๆ ที่ รฟม. มีและใช้งานอยู่ปัจจุบัน ทำงานร่วมกันได้อย่างมีประสิทธิภาพ

4.12 ผู้ขายต้องติดตั้งและส่งมอบซอฟต์แวร์ที่ใช้ในการวิเคราะห์และตรวจสอบคุณภาพของโค้ดรุ่นล่าสุดที่มีขายตามท้องตลาด อย่างน้อยในระดับ Developer ซึ่งสามารถตรวจสอบ Source Code ได้อย่างน้อย 1 ล้านบรรทัดต่อปี และโปรแกรมควบคุมเวอร์ชันของโค้ด (Source Code Version Control) รุ่นล่าสุดที่มีขายตามท้องตลาด อย่างน้อยในระดับ Enterprise จำนวน 8 License โดยสามารถใช้งานร่วมกับระบบที่เสนอได้ จนกว่าจะสิ้นสุดระยะเวลาของโครงการ โดยคณะกรรมการตรวจรับพัสดุได้ตรวจรับงานและตกลงรับมอบงานทั้งหมดที่ถูกต้องครบถ้วนเป็นที่เรียบร้อยแล้ว พร้อมสิทธิ์การใช้งานและมีลิขสิทธิ์ถูกต้องครบถ้วนตามกฎหมาย เพื่อให้ใช้งานกับระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA และสามารถทำงานบนระบบปฏิบัติการ ตามข้อ 4.12 ได้อย่างมีประสิทธิภาพ

4.13 ผู้ขายต้องไม่เปิดเผยข้อมูลอันเป็นความลับใด ๆ หรือข้อมูลอื่นใดทั้งหมดหรือบางส่วนที่ได้รับหรือรับรู้มาจาก รฟม. ให้ผู้อื่นทราบโดยมิได้รับความยินยอมจาก รฟม. และต้องควบคุม กำกับไม่ให้ผู้ปฏิบัติงานของผู้ขาย เปิดเผยข้อมูลอันเป็นความลับใด ๆ หรือข้อมูลอื่นใดทั้งหมดหรือบางส่วนที่ได้รับหรือรับรู้มาจาก รฟม. ให้ผู้อื่นทราบเช่นกัน หากมีความเสียหายต่อ รฟม. ผู้ขายต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นทั้งหมด

4.14 ผู้ปฏิบัติงานของผู้ขายทุกคนต้องลงนามในสัญญาว่าจะไม่เปิดเผยความลับของ รฟม. (Non-Disclosure Agreement: NDA) ก่อนเริ่มปฏิบัติงานให้ รฟม.

4.15 ผู้ขายต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รฟม. ตามภาคผนวก ก. หากผู้ขายไม่ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยฯ จนก่อให้เกิดความเสียหาย รฟม. ขอสงวนสิทธิ์ในการเรียกร้องค่าเสียหายอันเนื่องมาจากการไม่ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยดังกล่าว

/4.16 ผู้ขาย...

4.16 ผู้ขายต้องวิเคราะห์และปิดช่องโหว่ (Hardening) ของระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA และซอฟต์แวร์ที่ใช้ในการพัฒนาระบบ หากซอฟต์แวร์นั้น ๆ มีการประกาศช่องโหว่ รวมทั้งช่องโหว่ที่ รฟม. ตรวจพบ โดยปิดช่องโหว่ที่มีระดับความรุนแรงในระดับวิกฤติ (Critical) และระดับสูง (High) ครบทุกช่องโหว่ พร้อมส่งมอบเอกสารในงานงวดสุดท้าย

4.17 ผู้ขายต้องพัฒนาและออกแบบระบบโดยคำนึงถึงการรักษาความมั่นคงปลอดภัยสารสนเทศให้มีความปลอดภัยตามมาตรฐาน Open Web Application Security Project (OWASP) Top 10 ล่าสุด หรือมาตรฐาน Common Weakness Enumeration (CWE) Top 25 สำหรับ Web Application และ OWASP Mobile Top 10 สำหรับ Mobile Application ล่าสุด ณ ปีที่ส่งมอบงาน นับถัดจากวันลงนามในสัญญา หรือมาตรฐานที่ยอมรับในสากล หรือกำหนดซอฟต์แวร์ให้เป็นเวอร์ชันล่าสุดที่ได้รับการอัปเดตแล้ว

4.18 ผู้ขายต้องตรวจสอบความมั่นคงปลอดภัยของ Source Code (Source Code Review) ตามมาตรฐานที่ รฟม. กำหนด

4.19 ผู้ขายต้องทดสอบประสิทธิภาพการให้บริการในการตอบสนองการเรียกใช้งาน (Response Time) ของระบบฯ และ รฟม. จะทำการทดสอบประสิทธิภาพ Response Time บนเครือข่ายที่ รฟม. กำหนด โดยผลการทดสอบให้เป็นไปตามระยะเวลาที่ รฟม. กำหนด นับแต่ผู้ใช้ระบบส่งคำร้องขอข้อมูลและได้รับการแสดงผลบนหน้าจอของระบบ

4.20 ผู้ขายต้องดำเนินการการทดสอบสมรรถภาพและประสิทธิภาพของระบบ (Performance Test) บนเครือข่ายที่ รฟม. กำหนด โดยให้รองรับผู้ใช้งานพร้อมกันได้อย่างน้อย 1,000 คน พร้อมส่งมอบเอกสารในงานงวดสุดท้าย

4.21 ผู้ขายต้องดำเนินกระบวนการควบคุมเวอร์ชัน (Version Control) และ Source Code เมื่อมีการเปลี่ยนแปลง การแก้ไขระบบต่าง ๆ โดยส่งมอบเอกสารในงานงวดสุดท้าย

4.22 ผู้ขายต้องกำหนดสิทธิ์การเข้าถึงระบบที่แตกต่างกันในแต่ละระดับ (Role Matrix) โดยครอบคลุมถึงระบบงานย่อยทั้งหมด รวมถึง User กลุ่มต่าง ๆ ด้วย เช่น System User โดยส่งมอบเอกสารในงานงวดสุดท้าย

4.23 ผู้ขายต้องจัดทำคลิปวิดีโอการใช้งานระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA และระบบที่พัฒนาในโครงการนี้ เพื่อจัดทำเป็นฐานความรู้สำหรับการใช้งานระบบฯ โดยรองรับความละเอียดภาพขนาดไม่น้อยกว่า 1280 x 720 พิกเซล และส่งมอบเอกสารในงานงวดสุดท้าย

4.24 แอปพลิเคชันอย่างเป็นทางการบน Store ของทั้ง 2 ระบบปฏิบัติการ ได้แก่ ระบบปฏิบัติการ iOS และระบบปฏิบัติการ Android ให้ผู้ใช้ทั่วไปสามารถดาวน์โหลดแอปพลิเคชันได้จากผู้ให้บริการดาวน์โหลดแอปพลิเคชันเหล่านั้น ผู้ขายต้องเป็นผู้รับผิดชอบค่าใช้จ่ายที่เกี่ยวข้องทั้งหมด

4.25 ผู้ขายต้องจัดทำการปิดบังข้อมูลส่วนบุคคล รวมถึงข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) ด้วยวิธี Data Masking ข้อมูลที่แสดงในระบบฯ และเข้ารหัสข้อมูล (Encryption) ในฐานข้อมูลตามที่ รฟม. กำหนด

/5. <u>ข้อกำหนด</u>...

5. ข้อกำหนดของระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA

5.1 คุณลักษณะทั่วไปของระบบ

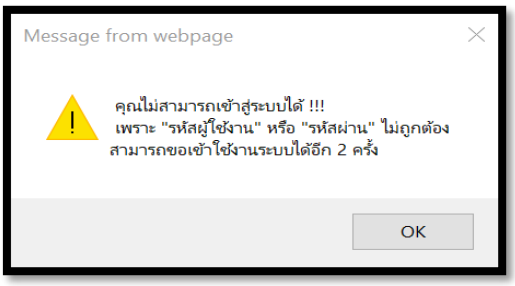
5.1.1 คุณลักษณะด้านเทคนิคของระบบ

5.1.1.1 รองรับการเชื่อมต่อกับระบบ Active Directory (AD) ที่ รฟม. ใช้งานอยู่สำหรับผู้ใช้งานที่เป็นพนักงานและผู้ปฏิบัติงานให้แก่ รฟม.

5.1.1.2 การเชื่อมต่อกับระบบ Active Directory (AD) จะต้องสามารถตรวจสอบจำนวนครั้งที่อนุญาตให้เข้าสู่ระบบผิดพลาด ดังนี้

- แสดงให้ผู้ใช้งานทราบว่า สามารถเข้าสู่ระบบผิดพลาดได้ไม่เกินกี่ครั้ง
- แสดงให้ผู้ใช้งานทราบว่า เข้าสู่ระบบผิดพลาดไปแล้วกี่ครั้ง
- แสดงให้ผู้ใช้งานทราบว่า กรณีเข้าสู่ระบบผิดพลาดเกินจำนวนครั้งที่กำหนดมีขั้นตอนดำเนินการแก้ไขอย่างไร

ตัวอย่างการแสดงข้อความเข้าสู่ระบบผิดพลาด



5.1.1.3 ระบบต้องมีการจัดการปลดล็อคผู้ใช้งานที่เข้าสู่ระบบผิดพลาด ในระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA เช่น กรณีที่ระบบ Active Directory (AD) ของ รฟม. (ระบบกลาง) จะกำหนดจำนวนครั้งการเข้าใช้งานระบบผิดพลาดไว้จำนวน 5 ครั้ง แต่ในระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA จะให้กำหนดการเข้าใช้งานระบบผิดพลาดไว้จำนวน 3 ครั้ง เพื่อให้ผู้ดูแลระบบดำเนินการปลดล็อคผู้ใช้งานในตัวระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTAได้เอง ก่อนที่จะล็อคที่ระบบ Active Directory (AD) ของ รฟม. (ระบบกลาง)

5.1.1.4 ส่วนการใช้งานบน Web Browser ระบบมีลักษณะเป็น Web Based Application ผ่านโปรโตคอล Https (Hypertext Transfer Protocol Secure) พร้อมติดตั้ง SSL ให้กับ รฟม. ด้วย

5.1.1.5 ระบบรองรับการทำงานของเว็บเบราว์เซอร์ได้อย่างน้อย 3 เว็บเบราว์เซอร์ เช่น Google Chrome, Mozilla Firefox, Microsoft Edge และเป็นเวอร์ชันที่ รฟม. ใช้งานอยู่ในปัจจุบัน โดยไม่ต้องลงโปรแกรมเสริมเพิ่มเติมเป็นอย่างน้อย รวมถึงระบบปฏิบัติการ IOS และ Android เช่น Safari และ Chrome เป็นต้น

5.1.1.6 ส่วนการใช้งานบน Smart Device ระบบมีลักษณะเป็น Mobile Application ซึ่งมีให้ดาวน์โหลดอย่างเป็นทางการบน Store โดยรองรับระบบปฏิบัติการ iOS และระบบปฏิบัติการ Android เป็นอย่างน้อย

/5.1.1.7 ระบบ...

5.1.1.7 ระบบรองรับการแสดงผลได้อย่างเหมาะสมบนอุปกรณ์ที่หลากหลาย (Responsive Web Design) เช่น คอมพิวเตอร์ แล็ปท็อป แท็บแล็ต หรือโทรศัพท์มือถือ เป็นอย่างน้อย และต้องแสดงผลได้อย่างเหมาะสมตามคุณลักษณะ ขนาด และความละเอียดของหน้าจอแสดงผล (Screen Size and Resolution)

5.1.1.8 ระบบรองรับการเชื่อมโยงข้อมูลกับระบบสารสนเทศที่ รฟม. ใช้งานอยู่ได้ในรูปแบบของ Web Service เช่น ระบบบริหารทรัพยากรบุคคล (HR) ในการเชื่อมโยงข้อมูลโครงสร้างองค์กร ข้อมูลพนักงาน เป็นต้น

5.1.1.9 ระบบรองรับการกำหนด Session Timeout ทันทีที่ผู้ใช้งาน Log out ออกจากระบบและกรณีที่ผู้ใช้งานไม่ได้มีการใช้งานระบบเกินกว่า 15 นาที ระบบจะ Logout โดยอัตโนมัติ และกรณีที่ผู้ใช้งานได้มีการ Log in ผ่านอุปกรณ์อื่นเพิ่มเติม

5.1.1.10 ระบบมีการตรวจสอบการเข้าใช้งานด้วยชื่อผู้ใช้งานเดียวกันพร้อมกัน ระบบจะให้ผู้ใช้งานที่เข้าใช้งานก่อน ทำการ Logout โดยอัตโนมัติ (Session Logout)

5.1.1.11 ระบบมีการตรวจสอบความถูกต้องของข้อมูลนำเข้า (Input Validation) ก่อนการบันทึกและ/หรือประมวลผลข้อมูล รวมทั้งตรวจสอบข้อมูลที่ส่งออกจากระบบ (Output Validation) เพื่อป้องกันการแสดงผลหรือการประมวลผลข้อมูลที่ไม่เหมาะสม

5.1.1.12 ระบบมีการตรวจสอบสิทธิในการเข้าถึงข้อมูล และสามารถแสดงข้อความแจ้งเตือนได้ (Authentication Testing)

5.1.1.13 สามารถกำหนดสิทธิ์การใช้งานระบบฯ ตามบทบาท (Role) และสามารถจัดกลุ่ม (Group) ผู้ใช้งานในแต่ละระดับของ Function ได้ พร้อมเปลี่ยนแปลงสิทธิ์ต่าง ๆ โดยผู้มีอำนาจหรือผู้มีสิทธิ์

5.1.1.14 สามารถบันทึกเหตุการณ์ (Log) ได้อย่างน้อยดังนี้

- ค้นหา แสดงผล และพิมพ์ประวัติการให้สิทธิ์ การเปลี่ยนแปลงสิทธิ์ การเพิกถอนสิทธิ์การใช้งานของผู้ใช้งานนั้น ๆ (History Role - based access control) และสามารถพิมพ์ออกเป็นรายงานได้
- ค้นหา แสดงผล และพิมพ์ประวัติการเข้าใช้งานระบบ (Transaction Log) รวมถึงการเพิ่มข้อมูล การแก้ไขข้อมูล การลบข้อมูล วัน เวลา และหมายเลขประจำเครื่องคอมพิวเตอร์ (IP Address) ในรูปแบบที่กำหนด เช่น PDF Excel CSV ได้

5.1.1.15 สามารถส่งข้อมูลบันทึกเหตุการณ์ (Log) ตามข้อ 5.1.1.13 ไปยังซอฟต์แวร์บันทึกเหตุการณ์ภายนอก (ArcSight Log Server) ของ รฟม. ได้

5.1.2 คุณลักษณะด้านการใช้งานของผู้ใช้งาน

5.1.2.1 ผู้ใช้งานซึ่งเป็นพนักงาน และผู้ปฏิบัติให้แก่ รฟม. จะต้องสามารถเข้าใช้งานด้วย Username และรหัสผ่าน ที่มีอยู่บนระบบ Active Directory (AD) ได้

5.1.2.2 ผู้ใช้งานทั่วไป ระบบรองรับการสมัครสมาชิกด้วยอีเมล (E-mail) แบบไม่จำกัดหรือเฉพาะ Domain โดยใช้ อีเมล (E-mail) เป็นชื่อผู้ใช้งาน (Username) ในการเข้าระบบ โดยจะต้องทำการเปิดการใช้งานระบบ (Activate) ผ่านอีเมล (E-mail) ก่อนจึงจะสามารถใช้งานได้

/5.1.2.3 ระบบ...

5.1.2.3 ระบบรองรับการเพิ่มผู้ใช้งาน (User) โดยผู้ดูแลระบบ (Admin) สามารถทำรายการผ่านหน้า Web Application ได้ระบบรองรับการค้นหา (Search) ข้อมูลตามคำสำคัญ (Keyword) ได้

5.1.2.4 ระบบรองรับการปิดการใช้งานของผู้ใช้งาน (Inactivate User) โดยผู้ดูแลระบบ (Admin) สามารถทำรายการผ่านหน้า Web Application ทั้งนี้ ระบบจะยังคงข้อมูลต่าง ๆ ของผู้ใช้งาน (User) ท่านนั้นไว้ในระบบเพื่อใช้ในการจัดทำสถิติ และรายงานอื่น ๆ ต่อได้

5.1.2.5 ระบบรองรับการลืมรหัสผ่าน (Forgot Password) สำหรับผู้ใช้งานทั่วไป

5.2 ระบบจัดการกำหนดสิทธิ์ (Authorization)

5.2.1 ระบบรองรับการกำหนดสิทธิ์ของผู้ใช้ (User Roles) ได้หลายระดับ เช่น สมาชิก (Member Staff) ผู้ดูแลระบบ (Admin) และสามารถมีผู้ดูแลระบบ (Admin) ได้มากกว่าหนึ่งคน

5.2.2 ระบบรองรับการจัดกลุ่มของผู้ใช้งาน (User) และกำหนดสิทธิ์ในการเข้าใช้งานแยกตามกลุ่มได้

5.2.3 สามารถกำหนดสิทธิ์การเข้าถึงหมวดหมู่ของระบบ โดยผู้ดูแลระบบกับกลุ่มผู้ใช้ได้

5.3 ระบบแสดงผลบนเว็บไซต์ (Website)

5.3.1 เมนูของระบบรองรับ 2 ภาษา คือ ภาษาไทยและภาษาอังกฤษ โดยมีปุ่มเปลี่ยนภาษา

5.3.2 มีหน้าเว็บแสดงรายการสื่ออิเล็กทรอนิกส์ถูกแนะนำโดยผู้ดูแลระบบ (Recommended)

5.3.3 มีหน้าเว็บแสดงรายการทั้งหมดของสื่ออิเล็กทรอนิกส์แต่ละชนิด เช่น ไฟล์ PDF E-Book หนังสือเสียง โดยแสดงภาพหน้าปก โดยสามารถแยกแสดงตามหมวดหมู่ (Category) และสามารถเรียงลำดับ (Sort) ตามชื่อผู้แต่ง ชื่อเรื่อง หรือวันที่ได้

5.3.4 มีส่วนแสดงข้อมูลที่ได้รับความนิยม (All-time, Monthly)

5.3.5 มีหน้าแสดงรายละเอียดข้อมูลต่าง ๆ เช่น ชื่อข้อมูล ชื่อผู้แต่ง เนื้อหาโดยย่อ หมวดหมู่ จำนวนหน้า เป็นต้น

5.3.6 มีฟังก์ชันการแชร์ข้อมูลไปยังสื่อสังคมออนไลน์ (Social) ต่าง ๆ ได้แก่ เฟสบุ๊ก (Facebook) ทวิตเตอร์ (Twitter) อีเมล (E-mail)

5.3.7 สามารถเรียกดูสื่ออิเล็กทรอนิกส์ที่อยู่หมวดหมู่เดียวกัน ผู้แต่ง (Author) หรือ หัวเรื่อง (Subject) เดียวกันได้

5.3.8 หน้าแสดงรายละเอียดข้อมูลสามารถแสดงข้อมูล MARC ของสื่ออิเล็กทรอนิกส์นั้นได้

5.3.9 สามารถเลือกรูปแบบการแสดงผลข้อมูลได้ทั้งรูปแบบรายการ (List) และรูปแบบแบบชั้นหนังสือ (Grid) ได้

5.3.10 สามารถให้คะแนน (Rating) สื่ออิเล็กทรอนิกส์นั้น ๆ ได้

5.3.11 กรณีการยืมเข้าชั้นหนังสือส่วนตัวต้องทำการเข้าลงชื่อเข้าระบบใช้งานระบบ (Login) ก่อน

/5.3.12 มีการ...

5.3.12 มีการแสดงสถานะของสื่ออิเล็กทรอนิกส์ เช่น สามารถยืมอ่านได้ (Add to my bookshelf) สามารถอ่านได้ทันทีกรณียืมไว้ที่ชั้นหนังสือส่วนตัวแล้ว (Read this book) จองคิวการอ่าน (Reserve-waiting list)

5.3.13 มีส่วนแสดงประวัติการยืม-จองส่วนตัวของสมาชิกแต่ละคน

5.3.14 มีหน้าแสดงข้อมูลผู้ใช้ (User Profile) สามารถแก้ไขข้อมูล ได้แก่ รูปโปรไฟล์ อีเมล (E-mail) ชื่อ นามสกุล เบอร์โทรศัพท์

5.3.15 มีชั้นหนังสือส่วนตัวสำหรับสมาชิก ที่แสดงรายการสื่ออิเล็กทรอนิกส์ ที่ถูกยืมไว้ สามารถเรียงลำดับ (Sort) ตามวันที่ที่ทำการยืมสื่ออิเล็กทรอนิกส์ หรือชื่อเรื่องได้ และสามารถแยกชั้นตามประเภทของสื่ออิเล็กทรอนิกส์ได้

5.4 ระบบแสดงผลบน Mobile Application

5.4.1 สามารถใช้งานกับอุปกรณ์ระบบ iOS (อุปกรณ์ iPad/iPhone) และ ระบบ Android OS (Smart Phone/Tablet) เวอร์ชันปัจจุบันได้

5.4.2 มีการแจ้งเตือนให้อัปเดตเมื่อมีเวอร์ชันใหม่

5.4.3 มีส่วนแสดงรายการสื่ออิเล็กทรอนิกส์ที่แนะนำโดยผู้ดูแลระบบ (Recommended)

5.4.4 มีหน้าแสดงรายการสื่ออิเล็กทรอนิกส์ทั้งหมดโดยแสดงภาพหน้าปก สามารถเรียงลำดับทรัพยากร (Sort) ตามผู้แต่ง ชื่อเรื่อง และวันที่ลงรายการได้

5.4.5 มีหน้าแสดงรายละเอียดสื่ออิเล็กทรอนิกส์ (หนังสือเล่มและอีบุ๊ก) โดยแสดงข้อมูล ได้แก่ ชื่อ ชื่อผู้แต่ง เนื้อหาโดยย่อ หมวดหมู่ จำนวนหน้า

5.4.6 มีฟังก์ชัน Social network sharing เพื่อแชร์ไปยังสื่อสังคมออนไลน์ (Social) ต่าง ๆ ได้แก่ เฟสบุ๊ก (Facebook) ทวิตเตอร์ (Twitter) และอีเมล (E-mail)

5.4.7 สามารถให้คะแนน (Rating) สื่ออิเล็กทรอนิกส์นั้น ๆ ได้

5.4.8 มีหน้าแสดงประวัติการยืม-จองคืนส่วนตัวของสมาชิกแต่ละคน

5.4.9 มีหน้าชั้นหนังสือส่วนตัวสำหรับสมาชิก แสดงรายการสื่ออิเล็กทรอนิกส์ที่ถูกยืมไว้ โดยเชื่อมโยงสถานะ (Synchronize) กับชั้นวางหนังสือส่วนตัวบนเว็บไซต์ (Website) และสามารถเรียงลำดับ (Sort) รายการตาม วันที่ยืม และชื่อเรื่องได้

5.5 ระบบสืบค้น

5.5.1 สามารถสืบค้นด้วยการสแกนเลขที่รหัสสื่ออิเล็กทรอนิกส์ (ISBN) ด้วยระบบบน Mobile Application

5.5.2 สามารถสืบค้นข้อมูลสื่ออิเล็กทรอนิกส์ ได้ทั้งคำค้นภาษาไทยและคำค้นภาษาอังกฤษ

5.5.3 สามารถสืบค้นแบบเร็วได้โดยการพิมพ์คำค้นได้ทันที

/5.5.4 สามารถ...

5.5.4 สามารถสืบค้นโดยระบบค้นหาขั้นสูง (Advanced search) โดยสามารถเลือกค้นหาแบบเจาะจงประเภทสื่ออิเล็กทรอนิกส์ คำค้น (Keyword) ชื่อหนังสือ (Book Name) ชื่อหัวข้อ (Title) ชื่อผู้แต่ง (Author) ชื่อเรื่อง (Subject) เลขที่รหัสสื่ออิเล็กทรอนิกส์ (ISBN) สำนักพิมพ์ (Publisher) รายละเอียด (Description)

5.5.5 สามารถแสดงผลการสืบค้นในรูปแบบหน้าปกและชื่อหนังสือได้

5.5.6 มีระบบช่วยค้นหาที่เมื่อพิมพ์คำค้นในช่องค้นหาจะแสดงรายการรายละเอียด (List) ชื่อเรื่องที่เกี่ยวข้องกับคำค้นนั้นโดยอัตโนมัติ (Auto complete)

5.6 ระบบจัดการผู้ใช้ (User Management)

5.6.1 สามารถนำเข้าข้อมูลผู้ใช้ด้วยไฟล์ Excel ได้ ตามแบบฟอร์มที่ รฟม. กำหนด

5.6.2 สามารถค้นหาและดูข้อมูลพื้นฐานต่าง ๆ ของผู้ใช้ได้

5.6.3 สามารถแบ่งกลุ่มผู้ใช้ได้

5.6.4 สามารถแก้ไข เพิ่ม ลบ ข้อมูลผู้ใช้ได้

5.6.5 สามารถกำหนดนโยบายการใช้งานได้ตามกลุ่มผู้ใช้

5.7 ระบบบริหารจัดการหนังสือเล่ม

5.7.1 การแสดงผลบนเว็บไซต์ (Website) เพิ่มเติม

- มีการแสดงสื่ออิเล็กทรอนิกส์ ได้แก่ หนังสือ นิตยสาร แผ่นซีดี แผ่นดีวีดี Flash drive
- แสดงหมวดหมู่เมนูหลัก เช่น หนังสือ นิตยสาร แผ่นซีดี แผ่นดีวีดี Flash drive เป็นต้น โดยแยกกันอย่างชัดเจน
- มีส่วนแสดงจำนวนฉบับ (Copy) ของสื่ออิเล็กทรอนิกส์ และรายละเอียดอื่น ๆ ได้แก่ สถานะ บาร์โคด เลขเรียกหนังสือ (Call number)

5.7.2 การแสดงผลบน Mobile Application เพิ่มเติม

- แสดงหมวดหมู่เมนูหลัก เช่น หนังสือ นิตยสาร แผ่นซีดี แผ่นดีวีดี เป็นต้น โดยแยกกันอย่างชัดเจน
- กรณีการจองสื่ออิเล็กทรอนิกส์ต้องทำการเข้าใช้งานระบบ (Login) ก่อน
- มีส่วนแสดงจำนวนฉบับ (Copy) ของสื่ออิเล็กทรอนิกส์ และรายละเอียดอื่น ๆ ได้แก่ สถานะ บาร์โคด เลขเรียกหนังสือ (Call number)

/5.7.3 ระบบ...

5.7.3 ระบบการจองหนังสือเล่ม

- สามารถจองหนังสือผ่านเว็บไซต์ (Website) และ Mobile Application ได้โดยมีการแจ้งเตือนไปยังผู้ดูแลระบบ (Admin) ผ่านอีเมล (E-mail) และแจ้งเตือน (Notification) ที่ระบบหลังบ้านเพื่อให้ทำการอนุมัติการจอง
- กรณีการจองได้รับการอนุมัติ จะมีการแจ้งเตือน (Notification) ไปยังผู้ใช้ทางอีเมล (E-mail) และแสดงแจ้งเตือน (Push Notification) เพื่อให้มารับหนังสือ นั้น ๆ เมื่อถึงคิว
- มีการแสดงสถานะการจองโดยแสดงจำนวนผู้จอง และสถานะจะเปลี่ยนเป็นถูกยืมเมื่อผู้จองมารับหนังสือนั้น ๆ ที่ห้องสมุด ในกรณีที่ผู้จองไม่มารับหนังสือในเวลาที่กำหนด สถานะการจองจะถูกยกเลิกอัตโนมัติ

5.7.4 การยืม-คืนและต่ออายุ

- มีระบบให้บริการยืม – คืน หนังสือหรือสื่ออิเล็กทรอนิกส์ของห้องสมุด ที่ใช้กับเครื่องอ่านบาร์โค้ด รวมถึงต้องจัดหาเครื่องอ่านบาร์โค้ดที่ใช้กับคอมพิวเตอร์ของ รฟม. และระบบงานนี้ได้จำนวน 1 เครื่อง
- สามารถต่ออายุการยืมได้เมื่อครบกำหนด โดยกดฟังก์ชันเลื่อนการคืนได้ผ่านเว็บไซต์ (Website) และ Mobile Application
- มีระบบการแจ้งเตือนไปยังผู้ยืมผ่าน Push ก่อนวันครบกำหนดการคืน เมื่อถึงวันกำหนดคืน และเมื่อเกินกำหนดการคืน

5.7.5 การกำหนดนโยบายการใช้บริการทรัพยากรในห้องสมุดแบบแยกประเภท สามารถกำหนดนโยบายการใช้บริการทรัพยากรในห้องสมุดโดยผู้ดูแลระบบ แยกตามประเภททรัพยากร โดยผูกกับกลุ่มผู้ใช้ ดังนี้

- จำนวนการยืมทรัพยากรสูงสุดที่สามารถยืมได้ต่อคน (Number of max borrow)
- จำนวนวันในการยืมทรัพยากรต่อครั้ง (Number of rental day)
- ค่าธรรมเนียมในการยืมทรัพยากรครั้งแรก (Rental fee (First period))
- ค่าปรับเกินกำหนดต่อวัน (Overdue fee (per day))
- จำนวนครั้งที่สามารถต่ออายุการยืมได้ (Renewal time)
- จำนวนวันที่ได้รับสำหรับการต่ออายุการยืมต่อครั้ง (Renewal period)
- จำนวนทรัพยากรสูงสุดที่สามารถจองได้ต่อคน (Number of max reserve)
- จำนวนวันที่ต้องเข้ามารับทรัพยากรหลังจากได้รับการ อนุมัติการจอง (Number of max reserve day)

/5.7.6 การลง...

5.7.6 การลงระเบียน (Cataloging)

- ระบบลงรายการอัตโนมัติโดยการนำเข้าไฟล์นามสกุล .mrc จากแหล่งอื่นได้
- ระบบลงรายการอัตโนมัติด้วยการค้นหาระเบียนหนังสือด้วย ISBN จากระบบฐานข้อมูลกลางที่จัดไว้ให้
- สามารถสร้างและบันทึกระเบียน (Bibliographic Record) เช่น รายละเอียดเลขหมู่หนังสือ ผู้แต่ง ผู้แต่งร่วม ผู้แปล ชื่อชุดหนังสือ ตาม Format มาตรฐาน MARC 21 ได้
- ระบบสามารถลงรูปภาพปกหนังสือได้

5.7.7 การพิมพ์ Utility

- สามารถพิมพ์บาร์โค้ดได้
- สามารถพิมพ์เลขเรียกหนังสือได้ (Call Number)
- สามารถแสดงตัวอย่างบาร์โค้ด และเลขเรียกหนังสือก่อนพิมพ์ได้
- ระบบพิมพ์ซ่อมโดยกำหนดตำแหน่งของบาร์โค้ดหรือเลขเรียกหนังสือได้บนกระดาษ A4 แบบ Grid 27 ช่อง (3x9 ช่อง)
- สามารถพิมพ์ด้วยเครื่องพิมพ์ปกติ โดยพิมพ์ลงบนสติ๊กเกอร์มาตรฐานได้ (5.5cm x 3cm)
- มีวัตถุดิบเพื่อรองรับการพิมพ์ลงบนสติ๊กเกอร์ได้อย่างน้อย 20,000 ชิ้น

5.7.8 ระบบรายงานการวิเคราะห์ มีฟังก์ชันดังนี้

<u>จำนวนผู้ใช้ทั้งหมด (User)</u>

- รายงานสรุปเชิงกราฟิก (Chart Reports)
- จำนวนหนังสือทั้งหมด (Book)
- จำนวนแมกกาซีนทั้งหมด (Magazine)
- จำนวนซีดี/ดีวีดีทั้งหมด (CD/DVD)
- จำนวน Flash drive ทั้งหมด
- หนังสือที่มียอดจองสูงสุด 20 อันดับ (Popular reserve)
- จำนวนทรัพยากรแยกตามประเภท (Number of books separate by type)
- สถิติการลงทะเบียนแยกตามอุปกรณ์ (User registration separate by device)
- สถิติการ Login แยกตามอุปกรณ์ (User login by device)
- จำนวนทรัพยากรแยกตามหมวดหมู่ (Number of book separate by category)
- สถิติทรัพยากรที่ถูกยืมมากที่สุด (20 Popular borrowing)
- สถิติคำที่ถูกค้นหามากที่สุด (20 Popular search word)

/<u>รายงานเชิง</u>...

<u>รายงานเชิงตาราง (Table Reports)</u>

สรุปตามตามช่วงเวลาที่กำหนดได้ (รายวัน รายเดือน รายปี) และสามารถ Export เป็นไฟล์ Excel ได้

- สมาชิกที่ยืมมากที่สุด (Top Borrowers)
- หมวดหมู่ที่นิยมมากสุด (Top Popular Categories)
- ทรัพยากรที่นิยมมากสุด (Top Popular Items)
- จำนวนการลงรายการทรัพยากรแบ่งตามประเภทแสดงแบบรายเดือน (Cataloging Summary)
- สถิติการยืม-คืนแยกแสดงแบบรายเดือน (Circulation Summary)
- สถิติการยืมเกินเวลา (Overdue Item Rating)
- รายการทรัพยากรที่ไม่ถูกยืมเลย (Not Borrow Items)
- รายการทรัพยากรใหม่ (New Resources)
- รายงานค่าปรับ (Fine Report)
- รายงานแสดงสถานะของทรัพยากร (Resource Status)
- รายงานการ Login (Login Summary)
- รายงานผู้เข้าชมระบบ (View Number)
- รายงานแสดงผู้เข้าชมทรัพยากรแต่ละรายการ (View per Resource)
- รายงานสรุปการยืม-คืน (Transaction)
- สามารถเลือกดูตามรหัสหนังสือ (Book Barcode) ชื่อหนังสือ (Book Title) ชื่อ (User First Name) นามสกุล (User Last) อีเมล (E-mail) หรือทั้งหมดได้
- สามารถเลือกดูตามวันที่ยืมได้
- สามารถเลือกดูตามวันที่คืนได้
- สามารถ Export เป็นไฟล์ Excel ได้
- รายงานสรุปการจอง (Reservation)
- สามารถเลือกดูตามรหัสหนังสือ (Book Barcode) ชื่อหนังสือ (Book Title) ชื่อ (User First Name) นามสกุล (User Last) อีเมล (E-mail) หรือทั้งหมดได้
- สามารถเลือกดูตามสถานะการจอง (Status Reserved) สถานะการอนุมัติการจอง (Approved), สถานะการส่งคืน (Delivered) สถานะการยกเลิก (Canceled) หรือทั้งหมดได้

/5.8 ระบบ...

5.8 ระบบบริหารจัดการหนังสืออีบุ๊ค (E-Library)

5.8.1 การแสดงผลบนเว็บไซต์ (Website) เพิ่มเติม

- มีหน้าการแสดงข้อมูลต่าง ๆ ได้แก่ สื่อหนังสือ (E-Book) สื่อแมกกาซีน (E-Magazine) สื่อดีวีดี, (Video clip) เอกสารดิจิทัล, ฐานข้อมูลออนไลน์
- การอ่านสื่อหนังสือ (E-Book) แบบออนไลน์ (Online) บนเว็บไซต์ (Website)
- สามารถพลิกอ่านได้เหมือนหนังสือจริง
- มีการแสดงสารบัญแบบภาพย่อ (Thumbnail)
- สามารถย่อขยายได้
- สามารถค้นหาคำในสื่อหนังสือ (E-Book) ได้ โดยต้นฉบับสื่อหนังสือ (E-Book) จะต้องเป็นชนิดที่ค้นหาได้ (Searchable file)

5.8.2 การแสดงผลบน Mobile Application

- แสดงหมวดหมู่เมนูหลักเช่น สื่อหนังสือ (E-Book) สื่อแมกกาซีน (E-Magazine) สื่อดีวีดี (Video clip) เอกสารดิจิทัล ฐานข้อมูลออนไลน์ แยกกันอย่างชัดเจน
- กรณีการดาวน์โหลด (Download) ได้ต้องทำการเข้าใช้ระบบระบบ (Login) ก่อน
- สามารถแสดงแสดงตัวอย่าง (Preview) ของสื่อหนังสือ (E-Book) สื่อแมกกาซีน (E-Magazine) ได้
- มีส่วนแสดงจำนวนทรัพยากรที่สามารถยืมได้ เช่น ไม่จำกัดจำนวน (Unlimited) สามารถยืมพร้อมกันได้ 1 คน (Only 1 more copies) ไม่สามารถยืมได้เนื่องจากมีคนยืมไปแล้ว (Out of library shelf) เป็นต้น
- มีส่วนแสดงสถานะของสื่อต่าง ๆ เช่น สถานะสามารถยืมอ่านได้ (Add to my Bookshelf) สถานะสามารถอ่านได้ทันทีกรณียืมไว้ที่ชั้นหนังสือส่วนตัวแล้ว (Read this Book) สถานะจองคิวการอ่าน (Reserve Waiting List)

5.8.3 การอ่านสื่อหนังสือ (E-Book) บน Mobile Application

- สามารถดาวน์โหลดสื่อหนังสือ (E-Book) มาอ่านแบบออฟไลน์ (Offline) ได้
- สามารถลบสื่อต่าง ๆ ออกจากอุปกรณ์ก่อนถึงกำหนดเวลาคืน
- สามารถเรียกคืนสื่อต่าง ๆ ได้อัตโนมัติเมื่อถึงกำหนดเวลาคืนได้
- มีฟังก์ชันคั่นหนังสือ (Bookmark) หน้าที่ต้องการและใส่โน้ตได้
- มีฟังก์ชันแชร์สื่อต่าง ๆ ไปยังสื่อสังคมออนไลน์ (Social) อย่าง เฟสบุ๊ก (Facebook) ทวิตเตอร์ (Twitter) อีเมล (E-mail) ได้
- มีการแสดงสารบัญแบบภาพย่อ (Thumbnail)
- สามารถย่อขยายด้วยนิ้วสัมผัส
- มีระบบป้องกันการบันทึกภาพหน้าจอในบางเมนูได้

/5.8.4 การสร้าง...

5.8.4 การสร้างสื่อหนังสือ (E-Book)

- รองรับการสร้างสื่อหนังสือ (E-Book) ผ่าน Web browser โดยไม่จำกัด IP Address และผู้ช้งาน (User Admin)

- ในการลงรายการระเบียนครั้งเดียว สามารถใช้งานบน Web browser และ Mobile Application ได้

- มีระบบการรักษาความปลอดภัยของการจัดเก็บข้อมูลต้นฉบับ PDF ด้วยการเข้ารหัส

- สามารถสร้างสื่อหนังสือ (E-Book) ได้จากไฟล์ต้นฉบับนามสกุล pdf

- สามารถนำเข้าไฟล์นามสกุล epub

5.8.5 การนำเข้าไฟล์เอกสารดิจิทัล มัลติมีเดีย และสื่ออื่น ๆ

- สามารถนำเข้าไฟล์เอกสารนามสกุล jpg, jpeg, png, txt, docx, xlsx, และ pptx โดยผู้อ่านสามารถดาวน์โหลดลงเครื่องได้

- สามารถสร้างช่องทางเชื่อมต่อ ฐานข้อมูลออนไลน์ เพื่อลิงก์ (Link) ไปที่เว็บฐานข้อมูลออนไลน์ต่าง ๆ ได้

- รองรับการจัดเก็บไฟล์วีดิโอ (VDO) ในรูปแบบนามสกุล mp4 หรือระบุเป็นลิงก์ (Link) จาก Youtube

- รองรับการจัดเก็บไฟล์เสียง ในรูปแบบนามสกุล mp3 ได้

5.8.6 การจองสื่อหนังสือ (E-Book)

- สามารถจองทรัพยากรผ่านเว็บไซต์ (Website) และ Mobile Application ได้

- สามารถกำหนดจำนวนการยืมพร้อมกัน (Concurrence) สำหรับทรัพยากรที่มีลิขสิทธิ์ได้

- ก่อนทำการจอง สามารถแสดงจำนวนคิวผู้จองของทรัพยากรนั้น ๆ ได้

- หลังทำการจอง จะแสดงลำดับคิวการจองที่ได้รับ

- กรณีถึงคิวที่ได้รับ ระบบจะแจ้งเตือนไปยังผู้ใช้ผ่านทางอีเมล (E-mail) และแสดงแจ้งเตือน (Push Notification) เพื่อให้ทำการยืมทรัพยากรนั้น ๆ

- กรณีที่ผู้จองไม่ทำการกดยืมในเวลาที่กำหนด สถานะการจองจะถูกยกเลิกอัตโนมัติ

5.8.7 การยืม-คืน

- สามารถยืมทรัพยากรได้ด้วยการดาวน์โหลดเข้าชั้นหนังสือส่วนตัว (My Bookshelf)

- สามารถคืนทรัพยากรที่ทำการยืมมาแล้ว ด้วยการลบออกจากชั้นส่วนตัว

- มีระบบการคืนอัตโนมัติเมื่อถึงกำหนด และสามารถคืนได้แบบอัตโนมัติแม้ไม่ได้ต่ออินเตอร์เน็ต

- มีระบบการแจ้งเตือนไปยังผู้ยืมผ่านทางทางอีเมล (E-mail) และแสดงแจ้งเตือน (Push Notification) ก่อนวันครบกำหนดการคืน และเมื่อถึงกำหนดคืน

/5.8.8 การกำหนด...

5.8.8 การกำหนดนโยบายการจอง-ยืม-คืน

- สามารถกำหนดนโยบายการจอง-ยืม-คืน โดยผู้ดูแลระบบ แยกตามประเภททรัพยากร โดยผูกกับกลุ่มผู้ใช้ ดังนี้
  - จำนวนการยืมทรัพยากรสูงสุดที่สามารถยืมได้ต่อคน (Number of max borrow)
  - จำนวนวันในการยืมทรัพยากรต่อครั้ง (Number of rental day)
  - จำนวนทรัพยากรสูงสุดที่สามารถจองได้ต่อคน (Number of max reserve)
  - จำนวนวันที่ต้องเข้ามากดรับทรัพยากรเมื่อถึงลำดับคิว (Number of max reserve day)

5.8.9 การลงระเบียน

- สามารถสร้างและบันทึกระเบียน (Bibliographic Record) เช่น ชื่อหนังสือ ชื่อผู้แต่ง ชื่อสำนักพิมพ์ จำนวนหน้า หมวดหมู่
- ระบบสามารถลงรูปภาพปกหนังสือได้

5.8.10 ระบบรายงานการวิเคราะห์ มีฟังก์ชันดังนี้

- รายงานสรุปเชิงกราฟิก (Dashboard)
- จำนวนผู้ใช้ทั้งหมด (Users)
- จำนวนหนังสือทั้งหมด (E-Books)
- จำนวนแมกกาซีนทั้งหมด (E-Magazine)
- จำนวนวิดีโอคลิปทั้งหมด (Multimedia)
- จำนวนเอกสารอิเล็กทรอนิกส์ทั้งหมด (Information)
- จำนวนยอดดาวน์โหลดทั้งหมด (Download)
- หนังสือที่มียอดจองสูงสุด 20 อันดับ (Popular reserve)
- จำนวนทรัพยากรแยกตามประเภท (Number of books separate by type)
- สถิติการลงทะเบียนแยกตามอุปกรณ์ (User registration separate by device)
- สถิติการ Login แยกตามอุปกรณ์ (User login by device)
- จำนวนทรัพยากรแยกตามหมวดหมู่ (Number of book separate by category)
- จำนวนวีดีโอคลิปแยกตามหมวดหมู่ (Number of VDO separate by category)
- สถิติทรัพยากรที่ถูกยืมมากที่สุด (Popular download)
- รายงานเชิงตาราง ที่สรุปตามตามช่วงเวลาที่กำหนดได้ (รายวัน รายเดือน รายปี) และสามารถ Export เป็นไฟล์ Excel ได้
- รายการทรัพยากรที่ถูกดาวน์โหลด (Download Report)
- รายการทรัพยากรที่ถูกจอง (Reserve Report)
- สถิติการดาวน์โหลดของสมาชิก (User Download Report)
- สมาชิกที่มีการดาวน์โหลดมากที่สุด (User Top Readers Report)
- รายงานการเข้าใช้ระบบของสมาชิก (User Login Report)
- รายการทรัพยากรทั้งหมด (Export all book)

/5.9 ระบบ...

5.9 ระบบบริหารจัดการข่าวและบทความ

5.9.1 การแสดงผลบนเว็บไซต์และแอปพลิเคชัน

- ข้อมูลเชื่อมโยงเป็นข้อมูลเดียวกันระหว่างเว็บไซต์และแอปพลิเคชัน
- มีพื้นที่แสดงข่าวใหม่ในหน้าแรก และหน้าแสดงข่าวทั้งหมดในรูปแบบ Timeline (คล้าย Facebook)
- รองรับบทความความรู้ออนไลน์แบบมีลิขสิทธิ์และไม่มีลิขสิทธิ์
- สามารถค้นหาข่าวหรือบทความความรู้ได้
- มีส่วนแสดงข่าวหรือบทความความรู้แนะนำ ข่าวหรือบทความความรู้ยอดนิยม
- สามารถกดเข้าดูรายละเอียดของข่าวหรือบทความความรู้ได้
- มีพื้นที่ให้สมาชิกแสดงความคิดเห็นได้และมีการกดถูกใจได้

5.9.2 การสร้างและการจัดการข่าวและบทความ

- สามารถสร้างและจัดการหมวดหมู่ของข่าวหรือบทความความรู้ได้
- สามารถสร้างข่าวหรือบทความความรู้โดยการใส่ ข้อมูล รูปภาพ วีดีโอ และลิงค์ได้
- สามารถตั้งให้แสดง/ไม่แสดง ลบ รวมถึงการปักหมุดข่าวหรือบทความความรู้ได้
- สามารถดูตัวอย่างก่อนโพสท์ข่าวหรือบทความความรู้ได้
- สามารถตั้งค่าให้ข่าวหรือบทความความรู้เป็นรายการแนะนำได้
- สามารถบันทึกค่าไว้ล่วงหน้าและกำหนดเวลาเผยแพร่ได้

5.10 ระบบประชาสัมพันธ์สื่อต่าง ๆ ข่าว และบทความในระบบ

5.10.1 สามารถประชาสัมพันธ์สื่อต่าง ๆ ข่าว และบทความที่มีในระบบผ่าน LINE Group โดยผู้ใช้สามารถคลิกไปที่ทรัพยากรนั้นๆ ได้ทันที

5.10.2 สามารถประชาสัมพันธ์สื่อต่าง ๆ ข่าว และบทความที่มีในระบบผ่านอีเมล (E-mail) โดยผู้ใช้สามารถคลิกไปที่สื่อต่าง ๆ ข่าว และบทความนั้นๆ ได้ทันที

5.10.3 สามารถประชาสัมพันธ์สื่อต่าง ๆ ข่าว และบทความที่มีในระบบผ่านแสดงแจ้งเตือน (Push Notification) โดยผู้ใช้สามารถคลิกไปที่สื่อต่าง ๆ ข่าว และบทความนั้น ๆ ได้ทันที

5.11 ระบบการจัดการหนังสือเสียง (Audiobook)

5.11.1 มีระบบบริหารจัดการในการสร้างหนังสือเสียง (Audiobook) จากไฟล์ mp3 ได้

5.11.2 รองรับการกำหนด (Concurrence)

5.11.3 สามารถจัดหมวดหมู่สำหรับหนังสือเสียง (Audiobook) ได้

5.11.4 รองรับหนังสือเสียง (Audiobook) ลิขสิทธิ์จากสำนักพิมพ์

/5.11.5 สามารถ...

5.11.5 สามารถฟังหนังสือเสียง (Audiobook) บนเว็บไซต์ (Website) และ Mobile Application

5.11.6 สามารถเล่นหนังสือเสียง (Audiobook) ในขณะพักหน้าจอได้ เฉพาะ Mobile Application

5.11.7 ผู้ขายต้องจัดหา Microphone ตัดเสียงสำหรับอัดเสียงเพื่อจัดทำสื่อหนังสือเสียง จำนวน 1 ชิ้น

5.12 ระบบการให้แต้มและแลกของรางวัล

5.12.1 ผู้ใช้สามารถได้รับแต้มแบบอัตโนมัติ จากกิจกรรมหล่านี้

- เข้าดูหน้ารายละเอียดทรัพยากร
- ยืมทรัพยากร
- จองทรัพยากร
- คืนทรัพยากรไม่เกินกำหนดเวลา (เฉพาะหนังสือเล่ม, ซีดี/ดีวีดี)
- ให้คะแนนในทรัพยากร
- แชร์ทรัพยากรผ่านสื่อสังคมออนไลน์ (Social)
- อ่านข่าวหรือบทความความรู้
- แสดงความคิดเห็นในข่าวหรือบทความความรู้
- กดถูกใจข่าวหรือบทความความรู้
- แชร์ข่าวหรือบทความความรู้ผ่านสื่อสังคมออนไลน์ (Social)

5.12.2 ผู้ดูแลระบบสามารถกำหนด

- รายการของรางวัลและแต้มที่ใช้แลก
- หมวดหมู่ของรางวัล
- การแจ้งเตือนแบบแสดงแจ้งเตือน (Push Notification) เมื่อผู้ใช้มีแต้มขั้นต่ำตามที่กำหนด
- ยกเลิกการแลกของรางวัลและคืนแต้มให้กับผู้ใช้ได้

5.12.3 ผู้ใช้สามารถทำการแลกของรางวัลผ่านระบบได้ โดยระบบจะทำการตัดแต้มออกอัตโนมัติ

- ผู้ดูแลระบบสามารถเรียกดูรายงานต่าง ๆ เหล่านี้ได้
- ประวัติการแลกของรางวัล
- ประวัติการได้รับแต้ม
- ของรางวัลที่ได้รับความนิยม
- รายการผู้ใช้งาน

5.12.4 ผู้ใช้งานสามารถเรียกดูรายงานต่าง ๆ เหล่านี้ได้

- ประวัติการแลกของรางวัล
- ประวัติการได้รับแต้ม

/5.13 ชั้นวางหนังสือ...

5.13 ชั้นวางหนังสือดิจิทัล (Digital Bookshelf) พร้อมระบบการจัดการบนตู้ให้บริการดิจิทัล (Digital Signage Kiosk)

5.13.1 มีส่วนแสดงชั้นหนังสืออิเล็กทรอนิกส์บนตู้ดิจิทัล (Digital Signage Kiosk)

5.13.2 สามารถแสดง บาร์โค้ด หรือคิวอาร์โค้ด ให้สแกนเพื่อยืม (ยกเว้นหนังสือเล่ม) หรือจองได้

5.13.3 มีส่วนแสดงหนังสือแนะนำในแต่ละหมวด

5.13.4 ขนาดจอแสดงผลของ Digital Signage Kiosk มีขนาด 55 นิ้ว แนวตั้ง สามารถทัชสกรีนได้ และมีความละเอียดในระดับ Full HD (1920 x 1080 พิกเซล) เป็นอย่างน้อย

5.13.5 Digital Signage Kiosk จะต้องมีลักษณะเป็นหน้าจอ Touch Screen

5.13.6 เครื่องประมวลผลสำหรับเครื่อง Digital Signage Kiosk ที่ใช้ระบบปฏิบัติการ Windows ระบบปฏิบัติการ Android หรือระบบปฏิบัติการอื่น ๆ โดยมีคุณลักษณะดังนี้

5.13.6.1 ใช้ระบบปฏิบัติการที่มีลิขสิทธิ์ถูกต้อง และเป็นเวอร์ชันล่าสุด ที่ให้บริการอยู่ในท้องตลาด นับถึงวันยื่นเอกสารประกวดราคา

5.13.6.2 มีหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า 4 Core และความเร็วของหน่วยประมวลผลพื้นฐานต้องไม่น้อยกว่า 1.8 GHz หรือดีกว่า

5.13.6.3 มีหน่วยความจำหลัก (RAM) ที่มีขนาดไม่น้อยกว่า 4GB

5.13.6.4 มีหน่วยจัดเก็บข้อมูล (Hard Disk) ขนาดความจุไม่น้อยกว่า 64 GB (กรณีใช้ระบบปฏิบัติการ Windows) หรือไม่น้อยกว่า 32 GB (กรณีใช้ระบบปฏิบัติการอื่น) จำนวน 1 หน่วย

5.14 เนื้อหาลิขสิทธิ์ (Content)

5.14.1 ระบบสามารถรองรับสื่อหนังสือ (E-Book) และสื่อแมกกาซีน (E-Magazine) ลิขสิทธิ์จากสำนักพิมพ์ในท้องตลาดได้ และมีการเข้ารหัสความปลอดภัยต้นฉบับ (Digital Right Management: DRM) มาตรฐาน 256 bit

5.14.2 มีสัญญาหรือหนังสือแต่งตั้งตัวแทนจำหน่ายเนื้อหาดิจิทัล (Digital Content) เช่น สื่อหนังสือ (E-Book) สื่อแมกกาซีน (E-Magazine) อย่างถูกต้องกับสำนักพิมพ์ชั้นนำทั้งภาษาไทยและภาษาอังกฤษ

5.14.3 ผู้ขายต้องสามารถจัดหาสื่อหนังสือ (E-Book) ที่มีลิขสิทธิ์จากสำนักพิมพ์ชั้นนำ โดยแสดงเป็นรายการให้การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย (รฟม.) เลือก และแสดงสัญญาการได้รับสิทธิให้นำต้นฉบับสื่อหนังสือ (E-Book) มาบริหารจัดการในระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA อย่างถูกต้อง

5.14.4 ผู้ขายต้องสามารถจัดหาสื่อแมกกาซีน (E-Magazine) ไม่น้อยกว่า 5 รายชื่อ ที่มีลิขสิทธิ์จากสำนักพิมพ์ชั้นนำ โดยแสดงเป็นรายการให้การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย (รฟม.) เลือก และแสดงสัญญาการได้รับสิทธิให้นำต้นฉบับมาบริหารจัดการในระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA อย่างถูกต้อง

5.14.5 ผู้ขายจะต้องจัดหา e-Book เนื้อหาที่มีลิขสิทธิ์อย่างน้อย 1,000 เล่ม และไม่มีลิขสิทธิ์อย่างน้อย 1,000 เล่ม ให้แก่ รฟม. โดยอย่างน้อย 500 เล่ม ของเนื้อหาที่มีลิขสิทธิ์ จะต้องมีปีที่ตีพิมพ์ไม่น้อยกว่าปี พ.ศ. 2563

/6. <u>ระยะเวลา</u>...

6. ระยะเวลาการดำเนินงาน

ระยะเวลาการดำเนินงาน 270 วัน (สองร้อยเจ็ดสิบวัน) นับถัดจากวันลงนามในสัญญา

7. สิ่งที่ต้องดำเนินการ และกำหนดเวลาส่งมอบพัสดุ

7.1 สิ่งที่ต้องดำเนินการ

7.1.1 ผู้ขายต้องจัดให้มีการประชุมเริ่มงานโครงการ (Kick off Project) โดยให้บุคลากรตามรายชื่อที่เสนอเข้าร่วมการประชุมในวันดังกล่าวด้วย พร้อมจัดส่งรายละเอียดแผนการดำเนินงานของโครงการฯ ในระดับสัปดาห์ ระบุกิจกรรม บุคคลรับผิดชอบ ความสัมพันธ์ระหว่างงานแต่ละงวด ส่งมอบงาน พร้อมข้อเสนอแนะ ให้แก่ รฟม. ภายใน 15 วัน นับถัดจากวันลงนามในสัญญา

7.1.2 ผู้ขายต้องจัดส่งรายงานผลการประชุมเริ่มงานโครงการ (Kick off Project) ให้แก่ รฟม. พิจารณาและให้ความเห็นชอบภายใน 15 วัน นับถัดจากวันประชุมเริ่มงานโครงการ (Kick off Project)

7.1.3 ผู้ขายต้องจัดส่งรายงานความก้าวหน้าการดำเนินงาน (Progress Report) โดยนำเสนอความคืบหน้าของการดำเนินงาน ปัญหาและอุปสรรค แนวทางการแก้ไข และแนวทางการดำเนินงานต่อไป ให้แก่ รฟม. ทุก ๆ ระยะ 90 วันนับถัดจากวันลงนามในสัญญา ตลอดจนเสร็จสิ้นการดำเนินงานงวดสุดท้าย (งานงวดที่ 3)

7.1.4 ผู้ขายต้องจัดให้มีการประชุมนำเสนอความก้าวหน้าการดำเนินงาน (Progress) ตามข้อ 7.1.3 ให้แก่ รฟม. ทุก ๆ งวดงาน ตลอดจนเสร็จสิ้นการดำเนินงานงวดสุดท้าย (งานงวดที่ 3)

7.1.5 ผู้ขายต้องจัดทำเอกสารอธิบายกระบวนการควบคุมเวอร์ชัน (Version Control) และ Source Code เมื่อมีการเปลี่ยนแปลง การแก้ไขระบบต่าง ๆ และจัดส่งเอกสารดังกล่าวให้แก่ รฟม. ในงานงวดสุดท้าย (งานงวดที่ 3)

7.1.6 ผู้ขายต้องจัดทำบัญชีทะเบียนทรัพย์สินสารสนเทศ (Asset Inventory) และจัดส่งเอกสารดังกล่าวให้แก่ รฟม. ในงานงวดสุดท้าย (งานงวดที่ 3)

7.1.7 ผู้ขายต้องแจ้งกำหนดเวลาส่งมอบระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA ที่ติดตั้งแล้วเสร็จพร้อมใช้งาน โดยก่อนส่งมอบระบบฯ ดังกล่าว ผู้ขายจะต้องแจ้งเป็นหนังสือให้ รฟม. ทราบล่วงหน้าเป็นเวลาไม่น้อยกว่า 5 วันทำการ

7.1.8 ผู้ขายต้องแจ้งกำหนดแผนงานฝึกอบรม พร้อมจัดส่งเอกสารประกอบการฝึกอบรม ให้แก่ รฟม. พิจารณาและให้ความเห็นชอบก่อนอบรมอย่างน้อย 14 วัน โดยจะต้องจัดเตรียมเอกสารประกอบการฝึกอบรมให้เพียงพอต่อจำนวนผู้เข้ารับการฝึกอบรม

7.1.9 ผู้ขายต้องจัดส่งบุคลากรมาประจำ รฟม. จำนวน 1 คน เพื่อสนับสนุนการใช้งานระบบฯ (Go Live Support) เป็นระยะเวลา 60 วัน นับถัดจากวันที่ได้ดำเนินการติดตั้งและส่งมอบระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA และคณะกรรมการตรวจรับพัสดุได้ตรวจรับงานและตกลงรับมอบงานทั้งหมดโดยถูกต้องครบถ้วนเป็นที่เรียบร้อยแล้ว หรือ ตามวันที่ รฟม. กำหนด โดยบุคลากรที่จัดส่งมานั้นจะต้องเป็นหนึ่งในบุคลากรหลักที่เป็นผู้ร่วมในการดำเนินงานโครงการ

/7.1.10 ในช่วง...

7.1.10 ในช่วงระยะเวลา Go Live Support (60 วัน) ผู้ขายจะต้องจัดส่งรายงานความก้าวหน้าการปฏิบัติงาน สรุปการประเมินผลการทำงานของระบบงาน และสรุปปัญหาที่เกิดขึ้นพร้อมวิธีการแก้ไขปัญหา (ถ้ามี) ทุก ๆ ระยะ 30 วัน ตลอดระยะเวลา 60 วันนับแต่วันที่เริ่มจัดส่งบุคลากรมาประจำ รฟม.

7.1.11 ผู้ขายต้องจัดส่งบุคลากรเข้ามา รฟม. ทุก ๆ ระยะ 60 วัน ตลอดระยะเวลารับประกันการใช้งาน นับตั้งแต่วันที่ได้ดำเนินการติดตั้งและส่งมอบระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA และคณะกรรมการตรวจรับพัสดุได้ตรวจรับงานและตกลงรับมอบงานทั้งหมดโดยถูกต้องครบถ้วนเป็นที่เรียบร้อยแล้ว หรือ ตามวันที่ รฟม. กำหนด เพื่อบำรุงรักษาเชิงป้องกัน (Preventive Maintenance) และดูแลให้ระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA สามารถทำงานได้อย่างมีประสิทธิภาพ และให้คำปรึกษาเกี่ยวกับระบบ พร้อมจัดทำรายงานสรุปผลการดำเนินงาน และสรุปปัญหาที่เกิดขึ้นพร้อมวิธีการแก้ไขปัญหา (ถ้ามี)

7.1.12 ผู้ขายจะต้องส่งบุคลากรเข้าร่วมการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness) เพื่อสร้างความตระหนักที่เหมาะสม รวมถึงทบทวนนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ และขั้นตอนปฏิบัติของ รฟม.

7.2 กำหนดเวลาส่งมอบพัสดุ

งานงวดที่ 1 ส่งมอบภายใน 90 วัน นับถัดจากวันลงนามในสัญญา

ลำดับ	งานที่ต้องส่งมอบ
1	รายงานการศึกษา วิเคราะห์ ออกแบบ และสรุปความต้องการของระบบงานปัจจุบัน (AS-IS) (System Requirement Specification) ของระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA พร้อมรูปแบบแผนภาพผังการทำงาน (Business Blueprint) โดยมีแผนภาพแสดงลำดับขั้นตอนการทำงานตาม Business Process Model and Notation (BPMN 2.0) ภาคผนวก ข.
2	รายงานความก้าวหน้าการดำเนินงาน (Progress Report) เล่มที่ 1 (90 วัน)

งานงวดที่ 2 ส่งมอบภายใน 180 วัน นับถัดจากวันลงนามในสัญญา

ลำดับ	งานที่ต้องส่งมอบ
1	รายงานการศึกษา วิเคราะห์ ออกแบบ และสรุปการปรับกระบวนงานใหม่ที่มีความเหมาะสม (To-Be Process) ของระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA รวมทั้งการออกแบบภาพรวมการเชื่อมต่อระหว่างระบบ ตามมาตรฐาน Unified Modeling Language (UML) ดังต่อไปนี้เป็นอย่างน้อย - แผนภาพการออกแบบภาพบริบทของระบบ (System Context) - แผนภาพ Use Case Diagram และ Use Case Description - แผนภาพสรุปการออกแบบฟังก์ชันของระบบงาน (Class Diagram) - แผนภาพผังการทำงาน (Business Blueprint) โดยมีแผนภาพแสดงลำดับขั้นตอนการทำงานตาม Business Process Model and Notation (BPMN 2.0) ภาคผนวก ข.

/2 นำเสนอ...

ลำดับ	งานที่ต้องส่งมอบ
2	นำเสนอการแสดงผลต้นแบบ (Prototype) ของ ระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA - เอกสารการออกแบบหน้าจอการทำงาน (Screen Layout) พร้อมขั้นตอนการทำงานสำหรับแต่ละหน้าจอ การรับและแสดงผล การตอบโต้กับผู้ใช้ (User Interface) - เอกสารการออกแบบหน้าจอรายงาน (Report Layout)
3	เอกสารการออกแบบฐานข้อมูล (Database Schema) และเอกสารอธิบายรายละเอียดข้อมูล (Data Dictionary) ที่มีการออกแบบไว้เบื้องต้นก่อนเริ่มพัฒนาระบบ
4	นำเสนอระบบที่ได้ออกแบบตามต้นแบบ (Prototype) ด้วยเครื่องมือ เช่น Figma (180 วัน)
5	รายงานความก้าวหน้าการดำเนินงาน (Progress Report) เล่มที่ 2 (180 วัน)

งานงวดที่ 3 ส่งมอบภายใน 270 วัน นับถัดจากวันลงนามในสัญญา

ลำดับ	งานที่ต้องส่งมอบ
1	ติดตั้งและส่งมอบซอฟต์แวร์ตรวจสอบ Source code (Source Code Review) และซอฟต์แวร์ควบคุม Source Code (Source Code Control) ตามข้อ 4.12 รวมถึงซอฟต์แวร์อื่น ๆ ที่เกี่ยวข้องทั้งหมดของระบบ ที่มีลิขสิทธิ์ถูกต้องตามกฎหมายและเป็นสิทธิ์การใช้งานของ รฟม.
2	ติดตั้งและส่งมอบระบบงาน พร้อมซอสโค้ดโปรแกรม (Source code) ที่ได้มีการพัฒนาขึ้น (ในกรณีที่มีการพัฒนาระบบ) ซึ่งผ่านการทดสอบและพร้อมใช้งานแล้ว รวมถึงหากมีการพัฒนา API ให้จัดส่งเอกสารวิธีการเรียกใช้งาน API ดังกล่าว (API Spec) ด้วย (ถ้ามี)
3	ติดตั้งและส่งมอบชั้นวางหนังสือดิจิทัล (Digital Bookshelf) พร้อมระบบการจัดการบนตู้ให้บริการดิจิทัล (Digital Signage Kiosk) ตามข้อ 5.13
4	เอกสารแผนการทดสอบระบบ ซึ่งประกอบด้วย Test Plan และ Test Case
5	เอกสารรับรองผลการทดสอบและผลการดำเนินการปรับปรุงระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA ก่อนการใช้งานจริง User Acceptance Test (UAT) ซึ่งประกอบด้วย Test Script และ Test Result
6	รายงานผลการทดสอบสอบในรูปแบบต่าง ๆ เช่น Input/Output Validation เอกสาร Authentication testing
7	รายงานการศึกษา วิเคราะห์ ออกแบบ ระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA (To-Be Process) และเอกสารการออกแบบฐานข้อมูล (Database Schema) เอกสารอธิบายรายละเอียดข้อมูล (Data Dictionary) ฉบับสมบูรณ์ (ซึ่งเป็นเอกสารที่ได้ส่งมอบแล้วในงานงวดก่อนหน้า งานงวดที่ 1 และ 2 ที่มีการปรับปรุงแก้ไข) โดยจัดทำเมื่อดำเนินการปรับปรุงแก้ไขระบบดังกล่าวแล้วเสร็จ

/8 ฝึกอบรม...

ลำดับ	งานที่ต้องส่งมอบ
8	ฝึกอบรมหลักสูตรการใช้งานระบบฯ สำหรับผู้ใช้งานทั่วไป และผู้ดูแลระบบ พร้อมส่งมอบคู่มือการใช้งาน และผลสรุปการประเมินผลการฝึกอบรม โดยมีรายละเอียดดังนี้ 1) คู่มือผู้ใช้งานทั่วไป (End User) เพื่อให้เข้าใจในการใช้งานระบบ 2) คู่มือผู้ใช้งานสำนักตรวจสอบ (Key User) เพื่อให้เข้าใจในการใช้งานระบบ 3) คู่มือผู้ดูแลระบบ (System Administrator) เพื่อใช้ในการกำหนดสิทธิ์ใช้งานระบบ และแก้ไขปัญหาเบื้องต้น รวมถึงเทคนิคต่าง ๆ ที่จำเป็นและควรรู้ 4) คู่มือการ Setup Backup และ Restore เพื่อใช้ในการติดตั้งระบบ จัดเก็บสำรองข้อมูล และกู้คืนระบบงาน 5) คู่มือการใช้งานเครื่องมือสำหรับการวิเคราะห์ข้อมูลธุรกิจ (Business Analytics Tool) ทั้งนี้ ผู้ขายต้องส่งมอบเอกสารที่มีการปรับปรุงแก้ไขหลังจากฝึกอบรมตามคู่มือข้อที่ 1 - 4 อย่างน้อย 1 เล่ม พร้อมทั้งส่งมอบคลิปวิดีโอการใช้งานระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA เพื่อเป็นฐานความรู้สำหรับการใช้งานระบบฯ
9	รายงานตามมาตรฐานความมั่นคงปลอดภัยสารสนเทศ ดังนี้ 1) รายงานสรุปผลการปิดช่องโหว่ ตามที่กำหนดในข้อ 4.17 2) รายงานสรุปผลการทดสอบประสิทธิภาพการให้บริการในการตอบสนองการเรียกใช้งาน (Response Time) 3) รายงานสรุปผลการตรวจสอบความมั่นคงปลอดภัยของ Source Code (Source Code Review) 4) รายงานรายละเอียดการกำหนดสิทธิ์การเข้าถึงระบบ (Role Matrix) 5) รายงานทะเบียนทรัพย์สินสารสนเทศ (Asset Inventory) 6) รายงานสรุปผลการทดสอบระบบ Backup และการกู้คืนข้อมูล (Restore) รายงานสรุปผลการทดสอบสมรรถภาพและประสิทธิภาพของระบบ (Performance Test)
10	รายงานสรุปผลการเชื่อมโยงข้อมูล (Web Service)
11	รายงานความก้าวหน้าการดำเนินงาน (Progress Report) เล่มที่ 3 (270 วัน)

ทั้งนี้ ผู้ขายต้องดำเนินงานต่าง ๆ และส่งมอบงานให้แก่ รฟม. โดยการส่งมอบงานที่เป็นเอกสารตามข้อ 7.1 และ 7.2 ผู้ขายต้องจัดทำเป็นรูปเล่มต้นฉบับ 1 ชุด และในรูปแบบเอกสารอิเล็กทรอนิกส์ (Soft file) บรรจุลง Universal Serial Bus On To Go (USB OTG) แบบ Type C เวอร์ชันใหม่ล่าสุด ความจุอย่างน้อย 128 GB ซึ่งรองรับได้ทั้งระบบ IOS และ Android จำนวนชุดไม่น้อยกว่าคณะกรรมการตรวจรับพัสดุ

/**8. การฝึกอบรม**...

8. <u>การฝึกอบรม</u>

ผู้ขายจะต้องดำเนินการจัดฝึกอบรม และประเมินผลการฝึกอบรม โดยแบ่งออกเป็นหลักสูตรดังต่อไปนี้

8.1 หลักสูตรสำหรับผู้ใช้งานทั่วไป (End User) จำนวนผู้เข้ารับการฝึกอบรมไม่เกิน 10 ท่าน เพื่อให้สามารถใช้งาน บันทึก และเรียกดูข้อมูลจากระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA ได้

8.2 หลักสูตรสำหรับผู้ใช้งานบรรณารักษ์ (Key User) จำนวนผู้เข้ารับการฝึกอบรมไม่เกิน 5 ท่าน เพื่อให้สามารถใช้งาน เรียกดู และวิเคราะห์ข้อมูลจากระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTAได้

8.3 หลักสูตรสำหรับผู้ดูแลระบบ (System Administrator) จำนวนผู้เข้ารับการฝึกอบรมไม่เกิน 5 ท่าน เพื่อให้สามารถใช้งานและแก้ไขปัญหาเบื้องต้น บริหารจัดการฐานข้อมูล การจัดเก็บและสำรองข้อมูล (Backup Data) รวมถึงวิธีการติดตั้งระบบฯ

8.4 ผู้ขายจะต้องจัดเตรียมอาหารว่าง เครื่องดื่ม และอาหารกลางวัน สำหรับผู้เข้าร่วมการฝึกอบรม ตามจำนวนผู้เข้ารับการอบรมตลอดระยะเวลาการฝึกอบรม

8.5 ผู้ขายจะต้องรับผิดชอบค่าใช้จ่ายที่เกี่ยวข้องกับการฝึกอบรม รวมทั้งค่าใช้จ่ายที่เกี่ยวข้องกับผู้เข้ารับการฝึกอบรม โดยดำเนินการจัดเตรียมเอกสารประกอบการฝึกอบรม สถานที่สำหรับฝึกอบรม อาหาร และอุปกรณ์ที่จำเป็นต่อการฝึกอบรมจำนวนไม่น้อยกว่าผู้เข้ารับการฝึกอบรม (เอกสารประกอบการฝึกอบรมจะต้องเป็นภาษาไทยเว้นแต่กรณีที่ต้องการอธิบายด้วยภาษาทางเทคนิคหรือภาษาเฉพาะให้ใช้ภาษาอังกฤษได้) ทั้งนี้ ก่อนเริ่มการฝึกอบรม ผู้ขายต้องเสนอรายละเอียดทั้งหมดของการอบรม เนื้อหา วิธีการสื่อสารฝึกอบรม เอกสารประกอบการฝึกอบรม และสถานที่ ให้ รฟม. พิจารณาเห็นชอบ ก่อน โดย รฟม. อาจขอให้ผู้ขายปรับรายละเอียดบางประการ อันจะช่วยให้การฝึกอบรมเกิดผลดียิ่งขึ้นแก่ผู้เข้าอบรม

8.6 ผู้ขายจะต้องจัดส่งผลสรุปการประเมินผลการฝึกอบรม เพื่อให้ทราบว่าผู้เข้ารับการฝึกอบรมมีความเข้าใจในการใช้งานระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA หลังจากที่ได้ฝึกอบรมการใช้งานไปแล้วมากน้อยเพียงใด

9. <u>งวดงานและการจ่ายเงิน</u>

รฟม. จะชำระเงินให้แก่ผู้ขายเมื่อผู้ขายได้ส่งมอบงานให้เป็นไปตามที่ระบุไว้ในข้อ 7 และคณะกรรมการตรวจรับพัสดุได้ตรวจรับงานระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA เป็นที่เรียบร้อยแล้ว โดย รฟม. จะชำระเงินตามสัญญา ซึ่งได้รวมภาษีมูลค่าเพิ่มตลอดจนภาษีอากรอื่น ๆ และค่าใช้จ่ายทั้งปวงด้วยแล้วให้แก่ผู้ขาย โดยแบ่งการชำระเงินเป็น 3 งวด ดังนี้

งวดที่ 1 ชำระเงินร้อยละ 30 ของวงเงินตามสัญญา เมื่อคณะกรรมการตรวจรับพัสดุได้ตรวจรับการส่งมอบงานที่ถูกต้อง ครบถ้วนตามงวดที่ 1 เรียบร้อยแล้ว

งวดที่ 2 ชำระเงินร้อยละ 30 ของวงเงินตามสัญญา เมื่อคณะกรรมการตรวจรับพัสดุได้ตรวจรับการส่งมอบงานที่ถูกต้อง ครบถ้วนตามงวดที่ 2 เรียบร้อยแล้ว

งวดที่ 3 ชำระเงินร้อยละ 40 ของวงเงินตามสัญญา เมื่อคณะกรรมการตรวจรับพัสดุได้ตรวจรับการส่งมอบงานที่ถูกต้อง ครบถ้วนตามงวดที่ 3 เรียบร้อยแล้ว

/10. <u>กำหนดระยะ</u>...

10. กำหนดระยะเวลารับประกันความชำรุดบกพร่อง

10.1 ผู้ขายจะต้องรับประกันการใช้งานระบบงานรวมถึงสิทธิ์การใช้งานหรือลิขสิทธิ์ที่เกี่ยวข้องเป็นระยะเวลา 1 ปี นับถัดจากวันที่ได้รับมอบงานที่ถูกต้องครบถ้วนดังกล่าว โดยผู้ขายมีหน้าที่ดูแล บำรุงรักษาระบบงานให้อยู่ในสภาพที่ใช้งานได้ดีอยู่เสมอ และจะต้องดำเนินการซ่อมแซมแก้ไขปัญหาข้อผิดพลาดที่เกิดขึ้นเมื่อผู้ใช้ไม่สามารถใช้งานได้ เพื่อให้ใช้งานได้ดีดังเดิมตามข้อกำหนดและขอบเขตของงานฯ ดังกล่าวด้วยค่าใช้จ่ายของผู้ขายเอง โดย รฟม. ไม่ต้องเสียค่าใช้จ่ายเพิ่มเติม

10.2 ในระหว่างระยะเวลารับประกันการใช้งาน 1 ปี หากผู้ขายต้องดำเนินการปรับปรุง/ เปลี่ยนแปลงส่วนใดส่วนหนึ่งที่เกี่ยวข้องกับระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA เช่น การ Customized/ Upgrade ของ Software หรือ Hardware เป็นต้น ผู้ขายต้องดำเนินการปรับปรุง/ เปลี่ยนแปลงระบบให้ใช้งานได้ดีดังเดิม โดย รฟม. ไม่ต้องเสียค่าใช้จ่ายเพิ่มเติม

10.3 ในระหว่างระยะเวลารับประกันการใช้งาน 1 ปี รฟม. หรือผู้แทนของ รฟม. อาจแจ้งปัญหา/ข้อผิดพลาดของระบบงาน ไปยังผู้ขายทางโทรศัพท์ หรือโทรศัพท์เคลื่อนที่ ไปรษณีย์อิเล็กทรอนิกส์ (E-mail) หรือช่องทางที่ รฟม. กำหนด ได้ทุกวัน ตามวันและเวลาทำการของ รฟม. (วันจันทร์ ถึง วันศุกร์ เวลาทำการ 08.00 - 17.00 น.) หรือแล้วแต่วันและเวลาที่ รฟม. กำหนดได้ (ในกรณีที่ไม่สามารถดำเนินการได้ในวันและเวลาทำการของ รฟม.) โดยผู้ขายจะต้องตรวจสอบและแก้ไขปัญหาให้แล้วเสร็จภายใน 1 วันทำการนับแต่เวลาที่ได้รับแจ้ง หากไม่สามารถดำเนินการแก้ไขได้ภายในระยะเวลาที่กำหนด เนื่องจากปัญหามีความซับซ้อน ผู้ขายจะต้องทำหนังสือแจ้งเป็นลายลักษณ์อักษรให้ รฟม. ทราบ โดยระบุถึงปัญหาและระยะเวลาที่จะใช้ในการดำเนินการแก้ไขให้แล้วเสร็จ ซึ่ง รฟม. จะพิจารณาว่าปัญหาดังกล่าวเป็นปัญหาที่มีความซับซ้อนหรือไม่ และจะใช้ระยะเวลาในการดำเนินการแก้ไขปัญหาเป็นระยะเวลาเท่าไร โดยคำวินิจฉัยของ รฟม. ถือเป็นที่สิ้นสุด

11. อัตราค่าปรับ

11.1 ในกรณีที่ผู้ขายไม่สามารถส่งมอบงานทั้งหมดให้แก่ รฟม. ได้ภายในระยะเวลาตามข้อ 6. ผู้ขายต้องยินยอมให้ รฟม. ปรับเป็นรายวันในอัตราร้อยละ 0.05 ของวงเงินตามสัญญา นับถัดจากวันที่กำหนดตามข้อ 6. หรือนับถัดจากวันที่ครบกำหนดระยะเวลาที่ รฟม. ได้มีการขยายให้จนถึงวันที่ผู้ขายได้ส่งมอบงานถูกต้องครบถ้วนเป็นที่เรียบร้อยแล้ว นอกจากนี้ ผู้ขายยอมให้ รฟม. เรียกค่าเสียหายอันเกิดขึ้นจากการที่ผู้ขายทำงานล่าช้าเฉพาะส่วนที่เกินกว่าจำนวนค่าปรับและค่าใช้จ่ายดังกล่าวได้อีกด้วย

11.2 ในกรณีที่ผู้ขายเปลี่ยนแปลงตัวบุคลากรหลัก ตามที่ระบุไว้ในขอบเขตของงานข้อ 4.1 ไม่ว่าจะเป็นการเปลี่ยนแปลงเพื่อปรับปรุงประสิทธิภาพของการทำงาน หรือด้วยสาเหตุอื่นซึ่งมีเหตุผลอันสมควร โดยไม่ได้แจ้งให้ รฟม. ทราบล่วงหน้า และไม่ได้รับความเห็นชอบจาก รฟม. ก่อน รฟม. มีสิทธิ์จะปรับเป็นรายวันในอัตราวันละ 2,000 บาท (สองพันบาทถ้วน) ต่อคน ตามจำนวนวันที่ผู้ขายเปลี่ยนแปลงตัวบุคลากรโดยไม่แจ้งให้ทราบล่วงหน้าและไม่ได้รับความเห็นชอบจาก รฟม. ก่อน (คิดค่าปรับตามวันทำการของ รฟม.) ทั้งนี้การเปลี่ยนแปลงตัวบุคลากรนี้จะต้องมีคุณสมบัติที่เท่าเดิมหรือดีกว่าบุคลากรที่ถูกเปลี่ยนตัวออกไป

/11.3 ในกรณี...

11.3 ในกรณีที่ผู้ขายไม่จัดส่งบุคลากรมาประจำ รฟม. ในช่วง Go live Support ตามระยะเวลาที่กำหนดในข้อ 7.1.9 หรือผู้ขายเปลี่ยนแปลงตัวบุคลากรดังกล่าว โดยไม่ได้แจ้งให้ รฟม. ทราบล่วงหน้า และไม่ได้รับความเห็นชอบจาก รฟม. ก่อน รฟม. มีสิทธิ์จะปรับเป็นรายวันในอัตราวันละ 2,000 บาท (สองพันบาทถ้วน) ตามสัดส่วนของระยะเวลาที่ไม่ได้จัดส่งบุคลากรมาประจำ หรือเปลี่ยนแปลงตัวบุคลากรมาประจำโดยไม่ได้แจ้งล่วงหน้าและไม่ได้รับความเห็นชอบจาก รฟม. ก่อน ทั้งนี้ การเปลี่ยนแปลงตัวบุคลากรมาประจำ รฟม. ไม่ว่าจะเป็นการเปลี่ยนแปลงด้วยสาเหตุใด ต้องมีเหตุผลสมควร และผู้ขายต้องแจ้งให้ รฟม. ทราบล่วงหน้าเป็นระยะเวลา 1 เดือน และได้รับความเห็นชอบจาก รฟม. ก่อนจึงจะเปลี่ยนแปลงตัวบุคลากรที่มาประจำได้

11.4 กรณีบุคลากรที่มาประจำ รฟม. ตามข้อ 7.1.9 ไม่สามารถมาปฏิบัติงานได้ เช่น เจ็บป่วยร้ายแรง ลาออก หรือเสียชีวิต เป็นต้น ผู้ขายต้องจัดส่งบุคลากรมาทดแทนทันทีเป็นการชั่วคราว และต้องแจ้งให้ รฟม. ทราบโดยพลัน ทั้งนี้ ผู้ขายต้องรีบดำเนินการจัดส่งบุคลากรอื่นมาทดแทนบุคลากรเดิม และมีหนังสือแจ้งการเปลี่ยนแปลงตัวบุคลากรให้ รฟม. ทราบภายใน 7 วันทำการ นับแต่วันที่มีการจัดส่งบุคลากรมาทดแทนเป็นการชั่วคราว หากผู้ขายไม่ดำเนินการ รฟม. มีสิทธิ์ปรับเป็นรายวันในอัตราวันละ 2,000 บาท (สองพันบาทถ้วน) จนกว่าผู้ขายจะจัดส่งบุคลากรมาทดแทนเป็นการชั่วคราว หรือ จัดส่งบุคลากรอื่นมาทดแทนบุคลากรเดิมและมีหนังสือแจ้งการเปลี่ยนแปลงตัวบุคลากรให้ รฟม. ทราบ

11.5 หากบุคลากรที่มาประจำ รฟม. ตามข้อ 7.1.9 ไม่ปฏิบัติตามหน้าที่และความรับผิดชอบของตน หรือปฏิบัติงานไม่มีประสิทธิภาพ รฟม. มีสิทธิพิจารณาปรับเปลี่ยนบุคลากรของผู้ขาย โดยผู้ขายต้องดำเนินการจัดส่งบุคลากรมาทดแทนภายในระยะเวลาที่ รฟม. กำหนด หากผู้ขายไม่จัดส่งบุคลากรมาประจำทดแทนบุคลากรเดิมที่ถูกปรับออกไป รฟม. มีสิทธิ์ปรับเป็นรายวันในอัตราวันละ 2,000 บาท (สองพันบาทถ้วน) นับแต่วันที่ครบระยะเวลาที่ รฟม. กำหนดให้จัดหาบุคลากรมาทดแทน ทั้งนี้ บุคลากรที่มาทดแทนต้องมีคุณสมบัติที่เท่าเดิมหรือดีกว่าบุคลากรเดิมที่ถูกปรับออกไป และบุคลากรที่มาทดแทนดังกล่าวต้องได้รับความเห็นชอบจาก รฟม. ก่อน

11.6 หากผู้ขายไม่สามารถปฏิบัติตาม หรือปฏิบัติไม่ครบถ้วนถูกต้องตามที่ระบุไว้ในข้อ 7.1.10 - 7.1.11 และข้อ 10.2 - 10.3 (ช่วงรับประกันการใช้งาน 1 ปี) ผู้ขายต้องถูกปรับเป็นรายวันในอัตราวันละ 2,000 บาท (สองพันบาทถ้วน) เศษของวันให้คิดเป็น 1 วัน นับแต่วันครบกำหนดเวลาดังกล่าว จนกว่าจะดำเนินการแล้วเสร็จ

11.7 ค่าปรับตามข้อ 11.1 - 11.6 ผู้ขายยินยอมชำระด้วยเงินสด หรือยินยอมให้ รฟม. หักเอาจากจำนวนเงินค่าสิ่งของที่ซื้อขายที่ต้องชำระ หรือเงินอื่น ๆ ที่ค้างจ่าย หรือหลักประกันที่ รฟม. ยึดถือไว้ได้ทันที โดยไม่ต้องแจ้งให้ทราบล่วงหน้า

12. วงเงินงบประมาณ

วงเงินงบประมาณสำหรับงานซื้อระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA จำนวน 4,000,000.00 บาท (สี่ล้านบาทถ้วน) รวมภาษีมูลค่าเพิ่มแล้ว

/**13. หลักเกณฑ์**...

13. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

ในการพิจารณาผู้ชนะการยื่นข้อเสนอราคา รฟม. จะใช้หลักเกณฑ์การประเมินค่าประสิทธิภาพต่อราคา (Price Performance) โดยการให้คะแนนตามปัจจัยหลักและน้ำหนักตามที่กำหนด ดังนี้

13.1 คุณภาพและคุณสมบัติที่เป็นประโยชน์ต่อ รฟม. กำหนดน้ำหนักเท่ากับร้อยละ 70 (ภาคผนวก ค.)

หลักเกณฑ์ในการพิจารณาแบ่งออกเป็น 5 หัวข้อ โดยมีคะแนนเต็มในการพิจารณาทั้งหมด 100 คะแนน โดยระบบจะคำนวณคะแนนออกมาเป็นร้อยละให้อัตโนมัติ ซึ่งมีรายละเอียดการให้คะแนนตามหลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอด้านเทคนิคแต่ละหัวข้อ

13.2 ราคาที่ยื่นข้อเสนอ (Price) กำหนดน้ำหนักเท่ากับร้อยละ 30

หลักเกณฑ์ในการพิจารณาราคา (Price) ให้ผู้มีราคารวมต่ำที่สุดได้ 100 คะแนน โดยระบบการจัดซื้อจัดจ้างภาครัฐด้วยระบบอิเล็กทรอนิกส์ (e-GP) จะคำนวณคะแนนให้อัตโนมัติ

โดยกำหนดน้ำหนักรวมทั้งหมดเท่ากับร้อยละ 100 และผู้ชนะการเสนอราคาต้องได้คะแนนในข้อ 13.1 ไม่น้อยกว่าร้อยละ 70

14. การจัดทำข้อเสนอโครงการ

ข้อเสนอด้านเทคนิค จะต้องมีรายละเอียดครอบคลุม ดังนี้

14.1 ให้ผู้ยื่นข้อเสนอจัดทำรายละเอียดคุณสมบัติของผู้ยื่นข้อเสนอ ตามภาคผนวก ง. แบบฟอร์มที่ 01

14.2 หนังสือรับรองผลงาน และข้อกำหนดหรือขอบเขตของงานของผลงานที่แล้วเสร็จ พร้อมทั้งรับรองสำเนาถูกต้อง (ตามรายละเอียดที่กำหนดในข้อ 3 คุณสมบัติของผู้ยื่นข้อเสนอ ข้อย่อยที่ 3.13) พร้อมด้วยสำเนาสัญญาหรือใบสั่งซื้อ/ใบสั่งจ้าง (ถ้ามี)

14.3 แบบฟอร์มรายละเอียดบริษัทและบุคลากรหลัก ให้ผู้ยื่นข้อเสนอจัดทำรายละเอียดประสบการณ์การดำเนินงานที่เป็นผลงานซึ่งได้ตรวจรับสมบูรณ์แล้วเสร็จในช่วง 5 ปี ตามภาคผนวก ง. แบบฟอร์มที่ 02 และรายละเอียดคุณสมบัติและประสบการณ์การทำงานของบุคลากรหลัก ตามภาคผนวก ง. แบบฟอร์มที่ 03 โดยอ้างถึงไว้ให้ชัดเจนท้ายบุคลากรนั้น ๆ ในแบบฟอร์มดังกล่าว **ทั้งนี้ รฟม. ขอสงวนสิทธิ์ที่จะพิจารณาเฉพาะข้อมูลที่ปรากฏอยู่ในแบบฟอร์มเท่านั้น**

14.4 รายละเอียดแนวทางและวิธีการดำเนินงานของโครงการ ดังนี้

- ภาพรวมสถาปัตยกรรมขององค์กร (Enterprise Architecture) ประกอบด้วยอย่างน้อย ดังนี้ สถาปัตยกรรมของ Technology Architecture, สถาปัตยกรรมของ Information Architecture, สถาปัตยกรรมของ Application Architecture, สถาปัตยกรรมของ Business Architecture เป็นต้น
- แนวความคิด (Conceptual) และรายละเอียด (Detailed) เกี่ยวกับการออกแบบและพัฒนาระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA เพื่อเพิ่มประสิทธิภาพการดำเนินงานด้านระบบงานห้องสมุด
- แนวทางการแก้ไขปัญหา เมื่อระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA ไม่สามารถใช้งานได้ หรือการให้คำปรึกษาเกี่ยวกับระบบฯ

ให้ผู้ยื่นข้อเสนอจัดทำรายละเอียดแนวทาง และวิธีการดำเนินงานของโครงการ ตามภาคผนวก ง. แบบฟอร์มที่ 04

/14.5 รายละเอียด...

14.5 รายละเอียดแนวทางและวิธีในการพัฒนาระบบ (Methodology) และซอฟต์แวร์หรือเครื่องมือ (Tools) ที่เหมาะสมหรือสอดคล้องตามข้อกำหนดและขอบเขตของงานโครงการดังกล่าว ได้แก่

- ซอฟต์แวร์หรือเครื่องมือ (Tools) ที่เสนอเพื่อใช้ในโครงการ
- ภาษาที่ใช้พัฒนาระบบ
- เครื่องมือที่ใช้พัฒนารายงาน
- ระบบปฏิบัติการ
- ระบบฐานข้อมูล
- รายชื่อหน่วยงานที่นำไปใช้การพัฒนา และติดตั้งระบบงานที่ทำกับหน่วยงานภาครัฐ หรือหน่วยงานเอกชน

ให้ผู้ยื่นข้อเสนอระบุรายละเอียดแนวทางและวิธีในการพัฒนาระบบ พร้อมทั้งจัดทำเอกสารเปรียบเทียบทางด้านเทคนิคเป็นรายข้อทุกข้อ (Statement of Compliance) ตามภาคผนวก ง. แบบฟอร์มที่ 04

14.6 แผนการดำเนินงาน ที่จะทำให้บรรลุวัตถุประสงค์และครบถ้วนตามข้อกำหนดและขอบเขตของงานระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA รวมถึงรายละเอียดอื่น ๆ ได้แก่

- แผนการดำเนินงานที่แสดงถึงระยะเวลาการดำเนินงานในส่วนต่าง ๆ รายละเอียดแผนการปฏิบัติงาน โดยอย่างน้อยต้องประกอบด้วยรายละเอียดกิจกรรม และช่วงระยะเวลาการทำงานของบุคลากรที่สอดคล้องกัน
- รายละเอียดข้อเสนอการจัดตั้งทีมทำงาน หน้าที่ความรับผิดชอบบุคลากรของผู้ยื่นข้อเสนอทั้งหมด และระยะเวลาการดำเนินงานทั้งหมด (คน - เดือน)
- แผนการฝึกอบรมการใช้งานระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA โดยจัดแบ่งหลักสูตรให้เหมาะสมกับจำนวนผู้เข้ารับการฝึกอบรม ซึ่งมีรายละเอียดหลักสูตรและช่วงระยะเวลาการฝึกอบรมอย่างเหมาะสม

ให้ผู้ยื่นข้อเสนอจัดทำรายละเอียดแผนการดำเนินงาน (Work Plan) ตามภาคผนวก ง. แบบฟอร์มที่ 05

14.7 ผู้ยื่นข้อเสนอจะต้องจัดเตรียมตัวอย่างผลงาน (Demo) โดยให้ใช้ผลงานเดิมที่เคยดำเนินการในอดีต มานำเสนอต่อ รฟม. ภายใน 5 วันทำการ นับถัดจากวันเสนอราคา ทั้งนี้ รฟม. จะเป็นผู้กำหนดวันและเวลา โดยจะแจ้งให้ทราบภายหลัง

/**ภาคผนวก ก.** ...

ภาคผนวก ก.

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) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) และความน่าเชื่อถือ (Reliability)

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

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

1. วัตถุประสงค์และขอบเขต

เพื่อให้การใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาและลดผลกระทบจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องหรือจากการถูกคุกคามจากภัยต่าง ๆ จึงได้กำหนดนโยบายเพื่อควบคุมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ดังนี้

1.1 การเข้าถึงหรือควบคุมการใช้งานสารสนเทศครอบคลุม 4 ด้าน คือ

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

/เข้าถึง...

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

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

1.1.3 การเข้าถึงระบบปฏิบัติการ (Operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยกำหนดให้มีการยืนยันตัวตนเพื่อระบุถึงตัวตนของผู้ใช้งาน รวมทั้งกำหนดให้มีการจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น

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

1.2 มีระบบสารสนเทศและระบบสำรองที่อยู่ในสภาพพร้อมใช้งาน รวมทั้งมีแผนเตรียมพร้อมในกรณีฉุกเฉินหรือกรณีที่ไม่สามารถดำเนินการตามวิธีการทางอิเล็กทรอนิกส์ได้ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

1.3 ตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศอย่างสม่ำเสมอ

2. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รฟม.

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

3. กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย (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)
ผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

สารบัญ

เรื่อง **หน้า**

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. อนุญาตให้มีสิทธิ์ในการเข้าถึง หรือใช้ข้อมูลหรือสินทรัพย์ต่าง ๆ ของ รฟม. โดยจะได้รับสิทธิ์ในการใช้ระบบตามประเภทงานตามอำนาจและต้องรับผิดชอบในการรักษาความลับของข้อมูล
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 การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ ได้แก่ ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลและสารสนเทศ เป็นต้น
14. ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด ที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

15. ข้อมูลจราจรทางคอมพิวเตอร์ (Traffic log) หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เวลา วันที่ ปริมาณ ระยะเวลา หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น
16. สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูล ซึ่งข้อมูลอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิกให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ
17. ระบบคอมพิวเตอร์ (Computer system) หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่งหรือสิ่งอื่นใด และแนวปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
18. ระบบเครือข่ายสื่อสารข้อมูล (Network system) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของ รฟม. เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น
19. สิทธิ์ของผู้ใช้งาน หมายถึง สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิพิเศษ และสิทธิ์อื่นใด ที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน
20. ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (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 รฟม. เช่น อุปกรณ์คอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีค่าลิขสิทธิ์ ข้อมูล ระบบข้อมูล ฯลฯ
25. จดหมายอิเล็กทรอนิกส์ (e-mail) หมายถึง ระบบที่บุคคลใช้ในการรับ - ส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหวและเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ โดยข่าวสารที่ส่งนั้นจะถูกเก็บไว้ในตู้จดหมาย (Mail box) ที่กำหนดไว้สำหรับผู้ใช้งาน ผู้รับสามารถเปิดอ่าน พิมพ์ลงกระดาษ หรือจะลบทิ้งก็ได้

26. ชุดคำสั่งไม่พึงประสงค์ (Malicious code) หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
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 แผนการอบรมทางด้านความมั่นคงปลอดภัยประจำปีซึ่งรวมถึงการสร้างความตระหนัก
   1.9 ผลการทดสอบแผนกู้คืนในปีที่ผ่านมา
   1.10 ข้อมูลภัยคุกคามต่าง ๆ ที่เคยเกิดขึ้นในอดีตและปัจจุบัน รวมทั้งภัยคุกคามที่ได้รับแจ้งจากหน่วยงานภายนอก
   1.11 ผลการตรวจสอบการปฏิบัติตามนโยบายความมั่นคงปลอดภัยโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก
2. จัดให้มีทรัพยากรด้านบุคลากร งบประมาณ การบริหารจัดการ และวัตถุดิบที่เพียงพอต่อการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศในแต่ละปีงบประมาณ
3. จัดให้มีบุคลากรดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศและกำหนดหน้าที่ความรับผิดชอบรวมทั้งปรับปรุงโครงสร้างดังกล่าวตามความจำเป็น
4. แสดงเจตนารมณ์หรือสื่อสารอย่างสม่ำเสมอเพื่อให้ผู้ใช้งานทั้งหมดได้เห็นถึงความสำคัญของการปฏิบัติตามนโยบายความมั่นคงปลอดภัยและนโยบายสนับสนุนต่าง ๆ โดยเคร่งครัดและเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับสารสนเทศขององค์กร รวมถึงสร้างความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ

ส่วนที่ 2
ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร

วัตถุประสงค์

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

ผู้รับผิดชอบ

- ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ ผู้อำนวยการฝ่ายทรัพยากรบุคคล ผู้อำนวยการฝ่าย/สำนัก ที่กำกับดูแลงานที่มีการว่าจ้างหน่วยงานภายนอก

อ้างอิงมาตรฐาน

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

แนวปฏิบัติ

1. การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to employment) เพื่อคัดสรรบุคลากรก่อนที่จะเข้ามาปฏิบัติงาน และเพื่อลดความเสี่ยงจากการปฏิบัติงานผิดพลาด การขโมย การปลอมแปลง และการนำระบบสารสนเทศหรือทรัพยากรสารสนเทศของ รฟม. ไปใช้ในทางที่ไม่เหมาะสม รวมทั้งเพื่อให้ผู้ใช้งานเข้าใจในหน้าที่ความรับผิดชอบของตนเอง
    1.1 การตรวจสอบคุณสมบัติของผู้สมัคร (Screening)
    ฝ่ายทรัพยากรบุคคล หรือฝ่าย/สำนัก ที่กำกับดูแลงานที่มีการว่าจ้างหน่วยงานภายนอกต้องตรวจสอบคุณสมบัติของผู้สมัคร (ทั้งกรณีการจ้างเป็นพนักงาน ลูกจ้าง การว่าจ้างหน่วยงานภายนอกเพื่อปฏิบัติงานให้ รฟม. รวมทั้งนิสิตนักศึกษาฝึกงาน) โดยผู้สมัครต้องไม่เคยกระทำผิดกฎหมาย ระเบียบ ข้อบังคับ หรือจริยธรรม รวมทั้งไม่มีประวัติในการบุกรุก แก้ไข ทำลาย หรือโจรกรรมข้อมูลในระบบเทคโนโลยีสารสนเทศมาก่อน และมีคุณสมบัติตามที่ รฟม. กำหนด
    1.2 การกำหนดเงื่อนไขการจ้างงาน (Terms and conditions of employment) การว่าจ้างให้มีเงื่อนไขการจ้างงานให้ครอบคลุมในเรื่องดังต่อไปนี้
        1.2.1 กำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศอย่างเป็นลายลักษณ์อักษร (Information security roles and responsibilities) แก่ผู้ใช้งาน โดยกำหนดให้สอดคล้องกับนโยบายความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของ รฟม.
        1.2.2 กำหนดให้มีการลงนามในสัญญาว่าจะไม่เปิดเผยความลับของ รฟม. (Non-Disclosure Agreement: NDA)

1.2.3 ระบบเทคโนโลยีสารสนเทศที่สร้างหรือพัฒนาโดยผู้ใช้งานในระหว่างการว่าจ้างถือเป็นสินทรัพย์ของ รฟม.

1.2.4 กำหนดความรับผิดชอบหรือบทลงโทษ หากผู้ใช้งานไม่ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รฟม. รวมทั้ง กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

2. การสร้างความมั่นคงปลอดภัยในระหว่างการจ้างงาน (During employment) เพื่อสร้างความตระหนักแก่ผู้ใช้งานเกี่ยวกับภัยที่เกี่ยวข้องกับการปฏิบัติงานสารสนเทศ รวมถึงให้ความรู้เพื่อให้สามารถป้องกันภัยดังกล่าวได้

2.1 หน้าที่ในการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management responsibilities)

ผู้บริหาร รฟม. ทุกระดับชั้นมีหน้าที่สนับสนุนและส่งเสริมเรื่องดังต่อไปนี้ แก่ผู้ใช้งาน

2.1.1 ประกาศนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ รฟม. เป็นลายลักษณ์อักษรให้ทุกคนรับทราบและปฏิบัติตาม

2.1.2 จูงใจให้ผู้ใช้งานปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ รฟม.

2.1.3 สร้างความตระหนักถึงความมั่นคงปลอดภัยด้านสารสนเทศที่เกี่ยวข้องกับหน้าที่ความรับผิดชอบของตนเองและของ รฟม.

2.2 การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่ผู้ใช้งาน (Information security awareness, education and training) การสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยอย่างสม่ำเสมอ

2.2.1 ผู้ดูแลระบบต้องแจ้งเตือนภัยคุกคาม และช่องโหว่ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศแก่ผู้ใช้งานที่เกี่ยวข้อง นอกจากนี้ต้องแจ้งเตือนให้ผู้ใช้งานเพิ่มความระมัดระวังความเสี่ยงต่าง ๆ เช่น ไวรัสคอมพิวเตอร์ เทคนิคการหลอกล่อทางจิตวิทยา (Social engineering) และช่องโหว่ทางเทคนิค เป็นต้น

2.2.2 ฝทท. ต้องดำเนินการฝึกอบรม หรือประชาสัมพันธ์เพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศแก่ผู้ใช้งานเป็นประจำทุกปี

2.2.3 ฝทท. ต้องแจ้งผู้ใช้งานให้ทราบ เมื่อมีการเปลี่ยนแปลงนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศของ รฟม. รวมทั้งอธิบายผลกระทบจากการเปลี่ยนแปลงดังกล่าว

2.3 การแจ้งเหตุการณ์ไม่ปกติ

ผู้ใช้งานต้องแจ้งเหตุการณ์ไม่ปกติด้านเทคโนโลยีสารสนเทศที่พบผ่านช่องทางที่ รฟม. กำหนดโดยเร็วที่สุด

2.4 การกำหนดบทลงโทษ

2.4.1 ความรับผิดตามกฎหมาย

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ไม่ได้ก่อให้เกิดสิทธิ์ทางกฎหมายที่ทำให้ผู้ใช้งานพ้นผิดแม้จะได้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ และผู้ใช้งานตกลงยินยอมที่จะไม่ดำเนินการใด ๆ ทางกฎหมายต่อ รฟม. ซึ่งได้ปฏิบัติตามระเบียบนี้ แต่อย่างไรก็ตามหากผู้ใช้งานกระทำการละเมิดหรือกระทำผิดตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ อาจเป็นความผิดทางวินัยและเป็นเหตุ

ให้ถูกลงโทษทางวินัยได้ รฟม. ไม่มีส่วนรับผิดชอบต่อการละเมิดทรัพย์สินทางปัญญาที่เกิดจากการใช้ระบบคอมพิวเตอร์

2.4.2 การพิจารณาโทษผู้กระทำผิด

ผู้ใช้งานที่กระทำความผิด ฝทท. จะเพิกถอนสิทธิ์การใช้งานและอาจเป็นความผิดทางวินัย หรือความผิดตามกฎหมายที่เกี่ยวข้อง

1) พนักงาน/ลูกจ้างที่ฝ่าฝืนหรือละเมิดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รฟม. ต้องถูกลงโทษตามกระบวนการทางวินัยของ รฟม. รวมถึงกฎหมายที่เกี่ยวข้อง

2) หน่วยงานภายนอกที่กระทำความผิด จะมีโทษตามที่ระบุไว้ในสัญญาหรือถูกเพิกถอนสิทธิ์การใช้งาน รวมถึงดำเนินการตามกฎหมายที่เกี่ยวข้อง

3. การสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน (Termination and change of employment)

เพื่อกำหนดหน้าที่ความรับผิดชอบเมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน ซึ่งรวมไปถึงการคืนทรัพย์สินและการถอดถอนสิทธิ์ในการเข้าถึง

3.1 การแจ้งการสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน

3.1.1 ฝ่ายทรัพยากรบุคคลต้องแจ้งให้ฝ่ายเทคโนโลยีสารสนเทศทราบทันทีหากพนักงานมีการลาออก โยกย้าย เกษียณ หรือเสียชีวิต เพื่อฝ่ายเทคโนโลยีสารสนเทศจะได้ตรวจสอบและบริหารจัดการสิทธิ์ในการเข้าถึงระบบเทคโนโลยีสารสนเทศ

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

3.2 การคืนสินทรัพย์ของ รฟม.

ผู้ดูแลระบบต้องตรวจสอบเพื่อเรียกคืนสินทรัพย์ของ รฟม. จากผู้ใช้งาน เมื่อการสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน

3.3 การถอดถอนสิทธิ์ในการเข้าถึง

3.3.1 ผู้ดูแลระบบต้องถอดถอนสิทธิ์ในการเข้าถึงของผู้ใช้งาน เมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน

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

3.3.3 ในกรณีที่ผู้ใช้งานที่สิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน มีการใช้บัญชีผู้ใช้งานร่วมกัน (Shared user ID) กับผู้ใช้งานอื่น ผู้บังคับบัญชาต้องเปลี่ยนรหัสผ่านทันทีหลังจากสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน

ส่วนที่ 3
การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

วัตถุประสงค์

- เพื่อควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าถึงอาคารสถานที่ และพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area)

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้อำนวยการฝ่ายจัดซื้อและบริการ

อ้างอิงมาตรฐาน

- หมวดที่ 7 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security)

แนวปฏิบัติ

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

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

5.1.4 เจ้าหน้าที่รักษาความปลอดภัย (รปภ.) ต้องตรวจสอบผู้ติดต่อ อุปกรณ์ พร้อมลงเวลาออกที่สมุดบันทึกหรือระบบสารสนเทศให้ถูกต้อง

5.2 ผู้ดูแลระบบ ต้องควบคุมการเข้า – ออกพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) ไม่ให้ผู้ไม่มีสิทธิ์เข้าถึงได้ โดยกำหนดพื้นที่การส่งมอบสินค้าและพื้นที่การเตรียมหรือประกอบอุปกรณ์สารสนเทศ (Unpack Area) ก่อนนำเข้าพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) และต้องควบคุมการเข้า - ออก เพื่อหลีกเลี่ยงการเข้าถึงระบบสารสนเทศและข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต โดยปฏิบัติตามขั้นตอนที่ รฟม. กำหนด

ส่วนที่ 4
การจัดการทรัพย์สิน

วัตถุประสงค์

- เพื่อบริหารจัดการทรัพย์สินสารสนเทศ ตั้งแต่การจัดหา การใช้งาน จนถึงการยกเลิกใช้งาน โดยมีการระบุสินทรัพย์ขององค์กรและกำหนดหน้าที่ความรับผิดชอบในการปกป้องทรัพย์สินสารสนเทศอย่างเหมาะสม

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- เจ้าของข้อมูล
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 4 การบริหารจัดการทรัพย์สิน (Asset management)

แนวปฏิบัติ

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

ก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อเพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลที่สำคัญได้ โดยพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

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

3.3 เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ใช้งาน ต้องมีการป้องกันสื่อบันทึกข้อมูลที่ใช้จัดเก็บข้อมูลสารสนเทศ ในกรณีที่มีการเคลื่อนย้ายเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต ถูกนำไปใช้งานผิดวัตถุประสงค์ รวมถึงป้องกันสื่อบันทึกข้อมูลไม่ให้ได้รับความเสียหาย โดยรักษาความปลอดภัยสารสนเทศตามขั้นตอนที่ รฟม. กำหนด

ส่วนที่ 5
การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

วัตถุประสงค์

- เพื่อควบคุมการจัดหา พัฒนา และบำรุงรักษาระบบสารสนเทศ ให้มีการกำหนดมาตรการการรักษาความมั่นคงปลอดภัย เพื่อป้องกันความผิดพลาด สูญหาย และการเปลี่ยนแปลงแก้ไขระบบ

ผู้รับผิดชอบ

- ผู้บังคับบัญชา
- ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

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

แนวปฏิบัติ

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

10. ผู้ดูแลระบบต้องควบคุมการจัดส่ง Source code ผ่านช่องทางที่มั่นคงปลอดภัยและเป็นช่องทางที่ รฟม. 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 ขอสิทธิ์เข้าถึงทรัพยากรหรือบริการโดยแอปพลิเคชัน (Application permission) บนอุปกรณ์เคลื่อนที่ของผู้ใช้งานเท่าที่จำเป็น และมีกระบวนการทบทวนการขอสิทธิ์เป็นประจำเพื่อป้องกันการละเมิดสิทธิ์ความเป็นส่วนตัวของผู้ใช้งาน
14. ผู้ดูแลระบบต้องควบคุมข้อมูลที่นำมาใช้ในการทดสอบระบบ (Test data) อย่างเหมาะสม โดยไม่นำข้อมูลจริงมาทดสอบ กรณีจำเป็นต้องใช้ข้อมูลจริงต้องได้รับอนุญาตข้อมูลจากเจ้าของก่อนนำมาใช้งาน และทำลายข้อมูลอย่างเหมาะสมตามขั้นตอนที่ รฟม. กำหนด
15. ผู้ดูแลระบบต้องแยกระบบสารสนเทศสำหรับการพัฒนา ทดสอบ และใช้งานจริงออกจากกันเพื่อลดความเสี่ยงที่เกิดจากการเปลี่ยนแปลงระบบสารสนเทศโดยไม่ได้รับอนุญาต และต้องมีการกำหนดสิทธิ์การเข้าถึงระบบสารสนเทศที่พัฒนา ทดสอบ หรือใช้งานจริง ทั้งระบบสารสนเทศใหม่ และการปรับปรุงแก้ไขระบบสารสนเทศเดิม
16. ผู้ดูแลระบบต้องมีการกำหนดขั้นตอนการทดสอบระบบสารสนเทศก่อนนำไปใช้งานจริง ทั้งในกรณีปรับปรุงระบบสารสนเทศเดิมและการพัฒนาระบบสารสนเทศใหม่
17. ผู้ดูแลระบบต้องติดตั้งซอฟต์แวร์บนระบบสารสนเทศที่ให้บริการ (Production) ตามขั้นตอนที่ รฟม. กำหนด และจำกัดสิทธิ์การติดตั้งซอฟต์แวร์เพื่อให้ระบบสารสนเทศต่าง ๆ มีความถูกต้องครบถ้วนและน่าเชื่อถือ
18. ผู้ดูแลระบบต้องนำซอฟต์แวร์ที่ไม่ละเมิดลิขสิทธิ์มาติดตั้งบนระบบสารสนเทศที่ให้บริการ (Production)
19. ผู้ดูแลระบบต้องกำกับดูแลให้ผู้รับจ้างปฏิบัติตามสัญญาหรือข้อตกลงการให้บริการที่ระบุไว้ โดยครอบคลุมถึงด้านความมั่นคงปลอดภัยสารสนเทศ และการปฏิบัติตามขั้นตอนที่เกี่ยวข้องต่าง ๆ ที่ รฟม. 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 รฟม.
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 ทั้งนี้ เพื่อควบคุมและป้องกันการเข้าถึง การล่วงรู้ และการแก้ไขระบบสารสนเทศของ รฟม. โดยไม่ได้รับอนุญาต

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- เจ้าของข้อมูล
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

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

แนวปฏิบัติ

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

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 รฟม. ให้บรรลุเป้าหมาย รวมทั้งข้อมูลที่เผยแพร่แก่ผู้รับบริการภายนอก

3) ข้อมูลและสารสนเทศที่สนับสนุนการปฏิบัติงานประจำ (Operation data) ได้แก่ ข้อมูลที่สนับสนุนการทำงานทั่วไปของ รฟม.

1.5.2 จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น 3 ระดับ คือ

1) ข้อมูลที่มีระดับความสำคัญมาก หมายถึง ข้อมูลที่ใช้สำหรับสนับสนุนการตัดสินใจของผู้บริหาร

2) ข้อมูลที่มีระดับความสำคัญปานกลาง หมายถึง ข้อมูลที่ใช้ปฏิบัติงานเฉพาะกลุ่มงาน แผนก กอง หรือฝ่ายภายในองค์กร

3) ข้อมูลที่มีระดับความสำคัญน้อย หมายถึง ข้อมูลที่พนักงาน/ลูกจ้างภายใน รฟม. สามารถเข้าถึงร่วมกันได้หรือสามารถเผยแพร่ได้

1.5.3 จัดแบ่งลำดับชั้นความลับของข้อมูลตามที่ รฟม. กำหนด

1.5.4 จัดแบ่งระดับชั้นการเข้าถึง

1) ระดับชั้นสำหรับผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และภารกิจที่ได้รับมอบหมาย

2) ระดับชั้นสำหรับผู้ปฏิบัติงานทั่วไป เข้าถึงข้อมูลที่ได้รับมอบหมายตามอำนาจหน้าที่

3) ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย มีสิทธิ์ในการบริหารจัดการระบบและเข้าถึงข้อมูลที่ได้รับมอบหมายตามอำนาจหน้าที่

1.6 เจ้าของข้อมูลและผู้ดูแลระบบต้องกำหนดเวลาการเข้าถึงระบบสารสนเทศ

1.7 ผู้ดูแลระบบต้องจำกัดช่องทางการเข้าถึงระบบเทคโนโลยีสารสนเทศตามช่องทาง ดังนี้

1) เครือข่ายภายในของ รฟม.

2) เครือข่ายภายนอก รฟม.

3) เครือข่ายอื่นที่จัดไว้ให้ เช่น ระบบเครือข่ายสื่อสารข้อมูล GIN

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

1.9 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องพิจารณาข้อกำหนดต่าง ๆ ที่มีผลทางกฎหมายซึ่งเกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศของ รฟม. เช่น พระราชบัญญัติ ข้อกำหนดทางกฎหมาย ข้อกำหนดในสัญญา

และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่น ๆ เป็นต้น เพื่อกำหนดสิทธิ์การเข้าถึงสารสนเทศและระบบเทคโนโลยีสารสนเทศของ รฟม.

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 รฟม. 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 ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้บริการ ใช้รหัสผ่านอย่างมั่นคงปลอดภัย ดังนี้

<u>กรณีแอปพลิเคชันทั่วไป</u>

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

<u>กรณีแอปพลิเคชันที่ใช้งานผ่านอุปกรณ์เคลื่อนที่ (Mobile device)</u>

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

2.2.12 ผู้ดูแลระบบและผู้ใช้งานต้องใช้รหัสผ่านอย่างปลอดภัย ดังนี้

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

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 รฟม. แก่หน่วยงานภายนอกที่เข้ามาปฏิบัติงานร่วมกับ รฟม.

2.3.7 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจัดให้มีการถอดถอนหรือเปลี่ยนแปลงสิทธิ์การเข้าถึงทันที เมื่อผู้ใช้งานเกษียณ เปลี่ยนแปลงหน้าที่ความรับผิดชอบ เปลี่ยนแปลงการจ้างงาน หรือไม่มีความจำเป็นในการใช้งานระบบเทคโนโลยีสารสนเทศ

2.3.8 ผู้ดูแลระบบต้องลบหรือระงับการใช้งานสิทธิ์ของผู้ใช้งานที่มากับระบบ (Default user) ในกรณีที่มีความจำเป็นต้องใช้งานต้องกำหนดรหัสผ่านอย่างมั่นคงปลอดภัย

2.4 การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of user access rights)

2.4.1 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องมีการสอบทานสิทธิ์การเข้าถึงของผู้ใช้งานระบบเมื่อ รฟม. มีการเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศหรือโครงสร้างองค์กร

2.4.2 ผู้ดูแลระบบ ต้องมีการสอบทานและระงับการใช้งานบัญชีผู้ใช้งานที่ไม่ได้ใช้งานเกิน 180 วัน หากผู้ใช้งานต้องการกลับมาใช้งานจะต้องยืนยันตัวตนให้ ฝทท. ทราบ ทั้งนี้ ระยะเวลาที่ไม่ได้ใช้งานของบัญชีผู้ใช้งานอาจจะขึ้นอยู่กับแต่ละระบบสารสนเทศ

3. การป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล และการควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย

3.1 การป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล (Unattended user equipment)

3.1.1 ผู้ดูแลระบบต้องจัดให้มีมาตรการสำหรับป้องกันระบบคอมพิวเตอร์ ระบบเครือข่ายสื่อสารข้อมูลและระบบเทคโนโลยีสารสนเทศ โดยการกำหนดค่าของระบบ (Configuration) ให้มีการล็อกหน้าจอสำหรับอุปกรณ์ที่ไม่มีพนักงานดูแล หรือล็อกอุปกรณ์อยู่เสมอ

3.1.2 ผู้ใช้งานและหน่วยงานภายนอก ต้องล็อกหน้าจออัตโนมัติเมื่อไม่มีการใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. 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 รฟม. การควบคุมการพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย การป้องกันพอร์ต (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ การแบ่งแยกเครือข่าย (Segregation in networks) อย่างเหมาะสม การควบคุมการเชื่อมต่อทางเครือข่าย และการควบคุมการกำหนดเส้นทางบนเครือข่าย

4.1 การใช้งานบริการเครือข่าย (Use of network services)

4.1.1 ผู้ดูแลระบบต้องควบคุมการเผยแพร่แผนผังระบบเครือข่ายสื่อสารข้อมูล (Network diagram) รวมถึงโครงสร้าง IP address ชื่อระบบ และชื่ออุปกรณ์สารสนเทศแก่ผู้ที่ไม่ได้รับอนุญาตหรือหน่วยงานภายนอก

4.1.2 ผู้ดูแลระบบต้องควบคุมการใช้งานระบบเครือข่ายสื่อสารข้อมูล เพื่อป้องกันการเข้าถึงระบบเครือข่ายสื่อสารข้อมูลและบริการของระบบเครือข่ายสื่อสารข้อมูลโดยไม่ได้รับอนุญาต

4.1.3 ผู้ดูแลระบบต้องควบคุมการเชื่อมต่อเครือข่ายภายนอก เพื่อใช้งานอินเทอร์เน็ต ซึ่งอาจเป็นช่องทางให้หน่วยงานภายนอกเข้าถึงสารสนเทศหรือระบบเทคโนโลยีสารสนเทศของ รฟม. โดยมิได้รับอนุญาต

4.1.4 ผู้ใช้งานต้องแจ้งความประสงค์ในการขอใช้งานบริการเครือข่ายแก่ ฝทท. และสามารถใช้บริการเครือข่ายได้หลังจากได้รับการอนุมัติจาก ฝทท. แล้ว

4.1.5 ผู้ใช้งาน ต้องไม่ใช้ระบบเครือข่ายสื่อสารข้อมูลเพื่อเป็นช่องทางในการเจาะระบบ (Hacking) หรือการสแกนช่องโหว่ของระบบโดยมิได้รับอนุญาต

4.2 การพิสูจน์ตัวตนของผู้ใช้งานที่อยู่ภายนอก รฟม. (User authentication for external connections)

ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนผ่านระบบ Active directory ของ รฟม. ก่อนอนุญาตให้ผู้ใช้งานที่อยู่ภายนอก รฟม. เข้าใช้งานเครือข่ายและระบบสารสนเทศของ รฟม.

4.3 การพิสูจน์ตัวตนของอุปกรณ์ในระบบเครือข่ายสื่อสารข้อมูล (Equipment identification in networks)

ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนของอุปกรณ์ในระบบเครือข่ายสื่อสารข้อมูล ได้แก่ การตรวจสอบ MAC address

4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection)

ผู้ดูแลระบบต้องระงับบริการและพอร์ต (Port) ที่ไม่มีความจำเป็นต้องใช้บนเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่าย

4.5 ผู้ดูแลระบบต้องติดตั้งระบบตรวจจับการบุกรุก (Instrusion prevention system/ instrusion detection system) ของระบบเครือข่าย

4.6 การแบ่งแยกเครือข่าย (Segregation in networks)

4.6.1 ผู้ดูแลระบบต้องจัดให้มีการแบ่งแยกเครือข่ายตามกลุ่มของผู้ใช้งาน หรือกลุ่มของระบบเทคโนโลยีสารสนเทศ เพื่อควบคุมการใช้งานในแต่ละเครือข่ายย่อยอย่างเหมาะสม โดยพิจารณาจากความ

ต้องการในการเข้าถึงข้อมูล ระดับความสำคัญของข้อมูล รวมถึงการพิจารณาด้านราคา ประสิทธิภาพ และผลกระทบทางด้านความปลอดภัยดังต่อไปนี้

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

4.6.2 ผู้ดูแลระบบจะกำหนดเส้นทางบนเครือข่ายที่เข้มงวด เพื่อจำกัดการเข้าถึงระยะไกลไปเฉพาะเครือข่ายที่กำหนดเท่านั้น

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

4.7 การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control)

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

4.7.2 ผู้ดูแลระบบต้องติดตั้ง Firewall ระหว่างเครือข่ายของ รฟม. กับเครือข่ายภายนอก ทั้งนี้ การติดตั้ง Firewall ต้องพิจารณาเรื่องดังต่อไปนี้

1) การป้องกันการจราจรจากภายนอก ต้องถูกกำหนดให้ใช้เส้นทางที่ผ่าน First tier firewall ที่มีความมั่นคงปลอดภัยเพื่อป้องกันทรัพย์สินสารสนเทศของ รฟม. และโครงสร้างพื้นฐานที่มีความสำคัญจากการเข้าถึงที่ไม่ได้รับอนุญาต
2) Firewall ต้องระบุตัวตนและพิสูจน์ตัวตนของผู้ใช้งานก่อนที่จะให้สิทธิ์การเข้าถึงอินเทอร์เฟส (Interface) เพื่อการบริหารจัดการ Firewall
3) Firewall ต้องตั้งค่าให้ระงับบัญชีผู้ใช้งานหลังจากมีความพยายามที่จะเข้าสู่ระบบไม่สำเร็จ 5 ครั้ง การยกเลิกการระงับต้องดำเนินการโดย ฝทท.
4) ไม่อนุญาตให้พิสูจน์ตัวตนผ่านทางอินเทอร์เฟส (Interface) การจัดการ Firewall จากระยะไกล (Remote)
5) ผู้ที่ได้รับการมอบหมายจาก ฝทท. เท่านั้นที่มีสิทธิ์ที่จะเปลี่ยนการตั้งค่าด้านความปลอดภัยบน Firewall
6) Firewall ต้องตั้งค่าให้บันทึกเหตุการณ์ด้านความมั่นคงปลอดภัย
7) Firewall ต้องได้รับการสอบทาน ทดสอบ และตรวจสอบอย่างสม่ำเสมอ
8) Firewall ต้องถูกบริหารจัดการผ่านทางการติดต่อสื่อสารที่มีการเข้ารหัส
9) ต้องปิดบริการและพอร์ต (Port) ที่ไม่จำเป็นต้องใช้บน Firewall

10) Firewall ประเภทซอฟต์แวร์ (Software) ต้องติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายแยกต่างหาก

11) Firewall ต้องสามารถป้องกันตัวเองจากการโจมตี DOS (Denial of service) ได้ อย่างเช่น Ping, Sweeps หรือ TCP SYN Floods เป็นต้น

12) ต้องใช้เวอร์ชันของซอฟต์แวร์ (Software) Firewall และระบบปฏิบัติการที่เจ้าของผลิตภัณฑ์ยังให้การสนับสนุน

13) ผู้ดูแล Firewall ต้องติดตามข้อมูลช่องโหว่จากผู้ให้บริการ (Vendor) เพื่อรับทราบข่าวสาร การ Upgrade และแพ็ตช์ (Patch) ที่จำเป็น และต้องติดตั้งแพ็ตช์ (Patch) ทั้งหมดที่เกี่ยวข้อง

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

1) เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการผ่านอินเทอร์เน็ต เช่น FTP, Email, Web และ External DNS server เป็นต้น ต้องติดตั้งอยู่ใน DMZ

2) การเข้าถึงจากระยะไกลต้องพิสูจน์ตัวตนที่ Firewall หรือผ่านบริการที่อยู่ใน DMZ

3) DNS Servers ต้องไม่อนุญาตให้มีการแลกเปลี่ยนโซน (Zone transfers) เว้นแต่มีเหตุจำเป็น

4.8 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control)

ผู้ดูแลระบบต้องควบคุมการกำหนดเส้นทางบนเครือข่ายเพื่อให้มั่นใจว่าการเชื่อมต่อเครื่องคอมพิวเตอร์และการไหลเวียนของสารสนเทศบนเครือข่าย โดยมีกลไกในการตรวจสอบที่อยู่ปลายทางและต้นทางของการเชื่อมต่อ เช่น การควบคุมโดย Firewall หรือ Proxy เป็นต้น

5. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)

ให้มีการควบคุมการเข้าถึงระบบปฏิบัติการอย่างมั่นคงปลอดภัย การควบคุมการระบุและพิสูจน์ตัวตนของผู้ใช้งาน การควบคุมระบบบริหารจัดการรหัสผ่าน การควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ (System utilities) การควบคุมการหมดเวลาการใช้งานระบบเทคโนโลยีสารสนเทศ และควบคุมการจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ

5.1 ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on procedures)

5.1.1 ผู้ดูแลระบบ ต้องจัดให้มีการควบคุมการเข้าถึงระบบปฏิบัติการอย่างมั่นคงปลอดภัยโดยขั้นตอนการเข้าสู่ระบบต้องเปิดเผยข้อมูลเกี่ยวกับระบบให้น้อยที่สุดเพื่อหลีกเลี่ยงผู้ใช้งานที่ไม่ได้รับอนุญาต ซึ่งขั้นตอนการ Log-on ต้องพิจารณา ดังนี้

1) หากกระบวนการเข้าสู่ระบบไม่สำเร็จ ระบบต้องไม่แสดงข้อมูลของระบบหรือแอปพลิเคชัน (Application) ที่ใช้งานอยู่

2) ระบบต้องแสดงข้อความเตือนผู้ใช้งานว่าสามารถเข้าใช้งานเครื่องคอมพิวเตอร์ได้เฉพาะผู้ที่มีสิทธิ์เท่านั้น

3) หากกระบวนการเข้าสู่ระบบไม่สำเร็จ ระบบต้องไม่แสดงข้อมูลที่สามารถระบุตัวตนของระบบ เช่น เครือข่ายที่ใช้งาน สถานที่ตั้งของระบบ หรือชื่อเครื่องคอมพิวเตอร์แม่ข่าย เป็นต้น

4) ระบบต้องไม่แสดงข้อความที่ชี้เฉพาะเหตุของการเข้าสู่ระบบไม่สำเร็จ เช่น ไม่แสดงข้อความว่าบัญชีผู้ใช้งานผิด หรือ รหัสผ่านผิด เป็นต้น
5) ห้ามเข้าสู่ระบบจากบัญชีผู้ใช้งานส่วนบุคคลเดียวกันมากกว่าหนึ่ง Session ในระบบเดียวกัน
6) ระบบต้องจำกัดจำนวนครั้งในการพยายามเข้าสู่ระบบที่ไม่สำเร็จ และต้องพิจารณาเงื่อนไขต่อไปนี้
   (ก) การเก็บบันทึกผลการเข้าสู่ระบบทั้งที่สำเร็จและไม่สำเร็จ
   (ข) หน่วงระยะเวลาในการเข้าใช้งานระบบครั้งต่อไป
   (ค) การตัดการเชื่อมต่อ
   (ง) การแสดงข้อความเตือนที่หน้าจอของผู้ดูแลระบบเมื่อมีการเข้าสู่ระบบเกินจำนวนครั้งที่จำกัดไว้
7) ระบบต้องแสดงวัน เวลา ในการเข้าสู่ระบบที่สำเร็จในครั้งก่อน พร้อมทั้งบันทึกจำนวนครั้งที่พยายามเข้าไม่สำเร็จนับแต่การเข้าสู่ระบบที่สำเร็จในครั้งก่อนของผู้ใช้งาน
8) ระบบต้องไม่ส่งรหัสผ่านแบบ Clear text ผ่านระบบเครือข่ายสื่อสารข้อมูล
9) ผู้ดูแลระบบต้องกำหนดจำนวนครั้งที่ยอมให้ใส่รหัสผ่านผิดได้ไม่เกิน 5 ครั้ง

5.2 การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication)

ผู้ดูแลระบบ ต้องจัดให้ผู้ใช้งานมีบัญชีผู้ใช้งานของแต่ละบุคคลเพื่อใช้พิสูจน์ตัวตนในการเข้าถึงระบบเทคโนโลยีสารสนเทศ และต้องใช้ระบบเทคโนโลยีสารสนเทศพิสูจน์ตัวตนผู้ใช้งานในการเข้าถึงระบบปฏิบัติการ โดยผ่านระบบ Active directory หรือ Lightweight Derectory Access Protocol (LDAP) ทุกครั้ง พร้อมทั้งบันทึกข้อมูลการเข้าถึง

5.3 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities)

ผู้ดูแลระบบ ต้องควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้บนระบบที่ใช้งานจริง (Production system) ดังนี้

5.3.1 ต้องจัดทำบัญชีโปรแกรมประเภทยูทิลิตี้ (System utilities) ที่นำมาใช้งาน

5.3.2 กำหนดความรับผิดชอบในการใช้โปรแกรมประเภทยูทิลิตี้ (System utilities) แต่ละรายการอย่างชัดเจนและสื่อสารให้ผู้เกี่ยวข้องทราบเพื่อถือปฏิบัติ

5.3.3 ให้มีการพิสูจน์ตัวตน และกำหนดสิทธิ์ในการใช้งานโปรแกรมประเภทยูทิลิตี้เฉพาะกลุ่มคนที่มีหน้าที่รับผิดชอบ

5.3.4 มีการบันทึกเหตุการณ์ (Log) การใช้งานโปรแกรมประเภทยูทิลิตี้ และต้องสอบทานจากผู้ดูแลระบบอย่างสม่ำเสมอ

5.3.5 ต้องทำการเพิกถอนหรือระงับโปรแกรมประเภทยูทิลิตี้ที่ไม่จำเป็น

5.4 การหมดเวลาการใช้งานระบบสารสนเทศ (Session time-out)

5.4.1 ผู้ดูแลระบบต้องกำหนด Session time-out ของระบบเทคโนโลยีสารสนเทศที่ไม่มีการใช้งานภายในระยะเวลา 15 นาที ทั้งนี้ ถ้าระบบที่ไม่สามารถตัดการเชื่อมต่อแบบอัตโนมัติได้ กำหนดให้ใช้โปรแกรมพักหน้าจอที่ต้องใส่รหัสผ่านหรือกำหนดให้มีการล็อกหน้าจอ

5.4.2 ผู้ดูแลระบบ และผู้ใช้งาน ต้องตั้งค่าให้มีโปรแกรมพักหน้าจอที่ต้องใส่รหัสผ่านสำหรับเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์แบบพกพา และเครื่องคอมพิวเตอร์แม่ข่าย ทั้งนี้

โปรแกรมพักหน้าจอกำหนดให้ป้อนรหัสผ่านหลังจากที่มีการทิ้งเครื่องดังกล่าวไว้โดยไม่มีการใช้งานเป็นเวลา 15 นาที

5.5 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)

5.5.1 ผู้ดูแลระบบ ต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง โดยต้องคำถึงระยะเวลาที่จำเป็นในกระบวนการดำเนินงานทางธุรกิจ ได้แก่ กำหนดให้เข้าใช้งานได้ในช่วงเวลาทำการของ รฟม. 08.00 น. – 17.00 น. และเชื่อมต่อเพื่อใช้งานได้ครั้งละไม่เกิน 3 ชั่วโมง

5.5.2 ผู้ใช้งาน หากมีความจำเป็นต้องใช้งานนอกเวลาที่กำหนดต้องขออนุมัติจากผู้บังคับบัญชาเท่านั้น

6. การควบคุมการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ (Application and information access control)

ให้มีการจำกัดการเข้าถึงสารสนเทศ และการแยกระบบเทคโนโลยีสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณที่ควบคุมเฉพาะ

6.1 การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)

6.1.1 เจ้าของข้อมูลและผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงแก่ผู้ใช้งานเท่าที่จำเป็นต้องใช้ในการปฏิบัติงาน โดยการให้สิทธิ์ต้องพิจารณาในเรื่องดังต่อไปนี้

1) การจำกัดไม่ให้ใช้ตัวเลือก (Options) ที่ไม่ได้รับอนุญาต
2) การจำกัดการเข้าถึง Command Line
3) การจำกัดการเข้าถึงข้อมูลและฟังก์ชันการใช้งานของแอปพลิเคชัน (Application) ที่ไม่เกี่ยวข้องกับหน้าที่ความรับผิดชอบ
4) การจำกัดระดับสิทธิ์ในการเข้าถึงไฟล์ เช่น อ่านอย่างเดียว เป็นต้น
5) การควบคุมการแจกจ่าย การเข้าถึงข้อมูล การนำข้อมูลออกจากระบบสารสนเทศ เช่น รายงาน เป็นต้น

6.1.2 เจ้าของข้อมูลและผู้ดูแลระบบ ควรกำหนดให้ระบบสารสนเทศรองรับการกำหนดสิทธิ์ในการเข้าถึงแบบกลุ่มได้

6.2 การแยกระบบสารสนเทศที่ไวต่อการรบกวน (Sensitive system isolation) มีผลกระทบต่อคนกลุ่มใหญ่ หรือระบบที่มีความสำคัญต่อหน่วยงาน ต้องดำเนินการดังนี้

6.2.1 เจ้าของข้อมูลและผู้ดูแลระบบ แยกระบบซึ่งไวต่อการรบกวนออกจากระบบอื่น ๆ และควบคุมสภาพแวดล้อมของระบบโดยเฉพาะ ได้แก่ ระบบ File sharing ระบบสารสนเทศทางการเงิน และระบบ Active directory โดยเข้าถึงได้ทั้งอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร (Mobile computing and teleworking)

6.2.2 ผู้ดูแลระบบต้องควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์เคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile computing and teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

6.2.3 เจ้าของข้อมูลที่เป็นเจ้าของระบบสารสนเทศที่มีความสำคัญสูงต้องเป็นผู้อนุญาต ในกรณีที่ระบบสารสนเทศที่มีความสำคัญสูงมีความจำเป็นต้องทำงานร่วมกับระบบสารสนเทศอื่นที่มีความสำคัญน้อยกว่า

7. การควบคุมการปฏิบัติงานจากภายนอก รฟม. (Teleworking)

7.1 ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนการใช้งาน และเชื่อมต่อผ่านช่องทางที่มีความปลอดภัยที่มีเทคโนโลยีเข้ารหัสป้องกัน

7.2 ผู้ดูแลระบบต้องทำการถอดถอนสิทธิ์ในการเข้าถึงของผู้ใช้งานจากภายนอกสำนักงาน เมื่อครบกำหนดระยะเวลาที่ขออนุญาต

7.3 ผู้ใช้งาน หากจำเป็นต้องมีการปฏิบัติงานจากภายนอกสำนักงานของ รฟม. ต้องได้รับการอนุญาตจากผู้บังคับบัญชาอย่างเป็นลายลักษณ์อักษร ในกรณีเร่งด่วนสามารถดำเนินการก่อน โดยแจ้งให้ผู้บังคับบัญชารับทราบด้วย โดยผู้บังคับบัญชาต้องพิจารณาเงื่อนไขในการเตรียมการ ดังต่อไปนี้

1) ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมของการปฏิบัติงานจากภายนอก รฟม.
2) ความมั่นคงปลอดภัยทางการสื่อสาร โดยยึดจากระดับความสำคัญ (Sensitivity) ของข้อมูลที่จะถูกเข้าถึงและส่งผ่านช่องทางการเชื่อมต่อสื่อสาร (Communication link) รวมถึงระดับความสำคัญ (Sensitivity) ของระบบภายใน รฟม.

7.4 ผู้ใช้งานต้องจัดเก็บเอกสารที่เป็นความลับในอุปกรณ์ที่ล็อกได้และมีการควบคุมการเข้าถึง โดยใช้หลักเกณฑ์การรักษาความลับเช่นเดียวกับสารสนเทศที่อยู่ในสำนักงานของ รฟม.

7.5 ผู้ใช้งาน ต้องติดตั้งโปรแกรมป้องกันไวรัสและ Personal firewall สำหรับอุปกรณ์ส่วนตัวที่ใช้เชื่อมต่อเครือข่ายของ รฟม. จากภายนอก

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

ส่วนที่ 7
การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

วัตถุประสงค์

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

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

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

แนวปฏิบัติ

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

ส่วนที่ 8
การควบคุมหน่วยงานภายนอกและผู้ใช้งานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

- เพื่อควบคุมหน่วยงานภายนอกและผู้ใช้งานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. ให้เป็นไปอย่างมั่นคงปลอดภัย

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้บังคับบัญชา
- หน่วยงานภายนอก
- ผู้ใช้งาน (บุคคลภายนอก)

อ้างอิงมาตรฐาน

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

แนวปฏิบัติ

1. ผู้ดูแลระบบต้องประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอกและผู้ใช้งานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศของ รฟม.
2. การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอกและผู้ใช้งานภายนอก
    2.1 เจ้าของข้อมูลต้องเป็นผู้อนุญาตการให้สิทธิ์แก่หน่วยงานภายนอกและผู้ใช้งานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของ รฟม. อย่างเป็นลายลักษณ์อักษร
    2.2 ผู้บังคับบัญชาต้องกำหนดให้มีการลงนามการไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของ รฟม.
    2.3 ผู้บังคับบัญชา ต้องควบคุมให้มีการกำหนดข้อตกลงและความรับผิดชอบที่เกี่ยวข้องกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศลงในสัญญากับหน่วยงานภายนอกที่ให้บริการด้านสารสนเทศและบริการด้านการสื่อสาร โดยให้ครอบคลุมรวมถึงผู้รับจ้างช่วง
    2.4 ผู้บังคับบัญชาต้องกำหนดให้จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกและผู้ใช้งานภายนอกระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศ ซึ่งมีรายละเอียด ดังนี้
        2.4.1 เหตุผลในการขอใช้
        2.4.2 ระยะเวลาในการใช้
        2.4.3 การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย
        2.4.4 การตรวจสอบ MAC address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

2.5 ผู้ดูแลระบบมีสิทธิ์ในการตรวจสอบการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอกและผู้ใช้งานภายนอก เพื่อควบคุมการใช้งานได้อย่างมั่นคงปลอดภัยตามสัญญา

2.6 ผู้ดูแลระบบต้องควบคุมให้หน่วยงานภายนอกจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งต้องปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อใช้สำหรับควบคุมหรือตรวจสอบการทำงาน และเพื่อให้มั่นใจว่าการปฏิบัติงานเป็นไปตามขอบเขตที่ได้กำหนดไว้

3. ผู้ดูแลระบบต้องแจ้งแนวปฏิบัติต่าง ๆ ที่เกี่ยวข้องแก่หน่วยงานภายนอกและผู้ใช้งานภายนอกเพื่อให้ปฏิบัติตาม
4. ผู้ดูแลระบบ ต้องกำกับดูแลหน่วยงานภายนอกและผู้ใช้งานภายนอกให้ปฏิบัติตามสัญญาหรือข้อตกลงการให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงด้านความมั่นคงปลอดภัย
5. ผู้ดูแลระบบ ต้องติดตาม ตรวจสอบรายงานหรือบันทึกการให้บริการของหน่วยงานภายนอกตามที่ว่าจ้างอย่างสม่ำเสมอตามสัญญาว่าจ้าง
6. ผู้ดูแลระบบ ต้องกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีหน้าที่ในการกำกับดูแล หรือหน่วยงานที่เกี่ยวข้องกับการบังคับใช้กฎหมาย รวมทั้งหน่วยงานที่ควบคุมดูแลสถานการณ์ฉุกเฉินภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน
7. ผู้ดูแลระบบ ต้องมีขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีความเชี่ยวชาญเฉพาะด้านหรือหน่วยงานที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน
8. ผู้ดูแลระบบต้องควบคุมการเปลี่ยนแปลงของหน่วยงานภายนอกที่ส่งผลกระทบต่อการให้บริการขององค์กร และต้องประเมินความเสี่ยงอย่างเหมาะสมเพื่อควบคุมผลกระทบอันเนื่องมาจากการเปลี่ยนแปลงนั้น
9. หน่วยงานภายนอกและผู้ใช้งานภายนอก ต้องใช้งานทรัพย์สินสารสนเทศของ รฟม. ด้วยความระมัดระวัง และรักษาความลับของ รฟม. ไม่นำไปเปิดเผย และต้องขออนุญาตพร้อมทั้งปฏิบัติตามเงื่อนไขในการเข้าถึงระบบสารสนเทศของ รฟม. ทุกครั้ง
10. หน่วยงานภายนอกและผู้ใช้งานภายนอกต้องแจ้งเหตุการณ์ไม่ปกติต่าง ๆ ด้านเทคโนโลยีสารสนเทศที่พบผ่านช่องทางที่ รฟม. กำหนดโดยเร็วที่สุด
11. หน่วยงานภายนอกและผู้ใช้งานภายนอกต้องจัดเก็บบัญชีผู้ใช้งานที่ รฟม. จัดทำไว้ให้ใช้งานเป็นความลับ เฉพาะบุคคล ไม่เปิดเผยให้ผู้อื่นรับทราบ

ส่วนที่ 9
การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ ของ รฟม.

วัตถุประสงค์

- เพื่อควบคุมการใช้งานทรัพย์สินของ รฟม. ประเภทเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ให้เหมาะสม 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 รฟม. ไม่สามารถควบคุมการใช้งานผ่านระบบ Active Directory ได้
    1.4 ผู้ใช้งานต้องใช้งานอย่างมีประสิทธิภาพเพื่องานของ รฟม.
    1.5 ผู้ใช้งานต้องไม่ติดตั้งโปรแกรมที่ละเมิดลิขสิทธิ์บนเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ของ รฟม.
    1.6 ผู้ใช้งานต้องขอนุญาตติดตั้งโปรแกรมในเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ตามขั้นตอนที่ รฟม. กำหนด
    1.7 ผู้ใช้งานต้องไม่ติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ของ รฟม. การดำเนินการดังกล่าวต้องดำเนินการโดยผู้ดูแลระบบเท่านั้น
    1.8 ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่อย่างละเอียด เพื่อให้สามารถใช้งานอย่างปลอดภัยและมีประสิทธิภาพ
    1.9 ผู้ใช้งานต้องไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ และรักษาให้มีสภาพเดิม
    1.10 ผู้ใช้งานต้องแจ้งซ่อมเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ที่อยู่ในความรับผิดชอบของ ฝทท. ให้ ฝทท. เป็นผู้ดำเนินการเท่านั้น
    1.11 ผู้ใช้งานต้องอัปเดต Patch และระบบปฏิบัติการให้ทันสมัยอยู่เสมอ
    1.12 ผู้ใช้งานต้องไม่สร้าง Shortcut ไว้บน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของ รฟม.

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 รฟม. 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 การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจำทำให้หน้าจอมีรอยขีดข่วนได้

1.13.15 รับผิดชอบในการป้องกันการสูญหาย เช่น ต้องล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

1.13.16 นำติดตัวไปด้วยเสมอ เช่น ไม่ละทิ้ง อุปกรณ์ประมวลผลประเภทพกพาในรถยนต์ ห้องพักในโรงแรม หรือห้องประชุม เป็นต้น ในกรณีที่มีความจำเป็นต้องละทิ้งให้จัดเก็บไว้ในสถานที่มั่นคงปลอดภัย

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 รฟม.

3.5 ผู้ใช้งาน หากพบหรือสงสัยว่าเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ติดชุดคำสั่งไม่พึงประสงค์ ให้รีบยกเลิกเชื่อมต่อเครื่องเข้ากับระบบเครือข่ายสื่อสารข้อมูลเพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่น ๆ ได้ และแจ้ง ฝทท. ทราบทันที

4. การสำรองข้อมูลและการกู้คืน

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

4.2 ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

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

ส่วนที่ 10
การใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์

วัตถุประสงค์

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

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

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

แนวปฏิบัติ

1. ผู้ดูแลระบบต้องควบคุมการเชื่อมต่อทางเครือข่ายสำหรับการเข้าถึงอินเทอร์เน็ตโดยพิจารณาเรื่องดังต่อไปนี้
   1) ผู้ดูแลระบบต้องไม่อนุญาตให้ใช้งานอุปกรณ์ Video streaming อุปกรณ์ audio streaming หรือ Download ไฟล์ที่มีขนาดใหญ่ ในกรณีที่จำเป็นต้องได้รับการอนุญาตจากผู้บังคับบัญชาก่อนเท่านั้น
   2) ผู้ดูแลระบบต้องจำกัดการใช้งานอินเทอร์เน็ตเพื่อเรื่องส่วนตัวหรือที่ไม่ใช่การดำเนินงานของ รฟม. ให้น้อยที่สุดเท่าที่เป็นไปได้ เช่น การระงับการเข้าถึง Website ที่ไม่จำเป็น การระงับการเข้าถึง Website ที่มีเนื้อหาต้องห้ามตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
   3) ผู้ดูแลระบบต้องป้องกันไม่ให้มีการรับส่งข้อมูลที่ไม่เหมาะสมจากภายนอก รฟม. เช่น
      (ก) Executable เช่น .EXE .COM เป็นต้น
      (ข) ไฟล์ (File) เสียง เช่น AUD .WAV และ.MP3 เป็นต้น
      (ค) ไฟล์ (File) วีดิทัศน์ เช่น .MPG .MPEG .MOV และ .AVI เป็นต้น
      (ง) Peer to Peer เช่น .torrent เป็นต้น

      ในกรณีที่มีความจำเป็นต้องได้รับอนุญาตจากผู้บังคับบัญชา และ ฝทท.
   4) ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่ รฟม. จัดสรรไว้เท่านั้น เช่น Proxy, Firewall เป็นต้น
   5) ผู้ดูแลระบบต้องทดสอบเส้นทางสำหรับการเชื่อมต่ออินเทอร์เน็ตขององค์กรระหว่างเส้นทางที่ใช้งานจริงและเส้นทางสำรองอย่างน้อยปีละ 2 ครั้ง
   6) ผู้ใช้งานต้องไม่เชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นมีความจำเป็นและขออนุญาตจาก ฝทท. 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. ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของ รฟม. เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น
6. ผู้ใช้งานจะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของ รฟม.
7. ผู้ใช้งานต้องหลีกเลี่ยงการกระทำที่สิ้นเปลืองทรัพยากรของเครือข่ายอินเทอร์เน็ต ดังนี้
    (ก) ส่งจดหมายอิเล็กทรอนิกส์ลูกโซ่
    (ข) ใช้เวลาในการเข้าถึงอินเทอร์เน็ตเกินความจำเป็นยกเว้นเพื่อปฏิบัติงานให้ รฟม.
    (ค) เล่นเกม Online
    (ง) เข้าห้องพูดคุย Online ที่ไม่ได้มีวัตถุประสงค์เพื่อปฏิบัติงานให้ รฟม.
8. ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับ รฟม.
9. ผู้ใช้งานต้องไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของ รฟม.
10. ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต
11. ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ที่จะทำให้ผู้อื่นเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย
12. ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน
13. ผู้ใช้งานต้องคำนึงว่าข้อมูลจากอินเทอร์เน็ตอาจไม่มีความทันสมัยหรือไม่มีความถูกต้อง ผู้ใช้งานต้องตรวจสอบความถูกต้องของข้อมูลจากแหล่งที่น่าเชื่อถือก่อนที่จะเผยแพร่ข้อมูลดังกล่าว
14. ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา
15. ผู้ใช้งานต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้ายในการเสนอความคิดเห็นที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของ รฟม. การทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น ๆ
16. ผู้ใช้งานต้องไม่บันทึกรหัสผ่านใน Web browser (Remember password) เพื่อป้องกันบุคคลอื่นที่สามารถเข้าถึงคอมพิวเตอร์ของผู้ใช้งานนำรหัสผ่านดังกล่าวไปใช้งานในอินเทอร์เน็ตโดยไม่ได้รับอนุญาต

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

19.10 ผู้ใช้งานต้องตระหนักไว้เสมอว่าข้อมูลต่าง ๆ ที่ผู้ใช้งานเผยแพร่ไว้บนบริการสื่อสังคมออนไลน์นั้นคงอยู่ถาวรและผู้อื่นอาจเข้าถึงและเผยแพร่ข้อมูลเหล่านั้นได้

19.11 ผู้ใช้งานต้องมีข้อพิจารณาในการรับเพื่อนเข้ากลุ่มที่ชัดเจน และควรประกาศข้อความปฏิเสธความรับผิดชอบที่เกี่ยวกับเนื้อหาหรือข้อความแสดงความคิดเห็นซึ่งถูกโพสต์จากเพื่อนในกลุ่มที่อาจปรากฏในเว็บไซต์ประเภท Social network ของผู้ใช้งานเอง

19.12 ผู้ใช้งานต้องติดตั้งซอฟต์แวร์ป้องกันไวรัส และอัปเดตฐานข้อมูลไวรัสของโปรแกรมอยู่เสมอ และต้องหลีกเลี่ยงการใช้โปรแกรมที่ละเมิดลิขสิทธิ์เพราะอาจจะมีโปรแกรมประสงค์ร้ายแฝงตัวอยู่ภายในเพื่อลักลอบ ปลอมแปลง หรือขโมยข้อมูลสำคัญของผู้ใช้งานได้

19.13 ผู้ใช้งานต้องระมัดระวังการใช้ถ้อยคำและภาษาที่อาจเป็นการดูหมิ่น ยุยง ท้าทาย หรือเป็นการละเมิดต่อบุคคลอื่น กรณีบุคคลอื่นมีความคิดเห็นที่แตกต่างพึงงดเว้นการโต้ตอบด้วยถ้อยคำรุนแรง

19.14 ผู้ใช้งานต้องระมัดระวังกระบวนการหาข่าว หรือภาพจากสื่อสังคมออนไลน์ โดยมีการตรวจสอบอย่างถี่ถ้วนรอบด้านและต้องอ้างอิงแหล่งที่มาเมื่อนำเสนอ เว้นแต่สามารถตรวจสอบและอ้างอิงจากแหล่งข่าวได้โดยตรง

19.15 หากผู้ใช้งานต้องการใช้สื่อสังคมออนไลน์เป็นเครื่องมือในการรายงานข่าวในนามของบุคคลธรรมดาต้องแสดงให้ชัดเจนว่า ข้อความใดเป็น "ข่าว" ข้อความใดเป็น "ความคิดเห็นส่วนตัว"

19.16 การส่งต่อหรือเผยแพร่ข้อมูลในสื่อสังคมออนไลน์ (Social media)

19.16.1 ผู้ใช้งานต้องไม่ส่งต่อหรือเผยแพร่ข้อมูลที่เป็นเท็จ ข่าวลือ ข่าวไม่ปรากฏที่มา เป็นเพียงการคาดเดา หรือส่งผลเสียหายกับบุคคล สังคม หรือ รฟม.

19.16.2 ผู้ใช้งานต้องไม่ส่งต่อหรือเผยแพร่ข้อมูลเรื่องบุคคลเสียชีวิต เด็กและเยาวชน ผู้สูญหาย ผู้ต้องหา เว้นเสียแต่ตรวจสอบข้อเท็จจริงแล้วและเห็นว่าเป็นประโยชน์ต่อสาธารณะ

19.16.3 ผู้ใช้งานต้องไม่ส่งต่อหรือเผยแพร่ข้อมูลที่กระทบต่อสิทธิความเป็นส่วนตัว และศักดิ์ศรีความเป็นมนุษย์

19.17 ผู้ใช้งานต้องตั้งค่าความปลอดภัยของการใช้งานสื่อสังคมออนไลน์ และระมัดระวังการถูกนำข้อมูลจากชื่อบัญชีไปใช้โดยไม่เหมาะสม ผิดวัตถุประสงค์ และลักษณะการแอบอ้างโดยบุคคลอื่น

20. ผู้ใช้งานต้องใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์โดยตระหนักถึงพระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่บังคับใช้อยู่เสมอ

ส่วนที่ 11
การใช้งานจดหมายอิเล็กทรอนิกส์

วัตถุประสงค์

- เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ของ รฟม. ให้มีความปลอดภัยและมีประสิทธิภาพ

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

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

แนวปฏิบัติ

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

ส่วนที่ 12
การสำรองข้อมูลและการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

วัตถุประสงค์

- เพื่อให้มีข้อมูลสำรองไว้ใช้งานในกรณีที่ข้อมูลหลักเกิดความเสียหายไม่สามารถใช้งานหรือเข้าถึงได้ หรือเมื่อเกิดภาวะฉุกเฉินต่าง ๆ
- เพื่อให้มีการปฏิบัติที่สอดคล้องกับกฎหมาย พระราชบัญญัติ หรือข้อบังคับภายนอกอื่น ๆ

ผู้รับผิดชอบ

- ผู้บังคับบัญชา
- ผู้ดูแลระบบ
- เจ้าของข้อมูล
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

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

แนวปฏิบัติ

1. การสำรองข้อมูลระบบแม่ข่าย

   ข้อมูลระบบแม่ข่ายและข้อมูลสำคัญซึ่งเป็นความลับของ รฟม. ต้องได้รับการเก็บรักษาไว้ที่ระบบเก็บข้อมูลส่วนกลาง และสำรองข้อมูลไว้อย่างสม่ำเสมอ เพื่อให้มีข้อมูลสำรองไว้ใช้ ในกรณีที่ข้อมูลหลักเกิดความเสียหายหรือไม่สามารถใช้งาน ความถี่ในการดำเนินการสำรองข้อมูลและขั้นตอนการสำรองข้อมูลระบบแม่ข่ายเป็นความรับผิดชอบของ ฝทท. โดยมีแนวปฏิบัติ ดังนี้

   1.1 ผู้บังคับบัญชากำหนดผู้รับผิดชอบในการสำรองข้อมูล

   1.2 ผู้ดูแลระบบต้องกำหนดชนิดของข้อมูลของระบบที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้ เช่น ข้อมูลค่าคอนฟิกกูเรชัน (Configuration) ข้อมูลคู่มือการปฏิบัติงานสำหรับระบบ ข้อมูลในฐานข้อมูลของระบบงาน ข้อมูลซอฟต์แวร์ เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ระบบงาน และซอฟต์แวร์อื่น ๆ เป็นต้น

   1.3 ผู้ดูแลระบบต้องสำรองข้อมูลตามความถี่ที่กำหนดไว้ ทั้งนี้ หากเป็นข้อมูลที่สนับสนุนกระบวนการทำงานที่สำคัญของ รฟม. ให้สำรองตามความถี่ที่ รฟม. กำหนด

   1.4 ผู้ดูแลระบบต้องตรวจสอบว่าการสำรองข้อมูลสำเร็จครบถ้วนหรือไม่ หากไม่สำเร็จให้หาสาเหตุและดำเนินการแก้ไขอีกครั้งหนึ่ง

   1.5 ผู้ดูแลระบบต้องนำข้อมูลที่สำรองไว้ไปเก็บไว้ทั้งภายในและนอก รฟม. อย่างน้อยอย่างละ 1 ชุด

   1.6 ผู้ดูแลระบบทดสอบกู้คืนข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าข้อมูลที่สำรองไว้มีความถูกต้อง ครบถ้วน และพร้อมใช้งาน

2. การสำรองข้อมูลคอมพิวเตอร์ส่วนบุคคล
ผู้ใช้งานจะต้องสำรองข้อมูลสำคัญที่เก็บรักษาไว้ในเครื่องคอมพิวเตอร์ส่วนบุคคลหรือคอมพิวเตอร์ หรืออุปกรณ์พกพาอื่น ๆ อย่างสม่ำเสมอ ความถี่ในการสำรองข้อมูลขึ้นอยู่กับความถี่ของการเปลี่ยนแปลงของข้อมูลและระดับความสำคัญของข้อมูลหากเกิดการสูญหาย
3. การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์
เพื่อให้สามารถระบุตัวบุคคลผู้ใช้งานได้อย่างถูกต้อง ผู้ดูแลระบบต้องดำเนินการดังนี้
   3.1 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 2) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 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 รฟม.
5. ผู้บังคับบัญชา ต้องควบคุมให้มีการป้องกันข้อมูลสำคัญขององค์กร ข้อมูลสำคัญที่เกี่ยวข้องกับข้อกำหนดทางกฎหมาย ระเบียบ ข้อบังคับ สัญญา ควรได้รับการป้องกันจากการสูญหาย ถูกทำลาย และปลอมแปลง

6. ผู้บังคับบัญชาต้องจัดให้มีการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยผู้ตรวจสอบภายใน (Internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External auditor) ตามระยะเวลาอย่างน้อยปีละ 1 ครั้ง
7. ผู้ดูแลระบบต้องกำหนดกระบวนการตรวจสอบและการแจ้งเตือนเมื่อเกิดเหตุผิดปกติเกี่ยวกับการใช้งานทรัพยากร (Capacity) กำหนดเกณฑ์การใช้งานทรัพยากรและวางแผนด้านทรัพยากรสารสนเทศให้รองรับการปฏิบัติงานในอนาคตอย่างเหมาะสม รวมถึงต้องติดตามผลการใช้งานทรัพยากรสารสนเทศ
8. ผู้ดูแลระบบต้องมีการตรวจสอบการทำงาน (Monitor) ของระบบรักษาความปลอดภัยและระบบปฏิบัติการอย่างสม่ำเสมอ
9. ผู้ดูแลระบบ ต้องป้องกันการเข้าใช้งานเครื่องมือที่ใช้เพื่อการตรวจสอบ เพื่อมิให้เกิดการใช้งานผิดประเภทหรือถูกละเมิดการใช้งาน (Compromise) โดยควบคุมการเข้าถึง และตรวจสอบการนำเครื่องมือไปใช้งานอย่างสม่ำเสมอ
10. ผู้ดูแลระบบต้องประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
11. ผู้บังคับบัญชาต้องติดตามผลการดำเนินการตามแผนบริหารจัดการความเสี่ยง (Risk treatment plan) เป็นประจำทุกไตรมาส
12. ผู้ดูแลระบบต้องประเมินความเสี่ยงแล้วจัดลำดับความสำคัญของความเสี่ยงนั้นและค้นหาวิธีการเพื่อลดความเสี่ยงตามขั้นตอนที่ รฟม. กำหนด พร้อมทั้งพิจารณาข้อดีข้อเสียของวิธีการเหล่านั้นเพื่อให้ผู้บริหารของ รฟม. ตัดสินใจเลือกวิธีการเพื่อลดความเสี่ยงหรือยอมรับความเสี่ยง เมื่อเลือกวิธีการลดความเสี่ยงแล้วผู้บริหารต้องจัดสรรทรัพยากรอย่างเพียงพอเพื่อดำเนินการ แนวทางการลดความเสี่ยง แบ่งได้เป็น 3 รูปแบบ ได้แก่
    12.1 การเลือกใช้เทคโนโลยี เพื่อใช้ในการลดความเสี่ยงและเพิ่มความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รฟม. เป็นวิธีที่จำเป็นต้องใช้งบประมาณและทรัพยากรอย่างเพียงพอในการดำเนินการ เช่น การเลือกใช้อุปกรณ์ Firewall มากกว่าหนึ่งผลิตภัณฑ์ในการป้องกันการเข้าถึงเครือข่ายที่สำคัญ การใช้อุปกรณ์สมาร์ทการ์ด หรือ USB Token ในการตรวจสอบยืนยันตัวตนในการเข้าใช้งานระบบจากภายนอก รฟม. เป็นต้น
    12.2 การปรับเปลี่ยนขั้นตอนปฏิบัติ ต้องออกแบบขั้นตอนปฏิบัติใหม่ที่รัดกุมและสามารถรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รฟม. ได้ดีขึ้น เมื่อออกแบบขั้นตอนปฏิบัติใหม่แล้วต้องมีการพิจารณาหารือความเหมาะสม ความเป็นไปได้ และผู้บริหารต้องเป็นผู้อนุมัติให้มีการบังคับใช้ขั้นตอนปฏิบัติใหม่นั้น
    12.3 ผู้ดูแลระบบต้องแจ้งขั้นตอนปฏิบัติให้ผู้เกี่ยวข้องรับรู้อย่างทั่วถึง รวมทั้งต้องจัดฝึกอบรมผู้ใช้งานที่เกี่ยวข้องเพื่อให้สามารถปฏิบัติตามขั้นตอนปฏิบัติใหม่ได้อย่างราบรื่นและมีประสิทธิภาพ
13. การตรวจสอบความปลอดภัยของระบบสารสนเทศ
    13.1 ผู้ดูแลระบบ ต้องวางแผนการตรวจสอบและประเมินช่องโหว่หรือจุดอ่อนด้านความมั่นคงปลอดภัยสารสนเทศและแจ้งผู้ที่เกี่ยวข้องเพื่อแก้ไขในกรณีที่พบว่าช่องโหว่หรือจุดอ่อนนั้นอาจเป็นเหตุการณ์ด้านความมั่นคงปลอดภัย 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 ข้อมูลถูกแก้ไข เปลี่ยนแปลง 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

- เพื่อให้มีการเข้ารหัสข้อมูลอย่างเหมาะสมและมีประสิทธิผลในการปกป้องความลับ ป้องกัน การปลอมแปลงข้อมูล และควบคุมความถูกต้องของข้อมูล

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- เจ้าของข้อมูล
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 6 การเข้ารหัสข้อมูล (Cryptography)

แนวปฏิบัติ

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

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

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

6.2 เมื่อมีการรับกุญแจสาธารณะ (Public key) มาใช้ ก่อนใช้งานจะต้องพิสูจน์ความถูกต้องของกุญแจสาธารณะ โดยสอบถามกับผู้ส่งหรือตรวจสอบกับผู้แทนในการรับรองความถูกต้องของกุญแจสาธารณะ (Certificate authority) ที่เชื่อถือได้เท่านั้น

6.3 ควบคุมการใช้งานและจัดเก็บกุญแจให้สอดคล้องกับการรักษาความลับข้อมูลตามที่ รฟม. กำหนด

ส่วนที่ 16
การนำอุปกรณ์ส่วนตัวมาใช้งาน (Bring your own device)

วัตถุประสงค์

- เพื่อควบคุมการนำอุปกรณ์ส่วนตัวมาเชื่อมต่อหรือเข้าถึงระบบสารสนเทศของ รฟม. ที่ใช้ในการบริหารจัดการระบบสารสนเทศของ รฟม. หรือปฏิบัติงานให้ รฟม. ทั้งนี้เพื่อป้องกันภัยคุกคามที่อาจจะเกิดขึ้นกับระบบสารสนเทศของ รฟม. รวมถึงเพื่อป้องกันไม่ให้ข้อมูลของ รฟม. เกิดการรั่วไหล

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 2 อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากระยะไกล (Mobile devices and teleworking)

แนวปฏิบัติ

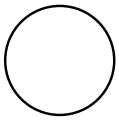
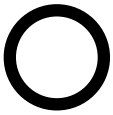
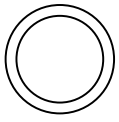
1. ผู้ดูแลระบบต้องกำหนดคุณสมบัติของระบบปฏิบัติการของอุปกรณ์ส่วนตัวที่อนุญาตให้นำมาเชื่อมต่อหรือเข้าถึงระบบงานสารสนเทศของ รฟม. ได้ โดยต้องเป็นระบบปฏิบัติการที่ไม่ล้าสมัย (Obsolete operating system) และยังได้รับการสนับสนุนการใช้งานจากเจ้าของผลิตภัณฑ์
2. ผู้ดูแลระบบต้องตัดการเชื่อมต่อหากระบบปฏิบัติการของอุปกรณ์ส่วนตัวที่อนุญาตให้นำมาเชื่อมต่อหรือเข้าถึงระบบงานสารสน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

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

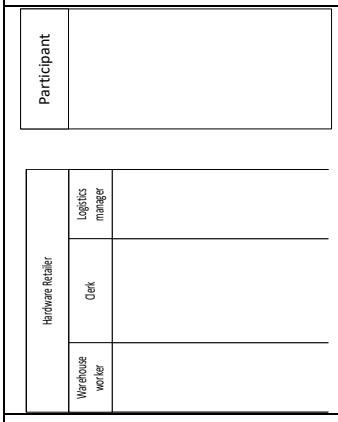
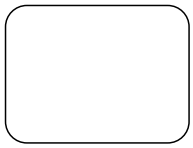
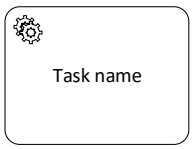
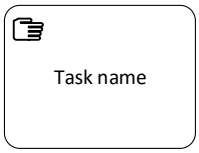
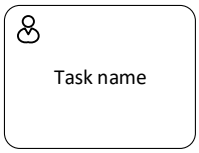
/ภาคผนวก ข....

ภาคผนวก ข.

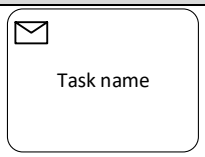
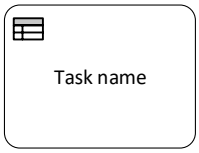
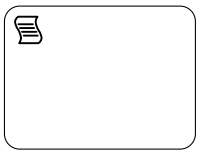
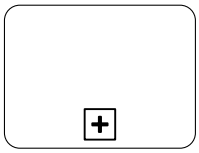
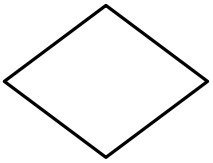
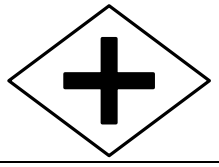
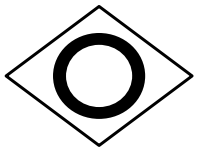
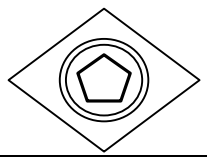
ผู้ขายต้องจัดทำรายงานของงานงวดที่ 1, 2 และ 3 ตามแผนภาพแสดงลำดับขั้นตอนตาม Business Process Model and Notation (BPMN 2.0) ดังนี้

ภาพสัญลักษณ์	ชื่อสัญลักษณ์	คำอธิบาย
	Start Event	สัญลักษณ์แสดงเหตุการณ์เริ่มต้นของการทำกิจกรรมในกระบวนการ เหตุการณ์เริ่มต้นที่เกิดขึ้นนี้มีตัวกระตุ้นที่ทำให้เกิดเหตุการณ์ได้หลายแบบ สัญลักษณ์ที่ใช้คือแสดงตัวกระตุ้นอยู่ภายในวงกลม เช่น  Message หมายถึงเหตุการณ์หรือข้อความที่ทำให้เกิดการเริ่มต้นกระบวนการ  Timer เหตุการณ์เกี่ยวกับเวลาที่ทำให้เกิดการเริ่มต้นของกระบวนการ
	End Event	เป็นสัญลักษณ์แสดงเหตุการณ์สิ้นสุดกระบวนการ เหตุการณ์สิ้นสุดที่เกิดขึ้นนี้มีตัวกระตุ้นที่ทำให้เกิดเหตุการณ์ได้หลายแบบ สัญลักษณ์ที่ใช้คือแสดงตัวกระตุ้นอยู่ภายในวงกลม เช่น  Terminate หมายถึงตัวกระตุ้นที่ทำให้เกิดเหตุการณ์สิ้นสุดกระบวนการ  Error หมายถึงตัวกระตุ้นเกี่ยวกับข้อผิดพลาดที่ทำให้เกิดเหตุการณ์สิ้นสุดกระบวนการ  Cancel หมายถึงตัวกระตุ้นเกี่ยวกับการยกเลิกที่ทำให้เกิดเหตุการณ์สิ้นสุดกระบวนการ
	Intermediate Event	สัญลักษณ์แสดงเหตุการณ์เกิดขึ้นในระหว่างกระบวนการ เหตุการณ์ที่เกิดขึ้นในระหว่างกระบวนการนี้มีตัวกระตุ้นที่ทำให้เกิดเหตุการณ์ได้หลายแบบสัญลักษณ์ที่ใช้คือแสดงตัวกระตุ้นอยู่ภายในวงกลม เช่น /<u>**ภาคผนวก ข.**</u>...  Message หมายถึงเหตุการณ์หรือข้อความที่เกิดขึ้นในระหว่างกระบวนการ

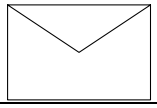
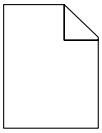
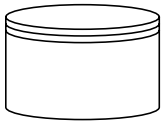
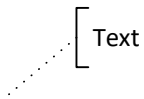
/Timer...

ภาพสัญลักษณ์	ชื่อสัญลักษณ์	คำอธิบาย
		Timer เหตุการณ์เกี่ยวกับเวลาที่เกิดขึ้นในระหว่างกระบวนการ เช่นถึงเวลาที่กำหนดแล้วจะเกิดกิจกรรมได้ต่อไป
	Pool/Lane	สัญลักษณ์แสดงผู้ที่เกี่ยวข้องในกระบวนการโดยสามารถแบ่งการแบ่งบทบาทหน้าที่ความรับผิดชอบของแต่ละคนหรือแต่ละหน่วยงาน
	Task	สัญลักษณ์ แสดงการทำกิจกรรมหรืองานในกระบวนการ เช่น การประมวลผลข้อมูล เป็นต้น
	Service Task	สัญลักษณ์แสดงการทำกิจกรรมหรืองานที่ทำโดยใช้ระบบอัตโนมัติหรือคอมพิวเตอร์เข้ามาช่วย เช่นการใช้ web service หรือใช้ automate application
	Manual Task	สัญลักษณ์แสดงกิจกรรมหรืองานที่ทำโดยไม่อาศัยคอมพิวเตอร์เข้ามาช่วย
	User Task	สัญลักษณ์ที่แสดงการทำงานของ user โดยใช้ระบบคอมพิวเตอร์หรือโปรแกรมประยุกต์เข้ามาช่วยในการทำกิจกรรมนั้น
	Send Task	สัญลักษณ์แสดงกิจกรรม/งานที่มีการส่งข้อมูลหรือข่าวสาร (message) ออกไปยังผู้เกี่ยวข้องที่อยู่ภายนอก

/Receive Task...

ภาพสัญลักษณ์	ชื่อสัญลักษณ์	คำอธิบาย
	Receive Task	สัญลักษณ์แสดงกิจกรรม/งานที่มีการรับข้อมูลจากกิจกรรมที่ส่งข้อมูลหรือข่าวสาร (message)
	Business Rule Task	สัญลักษณ์ที่แสดงกิจกรรม/งานที่มีการใช้ business rule engine ในการทำงาน
	Script Task	สัญลักษณ์แสดงกิจกรรม/งานที่มีการ execute script (script จะถูก execute โดย business process engine) เมื่อ script ทำงานเสร็จ ให้ถือว่ากิจกรรม/งานนั้นดำเนินการเสร็จสิ้นสมบูรณ์
	Collapsed Sub-Proces	สัญลักษณ์ที่แสดงกระบวนการย่อยที่อยู่ภายในกระบวนการ โดยมีการซ่อนรายละเอียดของกิจกรรมในกระบวนการย่อยไว้
	Exclusive Gateway	สัญลักษณ์แสดงการตัดสินใจเลือกทางใดทางหนึ่งเท่านั้นเพื่อดำเนินกิจกรรมในกระบวนการ
	Parallel Gateway	สัญลักษณ์แสดงการตัดสินใจ/ทางเลือกในการดำเนินกิจกรรมในกระบวนการที่สามารถทำคู่ขนานกันไปได้
	Inclusive Gateway	สัญลักษณ์แสดงการตัดสินใจ/ทางเลือกในการดำเนินกิจกรรมในกระบวนการ โดยอาจเลือกดำเนินกิจกรรมได้มากกว่า 1 ทางเลือก
	Event Gateway	สัญลักษณ์แสดงการตัดสินใจเลือกทางเลือกตามเหตุการณ์ที่เกิดขึ้น
	Sequence Flow	สัญลักษณ์แสดงลำดับขั้นการทำงานของกิจกรรม/งาน

/Message Flow...

ภาพสัญลักษณ์	ชื่อสัญลักษณ์	คำอธิบาย
	Message Flow	สัญลักษณ์แสดงทิศทางการไหลของ message ระหว่างผู้ที่เกี่ยวข้องในกระบวนการ
	Message	สัญลักษณ์แสดงการส่งข่าวสาร/ข้อความระหว่าง Pool
	Data object	สัญลักษณ์แสดงสิ่งที่กิจกรรม/งานผลิตออกมา
	Data Sotre	สัญลักษณ์แสดงการจัดเก็บข้อมูลแบบถาวร (persist data) ที่กิจกรรม/งานสามารถดึงมาใช้งานภายในกิจกรรม/งานหรือจัดเก็บข้อมูล
	Group	สัญลักษณ์แสดงการจัดกลุ่ม
	Text Annotation	สัญลักษณ์แสดงการอธิบายเพิ่มเติม เพื่อให้ผู้อ่านแผนภาพได้เข้าใจมากยิ่งขึ้น

/**ภาคผนวก ค.**...

ภาคผนวก ค.

1. หลักเกณฑ์การประเมินค่าประสิทธิภาพต่อราคา (Price Performance)

ในการพิจารณาผู้ชนะการเสนอราคา รฟม. จะใช้หลักเกณฑ์การประเมินค่าประสิทธิภาพต่อราคา (Price Performance) โดยพิจารณาให้คะแนนตามปัจจัยหลักและน้ำหนักตามที่กำหนด ดังนี้

1. คุณภาพและคุณสมบัติที่เป็นประโยชน์ต่อการดำเนินโครงการ กำหนดน้ำหนักเท่ากับร้อยละ 70
2. ราคาที่ยื่นข้อเสนอ (Price) กำหนดน้ำหนักเท่ากับร้อยละ 30

หลักเกณฑ์การให้คะแนนราคาที่ยื่นข้อเสนอ (Price) เป็นไปตามการคำนวณของระบบการจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ e-GP ของกรมบัญชีกลาง

2. หลักเกณฑ์การให้คะแนนคุณภาพและคุณสมบัติที่เป็นประโยชน์ต่อการดำเนินโครงการ

การให้คะแนนคุณภาพและคุณสมบัติที่เป็นประโยชน์ต่อการดำเนินโครงการ มีคะแนนรวมทั้งหมด 100 คะแนน ประกอบด้วยหัวข้อ ดังนี้

ลำดับที่	รายการ	คะแนนรวม	หมายเหตุ
1.	ผลงานของผู้ยื่นข้อเสนอ	20	
2.	ประสบการณ์ของทีมงาน	20	
3.	แนวทางและวิธีในการพัฒนาระบบ (Methodology)	15	
4.	แผนการดำเนินงาน (Work Plan)	15	
5.	นำเสนอผลงาน (Demo)	30	
	รวม	**100**	

หมายเหตุ – การคำนวณตัวเลขของการประเมินทุกหัวข้อกำหนดความละเอียดถึงทศนิยมจำนวนสองหลัก

โดยผู้ชนะการเสนอราคา ต้องได้คะแนนคุณภาพและคุณสมบัติที่เป็นประโยชน์ต่อการดำเนินโครงการไม่น้อยกว่าร้อยละ 70

/ทั้งนี้...

ทั้งนี้ มีรายละเอียดในการพิจารณาแต่ละหัวข้อ ดังนี้

1. การพิจารณาผลงานของผู้ยื่นข้อเสนอ (20 คะแนน)

การพิจารณาให้คะแนนผลงานของผู้ยื่นข้อเสนอ จะพิจารณาผู้ยื่นข้อเสนอที่มีหนังสือรับรองผลงาน ซึ่งลงนามโดยผู้มีอำนาจ และข้อกำหนดหรือขอบเขตของงานของผลงานนั้น พร้อมด้วยสำเนาสัญญาหรือใบสั่งซื้อ/ใบสั่งจ้าง (ถ้ามี) ทั้งนี้ รฟม. ขอสงวนสิทธิ์ที่จะตรวจสอบข้อเท็จจริงที่เสนอ โดยแบ่งการพิจารณาออกเป็น 2 ส่วนหลัก คือ

1.1 จำนวนผลงานที่มีความสอดคล้องกับลักษณะโครงการ (10 คะแนน)

การพิจารณาให้คะแนนจำนวนผลงาน จะพิจารณาผลงานของผู้ยื่นข้อเสนอที่เป็นผลงานซึ่งได้ตรวจรับสมบูรณ์แล้วในช่วง 5 ปีที่ผ่านมา นับถึงวันยื่นเอกสารประกวดราคา และขอบเขตของงาน โดยอ้างอิงตามภาคผนวก ง. แบบฟอร์มที่ 02 ซึ่งมีเกณฑ์การให้คะแนนจากผลงานที่มีขอบเขตของงานหรือลักษณะสอดคล้องตามคุณลักษณะเฉพาะของระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA

ผลงาน	คะแนน
เป็นผลงานที่มีขอบเขตของงานหรือลักษณะงานสอดคล้องตามคุณลักษณะเฉพาะของระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA ซึ่งมีมูลค่าต่อสัญญาไม่น้อยกว่า 1,000,000 บาท ย้อนหลังไม่เกิน 5 ปี นับถึงวันยื่นเอกสารประกวดราคา และมีจำนวนมากที่สุด ลำดับที่ 1	10.00
เป็นผลงานที่มีขอบเขตของงานหรือลักษณะงานสอดคล้องตามคุณลักษณะเฉพาะของระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA ซึ่งมีมูลค่าต่อสัญญาไม่น้อยกว่า 1,000,000 บาท ย้อนหลังไม่เกิน 5 ปี นับถึงวันยื่นเอกสารประกวดราคา และมีจำนวนเป็นลำดับที่ 2 เป็นต้นไป	7.00

หมายเหตุ - กรณีผู้ยื่นข้อเสนอยื่นผลงานหลายโครงการ หากโครงการใดไม่มีหนังสือรับรองผลงาน และข้อกำหนดหรือขอบเขตของงานของผลงานนั้น พร้อมด้วยสำเนาสัญญาหรือใบสั่งซื้อ/ใบสั่งจ้าง (ถ้ามี) จะได้รับการประเมินผลงานสำหรับโครงการนั้นเท่ากับศูนย์

1.2 มูลค่าของสัญญา (5 คะแนน)

การพิจารณาให้คะแนนมูลค่าของผลงาน จะพิจารณามูลค่าต่อสัญญา (พิจารณาเพียง 1 สัญญาที่มีมูลค่าสูงสุด) ของผู้ยื่นข้อเสนอที่เป็นผลงานซึ่งได้ตรวจรับสมบูรณ์แล้วในช่วง 5 ปีที่ผ่านมา นับถึงวันยื่นเอกสารประกวดราคา และขอบเขตของงาน โดยอ้างอิงตามภาคผนวก ง. แบบฟอร์มที่ 02 ซึ่งมีเกณฑ์การให้คะแนนจากผลงานที่มีขอบเขตของงานหรือลักษณะสอดคล้องตามคุณลักษณะเฉพาะของระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA

/เป็นผลงาน...

ผลงาน	คะแนน
เป็นผลงานที่มีขอบเขตของงานหรือลักษณะงานสอดคล้องตามคุณลักษณะเฉพาะของระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA ซึ่งมีมูลค่าต่อสัญญาไม่น้อยกว่า 1,000,000 บาท ย้อนหลังไม่เกิน 5 ปี นับถึงวันยื่นเอกสารประกวดราคา (มูลค่าต่อสัญญาสูงสุดลำดับที่ 1)	5.00
เป็นผลงานที่มีขอบเขตของงานหรือลักษณะงานสอดคล้องตามคุณลักษณะเฉพาะของระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA ซึ่งมีมูลค่าต่อสัญญาไม่น้อยกว่า 1,000,000 บาท ย้อนหลังไม่เกิน 5 ปี นับถึงวันยื่นเอกสารประกวดราคา (มูลค่าต่อสัญญา ลำดับที่ 2 เป็นต้นไป)	3.50

หมายเหตุ - กรณีผู้ยื่นข้อเสนอยื่นผลงานหลายโครงการ หากโครงการใดไม่มีหนังสือรับรองผลงาน และข้อกำหนดหรือขอบเขตของงานของผลงานนั้น พร้อมด้วยสำเนาสัญญาหรือใบสั่งซื้อ/ใบสั่งจ้าง (ถ้ามี) จะได้รับการประเมินผลงานสำหรับโครงการนั้นเท่ากับศูนย์

1.3 คู่สัญญา (5 คะแนน)

การพิจารณาให้คะแนนคู่สัญญา ที่มีหนังสือรับรองผลงานซึ่งลงนามโดยผู้มีอำนาจ และข้อกำหนดหรือขอบเขตของงานของผลงานนั้น พร้อมด้วยสำเนาสัญญาหรือใบสั่งซื้อ/ใบสั่งจ้าง (ถ้ามี) โดยอ้างอิงตามภาคผนวก ง. แบบฟอร์มที่ 02 ซึ่งมีเกณฑ์การให้คะแนน ดังนี้

		คะแนน
คู่สัญญา	● หน่วยงานของรัฐ	5.00
	● หน่วยงานเอกชน	3.50

หมายเหตุ - กรณีผู้ยื่นข้อเสนอยื่นผลงานหลายโครงการ หากโครงการใดไม่มีหนังสือรับรองผลงาน และข้อกำหนดหรือขอบเขตของงานของผลงานนั้น พร้อมด้วยสำเนาสัญญาหรือใบสั่งซื้อ/ใบสั่งจ้าง (ถ้ามี) จะได้รับการประเมินผลงานสำหรับโครงการนั้นเท่ากับศูนย์

2. การพิจารณาประสบการณ์ของทีมงาน (20 คะแนน)

การพิจารณาให้คะแนนประสบการณ์ของทีมงาน เมื่อจัดส่งบุคลากรหลักตามที่กำหนดในขอบเขตของงานซื้อระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA โดยแบ่งการพิจารณาออกเป็น 2 ส่วนหลัก คือ

2.1 การจัดส่งบุคลากรหลักตามที่กำหนด (5 คะแนน)

การพิจารณาให้คะแนนประสบการณ์ของทีมงาน เมื่อจัดส่งบุคลากรหลักตามที่กำหนดในขอบเขตของงาน (TOR) โดยอ้างอิงตามภาคผนวก ง. แบบฟอร์มที่ 03 ซึ่งมีเกณฑ์การให้คะแนน ดังนี้

ระดับ	เสนอครบถ้วน	เสนอไม่ครบถ้วน
คะแนน	5.00	0.00

เสนอครบถ้วน เสนอบุคลากรตามตำแหน่งงานที่กำหนดในขอบเขตของงาน (TOR) อย่างครบถ้วน

เสนอไม่ครบถ้วน เสนอบุคลากรตามตำแหน่งงานที่กำหนดในขอบเขตของงาน (TOR) ไม่ครบถ้วน

/2.2 ประสบการณ์...

2.2 ประสบการณ์การทำงานของบุคลากร (15 คะแนน)

การพิจารณาให้คะแนนประสบการณ์การทำงานของบุคลากร ตามตำแหน่งที่เสนอในโครงการ โดยอ้างอิงตามภาคผนวก ง. แบบฟอร์มที่ 03 ดังนี้

ผู้จัดการโครงการ (Project Manager)	3 คะแนน
นักวิเคราะห์ระบบ (System Analyst)	3 คะแนน
นักพัฒนาระบบ (Developer/ Programmer/ Technical)	3 คะแนน
วิศวกรระบบคอมพิวเตอร์ (System Engineer)	2 คะแนน
นักทดสอบระบบ (Implementer/ Tester)	2 คะแนน
ผู้ประสานงานโครงการ (Project Coordinator)	2 คะแนน
	รวม 15 คะแนน

ตำแหน่ง	**ประสบการณ์ (คะแนนที่ได้รับ)**				**ไม่เสนอบุคลากร**
ผู้จัดการโครงการ (Project Manager)	X > 10 ปี (3.00)	5 > X ≥ 10 ปี (2.25)	3 > X ≥ 5 ปี (1.50)	X ≤ 3 ปี (0.75)	0.00
นักวิเคราะห์ระบบ (System Analyst)	X > 5 ปี (3.00)	3 > X ≥ 5 ปี (2.25)	2 > X ≥ 3 ปี (1.50)	X ≤ 2 ปี (0.75)	0.00
นักพัฒนาระบบ (Developer/ Programmer/ Technical)	X > 5 ปี (3.00)	3 > X ≥ 5 ปี (2.25)	2 > X ≥ 3 ปี (1.50)	X ≤ 2 ปี (0.75)	0.00
วิศวกรระบบคอมพิวเตอร์ (System Engineer)	X > 3 ปี (2.00)	2 > X ≥ 3 ปี (1.50)	1 > X ≥ 2 ปี (1.00)	X ≤ 1 ปี (0.50)	0.00
นักทดสอบระบบ (Implementer/ Tester)	X > 3 ปี (2.00)	2 > X ≥ 3 ปี (1.50)	1 > X ≥ 2 ปี (1.00)	X ≤ 1 ปี (0.50)	0.00
ผู้ประสานงานโครงการ (Project Coordinator)	X > 3 ปี (2.00)	2 > X ≥ 3 ปี (1.50)	1 > X ≥ 2 ปี (1.00)	X ≤ 1 ปี (0.50)	0.00

<u>หมายเหตุ</u> การพิจารณาประสบการณ์ของทีมงาน ทั้ง 2 ข้อ

- หากเสนอบุคลากรที่ปฏิบัติงานหลายตำแหน่งต่อ 1 ท่าน จะพิจารณาให้ครบถ้วนในทุกตำแหน่ง
- หากเสนอจำนวนบุคลากรในแต่ละตำแหน่งมากกว่าที่กำหนด จะเลือกพิจารณาบุคลากรที่มีประสบการณ์สูงที่สุด
- กรณีที่บุคลากรไม่มีสำเนาหนังสือรับรองหรือประกาศนียบัตรที่แสดงวุฒิการศึกษา จะได้รับการประเมิน**เท่ากับศูนย์** ไม่ผ่านเกณฑ์
- หากมีการเปลี่ยนชื่อหรือนามสกุลให้แนบสำเนาหลักฐานการเปลี่ยนชื่อหรือนามสกุลมาด้วย ในกรณีที่ไม่มีสำเนาหลักฐานดังกล่าว จะได้รับการประเมิน**เท่ากับศูนย์** ไม่ผ่านเกณฑ์

/3. การพิจารณา...

3. การพิจารณาการนำเสนอแนวทาง วิธีการดำเนินงานของโครงการและวิธีในการพัฒนาระบบ (Methodology) (15 คะแนน)

การพิจารณาให้คะแนนการนำเสนอแนวทาง วิธีการดำเนินงานของโครงการและวิธีในการพัฒนาระบบ (Methodology) จะพิจารณาถึงแนวทาง วิธีการดำเนินงานของโครงการและวิธีในการพัฒนาระบบที่เหมาะสม หรือสอดคล้องตามขอบเขตของงานโครงการดังกล่าว โดยแบ่งการพิจารณาออกเป็น 3 ส่วนหลัก คือ

3.1 แนวทางและวิธีการดำเนินงานของโครงการ (5 คะแนน)

การพิจารณาให้คะแนนรายละเอียดแนวทางและวิธีการดำเนินงานของโครงการ โดยอ้างอิงตามภาคผนวก ง. แบบฟอร์มที่ 04 ซึ่งแบ่งการพิจารณาออกเป็น 3 ส่วนหลัก และมีเกณฑ์การให้คะแนน ดังนี้

1) ภาพรวมสถาปัตยกรรมขององค์กร (Enterprise Architecture)
2) แนวความคิด (Conceptual) และรายละเอียด (Detailed) เกี่ยวกับการออกแบบและพัฒนาระบบ
3) แนวทางการแก้ไขปัญหา เมื่อระบบไม่สามารถใช้งานได้

ระดับ	ดีกว่าเกณฑ์	ตามเกณฑ์	ต่ำกว่าเกณฑ์	ไม่นำเสนอ
คะแนน	5.00	3.50	2.00	0.00

ดีกว่าเกณฑ์ ผู้ยื่นข้อเสนอมีความเข้าใจสถานการณ์การดำเนินงานปัจจุบัน เข้าใจปัญหา/ ประเด็นสำคัญของขอบเขตของงาน (TOR) โดยมีการนำเสนอขั้นตอนการทำงาน รายละเอียดแนวทาง วิธีการดำเนินงานของโครงการในเนื้อหา 3 ส่วนหลักอย่างถูกต้อง เหมาะสม ครบถ้วนและดีกว่าที่ขอบเขตของงาน (TOR) กำหนด ได้แก่ สถาปัตยกรรมขององค์กร แนวความคิด (Conceptual) และรายละเอียด (Detailed) และแนวทางการแก้ไขปัญหา เมื่อระบบไม่สามารถใช้งานได้ โดยสอดคล้องตามที่ TOR กำหนดไว้ รวมถึงมีข้อคิดเห็นเพิ่มเติม

ตามเกณฑ์ ผู้ยื่นข้อเสนอมีความเข้าใจสถานการณ์การดำเนินงานปัจจุบัน เข้าใจปัญหา/ ประเด็นสำคัญ มีรายละเอียดแนวทางและวิธีการดำเนินงานสอดคล้องตามที่ขอบเขตของงาน (TOR) กำหนดไว้ โดยมีการนำเสนอข้อมูลในเนื้อหา 3 ส่วนหลักอย่างเหมาะสม และถูกต้องตามขอบเขตของงาน (TOR)

ต่ำกว่าเกณฑ์ ผู้ยื่นข้อเสนอมีความเข้าใจที่ผิดในขอบเขตของงาน (TOR) ที่กำหนดไว้ หรือมีความเข้าใจที่ไม่ครบถ้วน มีรายละเอียดในการนำเสนอที่ไม่สมบูรณ์ นำเสนอรายละเอียดแนวทาง วิธีการดำเนินงานของโครงการไม่สอดคล้องกับผลลัพธ์ตามที่ TOR กำหนดไว้ มีวิธีการทำงานไม่เหมาะสม หรือมีการนำเสนอที่ไม่เพียงพอตามมาตรฐานทั่วไป

ไม่นำเสนอ ผู้ยื่นข้อเสนอไม่นำเสนอรายละเอียดแนวทาง วิธีการดำเนินงานของโครงการ

/3.2 แนวทางและ...

3.2 แนวทางและวิธีในการพัฒนาระบบ (Methodology) และซอฟต์แวร์หรือเครื่องมือ (Tools) ที่ใช้ในการพัฒนา (5 คะแนน)

การพิจารณาให้คะแนนรายละเอียดแนวทางและวิธีในการพัฒนาระบบ (Methodology) และซอฟต์แวร์หรือเครื่องมือ (Tools) ที่ใช้ในการพัฒนา ที่เหมาะสมกับโครงการ โดยอ้างอิงตามภาคผนวก ง. แบบฟอร์มที่ 04 ซึ่งมีเกณฑ์การให้คะแนน ดังนี้

ระดับ	ดีกว่าเกณฑ์	ตามเกณฑ์	ต่ำกว่าเกณฑ์	ไม่นำเสนอ
คะแนน	5.00	3.50	2.00	0.00

ดีกว่าเกณฑ์ ผู้ยื่นข้อเสนอมีความเข้าใจสถานการณ์การดำเนินงานปัจจุบัน เข้าใจปัญหา/ ประเด็นสำคัญของขอบเขตของงาน (TOR) โดยมีการระบุวิธีการและซอฟต์แวร์หรือเครื่องมือ (Tools) ที่ใช้ในการพัฒนา ซึ่งเป็นมาตรฐานที่เหมาะสม เชื่อถือได้ ทันสมัย หรือนำนวัตกรรมใหม่มาประยุกต์ใช้ในงาน หรือนำซอฟต์แวร์/ ระบบงานที่เสนอไปใช้กับหน่วยงานภาครัฐหรือเอกชน โดยสอดคล้องตาม TOR

ตามเกณฑ์ ผู้ยื่นข้อเสนอมีความเข้าใจสถานการณ์การดำเนินงานปัจจุบัน เข้าใจปัญหา/ ประเด็นสำคัญ ระบุวิธีการและซอฟต์แวร์หรือเครื่องมือ (Tools) ที่ใช้ในการพัฒนา ซึ่งเป็นมาตรฐานที่เหมาะสม และสอดคล้องตาม TOR

ต่ำกว่าเกณฑ์ ผู้ยื่นข้อเสนอมีความเข้าใจที่ผิดในขอบเขตของงาน (TOR) ที่กำหนดไว้ หรือมีความเข้าใจที่ไม่ครบถ้วน มีรายละเอียดในการนำเสนอที่ไม่สมบูรณ์ วิธีการหรือซอฟต์แวร์หรือเครื่องมือ (Tools) ที่ใช้ในการพัฒนา ที่ไม่สอดคล้องกับผลลัพธ์ตาม TOR มีวิธีการทำงานไม่เหมาะสม หรือมีการนำเสนอที่ไม่เพียงพอตามมาตรฐานทั่วไป

ไม่นำเสนอ ผู้ยื่นข้อเสนอไม่นำเสนอวิธีการและซอฟต์แวร์หรือเครื่องมือ (Tools) ที่ใช้ในการพัฒนา

3.3 ตารางเปรียบเทียบทางด้านเทคนิค (5 คะแนน)

การพิจารณาให้คะแนนตารางเปรียบเทียบทางด้านเทคนิค โดยอ้างอิงตามภาคผนวก ง. แบบฟอร์มที่ 04 ซึ่งมีเกณฑ์การให้คะแนน ดังนี้

เกณฑ์การให้คะแนน	คะแนน
ดีกว่าเกณฑ์ (อันดับที่ 1)	5.00
ดีกว่าเกณฑ์	4.25
ตามเกณฑ์	3.50
ต่ำกว่าเกณฑ์ หรือไม่นำเสนอ	0.00

/ดีกว่าเกณฑ์...

ดีกว่าเกณฑ์ (อันดับที่ 1) ผู้ยื่นข้อเสนอจัดทำตารางเปรียบเทียบทางด้านเทคนิค (ตามภาคผนวก ค. แบบฟอร์มที่ 04) โดยมีการระบุข้อเปรียบเทียบทางด้านเทคนิคได้ดีกว่าข้อกำหนดที่ระบุไว้ หรือมีการนำเสนอข้อเสนอเพิ่มเติมโดยสอดคล้องตามขอบเขตของงาน (TOR) เป็นอันดับที่ 1 จากจำนวนผู้ยื่นข้อเสนอทั้งหมด

ดีกว่าเกณฑ์ ผู้ยื่นข้อเสนอจัดทำตารางเปรียบเทียบทางด้านเทคนิค (ตามภาคผนวก ค. แบบฟอร์มที่ 04) โดยมีการระบุข้อเปรียบเทียบทางด้านเทคนิคได้ดีกว่าข้อกำหนดที่ระบุไว้ **แต่ไม่ใช่**อันดับที่ 1 จากจำนวนผู้ยื่นข้อเสนอทั้งหมด

ตามเกณฑ์ ผู้ยื่นข้อเสนอจัดทำตารางเปรียบเทียบทางด้านเทคนิค (ตามภาคผนวก ค. แบบฟอร์มที่ 04) โดยระบุข้อเปรียบเทียบสิ่งที่ทำได้ตรงตามข้อกำหนดที่ระบุไว้ โดยไม่มีการนำเสนอขอบเขตของงานเพิ่มเติม

ต่ำกว่าเกณฑ์หรือไม่นำเสนอ ผู้ยื่นข้อเสนอไม่นำเสนอตารางเปรียบเทียบทางด้านเทคนิค (ตามภาคผนวก ค. แบบฟอร์มที่ 04) หรือนำเสนอแต่ระบุข้อเปรียบเทียบสิ่งที่ทำได้ต่ำกว่าข้อกำหนดที่ระบุไว้ ในข้อใดข้อหนึ่ง

4. แผนการดำเนินงาน (Work Plan) (15 คะแนน)

การให้คะแนนจะพิจารณาถึงความเข้าใจในแผนการดำเนินงาน ความชัดเจนของงานที่นำเสนอ และความครอบคลุมถึงสาระสำคัญตามขอบเขตของงาน (TOR) อย่างครบถ้วน โดยอ้างอิงตามภาคผนวก ง. แบบฟอร์มที่ 05 ซึ่งมีเกณฑ์การให้คะแนน ดังนี้

ระดับ	ดีกว่าเกณฑ์	ตามเกณฑ์	ต่ำกว่าเกณฑ์	ไม่นำเสนอ
คะแนน	15.00	10.50	6.00	0.00

ดีกว่าเกณฑ์ แผนการดำเนินงานมีความสอดคล้องเหมาะสมในรายละเอียดตามขอบเขตของงาน (TOR) อย่างครบถ้วน และเข้าใจทุกประเด็นสำคัญของข้อกำหนดของงาน นำเสนอวิธีการทำงาน ระยะเวลาของกิจกรรมหลักและกิจกรรมย่อยที่สอดคล้องกับผลลัพธ์ตามข้อกำหนดของงานในรายละเอียดที่ชัดเจน

ตามเกณฑ์ แผนการดำเนินงานมีความสอดคล้องเหมาะสมในรายละเอียดตามขอบเขตของงาน (TOR) อย่างครบถ้วน นำเสนอรายละเอียดวิธีการทำงาน ระยะเวลาของกิจกรรมหลักที่สอดคล้องกับผลลัพธ์ตามที่ข้อกำหนดของงานกำหนดไว้

ต่ำกว่าเกณฑ์ แผนการดำเนินงานตามขอบเขตของงาน (TOR) ไม่ครบถ้วน มีการนำเสนอรายละเอียดในกิจกรรมหลักหรือกิจกรรมย่อยที่ไม่สอดคล้องตาม TOR และแผนการดำเนินงานมีความเข้าใจที่ผิดในขอบเขตของงานที่ระบุไว้ใน TOR มีการนำเสนอที่ไม่เพียงพอตามมาตรฐานทั่วไป หรือมีวิธีการทำงานไม่เหมาะสม

ไม่นำเสนอ ผู้ยื่นข้อเสนอไม่นำเสนอแผนการดำเนินงาน

/5. นำเสนอผลงาน...

5. นำเสนอผลงาน (Demo) (30 คะแนน)

การพิจารณาให้คะแนนนำเสนอผลงาน (Demo) จากการนำเสนอผลงานที่เคยดำเนินการมาในอดีตที่สอดคล้องกับระบบบริหารห้องสมุดอิเล็กทรอนิกส์ e-Library MRTA ซึ่งมีเกณฑ์การให้คะแนน ดังนี้

หัวข้อประกอบการพิจารณา
5.1 คุณภาพของระบบที่นำเสนอ และความสวยงาม บนเว็บไซต์ เช่น ● สี Theme และสีตัวอักษรของระบบงาน ● ขนาดและรูปแบบตัวอักษรชัดเจนอ่านง่าย ● ความง่ายต่อการใช้งาน (User friendly) ในภาพรวม 5.2 คุณภาพของระบบที่นำเสนอ และความสวยงาม บน Mobile Application เช่น ● สี Theme และสีตัวอักษรของระบบงาน ● ขนาดและรูปแบบตัวอักษรชัดเจนอ่านง่าย ● ความง่ายต่อการใช้งาน (User friendly) ในอุปกรณ์ที่หลากหลาย 5.3 ฟังก์ชันการยืม - คืน และจองคิวหนังสือ ตรงตามข้อกำหนด (TOR) 5.4 ฟังก์ชันการบริหารจัดการข้อมูล - หนังสือเล่ม แมกกาซีน สื่อ - e-Book e-Magazine - หนังสือเสียง 5.5 อุปกรณ์ Digital Signage Kiosk 5.6 หน้าจอรูปแบบรายงาน และการนำไปใช้งานต่อได้

การพิจารณาให้คะแนนจะพิจารณาให้คะแนนแบบทอนสัดส่วน โดยมีรายละเอียด ดังนี้

เกณฑ์การให้คะแนน	คะแนนที่ได้รับ
คุณสมบัติดีเป็นลำดับที่ 1	30.00
คุณสมบัติดีเป็นลำดับที่ 2	20.00
คุณสมบัติดีเป็นลำดับที่ 3 เป็นต้นไป	10.00
ไม่นำเสนอหัวข้อนั้น ๆ	0.00

/**<u>ภาคผนวก ง.</u>** ...

<u>ภาคผนวก ง.</u>

ผู้ยื่นข้อเสนอต้องนำเสนอรายละเอียดข้อเสนอด้านเทคนิค ตามแบบฟอร์มที่ รฟม. กำหนด ดังต่อไปนี้

1. แบบฟอร์มที่ 01 รายละเอียดคุณสมบัติของผู้ยื่นข้อเสนอ
2. แบบฟอร์มที่ 02 รายละเอียดประสบการณ์การดำเนินงานที่เป็นผลงานซึ่งได้ตรวจรับสมบูรณ์แล้วเสร็จในช่วง 5 ปี
3. แบบฟอร์มที่ 03 รายละเอียดคุณสมบัติและประสบการณ์การทำงานของบุคลากรหลัก
4. แบบฟอร์มที่ 04 แนวทาง วิธีการดำเนินงาน และรายละเอียดการเปรียบเทียบทางด้านเทคนิค
5. แบบฟอร์มที่ 05 รายละเอียดแผนการดำเนินงาน (Work Plan)

/ **<u>แบบฟอร์มที่ 01</u>** ...

แบบฟอร์มที่ 01
รายละเอียดคุณสมบัติของผู้ยื่นข้อเสนอ

ลำดับ	รายการ	มีคุณสมบัติ (ระบุเครื่องหมาย √)	หมายเหตุ
1.	มีความสามารถตามกฎหมาย		
2.	ไม่เป็นบุคคลล้มละลาย		
3.	ไม่อยู่ระหว่างเลิกกิจการ		
4.	ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง		
5.	ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วน ผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย		
6.	มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา		
7.	เป็นนิติบุคคล ผู้มีอาชีพขายพัสดุที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว		
8.	ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ รฟม. ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้		

ลำดับ	รายการ	มีคุณสมบัติ (ระบุเครื่องหมาย √)	หมายเหตุ
9.	ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น		
10.	ผู้ยื่นข้อเสนอที่เสนอราคาในรูปแบบของ “กิจการร่วมค้า” ต้องมีคุณสมบัติ ดังนี้ กิจการร่วมค้าที่ผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน เว้นแต่ในกรณีกิจการร่วมค้าที่มีข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นสามารถใช้ผลงานของผู้เข้าร่วมค้ารายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงดังกล่าวจะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญามากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย		
11.	ผู้ยื่นข้อเสนอต้องลงทะเบียนที่มีข้อมูลถูกต้องครบถ้วนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e - GP) ของกรมบัญชีกลาง		
12.	ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการเป็นไปตามเงื่อนไขข้อ 1.1 - 1.2 ของหนังสือคณะกรรมการวินิจฉัยปัญหาการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ กรมบัญชีกลาง ด่วนที่สุดที่ กค(กวจ) 0405.2/ว124 ลงวันที่ 1 มีนาคม 2566 เรื่อง แนวทางปฏิบัติในการเร่งรัดการปฏิบัติงานตามสัญญาและการกำหนดคุณสมบัติของผู้มีสิทธิยื่นข้อเสนอ		
13.	ผู้ยื่นข้อเสนอจะต้องมีผลงานในประเทศไทยในลักษณะซอฟต์แวร์สำเร็จรูป (Software Package) ประเภทเดียวกันกับงานที่ประกวดราคาอิเล็กทรอนิกส์นี้ โดยมีผลงานอย่างน้อย 1 สัญญา วงเงินต่อสัญญาไม่น้อยกว่า 1,000,000 บาท (หนึ่งล้านบาทถ้วน) ทั้งนี้ ต้องเป็นผลงานที่ตรวจรับสมบูรณ์แล้ว ในช่วง 5 ปี ที่ผ่านมา นับถึงวันยื่นเอกสารประกวดราคา และเป็นผลงานที่ผู้ยื่นข้อเสนอเป็นคู่สัญญากับส่วนราชการ/ หน่วยงานตามกฎหมายว่าด้วยระเบียบบริหารราชการส่วนท้องถิ่น รัฐวิสาหกิจ หรือหน่วยงานเอกชน โดยแต่ละผลงานที่ยื่นต้องมีเอกสารดังนี้		

ลำดับ	รายการ	มีคุณสมบัติ (ระบุเครื่องหมาย √)	หมายเหตุ
	1. หนังสือรับรองผลงานจากผู้ว่าจ้างที่ลงนามโดยผู้มีอำนาจ 2. ข้อกำหนด หรือ ขอบเขตของงาน 3. สำเนาสัญญาหรือใบสั่งซื้อ/ ใบสั่งจ้าง (ถ้ามี) ทั้งนี้ รฟม.ขอสงวนสิทธิ์ที่จะตรวจสอบข้อเท็จจริงที่เสนอ		

ประทับตรา

(ถ้ามี)

ลงชื่อ_____(ลงนามผู้มีอำนาจจากบริษัท)_____.

(.....)

ตำแหน่ง.....

บริษัท.....

วันที่...../...../..... .....

แบบฟอร์มที่ 02

รายละเอียดประสบการณ์การดำเนินงานที่เป็นผลงานซึ่งได้ตรวจรับสมบูรณ์แล้วเสร็จในช่วง 5 ปี (ก่อนกรอกข้อมูลโปรดอ่านคำชี้แจงในการกรอกข้อมูลโดยละเอียด)

ข้อมูลรายละเอียดหน่วยงานที่อ้างอิง					ข้อมูลรายละเอียดโครงการที่อ้างอิง									
ลำดับ	ชื่อหน่วยงานผู้ว่าจ้าง	ที่อยู่	ประเภทหน่วยงาน	บุคคลที่สามารถติดต่อได้	ประเภทโครงการ	สัญญาที่	มูลค่าโครงการ	ระยะเวลาดำเนินงาน (จำนวนวัน)		ประเภทซอฟต์แวร์	ลักษณะงานที่ดำเนินการ	หนังสือรับรองผลการปฏิบัติงาน	สำเนาสัญญา	ข้อกำหนดและขอบเขตงาน	หมายเหตุ
								ตามสัญญา	ทำงานจริง			ระบุเครื่องหมาย √			
1	ชื่อหน่วยงาน		หน่วยงานราชการ/หน่วยงานรัฐวิสาหกิจ/หน่วยงานเอกชน	ชื่อ/ตำแหน่ง/โทรศัพท์/E-mail	ชื่อโครงการ	เลขที่สัญญา	.....บาท	.....วัน (วันที่แล้วเสร็จตามสัญญา DD/MM/YY)	.....วัน (วันที่ทำงานแล้วเสร็จจริง DD/MM/YY)	ซอฟต์แวร์สำเร็จรูป (ระบุชื่อ) /พัฒนาตามความต้องการ	เช่น พัฒนาระบบ.....				
				รวม (บาท)											

คำชี้แจง :

1) **โครงการที่ระบุในประสบการณ์ข้างต้นจะต้องแนบหนังสือรับรองผลงาน หรือสำเนาสัญญาหรือใบสั่งซื้อ/ใบสั่งจ้าง และข้อกำหนดและขอบเขตของงานของผลงาน ทั้งนี้ <u>หากไม่แนบเอกสารโครงการนั้น ๆ จะไม่นับคะแนน โครงการดังกล่าว</u>**
2) **ข้อมูลปีให้แสดงเป็นพุทธศักราช**
3) **ให้แสดงข้อมูลเป็นภาษาไทย ยกเว้นในส่วนที่จำเป็นต้องเป็นภาษาอังกฤษ เช่น ชื่อ เมือง ประเทศ ฯลฯ ตามความเหมาะสม**
4) **มูลค่าโครงการข้างต้น เป็นราคารวมภาษีมูลค่าเพิ่มแล้ว (ถ้ามี)**

ประทับตรา
(ถ้ามี)

ลงชื่อ_____(ลงนามผู้มีอำนาจจากบริษัท)_____.
(.....)
ตำแหน่ง.....
บริษัท.....
วันที่...../...../..... .....

แบบฟอร์มที่ 03

รายละเอียดคุณสมบัติและประสบการณ์การทำงานของบุคลากรหลัก (ก่อนกรอกข้อมูลโปรดอ่านคำชี้แจงในการกรอกข้อมูลโดยละเอียด)

รูปถ่าย
ไม่เกิน 6 เดือน

1. คุณสมบัติ

ลำดับที่ _____ **ตำแหน่ง** __(ตำแหน่ง เช่น ผู้จัดการโครงการ)

ชื่อภาษาไทย __(คำนำหน้าชื่อ ชื่อ นามสกุล)___ **วัน / เดือน / ปี เกิด** __(วันที่ / เดือน / ปี พ.ศ.)___ **อายุ** __(ปี)

สัญชาติ __(ไทย)___ **ถิ่นพำนักปัจจุบัน** __(กรุงเทพมหานคร ประเทศไทย)___

การศึกษา

ต่ำกว่าปริญญาตรี __(สาขาวิชา)_____ **สถานการศึกษา** _____(วิทยาลัย / มหาวิทยาลัย / ฯลฯ , ประเทศ)__ **ปีที่จบการศึกษา** __(พ.ศ.)___

ปริญญาตรี __(สาขาวิชา)_____ **สถานการศึกษา** _____(วิทยาลัย / มหาวิทยาลัย / ฯลฯ , ประเทศ)_____ **ปีที่จบการศึกษา** __(พ.ศ.)___

ปริญญาโท __(สาขาวิชา)_____ **สถานการศึกษา** _____(วิทยาลัย / มหาวิทยาลัย / ฯลฯ , ประเทศ)_____ **ปีที่จบการศึกษา** __(พ.ศ.)___

ปริญญาเอก __(สาขาวิชา)_____ **สถานการศึกษา** _____(วิทยาลัย / มหาวิทยาลัย / ฯลฯ , ประเทศ)_____ **ปีที่จบการศึกษา** __(พ.ศ.)___

สถานะการทำงานในปัจจุบัน

สถานที่ _____(ชื่อหน่วยงาน)_____ **ลักษณะการจ้าง** _____(อาชีพอิสระ/พนักงานประจำ/อื่นๆ โปรดระบุ))

ตำแหน่ง _____(ตำแหน่ง)_____ **ระยะเวลาการทำงาน** _____(ปี, เดือน)_____(สำหรับพนักงานประจำเท่านั้น)

ใบอนุญาตประกอบวิชาชีพ / สมาชิกสมาคม หรือ สถาบันที่เกี่ยวข้องกับวิชาชีพ ใบรับรอง (Certificate) (ถ้ามี) (ตัวอย่าง เช่น ใบรับรองด้าน เน็ตเวิร์ค/ โปรแกรมเมอร์/ ดาต้าเบส เป็นต้น)

1) .....

2) .....

3) .....

2. <u>ประสบการณ์การทำงาน</u> (ก่อนกรอกข้อมูลโปรดอ่านคำชี้แจงในการกรอกข้อมูลโดยละเอียด)

ช่วงเวลาที่ปฏิบัติงาน[1]	หน่วยงาน[2]	ประเภทโครงการ[3]	มูลค่าโครงการ[4]	ตำแหน่งที่รับผิดชอบ[5]	ลักษณะงานที่รับผิดชอบ[6]	หมายเหตุ
(เช่น พ.ย. 57 - ก.ค. 60 รวม 2 ปี 9 เดือน เป็นต้น)	1. (ชื่อหน่วยงาน)	(เช่น จัดทำแผนแม่บทเทคโนโลยีสารสนเทศ/ จัดทำแผนพัฒนาเทคโนโลยีสารสนเทศ/พัฒนาระบบเทคโนโลยีสารสนเทศ เป็นต้น)	..... บาท	(เช่น นักวิเคราะห์ระบบ / วิศวกรระบบ เป็นต้น)	(เช่น ออกแบบ พัฒนาระบบ/ วิเคราะห์ระบบ เป็นต้น)	

ข้าพเจ้าขอรับรองว่ารายละเอียดคุณสมบัติและประสบการณ์การทำงานข้างต้นนี้ เป็นความจริงทุกประการ

ลงชื่อ_____(ลงนามผู้มีอำนาจจากบริษัท)_____
(.....)
ตำแหน่ง.....
บริษัท.....
วันที่...../...../.....

ลงชื่อ_____(ลงนามบุคลากร)_____
(... ...)
วันที่...../...../.....

หมายเหตุ

- ในการประเมินผล รฟม. จะให้ความสำคัญต่อประสบการณ์การปฏิบัติงานแบบเต็มเวลา ดังนั้นในช่วงเวลาหนึ่งหากผู้รับผิดชอบปฏิบัติงานในหลายโครงการ รฟม. <u>จะไม่นับเวลาของแต่ละโครงการมารวมกัน</u> ผู้ยื่นข้อเสนอควรแสดงเฉพาะโครงการที่สำคัญที่สุดเพียงโครงการเดียวเท่านั้น
- **<u>ในกรณีระบุช่วงเวลาปฏิบัติงานเป็นปีโดยไม่ระบุเดือนที่ปฏิบัติงาน จะนับเวลาปฏิบัติงานโดยถือว่าบุคลากรผู้นั้นเริ่มปฏิบัติงานในปลายปีและแล้วเสร็จในต้นปีที่ระบุ</u>**
  เช่น ระบุการปฏิบัติงานในช่วงปี พ.ศ. 2543 - 2545 ก็จะนับเวลา ปฏิบัติงาน เป็น ธ.ค. 2543 - ม.ค. 2545 รวมเวลาปฏิบัติงาน 14 เดือน
  หรือ ระบุการปฏิบัติงานในช่วง ปี พ.ศ. 2542 ก็จะนับ เวลาปฏิบัติงาน เป็น ธ.ค. 2542 รวมเวลาปฏิบัติงาน 1 เดือน เป็นต้น

<u>คำชี้แจงในการกรอกรายละเอียดคุณสมบัติและประสบการณ์การทำงานของบุคลากร</u>

1.คุณสมบัติ

- กรอกตามแบบฟอร์มที่กำหนด
- โปรดแนบสำเนาใบประกาศนียบัตร หรือใบรับรองการศึกษาด้วย

2. ประสบการณ์การทำงาน

[1] ช่วงเวลาที่ปฏิบัติงาน: ให้ระบุเป็นเดือน ปี และระยะเวลาการทำงานให้ระบุเป็นจำนวนปี และเดือน ตามตัวอย่าง (ทั้งนี้หากไม่ระบุรายละเอียดช่วงเวลาที่ปฏิบัติงาน และระยะเวลาในการทำงานตามตัวอย่าง รฟม. ขอสงวนสิทธิ์ที่จะไม่ประเมินประสบการณ์ในช่วงเวลานั้น ๆ ทั้งหมด) ส่วนข้อมูลปีให้แสดงเป็นพุทธศักราช

- **<u>ในกรณีระบุช่วงเวลาปฏิบัติงานเป็นปีโดยไม่ระบุเดือนที่ปฏิบัติงาน จะนับเวลาปฏิบัติงานโดยถือว่าบุคลากรผู้นั้นเริ่มปฏิบัติงานในปลายปีและแล้วเสร็จในต้นปีที่ระบุ</u>**
  เช่น ระบุการปฏิบัติงานในช่วงปี พ.ศ. 2543 - 2545 ก็จะนับเวลา ปฏิบัติงาน เป็น ธ.ค. 2543 - ม.ค. 2545 รวมเวลาปฏิบัติงาน 14 เดือน
  หรือ ระบุการปฏิบัติงานในช่วง ปี พ.ศ. 2542 ก็จะนับ เวลาปฏิบัติงาน เป็น ธ.ค. 2542 รวมเวลาปฏิบัติงาน 1 เดือน เป็นต้น
- กรณีระบุช่วงเวลาปฏิบัติงานถึงปัจจุบัน จะนับถึงวันที่ให้ยื่นข้อเสนอ

[2] หน่วยงาน: ระบุชื่อหน่วยงานของโครงการ

[3] ประเภทโครงการ: การระบุข้อมูลประเภทโครงการ จะต้องสั้น และกระชับ แต่มีสาระสำคัญที่ครบถ้วน

[4] มูลค่าโครงการ: ระบุมูลค่าโครงการ เช่น โครงการจัดทำแผนแม่บทเทคโนโลยีสารสนเทศ โครงการจัดทำแผนพัฒนาเทคโนโลยีสารสนเทศ เป็นต้น

[5] ตำแหน่งที่รับผิดชอบ: ระบุเพียงตำแหน่งงานเพียงตำแหน่งเดียวที่บุคลากรรับผิดชอบในโครงการ

[6] ลักษณะงานที่รับผิดชอบ: การระบุรายละเอียดลักษณะงานที่รับผิดชอบ จะต้องสั้น และกระชับ แต่มีสาระสำคัญที่ครบถ้วน

อื่นๆ

- บุคลากรที่เสนอชื่อมาจะต้องลงนามรับรองเอกสารคุณสมบัติ ประสบการณ์การทำงาน และต้องลงนามกำกับเอกสารทุกหน้า ทั้งนี้ รฟม. สงวนสิทธิ์ที่จะไม่ประเมินบุคลากรนั้น ๆ หากไม่ลงนามรับรองเอกสารและลงนามกำกับเอกสารทุกหน้า
- ข้อมูลปีให้แสดงเป็นพุทธศักราช
- ให้แสดงข้อมูลเป็นภาษาไทย ยกเว้นในส่วนที่จำเป็นต้องเป็นภาษาอังกฤษ เช่น ชื่อ เมือง ประเทศ ตำแหน่ง ฯลฯ ตามความเหมาะสม
- ในการประเมินผล รฟม. จะให้ความสำคัญต่อประสบการณ์การปฏิบัติงานแบบเต็มเวลา ดังนั้นในช่วงเวลาหนึ่งหากรับผิดชอบปฏิบัติงานในหลายโครงการ รฟม. <u>จะไม่นับเวลาของแต่ละโครงการมารวมกัน</u> ผู้ยื่นข้อเสนอควรแสดงเฉพาะโครงการที่สำคัญที่สุด เพียงโครงการเดียวเท่านั้น
- กรณีผู้ยื่นข้อเสนอต่างเสนอชื่อบุคลากรหลักเป็นบุคคลเดียวกัน รฟม. ขอสงวนสิทธิ์ที่จะตัดชื่อบุคลากรรายนั้นออกจากการประเมินผลข้อเสนอของผู้ยื่นข้อเสนอทุกราย
- กรณีบุคลากรที่เสนอมีการเปลี่ยนชื่อหรือนามสกุล ให้แนบหลักฐานการเปลี่ยนชื่อหรือนามสกุลมาด้วย ทั้งนี้ รฟม. สงวนสิทธิ์ที่จะไม่ประเมินบุคลากรนั้น ๆ หากไม่มีการแนบเอกสารหลักฐานดังกล่าว
- รฟม. ขอสงวนสิทธิ์ที่จะพิจารณาเฉพาะข้อมูลบุคลากรที่ปรากฏอยู่ในแบบฟอร์มเท่านั้น
- รฟม. จะไม่ประเมินบุคลากรนั้น ๆ หากกรอกข้อมูลตามแบบฟอร์มไม่ครบถ้วน (ยกเว้นช่องมูลค่าโครงการ และช่องหมายเหตุ) หรือหากข้อมูลในแบบฟอร์ม และข้อมูลในข้อเสนอแตกต่างกัน
- รฟม. คาดหวังว่าข้อมูลต่าง ๆ ถูกต้องและเป็นไปตามความเป็นจริง ในกรณีที่มีความคลุมเครือ รฟม. อาจจะทำการตรวจสอบเพื่อยืนยันความถูกต้องของข้อมูลที่ให้มา รฟม. ขอสงวนสิทธิ์ที่จะรับหรือปฏิเสธข้อมูลบางส่วนหรือทั้งหมดที่เสนอมา และจะไม่รับผิดชอบข้อเรียกร้องที่เกิดขึ้นจากการกระทำดังกล่าว และจะไม่อธิบายหรือให้เหตุผลสำหรับการกระทำดังกล่าว

แบบฟอร์มที่ 04

แนวทาง วิธีการดำเนินงาน และรายละเอียดการเปรียบเทียบทางด้านเทคนิค

1. รายละเอียดแนวทางและวิธีการดำเนินงานของโครงการ รวมถึงเทคนิคที่ใช้ (ถ้ามี) (อ้างอิงตามข้อ 14. การจัดทำข้อเสนอโครงการ ข้อย่อย 14.4)

2. รายละเอียดแนวทางและวิธีในการพัฒนาระบบ (Methodology) และซอฟต์แวร์หรือเครื่องมือ (Tools) ที่ใช้ในการพัฒนา (อ้างอิงตามข้อ 14. การจัดทำข้อเสนอโครงการ ข้อย่อย 14.5)

3. ตารางเปรียบเทียบทางด้านเทคนิค

อ้างถึงข้อ	ข้อกำหนด/อุปกรณ์ที่ต้องการ	วิธีการดำเนินงาน/ อุปกรณ์ที่นำเสนอ	เปรียบเทียบกับข้อกำหนด /อุปกรณ์ที่ต้องการ			เอกสารอ้างอิง (ถ้ามี)
			ดีกว่า	ตรงตาม	ต่ำกว่า	
			(ระบุเครื่องหมาย√)			
ตัวอย่าง						
4. ขอบเขตการดำเนินการ						
4.1	ผู้ขายต้องมีทีมงานที่มีประสบการณ์ด้านการศึกษา ออกแบบ และพัฒนาระบบงาน อย่างน้อย ประกอบด้วยบุคลากรหลัก ดังนี้ 4.1.1 ผู้จัดการโครงการ (Project Manager) 4.1.2 นักวิเคราะห์ระบบ (System Analyst) 4.1.3 นักพัฒนาระบบ (Developer/ Programmer/ Technical) 4.1.4 วิศวกรระบบคอมพิวเตอร์ (System Engineer) 4.1.5 นักทดสอบระบบ (Implementer/ Tester) 4.1.6 ผู้ประสานงานโครงการ (Project Coordinator)	**รายละเอียดข้อกำหนดและขอบเขตของงานหรือคุณลักษณะที่ผู้ยื่นข้อเสนอนำเสนอ**				ระบุหมายเลขหน้าของเอกสารอ้างอิง
.....	.....					
.....	.....					

ประทับตรา
(ถ้ามี)

ลงชื่อ_ _ _ _(ลงนามผู้มีอำนาจจากบริษัท)_ _ _ _.
(.....)
ตำแหน่ง.....
บริษัท.....
วันที่...../...../.....

แบบฟอร์มที่ 05

รายละเอียดแผนการดำเนินงาน (Work Plan)

ลำดับ	กิจกรรม	Man - Day	ระยะเวลา (วัน)	เดือนที่ 1				เดือนที่ 2				เดือนที่ 3				เดือนที่ 4				ผู้รับผิดชอบ	
																				ชื่อ – นามสกุล	ชื่อตำแหน่ง
				1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4		
	ตัวอย่าง																				
1	ดำเนินการสำรวจและเก็บความต้องการกับผู้ใช้งาน	30	30																	1. XXXX XXXXXXXX 2. XXXX XXXXXXXX	XXXXXXX
2	วิเคราะห์และออกแบบหน้าจอระบบ และฐานข้อมูล	60	60																	1. XXXX XXXXXXXX 2. XXXX XXXXXXXX 3. XXXX XXXXXXXX	XXXXXXX
.....	.....	.....	.....																	.....	.....

ประทับตรา
(ถ้ามี)

ลงชื่อ_ _ _ _ (ลงนามผู้มีอำนาจจากบริษัท) _ _ _.
(.....)
ตำแหน่ง.....
บริษัท.....
วันที่...../...../.....