ต้นฉบับ

สัญญาเช่าระบบงานพิมพ์พร้อมหมึกพิมพ์

ประจำปีงบประมาณ ๒๕๖๗ - ๒๕๖๙

ระหว่าง

การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

กับ

บริษัท เคียวเซร่า ด็อกคิวเม้นท์ โซลูชั่น (ประเทศไทย) จำกัด

สัญญาเลขที่ ช.๒๕๖๗/๒

สัญญาเช่าระบบงานพิมพ์พร้อมหมึกพิมพ์ ประจำปีงบประมาณ ๒๕๖๗ - ๒๕๖๙

สัญญาเลขที่ ช.๒๕๖๗/๒

สัญญาฉบับนี้ทำขึ้น ณ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย สำนักงานตั้งอยู่เลขที่ ๑๗๕ ถนนพระราม ๙ แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร เมื่อวันที่ ๒ ตุลาคม ๒๕๖๖ ระหว่าง การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย โดยนายทวิช พึ่งตน ตำแหน่งผู้อำนวยการฝ่ายจัดซื้อและบริการ ปฏิบัติการแทนผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย ซึ่งต่อไปในสัญญานี้เรียกกว่า "ผู้เช่า" ฝ่ายหนึ่ง กับ บริษัท เคียวเซร่า ด็อกคิวเม้นท์ โซลูชั่น (ประเทศไทย) จำกัด ซึ่งจดทะเบียนเป็นนิติบุคคล ณ สำนักงานทะเบียนหุ้นส่วนบริษัท กรุงเทพมหานคร กรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ มีสำนักงานใหญ่อยู่เลขที่ ๓๓๕ ถนนรัชดาภิเษก แขวงวงศ์สว่าง เขตบางซื่อ กรุงเทพมหานคร โดย นายธงชัย อินทร์โสม ผู้รับมอบอำนาจจากผู้มีอำนาจลงนามผูกพันนิติบุคคล ปรากฏตามหนังสือรับรองของ สำนักงานทะเบียนหุ้นส่วนบริษัทกลาง กรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ ที่ E๑๐๐๙๑๒๒๐๔๗๑๘๖๘ ลงวันที่ ๒๙ สิงหาคม ๒๕๖๖ และหนังสือมอบอำนาจลงวันที่ ๒๘ กันยายน ๒๕๖๖ แนบท้ายสัญญานี้ ซึ่งต่อไปในสัญญานี้เรียกว่า "ผู้ให้เช่า" อีกฝ่ายหนึ่ง

คู่สัญญาได้ตกลงกันมีข้อความดังต่อไปนี้

ข้อ ๑. ข้อตกลงเช่า

ผู้เช่าตกลงเช่าและผู้ให้เช่าตกลงให้เช่าระบบงานพิมพ์พร้อมหมึกพิมพ์

๑.๑ เครื่องพิมพ์ ขาว-ดำ ขนาด A๔ จำนวน ๑๙ ชุด
ยี่ห้อ เคียวเซร่า รุ่น ECOSYS P๓๑๔๕dn

๑.๒ เครื่องพิมพ์ สี ขนาด A๔ จำนวน ๘ ชุด
ยี่ห้อ เคียวเซร่า รุ่น ECOSYS P๖๒๓๐cdn

๑.๓ เครื่องพิมพ์ สี ขนาด A๓ จำนวน ๙ ชุด
ยี่ห้อ เคียวเซร่า รุ่น TASKalfa ๓๕๕๔ci

๑.๔ เครื่องพิมพ์มัลติฟังก์ชัน สี ขนาด A๔ จำนวน ๔ ชุด
ยี่ห้อ เคียวเซร่า รุ่น ECOSYS M๖๖๓๕cidn

ซึ่งต่อไปในสัญญานี้เรียกว่า "ระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่า" เพื่อใช้ในกิจการของผู้เช่า ตามเอกสารแนบท้ายสัญญาผนวก ๑ และผนวก ๓

การเช่าระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่าตามวรรคหนึ่งมีผลบังคับตั้งแต่วันที่ลงนามในสัญญา แต่ระยะเวลาการคำนวณค่าเช่าตามสัญญานี้ให้มีกำหนดเริ่มตั้งแต่วันที่ ๑ ตุลาคม ๒๕๖๖ ถึงวันที่ ๓๐ กันยายน ๒๕๖๙ ทั้งนี้ระยะเวลาการคำนวณค่าเช่า ไม่นับรวมระยะเวลาติดตั้งและส่งมอบ

ผู้ให้เช่ารับรองว่าระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่าตามสัญญานี้เป็นระบบงานพิมพ์ใหม่ที่ไม่เคยใช้งานมาก่อน ผู้ให้เช่าได้ชำระภาษี อากร ค่าธรรมเนียมต่าง ๆ ครบถ้วนถูกต้องตามกฎหมายแล้ว ผู้ให้เช่ามีสิทธินำมาให้เช่าโดยปราศจากการรอนสิทธิ ทั้งรับรองว่าระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่ามีคุณสมบัติ คุณภาพและคุณลักษณะไม่ต่ำกว่าที่กำหนดไว้ในเอกสารแนบท้ายสัญญา ผนวก ๑ และ ผนวก ๓ และผู้ให้เช่าได้ตรวจสอบแล้วว่าระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่าตลอดจนอุปกรณ์ทั้งปวงปราศจากความชำรุดบกพร่อง

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA Document Solutions (Thailand) Corp., Ltd.

/ข้อ ๒. ค่าเช่า...

ข้อ ๒. ค่าเช่าระบบงานพิมพ์พร้อมหมึกพิมพ์

ผู้เช่าตกลงชำระค่าเช่าแก่ผู้ให้เช่าเป็นรายเดือนตามเดือนปฏิทินในอัตราค่าเช่าภายในวงเงินตามสัญญา จำนวนเงิน ๖,๔๐๖,๐๙๐.๐๐ บาท (หกล้านสี่แสนหกพันเก้าสิบบาทถ้วน) ซึ่งได้รวมภาษีมูลค่าเพิ่มตลอดจนภาษีอากรและค่าใช้จ่ายอื่นทั้งปวงด้วยแล้ว ในการคำนวณค่าเช่าเป็นรายเดือน ให้คำนวณจากปริมาณการพิมพ์ทั้งหมดในแต่ละเดือน (หักด้วยจำนวนกระดาษเสียจากที่ใช้งานจริงต่อเครื่องจำนวนไม่น้อยกว่าร้อยละ ๓ (สาม))

ปริมาณการพิมพ์ตามความในวรรคหนึ่ง ให้หมายความถึงกระดาษที่พิมพ์ออกมาโดยเรียบร้อยสมบูรณ์เท่านั้น การวินิจฉัยว่ากระดาษแผ่นใดเป็นกระดาษที่พิมพ์ออกมาเรียบร้อยสมบูรณ์หรือเป็นกระดาษเสียให้เป็นดุลพินิจของผู้เช่าหรือเจ้าหน้าที่ของผู้เช่า และการวินิจฉัยดังกล่าวให้เป็นที่สุด ผู้ให้เช่าจะโต้แย้งใด ๆ มิได้

ค่าเช่าตามวรรคหนึ่งได้รวมภาษีมูลค่าเพิ่ม ค่าใช้จ่ายในการบำรุงรักษาและซ่อมแซม ค่าตรวจสภาพ ค่าอะไหล่ ค่าวัสดุสิ้นเปลือง (ยกเว้นค่ากระดาษถ่ายเอกสาร) ไว้ด้วยแล้ว

ในการชำระค่าเช่า ผู้ให้เช่าต้องส่งใบแจ้งหนี้เรียกเก็บค่าเช่าเมื่อสิ้นเดือนแต่ละเดือน โดยผู้เช่าจะชำระค่าเช่าหลังจากที่ได้ตรวจสอบแล้วว่าถูกต้อง

ในกรณีที่การเช่าเดือนแรกและเดือนสุดท้ายเป็นการเช่าไม่เต็มเดือนปฏิทิน ให้ใช้วิธีการคำนวณค่าเช่าตามวรรคหนึ่ง แต่อัตราค่าเช่าให้คิดเป็นรายวันตามจำนวนวันที่เช่าจริง โดยคำนวณจากเดือนหนึ่งมี ๓๐ (สามสิบ) วัน

ข้อ ๓. เอกสารอันเป็นส่วนหนึ่งของสัญญา

เอกสารแนบท้ายสัญญาดังต่อไปนี้ให้ถือเป็นส่วนหนึ่งของสัญญานี้

๓.๑ ผนวก ๑	ขอบเขตของงานเช่าระบบงานพิมพ์พร้อมหมึกพิมพ์ ประจำปีงบประมาณ ๒๕๖๗ – ๒๕๖๙	จำนวน ๖๙ (หกสิบเก้า) หน้า
๓.๒ ผนวก ๒	ใบเสนอราคาเช่าด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding) และหนังสือยืนยันราคา	จำนวน ๓ (สาม) หน้า
๓.๓ ผนวก ๓	แค็ตตาล็อก คุณลักษณะและรายละเอียดของระบบงานพิมพ์ที่เช่า	จำนวน ๑๗ (สิบเจ็ด) หน้า
๓.๔ ผนวก ๔	เอกสารเกี่ยวกับนิติบุคคลของผู้ให้เช่า หนังสือมอบอำนาจ หลักประกันสัญญา และเอกสารอื่นที่เกี่ยวข้อง	จำนวน ๒๙ (ยี่สิบเก้า) หน้า

ความใดในเอกสารแนบท้ายสัญญาที่ขัดหรือแย้งกับข้อความในสัญญานี้ ให้ใช้ข้อความในสัญญานี้บังคับ และในกรณีที่เอกสารแนบท้ายสัญญาขัดแย้งกันเอง ผู้ให้เช่าจะต้องปฏิบัติตามคำวินิจฉัยของผู้เช่า คำวินิจฉัยของผู้เช่าให้ถือเป็นที่สุด และผู้ให้เช่าไม่มีสิทธิเรียกร้องค่าเช่า ค่าเสียหาย หรือค่าใช้จ่ายใด ๆ เพิ่มเติมจากผู้เช่าทั้งสิ้น

ข้อ ๔. การส่งมอบ

ผู้ให้เช่าต้องส่งมอบและติดตั้งระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่าตามสัญญานี้ ให้ถูกต้องครบถ้วนตามสัญญานี้ ในลักษณะพร้อมใช้งานได้ตามที่กำหนด ณ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย ภายใน ๖๐ วัน นับถัดจากวันที่ลงนามในสัญญา ซึ่งผู้ให้เช่าเป็นผู้จัดหาอุปกรณ์ประกอบ พร้อมทั้งเครื่องมือที่จำเป็นในการติดตั้งและใช้งาน โดยผู้ให้เช่าเป็นผู้ออกค่าใช้จ่ายเองทั้งสิ้น

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd

/ทั้งนี้ ผู้ให้เช่า...

ทั้งนี้ ผู้ให้เช่าต้องแจ้งเวลาติดตั้งแล้วเสร็จพร้อมที่จะใช้งานและส่งมอบเครื่องได้เป็นหนังสือต่อผู้เช่า ณ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย ในวันและเวลาทำการของผู้เช่าก่อนวันกำหนดส่งมอบตามวรรคหนึ่งไม่น้อยกว่า ๓ (สาม) วันทำการของผู้เช่า

ในการส่งมอบตามวรรคหนึ่ง ผู้ให้เช่าต้องส่งพนักงานมาดำเนินการทดสอบประสิทธิภาพและแนะนำวิธีการใช้เครื่องให้คณะกรรมการตรวจรับพัสดุได้พิจารณาตามรายละเอียดคุณลักษณะเฉพาะที่ระบุไว้ในข้อ ๑ และสำเนาที่ถ่ายจะต้องมีความชัดเจนสะอาดไม่มีรอยหมึกเปื้อนตามส่วนต่าง ๆ โดยในการนี้ผู้ให้เช่าไม่คิดค่าใช้จ่ายใด ๆ จากผู้เช่าทั้งสิ้น

ข้อ ๕. การตรวจรับ

เมื่อผู้เช่าได้ตรวจรับระบบงานพิมพ์พร้อมหมึกพิมพ์ที่ส่งมอบตามข้อ ๔ และเห็นว่าถูกต้องครบถ้วนตามสัญญานี้แล้ว ผู้เช่าจะออกหลักฐานการรับมอบระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่าไว้เป็นหนังสือเพื่อผู้ให้เช่านำมาใช้เป็นหลักฐานประกอบการขอรับเงินค่าเช่า

ในการตรวจรับระบบงานพิมพ์พร้อมหมึกพิมพ์ที่ส่งมอบตามวรรคหนึ่ง ถ้าปรากฏว่าระบบงานพิมพ์พร้อมหมึกพิมพ์ซึ่งผู้ให้เช่าส่งมอบไม่ถูกต้องครบถ้วนตามสัญญา หรือติดตั้งและส่งมอบถูกต้องครบถ้วนภายในกำหนดแต่ไม่สามารถใช้งานได้อย่างครบถ้วนและมีประสิทธิภาพตามสัญญา ผู้เช่าทรงไว้ซึ่งสิทธิที่จะไม่รับระบบงานพิมพ์พร้อมหมึกพิมพ์นั้น ในกรณีเช่นว่านี้ ผู้ให้เช่าต้องรีบนำระบบงานพิมพ์พร้อมหมึกพิมพ์นั้นกลับคืนไปทันที และต้องนำระบบงานพิมพ์พร้อมหมึกพิมพ์เครื่องใหม่ที่มีคุณสมบัติเดียวกัน หรือไม่ต่ำกว่าระบบงานพิมพ์พร้อมหมึกพิมพ์ที่กำหนดไว้ในสัญญานี้ มาส่งมอบให้ใหม่ ภายในกำหนดตามที่ได้รับแจ้งเป็นหนังสือจากผู้เช่าด้วยค่าใช้จ่ายของผู้ให้เช่าเองทั้งสิ้น และระยะเวลาที่เสียไปเพราะเหตุดังกล่าว ผู้ให้เช่าจะนำมาอ้างเป็นเหตุของดหรือลดค่าปรับหรือขยายเวลาส่งมอบไม่ได้

หากผู้ให้เช่าไม่นำระบบงานพิมพ์พร้อมหมึกพิมพ์ที่ส่งมอบไม่ถูกต้องกลับคืนไปในทันทีดังกล่าวในวรรคสอง และเกิดความเสียหายแก่ระบบงานพิมพ์พร้อมหมึกพิมพ์นั้น ผู้เช่าไม่ต้องรับผิดชอบในความเสียหายดังกล่าว

ในกรณีที่ผู้ให้เช่าส่งมอบระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่าถูกต้องแต่ไม่ครบจำนวน หรือส่งมอบครบจำนวนแต่ไม่ถูกต้องทั้งหมด ผู้เช่ามีสิทธิจะรับมอบเฉพาะส่วนที่ถูกต้อง โดยออกหลักฐานการรับมอบเฉพาะส่วนนั้นก็ได้ ในกรณีเช่นนี้ผู้เช่าจะชำระค่าเช่าเฉพาะระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่าที่รับมอบไว้

ข้อ ๖. การงดหรือลดค่าปรับ หรือขยายเวลาในการปฏิบัติตามสัญญา

ในกรณีที่ผู้ให้เช่าไม่สามารถส่งมอบระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่าให้แก่ผู้เช่าได้โดยครบถ้วนถูกต้องภายในกำหนดเวลาตามสัญญา หรือถ้าผู้ให้เช่าไม่ดำเนินการหรือไม่สามารถซ่อมแซมแก้ไขระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่าภายในระยะเวลาตามข้อ ๘.๒ และผู้ให้เช่าไม่จัดหาเครื่องระบบงานพิมพ์พร้อมหมึกพิมพ์ให้ผู้เช่าใช้แทนตามข้อ ๘.๓ อันเนื่องมาจากเหตุสุดวิสัย หรือเหตุใด ๆ อันเนื่องมาจากความผิดหรือความบกพร่องของฝ่ายผู้เช่า หรือจากพฤติการณ์อันหนึ่งอันใดที่ผู้ให้เช่าไม่ต้องรับผิดตามกฎหมาย หรือเหตุอื่นตามที่กำหนดในกฎกระทรวง ซึ่งออกตามความในกฎหมายว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ ผู้ให้เช่ามีสิทธิของดหรือลดค่าปรับหรือขยายกำหนดเวลาทำการตามสัญญาดังกล่าว โดยจะต้องแจ้งเหตุหรือพฤติการณ์ดังกล่าวพร้อมหลักฐานเป็นหนังสือให้ผู้เช่าทราบภายใน ๑๕ (สิบห้า) วัน นับถัดจากวันที่เหตุนั้นได้สิ้นสุดลง หรือตามที่กำหนดในกฎกระทรวงดังกล่าว แล้วแต่กรณี

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd.

/ถ้าผู้ให้เช่า...

ถ้าผู้ให้เช่าไม่ปฏิบัติให้เป็นไปตามความในวรรคหนึ่ง ให้ถือว่าผู้ให้เช่าได้สละสิทธิเรียกร้องในการที่จะของดหรือลดค่าปรับหรือขยายเวลาทำการตามสัญญาโดยไม่มีเงื่อนไขใด ๆ ทั้งสิ้น เว้นแต่กรณีเหตุเกิดจากความผิดหรือความบกพร่องของฝ่ายผู้เช่าซึ่งมีหลักฐานชัดแจ้ง หรือผู้เช่าทราบดีอยู่แล้วตั้งแต่ต้น

การงดหรือลดค่าปรับหรือขยายกำหนดเวลาทำการตามสัญญาตามวรรคหนึ่ง อยู่ในดุลพินิจของผู้เช่าที่จะพิจารณาตามที่เห็นสมควร

ข้อ ๗. การบำรุงรักษาตรวจสภาพและซ่อมแซมระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่า

ผู้ให้เช่ามีหน้าที่บำรุงรักษาระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่าให้อยู่ในสภาพใช้งานได้ดีอยู่เสมอด้วยค่าใช้จ่ายของผู้ให้เช่า โดยต้องจัดหาช่างผู้มีความรู้ ความชำนาญ และฝีมือดีมาตรวจสอบ บำรุงรักษาและซ่อมแซมแก้ไขระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่าตลอดอายุสัญญาเช่านี้ ให้เป็นไปตามขอบเขตของงานเช่าระบบงานพิมพ์พร้อมหมึกพิมพ์ ประจำปีงบประมาณ ๒๕๖๗ – ๒๕๖๙ แนบท้ายสัญญา ผนวก ๑

สิ่งของที่ใช้สิ้นเปลืองทุกชนิดรวมทั้งอะไหล่ ยกเว้นกระดาษสำหรับถ่ายเอกสาร ผู้ให้เช่าจะเป็นผู้จัดส่งให้โดยไม่คิดมูลค่า โดยที่ผู้ให้เช่าจะจัดให้มีไว้ในความครอบครองของผู้เช่าให้เพียงพออยู่เสมอ อุปกรณ์สิ้นเปลืองดังกล่าว เช่น ลูกโม่ถ่ายภาพ ผงหมึก ผงประจุภาพ หมึกพิมพ์ วัสดุที่ใช้ทำความสะอาดถุงกรอง แปรง น้ำมันหล่อลื่น และอุปกรณ์อื่น ๆ ที่จำเป็นเพื่อให้ระบบงานพิมพ์พร้อมหมึกพิมพ์ใช้งานได้ตามปกติตลอดเวลา

ข้อ ๘. หน้าที่ของผู้ให้เช่า

๘.๑ ผู้ให้เช่ามีหน้าที่ฝึกอบรมวิธีใช้ระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่าให้แก่เจ้าหน้าที่ของผู้เช่า จนสามารถใช้งานระบบงานพิมพ์พร้อมหมึกพิมพ์ได้ และผู้ให้เช่าตกลงจะฝึกอบรมวิธีการใช้ระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่าให้แก่เจ้าหน้าที่ของผู้เช่าทุกครั้ง หากผู้เช่าร้องขอโดยเหตุที่มีการเปลี่ยนแปลงโยกย้ายเจ้าหน้าที่ของผู้เช่าและเจ้าหน้าที่คนนั้นยังไม่เคยได้รับการฝึกอบรมมาก่อนโดยผู้ให้เช่าเป็นผู้รับผิดชอบค่าใช้จ่ายในการฝึกอบรมทั้งสิ้น

๘.๒ ในกรณีเครื่องระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่าชำรุดบกพร่องหรือขัดข้องใช้งานไม่ได้ตามปกติ ผู้ให้เช่าจะต้องจัดให้ช่างที่มีความรู้ความชำนาญและฝีมือดีมาจัดการซ่อมแซมแก้ไขให้อยู่ในสภาพใช้งานได้ดีตามปกติ โดยผู้ให้เช่าจะต้องเริ่มจัดการซ่อมแซมแก้ไขในทันทีที่ได้รับแจ้งจากผู้เช่าหรือผู้ที่ได้รับมอบหมายจากผู้เช่าแล้ว และให้แล้วเสร็จใช้งานได้ดีดังเดิมภายใน ๖ ชั่วโมง นับถัดจากเวลาที่ รฟม. ได้แจ้งให้ผู้ให้เช่ารับทราบรายละเอียดเป็นไปตามเอกสารแนบท้ายสัญญา ผนวก ๑

๘.๓ ในกรณีที่ระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่ามีความชำรุดบกพร่องหรือขัดข้องใช้งานไม่ได้ตามปกติ และการซ่อมแซมต้องใช้เวลาเกินกว่าที่กำหนดในข้อ ๘.๒ หรือไม่อาจซ่อมแซมแก้ไขให้ดีได้ดังเดิม ผู้ให้เช่าต้องจัดหาระบบงานพิมพ์พร้อมหมึกพิมพ์ที่มีคุณสมบัติ คุณภาพ ความสามารถ และประสิทธิภาพในการใช้งานไม่ต่ำกว่าของเครื่องเดิมมาให้ผู้เช่าใช้แทน รายละเอียดเป็นไปตามเอกสารแนบท้ายสัญญา ผนวก ๑

ข้อ ๙. ค่าปรับกรณีความชำรุดบกพร่องของระบบงานพิมพ์พร้อมหมึกพิมพ์

ถ้าผู้ให้เช่าไม่ดำเนินการหรือไม่สามารถซ่อมแซมแก้ไขระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่าภายในระยะเวลาตามข้อ ๘.๒ และผู้ให้เช่าไม่จัดหาระบบงานพิมพ์พร้อมหมึกพิมพ์ให้ผู้ให้เช่าใช้แทนตามข้อ ๘.๓ ผู้ให้เช่ายินยอมให้ผู้เช่าปรับเป็นรายชั่วโมง ในอัตราร้อยละ ๐.๐๑ (ศูนย์จุดศูนย์หนึ่ง) ของมูลค่าของสัญญาต่อการแจ้งผู้ให้เช่ารับทราบในแต่ละครั้ง ตั้งแต่พ้นกำหนดระยะเวลาตามข้อ ๘.๒ จนถึงวันที่ผู้ให้เช่าซ่อมแซมแก้ไขให้อยู่ในสภาพใช้งานได้ดีตามปกติ หรือผู้ให้เช่าจัดหาระบบงานพิมพ์พร้อมหมึกพิมพ์มาให้ผู้เช่าใช้งานแทน หรือ

/จนกว่าผู้เช่า...

จนกว่าผู้เช่าจะใช้สิทธิบอกเลิกสัญญา ทั้งนี้ ผู้เช่าไม่ต้องจ่ายค่าเช่าในระหว่างเวลาที่ผู้เช่าไม่สามารถใช้ระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่าตามสัญญานี้ โดยยินยอมให้ผู้เช่าหักค่าปรับดังกล่าวออกจากค่าเช่าตามข้อ ๒ หรือบังคับเอาจากหลักประกันตามข้อ ๑๐ ก็ได้

ข้อ ๑๐. หลักประกันการปฏิบัติตามสัญญา

ในขณะทำสัญญานี้ผู้ให้เช่าได้นำหลักประกันเป็นหนังสือค้ำประกันของธนาคารกสิกรไทย จำกัด (มหาชน) สาขามาร์เก็ต เพลส วงศ์สว่าง เลขที่ ๑๐๐๐๖๔๒๓๙๔๙๔ ลงวันที่ ๒๘ กันยายน ๒๕๖๖ เป็นจำนวนเงิน ๓๒๐,๓๐๕.๐๐ บาท (สามแสนสองหมื่นสามร้อยห้าบาทถ้วน) ซึ่งเท่ากับร้อยละ ๕ (ห้า) ของค่าเช่าทั้งหมดตามสัญญา มามอบให้แก่ผู้เช่าเพื่อเป็นหลักประกันการปฏิบัติตามสัญญานี้

กรณีผู้ให้เช่าใช้หนังสือค้ำประกันมาเป็นหลักประกันการปฏิบัติตามสัญญา หนังสือค้ำประกันดังกล่าวจะต้องออกโดยธนาคารที่ประกอบกิจการในประเทศไทย หรือโดยบริษัทเงินทุน หรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบตามแบบที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนด หรืออาจเป็นหนังสือค้ำประกันอิเล็กทรอนิกส์ตามวิธีการที่กรมบัญชีกลางกำหนดก็ได้ และจะต้องมีอายุการค้ำประกันตลอดไปจนกว่าผู้ให้เช่าพ้นข้อผูกพันตามสัญญานี้

หลักประกันที่ผู้ให้เช่านำมามอบให้ตามวรรคหนึ่ง จะต้องมีอายุครอบคลุมความรับผิดทั้งปวงของผู้ให้เช่าตลอดอายุสัญญา ถ้าหลักประกันที่ผู้ให้เช่านำมามอบให้ดังกล่าวลดลงหรือเสื่อมค่าลง หรือมีอายุไม่ครอบคลุมถึงความรับผิดของผู้ให้เช่าตลอดอายุสัญญา ไม่ว่าด้วยเหตุใด ๆ ก็ตาม รวมถึงกรณีผู้ให้เช่าส่งมอบและติดตั้งระบบงานพิมพ์พร้อมหมึกพิมพ์ล่าช้าเป็นเหตุให้ระยะเวลาการเช่าตามสัญญาเปลี่ยนแปลงไป ผู้ให้เช่าต้องหาหลักประกันใหม่หรือหลักประกันเพิ่มเติมให้มีจำนวนครบถ้วนตามวรรคหนึ่งมามอบให้แก่ผู้เช่าภายใน ๗ (เจ็ด) วัน นับถัดจากวันที่ได้รับแจ้งเป็นหนังสือจากผู้เช่า

หลักประกันที่ผู้ให้เช่านำมามอบไว้ตามข้อนี้ ผู้เช่าจะคืนให้แก่ผู้ให้เช่าโดยไม่มีดอกเบี้ยเมื่อผู้ให้เช่าพ้นจากข้อผูกพันและความรับผิดทั้งปวงตามสัญญานี้แล้ว

ข้อ ๑๑. การบอกเลิกสัญญา

เมื่อครบกำหนดส่งมอบระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่าตามสัญญาแล้ว ถ้าผู้ให้เช่าไม่ส่งมอบระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่า หรือส่งมอบแต่เพียงบางส่วนให้แก่ผู้เช่า หรือส่งมอบระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่าไม่ตรงตามสัญญาหรือมีคุณลักษณะเฉพาะไม่ถูกต้องตามสัญญา หรือส่งมอบแล้วเสร็จภายในกำหนดแต่ไม่สามารถใช้งานได้อย่างมีประสิทธิภาพหรือใช้งานได้ไม่ครบถ้วนตามสัญญา หรือผู้ให้เช่าไม่ปฏิบัติตามสัญญาข้อใดข้อหนึ่ง ผู้เช่ามีสิทธิบอกเลิกสัญญาทั้งหมดหรือแต่บางส่วนได้ การใช้สิทธิบอกเลิกสัญญานั้นไม่กระทบสิทธิของผู้เช่าที่จะเรียกร้องค่าเสียหายจากผู้ให้เช่า

ในกรณีที่ผู้เช่าใช้สิทธิบอกเลิกสัญญา ผู้เช่ามีสิทธิริบหรือบังคับจากหลักประกันตามข้อ ๑๐ เป็นจำนวนเงินทั้งหมดหรือแต่บางส่วนก็ได้แล้วแต่ผู้เช่าจะเห็นสมควร และถ้าผู้เช่าต้องเช่าระบบงานพิมพ์พร้อมหมึกพิมพ์จากบุคคลอื่นทั้งหมดหรือแต่บางส่วนภายในกำหนด ๓ (สาม) เดือน นับถัดจากวันบอกเลิกสัญญา ผู้ให้เช่ายอมรับผิดชดใช้ค่าเช่าที่เพิ่มขึ้นจากค่าเช่าที่กำหนดไว้ในสัญญานี้รวมทั้งค่าใช้จ่ายใด ๆ ที่ผู้เช่าต้องใช้จ่ายในการจัดหาผู้ให้เช่าระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่ารายใหม่ดังกล่าวด้วย

ขอกาน

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd.

/ในกรณี...

ในกรณีมีความจำเป็น ผู้เช่ามีสิทธิที่จะบอกเลิกสัญญาเช่านี้ก่อนครบกำหนดระยะเวลาการเช่าได้ โดยแจ้งเป็นหนังสือให้ผู้ให้เช่าทราบล่วงหน้าไม่น้อยกว่า ๓๐ (สามสิบ) วัน โดยผู้ให้เช่าจะไม่มีสิทธิเรียกร้องค่าเสียหายใด ๆ จากผู้เช่า

ข้อ ๑๒. ค่าปรับกรณีส่งมอบล่าช้า

ในกรณีที่ผู้ให้เช่าส่งมอบระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่าล่วงเลยกำหนดส่งมอบตามข้อ ๔ และผู้เช่ามิได้ใช้สิทธิบอกเลิกสัญญาตามข้อ ๑๑ วรรคหนึ่ง ผู้ให้เช่าจะต้องชำระค่าปรับให้ผู้เช่าเป็นรายวันสำหรับระบบงานพิมพ์พร้อมหมึกพิมพ์ที่ยังไม่ได้ส่งมอบตามสัญญา ในอัตราวันละ ๐.๒๐ บาท (ศูนย์จุดสองศูนย์) ต่อเครื่องที่ยังไม่ได้ส่งมอบ หรือส่งมอบแล้วแต่คุณสมบัติไม่ถูกต้อง หรือยังไม่สามารถใช้งานได้ นับถัดจากวันที่ครบกำหนดส่งมอบตามสัญญาจนถึงวันที่ผู้ให้เช่าได้นำระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่ามาส่งมอบให้แก่ผู้เช่าจนถูกต้องครบถ้วน

ในระหว่างที่ผู้เช่ายังมิได้ใช้สิทธิบอกเลิกสัญญานั้น หากผู้เช่าเห็นว่าผู้ให้เช่าไม่อาจปฏิบัติตามสัญญาต่อไปได้ ผู้เช่าจะใช้สิทธิบอกเลิกสัญญา และบังคับจากหลักประกันการปฏิบัติตามสัญญาตามข้อ ๑๐ กับเรียกร้องให้ชดใช้ค่าเช่าที่เพิ่มขึ้นตามที่กำหนดไว้ในข้อ ๑๑ วรรคสองก็ได้ และถ้าผู้เช่าได้แจ้งข้อเรียกร้องให้ชำระค่าปรับไปยังผู้ให้เช่าเมื่อครบกำหนดส่งมอบดังกล่าวแล้ว ผู้เช่ามีสิทธิที่จะปรับผู้ให้เช่าจนถึงวันบอกเลิกสัญญาได้อีกด้วย

ข้อ ๑๓. การบังคับค่าปรับ ค่าเสียหาย และค่าใช้จ่าย

ในกรณีที่ผู้ให้เช่าไม่ปฏิบัติตามสัญญาข้อใดข้อหนึ่งด้วยเหตุใด ๆ ก็ตาม จนเป็นเหตุให้เกิดค่าปรับ ค่าเสียหาย หรือค่าใช้จ่ายแก่ผู้เช่า ผู้ให้เช่าต้องชดใช้ค่าปรับ ค่าเสียหาย หรือค่าใช้จ่ายดังกล่าวให้แก่ผู้เช่าโดยสิ้นเชิงภายในกำหนด ๑๕ (สิบห้า) วัน นับถัดจากวันที่ได้รับแจ้งเป็นหนังสือจากผู้เช่า หากผู้ให้เช่าไม่ชดใช้ให้ถูกต้องครบถ้วนภายในระยะเวลาดังกล่าวให้ผู้เช่ามีสิทธิที่จะหักเอาจากค่าเช่าที่ต้องชำระหรือบังคับจากหลักประกันการปฏิบัติตามสัญญาได้ทันที

หากค่าปรับ ค่าเสียหาย หรือค่าใช้จ่ายที่บังคับจากค่าเช่าเดือนใด ๆ ที่ต้องชำระ หรือหลักประกันการปฏิบัติตามสัญญาแล้วยังไม่เพียงพอ ผู้ให้เช่ายินยอมชำระส่วนที่เหลือที่ยังขาดอยู่จนครบถ้วนตามจำนวนค่าปรับ ค่าเสียหาย หรือค่าใช้จ่ายนั้น ภายในกำหนด ๑๕ (สิบห้า) วัน นับถัดจากวันที่ได้รับแจ้งเป็นหนังสือจากผู้เช่า

ข้อ ๑๔. การโอนสิทธิของผู้ให้เช่า

ในระหว่างอายุสัญญาเช่า ห้ามผู้ให้เช่าโอนสิทธิหน้าที่ตามสัญญาหรือกรรมสิทธิ์ในระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่าแก่บุคคลอื่น เว้นแต่จะได้รับความยินยอมเป็นหนังสือจากผู้เช่าก่อน

ข้อ ๑๕. การนำระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่ากลับคืนเมื่อสัญญาสิ้นสุด

เมื่อสัญญาสิ้นสุดลงไม่ว่าจะเป็นการบอกเลิกสัญญาหรือครบกำหนดเวลาตามสัญญา ผู้ให้เช่าต้องนำระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่ากลับคืนไปภายใน ๑๕ (สิบห้า) วัน โดยผู้ให้เช่าเป็นผู้เสียค่าใช้จ่ายเองทั้งสิ้น

ถ้าผู้ให้เช่าไม่นำระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่ากลับคืนไปภายในกำหนดเวลาตามวรรคหนึ่ง ผู้เช่าไม่ต้องรับผิดชอบในความเสียหายใด ๆ ทั้งสิ้นที่เกิดแก่ระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่าอันมิใช่ความผิดของผู้เช่า

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd.

/ข้อ ๑๖. ข้อจำกัด...

ข้อ ๑๖. ข้อจำกัดความรับผิดของผู้เช่า

ผู้เช่าไม่ต้องรับผิดในความเสียหายหรือสูญหายเมื่อเกิดอัคคีภัยหรือภัยพิบัติใด ๆ หรือการโจรกรรมระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่าตลอดจนการสูญหายหรือความเสียหายใด ๆ ที่เกิดขึ้นแก่ระบบงานพิมพ์พร้อมหมึกพิมพ์ที่เช่า อันไม่ใช่เกิดจากความผิดของผู้เช่าตลอดระยะเวลาที่ระบบงานพิมพ์พร้อมหมึกพิมพ์อยู่ในความครอบครองของผู้เช่า

สัญญานี้มีผลย้อนหลังไปตั้งแต่วันที่ ๑ ตุลาคม ๒๕๖๖

สัญญานี้ทำขึ้นสองฉบับ มีข้อความถูกต้องตรงกัน คู่สัญญาได้อ่านและเข้าใจข้อความโดยละเอียดตลอดแล้ว จึงได้ลงลายมือชื่อ พร้อมประทับตรา (ถ้ามี) ไว้เป็นสำคัญต่อหน้าพยาน และคู่สัญญาต่างยึดถือไว้คนละหนึ่งฉบับ

(ลงชื่อ).....ผู้เช่า
(นายทวิช พึ่งตน)
ผู้อำนวยการฝ่ายจัดซื้อและบริการ
ปฏิบัติการแทน ผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd.

(ลงชื่อ).....ผู้ให้เช่า
(นายธงชัย อินทร์โสม)
ผู้รับมอบอำนาจตามกฎหมาย
บริษัท เคียวเซร่า ด็อกคิวเม้นท์ โซลูชั่น (ประเทศไทย) จำกัด

(ลงชื่อ).....พยาน
(นางฐิตารีย์ ศรีอาวุธ)
ผู้อำนวยการกองจัดหาพัสดุทั่วไป
การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

(ลงชื่อ).....พยาน
(นายธงชัย คล้ายจินดา)
บริษัท เคียวเซร่า ด็อกคิวเม้นท์ โซลูชั่น (ประเทศไทย) จำกัด

เลขที่โครงการ ๖๖๐๖๙๓๔๘๔๒๔
เลขคุมสัญญา ๖๖๐๙๒๑๐๐๐๐๙๓

ผนวก ๑

ขอบเขตของงานเช่าระบบงานพิมพ์พร้อมหมึกพิมพ์
ประจำปีงบประมาณ 2567 – 2569

1. ความเป็นมา

รฟม. ได้มีการจัดหาระบบงานพิมพ์พร้อมหมึกพิมพ์ เพื่อสนับสนุนการปฏิบัติงานด้วยวิธีการเช่า ซึ่งในปีงบประมาณ 2564-2566 โดยระบบจะหมดสัญญาเช่าในวันที่ 30 กันยายน 2566 ประกอบกับ รฟม. มีบุคลากรและภารกิจเพิ่มขึ้นอย่างมาก รวมทั้งสนับสนุนส่วนงานต่าง ๆ ดังนั้น รฟม. จึงมีความจำเป็นต้องจัดหาให้เพียงพอต่อการใช้งานทั้งในปัจจุบันและอนาคต

2. วัตถุประสงค์

เพื่อเช่าระบบงานพิมพ์พร้อมหมึกพิมพ์ทดแทนของเดิมที่หมดสัญญาเช่า และเช่าเพิ่มเติมให้เพียงพอต่อการปฏิบัติงาน โดยมีรายการและจำนวน ดังนี้

2.1 เครื่องพิมพ์ ขาว-ดำ ขนาด A4	จำนวน	19	ชุด
2.2 เครื่องพิมพ์ สี ขนาด A4	จำนวน	8	ชุด
2.3 เครื่องพิมพ์ สี ขนาด A3	จำนวน	9	ชุด
2.4 เครื่องพิมพ์มัลติฟังก์ชัน สี ขนาด A4	จำนวน	4	ชุด

3. คุณสมบัติผู้ยื่นข้อเสนอ

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นนิติบุคคลผู้มีอาชีพให้เช่าพัสดุที่ประกวดราคาเช่าด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ รฟม. ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่ รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

3.10 ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ต้องมีคุณสมบัติดังนี้

กิจการร่วมค้าที่ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน เว้นแต่ในกรณีกิจการร่วมค้าที่มีข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็น

/ผู้เข้าร่วมค้า...

ผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นสามารถใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงดังกล่าวจะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญามากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

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

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

3.13 ผู้ยื่นข้อเสนอต้องมีหนังสือรับรองการเป็นตัวแทนจำหน่ายเครื่องพิมพ์หรือเครื่องถ่ายเอกสาร ตามข้อ 2. จากบริษัทผู้ผลิต หรือบริษัทสาขาของผู้ผลิตในต่างประเทศ หรือบริษัทสาขาของผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทย โดยหนังสือรับรองดังกล่าว ต้องออกให้เพื่อมายื่นเอกสารเสนอราคาในครั้งนี้ และหนังสือนั้นต้องมีอายุไม่เกิน 90 วัน นับถัดจากวันที่ออกจนถึงวันที่ยื่นเอกสารประกวดราคา ทั้งนี้ไม่นับรวมซอฟต์แวร์ระบบควบคุมงานพิมพ์ โดยให้แนบหนังสือดังกล่าวมาพร้อมกับการยื่นเอกสารประกวดราคาครั้งนี้

4. หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

ในการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ รฟม. จะพิจารณาตัดสินโดยใช้หลักเกณฑ์ราคา โดยพิจารณาราคาต่ำสุด

5. ขอบเขตของการดำเนินงาน

ผู้ยื่นข้อเสนอที่ชนะการประกวดราคา (ผู้ให้เช่า) จะต้องดำเนินการดังนี้

5.1 จัดหาเครื่องพิมพ์พร้อมหมึกพิมพ์ตามรายการที่เสนอในข้อ 2.

5.2 ติดตั้งและส่งมอบเครื่องพิมพ์และระบบควบคุมงานพิมพ์ ตาม ภาคผนวก ก.

5.3 บำรุงรักษาและรับประกันความชำรุดบกพร่องเครื่องพิมพ์ตามรายการที่เสนอในข้อ 2.

5.4 จัดฝึกอบรมและจัดทำคู่มือ

6. เงื่อนไขและข้อกำหนดทั่วไป

6.1 รายการที่เสนอตามข้อ 2. ต้องเป็นของแท้ อยู่ในสภาพที่ใช้งานได้ดี เป็นรุ่นที่ยังอยู่ในสายการผลิต (Production Line) และต้องเป็นของใหม่ที่ยังมิได้ถูกติดตั้งใช้งาน ณ ที่ใดมาก่อน รวมทั้งต้องไม่ถูกนำมาปรับปรุงสภาพใหม่ (Reconditioned หรือ Rebuilt)

6.2 รายการที่เสนอตามข้อ 2. ต้องได้รับการรับรองคุณภาพตามมาตรฐานที่เกี่ยวข้องกับผลิตภัณฑ์ พร้อมทั้งต้องมีเอกสารรับรองโดยให้ยื่นเอกสารดังกล่าวมาพร้อมกับการยื่นเอกสารประกวดราคา ดังนี้

1) เป็นผลิตภัณฑ์ที่ประกอบจากโรงงานที่ได้รับรองมาตรฐาน ISO 9000 Series หรือเทียบเท่า

2) เป็นผลิตภัณฑ์ที่ได้รับรองมาตรฐานการประหยัดพลังงาน เช่น Energy Star หรือ EPEAT หรือเทียบเท่า

6.3 รายการที่เสนอตามข้อ 2. เป็นผลิตภัณฑ์ที่ได้มาตรฐานสิ่งแวดล้อมภายในประเทศ (ฉลากเขียว หรือตะกร้าเขียว หรือเทียบเท่า) หรือมาตรฐานสิ่งแวดล้อมจากต่างประเทศที่เป็นสมาชิกที่ได้รับรองระบบงาน GENICES ของเครือข่าย

/ฉลากสิ่งแวดล้อมโลก...

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd.

ฉลากสิ่งแวดล้อมโลก (Global Ecolabelling Network (GEN)) โดยเอกสารรับรองดังกล่าวต้องไม่หมดอายุ ณ วันยื่นเอกสารประกวดราคา โดยให้แนบหนังสือดังกล่าวมาพร้อมกับการยื่นเอกสารประกวดราคาครั้งนี้

6.4 รายการที่เสนอตามข้อ 2. ต้องมีคุณสมบัติตรงตาม Catalog หรือ Brochure ของบริษัทผู้ผลิตที่เสนอขายตามท้องตลาด โดยมีระบบหลัก หรือองค์ประกอบหลัก ที่มิได้ประกอบ หรือดัดแปลง เพื่อใช้เฉพาะการประกวดราคาครั้งนี้ โดยผู้ยื่นข้อเสนอจะต้องระบุยี่ห้อและรุ่นของผลิตภัณฑ์ที่เสนอ พร้อมทั้งต้องมี Catalog หรือ Brochure ที่ขีดเส้นใต้ พร้อมหัวข้อกำกับอุปกรณ์ที่เสนอไว้อย่างชัดเจน รวมถึงจัดทำตารางเปรียบเทียบคุณลักษณะเฉพาะของรายการที่เสนอตามข้อ 2. ตาม **ภาคผนวก ก. ดังตัวอย่างตาม ภาคผนวก ข.**

6.5 รายการที่เสนอตามข้อ 2. ต้องสามารถใช้งานกับระบบไฟฟ้า 220V AC 50Hz ตามมาตรฐานของไทยได้ โดยไม่ต้องใช้อุปกรณ์แปลงระบบไฟฟ้า และปลั๊กไฟฟ้าของอุปกรณ์ทุกรายการจะต้องเป็นชนิด 3 ขา (มีขาสำหรับสายดิน)

6.6 ในกรณีที่มีการส่งมอบรายการที่เสนอตามข้อ 2. ต่างไปจากที่กำหนดไว้หรือที่เสนอมา จะต้องมีเอกสารยืนยันจากบริษัทผู้ผลิต หรือจากบริษัทสาขาของผู้ผลิตในต่างประเทศ หรือจากบริษัทสาขาของผู้ผลิตในประเทศไทย หรือตัวแทนจำหน่ายในประเทศไทย ว่าเป็นรุ่นใหม่และจะต้องมีคุณสมบัติเทียบเท่าหรือดีกว่าที่กำหนดไว้หรือที่เสนอมา ทั้งนี้ รฟม. สงวนสิทธิ์ที่จะรับมอบหรือไม่ก็ได้

6.7 ภายหลังจากผู้ให้เช่าติดตั้งระบบงานพิมพ์ให้ รฟม. เป็นที่เรียบร้อยแล้ว รฟม. มีสิทธิ์ร้องขอผู้ให้เช่าดำเนินการย้ายเครื่องพิมพ์ตามรายการที่เสนอตามข้อ 2. และอุปกรณ์ที่เกี่ยวข้องได้ตลอดอายุสัญญา โดย รฟม. ไม่เสียค่าใช้จ่ายใด ๆ เพิ่มเติมทั้งสิ้น

6.8 ผู้ให้เช่าจะต้องจัดส่งเจ้าหน้าที่ที่มีความรู้ความสามารถด้านการซ่อมแซม แก้ไข และบำรุงรักษารายการที่เสนอตามข้อ 2. รวมทั้งอุปกรณ์ที่เกี่ยวข้อง และมีความประพฤติเรียบร้อย สุภาพ เหมาะกับตำแหน่งที่รับผิดชอบ มีบุคลิกภาพและมนุษยสัมพันธ์ที่ดี ไม่เคยมีความประพฤติในทางเสื่อมเสียมาก่อน มาประจำที่สำนักงานใหญ่ของ รฟม. ตลอดอายุสัญญา จำนวนไม่น้อยกว่า 1 คน ด้วยค่าใช้จ่ายของผู้ให้เช่าเอง โดยไม่คิดค่าใช้จ่ายใด ๆ เพิ่มเติมจากสัญญาเช่าต่อเดือนทั้งสิ้น รวมถึงค่าล่วงเวลา (ถ้ามี) โดยมีข้อกำหนดดังนี้

6.8.1 เจ้าหน้าที่จะต้องมีวุฒิการศึกษาไม่ต่ำกว่าระดับประกาศนียบัตรวิชาชีพชั้นสูง (ปวส.) โดยผู้ให้เช่าจะต้องแจ้งชื่อ-นามสกุล ประวัติการทำงาน และวุฒิการศึกษาของเจ้าหน้าที่ดังกล่าวให้คณะกรรมการตรวจรับพัสดุฯ ทราบภายในวันที่ส่งมอบ โดยกรอกรายละเอียดตาม**ภาคผนวก ค.** และจะต้องเริ่มปฏิบัติงานในวันถัดจากวันที่คณะกรรมการตรวจรับพัสดุฯ ได้ตรวจรับแล้วเสร็จ

6.8.2 ผู้ให้เช่าจะต้องดำเนินการให้สำนักงานตำรวจแห่งชาติตรวจประวัติอาชญากรรมด้วยลายนิ้วมือของเจ้าหน้าที่หลักที่จะเข้ามาปฏิบัติงานที่ รฟม. ด้วยค่าใช้จ่ายของผู้ให้เช่าเอง และแสดงหลักฐานการดำเนินการดังกล่าว โดยผู้ให้เช่าจะต้องนำผลดังกล่าวมาแสดงให้คณะกรรมการตรวจรับพัสดุฯ ทราบภายใน 30 วัน นับถัดจากวันที่คณะกรรมการตรวจรับพัสดุฯ ได้ตรวจรับแล้วเสร็จ โดยเจ้าหน้าที่ของผู้ให้เช่าจะต้องไม่มีประวัติอาชญากรรมเกี่ยวกับความผิดทางอาญา เว้นแต่โทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ ทั้งนี้ รฟม. ไม่อนุญาตให้เจ้าหน้าที่ที่มีประวัติอาชญากรรมเกี่ยวกับความผิดอาญาดังกล่าวเข้าทำงาน หากพบว่าเจ้าหน้าที่ของผู้ให้เช่ามีประวัติอาชญากรรมดังกล่าว ผู้ให้เช่าจะต้องเปลี่ยนตัวเจ้าหน้าที่คนดังกล่าว แล้วจัดหาเจ้าหน้าที่มาปฏิบัติงานแทน ทั้งนี้ หากผู้ให้เช่าฝ่าฝืน รฟม. จะถือว่าผิดสัญญา

6.8.3 เจ้าหน้าที่ของผู้ให้เช่าจะต้องปฏิบัติงานในวันจันทร์ – วันศุกร์ เวลา 8.00 – 17.00 น. (ระหว่างเวลา 12.00 – 13.00 น. เป็นเวลาพักรับประทานอาหารกลางวัน) เว้นวันหยุดที่ รฟม. กำหนดไว้ รวมเวลาทำงานวันละ 8 ชั่วโมง

6.8.4 เจ้าหน้าที่ของผู้ให้เช่าจะต้องจัดทำรายงานสรุปเวลาเข้า – ออกการปฏิบัติงาน ด้วยวิธีการลงเวลาตามแบบฟอร์มของผู้ให้เช่าเอง หรือตามที่ รฟม. กำหนด เป็นประจำทุกเดือน แล้วจัดส่งให้ผู้ควบคุมงานของฝ่ายเทคโนโลยีสารสนเทศ ภายในวันที่ 15 ของเดือนถัดไป

/6.8.5 เจ้าหน้า....

6.8.5 เจ้าหน้าที่ของผู้ให้เช่าจะต้องจัดทำรายงานการปฏิบัติงานตามสัญญาฯ ประจำเดือน จัดส่งให้ผู้ควบคุมงานของ ฝ่ายเทคโนโลยีสารสนเทศ ภายในวันที่ 15 ของเดือนถัดไป

6.8.6 ผู้ให้เช่าจะต้องจัดหาอุปกรณ์ และเครื่องมือสำหรับการปฏิบัติงาน ซ่อมแซม แก้ไขและบำรุงรักษารายการที่เสนอตามข้อ 2. อะไหล่สำรอง (Maintenance Kit Printer) รวมทั้งอุปกรณ์ที่เกี่ยวข้องให้แก่เจ้าหน้าที่ของผู้ให้เช่าที่มาปฏิบัติงานตามความเหมาะสม

6.8.7 กรณีผู้ให้เช่าต้องการเปลี่ยนตัวเจ้าหน้าที่ของผู้ให้เช่าประจำสำนักงานใหญ่ รฟม. แบบถาวร (ไม่รวมถึงเจ้าหน้าที่ขาดงาน ลางาน) จะต้องกรอกรายละเอียดตาม**ภาคผนวก ค.** และทำเป็นหนังสือยื่นต่อคณะกรรมการตรวจรับพัสดุเพื่อพิจารณาก่อนการเปลี่ยนตัวเจ้าหน้าที่ดังกล่าวไม่น้อยกว่า 3 วันทำการ

6.8.8 รฟม. มีสิทธิ์ขอเปลี่ยนตัวเจ้าหน้าที่ของผู้ให้เช่าได้ตลอดอายุสัญญา เมื่อ รฟม. เห็นว่าไม่มีคุณสมบัติตามข้อ 6.8 รวมถึงไม่มีความเหมาะสมที่จะปฏิบัติหน้าที่ และผู้ให้เช่าจะต้องหาเจ้าหน้าที่มาทดแทนโดยเร็วที่สุด

6.9 ราคาเช่าที่เสนอให้รวมถึง ค่าเช่าใช้ทั้งฮาร์ดแวร์ ซอฟต์แวร์ ค่าใช้จ่ายในการบำรุงรักษาและซ่อมแซมแก้ไข ค่าดำเนินการติดตั้ง ค่าขนย้าย ค่าเก็บรักษาทั้งก่อนและหลังการติดตั้ง (โกดังหรือคลังสินค้า) ค่าจ้างตามข้อ 6.8 ค่าหมึกพิมพ์ (ยกเว้นกระดาษเท่านั้น) อุปกรณ์อื่นใดที่ไม่ได้กล่าวถึง เพื่อให้สามารถใช้งานเข้ากับระบบคอมพิวเตอร์ของ รฟม. ที่มีและใช้งานอยู่ได้อย่างมีประสิทธิภาพ โดยไม่มีการคิดค่าใช้จ่ายใด ๆ เพิ่มเติมทั้งสิ้น

6.10 ปริมาณการใช้ตลอดอายุสัญญาสูงสุด ดังนี้

6.10.1 ขนาด A4 ขาว/ดำ จำนวน ประมาณ	1,800,000	หน้า
6.10.2 ขนาด A4 สี จำนวน ประมาณ	764,000	หน้า
6.10.3 ขนาด A3 ขาว/ดำ จำนวน ประมาณ	5,000	หน้า
6.10.4 ขนาด A3 สี จำนวน ประมาณ	27,000	หน้า

7. ระยะเวลาการเช่า

สัญญานี้มีผลบังคับตั้งแต่วันที่ลงนามในสัญญา แต่ระยะเวลาการคำนวณค่าเช่าตามสัญญานี้ให้มีกำหนดเริ่มตั้งแต่วันที่ 1 ตุลาคม 2566 ถึงวันที่ 30 กันยายน 2569 รวมระยะเวลาการเช่าทั้งสิ้น 36 เดือน ทั้งนี้ระยะเวลาการคำนวณค่าเช่า ไม่นับรวมระยะเวลาติดตั้งและส่งมอบ

8. วงเงินงบประมาณ

8,310,000 บาท (แปดล้านสามแสนหนึ่งหมื่นบาทถ้วน) (รวมภาษีมูลค่าเพิ่ม)

9. การชำระค่าเช่า

9.1 การชำระค่าเช่ารายการตามข้อ 2. รฟม. จะชำระค่าเช่าเป็นรายเดือน โดยคำนวณค่าเช่าจากปริมาณการพิมพ์ทั้งหมดในแต่ละเดือน (หักด้วยจำนวนกระดาษเสียจากที่ใช้งานจริงต่อเครื่องจำนวนไม่น้อยกว่า 3 %)

9.2 ผู้ให้เช่าต้องส่งเอกสารแจ้งหนี้เรียกเก็บค่าเช่า ปริมาณการใช้ พร้อมแนบเอกสารการบำรุงรักษาเป็นประจำทุกเดือน จนสิ้นสุดสัญญา

10. การติดตั้งและส่งมอบพัสดุ

10.1 ผู้ให้เช่าต้องติดตั้งรายการตามข้อ 2. ตามสัญญาให้ รฟม. ตามสถานที่ที่กำหนดภายใน 60 วันนับถัดจากวันที่ลงนามในสัญญา (ผู้ให้เช่าต้องเป็นผู้จัดหาบุคลากรและอุปกรณ์ประกอบพร้อมทั้งเครื่องมือที่จำเป็นในการดำเนินการต่าง ๆ ที่เกี่ยวข้อง โดยผู้ให้เช่าเป็นผู้ออกค่าใช้จ่ายเองทั้งสิ้น)

บริษัท เคียวเซร่า ดอคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA ชัดกานท์
KYOCERA Document Solutions (Thailand) Corp., Ltd.

/10.2 ผู้ให้เช่า...

10.2 ผู้ให้เช่าต้องจัดให้มีการประชุมเริ่มงาน และจัดส่งแผนการติดตั้งและแผนการบำรุงรักษาภายใน 15 วัน นับถัดจากวันลงนามในสัญญา โดยทำเป็นหนังสือยื่นต่อคณะกรรมการตรวจรับพัสดุฯ ผู้ให้เช่าต้องส่งผู้เข้าร่วมประชุมอย่างน้อย ดังนี้ ผู้จัดการโครงการ ตัวแทนฝ่ายขาย ตัวแทนฝ่ายซอฟต์แวร์และตัวแทนฝ่ายช่าง ทั้งนี้ ผู้เข้าร่วมประชุม 1 ท่านสามารถเป็นตัวแทนได้เพียง 1 ตำแหน่งเท่านั้น

10.3 ผู้ให้เช่าต้องจัดเตรียมสถานที่ รถรับ-ส่ง สิ่งอำนวยความสะดวกและอุปกรณ์ต่าง ๆ ที่เกี่ยวข้องสำหรับการตรวจสอบรายละเอียดคุณสมบัติของอุปกรณ์ตามข้อ 2. ตามสถานที่ที่ รฟม. กำหนดหรือสถานที่ของผู้ให้เช่าก่อนนำมาติดตั้งตามสถานที่ที่ รฟม. กำหนด โดย รฟม. ไม่เสียค่าใช้จ่ายใด ๆ เพิ่มเติมทั้งสิ้น

10.4 ผู้ให้เช่าต้องจัดทำสติกเกอร์ที่ระบุชื่อบริษัทผู้ให้เช่า เลขที่สัญญา ระยะเวลาการรับประกัน หมายเลขโทรศัพท์สำหรับการแจ้งปัญหา และหมายเลขของเครื่อง ติดให้กับรายการตามข้อ 2. ทุกรายการในตำแหน่งที่ให้เห็นได้อย่างชัดเจน **ดังตัวอย่างตาม ภาคผนวก ง.**

10.5 ภายหลังการติดตั้งแล้วผู้ให้เช่าต้องจัดทำเอกสารการติดตั้งรายการตามข้อ 2. ทุกรายการที่ระบุรายละเอียดต่าง ๆ เช่น ยี่ห้อ/ประเภทของอุปกรณ์/รุ่น/หมายเลขของเครื่อง/สถานที่ติดตั้ง/Mac Address ฯลฯ แล้วส่งมอบให้ รฟม. โดยเสนอต่อคณะกรรมการตรวจรับพัสดุ จำนวน 1 ชุด พร้อมไฟล์ต้นฉบับ (Soft File) ในรูปแบบ Microsoft Excel รวมถึงข้อมูลแผนการดำเนินการต่าง ๆ (ถ้ามี)

10.6 ผู้ให้เช่าต้องทำการติดตั้งซอฟต์แวร์ต่าง ๆ ที่จำเป็น ที่มาพร้อมกับรายการตามข้อ 2. ทุกรายการให้สามารถใช้งานเข้ากับระบบคอมพิวเตอร์ของ รฟม. ได้อย่างมีประสิทธิภาพ

10.7 ผู้ให้เช่าต้องเตรียมหมึกพิมพ์สำรองสำหรับรายการตามข้อ 2. แต่ละรุ่น โดยที่สำรองหมึกในแต่ละรุ่นไม่น้อยกว่าร้อยละ 20 ของรุ่นนั้น ๆ และส่งมอบหมึกพิมพ์สำรองทั้งหมดในวันตรวจรับพัสดุ หากหมึกพิมพ์สำรองเหลือน้อยกว่าร้อยละ 20 ผู้ให้เช่าต้องมาเปลี่ยนหมึกพิมพ์ และดำเนินการให้แล้วเสร็จ ในพื้นที่สำนักงานใหญ่ของ รฟม. และพื้นที่อื่นที่ รฟม. กำหนด (กรุงเทพฯ และปริมณฑล) ภายใน 8 ชม. นับถัดจากเวลาที่ รฟม. ได้แจ้งผู้ให้เช่ารับทราบทางโทรศัพท์ โทรศัพท์เคลื่อนที่ โทรสาร จดหมายอิเล็กทรอนิกส์ (E-mail) หรือช่องทางการติดต่ออื่น ๆ ที่ รฟม. กำหนด รวมถึงให้นำตลับหมึกพิมพ์ที่หมดแล้วกลับ

10.8 กรณีที่เครื่องพิมพ์มีน้ำหนักเกิน 35 กิโลกรัม จะต้องมีฐานวางที่มีล้อเลื่อนได้

10.9 ผู้ให้เช่าต้องส่งมอบเครื่องอ่านบัตร (Mifare Reader) จำนวน 1 เครื่อง ที่สามารถอ่านบัตรของพนักงานและบัตรของเจ้าหน้าที่ รฟม. ได้และสามารถลงทะเบียนบัตรของพนักงานในภายหลังได้ตลอดอายุของสัญญา

10.10 ผู้ให้เช่าต้องกำหนดปริมาณหรือเปลี่ยนแปลงปริมาณของการพิมพ์ตามที่ รฟม. กำหนด

10.11 ผู้ให้เช่าจะต้องมี ผู้จัดการโครงการ (Project Manager) เพื่อติดต่อและประสานงานอย่างน้อย 1 คน ซึ่งมีความรู้ความสามารถในการบริหารการจัดการและประสานงานได้เป็นอย่างดี

10.12 คณะกรรมการตรวจรับพัสดุจะทดสอบ ตรวจรับผลิตภัณฑ์ที่เสนอตามสัญญานี้ ต่อเมื่อคณะกรรมการตรวจรับพัสดุ รฟม. ได้รับหนังสือแจ้งจากผู้ให้เช่าว่าได้ติดตั้งแล้วเสร็จเรียบร้อยพร้อมที่จะส่งมอบแล้ว โดยผู้ให้เช่าต้องทำหนังสือแจ้งให้คณะกรรมการตรวจรับพัสดุรับทราบก่อนวันส่งมอบและตรวจรับไม่น้อยกว่า 3 วันทำการ พร้อมทั้งทำการสำเนาเอกสารทั้งหมดที่เกิดขึ้นระหว่างโครงการในรูปแบบเอกสารอิเล็กทรอนิกส์ที่สามารถแก้ไขปรับปรุงได้ เช่น .docx, .xlsx, .vsd เป็นต้น

10.13 การส่งมอบรายการตามข้อ 2. ที่ไม่ตรงตามสัญญา รฟม. มีสิทธิ์ที่จะไม่รับเครื่องพิมพ์นั้น ในกรณีนี้ผู้ให้เช่าต้องรีบนำกลับคืนไปแก้ไขให้ถูกต้องตามสัญญาและนำมาส่งมอบให้ใหม่ด้วยค่าใช้จ่ายของผู้ให้เช่าเอง และระยะเวลาที่เสียไปเพราะเหตุดังกล่าว ผู้ให้เช่าจะนำมาอ้างเป็นเหตุในการขอขยายระยะเวลา หรือของด หรือขอลดค่าปรับไม่ได้

11. การบำรุงรักษา

11.1 ผู้ให้เช่าจะต้องรับผิดชอบการบำรุงรักษารายการตามข้อ 2. ให้อยู่ในสภาพที่สามารถใช้งานได้ดีอยู่ตลอดอายุของสัญญาเช่า ซึ่งรวมถึงอุปกรณ์ต่าง ๆ ของรายการตามข้อ 2.

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd.

/11.2 ผู้ให้เช่า...

11.2 ผู้ให้เช่าจะต้องตรวจสอบ ทำความสะอาดรายการตามข้อ 2. โดยช่างผู้มีความชำนาญอย่างน้อยเดือนละ 1 ครั้ง ในวันและเวลาทำการของ รฟม. จนสิ้นสุดสัญญา พร้อมจัดทำรายงานการตรวจสอบเพื่อแจ้งให้ รฟม. ทราบหลังจากดำเนินการเรียบร้อยแล้ว ทั้งนี้ให้แนบเอกสารดังกล่าวมากับใบวางบิล รวมถึงรายงานผลการตรวจสอบให้ รฟม. ทราบทุกครั้งหลังจากที่ผู้ให้เช่าได้บำรุงรักษาเสร็จเรียบร้อยแล้ว โดยแนบเอกสารดังกล่าวมาพร้อมกับใบวางบิล หรือเอกสารที่เกี่ยวข้อง โดย รฟม. ไม่เสียค่าใช้จ่ายใด ๆ เพิ่มเติมทั้งสิ้น ซึ่งการดำเนินงานต้องมีอย่างน้อยดังนี้

1) ทำความสะอาดตัวเครื่องพิมพ์ทั้งภายในและภายนอก

2) ตรวจสอบประสิทธิภาพของเครื่องพิมพ์ และระบบควบคุมงานพิมพ์รวมถึงชิ้นส่วนที่เกี่ยวข้องให้พร้อมใช้งาน

3) ตรวจสอบจำนวนและสถานที่ติดตั้ง (ล่าสุด) ความเรียบร้อย ความครบถ้วนของเครื่อง หากมีการชำรุดเสียหาย ผู้ให้เช่าจะต้องทำรายงานให้ รฟม. ทราบภายใน 7 วัน นับถัดจากวันที่เข้ามาบำรุงรักษา มิฉะนั้น รฟม. ถือว่าผู้ให้เช่าไม่ติดใจที่จะเรียกร้องค่าเสียหายใด ๆ เพิ่มเติมทั้งสิ้น

12. การรับประกันความชำรุดบกพร่อง

12.1 ผู้ให้เช่ายอมรับประกันความชำรุดบกพร่องหรือขัดข้องของรายการตามข้อ 2. และระบบควบคุมงานพิมพ์ตามสัญญานี้ ตลอดอายุสัญญานับถัดจากวันที่ รฟม. ดำเนินการตรวจรับเรียบร้อยแล้วไปจนสิ้นสุดระยะเวลาตามสัญญา ถ้าภายในระยะเวลาดังกล่าวรายการตามข้อ 2. ชำรุดบกพร่อง หรือใช้งานไม่ได้ทั้งหมดหรือแต่บางส่วน และความชำรุดบกพร่องดังกล่าวมิใช่ความผิดของ รฟม. ผู้ให้เช่าจะต้องจัดให้เจ้าหน้าที่ที่มีความรู้ ความชำนาญ มาจัดการซ่อมแซมแก้ไขให้แล้วเสร็จสามารถใช้งานได้ดีดังเดิมภายใน 6 ชั่วโมง นับถัดจากเวลาที่ รฟม. ได้แจ้งให้ผู้ให้เช่ารับทราบทางโทรศัพท์ โทรศัพท์เคลื่อนที่ โทรสาร หรือจดหมายอิเล็กทรอนิกส์ (E-mail) หรือช่องทางการติดต่ออื่น ๆ ที่ รฟม. กำหนด กรณีที่แจ้งเหตุหลังเวลาปฏิบัติงานหรือวันหยุดราชการ ผู้ให้เช่าต้องเข้าดำเนินการแก้ไขปัญหาในวันทำการถัดไปภายในเวลาไม่เกิน 9.00 น. แล้วดำเนินการให้แล้วเสร็จภายใน 6 ชั่วโมง หรือ รฟม. อาจจะแจ้งให้ผู้ให้เช่าดำเนินการทันทีได้เป็นรายกรณีไปขึ้นอยู่กับปัญหาที่เกิดขึ้น โดยนับในวันและเวลาทำการของ รฟม.

12.2 ในกรณีที่ไม่สามารถซ่อมแซมให้แล้วเสร็จภายในกำหนดระยะเวลาดังกล่าว ผู้ให้เช่าต้องจัดหาเครื่องพิมพ์ที่มีคุณสมบัติไม่ต่ำกว่าของเดิมหรือดีกว่าและมีสภาพดี มาให้ รฟม. ใช้งานทดแทนจนกว่าจะซ่อมแซมรายการตามข้อ 2. ที่ชำรุดแล้วเสร็จสามารถใช้งานได้ดีดังเดิม ในกรณีที่ผู้ให้เช่าต้องนำรายการตามข้อ 2. ที่เสียหรือชำรุดไปซ่อมแซมแก้ไขภายนอก ผู้ให้เช่าต้องนำรายการตามข้อ 2. กลับมาคืนภายใน 10 วันทำการ โดยอะไหล่หรือวัสดุอุปกรณ์ที่นำมาใช้ในการซ่อมแซมแก้ไข หรือให้ใช้เป็นการชั่วคราว หรือที่นำมาเปลี่ยนให้ใหม่นั้น จะต้องมีคุณสมบัติไม่ต่ำกว่าของเดิม สำหรับกรณีการเปลี่ยนวัสดุอุปกรณ์ให้ใหม่ วัสดุอุปกรณ์นั้นจะต้องเป็นของใหม่ที่ไม่เคยถูกใช้งานมาก่อนและไม่เป็นของเก่าเก็บ

12.3 ในกรณีรายการตามข้อ 2. เสียจนไม่สามารถซ่อมแซมได้ ผู้ให้เช่าจะต้องจัดหาเครื่องพิมพ์ที่มีคุณสมบัติไม่ต่ำกว่าของเดิมและเป็นเครื่องใหม่ที่ไม่ผ่านการใช้งานมาก่อน มาเปลี่ยนทดแทนอย่างถาวร โดยผู้ให้เช่าต้องทำหนังสือแจ้งขอเปลี่ยนเครื่องพิมพ์เป็นลายลักษณ์อักษรแจ้งคณะกรรมการตรวจรับพัสดุพิจารณาและต้องได้รับการเห็นชอบก่อนการเปลี่ยนเครื่องพิมพ์ดังกล่าว

12.4 ในกรณีที่รายการตามข้อ 2. ชำรุดบกพร่องหรือไม่สามารถใช้งานได้ตามคุณสมบัติเดิมของเครื่องได้ในปัญหาเดิมซ้ำเป็นจำนวน 3 ครั้ง ภายในระยะเวลา 30 วันนับถัดจากวันที่มีการแจ้งอาการชำรุดบกพร่องครั้งแรก ผู้ให้เช่าจะต้องจัดหาเครื่องพิมพ์ที่มีคุณสมบัติไม่ต่ำกว่าของเดิมหรือดีกว่า และเป็นเครื่องใหม่มาเปลี่ยนทดแทนอย่างถาวร หากผู้ให้เช่าไม่สามารถจัดหาเครื่องพิมพ์ดังกล่าวมาทดแทนได้ รฟม. ไม่จำเป็นต้องจ่ายค่าเช่าในระหว่างเวลาที่ รฟม. ไม่สามารถใช้งานรายการตามข้อ 2. ได้

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd.

/12.5 ในกรณี...

12.5 ในกรณีที่การซ่อมแซมแก้ไขจำเป็นต้องมีการถ่ายโอนข้อมูลต่าง ๆ ใน Hard disk จากรายการตามข้อ 2. ทุกรายการ ที่ชำรุดไปยังเครื่องใหม่ ผู้ให้เช่าจะต้องทำการถ่ายโอนให้เรียบร้อยจนกว่าผู้ใช้งานสามารถใช้งานเครื่องใหม่ได้ตามปกติ โดยจะไม่นับเวลาที่ใช้ทำการถ่ายโอนข้อมูลเป็นระยะเวลาดำเนินการแก้ไข หลังจากถ่ายโอนข้อมูลต่าง ๆ ใน Hard disk แล้วเสร็จจะต้องทำลายข้อมูลซึ่งอยู่ภายใน Hard disk ลูกเดิมจนไม่สามารถกู้ข้อมูลกลับมาได้ พร้อมทั้งรายงานผลการทำลายข้อมูลในรายงานผลประจำเดือน

12.6 ในกรณีที่รายการตามข้อ 2. สูญหายผู้ให้เช่าจะต้องนำเครื่องพิมพ์ที่มีคุณสมบัติไม่ต่ำกว่ารุ่นเดิมหรือที่คณะกรรมการตรวจรับพัสดุสามารถยอมรับได้มาให้ รฟม. ใช้ทดแทนภายใน 3 วันทำการ นับถัดจากวันที่ รฟม. หรือเจ้าหน้าที่ของ รฟม. แจ้งให้ทราบ

13. การฝึกอบรมและการจัดทำคู่มือ

13.1 ผู้ให้เช่าต้องส่งมอบเอกสารคู่มือการใช้งานรายการตามข้อ 2. และคู่มือการใช้งานซอฟต์แวร์ รวมถึงผลิตภัณฑ์ที่เกี่ยวข้องเป็นภาษาไทย พร้อมรูปประกอบอย่างละเอียด ทั้งนี้ผู้ให้เช่าต้องส่งเอกสารต่าง ๆ ให้ผู้ควบคุมงานของฝ่ายเทคโนโลยีสารสนเทศ รฟม. ได้พิจารณา และเห็นชอบก่อนทำการส่งมอบ โดยต้องส่งมอบเอกสารทั้งหมดเป็นเอกสารสี พร้อมเอกสารอิเล็กทรอนิกส์ โดยประกอบไปด้วย

13.1.1 คู่มือการใช้งานของผู้ดูแลระบบ จำนวนไม่น้อยกว่า 5 ชุด

13.1.2 คู่มือการใช้งานของผู้ใช้งาน จำนวนไม่น้อยกว่าจำนวนเครื่องพิมพ์

13.2 ผู้ให้เช่าต้องเสนอรายละเอียดหลักสูตรและแผนการฝึกอบรม เพื่อถ่ายทอด วิธีการดูแล บริหารจัดการและแก้ไขปัญหาต่าง ๆ ที่จำเป็นต่อการดูแล บริหารจัดการซอฟต์แวร์และอุปกรณ์ฯ ส่งเอกสารประกอบการฝึกอบรมให้ผู้ควบคุมงานของฝ่ายเทคโนโลยีสารสนเทศ รฟม. พิจารณาและเห็นชอบก่อนทำการฝึกอบรม

13.3 ผู้ให้เช่าต้องทำการฝึกอบรมสำหรับเจ้าหน้าที่ผู้ดูแลระบบ ภายใน 60 วัน นับถัดจากวันที่ตรวจรับแล้วเสร็จ โดยเนื้อหาหลักสูตรต้องเป็นไปตามมาตรฐานของผลิตภัณฑ์ที่เสนอ ซึ่งต้องครอบคลุมเนื้อหาการติดตั้ง (Install) ปรับแต่ง (Configure) บริหารจัดการ (Manage) และแก้ไขปัญหา (Troubleshooting) อุปกรณ์และซอฟต์แวร์บริหารจัดการ เป็นอย่างน้อย โดยต้องฝึกอบรมเจ้าหน้าที่ผู้ดูแลระบบจำนวนไม่น้อยกว่า 3 คน จำนวนวันที่ทำการฝึกอบรมต้องไม่น้อยกว่า 1 วันทำการ ในการฝึกอบรมดังกล่าวผู้ให้เช่าต้องจัดเตรียมสถานที่ วิทยากรที่ได้รับการรับรองจากบริษัทผู้ผลิตหรือบริษัทสาขาของผู้ผลิตในประเทศไทยพร้อมเอกสารคู่มือการฝึกอบรมสี อาหารว่างจำนวน 2 มื้อ และอาหารกลางวันจำนวน 1 มื้อต่อวัน ตามจำนวนเจ้าหน้าที่ผู้ดูแลระบบที่ รฟม. กำหนด โดยผู้ให้เช่าเป็นผู้รับผิดชอบค่าใช้จ่ายทั้งหมด ทั้งนี้เอกสารคู่มือการฝึกอบรมสี ผู้ให้เช่าต้องจัดทำเสนอให้ผู้ควบคุมงานของฝ่ายเทคโนโลยีสารสนเทศ รฟม. พิจารณาและต้องได้รับการเห็นชอบก่อนทำการฝึกอบรม

13.4 ในกรณีที่ผู้ให้เช่าไม่สามารถดำเนินการฝึกอบรมได้ทันภายในกำหนดเวลาข้อ 13.3 รฟม. จะจัดส่งเจ้าหน้าที่ผู้ดูแลระบบตามจำนวนที่ รฟม. กำหนด ไปฝึกอบรมกับบริษัทที่รับฝึกอบรมภายนอก โดยค่าใช้จ่ายทั้งหมดที่เกี่ยวข้องจากการฝึกอบรมดังกล่าว เป็นค่าใช้จ่ายของผู้ให้เช่าเอง

13.5 ผู้ให้เช่าต้องให้คำปรึกษา แนะนำการใช้งานรายการตามข้อ 2. และผลิตภัณฑ์ที่เกี่ยวข้อง ที่ได้มาพร้อมสัญญานี้ แก่เจ้าหน้าที่ของ รฟม. เมื่อมีการร้องขอตลอดอายุสัญญา

14. อัตราค่าปรับ

14.1 ในกรณีผู้ให้เช่าไม่สามารถปฏิบัติตามเงื่อนไขการติดตั้งและส่งมอบ ที่ระบุตามข้อ 10. หรือการส่งมอบเครื่องเช่าล่าช้ากว่าที่กำหนดไว้ในสัญญาในบางรายการหรือทั้งหมด หรือส่งมอบแล้วแต่มีคุณสมบัติไม่ถูกต้องตามรายละเอียดและคุณลักษณะเฉพาะที่กำหนด หรือยังไม่สามารถใช้งานได้ โดยมิได้มีสาเหตุมาจากความผิดพลาด

/หรือความ...

หรือความบกพร่องของ รฟม. ผู้ให้เช่าจะต้องชำระค่าปรับให้แก่ รฟม. เป็นรายวันในอัตราค่าปรับร้อยละ 0.20 (ศูนย์จุดสองศูนย์) ของมูลค่าของสัญญาต่อเครื่องเช่าที่ยังไม่ได้ส่งมอบ หรือส่งมอบแล้วแต่คุณสมบัติไม่ถูกต้อง หรือยังไม่สามารถใช้งานได้โดยการปรับจะนับถัดจากวันครบกำหนดส่งมอบตามสัญญาจนถึงวันที่ผู้ให้เช่าได้นำเครื่องเช่ามาส่งมอบและติดตั้งให้แก่ รฟม. จนถูกต้องครบถ้วนแล้ว โดยหักจากค่าเช่าใช้บริการ

วิธีการคิดค่าปรับ

(มูลค่าของสัญญา/จำนวนเครื่องทั้งหมด) x อัตราค่าปรับร้อยละ 0.20 x (จำนวนเครื่องที่ยังไม่ได้ส่งมอบหรือส่งมอบแล้วแต่คุณสมบัติไม่ถูกต้องหรือยังไม่สามารถใช้งานได้)

14.2 กรณีตามข้อ 14.1 รฟม. มีสิทธิ์เลิกสัญญาได้ หาก รฟม. ใช้สิทธิ์บอกเลิกสัญญา นอกจากผู้ให้เช่ายินยอมให้ รฟม. คิดค่าปรับตามข้อ 14.1 โดยนับถัดจากวันครบกำหนดส่งมอบตามสัญญาจนถึงวันบอกเลิกสัญญาแล้ว ผู้ให้เช่ายินยอมให้ รฟม. ริบหลักประกันเป็นจำนวนทั้งหมดหรือแต่บางส่วนก็ได้ แล้วแต่ รฟม. จะเห็นสมควร

14.3 ในกรณีผู้ให้เช่าไม่สามารถปฏิบัติตามเงื่อนไขตามข้อ 11. ได้ รฟม. จะคิดค่าปรับในอัตราค่าปรับร้อยละ 0.10 (ศูนย์จุดหนึ่งศูนย์) ตามข้อ 2 ที่ยังไม่ได้บำรุงรักษาเดือนนั้น ๆ โดยค่าปรับข้างต้น รฟม. สามารถหักจากค่าเช่ารายเดือนหรือเงินอื่น ๆ ที่ค้างจ่ายได้ทันที โดย รฟม. ไม่ต้องบอกสงวนสิทธิ์แต่อย่างใด

14.4 หากผู้ให้เช่าไม่สามารถปฏิบัติตามเงื่อนไขตามข้อ 12. ผู้ให้เช่าจะถูกปรับเป็นรายชั่วโมงในอัตราร้อยละ 0.01 (ศูนย์จุดศูนย์หนึ่ง) ของมูลค่าของสัญญาต่อการแจ้งผู้ให้เช่ารับทราบในแต่ละครั้ง โดยเศษของชั่วโมงนับเป็นหนึ่งชั่วโมง นับถัดจากเวลาที่ รฟม. ได้แจ้งผู้ให้เช่ารับทราบถึงความชำรุดบกพร่องจนกว่าผู้ให้เช่าจะดำเนินการดังกล่าวแล้วเสร็จ โดยค่าปรับข้างต้นผู้ให้เช่ายินยอมให้ รฟม. สามารถหักจากค่าเช่ารายเดือนหรือเงินอื่น ๆ ที่ค้างจ่ายได้ทันที โดย รฟม. ไม่ต้องบอกสงวนสิทธิ์แต่อย่างใด

14.5 หากผู้ให้เช่าไม่สามารถปฏิบัติตามเงื่อนไขตามข้อ 13.3 ผู้ให้เช่าจะถูกปรับเป็นรายวันในอัตราร้อยละ 0.01 (ศูนย์จุดศูนย์หนึ่ง) ของมูลค่าของสัญญา นับถัดจากวันที่ครบกำหนดระยะเวลาที่ผู้ให้เช่าต้องดำเนินการ จนถึงวันที่เจ้าหน้าที่ผู้ดูแลระบบได้รับการฝึกอบรมจนแล้วเสร็จ โดยค่าปรับข้างต้นผู้ให้เช่ายินยอมให้ รฟม. สามารถหักจากค่าเช่ารายเดือนหรือเงินอื่น ๆ ที่ค้างจ่ายได้ทันที โดย รฟม. ไม่ต้องบอกสงวนสิทธิ์แต่อย่างใด

14.6 กรณีเจ้าหน้าที่ของผู้ให้เช่าปฏิบัติงานไม่ครบชั่วโมงการทำงาน ผู้ให้เช่ายินยอมให้ปรับในอัตราชั่วโมงละ 65 บาท (หกสิบห้าบาทถ้วน) (เศษของชั่วโมงให้นับเป็นหนึ่งชั่วโมง) โดยค่าปรับข้างต้นผู้ให้เช่ายินยอมให้ รฟม. สามารถหักจากค่าเช่ารายเดือนหรือเงินอื่น ๆ ที่ค้างจ่ายได้ทันที โดย รฟม. ไม่ต้องบอกสงวนสิทธิ์แต่อย่างใด

14.7 กรณีเจ้าหน้าที่ของผู้ให้เช่าไม่มาปฏิบัติงาน หรือมีความจำเป็นต้องหยุดงาน หรือไม่สามารถมาปฏิบัติงานได้ ผู้ให้เช่าต้องจัดส่งเจ้าหน้าที่ที่มีความรู้ความสามารถตามที่ รฟม. กำหนดไว้มาปฏิบัติงานแทนภายในเวลาไม่เกิน 9.00 น. ของวันทำงานนั้น โดยจะต้องแจ้งให้ รฟม. ทราบล่วงหน้าก่อนเจ้าหน้าที่จะเข้ามาปฏิบัติงานแทน หากผู้ให้เช่าไม่สามารถจัดหาเจ้าหน้าที่มาปฏิบัติงานแทนได้ หรือมาแล้วแต่ไม่สามารถปฏิบัติงานได้ ผู้ให้เช่ายินยอมให้ปรับในอัตรา 500 บาท (ห้าร้อยบาทถ้วน) ต่อวัน โดยค่าปรับข้างต้นผู้ให้เช่ายินยอมให้ รฟม. สามารถหักจากค่าเช่ารายเดือนหรือเงินอื่น ๆ ที่ค้างจ่ายได้ทันที โดย รฟม. ไม่ต้องบอกสงวนสิทธิ์แต่อย่างใด

15. เมื่อสิ้นสุดระยะเวลาสัญญา

15.1 เมื่อสิ้นสุดสัญญาเช่า หากการจัดหาหรือติดตั้งเครื่องพิมพ์ใหม่ของ รฟม. ยังดำเนินการไม่เสร็จเรียบร้อย รฟม. มีสิทธิ์ขอใช้รายการตามข้อ 2. ทั้งหมดหรือบางรายการต่อไป รวมถึงเจ้าหน้าที่ของผู้ให้เช่าตามข้อ 6.8 โดยคิดตามปริมาณการใช้งานจริงอ้างอิงจากสัญญา (หักด้วยกระดาษเสียจากจำนวนที่ใช้งานจริงต่อเครื่องจำนวนไม่น้อยกว่า 3 %) จนกว่า รฟม. จะจัดหาหรือติดตั้งเครื่องพิมพ์ใหม่สำเร็จ

/15.2 ภายหลัง...

15.2 ภายหลังจากที่ผู้ให้เช่าได้ดำเนินการตามข้อ 15.1 เรียบร้อยแล้ว หรือในกรณีที่ รฟม. บอกเลิกสัญญา ผู้ให้เช่าจะต้องขนย้ายเครื่องพิมพ์กลับคืนภายใน 15 วัน และผู้ให้เช่าจะต้องทำลายข้อมูล ซึ่งอยู่ภายในหน่วยเก็บข้อมูล (Hard disk) จนไม่สามารถกู้ข้อมูลกลับมาได้ โดย รฟม. จะไม่รับผิดชอบต่อความเสียหายหรือการสูญหายที่อาจเกิดขึ้นกับรายการตามข้อ 2. ทั้งหมด และผู้ให้เช่าจะต้องรับผิดชอบต่อค่าใช้จ่ายในการดำเนินการขนย้ายด้วย

16. ข้อสงวนสิทธิ์

16.1 ผู้ให้เช่าและ/หรือเจ้าหน้าที่ของผู้ให้เช่า ที่เข้าถึงระบบเทคโนโลยีสารสนเทศของ รฟม. ต้องรับทราบและปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของ รฟม. ตาม**ภาคผนวก จ.** และจะต้องรักษาความลับต่าง ๆ ที่ได้จากการปฏิบัติงาน โดยห้ามมิให้ผู้ให้เช่า และ/หรือเจ้าหน้าที่ของผู้ให้เช่านำข้อมูลส่วนหนึ่งส่วนใดหรือทั้งหมดที่ได้จากการปฏิบัติงานใน รฟม. ไปทำซ้ำ เผยแพร่ หรือวิเคราะห์ประมวลผลเพื่อการอื่นใด ไม่ว่าการกระทำดังกล่าวจะเป็นการหาผลประโยชน์หรือไม่ก็ตาม หาก รฟม. ตรวจพบผู้ให้เช่าต้องชดใช้ค่าเสียหายเป็นจำนวนเงินไม่น้อยกว่าค่าเช่าทั้งหมดที่กำหนดไว้ในสัญญา ทั้งนี้ ผู้ให้เช่าและ/หรือเจ้าหน้าที่ของผู้ให้เช่าต้องลงนามในสัญญาการเก็บรักษาข้อมูลไว้เป็นความลับ (Non-Disclosure Agreement) ตาม**ภาคผนวก ฉ.** ก่อนเริ่มปฏิบัติงานตามรูปแบบที่ รฟม. กำหนด

16.2 การใช้ประโยชน์ในเครื่องเช่าตามสัญญานี้ ผู้ให้เช่ายินยอมให้อยู่ภายใต้การจัดการและการควบคุมดูแลของ รฟม. โดยสิ้นเชิง นอกจาก รฟม. จะใช้ในการปฏิบัติงานของ รฟม. เองแล้ว รฟม. อาจให้ผู้อื่นมาใช้เครื่องเช่านี้ได้โดยอยู่ภายใต้การควบคุมดูแลของ รฟม.

16.3 ในกรณีที่ตรวจพบว่าเอกสารไม่ถูกต้อง หรือผิดพลาด หรือมีการร้องเรียน หรือมีการฟ้องร้องที่เกิดจากความผิดพลาดหรือข้อบกพร่องของผู้ให้เช่า ผู้ให้เช่าจะต้องเร่งดำเนินการแก้ไขให้ถูกต้อง และจะต้องรับผิดชอบค่าใช้จ่ายที่เกิดขึ้นจากความผิดพลาดหรือข้อบกพร่องนั้นทั้งสิ้น หากไม่ดำเนินการ รฟม. มีสิทธิ์บอกเลิกสัญญาและริบหลักประกันสัญญาทั้งหมดหรือบางส่วน ได้ตามเห็นสมควร

16.4 ในกรณีที่ รฟม. มีความจำเป็นต้องนำรายการตามข้อ 2. ไปใช้ในสถานที่อื่นนอกเหนือจากสถานที่ที่ติดตั้ง ผู้ให้เช่าจะต้องดำเนินการให้โดยไม่คิดค่าขนย้ายแต่ประการใด

16.5 ผู้ให้เช่าต้องไม่คิดอัตราค่าพิมพ์ขั้นต่ำต่อเดือนแต่ประการใด

16.6 ในกรณีที่ รฟม. มีความจำเป็นต้องเพิ่ม/ลด จำนวนรายการตามข้อ 2. หรืออุปกรณ์ที่เกี่ยวข้องภายในระยะเวลาของสัญญาผู้ให้เช่าจะต้องดำเนินการส่งมอบ ติดตั้ง หรือขนย้ายกลับคืน (แล้วแต่กรณี) ภายใน 7 วันทำการนับถัดจากวันที่ รฟม.หรือเจ้าหน้าที่ของ รฟม. ได้แจ้ง ผู้ให้เช่ารับทราบโดยทางโทรศัพท์ โทรศัพท์เคลื่อนที่ โทรสาร หรือจดหมายอิเล็กทรอนิกส์ (E-mail) (ในกรณีที่เป็นการขอเพิ่มจำนวนรายการตามข้อ 2. ผู้ให้เช่าจะต้องนำรายการตามข้อ 2. รุ่นเดิมหรือที่มีคุณสมบัติไม่ต่ำกว่ารุ่นเดิม มาให้ รฟม. โดยคิดอัตราค่าใช้งานตามที่ได้ตกลงราคาไว้ตามสัญญานี้)

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

16.8 กรณีที่ รฟม. ตรวจพบช่องโหว่หรือมีการประกาศช่องโหว่ของระบบงานพิมพ์อย่างเป็นทางการ ผู้ให้เช่าต้องปิดช่องโหว่ (Hardening) และรายงานผลการปิดช่องโหว่ให้ คณะกรรมการตรวจรับพัสดุฯ ทราบ

16.8.1 กรณีช่องโหว่วิกฤติ (Critical) ภายใน 30 วัน

16.8.2 กรณีช่องโหว่ระดับสูง (High) ภายใน 45 วัน

16.8.3 กรณีช่องโหว่ระดับปานกลาง (Medium) ภายใน 60 วัน

16.8.4 กรณีช่องโหว่ระดับระดับต่ำ (Low) ภายใน 120 วัน

นับแต่วันที่คณะกรรมการตรวจรับพัสดุฯ หรือผู้ควบคุมงาน แจ้งผู้ให้เช่ารับทราบหากผู้ให้เช่าไม่สามารถปิดช่องโหว่ดังกล่าวได้ผู้ให้เช่าจะต้องจัดทำแผนลดความเสี่ยงหรือกำหนดมาตรการควบคุมที่เหมาะสมเพื่อ

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd.

/ป้องกัน...

ป้องกันภัยคุกคามที่อาจจะเกิดขึ้น พร้อมระบุเหตุผลที่ไม่สามารถปิดช่องโหว่ให้คณะกรรมการตรวจรับพัสดุฯ ทราบภายในระยะเวลา 120 นับแต่วันที่คณะกรรมการตรวจรับพัสดุฯ หรือผู้ควบคุมงาน แจ้งผู้ให้เช่ารับทราบ

16.9 ผู้ให้เช่าจัดทำ Role Matrix เพื่อกำหนดสิทธิ์การเข้าถึงระบบโดยครอบคลุมถึง Module ย่อยทั้งหมด รวมถึง User กลุ่มต่าง ๆ ด้วย เช่น System User

16.10 ผู้ให้เช่าจะต้องไม่เอางานทั้งหมดหรือแต่บางส่วนไปจ้างช่วงอีกทอดหนึ่ง เว้นแต่การจ้างช่วงงาน แต่บางส่วนที่ได้รับอนุญาตเป็นหนังสือจากคณะกรรมการตรวจรับพัสดุฯ แล้วการที่ รฟม. ได้อนุญาตให้จ้างช่วงงานแต่บางส่วนดังกล่าวนั้น ไม่เป็นเหตุให้ผู้รับจ้างหลุดพ้นจากความรับผิดหรือพันธะหน้าที่ และผู้รับจ้างจะยังคงต้องรับผิดในความผิดและความประมาทเลินเล่อของผู้รับจ้างช่วง หรือของตัวแทนหรือลูกจ้างของผู้รับจ้างช่วงนั้นทุกประการ (หากมี)

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd.

ภาคผนวก ก.
รายละเอียดและคุณลักษณะเฉพาะ

1. <u>เครื่องพิมพ์ ขาว-ดำ ขนาด A4 มีคุณสมบัติอย่างน้อยหรือดีกว่าดังนี้</u>

1.1 เครื่องพิมพ์แบบเลเซอร์หรือแบบ LED

1.2 มีความเร็วในการพิมพ์ขาวดำ ไม่น้อยกว่า 40 แผ่นต่อนาทีที่ขนาดกระดาษ A4

1.3 มีความละเอียดในการพิมพ์ไม่น้อยกว่า 1200 จุดต่อนิ้ว

1.4 มีหน่วยความจำหลักไม่น้อยกว่า ขนาด 512 MB

1.5 มีช่องเชื่อมต่อระบบเครือข่าย (Ethernet) และ USB จำนวน 1 ช่อง

1.6 มีช่องใส่กระดาษป้อนมือ (Multi-Purpose Tray) ไม่น้อยกว่า 100 แผ่น

1.7 มีช่องใส่กระดาษ (Input Tray) ไม่น้อยกว่า 250 แผ่น

1.8 สามารถพิมพ์เอกสารสองหน้าได้อัตโนมัติ (Automatic Duplex)

1.9 สามารถพิมพ์งานบนกระดาษขนาด A4 , A5 และ Letter ได้

1.10 สามารถพิมพ์ได้ทั้งตัวอักษรภาษาไทยและภาษาอังกฤษ

1.11 รองรับภาษาในการพิมพ์แบบ PCL5 หรือ PCL6 และ Postscript Level 3

1.12 สามารถใช้งานกับระบบปฏิบัติการ Microsoft Windows 7 และ Microsoft Windows 10 และ Microsoft Windows 11 ได้

1.13 สามารถสรุปจำนวนการใช้งานการพิมพ์ได้

1.14 สามารถกำหนดค่าและจัดการเครื่องพิมพ์ผ่านระบบเครือข่ายได้

2. <u>เครื่องพิมพ์ สี ขนาด A4 มีคุณสมบัติอย่างน้อยหรือดีกว่าดังนี้</u>

2.1 เครื่องพิมพ์แบบเลเซอร์หรือแบบ LED

2.2 มีความเร็วในการพิมพ์สี ไม่น้อยกว่า 30 แผ่นต่อนาทีที่ขนาดกระดาษ A4

2.3 มีความละเอียดในการพิมพ์ไม่น้อยกว่า 1200 จุดต่อนิ้ว

2.4 มีหน่วยความจำหลักไม่น้อยกว่าขนาด 512 MB

2.5 มีช่องเชื่อมต่อระบบเครือข่าย (Ethernet) และ USB จำนวน 1 ช่อง

2.6 มีช่องใส่กระดาษป้อนมือ (Multi-Purpose Tray) ไม่น้อยกว่า 100 แผ่น

2.7 มีช่องใส่กระดาษ (Input Tray) ไม่น้อยกว่า 250 แผ่น

2.8 สามารถพิมพ์เอกสารสองหน้าได้อัตโนมัติ (Automatic Duplex)

2.9 สามารถพิมพ์งานบนกระดาษขนาด A4 , A5 และ Letter ได้

2.10 สามารถพิมพ์ได้ทั้งตัวอักษรภาษาไทยและภาษาอังกฤษ

2.11 รองรับภาษาในการพิมพ์แบบ PCL5 หรือ PCL6 และ Postscript Level 3

2.12 สามารถใช้งานกับระบบปฏิบัติการ Microsoft Windows 7 และ Microsoft Windows 10 และ Microsoft Windows 11 ได้

2.13 สามารถสรุปจำนวนการใช้งานการพิมพ์ได้

2.14 สามารถกำหนดค่าและจัดการเครื่องพิมพ์ผ่านระบบเครือข่ายได้

3. <u>เครื่องพิมพ์สี ขนาด A3 มีคุณสมบัติอย่างน้อยหรือดีกว่าดังนี้</u>

3.1 เครื่องพิมพ์แบบเลเซอร์หรือแบบ LED

บริษัท เคียวเซร่า ด็อคคิวเมนท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd.

/3.2 มีความ...

3.2 มีความเร็วในการพิมพ์สี ขนาด A4 ได้ไม่น้อยกว่า 30 แผ่นต่อนาที และ ขาว – ดำ ขนาด A4 ได้ไม่น้อยกว่า 30 แผ่นต่อนาที

3.3 มีความละเอียดในการพิมพ์ ไม่น้อยกว่า 600 จุดต่อนิ้ว

3.4 มีหน่วยความจำไม่น้อยกว่า 1 GB (คิดคำนวณโดยใช้ 1 GB = 1,000 MB)

3.5 มีช่องเชื่อมต่อระบบเครือข่าย (Ethernet) และ USB จำนวนไม่น้อยกว่า 1 ช่อง

3.6 มีช่องใส่กระดาษป้อนมือ (Multi-Purpose Tray) ไม่น้อยกว่า 90 แผ่น

3.7 มีช่องใส่กระดาษ (Input Tray) รวมกันไม่น้อยกว่า 250 แผ่น

3.8 สามารถพิมพ์เอกสารสองหน้าได้อัตโนมัติ (Automatic Duplex)

3.9 สามารถพิมพ์งานบนกระดาษขนาด A3 , A4 , A5 และ Letter ได้

3.10 สามารถพิมพ์ได้ทั้งตัวอักษรภาษาไทยและภาษาอังกฤษ

3.11 รองรับภาษาในการพิมพ์แบบ PCL5 หรือ PCL6 และ Postscript Level 3

3.12 เครื่องพิมพ์สามารถเข้าโปรแกรมประหยัดไฟโดยอัตโนมัติภายในเวลาที่กำหนดหลังการหยุดใช้

3.13 สามารถใช้งานบัตร Mifare ที่พนักงานและเจ้าหน้าที่ของ รฟม. ใช้งานอยู่ได้

3.14 รองรับการพิมพ์งานจากอุปกรณ์พกพา เช่น แท็บเล็ต หรือ สมาร์ทโฟน

3.15 สามารถใช้งานกับระบบปฏิบัติการ Microsoft Windows 7 และ Microsoft Windows 10 และ Microsoft Windows 11 ได้

3.16 สามารถสรุปจำนวนการใช้งานการพิมพ์ได้

3.17 สามารถกำหนดค่าและจัดการเครื่องพิมพ์ผ่านระบบเครือข่ายได้

4. เครื่องมัลติฟังก์ชัน สี ขนาด A4 มีคุณสมบัติอย่างน้อยหรือดีกว่าดังนี้

4.1 เครื่องพิมพ์แบบเลเซอร์หรือแบบ LED

4.2 เป็นเครื่องมัลติฟังก์ชันเลเซอร์สีที่ใช้หมึกพิมพ์ชนิดแห้ง

4.3 สามารถใช้งานฟังก์ชัน Print, Copy, Scan, fax

4.4 มีความเร็วในการพิมพ์สี ไม่น้อยกว่า 35 แผ่นต่อนาทีที่ขนาดกระดาษ A4

4.5 มีความละเอียดในการพิมพ์ไม่น้อยกว่า 600 จุดต่อนิ้ว

4.6 สามารถพิมพ์เอกสารสองหน้าได้อัตโนมัติ (Automatic Duplex)

4.7 สามารถพิมพ์เอกสารผ่านทาง USB ได้

4.8 มีความเร็วในการ Copy เอกสารสี ไม่น้อยกว่า 30 แผ่นต่อนาทีที่ขนาดกระดาษ A4

4.9 มีความละเอียดในการ Copy ไม่น้อยกว่า 600 จุดต่อนิ้ว

4.10 สามารถ Copy เอกสารสองหน้าได้อัตโนมัติ (Automatic Duplex)

4.11 สามารถ Scan แบบ Flatbed และ ADF (Automatic Document Feeder) ได้

4.12 มีความเร็วในการ Scan แบบ ADF ไม่น้อยกว่า 30 หน้าต่อนาทีที่ขนาดกระดาษ A4 (สีหรือขาวดำ) และมีความละเอียดในการ Scan แบบ ADF ไม่น้อยกว่า 600 จุดต่อนิ้ว

4.13 สามารถ Scan File Format แบบ PDF และ JPG ได้

4.14 มีฟังก์ชันการ Scan to Folder , Scan to USB และ Scan to E-mail

4.15 มีความละเอียดในการพิมพ์เอกสารจาก Fax ไม่น้อยกว่า 200 จุดต่อนิ้ว

4.16 มีหน่วยความจำหลักไม่น้อยกว่าขนาด 512 MB

4.17 มีช่องเชื่อมต่อระบบเครือข่าย (Ethernet) และ USB จำนวน 1 ช่อง

4.18 มีช่องใส่กระดาษป้อนมือ (Multi-Purpose Tray) ได้ไม่น้อยกว่า 90 แผ่น

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd.

/4.19 มีช่อง...

4.19 มีช่องใส่กระดาษ (Input Tray) ได้ไม่น้อยกว่า 250 แผ่น

4.20 สามารถพิมพ์งานบนกระดาษขนาด A4 , A5 และ Letter ได้

4.21 รองรับภาษาในการพิมพ์แบบ PCL5 หรือ PCL6 และ Postscript Level 3

4.22 สามารถใช้งานบัตร Mifare ที่พนักงานและเจ้าหน้าที่ของ รฟม. ใช้งานอยู่ได้

4.23 รองรับการพิมพ์งานจากอุปกรณ์พกพา เช่น แท็บเล็ต หรือ สมาร์ทโฟน

4.24 สามารถใช้งานกับระบบปฏิบัติการ Microsoft Windows 7 และ Microsoft Windows 10 และ Microsoft Windows 11 ได้

5. <u>ระบบควบคุมงานพิมพ์ มีคุณสมบัติอย่างน้อยหรือดีกว่าดังนี้</u>

5.1 สามารถเชื่อมต่อข้อมูลของผู้ใช้งานผ่านระบบ Active Directory (AD)

5.2 เป็นระบบที่สามารถควบคุมและกำหนดปริมาณการใช้งานเครื่องพิมพ์ได้ทั้งเอกสารสีและขาวดำ

5.3 สามารถควบคุมและกำหนดปริมาณการใช้งานแยกเป็นรายบุคคลหรือรายกลุ่มได้

5.4 สามารถปรับ ลด/เพิ่ม ปริมาณการใช้งานของผู้ใช้แต่ละคน หรือเป็นกลุ่มได้

5.5 สามารถกำหนดราคาของการพิมพ์เอกสารได้ทั้งเอกสารสี และเอกสารขาวดำ

5.6 สามารถแยกการคำนวณ การคิดราคาและปริมาณของงานที่สำเนาหรือสั่งพิมพ์ ที่เป็นงานที่มีทั้งหน้าสีและขาวดำ หากหน้าใดที่มีเฉพาะหน้าขาวดำจะคิดราคาการพิมพ์ขาวดำ และเฉพาะหน้าที่มีสีจะคิดราคาการพิมพ์ที่เป็นราคาสีได้

5.7 ซอฟต์แวร์ระบบบริหารจัดการสามารถทำงานบนระบบปฏิบัติการ Windows Server 2019 หรือดีกว่า

5.8 ซอฟต์แวร์ระบบบริหารจัดการสามารถกำหนดสิทธิ์การเข้าถึงการใช้งานได้

5.9 ระบบสามารถคำนวณค่าใช้จ่ายและกำหนดราคาต่อแผ่นได้ทั้ง สีและขาวดำ

5.10 ระบบสามารถแยกรายละเอียดข้อมูล (Log) หรือรายงาน (Report) โดยสามารถแสดงการสำเนา การพิมพ์ และสแกน ที่ผ่านการใช้งานจากเครื่องพิมพ์เป็นตารางข้อมูลได้

5.11 สามารถเชื่อมต่อระบบระหว่างสาขาหลัก (Master Site) และสาขาย่อย (Secondary Site) ได้ โดยการพิมพ์งานที่สาขาย่อยต้องใช้ระบบที่สาขาย่อยได้

5.12 ระบบสามารถพิมพ์งานแล้วผู้ใช้งานสามารถรับงานพิมพ์จากเครื่องถ่ายเอกสารหรือเครื่องพิมพ์ได้ในระบบเครือข่ายเดียวกัน

5.13 มีซอฟต์แวร์ระบบบริหารจัดการทรัพยากรเครื่องพิมพ์ที่เป็นซอฟต์แวร์สำเร็จรูปที่มีลิขสิทธิ์ถูกต้องตามกฎหมายครอบคลุมตลอดอายุสัญญา

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd.

ภาคผนวก ข.

ตัวอย่างตารางเปรียบเทียบคุณลักษณะเฉพาะ

หัวข้อ	คุณลักษณะเฉพาะ (ภาคผนวก ก.)	คุณลักษณะเฉพาะที่เสนอ	ข้อกำหนด	เอกสารอ้างอิง	หมายเหตุ
1.	เครื่องพิมพ์ ขาว-ดำ ขนาด A4 มีคุณสมบัติอย่างน้อยหรือดีกว่าดังนี้	เครื่องพิมพ์ ขาว-ดำ ยี่ห้อ รุ่น			
1.1	เครื่องพิมพ์แบบเลเซอร์หรือแบบ LED	เครื่องพิมพ์แบบเลเซอร์	ตรงตามข้อกำหนด	ชื่อ Catalog/ Brochure ..... หน้า	
1.2	มีความเร็วในการพิมพ์ขาวดำไม่น้อยกว่า 40 แผ่นต่อนาทีที่ขนาดกระดาษ A4	ความเร็วในการพิมพ์ขาวดำ 60 แผ่นต่อนาทีที่ขนาดกระดาษ A4	ดีกว่าข้อกำหนด	ชื่อ Catalog/ Brochure ..... หน้า	
1.3	มีความละเอียดในการพิมพ์ไม่น้อยกว่า 1200 จุดต่อนิ้ว	มีความละเอียดในการพิมพ์ไม่น้อยกว่า 600 จุดต่อนิ้ว	ไม่ตรงตามข้อกำหนด	ชื่อ Catalog/ Brochure ..... หน้า	
1...					
2.					
3.					
...					

ประทับตรา
(ถ้ามี)

ลงชื่อ____(ลงนามผู้มีอำนาจจากบริษัท)____.
(.....)
ตำแหน่ง.....

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd.

ภาคผนวก ค.

รายละเอียดคุณสมบัติและประสบการณ์การทำงานของเจ้าหน้าที่

รายละเอียดคุณสมบัติและประสบการณ์การทำงานของเจ้าหน้าที่

การเก็บรวบรวมข้อมูลส่วนบุคคลในเอกสารนี้ จัดทำขึ้นภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ด้วยวัตถุประสงค์เพื่อตรวจสอบข้อมูลของเจ้าหน้าที่ที่เข้ามาปฏิบัติงานให้ รฟม. ซึ่งเป็นการประมวลผลข้อมูลส่วนบุคคลเพื่อปฏิบัติตามสัญญา โดยเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็นจากเจ้าของข้อมูลส่วนบุคคล ซึ่ง รฟม. จะจัดเก็บข้อมูลส่วนบุคคลจนกว่าจะสิ้นสุดข้อผูกพันตามสัญญา ทั้งนี้ หากมีข้อสอบถามหรือขอใช้สิทธิ์ของเจ้าของข้อมูลส่วนบุคคล สามารถติดต่อได้ที่ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย สำนักงานใหญ่ เว็บไซต์ www.mrta.co.th โทรศัพท์ 0 2716 4000

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

รูปถ่าย
ไม่เกิน 6 เดือน

การศึกษา

ประกาศนียบัตรวิชาชีพชั้นสูง (ปวส.) _(สาขาวิชา)_ **สถานศึกษา** _(วิทยาลัย / มหาวิทยาลัย / ฯลฯ ประเทศ)_ **ปีที่จบการศึกษา** _(พ.ศ.)

ปริญญาตรี _(สาขาวิชา)_ **สถานศึกษา** _(วิทยาลัย / มหาวิทยาลัย / ฯลฯ , ประเทศ)_ **ปีที่จบการศึกษา** _(พ.ศ.)

สถานะการทำงานในปัจจุบัน

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

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

ผลการตรวจประวัติอาชญากรรมด้วยลายนิ้วมือ _○_ ไม่มีประวัติอาชญากรรม

ประสบการณ์การทำงาน

ลำดับที่ 1

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

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

ข้าพเจ้าขอรับรองว่ารายละเอียดคุณสมบัติและประสบการณ์การทำงานข้างต้นนี้ เป็นความจริงทุกประการ

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

ลงชื่อ_(ลงนามเจ้าหน้าที่)_
(.....)
วันที่...../...../.....

หมายเหตุ

- แนบหลักฐานสำเนาหนังสือรับรองวุฒิการศึกษา หรือประกาศนียบัตร และผลการตรวจประวัติอาชญากรรมด้วยลายนิ้วมือ เพื่อประกอบการพิจารณา
- แนบหลักฐานการเปลี่ยนชื่อหรือนามสกุล (ถ้ามี) เพื่อประกอบการพิจารณา
- ข้อมูลปีให้แสดงเป็นพุทธศักราช

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd.

ภาคผนวก ง.

ตัวอย่างสติกเกอร์

ตราบริษัท

ประเภทเครื่อง.....

รุ่นเครื่อง.....หมายเลขเครื่อง.....

บริษัท.....

เลขที่สัญญา .....

ระยะเวลาการรับประกัน .....

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด

KYOCERA

KYOCERA Document Solutions (Thailand) Corp., Ltd.

ภาคผนวก จ.

ประกาศการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

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

ประกาศการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ (ฉบับปรับปรุงครั้งที่ 11)

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

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

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

1. วัตถุประสงค์และขอบเขต

เพื่อให้การใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาและลดผลกระทบจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องหรือจากการถูกคุกคามจากภัยต่าง ๆ จึงได้กำหนดนโยบายเพื่อควบคุมการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ดังนี้

1.1 การเข้าถึงหรือควบคุมการใช้งานสารสนเทศครอบคลุม 4 ด้าน คือ

1.1.1 การเข้าถึงระบบสารสนเทศ (Access control) ต้องตรวจสอบการอนุมัติสิทธิ์การเข้าถึงระบบและกำหนดรหัสผ่าน การลงทะเบียนผู้ใช้งานเพื่อให้ผู้ใช้ที่มีสิทธิ์ (User authentication) เท่านั้นที่สามารถ /เข้าถึง ...

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

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

1.1.3 การเข้าถึงระบบปฏิบัติการ (Operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยกำหนดให้มีการยืนยันตัวตนเพื่อระบุถึงตัวตนของผู้ใช้งาน รวมทั้งกำหนดให้มีการจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น

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

1.2 มีระบบสารสนเทศและระบบสำรองที่อยู่ในสภาพพร้อมใช้งาน รวมทั้งมีแผนเตรียมพร้อมในกรณีฉุกเฉินหรือกรณีที่ไม่สามารถดำเนินการตามวิธีการทางอิเล็กทรอนิกส์ได้ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

1.3 ตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศอย่างสม่ำเสมอ

2. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รฟม.

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รฟม. ใช้แนวทางและกระบวนการอ้างอิงตาม 1) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานรัฐ พ.ศ. 2553 2) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555 และ 3) มาตรฐาน ISO/IEC 27001:2013 โดยแบ่งแนวปฏิบัติออกเป็น 16 ส่วนตามเอกสารแนบท้ายประกาศ ดังต่อไปนี้

2.1 นโยบายการบริหารจัดการความมั่นคงปลอดภัยสำหรับผู้บริหาร (ส่วนที่ 1)

2.2 ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร (ส่วนที่ 2)

2.3 การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (ส่วนที่ 3)

2.4 การจัดการทรัพย์สิน (ส่วนที่ 4)

2.5 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (ส่วนที่ 5)

2.6 การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ (ส่วนที่ 6)

2.7 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (ส่วนที่ 7)

2.8 การควบคุมหน่วยงานภายนอกและผู้ใช้งาน (บุคคลภายนอก) เข้าถึงระบบเทคโนโลยีสารสนเทศ (ส่วนที่ 8)

2.9 การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ของ รฟม. (ส่วนที่ 9)

2.10 การใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์ (ส่วนที่ 10)

/2.11 การใช้งาน ...

2.11 การใช้งานจดหมายอิเล็กทรอนิกส์ (ส่วนที่ 11)

2.12 การสำรองข้อมูลและการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (ส่วนที่ 12)

2.13 การตรวจสอบและประเมินความเสี่ยง (ส่วนที่ 13)

2.14 การถ่ายโอน และการแลกเปลี่ยนข้อมูลสารสนเทศ (ส่วนที่ 14)

2.15 การควบคุมการเข้ารหัส (ส่วนที่ 15)

2.16 การนำอุปกรณ์ส่วนตัวมาใช้งาน (Bring your own device) (ส่วนที่ 16)

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

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

นโยบายนี้ให้ใช้บังคับเมื่อพ้นกำหนด 7 วัน นับแต่วันที่ผู้มีอำนาจลงนาม

ประกาศ ณ วันที่ 7 กันยายน พ.ศ. 2565

(นายภคพงศ์ ศิริกันทรมาศ)
ผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

เอกสารแนบท้ายประกาศ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ของ รฟม.

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

1. รฟม. หมายถึง การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
2. ฝทท. หมายถึง ฝ่ายเทคโนโลยีสารสนเทศ
3. ผู้บริหารระดับสูงสุด หมายถึง ผู้ว่าการการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย
4. ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของ รฟม.
5. ผู้ใช้งาน หมายถึง บุคคลที่ได้รับอนุญาตให้สามารถเข้าใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. ดังนี้
   - บุคลากรของ รฟม.
   - บุคคลภายนอกที่ รฟม. อนุญาตให้เข้ามาใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. ได้ชั่วคราว เพื่อประโยชน์ในการดำเนินการของ รฟม. ได้แก่ พนักงานหรือลูกจ้างบริษัทภายนอกที่เข้ามาติดตั้งหรือดูแลรักษาระบบให้กับ รฟม. ที่ปรึกษา ผู้ปฏิบัติงานตามสัญญา หรือนิสิตนักศึกษาฝึกงาน
6. ผู้ใช้งานภายนอก หมายถึง ลูกค้าหรือบุคคลภายนอกที่ไม่ใช่กลุ่มผู้ใช้งานตามข้อ 5. ที่ใช้บริการระบบงานสารสนเทศของ รฟม. ผ่านเครือข่ายสาธารณะ (Internet)
7. หน่วยงานภายนอก หมายถึง องค์กร ซึ่ง รฟม. อนุญาตให้มีสิทธิ์ในการเข้าถึง หรือใช้ข้อมูล หรือสินทรัพย์ต่าง ๆ ของ รฟม. โดยจะได้รับสิทธิ์ในการใช้ระบบตามประเภทงานตามอำนาจและต้องรับผิดชอบในการรักษาความลับของข้อมูล
8. ผู้ดูแลระบบ หมายถึง พนักงานที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบสารสนเทศ
9. เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
10. มาตรฐาน หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย
11. ขั้นตอนปฏิบัติ หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานตามที่ได้กำหนดไว้ตามวัตถุประสงค์
12. แนวปฏิบัติ หมายถึง แนวทางที่ต้องปฏิบัติตามเพื่อให้สามารถบรรลุวัตถุประสงค์หรือเป้าหมายได้ง่ายขึ้น
13. ระบบเทคโนโลยีสารสนเทศ (Information technology system) หมายถึง ระบบงานของ รฟม. ที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายสื่อสารข้อมูลมาช่วยในการสร้างสารสนเทศที่ รฟม. สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุน การให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ ได้แก่ ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลและสารสนเทศ เป็นต้น

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd

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

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd.

และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ โดยข่าวสารที่ส่งนั้นจะถูกเก็บไว้ในตู้จดหมาย (Mail box) ที่กำหนดไว้สำหรับผู้ใช้งาน ผู้รับสามารถเปิดอ่าน พิมพ์ลงกระดาษ หรือจะลบทิ้งก็ได้

26. ชุดคำสั่งไม่พึงประสงค์ (Malicious code) หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
27. เครื่องคอมพิวเตอร์ หมายถึง เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ และเครื่องคอมพิวเตอร์แบบพกพา
28. อุปกรณ์เคลื่อนที่ (Mobile device) หมายถึง อุปกรณ์อิเล็กทรอนิกส์แบบพกพา ซึ่งมีความสามารถในการเชื่อมต่อกับอุปกรณ์อื่นเพื่อรับส่งข้อมูลผ่านระบบเครือข่ายโทรคมนาคมไร้สายหรือโดยอาศัยคลื่นแม่เหล็กไฟฟ้าเป็นสื่อกลาง เช่น Tablet, Smart Phone
29. อุปกรณ์ส่วนตัว หมายถึง อุปกรณ์ที่ รฟม. ไม่ได้เป็นผู้จัดสรรให้ใช้งาน แต่เป็นอุปกรณ์ส่วนตัวของผู้ใช้งานที่นำมาเชื่อมต่อกับเครือข่ายภายในของ รฟม. เช่น เครื่องคอมพิวเตอร์ส่วนบุคคล (Personal computer) เครื่องคอมพิวเตอร์พกพา (Notebook) อุปกรณ์เคลื่อนที่ (Mobile device) หรือ Removable media เป็นต้น

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd.

ส่วนที่ 1
นโยบายการบริหารจัดการความมั่นคงปลอดภัยสำหรับผู้บริหาร

วัตถุประสงค์

- เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรมีความสอดคล้องกับมาตรฐานสากลและกฎหมายด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง

ผู้รับผิดชอบ

- ผู้บริหารสูงสุด

อ้างอิงมาตรฐาน

- หมวดที่ 1 นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information security policy)

แนวปฏิบัติ

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

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd.

ส่วนที่ 2
ความมั่นคงปลอดภัยที่เกี่ยวกับบุคลากร

วัตถุประสงค์

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

ผู้รับผิดชอบ

- ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ ผู้อำนวยการฝ่ายทรัพยากรบุคคล ผู้อำนวยการฝ่าย/สำนัก ที่กำกับดูแลงานที่มีการว่าจ้างหน่วยงานภายนอก

อ้างอิงมาตรฐาน

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

แนวปฏิบัติ

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

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

2. การสร้างความมั่นคงปลอดภัยในระหว่างการจ้างงาน (During employment) เพื่อสร้างความตระหนักแก่ผู้ใช้งานเกี่ยวกับภัยที่เกี่ยวข้องกับการปฏิบัติงานสารสนเทศ รวมถึงให้ความรู้เพื่อให้สามารถป้องกันภัยดังกล่าวได้

2.1 หน้าที่ในการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management responsibilities)
ผู้บริหาร รฟม. ทุกระดับชั้นมีหน้าที่สนับสนุนและส่งเสริมเรื่องดังต่อไปนี้ แก่ผู้ใช้งาน

2.1.1 ประกาศนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ รฟม. เป็นลายลักษณ์อักษรให้ทุกคนรับทราบและปฏิบัติตาม

2.1.2 จูงใจให้ผู้ใช้งานปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ รฟม.

2.1.3 สร้างความตระหนักถึงความมั่นคงปลอดภัยด้านสารสนเทศที่เกี่ยวข้องกับหน้าที่ความรับผิดชอบของตนเองและของ รฟม.

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

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

2.2.2 ฝทท. ต้องดำเนินการฝึกอบรม หรือประชาสัมพันธ์เพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศแก่ผู้ใช้งานเป็นประจำทุกปี

2.2.3 ฝทท. ต้องแจ้งผู้ใช้งานให้ทราบ เมื่อมีการเปลี่ยนแปลงนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศของ รฟม. รวมทั้งอธิบายผลกระทบจากการเปลี่ยนแปลงดังกล่าว

2.3 การกำหนดบทลงโทษ

2.3.1 ความรับผิดตามกฎหมาย

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ไม่ได้ก่อให้เกิดสิทธิ์ทางกฎหมายที่ทำให้ผู้ใช้งานพ้นผิดแม้จะได้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ และผู้ใช้งานตกลงยินยอมที่จะไม่ดำเนินการใด ๆ ทางกฎหมายต่อ รฟม. ซึ่งได้ปฏิบัติตามระเบียบนี้ แต่อย่างไรก็ตามหากผู้ใช้งานกระทำการละเมิดหรือกระทำผิดตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ อาจเป็นความผิดทางวินัยและเป็นเหตุให้ถูกลงโทษทางวินัยได้ รฟม. ไม่มีส่วนรับผิดชอบต่อการละเมิดทรัพย์สินทางปัญญาที่เกิดจากการใช้ระบบคอมพิวเตอร์

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd.

2.3.2 การพิจารณาโทษผู้กระทำผิด

ผู้ใช้งานที่กระทำความผิด ฝทท. จะเพิกถอนสิทธิ์การใช้งานและอาจเป็นความผิดทางวินัย หรือความผิดตามกฎหมายที่เกี่ยวข้อง

1) พนักงาน/ลูกจ้างที่ฝ่าฝืนหรือละเมิดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รฟม. ต้องถูกลงโทษตามกระบวนการทางวินัยของ รฟม. รวมถึงกฎหมายที่เกี่ยวข้อง

2) หน่วยงานภายนอกที่กระทำความผิด จะมีโทษตามที่ระบุไว้ในสัญญาหรือถูกเพิกถอนสิทธิ์การใช้งาน รวมถึงดำเนินการตามกฎหมายที่เกี่ยวข้อง

3. การสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน (Termination and change of employment)

เพื่อกำหนดหน้าที่ความรับผิดชอบเมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน ซึ่งรวมไปถึงการคืนทรัพย์สินและการถอดถอนสิทธิ์ในการเข้าถึง

3.1 การแจ้งการสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน

3.1.1 ฝ่ายทรัพยากรบุคคลต้องแจ้งให้ฝ่ายเทคโนโลยีสารสนเทศทราบทันทีหากพนักงานมีการลาออก โยกย้าย เกษียณ หรือเสียชีวิต เพื่อฝ่ายเทคโนโลยีสารสนเทศจะได้ตรวจสอบและบริหารจัดการสิทธิ์ในการเข้าถึงระบบเทคโนโลยีสารสนเทศ

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

3.2 การคืนสินทรัพย์ของ รฟม.

ผู้ดูแลระบบต้องตรวจสอบเพื่อเรียกคืนสินทรัพย์ของ รฟม. จากผู้ใช้งาน เมื่อการสิ้นสุดหรือการเปลี่ยนแปลงการจ้างงาน

3.3 การถอดถอนสิทธิ์ในการเข้าถึง

3.3.1 ผู้ดูแลระบบต้องถอดถอนสิทธิ์ในการเข้าถึงของผู้ใช้งาน เมื่อสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน

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

3.3.3 ในกรณีที่ผู้ใช้งานที่สิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน มีการใช้บัญชีผู้ใช้งานร่วมกัน (Shared user ID) กับผู้ใช้งานอื่น ผู้บังคับบัญชาต้องเปลี่ยนรหัสผ่านทันทีหลังจากสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd

ส่วนที่ 3
การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

วัตถุประสงค์

- เพื่อควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าถึงอาคารสถานที่ และพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area)

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้อำนวยการฝ่ายจัดซื้อและบริการ

อ้างอิงมาตรฐาน

- หมวดที่ 7 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental security)

แนวปฏิบัติ

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

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

5.1.4 เจ้าหน้าที่รักษาความปลอดภัย (รปภ.) ต้องตรวจสอบผู้ติดต่อ อุปกรณ์ พร้อมลงเวลาออกที่สมุดบันทึกหรือระบบสารสนเทศให้ถูกต้อง

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

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd.

ส่วนที่ 4
การจัดการทรัพย์สิน

วัตถุประสงค์

- เพื่อบริหารจัดการทรัพย์สินสารสนเทศ ตั้งแต่การจัดหา การใช้งาน จนถึงการยกเลิกใช้งาน โดยมีการระบุสินทรัพย์ขององค์กรและกำหนดหน้าที่ความรับผิดชอบในการปกป้องทรัพย์สินสารสนเทศอย่างเหมาะสม

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- เจ้าของข้อมูล
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 4 การบริหารจัดการทรัพย์สิน (Asset management)

แนวปฏิบัติ

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

ก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อเพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลที่สำคัญได้ โดยพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

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

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

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd.

ส่วนที่ 5
การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

วัตถุประสงค์

- เพื่อควบคุมการจัดหา พัฒนา และบำรุงรักษาระบบสารสนเทศ ให้มีการกำหนดมาตรการการรักษาความมั่นคงปลอดภัย เพื่อป้องกันความผิดพลาด สูญหาย และการเปลี่ยนแปลงแก้ไขระบบ

ผู้รับผิดชอบ

- ผู้บังคับบัญชา
- ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

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

แนวปฏิบัติ

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

10. ผู้ดูแลระบบต้องแสดงข้อมูลของผู้ใช้งานอย่างรัดกุม เช่น การปิดบังข้อมูลสำคัญของผู้ใช้งาน (Sensitive data masking) เป็นต้น
11. กรณีของแอปพลิเคชันที่ใช้งานผ่านอุปกรณ์เคลื่อนที่ (Mobile device) ให้ผู้ดูแลระบบดำเนินการ ดังนี้
    11.1 ปิดบังหน้าจอเมื่อย่อแอปพลิเคชัน (Application blurring) เพื่อลดความเสี่ยงที่ข้อมูลสำคัญของผู้ใช้งานจะรั่วไหล
    11.2 ขอสิทธิ์เข้าถึงทรัพยากรหรือบริการโดยแอปพลิเคชัน (Application permission) บนอุปกรณ์เคลื่อนที่ของผู้ใช้งานเท่าที่จำเป็น และมีกระบวนการทบทวนการขอสิทธิ์เป็นประจำเพื่อป้องกันการละเมิดสิทธิ์ความเป็นส่วนตัวของผู้ใช้งาน
12. ผู้ดูแลระบบต้องควบคุมข้อมูลที่นำมาใช้ในการทดสอบระบบ (Test data) อย่างเหมาะสม โดยไม่นำข้อมูลจริงมาทดสอบ กรณีจำเป็นต้องใช้ข้อมูลจริงต้องได้รับอนุญาตข้อมูลจากเจ้าของก่อนนำมาใช้งาน และทำลายข้อมูลอย่างเหมาะสมตามขั้นตอนที่ รฟม. กำหนด
13. ผู้ดูแลระบบต้องแยกระบบสารสนเทศสำหรับการพัฒนา ทดสอบ และใช้งานจริงออกจากกันเพื่อลดความเสี่ยงที่เกิดจากการเปลี่ยนแปลงระบบสารสนเทศโดยไม่ได้รับอนุญาต และต้องมีการกำหนดสิทธิ์การเข้าถึงระบบสารสนเทศที่พัฒนา ทดสอบ หรือใช้งานจริง ทั้งระบบสารสนเทศใหม่ และการปรับปรุงแก้ไขระบบสารสนเทศเดิม
14. ผู้ดูแลระบบต้องมีการกำหนดขั้นตอนการทดสอบระบบสารสนเทศก่อนนำไปใช้งานจริง ทั้งในกรณีปรับปรุงระบบสารสนเทศเดิมและการพัฒนาระบบสารสนเทศใหม่
15. ผู้ดูแลระบบต้องติดตั้งซอฟต์แวร์บนระบบสารสนเทศที่ให้บริการ (Production) ตามขั้นตอนที่ รฟม. กำหนด และจำกัดสิทธิ์การติดตั้งซอฟต์แวร์เพื่อให้ระบบสารสนเทศต่าง ๆ มีความถูกต้องครบถ้วนและน่าเชื่อถือ
16. ผู้ดูแลระบบต้องนำซอฟต์แวร์ที่ไม่ละเมิดลิขสิทธิ์มาติดตั้งบนระบบสารสนเทศที่ให้บริการ (Production)
17. ผู้ดูแลระบบต้องกำกับดูแลให้ผู้รับจ้างปฏิบัติตามสัญญาหรือข้อตกลงการให้บริการที่ระบุไว้ โดยครอบคลุมถึงด้านความมั่นคงปลอดภัยสารสนเทศ และการปฏิบัติตามขั้นตอนที่เกี่ยวข้องต่าง ๆ ที่ รฟม. กำหนดไว้
18. ผู้ดูแลระบบ ต้องติดตาม ตรวจสอบรายงาน หรือบันทึกการให้บริการของบุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามสัญญาว่าจ้างอย่างสม่ำเสมอ
19. ผู้ดูแลระบบ ต้องดูแลให้ทรัพย์สินสารสนเทศได้รับการบำรุงรักษาและซ่อมแซมตามความต้องการ รวมทั้งต้องมีการบันทึกประวัติการทำงานผิดปกติ การบำรุงรักษา และการซ่อมแซมอุปกรณ์นั้น ๆ อย่างสม่ำเสมอ
20. ผู้ดูแลระบบจะต้องปิดช่องโหว่ของระบบสารสนเทศที่มีระดับความรุนแรงในระดับวิกฤติ (Critical) และระดับความรุนแรงระดับสูง (High) ทั้งหมดก่อนนำไปใช้งานจริง (Production) หรือก่อนเริ่ม Go live โดยเฉพาะระบบที่ให้บริการผ่านเครือข่ายอินเทอร์เน็ต (Internet facing) และระบบที่มีความสำคัญต่อการดำเนินงานของ รฟม.
21. ผู้ดูแลระบบต้องพิจารณาเลือกใช้ Version ของ Software ดังนี้
    21.1 กรณีนำ Software เดิมมาใช้ในการจัดหาหรือพัฒนาระบบ จะต้องนำผลการตรวจสอบช่องโหว่และผลการทดสอบเจาะระบบมาประกอบการพิจารณาคัดเลือกเวอร์ชันของ Software ด้วย เพื่อป้องกันไม่ให้เกิดช่องโหว่เดิมรวมถึงเพื่อลดภาระงานในการปิดช่องโหว่เดิมซ้ำ
    21.2 กรณีเป็น Software ที่ไม่เคยนำมาใช้งานให้เลือกใช้ Software เวอร์ชันล่าสุด

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd.

ส่วนที่ 6
การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

- เพื่อควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศตั้งแต่การกำหนดสิทธิ์ กำหนดประเภทของข้อมูล จัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ระดับชั้นการเข้าถึง เวลาที่เข้าถึงได้ และช่องทางการเข้าถึง ทั้งนี้ เพื่อควบคุมและป้องกันการเข้าถึง การล่วงรู้ และการแก้ไขระบบสารสนเทศของ รฟม. โดยไม่ได้รับอนุญาต

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- เจ้าของข้อมูล
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

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

แนวปฏิบัติ

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

1.5 ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ใช้งาน ต้องปฏิบัติ ดังนี้

1.5.1 แบ่งประเภทข้อมูล ดังนี้

1) ข้อมูลและสารสนเทศสำหรับสนับสนุนการตัดสินใจของผู้บริหาร ได้แก่ ข้อมูลสารสนเทศที่มีความสำคัญหรือมีความจำเป็นเร่งด่วนที่ต้องติดตามอย่างใกล้ชิดเพื่อประกอบการตัดสินใจเชิงนโยบาย กำหนดนโยบาย และการวางแผนของผู้บริหารระดับสูง

2) ข้อมูลและสารสนเทศสนับสนุนเชิงยุทธศาสตร์ (Strategy data) ได้แก่ ข้อมูลและสารสนเทศเชิงวิชาการเพื่อสนับสนุนการดำเนินงานตามพันธกิจและยุทธศาสตร์ของ รฟม. ให้บรรลุเป้าหมาย รวมทั้งข้อมูลที่เผยแพร่แก่ผู้รับบริการภายนอก

3) ข้อมูลและสารสนเทศที่สนับสนุนการปฏิบัติงานประจำ (Operation data) ได้แก่ ข้อมูลที่สนับสนุนการทำงานทั่วไปของ รฟม.

1.5.2 จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น 3 ระดับ คือ

1) ข้อมูลที่มีระดับความสำคัญมาก หมายถึง ข้อมูลที่ใช้สำหรับสนับสนุนการตัดสินใจของผู้บริหาร

2) ข้อมูลที่มีระดับความสำคัญปานกลาง หมายถึง ข้อมูลที่ใช้ปฏิบัติงานเฉพาะกลุ่มงาน แผนก กอง หรือฝ่ายภายในองค์กร

3) ข้อมูลที่มีระดับความสำคัญน้อย หมายถึง ข้อมูลที่พนักงาน/ลูกจ้างภายใน รฟม. สามารถเข้าถึงร่วมกันได้หรือสามารถเผยแพร่ได้

1.5.3 จัดแบ่งลำดับชั้นความลับของข้อมูลตามที่ รฟม. กำหนด

1.5.4 จัดแบ่งระดับชั้นการเข้าถึง

1) ระดับชั้นสำหรับผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และภารกิจที่ได้รับมอบหมาย

2) ระดับชั้นสำหรับผู้ปฏิบัติงานทั่วไป เข้าถึงข้อมูลที่ได้รับมอบหมายตามอำนาจหน้าที่

3) ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย มีสิทธิ์ในการบริหารจัดการระบบและเข้าถึงข้อมูลที่ได้รับมอบหมายตามอำนาจหน้าที่

1.6 เจ้าของข้อมูลและผู้ดูแลระบบต้องกำหนดเวลาการเข้าถึงระบบสารสนเทศ

1.7 ผู้ดูแลระบบต้องจำกัดช่องทางการเข้าถึงระบบเทคโนโลยีสารสนเทศตามช่องทาง ดังนี้

1) เครือข่ายภายในของ รฟม.

2) เครือข่ายภายนอก รฟม.

3) เครือข่ายอื่นที่จัดไว้ให้ เช่น ระบบเครือข่ายสื่อสารข้อมูล GIN

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

1.8 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องพิจารณาข้อกำหนดต่าง ๆ ที่มีผลทางกฎหมายซึ่งเกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศของ รฟม. เช่น พระราชบัญญัติ ข้อกำหนดทางกฎหมาย ข้อกำหนดในสัญญา

และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่น ๆ เป็นต้น เพื่อกำหนดสิทธิ์การเข้าถึงสารสนเทศและระบบเทคโนโลยีสารสนเทศของ รฟม.

1.9 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องมีการสอบทานสิทธิ์ในการเข้าถึงระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ พร้อมทั้งเพิกถอนสิทธิ์เมื่อพบเห็นสิทธิ์ที่ไม่ถูกต้องตามสิทธิ์ในการเข้าถึง (Authorization matrix)

2. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)

ให้มีการควบคุมการลงทะเบียนผู้ใช้งาน การบริหารจัดการรหัสผ่าน การบริหารจัดการสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศ และการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน

2.1 การลงทะเบียนผู้ใช้งาน (User registration)

2.1.1 ผู้ดูแลระบบต้องบริหารจัดการและควบคุมบัญชีชื่อผู้ใช้งาน (Username) มิให้มีการใช้งานบัญชีชื่อผู้ใช้งานซ้ำกัน ทั้งนี้ ในส่วนของพนักงาน/ลูกจ้าง รฟม. ให้กำหนดชื่อผู้ใช้งาน (Username) ตามมาตรฐานจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ใช้ในองค์กร

2.1.2 เจ้าของข้อมูลต้องเป็นผู้อนุมัติการสร้างบัญชีผู้ใช้งานชั่วคราว (Temporary user) และต้องจำกัดช่วงเวลาการใช้งานเท่าที่จำเป็น

2.2 การบริหารจัดการรหัสผ่าน (User password management)

2.2.1 ผู้ดูแลระบบและผู้รับจ้าง ต้องกำหนดความยาวรหัสผ่านอย่างน้อย 12 หลัก

2.2.2 บุคลากรของ รฟม. (พนักงาน/ลูกจ้างของ รฟม.) ต้องกำหนดความยาวรหัสผ่านอย่างน้อย 8 หลัก

2.2.3 ผู้ดูแลระบบกำหนดรหัสผ่านแบบชั่วคราวโดยใช้วิธีการสุ่ม และบังคับให้มีการเปลี่ยนรหัสผ่านเมื่อผู้ใช้งานเข้าใช้งานระบบในครั้งแรก (บังคับใช้เฉพาะกรณีข้อ 2.2.1 – 2.2.2)

2.2.4 ผู้ดูแลระบบและผู้รับจ้าง รวมถึงบุคลากรของ รฟม. (พนักงาน/ลูกจ้างของ รฟม.) ตามข้อ 2.2.1 – 2.2.2 ต้องปฏิบัติเพิ่มเติม ดังนี้

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

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

3) ต้องไม่ใช้งานรหัสผ่านโดยกระบวนการเข้าใช้งานโดยอัตโนมัติ ได้แก่ การกำหนดค่า “Remember Password” เป็นต้น

4) ต้องเก็บรหัสผ่านไว้เป็นความลับเฉพาะบุคคล ไม่เปิดเผยให้ผู้อื่นรับทราบ และไม่พิมพ์รหัสผ่านในลักษณะเปิดเผย เช่น พิมพ์รหัสผ่านต่อหน้าผู้ใช้งานคนอื่น เป็นต้น

5) ต้องไม่ใช้บัญชีชื่อผู้ใช้งานและรหัสผ่านร่วมกันกับผู้อื่น แม้ว่าบัญชีชื่อผู้ใช้งานจะได้รับการอนุญาตจากเจ้าของชื่อผู้ใช้งานบุคคลนั้นก็ตาม

6) ต้องเปลี่ยนแปลงรหัสผ่านเป็นประจำอย่างน้อยทุก 6 เดือน

7) ต้องเปลี่ยนแปลงรหัสผ่านเมื่อมีการแจ้งเตือนจากระบบ หรือสงสัยว่ารหัสผ่านล่วงรู้โดยบุคคลอื่น

2.2.5 ผู้ดูแลระบบ ต้องกำหนดให้มีการเข้ารหัสข้อมูลรหัสผ่านในระบบ

2.2.6 ผู้ดูแลระบบ ต้องจัดให้มีการควบคุมรหัสผ่านอย่างเข้มงวด

2.2.7 ผู้ดูแลระบบต้องจัดส่งบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ด้วยวิธีการที่ปลอดภัย

2.2.8 ผู้ดูแลระบบต้องควบคุมดูแลระบบปฏิบัติการ ฐานข้อมูล และระบบงานสารสนเทศ (Application) ที่จัดเก็บบัญชีผู้ใช้งานและรหัสผ่านอย่างเข้มงวด โดยให้เข้าถึงได้เฉพาะผู้ดูแลระบบที่ได้รับอนุญาตเท่านั้น

2.2.9 ผู้ดูแลระบบต้องกำหนดวิธีการหรือกระบวนการยืนยันตัวตนที่ปลอดภัย เช่น กรณีที่ลืมรหัสผ่าน

2.2.10 ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานภายนอกที่สมัครใช้บริการระบบงานสารสนเทศของ รฟม. ใช้รหัสผ่านอย่างมั่นคงปลอดภัย ดังนี้

<u>กรณีแอปพลิเคชันทั่วไป</u>

1) กำหนดความยาวรหัสผ่านอย่างน้อย 8 หลัก ซึ่งประกอบด้วย ตัวอักษร ตัวเลข และอักขระพิเศษ เช่น (a-Z) (0-9) (@ , # , & , " , ' , *, =, < , > , % , $, + , ?) เป็นต้น
2) ไม่บังคับให้เปลี่ยนรหัสผ่าน ทั้งนี้ขึ้นอยู่กับความสมัครใจในการเปลี่ยนรหัสผ่าน และระบบต้องรองรับการเปลี่ยนรหัสผ่านในกรณีต่าง ๆ ด้วยวิธีการที่ปลอดภัย

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

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

2.3 การบริหารจัดการสิทธิ์ (Privilege management)

2.3.1 ผู้บังคับบัญชาต้องกำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียน การเพิกถอนสิทธิ์ การเปลี่ยนแปลงสิทธิ์ และการทบทวนสิทธิ์ของผู้ใช้งานอย่างเป็นลายลักษณ์อักษร

2.3.2 กำหนดสิทธิ์ที่เหมาะสมกับผู้ใช้งานตามความจำเป็นและสอดคล้องกับหน้าที่ความรับผิดชอบและจัดเก็บประวัติ (Log) การลงทะเบียน การเพิกถอนสิทธิ์ และการเปลี่ยนแปลงสิทธิ์ของผู้ใช้งาน

2.3.3 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจัดให้มีการควบคุมและจำกัดสิทธิ์ในการใช้งานระบบตามความจำเป็นในการใช้งานเท่านั้น

1) สิทธิ์ในการสร้างข้อมูล (Create)
2) สิทธิ์ในการอ่านข้อมูลหรือเรียกดูข้อมูล (READ)
3) สิทธิ์ในการปรับปรุงข้อมูล (Modify / Update)
4) สิทธิ์ในการลบข้อมูล (Delete)
5) สิทธิ์ในการมอบหมายสิทธิ์ในการดำเนินการแทน (Assign)
6) สิทธิ์ในการรับรองความถูกต้องครบถ้วนของข้อมูล (Approve/Authenticate)
7) ไม่มีสิทธิ์

2.3.4 เจ้าของข้อมูลและผู้ดูแลระบบต้องเป็นผู้อนุมัติการให้สิทธิ์เพื่อเข้าถึงสารสนเทศหรือระบบเทคโนโลยีสารสนเทศใด ๆ อย่างเป็นลายลักษณ์อักษร

2.3.5 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจำกัดจำนวนผู้ใช้งานที่ทำหน้าที่เป็นผู้ให้สิทธิ์กับผู้ใช้งานให้น้อยที่สุดตามความเหมาะสม

2.3.6 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจำกัดระยะเวลาการใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. แก่หน่วยงานภายนอกที่เข้ามาปฏิบัติงานร่วมกับ รฟม.

2.3.7 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องจัดให้มีการถอดถอนหรือเปลี่ยนแปลงสิทธิ์การเข้าถึงทันทีเมื่อผู้ใช้งานเกษียณ เปลี่ยนแปลงหน้าที่ความรับผิดชอบ เปลี่ยนแปลงการจ้างงาน หรือไม่มีความจำเป็นในการใช้งานระบบเทคโนโลยีสารสนเทศ

2.3.8 ผู้ดูแลระบบต้องลบหรือระงับการใช้งานสิทธิ์ของผู้ใช้งานที่มากับระบบ (Default user) ในกรณีที่มีความจำเป็นต้องใช้งานต้องกำหนดรหัสผ่านอย่างมั่นคงปลอดภัย

2.4 การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of user access rights)

2.4.1 เจ้าของข้อมูลและผู้ดูแลระบบ ต้องมีการสอบทานสิทธิ์การเข้าถึงของผู้ใช้งานระบบเมื่อ รฟม. มีการเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศหรือโครงสร้างองค์กร

2.4.2 ผู้ดูแลระบบ ต้องมีการสอบทานและระงับการใช้งานบัญชีผู้ใช้งานที่ไม่ได้ใช้งานเกิน 180 วัน หากผู้ใช้งานต้องการกลับมาใช้งานจะต้องยืนยันตัวตนให้ ฝทท. ทราบ ทั้งนี้ ระยะเวลาที่ไม่ได้ใช้งานของบัญชีผู้ใช้งานอาจจะขึ้นอยู่กับแต่ละระบบสารสนเทศ

3. การป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล และการควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย

3.1 การป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล (Unattended user equipment)

3.1.1 ผู้ดูแลระบบต้องจัดให้มีมาตรการสำหรับป้องกันระบบคอมพิวเตอร์ ระบบเครือข่ายสื่อสารข้อมูล และระบบเทคโนโลยีสารสนเทศ โดยการกำหนดค่าของระบบ (Configuration) ให้มีการล็อกหน้าจอสำหรับอุปกรณ์ที่ไม่มีพนักงานดูแล หรือล็อกอุปกรณ์อยู่เสมอ

3.1.2 ผู้ใช้งานและหน่วยงานภายนอก ต้องล็อกหน้าจออัตโนมัติเมื่อไม่มีการใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. ตามระยะเวลาที่กำหนด โดยต้องพักหน้าจอ (Screen saver) อัตโนมัติหลังจากที่ไม่มีการใช้งานคอมพิวเตอร์เป็นระยะเวลานานกว่า 15 นาที ผู้ใช้งานและหน่วยงานภายนอกจะใช้งานต่อได้เมื่อมีการใส่รหัสผ่านที่ถูกต้อง

3.1.3 ผู้ใช้งานต้อง Log out ออกจากเครื่องคอมพิวเตอร์เมื่อมีความจำเป็นต้องละทิ้งเครื่องคอมพิวเตอร์

3.1.4 ผู้ใช้งานต้องป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ เช่น กล้องดิจิทัล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสารโดยไม่ได้รับอนุญาต

3.2 การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear desk and clear screen control)

3.2.1 ผู้บังคับบัญชาต้องกำหนดให้มีผู้รับผิดชอบในการดูแลสถานที่ที่มีการรับ - ส่งแฟกซ์ หรือจดหมายเข้า - ออก

3.2.2 ผู้ใช้งานต้องออกจากระบบคอมพิวเตอร์ (Log out) ทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล

3.2.3 ผู้ใช้งานต้องจัดเก็บข้อมูลสำคัญแยกต่างหาก และป้องกันให้มีความปลอดภัยอย่างพอเพียง

3.2.4 ผู้ใช้งานต้องนำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd.

4. การควบคุมการเข้าถึงเครือข่าย (Network access control)

ให้มีการควบคุมการใช้งานบริการเครือข่าย การควบคุมการพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอก รฟม. การควบคุมการพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย การป้องกันพอร์ต (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ การแบ่งแยกเครือข่าย (Segregation in networks) อย่างเหมาะสม การควบคุมการเชื่อมต่อทางเครือข่าย และการควบคุมการกำหนดเส้นทางบนเครือข่าย

4.1 การใช้งานบริการเครือข่าย (Use of network services)

4.1.1 ผู้ดูแลระบบต้องควบคุมการเผยแพร่แผนผังระบบเครือข่ายสื่อสารข้อมูล (Network diagram) รวมถึงโครงสร้าง IP address ชื่อระบบ และชื่ออุปกรณ์สารสนเทศแก่ผู้ที่ไม่ได้รับอนุญาตหรือหน่วยงานภายนอก

4.1.2 ผู้ดูแลระบบต้องควบคุมการใช้งานระบบเครือข่ายสื่อสารข้อมูล เพื่อป้องกันการเข้าถึงระบบเครือข่ายสื่อสารข้อมูลและบริการของระบบเครือข่ายสื่อสารข้อมูลโดยไม่ได้รับอนุญาต

4.1.3 ผู้ดูแลระบบต้องควบคุมการเชื่อมต่อเครือข่ายภายนอก เพื่อใช้งานอินเทอร์เน็ต ซึ่งอาจเป็นช่องทางให้หน่วยงานภายนอกเข้าถึงสารสนเทศหรือระบบเทคโนโลยีสารสนเทศของ รฟม. โดยมิได้รับอนุญาต

4.1.4 ผู้ใช้งานต้องแจ้งความประสงค์ในการขอใช้งานบริการเครือข่ายแก่ ฝทท. และสามารถใช้บริการเครือข่ายได้หลังจากได้รับการอนุมัติจาก ฝทท. แล้ว

4.1.5 ผู้ใช้งาน ต้องไม่ใช้ระบบเครือข่ายสื่อสารข้อมูลเพื่อเป็นช่องทางในการเจาะระบบ (Hacking) หรือการสแกนช่องโหว่ของระบบโดยมิได้รับอนุญาต

4.2 การพิสูจน์ตัวตนของผู้ใช้งานที่อยู่ภายนอก รฟม. (User authentication for external connections)

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

4.3 การพิสูจน์ตัวตนของอุปกรณ์ในระบบเครือข่ายสื่อสารข้อมูล (Equipment identification in networks)

ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนของอุปกรณ์ในระบบเครือข่ายสื่อสารข้อมูล ได้แก่ การตรวจสอบ MAC address

4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection)

ผู้ดูแลระบบต้องระงับบริการและพอร์ต (Port) ที่ไม่มีความจำเป็นต้องใช้บนเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่าย

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

4.6 การแบ่งแยกเครือข่าย (Segregation in networks)

4.6.1 ผู้ดูแลระบบต้องจัดให้มีการแบ่งแยกเครือข่ายตามกลุ่มของผู้ใช้งาน หรือกลุ่มของระบบเทคโนโลยีสารสนเทศ เพื่อควบคุมการใช้งานในแต่ละเครือข่ายย่อยอย่างเหมาะสม โดยพิจารณา

จากความต้องการในการเข้าถึงข้อมูล ระดับความสำคัญของข้อมูล รวมถึงการพิจารณาด้านราคา ประสิทธิภาพ และผลกระทบทางด้านความปลอดภัยดังต่อไปนี้

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

4.6.2 ผู้ดูแลระบบจะกำหนดเส้นทางบนเครือข่ายที่เข้มงวด เพื่อจำกัดการเข้าถึงระยะไกลไปเฉพาะเครือข่ายที่กำหนดเท่านั้น

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

4.7 การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control)

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

4.7.2 ผู้ดูแลระบบต้องติดตั้ง Firewall ระหว่างเครือข่ายของ รฟม. กับเครือข่ายภายนอก ทั้งนี้ การติดตั้ง Firewall ต้องพิจารณาเรื่องดังต่อไปนี้

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

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

12) ต้องใช้เวอร์ชันของซอฟต์แวร์ (Software) Firewall และระบบปฏิบัติการที่เจ้าของผลิตภัณฑ์ยังให้การสนับสนุน

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

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

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

2) การเข้าถึงจากระยะไกลต้องพิสูจน์ตัวตนที่ Firewall หรือผ่านบริการที่อยู่ใน DMZ

3) DNS Servers ต้องไม่อนุญาตให้มีการแลกเปลี่ยนโซน (Zone transfers) เว้นแต่มีเหตุจำเป็น

4.8 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control)

ผู้ดูแลระบบต้องควบคุมการกำหนดเส้นทางบนเครือข่ายเพื่อให้มั่นใจว่าการเชื่อมต่อเครื่องคอมพิวเตอร์และการไหลเวียนของสารสนเทศบนเครือข่าย โดยมีกลไกในการตรวจสอบที่อยู่ปลายทางและต้นทางของการเชื่อมต่อ เช่น การควบคุมโดย Firewall หรือ Proxy เป็นต้น

5. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)

ให้มีการควบคุมการเข้าถึงระบบปฏิบัติการอย่างมั่นคงปลอดภัย การควบคุมการระบุและพิสูจน์ตัวตนของผู้ใช้งาน การควบคุมระบบบริหารจัดการรหัสผ่าน การควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ (System utilities) การควบคุมการหมดเวลาการใช้งานระบบเทคโนโลยีสารสนเทศ และควบคุมการจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ

5.1 ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on procedures)

5.1.1 ผู้ดูแลระบบ ต้องจัดให้มีการควบคุมการเข้าถึงระบบปฏิบัติการอย่างมั่นคงปลอดภัยโดยขั้นตอนการเข้าสู่ระบบต้องเปิดเผยข้อมูลเกี่ยวกับระบบให้น้อยที่สุดเพื่อหลีกเลี่ยงผู้ใช้งานที่ไม่ได้รับอนุญาต ซึ่งขั้นตอนการ Log-on ต้องพิจารณา ดังนี้

1) หากกระบวนการเข้าสู่ระบบไม่สำเร็จ ระบบต้องไม่แสดงข้อมูลของระบบหรือแอปพลิเคชัน (Application) ที่ใช้งานอยู่

2) ระบบต้องแสดงข้อความเตือนผู้ใช้งานว่าสามารถเข้าใช้งานเครื่องคอมพิวเตอร์ได้เฉพาะผู้ที่มีสิทธิ์เท่านั้น

3) หากกระบวนการเข้าสู่ระบบไม่สำเร็จ ระบบต้องไม่แสดงข้อมูลที่สามารถระบุตัวตนของระบบ เช่น เครือข่ายที่ใช้งาน สถานที่ตั้งของระบบ หรือชื่อเครื่องคอมพิวเตอร์แม่ข่าย เป็นต้น

4) ระบบต้องไม่แสดงข้อความที่ชี้เฉพาะเหตุของการเข้าสู่ระบบไม่สำเร็จ เช่น ไม่แสดงข้อความว่าบัญชีผู้ใช้งานผิด หรือ รหัสผ่านผิด เป็นต้น

5) ห้ามเข้าสู่ระบบจากบัญชีผู้ใช้งานส่วนบุคคลเดียวกันมากกว่าหนึ่ง Session ในระบบเดียวกัน

6) ระบบต้องจำกัดจำนวนครั้งในการพยายามเข้าสู่ระบบที่ไม่สำเร็จ และต้องพิจารณาเงื่อนไขต่อไปนี้
   (ก) การเก็บบันทึกผลการเข้าสู่ระบบทั้งที่สำเร็จและไม่สำเร็จ
   (ข) หน่วงระยะเวลาในการเข้าใช้งานระบบครั้งต่อไป
   (ค) การตัดการเชื่อมต่อ
   (ง) การแสดงข้อความเตือนที่หน้าจอของผู้ดูแลระบบเมื่อมีการเข้าสู่ระบบเกินจำนวนครั้งที่จำกัดไว้
7) ระบบต้องแสดงวัน เวลา ในการเข้าสู่ระบบที่สำเร็จในครั้งก่อน พร้อมทั้งบันทึกจำนวนครั้งที่พยายามเข้าไม่สำเร็จนับแต่การเข้าสู่ระบบที่สำเร็จในครั้งก่อนของผู้ใช้งาน
8) ระบบต้องไม่ส่งรหัสผ่านแบบ Clear text ผ่านระบบเครือข่ายสื่อสารข้อมูล
9) ผู้ดูแลระบบต้องกำหนดจำนวนครั้งที่ยอมให้ใส่รหัสผ่านผิดได้ไม่เกิน 5 ครั้ง

5.2 การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication)
ผู้ดูแลระบบ ต้องจัดให้ผู้ใช้งานมีบัญชีผู้ใช้งานของแต่ละบุคคลเพื่อใช้พิสูจน์ตัวตนในการเข้าถึงระบบเทคโนโลยีสารสนเทศ และต้องใช้ระบบเทคโนโลยีสารสนเทศพิสูจน์ตัวตนผู้ใช้งานในการเข้าถึงระบบปฏิบัติการโดยผ่านระบบ Active directory หรือ Lightweight Derectory Access Protocol (LDAP) ทุกครั้ง พร้อมทั้งบันทึกข้อมูลการเข้าถึง

5.3 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities)
ผู้ดูแลระบบ ต้องควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้บนระบบที่ใช้งานจริง (Production system) ดังนี้

5.3.1 ต้องจัดทำบัญชีโปรแกรมประเภทยูทิลิตี้ (System utilities) ที่นำมาใช้งาน
5.3.2 กำหนดความรับผิดชอบในการใช้โปรแกรมประเภทยูทิลิตี้ (System utilities) แต่ละรายการอย่างชัดเจนและสื่อสารให้ผู้เกี่ยวข้องทราบเพื่อถือปฏิบัติ
5.3.3 ให้มีการพิสูจน์ตัวตน และกำหนดสิทธิ์ในการใช้งานโปรแกรมประเภทยูทิลิตี้เฉพาะกลุ่มคนที่มีหน้าที่รับผิดชอบ
5.3.4 มีการบันทึกเหตุการณ์ (Log) การใช้งานโปรแกรมประเภทยูทิลิตี้ และต้องสอบทานจากผู้ดูแลระบบอย่างสม่ำเสมอ
5.3.5 ต้องทำการเพิกถอนหรือระงับโปรแกรมประเภทยูทิลิตี้ที่ไม่จำเป็น

5.4 การหมดเวลาการใช้งานระบบสารสนเทศ (Session time-out)

5.4.1 ผู้ดูแลระบบต้องกำหนด Session time-out ของระบบเทคโนโลยีสารสนเทศที่ไม่มีการใช้งานภายในระยะเวลา 15 นาที ทั้งนี้ ถ้าระบบที่ไม่สามารถตัดการเชื่อมต่อแบบอัตโนมัติได้ กำหนดให้ใช้โปรแกรมพักหน้าจอที่ต้องใส่รหัสผ่านหรือกำหนดให้มีการล็อกหน้าจอ
5.4.2 ผู้ดูแลระบบ และผู้ใช้งาน ต้องตั้งค่าให้มีโปรแกรมพักหน้าจอที่ต้องใส่รหัสผ่านสำหรับเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์แบบพกพา และเครื่องคอมพิวเตอร์แม่ข่าย ทั้งนี้ โปรแกรมพักหน้าจอกำหนดให้ป้อนรหัสผ่านหลังจากที่มีการทิ้งเครื่องดังกล่าวไว้โดยไม่มีการใช้งานเป็นเวลา 15 นาที

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd.

5.5 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)

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

5.5.2 ผู้ใช้งาน หากมีความจำเป็นต้องใช้งานนอกเวลาที่กำหนดต้องขออนุมัติจากผู้บังคับบัญชาเท่านั้น

6. การควบคุมการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ (Application and information access control) ให้มีการจำกัดการเข้าถึงสารสนเทศ และการแยกระบบเทคโนโลยีสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณที่ควบคุมเฉพาะ

6.1 การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)

6.1.1 เจ้าของข้อมูลและผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงแก่ผู้ใช้งานเท่าที่จำเป็นต้องใช้ในการปฏิบัติงาน โดยการให้สิทธิ์ต้องพิจารณาในเรื่องดังต่อไปนี้

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

6.1.2 เจ้าของข้อมูลและผู้ดูแลระบบ ควรกำหนดให้ระบบสารสนเทศรองรับการกำหนดสิทธิ์ในการเข้าถึงแบบกลุ่มได้

6.2 การแยกระบบสารสนเทศที่ไวต่อการรบกวน (Sensitive system isolation) มีผลกระทบต่อคนกลุ่มใหญ่ หรือระบบที่มีความสำคัญต่อหน่วยงาน ต้องดำเนินการดังนี้

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

6.2.2 ผู้ดูแลระบบต้องควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์เคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile computing and teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

6.2.3 เจ้าของข้อมูลที่เป็นเจ้าของระบบสารสนเทศที่มีความสำคัญสูงต้องเป็นผู้อนุญาต ในกรณีที่ระบบสารสนเทศที่มีความสำคัญสูงมีความจำเป็นต้องทำงานร่วมกับระบบสารสนเทศอื่นที่มีความสำคัญน้อยกว่า

7. การควบคุมการปฏิบัติงานจากภายนอก รฟม. (Teleworking)

7.1 ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนการใช้งาน และเชื่อมต่อผ่านช่องทางที่มีความปลอดภัยที่มีเทคโนโลยีเข้ารหัสป้องกัน

7.2 ผู้ดูแลระบบต้องทำการถอดถอนสิทธิ์ในการเข้าถึงของผู้ใช้งานจากภายนอกสำนักงาน เมื่อครบกำหนดระยะเวลาที่ขออนุญาต

7.3 ผู้ใช้งาน หากจำเป็นต้องมีการปฏิบัติงานจากภายนอกสำนักงานของ รฟม. ต้องได้รับการอนุญาตจากผู้บังคับบัญชาอย่างเป็นลายลักษณ์อักษร ในกรณีเร่งด่วนสามารถดำเนินการก่อน โดยแจ้งให้ผู้บังคับบัญชารับทราบด้วย โดยผู้บังคับบัญชาต้องพิจารณาเงื่อนไขในการเตรียมการ ดังต่อไปนี้

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

7.4 ผู้ใช้งานต้องจัดเก็บเอกสารที่เป็นความลับในอุปกรณ์ที่ล็อกได้และมีการควบคุมการเข้าถึง โดยใช้หลักเกณฑ์การรักษาความลับเช่นเดียวกับสารสนเทศที่อยู่ในสำนักงานของ รฟม.

7.5 ผู้ใช้งาน ต้องติดตั้งโปรแกรมป้องกันไวรัสและ Personal firewall สำหรับอุปกรณ์ส่วนตัวที่ใช้เชื่อมต่อเครือข่ายของ รฟม. จากภายนอก

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

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd.

ส่วนที่ 7
การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

วัตถุประสงค์

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

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

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

แนวปฏิบัติ

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

ส่วนที่ 8

การควบคุมหน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) เข้าถึงระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

- เพื่อควบคุมหน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) ที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของ รฟม. ให้เป็นไปอย่างมั่นคงปลอดภัย

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้บังคับบัญชา
- หน่วยงานภายนอก
- ผู้ใช้งาน (บุคคลภายนอก)

อ้างอิงมาตรฐาน

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

แนวปฏิบัติ

1. ผู้ดูแลระบบต้องประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศของ รฟม.
2. การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก)
   2.1 เจ้าของข้อมูลต้องเป็นผู้อนุญาตการให้สิทธิ์แก่หน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) ที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของ รฟม. อย่างเป็นลายลักษณ์อักษร
   2.2 ผู้บังคับบัญชาต้องกำหนดให้มีการลงนามการไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของ รฟม.
   2.3 ผู้บังคับบัญชา ต้องควบคุมให้มีการกำหนดข้อตกลงและความรับผิดชอบที่เกี่ยวข้องกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศลงในสัญญากับผู้ให้บริการภายนอกที่ให้บริการด้านสารสนเทศและบริการด้านการสื่อสาร โดยให้ครอบคลุมรวมถึงผู้รับจ้างช่วง
   2.4 ผู้บังคับบัญชาต้องกำหนดให้จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) ระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศ ซึ่งมีรายละเอียด ดังนี้
      2.4.1 เหตุผลในการขอใช้
      2.4.2 ระยะเวลาในการใช้
      2.4.3 การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย
      2.4.4 การตรวจสอบ MAC address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

2.5 ผู้ดูแลระบบมีสิทธิ์ในการตรวจสอบการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) เพื่อควบคุมการใช้งานได้อย่างมั่นคงปลอดภัยตามสัญญา

2.6 ผู้ดูแลระบบต้องควบคุมให้หน่วยงานภายนอกจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งต้องปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อใช้สำหรับควบคุมหรือตรวจสอบการทำงานและเพื่อให้มั่นใจว่าการปฏิบัติงานเป็นไปตามขอบเขตที่ได้กำหนดไว้

3. ผู้ดูแลระบบต้องแจ้งแนวปฏิบัติต่าง ๆ ที่เกี่ยวข้อง แก่ผู้รับจ้างภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) เพื่อให้ปฏิบัติตาม
4. ผู้ดูแลระบบ ต้องกำกับดูแลหน่วยงานภายนอก หรือผู้ใช้งาน (บุคคลภายนอก) ให้ปฏิบัติตามสัญญาหรือข้อตกลงการให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงด้านความมั่นคงปลอดภัย
5. ผู้ดูแลระบบ ต้องติดตาม ตรวจสอบรายงานหรือบันทึกการให้บริการของหน่วยงานภายนอกหรือบุคคลที่ให้บริการแก่หน่วยงานตามที่ว่าจ้างอย่างสม่ำเสมอตามสัญญาว่าจ้าง
6. ผู้ดูแลระบบ ต้องกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีหน้าที่ในการกำกับดูแลหรือหน่วยงานที่เกี่ยวข้องกับการบังคับใช้กฎหมาย รวมทั้งหน่วยงานที่ควบคุมดูแลสถานการณ์ฉุกเฉินภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน
7. ผู้ดูแลระบบ ต้องมีขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีความเชี่ยวชาญเฉพาะด้านหรือหน่วยงานที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน
8. ผู้ดูแลระบบต้องควบคุมการเปลี่ยนแปลงของหน่วยงานภายนอกที่ส่งผลกระทบต่อการให้บริการขององค์กรและต้องประเมินความเสี่ยงอย่างเหมาะสมเพื่อควบคุมผลกระทบอันเนื่องมาจากการเปลี่ยนแปลงนั้น
9. หน่วยงานภายนอกหรือผู้ใช้งาน (บุคคลภายนอก) ต้องใช้งานทรัพย์สินสารสนเทศของ รฟม. ด้วยความระมัดระวัง และรักษาความลับของ รฟม. ไม่นำไปเปิดเผย และต้องขออนุญาตพร้อมทั้งปฏิบัติตามเงื่อนไขในการเข้าถึงระบบสารสนเทศของ รฟม. ทุกครั้ง

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd.

ส่วนที่ 9
การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ ของ รฟม.

วัตถุประสงค์

- เพื่อควบคุมการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ ที่ รฟม. จัดไว้ให้ใช้อย่างเหมาะสม ทั้งนี้ เพื่อป้องกันการสูญหาย เสียหาย หรือถูกเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

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

แนวปฏิบัติ

1. การใช้งานทั่วไป
   - 1.1 ผู้ดูแลระบบต้องกำหนดบัญชีซอฟต์แวร์มาตรฐาน (Software standard) ที่อนุญาตให้ติดตั้งบนเครื่องคอมพิวเตอร์ของผู้ใช้งาน และปรับปรุงให้เป็นปัจจุบันเสมอ
   - 1.2 ผู้ดูแลระบบต้องเป็นผู้กำหนดการตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) เท่านั้น
   - 1.3 ผู้ใช้งานต้องใช้งานอย่างมีประสิทธิภาพเพื่องานของ รฟม.
   - 1.4 ผู้ใช้งานต้องไม่ติดตั้งโปรแกรมที่ละเมิดลิขสิทธิ์บนเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ของ รฟม.
   - 1.5 ผู้ใช้งานต้องขอนุญาตติดตั้งโปรแกรมในเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ตามขั้นตอนที่ รฟม. กำหนด
   - 1.6 ผู้ใช้งานต้องไม่ติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ของ รฟม. การดำเนินการดังกล่าวต้องดำเนินการโดยผู้ดูแลระบบเท่านั้น
   - 1.7 ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่อย่างละเอียด เพื่อให้สามารถใช้งานอย่างปลอดภัยและมีประสิทธิภาพ
   - 1.8 ผู้ใช้งานต้องไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ และรักษาให้มีสภาพเดิม
   - 1.9 ผู้ใช้งานต้องแจ้งซ่อมเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่เพื่อให้ ฝทท. เป็นผู้ดำเนินการเท่านั้น
   - 1.10 ผู้ใช้งานต้องไม่สร้าง Shortcut ไว้บน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของ รฟม.
   - 1.11 กรณีเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์เคลื่อนที่ ผู้ใช้งานต้องปฏิบัติ ดังนี้
     - 1.11.1 ในกรณีที่มีการใช้งานอุปกรณ์ประเภทพกพาในที่สาธารณะ ห้องประชุม และพื้นที่ภายนอก อื่น ๆ ที่ไม่มีการป้องกัน หรือไม่ได้อยู่ในบริเวณของ รฟม. ให้ป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต เช่น ไม่เปิดการเชื่อมต่อแบบไร้สายโดยไม่มีการเข้ารหัสข้อมูล เป็นต้น

1.11.2 ต้องระมัดระวังการเคลื่อนย้าย โดยต้องใส่กระเป๋าเพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงานหรือหลุดมือ เป็นต้น

1.11.3 ไม่ใส่ในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับหรืออาจถูกจับโยนได้

1.11.4 การใช้งานเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัดต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

1.11.5 หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอย ขีดข่วน หรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

1.11.6 ไม่วางของทับบนหน้าจอและแป้นพิมพ์

1.11.7 การเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

1.11.8 ไม่คลื่อนย้ายเครื่องในขณะที่ Harddisk กำลังทำงาน

1.11.9 ไม่ใช้หรือวางใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่าง ๆ เป็นต้น

1.11.10 ไม่วางใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูง เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น

1.11.11 ไม่ติดตั้งหรือวางในที่ที่มีการสั่นสะเทือน เช่น ในยานพาหนะที่กำลังเคลื่อนที่

1.11.12 การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจำทำให้หน้าจอมีรอยขีดข่วนได้

1.11.13 รับผิดชอบในการป้องกันการสูญหาย เช่น ต้องล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

1.11.14 นำติดตัวไปด้วยเสมอ เช่น ไม่ละทิ้ง อุปกรณ์ประมวลผลประเภทพกพาในรถยนต์ ห้องพักในโรงแรม หรือห้องประชุม เป็นต้น ในกรณีที่มีความจำเป็นต้องละทิ้งให้จัดเก็บไว้ในสถานที่มั่นคงปลอดภัย

1.11.15 ไม่เก็บหรือใช้งานในสถานที่ที่มีความร้อน ความชื้นหรือฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

1.11.16 ไม่เปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub component) ที่ติดตั้งอยู่ภายใน เช่น แบตเตอรี่ หน่วยความจำ

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

3. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malicious code)

3.1 ผู้ดูแลระบบต้องควบคุมการ Update ระบบปฏิบัติการ เว็บเบราว์เซอร์ และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

3.2 ผู้ดูแลระบบต้องติดตั้งและปรับปรุงโปรแกรมป้องกันไวรัสให้ทันสมัยอยู่เสมอ

3.3 ผู้ใช้งานต้องไม่ปิดหรือยกเลิกระบบการป้องกันไวรัสที่ติดตั้งอยู่

3.4 ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อบันทึกต่าง ๆ เช่น Thumb drive และ Data storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์ของ รฟม.

3.5 ผู้ใช้งาน หากพบหรือสงสัยว่าเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ติดชุดคำสั่งไม่พึงประสงค์ ให้รีบยกเลิกเชื่อมต่อเครื่องเข้ากับระบบเครือข่ายสื่อสารข้อมูลเพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่น ๆ ได้ และแจ้ง ฝทท. ทราบทันที

4. การสำรองข้อมูลและการกู้คืน

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

4.2 ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

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

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd.

ส่วนที่ 10
การใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์

วัตถุประสงค์

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

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

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

แนวปฏิบัติ

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

      ในกรณีที่มีความจำเป็นต้องได้รับอนุญาตจากผู้บังคับบัญชา และ ฝทท.
   4) ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่ รฟม. จัดสรรไว้เท่านั้น เช่น Proxy, Firewall เป็นต้น
   5) ผู้ดูแลระบบต้องทดสอบเส้นทางสำหรับการเชื่อมต่ออินเทอร์เน็ตขององค์กรระหว่างเส้นทางที่ใช้งานจริงและเส้นทางสำรองอย่างน้อยปีละ 2 ครั้ง
   6) ผู้ใช้งานต้องไม่เชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นมีความจำเป็นและขออนุญาตจาก ฝทท. เป็นลายลักษณ์อักษรแล้ว
   7) ผู้ใช้งานต้องขออนุญาตติดตั้งซอฟต์แวร์ (Software) ที่ Download จากอินเทอร์เน็ต และการติดตั้งต้องดำเนินการโดยผู้ที่ได้รับมอบหมายจากผู้ดูแลระบบเท่านั้น

2. ผู้ใช้งานต้องไม่มีเจตนาปิดบังหรือบิดเบือนตัวตนเมื่อมีการใช้งานอินเทอร์เน็ต
3. ผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัส พร้อมทั้งต้องปรับปรุง Virus signature ที่เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพาให้มีความทันสมัยอยู่เสมอ ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web browser) และต้องปิดช่องโหว่ของระบบปฏิบัติการที่เว็บเบราว์เซอร์ติดตั้งอยู่
4. ผู้ใช้งานจะต้องตรวจสอบไวรัส (Virus scanning) ก่อนการรับ - ส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ต
5. ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของ รฟม. เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น
6. ผู้ใช้งานจะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของ รฟม.
7. ผู้ใช้งานต้องหลีกเลี่ยงการกระทำที่สิ้นเปลืองทรัพยากรของเครือข่ายอินเทอร์เน็ต ดังนี้
   (ก) ส่งจดหมายอิเล็กทรอนิกส์ที่มีขนาดใหญ่หรือจดหมายอิเล็กทรอนิกส์ลูกโซ่
   (ข) ใช้เวลาในการเข้าถึงอินเทอร์เน็ตเกินความจำเป็น
   (ค) เล่นเกม Online
   (ง) เข้าห้องพูดคุย Online
8. ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับ รฟม.
9. ผู้ใช้งานต้องไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของ รฟม.
10. ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต
11. ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ที่จะทำให้ผู้อื่นเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย
12. ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน
13. ผู้ใช้งานต้องคำนึงว่าข้อมูลจากอินเทอร์เน็ตอาจไม่มีความทันสมัยหรือไม่มีความถูกต้อง ผู้ใช้งานต้องตรวจสอบความถูกต้องของข้อมูลจากแหล่งที่น่าเชื่อถือก่อนที่จะเผยแพร่ข้อมูลดังกล่าว
14. ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา
15. ผู้ใช้งานต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้ายในการเสนอความคิดเห็นที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของ รฟม. การทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น ๆ
16. ผู้ใช้งานต้องไม่บันทึกรหัสผ่านใน Web browser (Remember password) เพื่อป้องกันบุคคลอื่นที่สามารถเข้าถึงคอมพิวเตอร์ของผู้ใช้งานนำรหัสผ่านดังกล่าวไปใช้งานในอินเทอร์เน็ตโดยไม่ได้รับอนุญาต

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd.

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

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd.

19.10 ผู้ใช้งานต้องตระหนักไว้เสมอว่าข้อมูลต่าง ๆ ที่ผู้ใช้งานเผยแพร่ไว้บนบริการสื่อสังคมออนไลน์นั้นคงอยู่ถาวรและผู้อื่นอาจเข้าถึงและเผยแพร่ข้อมูลเหล่านั้นได้

19.11 ผู้ใช้งานต้องมีข้อพิจารณาในการรับเพื่อนเข้ากลุ่มที่ชัดเจน และควรประกาศข้อความปฏิเสธความรับผิดชอบที่เกี่ยวกับเนื้อหาหรือข้อความแสดงความคิดเห็นซึ่งถูกโพสต์จากเพื่อนในกลุ่มที่อาจปรากฏในเว็บไซต์ประเภท Social network ของผู้ใช้งานเอง

19.12 ผู้ใช้งานต้องติดตั้งซอฟต์แวร์ป้องกันไวรัส และอัปเดตฐานข้อมูลไวรัสของโปรแกรมอยู่เสมอ และต้องหลีกเลี่ยงการใช้โปรแกรมที่ละเมิดลิขสิทธิ์เพราะอาจจะมีโปรแกรมประสงค์ร้ายแฝงตัวอยู่ภายในเพื่อลักลอบ ปลอมแปลง หรือขโมยข้อมูลสำคัญของผู้ใช้งานได้

19.13 ผู้ใช้งานต้องระมัดระวังการใช้ถ้อยคำและภาษาที่อาจเป็นการดูหมิ่น ยุยง ท้าทาย หรือเป็นการละเมิดต่อบุคคลอื่น กรณีบุคคลอื่นมีความคิดเห็นที่แตกต่างพึงงดเว้นการโต้ตอบด้วยถ้อยคำรุนแรง

19.14 ผู้ใช้งานต้องระมัดระวังกระบวนการหาข่าว หรือภาพจากสื่อสังคมออนไลน์ โดยมีการตรวจสอบอย่างถี่ถ้วนรอบด้านและต้องอ้างอิงแหล่งที่มาเมื่อนำเสนอ เว้นแต่สามารถตรวจสอบและอ้างอิงจากแหล่งข่าวได้โดยตรง

19.15 หากผู้ใช้งานต้องการใช้สื่อสังคมออนไลน์เป็นเครื่องมือในการรายงานข่าวในนามของบุคคลธรรมดาต้องแสดงให้ชัดเจนว่า ข้อความใดเป็น "ข่าว" ข้อความใดเป็น "ความคิดเห็นส่วนตัว"

19.16 การส่งต่อหรือเผยแพร่ข้อมูลในสื่อสังคมออนไลน์ (Social media)

19.16.1 ผู้ใช้งานต้องไม่ส่งต่อหรือเผยแพร่ข้อมูลที่เป็นเท็จ ข่าวลือ ข่าวไม่ปรากฏที่มา เป็นเพียงการคาดเดา หรือส่งผลเสียหายกับบุคคล สังคม หรือ รฟม.

19.16.2 ผู้ใช้งานต้องไม่ส่งต่อหรือเผยแพร่ข้อมูลเรื่องบุคคลเสียชีวิต เด็กและเยาวชน ผู้สูญหาย ผู้ต้องหา เว้นเสียแต่ตรวจสอบข้อเท็จจริงแล้วและเห็นว่าเป็นประโยชน์ต่อสาธารณะ

19.16.3 ผู้ใช้งานต้องไม่ส่งต่อหรือเผยแพร่ข้อมูลที่กระทบต่อสิทธิความเป็นส่วนตัว และศักดิ์ศรีความเป็นมนุษย์

19.17 ผู้ใช้งานต้องตั้งค่าความปลอดภัยของการใช้งานสื่อสังคมออนไลน์ และระมัดระวังการถูกนำข้อมูลจากชื่อบัญชีไปใช้โดยไม่เหมาะสม ผิดวัตถุประสงค์ และลักษณะการแอบอ้างโดยบุคคลอื่น

20. ผู้ใช้งานต้องใช้งานอินเทอร์เน็ตและสื่อสังคมออนไลน์โดยตระหนักถึงพระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่บังคับใช้อยู่เสมอ

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd

ส่วนที่ 11
การใช้งานจดหมายอิเล็กทรอนิกส์

วัตถุประสงค์

- เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ของ รฟม. ให้มีความปลอดภัยและมีประสิทธิภาพ

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

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

แนวปฏิบัติ

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

ส่วนที่ 12
การสำรองข้อมูลและการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

วัตถุประสงค์

- เพื่อให้มีข้อมูลสำรองไว้ใช้งานในกรณีที่ข้อมูลหลักเกิดความเสียหายไม่สามารถใช้งานหรือเข้าถึงได้ หรือเมื่อเกิดภาวะฉุกเฉินต่าง ๆ
- เพื่อให้มีการปฏิบัติที่สอดคล้องกับกฎหมาย พระราชบัญญัติ หรือข้อบังคับภายนอกอื่น ๆ

ผู้รับผิดชอบ

- ผู้บังคับบัญชา
- ผู้ดูแลระบบ
- เจ้าของข้อมูล
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

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

แนวปฏิบัติ

1. การสำรองข้อมูลระบบแม่ข่าย

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

   1.1 ผู้บังคับบัญชากำหนดผู้รับผิดชอบในการสำรองข้อมูล

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

   1.3 ผู้ดูแลระบบต้องสำรองข้อมูลตามความถี่ที่กำหนดไว้ ทั้งนี้ หากเป็นข้อมูลที่สนับสนุนกระบวนการทำงานที่สำคัญของ รฟม. ให้สำรองตามความถี่ที่ รฟม. กำหนด

   1.4 ผู้ดูแลระบบต้องตรวจสอบว่าการสำรองข้อมูลสำเร็จครบถ้วนหรือไม่ หากไม่สำเร็จให้หาสาเหตุและดำเนินการแก้ไขอีกครั้งหนึ่ง

   1.5 ผู้ดูแลระบบต้องนำข้อมูลที่สำรองไว้ไปเก็บไว้ทั้งภายในและนอก รฟม. อย่างน้อยอย่างละ 1 ชุด

   1.6 ผู้ดูแลระบบทดสอบกู้คืนข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าข้อมูลที่สำรองไว้มีความถูกต้อง ครบถ้วน และพร้อมใช้งาน

2. การสำรองข้อมูลคอมพิวเตอร์ส่วนบุคคล

ผู้ใช้งานจะต้องสำรองข้อมูลสำคัญที่เก็บรักษาไว้ในเครื่องคอมพิวเตอร์ส่วนบุคคลหรือคอมพิวเตอร์ หรืออุปกรณ์พกพาอื่น ๆ อย่างสม่ำเสมอ ความถี่ในการสำรองข้อมูลขึ้นอยู่กับความถี่ของการเปลี่ยนแปลงของข้อมูลและระดับความสำคัญของข้อมูลหากเกิดการสูญหาย

3. การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์

เพื่อให้สามารถระบุตัวบุคคลผู้ใช้งานได้อย่างถูกต้อง ผู้ดูแลระบบต้องดำเนินการดังนี้

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

3.2 เก็บรักษาข้อมูลจราจรคอมพิวเตอร์ในสื่อที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง มีการเก็บรักษาความลับของข้อมูลตามระดับชั้นความลับในการเข้าถึงตามที่ รฟม. กำหนด โดยระบุตัวบุคคลที่สามารถเข้าถึงสื่อดังกล่าวได้

3.3 ประเภทของสารสนเทศที่เก็บรักษา แสดงตามตาราง

ประเภทของสารสนเทศ	กฎหมายที่เกี่ยวข้อง	ระยะเวลาการจัดเก็บรักษา (ปี)
Authentication server logs (RADIUS, TACACS)	1) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 2) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 3) ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564	1
Email server logs		1
Web application server logs		1
NTP server logs		1
DHCP server logs		1
IPS logs		1
Firewalls logs		1
Routers & Switches logs		1
Active directory logs		1

4. การจัดเก็บบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and monitoring)
   4.1 ผู้ดูแลระบบต้องมีการจัดเก็บบันทึกเหตุการณ์ (Event logs) การใช้งานระบบสารสนเทศ
   4.2 ผู้ดูแลระบบต้องเก็บบันทึกข้อมูล Audit log ซึ่งบันทึกกิจกรรมการใช้งานของผู้ใช้งานระบบสารสนเทศและเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยต่าง ๆ เพื่อประโยชน์ในการสืบสวน สอบสวน และเพื่อการติดตามการควบคุมการเข้าถึง
   4.3 ผู้ดูแลระบบต้องมีการตรวจสอบข้อมูลบันทึกเหตุการณ์อย่างสม่ำเสมอ (Log review)
   4.4 ผู้ดูแลระบบต้องไม่ลบข้อมูลล็อก (Log) หรือปิดการใช้งานการบันทึกข้อมูลล็อก (Log)
   4.5 ผู้ดูแลระบบต้องป้องกันระบบสารสนเทศที่จัดเก็บล็อก (Log) และข้อมูลล็อก (Log) เพื่อป้องกันการเข้าถึงหรือแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต
5. การเตรียมความพร้อมกรณีฉุกเฉิน

   เพื่อให้มีการบริหารจัดการความต่อเนื่องให้กับกระบวนการทางธุรกิจที่สำคัญขององค์กร เมื่อมีเหตุการณ์ที่ทำให้เกิดการหยุดชะงักหรือติดขัดต่อกระบวนการดังกล่าว โดยมีแนวปฏิบัติ ดังนี้
   5.1 ผู้ดูแลระบบต้องกำหนดระบบที่มีความสำคัญทั้งหมดขององค์กร และจัดทำเป็นบัญชีรายชื่อระบบดังกล่าวรวมทั้งปรับปรุงรายชื่อระบบสำคัญและบัญชีฯ ตามความเป็นจริง
   5.2 เจ้าของข้อมูลและผู้ดูแลระบบประเมินความเสี่ยงสำหรับระบบเหล่านั้น กำหนดมาตรการเพื่อลดความเสี่ยงที่พบและจัดทำรายงานการประเมินความเสี่ยง
   5.3 ผู้ดูแลระบบจัดทำและปรับปรุงแผนกู้คืนระบบอย่างน้อยปีละ 1 ครั้ง
   5.4 เจ้าของข้อมูลและผู้ดูแลระบบต้องทดสอบแผนกู้คืนระบบอย่างน้อยปีละ 1 ครั้ง บันทึกผลการทดสอบรวมถึงปัญหาที่พบ และนำเสนอผลการทดสอบและแนวทางแก้ไขต่อผู้บังคับบัญชา
   5.5 ผู้ดูแลระบบต้องจัดประชุมและชี้แจงให้ผู้ที่เกี่ยวข้องทั้งหมดได้รับทราบเกี่ยวกับแผนและผลของการฝึกซ้อมการกู้คืนระบบ

ส่วนที่ 13
การตรวจสอบและประเมินความเสี่ยง

วัตถุประสงค์

- เพื่อให้มีการตรวจสอบการดำเนินงานของระบบจัดการความมั่นคงปลอดภัยสารสนเทศ และปรับปรุงอย่างต่อเนื่อง
- เพื่อควบคุม และติดตามการปฏิบัติงานของผู้ดูแลระบบสารสนเทศ ให้สอดคล้องตามข้อกำหนด กฎหมาย หรือระเบียบข้อบังคับที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ
- เพื่อประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของสารสนเทศและบริหารจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

ผู้รับผิดชอบ

- ผู้บังคับบัญชา
- ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

- ข้อกำหนดหลัก: การวางแผน (Planning)
- ข้อกำหนดหลัก: การตรวจประเมินภายใน (Internal Audit)
- หมวดที่ 8 ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations security)
- หมวดที่ 14 ความสอดคล้อง (Compliance)

แนวปฏิบัติ

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

7. ผู้ดูแลระบบ ต้องติดตามผลการใช้งานทรัพยากรสารสนเทศ (Capacity) และวางแผนด้านทรัพยากรสารสนเทศให้รองรับการปฏิบัติงานในอนาคตอย่างเหมาะสม
8. ผู้ดูแลระบบ ต้องป้องกันการเข้าใช้งานเครื่องมือที่ใช้เพื่อการตรวจสอบ เพื่อมิให้เกิดการใช้งานผิดประเภทหรือถูกละเมิดการใช้งาน (Compromise) โดยควบคุมการเข้าถึง และตรวจสอบการนำเครื่องมือไปใช้งานอย่างสม่ำเสมอ
9. ผู้ดูแลระบบต้องประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
10. ผู้บังคับบัญชาต้องติดตามผลการดำเนินการตามแผนบริหารจัดการความเสี่ยง (Risk treatment plan) เป็นประจำทุกไตรมาส
11. ผู้ดูแลระบบต้องประเมินความเสี่ยงแล้วจัดลำดับความสำคัญของความเสี่ยงนั้นและค้นหาวิธีการเพื่อลดความเสี่ยงตามขั้นตอนที่ รฟม. กำหนด พร้อมทั้งพิจารณาข้อดีข้อเสียของวิธีการเหล่านั้นเพื่อให้ผู้บริหารของ รฟม. ตัดสินใจเลือกวิธีการเพื่อลดความเสี่ยงหรือยอมรับความเสี่ยง เมื่อเลือกวิธีการลดความเสี่ยงแล้วผู้บริหารต้องจัดสรรทรัพยากรอย่างเพียงพอเพื่อดำเนินการ แนวทางการลดความเสี่ยง แบ่งได้เป็น 3 รูปแบบ ได้แก่
    11.1 การเลือกใช้เทคโนโลยี เพื่อใช้ในการลดความเสี่ยงและเพิ่มความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รฟม. เป็นวิธีที่จำเป็นต้องใช้งบประมาณและทรัพยากรอย่างเพียงพอในการดำเนินการ เช่น การเลือกใช้อุปกรณ์ Firewall มากกว่าหนึ่งผลิตภัณฑ์ในการป้องกันการเข้าถึงเครือข่ายที่สำคัญ การใช้อุปกรณ์สมาร์ทการ์ด หรือ USB Token ในการตรวจสอบยืนยันตัวตนในการเข้าใช้งานระบบจากภายนอก รฟม. เป็นต้น
    11.2 การปรับเปลี่ยนขั้นตอนปฏิบัติ ต้องออกแบบขั้นตอนปฏิบัติใหม่ที่รัดกุมและสามารถรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รฟม. ได้ดีขึ้น เมื่อออกแบบขั้นตอนปฏิบัติใหม่แล้วต้องมีการพิจารณาหารือความเหมาะสม ความเป็นไปได้ และผู้บริหารต้องเป็นผู้อนุมัติให้มีการบังคับใช้ขั้นตอนปฏิบัติใหม่นั้น
    11.3 ผู้ดูแลระบบต้องแจ้งขั้นตอนปฏิบัติให้ผู้เกี่ยวข้องรับรู้อย่างทั่วถึง รวมทั้งต้องจัดฝึกอบรมผู้ใช้งานที่เกี่ยวข้องเพื่อให้สามารถปฏิบัติตามขั้นตอนปฏิบัติใหม่ได้อย่างราบรื่นและมีประสิทธิภาพ
12. การตรวจสอบความปลอดภัยของระบบสารสนเทศ
    12.1 ผู้ดูแลระบบ ต้องวางแผนการตรวจสอบและประเมินช่องโหว่หรือจุดอ่อนด้านความมั่นคงปลอดภัยสารสนเทศ และแจ้งผู้ที่เกี่ยวข้องเพื่อแก้ไขในกรณีที่พบว่าช่องโหว่หรือจุดอ่อนนั้นอาจเป็นเหตุการณ์ด้านความมั่นคงปลอดภัย อย่างน้อยปีละ 1 ครั้ง
    12.2 ผู้ดูแลระบบต้องตรวจสอบระบบสารสนเทศที่จะต้องมีการปรับปรุงเมื่อมีเวอร์ชันใหม่ (Patch) รวมทั้งข้อมูลที่เกี่ยวข้องกับช่องโหว่ด้านเทคนิคอย่างสม่ำเสมอเพื่อให้ทราบถึงภัยคุกคามและความเสี่ยง รวมถึงหาวิธีป้องกันและแก้ไขที่เหมาะสมกับช่องโหว่นั้น
    12.3 ผู้ใช้งาน ผู้ดูแลระบบ และหน่วยงานภายนอก ต้องบันทึกและรายงานช่องโหว่หรือจุดอ่อนใด ๆ ด้านความมั่นคงปลอดภัยสารสนเทศ ที่อาจสังเกตพบระหว่างการติดตามการใช้งานระบบสารสนเทศ ผ่านช่องทางบริหารจัดการที่กำหนดไว้อย่างเหมาะสม และต้องดำเนินการปิดช่องโหว่ที่มีการตรวจพบหรือได้รับแจ้ง
13. ผู้ดูแลระบบต้องมีการบริหารจัดการการเปลี่ยนแปลงเกี่ยวกับการจัดเตรียมการให้บริการ การดูแลปรับปรุงนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ขั้นตอนปฏิบัติงาน หรือการควบคุมเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ โดยคำนึงถึงระดับความสำคัญของการดำเนินธุรกิจที่เกี่ยวข้องและการประเมินความเสี่ยงอย่างต่อเนื่อง

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd.

ส่วนที่ 14
การถ่ายโอน และแลกเปลี่ยนข้อมูลสารสนเทศ

วัตถุประสงค์

- เพื่อให้มีการควบคุมการถ่ายโอนและแลกเปลี่ยนข้อมูลสารสนเทศ ป้องกันการรั่วไหล หรือมีการแก้ไขข้อมูลโดยที่ไม่ได้รับอนุญาต รวมถึงการป้องกันสื่อบันทึกข้อมูลให้มีความปลอดภัยเป็นไปตามข้อกำหนด

ผู้รับผิดชอบ

- ผู้บังคับบัญชา
- เจ้าของข้อมูล
- ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

- หมวดที่ 9 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)

แนวปฏิบัติ

1. ผู้บังคับบัญชา ต้องควบคุมให้มีการจัดทำนโยบาย และขั้นตอนการปฏิบัติเพื่อป้องกันข้อมูลสารสนเทศที่มีการสื่อสาร หรือแลกเปลี่ยนผ่านระบบสารสนเทศให้เหมาะสมตามระดับชั้นความลับข้อมูลสารสนเทศตามขั้นตอนที่ รฟม. กำหนด
2. ผู้บังคับบัญชา และเจ้าของข้อมูล ต้องควบคุมให้มีการจัดทำข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศระหว่างองค์กรกับบุคคลหรือหน่วยงานภายนอก
3. ผู้ดูแลระบบ ต้องมีการป้องกันข้อมูลสารสนเทศที่มีการสื่อสารกันผ่านข้อมูลอิเล็กทรอนิกส์ (Electronic messaging) เช่น จดหมายอิเล็กทรอนิกส์ (E-mail) หรือ Instant messaging ด้วยวิธีการหรือมาตรการที่เหมาะสม
4. ผู้ดูแลระบบ ต้องป้องกันข้อมูลสารสนเทศที่มีการแลกเปลี่ยนในการทำพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce) ผ่านเครือข่ายคอมพิวเตอร์สาธารณะ เพื่อมิให้มีการฉ้อโกง ละเมิดสัญญา หรือมีการรั่วไหลหรือข้อมูลสารสนเทศถูกแก้ไขโดยมิได้รับอนุญาต
5. ผู้ดูแลระบบ ต้องป้องกันข้อมูลสารสนเทศที่มีการสื่อสาร หรือแลกเปลี่ยนในการทำธุรกรรมทางออนไลน์ (Online transaction) เพื่อมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ ส่งข้อมูลไปผิดที่ การรั่วไหลของข้อมูล ข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ หรือถูกส่งซ้ำโดยมิได้รับอนุญาต
6. ผู้ดูแลระบบ ต้องควบคุมการรับส่งข้อมูลสารสนเทศเพื่อป้องกันความผิดพลาด ดังนี้
   - 6.1 ความไม่สมบูรณ์ของข้อมูลสารสนเทศที่รับ-ส่ง
   - 6.2 การส่งข้อมูลสารสนเทศผิดจุดหมายปลายทาง
   - 6.3 การเปลี่ยนแปลงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต
   - 6.4 การเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต
   - 6.5 การเข้าถึงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต
   - 6.6 การนำข้อมูลสารสนเทศกลับมาใช้ใหม่โดยไม่ได้รับอนุญาต
7. เจ้าของข้อมูล และผู้ดูแลระบบ ต้องมีการป้องกันข้อมูลสารสนเทศที่มีการเผยแพร่ต่อสาธารณชนมิให้มีการแก้ไขเปลี่ยนแปลงโดยมิได้รับอนุญาต เพื่อรักษาความถูกต้องครบถ้วนของข้อมูลสารสนเทศ

ส่วนที่ 15
การควบคุมการเข้ารหัส

วัตถุประสงค์

- เพื่อให้มีการเข้ารหัสข้อมูลอย่างเหมาะสมและมีประสิทธิผลในการปกป้องความลับ ป้องกัน การปลอมแปลงข้อมูล และควบคุมความถูกต้องของข้อมูล

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- เจ้าของข้อมูล
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 6 การเข้ารหัสข้อมูล (Cryptography)

แนวปฏิบัติ

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

ประเภทกุญแจ / วิธีการเข้ารหัส	เกณฑ์ขั้นต่ำ	ความยาวกุญแจ (อย่างน้อย)
กุญแจแบบสมมาตร (Symmetric)	AES	256 bits
กุญแจแบบอสมมาตร (Asymmetric)	RSA	1024 bits
การ Hashing	SHA-256	256 bits

4. ผู้ดูแลระบบ ต้องมีการทบทวนขั้นตอนวิธี (Algorithm) และความยาวของกุญแจที่เข้ารหัสอย่างน้อยปีละ 1 ครั้ง เพื่อให้ยังสามารถรักษาไว้ซึ่งความมั่นคงปลอดภัย
5. ผู้ดูแลระบบ ต้องกำหนดให้มีการบริหารจัดการกุญแจที่ใช้ในการเข้ารหัส ดังนี้
   5.1 การสร้างกุญแจรหัสควรกระทำในสถานที่ที่มีมาตรการป้องกันความปลอดภัย
   5.2 เมื่อมีการสร้างกุญแจรหัสที่เป็นกุญแจลับ (Private key) ควรส่งมอบให้กับเจ้าของกุญแจโดยตรงโดยวิธีการที่ปลอดภัย
   5.3 ควรจัดให้มีการเก็บบันทึก Log เพื่อการตรวจสอบสำหรับกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับการจัดการกุญแจรหัส

6. ผู้ใช้งาน ควรรักษาความปลอดภัยในการใช้งานกุญแจ ดังนี้

6.1 เก็บกุญแจรหัสในสถานที่ที่ปลอดภัย เช่น ตู้นิรภัย หรือสื่อบันทึกที่ปลอดภัย และไม่มีใครสามารถเข้าถึงได้

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

6.3 ควบคุมการใช้งานและจัดเก็บกุญแจให้สอดคล้องกับการรักษาความลับข้อมูลตามที่ รฟม. กำหนด

ส่วนที่ 16
การนำอุปกรณ์ส่วนตัวมาใช้งาน (Bring your own device)

วัตถุประสงค์

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

ผู้รับผิดชอบ

- ผู้ดูแลระบบ
- ผู้ใช้งาน

อ้างอิงมาตรฐาน

- หมวดที่ 2 อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากระยะไกล (Mobile devices and teleworking)

แนวปฏิบัติ

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

ภาคผนวก ฉ.

สัญญาการเก็บรักษาข้อมูลไว้เป็นความลับ (Non-Disclosure Agreement)

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd.

สัญญาการเก็บรักษาข้อมูลไว้เป็นความลับ

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

การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย สำนักงานตั้งอยู่เลขที่ 175 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร โดย ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ ซึ่งต่อไปในสัญญานี้เรียกว่า "รฟม." ฝ่ายหนึ่ง กับ

นาย/นาง/นางสาว/..... เลขที่บัตรประชาชน..... ซึ่งต่อไปในสัญญานี้เรียกว่า "ผู้รับข้อมูล" อีกฝ่ายหนึ่ง

ตามที่..... ได้ตกลงทำสัญญาเลขที่..... เมื่อวันที่..... กับ รฟม. ซึ่งต่อไปในสัญญานี้เรียกว่า "สัญญาโครงการ" โดย..... จะได้รับข้อมูลจาก รฟม. เพื่อใช้ในการปฏิบัติงาน ซึ่งในการดำเนินงานดังกล่าวได้มอบหมายให้ผู้รับข้อมูลประสานขอข้อมูลจาก รฟม. เพื่อนำไปประกอบการปฏิบัติงานที่เกี่ยวข้องสำหรับการดำเนินโครงการ .....นั้น

ทั้งสองฝ่ายจึงตกลงทำสัญญากัน ดังมีข้อความต่อไปนี้

1. ในสัญญาฉบับนี้ "ข้อมูล" หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริง ข้อมูล หรือสิ่งใด ๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพสิ่งของนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

2. ผู้รับข้อมูลให้สัญญาแก่ รฟม. ว่าข้อมูลที่ได้รับจาก รฟม. หรือในนามของ รฟม. ผู้รับข้อมูล จะใช้เพื่อประกอบการปฏิบัติงานที่เกี่ยวข้องสำหรับดำเนินโครงการ โครงการเช่าเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ ตามสัญญาโครงการเท่านั้น และจะไม่นำไปใช้เพื่อวัตถุประสงค์อื่น เช่น ใช้เพื่อวัตถุประสงค์ในเชิงพาณิชย์ การพัฒนาเป็นผลิตภัณฑ์หรือเทคโนโลยีอื่น การใช้หรือพยายามใช้ข้อมูลเพื่อการอื่น การอ้างอิงหรือรวมเข้าไปเป็นส่วนหนึ่งของการประดิษฐ์ใด ๆ การรับขอความคุ้มครองจากทรัพย์สินทางปัญญาใด ๆ ของผู้รับข้อมูล เว้นแต่ได้รับการอนุญาตจาก รฟม. เป็นลายลักษณ์อักษรก่อน

/3. ผู้รับข้อมูล ...

3. ผู้รับข้อมูลจะต้องปกปิดข้อมูลทั้งหมดที่ได้มีการเปิดเผยภายใต้สัญญาโครงการนี้ไว้เป็นความลับอย่างเคร่งครัด

4. ถ้าข้อกำหนดใด ๆ ตามสัญญาฉบับนี้ตกเป็นโมฆะ ให้ข้อสัญญาที่เหลืออยู่ในสัญญาฉบับนี้คงใช้บังคับและมีผลอยู่อย่างสมบูรณ์

5. หากผู้รับข้อมูลไม่ปฏิบัติตามกฎหมาย หรือฝ่าฝืนสัญญานี้ไม่ว่าข้อใดข้อหนึ่ง ผู้รับข้อมูลยินยอมชดใช้ค่าเสียหายใด ๆ ที่เกิดขึ้นหรือที่เกี่ยวเนื่องแก่ รฟม. ทั้งสิ้น

สัญญาฉบับนี้ทำขึ้นเป็นสองฉบับมีข้อความถูกต้องตรงกัน คู่สัญญาได้อ่านและเข้าใจข้อความในสัญญานี้แล้ว เห็นว่าถูกต้องตรงตามเจตนาของตน จึงได้ลงนามและประทับตรา (ถ้ามี) ไว้ต่อหน้าพยานและยึดถือไว้ฝ่ายละหนึ่งฉบับ

การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย

ลงชื่อ .....
(.....)
ตำแหน่ง ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ
วันที่..... /..... /.....

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

ลงชื่อ ..... พยาน
(.....)
ตำแหน่ง พนักงานบริหารระบบคอมพิวเตอร์ 7
วันที่..... /..... /.....

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

บริษัท เคียวเซร่า ด็อคคิวเม้นท์ โซลูชั่นส์ (ประเทศไทย) จำกัด
KYOCERA
KYOCERA Document Solutions (Thailand) Corp., Ltd