ขอบเขตของงาน (Terms of Reference: TOR)
โครงการเพิ่มประสิทธิภาพการรักษาความมั่นคงปลอดภัยของข้อมูลและป้องกันภัยทางไซเบอร์ ระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ใหม่ สำนักงานปลัดกระทรวงการคลัง แขวงพญาไท เขตพญาไท กรุงเทพมหานคร

๑. ความเป็นมา

สำนักงานปลัดกระทรวงการคลัง ได้จัดทำโครงการพัฒนาระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ใหม่ (New GFMIS Thai) โดยใช้เทคโนโลยีแบบระบบเปิด (Open System) เพื่อพัฒนาระบบให้มีประสิทธิภาพ มีความยืดหยุ่น ครอบคลุมการเบิกจ่ายเงินทั่วประเทศ และรองรับการขยายตัวในอนาคต โดยเริ่มใช้งานเมื่อวันที่ ๔ เมษายน ๒๕๖๕ ภายหลังมีการประเมินความเสี่ยงและประเมินผลการใช้งาน พบว่ามีความจำเป็นต้องปรับปรุงประสิทธิภาพในหลายส่วน ได้แก่ การรักษาความมั่นคงปลอดภัยข้อมูลสำหรับระบบทดสอบ (Dev/QA) ปัจจุบันข้อมูลที่ใช้สำหรับการพัฒนาซอฟต์แวร์ด้านการทดสอบและประกันคุณภาพระบบเป็นการสำเนาข้อมูลจากระบบงานจริงมาเพื่อใช้ในการทดสอบ ซึ่งข้อมูลดังกล่าวมีข้อมูลส่วนบุคคล (Personal Identifiable Information: PII) เป็นส่วนหนึ่งของข้อมูลที่ต้องดำเนินการทดสอบและมีการปกปิดข้อมูลแบบ Manual ซึ่งทำได้บางส่วน ไม่สามารถทำได้สำหรับปริมาณข้อมูลจำนวนมาก โดยยังไม่มีการปกปิดข้อมูล (Data Masking) เหล่านั้นอย่างเป็นรูปธรรม ซึ่งการป้องกันข้อมูลส่วนบุคคลเป็นกฎหมายและข้อบังคับที่ต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และเพื่อให้เป็นไปมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๒๒ รวมทั้งเป็นการดำเนินการตามข้อสังเกต/ข้อเสนอแนะ ของสำนักงานการตรวจเงินแผ่นดิน (สตง.) การจัดการข้อมูลระบบสารสนเทศเพื่อการบริหาร (MIS) ปัจจุบันระบบฐานข้อมูลสำหรับระบบสารสนเทศเพื่อการบริหาร (MIS) มีปริมาณข้อมูลขนาดใหญ่มากขึ้นทำให้ประสิทธิภาพในการสืบค้นข้อมูลลดลง เนื่องจากเมื่อระบบต้องประมวลผลข้อมูลในฐานข้อมูลทั้งหมด อาจทำให้ระบบตอบสนองช้าลง โดยเฉพาะเมื่อมีการสืบค้นข้อมูลเฉพาะบางช่วงเวลา รวมถึงข้อจำกัดด้านความซับซ้อนในการจัดการข้อมูล เช่น การลบข้อมูลเก่าหรือการสำรองข้อมูล จะต้องดำเนินการทั้งฐานข้อมูลทำให้ใช้เวลาและใช้ทรัพยากรมากขึ้น โดยส่งผลกระทบโดยตรงต่อผู้ใช้งานระบบ MIS จำนวนมากกว่า ๒๔,๕๖๒ หน่วยเบิกจ่าย การเพิ่มประสิทธิภาพการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของระบบเครือข่ายและเว็บแอพพลิเคชัน ปัจจุบันการรักษาความปลอดภัยเครือข่ายมีการแบ่งโซน (Network Segmentation) โดยใช้อุปกรณ์ป้องกันเครือข่ายหลัก (Firewall) มาทำอุปกรณ์ป้องกันเครือข่ายเสมือน (Virtual Firewall) สำหรับป้องกันระบบเครือข่ายอินเทอร์เน็ต ด้วยปริมาณการเข้าถึงระบบผ่านช่องทางอินเทอร์เน็ตมีมากขึ้น ส่งผลให้ประสิทธิภาพของอุปกรณ์ป้องกันเครือข่ายหลักลดลง เนื่องจากมีการประมวลผลมากขึ้น สำหรับอุปกรณ์ป้องกันเว็บแอพพลิเคชัน (WAF) เดิมที่มีอยู่ มีข้อจำกัดในเรื่องประสิทธิภาพและการจัดเก็บการจราจรข้อมูล (Log) ที่มีปริมาณจำกัด ส่งผลให้ประสิทธิภาพในการรักษาความมั่นคงปลอดภัยเครือข่ายและแอพพลิเคชันลดลงและไม่สามารถรองรับอัตราการเติบโตของการใช้งานได้อย่างเพียงพอและเหมาะสม ซึ่งเป็นความเสี่ยงในช่วงปิดปีงบประมาณที่มีปริมาณการใช้งานเป็นจำนวนมาก อาจทำให้ไม่สามารถให้บริการระบบได้อย่างต่อเนื่อง

๒. วัตถุประสงค์

๒.๑ เพื่อจัดหาเครื่องคอมพิวเตอร์และอุปกรณ์สำหรับเพิ่มประสิทธิภาพการให้บริการระบบและป้องกันภัยทางไซเบอร์ระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ใหม่ (New GFMIS Thai)

๒.๒ เพื่อเพิ่มประสิทธิภาพการรักษาความมั่นคงปลอดภัยข้อมูลสำหรับระบบทดสอบและการจัดการฐานข้อมูลของระบบสารสนเทศเพื่อการบริหาร (MIS)

๒.๓ เพื่อเพิ่มประสิทธิภาพการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของระบบเครือข่ายและเว็บแอพพลิเคชัน

๓. เป้าหมาย

ระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ใหม่ มีการรักษาความมั่นคงปลอดภัยของข้อมูลสำหรับระบบทดสอบ (Dev/QA) และมีการจัดการฐานข้อมูลระบบสารสนเทศเพื่อการบริหาร (MIS) อย่างมีประสิทธิภาพ รวมทั้งมีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของระบบเครือข่ายและเว็บแอพพลิเคชันที่มีประสิทธิภาพ เป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และตามมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๒๒

๔. คุณสมบัติของผู้ยื่นข้อเสนอ

๔.๑ มีความสามารถตามกฎหมาย

๔.๒ ไม่เป็นบุคคลล้มละลาย

๔.๓ ไม่อยู่ระหว่างเลิกกิจการ

๔.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๔.๕ ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๔.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๔.๗ เป็นบุคคลธรรมดาหรือนิติบุคคล ผู้มีอาชีพขายพัสดุที่ประกวดราคาซื้อด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

๔.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ สำนักงานปลัดกระทรวงการคลัง ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๔.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอ ได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

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

๔.๑๑ ผู้ยื่นข้อเสนอต้องมีหนังสือรับรองผลงานเกี่ยวกับการขายและติดตั้งระบบเครื่องคอมพิวเตอร์หรือระบบเครือข่าย และติดตั้งซอฟต์แวร์ระบบ สำเร็จมาแล้วให้กับหน่วยงานของรัฐ ภายในระยะเวลา ๕ ปี นับจากวันที่ส่งมอบงานงวดสุดท้ายจนถึงวันยื่นข้อเสนอ โดยมีมูลค่าของผลงานต่อโครงการไม่น้อยกว่า ๔๐,๐๐๐,๐๐๐.- บาท (สี่สิบล้านบาท) จำนวนหนึ่งสัญญา พร้อมแสดงสำเนาสัญญาและหนังสือรับรองผลงานที่กล่าวอ้างที่ออกโดยหน่วยงานดังกล่าว

๔.๑๒ ผู้ยื่นข้อเสนอที่เป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า ๑ ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ โดยแสดงสำเนาเอกสารหรือหลักฐานมาพร้อมการยื่นข้อเสนอ

.....ประธาน.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการและเลขานุการ

๔.๑๓ ผู้ยื่นข้อเสนอที่เป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า จะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอไม่ต่ำกว่า ๒๐ ล้านบาท โดยแสดงสำเนาเอกสารหรือหลักฐานมาพร้อมการยื่นข้อเสนอ

๔.๑๔ กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียนหรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง (สินเชื่อที่ธนาคารภายในประเทศหรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้าประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรองหรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอนับถึงวันยื่นข้อเสนอไม่เกิน ๙๐ วัน) โดยแสดงสำเนาแบบหนังสือรับรองวงเงินสินเชื่อ (ตามแบบที่กรมบัญชีกลางกำหนด) มาพร้อมการยื่นข้อเสนอ

๔.๑๕ กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ หรือ เป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย (ฉบับที่ ๑๐) พ.ศ. ๒๕๖๑ ไม่ต้องยื่นเอกสารข้อเสนอตามข้อ ๔.๑๒ – ๔.๑๔

๕. ข้อกำหนดและเงื่อนไขในการยื่นข้อเสนอ

ผู้ยื่นข้อเสนอจะต้องปฏิบัติตามข้อกำหนดและเงื่อนไขในการยื่นข้อเสนอให้ครบถ้วนถูกต้อง รวมทั้งต้องปฏิบัติ ดังต่อไปนี้

๑) ผู้ยื่นข้อเสนอต้องเป็นผู้ได้รับหนังสือแต่งตั้งให้เป็นตัวแทนจำหน่ายอุปกรณ์ที่เสนอจากผู้ผลิต หรือสาขาของผู้ผลิต หรือตัวแทนจำหน่ายในประเทศไทย โดยเป็นหนังสือที่แต่งตั้งสำหรับโครงการที่เสนอโดยเฉพาะ ยื่นมาพร้อมกับการยื่นข้อเสนอ

๒) ผู้ยื่นข้อเสนอต้องระบุยี่ห้อ รุ่น (Model) อุปกรณ์ที่เสนอทุกรายการในเอกสารรายการพัสดุ หรือเอกสารข้อกำหนดทางเทคนิค (Technical Proposal) ให้ชัดเจน พร้อมแคตตาล็อกของอุปกรณ์ที่เสนอ โดยต้องทำตารางเปรียบเทียบคุณลักษณะเฉพาะพร้อมอ้างอิงแคตตาล็อก มาพร้อมการยื่นข้อเสนอ

๓) อุปกรณ์ทุกชิ้นที่เสนอต้องเป็นของแท้ ของใหม่ ไม่เคยใช้งานมาก่อน ไม่เป็นของเก่าเก็บ ต้องอยู่ในสภาพที่ใช้งานได้ทันที และต้องมีคุณลักษณะเฉพาะตรงตามที่กำหนดไว้ หรือดีกว่าข้อกำหนด

๖. ขอบเขตของงาน

โครงการเพิ่มประสิทธิภาพการรักษาความมั่นคงปลอดภัยของข้อมูลและป้องกันภัยทางไซเบอร์ระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ใหม่ สำนักงานปลัดกระทรวงการคลัง แขวงพญาไท เขตพญาไท กรุงเทพมหานคร ผู้ชนะการประกวดราคาต้องดำเนินการดังนี้

๖.๑ จัดหาอุปกรณ์คอมพิวเตอร์และซอฟต์แวร์ในโครงการ ซึ่งมีรายละเอียดคุณลักษณะเฉพาะตามเอกสารแนบ ๑

๖.๒ การบริหารงานโครงการ ตามเอกสารแนบ ๒

๖.๓ ออกแบบและติดตั้งอุปกรณ์คอมพิวเตอร์และซอฟต์แวร์ในโครงการ ตามเอกสารแนบ ๒

๖.๔ ทดสอบการเข้าถึงและความมั่นคงปลอดภัยระบบ (Security Test) ตามเอกสารแนบ ๒

๖.๕ โอนย้ายระบบสารสนเทศเพื่อการบริหาร (MIS) เดิมให้สามารถทำงานร่วมกับอุปกรณ์คอมพิวเตอร์และซอฟต์แวร์ในโครงการ ตามเอกสารแนบ ๑

๖.๖ จัดฝึกอบรมและจัดทำเอกสารต่าง ๆ ตามเอกสารแนบ ๓

๖.๗ บริการบำรุงรักษาและซ่อมแซมแก้ไขระบบ ตามเอกสารแนบ ๔

๗. ระยะเวลาดำเนินการ

ส่งมอบและติดตั้งอุปกรณ์ทั้งหมดในโครงการ ภายใน ๒๑๐ วัน นับถัดจากวันลงนามในสัญญา

๘. ระยะเวลาส่งมอบงานและเงื่อนไขการชำระเงิน

ผู้ชนะการประกวดราคาจะต้องส่งมอบงาน ดังต่อไปนี้

งานงวดที่ ๑ ส่งมอบงาน ภายใน ๓๐ วัน นับถัดจากวันลงนามในสัญญา ดังนี้

๑. ส่งมอบแผนการดำเนินงานโครงการและรายชื่อบุคลากรพร้อมประวัติ

๒. ส่งมอบแผนการติดตั้งเครื่องคอมพิวเตอร์และอุปกรณ์ในโครงการทั้งหมด

๓. ส่งมอบเอกสารจำนวน ๑ ชุด และสำเนาในรูปแบบอิเล็กทรอนิกส์ลงใน Thumb Drive จำนวน ๖ ชุด

งานงวดที่ ๒ ส่งมอบงาน ภายใน ๑๒๐ วัน นับถัดจากวันลงนามในสัญญา ดังนี้

๑. ส่งมอบแผนภาพการออกแบบและติดตั้งระบบเครือข่าย และ Single Line Diagram สำหรับระบบไฟฟ้าเพื่อการติดตั้งอุปกรณ์ในโครงการ

๒. ส่งมอบเครื่องคอมพิวเตอร์และอุปกรณ์ในโครงการทั้งหมด

๓. ส่งมอบซอฟต์แวร์พร้อมลิขสิทธิ์ที่ถูกต้องตามกฎหมาย

๔. ส่งมอบแผนการทดสอบและแผนการโอนย้ายระบบเดิม

๕. ส่งมอบเอกสารจำนวน ๑ ชุด และสำเนาในรูปแบบอิเล็กทรอนิกส์ลงใน Thumb Drive จำนวน ๖ ชุด

งานงวดที่ ๓ ส่งมอบงาน ภายใน ๑๘๐ วัน นับถัดจากวันลงนามในสัญญา ดังนี้

๑. ส่งมอบผลการติดตั้งเครื่องคอมพิวเตอร์และอุปกรณ์ และการติดตั้งซอฟต์แวร์ในโครงการทั้งหมด

๒. ส่งมอบผลการทดสอบอุปกรณ์ในโครงการทั้งหมด

๓. ส่งมอบเอกสารจำนวน ๑ ชุด และสำเนาในรูปแบบอิเล็กทรอนิกส์ลงใน Thumb Drive จำนวน ๖ ชุด

งานงวดที่ ๔ ส่งมอบงาน ภายใน ๒๑๐ วัน นับถัดจากวันลงนามในสัญญา ดังนี้

๑. ส่งมอบผลการโอนย้ายระบบเดิม

๒. ส่งมอบผลการฝึกอบรมและเอกสารต่าง ๆ

๓. ส่งมอบเอกสารการบำรุงรักษาและซ่อมแซมแก้ไขระบบ

๔. ส่งมอบเอกสารจำนวน ๑ ชุด และสำเนาในรูปแบบอิเล็กทรอนิกส์ลงใน Thumb Drive จำนวน ๖ ชุด

เงื่อนไขการชำระเงิน จะแบ่งการชำระเงินเป็น ๔ งวด ดังนี้

งวดที่ ๑ ชำระเงินในอัตราร้อยละ ๑๐ ของจำนวนเงินตามสัญญา
เมื่อคณะกรรมการตรวจรับได้ตรวจรับการส่งมอบงานงวดที่ ๑ เรียบร้อยแล้ว

งวดที่ ๒ ชำระเงินในอัตราร้อยละ ๔๐ ของจำนวนเงินตามสัญญา
เมื่อคณะกรรมการตรวจรับได้ตรวจรับการส่งมอบงานงวดที่ ๒ เรียบร้อยแล้ว

.....ประธาน.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการและเลขานุการ

งวดที่ ๓ ชำระเงินในอัตราร้อยละ ๔๐ ของจำนวนเงินตามสัญญา
เมื่อคณะกรรมการตรวจรับได้ตรวจรับการส่งมอบงานงวดที่ ๓ เรียบร้อยแล้ว

งวดที่ ๔ ชำระเงินในอัตราร้อยละ ๑๐ ของจำนวนเงินตามสัญญา
เมื่อคณะกรรมการตรวจรับได้ตรวจรับการส่งมอบงานงวดที่ ๔ เรียบร้อยแล้ว

๙. วงเงินในการจัดหา

วงเงินงบประมาณทั้งสิ้น ๙๓,๖๖๐,๐๐๐.- บาท (เก้าสิบสามล้านหกแสนหกหมื่นบาทถ้วน) ซึ่งเป็นราคาที่รวมภาษีมูลค่าเพิ่ม และค่าใช้จ่ายอื่นใดทั้งปวงไว้ด้วยแล้ว โดยเบิกจ่ายจากเงินงบประมาณรายจ่าย ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

๑๐. หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

ใช้เกณฑ์ราคาในการคัดเลือก

๑๑. ค่าปรับ

ผู้ชนะการประกวดราคาต้องดำเนินการตามที่กำหนดไว้ในขอบเขตของงานข้างต้นให้ครบถ้วน และหากไม่สามารถดำเนินการได้ครบถ้วนหรือถูกต้อง ผู้ขายยินยอมให้ผู้ซื้อปรับเป็นรายวันในอัตราร้อยละ ๐.๒๐ (ศูนย์จุดสองศูนย์) ของราคาสิ่งของที่ยังไม่ได้รับมอบ จนกว่าจะดำเนินการแล้วเสร็จหรือผู้ซื้อใช้สิทธิบอกเลิกสัญญา

๑๒. การรับประกันความเสียหาย

ในกรณีที่บุคคลภายนอกกล่าวอ้างหรือใช้สิทธิเรียกร้องใด ๆ ว่ามีการละเมิดลิขสิทธิ์หรือสิทธิบัตรหรือสิทธิใด ๆ เกี่ยวกับโครงการตามสัญญานี้ โดยสำนักงานปลัดกระทรวงการคลังมิได้แก้ไขดัดแปลงไปจากเดิม ผู้ชนะการประกวดราคาจะต้องดำเนินการทั้งปวงเพื่อให้การกล่าวอ้างหรือการเรียกร้องดังกล่าวระงับสิ้นไปโดยเร็ว หากสำนักงานปลัดกระทรวงการคลังต้องรับผิดชดใช้ค่าเสียหายต่อบุคคลภายนอกเนื่องจากผลแห่งการละเมิดลิขสิทธิ์หรือสิทธิบัตรหรือสิทธิใด ๆ ดังกล่าว ผู้ชนะการประกวดราคาจะต้องเป็นผู้ชำระค่าเสียหายและค่าใช้จ่ายรวมทั้งค่าฤชาธรรมเนียมและค่าทนายความแทนสำนักงานปลัดกระทรวงการคลัง ทั้งนี้ สำนักงานปลัดกระทรวงการคลัง จะแจ้งให้ผู้ชนะการประกวดราคาทราบเป็นลายลักษณ์อักษรเมื่อมีการกล่าวอ้างหรือใช้สิทธิเรียกร้องดังกล่าวโดยไม่ชักช้า

๑๓. ความรับผิดของผู้ขาย

ผู้ขายจะต้องรับผิดต่อผู้ซื้อในกรณีที่ผู้ขาย ผู้แทน ช่าง หรือลูกจ้างของผู้ขาย จงใจหรือประมาทเลินเล่อหรือไม่มีความรู้ความชำนาญพอ กระทำหรืองดเว้นการกระทำใด ๆ เป็นเหตุให้คอมพิวเตอร์ของ ผู้ซื้อเสียหายหรือไม่อยู่ในสภาพที่ใช้การได้ดี โดยไม่อาจแก้ไขได้ โดยผู้ขายจะต้องจัดหาคอมพิวเตอร์ที่มีคุณภาพ ประสิทธิภาพและความสามารถในการใช้งานไม่ต่ำกว่าของเดิมชดใช้แทน หรือชดใช้ราคาคอมพิวเตอร์ ในขณะที่เกิดความเสียหายในกรณีที่ไม่อาจจัดหาคอมพิวเตอร์ดังกล่าวชดใช้แทนได้ ให้แก่ผู้ซื้อ ภายในเวลาที่ผู้ซื้อกำหนดนับตั้งแต่เวลาที่ผู้ซื้อบอกกล่าวเป็นหนังสือให้ผู้ขายจัดหาคอมพิวเตอร์มาชดใช้ให้แทนหรือชดใช้ราคาคอมพิวเตอร์ตามวรรคหนึ่ง ผู้ขายยินยอมให้ผู้ซื้อปรับเป็นรายวันในอัตราร้อยละ ๐.๒๐ (ศูนย์จุดสองศูนย์) ของราคาสิ่งของที่ยังไม่ได้รับมอบ จนกว่าผู้ซื้อบอกเลิกสัญญา และหากผู้ซื้อต้องใช้คอมพิวเตอร์ที่อื่นประมวลผล ผู้ขายยินยอมชดใช้ค่าใช้จ่ายเพื่อการดังกล่าวทั้งสิ้นแทนผู้ซื้ออีกด้วย

.....ประธาน.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการและเลขานุการ

๑๔. ความต้องการด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ และข้อตกลงในการเก็บรักษาความลับข้อมูลหรือเอกสาร

ผู้ขายต้องปฏิบัติตามนโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Policy) และวิธีปฏิบัติที่เกี่ยวข้องของสำนักงานปลัดกระทรวงการคลังอย่างเคร่งครัด ดังนี้

๑๔.๑ ผู้ขายและผู้ปฏิบัติงานของผู้ขายต้องปฏิบัติตามนโยบายและวิธีปฏิบัติที่เกี่ยวข้องของสำนักงานปลัดกระทรวงการคลังอย่างเคร่งครัด หากพบว่าผู้ขายหรือผู้ปฏิบัติงานของผู้ขายไม่ปฏิบัติตามนโยบายและวิธีปฏิบัติที่เกี่ยวข้องจนก่อให้เกิดความเสียหาย สำนักงานปลัดกระทรวงการคลังขอสงวนสิทธิ์ในการเรียกร้องค่าเสียหายอันเนื่องมาจากการไม่ปฏิบัติตามนโยบายและวิธีปฏิบัติที่เกี่ยวข้อง โดยนโยบายและวิธีปฏิบัติที่เกี่ยวข้องประกอบด้วยอย่างน้อยดังต่อไปนี้

๑๔.๑.๑ นโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Policy)

๑๔.๑.๒ นโยบายความมั่นคงปลอดภัยด้านสถานที่และสภาพแวดล้อม (Physical and Environmental Security Policy)

๑๔.๑.๓ แนวทางปฏิบัติการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ (ISMS Procedure) และนโยบายและวิธีปฏิบัติที่เกี่ยวข้องอื่น ๆ ที่จัดทำขึ้นภายหลังและมีการแจ้งให้ทราบ

๑๔.๒ ผู้ขายต้องยินยอมให้สำนักงานปลัดกระทรวงการคลัง หรือหน่วยงานภายนอกที่ สำนักงานปลัดกระทรวงการคลัง มอบหมาย หรือหน่วยงานกำกับดูแล สำนักงานปลัดกระทรวงการคลัง มีสิทธิในการเข้าตรวจสอบการทำงานรวมถึงสิทธิในการเรียกดูข้อมูลที่เกี่ยวข้อง

๑๔.๓ ซอฟต์แวร์ทุกประเภทที่นำมาใช้กับงานกับสำนักงานปลัดกระทรวงการคลัง ต้องมีลิขสิทธิ์ใช้งานถูกต้องตามกฎหมาย และต้องไม่มีโปรแกรมแอบแฝงหรือโปรแกรมมุ่งร้ายใด ๆ ฝังตัวอยู่ และหากสำนักงานปลัดกระทรวงการคลังตรวจพบว่ามีโปรแกรมดังกล่าวและได้ก่อให้เกิดความเสียหายต่อระบบงานระบบคอมพิวเตอร์ และระบบเครือข่ายสื่อสารของสำนักงานปลัดกระทรวงการคลัง ผู้ยื่นข้อเสนอต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นทั้งหมด

๑๔.๔ ผู้ขายต้องดำเนินการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Risk Management) ภายในโครงการ โดยจะต้องนำเสนอข้อมูลเกี่ยวกับความเสี่ยงที่อาจเกิดขึ้นและแนวทางในการบริหารจัดการความเสี่ยงเหล่านั้นให้กับสำนักงานปลัดกระทรวงการคลังได้ทราบอย่างสม่ำเสมอตลอดระยะเวลาการดำเนินโครงการ

๑๔.๕ ผู้ขายต้องไม่เปิดเผยข้อมูลอันเป็นความลับใด ๆ หรือข้อมูลอื่นใดทั้งหมดหรือบางส่วนที่ได้รับหรือรับรู้มาจากสำนักงานปลัดกระทรวงการคลังให้ผู้อื่นทราบโดยมิได้รับความยินยอมจากสำนักงานปลัดกระทรวงการคลังและต้องควบคุม กำกับไม่ให้ผู้ปฏิบัติงานของผู้ขายเปิดเผยข้อมูลอันเป็นความลับใด ๆ หรือข้อมูลอื่นใดทั้งหมดหรือบางส่วนที่ได้รับหรือรับรู้มาจากสำนักงานปลัดกระทรวงการคลังให้ผู้อื่นทราบเช่นกัน หากมีความเสียหายต่อสำนักงานปลัดกระทรวงการคลัง ผู้ขายต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นทั้งหมด

๑๔.๖ ผู้ขายต้องทำความเข้าใจ ลงนาม และปฏิบัติตามบันทึกข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement: NDA) และบันทึกข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) รวมทั้งเงื่อนไขอื่นหรือข้อกำหนดต่าง ๆ ที่เกี่ยวข้องกับการไม่เปิดเผยความลับของข้อมูลสำคัญของสำนักงานปลัดกระทรวงการคลัง

๑๕. หน่วยงานผู้รับผิดชอบดำเนินการ

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง

.....ประธาน.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการและเลขานุการ

๑๖. ข้อสงวนสิทธิในการยื่นข้อเสนอและอื่น ๆ

๑๖.๑ การจัดซื้อหรือการจัดจ้างครั้งนี้จะมีการลงนามในสัญญาหรือข้อตกลงเป็นหนังสือได้ต่อเมื่อพระราชบัญญัติงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. ๒๕๖๙ มีผลใช้บังคับ และได้รับจัดสรรงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. ๒๕๖๙ จากสำนักงบประมาณแล้ว สำหรับกรณีที่ไม่ได้รับการจัดสรรงบประมาณรายจ่ายเพื่อการจัดหาในครั้งนี้ ส่วนราชการสามารถยกเลิกจัดหาได้

๑๖.๒ หากข้อความใดในขอบเขตของงานมีความขัดแย้งกัน ให้ยึดถือตามข้อกำหนดที่เป็นประโยชน์กับสำนักงานปลัดกระทรวงการคลัง

.....ประธาน.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการและเลขานุการ

ท่านสามารถเสนอแนะวิจารณ์ หรือแสดงความคิดเห็นโดยเปิดเผย

๑. **ทางไปรษณีย์** โครงการเพิ่มประสิทธิภาพการรักษาความมั่นคงปลอดภัยของข้อมูลและป้องกันภัยทางไซเบอร์ระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ใหม่ สำนักงานปลัดกระทรวงการคลัง แขวงพญาไท เขตพญาไท กรุงเทพมหานคร
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงการคลัง
ถนนพระราม ๖ แขวงพญาไท เขตพญาไท
กรุงเทพมหานคร ๑๐๔๐๐

๒. **ทาง e-Mail** tor-securitygfmis@mof.go.th

๓. **ทางโทรศัพท์** หมายเลข ๐๒-๑๒๖-๕๙๐๐ ต่อ ๓๐๓๒๔ , ๓๐๒๒๐

ทั้งนี้ โปรดแจ้ง ชื่อ ที่อยู่ พร้อมหมายเลขโทรศัพท์ติดต่อกลับด้วย

.....ประธาน.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการและเลขานุการ

เอกสารแนบ ๑
รายละเอียดคุณลักษณะเฉพาะ

ดำเนินงานโครงการเพิ่มประสิทธิภาพการรักษาความมั่นคงปลอดภัยของข้อมูลและป้องกันภัยทางไซเบอร์ระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ใหม่ สำนักงานปลัดกระทรวงการคลัง แขวงพญาไท เขตพญาไท กรุงเทพมหานคร โดยการจัดหาอุปกรณ์คอมพิวเตอร์และซอฟต์แวร์ ที่จัดซื้อครั้งนี้จะต้องเป็นของแท้ ของใหม่ ไม่เคยใช้งานมาก่อน ไม่เป็นของเก่าเก็บ อยู่ในสภาพที่ใช้งานได้ทันที โดยจะต้องได้รับหนังสือรับรองในการสนับสนุนการจำหน่าย ติดตั้งและบำรุงรักษาอุปกรณ์คอมพิวเตอร์และซอฟต์แวร์ในโครงการจากผู้ผลิต หรือสาขาของผู้ผลิต หรือตัวแทนจำหน่ายในประเทศไทย ซึ่งออกให้สำหรับโครงการเพิ่มประสิทธิภาพการรักษาความมั่นคงปลอดภัยของข้อมูลและป้องกันภัยทางไซเบอร์ระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ใหม่ สำนักงานปลัดกระทรวงการคลัง แขวงพญาไท เขตพญาไท กรุงเทพมหานคร และยื่นมาพร้อมกับการยื่นข้อเสนอในครั้งนี้

อุปกรณ์คอมพิวเตอร์และซอฟต์แวร์ ที่จัดซื้อครั้งนี้ มีคุณลักษณะเฉพาะอย่างน้อย ดังต่อไปนี้

๑. เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูลสำหรับระบบ MIS ติดตั้งที่ศูนย์คอมพิวเตอร์หลัก (DC) ประกอบด้วย

๑.๑ เครื่องคอมพิวเตอร์แม่ข่าย (สำหรับระบบฐานข้อมูล) จำนวน ๒ ชุด โดยแต่ละชุดมีคุณลักษณะเฉพาะอย่างน้อยดังนี้

๑) เครื่องคอมพิวเตอร์แม่ข่ายที่เสนอต้องเป็นเครื่องคอมพิวเตอร์แม่ข่ายที่มีขนาดไม่น้อยกว่า ๒U สำหรับใช้งานกับระบบฐานข้อมูล โดยจะต้องสามารถทำงานร่วมกันกับซอฟต์แวร์ฐานข้อมูลที่เสนอได้

๒) เครื่องคอมพิวเตอร์แม่ข่ายที่นำเสนอสามารถทำงานร่วมกับซอฟต์แวร์ฐานข้อมูลที่นำเสนอแบบมีเสถียรภาพสูง (High Availability) แบบ Active-Standby ได้

๓) มีหน่วยประมวลผลกลาง (CPU) แบบ X๘๖ หรือดีกว่า จำนวนไม่น้อยกว่า ๒ หน่วย โดยแต่ละหน่วยมีจำนวน CPU Core ไม่น้อยกว่า ๓๒ Core และมีความเร็วสัญญาณนาฬิกา (Clock Speed) ไม่น้อยกว่า ๒.๖ GHz

๔) มีหน่วยความจำหลัก (Memory) จำนวนรวมไม่น้อยกว่า ๑ TB

๕) มีหน่วยจัดเก็บข้อมูล (Hard Drive) ชนิด NVMe SSD ที่มีขนาดความจุ (RAW Capacity) ไม่น้อยกว่า ๔๐๐ GB จำนวนไม่น้อยกว่า ๒ หน่วย

๖) มีช่องเชื่อมต่อ Host Bus Adapter (HBA) แบบ SAS หรือดีกว่า จำนวนรวมไม่น้อยกว่า ๔ ช่อง สำหรับเชื่อมต่ออุปกรณ์จัดเก็บข้อมูล

๗) มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ ๑๐/๒๕ Gb Ethernet หรือดีกว่า จำนวนไม่น้อยกว่า ๖ ช่อง พร้อม transceiver module ความเร็วไม่น้อยกว่า ๑๐ Gbps sfp+

๘) มีระบบปฏิบัติการ Enterprise Linux แบบ ๖๔ bit ที่มีลิขสิทธิ์การใช้งานถูกต้องตามกฎหมาย และสามารถร้องขอการสนับสนุน (Support) ในการแก้ไขปัญหาจากบริษัทเจ้าของผลิตภัณฑ์ได้

๙) มีซอฟต์แวร์เครื่องคอมพิวเตอร์แม่ข่ายเสมือน (Virtualization) ที่มีลิขสิทธิ์การใช้งานถูกต้องตามกฎหมาย และสามารถร้องขอการสนับสนุน (Support) ในการแก้ไขปัญหาจากบริษัทเจ้าของผลิตภัณฑ์ได้

๑๐) สามารถบริหารจัดการระบบ (Remote Management) ผ่านทาง Browser Interface และ Command-Line ได้

๑๑) เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูลที่เสนอ ต้องติดตั้งซอฟต์แวร์สำหรับการ Provisioning ระบบฐานข้อมูลได้โดยง่าย โดยสามารถทำการ Provision Database ผ่าน GUI หรือ Browser Interface ได้

๑๒) เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูลที่เสนอ ต้องติดตั้งเครื่องมือหรือซอฟต์แวร์สำหรับการสำรองข้อมูลระบบฐานข้อมูล (Database Backup) โดยจะต้องทำการ Backup และ Restore ระบบฐานข้อมูลได้ และสามารถสร้าง Backup Policy เพื่อกำหนด Backup Location และ Recovery Window ผ่าน GUI หรือ Browser Interface ได้

๑๓) มีแหล่งจ่ายไฟแบบ Hot Plug Redundant Power Supply หรือ Hot Swappable Redundant Power Supply จำนวน ๒ หน่วย

๑.๒ อุปกรณ์จัดเก็บข้อมูลแบบภายนอกสำหรับระบบฐานข้อมูล จำนวน ๑ ชุด มีคุณลักษณะเฉพาะอย่างน้อย ดังนี้

๑) เป็นอุปกรณ์จัดเก็บข้อมูล (Disk Enclosure/Disk shelf) หรือเครื่องแม่ข่ายแบบ Storage Server หรือ Storage Node

๒) มีหน่วยจัดเก็บข้อมูลชนิด SSD หรือ NVMe SSD หรือดีกว่า ที่มีขนาดความจุรวมทั้งหมดไม่น้อยกว่า ๑๓๖ TB (RAW Capacity)

๓) รองรับจำนวนหน่วยจัดเก็บข้อมูลได้รวมไม่น้อยกว่า ๒๔ หน่วย และรองรับการขยายเพิ่มเติมได้รวมทั้งหมดไม่น้อยกว่า ๔๘ หน่วย โดยการเพิ่ม Disk Enclosure/Disk Shelf ในอนาคต

๔) มีแหล่งจ่ายไฟฟ้า (Power Supply) แบบ Redundant และรองรับการทำงานแบบ Hot Swap หรือ Hot Plug จำนวนไม่น้อยกว่า ๒ หน่วย

๒. เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูลสำหรับระบบ MIS และระบบทดสอบ (Dev/QA) ติดตั้งที่ศูนย์คอมพิวเตอร์สำรอง (DR) ประกอบด้วย

๒.๑ เครื่องคอมพิวเตอร์แม่ข่าย (สำหรับระบบฐานข้อมูล) จำนวน ๒ ชุด โดยแต่ละชุดมีคุณลักษณะเฉพาะอย่างน้อยดังนี้

๑) เครื่องคอมพิวเตอร์แม่ข่ายที่เสนอต้องเป็นเครื่องคอมพิวเตอร์แม่ข่ายที่มีขนาดไม่น้อยกว่า ๒U สำหรับใช้งานกับระบบฐานข้อมูล โดยจะต้องสามารถทำงานร่วมกันกับซอฟต์แวร์ฐานข้อมูลที่เสนอได้

๒) เครื่องคอมพิวเตอร์แม่ข่ายที่นำเสนอสามารถทำงานร่วมกับซอฟต์แวร์ฐานข้อมูลที่นำเสนอแบบมีเสถียรภาพสูง (High Availability) แบบ Active-Standby ได้

๓) มีหน่วยประมวลผลกลาง (CPU) แบบ X๘๖ หรือดีกว่า จำนวนไม่น้อยกว่า ๒ หน่วย โดยแต่ละหน่วยมีจำนวน CPU Core ไม่น้อยกว่า ๓๒ Core และมีความเร็วสัญญาณนาฬิกา (Clock Speed) ไม่น้อยกว่า ๒.๖ GHz

๔) มีหน่วยความจำหลัก (Memory) จำนวนรวมไม่น้อยกว่า ๑.๕ TB

๕) มีหน่วยจัดเก็บข้อมูล (Hard Drive) ชนิด NVMe SSD ที่มีขนาดความจุ (RAW Capacity) ไม่น้อยกว่า ๔๐๐ GB จำนวนไม่น้อยกว่า ๒ หน่วย

๖) มีช่องเชื่อมต่อ Host Bus Adapter (HBA) แบบ SAS หรือดีกว่า จำนวนรวมไม่น้อยกว่า ๔ ช่อง สำหรับเชื่อมต่ออุปกรณ์จัดเก็บข้อมูล

๗) มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ ๑๐/๒๕ Gb Ethernet หรือดีกว่า จำนวนไม่น้อยกว่า ๖ ช่อง พร้อม transceiver module ความเร็วไม่น้อยกว่า ๑๐ Gbps sfp+

๘) มีระบบปฏิบัติการ Enterprise Linux แบบ ๖๔ bit ที่มีลิขสิทธิ์การใช้งานถูกต้องตามกฎหมาย และสามารถร้องขอการสนับสนุน (Support) ในการแก้ไขปัญหาจากบริษัทเจ้าของผลิตภัณฑ์ได้

๙) มีซอฟท์แวร์เครื่องคอมพิวเตอร์แม่ข่ายเสมือน (Virtualization) ที่มีลิขสิทธิ์การใช้งานถูกต้องตามกฎหมาย และสามารถร้องขอการสนับสนุน (Support) ในการแก้ไขปัญหาจากบริษัทเจ้าของผลิตภัณฑ์ได้

๑๐) สามารถบริหารจัดการระบบ (Remote Management) ผ่านทาง Browser Interface และ Command-Line ได้

๑๑) เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูลที่เสนอ ต้องติดตั้งซอฟต์แวร์สำหรับการ Provisioning ระบบฐานข้อมูลได้โดยง่าย โดยสามารถทำการ Provision Database ผ่าน GUI หรือ Browser Interface ได้

๑๒) เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูลที่เสนอ ต้องติดตั้งเครื่องมือ หรือซอฟต์แวร์สำหรับการสำรองข้อมูลระบบฐานข้อมูล (Database Backup) โดยจะต้องทำการ Backup และ Restore ระบบฐานข้อมูลได้ และสามารถสร้าง Backup Policy เพื่อกำหนด Backup Location และ Recovery Window ผ่าน GUI หรือ Browser Interface ได้

๑๓) มีแหล่งจ่ายไฟแบบ Hot Plug Redundant Power Supply หรือ Hot Swappable Redundant Power Supply จำนวน ๒ หน่วย

๒.๒ อุปกรณ์จัดเก็บข้อมูลแบบภายนอกสำหรับระบบฐานข้อมูล จำนวน ๑ ชุด มีคุณลักษณะเฉพาะอย่างน้อย ดังนี้

๑) เป็นอุปกรณ์จัดเก็บข้อมูล (Disk Enclosure/Disk shelf) หรือเครื่องแม่ข่ายแบบ Storage Server หรือ Storage Node

๒) มีหน่วยจัดเก็บข้อมูลแบบ SSD หรือ NVMe SSD หรือดีกว่า ที่มีขนาดความจุรวมทั้งหมดไม่น้อยกว่า ๑๘๐ TB (RAW Capacity)

๓) รองรับการขยายเพิ่มเติมได้รวมทั้งหมดไม่น้อยกว่า ๔๘ หน่วย โดยการเพิ่ม Disk Enclosure/Disk Shelf ในอนาคต

๔) มีแหล่งจ่ายไฟฟ้า (Power Supply) แบบ Redundant และรองรับการทำงานแบบ Hot Swap หรือ Hot Plug จำนวนไม่น้อยกว่า ๒ หน่วย

๓. อุปกรณ์ป้องกันเครือข่ายสำหรับป้องกันภัยทางไซเบอร์ (Next Generation Firewall) ติดตั้งที่ศูนย์คอมพิวเตอร์หลัก (DC) จำนวน ๒ ชุด โดยมีคุณลักษณะเฉพาะอย่างน้อยดังนี้

๓.๑ เป็นอุปกรณ์ Appliance-Based Firewall ที่สร้างขึ้นเพื่อทำหน้าที่ตรวจจับและควบคุม Application, User, Content โดยเฉพาะ (Application Firewall)

๓.๒ มี Network Interface อย่างน้อยดังนี้

๑) Interface แบบ ๑G/๒.๕G/๕G/๑๐G (RJ๔๕) หรือดีกว่าไม่น้อยกว่า ๑๒ พอร์ท

๒) ช่องเชื่อมต่อแบบ ๑G/๑๐G SFP/SFP+ หรือดีกว่า ไม่น้อยกว่า ๑๐ ช่อง

๓) ช่องเชื่อมต่อแบบ ๑G/๑๐G/๒๕G SFP/SFP+/SFP๒๘ หรือดีกว่า ไม่น้อยกว่า ๔ ช่อง

๓.๓ มี Interface HA แบบ ๑๐/๑๐๐/๑๐๐๐ หรือดีกว่า ไม่น้อยกว่า ๒ พอร์ท, ๑๐G SFP+ หรือดีกว่า ไม่น้อยกว่า ๑ พอร์ท และมี Interface แบบ ๑๐/๑๐๐/๑๐๐ (RJ๔๕) ดีกว่าสำหรับบริหารจัดการโดยเฉพาะ (Out of Band Management) ไม่น้อยกว่า ๑ พอร์ท โดยทั้งหมดไม่นับรวมกับ interface จากข้อที่กำหนดในข้อก่อนหน้านี้

๓.๔ มี Application Firewall Throughput ไม่น้อยกว่า ๑๙ Gbps ในแบบ Appmix หรือ Enterprise testing condition หรือ Enterprise traffic mix

๓.๕ มี Threat prevention Throughput ไม่น้อยกว่า ๑๐ Gbps ในแบบ Appmix หรือ Enterprise testing condition หรือ Enterprise traffic mix

๓.๖ มี storage ชนิด SSD สำหรับจัดเก็บข้อมูลระบบ (System Storage) ขนาดไม่ต่ำกว่า ๒๔๐GB หรือดีกว่า

๓.๗ สามารถติดตั้งในรูปแบบ Transparent Inline (Virtual Wire), Non-Inline Monitoring (Tap), L๒ และ L๓ หรือเทียบเท่าได้

๓.๘ สามารถทำ Routing แบบ Static, RIP, BGP, OSPF, Multicast และ Policy Based Forwarding หรือ Policy based Routing ได้เป็นอย่างน้อย

๓.๙ สามารถทำการตรวจสอบทราฟฟิคที่เข้ารหัส SSL ด้วยการทำ SSL decryption (ทั้งแบบ Inbound และ Outbound) รวมทั้งการทำ SSL Decryption Broker หรือ Network Packet Broker ได้ หรือนำเสนอระบบอื่น ๆเพิ่มเติม เพื่อให้สามารถทำได้ตามข้อกำหนด โดยมี Throughput ไม่น้อยกว่า Firewall Throughput

๓.๑๐ สามารถทำงานร่วมกับระบบการพิสูจน์ตัวตน (Authentication Systems) ได้แก่ Active Directory, LDAP, Radius เพื่อทำการติดตามผู้ใช้ได้เป็นอย่างน้อย

๓.๑๑ สามารถรับ Syslog จากระบบที่มีอยู่ได้ เพื่อใช้ในการยืนยันตัวตน ของ User ที่ใช้งาน โดยรองรับทั้ง User Log-in และ User Log-out ได้ หรือนำเสนอระบบอื่น ๆ เพิ่มเติม เพื่อให้สามารถทำได้ตามข้อกำหนด

๓.๑๒ สามารถควบคุมประเภทของไฟล์ที่อนุญาตให้ download และ upload บนแต่ละ Application ได้ รวมทั้งสามารถป้องกันการรั่วไหลของข้อมูล (Data Filtering) ออกจากระบบเครือข่าย เช่น หมายเลขบัตรเครดิต และสามารถสร้างรูปแบบการตรวจสอบได้ตามความต้องการ

๓.๑๓ สามารถป้องกันภัยคุกคามประเภท Vulnerability และ Spyware ได้โดยสามารถมีการอัพเดท Signature ใหม่แบบอัตโนมัติได้

๓.๑๔ สามารถกำหนดนโยบายการเข้าถึง website (URL Filtering) สามารถติดตามและควบคุมการเข้าถึงเว็บได้ตาม Category, Block list, Allow list ที่กำหนดได้ และต้องมีการจัด category ให้กับแต่ละ website ไม่น้อยกว่า ๒ category (Multi-Category URL Filtering) ได้แบบอัตโนมัติ หรือนำเสนอระบบอื่น ๆ เพิ่มเติม เพื่อสามารถทำได้ตามข้อกำหนด โดยมี Throughput ไม่น้อยกว่า Firewall Throughput

๓.๑๕ สามารถตรวจจับ, วิเคราะห์ และ ป้องกัน การเข้าถึง Malicious Domain ภายในองค์กรได้แบบ Real-time (DNS Security) โดยต้องมีการใช้ระบบ Machine Learning หรือ AI ในการตรวจจับ Domain ที่ผิดปกติ เช่น DGA Domain, DNS Tunneling, Fast Flux Domain, Dangling DNS Attacks, Wildcard DNS ในรูปแบบของการทำงานแบบ Inline Protection เป็นอย่างน้อย หรือนำเสนอระบบอื่น ๆ เพิ่มเติม เพื่อสามารถทำได้ตามข้อกำหนด โดยระบบที่นำเสนอจะต้องมี Throughput ไม่น้อยกว่า Firewall Throughput ของอุปกรณ์

๓.๑๖ มีระบบตรวจจับ Advanced Malware แบบ Cloud-Based และใช้เทคโนโลยีแบบ Sandbox , Machine Learning และ Bare Metal Analysis เพื่อใช้ระบุ Malware ประเภทใหม่ (Zero-day Malware) ซึ่งไม่มีในฐานข้อมูลการบุกรุกโจมตีได้ รวมถึงสามารถสร้างรูปแบบการโจมตี (Signature) ดังกล่าวขึ้นมาเพื่อใช้ป้องกันระบบเครือข่ายได้โดยอัตโนมัติ หรือนำเสนอระบบอื่น ๆ เพิ่มเติม เพื่อสามารถทำได้ตามข้อกำหนด โดยมี Throughput ไม่น้อยกว่า Firewall Throughput

๓.๑๗ สามารถเรียกดูสรุปข้อมูลของ Data ในรูปแบบของกราฟฟิคได้ และสามารถทำรายงานต่าง ๆ ได้ โดยไม่ต้องเสนออุปกรณ์อื่นเพิ่มเติมอย่างน้อยดังนี้

๑) Top Application, Application Category

๒) Top Source, User, Destination

๓) User activity report

๓.๑๘ สามารถทำรายงานรวมถึงปรับแต่งรายงานตามความต้องการ ในรูปแบบ PDF ได้เป็นอย่างน้อย พร้อมทั้งตั้งเวลาส่งรายงานผ่านทาง Email แบบอัตโนมัติได้

๓.๑๙ รองรับการติดตั้งเพื่อทำ High Availability แบบ Active-Active และ Active-Passive ได้

๓.๒๐ มีแหล่งจ่ายไฟฟ้า (Power Supply) แบบ redundant จำนวนไม่น้อยกว่า ๒ ชุด หรือสามารถถอดเปลี่ยนได้โดยไม่มีผลกระทบต่อการให้บริการ (Without Services Interruption)

๔. อุปกรณ์ป้องกันเว็บแอพพลิเคชันสำหรับป้องกันภัยทางไซเบอร์ (Web Application Firewall) จำนวน ๒ ชุด โดยมีคุณลักษณะเฉพาะอย่างน้อยดังต่อไปนี้

๔.๑ เป็นอุปกรณ์ที่ทำหน้าที่ป้องกันการโจมตีด้าน Web Application หรือ Web Service โดยเฉพาะ สามารถติดตั้งใน Rack มาตรฐานขนาด ๑๙ นิ้วได้

๔.๒ สามารถรองรับ Throughput ได้ไม่น้อยกว่า ๑๐ Gbps

๔.๓ มีพอร์ตการเชื่อมต่อ ๑๐ Gigabit Fiber Ports (SFP๒๘/SFP+/SFP) ไม่น้อยกว่า ๘ พอร์ต และรองรับ ๑๐๐G/๔๐G (QSFP+/QSFP๒๘) ไม่น้อยกว่า ๒ port พร้อมโมดูลการใช้งานหรือเสนออุปกรณ์อื่นที่สามารถทำงานทดแทน

๔.๔ มี Memory ไม่น้อยกว่า ๑๒๘ GB และ Hard drive แบบ SSD ที่มีความจุไม่น้อยกว่า ๙๖๐ GB

๔.๕ สามารถทำ SSL Offload ได้ โดยรองรับ TLS v๑.๐, TLS v๑.๑, TLS v๑.๒, TLS v๑.๓ เป็นอย่างน้อย

๔.๖ สามารถทำ SSL/TLS แบบ RSA ๒K Keys ไม่น้อยกว่า ๓๐,๐๐๐ TPS และ ECDSA P-๒๕๖ ไม่น้อยกว่า ๑๐,๐๐๐ TPS

๔.๗ สามารถป้องกันการโจมตีแบบ SQL injection, Cross-site scripting, HTTP protocol compliance, data leakage, shellshock, Brute Force และ Credential Stuffing ได้เป็นอย่างน้อย

๔.๘ สามารถตรวจจับและป้องกัน Web Application ตามรูปแบบการถูกโจมตี OWASP Top ๑๐ ได้เป็นอย่างน้อย

๔.๙ สามารถทำ Proactive Bot Protection ที่ป้องกันการโจมตีจำพวก BOT และ attack tools ได้ โดยมี BOT Categories หรือ Signature ที่ใช้ในการป้องกัน หรือเสนออุปกรณ์ที่สามารถทำงานทดแทน

๔.๑๐ มีความสามารถในการทำ Behavioral DoS ที่ทำงานแบบ Automatic Protection ได้ โดยสามารถทำการ Learning และทำ data analysis วิเคราะห์จากพฤติกรรมของการใช้งานได้ หรือเสนออุปกรณ์ที่สามารถทำงานทดแทน

๔.๑๑ สามารถทำ Geolocation-based blocking ได้

๔.๑๒ สามารถทำงานเป็น Server Load Balance สำหรับ Web Application โดยรองรับรูปแบบการทำงานดังนี้ Round Robin, Least Connection, Weighted Least Connections หรือเสนออุปกรณ์ที่สามารถทำ Server Load Balance ทำงานทดแทน

๔.๑๓ สามารถรองรับการทำ Session Persistence ได้โดยวิธีการ Cookie, Source Address, Destination Address และ Host เป็นอย่างน้อย หรือเสนออุปกรณ์ที่สามารถทำงานทดแทน

๔.๑๔ สามารถทำ Service Health Check เพื่อตรวจสอบการตอบสนองของ Server โดยรองรับการ Monitor ในรูปแบบ HTTP, HTTPS, TCP และ ICMP เป็นอย่างน้อย

๔.๑๕ สามารถจัดทำ Security Report และสามารถ Custom report ได้

๔.๑๖ สามารถทำการส่ง Logs ไปยังอุปกรณ์ภายนอกด้วย Syslog ได้

๔.๑๗ มี Signature ที่สามารถ update ได้ทั้งแบบ Automatic และ Manual ได้

๔.๑๘ สามารถส่ง Notification ผ่าน SNMP หรือ Syslog หรือ email ได้เป็นอย่างน้อย

๔.๑๙ มี Power Supply อย่างน้อย ๒ ชุด เพื่อทำ Redundant power supply แบบ Hot-swappable ได้

๔.๒๐ อุปกรณ์ที่นำเสนอต้องผ่านมาตรฐาน FCC และ CE หรือ UL

๕. ระบบรักษาความมั่นคงปลอดภัยของข้อมูล ประกอบด้วย

๕.๑ ซอฟต์แวร์ระบบจัดการฐานข้อมูล (Enterprise Edition) พร้อมสิทธิ์ในการใช้งานที่เป็นแบบถาวร (Perpetual License) จำนวน ๖ Licenses โดยมีคุณลักษณะเฉพาะอย่างน้อยดังนี้

๕.๑.๑ เป็นระบบจัดการฐานข้อมูลเชิงสัมพันธ์ที่สนับสนุนการทำงานแบบออบเจ็กต์ (Object-Relational Database Management System)

๕.๑.๒ สามารถทำการเก็บข้อมูลและแสดงผลได้ทั้งภาษาไทยและภาษาอังกฤษมีระบบจัดเรียงลำดับภาษาไทย โดยโปรแกรมในการเรียงลำดับ (Sort) จะมีอยู่ใน Kernel

๕.๑.๓ ผู้ดูแลระบบสามารถกำหนดจำนวน CPU ที่ฐานข้อมูลหนึ่งๆ สามารถใช้งานได้ในระดับ Parameter ของฐานข้อมูล เพื่อให้สามารถเพิ่มหรือลดจำนวน CPU ที่ฐานข้อมูลต้องการใช้งานในขณะนั้นได้ตรงตามความต้องการ

๕.๑.๔ สามารถทำการเก็บผลลัพธ์ที่ได้จากการส่งคำสั่ง SQL ไว้ในหน่วยความจำของฐานข้อมูล (Query Result Cache) เพื่อให้สามารถนำผลลัพธ์นั้นมาใช้ได้ในทันทีโดยไม่ต้องทำการคำนวณ, ค้นหาผลลัพธ์จากฐานข้อมูลใหม่อีกครั้งหนึ่ง

๕.๑.๕ สามารถสนับสนุนการทำงานแบบ Parallel โดยสามารถปรับเงื่อนไขของจำนวน Parallel ได้โดยอัตโนมัติ โดยดูจากขนาดของ object, ความยากง่ายของ SQL Statement, Hardware Resource

๕.๑.๖ มีเครื่องมือในการเปรียบเทียบข้อมูลของแต่ละ schema ในหลาย ๆ database ได้ รวมไปถึง object ต่าง ๆ ในระบบ database, สามารถคัดลอก object ต่าง ๆ ข้าม schema หรือ ข้าม database ได้ โดยระบบหรือกระบวนการต้องสามารถมี option ให้สามารถคัดลอกได้ทั้งหมด หรือ แค่บางส่วน

๕.๒ ซอฟต์แวร์การปกปิดข้อมูล (Data Masking) พร้อมสิทธิ์ในการใช้งานที่เป็นแบบถาวร (Perpetual License) โดยมีคุณลักษณะเฉพาะอย่างน้อยดังนี้

๕.๒.๑ สามารถปิดบัง (Masking) ข้อมูลด้วยเทคนิคต่าง ๆ โดยไม่จำเป็นต้องแก้ไขหรือพัฒนาโปรแกรมเพิ่มเติม ได้อย่างน้อยดังนี้

๑) สามารถปกปิด (Masking) แบบสุ่มสลับตัวอักษรในชุดข้อมูลได้ (Shuffle Masking)

๒) สามารถปกปิด (Masking) แบบเข้ารหัสได้ (Encryption) เช่น เข้ารหัสข้อมูลส่วนบุคคล

๓) สามารถปกปิด (Masking) แบบสุ่มข้อมูลที่มีแบบแผนได้ (Formation Preserving Randomization) เช่น สุ่มข้อมูลตามตำแหน่ง, ตามความยาวที่กำหนดของตัวอักษร

๔) สามารถปกปิด (Masking) แบบตามเงื่อนไขได้ (Conditional Masking)

๕) สามารถปกปิด (Masking) แบบเลือกเป็นกลุ่มได้ (Compound Masking) เช่น ปกปิดกลุ่มของ columns ชื่อ และ สกุล ด้วยวิธีสุ่ม เป็นต้น

๖) สามารถปกปิด (Masking) แบบให้ผลลัพธ์ที่มีความเหมือนกันแบบสม่ำเสมอสำหรับข้อมูลต้นทางเดียวกัน (Deterministic Masking)

๗) สามารถปกปิด (Masking) แบบตามเงื่อนไขได้แบบทำในลักษณะ scripts ได้ (User-defined PL/SQL Masking)

๕.๒.๒ สามารถทอน (Subsetting) ข้อมูล โดยสามารถกำหนดเงื่อนไขในการทอนข้อมูล ได้ดังนี้

๑) อัตราส่วนปริมาณของข้อมูล

๒) ตามช่วงเวลาที่กำหนด

๓) ตาม Column ของตาราง

๕.๒.๓ สามารถกำหนดหรือค้นหาความสัมพันธ์แบบ Parent-Child Relationship ของข้อมูลที่เป็น Sensitive Dataได้

๕.๒.๔ สามารถกำหนดการทำงานในลักษณะการทำซ้ำ (Clone) และการปิดบังข้อมูล (Masking) ภายในกระบวนงานเดียวได้

๕.๒.๕ สามารถบริหารจัดการการปิดบัง และทอนข้อมูลแบบรวมศูนย์ได้ผ่าน GUI และ Command Line

๕.๒.๖ มีลิขสิทธิ์ซอฟต์แวร์แบบ Perpetual License และมีสิทธิการใช้งานแบบไม่จำกัดจำนวนผู้ใช้ ครอบคลุมการทำงานของจำนวนแกนรวมของหน่วยประมวลผล ไม่น้อยกว่า ๑๒ แกน (Processor Cores)

๖. ซอฟต์แวร์การทำ Data Partitioning บนระบบจัดการฐานข้อมูลสำหรับระบบสารสนเทศเพื่อการบริหาร (MIS) พร้อมสิทธิ์ในการใช้งานที่เป็นแบบถาวร (Perpetual License) โดยมีคุณสมบัติเฉพาะอย่างน้อยดังนี้

๖.๑ สามารถแบ่ง Table เป็นส่วนย่อย ๆ (Partitions) ไว้ใช้จัดการ Table และ Index ที่มีขนาดใหญ่ โดยที่การเข้าถึงข้อมูลยังทำได้โดยไม่ต้องเปลี่ยนแปลงคำสั่ง SQL เพื่อทำให้การ Access ข้อมูลทำได้เร็วขึ้น

๖.๒ สามารถ Off-line ข้อมูลบางส่วนของ Table เพื่อทำการ Backup หรือลบข้อมูลโดยที่ผู้ใช้ยังสามารถเข้าถึงข้อมูลส่วนอื่นของ Table ได้

๖.๓ การกำหนดการแบ่ง Partition ต้องสามารถรองรับการแบ่ง partition ได้ดังต่อไปนี้ ได้เป็นอย่างน้อย

๑) กำหนดการแบ่ง Partition โดยใช้การกำหนดช่วงของข้อมูลในแต่ละ Partition (Range Partitioning)

๒) กำหนดการแบ่ง Partition โดยใช้การกำหนดค่าของข้อมูลในแต่ละ Partition (List Partitioning)

๓) กำหนดการแบ่ง Partition โดยใช้ Hash Function (Hash Partitioning)

๔) กำหนดการแบ่ง Partition โดยใช้ Range Partitioning ผสมกับ Hash Partitioning หรือ List Partitioning หรือ Range Partitioning ผสมกับ Range Partitioning หรือ List Partitioning ผสมกับ List Partitioning (Composite Partitioning)

๖.๔ สามารถรวม (Merge) หรือ แบ่ง (Split) Partition ได้แบบ Online

๖.๕ สามารถสร้าง Partition Index ทั้งในระดับ Table (Global Partition Index) และ Index ระดับ Partition (Local Partition Index)

๖.๖ สามารถสร้าง Index (Merge) หรือแบ่ง (Split) Partition ได้แบบ Online

๖.๗ สามารถสร้างหรือแบ่ง Range Partition (Range Interval Partitioning) แบบอัตโนมัติ เมื่อมีข้อมูลใหม่เข้ามาแล้วไม่ได้อยู่ในข้อกำหนดของ Range partition

๖.๘ สามารถกำหนดพื้นที่การจัดเก็บข้อมูล (Tablespace) ของแต่ละ Partition แยกกันได้

๖.๙ สามารถสร้าง Hybrid partition Table ที่เรียกดูข้อมูลที่จัดเก็บในฐานข้อมูลและไฟล์นอกฐานข้อมูล โดยต้องรองรับ csv file, Parquet, Hadoop Distributed File System (HDFS) ได้เป็นอย่างน้อย

๖.๑๐ มีลิขสิทธิ์ซอฟต์แวร์แบบ Perpetual License และมีสิทธิการใช้งานแบบไม่จำกัดจำนวนผู้ใช้ ครอบคลุมการทำงานของจำนวนแกนรวมของหน่วยประมวลผลไม่น้อยกว่า ๑๖ แกน (Processor Cores)

๗. การโอนย้ายระบบสารสนเทศเพื่อการบริหาร (MIS)

๗.๑ จัดทำแผนงานการโอนย้ายระบบสารสนเทศเพื่อการบริหาร (MIS) ไปยังเครื่องคอมพิวเตอร์ที่ติดตั้งใหม่ในโครงการ

๗.๒ ดำเนินการโอนย้ายระบบสารสนเทศเพื่อการบริหาร (MIS) ที่ใช้อยู่ในปัจจุบันไปยังเครื่องคอมพิวเตอร์ที่ติดตั้งใหม่ โดยการโอนย้ายต้องไม่ส่งผลกระทบต่อการใช้งานระบบสารสนเทศเพื่อการบริหาร (MIS) ของผู้ใช้งาน

.....ประธาน.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการและเลขานุการ

เอกสารแนบ ๒
รายละเอียดการดำเนินการโครงการ

๑. การบริหารงานโครงการ

๑.๑ ต้องเสนอแผนการดำเนินการโครงการและรายชื่อบุคลากรในการดำเนินการโครงการให้คณะกรรมการตรวจรับพัสดุเห็นชอบก่อนดำเนินการ และคณะกรรมการตรวจรับพัสดุสงวนสิทธิ์ที่จะปรับเปลี่ยนแผนการดำเนินงาน ทีมงาน และบุคลากรได้ตามความเหมาะสมหากพบปัญหาอุปสรรคหรือมีเหตุทำให้ไม่สามารถดำเนินการได้ตามแผน และต้องปรับปรุงและเสนอแผนการดำเนินงานใหม่ ให้คณะกรรมการตรวจรับพัสดุพิจารณาเห็นชอบ

๑.๒ ต้องจัดทำแผนการดำเนินการโครงการ (Project Plan) ให้เป็นไปตามกรอบระยะเวลาที่กำหนด โดยแผนการดำเนินงานโครงการต้องประกอบไปด้วยแผนการดำเนินการอย่างน้อยดังนี้

๑.๒.๑ แผนการดำเนินงานหลัก (Master Plan) ต้องจัดทำในรูปแบบ Gantt Chart โดยจัดทำบนซอฟต์แวร์บริหารโครงการ

๑.๒.๒ กิจกรรมทางด้านเทคนิค อาทิ การเริ่มโครงการ การออกแบบ การจัดเตรียมพื้นที่ การติดตั้ง การทดสอบ การฝึกอบรม การส่งมอบ การให้บริการบำรุงรักษา

๑.๒.๓ กิจกรรมที่ไม่ใช่ด้านเทคนิค อาทิ การประสานงาน การจัดประชุม

๑.๒.๔ สิ่งที่ส่งมอบตามงวดงาน

๑.๒.๕ รายละเอียดของแผนอย่างน้อยต้องระบุ กิจกรรม กำหนดเวลาดำเนินการ ผู้รับผิดชอบและหน่วยงานที่เกี่ยวข้องในแต่ละกิจกรรม

๑.๒.๖ โครงสร้างการบริหารงานโครงการ และจัดสรรบุคลากรตามทีมงาน โดยมีการจัดแบ่งโครงสร้างทีมงานหลักอย่างน้อย ได้แก่ ทีมงานบริหารโครงการ ทีมออกแบบและติดตั้งระบบโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ ทีมทดสอบ เป็นต้น

๑.๒.๗ การบริหารความเสี่ยงโครงการ

๑.๓ ต้องจัดเตรียมระบบหรือโปรแกรมเครื่องมือในรูปแบบของโปรแกรมบนคลาวด์ หรือติดตั้งใช้งานบนเครือข่ายสำหรับติดตามความคืบหน้าและบริหารโครงการ มีลิขสิทธิ์การใช้งานถูกต้องตลอดระยะเวลาโครงการ โดยมีคุณสมบัติอย่างน้อยดังนี้

๑.๓.๑ เป็นเครื่องมือที่ใช้ในการทำงานร่วมกัน ระหว่างคน ระหว่างทีมงาน

๑.๓.๒ สามารถสร้างและจัดการโครงการ

๑.๓.๓ สามารถกำหนดสมาชิกหรือทีมงาน และสามารถมอบหมายงาน

๑.๓.๔ สามารถสร้างและจัดการงานและงานย่อย

๑.๓.๕ สามารถกำหนดระยะเวลาเริ่มและสิ้นสุด

๑.๓.๖ สามารถสนทนาและแสดงความคิดเห็น รวมทั้งดูสถานะงานและโครงการทั้งหมดของทีมในที่เดียว

๑.๓.๗ สามารถแนบไฟล์จากคอมพิวเตอร์, Dropbox, Box, OneDrive หรือ Google Drive ในงานหรือการสนทนาได้

๑.๓.๘ สามารถแสดงในรูปแบบ Dashboard เพื่อแสดงความคืบหน้าเกี่ยวกับโครงการทั้งหมด

๑.๓.๙ สามารถวางแผนแต่ละวันของแต่ละสมาชิกด้วยการจัดลำดับความสำคัญรายการสิ่งที่ต้องทำ

๑.๓.๑๐ สามารถดูรายการงานต่าง ๆ ในปฏิทิน

๑.๓.๑๑ สามารถทำฟังก์ชันค้นหา เพื่อค้นหางานที่ต้องการได้อย่างรวดเร็ว

๑.๓.๑๒ สามารถรับการอัปเดตอัตโนมัติเกี่ยวกับงานที่แต่ละสมาชิกเกี่ยวข้อง

๑.๔ เฝ้าติดตามและรายงานความคืบหน้าตลอดระยะเวลาโครงการให้คณะกรรมการตรวจรับพัสดุทราบ และหากพบปัญหาและอุปสรรคต่าง ๆ ที่อาจเกิดขึ้น จะต้องรายงานและจัดการประชุมผู้เกี่ยวข้องโดยด่วน

๑.๕ การบริหารความเสี่ยง ต้องดำเนินการอย่างน้อย ดังนี้

๑.๕.๑ ต้องเสนอแผนการบริหารความเสี่ยง (Risk Management) ซึ่งระบุความเสี่ยงที่อาจมีผลกระทบต่อผลสำเร็จของโครงการ รวมทั้งไม่เป็นไปตามเกณฑ์ของการส่งมอบ หรือเกิดความล่าช้าจากกำหนดส่งที่ตกลงกันไว้ในสัญญา

๑.๕.๒ ต้องระบุและวิเคราะห์ความเสี่ยงให้ครอบคลุมประเด็นความเสี่ยงอย่างน้อยดังนี้

- ด้านการจัดการความต้องการ
- ด้านข้อกำหนดและข้อเสนอ
- ด้านสถานที่ติดตั้ง
- ด้านหน่วยงานเกี่ยวข้อง
- ด้านเทคโนโลยี
- ด้านกระบวนการทำงานและการอนุมัติงาน
- ด้านเครื่องมือและทรัพยากรโครงการ

๑.๕.๓ ในแผนการบริหารความเสี่ยง (Risk Management) ต้องประเมินระดับโอกาสของความเสี่ยงที่จะเกิดขึ้น การประเมินผลกระทบและระดับผลกระทบของความเสี่ยง การป้องกันและบรรเทาผลกระทบที่จะเกิดขึ้นเป็นประจำอย่างต่อเนื่องตลอดทั้งโครงการ

๒. การออกแบบและการติดตั้ง

๒.๑ ออกแบบการติดตั้งอุปกรณ์คอมพิวเตอร์ ที่ศูนย์คอมพิวเตอร์หลัก (DC) และศูนย์คอมพิวเตอร์สำรอง (DR) ของระบบ New GFMIS Thai โดยต้องดำเนินการอย่างน้อย ดังนี้

๒.๑.๑ สำรวจพื้นที่และจัดทำแผนภาพการออกแบบและติดตั้งอุปกรณ์คอมพิวเตอร์

๒.๑.๒ สำรวจและจัดทำแผนภาพการออกแบบและติดตั้งระบบเครือข่าย

๒.๑.๓ สำรวจและจัดทำ Single Line Diagram สำหรับระบบไฟฟ้าเพื่อการติดตั้งอุปกรณ์

๒.๑.๔ จัดทำเอกสารการออกแบบการติดตั้งอุปกรณ์ ระบบไฟฟ้าและระบบเครือข่าย และต้องได้รับความเห็นชอบจากคณะกรรมการตรวจรับพัสดุก่อนเริ่มดำเนินการติดตั้ง

๒.๒ ต้องดำเนินการจัดเตรียมพื้นที่ (Site Preparation) และติดตั้งอุปกรณ์คอมพิวเตอร์ ที่ศูนย์คอมพิวเตอร์หลัก (DC) และศูนย์คอมพิวเตอร์สำรอง (DR) ของระบบ New GFMIS Thai โดยดำเนินการอย่างน้อยดังนี้

๒.๒.๑ จัดเตรียมพื้นที่โดยการติดตั้งงานระบบไฟฟ้าและระบบเครือข่าย

๒.๒.๒ ติดตั้งและกำหนดค่าอุปกรณ์คอมพิวเตอร์ ซอฟต์แวร์ อุปกรณ์ระบบเครือข่าย และอื่น ๆ ตามรายการที่เสนอให้พร้อมใช้งาน

๒.๓ ต้องเสนอแผนการติดตั้งเครื่องคอมพิวเตอร์ ซอฟต์แวร์และอุปกรณ์ในโครงการทั้งหมดให้คณะกรรมการตรวจรับพัสดุเห็นชอบก่อนดำเนินการ

๒.๔ ต้องส่งมอบลิขสิทธิ์ซอฟต์แวร์ที่ถูกต้องตามกฎหมาย

๒.๕ ต้องติดตั้งเครื่องคอมพิวเตอร์ ซอฟต์แวร์และอุปกรณ์ในโครงการทั้งหมด ให้สามารถรองรับการใช้งานจริงได้ตามวัตถุประสงค์ หรือตามที่คณะกรรมการตรวจรับพัสดุกำหนด และจัดทำเอกสารสรุปผลการติดตั้งอุปกรณ์ในโครงการ

๒.๖ ต้องรับผิดชอบในการจัดหาอุปกรณ์อื่น ๆ ที่จำเป็นเพิ่มเติมให้เพียงพอสำหรับการติดตั้ง ซึ่งรวมถึงระบบคอมพิวเตอร์แม่ข่าย (Server) ระบบฐานข้อมูล ระบบจัดเก็บข้อมูล ซอฟต์แวร์เครื่องมือสำเร็จรูป (System Tools) และลิขสิทธิ์ต่าง ๆเพื่อให้สามารถติดตั้งเครื่องคอมพิวเตอร์และอุปกรณ์รวมทั้งซอฟต์แวร์ต่าง ๆ ได้อย่างครบถ้วนสมบูรณ์และมีประสิทธิภาพ

๒.๗ การติดตั้งต้องไม่กระทบต่อการทำงานของเครื่องคอมพิวเตอร์และอุปกรณ์เดิม หรือก่อให้เกิดความเสียหายแก่สำนักงานปลัดกระทรวงการคลัง และในกรณีที่เกิดความเสียหาย ผู้ขายต้องรับผิดชอบค่าใช้จ่ายที่เกิดขึ้น และต้องดำเนินการให้สามารถใช้งานได้ตามปกติ

๒.๘ ต้องปรับแต่งประสิทธิภาพ (PERFORMANCE TUNING) ของอุปกรณ์ให้ทำงานได้อย่างมีประสิทธิภาพ

๒.๙ ต้องทำ Label ตามรูปแบบที่คณะกรรมการตรวจรับพัสดุกำหนด และติดที่อุปกรณ์ในโครงการทั้งหมด

๒.๑๐ ดำเนินการเปิดใช้งานโหมด Blocking ในอุปกรณ์ Web Application Firewall (WAF) ที่ติดตั้งในโครงการหรือตามที่คณะกรรมการตรวจรับพัสดุกำหนด

๒.๑๑ ต้องดำเนินการทำ Data Masking ข้อมูลสำหรับระบบทดสอบ (Dev/QAS) ของระบบ New GFMIS Thai หรือตามที่คณะกรรมการตรวจรับพัสดุกำหนด

๓. การทดสอบ

๓.๑ ต้องดำเนินการทดสอบเครื่องคอมพิวเตอร์และอุปกรณ์ทั้งหมดหลังติดตั้งเสร็จสิ้น

๓.๒ ต้องจัดทำแผนการทดสอบที่แสดงขั้นตอนการทดสอบโดยละเอียด และต้องได้รับความเห็นชอบจากคณะกรรมการตรวจรับพัสดุก่อนทดสอบ

๓.๓ ต้องจัดเตรียมสภาพแวดล้อมการทดสอบ (Benchmark Test Lab) เพื่อความพร้อมในการทดสอบโดยอย่างน้อยประกอบด้วยข้อมูล ระบบฐานข้อมูล เครื่องคอมพิวเตอร์แม่ข่าย (Server) เครื่องคอมพิวเตอร์ลูกข่าย และอุปกรณ์ที่เกี่ยวข้อง

๓.๔ ต้องจัดหาและติดตั้งอุปกรณ์ หรือซอฟต์แวร์ที่เกี่ยวข้องกับการทดสอบ และหากระหว่างการทดสอบมีอุปกรณ์หรือซอฟต์แวร์ใด ๆ เกิดความชำรุดเสียหาย ต้องจัดหาอุปกรณ์หรือซอฟต์แวร์นั้นมาทดแทนให้ครบถ้วน เพื่อให้เกิดความสมบูรณ์เพียงพอต่อการทดสอบระบบ และหากการทดแทนนั้นมีค่าใช้จ่ายเกิดขึ้นต้องเป็นผู้รับผิดชอบทั้งหมด

๓.๕ ต้องทดสอบสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery Test) โดยจัดทำแผนทดสอบการสำรองข้อมูลและเรียกคืนข้อมูล และต้องได้รับความเห็นชอบจากคณะกรรมการตรวจรับพัสดุก่อนดำเนินการ โดยต้องร่วมทดสอบการสำรองและเรียกคืนข้อมูลร่วมกับเจ้าหน้าที่ที่เกี่ยวข้องเพื่อให้แน่ใจว่าระบบระบบสารสนเทศเพื่อการบริหาร (MIS) สามารถคืนสู่สภาวะปกติและทำงานได้อย่างต่อเนื่อง

๓.๖ ต้องทดสอบย้ายการทำงานของระบบ (Switch Over Test) โดยจัดทำแผนทดสอบการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และระบบเครือข่าย รวมถึงอุปกรณ์อื่น ๆ ที่เกี่ยวข้องโดยต้องได้รับความเห็นชอบจากคณะกรรมการตรวจรับพัสดุ เพื่อให้มั่นใจว่าระบบสารสนเทศเพื่อการบริหาร (MIS) สามารถย้ายการทำงานจากที่หนึ่งไปยังอีกที่หนึ่งได้ โดยระบบยังสามารถงานได้อย่างต่อเนื่องและมีประสิทธิภาพ

.....ประธาน.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการและเลขานุการ

๔. การทดสอบการเข้าถึงและความมั่นคงปลอดภัยระบบ (Security Test)

การทดสอบการเข้าถึงและความมั่นคงปลอดภัยระบบ (Security Test) เพื่อประเมินสถานะความมั่นคงปลอดภัย ลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสารและไซเบอร์ และเตรียมความพร้อมในการรับมือกับภัยคุกคามดังกล่าวที่อาจเกิดขึ้นในโครงการด้วยวิธีการทดสอบช่องโหว่และบุกรุกระบบ (Vulnerability Assessment & Penetration Testing) โดยการจ้างผู้เชี่ยวชาญภายนอกเข้ามาตรวจสอบ (๓rd Party Auditor)

๔.๑ ความต้องการทั่วไป

๔.๑.๑ ต้องจ้างผู้เชี่ยวชาญภายนอกเข้ามาตรวจสอบ (๓rd Party Auditor) ซึ่งมีความเชี่ยวชาญเฉพาะและมีอาชีพในด้านการทดสอบช่องโหว่และบุกรุกระบบ โดยต้องได้รับความเห็นชอบในทีมงานผู้เชี่ยวชาญจากคณะกรรมการตรวจรับพัสดุก่อน เพื่อดำเนินการการทดสอบการเข้าถึงและความมั่นคงปลอดภัยระบบ (Security Test) ด้วยวิธีการทดสอบช่องโหว่และบุกรุกระบบ Vulnerability Assessment & Penetration Testing) ตามมาตรฐาน ISO/IEC ๒๗๐๐๑

๔.๑.๒ ผู้เชี่ยวชาญภายนอกต้องดำเนินการทดสอบการเข้าถึงและความมั่นคงปลอดภัยระบบ (Security Test) ในช่วงการส่งมอบระบบจนมั่นใจว่าระบบไม่มีช่องโหว่และโอกาสการบุกรุกระบบ ที่มีความเสี่ยงในระดับปานกลางและสูง

๔.๒ ความต้องการด้านเทคนิคการทดสอบการเข้าถึงและความมั่นคงปลอดภัยระบบ

๔.๒.๑ ต้องตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Vulnerability Assessment) จากเครือข่ายภายในและภายนอกของระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ใหม่ (New GFMIS Thai) โดยการดำเนินการจะต้องใช้เครื่องมือตรวจสอบ (Scanning Tool) จำนวนไม่น้อยกว่า ๒ ชนิด และดำเนินการวิเคราะห์ผลการตรวจสอบเปรียบเทียบทุกเครื่องมือ รวมถึงเชื่อมโยงช่องโหว่ที่ตรวจพบกับมาตรฐาน Common Vulnerabilities Scoring System (CVSS) และ CIS Critical Security Controls (Top ๒๐) เวอร์ชันล่าสุด รวมทั้งจัดทำรายงานวิเคราะห์ผลการตรวจสอบ คำแนะนำการปรับปรุงระบบหรือการแก้ไขปิดช่องโหว่ที่ตรวจพบ จัดลำดับความเสี่ยงที่ต้องเร่งดำเนินการแก้ไข และดำเนินการแก้ไขปิดช่องโหว่ที่ตรวจพบ

๔.๒.๒ ในการทดสอบการเข้าถึงและความมั่นคงปลอดภัยระบบ (Security Test) แต่ละครั้ง ต้องจัดทำรายงานผลการดำเนินการตรวจสอบช่องโหว่ที่สำคัญ (Vulnerability Assessment) ซึ่งประกอบด้วยรายละเอียดดังนี้

๑) สรุปผลการดำเนินการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญและการจัดลำดับความเสี่ยงที่ต้องเร่งดำเนินการแก้ไข

๒) สรุปผลการตรวจสอบจากการใช้เครื่องมือตรวจสอบ (Scanning Tool)

๓) สรุปการดำเนินการแก้ไขปิดช่องโหว่ที่ตรวจพบ

๔.๒.๓ การทดสอบด้านความมั่นคงปลอดภัยระบบสำหรับการทำ Data Masking ต้องดำเนินการอย่างน้อยดังนี้

๔.๒.๓.๑ ทดสอบความปลอดภัยของข้อมูลที่ถูกปกปิด (Mask) ดังนี้

๑) ตรวจสอบความถูกต้องของการ Mask ข้อมูลตามนโยบายที่กำหนด (Data Masking Policy) เช่น การสุ่มข้อมูล (Randomization) หรือการแปลงข้อมูล (Transformation) ไม่สามารถย้อนกลับได้

๒) ตรวจสอบว่าข้อมูลที่ Mask แล้วไม่มีข้อมูลจริงหลุดออกมา

๔.๒.๓.๒ ทดสอบความปลอดภัยของการเข้าถึงข้อมูล (Access Control) ดังนี้

๑) ตรวจสอบการกำหนดสิทธิ์ผู้ใช้งาน (User Privileges) ให้เหมาะสม เช่น ผู้ดูแลระบบ (Admin) กับผู้ใช้งานทั่วไป (End-User)

๒) ทดสอบการป้องกันการเข้าถึงข้อมูลต้นฉบับ (Unmasked Data) โดยไม่ได้รับอนุญาต

๔.๒.๓.๓ ทดสอบกระบวนการ Mask ข้อมูล ดังนี้

๑) ทดสอบการตั้งค่า Masking Templates ว่าสามารถใช้งานได้อย่างถูกต้อง

๒) ตรวจสอบกระบวนการ Masking ว่าไม่มีผลกระทบต่อการทำงานปกติของระบบ (Non-Disruptive Operation)

๓) ทดสอบการบันทึกและการรายงาน (Audit Logs) เพื่อให้สามารถตรวจสอบย้อนหลังได้

๔.๒.๓.๔ ทดสอบประสิทธิภาพ (Performance Testing) ดังนี้

๑) ทดสอบว่าระบบยังคงทำงานได้อย่างมีประสิทธิภาพภายใต้การใช้งาน Masking ในฐานข้อมูลขนาดใหญ่

๔.๒.๓.๕ ทดสอบความสอดคล้องกับกฎหมายและมาตรฐาน ดังนี้

๑) ตรวจสอบว่ากระบวนการ Mask ข้อมูลเป็นไปตามข้อกำหนดของกฎหมาย เช่น PDPA (Personal Data Protection Act)

๒) ตรวจสอบว่าระบบรองรับการตรวจสอบตามมาตรฐานความปลอดภัย ISO/IEC ๒๗๐๐๑

๔.๒.๓.๖ ทดสอบการบูรณาการระบบ (Integration Testing) ดังนี้

๑) ทดสอบความเข้ากันได้กับระบบฐานข้อมูลอื่น ๆ

๒) ตรวจสอบว่าการ Mask ข้อมูลไม่กระทบต่อการทำงานของแอปพลิเคชันที่เชื่อมต่อ

๕. จัดทำแนวทางการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ

จัดทำแนวทางการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทางของมาตรฐานสากล ISO/IEC ๒๗๐๐๑ และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ โดยมีขอบเขตครอบคลุมระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ใหม่ (New GFMIS Thai) ระบบสารสนเทศการเงินการคลังเพื่อรองรับองค์กรปกครองส่วนท้องถิ่น ระบบการเชื่อมโยงระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ใหม่ (New GFMIS Thai) กับระบบบัญชีคอมพิวเตอร์ขององค์กรปกครองส่วนท้องถิ่น (e-LAAS) โครงการเพิ่มประสิทธิภาพการรักษาความมั่นคงปลอดภัยของข้อมูลและป้องกันภัยทางไซเบอร์ระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ใหม่ สำนักงานปลัดกระทรวงการคลัง แขวงพญาไท เขตพญาไท กรุงเทพมหานคร และระบบอื่น ๆ ที่เกี่ยวข้อง โดยมีรายละเอียดอย่างน้อยดังนี้

๕.๑ จัดทำบัญชีทรัพย์สิน (Asset Inventory) และรวบรวมข้อมูลที่เกี่ยวกับทรัพย์สินทั้งหมด โดยต้องกำหนดค่า CIA (Confidential, Integrity, Available) ของทรัพย์สินทั้งหมด เพื่อใช้ในการวิเคราะห์ความเสี่ยง (Risk Assessment)

๕.๒ จัดทำการแนวทางบริหารความเสี่ยง (Risk Management) และประเมินความเสี่ยง (Risk Assessment) ตามบัญชีทรัพย์สิน และจัดทำแผนจัดการความเสี่ยง (Risk Mitigation Plan)

๕.๓ จัดทำ Logical Diagram โดยครอบคลุมระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ใหม่ (New GFMIS Thai) ระบบสารสนเทศการเงินการคลังเพื่อรองรับองค์กรปกครองส่วนท้องถิ่น ระบบการเชื่อมโยงระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ใหม่ (New GFMIS Thai) กับระบบบัญชีคอมพิวเตอร์ขององค์กรปกครองส่วนท้องถิ่น (e-LAAS) และโครงการเพิ่มประสิทธิภาพการรักษาความมั่นคงปลอดภัยของข้อมูลและป้องกันภัยทางไซเบอร์ระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ใหม่ สำนักงานปลัดกระทรวงการคลัง แขวงพญาไท เขตพญาไท กรุงเทพมหานคร

เอกสารแนบ ๓
รายละเอียดการฝึกอบรมและเอกสารต่าง ๆ

๑. การฝึกอบรม

๑.๑ ต้องจัดทำรายละเอียดหลักสูตรการฝึกอบรมและแผนการฝึกอบรม เสนอคณะกรรมการตรวจรับพัสดุเห็นชอบก่อนทุกหลักสูตร โดยมีรายละเอียดประกอบด้วย

(๑) หัวข้อการฝึกอบรม
(๒) วัตถุประสงค์และเป้าหมาย
(๓) กลุ่มผู้เข้าฝึกอบรม
(๔) คุณสมบัติผู้เข้าฝึกอบรม
(๕) วิทยากร/ผู้ช่วยวิทยากร
(๖) ระยะเวลาการฝึกอบรม
(๗) รายละเอียดเนื้อหาการฝึกอบรม

หากคณะกรรมการตรวจรับพัสดุพิจารณาแล้วเห็นว่า การปฏิบัติงานของบุคลากรผู้ให้การฝึกอบรมไม่เป็นที่น่าพอใจ ผู้เข้ารับการฝึกอบรมไม่มีความเข้าใจ หรือไม่สามารถนำไปปฏิบัติงานได้ คณะกรรมการตรวจรับพัสดุขอสงวนสิทธิ์ที่จะขอเปลี่ยนแปลงตัวบุคลากรที่ให้การฝึกอบรมได้ หรือ ปรับปรุงเนื้อหาการฝึกอบรม และดำเนินการจัดให้มีการฝึกอบรมใหม่ได้อีกครั้ง โดยต้องรับผิดชอบค่าใช้จ่ายและจะนำมาเป็นเหตุข้ออ้างในการล่าช้าของงานไม่ได้

๑.๒ ต้องรับผิดชอบค่าใช้จ่ายทั้งหมดในการฝึกอบรม ได้แก่

(๑) เอกสารการฝึกอบรม (Hard Copy) ให้ผู้เข้าอบรม ๑ ชุด ต่อ ๑ คน อุปกรณ์ต่าง ๆ ที่ใช้ในการฝึกอบรม
(๒) อาหารว่างและเครื่องดื่ม และอาหารสำหรับผู้เข้าอบรม และผู้เข้าร่วมประชุมที่เกี่ยวข้อง
(๓) จัดฝึกอบรมในช่วงระยะเวลาที่กำหนด โดยจะต้องจัดเตรียมสถานที่ฝึกอบรมที่ได้มาตรฐานเพื่อใช้สำหรับการฝึกอบรมพร้อมรถรับ-ส่งผู้อบรม หรือหากสามารถจัดอบรม ณ สถานที่ภายในกระทรวงการคลังได้ จะต้องรับผิดชอบค่าเช่าสถานที่ ค่าเช่าอุปกรณ์และเครื่องมือทั้งหมด หรือตามที่คณะกรรมการตรวจรับพัสดุกำหนด
(๔) จัดเตรียมเครื่องคอมพิวเตอร์ และอุปกรณ์อื่น ๆ สำหรับการฝึกอบรม พร้อมติดตั้ง ซอฟต์แวร์/โปรแกรมที่จำเป็นต้องใช้ หรือตามที่คณะกรรมการตรวจรับพัสดุกำหนด

๑.๓ ต้องอบรมวิธีการปฏิบัติงาน/การใช้งาน เครื่องคอมพิวเตอร์และอุปกรณ์ที่จัดหาในโครงการ แก่ผู้ดูแลระบบ

๑.๔ ต้องอบรมเกี่ยวกับการใช้งานสำหรับปรับปรุงระบบการติดตั้ง การตรวจสอบ Driver ต่าง ๆ ในโครงการและระบบที่เกี่ยวข้อง แก่ผู้ดูแลระบบ

๑.๕ ต้องอบรมการใช้งานซอฟต์แวร์ที่ติดตั้งในโครงการทั้งหมด

๑.๖ วิทยากรที่ฝึกอบรม ต้องเป็นผู้เชี่ยวชาญของบริษัทที่เป็นเจ้าของผลิตภัณฑ์/ระบบที่พัฒนา หรือวิทยากรจากสถาบันการศึกษาที่ได้รับลิขสิทธิ์การสอนจากเจ้าของผลิตภัณฑ์/ระบบที่พัฒนา หรือเป็นวิทยากรผู้มีความรู้ความเชี่ยวชาญเป็นอย่างดี และมีความรู้ความเข้าใจในเนื้อหาและการทำงานของระบบงานที่ได้ทำการพัฒนาและติดตั้งให้กับสำนักงานปลัดกระทรวงการคลังเป็นอย่างดี

๑.๗ ต้องจัดทำคู่มือสำหรับการฝึกอบรมทุกหลักสูตร

๑.๘ ต้องจัดทำสื่อการเรียนการสอนในรูปแบบของ Training Video พร้อมเอกสารประกอบ เพื่อเป็นประโยชน์สำหรับผู้เข้าอบรมให้สามารถนำมาศึกษาทบทวน เรียนรู้ใหม่ในภายหลัง หรือใช้เป็นสื่อการเรียนการสอนสำหรับผู้ที่จะมาปฏิบัติงานใหม่ ยกเว้นคอร์สอบรมโดยศูนย์อบรมภายนอกที่ได้รับการรับรองจากหลักสูตร (Certified Training Center)

.....ประธาน.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการและเลขานุการ

๑.๙ ต้องจัดฝึกอบรม โดยหลักสูตรที่จัดฝึกอบรม ประกอบด้วยหลักสูตรอย่างน้อยดังนี้ ทั้งนี้ จำนวนผู้เข้ารับการอบรมและระยะเวลาการอบรมสามารถปรับเปลี่ยนเพิ่มลดได้ตามความเหมาะสม

หลักสูตรการอบรม	กลุ่มของผู้เข้ารับการอบรม	รูปแบบการอบรม	จำนวนผู้เข้าอบรม	ระยะเวลาการอบรม
๑) การใช้งานเครื่องมือและซอฟต์แวร์ต่าง ๆ ที่ใช้ในโครงการ	ผู้ดูแลระบบ / เจ้าหน้าที่ทางเทคนิค (IT)	ห้องอบรมหรือออนไลน์ พร้อม VDO และสื่อการสอน	๑๐ คน	ตามมาตรฐานของเครื่องมือที่กำหนด
๒) การติดตั้งเครื่องคอมพิวเตอร์และอุปกรณ์ที่เสนอในโครงการ	ผู้ดูแลระบบ / เจ้าหน้าที่ทางเทคนิค (IT)	ห้องอบรมหรือออนไลน์ พร้อม VDO และสื่อการสอน	๑๐ คน	๕ วัน
๓) การทำงานของซอฟต์แวร์การปกปิดข้อมูล (Data Masking)	ผู้ดูแลระบบ / ผู้ใช้งานหลัก (Super User)	ห้องอบรมหรือออนไลน์ พร้อม VDO และสื่อการสอน	๑๐ คน	๑ วัน
๔) การทำงานของซอฟต์แวร์การทำ Data Partitioning	ผู้ดูแลระบบ / ผู้ใช้งานหลัก (Super User)	ห้องอบรมหรือออนไลน์ พร้อม VDO และสื่อการสอน	๑๐ คน	๑ วัน
๕) หลักสูตร ISO/IEC ๒๗๐๐๑:๒๐๒๒ Internal Audit	กลุ่มเจ้าหน้าที่ด้านเทคนิค (IT)	ศูนย์อบรมภายนอกที่ได้รับการรับรองจากหลักสูตร (Certified Training Center)	๖ คน	๒ วัน

หมายเหตุ: หลักสูตรการฝึกอบรมด้านการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศตามหลักสูตรอบรมลำดับที่ ๕) ให้รวมค่าใช้จ่ายในการสอบเพื่อรับประกาศนียบัตรตามหลักสูตรนั้น (ถ้ามี) อย่างน้อย ๑ ครั้ง

๒. เอกสารต่าง ๆ

ต้องส่งมอบเอกสารและคู่มือต่าง ๆ ดังต่อไปนี้

๒.๑ เอกสารรายการเครื่องคอมพิวเตอร์และอุปกรณ์ที่เกี่ยวข้อง (System Architecture) Software พร้อมสิทธิ์การใช้งาน

๒.๒ เอกสารและคู่มือระบบงานต่าง ๆ อย่างน้อย ดังนี้

๒.๒.๑ คู่มือการติดตั้งซอฟต์แวร์หรือระบบ (System & Component Installation)

๒.๒.๒ คู่มือการตั้งค่าระบบ (System, Network & Security Configuration (Default & Customize))

๒.๒.๓ คู่มือ Operation Procedure

๒.๒.๔ คู่มือการเปิดและปิดระบบ

๒.๒.๕ คู่มือการตรวจสอบระบบ (Monitor) และการใช้งาน Monitoring Tool

๒.๒.๖ งานที่ต้องปฏิบัติงานเป็นประจำ (Routine Job)

๒.๒.๗ งานบำรุงรักษาและปรับแต่งระบบ (House Keeping Job)

๒.๒.๘ คู่มือสำหรับผู้ดูแลระบบ (Operation Manual)

๒.๒.๙ คู่มือการใช้งานซอฟต์แวร์การปกปิดข้อมูล (Data Masking)

๒.๒.๑๐ คู่มือการสำรองข้อมูล (Backup & Recovery)

เอกสารแนบ ๔
การบำรุงรักษาและซ่อมแซมแก้ไข

ต้องดำเนินการบำรุงรักษา ซ่อมแซม แก้ไข หรือเปลี่ยนแทน สำหรับโครงการเพิ่มประสิทธิภาพการรักษาความมั่นคงปลอดภัยของข้อมูลและป้องกันภัยทางไซเบอร์ระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ใหม่ สำนักงานปลัดกระทรวงการคลัง แขวงพญาไท เขตพญาไท กรุงเทพมหานคร นับถัดจากวันที่ตรวจรับงานงวดสุดท้ายเสร็จสมบูรณ์ทั้งหมด โดยไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้น โดยต้องปฏิบัติตามเงื่อนไขดังต่อไปนี้

๑. การบำรุงรักษา

๑.๑ ต้องทำการบำรุงรักษาซ่อมแซมแก้ไขอุปกรณ์คอมพิวเตอร์ในโครงการทั้งหมด นับถัดจากวันที่ตรวจรับงานงวดสุดท้ายเสร็จสมบูรณ์ทั้งหมด เป็นระยะเวลา ๒ ปี โดยไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้นจากสำนักงานปลัดกระทรวงการคลัง

๑.๒ ต้องรับประกันซอฟต์แวร์เป็นระยะเวลา ๑ ปี นับถัดจากวันที่ตรวจรับงานงวดสุดท้ายเสร็จสมบูรณ์ทั้งหมด

๑.๓ ต้องดำเนินการให้มีการรับประกันอุปกรณ์คอมพิวเตอร์และซอฟต์แวร์ที่เกี่ยวข้อง มีบริการสนับสนุนหลังการขาย ณ สถานที่ติดตั้ง (On-Site Service) แบบ ๒๔ ชั่วโมง x ๗ วัน

๑.๔ ต้องส่งแผนการบำรุงรักษา Preventive Maintenance ก่อนทำการบำรุงรักษา Preventive Maintenance

๑.๕ ต้องทำการบำรุงรักษา Preventive Maintenance เครื่องคอมพิวเตอร์หรืออุปกรณ์ที่เกี่ยวข้องอย่างน้อย ๓ เดือนต่อ ๑ ครั้ง โดยจะต้องแจ้งรายละเอียดดังนี้

๑.๕.๑ งวดงานที่บำรุงรักษา

๑.๕.๒ ชื่อรายการที่ทำ Preventive Maintenance

๑.๕.๓ เวลาและสถานที่ทำ Preventive Maintenance

๑.๕.๔ วิธีการ/ขั้นตอนของการทำ Preventive Maintenance

๑.๕.๕ วิธีการทดสอบการทำงานหลังทำ Preventive Maintenance เรียบร้อย

๑.๖ แผนการบำรุงรักษา Preventive Maintenance จะต้องไม่กระทบกระเทือนต่อการปฏิบัติงานของเจ้าหน้าที่ผู้ใช้งานระบบคอมพิวเตอร์

๑.๗ ในช่วงระยะเวลารับประกัน จะต้องดำเนินการบำรุงรักษาระบบ ดังนี้

๑.๗.๑ ต้องมีเจ้าหน้าที่ทางเทคนิคหรือผู้เชี่ยวชาญเฉพาะ เพื่อให้คำปรึกษาได้ตลอด ๒๔ ชั่วโมง ในกรณีที่มีความจำเป็นเร่งด่วน ต้องส่งเจ้าหน้าที่เข้ามาดำเนินการ ณ สถานที่ติดตั้งระบบตลอดระยะเวลาการรับประกัน

๑.๗.๒ การรับแจ้งเหตุขัดข้อง (Incident Management) และการแก้ไขปัญหา (Problem Management)

๑) ต้องจัดหาศูนย์บริการรับและแก้ไขปัญหาเหตุขัดข้องของระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศให้กับสำนักงานปลัดกระทรวงการคลัง เพื่อให้สามารถแจ้งเหตุขัดข้องได้ทั้งในเวลาและนอกเวลาราชการตลอด ๒๔ ชั่วโมง โดยทางโทรศัพท์ (Hot Line) โทรสาร เว็บไซต์ และระบบสารสนเทศเพื่อการบริหารจัดการการรับแจ้งเหตุขัดข้อง (Help Desk System) เมื่อพบความไม่สะดวกความขัดข้องไม่สามารถใช้งานระบบได้ตามปกติหรือพบความล้มเหลว เพื่อให้ผู้แจ้งบันทึกคำร้องขอให้แก้เหตุขัดข้องดังกล่าว ไว้เป็นหลักฐานทั้งสองฝ่าย รวมทั้งสามารถตรวจสอบ

สถานะความคืบหน้าของการให้บริการได้ และมีระบบฐานข้อมูลอุปกรณ์ครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วงที่อยู่ในสัญญาบำรุงรักษาและซ่อมแซมแก้ไข สำหรับเก็บประวัติ (Log Book) การซ่อมบำรุงอุปกรณ์เหล่านั้น

๒) ทุกครั้งที่มีการให้บริการต่าง ๆ กับสำนักงานปลัดกระทรวงการคลัง ต้องจัดทำเอกสารการให้บริการ ซึ่งระบุถึงวัน เวลาและสถานที่ วัตถุประสงค์ และกิจกรรมการให้บริการ รวมถึงรายการอุปกรณ์คอมพิวเตอร์ อุปกรณ์ต่อพ่วงและอุปกรณ์อื่น ๆ ที่ต้องนำเข้าและออกจากสถานที่ เพื่อนำไปแก้ไขซ่อมแซม การเปลี่ยนทดแทน หรือกิจกรรมอื่น ๆ เพื่อให้เจ้าหน้าที่ที่ได้รับมอบหมายลงนามรับทราบและอนุมัติก่อนการดำเนินการ โดยจะต้องมอบสำเนาเอกสารการให้บริการดังกล่าว ให้กับหน่วยงานจัดเก็บไว้เพื่อเป็นหลักฐานอ้างอิงต่อไป

๓) ต้องจำแนกประเภทของการรับแจ้ง จำแนกประเภทของเหตุขัดข้องตามประเภทการใช้งานได้

๔) เจ้าหน้าที่ผู้รับเรื่องต้องพยายามแก้ไขเหตุขัดข้องที่เกิดขึ้นทันทีที่การแจ้งเหตุขัดข้องถูกบันทึกลงในระบบ Help Desk รวมทั้งให้คำแนะนำในการตรวจสอบสาเหตุและการแก้ไขปัญหาเบื้องต้นให้แก่ผู้แจ้งเหตุได้

๕) ต้องบันทึกรายละเอียดขั้นตอนสถานะการแก้ไขเหตุขัดข้อง ระยะเวลาดำเนินการในแต่ละขั้นตอน อย่างชัดเจน

๖) ในการแก้ไขเหตุขัดข้อง ต้องถ่ายโอนข้อมูลจากฐานข้อมูลสำรองเพื่อให้ระบบสามารถดำเนินการได้อย่างต่อเนื่อง

๗) เมื่อดำเนินการแก้ไขเหตุขัดข้องแล้ว ต้องนำผลการดำเนินการเข้าสู่ระบบ Help Desk และยืนยันว่าเหตุขัดข้องนั้นได้รับการแก้ไขให้กับผู้แจ้งเหตุแล้ว เมื่อผู้แจ้งเหตุยืนยันผลการแก้ไขเรียบร้อยและระบบกลับเข้าสู่สถานะของการใช้งานได้ปกติ ต้องดำเนินการปรับปรุงสถานะของเหตุการณ์ในระบบให้เป็น “ปิด”รวมทั้งบันทึกสาเหตุ (Root Cause) ของเหตุขัดข้อง และวิธีการแก้ไข

๘) ต้องวิเคราะห์เหตุขัดข้องต่าง ๆ ซึ่งรวมถึงกรณีมีเหตุขัดข้องเดิมที่เกิดขึ้นซ้ำ เพื่อหาแนวทางป้องกันในการแก้ไขเหตุขัดข้องอย่างถาวร

๙) จัดทำรายงานสรุปผลการรับแจ้งเหตุขัดข้อง (Incident Management) และการแก้ไขปัญหา (Problem Management) เป็นราย ๓ เดือน โดยมีรายละเอียดดังนี้

- รายงานผลการรับแจ้งเหตุขัดข้อง (Incident Management) และการแก้ไขปัญหา (Problem Management)
- รายงานการวิเคราะห์เหตุการณ์ขัดข้อง เพื่อหาแนวทางป้องกัน ในการแก้ไขเหตุขัดข้องอย่างถาวร

.....ประธาน.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการและเลขานุการ

๒. การซ่อมแซมแก้ไข

ต้องดำเนินการซ่อมแซมแก้ไขข้อบกพร่อง หรือเปลี่ยนทดแทน อุปกรณ์คอมพิวเตอร์หรือซอฟต์แวร์ระบบในโครงการ ที่มีความบกพร่องหรือใช้การไม่ได้ โดยความชำรุดนี้มิได้เกิดจากความผิดพลาดของผู้ซื้อ โดยต้องดำเนินการอย่างน้อยดังนี้

๒.๑ ต้องเริ่มดำเนินการแก้ไขซ่อมแซมอุปกรณ์คอมพิวเตอร์ภายใน ๓ ชั่วโมง นับจากที่ได้รับแจ้ง กรณีที่อุปกรณ์คอมพิวเตอร์ไม่สามารถทำงานได้และทำให้ระบบหยุดให้บริการมากกว่า ๒๔ ชั่วโมง ต้องนำอุปกรณ์สำรองที่มีคุณสมบัติและประสิทธิภาพเทียบเท่าหรือดีกว่ามาให้ใช้งานทดแทน

๒.๒ กรณีที่สามารถแก้ไขได้ในทันที ผู้ขายต้องดำเนินการแก้ไขให้แล้วเสร็จภายใน ๖ ชั่วโมง นับตั้งแต่ได้รับแจ้ง หากผู้ขายไม่สามารถดำเนินการแก้ไขภายในเวลาดังกล่าว ผู้ขายต้องถูกปรับในอัตราชั่วโมงละ ๑,๐๐๐ บาท (หนึ่งพันบาทถ้วน) เศษของชั่วโมงนับเป็น ๑ ชั่วโมง ไม่เว้นวันหยุดราชการและวันหยุดตามมติคณะรัฐมนตรี

๒.๓ กรณีที่ไม่สามารถแก้ไขได้ในทันที ผู้ขายต้องจัดหาอุปกรณ์สำรองที่มีคุณสมบัติและประสิทธิภาพเทียบเท่าหรือดีกว่า มาให้ใช้งานทดแทนภายใน ๑๒ ชั่วโมง นับตั้งแต่ได้รับแจ้ง หากผู้ขายไม่สามารถดำเนินการได้ภายในเวลาดังกล่าว ผู้ขายต้องถูกปรับในอัตราชั่วโมงละ ๑,๐๐๐ บาท (หนึ่งพันบาทถ้วน) เศษของชั่วโมงนับเป็น ๑ ชั่วโมง ไม่เว้นวันหยุดราชการและวันหยุดตามมติคณะรัฐมนตรี

๒.๔ จัดหาเครื่องคอมพิวเตอร์แม่ข่ายอุปกรณ์ที่เกี่ยวข้อง และซอฟต์แวร์พร้อมลิขสิทธิ์ ที่มีคุณสมบัติและประสิทธิภาพเทียบเท่าหรือดีกว่า จัดเก็บไว้ในสถานที่ที่พร้อมจะนำมาเพื่อใช้ทดแทนได้ทันที

๒.๕ เมื่อดำเนินการแก้ไขเหตุขัดข้องและแจ้งเหตุขัดข้องนั้นให้กับผู้แจ้งเหตุแล้ว ให้บันทึกสาเหตุ (Root Cause) ของเหตุขัดข้อง และวิธีการแก้ไข ซึ่งรวมถึงกรณีมีเหตุขัดข้องเดิมที่เกิดขึ้นซ้ำ เพื่อหาแนวทางป้องกันในการแก้ไขเหตุขัดข้องอย่างถาวร

๓. แผนการบำรุงรักษาและประมาณการค่าใช้จ่ายการบำรุงรักษา

๓.๑ ต้องจัดทำแผนการบำรุงรักษา ตามขอบเขตข้อ ๑ และ ๒ ให้คณะกรรมการตรวจรับพัสดุเห็นชอบ โดยประกอบด้วยรายละเอียดอย่างน้อยได้แก่

๓.๑.๑ ขั้นตอนและช่องทางการรับแจ้งเหตุขัดข้อง และการแก้ไขปัญหา

๓.๑.๒ ขั้นตอนการบำรุงรักษาในรายละเอียดตามข้อ ๑ และ ๒

๓.๑.๓ แผนงานการบำรุงรักษา Preventive Maintenance พร้อมรายการอุปกรณ์ทั้งหมด และแสดงกิจกรรมการบำรุงรักษาของแต่ละรายการ

๓.๒ ต้องจัดทำรายงานประมาณการค่าใช้จ่ายการบำรุงรักษาอุปกรณ์คอมพิวเตอร์และซอฟต์แวร์จำแนกตามรายการ (Break Down Maintenance Cost) รายปี เป็นระยะเวลา ๕ ปี ภายหลังสิ้นสุดระยะเวลาประกัน ให้คณะกรรมการตรวจรับพัสดุเห็นชอบ โดยประกอบด้วยรายละเอียดอย่างน้อยได้แก่

๓.๒.๑ ประมาณการค่าใช้จ่ายการบำรุงรักษาของอุปกรณ์คอมพิวเตอร์และซอฟต์แวร์จำแนกตามรายการ (Break Down Maintenance Cost) รายปี เป็นระยะเวลา ๕ ปี

๓.๒.๒ ขอบเขตการบำรุงรักษาแต่ละรายการของอุปกรณ์คอมพิวเตอร์และซอฟต์แวร์ตามข้อ ๓.๒.๑

.....ประธาน.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการและเลขานุการ