



ขอบเขตของงาน

งานจ้างบริหารจัดการความสัมพันธ์ของลูกค้า (Customer Relationship Management: CRM)

1. หลักการและเหตุผล

การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย (รฟม.) เป็นรัฐวิสาหกิจที่ดำเนินธุรกิจเกี่ยวกับกิจการรถไฟฟ้าและธุรกิจอื่นเพื่อประโยชน์แก่ รฟม. หรือประชาชน โดยกลุ่มลูกค้าซึ่งเป็นหนึ่งในกลุ่มผู้มีส่วนได้ส่วนเสียที่สำคัญของ รฟม. ประกอบด้วย ผู้ใช้บริการรถไฟฟ้า ผู้ใช้บริการอาคารและลานจอดรถ และผู้เช่าอสังหาริมทรัพย์ของ รฟม. มีความต้องการ ความคาดหวังที่ได้รับสินค้าหรือบริการที่มีมาตรฐาน มีคุณภาพ และคุ้มค่า

รฟม. มีความจำเป็นต้องปรับปรุงกระบวนการดำเนินงานด้านการบริหารความสัมพันธ์ลูกค้าผ่านช่องทาง LINE Official Account: @MRTA เพื่อเป็นเครื่องมือในการสื่อสารการตลาดเชิงรุก ยกกระดับประสบการณ์ และเพิ่มประสิทธิภาพในการให้บริการ ซึ่งจะช่วยให้ รฟม. เข้าใจพฤติกรรม ความต้องการ และความคาดหวังของกลุ่มลูกค้าเป้าหมายในเชิงลึก อันจะนำไปสู่การออกแบบกลยุทธ์การตลาด การประชาสัมพันธ์ และการสร้างความร่วมมือทางธุรกิจที่ตอบสนองต่อความต้องการของผู้ใช้บริการได้อย่างตรงจุด และมีประสิทธิผลสูงสุด

ดังนั้น รฟม. จึงมีความประสงค์ในการว่าจ้างดำเนินการบริหารจัดการความสัมพันธ์ลูกค้า (CRM) ผ่าน LINE Official Account: @MRTA เพื่อสนับสนุนการตลาดเชิงธุรกิจ และการวางกลยุทธ์ด้านการตลาด เพื่อให้สามารถนำเทคโนโลยีดิจิทัลมาปรับปรุงกระบวนการทำงานที่เกี่ยวข้องกับลูกค้า การให้บริการ การเข้าถึงความต้องการของประชาชนในการใช้บริการและการสื่อสารให้มีประสิทธิภาพมากขึ้น รวมถึงเพื่อยกระดับประสบการณ์ลูกค้าของ รฟม. จากการมอบสิทธิพิเศษในรูปแบบต่าง ๆ ผ่านกิจกรรมทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้าจาก รฟม. และการเสริมสร้างภาพลักษณ์ที่ทันสมัยให้กับองค์กร

  นิตยา  

/2. วัตถุประสงค์...

2. วัตถุประสงค์

2.1 เพื่อบูรณาการฐานข้อมูลลูกค้าของ รฟม. ให้สามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ และยกระดับประสบการณ์ของลูกค้า ผ่านการจัดการความสัมพันธ์ของลูกค้า

2.2 เพื่อออกแบบการบริหารจัดการความสัมพันธ์ของลูกค้า (Customer Relationship Management: CRM) ผ่านแพลตฟอร์ม LINE Official Account: @MRTA เพื่อเป็นเครื่องมือในการสื่อสารการตลาดเชิงรุกยกระดับประสบการณ์ และเพิ่มประสิทธิภาพในการให้บริการ

2.3 เพื่อส่งเสริมการตลาดเชิงรุกจากการบูรณาการข้อมูลจากการบริหารจัดการความสัมพันธ์ลูกค้า (Customer Relationship Management: CRM) เพื่อความร่วมมือกับพันธมิตรทางธุรกิจ

3. คุณสมบัติของผู้รับจ้าง

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทำงานและได้แจ้งเวียนชื่อให้เป็นผู้ทำงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทำงานเป็นหุ้นส่วนผู้จัดการ กรรมการ ผู้จัดการ ผู้บริหาร หรือผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐประกาศกำหนดในราชกิจจานุเบกษา

3.7 เป็นนิติบุคคลผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ รฟม. ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรม ในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นนั้น

3.10 ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ “กิจการร่วมค้า” ต้องมีคุณสมบัติ ดังนี้

3.10.1 การกำหนดสัดส่วนในการเข้าร่วมค้าของคู่สัญญา

กรณีที่มีข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงฯ จะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย



3.10.2 กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลักกิจการร่วมค่านั้น ต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลักผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน หรือหนังสือเชิญชวน

3.10.3 การยื่นข้อเสนอของกิจการร่วมค้า

1) กรณีที่ข้อตกลงฯ กำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

2) การยื่นข้อเสนอด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e - bidding) ให้ผู้เข้าร่วมค้าที่ได้รับมอบหมายหรือมอบอำนาจตามข้อ 1) ดำเนินการซื้อและดาวน์โหลดเอกสารประกวดราคาอิเล็กทรอนิกส์ กรณีที่มีการจำหน่ายเอกสารจ้างทำของจึงจะมีสิทธิในการเข้ายื่นข้อเสนอในนามกิจการร่วมค้าได้

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

3.12 ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

3.12.1 กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยหรือต่างประเทศซึ่งได้จดทะเบียนเกินกว่า 1 ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก 1 ปีสุดท้ายก่อนวันยื่นข้อเสนองบแสดงฐานะการเงิน 1 ปีสุดท้ายก่อนวันยื่นข้อเสนอ หมายถึง งบแสดงฐานะการเงินย้อนไปก่อนวันที่หน่วยงานของรัฐกำหนดให้เป็นวันยื่นข้อเสนอ 1 ปีปฏิทิน เว้นแต่กรณีนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยหากวันยื่นข้อเสนอเป็นช่วงระยะเวลาที่กรมพัฒนาธุรกิจการค้ากำหนดให้นิติบุคคลยื่นงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ซึ่งจะอยู่ในช่วงเดือนมกราคม - เดือนพฤษภาคม ของทุกปี โดยนิติบุคคลที่เป็นผู้ยื่นข้อเสนออยู่นั้นยังอยู่ในช่วงของการยื่นงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า คือ ช่วงเดือนมกราคม - เดือนพฤษภาคม กรณีนี้ให้สามารถยื่นงบแสดงฐานะการเงินย้อนไปอีก 1 ปี ได้

3.12.2 กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีกิจการรายงาน งบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า หรือกรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศ ซึ่งยังไม่มีกิจการรายงานงบแสดงฐานะการเงิน ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ไม่ต่ำกว่า 8 ล้านบาท



3.12.3 สำหรับการซื้อจัดจ้างครั้งหนึ่งที่มีวงเงินเกิน 500,000 บาทขึ้นไปกรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดาให้พิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน 90 วัน ก่อนวันยื่นข้อเสนอโดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

3.12.4 กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียนหรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ สามารถดำเนินการได้ดังนี้

1) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย หรือบุคคลธรรมดาที่ถือสัญชาติไทย ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารภายในประเทศหรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้าประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรองหรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน 90 วัน

2) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศหรือบุคคลธรรมดาที่ไม่ได้ถือสัญชาติไทย ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้าประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ หรือเป็นสินเชื่อที่ธนาคารต่างประเทศหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้าประกันตามประกาศของธนาคารกลางต่างประเทศนั้น ตามรายชื่อบริษัทที่ธนาคารกลางต่างประเทศนั้นแจ้งเวียนให้ทราบโดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน 90 วัน

3.12.5 กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศหรือบุคคลธรรมดาที่ไม่ได้ถือสัญชาติไทยตามข้อ 2 ข้อ 3 และข้อ 4 (2) มูลค่าจะต้องเป็นไปตามอัตราแลกเปลี่ยนเงินตราตามประกาศที่ธนาคารแห่งประเทศไทยกำหนด ในช่วงระหว่างวันที่เผยแพร่ประกาศและเอกสารประกวดราคาในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (e - GP) จนถึงวันเสนอราคาทั้งนี้ ผู้ยื่นข้อเสนอจะต้องยื่นเอกสารที่แสดงให้เห็นถึงข้อมูลเกี่ยวกับมูลค่าสุทธิของกิจการแล้วแต่กรณี ประกอบกับเอกสารดังกล่าวจะต้องผ่านการรับรองตามระเบียบกระทรวงการต่างประเทศว่าด้วยการรับรองเอกสาร พ.ศ. 2539 และที่แก้ไขเพิ่มเติมกำหนด โดยจะต้องยื่นเอกสารดังกล่าวในวันยื่นข้อเสนอ หากผู้ยื่นข้อเสนอไม่ได้มีการยื่นเอกสารดังกล่าวมาพร้อมกับการยื่นข้อเสนอให้ถือว่าผู้ยื่นข้อเสนอรายนั้นยื่นเอกสารไม่ครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารประกวดราคา

 13.12.6...

3.12.6 กรณีตามข้อ 3.12.1 - ข้อ 3.12.5 ไม่ใช่บังคับกับกรณีดังต่อไปนี้

- 1) กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐภายในประเทศ
- 2) นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย พ.ศ. 2483 และที่แก้ไขเพิ่มเติม
- 3) งานจ้างก่อสร้างที่กรมบัญชีกลางได้ขึ้นทะเบียนผู้ประกอบการงานก่อสร้างแล้ว และงานจ้างก่อสร้างที่หน่วยงานของรัฐที่ได้มีการจัดทำบัญชีผู้ประกอบการงานก่อสร้างที่มีคุณสมบัติเบื้องต้นไว้แล้วก่อนวันที่พระราชบัญญัติการจัดซื้อจัดจ้างฯ มีผลใช้บังคับ
- 4) การจัดซื้อจัดจ้างตามมาตรา 56 วรรคหนึ่ง (2) (ข) และ (ค) แห่งพระราชบัญญัติการจัดซื้อจัดจ้างฯ
- 5) การซื้อสิ่งหาริมทรัพย์และการเช่าสิ่งหาริมทรัพย์
- 6) กรณีงานจ้างบริการหรืองานจ้างเหมาบริการกับบุคคลธรรมดา เช่น จ้างพนักงานขับรถ ครูชาวต่างชาติ พนักงานเก็บขยะ พนักงานบันทึกข้อมูล เป็นต้น

4. ขอบเขตการดำเนินงาน

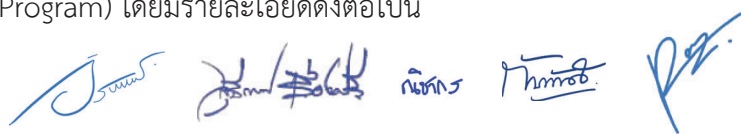
ผู้รับจ้างจะต้องดำเนินการตามขอบเขตการดำเนินงานที่ รฟม. กำหนด และรับผิดชอบค่าใช้จ่ายที่เกิดขึ้นตลอดทั้งงานจ้างฯ โดยมีรายละเอียด ดังนี้

การวางแผนกลยุทธ์ทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้า

4.1 ผู้รับจ้างจะต้องศึกษา วางแผนกลยุทธ์การดำเนินงานทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้าของ รฟม. ผ่านช่องทาง LINE Official Account: @MRTA และจัดทำหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) ตลอดระยะเวลาการดำเนินงานตามสัญญาจ้าง สำหรับพฤติกรรมการใช้งานของกลุ่มเป้าหมาย เพื่อประชาสัมพันธ์ข้อความโปรโมชั่น กิจกรรมทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้า หรือโฆษณาต่าง ๆ ให้สอดคล้องกับกลุ่มเป้าหมายของ รฟม. ได้แก่ กลุ่มลูกค้า รฟม. (ผู้ใช้บริการรถไฟฟ้ามหานคร ผู้ใช้อาคารและลานจอดรถ รฟม. และ ผู้เช่าสิ่งหาริมทรัพย์ของ รฟม.) และลูกค้าในอนาคต ได้อย่างมีประสิทธิภาพ และวิเคราะห์ทิศทางการตลาดในปัจจุบัน และการบริการอยู่เสมอเพื่อนำมาปรับปรุงแผนกลยุทธ์ทางการตลาดให้มีความทันสมัย และเป็นปัจจุบัน เพื่อตอบสนองความต้องการกลุ่มลูกค้าของ รฟม. โดยจะต้องนำเสนอให้ รฟม. เห็นชอบก่อนดำเนินการ

4.2 ศึกษาและวางกลยุทธ์ในการรักษฐานผู้ติดตาม (Followers) เพื่อลดอัตราการบล็อกช่องทาง (Block Rate) ไม่เกินร้อยละ 20 ของผู้ติดตามทั้งหมดในช่องทาง LINE Official Account: @MRTA โดยจะต้องนำเสนอให้ รฟม. เห็นชอบก่อนดำเนินการ

4.3 ผู้รับจ้างจะต้องศึกษา วิเคราะห์ และจัดทำแผนการบริหารสิทธิประโยชน์ (Privilege Point Program) สำหรับการบริหารความสัมพันธ์ลูกค้าผ่านทาง LINE Official Account: @MRTA และหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) โดยมีรายละเอียดดังต่อไปนี้



/การออกแบบ...

การออกแบบ: กำหนดและออกแบบแนวคิดทิศทางของงานจ้างบริหารจัดการความสัมพันธ์ของลูกค้าฯ ซึ่งรวมถึงเงื่อนไขและกลไกการได้รับคะแนนสะสม การใช้งานคะแนน และการแลกของรางวัลให้สอดคล้องกับขอบเขตของงาน และจำนวนพันธมิตรที่ผู้รับจ้างเป็นผู้ดำเนินการจัดหา โดยให้เหมาะสมกับกลุ่มลูกค้าที่เข้าร่วมกิจกรรมทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้า

การบริหารมูลค่าของรางวัล: วิเคราะห์ จัดทำ และนำเสนอมูลค่าของรางวัลที่จะนำมาใช้ในงานจ้างบริหารจัดการความสัมพันธ์ของลูกค้าฯ โดยต้องจัดสรรมูลค่าดังกล่าวให้เพียงพอตลอดระยะเวลาการดำเนินงานตามสัญญาจ้าง

การจัดทำ/จัดทำ : ผู้รับจ้างจะต้องจัดทำ/จัดหาของรางวัลและสิทธิพิเศษสำหรับการแลกของรางวัลสำหรับผู้เข้าร่วมกิจกรรมทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้า ให้เพียงพอต่อระยะเวลาของสัญญาและกิจกรรม

ทั้งนี้ ผู้รับจ้างจะต้องจัดทำรายละเอียดทั้งหมดในรูปแบบของแผนการดำเนินงานเป็นรายเดือนและรายปี หรือตามที่ รพม. เห็นสมควร โดยจะต้องนำเสนอให้ รพม. พิจารณาให้ความเห็นชอบก่อนดำเนินการ

การบริหารจัดการความสัมพันธ์ของลูกค้า (Customer Relationship Management: CRM)

ผ่านทาง LINE Official Account: @MRTA และหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program)

4.4 ผู้รับจ้างจะต้องเป็นผู้รับผิดชอบค่าใช้จ่ายในการดำเนินการต่ออายุบัญชีการใช้งาน Line OA เป็นรายปี และค่าใช้จ่ายแพ็คเกจข้อความ (LINE Official Account Package) รวมถึงแพ็คเกจเสริม (Additional Message) ตลอดระยะเวลาการดำเนินงานตามสัญญาจ้าง เพื่อให้สามารถใช้งานได้อย่างต่อเนื่อง และสามารถส่งข้อความจำนวนไม่น้อยกว่า 20,000,000 ข้อความ (ยี่สิบล้านข้อความ) ตลอดระยะเวลาการดำเนินงานตามสัญญาจ้าง ถึงผู้ติดตามที่เกี่ยวข้องกับการบริหารความสัมพันธ์ลูกค้าผ่านทาง LINE Official Account: @MRTA หรืองานอื่น ๆ ที่เกี่ยวข้องกับ รพม.

4.5 ผู้รับจ้างจะต้องดำเนินการอัปเดตข้อมูล นำเข้าเนื้อหากิจกรรมทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้า ข่าวประชาสัมพันธ์ และข้อมูลสำคัญอื่น ๆ ของ รพม. ทั้งภาษาไทยและภาษาอังกฤษ หรือตามที่ รพม. เห็นชอบ ตลอดจนวางแผนและดำเนินการส่งข้อความแบบกลุ่ม (Broadcast) ให้เหมาะสมกับกลุ่มเป้าหมาย เพื่อแจ้งข้อมูลข่าวสาร การแจ้งเตือนต่าง ๆ และนำเสนอกิจกรรมทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้า ที่เกี่ยวข้องกับการบริหารความสัมพันธ์ลูกค้า หรืองานอื่น ๆ ที่เกี่ยวข้องกับ รพม. ตลอดระยะเวลาการดำเนินงานตามสัญญาจ้าง

4.6 ดำเนินการดูแลระบบตอบกลับอัตโนมัติ (Auto-Reply) ที่เกี่ยวข้องกับการบริหารจัดการความสัมพันธ์ของลูกค้าฯ โดยการตั้งค่าเซตบทให้ทำงานอย่างมีประสิทธิภาพ และจะต้องกำหนด Keyword จากคำถามที่ลูกค้ามักถามบ่อยๆ เช่น สะสมแต้ม, ของรางวัล เพื่อให้ตอบคำถามกลับอัตโนมัติได้ทันที ทั้งนี้จะต้องนำเสนอให้ รพม. เห็นชอบก่อน

4.7 ผู้รับจ้างจะต้องจัดทำ และพัฒนารูปแบบการแสดงผล รวมถึงปรับปรุงคุณสมบัติ (Features) ต่าง ๆ ที่เหมาะสมและมีประโยชน์ โดยคำนึงถึงการให้ข้อมูลที่สมบูรณ์ต่อกลุ่มเป้าหมายและง่ายต่อการใช้งาน และสอดคล้องกับแผนการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้าฯ ตามข้อ 4.1 และแผนการบริหารสิทธิประโยชน์ (Privilege Point Program) ตามข้อ 4.3

4.8 ผู้รับจ้างจะต้องบริหารจัดการฟังก์ชันการบริหารจัดการความสัมพันธ์ลูกค้า ผ่านทาง LINE Official Account: @MRTA และหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) ในส่วนที่เกี่ยวข้องกับกิจกรรมทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้า ในการคำนวณคะแนนสะสมของลูกค้าให้มีความถูกต้องแม่นยำ

4.9 ดำเนินการออกแบบเมนูลัดด้านล่าง Rich Menu โดยสามารถตั้งค่าปุ่มให้สามารถเข้าถึงส่วนต่าง ๆ ได้ทันที และสามารถกำหนดได้ว่า ต้องการให้ผู้ติดตามกดแล้วไปที่เมนูหรือช่องทางใด เช่น เมนูบัตรโดยสาร เมนู Promotion/Special Deal เมนูแผนที่เส้นทาง/ค่าโดยสาร เมนูที่จอดรถ ติดต่อสอบถาม เมนู MRTA Rewards เป็นต้น อย่างน้อย 3 รูปแบบ หรือตามที่ รฟม. เห็นสมควร ทั้งนี้ ผู้รับจ้างจะต้องเป็นผู้นำเสนอรูปแบบของเมนูลัด Rich Menu ให้ รฟม. เห็นชอบก่อน

4.10 ดำเนินการออกแบบ Card Message หรือข้อความในรูปแบบของภาพสไลด์ เพื่อให้สามารถเลือกดูข้อมูลได้ด้วยการปิดภาพไปด้านข้าง เช่น การโปรโมทงานอีเวนต์ หรืออื่น ๆ ที่เกี่ยวข้อง โดยให้สอดคล้องกับจำนวนกิจกรรมทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้า หรือตามที่ รฟม. เห็นสมควร

4.11 ดำเนินการออกแบบดีไซน์สำหรับ Greeting Message ข้อความทักทายที่จะ Pop-Up ขึ้นจำนวนไม่น้อยกว่า 10 ข้อความ หรือตาม รฟม. เห็นชอบ ตลอดระยะเวลาการดำเนินงานตามสัญญาจ้าง เมื่อมีการเพิ่มการติดตาม (Add Friend) LINE OA เป็นครั้งแรก เพื่อสร้างประสบการณ์ที่ดีให้กับผู้ใช้งาน

4.12 ผู้รับจ้างจะต้องออกแบบ และจัดเก็บข้อมูลของผู้เข้าร่วมกิจกรรมทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้าในหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) ดังนี้

- 1) ชื่อ – สกุล
- 2) ชื่อ LINE ID
- 3) อีเมล
- 4) เบอร์โทรศัพท์
- 5) ที่อยู่ (สำหรับจัดส่งของรางวัล)

โดยผู้รับจ้างจะต้องเป็นผู้รับผิดชอบในการออกแบบ จัดเก็บข้อมูลแต่เพียงผู้เดียว และจะปฏิบัติงานภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล และกฎหมาย กฎระเบียบ และข้อบังคับตามเงื่อนไขอื่น ๆ ข้อ 10.12 – 10.16

4.13 หน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) จะต้องสามารถกำหนดเงื่อนไขและแสดงรายละเอียดของสิทธิพิเศษได้อย่างครบถ้วน เช่น กำหนดเงื่อนไขการจัดสรรการสะสมแต้ม การแลกของรางวัล และการใช้งานของลูกค้าย ซึ่งจะต้องสามารถแยกหรือรวมกลุ่มระหว่างผู้ใช้บริการอาคารและลานจอดรถของ รฟม. กับผู้เข้าร่วมกิจกรรมทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้าต่าง ๆ ได้ตามที่ รฟม. กำหนด นอกจากนี้ จะต้องสามารถระบุข้อมูลของรายการสิทธิพิเศษ จำนวนคะแนนที่ใช้แลก หรือของรางวัล เพื่อแสดงผลบน LINE Official Account: @MRTA และหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) ได้ ทั้งนี้ เงื่อนไขและข้อมูลสิทธิพิเศษทั้งหมดจะต้องได้รับความเห็นชอบจาก รฟม. ก่อนดำเนินการ

4.14 หน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) จะต้องสามารถแสดงรายการของรางวัลทั้งหมด ผ่านหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) พร้อมทั้งสามารถค้นหาจากรหัสหรือชื่อของรางวัลได้ เป็นอย่างน้อย รวมทั้งสามารถตั้งคำถามหรือประเภทสินค้า ของรางวัล สิทธิพิเศษต่าง ๆ โดยการกำหนด ในครั้งแรกก่อนการเปิดให้ลูกค้าเริ่มใช้บริการ ทั้งนี้ ผู้รับจ้างจะต้องนำเสนอรูปแบบการแสดงผลรายการของรางวัล สิทธิพิเศษ พร้อมทั้งรูปแบบการค้นหาจากชื่อของรางวัลและรหัส ให้ รฟม. เห็นชอบก่อนดำเนินการ

4.15 หน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) จะต้องตั้งค่าคำค้นหาด้วยชื่อของรางวัล โดยระบบจะแสดงผลของรางวัลประเภทเดียวกับคำที่ค้นหา เช่น ค้นหาว่า กาแฟ หน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) จะต้องแสดงผลของรางวัลและสิทธิพิเศษทุกร้านค้า หรือที่เกี่ยวข้องกับคำที่ค้นหา

4.16 หน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) จะต้องสามารถตัดคะแนนเมื่อลูกค้าแลก ของรางวัล/สิทธิพิเศษ หรือใช้คะแนนจากวันที่/ช่วงเวลาของคะแนน และจะต้องแสดงข้อความหากของรางวัลหรือ สิทธิพิเศษหมด (Sold Out) หรือคำอื่น ๆ แบบ Real-time ตามที่ รฟม. เลือกใช้ให้สอดคล้องกับความหมาย ในการใช้งาน

4.17 หน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) จะต้องสามารถแสดงประวัติการแลกคะแนน สะสม และอายุของคะแนนสะสมของลูกค้าได้

4.18 หน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) จะต้องสามารถใส่รหัสดิจิทัลโค้ด (E-Coupon Code) ได้ตามที่ รฟม. กำหนด และจะต้องสามารถสร้างรหัสใหม่ในรูปแบบรหัสดิจิทัลโค้ดที่ไม่ซ้ำกันได้ โดยแสดง ให้ลูกค้าใช้งานในรูปแบบรหัสตัวเลขและตัวหนังสือ Barcode และ QR Code สำหรับของรางวัลที่ไม่ต้องจัดส่ง เพื่อให้ลูกค้าสามารถนำมาใช้ในการแลกซื้อ/แลกรับของรางวัล สิทธิพิเศษต่าง ๆ ที่กำหนด

4.19 หน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) จะต้องสามารถติดตามสถานะของรางวัลที่เป็น Physical ได้ และจะต้องมีเลขพัสดุให้กับลูกค้าสำหรับใช้ตรวจสอบด้วยตนเองผ่านแพลตฟอร์มอื่น ๆ

4.20 หน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) จะต้องสามารถแสดงแบบประเมิน ความพึงพอใจหลังจากการแลกของรางวัล และหลังจากการร่วมกิจกรรม หรือตามที่ รฟม. กำหนด เพื่อเก็บ รวบรวมความคิดเห็นและใช้ในการวิเคราะห์ความพึงพอใจ ความต้องการ ความคาดหวังของลูกค้าที่ร่วมแลกของ รางวัล สิทธิพิเศษ และร่วมกิจกรรม



4.21 หน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) จะต้องสามารถแสดงผลเป็นรูปแบบ Dashboard เพื่อดูภาพรวมต่าง ๆ ของการแลกของรางวัล การจัดการของรางวัลในแต่ละกิจกรรมทางการตลาด ด้านการบริหารความสัมพันธ์ลูกค้า โดยจะต้องรองรับการนำข้อมูลออกไปใช้งานได้หลายรูปแบบ เช่น .xlsx .jpeg .csv เป็นต้น

4.22 ผู้รับจ้างต้องให้สิทธิเจ้าหน้าที่ รฟม. ให้สามารถเข้าดูข้อมูล และสามารถบริหารจัดการรายการต่าง ๆ ได้ บนหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program)

4.23 รูปแบบของการบริหารความสัมพันธ์ของลูกค้าผ่านทาง LINE Official Account: @MRTA และหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) ที่ผู้รับจ้างจะต้องนำเสนอ นั้น จะต้องดำเนินการในรูปแบบที่มีการรับรองความปลอดภัย นำเชื่อถือและการใช้งานตามมาตรฐานสากล โดยผู้รับจ้างจะต้องนำเสนอรูปแบบการดำเนินงานด้านความปลอดภัยต่าง ๆ เช่น การยืนยันตัวตน เป็นต้น ทั้งนี้ จะต้องให้ รฟม. เห็นชอบก่อน

4.24 ผู้รับจ้างจะต้องให้คำแนะนำ และคำปรึกษาเมื่อ รฟม. ต้องการเกี่ยวกับการใช้งานการบริหารความสัมพันธ์ลูกค้าผ่านทาง LINE Official Account: @MRTA และหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) รวมถึงอธิบายเกี่ยวกับรายละเอียดของเอกสารคู่มือระบบงาน รวมถึงการแก้ปัญหาหรือวิธีการที่จะแก้ไขระบบงานให้ดีขึ้นตลอดสัญญาตามที่ได้รับแจ้งจาก รฟม. ตลอดระยะเวลาการดำเนินงานตามสัญญาจ้าง

4.25 เมื่อสิ้นสุดสัญญา ผู้รับจ้างต้องนำส่งข้อมูลทั้งหมดที่อยูในการบริหารความสัมพันธ์ลูกค้าผ่านทาง LINE Official Account: @MRTA และหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) ที่เกี่ยวข้องกับการสะสมคะแนนแลกลิทธิพิเศษสำหรับลูกค้า ให้กับ รฟม. โดยผู้รับจ้างต้องไม่มีการเรียกเก็บค่าใช้จ่ายใด ๆ เพิ่มเติมกับ รฟม.

4.26 ผู้รับจ้างจะต้องไม่เก็บหรือนำข้อมูลที่ได้จากการดำเนินการตามสัญญาไปใช้ประโยชน์นอกเหนือจากที่ รฟม. กำหนด ทั้งนี้ หากสิ้นสุดสัญญาและผู้รับจ้างได้ดำเนินการตามข้อ 4.25 เรียบร้อยแล้ว ผู้รับจ้างจะต้องทำลายข้อมูลทดสอบ หรือข้อมูลอื่น ๆ ของ รฟม. ที่บริษัทจัดเก็บไว้ โดยจะต้องมีการจัดทำเอกสารการทำลายข้อมูล และเสนอให้ รฟม. พิจารณาเห็นชอบก่อนดำเนินการ

4.27 ผู้รับจ้างต้องทำหน้าที่บำรุงรักษาช่องทาง LINE Official Account: @MRTA และหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) หรืออื่น ๆ ของ รฟม. ที่เกี่ยวข้องกับขอบเขตของงาน เพื่อให้การทำงานเป็นไปอย่างต่อเนื่อง มีประสิทธิภาพ และทำงานได้ตามเงื่อนไขที่กำหนดได้ตลอดระยะเวลาการดำเนินงานตามสัญญาจ้าง ทั้งนี้ หากเกิดปัญหาขึ้น ผู้รับจ้างต้องดำเนินการแก้ไขให้แล้วเสร็จเป็นปกติ ภายในระยะเวลา 1 วัน นับถัดจากที่ได้รับแจ้งผ่านช่องทาง LINE Official Account: @MRTA และหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) หรือช่องทางอื่น ๆ ที่ รฟม. กำหนด



4.28 กรณีที่มีการใช้งานระบบหรือซอฟต์แวร์ประมวลผลข้อมูลร่วมกับ LINE Official Account: @MRTA ผู้รับจ้างจะต้องทดสอบเจาะระบบ (Penetration Testing) และปิดช่องโหว่ (Hardening) ของระบบหรือซอฟต์แวร์ที่เกี่ยวข้อง พร้อมทั้งจัดส่งเอกสารผลการดำเนินการให้ รฟม. พิจารณาผลก่อนเริ่มใช้งานระบบ และหากระบบหรือซอฟต์แวร์นั้น ๆ มีการประกาศช่องโหว่ที่เกี่ยวข้องผู้รับจ้างจะต้องปิดช่องโหว่ของระบบที่เกี่ยวข้องโดยไม่มีค่าใช้จ่ายเพิ่มเติม โดยกำหนดให้ปิดช่องโหว่ ดังนี้

- 1) ระดับวิกฤติ (Critical) ภายใน 30 วัน
- 2) ระดับสูง (High) ภายใน 45 วัน
- 3) ระดับปานกลาง (Medium) ภายใน 60 วัน
- 4) ระดับต่ำ (Low) ภายใน 120 วัน

ทั้งนี้ หากผู้รับจ้างไม่สามารถปิดช่องโหว่ให้แล้วเสร็จภายในระยะเวลาที่กำหนด ผู้รับจ้างจะต้องจัดทำเอกสารรายงานผล ซึ่งระบุรายละเอียดและสาเหตุที่ไม่สามารถปิดช่องโหว่ พร้อมทั้งจัดส่งให้ รฟม. พิจารณาให้ความเห็นชอบ เว้นแต่กรณีที่ซอฟต์แวร์นั้น ๆ เป็นซอฟต์แวร์สำเร็จรูปที่มีการเช่าหรือซื้อจากผู้ผลิต ผู้รับจ้างจะต้องจัดส่งใบรับรองมาตรฐาน (Certificate) เช่น ISO/IEC หรือใบรับรองมาตรฐานด้านความปลอดภัยจากผู้ผลิตให้ รฟม. พิจารณาก่อนเริ่มใช้งานระบบ เพื่อยืนยันว่าซอฟต์แวร์ดังกล่าวทำงานได้ตามมาตรฐานความมั่นคงปลอดภัยในปัจจุบัน

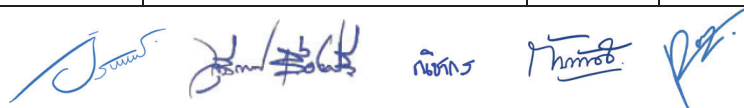
4.29 เมื่อผู้รับจ้างจะเข้าดำเนินการเพื่อแก้ไขปัญหาต่าง ๆ จะต้องแจ้งให้เจ้าหน้าที่ผู้รับผิดชอบของ รฟม. ทราบและเห็นชอบก่อนเข้าดำเนินการ

การจัดหาพันธมิตร บริหารจัดการของรางวัล และสิทธิพิเศษ

4.30 ผู้รับจ้างจะต้องจัดหาพันธมิตรในการทำเรื่องสิทธิพิเศษในรูปแบบของการทำ Co-Promotion หรือรูปแบบอื่นใดตามความเหมาะสมตามที่ รฟม. เห็นชอบ และจัดทำของรางวัลเพื่อดำเนินกิจกรรมทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้า รวมถึงการบริหารจัดการ Stock ให้เป็นไปตามแผน ทั้งที่เกิดจากการใช้คะแนนสะสม และการใช้สิทธิพิเศษของลูกค้าภายในระยะเวลาตามประเภทและจำนวนที่ รฟม. กำหนด

4.31 ผู้รับจ้างจะต้องมีร้านค้า/แบรนด์ ในหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) สำหรับบริหารจัดการของรางวัลและสิทธิพิเศษ สะสมไม่น้อยกว่า 60 ร้านค้าหรือแบรนด์ ตลอดระยะเวลาการดำเนินงานตามสัญญาจ้าง และจัดแบ่งกลุ่มร้านค้า/แบรนด์อย่างเหมาะสม ดังนี้

ลำดับ	ประเภท	ตัวอย่าง	จำนวน (สะสม) ปีที่ 1	จำนวน (สะสม) ปีที่ 2	จำนวน (สะสม) ปีที่ 3
1	กลุ่มสิทธิพิเศษจากห้างสรรพสินค้า/ ร้านค้าขนาดใหญ่	The 1 Points / M Point/ ONESIAM Coin เป็นต้น	1	2	3

 /ลำดับ...

ลำดับ	ประเภท	ตัวอย่าง	จำนวน (สะสม) ปีที่ 1	จำนวน (สะสม) ปีที่ 2	จำนวน (สะสม) ปีที่ 3
2	กลุ่มบริษัทที่ผลิตสินค้า หรือ บริการ (Product & Service) ร้านอาหาร (Food Chain) และ แบรนด์ชั้นนำ (Brand)	True Point / Blue Card / Grab Rewards / AirAsia BIG Rewards / Minor Plus / Starbucks Rewards / KFC / McDonald เป็นต้น	10	20	30
3	กลุ่มผู้ประกอบการรายย่อย	ผู้เช่าร้านค้าเชิงพาณิชย์ของ รฟม. ร้านค้าตามแนวสายทาง รถไฟฟ้ามหานคร	10	20	30

หมายเหตุ: รายชื่อร้านค้า/แบรนด์ ปีที่ 2 และ 3 สามารถซ้ำกับปีที่ 1 และ 2 ได้ตามลำดับ

โดยผู้รับจ้างจะต้องสามารถส่งข้อมูลของรางวัลและสิทธิพิเศษจากร้านค้า หรือแบรนด์ดังกล่าว ให้ รฟม. พิจารณา ก่อนแสดงผลบนหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) ภายในระยะเวลา 15 วัน นับตั้งแต่ รฟม. เลือกร้านค้า/แบรนด์ และจะต้องให้สอดคล้องกับแผนการบริหารสิทธิประโยชน์ (Privilege Point Program) ข้อ 4.3

4.32 ผู้รับจ้างจะต้องทำหน้าที่นำของรางวัลและสิทธิพิเศษที่ผู้รับจ้างจัดหา รวมถึงบริการที่ รฟม. ให้บริการและสินค้าของรางวัล (Premium Gift) ที่ รฟม. เป็นผู้จัดหาขึ้นบนหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) หรือช่องทางอื่น ๆ ที่ รฟม. เห็นสมควร ทั้งนี้ จะต้องสอดคล้องกับแผนการบริหารสิทธิประโยชน์ (Privilege Point Program) ข้อ 4.3 โดยกำหนดรายละเอียดของรางวัลและสิทธิพิเศษอย่างน้อย ดังนี้

- (1) ชื่อของรางวัลและสิทธิพิเศษ
- (2) รายละเอียดต่าง ๆ ซึ่งอยู่ในรูปแบบของ ข้อความ รูปภาพ วิดีโอ เป็นต้น
- (3) กำหนดคะแนนที่ใช้แลกของรางวัล
- (4) ประเภทของรางวัล เช่น ประเภท Physical หรือ Non-Physical

4.33 ผู้รับจ้างจะต้องมีการจัดส่งของรางวัลตามที่อยู่ของลูกค้าที่ได้ลงทะเบียนไว้ ทั้งนี้ ในกรณีที่รางวัลนั้น เป็นรูปแบบ Physical โดยส่งออกของรางวัลให้แก่ลูกค้า ภายใน 15 วัน หลังจากที่ถูกแจ้งความประสงค์แลก ของรางวัล เว้นแต่หากมีกรณีฉุกเฉินผู้รับจ้างจะต้องแจ้งให้ รฟม. รับทราบก่อน เพื่อวางแผนการดำเนินงานจัดส่ง รางวัลให้แก่ลูกค้า

4.34 ผู้รับจ้างจะต้องดูแลและบริหารสินค้าคงคลัง ในส่วนที่เป็นบริการที่ รฟม. ให้บริการ และสินค้า ของรางวัล (Premium Gift) ที่ รฟม. เป็นผู้จัดหา และต้องจัดส่งสินค้าคงเหลือกลับคืนให้ รฟม. ในกรณีที่ รฟม. ต้องการหรือเมื่อสิ้นสุดระยะเวลาการดำเนินงาน

  นิตยาร  

/4.35 ผู้รับจ้าง...

4.35 ผู้รับจ้างมีหน้าที่รับผิดชอบในการติดต่อ ประสานงาน ขออนุญาต และดำเนินการอื่นใดที่เกี่ยวข้องกับสัญญาจ้างทั้งหมด ทั้งหน่วยงานภาครัฐ/เอกชน หรืออื่น ๆ ตามที่ รฟม. กำหนด เพื่อให้การดำเนินงานตามขอบเขตของงานสำเร็จลุล่วงตามวัตถุประสงค์และระยะเวลาที่กำหนด และหากมีค่าใช้จ่ายในการปฏิบัติงาน ผู้รับจ้างจะต้องเป็นผู้รับผิดชอบค่าใช้จ่ายทั้งหมด

4.36 ในกรณีที่มีการแลกรับของรางวัลผ่านช่องทาง LINE Official Account: @MRTA และหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) หรือช่องอื่น ๆ ของ รฟม. ที่เกี่ยวข้องกับขอบเขตของงาน ผู้รับจ้างจะต้องเป็นผู้รับผิดชอบในการออกค่าใช้จ่าย และชำระภาษีหัก ณ ที่จ่าย หรือค่าธรรมเนียมอื่นใดที่เกี่ยวข้องกับการมอบของรางวัลนั้น ๆ แทน รฟม. และผู้ได้รับรางวัลทั้งหมด ทั้งนี้ หากเกิดข้อร้องเรียน หรือการถูกประเมินภาษีย้อนหลังจากการดำเนินกิจกรรมดังกล่าว รฟม. จะไม่มีส่วนรับผิดชอบต่อค่าใช้จ่ายหรือความเสียหายใด ๆ และผู้รับจ้างจะต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว

การจัดกิจกรรมทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้า

ผ่านทาง LINE Official Account: @MRTA และหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program)

4.37 ผู้รับจ้างจะต้องจัดให้มีกิจกรรมทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้า ผ่านช่องทาง LINE Official Account: @MRTA และหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) จำนวนไม่น้อยกว่า 12 กิจกรรม ให้ครอบคลุมตลอดระยะเวลาการดำเนินงานตามสัญญาจ้างหรือตามที่ รฟม. เห็นสมควร ตลอด โดยจัดทำเป็นแผนระยะสั้น และแผนระยะกลาง เช่น รูปแบบของการดำเนินกิจกรรมทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้า ระยะเวลาของกิจกรรม กลุ่มเป้าหมาย และการจัดเก็บข้อมูล ให้สอดคล้องกับการดำเนินงาน และตามที่ รฟม. กำหนด ทั้งนี้จะต้องนำเสนอให้ รฟม. เห็นชอบก่อนดำเนินการ เพื่อตอบโจทย์กลุ่มเป้าหมายและดึงดูดให้มีการติดตามทางช่องทาง LINE Official Account: @MRTA เพิ่มขึ้น โดยแต่ละกิจกรรมต้องมีการวัดผลที่ได้จำนวนผู้ติดตามใหม่ (New Followers) ที่เกี่ยวข้องกับงานด้านการบริหารจัดการความสัมพันธ์ของลูกค้า จำนวนไม่น้อยกว่า 200 ผู้ติดตาม/กิจกรรม

4.38 ผู้รับจ้างต้องสรุปผลการดำเนินงานตามแผนทั้งหมด พร้อมจัดทำข้อเสนอแนะของงานจ้างฯ โดยมีรายงานอย่างน้อย ดังนี้

- (1) จำนวนการสมัครสมาชิก
- (2) จำนวนผู้เข้าร่วมกิจกรรมฯ ของ รฟม. (Engagement user) / รายกิจกรรม
- (3) จำนวนผู้ติดตามที่เพิ่มขึ้น (New Follower)
- (4) อัตราการบล็อก (Block Rate) และอัตราการเปิด (Open rate)
- (5) รายงานผลการจัดส่งของรางวัล
- (6) จำนวนข้อความที่ส่ง
- (7) จำนวนพันธมิตรที่ร่วมกับ รฟม.
- (8) รายงานผลการจัดทำสื่อประชาสัมพันธ์



(9) รายงานผลด้านการบริหารจัดการของรางวัลและสิทธิพิเศษ เช่น ผลการ Redeem และสรุปสินค้าคงคลัง เป็นต้น

(10) รายงานสรุปการแจ้งปัญหาของการบริหารความสัมพันธ์ลูกค้าฯ จาก LINE Official Account: @MRTA หน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) และ Call Center โดยระบุสาเหตุและวิธีแก้ปัญหา

(11) รายงานข้อตกลงระดับการให้บริการ (Service Level Agreement) และเวลาในการกู้คืนระบบ (Recovery Time) โดยระบุสาเหตุและวิธีแก้ปัญหา

4.39 ผู้รับจ้างจะต้องให้มีศูนย์บริการลูกค้า (Call Center) และผู้ดูแลระบบ (Admin) จำนวนไม่น้อยกว่า 1 คน เพื่ออำนวยความสะดวกสำหรับการให้บริการข้อมูล โดยมีรายละเอียดดังนี้

(1) จัดให้มีเจ้าหน้าที่ที่มีประสบการณ์และความเชี่ยวชาญ สำหรับให้คำแนะนำและตอบข้อซักถามเกี่ยวกับเงื่อนไขการสะสมคะแนน การตรวจสอบสถานะคะแนน ขั้นตอนการแลกรับของรางวัล และการติดตามความคืบหน้าในประเด็นที่เกี่ยวข้องกับการจัดส่งของรางวัล ตลอดจนรายละเอียดอื่น ๆ ที่เกี่ยวข้องกับขอบเขตของงานฯ กรณีที่ได้รับแจ้งปัญหาผ่านช่องทาง LINE Official Account: @MRTA และหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) หรืออื่น ๆ ของ รฟม. ที่เกี่ยวข้อง

(2) การให้บริการศูนย์บริการลูกค้า (Call Center) และผู้ดูแลระบบ (Admin) จะต้องสามารถให้บริการได้ทุกวันตลอด 24 ชั่วโมง หรือตามที่ รฟม. เห็นสมควร

4.40 การจัดกิจกรรมทางการตลาดด้านการบริหารความสัมพันธ์ลูกค้าผ่านทาง LINE Official Account: @MRTA และหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) จะต้องสามารถดำเนินงานร่วมกับกิจกรรมอื่น ๆ ตามที่ รฟม. ร้องขอ โดยผู้รับจ้างจะต้องมีหน้าที่ดำเนินการร่วมกับ รฟม. หรือผู้แทนอื่น ๆ ตามที่ รฟม. กำหนด

5. กำหนดเวลาส่งมอบพัสดุ

ผู้รับจ้างจะต้องดำเนินการตามขอบเขตของงานจ้างบริหารจัดการความสัมพันธ์ของลูกค้า (Customer Relationship Management: CRM) ภายในระยะเวลา 1,100 วัน (หนึ่งพันหนึ่งร้อยวัน) นับถัดจากวันลงนามในสัญญาจ้าง

6. หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

พิจารณาคัดเลือกข้อเสนอครั้งนี้ รฟม. ใช้หลักเกณฑ์ราคาประกอบเกณฑ์อื่น (Price Performance) โดยกำหนดสัดส่วนของน้ำหนักในการให้คะแนนตามปัจจัยหลัก และน้ำหนักที่กำหนด ดังนี้

- | | |
|---|---|
| 1) ราคาที่ยื่นข้อเสนอ (Price) | กำหนดน้ำหนักเท่ากับ ร้อยละ 30 (100 คะแนน) |
| 2) ข้อเสนอด้านเทคนิค คุณภาพและคุณสมบัติ | กำหนดน้ำหนักเท่ากับ ร้อยละ 70 (100 คะแนน) |
- ที่เป็นประโยชน์ต่อ รฟม.

/7. งบประมาณ...



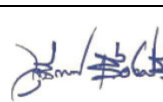
7. งบประมาณ

วงเงินงบประมาณงานจ้างบริหารจัดการความสัมพันธ์ของลูกค้า (Customer Relationship Management: CRM) จำนวนเงินทั้งสิ้น 21,000,000 บาท (ยี่สิบเอ็ดล้านบาทถ้วน) ซึ่งได้รวมภาษีมูลค่าเพิ่ม ตลอดจนภาษีอากรอื่น ๆ และค่าใช้จ่ายทั้งปวงแล้ว

8. งวดงานและการจ่ายเงิน

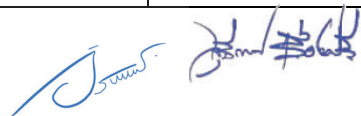
รฟม. จะต้องชำระเงินตามสัญญาเป็นการชำระแบบรายงวด ซึ่งได้รวมภาษีมูลค่าเพิ่ม ตลอดจนภาษีอากรอื่น ๆ และค่าใช้จ่ายทั้งปวงแล้ว โดยมีรายละเอียดการชำระเงินแบ่งเป็น 12 งวด ดังนี้

งวดงาน	จำนวนเงิน	รายละเอียดการส่งมอบงาน	กำหนดวันส่งมอบ
1	ร้อยละ 15 ของมูลค่าตามสัญญา	1. จัดทำแผน และส่งมอบแผนการดำเนินงานด้านวางแผนกลยุทธ์ทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้า (สำหรับปีที่ 1) <u>ตามข้อ 4.1 – 4.3</u> 2. นำเสนอแผนการจัดอบรม ครั้งที่ 1 <u>ตามข้อ 10.3</u> 3. รายงานความคืบหน้าการบริหารจัดการความสัมพันธ์ของลูกค้า (Customer Relationship Management: CRM) ผ่านทาง LINE Official Account: @MRTA และหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) <u>ตามข้อ 4.4 – 4.23</u> 4. ทดสอบระบบและซอฟต์แวร์ที่เกี่ยวข้อง<u>ตามข้อ 4.28</u> 5. รายงานผลการดำเนินงานด้านบริหารจัดการของรางวัลและสิทธิพิเศษ <u>ตามข้อ 4.30 – 4.32</u> 6. จัดเตรียมความพร้อมศูนย์บริการลูกค้าและผู้ดูแลระบบ <u>ตามข้อ 4.39</u> 7. จัดหาอุปกรณ์อิเล็กทรอนิกส์ <u>ตามข้อ 10.4</u>	ภายใน 90 วันนับถัดจากวันที่ลงนามสัญญา

  นิตกร 

/งวดงาน...

งวดงาน	จำนวนเงิน	รายละเอียดการส่งมอบงาน	กำหนดวันส่งมอบ
		8. ดำเนินการจัดกิจกรรมทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้า และรายงานสรุปผลการจัดกิจกรรมฯ ตามข้อ 4.37 – 4.38	
2	ร้อยละ 7 ของมูลค่า ตามสัญญา	1. ดำเนินการจัดกิจกรรมทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้า และรายงานสรุปผลการจัดกิจกรรมฯ ตามข้อ 4.37 – 4.38 2. รายงานผลการดำเนินงานด้านบริหารจัดการของรางวัลและสิทธิพิเศษ ตามข้อ 4.31, 4.32 และ 4.34 3. จัดอบรม และรายงานสรุปผลการจัดอบรม ครั้งที่ 1 ตามข้อ 10.3	ภายใน 180 วันนับถัดจากวันที่ลงนามสัญญา
3	ร้อยละ 7 ของมูลค่า ตามสัญญา	1. ดำเนินการจัดกิจกรรมทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้า และรายงานสรุปผลการจัดกิจกรรมฯ ตามข้อ 4.37 – 4.38 2. รายงานผลการดำเนินงานด้านบริหารจัดการของรางวัลและสิทธิพิเศษ ตามข้อ 4.31, 4.32 และ 4.34	ภายใน 270 วันนับถัดจากวันที่ลงนามสัญญา
4	ร้อยละ 10 ของมูลค่า ตามสัญญา	1. ต่ออายุบัญชีการใช้งาน LINE OA ตามข้อ 4.4 2. จัดทำแผน และส่งมอบแผนการดำเนินงานด้านวางแผนกลยุทธ์ทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้า (สำหรับปีที่ 2) ตามข้อ 4.1 – 4.3 3. รายงานผลการดำเนินงานด้านบริหารจัดการของรางวัลและสิทธิพิเศษ ตามข้อ 4.30 – 4.32 4. ดำเนินการจัดกิจกรรมทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้า และรายงานสรุปผลการจัดกิจกรรมฯ ตามข้อ 4.37 – 4.38 5. นำเสนอแผนการจัดอบรม ครั้งที่ 2 ตามข้อ 10.3	ภายใน 360 วันนับถัดจากวันที่ลงนามสัญญา




/งวดงาน...

งวดงาน	จำนวนเงิน	รายละเอียดการส่งมอบงาน	กำหนดวันส่งมอบ
5	ร้อยละ 7 ของมูลค่า ตาสัญญา	1. ดำเนินการจัดกิจกรรมทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้า และรายงานสรุปผลการจัดกิจกรรมฯ <u>ตามข้อ 4.37 – 4.38</u> 2. รายงานผลการดำเนินงานด้านบริหารจัดการของรางวัล และสิทธิพิเศษ <u>ตามข้อ 4.31, 4.32 และ 4.34</u> 3. จัดอบรม และรายงานสรุปผลการจัดอบรม ครั้งที่ 2 <u>ตามข้อ 10.3</u>	ภายใน 450 วันนับถัดจากวันที่ลงนามสัญญา
6	ร้อยละ 7 ของมูลค่า ตาสัญญา	1. ดำเนินการจัดกิจกรรมทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้า และรายงานสรุปผลการจัดกิจกรรมฯ <u>ตามข้อ 4.37 – 4.38</u> 2. รายงานผลการดำเนินงานด้านบริหารจัดการของรางวัล และสิทธิพิเศษ <u>ตามข้อ 4.31, 4.32 และ 4.34</u>	ภายใน 540 วันนับถัดจากวันที่ลงนามสัญญา
7	ร้อยละ 7 ของมูลค่า ตาสัญญา	1. ดำเนินการจัดกิจกรรมทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้า และรายงานสรุปผลการจัดกิจกรรมฯ <u>ตามข้อ 4.37 – 4.38</u> 2. รายงานผลการดำเนินงานด้านบริหารจัดการของรางวัล และสิทธิพิเศษ <u>ตามข้อ 4.31, 4.32 และ 4.34</u>	ภายใน 630 วันนับถัดจากวันที่ลงนามสัญญา
8	ร้อยละ 10 ของมูลค่า ตาสัญญา	1. ต่ออายุบัญชีการใช้งาน LINE OA <u>ตามข้อ 4.4</u> 2. จัดทำแผน และส่งมอบแผนการดำเนินงานด้านวางแผนกลยุทธ์ทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้า (สำหรับปีที่ 3) <u>ตามข้อ 4.1 – 4.3</u> 3. รายงานผลการดำเนินงานด้านบริหารจัดการของรางวัล และสิทธิพิเศษ <u>ตามข้อ 4.30 – 4.32</u>	ภายใน 720 วันนับถัดจากวันที่ลงนามสัญญา

  นิตยา   /งวดงาน...

งวดงาน	จำนวนเงิน	รายละเอียดการส่งมอบงาน	กำหนดวันส่งมอบ
		4. ดำเนินการจัดกิจกรรมทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้า และรายงานสรุปผลการจัดกิจกรรมฯ ตามข้อ 4.37 – 4.38	
9	ร้อยละ 7 ของมูลค่า ตาสัญญา	1. ดำเนินการจัดกิจกรรมทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้า และรายงานสรุปผลการจัดกิจกรรมฯ ตามข้อ 4.37 – 4.38 2. รายงานผลการดำเนินงานด้านบริหารจัดการของรางวัลและสิทธิพิเศษ ตามข้อ 4.31, 4.32 และ 4.34	ภายใน 810 วันนับถัดจากวันที่ลงนามสัญญา
10	ร้อยละ 7 ของมูลค่า ตาสัญญา	1. ดำเนินการจัดกิจกรรมทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้า และรายงานสรุปผลการจัดกิจกรรมฯ ตามข้อ 4.37 – 4.38 2. รายงานผลการดำเนินงานด้านบริหารจัดการของรางวัลและสิทธิพิเศษ ตามข้อ 4.31, 4.32 และ 4.34	ภายใน 900 วันนับถัดจากวันที่ลงนามสัญญา
11	ร้อยละ 7 ของมูลค่า ตาสัญญา	1. ดำเนินการจัดกิจกรรมทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้า และรายงานสรุปผลการจัดกิจกรรมฯ ตามข้อ 4.37 – 4.38 2. รายงานผลการดำเนินงานด้านบริหารจัดการของรางวัลและสิทธิพิเศษ ตามข้อ 4.31, 4.32 และ 4.34	ภายใน 990 วันนับถัดจากวันที่ลงนามสัญญา
12	ร้อยละ 9 ของมูลค่า ตาสัญญา	1. นำส่งข้อมูลทั้งหมดที่อยู่ในการบริหารความสัมพันธ์ลูกค้าฯ ให้กับ รพม. ตามข้อ 4.25 2. ทำลายข้อมูลทดสอบ หรือข้อมูลอื่น ๆ ของ รพม. ตามข้อ 4.26 3. ดำเนินการจัดกิจกรรมทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้า และรายงานสรุปผลการจัดกิจกรรมฯ ตามข้อ 4.37 – 4.38 4. รายงานผลการดำเนินงานด้านบริหารจัดการของรางวัลและสิทธิพิเศษ ตามข้อ 4.31, 4.32 และ 4.34	ภายใน 1,100 วันนับถัดจากวันที่ลงนามสัญญา

  นิตยา คุ้มศรี 

9. อัตราค่าปรับ

ในกรณีที่ผู้รับจ้างไม่สามารถส่งมอบงานตามรายงวดให้แก่ รพม. ได้ภายในระยะเวลาที่กำหนดตามข้อที่ 8 ผู้รับจ้างจะต้องชำระค่าปรับให้แก่ รพม. ดังนี้

9.1 กรณีเกิดการชำรุดบกพร่องของระบบหรือขัดข้องอันเนื่องมาจากการใช้งานตามปกติ ตามข้อ 4.27 ผู้รับจ้างจะต้องดำเนินการแก้ไขให้แล้วเสร็จภายใน 1 วัน นับตั้งแต่วันที่ได้รับความแจ้งจาก รพม. โดยไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้น หากผู้รับจ้างแก้ไขไม่แล้วเสร็จภายในกำหนดเวลาดังกล่าว ผู้รับจ้างยินยอมให้ รพม. ปรับเป็นรายชั่วโมง ในอัตราร้อยละ 0.01 (ศูนย์จุดศูนย์หนึ่ง) ของมูลค่าร้อยละค่าจ้างงวดงานนั้น ๆ (รวมภาษีมูลค่าเพิ่ม) แต่จะต้องไม่ต่ำกว่าชั่วโมงละ 100.00 บาท (หนึ่งร้อยบาท) โดยเศษของชั่วโมงให้คิดเป็น 1 ชั่วโมง นับตั้งแต่พ้นกำหนดเวลา 1 วันดังกล่าว จนกว่าผู้รับจ้างจะแก้ไขให้ระบบสามารถใช้งานได้ตามปกติ โดยผู้รับจ้างยินยอมให้ รพม. หักค่าปรับดังกล่าวออกจากค่าจ้างตามงวดงานได้ทันที

9.2 ผู้รับจ้างยินยอมให้ รพม. ปรับตามจำนวนร้านค้าหรือแบรนด์ที่ขาดหายไปจากเป้าหมายขั้นต่ำตามข้อ 4.31 โดยคิดค่าปรับเป็นรายร้านค้า/แบรนด์ ในอัตราร้อยละ 0.01 (ศูนย์จุดศูนย์หนึ่ง) ของมูลค่าค่าจ้างในงวดงานที่ 5, งวดงานที่ 9 และงวดงานที่ 12 (รวมภาษีมูลค่าเพิ่ม) แต่จะต้องไม่ต่ำกว่าร้านค้า/แบรนด์ละ 100.00 บาท (หนึ่งร้อยบาท) โดยพิจารณาจากจำนวนร้านค้า/แบรนด์ที่ขาดหายไป ณ วันส่งมอบงานในงวดนั้น ๆ

9.3 กรณีผู้รับจ้างไม่สามารถดำเนินการแก้ไขปัญหาของผู้ใช้งานตามข้อ 4.39 (1) ผู้รับจ้างยินยอมให้ รพม. ปรับเป็นรายชั่วโมง ในอัตราร้อยละ 0.01 (ศูนย์จุดศูนย์หนึ่ง) ของมูลค่าร้อยละค่าจ้างงวดงานนั้น ๆ (รวมภาษีมูลค่าเพิ่ม) แต่จะต้องไม่ต่ำกว่าชั่วโมงละ 100.00 บาท (หนึ่งร้อยบาท) โดยเศษของชั่วโมงให้คิดเป็น 1 ชั่วโมง นับตั้งแต่วันที่พ้นกำหนดระยะเวลาดังกล่าว จนกว่าผู้รับจ้างจะดำเนินการแก้ไขให้แล้วเสร็จและใช้งานได้ตามปกติ โดยผู้รับจ้างยินยอมให้ รพม. หักค่าปรับดังกล่าวออกจากค่าจ้างตามงวดงานได้ทันที

9.4 กรณีผู้รับจ้างไม่สามารถจัดหาจำนวนผู้ติดตาม (Follower) ได้ครบถ้วนตามเป้าหมายขั้นต่ำที่กำหนดไว้ตามข้อ 4.37 ผู้รับจ้างยินยอมให้ รพม. ปรับตามจำนวนผู้ติดตามที่ขาดหายไป โดยคิดค่าปรับเป็นรายบุคคลต่อ 1 ผู้ติดตามที่ขาดหายไป ในอัตราร้อยละ 0.01 (ศูนย์จุดศูนย์หนึ่ง) ของมูลค่าร้อยละค่าจ้างงวดงานนั้น ๆ (รวมภาษีมูลค่าเพิ่ม) แต่จะต้องไม่ต่ำกว่ารายละ 100.00 บาท (หนึ่งร้อยบาท) โดยพิจารณาจากจำนวนผู้ติดตามที่ขาดหายไป ณ วันส่งมอบงานงวดนั้น ๆ หรือวันที่กำหนดแล้วเสร็จตามสัญญา

9.5 ในกรณีที่ผู้รับจ้างไม่สามารถส่งมอบงานรายงวดให้แก่ รพม. ได้ภายในระยะเวลาที่กำหนดในข้อ 8 ผู้รับจ้างต้องยินยอมให้ รพม. ปรับเป็นรายวันในอัตราร้อยละ 0.01 (ศูนย์จุดศูนย์หนึ่ง) ของวงเงินค่าจ้างตามรายงวดที่ได้ส่งมอบงานล่าช้าในงวดนั้น ๆ นับถัดจากวันที่กำหนดแล้วเสร็จตามสัญญา หรือวันที่ครบกำหนดระยะเวลาที่ รพม. ได้มีการขยายให้ ในกรณีที่งานแล้วเสร็จล่าช้าเกิดขึ้นเนื่องจาก รพม. หรือบุคคลที่ 3 หรือเหตุสุดวิสัย ซึ่งผู้รับจ้างมีสิทธิ์ที่จะได้รับการขยายระยะเวลาของสัญญาออกไปเท่ากับเวลาที่เสียไปเนื่องจากเหตุดังกล่าวข้างต้น จนถึงวันที่ผู้รับจ้างได้ส่งมอบงานถูกต้องครบถ้วนเป็นที่เรียบร้อยแล้ว ทั้งนี้ ผู้รับจ้างไม่มีสิทธิ์เรียกร้องเงินค่าใช้จายใด ๆ เพิ่มเติมจาก รพม.



10. เงื่อนไขอื่น ๆ

10.1 ผู้รับจ้างจะต้องจัดให้มีการประชุมการเริ่มงาน (Kick Off Meeting) เพื่อชี้แจงรายละเอียดแผนการดำเนินงานในระดับเดือนโดยระบุกิจกรรม ให้แก่ รฟม. ภายใน 7 วันนับถัดจากวันที่ลงนามในสัญญา และต้องจัดส่งรายงานการประชุมการเริ่มงาน (Kick Off Meeting) ให้แก่ รฟม. พิจารณาภายใน 15 วัน นับถัดจากวันที่ลงนามในสัญญา

10.2 ผู้รับจ้างจะต้องเป็นผู้จัดทำสื่อประชาสัมพันธ์ และดำเนินการเผยแพร่สื่อประชาสัมพันธ์ ตลอดระยะเวลาการดำเนินงานตามสัญญาจ้าง โดยมีรายละเอียดการดำเนินงาน ดังนี้

รูปแบบชิ้นงาน: สื่อประชาสัมพันธ์ที่ต้องดำเนินการ ประกอบด้วย

(1) การออกแบบและผลิตสื่อประชาสัมพันธ์ในรูปแบบ Rich Message, Rich Menu, Infographic หรืออื่นๆ ที่เกี่ยวข้องกับการดำเนินงาน ทั้งแบบภาพนิ่ง ภาพเคลื่อนไหว ต้นแบบ (Key Visual) พร้อมปรับขนาดชิ้นงานให้มีความเหมาะสมกับสื่อโฆษณาแต่ละประเภท

(2) ชิ้นงานสื่อโฆษณาประชาสัมพันธ์รูปแบบอื่น ๆ ที่สอดคล้องกับงานจ้างฯ (ถ้ามี)

การเผยแพร่: เผยแพร่ผ่านช่องทางออนไลน์อย่างน้อย 2 ช่องทาง (LINE Official Account: @MRTA และ Facebook ของ รฟม. หรือตามที่ รฟม. เห็นสมควร) ให้สอดคล้องกับจำนวนกิจกรรมทางการตลาดด้านการบริหารจัดการความสัมพันธ์ของลูกค้า โดยผู้รับจ้างจะต้องเป็นผู้จัดหาและดำเนินการ โดยจะต้องได้รับความเห็นชอบจาก รฟม. ก่อนเผยแพร่

10.3 ผู้รับจ้างจะต้องจัดอบรมหรือการสัมมนาให้แก่พนักงานของ รฟม. ที่เกี่ยวข้อง จำนวนไม่น้อยกว่า 5 คน เพื่อเป็นการพัฒนาทักษะ และศักยภาพด้านการบริหารลูกค้าสัมพันธ์ และด้านเทคโนโลยี หรือหัวข้ออื่น ๆ ที่เกี่ยวข้องกับการดำเนินงาน จำนวนไม่น้อยกว่า 2 ครั้ง ตลอดระยะเวลาการดำเนินงานตามสัญญาจ้าง หรือตามที่ รฟม. เห็นสมควร ทั้งนี้ ผู้รับจ้างต้องนำเสนอรายละเอียด รูปแบบ และแผนการจัดการฝึกอบรมดังกล่าว ให้ รฟม. เห็นชอบก่อนเริ่มดำเนินการ

10.4 ผู้รับจ้างจะต้องจัดหาอุปกรณ์อิเล็กทรอนิกส์เคลื่อนที่ Tablet ที่รองรับระบบปฏิบัติการ iOS และ Android ที่เป็นปัจจุบัน เป็นอย่างน้อย ไม่น้อยกว่า จำนวน 3 เครื่อง/ชุด หรือที่เหมาะสมตลอดระยะเวลาการดำเนินงานตามสัญญาจ้าง โดยมีความจุจัดเก็บ 256 GB ขึ้นไป พร้อมทั้งติดตั้งแอปพลิเคชัน หรือระบบที่พร้อมสำหรับการใช้งานด้านการบริหารความสัมพันธ์ลูกค้าผ่านทาง LINE Official Account: @MRTA หรืออื่น ๆ ที่เกี่ยวข้อง รวมทั้งอุปกรณ์เสริม (สายเคเบิลสำหรับชาร์จ" (Charging Cable) ให้กับคณะกรรมการตรวจรับพัสดุ และเจ้าหน้าที่ผู้ที่มีหน้าที่รับผิดชอบงานจ้างฯ ตลอดระยะเวลาการดำเนินงานตามสัญญา

10.5 ผู้รับจ้างจะต้องจัดให้มีเจ้าหน้าที่ที่มีประสบการณ์ดูแลด้านการบริหารจัดการความสัมพันธ์ และงานอื่น ๆ ที่เกี่ยวข้องกับการดำเนินงานตลอดระยะเวลาการดำเนินงานตามสัญญาจ้าง รฟม. และจะต้องจัดให้มีเจ้าหน้าที่เพื่อประสานงานกับ รฟม. (ทีมงานกองการตลาดและลูกค้าสัมพันธ์ฝ่ายพัฒนาธุรกิจ รฟม.) รวมทั้งช่องทางการติดต่อประสานงาน ในการประชุมวางแผนและแก้ไขปัญหาหารือร่วมกันทุกขั้นตอนเกี่ยวกับการดำเนินงาน และประเด็นสำคัญต่าง ๆ รวมทั้งวางแผนการจัดการความเสี่ยงต่าง ๆ วิธีการแก้ไขปัญหาที่อาจเกิดขึ้นหรือเกิดขึ้น

 /ระหว่าง...

ระหว่างการค้าบริการทางด้านการบริหารจัดการความสัมพันธ์ในทุกขั้นตอน เพื่อลดปัญหา และ
ช่องว่างระหว่างการทำงาน เพื่อให้งานสามารถดำเนินงานแล้วเสร็จตามกำหนด

10.6 ภาพ เสียง เพลง กราฟฟิก หรืออื่น ๆ ไม่ว่าจะเรียกว่าอย่างไรก็ตาม ที่ใช้ประกอบการผลิตและ
เผยแพร่งานที่เกี่ยวข้องทั้งหมดภายใต้งานจ้างในครั้งนี้ จะต้องไม่ละเมิดลิขสิทธิ์ใด ๆ ทั้งสิ้น หากมีการร้องเรียนหรือ
ฟ้องร้อง ผู้รับจ้างจะต้องเป็นผู้รับผิดชอบทั้งหมดโดยจะเรียกร้องค่าเสียหายจาก รฟม. ไม่ได้

10.7 ในกรณีที่มีการจำหน่าย จ่าย โอน หรือมอบสิทธิ์ใด ๆ ให้แก่บุคคลภายนอกไปยังต่างประเทศ
ผู้รับจ้างจะต้องได้รับความยินยอมเป็นลายลักษณ์อักษร และตกลงรายละเอียดร่วมกับ รฟม. อีกครั้งหนึ่งก่อน
ดำเนินการ

10.8 หาก รฟม. มีการพัฒนาแอปพลิเคชัน MRTA Connect , MRTA Parking หรืออื่น ๆ ที่เกี่ยวข้อง
และมีความจำเป็นจะต้องใช้งานข้อมูลที่เกี่ยวข้องกับการบริหารจัดการความสัมพันธ์ลูกค้าผ่านทาง LINE Official
Account: @MRTA และหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) ผู้รับจ้างจะต้องอำนวยความสะดวก
และดำเนินการในส่วนที่เกี่ยวข้องเพื่อให้สามารถจัดส่ง เคลื่อนย้าย และใช้งานร่วมกันได้อย่างมีประสิทธิภาพ
โดยไม่มีค่าใช้จ่ายในการดำเนินงานใด ๆ เพิ่มเติม

10.9 ในกรณีที่ต้องใช้สถานที่เพื่อจัดกิจกรรมทางการตลาดด้านการบริหารจัดการความสัมพันธ์ ซึ่งพื้นที่
ดังกล่าวไม่ใช่กรรมสิทธิ์ของ รฟม. ผู้รับจ้างจะต้องเป็นผู้ติดต่อประสานงานกับเจ้าของสถานที่ซึ่งเป็นหน่วยงาน
ภายนอกหรือบุคคลที่สาม โดยจะต้องปฏิบัติตามขั้นตอนและกฎระเบียบของการใช้สถานที่ รวมถึงมาตรฐานความ
ปลอดภัยอย่างเคร่งครัด รวมทั้งใช้ความระมัดระวังไม่ก่อให้เกิดปัญหาใด ๆ ที่อาจส่งผลกระทบต่อการจัดกิจกรรมฯ
และผลกระทบในทางลบต่อภาพลักษณ์ของ รฟม. ทั้งนี้ หากมีการร้องเรียนมายัง รฟม. ผู้รับจ้างจะต้องเป็น
ผู้รับผิดชอบตอบข้อร้องเรียนในนามของผู้รับจ้าง โดย รฟม. ไม่มีส่วนเกี่ยวข้องกับเรื่องดังกล่าวแต่อย่างใด
และกรณีที่เกิดความเสียหายผู้รับจ้างจะต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว ทั้งนี้ ผู้รับจ้างจะต้องเป็นผู้รับผิดชอบ
ค่าใช้จ่ายสำหรับการใช้สถานที่หรืออื่นใดที่เกี่ยวข้องทั้งหมด

10.10 ในกรณีที่ขอใช้สถานที่ของ รฟม. เพื่อจัดกิจกรรมทางการตลาดด้านการบริหารจัดการ
ความสัมพันธ์ ผู้รับจ้างจะต้องปฏิบัติตามกฎระเบียบของการใช้สถานที่ รวมถึงมาตรฐานความปลอดภัยอย่าง
เคร่งครัด โดยเฉพาะสถานที่ภายในบริเวณสถานีรถไฟฟ้าและภายในขบวนรถไฟฟ้า โดยผู้รับจ้างต้องใช้ความ
ระมัดระวังไม่ก่อให้เกิดปัญหาใด ๆ ที่อาจส่งผลกระทบต่อการจัดกิจกรรมทางการตลาดด้านการบริหารจัดการ
ความสัมพันธ์และผลกระทบในทางลบต่อภาพลักษณ์ของ รฟม. และหากมีการร้องเรียนหรือเกิดปัญหาที่เกี่ยวข้อง
กับการจัดกิจกรรมฯ ผู้รับจ้างจะต้องรับผิดชอบดำเนินการแก้ไขปัญหาโดยทันที และกรณีมีความเสียหายเกิดขึ้นผู้รับจ้าง
จะต้องเป็นผู้รับผิดชอบค่าใช้จ่ายที่เกิดขึ้นทั้งหมด ทั้งนี้ ผู้รับจ้างจะต้องขออนุญาตการใช้สถานที่จาก รฟม.
ก่อนดำเนินการ และ รฟม. จะสนับสนุนการใช้สถานที่โดยไม่มีค่าใช้จ่ายแต่อย่างใด



10.11 ในการส่งมอบงาน ผู้รับจ้างจะต้องจัดทำรายงานผลการดำเนินงานของทางตลาดด้านการบริหารจัดการความสัมพันธ์ และ/หรือการปฏิบัติงานอื่น ๆ ที่มีการดำเนินงานแล้วเสร็จทั้งหมด ของแต่ละงวดงาน พร้อมรายงานประเมินผลการดำเนินงาน เป็นรูปเล่มอย่างน้อย 1 ชุด พร้อมไฟล์อิเล็กทรอนิกส์รายงาน ข้อมูลดิบ และเอกสารที่เกี่ยวข้องกับการดำเนินงานทั้งหมดบรรจุใน USB Flash Drive หรือ External Hard Disk ตามความเหมาะสม ให้แก่ รพม. ภายในระยะเวลาที่กำหนดในแต่ละงวดงานตามข้อ 8

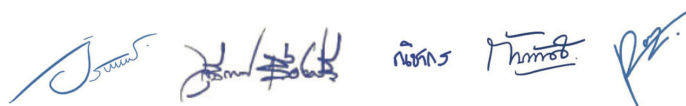
10.12 ผู้รับจ้างต้องศึกษาทำความเข้าใจและปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA: Personal Data Protection Act) รวมไปถึงกฎหมายที่เกี่ยวข้องตลอดระยะเวลาการดำเนินงานตามสัญญาจ้าง หากผู้รับจ้างไม่ปฏิบัติตามนโยบายดังกล่าว จนก่อให้เกิดความเสียหาย ผู้รับจ้างจะต้องเป็นผู้รับผิดชอบค่าเสียหายดังกล่าว

10.13 ผู้รับจ้างจะต้องปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2568 ของ รพม. ตามภาคผนวก ก หากผู้รับจ้างไม่ปฏิบัติตามนโยบายดังกล่าว จนก่อให้เกิดความเสียหายผู้รับจ้างจะต้องเป็นผู้รับผิดชอบค่าเสียหายดังกล่าว

10.14 ผู้รับจ้างต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รพม. และมาตรฐานที่เป็นที่ยอมรับตลอดระยะเวลาการดำเนินงานตามสัญญาจ้าง ตามภาคผนวก ข หากผู้รับจ้างไม่ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยฯ จนก่อให้เกิดความเสียหาย ผู้รับจ้างจะต้องเป็นผู้รับผิดชอบค่าเสียหายดังกล่าวโดยจะต้องเป็นผู้รับผิดชอบสูงสุดตามที่กฎหมายกำหนดทุกกรณี

10.15 ผู้ปฏิบัติงานของผู้รับจ้างทุกคนต้องลงนามในสัญญาว่าจะไม่เปิดเผยความลับของ รพม. (Non-Disclosure Agreement: NDA) ก่อนเริ่มปฏิบัติงานให้ รพม. ตามภาคผนวก ค

10.16 หากผู้รับจ้างกระทำการใด ๆ ที่ฝ่าฝืนเงื่อนไขและข้อกำหนด (TOR) งานจ้างบริหารจัดการความสัมพันธ์ของลูกค้า (Customer Relationship Management: CRM) ของ รพม. จนเป็นเหตุให้ รพม. และบุคคลภายนอกเสียหาย ตลอดจนพันธมิตรที่เกี่ยวข้องกับ รพม. จนเกิดการโดนฟ้องร้อง ผู้รับจ้างจะต้องเป็นผู้รับผิดชอบในการดำเนินการทางคดี และชดใช้ค่าเสียหายที่เกิดขึ้นเองทั้งหมด



11. หลักฐานการยื่นข้อเสนอ

ผู้ยื่นข้อเสนอจะต้องยื่นเอกสารหลักฐานพร้อมกับรับรองสำเนาถูกต้องมาพร้อมกับเสนอราคา พร้อมจัดส่งเอกสารหลักฐานด้านเทคนิคตามข้อ 6 ผ่านทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (e-GP) ดังนี้

11.1 สำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล

11.2 สำเนาหนังสือบริษัทนิติ

11.3 บัญชีรายชื่อกรรมการผู้จัดการ

11.4 บัญชีผู้ถือหุ้นรายใหญ่ (ถ้ามี)

11.5 ผู้มีอำนาจควบคุม (ถ้ามี)

11.6 หนังสือมอบอำนาจ (ถ้ามี)

11.7 สำเนาสัญญาหรือสำเนาใบสั่งซื้อสั่งจ้าง ที่มีลักษณะเดียวกันกับงานจ้างในครั้งนี้

11.8 สำเนาหนังสือรับรองผลงาน

11.9 ในกรณีผู้ยื่นข้อเสนอเป็นผู้ยื่นข้อเสนอร่วมกันในฐานะเป็นผู้ร่วมค้า ให้ยื่นสำเนาสัญญาของการเข้าร่วมค้า และเอกสารตามข้อ 3 ของผู้ร่วมค้า

11.10 สำเนาใบสำคัญแสดงการจดทะเบียนห้างหุ้นส่วนบริษัท

11.11 สำเนาใบทะเบียนภาษีมูลค่าเพิ่ม (ภ.พ.20) (ถ้ามี)

11.12 เอกสารประกอบการพิจารณาคัดเลือกข้อเสนอ ดังนี้

11.12.1 แผนกลยุทธ์การบริหารจัดการความสัมพันธ์ของลูกค้า (Customer Relationship Management: CRM) ผ่านทาง Line Official Account: @MRTA และหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program)

11.12.2 แผนการบริหารจัดการของรางวัล ที่นำเสนอให้กับลูกค้าในการแลกรับสิทธิในหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program)

11.13 ชื่อ-นามสกุล หมายเลขโทรศัพท์ และอีเมล ผู้ประสานงานของผู้ยื่นข้อเสนอ จำนวน 1 – 2 คน เพื่อให้ รฟม. สามารถติดต่อประสานงานได้

Handwritten signatures and stamps at the bottom of the page. From left to right: a signature, a stamp with the name 'สมชาย ใจดี', the word 'กิตติกร', a stamp with the name 'กิตติกร', and a signature.

หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

งานจ้างบริหารจัดการความสัมพันธ์ของลูกค้า (Customer Relationship Management: CRM)

ในการพิจารณาผู้ชนะการเสนอราคา รฟม. จะพิจารณาตัดสินโดยใช้หลักเกณฑ์ราคาประกอบเกณฑ์อื่น (Price Performance) โดยมีรายละเอียด ดังนี้

1. ราคาที่ยื่นข้อเสนอ (Price) กำหนดน้ำหนักเท่ากับร้อยละ 30 (100 คะแนน)

หลักเกณฑ์การให้คะแนนราคาที่ยื่นข้อเสนอ (Price) เป็นไปตามการคำนวณของระบบจัดซื้อจัดจ้างภาครัฐ ด้วยอิเล็กทรอนิกส์ e-GP ของกรมบัญชีกลาง

2. การพิจารณาเกณฑ์ด้านคุณภาพ กำหนดน้ำหนักเท่ากับร้อยละ 70 (100 คะแนน)

รายละเอียดหลักเกณฑ์การให้คะแนนเกณฑ์ด้านคุณภาพ ประกอบด้วยหัวข้อ ดังนี้

ลำดับที่	รายการ	คะแนนรวม
1.	ผลงานและประสบการณ์ของผู้ยื่นข้อเสนอ	10
2.	การนำเสนอแผนกลยุทธ์การบริหารจัดการความสัมพันธ์ของลูกค้า Customer Relationship Management: CRM) ผ่านทาง LINE Official Account: @MRTA และหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) 2.1 นำเสนอแผนให้สอดคล้องกับกลุ่มเป้าหมายของ รฟม. ในการยกระดับประสบการณ์ของลูกค้า (20 คะแนน) 2.2 แนวทางการสร้างโอกาสทางธุรกิจ ส่งเสริมการเพิ่มรายได้ เพิ่มจำนวนลูกค้าใหม่ เพิ่มจำนวนผู้ใช้บริการรถไฟฟ้า และเกิดการร่วมมือกับพันธมิตร (20 คะแนน) 2.3 ออกแบบฟังก์ชัน และการดูแลบริหารจัดการความสัมพันธ์ของลูกค้า (Customer Relationship Management: CRM) ผ่านทาง LINE Official Account: @MRTA และหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) ที่รองรับใช้งานอย่างต่อเนื่อง ตลอดอายุสัญญาของงานจ้าง (20 คะแนน)	60
3.	การนำเสนอแผนการบริหารจัดการของรางวัล ที่นำเสนอให้กับลูกค้าในการแลกรับสิทธิในหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program)	20
4.	เข้าร่วมนำเสนอกลยุทธ์และแผนการดำเนินงาน รวมถึงประเภทของรางวัล	10
	รวม	100

  นิตยา  

/ผู้เสนอราคา...

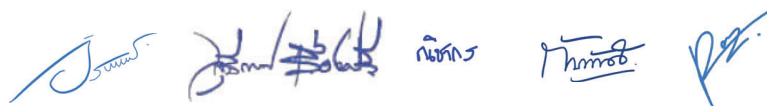
ผู้เสนอราคาจะต้องนำเสนอกลยุทธ์และแผนการดำเนินงาน รวมถึงประเภทของรางวัล ต่อคณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์ เพื่อให้คณะกรรมการฯ พิจารณา ภายใน 5 วันทำการ นับถัดจากวันที่ยื่นข้อเสนอ โดย รพม. จะนัดหมายวันและเวลากับผู้ยื่นข้อเสนอเพื่อเข้ามานำเสนอผลงาน ณ การรถไฟฯขนส่งมวลชนแห่งประเทศไทย (สำนักงานใหญ่) ถนนพระราม 9 เขตห้วยขวาง กรุงเทพฯ โดยต้องนำเสนอในรูปแบบ Presentation ภายในระยะเวลา 1 ชั่วโมง และเตรียมเอกสารสำหรับการนำเสนอตามจำนวนคณะกรรมการฯ เพื่อประกอบการพิจารณา ทั้งนี้ มีรายละเอียดการพิจารณาแต่ละหัวข้อ ดังนี้

1) ผลงานและประสบการณ์ (10 คะแนน)

รพม. จะพิจารณาให้คะแนนจากจำนวนของสัญญาที่มีลักษณะเดียวกันกับงานจ้างในครั้งนี้ ซึ่งเกี่ยวข้องกับการบริหารจัดการความสัมพันธ์ของลูกค้า (Customer Relationship Management: CRM) ผ่านแพลตฟอร์มดิจิทัล Digital Platform ที่ดำเนินการแล้วเสร็จภายในระยะเวลาไม่เกิน 3 ปี นับถึงวันที่ยื่นข้อเสนอและจะต้องมีวงเงินของสัญญาไม่น้อยกว่า 2,000,000 บาท (สองล้านบาทถ้วน) โดยผู้ยื่นข้อเสนอจะต้องมีสำเนาสัญญาหรือใบสั่งซื้อสั่งจ้างที่แสดงถึงขอบเขตและมูลค่าของงานจ้างนั้น ๆ ซึ่งเป็นคู่สัญญาโดยตรงกับหน่วยงานของรัฐหรือเอกชนที่ รพม. เชื่อถือ และหนังสือรับรองผลงาน (ถ้ามี) โดยมีหลักเกณฑ์ในการพิจารณา ดังนี้

รายละเอียด	คะแนน
นำเสนอผลงานที่เกี่ยวข้องกับการบริหารจัดการความสัมพันธ์ของลูกค้า มากกว่า 5 ผลงาน	10
นำเสนอผลงานที่เกี่ยวข้องกับการบริหารจัดการความสัมพันธ์ของลูกค้า ตั้งแต่ 3 - 4 ผลงาน	7
นำเสนอผลงานที่เกี่ยวข้อง น้อยกว่า 3 ผลงาน หรือไม่มีการนำเสนอผลงานการบริหารจัดการความสัมพันธ์ของลูกค้า	0

* รพม. ขอสงวนสิทธิ์ผลการตัดสินของคณะกรรมการถือเป็นที่สุด

 นิตกร

2) การนำเสนอแผนกลยุทธ์การบริหารจัดการความสัมพันธ์ของลูกค้า (Customer Relationship Management: CRM) ผ่านทาง Line Official Account: @MRTA และหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) (60 คะแนน)

2.1 นำเสนอแผนให้สอดคล้องกับกลุ่มเป้าหมายของ รฟม. ในการยกระดับประสบการณ์ของลูกค้า (20 คะแนน)

รฟม. จะพิจารณาจากการนำเสนอแผนการบริหารจัดการความสัมพันธ์ของลูกค้า กับกลุ่มเป้าหมายของ รฟม. ในการยกระดับประสบการณ์ของลูกค้า โดยให้สอดคล้องกับขอบเขตของงาน ระยะเวลาของกิจกรรม และวิธีการจัดการบริหารการดำเนินงานและข้อมูลอื่น ๆ ที่เกี่ยวข้องได้อย่างครบถ้วน ถูกต้อง เหมาะสม โดยมีคำอธิบายหลักเกณฑ์การให้คะแนน ดังนี้

รายละเอียด	คะแนน
- มีการนำเสนอกรอบแนวคิด/กลยุทธ์/แผนงานในการดำเนินงานด้านการบริหารจัดการความสัมพันธ์ของลูกค้า ที่สอดคล้องและมากกว่าที่ขอบเขตงานกำหนด เช่น แสดงรายละเอียดระยะเวลาที่ใช้ในขั้นตอนต่าง ๆ ของงานจ้างอย่างละเอียด ครบถ้วน เป็นต้น และสามารถวัดผลการดำเนินงานได้อย่างชัดเจน เป็นรูปธรรม รวมทั้งแสดงให้เห็นถึงความเข้าใจในการดำเนินงานได้อย่างครบถ้วนสมบูรณ์ - มีความคิดสร้างสรรค์ดีมาก โดดเด่น ทันสมัย และน่าสนใจ - มีแผนบริหารความเสี่ยง/สถานการณ์ฉุกเฉิน	20
- มีการนำเสนอกรอบแนวคิด/กลยุทธ์/แผนงานในการดำเนินงานด้านการบริหารจัดการความสัมพันธ์ของลูกค้า ที่สอดคล้องกับขอบเขตงานที่กำหนด เช่น แสดงรายละเอียดระยะเวลาที่ใช้ในขั้นตอนต่าง ๆ ของงานจ้าง เป็นต้น และสามารถวัดผลการดำเนินงานได้อย่างเป็นรูปธรรม และแสดงให้เห็นถึงความเข้าใจในการดำเนินงาน - มีความคิดสร้างสรรค์ - มีแผนบริหารความเสี่ยง/สถานการณ์ฉุกเฉิน	15
- มีการนำเสนอกรอบแนวคิด/กลยุทธ์/แผนงานในการดำเนินงานด้านการบริหารจัดการความสัมพันธ์ของลูกค้า แต่แสดงรายละเอียดไม่ครบถ้วนตามขอบเขตของงานที่กำหนด - มีความคิดสร้างสรรค์	5
- ไม่มีการนำเสนอกรอบแนวคิด/กลยุทธ์/แผนงานในการดำเนินงานด้านการบริหารจัดการความสัมพันธ์ของลูกค้า	0

* รฟม. ขอสงวนสิทธิ์ผลการตัดสินของคณะกรรมการถือเป็นที่สุด

 นิตกร

/2.2 แนวทาง...

2.2 แนวทางการสร้างโอกาสทางธุรกิจ ส่งเสริมการเพิ่มรายได้ เพิ่มจำนวนลูกค้าใหม่ เพิ่มจำนวนผู้ใช้บริการรถไฟฟ้า และเกิดการร่วมมือกับพันธมิตร (20 คะแนน)

รฟม. จะพิจารณาจากการนำเสนอกลยุทธ์และแผนการสร้างโอกาสทางธุรกิจฯ กับกลุ่มเป้าหมายของ รฟม. ในการยกระดับประสิทธิภาพของลูกค้าย โดยประเมินจากความเป็นไปได้ของแผนงาน ตัวชี้วัดความสำเร็จที่ชัดเจน และความพร้อมของเครือข่ายพันธมิตร ให้สอดคล้องกับขอบเขตของงาน ระยะเวลาของกิจกรรม และวิธีการจัดการบริหาร การดำเนินงาน รวมถึงการนำเสนอข้อมูลวิเคราะห์เพื่อเพิ่มประสิทธิภาพการทำการตลาด ได้อย่างครบถ้วน ถูกต้อง เหมาะสม โดยมีคำอธิบายหลักเกณฑ์การให้คะแนน ดังนี้

รายละเอียด	คะแนน
- มีการนำเสนอกลยุทธ์และแผนการสร้างโอกาสทางธุรกิจ (ในการเพิ่มรายได้ เพิ่มจำนวนลูกค้า เพิ่มจำนวนผู้ใช้บริการรถไฟฟ้า และเกิดการร่วมมือกับพันธมิตร) สอดคล้องและ<u>มากกว่า</u>ที่ขอบเขตงาน กำหนด เช่น แนวทางการสร้างโอกาสทางธุรกิจในการร่วมมือกับกลุ่มแบรนด์สินค้าชั้นนำ หรือร้านอาหาร เป็นต้น และสามารถวัดผลการดำเนินงานได้อย่างชัดเจน เป็น<u>รูปธรรม</u> รวมทั้งแสดงให้เห็นถึงความเข้าใจในการดำเนินงานได้อย่างครบถ้วนสมบูรณ์ - มีแผนบริหารความเสี่ยง/สถานการณ์ฉุกเฉิน	20
- มีการนำเสนอกลยุทธ์และแผนการสร้างโอกาสทางธุรกิจ (ในการเพิ่มรายได้ เพิ่มจำนวนลูกค้า เพิ่มจำนวนผู้ใช้บริการรถไฟฟ้า และเกิดการร่วมมือกับพันธมิตร) <u>สอดคล้อง</u>กับขอบเขตงานที่กำหนด เช่น แนวทางการสร้างโอกาสทางธุรกิจในการร่วมมือกับกลุ่มแบรนด์สินค้าชั้นนำ หรือร้านอาหาร เป็นต้น และสามารถวัดผลการดำเนินงานได้อย่างเป็น<u>รูปธรรม</u> และแสดงให้เห็นถึงความเข้าใจในการดำเนินงาน - มีแผนบริหารความเสี่ยง/สถานการณ์ฉุกเฉิน	15
- มีการนำเสนอกลยุทธ์และแผนการสร้างโอกาสทางธุรกิจ (ในการเพิ่มรายได้ เพิ่มลูกค้า เพิ่มผู้ใช้บริการรถไฟฟ้า และการร่วมมือกับพันธมิตร) <u>ไม่ครบถ้วน</u>ตามขอบเขตงานที่กำหนด	5
- ไม่มีการนำเสนอกลยุทธ์และแผนการสร้างโอกาสทางธุรกิจฯ	0

* รฟม. ขอสงวนสิทธิ์ผลการตัดสินของคณะกรรมการถือเป็นที่สุด

 นิตกร ทัมมธ

2.3 ออกแบบฟังก์ชัน และการดูแลบริหารจัดการความสัมพันธ์ของลูกค้า (Customer Relationship Management: CRM) ผ่านทาง LINE Official Account: @MRTA และหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) ที่รองรับให้สามารถใช้งานอย่างต่อเนื่อง ตลอดอายุสัญญาของงานจ้าง (20 คะแนน)

รฟม. จะพิจารณาจากการนำเสนอรูปแบบการออกแบบฟังก์ชันการดูแลบริหารจัดการความสัมพันธ์ของลูกค้า (Customer Relationship Management: CRM) ผ่านทาง LINE Official Account: @MRTA และหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) โดยประเมินจากความเป็นไปได้ของฟังก์ชันการใช้งานต่าง ๆ ทั้งนี้ ฟังก์ชันและหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) จะต้องสามารถใช้งานได้อย่างเสถียรต่อเนื่อง ใช้งานง่าย และเป็นมิตรต่อผู้ใช้งาน โดยมีคำอธิบายหลักเกณฑ์การให้คะแนน ดังนี้

รายละเอียด	คะแนน
- มีการออกแบบฟังก์ชันต่าง ๆ บนหน้า LINE Official Account: @MRTA และหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) เช่น ฟังก์ชันการค้นหาของรางวัล มินิเกมส์ เป็นต้น โดยให้สอดคล้องและมากกว่าที่ขอบเขตของงานกำหนด และมีแนวทางที่ชัดเจน ใช้งานง่าย - มีความคิดสร้างสรรค์ดีมาก โดดเด่น ทันสมัย และน่าสนใจ - มีแผนบริหารความเสี่ยง/สถานการณ์ฉุกเฉิน	20
- มีการออกแบบฟังก์ชันต่าง ๆ บนหน้า LINE Official Account: @MRTA และหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) ในหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) เช่น ฟังก์ชันการค้นหาของรางวัล มินิเกมส์ เป็นต้น โดยให้สอดคล้องกับขอบเขตของงานที่กำหนด - มีความคิดสร้างสรรค์ - มีแผนบริหารความเสี่ยง/สถานการณ์ฉุกเฉิน	15
- มีการออกแบบฟังก์ชันต่าง ๆ บนหน้า LINE Official Account: @MRTA และหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) ในหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) เช่น ฟังก์ชันการค้นหาของรางวัล มินิเกมส์ เป็นต้น แต่ไม่ครบถ้วนตามขอบเขตของงานที่กำหนด - มีความคิดสร้างสรรค์	5
- ไม่มีการออกแบบฟังก์ชันต่าง ๆ บนหน้า LINE Official Account: @MRTA และหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program)	0

* รฟม. ขอสงวนสิทธิ์ผลการตัดสินของคณะกรรมการถือเป็นที่สุด

/3) การนำเสนอ...

3) การนำเสนอแผนการบริหารจัดการของรางวัล ที่นำเสนอให้กับลูกค้าในการแลกรับสิทธิในหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) (20 คะแนน)

รพม. จะพิจารณาจากการนำเสนอแผนการบริหารจัดการของรางวัล รูปแบบการแลกรับของรางวัล ประเภทของรางวัล (ซึ่งจะต้องมีศักยภาพในการดึงดูดให้ลูกค้าอยากเข้ามาใช้งานและสะสมคะแนนจริง) โดยมุ่งเน้นให้เกิดผลผลิต (Output) และผลลัพธ์ (Outcome) เชิงกลยุทธ์จากการแลกรับของรางวัล เช่น ประเภทของรางวัล ที่กระตุ้นให้เกิดการใช้ผลิตภัณฑ์และบริการของ รพม. เป็นต้น เพื่อให้กับลูกค้าใช้แลกรับสิทธิพิเศษต่าง ๆ บนหน้าต่างสมาชิกสะสมคะแนน (Loyalty Program) โดยมีหลักเกณฑ์การให้คะแนน ดังนี้

รายละเอียด	คะแนน
- แสดงแผนการบริหารจัดการของรางวัล (การจัดทำ จัดหา การสต็อก และการแลกรับ เป็นต้น) สอดคล้องและมากกว่าที่ขอบเขตของงานกำหนด ได้อย่างชัดเจนและเป็นรูปธรรม - นำเสนอประเภทของรางวัล ให้สอดคล้องกับขอบเขตของงานกำหนดมีความโดดเด่น มุ่งเน้นผลผลิต และผลลัพธ์เชิงกลยุทธ์อย่างชัดเจน และสามารถดำเนินงานได้จริง - มีแผนบริหารความเสี่ยง/สถานการณ์ฉุกเฉิน	20
- แสดงแผนการบริหารจัดการของรางวัล (การจัดทำ จัดหา การสต็อก และการแลกรับ เป็นต้น) สอดคล้องกับขอบเขตของงานที่กำหนด - นำเสนอประเภทของรางวัล สอดคล้องกับขอบเขตของงานที่กำหนด และสามารถดำเนินงานได้จริง แต่ยังไม่ได้มุ่งเน้นผลผลิต และผลลัพธ์เชิงกลยุทธ์อย่างชัดเจน - มีแผนบริหารความเสี่ยง/สถานการณ์ฉุกเฉิน	15
- แสดงแผนการบริหารจัดการของรางวัล (การจัดทำ จัดหา การสต็อก และการแลกรับ เป็นต้น) - นำเสนอประเภทของรางวัล แต่ไม่ครบถ้วนตามขอบเขตของงาน เป้าหมายและวัตถุประสงค์ในการดำเนินงาน	5
- ไม่มีการนำเสนอแผนการบริหารจัดการของรางวัล และประเภทของรางวัล	0

* รพม. ขอสงวนสิทธิ์ผลการตัดสินของคณะกรรมการถือเป็นที่สุด

 นิตย ธีมอ. ๒๕

/4) เข้าร่วม...

4) เข้าร่วมนำเสนอกลยุทธ์และแผนการดำเนินงาน รวมถึงประเภทของรางวัล (10 คะแนน)

รฟม. จะพิจารณาจากการที่ผู้ยื่นข้อเสนอเข้าร่วมการนำเสนอกลยุทธ์และแผนการดำเนินงาน รวมถึงประเภทของรางวัล ณ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย (สำนักงานใหญ่) ตามวันและเวลาที่กำหนด โดยจะต้องมีความตรงต่อเวลาและสามารถนำเสนอกลยุทธ์ฯ และข้อมูลต่าง ๆ ตามวัตถุประสงค์ที่ระบุในขอบเขตของงาน ภายในระยะเวลาที่กำหนด พร้อมทั้งแสดงให้เห็นถึงความพร้อมในการนำเสนอ ชี้แจงหรือตอบคำถามจากคณะกรรมการ ได้อย่างถูกต้อง ครบถ้วน โดยมีหลักเกณฑ์การให้คะแนน ดังนี้

รายละเอียด	คะแนน
- ผู้ยื่นข้อเสนอเข้ามานำเสนอกลยุทธ์และแผนการดำเนินงาน รวมถึงประเภทของรางวัล ตรงตามวัน เวลา และสถานที่ที่ รฟม. กำหนด โดยรูปแบบการนำเสนอจะต้องมีความโดดเด่น น่าสนใจ ลำดับเรื่อง อย่างเป็นระบบในการนำเสนอกลยุทธ์ฯ และข้อมูลต่าง ๆ ที่เกี่ยวข้อง ตามวัตถุประสงค์ที่ระบุในขอบเขตของงานภายในระยะเวลาที่กำหนด และมีความตรงต่อเวลา พร้อมทั้งแสดงให้เห็นถึงความพร้อมในการนำเสนอ ชี้แจงหรือตอบคำถามจากคณะกรรมการได้อย่างถูกต้อง ครบถ้วน และประโยชน์ที่ รฟม. จะได้รับนอกเหนือจากขอบเขตของงาน	10
- ผู้ยื่นข้อเสนอเข้ามานำเสนอกลยุทธ์และแผนการดำเนินงาน รวมถึงประเภทของรางวัล ตรงตามวัน เวลาและสถานที่ที่ รฟม. กำหนด และตามวัตถุประสงค์ที่ระบุในขอบเขตของงาน	5
- ไม่มีการเข้ามานำเสนอกลยุทธ์และแผนการดำเนินงาน รวมถึงประเภทของรางวัล	0

* รฟม. ขอสงวนสิทธิ์ผลการตัดสินของคณะกรรมการถือเป็นที่สุด



ภาคผนวก ก



การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

MASS RAPID TRANSIT AUTHORITY OF THAILAND

รัฐวิสาหกิจภายใต้กำกับของรัฐมนตรีว่าการกระทรวงคมนาคม

A STATE ENTERPRISE UNDER SUPERVISION OF MINISTER OF TRANSPORT

ประกาศการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2568

ด้วยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 ประกอบกับข้อ 4 และข้อ 5 ของประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป เพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม

การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย (รฟม.) ตระหนักและให้ความสำคัญในการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความครอบครองหรือควบคุมดูแลของ รฟม. จึงเห็นสมควรปรับปรุงประกาศการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2566 ลงวันที่ 25 ธันวาคม 2566 โดยอาศัยอำนาจตามความในมาตรา 24 วรรคหนึ่ง แห่งพระราชบัญญัติการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย พ.ศ. 2543 ผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย จึงออกประกาศไว้ดังต่อไปนี้

ข้อ 1 ประกาศนี้เรียกว่า “ประกาศการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2568”

ข้อ 2 ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนด 7 วัน นับถัดจากวันที่ประกาศเป็นต้นไป

ข้อ 3 ให้ยกเลิกประกาศการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2566 ลงวันที่ 25 ธันวาคม 2566

ข้อ 4 หลักการสำคัญในการคุ้มครองข้อมูลส่วนบุคคล

รฟม. จะเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล โดยอยู่บนพื้นฐานหลักการสำคัญในการคุ้มครองข้อมูลส่วนบุคคล ดังนี้

/ (1) เก็บรวบรวม ...

(1) เก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลเป็นไปโดยชอบด้วยกฎหมาย เป็นธรรม และมีความโปร่งใส ต่อเจ้าของข้อมูลส่วนบุคคล (Lawfulness, Fairness and Transparency)

(2) เก็บรวบรวมข้อมูลส่วนบุคคลด้วยวิธีการที่ชอบด้วยกฎหมาย และจัดเก็บข้อมูล เท่าที่จำเป็นตามวัตถุประสงค์ในการดำเนินงาน และตามที่กฎหมายกำหนดเท่านั้น (Purpose Limitation) โดยจะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนหรือในขณะที่เก็บรวบรวมข้อมูลส่วนบุคคล เว้นแต่เป็นกรณีที่กฎหมายกำหนดให้สามารถประมวลผลข้อมูลส่วนบุคคลได้โดยไม่ต้องได้รับความยินยอม

(3) เก็บรวบรวมข้อมูลส่วนบุคคลเท่าที่จำเป็นตามวัตถุประสงค์อันชอบด้วยกฎหมาย (Data Minimization)

(4) ทำให้ข้อมูลส่วนบุคคลมีความถูกต้องและเป็นปัจจุบัน พร้อมใช้งาน รวมถึงต้องมีการดำเนินการเพื่อให้แน่ใจว่าข้อมูลส่วนบุคคลที่ไม่ถูกต้องจะได้รับการปรับปรุงแก้ไข (Accuracy)

(5) ประมวลผลข้อมูลส่วนบุคคลตามระยะเวลาเท่าที่จำเป็นต่อการประมวลผล ข้อมูลส่วนบุคคล (Storage Limitation) เว้นแต่กรณีมีกฎหมายกำหนดไว้ต้องจัดเก็บข้อมูลส่วนบุคคลไว้นานกว่าระยะเวลาเท่าที่จำเป็นดังกล่าว

(6) การประมวลผลข้อมูลส่วนบุคคลต้องมีมาตรการในการรักษาความมั่นคงปลอดภัย ที่เหมาะสม รวมถึงมีการป้องกันการประมวลผลข้อมูลส่วนบุคคลโดยไม่มีสิทธิหรือโดยไม่ชอบด้วยกฎหมาย และป้องกันการสูญหายโดยอุบัติเหตุ การถูกทำลาย หรือถูกทำให้เสียหาย (Integrity and Confidentiality)

ข้อ 5 ขอบเขตการบังคับใช้

นโยบายการคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ มีขอบเขตการบังคับใช้ครอบคลุม การประมวลผลข้อมูลส่วนบุคคลที่อยู่ในความครอบครองหรือควบคุมดูแลของ รพม.

สำหรับข้อมูลส่วนบุคคลที่ได้เก็บรวบรวมไว้ก่อนวันที่พระราชบัญญัติคุ้มครอง ข้อมูลส่วนบุคคล พ.ศ. 2562 ใช้บังคับ รพม. จะเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปตามวัตถุประสงค์เดิม

ข้อ 6 หลักการสำคัญในการประมวลผลข้อมูลส่วนบุคคล

รพม. จะประมวลผลข้อมูลส่วนบุคคลโดยปฏิบัติตามหลักการสำคัญในการประมวลผล ข้อมูลส่วนบุคคล ดังนี้

(1) ต้องแจ้งรายละเอียดการประมวลผลข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคล ทราบก่อนหรือในขณะที่เก็บรวบรวมข้อมูลส่วนบุคคล

(2) ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนการประมวลผลข้อมูล ส่วนบุคคล เว้นแต่กรณีดังต่อไปนี้ สามารถประมวลผลข้อมูลส่วนบุคคลได้โดยไม่ต้องได้รับความยินยอม

(ก) เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์ หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัย หรือสถิติ

/(ข) เพื่อ ...



- (ข) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล
 - (ค) เพื่อปฏิบัติตามกฎหมาย
 - (ง) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญา
 - (จ) เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินการกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล
 - (ฉ) เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล หรือบุคคล หรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล
- (3) ไม่เก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหว รวมถึงการเก็บรวบรวมข้อมูลส่วนบุคคลของผู้เยาว์ คนไร้ความสามารถ หรือคนเสมือนไร้ความสามารถ เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลหรือผู้มีอำนาจกระทำแทนเจ้าของข้อมูลส่วนบุคคลโดยชัดแจ้ง หรือได้รับยกเว้นตามที่กฎหมายกำหนด
- (4) ไม่เปิดเผยข้อมูลส่วนบุคคลที่มีการจัดเก็บรวบรวมไว้ให้กับบุคคลอื่น เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูลโดยทำหนังสือให้ความยินยอมเปิดเผยข้อมูลส่วนบุคคลเป็นลายลักษณ์อักษร หรือกรณีตามมาตรา 80 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือตามมาตรา 24 แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

ข้อ 7 บทกำหนดโทษ

ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล หรือผู้มีอำนาจหน้าที่รับผิดชอบในการดำเนินงานเรื่องใดเรื่องหนึ่งตามหน้าที่ของตน หากละเลยหรือละเว้นไม่ปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล อาจมีผลให้ได้รับโทษทางวินัยตามระเบียบของ รฟม. และอาจได้รับโทษที่กำหนดโดยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมทั้งกฎหมายลำดับรอง กฎ ระเบียบ หรือคำสั่งที่เกี่ยวข้อง

ข้อ 8 ช่องทางการติดต่อ

หากเจ้าของข้อมูลส่วนบุคคลมีข้อสงสัย ข้อเสนอแนะ หรือข้อกังวลเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของ รฟม. หรือเกี่ยวกับนโยบายนี้ หรือต้องการใช้สิทธิตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล เจ้าของข้อมูลสามารถติดต่อสอบถามได้ที่

(1) ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย (รฟม.)

175 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310

หมายเลขโทรศัพท์ 0 2716 4000

ช่องทางการติดต่อ saraban@mrt.co.th

/(2) เจ้าหน้าที่ ...



(2) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO)

คณะกรรมการเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

175 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310

หมายเลขโทรศัพท์ 0 2716 4000

ช่องทางการติดต่อ saraban@mrta.co.th

ข้อ 9 แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของ รฟม.

แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของ รฟม. มีรายละเอียดตามเอกสารแนบท้าย

ประกาศ ประกอบด้วย

หมวด 1 แนวปฏิบัติสำหรับผู้ควบคุมข้อมูลส่วนบุคคล

หมวด 2 แนวปฏิบัติสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล

ประกาศ ณ วันที่ 21 กรกฎาคม พ.ศ. 2568



(นายกาฬฉลวย อุดมธรรมภักดี)

ผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย



สารบัญ

เรื่อง	หน้า
คำนิยาม	1
หมวด 1 แนวปฏิบัติสำหรับผู้ควบคุมข้อมูลส่วนบุคคล.....	3
ส่วนที่ 1 ระบบบริหารจัดการด้านการคุ้มครองข้อมูลส่วนบุคคล	3
ส่วนที่ 2 การประมวลผลข้อมูลส่วนบุคคล.....	6
ส่วนที่ 3 มาตรการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคล	13
ส่วนที่ 4 การส่งมอบข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่น และการใช้หรือเปิดเผยข้อมูลส่วนบุคคล ที่ได้รับมอบจากบุคคลหรือนิติบุคคลอื่น.....	16
ส่วนที่ 5 การควบคุมการลบหรือทำลายข้อมูลส่วนบุคคล.....	18
ส่วนที่ 6 การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล	22
หมวด 2 แนวปฏิบัติสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล	23

เอกสารแนบท้ายประกาศ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล
พ.ศ. 2568

แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของ รฟม.

คำนิยาม

คำนิยามที่ใช้ในแนวปฏิบัตินี้ ประกอบด้วย

1. ผู้ควบคุมข้อมูลส่วนบุคคล หมายถึง บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
2. รฟม. หมายถึง การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทยซึ่งมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล
3. ผู้ว่ากรม หมายถึง ผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
4. ผู้บริหาร รฟม. หมายถึง กลุ่มพนักงานบริหารระดับสูง (ระดับ 11 - 14) และกลุ่มพนักงานระดับบังคับบัญชา (ระดับ 8 - 10)
5. เจ้าของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล หมายถึง ฝ่าย/ สำนัก/ สำนักงาน ที่รับผิดชอบในการกำหนดวัตถุประสงค์ และกำหนดรายการข้อมูลส่วนบุคคลที่ต้องเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของกิจกรรมนั้น ๆ ในนามของ รฟม. รวมถึงพนักงาน รฟม. ที่ได้รับมอบหมายให้เก็บรวบรวม ใช้ เปิดเผย และเข้าถึงข้อมูลส่วนบุคคล ตามวัตถุประสงค์ของกิจกรรมนั้น ๆ ในนามของ รฟม.
6. คณะกรรมการเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หมายถึง กลุ่มของบุคคลซึ่งได้รับมอบหมายจากผู้ว่าการให้ทำหน้าที่เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ตามมาตรา 42 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
7. ผู้ประมวลผลข้อมูลส่วนบุคคล หมายถึง บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล
8. ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ
9. การปกปิดข้อมูล (Data Masking) หมายถึง การปกปิดข้อมูลจริงเพื่อให้ข้อมูลนั้นแสดงเป็นข้อมูลหลอกหรือนามแฝง
10. ข้อมูลนิรนาม (Anonymization Data) หมายถึง ข้อมูลที่ผ่านกระบวนการซึ่งทำให้ไม่สามารถระบุตัวตนหรือแสดงตัวตนได้ทั้งในปัจจุบันและอนาคต และไม่ใช่อข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
11. การจัดทำข้อมูลนิรนาม (Data Anonymization) หมายความว่า กระบวนการทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุหรือเชื่อมโยงข้อมูลไปถึงตัวบุคคลได้ทั้งในปัจจุบันและอนาคต โดยใช้เทคนิคหลายเทคนิคร่วมกันจนมั่นใจว่าไม่สามารถระบุตัวตนได้ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

12. การจัดทำข้อมูลแฝง (Data Pseudonymization) หมายความว่า กระบวนการเปลี่ยนแปลงข้อมูลส่วนบุคคลด้วยการใช้อักขระแฝงหรือวิธีการอื่นใด เช่น การเข้ารหัสข้อมูล (Encryption) การเข้าฟังก์ชันแฮช (Hashing) การเก็บข้อมูลแยกส่วนโดยเชื่อมผ่านโทเคน (Tokenization) โดยยังสามารถเชื่อมโยงข้อมูลเพื่อระบุตัวตนได้เมื่อมีข้อมูลเพิ่มเติมประกอบและไม่ถือเป็นข้อมูลนิรนาม
13. การประมวลผลข้อมูลส่วนบุคคล หมายถึง การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล
14. เจ้าของข้อมูลส่วนบุคคล หมายถึง บุคคลที่ข้อมูลส่วนบุคคลสามารถระบุถึงตัวบุคคลนั้น ไม่รวมผู้ถึงแก่กรรมและนิติบุคคล
15. ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) หมายถึง ข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับผู้ประมวลผลข้อมูลส่วนบุคคล เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
16. ความมั่นคงปลอดภัย หมายถึง การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคล เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ
17. การละเมิดข้อมูลส่วนบุคคล หมายถึง การละเมิดมาตรการรักษาความมั่นคงปลอดภัยที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเป็นเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบ การกระทำ ความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด ซึ่งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแต่ละเหตุอาจเกี่ยวข้องกับการละเมิดประเภทใดประเภทหนึ่งหรือหลายประเภท ดังต่อไปนี้
 - (1) การละเมิดความลับของข้อมูลส่วนบุคคล (Confidentiality Breach) ซึ่งมีการเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ
 - (2) การละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคล (Integrity Breach) ซึ่งมีการเปลี่ยนแปลงแก้ไขข้อมูลส่วนบุคคลให้ไม่ถูกต้อง ไม่สมบูรณ์ หรือไม่ครบถ้วน โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ
 - (3) การละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคล (Availability Breach) ซึ่งทำให้ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ หรือมีการทำลายข้อมูลส่วนบุคคล ทำให้ข้อมูลส่วนบุคคลไม่อยู่ในสภาพที่พร้อมใช้งานได้ตามปกติ
18. ผู้พบเห็นเหตุการณ์ หมายถึง ผู้พบเห็นเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
19. ผู้ดูแลระบบ หมายถึง พนักงาน รฟม. ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบสารสนเทศ และพนักงานของผู้รับจ้างที่รับผิดชอบติดตั้งหรือบำรุงรักษาระบบสารสนเทศให้ รฟม.

หมวด 1

แนวปฏิบัติสำหรับผู้ควบคุมข้อมูลส่วนบุคคล

ส่วนที่ 1

ระบบบริหารจัดการด้านการคุ้มครองข้อมูลส่วนบุคคล

วัตถุประสงค์

- เพื่อให้การปฏิบัติงานของ รฟม. เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- เพื่อเป็นแนวปฏิบัติในการบริหารจัดการการคุ้มครองข้อมูลส่วนบุคคลอย่างชัดเจนและมีประสิทธิภาพ

กฎหมายที่เกี่ยวข้อง

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

มาตรา 37 ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(1) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด

มาตรา 77 ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลอันเป็นการฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติแห่งพระราชบัญญัตินี้ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ต้องชดเชยค่าสินไหมทดแทนเพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคล ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ก็ตาม เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้นจะพิสูจน์ได้ว่า

(1) ความเสียหายนั้นเกิดจากเหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั่นเอง

(2) เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมาย

มาตรา 79 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 27 วรรคหนึ่งหรือวรรคสอง หรือไม่ปฏิบัติตามมาตรา 28 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 26 โดยประการที่น่าจะก่อให้เกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ

ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 27 วรรคหนึ่งหรือวรรคสอง หรือไม่ปฏิบัติตามมาตรา 28 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 26 เพื่อแสวงหาประโยชน์ที่มีครุได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งล้านบาท หรือทั้งจำทั้งปรับ

ความผิดตามมาตรานี้เป็นความผิดอันยอมความได้

มาตรา 80 ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ถ้าผู้นั้นนำไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ ความในวรรคหนึ่ง มิให้นำมาใช้บังคับแก่การเปิดเผย ในกรณีดังต่อไปนี้

- (1) การเปิดเผยตามหน้าที่
- (2) การเปิดเผยเพื่อประโยชน์แก่การสอบสวน หรือการพิจารณาคดี
- (3) การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย
- (4) การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล
- (5) การเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่าง ๆ ที่เปิดเผยต่อสาธารณะ

มาตรา 81 ในกรณีที่ผู้กระทำความผิดตามพระราชบัญญัตินี้เป็นนิติบุคคล ถ้าการกระทำความผิดของนิติบุคคลนั้นเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย

- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565

อ้างอิงมาตรฐาน

- ISO/IEC 27701:2019 Annex A5

ผู้รับผิดชอบ

- ผู้ว่าการ
- คณะกรรมการเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
- ผู้บริหาร รฟม.
- ผทท.

แนวปฏิบัติ

1. ผู้ว่าการต้องกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคล และทบทวน/ปรับปรุงนโยบายอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ โดยนโยบายการคุ้มครองข้อมูลส่วนบุคคลต้องผ่านการพิจารณาให้ข้อสังเกตจากคณะกรรมการเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
2. ผู้ว่าการต้องจัดให้มีบุคลากรดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคลและกำหนดหน้าที่ความรับผิดชอบ รวมทั้งปรับปรุงโครงสร้างดังกล่าวตามความจำเป็น
3. ผู้ว่าการต้องจัดให้มีทรัพยากรที่จำเป็นต่อการบริหารจัดการด้านการคุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอ รวมถึงสร้างความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล
4. ผู้ว่าการต้องกำหนดแนวปฏิบัติที่เกี่ยวข้องกับระบบการบริหารจัดการด้านการคุ้มครองข้อมูลส่วนบุคคล ประกอบด้วย

- 4.1 แนวปฏิบัติในการจัดทำและควบคุมบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล
- 4.2 แนวปฏิบัติในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
- 4.3 แนวปฏิบัติในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล โดยครอบคลุมหลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
- 4.4 แนวปฏิบัติในการจัดการคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล โดยครอบคลุมการบันทึกการปฏิเสธคำขอใช้สิทธิของเจ้าของ
- 4.5 แนวปฏิบัติการประเมินผลกระทบด้านความเป็นส่วนตัว (Privacy Impact Assessment)
- 4.6 แนวปฏิบัติการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment)
- 4.7 แนวปฏิบัติการจัดเก็บข้อมูลส่วนบุคคล โดยครอบคลุมการจัดทำข้อมูลนิรนาม
- 4.8 แนวปฏิบัติการประเมินมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลของผู้ประมวลผลข้อมูลส่วนบุคคล
5. ผู้ว่าจ้างต้องกำหนดให้มีการทบทวน/ปรับปรุงแนวปฏิบัติที่สนับสนุนการทำงานต่าง ๆ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ เพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม
6. ผู้ว่าจ้างต้องประกาศนโยบาย แนวปฏิบัติ และมาตรการคุ้มครองข้อมูลส่วนบุคคลให้บุคลากร รพม. รับทราบ และถือปฏิบัติ
7. ผู้บริหาร รพม. ต้องแสดงเจตนารมณ์หรือสื่อสารอย่างสม่ำเสมอ เพื่อให้บุคลากร รพม. ทุกคนได้เห็นถึงความสำคัญของการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลโดยเคร่งครัด
8. การสร้างความตระหนักด้านการคุ้มครองข้อมูลส่วนบุคคล
 - 8.1 ผู้บริหาร รพม. ทุกระดับชั้น มีหน้าที่สนับสนุนและส่งเสริมการคุ้มครองข้อมูลส่วนบุคคลแก่พนักงาน รพม. ต่อไปนี้
 - (1) จูงใจให้พนักงานเจ้าหน้าที่ปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล
 - (2) สร้างความตระหนักถึงการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับหน้าที่ความรับผิดชอบของตนเอง และของ รพม.
 - 8.2 ผทพ. ต้องจัดให้มีฝึกอบรมหรือประชาสัมพันธ์แก่พนักงานเจ้าหน้าที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล เพื่อสร้างความตระหนักด้านการคุ้มครองข้อมูลส่วนบุคคลแก่ผู้ใช้งานเป็นประจำทุกปี

ส่วนที่ 2

การประมวลผลข้อมูลส่วนบุคคล

วัตถุประสงค์

- เพื่อกำหนดแนวทางในการเก็บ รวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล

กฎหมายที่เกี่ยวข้อง

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

มาตรา 21 ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือในขณะที่เก็บรวบรวม

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่แตกต่างไปจากวัตถุประสงค์ที่ได้แจ้งไว้ตามวรรคหนึ่งจะกระทำมิได้ เว้นแต่

(1) ได้แจ้งวัตถุประสงค์ใหม่นั้นให้เจ้าของข้อมูลส่วนบุคคลทราบและได้รับความยินยอมก่อนเก็บรวบรวม ใช้ หรือเปิดเผยแล้ว

(2) บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้

มาตรา 23 ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะที่เก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียด ดังต่อไปนี้ เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว

(1) วัตถุประสงค์ของการเก็บรวบรวมเพื่อการนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยซึ่งรวมถึงวัตถุประสงค์ตามที่มาตรา 24 ให้อำนาจในการเก็บรวบรวมได้โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

(2) แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญาหรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล

(3) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม

(4) ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย

(5) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อในกรณีที่ตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ให้แจ้งข้อมูล สถานที่ติดต่อ และวิธีการติดต่อของตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย

(6) สิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 19 วรรคห้า มาตรา 30 วรรคหนึ่ง มาตรา 31 วรรคหนึ่ง มาตรา 32 วรรคหนึ่ง มาตรา 33 วรรคหนึ่ง มาตรา 34 วรรคหนึ่ง มาตรา 36 วรรคหนึ่ง และมาตรา 37 วรรคหนึ่ง

มาตรา 24 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

- (1) เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ตามที่คณะกรรมการประกาศกำหนด
- (2) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล
- (3) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น
- (4) เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินการกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจอธิปไตยที่มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล
- (5) เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล
- (6) เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

มาตรา 25 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่

- (1) ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า แต่ต้องไม่เกินสามสิบวันนับแต่วันที่เก็บรวบรวมและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
- (2) เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26

ให้นำบทบัญญัติเกี่ยวกับการแจ้งวัตถุประสงค์ใหม่ตามมาตรา 21 และการแจ้งรายละเอียดตามมาตรา 23 มาใช้บังคับกับการเก็บรวบรวมข้อมูลส่วนบุคคลที่ต้องได้รับความยินยอมตามวรรคหนึ่งโดยอนุโลม เว้นแต่กรณีดังต่อไปนี้

- (1) เจ้าของข้อมูลส่วนบุคคลทราบวัตถุประสงค์ใหม่หรือรายละเอียดนั้นอยู่แล้ว
- (2) ผู้ควบคุมข้อมูลส่วนบุคคลพิสูจน์ได้ว่าการแจ้งวัตถุประสงค์ใหม่หรือรายละเอียดดังกล่าวไม่สามารถทำได้หรือจะเป็นอุปสรรคต่อการใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งเพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ในกรณีนี้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิ เสรีภาพ และประโยชน์ของเจ้าของข้อมูลส่วนบุคคล
- (3) การใช้หรือการเปิดเผยข้อมูลส่วนบุคคลต้องกระทำโดยเร่งด่วนตามที่กฎหมายกำหนด ซึ่งได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

(4) เมื่อผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้ซึ่งล่วงรู้หรือได้มาซึ่งข้อมูลส่วนบุคคลจากหน้าที่หรือจากการประกอบอาชีพหรือวิชาชีพและต้องรักษาวัตถุประสงค์ใหม่หรือรายละเอียดบางประการตามมาตรา 23 ไว้เป็นความลับตามที่กฎหมายกำหนด

การแจ้งรายละเอียดตามวรรคสอง ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบภายในสามสิบวันนับแต่วันที่เก็บรวบรวมตามมาตรา 21 เว้นแต่กรณีที่นำข้อมูลส่วนบุคคลไปใช้เพื่อการติดต่อกับเจ้าของข้อมูลส่วนบุคคลต้องแจ้งในการติดต่อกครั้งแรก และกรณีที่นำข้อมูลส่วนบุคคลไปเปิดเผย ต้องแจ้งก่อนที่จะนำข้อมูลส่วนบุคคลไปเปิดเผยเป็นครั้งแรก

มาตรา 26 ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสุขภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนดโดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(1) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม

(2) เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิสมาคม หรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสุขภาพแรงงานให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรนั้น

(3) เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล

(4) เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมายการปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

(5) เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ

(ก) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของ ลูกจ้างการวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์

(ข) ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

(ค) การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคม ซึ่งการเก็บรวบรวมข้อมูลส่วนบุคคลเป็นสิ่งจำเป็นในการปฏิบัติตามสิทธิหรือหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคล โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

(ง) การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น ทั้งนี้ ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น และได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ตามที่คณะกรรมการประกาศกำหนด

(จ) ประโยชน์สาธารณะที่สำคัญ โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

ข้อมูลชีวภาพตามวรรคหนึ่งให้หมายถึงข้อมูลส่วนบุคคลที่เกิดจากการใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวข้องกับการนำลักษณะเด่นทางกายภาพหรือทางพฤติกรรมของบุคคลมาใช้ทำให้สามารถยืนยันตัวตนของบุคคลนั้นที่ไม่เหมือนกับบุคคลอื่นได้ เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองม่านตา หรือข้อมูลจำลองลายนิ้วมือ

ในกรณีที่เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมต้องกระทำภายใต้การควบคุมของหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมายหรือได้จัดให้มีมาตรการคุ้มครองข้อมูลส่วนบุคคลตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด

มาตรา 27 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26

บุคคลหรือนิติบุคคลที่ได้รับข้อมูลส่วนบุคคลมาจากการเปิดเผยตามวรรคหนึ่ง จะต้องไม่ใช่หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลส่วนบุคคลในการขอรับข้อมูลส่วนบุคคลนั้น

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกการใช้หรือเปิดเผยนั้นไว้ในรายการตามมาตรา 39

มาตรา 39 ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกการอย่างน้อยดังต่อไปนี้ เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานสามารถตรวจสอบได้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้

- (1) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
- (2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท
- (3) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล
- (4) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

(5) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น

(6) การใช้หรือเปิดเผยตามมาตรา 27 วรรคสาม

(7) การปฏิเสธคำขอหรือการคัดค้านตามมาตรา 30 วรรคสาม มาตรา 31 วรรคสาม มาตรา 32 วรรคสาม และมาตรา 36 วรรคหนึ่ง

(8) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา 37 (1)

ความในวรรคหนึ่งให้นำมาใช้บังคับกับตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 5 วรรคสอง โดยอนุโลม

ความใน (1) (2) (3) (4) (5) (6) และ (8) อาจยกเว้นมิให้นำมาใช้บังคับกับผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด เว้นแต่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมิใช่กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว หรือมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26

มาตรา 40 ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(1) ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้

(2) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

(3) จัดทำและเก็บรักษาบันทึกการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

ผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งไม่ปฏิบัติตาม (1) สำหรับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลใด ให้ถือว่าผู้ประมวลผลข้อมูลส่วนบุคคลเป็นผู้ควบคุมข้อมูลส่วนบุคคลสำหรับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้น

การดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีข้อตกลงระหว่างกัน เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัตินี้

ความใน (3) อาจยกเว้นมิให้นำมาใช้บังคับกับผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด เว้นแต่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมิใช่กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว หรือมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26

อ้างอิงมาตรฐาน

- ISO/IEC 27701:2019 Annex A7.2 A7.3 และ A7.4

ผู้รับผิดชอบ

- เจ้าของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

แนวปฏิบัติ

1. เจ้าของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลต้องกำหนดวัตถุประสงค์ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลให้ชัดเจน
2. เจ้าของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลต้องกำหนดรายการข้อมูลส่วนบุคคลที่ต้องเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็นตามวัตถุประสงค์อันชอบด้วยกฎหมายและอยู่ภายใต้การดำเนินงานของ รฟม. เท่านั้น
3. เจ้าของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลต้องไม่เก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่เป็นวัตถุประสงค์อันชอบด้วยกฎหมายและอยู่ภายใต้การดำเนินงานของ รฟม. เท่านั้น
4. เจ้าของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลต้องจัดทำ หรือทบทวน/ปรับปรุงบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activity: RoPA) เพื่อควบคุมการประมวลผลข้อมูลส่วนบุคคลและให้เจ้าของข้อมูลส่วนบุคคลตรวจสอบได้ ทั้งนี้ ในการทบทวน/ปรับปรุงให้ดำเนินการอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ โดยอย่างน้อยต้องประกอบไปด้วยรายละเอียดตามมาตรา 39 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ดังต่อไปนี้
 - (1) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
 - (2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท
 - (3) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล
 - (4) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
 - (5) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคล และเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น
 - (6) การใช้หรือเปิดเผยตามมาตรา 27 วรรคสาม
 - (7) การปฏิเสธคำขอหรือการคัดค้านตามมาตรา 30 วรรคสาม มาตรา 31 วรรคสาม มาตรา 32 วรรคสาม และมาตรา 36 วรรคหนึ่ง
 - (8) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา 37 (1)
 - (9) ฐานการประมวลผลข้อมูลส่วนบุคคลตามกฎหมาย
 - (10) วิธีการแจ้งรายละเอียดการประมวลผลข้อมูลส่วนบุคคล
 - (11) วิธีการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล (หากมี)

5. เจ้าของกิจการประมวลผลข้อมูลส่วนบุคคล ต้องจัดทำ หรือทบทวน/ปรับปรุงหนังสือแจ้งการประมวลผลข้อมูลส่วนบุคคล (Privacy Notice) เพื่อแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะที่เก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียดของการประมวลผลข้อมูลส่วนบุคคล โดยอย่างน้อยต้องประกอบไปด้วยรายละเอียดตามมาตรา 23 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ดังต่อไปนี้
 - (1) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคล
 - (2) ฐานการประมวลผลข้อมูลส่วนบุคคลตามกฎหมาย และต้องแจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญาหรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล
 - (3) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
 - (4) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลเป็นเวลา 10 ปี
 - (5) ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย
 - (6) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคลประกอบด้วย สถานที่ติดต่อ และวิธีการติดต่อ
 - (7) ข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลประกอบด้วย สถานที่ติดต่อ และวิธีการติดต่อ
 - (8) สิทธิของเจ้าของข้อมูลส่วนบุคคล
 - (9) ฐานการประมวลผลข้อมูลส่วนบุคคลตามกฎหมายทั้งนี้ การทบทวน/ปรับปรุงหนังสือแจ้งการประมวลผลข้อมูลส่วนบุคคล (Privacy Notice) ให้ดำเนินการเมื่อมีการเปลี่ยนแปลงรายละเอียดของบันทึกกิจการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activity: RoPA)
6. เจ้าของกิจการประมวลผลข้อมูลส่วนบุคคล แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะที่เก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียดของการประมวลผลข้อมูลส่วนบุคคล ตามข้อ 4. ผ่านช่องทางใดก็ได้ เช่น การแจ้งเป็นหนังสือ การแจ้งทางข้อความโทรศัพท์มือถือ การแจ้งทางอีเมล หรือโดยวิธีการทางอิเล็กทรอนิกส์อื่นใด เช่น QR Code หรือ URL เป็นต้น
7. เจ้าของกิจการประมวลผลข้อมูลส่วนบุคคล หากจำเป็นต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลให้ปฏิบัติตามแนวปฏิบัติในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
8. เจ้าของกิจการประมวลผลข้อมูลส่วนบุคคล ต้องประเมินผลกระทบด้านความเป็นส่วนตัว (Privacy Impact Assessment) และประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment) ตามแนวปฏิบัติที่ รพม. กำหนด รวมถึงกำหนดมาตรการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลที่เหมาะสม
9. เจ้าของกิจการประมวลผลข้อมูลส่วนบุคคลที่กำกับดูแลสัญญาจ้างที่มีการประมวลผลข้อมูลส่วนบุคคล ต้องควบคุมและตรวจสอบการดำเนินงานของผู้ประมวลผลข้อมูลส่วนบุคคล รวมถึงลูกจ้างของผู้ประมวลผลข้อมูลส่วนบุคคลให้ประมวลผลข้อมูลส่วนบุคคลเป็นไปตามที่สัญญาจ้างกำหนดและเป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ส่วนที่ 3

มาตรการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคล

วัตถุประสงค์

- เพื่อกำหนดมาตรการรักษาความมั่นคงปลอดภัยในการป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

กฎหมายที่เกี่ยวข้อง

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
มาตรา 37 ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้
(1) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวน มาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษา ความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุม ข้อมูลส่วนบุคคล พ.ศ. 2565
- ประกาศการรถไฟฯขนส่งมวลชนแห่งประเทศไทย เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของ ระบบเทคโนโลยีสารสนเทศ

อ้างอิงมาตรฐาน

- ISO/IEC 27701:2019 Annex A6

ผู้รับผิดชอบ

- เจ้าของกิจการผลการประมวลผลข้อมูลส่วนบุคคล

แนวปฏิบัติ

1. เจ้าของกิจการผลการประมวลผลข้อมูลส่วนบุคคลต้องรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล โดยครอบคลุม ทั้งในรูปแบบเอกสาร อิเล็กทรอนิกส์ หรืออื่นใด ให้สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยของระบบ เทคโนโลยีสารสนเทศ ระเบียบ หรือข้อบังคับขององค์กร
2. เจ้าของกิจการผลการประมวลผลข้อมูลส่วนบุคคลต้องประมวลผลข้อมูลส่วนบุคคลอย่างระมัดระวัง และประมวลผล เพื่อปฏิบัติงานของ รฟม. เท่านั้น
3. การบริหารจัดการข้อมูลส่วนบุคคล
 - 3.1 เจ้าของกิจการผลการประมวลผลข้อมูลส่วนบุคคลต้องกำหนดรายการข้อมูลส่วนบุคคล ระบุผู้รับผิดชอบ ดูแลข้อมูลส่วนบุคคล จัดประเภทข้อมูลส่วนบุคคล กำหนดลำดับชั้นความลับ และกำหนดการเข้าถึง ข้อมูลส่วนบุคคล เพื่อควบคุมดูแลข้อมูลส่วนบุคคลตลอดวงจรชีวิตข้อมูล

3.2 เจ้าของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลต้องจัดทำป้ายกำกับข้อมูลส่วนบุคคล (Labeling) ให้ชัดเจน พร้อมทั้งจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่สอดคล้องกับประเภทข้อมูลส่วนบุคคลและระดับชั้นความลับที่ รพม. กำหนด

4. การควบคุมการเข้าถึงข้อมูลส่วนบุคคล

4.1 เจ้าของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลต้องกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลที่เหมาะสม และสอดคล้องกับหน้าที่ความรับผิดชอบของผู้ประมวลผลข้อมูลส่วนบุคคล พร้อมทั้งทบทวนเมื่อมีการเปลี่ยนแปลง

4.2 ขั้นตอนปฏิบัติในการจัดเก็บข้อมูลส่วนบุคคล

เจ้าของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลต้องปฏิบัติ ดังนี้

4.2.1 จัดประเภทข้อมูลส่วนบุคคล ดังนี้

- (1) ข้อมูลส่วนบุคคลทั่วไป เช่น ชื่อ-นามสกุล ที่อยู่ หมายเลขโทรศัพท์ เป็นต้น
- (2) ข้อมูลส่วนบุคคลอ่อนไหว เช่น
 - เชื้อชาติ
 - เผ่าพันธุ์
 - ความคิดเห็นทางการเมือง
 - ความเชื่อในลัทธิ ศาสนา หรือปรัชญา
 - พฤติกรรมทางเพศ
 - ประวัติอาชญากรรม
 - ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต
 - ข้อมูลสภาพแรงงาน
 - ข้อมูลพันธุกรรม
 - ข้อมูลชีวภาพ
 - ข้อมูลทางชีวมิติ (Biometric) เช่น รูปภาพใบหน้า ลายนิ้วมือ फिल्मเอกซเรย์ ข้อมูลสแกนม่านตา ข้อมูลอัตลักษณ์เสียง และข้อมูลพันธุกรรม
 - ข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด

4.2.2 จัดแบ่งระดับความสำคัญของข้อมูลออกเป็น 3 ระดับ คือ

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

4.2.3 จัดแบ่งลำดับชั้นความลับของข้อมูลตามที่ รพม. กำหนด

4.2.4 จัดแบ่งระดับชั้นการเข้าถึงข้อมูลส่วนบุคคล

- (1) ระดับชั้นสำหรับผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และภารกิจที่ได้รับมอบหมาย
- (2) ระดับชั้นสำหรับผู้ปฏิบัติงานทั่วไป เข้าถึงข้อมูลที่ได้รับมอบหมายตามอำนาจหน้าที่
- (3) ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย มีสิทธิ์ในการบริหารจัดการระบบ และเข้าถึงข้อมูลที่ได้รับมอบหมายตามอำนาจหน้าที่

4.3 เจ้าของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล ต้องพิจารณาข้อกำหนดต่าง ๆ ที่มีผลทางกฎหมาย ซึ่งเกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล เช่น พระราชบัญญัติ ข้อกำหนดทางกฎหมาย ข้อกำหนดในสัญญา และข้อกำหนดทางด้านการคุ้มครองข้อมูลส่วนบุคคลอื่น ๆ เป็นต้น เพื่อกำหนดสิทธิ์การเข้าถึงข้อมูลส่วนบุคคล

4.4 เจ้าของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล ต้องควบคุมการใช้งานข้อมูลส่วนบุคคลให้มีการใช้งานที่สอดคล้องกับกฎหมาย พระราชบัญญัติ กฎระเบียบ ข้อบังคับที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

5. เจ้าของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลต้องปกปิดข้อมูล (Data Masking) ให้สอดคล้องกับประเภทข้อมูลส่วนบุคคล และระดับชั้นความลับที่ รพม. กำหนด

ส่วนที่ 4

การส่งมอบข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่น และการใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้รับมอบจากบุคคลหรือนิติบุคคลอื่น

วัตถุประสงค์

- เพื่อป้องกันมิให้บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ รพม. ใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ
- เพื่อควบคุมให้ รพม. ใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้รับมาจากบุคคลหรือนิติบุคคลอื่นตามวัตถุประสงค์ที่กำหนดไว้

กฎหมายที่เกี่ยวข้อง

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

มาตรา 27 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26

บุคคลหรือนิติบุคคลที่ได้รับข้อมูลส่วนบุคคลมาจากการเปิดเผยตามวรรคหนึ่ง จะต้องไม่ใช่หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลส่วนบุคคลในการขอรับข้อมูลส่วนบุคคลนั้น

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกการใช้หรือเปิดเผยนั้นไว้ในรายการตามมาตรา 39

มาตรา 37 ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(2) ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้รับใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

มาตรา 40 ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

การดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีข้อตกลงระหว่างกัน เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัตินี้

อ้างอิงมาตรฐาน

- ISO/IEC 27701:2019 Annex A7.2 และ A7.3

ผู้รับผิดชอบ

- เจ้าของกิจการกรรมการประมวลผลข้อมูลส่วนบุคคล

แนวปฏิบัติ

1. การส่งมอบข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่น
 - 1.1 เจ้าของกิจการประมวลผลข้อมูลส่วนบุคคล ต้องไม่เปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับการยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
 - 1.2 เจ้าของกิจการประมวลผลข้อมูลส่วนบุคคล ต้องบันทึกการเปิดเผยข้อมูลส่วนบุคคลที่ได้รับการยกเว้นไม่ต้องขอความยินยอมในบันทึกกิจการประมวลผลข้อมูลส่วนบุคคล
 - 1.3 เจ้าของกิจการประมวลผลข้อมูลส่วนบุคคล ต้องจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) กับผู้ประมวลผลข้อมูลส่วนบุคคลเมื่อมีการส่งมอบข้อมูลส่วนบุคคลให้ผู้ประมวลผลข้อมูลส่วนบุคคล เพื่อควบคุมให้ผู้ประมวลผลข้อมูลส่วนบุคคล (ภายนอก) ดำเนินการตามที่ รฟม. กำหนด
 - 1.4 เจ้าของกิจการประมวลผลข้อมูลส่วนบุคคล ต้องจัดทำข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (Data Sharing Agreement: DSA) กับบุคคลหรือนิติบุคคลอื่น
 - 1.5 เจ้าของกิจการประมวลผลข้อมูลส่วนบุคคล ต้องส่งมอบข้อมูลส่วนบุคคลด้วยวิธีการที่ปลอดภัย และสอดคล้องกับระดับชั้นความลับของข้อมูลตามที่ รฟม. กำหนด
 - 1.6 เจ้าของกิจการประมวลผลข้อมูลส่วนบุคคล ต้องบันทึกข้อมูลของผู้ร้องขอก่อนส่งมอบข้อมูลส่วนบุคคล ดังนี้
 - (1) ชื่อ-นามสกุล
 - (2) ข้อมูลสำหรับการติดต่อ เช่น หมายเลขโทรศัพท์ อีเมล
 - (3) วัน เดือน ปี ที่ให้ข้อมูล
 - (4) ฐานทางกฎหมายที่ใช้สำหรับเข้าถึงข้อมูลส่วนบุคคล
 - (5) วัตถุประสงค์การนำไปใช้งาน และ/หรือ เผย
2. การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้รับมอบจากบุคคลหรือนิติบุคคลอื่น
 - 2.1 เจ้าของกิจการประมวลผลข้อมูลส่วนบุคคล ต้องไม่เปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับการยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
 - 2.2 เจ้าของกิจการประมวลผลข้อมูลส่วนบุคคลที่ได้รับข้อมูลส่วนบุคคลมาจากการเปิดเผยข้อมูลส่วนบุคคลจากบุคคลหรือนิติบุคคลอื่น จะต้องไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลส่วนบุคคลในการขอรับข้อมูลส่วนบุคคลนั้น

ส่วนที่ 5

การควบคุมการลบหรือทำลายข้อมูลส่วนบุคคล

วัตถุประสงค์

- เพื่อควบคุมการลบหรือทำลายข้อมูลส่วนบุคคล เมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้อนุญาตยินยอม

กฎหมายที่เกี่ยวข้อง

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

มาตรา 24 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(1) เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ตามที่คณะกรรมการประกาศกำหนด

(4) เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

มาตรา 26 ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสุขภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(5) เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ

(ก) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ ในกรณีที่มิใช่การปฏิบัติตามกฎหมาย และข้อมูลส่วนบุคคลนั้น อยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์

(ข) ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

มาตรา 33 เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ในกรณีดังต่อไปนี้

(1) เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

(2) เมื่อเจ้าของข้อมูลส่วนบุคคลถอนความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคลไม่มีอำนาจตามกฎหมายที่จะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นได้ต่อไป

(3) เมื่อเจ้าของข้อมูลส่วนบุคคลคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 32 (1) และผู้ควบคุมข้อมูลส่วนบุคคลไม่อาจปฏิเสธคำขอตามมาตรา 32 (1) (ก) หรือ (ข) ได้ หรือเป็นการคัดค้านตามมาตรา 32 (2)

(4) เมื่อข้อมูลส่วนบุคคลได้ถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ชอบด้วยกฎหมายตามที่กำหนดไว้ในหมวดนี้

ความในวรรคหนึ่งมิให้นำมาใช้บังคับกับการเก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น การเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา 24 (1) หรือ (4) หรือมาตรา 26 (5) (ก) หรือ (ข) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้ทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่เปิดเผยต่อสาธารณะและผู้ควบคุมข้อมูลส่วนบุคคลถูกขอให้ลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลต้องเป็นผู้รับผิดชอบดำเนินการทั้งในทางเทคโนโลยีและค่าใช้จ่ายเพื่อให้เป็นไปตามคำขอนั้น โดยแจ้งผู้ควบคุมข้อมูลส่วนบุคคลอื่น ๆ เพื่อให้ได้รับคำตอบในการดำเนินการให้เป็นไปตามคำขอ

กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามวรรคหนึ่งหรือวรรคสาม เจ้าของข้อมูลส่วนบุคคล มีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการได้

คณะกรรมการอาจประกาศกำหนดหลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลตามวรรคหนึ่งก็ได้

มาตรา 37 ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(3) จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอมเว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็นการเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา 24 (1) หรือ (4) หรือมาตรา 26 (5) (ก) หรือ (ข) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือ

เพื่อการปฏิบัติตามกฎหมาย ทั้งนี้ ให้นำความในมาตรา 33 วรรคห้า มาใช้บังคับกับการลบหรือทำลายข้อมูลส่วนบุคคลโดยอนุโลม

อ้างอิงมาตรฐาน

- ISO/IEC 27701:2019 Annex A5

ผู้รับผิดชอบ

- เจ้าของกิจการการประมวลผลข้อมูลส่วนบุคคล

แนวปฏิบัติ

1. เจ้าของกิจการการประมวลผลข้อมูลส่วนบุคคล ต้องจัดเก็บข้อมูลส่วนบุคคลไว้ในระยะเวลาเท่าที่ข้อมูลนั้นยังมีความจำเป็นตามวัตถุประสงค์ที่ระบุไว้ในบันทึกกิจการการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activity: RoPA)
2. เจ้าของกิจการการประมวลผลข้อมูลส่วนบุคคล ต้องทบทวนข้อมูลส่วนบุคคลที่อยู่ในความดูแลของตน ที่ครบกำหนดระยะเวลาใช้งานตามวัตถุประสงค์อย่างสม่ำเสมอ
3. เมื่อพ้นระยะเวลาและข้อมูลส่วนบุคคลสิ้นความจำเป็นตามวัตถุประสงค์แล้ว เจ้าของกิจการการประมวลผลข้อมูลส่วนบุคคล ต้องลบ ทำลาย หรือทำให้เป็นข้อมูลนิรนามตามรูปแบบและมาตรฐานการลบทำลายข้อมูลส่วนบุคคลที่คณะกรรมการหรือกฎหมายได้ประกาศกำหนด หรือตามมาตรฐานสากล หรือตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของ รพม. กำหนด หรือตามระเบียบข้อบังคับอื่น ๆ ของ รพม.
4. ในกรณีที่มิใช่ข้อพิพาทการใช้สิทธิหรือคดีความอันเกี่ยวข้องกับข้อมูลส่วนบุคคล เจ้าของกิจการการประมวลผลข้อมูลส่วนบุคคลสามารถขอสงวนสิทธิในการเก็บรักษาข้อมูลนั้นต่อไปจนกว่าข้อพิพาทนั้นจะได้มีคำสั่งหรือคำพิพากษาถึงที่สุด
5. ในกรณีที่เจ้าของข้อมูลส่วนบุคคลขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล เจ้าของกิจการการประมวลผลข้อมูลส่วนบุคคลต้องปฏิบัติตามแนวปฏิบัติขั้นตอนจัดการคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (ในส่วนของสิทธิในการขอให้ลบหรือทำลายข้อมูลส่วนบุคคล) และหากจำเป็นต้องปฏิเสธคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลต้องบันทึกการปฏิเสธคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลในบันทึกกิจการการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activity: RoPA)
6. เจ้าของกิจการการประมวลผลข้อมูลส่วนบุคคล สามารถยกเว้นการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวตนได้ ในกรณีที่เจ้าของกิจการการประมวลผลข้อมูลส่วนบุคคลมีเหตุผลความจำเป็นที่เหนือกว่าสิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมาย เช่น
 - เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุ เพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

- เพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล
- เพื่อประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการ ด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและ การให้บริการด้านสังคมสงเคราะห์ การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาด ที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์
- เพื่อการใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้อง ตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย

ส่วนที่ 6

การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

วัตถุประสงค์

- เพื่อแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลให้เป็นไปตามหลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

กฎหมายที่เกี่ยวข้อง

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
มาตรา 37 ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้
(4) แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่มีการละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและช้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด
- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565

ผู้รับผิดชอบ

- เจ้าของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล
- ผู้ว่าการ
- คณะกรรมการเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
- ผู้พบเห็นเหตุการณ์

แนวปฏิบัติ

1. ผู้พบเห็นเหตุการณ์ ต้องแจ้งให้ รพม. รับทราบเหตุการละเมิดข้อมูลส่วนบุคคลตามแนวปฏิบัติในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล
2. เมื่อได้รับแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล เจ้าของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล ผู้ว่าการ และคณะกรรมการเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ต้องปฏิบัติตามแนวปฏิบัติในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล
3. เจ้าของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล ต้องให้ความร่วมมือกับเจ้าหน้าที่ของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เมื่อถูกร้องขอให้ส่งเอกสารหรือข้อมูลเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล รวมถึงการชี้แจงข้อเท็จจริงเพื่อสนับสนุนการตรวจสอบและการปฏิบัติงานของเจ้าหน้าที่ของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

หมวด 2

แนวปฏิบัติสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล

วัตถุประสงค์

- เพื่อเป็นแนวปฏิบัติให้ผู้ประมวลผลข้อมูลส่วนบุคคลนำไปปฏิบัติให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล

กฎหมายที่เกี่ยวข้อง

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

มาตรา 40 ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(1) ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้

(2) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

(3) จัดทำและเก็บรักษาบันทึกการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

ผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งไม่ปฏิบัติตาม (1) สำหรับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลใด ให้ถือว่าผู้ประมวลผลข้อมูลส่วนบุคคลเป็นผู้ควบคุมข้อมูลส่วนบุคคลสำหรับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้น

การดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีข้อตกลงระหว่างกัน เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัตินี้

ความใน (3) อาจยกเว้นมิให้นำมาใช้บังคับกับผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด เว้นแต่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมิใช่กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว หรือมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26

- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. 2565

อ้างอิงมาตรฐาน

- ISO/IEC 27701:2019 Annex A 8

ผู้รับผิดชอบ

- ผู้ประมวลผลข้อมูลส่วนบุคคล

แนวปฏิบัติ

1. ผู้ประมวลผลข้อมูลส่วนบุคคลต้องเก็บรวบรวมข้อมูลส่วนบุคคลตามที่ รพม. กำหนดเท่านั้น
2. ผู้ประมวลผลข้อมูลส่วนบุคคลต้องไม่เก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่เป็นวัตถุประสงค์อันชอบด้วยกฎหมายและอยู่ภายใต้การดำเนินงานของ รพม. เท่านั้น
3. ผู้ประมวลผลข้อมูลส่วนบุคคล ต้องรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคล เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยให้ปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ และนโยบายของ รพม. อย่างเคร่งครัด
4. ผู้ประมวลผลข้อมูลส่วนบุคคล ต้องจัดทำบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activity: RoPA) เพื่อควบคุมการประมวลผลข้อมูลส่วนบุคคลและให้เจ้าของข้อมูลส่วนบุคคลตรวจสอบได้ ทั้งนี้ ในการทบทวน/ปรับปรุงให้ดำเนินการอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ โดยอย่างน้อยต้องประกอบด้วยรายละเอียดตามมาตรา 39 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ดังต่อไปนี้
 - (1) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
 - (2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท
 - (3) ข้อมูลเกี่ยวกับผู้ประมวลผลข้อมูลส่วนบุคคล
 - (4) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล
 - (5) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
 - (6) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคล และเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น
 - (7) การใช้หรือเปิดเผยตามมาตรา 27 วรรคสาม
 - (8) การปฏิเสธคำขอหรือการคัดค้านตามมาตรา 30 วรรคสาม มาตรา 31 วรรคสาม มาตรา 32 วรรคสาม และมาตรา 36 วรรคหนึ่ง
 - (9) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา 37 (1)
 - (10) ฐานการประมวลผลข้อมูลส่วนบุคคลตามกฎหมาย
 - (11) วิธีการแจ้งรายละเอียดการประมวลผลข้อมูลส่วนบุคคล
 - (12) วิธีการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล (หากมี)
5. ผู้ประมวลผลข้อมูลส่วนบุคคล ต้องใช้ข้อมูลส่วนบุคคลอย่างระมัดระวัง และใช้เพื่อปฏิบัติงานของ รพม. เท่านั้น รวมทั้งต้องปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ และนโยบาย ของ รพม.
6. ผู้ประมวลผลข้อมูลส่วนบุคคล ต้องควบคุมการเข้าถึงข้อมูลส่วนบุคคล ดังนี้
 - 6.1 ต้องกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลที่เหมาะสมและสอดคล้องกับหน้าที่ความรับผิดชอบของผู้ประมวลผลข้อมูลส่วนบุคคล พร้อมทั้งทบทวนเมื่อมีการเปลี่ยนแปลง

6.2 ขั้นตอนปฏิบัติในการจัดเก็บข้อมูลส่วนบุคคล

6.2.1 จัดประเภทข้อมูลส่วนบุคคล ดังนี้

- (1) ข้อมูลส่วนบุคคลทั่วไป เช่น ชื่อ-นามสกุล ที่อยู่ หมายเลขโทรศัพท์ เป็นต้น
- (2) ข้อมูลส่วนบุคคลอ่อนไหว เช่น
 - เชื้อชาติ
 - เผ่าพันธุ์
 - ความคิดเห็นทางการเมือง
 - ความเชื่อในลัทธิ ศาสนาหรือปรัชญา
 - พฤติกรรมทางเพศ
 - ประวัติอาชญากรรม
 - ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต
 - ข้อมูลสภาพแรงงาน
 - ข้อมูลพันธุกรรม
 - ข้อมูลชีวภาพ
 - ข้อมูลทางชีวมิติ (Biometric) เช่น รูปภาพใบหน้า ลายนิ้วมือ फिल्मเอกซเรย์ ข้อมูลสแกนม่านตา ข้อมูลอัตลักษณ์เสียง และข้อมูลพันธุกรรม เป็นต้น
 - ข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด

6.2.2 จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น 3 ระดับ คือ

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

6.2.3 จัดแบ่งลำดับชั้นความลับของข้อมูลตามที่ รพม. กำหนด

6.2.4 จัดแบ่งระดับชั้นการเข้าถึง

- (1) ระดับชั้นสำหรับผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และภารกิจที่ได้รับมอบหมาย
- (2) ระดับชั้นสำหรับผู้ปฏิบัติงานทั่วไป เข้าถึงข้อมูลที่ได้รับมอบหมายตามอำนาจหน้าที่
- (3) ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย มีสิทธิ์ในการบริหารจัดการระบบ และเข้าถึงข้อมูลที่ได้รับมอบหมายตามอำนาจหน้าที่

6.3 ผู้ประมวลผลข้อมูลส่วนบุคคล ต้องพิจารณาข้อกำหนดต่าง ๆ ที่มีผลทางกฎหมาย ซึ่งเกี่ยวข้องกับ การคุ้มครองข้อมูลส่วนบุคคล เช่น พระราชบัญญัติ ข้อกำหนดทางกฎหมาย ข้อกำหนดในสัญญา และ

ข้อกำหนดทางด้านการคุ้มครองข้อมูลส่วนบุคคลอื่น ๆ รวมทั้งระเบียบ ข้อบังคับ ของ รฟม. เป็นต้น เพื่อกำหนดสิทธิการเข้าถึงข้อมูลส่วนบุคคล

7. ผู้ประมวลผลข้อมูลส่วนบุคคล ต้องควบคุมการใช้งานข้อมูลส่วนบุคคลให้มีการใช้งานที่สอดคล้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงกฎหมายลำดับรองที่เกี่ยวข้อง
8. ผู้ประมวลผลข้อมูลส่วนบุคคล ต้องประมวลผลข้อมูลส่วนบุคคลตามข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) ที่ตกลงไว้กับ รฟม. เท่านั้น
9. เมื่อผู้ประมวลผลข้อมูลส่วนบุคคลพบเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ต้องแจ้งให้ รฟม. รับทราบตามช่องทางและแนวปฏิบัติที่ รฟม. กำหนด
10. ผู้ประมวลผลข้อมูลส่วนบุคคล ต้องให้ความร่วมมือกับเจ้าหน้าที่ของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และ รฟม. เมื่อถูกร้องขอให้ส่งเอกสารหรือข้อมูลเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล รวมถึงการชี้แจงข้อเท็จจริงเพื่อสนับสนุนการตรวจสอบและการปฏิบัติงานของเจ้าหน้าที่ของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ภาคผนวก ข



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

ประกาศการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (ฉบับปรับปรุงครั้งที่ 14)

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

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

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

1. วัตถุประสงค์และขอบเขต

เพื่อให้การใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาและลดผลกระทบจากการใช้งานระบบเทคโนโลยีสารสนเทศ ในลักษณะที่ไม่ถูกต้องหรือจากการถูกคุกคามจากภัยต่าง ๆ จึงได้กำหนดนโยบายเพื่อควบคุมการรักษาความมั่นคงปลอดภัย ของระบบเทคโนโลยีสารสนเทศ ดังนี้

1.1 การเข้าถึงหรือควบคุมการใช้งานสารสนเทศครอบคลุม 4 ด้าน คือ

- 1.1.1 การเข้าถึงระบบสารสนเทศ (Access control) ต้องตรวจสอบการอนุมัติสิทธิการเข้าถึงระบบและ กำหนดรหัสผ่าน การลงทะเบียนผู้ใช้งานเพื่อให้ผู้ใช้ที่มีสิทธิ์ (User authentication) เท่านั้นที่สามารถ เข้าถึงระบบได้ รวมถึงมีการเก็บบันทึกข้อมูลการเข้าถึงระบบ (Access log) และข้อมูลจราจรทางคอมพิวเตอร์ ทั้งนี้ การให้สิทธิการใช้งานระบบสารสนเทศนั้นต้องให้สิทธิอย่างเหมาะสมและเพียงพอ (Need to know and Need to use)

/1.1.2 การเข้าถึง

- 1.1.2 การเข้าถึงระบบเครือข่าย (Network access control) ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ การรับ - ส่ง หรือการไหลเวียนข้อมูลหรือสารสนเทศจะต้องผ่านระบบการรักษาความปลอดภัยที่องค์กร จัดสรรไว้ เช่น Firewall IDS/IPS Proxy หรือการตรวจสอบไวรัสคอมพิวเตอร์ เป็นต้น เพื่อควบคุมและ ป้องกันภัยคุกคามอย่างเป็นระบบ
 - 1.1.3 การเข้าถึงระบบปฏิบัติการ (Operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการ โดยไม่ได้รับอนุญาต โดยกำหนดให้มีการยืนยันตัวตนเพื่อระบุถึงตัวตนของผู้ใช้งาน รวมทั้งกำหนดให้ มี การจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้ความมั่นคงปลอดภัยมากยิ่งขึ้น
 - 1.1.4 การเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information access control) ต้องกำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศ โดยให้สิทธิ์เฉพาะระบบงานสารสนเทศ ที่ต้องปฏิบัติตามหน้าที่เท่านั้น รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานระบบสารสนเทศอย่างสม่ำเสมอ
 - 1.2 มีระบบสารสนเทศและระบบสำรองที่อยู่ในสภาพพร้อมใช้งาน รวมทั้งมีแผนเตรียมพร้อมในกรณีฉุกเฉินหรือ กรณีที่ไม่สามารถดำเนินการตามวิธีการทางอิเล็กทรอนิกส์ได้ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติ อย่างต่อเนื่อง
 - 1.3 ตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศอย่างสม่ำเสมอ
2. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รพม.
- แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รพม. ใช้แนวทางและกระบวนการ อ้างอิงตาม 1) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องนโยบายและแนวปฏิบัติในการรักษาความ มั่นคง ปลอดภัยด้านสารสนเทศของหน่วยงานรัฐ พ.ศ. 2553 2) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐาน การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555 และ 3) มาตรฐาน ISO/IEC 27001:2022 โดยแบ่งแนวปฏิบัติออกเป็น 17 ส่วน ตามเอกสารแนบท้ายประกาศ ดังต่อไปนี้
- 2.1 นโยบายการบริหารจัดการความมั่นคงปลอดภัยสำหรับผู้บริหาร (ส่วนที่ 1)
 - 2.2 ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร (ส่วนที่ 2)
 - 2.3 การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (ส่วนที่ 3)
 - 2.4 การจัดการทรัพย์สิน (ส่วนที่ 4)
 - 2.5 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (ส่วนที่ 5)
 - 2.6 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ (ส่วนที่ 6)
 - 2.7 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (ส่วนที่ 7)
 - 2.8 การควบคุมหน่วยงานภายนอกและผู้ใช้งาน (บุคคลภายนอก) เข้าถึงระบบเทคโนโลยีสารสนเทศ (ส่วนที่ 8)
 - 2.9 การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ของ รพม. (ส่วนที่ 9)
 - 2.10 การใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์ (ส่วนที่ 10)
 - 2.11 การใช้งานจดหมายอิเล็กทรอนิกส์ (ส่วนที่ 11)
 - 2.12 การสำรองข้อมูลและการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (ส่วนที่ 12)
 - 2.13 การตรวจสอบและประเมินความเสี่ยง (ส่วนที่ 13)
 - 2.14 การถ่ายโอน และการแลกเปลี่ยนข้อมูลสารสนเทศ (ส่วนที่ 14)
 - 2.15 การควบคุมการเข้ารหัส (ส่วนที่ 15)
 - 2.16 การนำอุปกรณ์ส่วนตัวมาใช้งาน (Bring your own device) (ส่วนที่ 16)
 - 2.17 การใช้บริการ Cloud (Cloud Services) (ส่วนที่ 17)

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

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

นโยบายนี้ให้ใช้บังคับเมื่อพ้นกำหนด 7 วัน นับแต่วันที่ผู้มีอำนาจลงนาม

ประกาศ ณ วันที่ 15 กันยายน พ.ศ. 2568



(นายกาจผจญ อุดมธรรมภักดี)

ผู้ว่าการการรถไฟฟ้ามหานครแห่งประเทศไทย



สารบัญ

เรื่อง	หน้า
คำนิยาม.....	1
ส่วนที่ 1 นโยบายการบริหารจัดการความมั่นคงปลอดภัยสำหรับผู้บริหาร.....	3
ส่วนที่ 2 ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร.....	4
ส่วนที่ 3 การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม.....	7
ส่วนที่ 4 การจัดการทรัพย์สิน	8
ส่วนที่ 5 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ.....	10
ส่วนที่ 6 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ	12
ส่วนที่ 7 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย	22
ส่วนที่ 8 การควบคุมหน่วยงานภายนอกหรือผู้ใช้งานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ.....	23
ส่วนที่ 9 การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ ของ รพม.	25
ส่วนที่ 10 การใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์	28
ส่วนที่ 11 การใช้งานจดหมายอิเล็กทรอนิกส์	32
ส่วนที่ 12 การสำรองข้อมูลและการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์	33
ส่วนที่ 13 การตรวจสอบและประเมินความเสี่ยง.....	35
ส่วนที่ 14 การถ่ายโอน และแลกเปลี่ยนข้อมูลสารสนเทศ.....	38
ส่วนที่ 15 การควบคุมการเข้ารหัส	39
ส่วนที่ 16 การนำอุปกรณ์ส่วนตัวมาใช้งาน (Bring your own device).....	40
ส่วนที่ 17 การใช้บริการ Cloud (Cloud Services).....	49

เอกสารแนบท้ายประกาศ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ของ รฟม.

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

1. รฟม. หมายถึง การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
2. ฝทท. หมายถึง ฝ่ายเทคโนโลยีสารสนเทศ
3. ฝทบ. หมายถึง ฝ่ายทรัพยากรบุคคล
4. ผู้บริหารระดับสูงสุด หมายถึง ผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
5. ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของ รฟม.
6. ผู้ใช้งาน หมายถึง บุคคลที่ได้รับอนุญาตให้สามารถเข้าใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. เพื่อประโยชน์ในการดำเนินงานของ รฟม. ดังนี้
 - ผู้ใช้งานภายใน หมายถึง บุคลากรของ รฟม.
 - ผู้ใช้งานภายนอก หมายถึง บุคคลภายนอกที่ รฟม. อนุญาตให้เข้ามาใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. เช่น ที่ปรึกษา ผู้ปฏิบัติงานตามสัญญา หรือนิสิตนักศึกษาฝึกงาน เป็นต้น
7. ผู้ให้บริการ หมายถึง ผู้ที่สมัครใช้บริการระบบงานสารสนเทศของ รฟม. ผ่านเครือข่ายสาธารณะ (Internet)
8. หน่วยงานภายนอก หมายถึง องค์กรต่าง ๆ รวมถึงผู้รับจ้าง ซึ่ง รฟม. อนุญาตให้มีสิทธิ์ในการเข้าถึง หรือใช้ข้อมูลหรือสินทรัพย์ต่าง ๆ ของ รฟม. โดยจะได้รับสิทธิ์ในการใช้ระบบตามประเภทงานตามอำนาจและต้องรับผิดชอบในการรักษาความลับของข้อมูล
9. ผู้ดูแลระบบ หมายถึง พนักงานที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบสารสนเทศ และพนักงานของผู้รับจ้างที่รับผิดชอบติดตั้งหรือบำรุงรักษาระบบสารสนเทศให้ รฟม.
10. เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
11. มาตรฐาน หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย
12. ขั้นตอนปฏิบัติ หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานตามที่ได้กำหนดไว้ตามวัตถุประสงค์
13. แนวปฏิบัติ หมายถึง แนวทางที่ต้องปฏิบัติตามเพื่อให้สามารถบรรลุวัตถุประสงค์หรือเป้าหมายได้ง่ายขึ้น
14. ระบบเทคโนโลยีสารสนเทศ (Information technology system) หมายถึง ระบบงานของ รฟม. ที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายสื่อสารข้อมูลมาช่วยในการสร้างสารสนเทศที่ รฟม. สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุน การให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสารซึ่งมีองค์ประกอบ ได้แก่ ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลและสารสนเทศ เป็นต้น
15. ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด ที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์
16. ข้อมูลจราจรทางคอมพิวเตอร์ (Traffic log) หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เวลา วันที่ ปริมาณ ระยะเวลา หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น
17. สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งข้อมูลอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิกให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

18. ระบบคอมพิวเตอร์ (Computer system) หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่งหรือสิ่งอื่นใด และแนวปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
19. ระบบเครือข่ายสื่อสารข้อมูล (Network system) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของ รพม. เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น
20. สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน
21. ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) และความน่าเชื่อถือ (Reliability)
22. เหตุการณ์ด้านความมั่นคงปลอดภัย หมายถึง เหตุการณ์ที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย มาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อื่นไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
23. สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม
24. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้อีกได้
25. สินทรัพย์ (Assets) หมายถึง สินทรัพย์ด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารของ รพม. เช่น อุปกรณ์คอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีค่าลิขสิทธิ์ ข้อมูล ระบบข้อมูล ฯลฯ
26. จดหมายอิเล็กทรอนิกส์ (Email) หมายถึง ระบบที่บุคคลใช้ในการรับ - ส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ โดยข่าวสารที่ส่งนั้นจะถูกเก็บไว้ในตู้จดหมาย (Mail box) ที่กำหนดไว้สำหรับผู้ใช้งาน ผู้รับสามารถเปิดอ่าน พิมพ์ลงกระดาษ หรือจะลบทิ้งก็ได้
27. ชุดคำสั่งไม่พึงประสงค์ (Malicious code) หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
28. เครื่องคอมพิวเตอร์ หมายถึง เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ และเครื่องคอมพิวเตอร์แบบพกพา
29. อุปกรณ์เคลื่อนที่ (Mobile device) หมายถึง อุปกรณ์อิเล็กทรอนิกส์แบบพกพา ซึ่งมีความสามารถในการเชื่อมต่อกับอุปกรณ์อื่นเพื่อรับส่งข้อมูลผ่านระบบเครือข่ายโทรคมนาคมไร้สายหรือโดยอาศัยคลื่นแม่เหล็กไฟฟ้าเป็นสื่อกลาง เช่น Tablet, Smart Phone
30. ทรัพย์สินของ รพม. หมายถึง ครุภัณฑ์ รพม. และทรัพย์สินที่ไม่มีการขึ้นทะเบียนครุภัณฑ์ที่ รพม. จัดสรรงบประมาณเพื่อเป็นค่าใช้จ่ายให้ทั้งหมดหรือบางส่วน
31. อุปกรณ์ส่วนตัว หมายถึง อุปกรณ์ที่ไม่ใช่ทรัพย์สินของ รพม. ที่ผู้ใช้งานนำมาเชื่อมต่อกับระบบสารสนเทศของ รพม. เช่น เครื่องคอมพิวเตอร์ส่วนบุคคล (Personal computer) เครื่องคอมพิวเตอร์พกพา (Notebook) อุปกรณ์เคลื่อนที่ (Mobile device) Removable media หรืออุปกรณ์คอมพิวเตอร์ของโครงการรถไฟฟ้า เป็นต้น

ส่วนที่ 1

นโยบายการบริหารจัดการความมั่นคงปลอดภัยสำหรับผู้บริหาร

วัตถุประสงค์

- เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรมีความสอดคล้องกับมาตรฐานสากลและกฎหมายด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง

ผู้รับผิดชอบ

- ผู้บริหารสูงสุด

อ้างอิงมาตรฐาน: ISO/IEC 27001:2022

- มาตรการควบคุมด้านองค์กร (Organizational Controls)

แนวปฏิบัติ

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

ส่วนที่ 2

ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร

วัตถุประสงค์

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

ผู้รับผิดชอบ

- ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ ผู้อำนวยการฝ่ายทรัพยากรบุคคล ผู้อำนวยการฝ่าย/สำนัก/สำนักงาน ที่กำกับดูแลงานที่มีการว่าจ้างหน่วยงานภายนอก

อ้างอิงมาตรฐาน: ISO/IEC 27001:2022

- มาตรการควบคุมด้านองค์กร (Organizational Controls)
- มาตรการควบคุมด้านบุคลากร (People Controls)

แนวปฏิบัติ

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

ฝทบ. หรือฝ่าย/สำนัก/สำนักงาน ที่กำกับดูแลงานที่มีการว่าจ้างหน่วยงานภายนอก/บุคคลภายนอกต้องตรวจสอบคุณสมบัติของผู้สมัคร (ทั้งกรณีการจ้างเป็นพนักงาน ลูกจ้าง การว่าจ้างหน่วยงานภายนอก/บุคคลภายนอก เพื่อปฏิบัติงานให้ รพม. รวมทั้งนิสิตนักศึกษาฝึกงาน) โดยผู้สมัครต้องไม่เคยกระทำความผิดกฎหมาย ระเบียบ ข้อบังคับ หรือจริยธรรม รวมทั้งไม่มีประวัติในการบุกรุก แก๊ง ทำลาย หรือโจรกรรมข้อมูลในระบบเทคโนโลยีสารสนเทศมาก่อน และมีคุณสมบัติตามที่ รพม. กำหนด
 - 1.2 การกำหนดเงื่อนไขการจ้างงาน (Terms and Conditions of Employment) การว่าจ้างให้มีเงื่อนไขการจ้างงานให้ครอบคลุมในเรื่องดังต่อไปนี้
 - 1.2.1 กำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศอย่างเป็นลายลักษณ์อักษร (Information Security Roles and Responsibilities) แก่ผู้ใช้งาน โดยกำหนดให้สอดคล้องกับนโยบายความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของ รพม.
 - 1.2.2 กำหนดให้มีการลงนามในสัญญาว่าจะไม่เปิดเผยความลับของ รพม. (Non-Disclosure Agreement: NDA)
 - 1.2.3 ระบบเทคโนโลยีสารสนเทศที่สร้างหรือพัฒนาโดยผู้ใช้งานในระหว่างการทำงานถือเป็นสินทรัพย์ของ รพม.
 - 1.2.4 กำหนดความรับผิดชอบหรือบทลงโทษ หากผู้ใช้งานไม่ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รพม. รวมทั้ง กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

2. การสร้างความมั่นคงปลอดภัยในระหว่างการทำงาน (During Employment) เพื่อสร้างความตระหนักแก่ผู้ใช้งานเกี่ยวกับภัยที่เกี่ยวข้องกับการปฏิบัติงานสารสนเทศ รวมถึงให้ความรู้เพื่อให้สามารถป้องกันภัยดังกล่าวได้
 - 2.1 หน้าที่ในการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management Responsibilities)

ผู้บริหาร รพม. ทุกระดับชั้นมีหน้าที่สนับสนุนและส่งเสริมเรื่องดังต่อไปนี้ แก่ผู้ใช้งาน

 - 2.1.1 ประกาศนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ รพม. เป็นลายลักษณ์อักษรให้ทุกคนรับทราบและปฏิบัติตาม
 - 2.1.2 จูงใจให้ผู้ใช้งานปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ รพม.
 - 2.1.3 สร้างความตระหนักถึงความมั่นคงปลอดภัยด้านสารสนเทศที่เกี่ยวข้องกับหน้าที่ความรับผิดชอบของตนเองและของ รพม.
 - 2.2 การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่ผู้ใช้งาน (Information Security Awareness, Education and Training) การสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยอย่างสม่ำเสมอ
 - 2.2.1 ผู้ดูแลระบบต้องแจ้งเตือนภัยคุกคาม และช่องโหว่ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศแก่ผู้ใช้งานที่เกี่ยวข้อง นอกจากนี้ต้องแจ้งเตือนให้ผู้ใช้งานเพิ่มความระมัดระวังความเสี่ยงต่าง ๆ เช่น ไวรัสมัลแวร์ เทคนิคการหลอกล่อทางจิตวิทยา (Social Engineering) และช่องโหว่ทางเทคนิค เป็นต้น
 - 2.2.2 ฝทท. ต้องดำเนินการฝึกอบรม หรือประชาสัมพันธ์เพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศแก่ผู้ใช้งานเป็นประจำทุกปี
 - 2.2.3 ฝทท. ต้องแจ้งผู้ใช้งานให้ทราบ เมื่อมีการเปลี่ยนแปลงนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศของ รพม. รวมทั้งอธิบายผลกระทบจากการเปลี่ยนแปลงดังกล่าว
 - 2.3 การแจ้งเหตุการณ์ไม่ปกติ

ผู้ใช้งานต้องแจ้งเหตุการณ์ไม่ปกติด้านเทคโนโลยีสารสนเทศที่พบผ่านช่องทางที่ รพม. กำหนดโดยเร็วที่สุด
 - 2.4 การกำหนดบทลงโทษ
 - 2.4.1 ความรับผิดตามกฎหมาย

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ไม่ได้ก่อให้เกิดสิทธิทางกฎหมายที่ทำให้ผู้ใช้งานพ้นผิดแม้จะได้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ และผู้ใช้งานตกลงยินยอมที่จะไม่ดำเนินการใด ๆ ทางกฎหมายต่อ รพม. ซึ่งได้ปฏิบัติตามระเบียบนี้ แต่อย่างไรก็ตามหากผู้ใช้งานกระทำการละเมิดหรือกระทำผิดตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ อาจเป็นความผิดทางวินัยและเป็นเหตุให้ถูกลงโทษทางวินัยได้ รพม. ไม่มีส่วนรับผิดชอบต่อการละเมิดทรัพย์สินทางปัญญาที่เกิดจากการใช้ระบบคอมพิวเตอร์
 - 2.4.2 การพิจารณาโทษผู้กระทำความผิด

ผู้ใช้งานที่กระทำความผิด ฝทท. จะเพิกถอนสิทธิการใช้งานและอาจเป็นความผิดทางวินัย หรือความผิดตามกฎหมายที่เกี่ยวข้อง

 - 1) พนักงาน/ลูกจ้างที่ฝ่าฝืนหรือละเมิดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รพม. ต้องถูกลงโทษตามกระบวนการทางวินัยของ รพม. รวมถึงกฎหมายที่เกี่ยวข้อง
 - 2) หน่วยงานภายนอก/บุคคลภายนอกที่กระทำความผิด จะมีโทษตามที่ระบุไว้ในสัญญาหรือถูกเพิกถอนสิทธิการใช้งาน รวมถึงดำเนินการตามกฎหมายที่เกี่ยวข้อง

3. การสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน (Termination and Change of Employment)
เพื่อกำหนดหน้าที่ความรับผิดชอบเมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน ซึ่งรวมไปถึงการคืนทรัพย์สินและการถอดถอนสิทธิ์ในการเข้าถึง
 - 3.1 การแจ้งการสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน
 - 3.1.1 ฝทบ. ต้องแจ้งให้ ฝทท. ทราบทันทีหากพนักงานมีการลาออก โยกย้าย เกษียณ หรือเสียชีวิต เพื่อ ฝทท. จะได้ตรวจสอบและบริหารจัดการสิทธิ์ในการเข้าถึงระบบเทคโนโลยีสารสนเทศ
 - 3.1.2 ฝ่าย/สำนัก/สำนักงาน ที่กำกับดูแลงานที่มีการว่าจ้างหน่วยงานภายนอก/บุคคลภายนอก ต้องแจ้งให้ ฝทท. ทราบทันทีในกรณีที่ผู้รับจ้างภายนอกสิ้นสุดสัญญาจ้างหรือมีการยกเลิกสัญญาจ้าง เพื่อให้ ฝทท. ตรวจสอบการใช้งานระบบสารสนเทศและถอดถอนสิทธิ์ในการเข้าถึงระบบสารสนเทศของ รพม.
 - 3.2 การคืนทรัพย์สินของ รพม.
ผู้ดูแลระบบต้องตรวจสอบเพื่อเรียกคืนทรัพย์สินของ รพม. จากผู้ใช้งาน เมื่อการสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน
 - 3.3 การถอดถอนสิทธิ์ในการเข้าถึง
 - 3.3.1 ผู้ดูแลระบบต้องถอดถอนสิทธิ์ในการเข้าถึงของผู้ใช้งาน เมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน
 - 3.3.2 การถอดถอนสิทธิ์ในการเข้าถึงหมายถึงทางกายภาพ (Physical) และทางตรรกะ (Logical) เช่น กุญแจ บัตรแสดงตน บัตรประจำตัวผู้ใช้งาน และบัญชีผู้ใช้งาน เป็นต้น
 - 3.3.3 ในกรณีที่ผู้ใช้งานที่สิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน มีการใช้บัญชีผู้ใช้งานร่วมกัน (Shared User ID) กับผู้ใช้งานอื่น ผู้บังคับบัญชาต้องเปลี่ยนรหัสผ่านทันทีหลังจากสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน

ส่วนที่ 3

การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

วัตถุประสงค์

- เพื่อควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าถึงอาคารสถานที่ และพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area)

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้อำนวยการฝ่ายจัดซื้อและบริการ

อ้างอิงมาตรฐาน: ISO/IEC 27001:2022

- มาตรการควบคุมด้านกายภาพ (Physical Controls)

แนวปฏิบัติ

1. ผู้ดูแลระบบ ต้องออกแบบ และติดตั้งอุปกรณ์หรือระบบสนับสนุน (Facilities) เพื่อป้องกันความมั่นคงปลอดภัยด้านกายภาพ เช่น อุปกรณ์ดับเพลิง ระบบสำรองไฟฟ้า เครื่องกำเนิดไฟฟ้า ระบบปรับอากาศและควบคุมความชื้น ระบบเตือนภัยน้ำรั่ว และต้องมีการบำรุงรักษาอย่างสม่ำเสมอ
2. ผู้ดูแลระบบต้องติดตั้งอุปกรณ์สารสนเทศในตู้แร็ก (Rack) หรือสถานที่ที่มีความมั่นคงปลอดภัยและมีการปิดล็อก
3. ผู้ดูแลระบบ ต้องมีการป้องกันสายเคเบิลที่ใช้เพื่อการสื่อสารหรือสายไฟ มิให้มีการดักจับสัญญาณ (Interception) หรือมีความเสียหายเกิดขึ้น โดยจะต้องเดินสายเคเบิลผ่านท่อร้อยสายหรือทางเดินสายที่มีความมั่นคงปลอดภัยจากการเข้าถึง และไม่เดินสายผ่านพื้นที่ที่เข้าถึงได้อย่างสาธารณะ รวมทั้งสายเคเบิลสื่อสารและสายไฟฟ้าต้องแยกจากกันโดยมีระยะห่างที่เหมาะสม
4. การกำหนดบริเวณที่มีการรักษาความมั่นคงปลอดภัย
กำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม เพื่อเป็นการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้ โดยแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศออกเป็น
 - 4.1 พื้นที่ทำงาน (Working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน
 - 4.2 พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) หมายถึง พื้นที่ศูนย์ของข้อมูล (Data center)
5. การควบคุมการเข้าออก อาคาร สถานที่
 - 5.1 กำหนดสิทธิ์ของผู้ใช้งานและหน่วยงานภายนอกในการเข้าถึงสถานที่ โดยแบ่งแยกได้ ดังนี้
 - 5.1.1 ผู้ดูแลระบบต้องกำหนดสิทธิ์แก่ผู้ใช้งานที่มีสิทธิ์เข้า - ออก และกำหนดช่วงระยะเวลาที่มีสิทธิ์ในการเข้า - ออกแต่ละพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศอย่างชัดเจน
 - 5.1.2 เจ้าหน้าที่รักษาความปลอดภัย (รปภ.) จะต้องให้หน่วยงานภายนอก/บุคคลภายนอกแลกบัตรที่สามารถระบุตัวตนของบุคคลนั้น ๆ ก่อนเข้าถึงอาคารของ รพม. เช่น บัตรประจำตัวประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วบันทึกข้อมูลบัตรในสมุดบันทึกหรือระบบงานสารสนเทศ
 - 5.1.3 หน่วยงานภายนอก/บุคคลภายนอกที่มาติดต่อต้องติดบัตรผู้ติดต่อ (Visitor) ตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ใน รพม. และคืนบัตรผู้ติดต่อ (Visitor) ก่อนออกจากอาคารของ รพม.
 - 5.1.4 เจ้าหน้าที่รักษาความปลอดภัย (รปภ.) ต้องตรวจสอบผู้ติดต่อ อุปกรณ์ พร้อมลงเวลาออกที่สมุดบันทึกหรือระบบสารสนเทศให้ถูกต้อง
 - 5.2 ผู้ดูแลระบบ ต้องควบคุมการเข้า - ออกพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) ไม่ให้ผู้ไม่มีสิทธิ์เข้าถึงได้ โดยกำหนดพื้นที่การส่งมอบสินค้าและพื้นที่การเตรียมหรือประกอบอุปกรณ์สารสนเทศ (Unpack Area) ก่อนนำเข้าพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) และต้องควบคุมการเข้า - ออก เพื่อหลีกเลี่ยงการเข้าถึงระบบสารสนเทศและข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต โดยปฏิบัติตามขั้นตอนที่ รพม. กำหนด

ส่วนที่ 4

การจัดการทรัพย์สิน

วัตถุประสงค์

- เพื่อบริหารจัดการทรัพย์สินสารสนเทศ ตั้งแต่การจัดหา การใช้งาน จนถึงการยกเลิกใช้งาน โดยมีการระบุทรัพย์สินขององค์กรและกำหนดหน้าที่ความรับผิดชอบในการปกป้องทรัพย์สินสารสนเทศอย่างเหมาะสม

ผู้รับผิดชอบ

- ผู้บังคับบัญชา
- ผู้ดูแลระบบ
- เจ้าของข้อมูล
- ผู้ใช้งาน

อ้างอิงมาตรฐาน: ISO/IEC 27001:2022

- มาตรการควบคุมด้านองค์กร (Organizational Controls)
- มาตรการควบคุมด้านกายภาพ (Physical Controls)
- มาตรการควบคุมด้านเทคโนโลยี (Technological Controls)

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 เจ้าของข้อมูลต้องมีการเข้ารหัสข้อมูลที่อ่อนไหว (Sensitive Data) ของ รฟม. ที่จัดเก็บอยู่ในสื่อบันทึกแบบถอดได้
 - 3.3 เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูลตามขั้นตอนที่ รฟม. กำหนด โดยไม่สามารถกู้คืนข้อมูลกลับมาได้อีกก่อนจะกำจัดอุปกรณ์ดังกล่าวหรือก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อเพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลที่สำคัญได้ 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

- 3.4 เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ใช้งาน ต้องมีการป้องกันสื่อบันทึกข้อมูลที่จัดเก็บข้อมูลสารสนเทศ ในกรณีที่มีการเคลื่อนย้ายเพื่อป้องกันการเข้าถึงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต ถูกนำไปใช้งานผิดวัตถุประสงค์ รวมถึงป้องกันสื่อบันทึกข้อมูลไม่ให้เกิดความเสียหาย โดยรักษาความปลอดภัยสารสนเทศตามขั้นตอนที่ รพม. กำหนด
4. การบริหารจัดการค่าคอนฟิกูเรชัน (Configuration Management)
- 4.1 ผู้บังคับบัญชาต้องกำหนดให้มีแนวทางการบริหารจัดการค่าคอนฟิกูเรชัน (Configuration Management)
- 4.2 ผู้ดูแลระบบต้องกำหนดค่า Minimum Baseline Standard เพื่อเป็นมาตรฐานในการการตั้งค่าของระบบปฏิบัติการ ระบบฐานข้อมูล ระบบงาน และอุปกรณ์เครือข่ายสื่อสารต่าง ๆ อย่างเป็นลายลักษณ์อักษร และต้องการทบทวนปรับปรุงให้เป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง
- 4.3 ผู้ดูแลระบบต้องควบคุมการเปลี่ยนแปลงการตั้งค่าของระบบปฏิบัติการ ระบบฐานข้อมูล ระบบงาน และอุปกรณ์เครือข่ายสื่อสารต่าง ๆ ตามขั้นตอนปฏิบัติการควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบที่ รพม. กำหนด
- 4.4 ผู้ดูแลระบบต้องควบคุมเวอร์ชันของค่าคอนฟิกูเรชัน (System Configuration Version Control)
- 4.5 ผู้ดูแลระบบต้องมีการสอบทานค่าคอนฟิกูเรชันของระบบปฏิบัติการ ระบบฐานข้อมูล ระบบงาน และอุปกรณ์เครือข่ายสื่อสารต่าง ๆ อย่างน้อยปีละ 1 ครั้ง

ส่วนที่ 5

การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

วัตถุประสงค์

- เพื่อควบคุมการจัดหา พัฒนา และบำรุงรักษาระบบสารสนเทศ ให้มีการกำหนดมาตรการการรักษาความมั่นคงปลอดภัย เพื่อป้องกันความผิดพลาด สูญหาย และการเปลี่ยนแปลงแก้ไขระบบ

ผู้รับผิดชอบ

- ผู้บังคับบัญชา
- ผู้ดูแลระบบ

อ้างอิงมาตรฐาน: ISO/IEC 27001:2022

- มาตรการควบคุมด้านองค์กร (Organizational Controls)
- มาตรการควบคุมด้านเทคโนโลยี (Technological Controls)

แนวปฏิบัติ

1. ผู้บังคับบัญชา ต้องควบคุมให้มีการกำหนดข้อตกลงและความรับผิดชอบที่เกี่ยวข้องกับความเสถียรด้านความมั่นคงปลอดภัยสารสนเทศลงในสัญญากับผู้ให้บริการภายนอก โดยให้ครอบคลุมรวมถึงผู้รับจ้างช่วงด้วย
2. ผู้บังคับบัญชาต้องควบคุมให้มีการข้อตกลง (Sign Off) ก่อนเริ่มใช้งานระบบจริง (Production) หรือก่อนเริ่ม Go Live
3. ผู้ดูแลระบบ ต้องจัดทำข้อกำหนดโดยระบุถึงการควบคุมความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร เช่น วิธีการแบบปลอดภัยในการพัฒนาโปรแกรมตามมาตรฐาน OWASP (Open Web Application Security Project) Top 10 หรือมาตรฐาน CWE (Common Weakness Enumeration) Top 25 หรือมาตรฐานที่ยอมรับในสากล
4. ผู้ดูแลระบบต้องออกแบบโครงสร้างการจัดวางระบบงานและเสนอผู้บังคับบัญชาเห็นชอบก่อนเริ่ม Go Live
5. ผู้ดูแลระบบ ต้องมีการออกแบบระบบเพื่อตรวจสอบข้อมูลที่จะรับเข้าสู่แอปพลิเคชัน ข้อมูลที่เกิดจากการประมวลผล และข้อมูลที่อยู่ระหว่างการประมวลผล เพื่อตรวจหาและป้องกันความไม่ถูกต้องที่เกิดขึ้นกับข้อมูล เช่น หน่วยความจำล้น (Buffer Overflows) การใช้ตัวแปรผิดประเภท และต้องมีมาตรการป้องกันหรือควบคุมความล้มเหลวระหว่างการประมวลผล (Rollback)
6. ผู้ดูแลระบบต้องมีการควบคุมการเข้าถึงและควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบตามขั้นตอนที่ รพม. กำหนดเพื่อควบคุมผลกระทบที่เกิดขึ้น
7. ผู้ดูแลระบบต้องจำกัดให้มีการเปลี่ยนแปลงใด ๆ ต่อซอฟต์แวร์ที่ใช้งาน (Software Package) โดยเปลี่ยนแปลงเฉพาะที่จำเป็นเท่านั้น และควบคุมทุก ๆ การเปลี่ยนแปลงอย่างเข้มงวดตามขั้นตอนที่ รพม. กำหนด
8. ผู้ดูแลระบบต้องจำกัดการเข้าถึง Source Code ให้เข้าถึงได้เฉพาะผู้ที่มีสิทธิ์เท่านั้น
9. ผู้ดูแลระบบต้องจัดทำ Source Code Review เพื่อหาข้อผิดพลาดหรือสิ่งผิดปกติและปรับปรุง Source Code ให้มีคุณภาพ
10. ผู้ดูแลระบบต้องควบคุมการจัดส่ง Source Code ผ่านช่องทางที่มั่นคงปลอดภัยและเป็นช่องทางที่ รพม. กำหนดให้ใช้งานเท่านั้น
11. ผู้ดูแลระบบต้องปิดบังข้อมูลส่วนบุคคล (Data Masking) ที่จัดเก็บอยู่ในระบบงานสารสนเทศด้วยวิธีการที่เหมาะสม
12. ผู้ดูแลระบบต้องแสดงข้อมูลของผู้ใช้งานอย่างรัดกุม เช่น การปิดบังข้อมูลสำคัญของผู้ใช้งาน (Sensitive Data Masking) เป็นต้น

13. กรณีของแอปพลิเคชันที่ใช้งานผ่านอุปกรณ์เคลื่อนที่ (Mobile device) ให้ผู้ดูแลระบบดำเนินการ ดังนี้
 - 13.1 ปิดบังหน้าจอเมื่อย่อแอปพลิเคชัน (Application Blurring) เพื่อลดความเสี่ยงที่ข้อมูลสำคัญของผู้ใช้งานจะรั่วไหล
 - 13.2 ขอสสิทธ์เข้าถึงทรัพยากรหรือบริการโดยแอปพลิเคชัน (Application Permission) บนอุปกรณ์เคลื่อนที่ของผู้ใช้งานเท่าที่จำเป็น และมีกระบวนการทบทวนการขอสสิทธ์เป็นประจำเพื่อป้องกันการละเมิดสิทธ์ความเป็นส่วนตัวของผู้ใช้งาน
14. ผู้ดูแลระบบต้องควบคุมข้อมูลที่นำมาใช้ในการทดสอบระบบ (Test Data) อย่างเหมาะสม โดยไม่นำข้อมูลจริงมาทดสอบ กรณีจำเป็นต้องใช้ข้อมูลจริงต้องได้รับอนุญาตข้อมูลจากเจ้าของก่อนนำมาใช้งาน และทำลายข้อมูลอย่างเหมาะสมตามขั้นตอนที่ รพม. กำหนด
15. ผู้ดูแลระบบต้องแยกระบบสารสนเทศสำหรับการพัฒนา ทดสอบ และใช้งานจริงออกจากกันเพื่อลดความเสี่ยงที่เกิดจากการเปลี่ยนแปลงระบบสารสนเทศโดยไม่ได้รับอนุญาต และต้องมีการกำหนดสิทธ์การเข้าถึงระบบสารสนเทศที่พัฒนา ทดสอบ หรือใช้งานจริง ทั้งระบบสารสนเทศใหม่ และการปรับปรุงแก้ไขระบบสารสนเทศเดิม
16. ผู้ดูแลระบบต้องมีการกำหนดขั้นตอนการทดสอบระบบสารสนเทศก่อนนำไปใช้งานจริง ทั้งในกรณีปรับปรุงระบบสารสนเทศเดิมและการพัฒนาระบบสารสนเทศใหม่
17. ผู้ดูแลระบบต้องติดตั้งซอฟต์แวร์บนระบบสารสนเทศที่ให้บริการ (Production) ตามขั้นตอนที่ รพม. กำหนด และจำกัดสิทธ์การติดตั้งซอฟต์แวร์เพื่อให้ระบบสารสนเทศต่าง ๆ มีความถูกต้องครบถ้วนและน่าเชื่อถือ
18. ผู้ดูแลระบบต้องนำซอฟต์แวร์ที่ไม่ละเมิดสิทธ์มาติดตั้งบนระบบสารสนเทศที่ให้บริการ (Production)
19. ผู้ดูแลระบบต้องกำกับดูแลให้ผู้รับจ้างปฏิบัติตามสัญญาหรือข้อตกลงการให้บริการที่ระบุไว้ โดยครอบคลุมถึงด้านความมั่นคงปลอดภัยสารสนเทศ และการปฏิบัติตามขั้นตอนที่เกี่ยวข้องต่าง ๆ ที่ รพม. กำหนดไว้
20. ผู้ดูแลระบบ ต้องติดตาม ตรวจสอบรายงาน หรือบันทึกการให้บริการของบุคคล/หน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามสัญญาว่าจ้างอย่างสม่ำเสมอ
21. ผู้ดูแลระบบ ต้องดูแลให้ทรัพย์สินสารสนเทศได้รับการบำรุงรักษาและซ่อมแซมตามความต้องการ รวมทั้งต้องมีการบันทึกประวัติการทำงานผิดปกติ การบำรุงรักษา และการซ่อมแซมอุปกรณ์นั้น ๆ อย่างสม่ำเสมอ
22. ผู้ดูแลระบบจะต้องปิดช่องโหว่ของระบบสารสนเทศที่มีระดับความรุนแรงในระดับวิกฤติ (Critical) และระดับสูง (High) ทั้งหมดก่อนนำไปใช้งานจริง (Production) หรือก่อนเริ่ม Go Live โดยเฉพาะระบบที่ให้บริการผ่านเครือข่ายอินเทอร์เน็ต (Internet Facing) และระบบที่มีความสำคัญต่อการดำเนินงานของ รพม.
23. ผู้ดูแลระบบต้องพิจารณาเลือกใช้ Version ของ Software ดังนี้
 - 23.1 กรณีนำ Software เดิมมาใช้ในการจัดหาหรือพัฒนาระบบ จะต้องนำผลการตรวจสอบช่องโหว่และผลการทดสอบเจาะระบบมาประกอบการพิจารณาคัดเลือกเวอร์ชันของ Software ด้วย เพื่อป้องกันไม่ให้เกิดช่องโหว่เดิม รวมถึงเพื่อลดภาระงานในการปิดช่องโหว่เดิมซ้ำ
 - 23.2 กรณีเป็น Software ที่ไม่เคยนำมาใช้งานให้เลือกใช้ Software เวอร์ชันล่าสุด

ส่วนที่ 6

การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

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

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- เจ้าของข้อมูล
- ผู้ใช้งาน

อ้างอิงมาตรฐาน: ISO/IEC 27001:2022

- มาตรการควบคุมด้านองค์กร (Organizational Controls)
- มาตรการควบคุมด้านเทคโนโลยี (Technological Controls)

แนวปฏิบัติ

1. การควบคุมการเข้าถึงระบบสารสนเทศ (Access Control)
 - 1.1 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องร่วมกันกำหนดสิทธิ์ในการเข้าถึงระบบสารสนเทศ (Authorization Matrix) ที่เหมาะสมและสอดคล้องกับหน้าที่ความรับผิดชอบของผู้ใช้งาน และทบทวนเมื่อมีการเปลี่ยนแปลง
 - 1.2 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องร่วมกันกำหนดระดับการอนุมัติ (Authorization Level) การเข้าถึงระบบเทคโนโลยีสารสนเทศ
 - 1.3 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจัดให้มีการแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties) ในการเข้าถึงระบบเทคโนโลยีสารสนเทศอย่างเหมาะสม เช่น มีการแบ่งแยกหน้าที่ระหว่างการแจ้งความประสงค์ การเข้าถึงและการอนุมัติการเข้าถึง เป็นต้น
 - 1.4 กรณีของแอปพลิเคชันที่ใช้งานผ่านอุปกรณ์เคลื่อนที่ (Mobile device) ผู้ดูแลระบบต้องปฏิบัติ ดังนี้
 - 1.4.1 ไม่อนุญาตให้อุปกรณ์เคลื่อนที่ที่ใช้ระบบปฏิบัติการล้าสมัย (Obsolete Operating System) ใช้งานแอปพลิเคชัน หรือหากอนุญาตให้ใช้บริการได้ควรมีมาตรการรองรับเพื่อลดความเสี่ยงที่ รพม. จะได้รับรวมถึงลดผลกระทบต่อผู้ใช้งานตามความเหมาะสม เช่น การเพิ่มมาตรการยืนยันตัวตน เป็นต้น
 - 1.4.2 ไม่อนุญาตให้อุปกรณ์ที่มีการปรับแต่งการเข้าถึงระบบปฏิบัติการ (Rooted/Jailbroken) ใช้งานแอปพลิเคชัน เพื่อลดความเสี่ยงที่ผู้ไม่ประสงค์ดีสามารถเข้าถึงข้อมูลสำคัญของผู้ใช้งานและละเมิดหรือหลีกเลี่ยงมาตรการการรักษาความมั่นคงปลอดภัยที่ รพม. กำหนดไว้
 - 1.4.3 ไม่อนุญาตให้ผู้ใช้งานใช้แอปพลิเคชันเวอร์ชันต่ำกว่าที่ รพม. กำหนด เพื่อให้แอปพลิเคชันมีการรักษาความมั่นคงปลอดภัยเป็นไปตามมาตรฐานของ รพม.
 - 1.5 ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ใช้งาน ต้องปฏิบัติ ดังนี้

 - 1.5.1 แบ่งประเภทข้อมูล ดังนี้
 - 1) ข้อมูลและสารสนเทศสำหรับสนับสนุนการตัดสินใจของผู้บริหาร ได้แก่ ข้อมูลสารสนเทศที่มีความสำคัญหรือมีความจำเป็นเร่งด่วนที่ต้องติดตามอย่างใกล้ชิดเพื่อประกอบการตัดสินใจเชิงนโยบาย กำหนดนโยบาย และการวางแผนของผู้บริหารระดับสูง

- 2) ข้อมูลและสารสนเทศสนับสนุนเชิงยุทธศาสตร์ (Strategy Data) ได้แก่ ข้อมูลและสารสนเทศเชิงวิชาการเพื่อสนับสนุนการดำเนินงานตามพันธกิจและยุทธศาสตร์ของ รพม. ให้บรรลุเป้าหมาย รวมทั้งข้อมูลที่เผยแพร่แก่ผู้รับบริการภายนอก
 - 3) ข้อมูลและสารสนเทศที่สนับสนุนการปฏิบัติงานประจำ (Operation Data) ได้แก่ ข้อมูลที่สนับสนุนการทำงานทั่วไปของ รพม.
- 1.5.2 จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น 3 ระดับ คือ
- 1) ข้อมูลที่มีระดับความสำคัญมาก หมายถึง ข้อมูลที่ใช้สำหรับสนับสนุนการตัดสินใจของผู้บริหาร
 - 2) ข้อมูลที่มีระดับความสำคัญปานกลาง หมายถึง ข้อมูลที่ใช้ปฏิบัติงานเฉพาะกลุ่มงาน แผนก กอง หรือฝ่าย/สำนัก/สำนักงาน ภายในองค์กร
 - 3) ข้อมูลที่มีระดับความสำคัญน้อย หมายถึง ข้อมูลที่พนักงาน/ลูกจ้างภายใน รพม. สามารถเข้าถึงร่วมกันได้หรือสามารถเผยแพร่ได้
- 1.5.3 จัดแบ่งลำดับชั้นความลับของข้อมูลตามที่ รพม. กำหนด
- 1.5.4 จัดแบ่งระดับชั้นการเข้าถึง
- 1) ระดับชั้นสำหรับผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และภารกิจที่ได้รับมอบหมาย
 - 2) ระดับชั้นสำหรับผู้ปฏิบัติงานทั่วไป เข้าถึงข้อมูลที่ได้รับมอบหมายตามอำนาจหน้าที่
 - 3) ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย มีสิทธิ์ในการบริหารจัดการระบบและเข้าถึงข้อมูลที่ได้รับมอบหมายตามอำนาจหน้าที่
- 1.6 เจ้าของข้อมูลและผู้ดูแลระบบต้องกำหนดเวลาการเข้าถึงระบบสารสนเทศ
- 1.7 ผู้ดูแลระบบต้องจำกัดช่องทางการเข้าถึงระบบเทคโนโลยีสารสนเทศตามช่องทาง ดังนี้
- 1) เครือข่ายภายในของ รพม.
 - 2) เครือข่ายภายนอก รพม.
 - 3) เครือข่ายอื่นที่จัดไว้ให้ เช่น ระบบเครือข่ายสื่อสารข้อมูล GIN
- 1.8 ผู้ดูแลระบบต้องกำกับดูแล Default Permission ของไฟล์ (File) และ โฟลเดอร์ (Folder) ที่สร้างขึ้นให้มีการจำกัดสิทธิ์ในการเข้าถึง
- 1.9 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องพิจารณาข้อกำหนดต่าง ๆ ที่มีผลทางกฎหมายซึ่งเกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศของ รพม. เช่น พระราชบัญญัติ ข้อกำหนดทางกฎหมาย ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่น ๆ เป็นต้น เพื่อกำหนดสิทธิ์การเข้าถึงสารสนเทศและระบบเทคโนโลยีสารสนเทศของ รพม.
- 1.10 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องมีการสอบทานสิทธิ์ในการเข้าถึงระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ พร้อมทั้งเพิกถอนสิทธิ์เมื่อพบเห็นสิทธิ์ที่ไม่ถูกต้องตามสิทธิ์ในการเข้าถึง (Authorization Matrix)
2. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)
- ให้มีการควบคุมการลงทะเบียนผู้ใช้งาน การบริหารจัดการรหัสผ่าน การบริหารจัดการสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศ และการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน
- 2.1 การลงทะเบียนผู้ใช้งาน (User Registration)
- 2.1.1 ผู้ดูแลระบบต้องบริหารจัดการและควบคุมบัญชีชื่อผู้ใช้งาน (Username) มิให้มีการใช้งานบัญชีชื่อผู้ใช้งานซ้ำกัน ทั้งนี้ ในส่วนของพนักงาน/ลูกจ้าง รพม. ให้กำหนดชื่อผู้ใช้งาน (Username) ตามมาตรฐานจดหมายอิเล็กทรอนิกส์ (Email) 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 และไม่ซ้ำกับรหัสผ่านเดิม 3 ครั้งก่อนหน้า
 - 2) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทุก ๆ 6 เดือน และไม่ซ้ำกับรหัสผ่านเดิม 3 ครั้งก่อนหน้า
 - 3) ผู้ใช้งานเชิงระบบ (System account) ให้พิจารณาเปลี่ยนรหัสผ่านตามความเหมาะสม
- 2.2.6 ผู้ดูแลระบบต้องกำหนดให้มีการเข้ารหัสข้อมูลรหัสผ่านในระบบ
- 2.2.7 ผู้ดูแลระบบต้องจัดให้มีการควบคุมรหัสผ่านอย่างเข้มงวด
- 2.2.8 ผู้ดูแลระบบต้องจัดส่งบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ด้วยวิธีการที่ปลอดภัย
- 2.2.9 ผู้ดูแลระบบต้องควบคุมดูแลระบบปฏิบัติการ ระบบฐานข้อมูล และระบบงานสารสนเทศ (Application) ที่จัดเก็บบัญชีผู้ใช้งานและรหัสผ่านอย่างเข้มงวด โดยให้เข้าถึงได้เฉพาะผู้ดูแลระบบที่ได้รับอนุญาตเท่านั้น
- 2.2.10 ผู้ดูแลระบบต้องกำหนดวิธีการหรือกระบวนการยืนยันตัวตนที่ปลอดภัย เช่น กรณีที่ลืมรหัสผ่าน
- 2.2.11 ผู้ดูแลระบบต้องกำหนดให้ผู้ให้บริการ ใช้รหัสผ่านอย่างมั่นคงปลอดภัย ดังนี้

กรณีแอปพลิเคชันทั่วไป

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

กรณีแอปพลิเคชันที่ใช้งานผ่านอุปกรณ์เคลื่อนที่ (Mobile device)

- 1) กำหนดรหัสผ่านโดยใช้ PIN code หรือรหัสผ่านที่ซับซ้อน (PIN/Password Complexity) โดยกรณี PIN Code ต้องใช้รหัสผ่าน 6 หลักขึ้นไป
 - 2) ไม่บังคับให้เปลี่ยนรหัสผ่าน ทั้งนี้ขึ้นอยู่กับความสมัครใจในการเปลี่ยนรหัสผ่าน และระบบต้องรองรับการเปลี่ยนรหัสผ่านในกรณีต่าง ๆ ด้วยวิธีการที่ปลอดภัย
- 2.2.12 ผู้ดูแลระบบและผู้ใช้งานต้องใช้รหัสผ่านอย่างปลอดภัย ดังนี้
- 1) ต้องกำหนดรหัสผ่านที่ไม่สามารถคาดเดาได้ง่าย เช่น คำที่อยู่ในพจนานุกรม “qwerty” “abcde” “12345” ชื่อ-นามสกุล วันเดือนปีเกิด ที่อยู่ หรือเบอร์โทรศัพท์ เป็นต้น
 - 2) ต้องไม่ใช้งานรหัสผ่านโดยการเข้าใช้งานโดยอัตโนมัติ ได้แก่ การกำหนดค่า “Remember Password” เป็นต้น

- 3) ต้องเก็บรหัสผ่านไว้เป็นความลับเฉพาะบุคคล ไม่เปิดเผยให้ผู้อื่นรับทราบ และไม่พิมพ์รหัสผ่านในลักษณะเปิดเผย เช่น พิมพ์รหัสผ่านต่อหน้าผู้ใช้งานคนอื่น เป็นต้น
- 4) ต้องไม่ใช้บัญชีชื่อผู้ใช้งานและรหัสผ่านร่วมกันกับผู้อื่น แม้ว่าบัญชีชื่อผู้ใช้งานจะได้รับการอนุญาตจากเจ้าของชื่อผู้ใช้งานบุคคลนั้นก็ตาม
- 5) ต้องเปลี่ยนแปลงรหัสผ่านเมื่อมีการแจ้งเตือนจากระบบ หรือสงสัยว่ารหัสผ่านลวงรู้โดยบุคคลอื่น

2.3 การบริหารจัดการสิทธิ์ (Privilege Management)

- 2.3.1 ผู้บังคับบัญชาต้องกำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียน การเพิ่มสิทธิ์ การเพิกถอนสิทธิ์ การเปลี่ยนแปลงสิทธิ์ และการทบทวนสิทธิ์ของผู้ใช้งานอย่างเป็นลายลักษณ์อักษร
- 2.3.2 กำหนดสิทธิ์ที่เหมาะสมกับผู้ใช้งานตามความจำเป็นและสอดคล้องกับหน้าที่ความรับผิดชอบและจัดเก็บประวัติ (Log) การลงทะเบียน การเพิ่มสิทธิ์ 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 ต้องจำกัดระยะเวลาการใช้งานระบบเทคโนโลยีสารสนเทศของรพม. แก่หน่วยงานภายนอกที่เข้ามาปฏิบัติงานร่วมกับ รพม.
- 2.3.7 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจัดให้มีการถอดถอนสิทธิ์หรือเปลี่ยนแปลงสิทธิ์การเข้าถึงทันทีเมื่อผู้ใช้งานเกษียณ เปลี่ยนแปลงหน้าที่ความรับผิดชอบ เปลี่ยนแปลงการจ้างงาน หรือไม่มีความจำเป็นในการใช้งานระบบเทคโนโลยีสารสนเทศ
- 2.3.8 ผู้ดูแลระบบต้องลบหรือระงับการใช้งานสิทธิ์ของผู้ใช้งานที่มากับระบบ (Default User) ในกรณีที่มีความจำเป็นต้องใช้งานต้องกำหนดรหัสผ่านอย่างมั่นคงปลอดภัย

2.4 การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

- 2.4.1 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องมีการสอบทานสิทธิ์การเข้าถึงของผู้ใช้งานระบบเมื่อ รพม. มีการเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศหรือโครงสร้างองค์กร
- 2.4.2 ผู้ดูแลระบบ ต้องมีการสอบทานและระงับการใช้งานบัญชีผู้ใช้งานที่ไม่ได้ใช้งานนานเกิน 180 วัน หากผู้ใช้งานต้องการกลับมาใช้งานจะต้องยืนยันตัวตนให้ ผทท. ทราบ ทั้งนี้ ระยะเวลาที่ไม่ได้ใช้งานของบัญชีผู้ใช้งานอาจจะขึ้นอยู่กับแต่ละระบบสารสนเทศ

3. การป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล และการควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ไม่ปลอดภัย
 - 3.1 การป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล (Unattended User Equipment)
 - 3.1.1 ผู้ดูแลระบบต้องจัดให้มีมาตรการสำหรับป้องกันระบบคอมพิวเตอร์ ระบบเครือข่ายสื่อสารข้อมูล และระบบเทคโนโลยีสารสนเทศ โดยการกำหนดค่าของระบบ (Configuration) ให้มีการล็อกหน้าจอสำหรับอุปกรณ์ที่ไม่มีพนักงานดูแล หรือล็อกอุปกรณ์อยู่เสมอ
 - 3.1.2 ผู้ใช้งานและหน่วยงานภายนอก/บุคคลภายนอก ต้องล็อกหน้าจออัตโนมัติเมื่อไม่มีการใช้งานระบบเทคโนโลยีสารสนเทศของ รพม. ตามระยะเวลาที่กำหนด โดยต้องพักหน้าจอ (Screen Saver) อัตโนมัติหลังจากที่ไม่มีการใช้งานคอมพิวเตอร์เป็นระยะเวลานานกว่า 15 นาที ผู้ใช้งานและหน่วยงานภายนอก/บุคคลภายนอกจะใช้งานต่อได้เมื่อมีการใส่รหัสผ่านที่ถูกต้อง
 - 3.1.3 ผู้ใช้งานต้อง Logout 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 (Logout) ทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่ผู้ดูแล
 - 3.2.3 ผู้ใช้งานต้องจัดเก็บข้อมูลสำคัญแยกต่างหาก และป้องกันให้มีความปลอดภัยอย่างพอเพียง
 - 3.2.4 ผู้ใช้งานต้องนำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ
4. การควบคุมการเข้าถึงเครือข่าย (Network Access Control)
 ให้มีการควบคุมการใช้งานบริการเครือข่าย การควบคุมการพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอก รพม. การควบคุมการพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย การป้องกันพอร์ต (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ การแบ่งแยกเครือข่าย (Segregation in networks) อย่างเหมาะสม การควบคุมการเชื่อมต่อทางเครือข่าย และการควบคุมการกำหนดเส้นทางบนเครือข่าย
 - 4.1 การใช้งานบริการเครือข่าย (Use of Network Services)
 - 4.1.1 ผู้ดูแลระบบต้องควบคุมการเผยแพร่แผนผังระบบเครือข่ายสื่อสารข้อมูล (Network Diagram) รวมถึงโครงสร้าง IP Address ชื่อระบบ และชื่ออุปกรณ์สารสนเทศแก่ผู้ที่ไม่ได้รับอนุญาตหรือหน่วยงานภายนอก/บุคคลภายนอก
 - 4.1.2 ผู้ดูแลระบบต้องควบคุมการใช้งานระบบเครือข่ายสื่อสารข้อมูล เพื่อป้องกันการเข้าถึงระบบเครือข่ายสื่อสารข้อมูลและบริการของระบบเครือข่ายสื่อสารข้อมูลโดยไม่ได้รับอนุญาต
 - 4.1.3 ผู้ดูแลระบบต้องควบคุมการเชื่อมต่อเครือข่ายภายนอก เพื่อใช้งานอินเทอร์เน็ต ซึ่งอาจเป็นช่องทางให้หน่วยงานภายนอก/บุคคลภายนอกเข้าถึงสารสนเทศหรือระบบเทคโนโลยีสารสนเทศของ รพม. โดยมีได้รับอนุญาต
 - 4.1.4 ผู้ใช้งานต้องแจ้งความประสงค์ในการขอใช้งานบริการเครือข่ายแก่ ฝทท. และสามารถใช้บริการเครือข่ายได้หลังจากได้รับการอนุมัติจาก ฝทท. แล้ว
 - 4.1.5 ผู้ใช้งาน ต้องไม่ใช้ระบบเครือข่ายสื่อสารข้อมูลเพื่อเป็นช่องทางในการเจาะระบบ (Hacking) หรือการสแกนช่องโหว่ของระบบโดยไม่ได้รับอนุญาต
 - 4.2 การพิสูจน์ตัวตนของผู้ใช้งานที่อยู่ภายนอก รพม. (User Authentication for External Connections)
 ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนผ่านระบบ Active Directory ของ รพม. ก่อนอนุญาตให้ผู้ใช้งานที่อยู่ภายนอก รพม. เข้าใช้งานเครือข่ายและระบบสารสนเทศของ รพม.

- 4.3 การพิสูจน์ตัวตนของอุปกรณ์ในระบบเครือข่ายสื่อสารข้อมูล (Equipment Identification in Networks)
ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนของอุปกรณ์ในระบบเครือข่ายสื่อสารข้อมูล ได้แก่ การตรวจสอบ MAC Address
- 4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection)
ผู้ดูแลระบบต้องระงับบริการและพอร์ต (Port) ที่ไม่มีความจำเป็นต้องใช้บนเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่าย
- 4.5 ผู้ดูแลระบบต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/ Intrusion Detection System) ของระบบเครือข่าย
- 4.6 การแบ่งแยกเครือข่าย (Segregation in Networks)
 - 4.6.1 ผู้ดูแลระบบต้องจัดให้มีการแบ่งแยกเครือข่ายตามกลุ่มของผู้ใช้งาน หรือกลุ่มของระบบเทคโนโลยีสารสนเทศ เพื่อควบคุมการใช้งานในแต่ละเครือข่ายอย่างเหมาะสม โดยพิจารณาจากความต้องการในการเข้าถึงข้อมูล ระดับความสำคัญของข้อมูล รวมถึงการพิจารณาด้านราคา ประสิทธิภาพ และผลกระทบทางด้านความปลอดภัยดังต่อไปนี้
 - 1) เครือข่ายที่อนุญาตให้เข้าถึงจากภายนอกและเครือข่ายที่ใช้ภายใน รพม.
 - 2) เครือข่ายแอปพลิเคชัน (Application) ที่มีความสำคัญกับเครือข่ายอื่น ๆ ที่มีความสำคัญน้อยกว่า
 - 3) เครือข่ายสำหรับเครื่องให้บริการ (Server Farm) กับเครือข่ายของผู้ใช้งาน ควรมีการติดตั้งอุปกรณ์ที่สามารถแบ่งแยกเครือข่ายได้ เช่น Firewall หรือ Switch ที่สามารถแบ่ง VLAN ได้ เป็นต้น
 - 4.6.2 ผู้ดูแลระบบจะกำหนดเส้นทางบนเครือข่ายที่เข้มงวด เพื่อจำกัดการเข้าถึงระยะไกลไปเฉพาะเครือข่ายที่กำหนดเท่านั้น
 - 4.6.3 ผู้ดูแลระบบต้องตั้งค่า (Configuration) อุปกรณ์เครือข่าย เช่น Firewall หรือ Router มิให้สามารถบริหารจัดการจากภายนอกเครือข่ายได้ เว้นแต่ในกรณีฉุกเฉินซึ่งต้องได้รับการอนุญาตจากผู้ดูแลระบบเท่านั้น
- 4.7 การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)
 - 4.7.1 ผู้ดูแลระบบต้องจำกัดการใช้งานเครือข่ายของผู้ใช้งานในการเชื่อมต่อกับเครือข่ายของ รพม. เช่น Router หรือ Firewall เป็นต้น พร้อมทั้งติดตั้งระบบควบคุมเพื่อกลั่นกรองข้อมูลที่รับ - ส่ง เช่น Web Filtering, Email Filtering เป็นต้น เพื่อให้การเชื่อมต่อมีความปลอดภัย
 - 4.7.2 ผู้ดูแลระบบต้องติดตั้ง Firewall ระหว่างเครือข่ายของ รพม. กับเครือข่ายภายนอก ทั้งนี้ การติดตั้ง Firewall ต้องพิจารณาเรื่องดังต่อไปนี้
 - 1) การป้องกันการจราจรจากภายนอก ต้องถูกกำหนดให้ใช้เส้นทางที่ผ่าน First Tier Firewall ที่มีความมั่นคงปลอดภัยเพื่อป้องกันทรัพย์สินสารสนเทศของ รพม. และโครงสร้างพื้นฐานที่มีความสำคัญจากการเข้าถึงที่ไม่ได้รับอนุญาต
 - 2) Firewall ต้องระบุตัวตนและพิสูจน์ตัวตนของผู้ใช้งานก่อนที่จะให้สิทธิ์การเข้าถึงอินเทอร์เน็ต (Interface) เพื่อการบริหารจัดการ Firewall
 - 3) Firewall ต้องตั้งค่าให้ระงับบัญชีผู้ใช้งานหลังจากมีความพยายามที่จะเข้าสู่ระบบไม่สำเร็จ 5 ครั้ง การยกเลิกการระงับต้องดำเนินการโดย ผทท.
 - 4) ไม่อนุญาตให้พิสูจน์ตัวตนผ่านทางอินเทอร์เน็ต (Interface) การจัดการ Firewall จากระยะไกล (Remote)

- 5) ผู้ที่ได้รับการมอบหมายจาก ผพท. เท่านั้นที่มีสิทธิ์ที่จะเปลี่ยนการตั้งค่าด้านความปลอดภัยบน Firewall
- 6) Firewall ต้องตั้งค่าให้บันทึกเหตุการณ์ด้านความมั่นคงปลอดภัย
- 7) Firewall ต้องได้รับการสอบทาน ทดสอบ และตรวจสอบอย่างสม่ำเสมอ
- 8) Firewall ต้องถูกบริหารจัดการผ่านทาง การติดต่อสื่อสารที่มีการเข้ารหัส
- 9) ต้องปิดบริการและพอร์ต (Port) ที่ไม่จำเป็นต้องใช้บน Firewall
- 10) Firewall ประเภทซอฟต์แวร์ (Software) ต้องติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายแยกต่างหาก
- 11) Firewall ต้องสามารถป้องกันตัวเองจากการโจมตี DOS (Denial of service) ได้อย่างเช่น Ping, Sweeps หรือ TCP SYN Floods เป็นต้น
- 12) ต้องใช้เวอร์ชันของซอฟต์แวร์ (Software) Firewall และระบบปฏิบัติการที่เจ้าของผลิตภัณฑ์ยังให้การสนับสนุน
- 13) ผู้ดูแล Firewall ต้องติดตามข้อมูลช่องโหว่จากผู้ให้บริการ (Vendor) เพื่อรับทราบข่าวสารการ Upgrade และแพตช์ (Patch) ที่จำเป็น และต้องติดตั้งแพตช์ (Patch) ทั้งหมดที่เกี่ยวข้อง

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

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

4.8 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network Routing Control)

ผู้ดูแลระบบต้องควบคุมการกำหนดเส้นทางบนเครือข่ายเพื่อให้มั่นใจว่าการเชื่อมต่อเครื่องคอมพิวเตอร์และการไหลเวียนของสารสนเทศบนเครือข่าย โดยมีกลไกในการตรวจสอบที่อยู่ปลายทางและต้นทางของการเชื่อมต่อ เช่น การควบคุมโดย Firewall หรือ Proxy เป็นต้น

5. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system Access Control)

ให้มีการควบคุมการเข้าถึงระบบปฏิบัติการอย่างมั่นคงปลอดภัย การควบคุมการระบุและพิสูจน์ตัวตนของผู้ใช้งาน การควบคุมระบบบริหารจัดการรหัสผ่าน การควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ (System Utilities) การควบคุมการหมดเวลาการใช้งานระบบเทคโนโลยีสารสนเทศ และควบคุมการจำกัดระยะเวลาการเชื่อมต่อบนระบบเทคโนโลยีสารสนเทศ

5.1 ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure Logon Procedures)

5.1.1 ผู้ดูแลระบบ ต้องจัดให้มีการควบคุมการเข้าถึงระบบปฏิบัติการอย่างมั่นคงปลอดภัย โดยขั้นตอนการเข้าสู่ระบบต้องเปิดเผยข้อมูลเกี่ยวกับระบบให้น้อยที่สุดเพื่อหลีกเลี่ยงผู้ใช้งานที่ไม่ได้รับอนุญาต ซึ่งขั้นตอนการ Logon ต้องพิจารณา ดังนี้

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

- 4) ระบบต้องไม่แสดงข้อความที่ชี้เฉพาะเหตุของการเข้าสู่ระบบไม่สำเร็จ เช่น ไม่แสดงข้อความว่า บัญชีผู้ใช้งานผิด หรือ รหัสผ่านผิด เป็นต้น
 - 5) ห้ามเข้าสู่ระบบจากบัญชีผู้ใช้งานส่วนบุคคลเดียวกันมากกว่าหนึ่ง Session ในระบบเดียวกัน
 - 6) ระบบต้องจำกัดจำนวนครั้งในการพยายามเข้าสู่ระบบที่ไม่สำเร็จ และต้องพิจารณาเงื่อนไขต่อไปนี้อย่างเคร่งครัด
 - (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 และต้องใช้ระบบเทคโนโลยีสารสนเทศพิสูจน์ตัวตนผู้ใช้งานในการเข้าถึงระบบปฏิบัติการผ่านระบบ Active Directory (AD) หรือ Lightweight Directory Access Protocol (LDAP) ทุกครั้ง พร้อมทั้งบันทึกข้อมูลการเข้าถึง
- 5.3 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of System Utilities)
- ผู้ดูแลระบบ ต้องควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้บนระบบที่ใช้งานจริง (Production System) ดังนี้
- 5.3.1 ต้องจัดทำบัญชีโปรแกรมประเภทยูทิลิตี้ (System Utilities) ที่นำมาใช้งาน
 - 5.3.2 กำหนดความรับผิดชอบในการใช้โปรแกรมประเภทยูทิลิตี้ (System Utilities) แต่ละรายการอย่างชัดเจนและสื่อสารให้ผู้เกี่ยวข้องทราบเพื่อถือปฏิบัติ
 - 5.3.3 ให้มีการพิสูจน์ตัวตน และกำหนดสิทธิ์ในการใช้งานโปรแกรมประเภทยูทิลิตี้เฉพาะกลุ่มคนที่มีหน้าที่รับผิดชอบ
 - 5.3.4 มีการบันทึกเหตุการณ์ (Log) การใช้งานโปรแกรมประเภทยูทิลิตี้ และต้องสอบทานจากผู้ดูแลระบบอย่างสม่ำเสมอ
 - 5.3.5 ต้องทำการเพิกถอนหรือระงับโปรแกรมประเภทยูทิลิตี้ที่ไม่จำเป็น
- 5.4 การหมดเวลาการใช้งานระบบสารสนเทศ (Session Timeout)
- 5.4.1 ผู้ดูแลระบบต้องกำหนด Session Timeout ของระบบเทคโนโลยีสารสนเทศที่ไม่มีการใช้งานภายในระยะเวลา 15 นาที หากระบบใดที่ไม่สามารถกำหนด Session Timeout ภายในระยะเวลา 15 นาทีได้ ให้กำหนดเป็นระยะเวลาน้อยที่สุดที่จะสามารถกำหนดได้ ทั้งนี้ ถ้าระบบที่ไม่สามารถตัดการเชื่อมต่อแบบอัตโนมัติได้ กำหนดให้ใช้โปรแกรมพักหน้าจอที่ต้องใส่รหัสผ่านหรือกำหนดให้มีการล็อกหน้าจอ
 - 5.4.2 ผู้ดูแลระบบ และผู้ใช้งาน ต้องตั้งค่าให้มีโปรแกรมพักหน้าจอที่ต้องใส่รหัสผ่านสำหรับเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์แบบพกพา และเครื่องคอมพิวเตอร์แม่ข่าย ทั้งนี้ โปรแกรมพักหน้าจอกำหนดให้ป้อนรหัสผ่านหลังจากที่มีการทิ้งเครื่องดังกล่าวไว้โดยไม่มีการใช้งานเป็นระยะเวลา 15 นาที

- 5.5 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time)
 - 5.5.1 ผู้ดูแลระบบ ต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง โดยต้องคำนึงถึงระยะเวลาที่จำเป็นในกระบวนการดำเนินงานทางธุรกิจ ได้แก่ กำหนดให้เข้าใช้งานได้ในช่วงเวลาทำการของ รพม. 08.00 น. – 17.00 น. และเชื่อมต่อเพื่อใช้งานได้ครั้งละไม่เกิน 3 ชั่วโมง
 - 5.5.2 ผู้ใช้งาน หากมีความจำเป็นต้องใช้งานนอกเวลาที่กำหนดต้องขออนุมัติจากผู้บังคับบัญชาเท่านั้น
6. การควบคุมการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ (Application and Information Access Control)
 ให้มีการจำกัดการเข้าถึงสารสนเทศ และการแยกระบบเทคโนโลยีสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณที่ควบคุมเฉพาะ
 - 6.1 การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)
 - 6.1.1 เจ้าของข้อมูลและผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงแก่ผู้ใช้งานเท่าที่จำเป็นต้องใช้ในการปฏิบัติงาน โดยการให้สิทธิ์ต้องพิจารณาในเรื่องดังต่อไปนี้
 - 1) การจำกัดไม่ให้ใช้ตัวเลือก (Options) ที่ไม่ได้รับอนุญาต
 - 2) การจำกัดการเข้าถึง Command Line
 - 3) การจำกัดการเข้าถึงข้อมูลและฟังก์ชันการใช้งานของแอปพลิเคชัน (Application) ที่ไม่เกี่ยวข้องกับหน้าที่ความรับผิดชอบ
 - 4) การจำกัดระดับสิทธิ์ในการเข้าถึงไฟล์ เช่น อ่านอย่างเดียว เป็นต้น
 - 5) การควบคุมการแจกจ่าย การเข้าถึงข้อมูล การนำข้อมูลออกจากระบบสารสนเทศ เช่น รายงาน เป็นต้น
 - 6.1.2 เจ้าของข้อมูลและผู้ดูแลระบบ ควรกำหนดให้ระบบสารสนเทศรองรับการกำหนดสิทธิ์ในการเข้าถึงแบบกลุ่มได้
 - 6.2 การแยกระบบสารสนเทศที่ไวต่อการรบกวน (Sensitive System Isolation) มีผลกระทบต่อคนกลุ่มใหญ่หรือระบบที่มีความสำคัญต่อหน่วยงาน ต้องดำเนินการดังนี้
 - 6.2.1 เจ้าของข้อมูลและผู้ดูแลระบบ แยกระบบซึ่งไวต่อการรบกวนออกจากระบบอื่น ๆ และควบคุมสภาพแวดล้อมของระบบโดยเฉพาะ ได้แก่ ระบบ File Sharing ระบบสารสนเทศทางการเงิน และระบบ Active Directory (AD) โดยเข้าถึงได้ทั้งอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร (Mobile Computing and Teleworking)
 - 6.2.2 ผู้ดูแลระบบต้องควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์เคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile Computing and Teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว
 - 6.2.3 เจ้าของข้อมูลที่เป็นเจ้าของระบบสารสนเทศที่มีความสำคัญสูงต้องเป็นผู้อนุญาต ในกรณีที่ระบบสารสนเทศที่มีความสำคัญสูงมีความจำเป็นต้องทำงานร่วมกับระบบสารสนเทศอื่นที่มีความสำคัญน้อยกว่า
7. การควบคุมการปฏิบัติงานจากภายนอก รพม. (Teleworking)
 - 7.1 ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนการใช้งาน และเชื่อมต่อผ่านช่องทางที่มีความปลอดภัยที่มีเทคโนโลยีเข้ารหัสป้องกัน
 - 7.2 ผู้ดูแลระบบต้องทำการถอดถอนสิทธิ์ในการเข้าถึงของผู้ใช้งานจากภายนอกสำนักงาน เมื่อครบกำหนดระยะเวลาที่ขออนุญาต
 - 7.3 ผู้ใช้งาน หากจำเป็นต้องมีการปฏิบัติงานจากภายนอกสำนักงานของ รพม. ต้องได้รับการอนุญาตจากผู้บังคับบัญชาอย่างเป็นลายลักษณ์อักษร ในกรณีเร่งด่วนสามารถดำเนินการก่อน โดยแจ้งให้ผู้บังคับบัญชารับทราบด้วย โดยผู้บังคับบัญชาต้องพิจารณาเงื่อนไขในการเตรียมการ ดังต่อไปนี้

- 1) ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมของการปฏิบัติงานจากภายนอก 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 พระราชบัญญัติกฏระเบียบ ข้อบังคับที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ส่วนที่ 7

การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

วัตถุประสงค์

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

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

อ้างอิงมาตรฐาน: ISO/IEC 27001:2022

- มาตรการควบคุมด้านองค์กร (Organizational Controls)
- มาตรการควบคุมด้านเทคโนโลยี (Technological Controls)

แนวปฏิบัติ

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

ส่วนที่ 8

การควบคุมหน่วยงานภายนอกและผู้ใช้งานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

- เพื่อควบคุมหน่วยงานภายนอกและผู้ใช้งานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของ รพม. ให้เป็นไปอย่างมั่นคงปลอดภัย

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้บังคับบัญชา
- หน่วยงานภายนอก
- ผู้ใช้งาน (บุคคลภายนอก)

อ้างอิงมาตรฐาน: ISO/IEC 27001:2022

- มาตรการควบคุมด้านองค์กร (Organizational Controls)
- มาตรการควบคุมด้านกายภาพ (Physical Controls)

แนวปฏิบัติ

1. ผู้ดูแลระบบต้องประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผล โดยหน่วยงานภายนอกและผู้ใช้งานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศของ รพม.
2. การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอกและผู้ใช้งานภายนอก
 - 2.1 เจ้าของข้อมูลต้องเป็นผู้อนุญาตการให้สิทธิ์แก่หน่วยงานภายนอกและผู้ใช้งานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของ รพม. อย่างเป็นลายลักษณ์อักษร
 - 2.2 ผู้บังคับบัญชาต้องกำหนดให้มีการลงนามการไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของ รพม.
 - 2.3 ผู้บังคับบัญชา ต้องควบคุมให้มีการกำหนดข้อตกลงและความรับผิดชอบที่เกี่ยวข้องกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศลงในสัญญา กับหน่วยงานภายนอกที่ให้บริการด้านสารสนเทศและบริการด้านการสื่อสาร โดยให้ครอบคลุมรวมถึงผู้รับจ้างช่วง
 - 2.4 ผู้บังคับบัญชาต้องกำหนดให้จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกและผู้ใช้งานภายนอกระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศ ซึ่งมีรายละเอียด ดังนี้
 - 2.4.1 เหตุผลในการขอใช้
 - 2.4.2 ระยะเวลาในการใช้
 - 2.4.3 การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย
 - 2.4.4 การตรวจสอบ MAC address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ
 - 2.5 ผู้ดูแลระบบมีสิทธิ์ในการตรวจสอบการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอกและผู้ใช้งานภายนอก เพื่อควบคุมการใช้งานได้อย่างมั่นคงปลอดภัยตามสัญญา
 - 2.6 ผู้ดูแลระบบต้องควบคุมให้หน่วยงานภายนอกจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งต้องปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อใช้สำหรับควบคุมหรือตรวจสอบการทำงาน เพื่อให้มั่นใจว่าการปฏิบัติงานเป็นไปตามขอบเขตที่ได้กำหนดไว้
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 และต้องประเมินความเสี่ยงอย่างเหมาะสมเพื่อควบคุมผลกระทบอันเนื่องมาจากการเปลี่ยนเปลี่ยนนั้น
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 รพม.

วัตถุประสงค์

- เพื่อควบคุมการใช้งานทรัพย์สินของ รพม. ประเภทเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ที่เหมาะสม ทั้งนี้ เพื่อป้องกันการสูญหาย เสียหาย หรือถูกเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

อ้างอิงมาตรฐาน: ISO/IEC 27001:2022

- มาตรการควบคุมด้านองค์กร (Organizational Controls)
- มาตรการควบคุมด้านบุคลากร (People Controls)
- มาตรการควบคุมด้านกายภาพ (Physical Controls)
- มาตรการควบคุมด้านเทคโนโลยี (Technological Controls)

แนวปฏิบัติ

1. การใช้งานทั่วไป

- 1.1 ผู้ดูแลระบบต้องกำหนดบัญชีซอฟต์แวร์มาตรฐาน (Software Standard) ที่อนุญาตให้ติดตั้งบนเครื่องคอมพิวเตอร์ของผู้ใช้งาน และปรับปรุงให้เป็นปัจจุบันเสมอ
- 1.2 ผู้ดูแลระบบต้องเป็นผู้กำหนดการตั้งชื่อเครื่องคอมพิวเตอร์ (Computer Name) เท่านั้น
- 1.3 ผู้ใช้งานต้องติดตั้งโปรแกรมสำหรับควบคุมการใช้งานอุปกรณ์เคลื่อนที่ (Mobile Device Management: MDM) รวมถึงอุปกรณ์อื่น ๆ ที่ รพม. ไม่สามารถควบคุมการใช้งานผ่านระบบ Active Directory (AD) ได้
- 1.4 ผู้ใช้งานต้องใช้งานอย่างมีประสิทธิภาพเพื่องานของ รพม.
- 1.5 ผู้ใช้งานต้องไม่ติดตั้งโปรแกรมที่ละเมิดลิขสิทธิ์บนเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ของ รพม.
- 1.6 ผู้ใช้งานต้องขออนุญาตติดตั้งโปรแกรมในเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ตามขั้นตอนที่ รพม. กำหนด
- 1.7 ผู้ใช้งานต้องไม่ติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ของ รพม. การดำเนินการดังกล่าวต้องดำเนินการโดยผู้ดูแลระบบเท่านั้น
- 1.8 ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่อย่างละเอียด เพื่อให้สามารถใช้งานอย่างปลอดภัยและมีประสิทธิภาพ
- 1.9 ผู้ใช้งานต้องไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ และรักษาให้มีสภาพเดิม
- 1.10 ผู้ใช้งานต้องแจ้งซ่อมเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ที่อยู่ในความรับผิดชอบของ ผทท. ให้ ผทท. เป็นผู้ดำเนินการเท่านั้น
- 1.11 ผู้ใช้งานต้องอัปเดต Patch และระบบปฏิบัติการให้ทันสมัยอยู่เสมอ
- 1.12 ผู้ใช้งานต้องไม่สร้าง Shortcut ไว้บน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของ รพม.
- 1.13 กรณีเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์เคลื่อนที่ ผู้ใช้งานต้องปฏิบัติเพิ่มเติม ดังนี้
 - 1.13.1 ต้องติดตั้ง Application จาก Official Store หรือเว็บไซต์ที่ให้บริการผ่านโปรโตคอล HTTPS
 - 1.13.2 ไม่ปรับแต่งการเข้าถึงระบบปฏิบัติการ (Rooted/Jailbroken)
 - 1.13.3 ในกรณีที่มีการใช้งานอุปกรณ์ประเภทพกพาในที่สาธารณะ ห้องประชุม และพื้นที่ภายนอกอื่น ๆ ที่ไม่มีการป้องกัน หรือไม่ได้อยู่ในบริเวณของ รพม. ให้ป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต เช่น ไม่เปิดการเชื่อมต่อแบบไร้สายโดยไม่มีการเข้ารหัสข้อมูล เป็นต้น

- 1.13.4 ต้องระมัดระวังการเคลื่อนย้าย โดยต้องใส่กระเป๋าเพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงานหรือหลุดมือ เป็นต้น
 - 1.13.5 ไม่ใส่ในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับหรืออาจถูกจับโยนได้
 - 1.13.6 การใช้งานเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัดต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง
 - 1.13.7 หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอย ชีตข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้
 - 1.13.8 ไม่วางของทับบนหน้าจอและแป้นพิมพ์
 - 1.13.9 การเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น
 - 1.13.10 ไม่เคลื่อนย้ายเครื่องในขณะที่ Harddisk กำลังทำงาน
 - 1.13.11 ไม่ใช้หรือวางใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่าง ๆ เป็นต้น
 - 1.13.12 ไม่วางใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูง เช่น แม่เหล็ก โทรศัพท์ ไมโครเวฟ ตู้เย็น เป็นต้น
 - 1.13.13 ไม่ติดตั้งหรือวางในที่ที่มีการสั่นสะเทือน เช่น ในยานพาหนะที่กำลังเคลื่อนที่
 - 1.13.14 การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้
 - 1.13.15 รับผิดชอบในการป้องกันการสูญหาย เช่น ต้องล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย
 - 1.13.16 นำติดตัวไปด้วยเสมอ เช่น ไม่ละทิ้ง อุปกรณ์ประมวลผลประเภทพกพาในรถยนต์ ห้องพัก ในโรงแรม 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 รพม.
 - 3.5 ผู้ใช้งาน หากพบหรือสงสัยว่าเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ติดชุดคำสั่งไม่พึงประสงค์ ให้รีบยกเลิกเชื่อมต่อเครื่องเข้ากับระบบเครือข่ายสื่อสารข้อมูลเพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่น ๆ ได้ และแจ้ง ผทท. ทราบทันที

4. การสำรองข้อมูลและการกู้คืน
 - 4.1 ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ไว้บนสื่อบันทึกอื่น ๆ เช่น ระบบ File Sharing, CD, DVD, External harddisk เป็นต้น
 - 4.2 ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลสำรองไว้อย่างสม่ำเสมอ
5. ผู้ดูแลระบบ ต้องควบคุมให้เครื่องคอมพิวเตอร์ได้รับการปรับตั้งค่าอย่างเหมาะสม เพื่อป้องกันการใช้งานหรือติดตั้ง Mobile Code เช่น Active X, Java จากแหล่งที่น่าเชื่อถือ

ส่วนที่ 10

การใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์

วัตถุประสงค์

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

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

อ้างอิงมาตรฐาน: ISO/IEC 27001:2022

- มาตรการควบคุมด้านองค์กร (Organizational Controls)
- มาตรการควบคุมด้านเทคโนโลยี (Technological Controls)

แนวปฏิบัติ

1. ผู้ดูแลระบบต้องควบคุมการเชื่อมต่อทางเครือข่ายสำหรับการเข้าถึงอินเทอร์เน็ตโดยพิจารณาเรื่องดังต่อไปนี้
 - 1) ผู้ดูแลระบบต้องไม่อนุญาตให้ใช้งานอุปกรณ์ Video Streaming อุปกรณ์ Audio streaming หรือ Download ไฟล์ที่มีขนาดใหญ่ ในกรณีที่ต้องได้รับการอนุญาตจากผู้บังคับบัญชาก่อนเท่านั้น
 - 2) ผู้ดูแลระบบต้องจำกัดการใช้งานอินเทอร์เน็ตเพื่อเรื่องส่วนตัวหรือที่ไม่ใช่การดำเนินงานของ รพม. ให้น้อยที่สุดเท่าที่เป็นไปได้ เช่น การระงับการเข้าถึง Website ที่ไม่จำเป็น การระงับการเข้าถึง Website ที่มีเนื้อหาต้องห้ามตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
 - 3) ผู้ดูแลระบบต้องป้องกันไม่ให้มีการรับส่งข้อมูลที่ไม่เหมาะสมจากภายนอก รพม. เช่น
 - (ก) Executable เช่น .EXE .COM เป็นต้น
 - (ข) ไฟล์ (File) เสียง เช่น AUD .WAV และ .MP3 เป็นต้น
 - (ค) ไฟล์ (File) วิดีทัศน์ เช่น .MPG .MPEG .MOV และ .AVI เป็นต้น
 - (ง) Peer to Peer เช่น .torrent เป็นต้น
 ในกรณีที่มีความจำเป็นต้องได้รับอนุญาตจากผู้บังคับบัญชา และ ผทท.
 - 4) ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่ รพม. จัดสรรไว้เท่านั้น เช่น Proxy, Firewall เป็นต้น
 - 5) ผู้ดูแลระบบต้องทดสอบเส้นทางการเชื่อมต่ออินเทอร์เน็ตขององค์กรระหว่างเส้นทางที่ใช้งานจริงและเส้นทางสำรองอย่างน้อยปีละ 2 ครั้ง
 - 6) ผู้ใช้งานต้องไม่เชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นมีความจำเป็นและขออนุญาตจาก ผทท. เป็นลายลักษณ์อักษรแล้ว
 - 7) ผู้ใช้งานต้องขออนุญาตติดตั้งซอฟต์แวร์ (Software) ที่ Download จากอินเทอร์เน็ต และการติดตั้งต้องดำเนินการโดยผู้ที่ได้รับมอบหมายจากผู้ดูแลระบบเท่านั้น
2. ผู้ใช้งานต้องไม่มีเจตนาปิดบังหรือบิดเบือนตัวตนเมื่อมีการใช้งานอินเทอร์เน็ต
3. ผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัส พร้อมทั้งต้องปรับปรุง Virus Signature ที่เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพาให้มีความทันสมัยอยู่เสมอ ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web Browser) และต้องปิดช่องโหว่ของระบบปฏิบัติการที่เว็บเบราว์เซอร์ติดตั้งอยู่
4. ผู้ใช้งานจะต้องตรวจสอบไวรัส (Virus Scanning) ก่อนการรับ - ส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ต

5. ผู้ใช้งานต้องไม่ใช่เครือข่ายอินเทอร์เน็ตของ รพม. เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น
6. ผู้ใช้งานจะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของ รพม.
7. ผู้ใช้งานต้องหลีกเลี่ยงการกระทำที่สิ้นเปลืองทรัพยากรของเครือข่ายอินเทอร์เน็ต ดังนี้
 - (ก) ส่งจดหมายอิเล็กทรอนิกส์ลูกโซ่
 - (ข) ใช้เวลาในการเข้าถึงอินเทอร์เน็ตเกินความจำเป็นยกเว้นเพื่อปฏิบัติงานให้ รพม.
 - (ค) เล่นเกม Online
 - (ง) เข้าห้องพูดคุย Online ที่ไม่ได้มีวัตถุประสงค์เพื่อปฏิบัติงานให้ รพม.
8. ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับ รพม.
9. ผู้ใช้งานต้องไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของ รพม.
10. ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต
11. ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ที่จะทำให้ผู้อื่นเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย
12. ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน
13. ผู้ใช้งานต้องคำนึงว่าข้อมูลจากอินเทอร์เน็ตอาจไม่มีความทันสมัยหรือไม่มีความถูกต้อง ผู้ใช้งานต้องตรวจสอบความถูกต้องของข้อมูลจากแหล่งที่น่าเชื่อถือก่อนที่จะเผยแพร่ข้อมูลดังกล่าว
14. ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา
15. ผู้ใช้งานต้องไม่ใช่ข้อมูลที่ร้ายแรง ให้อภัยในการเสนอความคิดเห็นที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของ รพม. การทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น ๆ
16. ผู้ใช้งานต้องไม่บันทึกรหัสผ่านใน Web Browser (Remember Password) เพื่อป้องกันบุคคลอื่นที่สามารถเข้าถึงคอมพิวเตอร์ของผู้ใช้งานนำรหัสผ่านดังกล่าวไปใช้งานในอินเทอร์เน็ตโดยไม่ได้รับอนุญาต
17. ผู้ใช้งานต้องไม่ Download เอกสาร หรือสารสนเทศต่าง ๆ เช่น ข้อมูล รูปภาพ วิดีโอ เสียง และซอฟต์แวร์ (Software) ที่ละเมิดลิขสิทธิ์ หรือผิดกฎหมาย
18. ผู้ใช้งานต้องปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ ภายหลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว
19. การใช้งานสื่อสังคมออนไลน์ (Social Network)
 - 19.1 ผู้ใช้งานต้องระมัดระวังในการนำเสนอข้อมูลข่าวสาร การส่งข้อความ หรือการแสดงความคิดเห็นผ่านสื่อสังคมออนไลน์เพื่อไม่ก่อให้เกิดความเสียหายแก่ รพม.
 - 19.2 ผู้ใช้งานต้องระมัดระวังในการใช้สื่อสังคมออนไลน์ เนื่องจากพื้นที่บนสื่อสังคมออนไลน์เป็นพื้นที่สาธารณะไม่ใช่พื้นที่ส่วนบุคคล ซึ่งข้อมูลการใช้งานต่าง ๆ จะถูกบันทึกไว้และอาจมีผลทางกฎหมาย ถึงแม้จะเป็นการแสดงความคิดเห็นในนามชื่อบุคคลส่วนตัว และพึงตระหนักถึงผลกระทบที่อาจเกิดขึ้นกับ รพม. ได้

- 19.3 ผู้ใช้งานที่ใช้สื่อสังคมออนไลน์เป็นเครื่องมือสื่อสารข้อมูลในกิจการของ รพม. หรือชื่อบุคคลที่ทำให้เข้าใจได้ว่าเป็นบุคคลในสังกัด ต้องแสดงภาพ และข้อมูลให้ถูกต้องชัดเจนในข้อมูล โปรไฟล์ (Profile) และพึงใช้ด้วยความสุภาพและมีวิจารณญาณ
- 19.4 ผู้ใช้งานควรตั้งคำถามที่ใช้ในกรณีกู้คืนบัญชีผู้ใช้งานหรือกู้คืนรหัสผ่าน (Forgot Your Password) ควรเลือกใช้ข้อมูลหรือคำถามที่เป็นส่วนบุคคลและเป็นข้อมูลที่ผู้อื่นคาดเดาได้ยากเพื่อป้องกันการสุ่มคำถามจากผู้ประสงค์ร้าย
- 19.5 ผู้ใช้งานต้องไม่ใช้ระบบอีเมลของเว็บไซต์ประเภทสื่อสังคมออนไลน์ หากจำเป็นต้องใช้จะต้องระมัดระวังในการคลิกลิงก์ที่น่าสงสัย โดยเฉพาะอีเมลแจ้งเตือนจากเว็บไซต์ต่าง ๆ ในลักษณะเชิญให้คลิกลิงก์ที่แนบมาในอีเมล ผู้ใช้งานต้องสงสัยว่าลิงก์ดังกล่าวเป็นลิงก์ที่ไม่ปลอดภัย (ลิงก์ที่ถูกสร้างมาเพื่อใช้ขโมยข้อมูลส่วนบุคคล ด้วยการนำไปสู่เว็บไซต์ที่ดูน่าเชื่อถือที่ผู้ประสงค์ร้ายสร้างไว้เพื่อให้ผู้ใช้งานกรอกข้อมูลส่วนบุคคล เช่น รหัสผ่าน เป็นต้น)
- 19.6 ผู้ใช้งานต้องศึกษาการตั้งค่าความเป็นส่วนตัวหรือ “Privacy Settings” ให้เข้าใจเป็นอย่างดีและปรับแต่งการตั้งค่าความเป็นส่วนตัวให้เหมาะสมเพื่อป้องกันการถูกละเมิดความเป็นส่วนตัวซึ่งอาจจะส่งผลกระทบต่อตนเองหรือ รพม.
- 19.7 ผู้ใช้งานต้องใช้งานสื่อสังคมออนไลน์อย่างเหมาะสม โดยไม่ละเมิดกฎหมายและไม่ก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานขององค์กร
- 19.8 ผู้ใช้งานควรปิดการใช้งานระบบโพสต์ข้อความสาธารณะทุก ๆ ส่วนของเว็บไซต์ประเภท Social Network หากจำเป็นต้องใช้งานต้องปรับค่าให้มีการตรวจสอบข้อความก่อนเพื่อหลีกเลี่ยงโอกาสแพร่กระจายลิงก์ที่ไม่ปลอดภัยจากผู้ประสงค์ร้าย ซึ่งเป็นหนึ่งในเทคนิคที่ใช้ในการโจมตีประเภท Spear Phishing
- 19.9 ผู้ใช้งานต้องตรวจสอบก่อนจะรับเพื่อนเข้ากลุ่มในเว็บไซต์ประเภท Social Network โดยต้องแน่ใจว่าข้อมูลส่วนตัวของเพื่อนคนนั้น เช่น รูปถ่ายและประวัติส่วนตัวไม่ถูกแก้ไขเพื่อปลอมแปลงตัวตนจากผู้ประสงค์ร้ายที่หวังแอบอ้างเพื่อคุกคามเป้าหมาย
- 19.10 ผู้ใช้งานต้องตระหนักไว้เสมอว่าข้อมูลต่าง ๆ ที่ผู้ใช้งานเผยแพร่ไว้บนบริการสื่อสังคมออนไลน์นั้น คงอยู่ถาวรและผู้อื่นอาจเข้าถึงและเผยแพร่ข้อมูลเหล่านั้นได้
- 19.11 ผู้ใช้งานต้องมีข้อพิจารณาในการรับเพื่อนเข้ากลุ่มที่ชัดเจน และควรประกาศข้อความปฏิเสธความรับผิดชอบที่เกี่ยวกับเนื้อหาหรือข้อความแสดงความคิดเห็นซึ่งถูกโพสต์จากเพื่อนในกลุ่มที่อาจปรากฏในเว็บไซต์ประเภท Social Network ของผู้ใช้งานเอง
- 19.12 ผู้ใช้งานต้องติดตั้งซอฟต์แวร์ป้องกันไวรัส และอัปเดตฐานข้อมูลไวรัสของโปรแกรมอยู่เสมอ และต้องหลีกเลี่ยงการใช้โปรแกรมที่ละเมิดลิขสิทธิ์เพราะอาจจะมีโปรแกรมประสงค์ร้ายแฝงตัวอยู่ภายในเพื่อลักลอบ ปลอมแปลง หรือขโมยข้อมูลสำคัญของผู้ใช้งานได้
- 19.13 ผู้ใช้งานต้องระมัดระวังการใช้ถ้อยคำและภาษาที่อาจเป็นการดูหมิ่น ยุยง ทำร้าย หรือเป็นการละเมิดต่อบุคคลอื่น กรณีบุคคลอื่นมีความคิดเห็นที่แตกต่างพึงงดเว้นการโต้ตอบด้วยถ้อยคำรุนแรง
- 19.14 ผู้ใช้งานต้องระมัดระวังกระบวนการหาข่าว หรือภาพจากสื่อสังคมออนไลน์ โดยมีการตรวจสอบอย่างถี่ถ้วนรอบด้านและต้องอ้างอิงแหล่งที่มาเมื่อนำเสนอ เว้นแต่สามารถตรวจสอบและอ้างอิงจากแหล่งข่าวได้โดยตรง
- 19.15 หากผู้ใช้งานต้องการใช้สื่อสังคมออนไลน์เป็นเครื่องมือในการรายงานข่าวในนามของบุคคลธรรมดาต้องแสดงให้เห็นชัดเจนว่า ข้อความใดเป็น "ข่าว" ข้อความใดเป็น "ความคิดเห็นส่วนตัว"
- 19.16 การส่งต่อหรือเผยแพร่ข้อมูลในสื่อสังคมออนไลน์ (Social Media)

- 19.16.1 ผู้ใช้งานต้องไม่ส่งต่อหรือเผยแพร่ข้อมูลที่เป็นเท็จ ข่าวลือ ข่าวไม่ปรากฏที่มา เป็นเพียงการคาดเดา หรือส่งผลเสียหายกับบุคคล สังคม หรือ รฟม.
- 19.16.2 ผู้ใช้งานต้องไม่ส่งต่อหรือเผยแพร่ข้อมูลเรื่องบุคคลเสียชีวิต เด็กและเยาวชน ผู้สูญหาย ผู้ต้องหา เว้นเสียแต่ตรวจสอบข้อเท็จจริงแล้วและเห็นว่าเป็นประโยชน์ต่อสาธารณะ
- 19.16.3 ผู้ใช้งานต้องไม่ส่งต่อหรือเผยแพร่ข้อมูลที่กระทบต่อสิทธิความเป็นส่วนตัว และศักดิ์ศรีความเป็นมนุษย์
- 19.17 ผู้ใช้งานต้องตั้งค่าความปลอดภัยของการใช้งานสื่อสังคมออนไลน์ และระมัดระวังการถูกนำข้อมูลจากข้อบัญญัติไปใช้โดยไม่เหมาะสม ผิดวัตถุประสงค์ และลักษณะการแอบอ้างโดยบุคคลอื่น
- 20. ผู้ใช้งานต้องใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์โดยตระหนักถึงพระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่บังคับใช้อยู่เสมอ

ส่วนที่ 11

การใช้งานจดหมายอิเล็กทรอนิกส์

วัตถุประสงค์

- เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ของ รพม. ให้มีความปลอดภัยและมีประสิทธิภาพ

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

อ้างอิงมาตรฐาน: ISO/IEC 27001:2022

- มาตรการควบคุมด้านองค์กร (Organizational Controls)
- มาตรการควบคุมด้านเทคโนโลยี (Technological Controls)

แนวปฏิบัติ

1. ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของ รพม. ให้เหมาะสมกับหน้าที่ความรับผิดชอบของผู้ใช้งาน รวมทั้งทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ
2. ผู้ดูแลระบบต้องกำหนดบัญชีผู้ใช้งานตามมาตรฐานจดหมายอิเล็กทรอนิกส์ (Email) ที่ใช้ในองค์กร
3. ผู้ใช้งานต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ไม่ให้เกิดความเสียหายต่อ รพม. ละเมิดลิขสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น ผิดกฎหมาย ละเมิดศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ของ รพม.
4. ผู้ใช้งานต้องไม่ใช่ที่อยู่จดหมายอิเล็กทรอนิกส์ (Email Address) ของผู้อื่นเพื่ออ่าน รับ - ส่งข้อความ ยกเว้นได้รับการยินยอมจากเจ้าของบัญชีและให้ถือว่าเจ้าของบัญชีจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน
5. ผู้ใช้งานต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของ รพม. เพื่อปฏิบัติงาน ติดต่อ และประสานงานของ รพม. เท่านั้น
6. ผู้ใช้งานต้องไม่ใช่ที่อยู่จดหมายอิเล็กทรอนิกส์ฟรีของเอกชนในการปฏิบัติงาน ติดต่อ และประสานงานของ รพม.
7. ผู้ใช้งานต้อง Logout ออกจากระบบทุกครั้ง หลังจากใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้นเพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์
8. ผู้ใช้งานต้องตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนเปิดอ่าน โดยใช้โปรแกรมป้องกันไวรัสเพื่อตรวจสอบมัลแวร์ต่าง ๆ
9. ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์ที่ได้รับจากผู้ส่งที่ไม่รู้จัก
10. ผู้ใช้งานต้องใช้ข้อความที่สุภาพในการรับ - ส่งจดหมายอิเล็กทรอนิกส์ และไม่ส่งจดหมายที่มีเนื้อหาอาจทำให้ รพม. เสียชื่อเสียงหรือทำให้เกิดความแตกแยกภายใน รพม.
11. ผู้ใช้งานต้องไม่ระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์และต้องเข้ารหัสเพื่อป้องกันการเข้าถึงข้อมูลโดยผู้ไม่เกี่ยวข้องเมื่อมีการส่งข้อมูลที่เป็นความลับ
12. ผู้ใช้งานต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และต้องจัดเก็บจดหมายอิเล็กทรอนิกส์ในตู้ของตนให้เหลือจำนวนน้อยที่สุด หากมีข้อมูลที่ต้องนำมาใช้อ้างอิงในการปฏิบัติงานภายหลังให้ผู้ใช้งานโอนย้ายจดหมายอิเล็กทรอนิกส์มายังเครื่องคอมพิวเตอร์ของตน ทั้งนี้ เพื่อลดปริมาณการใช้เนื้อที่ของระบบจดหมายอิเล็กทรอนิกส์

ส่วนที่ 12

การสำรองข้อมูลและการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

วัตถุประสงค์

- เพื่อให้มีข้อมูลสำรองไว้ใช้งานในกรณีที่ข้อมูลหลักเกิดความเสียหายไม่สามารถใช้งานหรือเข้าถึงได้ หรือเมื่อเกิดภาวะฉุกเฉินต่าง ๆ
- เพื่อให้มีการปฏิบัติที่สอดคล้องกับกฎหมาย พระราชบัญญัติ หรือข้อบังคับภายนอกอื่น ๆ

ผู้รับผิดชอบ

- ผู้บังคับบัญชา
- ผู้ดูแลระบบ
- เจ้าของข้อมูล
- ผู้ใช้งาน

อ้างอิงมาตรฐาน: ISO/IEC 27001:2022

- มาตรการควบคุมด้านองค์กร (Organizational Controls)
- มาตรการควบคุมด้านเทคโนโลยี (Technological Controls)

แนวปฏิบัติ

1. การสำรองข้อมูลระบบแม่ข่าย

ข้อมูลระบบแม่ข่ายและข้อมูลสำคัญซึ่งเป็นความลับของ รพม. ต้องได้รับการเก็บรักษาไว้ที่ระบบเก็บข้อมูล ส่วนกลาง และสำรองข้อมูลไว้อย่างสม่ำเสมอ เพื่อให้มีข้อมูลสำรองไว้ใช้ ในกรณีที่ข้อมูลหลักเกิดความเสียหายหรือไม่สามารถใช้งาน ความถี่ในการดำเนินการสำรองข้อมูลและขั้นตอนการสำรองข้อมูลระบบแม่ข่ายเป็นความรับผิดชอบของ ฝทท. โดยมีแนวปฏิบัติ ดังนี้

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

2. การสำรองข้อมูลคอมพิวเตอร์ส่วนบุคคล

ผู้ใช้งานจะต้องสำรองข้อมูลสำคัญที่เก็บรักษาไว้ในเครื่องคอมพิวเตอร์ส่วนบุคคลหรือคอมพิวเตอร์ หรืออุปกรณ์พกพาอื่น ๆ อย่างสม่ำเสมอ ความถี่ในการสำรองข้อมูลขึ้นอยู่กับความถี่ของการเปลี่ยนแปลงของข้อมูลและระดับความสำคัญของข้อมูลหากเกิดการสูญหาย

3. การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์

เพื่อให้สามารถระบุตัวบุคคลผู้ใช้งานได้อย่างถูกต้อง ผู้ดูแลระบบต้องดำเนินการ ดังนี้

- 3.1 เลือกใช้นาฬิกาจากแหล่งที่น่าเชื่อถือที่มีการเชื่อมต่อในลำดับชั้น Stratum 0 โดยนาฬิกาจากแหล่งดังกล่าวจะต้องได้รับการอนุมัติให้ใช้งาน
- 3.2 ตั้งนาฬิกาของอุปกรณ์ที่ให้บริการทุกชนิดจาก NTP Server ของ รพม. 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 รพม. 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

ส่วนที่ 13

การตรวจสอบและประเมินความเสี่ยง

วัตถุประสงค์

- เพื่อให้มีการตรวจสอบการดำเนินงานของระบบจัดการความมั่นคงปลอดภัยสารสนเทศ และปรับปรุงอย่างต่อเนื่อง
- เพื่อควบคุม และติดตามการปฏิบัติงานของผู้ดูแลระบบสารสนเทศ ให้สอดคล้องตามข้อกำหนด กฎหมาย หรือระเบียบข้อบังคับที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ
- เพื่อประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของสารสนเทศและบริหารจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

ผู้รับผิดชอบ

- ผู้บังคับบัญชา
- ผู้ดูแลระบบ

อ้างอิงมาตรฐาน: ISO/IEC 27001:2022

- ข้อกำหนดหลัก: การวางแผน (Planning)
- ข้อกำหนดหลัก: การตรวจประเมินภายใน (Internal Audit)
- มาตรการควบคุมด้านองค์กร (Organizational Controls)
- มาตรการควบคุมด้านเทคโนโลยี (Technological Controls)

แนวปฏิบัติ

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

8. ผู้ดูแลระบบต้องมีการตรวจสอบการทำงาน (Monitor) ของระบบสารสนเทศอย่างสม่ำเสมอและเสนอผู้บังคับบัญชา รับทราบเมื่อมีเหตุการณ์ผิดปกติเกิดขึ้น รวมถึงแจ้งผู้เกี่ยวข้องเพื่อดำเนินการแก้ไขโดยไม่ชักช้า
9. ผู้ดูแลระบบ ต้องป้องกันการเข้าใช้งานเครื่องมือที่ใช้เพื่อการตรวจสอบ เพื่อมิให้เกิดการใช้งานผิดประเภทหรือถูก ละเมิดการใช้งาน (Compromise) โดยควบคุมการเข้าถึง และตรวจสอบการนำเครื่องมือไปใช้งานอย่างสม่ำเสมอ
10. ผู้ดูแลระบบต้องประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการ เปลี่ยนแปลงอย่างมีนัยสำคัญ
11. ผู้บังคับบัญชาต้องติดตามผลการดำเนินการตามแผนบริหารจัดการความเสี่ยง (Risk Treatment Plan) เป็นประจำทุกไตรมาส
12. ผู้ดูแลระบบต้องประเมินความเสี่ยงแล้วจัดลำดับความสำคัญของความเสี่ยงนั้นและค้นหาวิธีการเพื่อลดความเสี่ยง ตามขั้นตอนที่ รพม. กำหนด พร้อมทั้งพิจารณาข้อดีข้อเสียของวิธีการเหล่านั้นเพื่อให้ผู้บริหารของ รพม. ตัดสินใจ เลือกวิธีการเพื่อลดความเสี่ยงหรือยอมรับความเสี่ยง เมื่อเลือกวิธีการลดความเสี่ยงแล้วผู้บริหารต้องจัดสรร ทรัพยากรอย่างเพียงพอเพื่อดำเนินการ แนวทางการลดความเสี่ยง แบ่งได้เป็น 3 รูปแบบ ได้แก่
 - 12.1 การเลือกใช้เทคโนโลยี เพื่อใช้ในการลดความเสี่ยงและเพิ่มความมั่นคงปลอดภัยของระบบเทคโนโลยี สารสนเทศ รพม. เป็นวิธีที่จำเป็นต้องใช้งบประมาณและทรัพยากรอย่างเพียงพอในการดำเนินการ เช่น การเลือกใช้อุปกรณ์ Firewall มากกว่าหนึ่งผลิตภัณฑ์ในการป้องกันการเข้าถึงเครือข่ายที่สำคัญ การใช้ อุปกรณ์สมาร์ตการ์ด หรือ USB Token ในการตรวจสอบยืนยันตัวตนในการเข้าใช้งานระบบจากภายนอก รพม. เป็นต้น
 - 12.2 การปรับเปลี่ยนขั้นตอนปฏิบัติ ต้องออกแบบขั้นตอนปฏิบัติใหม่ที่รัดกุมและสามารถรักษาความมั่นคง ปลอดภัยของระบบเทคโนโลยีสารสนเทศ รพม. ได้ดีขึ้น เมื่อออกแบบขั้นตอนปฏิบัติใหม่แล้วต้องมีการ พิจารณาหรือความเหมาะสม ความเป็นไปได้ และผู้บริหารต้องเป็นผู้อนุมัติให้มีการบังคับใช้ขั้นตอน ปฏิบัติใหม่นั้น
 - 12.3 ผู้ดูแลระบบต้องแจ้งขั้นตอนปฏิบัติให้ผู้เกี่ยวข้องรับรู้อย่างทั่วถึง รวมทั้งต้องจัดฝึกอบรมผู้ใช้งาน ที่เกี่ยวข้องเพื่อให้สามารถปฏิบัติตามขั้นตอนปฏิบัติใหม่ได้อย่างราบรื่นและมีประสิทธิภาพ
13. การตรวจสอบความปลอดภัยของระบบสารสนเทศ
 - 13.1 ผู้ดูแลระบบ ต้องวางแผนการตรวจสอบและประเมินช่องโหว่หรือจุดอ่อนด้านความมั่นคงปลอดภัย สารสนเทศ และแจ้งผู้ที่เกี่ยวข้องเพื่อแก้ไขในกรณีที่พบว่าช่องโหว่หรือจุดอ่อนนั้นอาจเป็นเหตุการณ์ด้าน ความมั่นคงปลอดภัย อย่างน้อยปีละ 1 ครั้ง
 - 13.2 ผู้ดูแลระบบต้องตรวจสอบระบบสารสนเทศที่จะต้องมีการปรับปรุงเมื่อมีเวอร์ชันใหม่ (Patch) รวมทั้งข้อมูล ที่เกี่ยวข้องกับช่องโหว่ด้านเทคนิคอย่างสม่ำเสมอเพื่อให้ทราบถึงภัยคุกคามและความเสี่ยง รวมถึงหาวิธีป้องกัน และแก้ไขที่เหมาะสมกับช่องโหว่นั้น
 - 13.3 ผู้ใช้งาน ผู้ดูแลระบบ และหน่วยงานภายนอก ต้องบันทึกและรายงานช่องโหว่หรือจุดอ่อนใด ๆ ด้านความมั่นคง ปลอดภัยสารสนเทศ ที่อาจสังเกตพบระหว่างการติดตามการใช้งานระบบสารสนเทศ ผ่านช่องทางบริหาร จัดการที่กำหนดไว้อย่างเหมาะสม และต้องดำเนินการปิดช่องโหว่ที่มีการตรวจพบหรือได้รับแจ้ง
14. การวิเคราะห์ข้อมูลเชิงลึกของภัยคุกคาม (Threat Intelligence)
 - 14.1 ผู้ดูแลระบบต้องรวบรวมข้อมูลที่เกี่ยวข้องกับภัยคุกคามทั้งจากภายในและภายนอกองค์กร เช่น ช่องโหว่ หรือ เหตุการณ์ภัยคุกคามต่าง ๆ ที่เกิดขึ้น
 - 14.2 ผู้ดูแลระบบต้องนำข้อมูลภัยคุกคามที่รวบรวมได้มาวิเคราะห์เชิงลึก ได้แก่ Tactics, Techniques หรือ Procedures (TTPs) ที่กลุ่มผู้ไม่ประสงค์ดีนำมาใช้ รวมถึงแรงจูงใจ เป้าหมาย และพฤติกรรมการณ์โจมตี ของผู้ไม่ประสงค์ดี เพื่อให้ รพม. สามารถจัดเตรียมวิธีการป้องกันหรือวิธีการรับมือกับภัยคุกคาม ได้อย่างมีประสิทธิภาพและทันทั่วถึง

15. ผู้ดูแลระบบต้องมีการบริหารจัดการการเปลี่ยนแปลงเกี่ยวกับการจัดเตรียมการให้บริการ การดูแลปรับปรุงนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ขั้นตอนปฏิบัติงาน หรือการควบคุมเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ โดยคำนึงถึงระดับความสำคัญของการดำเนินธุรกิจที่เกี่ยวข้องและการประเมินความเสี่ยงอย่างต่อเนื่อง
16. การเตรียมความพร้อมกรณีฉุกเฉิน

เพื่อให้มีการบริหารจัดการความต่อเนื่องให้กับกระบวนการทางธุรกิจที่สำคัญขององค์กร เมื่อมีเหตุการณ์ที่ทำให้เกิดการหยุดชะงักหรือติดขัดต่อกระบวนการดังกล่าว โดยมีแนวปฏิบัติ ดังนี้

 - 16.1 ผู้ดูแลระบบต้องกำหนดระบบที่มีความสำคัญทั้งหมดขององค์กร และจัดทำเป็นบัญชีรายชื่อระบบดังกล่าวรวมทั้งปรับปรุงรายชื่อระบบสำคัญและบัญชีฯ ตามความเป็นจริง
 - 16.2 เจ้าของข้อมูลและผู้ดูแลระบบประเมินความเสี่ยงสำหรับระบบเหล่านั้น กำหนดมาตรการเพื่อลดความเสี่ยงที่พบและจัดทำรายงานการประเมินความเสี่ยง
 - 16.3 ผู้ดูแลระบบต้องทบทวน/ปรับปรุงแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) อย่างน้อยปีละ 1 ครั้ง
 - 16.4 ผู้ดูแลระบบจัดทำและปรับปรุงแผนกู้คืนระบบอย่างน้อยปีละ 1 ครั้ง
 - 16.5 เจ้าของข้อมูลและผู้ดูแลระบบต้องทดสอบแผนบริหารความต่อเนื่องทางธุรกิจและแผนกู้คืนระบบอย่างน้อยปีละ 1 ครั้ง พร้อมทั้งบันทึกผลการทดสอบรวมถึงปัญหาที่พบ และนำเสนอผลการทดสอบและแนวทางแก้ไขต่อผู้บังคับบัญชา
 - 16.6 ผู้ดูแลระบบต้องจัดประชุมและชี้แจงให้ผู้ที่เกี่ยวข้องทั้งหมดได้รับทราบเกี่ยวกับแผนบริหารความต่อเนื่องทางธุรกิจและแผนกู้คืน และผลของการฝึกซ้อมการกู้คืนระบบและผลการทดสอบแผนบริหารความต่อเนื่องทางธุรกิจ

ส่วนที่ 14

การถ่ายโอน และแลกเปลี่ยนข้อมูลสารสนเทศ

วัตถุประสงค์

- เพื่อให้มีการควบคุมการถ่ายโอนและแลกเปลี่ยนข้อมูลสารสนเทศ ป้องกันการรั่วไหล หรือมีการแก้ไขข้อมูลโดยที่ไม่ได้รับอนุญาต รวมถึงการป้องกันสื่อบันทึกข้อมูลให้มีความปลอดภัยเป็นไปตามข้อกำหนด

ผู้รับผิดชอบ

- ผู้บังคับบัญชา
- เจ้าของข้อมูล
- ผู้ดูแลระบบ

อ้างอิงมาตรฐาน: ISO/IEC 27001:2022

- มาตรการควบคุมด้านองค์กร (Organizational Controls)
- มาตรการควบคุมด้านเทคโนโลยี (Technological Controls)

แนวปฏิบัติ

1. ผู้บังคับบัญชา ต้องควบคุมให้มีการจัดทำนโยบาย และขั้นตอนการปฏิบัติเพื่อป้องกันข้อมูลสารสนเทศที่มีการสื่อสาร หรือแลกเปลี่ยนผ่านระบบสารสนเทศให้เหมาะสมตามระดับชั้นความลับข้อมูลสารสนเทศ ตามขั้นตอนที่ รฟม. กำหนด
2. ผู้บังคับบัญชา และเจ้าของข้อมูล ต้องควบคุมให้มีการจัดทำข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศระหว่าง องค์กรกับบุคคลหรือหน่วยงานภายนอก
3. ผู้ดูแลระบบต้องแลกเปลี่ยนข้อมูลสารสนเทศต้องแลกเปลี่ยนผ่านช่องทางที่ปลอดภัย เช่น Web Service ที่ใช้งานผ่านโปรโตคอล HTTPS
4. ผู้ดูแลระบบต้องปิดบังข้อมูล (Data Masking) ทั้งข้อมูลส่วนบุคคลและข้อมูลอ่อนไหวขององค์กร (Sensitive Data) ที่มีการถ่ายโอนหรือแลกเปลี่ยนข้อมูล
5. ผู้ดูแลระบบ ต้องมีการป้องกันข้อมูลสารสนเทศที่มีการสื่อสารกันผ่านข้อมูลอิเล็กทรอนิกส์ (Electronic Messaging) เช่น จดหมายอิเล็กทรอนิกส์ (Email) หรือ Instant Messaging ด้วยวิธีการหรือมาตรการที่เหมาะสม
6. ผู้ดูแลระบบ ต้องป้องกันข้อมูลสารสนเทศที่มีการแลกเปลี่ยนในการทำพาณิชย์อิเล็กทรอนิกส์ (Electronic Commerce) ผ่านเครือข่ายคอมพิวเตอร์สาธารณะ เพื่อมิให้มีการฉ้อโกง ละเมิดสัญญา หรือมีการรั่วไหล หรือข้อมูลสารสนเทศถูกแก้ไขโดยมิได้รับอนุญาต
7. ผู้ดูแลระบบ ต้องป้องกันข้อมูลสารสนเทศที่มีการสื่อสาร หรือแลกเปลี่ยนในการทำธุรกรรมทางออนไลน์ (Online Transaction) เพื่อมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ ส่งข้อมูลไปผิดที่ การรั่วไหลของข้อมูล ข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ หรือถูกส่งซ้ำโดยมิได้รับอนุญาต
8. ผู้ดูแลระบบ ต้องควบคุมการรับส่งข้อมูลสารสนเทศเพื่อป้องกันความผิดพลาด ดังนี้
 - 8.1 ความไม่สมบูรณ์ของข้อมูลสารสนเทศที่รับ-ส่ง
 - 8.2 การส่งข้อมูลสารสนเทศผิดจุดหมายปลายทาง
 - 8.3 การเปลี่ยนแปลงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต
 - 8.4 การเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต
 - 8.5 การเข้าถึงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต
 - 8.6 การนำข้อมูลสารสนเทศกลับมาใช้ใหม่โดยไม่ได้รับอนุญาต
9. เจ้าของข้อมูล และผู้ดูแลระบบ ต้องมีการป้องกันข้อมูลสารสนเทศที่มีการเผยแพร่ต่อสาธารณชน มิให้มีการแก้ไขเปลี่ยนแปลงโดยมิได้รับอนุญาต เพื่อรักษาความถูกต้องครบถ้วนของข้อมูลสารสนเทศ

ส่วนที่ 15

การควบคุมการเข้ารหัส

วัตถุประสงค์

- เพื่อให้มีการเข้ารหัสข้อมูลอย่างเหมาะสมและมีประสิทธิภาพในการปกป้องความลับ ป้องกัน การปลอมแปลงข้อมูล และ ควบคุมความถูกต้องของข้อมูล

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- เจ้าของข้อมูล
- ผู้ใช้งาน

อ้างอิงมาตรฐาน: ISO/IEC 27001:2022

- มาตรการควบคุมด้านเทคโนโลยี (Technological Controls)

แนวปฏิบัติ

- เจ้าของข้อมูล ต้องเข้ารหัส หรือการใส่รหัสผ่านข้อมูลอิเล็กทรอนิกส์ขององค์กรตามระดับชั้นความลับเพื่อป้องกัน ผู้ไม่มีสิทธิ์เข้าถึง ตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และตามขั้นตอนที่ รพม. กำหนด
- เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ใช้งานต้องปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 ในการนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับจะต้องใช้วิธีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล
- ผู้ดูแลระบบ ต้องใช้วิธีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล หลีกเลี่ยงการใช้รูปแบบการเข้ารหัส ที่พัฒนาขึ้นเอง 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

- ผู้ดูแลระบบ ต้องมีการทบทวนขั้นตอนวิธี (Algorithm) และความยาวของกุญแจที่เข้ารหัสอย่างน้อยปีละ 1 ครั้ง เพื่อให้ยังสามารถรักษาไว้ซึ่งความมั่นคงปลอดภัย
- ผู้ดูแลระบบ ต้องกำหนดให้มีการบริหารจัดการกุญแจที่ใช้ในการเข้ารหัส ดังนี้
 - การสร้างกุญแจรหัสควรกระทำในสถานที่ที่มีมาตรการป้องกันความปลอดภัย
 - เมื่อมีการสร้างกุญแจรหัสที่เป็นกุญแจลับ (Private key) ควรส่งมอบให้กับเจ้าของกุญแจโดยตรง โดยวิธีการที่ปลอดภัย
 - ควรจัดให้มีการเก็บบันทึก Log เพื่อการตรวจสอบสำหรับกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับการจัดการกุญแจรหัส
- ผู้ใช้งาน ควรรักษาความปลอดภัยในการใช้งานกุญแจ ดังนี้
 - เก็บกุญแจรหัสในสถานที่ที่ปลอดภัย เช่น ตู้รับภัย หรือสื่อบันทึกที่ปลอดภัย และไม่มีใครสามารถเข้าถึงได้
 - เมื่อมีการรับกุญแจสาธารณะ (Public Key) มาใช้ ก่อนใช้งานจะต้องพิสูจน์ความถูกต้องของกุญแจสาธารณะ โดยสอบถามกับผู้ส่งหรือตรวจสอบกับผู้แทนในการรับรองความถูกต้องของกุญแจสาธารณะ (Certificate Authority) ที่เชื่อถือได้เท่านั้น
 - ควบคุมการใช้งานและจัดเก็บกุญแจให้สอดคล้องกับการรักษาความลับข้อมูลตามที่ รพม. กำหนด

ส่วนที่ 16

การนำอุปกรณ์ส่วนตัวมาใช้งาน (Bring your own device)

วัตถุประสงค์

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

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

อ้างอิงมาตรฐาน: ISO/IEC 27001:2022

- มาตรการควบคุมด้านบุคลากร (People Controls)
- มาตรการควบคุมด้านเทคโนโลยี (Technological Controls)

แนวปฏิบัติ

1. ผู้ดูแลระบบต้องกำหนดคุณสมบัติของระบบปฏิบัติการของอุปกรณ์ส่วนตัวที่อนุญาตให้นำมาเชื่อมต่อหรือเข้าถึงระบบงานสารสนเทศของ รพม. ได้ โดยต้องเป็นระบบปฏิบัติการที่ไม่ล้าสมัย (Obsolete Operating System) และยังได้รับการสนับสนุนการใช้งานจากเจ้าของผลิตภัณฑ์
2. ผู้ดูแลระบบต้องตัดการเชื่อมต่อหากระบบปฏิบัติการของอุปกรณ์ส่วนตัวที่อนุญาตให้นำมาเชื่อมต่อหรือเข้าถึงระบบงานสารสนเทศของ รพม. เกิดการล้าสมัย (Obsolete Operating System) หรือเจ้าของผลิตภัณฑ์ไม่สนับสนุนการใช้งานแล้ว
3. ผู้ดูแลระบบต้องมีมาตรการป้องกันมัลแวร์ และตรวจสอบการอัปเดต Patch เวอร์ชันของระบบปฏิบัติการที่เจ้าของผลิตภัณฑ์ยังให้การสนับสนุนการใช้งาน
4. ผู้ดูแลระบบต้องไม่อนุญาตให้อุปกรณ์ที่มีการปรับแต่งการเข้าถึงระบบปฏิบัติการ (Rooted/Jailbroken) มาเชื่อมต่อหรือเข้าถึงระบบสารสนเทศของ รพม.
5. ผู้ดูแลระบบต้องแบ่งแยกเครือข่ายของอุปกรณ์ส่วนตัวที่นำมาเชื่อมต่อหรือเข้าถึงระบบสารสนเทศของ รพม.
6. ผู้ดูแลระบบต้องทบทวนเวอร์ชันของระบบปฏิบัติการที่อนุญาตให้นำมาเชื่อมต่อกับระบบสารสนเทศของ รพม. อย่างน้อยปีละ 2 ครั้ง หากมีการเปลี่ยนแปลงเวอร์ชันของระบบปฏิบัติการที่อนุญาตให้เข้าถึงระบบสารสนเทศของ รพม. ผู้ดูแลระบบต้องแจ้งให้ผู้ใช้งานรับทราบล่วงหน้า 7 วัน ก่อนเริ่มบังคับใช้
7. ผู้ใช้งานต้องติดตั้งโปรแกรมป้องกันมัลแวร์ตามเงื่อนไขที่ รพม. กำหนด
8. ผู้ใช้งานต้องไม่นำอุปกรณ์ส่วนตัวที่ติดตั้งแอปพลิเคชันนอก Official Store มาเชื่อมต่อหรือเข้าถึงระบบงานสารสนเทศของ รพม.
9. ผู้ใช้งานต้องไม่นำอุปกรณ์ส่วนตัวที่ติดตั้งโปรแกรมละเมิดลิขสิทธิ์มาเชื่อมต่อหรือเข้าถึงระบบงานสารสนเทศของ รพม.
10. ผู้ใช้งานต้องอัปเดต Patch ของระบบปฏิบัติการที่อุปกรณ์ส่วนตัวให้เป็นเวอร์ชันล่าสุด รวมถึงต้องเป็นระบบปฏิบัติการที่เจ้าของผลิตภัณฑ์ยังให้การสนับสนุนการใช้งาน
11. ผู้ใช้งานต้องยืนยันตัวตนก่อนเข้าถึงระบบสารสนเทศของ รพม. ทุกครั้ง
12. ผู้ใช้งานต้องติดตั้ง Network Access Control agent (NAC agent) หรือ Mobile Device Management Agent (MDM Agent) ตามที่ รพม. กำหนด เพื่อควบคุมการใช้งานเครือข่ายและการเข้าถึงระบบสารสนเทศของ รพม.
13. กรณีอุปกรณ์ส่วนตัวสูญหายหรือถูกขโมยผู้ใช้งานต้องแจ้งผู้ดูแลระบบโดยเร็วที่สุด เพื่อจัดการข้อมูลที่จัดเก็บอยู่ในอุปกรณ์ส่วนตัวของผู้ใช้งาน
14. ผู้ใช้งานต้องเข้าถึงระบบสารสนเทศของ รพม. ผ่านช่องทางที่ รพม. กำหนด เช่น VPN

ส่วนที่ 17

การใช้บริการ Cloud (Cloud Services)

วัตถุประสงค์

- เพื่อควบคุมการเลือกใช้งาน การบริหารจัดการ และการยกเลิกการใช้บริการ Cloud อย่างปลอดภัย

ผู้รับผิดชอบ

- ผู้บังคับบัญชา
- ผู้ดูแลระบบ
- เจ้าของระบบ/เจ้าของข้อมูล

อ้างอิงมาตรฐาน: ISO/IEC 27001:2022

- มาตรการควบคุมด้านองค์กร (Organizational Controls)

แนวปฏิบัติ

1. ผู้บังคับบัญชาต้องควบคุม กำกับ ดูแล ให้การใช้งานบริการ Cloud สอดคล้องตามที่กฎหมาย นโยบาย ระเบียบ หรือข้อบังคับที่ภาครัฐกำหนด
2. ผู้ดูแลระบบต้องวิเคราะห์ความเสี่ยงก่อนเลือกบริการ Cloud มาใช้งานภายในองค์กร
3. ผู้ดูแลระบบต้องเลือกใช้บริการ Cloud ตามที่กฎหมาย นโยบาย ระเบียบ หรือข้อบังคับที่ภาครัฐกำหนด
4. ผู้ดูแลระบบต้องเลือกผู้ให้บริการ Cloud (Cloud Service Provider) ที่เหมาะสมกับการดำเนินงานองค์กร
5. ผู้ดูแลระบบต้องพิจารณาข้อกำหนดหรือเงื่อนไขของผู้ให้บริการ Cloud (Cloud Service Provider) ให้ชัดเจน ก่อนตัดสินใจเลือกใช้บริการ
6. ผู้ดูแลระบบต้องเลือกใช้บริการ Cloud ที่เหมาะสมกับการดำเนินงานขององค์กร
7. ผู้ดูแลระบบต้องเลือกใช้บริการ Cloud ที่มีการรักษาความปลอดภัย การบริหารจัดการความต่อเนื่องทางธุรกิจ และการจัดให้มีระบบฉุกเฉินสำรองตามมาตรฐานสากล เช่น ISO, NIST หรือ CSA STAR
8. ผู้ดูแลระบบต้องเลือกใช้บริการ Cloud ที่มีความพร้อมใช้งานของบริการครอบคลุมร้อยละของเวลาที่พร้อมให้บริการต่อปี (Uptime) อย่างน้อยร้อยละ 99.00
9. ผู้ดูแลระบบต้องเลือกใช้บริการ Cloud ที่มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation: GDPR) หรือเทียบเท่า
10. ผู้ดูแลระบบ และเจ้าของระบบ/เจ้าของข้อมูลต้องพิจารณาเอกสารสนเทศที่จะนำไปใช้งานบนระบบ Cloud ให้สอดคล้องตามที่กฎหมาย นโยบาย ระเบียบ หรือข้อบังคับที่ภาครัฐกำหนด
11. ผู้ดูแลระบบต้องติดตาม ทบทวน และประเมินผลการใช้บริการ Cloud อย่างน้อยปีละ 1 ครั้ง

ภาคผนวก ค



สัญญาการเก็บรักษาข้อมูลไว้เป็นความลับ

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

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

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

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

ทั้งสองฝ่ายจึงตกลงทำสัญญากัน ดังมีข้อความต่อไปนี้

1. ในสัญญาฉบับนี้ “ข้อมูล” หมายถึง สิ่งที่มีสาระสำคัญให้รู้เรื่องราวข้อเท็จจริง ข้อมูลหรือสิ่งใด ๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพสิ่งของนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

2. ผู้รับข้อมูลให้สัญญาแก่ รฟม. ว่าข้อมูลที่รับจาก รฟม. หรือในนามของ รฟม. ผู้รับข้อมูลจะใช้เพื่อประกอบการปฏิบัติงานที่เกี่ยวข้องสำหรับดำเนินโครงการ
ตามสัญญาโครงการเท่านั้น และจะไม่นำไปใช้เพื่อวัตถุประสงค์อื่น เช่น ใช้เพื่อวัตถุประสงค์ในเชิงพาณิชย์ การพัฒนาเป็นผลิตภัณฑ์หรือเทคโนโลยีอื่น การใช้หรือพยายามใช้ข้อมูลเพื่อการอื่น การอ้างอิงหรือรวมเข้าไปเป็นส่วนหนึ่งของการประดิษฐ์ใด ๆ การรับขอความคุ้มครองจากทรัพย์สินทางปัญญาใด ๆ ของผู้รับข้อมูล เว้นแต่ได้รับการอนุญาตจาก รฟม. เป็นลายลักษณ์อักษรก่อน

3. ผู้รับข้อมูลจะต้องปกปิดข้อมูลทั้งหมดที่ได้มีการเปิดเผยภายใต้สัญญาโครงการนี้ไว้เป็นความลับอย่างเคร่งครัด

4. ถ้าข้อกำหนดใด ๆ ตามสัญญาฉบับนี้ตกเป็นโมฆะ ให้ข้อสัญญาที่เหลืออยู่ในสัญญาฉบับนี้คงใช้บังคับและมีผลอยู่อย่างสมบูรณ์

5. หากผู้รับข้อมูลไม่ปฏิบัติตามกฎหมาย หรือฝ่าฝืนสัญญาไม่ว่าข้อใดข้อหนึ่ง ผู้รับข้อมูลยินยอมชดใช้ค่าเสียหายใด ๆ ที่เกิดขึ้นหรือที่เกี่ยวข้องเนื่องแก่ รพม. ทั้งสิ้น

สัญญานี้ทำขึ้นเป็นสองฉบับมีข้อความถูกต้องตรงกัน คู่สัญญาได้อ่านและเข้าใจข้อความในสัญญานี้แล้ว เห็นว่าถูกต้องตรงตามเจตนาของตน จึงได้ลงนามและประทับตรา (ถ้ามี) ไว้ต่อหน้าพยานและยึดถือไว้ฝ่ายละหนึ่งฉบับ

การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

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

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

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

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