- ร่าง -

ขอบเขตของงาน (Terms of Reference: TOR)
โครงการปรับปรุงและเพิ่มประสิทธิภาพระบบโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ
ของระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ใหม่

๑. ความเป็นมา

ตามที่กระทรวงการคลังได้จัดทำโครงการพัฒนาระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ใหม่ (New GFMIS Thai) โดยใช้เทคโนโลยีแบบระบบเปิด (Open System) ให้มีประสิทธิภาพ มีความยืดหยุ่น ครอบคลุมการเบิกจ่ายเงินทั่วประเทศ และรองรับการขยายตัวในอนาคต โดยระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ใหม่ (New GFMIS Thai) ถูกกำหนดให้เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ซึ่งต้องปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งปัจจุบันระบบโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศของระบบ New GFMIS Thai ได้รับการรับรองตามมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๒๒ และสำนักงานปลัดกระทรวงการคลัง ได้จัดทำระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๒๒ ซึ่งจากการประเมินความเสี่ยงและประสิทธิภาพของระบบโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศของระบบ New GFMIS Thai พบว่า ๑) เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูลแบบรวมศูนย์มีอายุการใช้งานเกินกว่า ๗ ปี และผลิตภัณฑ์ได้ยุติการสนับสนุน (End of Support: EOS) ซึ่งมีความเสี่ยงต่อการให้บริการจึงมีความจำเป็นต้องจัดหาทดแทน ๒) ระบบการสำรองและกู้คืน (Backup System) มีอายุการใช้งานเกินกว่า ๗ ปี และไม่รองรับการสำรองข้อมูลคอนเทนเนอร์ (Backup Container) ที่จัดเก็บบนระบบ Kubernetes ๓) ระบบการพิสูจน์และยืนยันตัวตน มีข้อจำกัดในการรองรับจำนวนการเข้าใช้งานพร้อมกันของผู้ใช้งานที่เพิ่มขึ้น ๔) การโอนย้ายและปรับปรุงแอปพลิเคชันของระบบ New GFMIS Thai ให้ทันสมัย (Modernization Application) ผ่านแพลตฟอร์ม DevSecOps เพื่อให้แอปพลิเคชันมีมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับการพัฒนาซอฟต์แวร์ด้านการทดสอบและประกันคุณภาพระบบในระดับเดียวกัน ดังนั้น จึงมีความจำเป็นต้องมีการปรับปรุงระบบโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศของระบบ New GFMIS Thai เพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัยและเพิ่มประสิทธิภาพระบบโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ ให้สามารถให้บริการระบบ New GFMIS Thai ได้อย่างต่อเนื่องและมีประสิทธิภาพ

๒. วัตถุประสงค์

๒.๑ เพื่อปรับปรุงและเพิ่มประสิทธิภาพระบบโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศของระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ใหม่ (New GFMIS Thai)

๒.๒ เพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัยของระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ใหม่ (New GFMIS Thai)

๒.๓ เพื่อโอนย้ายและปรับปรุงแอปพลิเคชันของระบบ New GFMIS Thai ไปยัง DevSecOps Platform

๓. เป้าหมาย

ระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ใหม่ (New GFMIS Thai) มีระบบโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศที่ทันสมัย สามารถรองรับการให้บริการระบบ New GFMIS Thai ได้อย่างมีประสิทธิภาพ และรองรับจำนวนผู้ใช้งานที่เพิ่มขึ้นในอนาคต สอดคล้องและเป็นไปตามการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๒๒

๔. คุณสมบัติของผู้ยื่นข้อเสนอ

๔.๑ มีความสามารถตามกฎหมาย

๔.๒ ไม่เป็นบุคคลล้มละลาย

๔.๓ ไม่อยู่ระหว่างเลิกกิจการ

๔.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

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

๔.๑๓ ผู้ยื่นข้อเสนอที่เป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า จะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอไม่ต่ำกว่า ๖๐ ล้านบาท โดยแสดงสำเนาเอกสารหรือหลักฐานมาพร้อมการยื่นข้อเสนอ

๔.๑๔ กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียนหรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง (สินเชื่อที่ธนาคารภายในประเทศหรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์

และประกอบธุรกิจค้าประกันตามประกาศของธนาคารแห่งประเทศไทย 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 โดยเป็นหนังสือที่แต่งตั้งสำหรับโครงการที่เสนอโดยเฉพาะยื่นมาพร้อมกับการยื่นข้อเสนอ

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

๓) อุปกรณ์ทุกชิ้นที่เสนอต้องเป็นของแท้ ของใหม่ ไม่เคยใช้งานมาก่อน ไม่เป็นของเก่าเก็บ ต้องอยู่ในสภาพที่ใช้งานได้ทันที และต้องมีคุณลักษณะเฉพาะตรงตามที่กำหนดไว้ หรือดีกว่าข้อกำหนด

๖. ขอบเขตของงาน

โครงการปรับปรุงและเพิ่มประสิทธิภาพระบบโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศของระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ใหม่ ต้องดำเนินการอย่างน้อยดังนี้

๖.๑ จัดหาอุปกรณ์คอมพิวเตอร์และซอฟต์แวร์ในโครงการ ซึ่งมีรายละเอียดคุณลักษณะเฉพาะตามเอกสารแนบ ๑

๖.๒ ปรับปรุงระบบพิสูจน์และยืนยันตัวตน (Authentication and Identity Management Enhancement) และพัฒนากระบวนการตรวจสอบสิทธิ์และยืนยันตัวตนให้มีความปลอดภัย ทันสมัย รองรับการใช้งานในองค์กรขนาดใหญ่ พร้อมเสริมมาตรการป้องกันภัยคุกคามไซเบอร์ตามมาตรฐานสากล รายละเอียดตามเอกสารแนบ ๑

๖.๓ โอนย้ายและปรับปรุงแอปพลิเคชันของระบบ New GFMIS Thai ให้ทันสมัย (Modernization) บนแพลตฟอร์ม DevSecOps และดำเนินการปรับปรุงโค้ดและสถาปัตยกรรมแอปพลิเคชันให้เหมาะสมกับสภาพแวดล้อมใหม่ ตามเอกสารแนบ ๑

๖.๔ การบริหารงานโครงการ รายละเอียดตามเอกสารแนบ ๒

๖.๕ ออกแบบและติดตั้งอุปกรณ์คอมพิวเตอร์และซอฟต์แวร์ในโครงการ รายละเอียดตามเอกสารแนบ ๒

๖.๖ ทดสอบการเข้าถึงและความมั่นคงปลอดภัยระบบ (Security Test) รายละเอียดตามเอกสารแนบ ๒

๖.๗ จัดฝึกอบรมและจัดทำเอกสารต่าง ๆ ตามเอกสารแนบ ๓

๖.๘ บริการบำรุงรักษาและซ่อมแซมแก้ไขระบบ ตามเอกสารแนบ ๔

๗. ระยะเวลาดำเนินการ

ส่งมอบงานตามขอบเขตของงาน ภายใน ๒๗๐ วัน นับถัดจากวันลงนามในสัญญา

๘. ระยะเวลาส่งมอบงานและเงื่อนไขการชำระเงิน

ผู้ชนะการประกวดราคาจะต้องส่งมอบงาน ดังต่อไปนี้

งานงวดที่ ๑ ส่งมอบงาน ภายใน ๖๐ วัน นับถัดจากวันลงนามในสัญญา ดังนี้

๑. ส่งมอบแผนการดำเนินงานโครงการและรายชื่อบุคลากรพร้อมประวัติ

๒. ส่งมอบแผนการติดตั้งเครื่องคอมพิวเตอร์และอุปกรณ์ในโครงการทั้งหมด

๓. ส่งมอบแผนงานการโอนย้ายระบบงานเดิมไปยัง DevSecOps Platform

๔. ส่งมอบเอกสารจำนวน ๑ ชุด และสำเนาในรูปแบบอิเล็กทรอนิกส์ลงใน Thumb Drive จำนวน ๖ ชุด

งานงวดที่ ๒ ส่งมอบงาน ภายใน ๑๕๐ วัน นับถัดจากวันลงนามในสัญญา ดังนี้

๑. ส่งมอบแผนภาพการออกแบบและติดตั้งระบบคอมพิวเตอร์แม่ข่ายและอุปกรณ์ทั้งหมดในโครงการ

๒. ส่งมอบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ในโครงการทั้งหมด

๓. ส่งมอบซอฟต์แวร์พร้อมลิขสิทธิ์ที่ถูกต้องตามกฎหมาย

๔. ส่งมอบแผนการทดสอบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ในโครงการทั้งหมด

๕. ส่งมอบเอกสารจำนวน ๑ ชุด และสำเนาในรูปแบบอิเล็กทรอนิกส์ลงใน Thumb Drive จำนวน ๖ ชุด

งานงวดที่ ๓ ส่งมอบงาน ภายใน ๒๑๐ วัน นับถัดจากวันลงนามในสัญญา ดังนี้

๑. ส่งมอบผลการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ และการติดตั้งซอฟต์แวร์ในโครงการทั้งหมด

๒. ส่งมอบผลการทดสอบอุปกรณ์ในโครงการทั้งหมด

๓. ส่งมอบผลการปรับปรุงและพัฒนาระบบพิสูจน์และยืนยันตัวตน

๔. ส่งมอบแผนการฝึกอบรม

๕. ส่งมอบเอกสารจำนวน ๑ ชุด และสำเนาในรูปแบบอิเล็กทรอนิกส์ลงใน Thumb Drive จำนวน ๖ ชุด

งานงวดที่ ๔ ส่งมอบงาน ภายใน ๒๗๐ วัน นับถัดจากวันลงนามในสัญญา ดังนี้

๑. ส่งมอบผลการโอนย้ายระบบเดิมไป DevSecOps Platform

๒. ส่งมอบผลการปรับปรุงแอปพลิเคชันของระบบ New GFMIS Thai

๓. ส่งมอบผลการฝึกอบรมและเอกสารต่าง ๆ

๔. ส่งมอบเอกสารการบำรุงรักษาและซ่อมแซมแก้ไขระบบ

๕. 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 ๕๐ ของจำนวนเงินตามสัญญา
เมื่อคณะกรรมการตรวจรับได้ตรวจรับการส่งมอบงานงวดที่ ๒ เรียบร้อยแล้ว

งวดที่ ๓ ชำระเงินในอัตราร้อยละ ๓๐ ของจำนวนเงินตามสัญญา
เมื่อคณะกรรมการตรวจรับได้ตรวจรับการส่งมอบงานงวดที่ ๓ เรียบร้อยแล้ว

งวดที่ ๔ ชำระเงินในอัตราร้อยละ ๑๐ ของจำนวนเงินตามสัญญา
เมื่อคณะกรรมการตรวจรับได้ตรวจรับการส่งมอบงานงวดที่ ๔ เรียบร้อยแล้ว

๙. วงเงินในการจัดหา

วงเงินงบประมาณทั้งสิ้น ๑๖๑,๕๘๑,๐๐๐.- บาท (หนึ่งร้อยหกสิบเอ็ดล้านห้าแสนแปดหมื่นหนึ่งพันบาทถ้วน) ซึ่งเป็นราคาที่รวมภาษีมูลค่าเพิ่ม และค่าใช้จ่ายอื่นใดทั้งปวงไว้ด้วยแล้ว โดยเบิกจ่ายจากเงินงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. ๒๕๗๐

๑๐. หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

ใช้เกณฑ์ราคาในการคัดเลือก

๑๑. ค่าปรับ

ผู้ขายต้องดำเนินการตามที่กำหนดไว้ในขอบเขตของงานข้างต้นให้ครบถ้วน 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

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 และหากสำนักงานปลัดกระทรวงการคลังตรวจพบว่ามีโปรแกรมดังกล่าวและได้ก่อให้เกิดความเสียหายต่อระบบงาน ระบบคอมพิวเตอร์ และระบบเครือข่ายสื่อสารของสำนักงานปลัดกระทรวงการคลัง ผู้ยื่นข้อเสนอต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นทั้งหมด

๑๔.๔ ผู้ขายต้องดำเนินการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Risk Management) ภายในโครงการ โดยจะต้องนำเสนอข้อมูลเกี่ยวกับความเสี่ยงที่อาจเกิดขึ้นและแนวทางในการบริหารจัดการความเสี่ยงเหล่านั้นให้กับสำนักงานปลัดกระทรวงการคลังได้ทราบอย่างสม่ำเสมอตลอดระยะเวลาการดำเนินโครงการ

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

๑๕. ข้อมูลส่วนบุคคล

๑๕.๑ นโยบายคุ้มครองข้อมูลส่วนบุคคล

ผู้ขายได้รับทราบและตกลงจะปฏิบัติตามประกาศสำนักงานปลัดกระทรวงการคลัง เรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) สำนักงานปลัดกระทรวงการคลัง ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ประกาศ ณ วันที่ ๔ กุมภาพันธ์ ๒๕๖๙ หรือตามประกาศฉบับที่ปรับปรุงล่าสุด รวมถึงนโยบายและประกาศอื่นใดที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานปลัดกระทรวงการคลัง

๑๕.๒ การประมวลผลข้อมูลส่วนบุคคลในนามของสำนักงานปลัดกระทรวงการคลัง

การดำเนินงานของโครงการนี้ ผู้ขายไม่มีการประมวลผลข้อมูลส่วนบุคคลในนามของสำนักงานปลัดกระทรวงการคลัง

๑๖. การรักษาข้อมูลไว้เป็นความลับ

๑๖.๑ ผู้ขาย/ผู้รับจ้าง พนักงาน ลูกจ้าง ตัวแทน หรือบุคคลอื่นใดที่ได้รับมอบหมายจากผู้ขาย/ผู้รับจ้าง ต้องเก็บรักษาข้อมูลและรายละเอียดต่าง ๆ ที่เกิดขึ้นจากการทำงานตามสัญญาหรือข้อตกลง ทั้งในระหว่างระยะเวลาในสัญญาและหลังสิ้นสุดสัญญาไว้เป็นความลับ ไม่มอบหรือเปิดเผยข้อมูลแก่ผู้อื่นโดยไม่ได้รับอนุญาตจาก สป.กค. และ/หรือเอาไปเพื่อประโยชน์อื่นใดแก่ตนเอง โดยหากมีการนำไปใช้ หรือเปิดเผย หรือเผยแพร่ข้อมูลดังกล่าวอันจะก่อให้เกิดความเสียหายแก่ สป.กค. ผู้ขาย/ผู้รับจ้าง จะต้องรับผิดชอบต่อการกระทำดังกล่าว และ สป.กค. มีสิทธิดำเนินการตามกฎหมายกับผู้ขาย/ผู้รับจ้าง

๑๖.๒ ข้อมูลที่เป็นความลับทั้งที่อยู่ในรูปของเอกสาร โปรแกรมคอมพิวเตอร์ ข้อมูลอิเล็กทรอนิกส์ที่บันทึกลงในสื่อต่าง ๆ หรือสิ่งอื่นใดที่เป็นรูปธรรมที่ สป.กค. เปิดเผยแก่ผู้ขาย/ผู้รับจ้าง ผู้ขาย/ผู้รับจ้าง ต้องทำเครื่องหมาย “ลับ” ไว้กับสิ่งนั้นอย่างชัดเจน ส่วนการเปิดเผยข้อมูลที่เป็นความลับด้วยวาจาหรือด้วยวิธีการอื่นใดที่ไม่เป็นรูปธรรม ซึ่ง สป.กค. ได้แจ้งให้ผู้ขาย/ผู้รับจ้าง ทราบ ณ เวลาเปิดเผยนั้นว่าเป็นการเปิดเผยข้อมูลที่เป็นความลับ ผู้ขาย/ผู้รับจ้าง จะต้องสรุปสาระสำคัญของข้อมูลที่เป็นความลับดังกล่าวเป็นลายลักษณ์อักษร พร้อมทั้งทำเครื่องหมาย “ลับ” หรือเครื่องหมายที่มีความหมายทำนองเดียวกันนี้ไว้กับข้อความสรุปนั้นอย่างชัดเจน พร้อมทั้งส่งมอบข้อความสรุปดังกล่าว ให้แก่ สป.กค. ภายใน ๑๕ วัน นับตั้งแต่วันที่ สป.กค. เปิดเผยข้อมูลที่เป็นความลับนั้น

๑๖.๓ ผู้ขาย/ผู้รับจ้างตกลงจะเก็บรักษาข้อมูลที่เป็นความลับที่ สป.กค. ได้เปิดเผยแก่ผู้ขาย/ผู้รับจ้าง รวมถึงจะจัดให้มีมาตรการที่เหมาะสมตามมาตรฐานของการรักษาความมั่นคงปลอดภัยของข้อมูลที่เป็นความลับนั้น เพื่อป้องกันมิให้บุคคลภายนอกเข้าถึงข้อมูลที่เป็นความลับได้

๑๗. หน่วยงานผู้รับผิดชอบดำเนินการ

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง

๑๘. ข้อสงวนสิทธิในการยื่นข้อเสนอและอื่น ๆ

๑๘.๑ การจัดซื้อหรือการจัดจ้างครั้งนี้จะมีการลงนามในสัญญาหรือข้อตกลงเป็นหนังสือได้ต่อเมื่อพระราชบัญญัติงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. ๒๕๗๐ มีผลใช้บังคับ และได้รับจัดสรรงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. ๒๕๗๐ จากสำนักงบประมาณแล้ว สำหรับกรณีที่ไม่ได้รับการจัดสรรงบประมาณรายจ่ายเพื่อการจัดหาในครั้งนี้ ส่วนราชการสามารถยกเลิกจัดหาได้

๑๘.๒ หากข้อความใดในขอบเขตของงานมีความขัดแย้งกัน ให้ยึดถือตามข้อกำหนดที่เป็นประโยชน์กับสำนักงานปลัดกระทรวงการคลัง

ท่านสามารถเสนอแนะวิจารณ์ หรือแสดงความคิดเห็นโดยเปิดเผย

๑. **ทางไปรษณีย์** โครงการปรับปรุงและเพิ่มประสิทธิภาพระบบโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศของระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ใหม่
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงการคลัง
ถนนพระรามที่ ๖ แขวงพญาไท เขตพญาไท
กรุงเทพมหานคร ๑๐๔๐๐

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

๓. **ทางโทรศัพท์** หมายเลข ๐๒-๑๒๖-๕๙๐๐ ต่อ ๓๐๓๒๑ , ๓๐๒๒๐

๔. **ทาง ระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (e - GP)**

ผู้ประกอบการและผู้สนใจทั่วไป สามารถแสดงความคิดเห็นผ่านระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (e-GP) ได้ ๒ วิธี ดังนี้
(๑) การแสดงความคิดเห็นผ่านหน้าเว็บไซต์ www.gprocurement.go.th
สำหรับผู้ประกอบการและผู้สนใจทั่วไป
(๒) login เข้าสู่ระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (e - GP)
สำหรับผู้ประกอบการที่เป็นลงทะเบียนเป็นผู้ค้ากับภาครัฐในระบบ e-GP
(หนังสือคณะกรรมการวินิจฉัยปัญหาการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ กรมบัญชีกลาง ด่วนที่สุด ที่ กค (กวจ) ๐๔๐๕.๒/ว ๒๑๐ ลงวันที่ ๒๔ มีนาคม ๒๕๖๙)

ทั้งนี้ โปรดแจ้ง ชื่อ ที่อยู่ พร้อมหมายเลขโทรศัพท์ติดต่อกลับด้วย

เอกสารแนบ ๑
รายละเอียดคุณลักษณะเฉพาะ

โครงการปรับปรุงและเพิ่มประสิทธิภาพระบบโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศของระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ใหม่ เป็นการจัดหาอุปกรณ์คอมพิวเตอร์และซอฟต์แวร์ โดยการจัดซื้อครั้งนี้ ต้องเป็นของแท้ ของใหม่ ไม่เคยใช้งานมาก่อน ไม่เป็นของเก่าเก็บ อยู่ในสภาพที่ใช้งานได้ทันที และต้องได้รับหนังสือรับรองในการสนับสนุนการจำหน่าย ติดตั้งและบำรุงรักษาอุปกรณ์คอมพิวเตอร์และซอฟต์แวร์ในโครงการจากผู้ผลิต หรือสาขาของผู้ผลิต หรือตัวแทนจำหน่ายในประเทศไทย ซึ่งออกให้สำหรับโครงการปรับปรุงและเพิ่มประสิทธิภาพระบบโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศของระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ใหม่ และยื่นมาพร้อมกับการยื่นข้อเสนอในครั้งนี้

อุปกรณ์คอมพิวเตอร์และซอฟต์แวร์ ที่จัดซื้อครั้งนี้ มีคุณลักษณะเฉพาะอย่างน้อย ดังต่อไปนี้

๑. เครื่องคอมพิวเตอร์แม่ข่ายสำหรับระบบฐานข้อมูล จำนวน ๒ ชุด ติดตั้งที่ศูนย์คอมพิวเตอร์หลัก (DC) และศูนย์คอมพิวเตอร์สำรอง (DR) โดยแต่ละชุดมีคุณลักษณะเฉพาะอย่างน้อยดังนี้

๑.๑ มีสถาปัตยกรรมระบบฐานข้อมูลแบบรวมศูนย์ซึ่งประกอบด้วย เครื่องคอมพิวเตอร์แม่ข่าย (Compute Node หรือ Database Server) อุปกรณ์ Network และอุปกรณ์จัดเก็บข้อมูล (Storage Controller หรือ Storage Server) ติดตั้งภายในตู้ Rack เดียวกัน

๑.๒ เครื่องคอมพิวเตอร์แม่ข่าย (Compute node หรือ Database Server) อุปกรณ์ Network อุปกรณ์จัดเก็บข้อมูล (Storage Controller หรือ Storage Server) และแหล่งจ่ายไฟฟ้า (Power Supply) เป็นแบบ Redundant

๑.๓ เครื่องคอมพิวเตอร์แม่ข่าย (Compute node หรือ Database Server) อุปกรณ์ Network อุปกรณ์จัดเก็บข้อมูล (Storage Controller หรือ Storage Server) มีแหล่งจ่ายไฟฟ้า (Power Supply) ที่สามารถรองรับการถอดเปลี่ยนแบบ Hot Swap หรือ Hot Plug ได้

๑.๔ มีแหล่งจ่ายไฟฟ้า Power Distribution Units (PDU) แบบ Redundant

๑.๕ มี Compute Node หรือ Database Server จำนวนไม่น้อยกว่า ๒ หน่วย และรองรับการเพิ่มขยายได้ไม่น้อยกว่า ๘ หน่วย โดยแต่ละหน่วยมีคุณลักษณะเฉพาะอย่างน้อยดังนี้

๑.๕.๑ เครื่องคอมพิวเตอร์แม่ข่ายที่เสนอต้องเป็นเครื่องคอมพิวเตอร์แม่ข่ายที่สามารถใช้งานร่วมกับระบบฐานข้อมูลเดิมได้

๑.๕.๒ มีหน่วยประมวลผลกลาง (CPU) X๘๖ จำนวนไม่น้อยกว่า ๒ หน่วย โดยแต่ละหน่วยมีจำนวน Core ไม่น้อยกว่า ๙๖ Core หรือมีจำนวน Core รวมไม่น้อยกว่า ๑๙๒ Core

๑.๕.๓ มีหน่วยความจำหลัก (Main Memory) ชนิด DDR๕ หรือดีกว่า จำนวนรวมไม่น้อยกว่า ๒๐๐๐ GB

๑.๕.๔ มีหน่วยเก็บข้อมูลแบบ NVMe SSD หรือดีกว่า ที่ทำงานแบบ Hot Swap หรือ Hot Plug ได้ ขนาดไม่น้อยกว่า ๓ TB ต่อหน่วย จำนวนไม่น้อยกว่า ๒ หน่วย

๑.๕.๕ มี Ethernet Adapter ที่มีความเร็ว ๑๐ Gbps หรือดีกว่า จำนวนไม่น้อยกว่า ๖ ช่อง พร้อม Transceiver ชนิด ๑๐Gbps SFP+ SR จำนวนไม่น้อยกว่า ๖ หน่วย

๑.๕.๖ มีช่องเชื่อมต่อแบบ Ethernet Adapter ชนิด ๑๐๐ Gb QSFP๒๘ หรือดีกว่า จำนวนไม่น้อยกว่า ๒ ช่อง

๑.๕.๗ มีระบบปฏิบัติการ UNIX หรือ Enterprise Linux แบบ ๖๔ บิต แบบไม่จำกัดจำนวนผู้ใช้ที่มีลิขสิทธิ์การใช้งานถูกต้องตามกฎหมาย

๑.๕.๘ สามารถทำการแบ่งทรัพยากรสำหรับ เครื่องคอมพิวเตอร์แม่ข่าย Compute node หรือ Database Server ออกเป็นส่วนๆได้ โดยแต่ละ Virtual Machine จะต้องมีระบบปฏิบัติการ (Operating System) ซึ่งทำงานเป็นอิสระต่อกัน (Isolation) และต้องจัดสรรทรัพยากร แบบไม่จำกัดจำนวนผู้ใช้ที่มีลิขสิทธิ์การใช้งานถูกต้องตามกฎหมาย

๑.๖ มี Storage Controller หรือ Storage Server จำนวนไม่น้อยกว่า ๓ หน่วย และรองรับการเพิ่มขยายได้ไม่น้อยกว่า ๘ หน่วย โดยแต่ละหน่วยมีคุณลักษณะเฉพาะอย่างน้อยดังนี้

๑.๖.๑ มีหน่วยประมวลผลกลาง (CPU) X๘๖ จำนวนไม่น้อยกว่า ๒ หน่วย โดยแต่ละหน่วยมีจำนวน Core ไม่น้อยกว่า ไม่น้อยกว่า ๓๒ Core หรือมีจำนวน Core รวมไม่น้อยกว่า ๖๔ Core

๑.๖.๒ มีหน่วยความจำหลัก (Main Memory) ชนิด DDR๕ หรือดีกว่า จำนวนรวมไม่น้อยกว่า ๒๕๖ GB

๑.๖.๓ มีหน่วยจัดเก็บข้อมูล ชนิด SAS ๗๒๐๐ RPM หรือดีกว่า จำนวนไม่น้อยกว่า ๑๒ หน่วย โดยแต่ละหน่วยมีขนาดความจุไม่น้อยกว่า ๒๒ TB (RAW Capacity)

๑.๖.๔ มีหน่วยจัดเก็บข้อมูล ประเภท Flash ชนิด NVMe หรือดีกว่า จำนวนไม่น้อยกว่า ๔ หน่วย โดยแต่ละหน่วยมีขนาดความจุไม่น้อยกว่า ๖.๘ TB (RAW Capacity)

๑.๖.๕ สามารถบีบอัดข้อมูลของระบบฐานข้อมูล (Database Compression) แบบแถว (Row Compression) หรือแบบคอลัมน์ (Columnar Compression) หรือเทียบเท่า ได้เป็นอย่างน้อย เพื่อประหยัดพื้นที่ในการจัดเก็บข้อมูล โดยใช้ความสามารถของ Storage Controller หรือ Storage Server หรือระบบโปรแกรมฐานข้อมูลที่นำเสนอ

๑.๖.๖ มีช่องเชื่อมต่อแบบ Ethernet Adapter ชนิด ๑๐๐ Gb QSFP๒๘ หรือดีกว่า จำนวนไม่น้อยกว่า ๒ ช่อง

๑.๗ มีอุปกรณ์กระจายสัญญาณ (Switch) สำหรับการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์แม่ข่าย จำนวนอย่างน้อย ๒ ชุด โดยแต่ละชุดจะต้องเป็นอุปกรณ์กระจายสัญญาณชนิด ๑๐๐ Gb หรือดีกว่า รองรับพอร์ตชนิด ๑๐/๒๕/๔๐/๑๐๐ Gbps จำนวนไม่น้อยกว่า ๓๖ พอร์ต

๑.๘ มี Management Switch สำหรับการบริหารจัดการ Compute node หรือ Database Server และ Storage Controller หรือ Storage Server แบบ ๔๘-port ความเร็ว ๑๐๐๐ Mb/s หรือดีกว่า จำนวน ๑ ชุด

๒. อุปกรณ์สำหรับใช้งานเป็นเครื่องสำรองข้อมูลแบบเบ็ดเสร็จ (Backup Appliance) ติดตั้งที่ศูนย์คอมพิวเตอร์หลัก (DC) จำนวน ๑ ชุด โดยมีคุณลักษณะเฉพาะอย่างน้อยดังนี้

๒.๑ อุปกรณ์เป็นแบบ Appliance ที่ถูกออกแบบมาสำหรับระบบสำรองข้อมูลโดยเฉพาะ มีการติดตั้ง Hardware และ Software Storage system

๒.๒ มีหน่วยประมวลผลหลักไม่น้อยกว่า ๑๖ Core และมีความเร็วไม่น้อยกว่า ๒.๐ GHz จำนวนไม่น้อยกว่า ๒ Processor

๒.๓ มีหน่วยความจำหลักขนาดรวมไม่น้อยกว่า ๒๕๖ GB

๒.๔ มีหน่วยจัดเก็บข้อมูล ชนิด NL-SAS หรือ SAS หรือดีกว่า ชนิด Hot Pluggable หรือ Hot Swap โดยมีการติดตั้ง RAID ๖ ที่มีขนาดความจุรวมที่สามารถใช้งานได้ (Usable Capacity) ๗๐ TiB (หรือ ๘๐ TB) และรองรับการขยายได้สูงสุด ๔๐๐ TB

๒.๕ รองรับการขยาย Throughput ได้ไม่น้อยกว่า ๓๐TB ต่อชั่วโมง จากการทำ Deduplication บนตัวอุปกรณ์ (Server-side)

๒.๖ มีช่องเชื่อมต่อแบบ Fibre Channel ความเร็วไม่น้อยกว่า ๓๒ Gbps หรือดีกว่า จำนวนไม่น้อยกว่า ๔ Port

๒.๗ มีช่องเชื่อมต่อเครือข่าย (Network Interface) แบบ ๑๐ Gigabit Ethernet แบบ SFP+ จำนวนไม่น้อยกว่า ๖ Port

๒.๘ มีช่องเชื่อมต่อเครือข่าย (Network Interface) แบบ ๑๐ Gigabit Ethernet จำนวนไม่น้อยกว่า ๔ Port

๒.๙ มีแหล่งจ่ายไฟแบบ Hot Plug Redundant Power Supply หรือ Hot Swappable Power Supply จำนวน ๒ หน่วย

๒.๑๐ อุปกรณ์ที่นำเสนอต้องทำงานด้วยรูปแบบ Container Technology โดยสามารถสร้าง Backup Applications ได้หลาย instance ในอุปกรณ์เดียว

๒.๑๑ อุปกรณ์มีระบบตรวจจับการบุกรุก (IDS) และระบบป้องกันการบุกรุก (IPS)

๒.๑๒ อุปกรณ์เป็นแบบ Zero Trust Architecture และ มีการทำ Hardening ของระบบ ตามกระบวนการของ STIG

๒.๑๓ มีความสามารถในการ Monitor Hardware ต่าง ๆ ของอุปกรณ์ ได้เช่น CPU, Disks, Power, Fan, RAID และ Fibre Channel ได้

๒.๑๔ มีการป้องกันการเปลี่ยนค่า Operating System, Services, Network และ Drivers ด้วยการ Lockdown Operating System

๒.๑๕ มี Multi-factor Authentication โดยรองรับ TOTP ของ Microsoft Authenticator, Google Authenticator และ Okta Authenticator

๒.๑๖ รองรับการตั้งค่า Replicate แบบ Air Gap ได้ในรูปแบบ Pull Model หรือ Reverse Connection

๒.๑๗ อุปกรณ์มี Firewall ป้องกันการเข้าถึงระบบ โดยอนุญาตให้เข้าถึงได้เฉพาะงานสำรองข้อมูล

๒.๑๘ มี Immutable หรือ WORM Storage แบบ Enterprise Mode และ Compliance Mode

๒.๑๙ รองรับการใช้ Port Fibre Channel ของตัวอุปกรณ์ สำรองข้อมูลไปยัง Tape Drive ได้

๓. อุปกรณ์สำหรับใช้งานเป็นเครื่องสำรองข้อมูลแบบเบ็ดเสร็จ (Backup Appliance) ติดตั้งที่ศูนย์คอมพิวเตอร์สำรอง (DR) จำนวน ๑ ชุด โดยมีคุณลักษณะเฉพาะอย่างน้อยดังนี้

๓.๑ อุปกรณ์เป็นแบบ Appliance ที่ถูกออกแบบมาสำหรับระบบสำรองข้อมูลโดยเฉพาะมีการติดตั้ง Hardware และ Software Storage System

๓.๒ มีหน่วยประมวลผลหลักไม่น้อยกว่า ๑๖ Core และมีความเร็วไม่น้อยกว่า ๒.๐ GHz จำนวนไม่น้อยกว่า ๒ Processor

๓.๓ มีหน่วยความจำหลักขนาดรวมไม่น้อยกว่า ๒๕๖ GB

๓.๔ มีหน่วยจัดเก็บข้อมูล ชนิด NL-SAS หรือ SAS หรือดีกว่า ชนิด Hot Pluggable หรือ Hot Swap โดยมีการติดตั้ง RAID ๖ ที่มีขนาดความจุรวมที่สามารถใช้งานได้ (Usable Capacity) ๑๔๐ TiB (๑๕๐ TB) และรองรับการขยายได้สูงสุด ๔๐๐ TB โดยต้องเป็น Disk จาก ผลิตภัณฑ์เดียวกัน

๓.๕ รองรับการขยาย Throughput ได้ไม่น้อยกว่า ๓๐TB ต่อชั่วโมง จากการทำ Deduplication บนตัวอุปกรณ์ (Server-side)

๓.๖ มีช่องเชื่อมต่อแบบ Fibre Channel ความเร็วไม่น้อยกว่า ๓๒ Gbps หรือดีกว่า จำนวนไม่น้อยกว่า ๔ Port

๓.๗ มีช่องเชื่อมต่อเครือข่าย (Network Interface) แบบ ๑๐ Gigabit Ethernet แบบ SFP+ จำนวนไม่น้อยกว่า ๖ Port

๓.๘ มีช่องเชื่อมต่อเครือข่าย (Network Interface) แบบ ๑๐ Gigabit Ethernet จำนวนไม่น้อยกว่า ๔ Port

๓.๙ มีแหล่งจ่ายไฟแบบ Hot Plug Redundant Power Supply หรือ Hot Swappable Power Supply จำนวน ๒ หน่วย

๓.๑๐ อุปกรณ์ที่นำเสนอต้องทำงานด้วยรูปแบบ Container Technology โดยสามารถสร้าง Backup Applications ได้หลาย Instance ในอุปกรณ์เดียว

๓.๑๑ อุปกรณ์มีระบบตรวจจับการบุกรุก (IDS) และระบบป้องกันการบุกรุก (IPS)

๓.๑๒ อุปกรณ์เป็นแบบ Zero Trust Architecture และ มีการทำ Hardening ของระบบ ตามกระบวนการของ STIG

๓.๑๓ มีความสามารถในการ Monitor Hardware ต่าง ๆ ของอุปกรณ์ ได้เช่น CPU, Disks, Power, Fan, RAID และ Fibre Channel ได้

๓.๑๔ มีการป้องกันการเปลี่ยนค่า Operating system, Services, Network และ Drivers ด้วยการ Lockdown Operating System

๓.๑๕ มี Multi-factor Authentication โดยรองรับ TOTP ของ Microsoft Authenticator, Google Authenticator และ Okta Authenticator

๓.๑๖ รองรับการตั้งค่า Replicate แบบ Air Gap ได้ในรูปแบบ Pull Model หรือ Reverse Connection

๓.๑๗ อุปกรณ์มี Firewall ป้องกันการเข้าถึงระบบ โดยอนุญาตให้เข้าถึงได้เฉพาะงานสำรองข้อมูล

๓.๑๘ มี Immutable หรือ WORM Storage แบบ Enterprise Mode และ Compliance Mode

๓.๑๙ รองรับการใช้ Port Fibre Channel ของตัวอุปกรณ์ สำรองข้อมูลไปยัง Tape Drive ได้

๔. ซอฟต์แวร์ระบบ ประกอบด้วย

๔.๑ ซอฟต์แวร์ระบบสำรองข้อมูลสำหรับ Kubernetes โดยมีคุณลักษณะเฉพาะอย่างน้อยดังนี้

๔.๑.๑ เป็นระบบจัดการการสำรองและการกู้คืนข้อมูล แบบรวมศูนย์ (Centralized Management) โดยต้องสามารถติดตั้ง manager software บนระบบปฏิบัติการ Windows และ Linux ได้เป็นอย่างน้อย

๔.๑.๒ รองรับการสำรองข้อมูลเครื่องลูกข่ายที่มีระบบปฏิบัติการดังต่อไปนี้เป็นอย่างน้อย Windows, AIX, Solaris, HP-UX, Redhat, SUSE, CentOS, Oracle Linux, และ UBUNTU ได้

๔.๑.๓ สถาปัตยกรรมแบบ ๓ Tiers เพื่อสามารถรองรับการขยายประสิทธิภาพระบบสำรองข้อมูลได้ในอนาคต

๔.๑.๔ สามารถบริหารจัดการระบบสำรองข้อมูลจากส่วนกลางได้ (Centralized Management) ผ่านทาง Console GUI หรือ Web GUI

๔.๑.๕ รองรับการสำรองข้อมูลระบบที่เป็น Virtual ได้ ทั้ง VMware vSphere, Microsoft Hyper-V และ Nutanix AHV แบบ Agentless และไม่จำเป็นต้องติดตั้ง Proxy แยกจากระบบสำรองข้อมูล โดยสำรองข้อมูลเฉพาะ Changed Block เพื่อลดปริมาณข้อมูลที่ทำการ Backup พร้อมทั้งคงความสามารถในการ Restore ในรูปแบบ Full Restore ได้

๔.๑.๖ รองรับทำการสำรองและกู้คืนข้อมูลของ Application Database ต่าง ๆ ได้ในรูปแบบ Online Backup ช่วยให้ Application ทำงานได้อย่างต่อเนื่องแม้จะมีการสำรองข้อมูล เช่น Oracle, SAP, Informix, DB๒ , SAP ASE, MySQL, MariaDB, Microsoft SQL Server, Microsoft Exchange Server, Lotus Notes, Microsoft SharePoint, Microsoft Active Directory เป็นต้น

๔.๑.๗ รองรับการกู้คืนข้อมูลของ Exchange, SharePoint, Active Directory แบบ Granular Recovery คือจากการสำรองข้อมูลเพียงครั้งเดียว แต่สามารถเลือกการกู้คืนได้หลายรูปแบบ ได้แก่ ในระดับ E-mail, Document เอกสาร, Database เพื่อเป็นการประหยัดทรัพยากรในการสำรองข้อมูล

๔.๑.๘ รองรับการสำรองข้อมูลฐานข้อมูล Oracle เฉพาะส่วนต่าง และสร้างเป็น Full Backup และสามารถเปิดใช้งานไฟล์ฐานข้อมูล Oracle ที่ถูกสำรอง ได้จากอุปกรณ์สำรองข้อมูลที่เสนอ

๔.๑.๙ รองรับการสำรองข้อมูลแบบ Agentless ของข้อมูลประเภท Distributed File System เช่น Hadoop, และ HBASE โดยการส่งข้อมูลแบบกระจายหลายช่องทาง (Parallel Streaming) เพื่อเพิ่มประสิทธิภาพ

๔.๑.๑๐ รองรับการจัดเก็บข้อมูลสำรองในแบบ Immutable และ Indelible ข้อมูลได้ในแบบ Enterprise และ Compliance ได้ทุกประเภทของข้อมูลสำรอง อาทิเช่น VM และ File System เป็นต้น

๔.๑.๑๑ รองรับการแสดงความผิดปกติของการสำรองข้อมูล (Anomaly Detection) เช่น ขนาดข้อมูล, จำนวนไฟล์, การส่งข้อมูล, การลดความซ้ำซ้อน และระยะเวลาการสำรองข้อมูล รวมถึงต้องสามารถรายงานผ่านหน้า WebUI ของระบบได้

๔.๑.๑๒ สามารถแจ้งผลของการ Backup หรือ Event ต่าง ๆ ผ่านทาง E-mail ได้

๔.๑.๑๓ รองรับการสังเคราะห์ Full Backup และ Incremental Backup เพื่อสร้างเป็น Full Backup ชุดใหม่ได้

๔.๑.๑๔ สามารถทำการ Replicate Backup Image แบบลดความซ้ำซ้อน (Deduplication) จากศูนย์คอมพิวเตอร์หลักไปยังศูนย์คอมพิวเตอร์สำรองได้ โดย Backup Server ทั้งสองศูนย์มีความเป็นอิสระจากกันหรืออยู่คนละโดเมนกัน ในกรณีที่ Backup Server ที่ศูนย์ใดศูนย์หนึ่งมีปัญหา Backup Server อีกศูนย์หนึ่งยังคงทำงานและสามารถกู้ข้อมูลได้ในทันที

๔.๑.๑๕ สามารถสำรองและกู้คืนข้อมูล Namespaces ของ Kubernetes ผ่าน WebUI ได้ และสามารถเลือกกู้คืนข้อมูล ได้ดังนี้ ConfigMaps, Namespaces, secrets, persistent volume

๔.๑.๑๖ สามารถสำรองข้อมูล Kubernetes ในรูปแบบสำรองเฉพาะส่วนต่างและสามารถกู้คืนในรูปแบบ Full ได้ เพื่อลดระยะเวลาการสำรองข้อมูล

๔.๑.๑๗ สามารถสร้างกลุ่มการจัดการที่มีความยืดหยุ่น โดยสามารถค้นหาและคัดกรอง Namespace ตามชนิดของทรัพยากรที่กำหนดได้ เช่น Virtual Machine, Persistent Volume และ Persistent Volume Claim เพื่อนำกลุ่มดังกล่าวเข้าสู่นโยบายการสำรองข้อมูลโดยอัตโนมัติ

๔.๑.๑๘ มีลิขสิทธิ์การสำรองและกู้คืนข้อมูลแบบไม่จำกัดจำนวนเครื่อง โดยมีลิขสิทธิ์อย่างน้อย ๔๐TB

๔.๒ ระบบบริหารการเข้าถึงแบบรวมศูนย์ (Identity Management System) ประกอบด้วย

๔.๒.๑ ซอฟต์แวร์ระบบปฏิบัติการสำหรับเครื่องแม่ข่าย โดยมีคุณลักษณะเฉพาะอย่างน้อยดังนี้

๔.๒.๑.๑ เป็นระบบปฏิบัติการ Linux System

๔.๒.๑.๒ สามารถใช้งานได้กับเครื่องแม่ข่ายที่มีสถาปัตยกรรมแบบ AMD and Intel ๖๔-bit Architectures

๔.๒.๑.๓ สามารถติดตั้งใช้งานได้บนระบบเครื่องแม่ข่ายประเภท Physical หรือ Bare Metal ได้

๔.๒.๑.๔ สามารถติดตั้งใช้งานได้บนระบบเครื่องแม่ข่ายเสมือนได้แก่ VMware vSphere, Microsoft Hyper-V หรือ Nutanix AHV เป็นอย่างน้อย

๔.๒.๑.๕ สามารถทำงานร่วมกับระบบจัดเก็บข้อมูล (File System) ชนิด xfs, ext๔, NFS, SMB, CIFS และ GFS๒

๔.๒.๑.๖ สนับสนุนการติดตั้งเคอร์เนลแพตช์ (Kernel Patch) ได้โดยไม่จำเป็นต้องรีบูต (Reboot) หรือรีสตาร์ท (Restart) Process ใดๆ

๔.๒.๑.๗ สนับสนุนมาตรฐานและการจัดการด้านความปลอดภัย SELinux, FIPS ๑๔๐-๒ หรือ FIPS ๑๔๐-๓ เป็นอย่างน้อย

๔.๒.๑.๘ มีลิขสิทธิ์การใช้งานถูกต้องตามกฎหมายและครอบคลุมจำนวนการใช้งานไม่น้อยกว่า ๔ License (๑ License เท่ากับ ๒ VMs)

๔.๒.๒ ซอฟต์แวร์จัดการการยืนยันตัวตนและสิทธิ์การเข้าถึงระบบ โดยมีคุณลักษณะเฉพาะอย่างน้อยดังนี้

๔.๒.๒.๑ สามารถเข้าใช้งาน Web Application ทั้งหมดด้วยการล็อกอินเพียงครั้งเดียว เพื่อให้ระบบ Single Sign On ทำการ Sign On เข้าไปยัง Application ได้อย่างอัตโนมัติผ่านการมาตรฐาน SAML๒.๐, OAuth๒.๐, และ OpenID Connect

๔.๒.๒.๒ สามารถทำงานร่วมกับ Directory Service ได้หลากหลายผ่านทาง Protocol LDAP และ Active Directory

๔.๒.๒.๓ สามารถกำหนดนโยบายการควบคุมการเข้าถึง (Access Control) ให้กับผู้ใช้และ Client Applications หรือ Clients ได้

๔.๒.๒.๔ สามารถตัดการทำงานโดยอัตโนมัติเมื่อไม่มีการใช้งานในช่วงเวลาที่กำหนด (Session Timeout)

๔.๒.๒.๕ มีหน้าจอกำหนดสิทธิ์การใช้งานแบบกราฟิก (GUI) โดยใช้งานผ่านทาง Web Browser ได้ และ REST API ได้

๔.๒.๒.๖ รองรับการ log in ด้วย Social Log in เช่น Google, GitHub, Facebook, และ Twitter เป็นต้น

๔.๒.๒.๗ มีลิขสิทธิ์การใช้งานถูกต้องตามกฎหมายและครอบคลุมจำนวนการใช้งานไม่น้อยกว่า ๙ License (๑ License เท่ากับ ๔ vCPU)

๕. การพัฒนาระบบสารสนเทศ ประกอบด้วย

๕.๑ การพัฒนาระบบบริหารการเข้าถึงแบบรวมศูนย์ (Identity Management System)

๕.๑.๑ ศึกษาระบบงานเดิมที่ใช้งานบน WSO๒ Identity Server

๕.๑.๒ รวบรวมข้อมูลแอปพลิเคชันที่เชื่อมต่ออยู่กับระบบเดิม และจัดทำเอกสาร System Architecture Design และ Migration Plan

๕.๑.๓ ออกแบบระบบ Logging, Monitoring และ Alerting สำหรับการติดตามการทำงานของแอปพลิเคชัน

๕.๑.๔ ออกแบบสถาปัตยกรรมระบบใหม่ให้รองรับ High Availability (HA) Cluster

๕.๑.๕ กำหนดมาตรฐานการบริหารจัดการทรัพยากร (Resource Management) เช่น CPU, Memory, Scaling Policy เป็นต้น

๕.๑.๖ ติดตั้งซอฟต์แวร์ระบบบริหารการเข้าถึงแบบรวมศูนย์ (Identity Management System) ให้สามารถทำงานร่วมกับ Ldap เดิมของทางระบบ New GFMIS Thai ได้

๕.๑.๗ จัดทำแผนทดสอบ (Test Plan) และกรณีทดสอบ (Test Cases)

๕.๑.๘ ทดสอบการทำงานร่วมกับระบบ New GFMIS Thai เดิม เช่นการ Login แบบ User Password และ Soft Token รวมถึงการทดสอบร่วมกับระบบลงทะเบียน (Web Register)

๕.๑.๙ ทดสอบการทำงานของระบบ (Functional, Integration และ Performance Testing)

๕.๑.๑๐ ปรับแต่งค่า (Tuning) เพื่อให้ระบบทำงานได้อย่างมีเสถียรภาพและมีประสิทธิภาพสูงสุด

๕.๑.๑๑ จัดทำเอกสารโครงสร้างระบบ (System Design Document), คู่มือการบริหารจัดการ (Operation Manual) และแนวทางการบำรุงรักษา (Maintenance Guideline)

๕.๒ การปรับปรุงแอปพลิเคชันให้ทำงานบนแพลตฟอร์ม Kubernetes ต้องดำเนินการอย่างน้อยดังนี้

๕.๒.๑ รวบรวมข้อมูลและจัดทำบัญชีรายการแอปพลิเคชัน (Application Inventory Assessment)

๑) รวบรวมรายการแอปพลิเคชันทั้งหมดที่ต้องปรับปรุง

๒) วิเคราะห์โครงสร้าง สภาพแวดล้อมการทำงาน (Runtime Environment) และการเชื่อมโยงกับระบบอื่น (Dependencies)

๕.๒.๒ ปรับปรุงและจัดเตรียมแอปพลิเคชันสำหรับการย้าย (Application Refactoring and Containerization)

๑) ปรับโครงสร้างโค้ด (Refactor) เพื่อให้รองรับการทำงานในสภาพแวดล้อม Container

๒) จัดทำ Dockerfile และ Pipeline สำหรับ Build/Deploy ผ่านระบบ DevSecOps

๓) กำหนด Policy สำหรับการสแกนช่องโหว่ของ Container Image และการตรวจสอบความมั่นคงปลอดภัยก่อนใช้งานจริง

๕.๒.๓ ทดสอบการเชื่อมต่อแอปพลิเคชันกับระบบฐานข้อมูลและบริการภายนอก (External Services) ให้สามารถทำงานได้

๕.๒.๔ แยกข้อมูลค่ากำหนดระบบ (Config) และข้อมูลอ่อนไหว (เช่น Password, Token, Certificate) ของแต่ละ environment และทดสอบการทำงานให้สามารถทำงานได้ปกติดังเดิม

๕.๓ การโอนย้ายแอปพลิเคชันบนแพลตฟอร์ม Kubernetes ต้องดำเนินการอย่างน้อยดังนี้

๕.๓.๑ รวบรวมข้อมูลและจัดทำบัญชีรายการแอปพลิเคชัน (Application Inventory Assessment) ที่ต้องการโอนย้าย

๕.๓.๒ วิเคราะห์โครงสร้าง สภาพแวดล้อมการทำงาน (Runtime Environment) และการเชื่อมโยงกับระบบอื่น ๆ (Dependencies)

๕.๓.๓ วิเคราะห์ความพร้อมของแอปพลิเคชันต่อการย้าย (Application Readiness Analysis)

๑) ตรวจสอบการรองรับเทคโนโลยี Containerization ของแต่ละแอปพลิเคชัน

๒) วิเคราะห์ความเข้ากันได้ของฐานข้อมูล บริการภายนอก (External Services) และระบบเครือข่าย

๓) จัดทำรายงานผลการวิเคราะห์ความพร้อม พร้อมข้อเสนอแนะในการปรับปรุง

๕.๓.๔ จัดลำดับความสำคัญของแอปพลิเคชันที่จะดำเนินการย้ายก่อน-หลัง ตามความเสี่ยงและความสำคัญเชิงธุรกิจ

๕.๓.๕ ออกแบบสถาปัตยกรรมแอปพลิเคชันบน Kubernetes (Kubernetes Application Architecture Design)

๑) ออกแบบโครงสร้าง Deployment, Service, Ingress, Persistent Volume และ ConfigMap ของแต่ละแอปพลิเคชัน

๒) กำหนดมาตรฐานการบริหารจัดการทรัพยากร (Resource Management) เช่น CPU, Memory, Scaling Policy

๓) ออกแบบระบบ Logging, Monitoring และ Alerting สำหรับการติดตามการทำงานของแอปพลิเคชัน

๕.๓.๖ ดำเนินการโอนย้ายและทดสอบการทำงานบนแพลตฟอร์ม Kubernetes (Migration and Validation Testing) โดยต้องดำเนินการอย่างน้อยดังนี้

๑) ดำเนินการย้าย (Deploy) แอปพลิเคชันขึ้นบนแพลตฟอร์ม Kubernetes ตามลำดับที่กำหนด

๒) ทดสอบการทำงานของระบบ (Functional, Integration และ Performance Testing)

๓) ปรับแต่งค่า (Tuning) เพื่อให้ระบบทำงานได้อย่างมีเสถียรภาพและมีประสิทธิภาพสูงสุด

๔) จัดทำเอกสารแสดงโครงสร้างระบบ (System Design Document), คู่มือการบริหารจัดการ (Operation Manual) และแนวทางการบำรุงรักษา (Maintenance Guideline)

๕.๓.๗ ต้องดำเนินการโอนย้ายแอปพลิเคชันบนแพลตฟอร์ม Kubernetes อย่างน้อย ๔ ระบบงาน หรือตามที่คณะกรรมการตรวจรับพัสดุกำหนด

๕.๔ การพัฒนาและปรับปรุงระบบงาน New GFMIS Thai ต้องดำเนินการอย่างน้อยดังนี้

๕.๔.๑ สำรวจและจัดทำรายการไลบรารีของระบบงาน GFMIS เดิม (Application Library Inventory Assessment)

๑) สำรวจและรวบรวมรายการไลบรารีทั้งหมดที่ใช้งานอยู่ในระบบงาน GFMIS เดิม ทั้งส่วน Front-end, Back-end, Middleware และ Framework ที่เกี่ยวข้อง

๒) ตรวจสอบเวอร์ชัน ปลายทางการสนับสนุน (End of Support: EOS) และความเข้ากันได้ของแต่ละไลบรารี

๓) จัดทำบัญชีรายการ (Inventory List) พร้อมระบุสถานะความปลอดภัยของแต่ละรายการ

๕.๔.๒ ตรวจสอบช่องโหว่และประเมินความเสี่ยงด้านความมั่นคงปลอดภัย (Vulnerability Scanning and Risk Assessment)

๑) ใช้เครื่องมือสแกนช่องโหว่ (Vulnerability Scanner) ที่เป็นไปตามมาตรฐาน OWASP หรือ NIST SP ๘๐๐-๕๓

๒) วิเคราะห์ระดับความรุนแรงของช่องโหว่ (Severity Level: Critical, High, Medium, Low)

๓) จัดทำรายงานผลการประเมินความเสี่ยง และแนวทางการแก้ไข (Remediation Plan)

๕.๔.๓ ดำเนินการอัปเดตและปรับปรุงไลบรารี (Library Update and Patch Implementation)

๑) อัปเดตเวอร์ชันของไลบรารีที่หมดอายุการสนับสนุนหรือมีช่องโหว่ร้ายแรง

๒) ติดตั้งแพตช์ (Patch) หรือปรับปรุงส่วนประกอบของซอฟต์แวร์ให้เป็นเวอร์ชันที่ปลอดภัยและผ่านการตรวจสอบแล้ว

๓) ตรวจสอบความเข้ากันได้ของระบบหลังการอัปเดต เพื่อไม่ให้กระทบต่อฟังก์ชันการทำงานเดิมของระบบ

๕.๔.๔ ทดสอบการทำงานของระบบหลังการอัปเดต (System Validation and Regression Testing)

๑) ทดสอบการทำงานของแอปพลิเคชันที่ได้รับการอัปเดตในสภาพแวดล้อม Dev/QA ก่อนนำขึ้นระบบจริง

๒) ทำการทดสอบแบบ Regression Test เพื่อยืนยันว่าไม่มีผลกระทบต่อโมดูลอื่น

๓) บันทึกผลการทดสอบและจัดทำรายงานยืนยันความถูกต้อง

๕.๔.๕ จัดทำแนวทางและกระบวนการบริหารจัดการการอัปเดตในอนาคต (Library Maintenance and Governance Process)

๑) จัดทำคู่มือแนวทางการบริหารจัดการการอัปเดตไลบรารี (Library Update Guideline) และการตรวจสอบช่องโหว่ประจำรอบ

๒) กำหนดรอบการตรวจสอบและปรับปรุงไลบรารี (เช่น รายไตรมาส หรือทุกครั้งที่มีการเผยแพร่ช่องโหว่ระดับวิกฤติ)

๕.๔.๖ ต้องดำเนินการพัฒนาและปรับปรุงระบบงาน New GFMIS Thai อย่างน้อย ๓ ระบบงาน หรือตามที่คณะกรรมการตรวจรับพัสดุกำหนด

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 เฝ้าติดตามและรายงานความคืบหน้าตลอดระยะเวลาโครงการให้คณะกรรมการตรวจรับพัสดุทราบและหากพบปัญหาและอุปสรรคต่าง 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 ออกแบบการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ ณ ศูนย์คอมพิวเตอร์หลัก (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 ณ ศูนย์คอมพิวเตอร์หลัก (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 ต้องติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย ซอฟต์แวร์และอุปกรณ์ในโครงการทั้งหมด ให้สามารถรองรับการใช้งานจริงได้ตามวัตถุประสงค์ หรือตามที่คณะกรรมการตรวจรับพัสดุกำหนด และจัดทำเอกสารสรุปผลการติดตั้งอุปกรณ์ในโครงการ

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

๒.๗ การติดตั้งต้องไม่กระทบต่อการทำงานของเครื่องคอมพิวเตอร์และอุปกรณ์เดิม หรือก่อให้เกิดความเสียหายแก่สำนักงานปลัดกระทรวงการคลัง และในกรณีที่เกิดความเสียหายผู้ขายต้องรับผิดชอบค่าใช้จ่ายที่เกิดขึ้น และต้องดำเนินการให้สามารถใช้งานได้ตามปกติ

๒.๘ ต้องปรับแต่งประสิทธิภาพ (PERFORMANCE TUNING) ของอุปกรณ์ให้ทำงานได้อย่างมีประสิทธิภาพ

๒.๙ ต้องทำ Label ตามรูปแบบที่คณะกรรมการตรวจรับพัสดุกำหนด และติดที่อุปกรณ์ในโครงการทั้งหมด

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 โดยต้องร่วมทดสอบการสำรองและเรียกคืนข้อมูลร่วมกับเจ้าหน้าที่ที่เกี่ยวข้องเพื่อให้แน่ใจว่าระบบสามารถคืนสู่สภาวะปกติและทำงานได้อย่างต่อเนื่อง

๓.๖ ต้องทดสอบย้ายการทำงานของระบบ (Switch Over Test) โดยจัดทำแผนทดสอบการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และระบบเครือข่าย รวมถึงอุปกรณ์อื่น ๆ ที่เกี่ยวข้องโดยต้องได้รับความเห็นชอบจากคณะกรรมการตรวจรับ โดยระบบยังสามารถงานได้อย่างต่อเนื่องและมีประสิทธิภาพ

๔. การทดสอบการเข้าถึงและความมั่นคงปลอดภัยระบบ (Security Test)

ต้องดำเนินการทดสอบการเข้าถึงและความมั่นคงปลอดภัยระบบ (Security Test) ของอุปกรณ์คอมพิวเตอร์ในโครงการทั้งหมดอย่างน้อยดังนี้

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

๔.๒ 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

๔.๓ ในการทดสอบการเข้าถึงและความมั่นคงปลอดภัยระบบ (Security Test) แต่ละครั้ง ต้องจัดทำรายงานผลการดำเนินการตรวจสอบช่องโหว่ที่สำคัญ (Vulnerability Assessment) ประกอบด้วยข้อมูลดังต่อไปนี้เป็นอย่างน้อย

๑) สรุปผลการดำเนินการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญและการจัดลำดับความเสี่ยงที่ต้องเร่งดำเนินการแก้ไข

๒) สรุปผลการตรวจสอบจากการใช้เครื่องมือตรวจสอบ (Scanning Tool)

๓) สรุปการดำเนินการแก้ไขปิดช่องโหว่ที่ตรวจพบ

๔.๔ ผู้เชี่ยวชาญภายนอกต้องดำเนินการทดสอบการเข้าถึงและความมั่นคงปลอดภัยระบบ (Security Test) ในช่วงการส่งมอบระบบจนมั่นใจว่าระบบไม่มีช่องโหว่และโอกาสการบุกรุกระบบที่มีความเสี่ยงในระดับปานกลางและสูง

๕. จัดทำแนวทางการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ

จัดทำแนวทางการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ ตามแนวทางของมาตรฐานสากล ISO/IEC ๒๗๐๐๑ และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ 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) โครงการเพิ่มประสิทธิภาพการรักษาความมั่นคงปลอดภัยของข้อมูลและป้องกันภัยทางไซเบอร์ระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ใหม่ สำนักงานปลัดกระทรวงการคลัง แขวงพญาไท เขตพญาไท กรุงเทพมหานคร และโครงการปรับปรุงและเพิ่มประสิทธิภาพระบบโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศของระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ใหม่

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 โดยจะต้องจัดเตรียมสถานที่ฝึกอบรมที่ได้มาตรฐาน เพื่อใช้สำหรับการฝึกอบรมพร้อมรถรับ-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

๑.๙ ต้องจัดฝึกอบรม โดยหลักสูตรที่จัดฝึกอบรม ประกอบด้วยหลักสูตรอย่างน้อยดังนี้ ทั้งนี้ จำนวนผู้เข้ารับการอบรมและระยะเวลาการอบรมสามารถปรับเปลี่ยนเพิ่มลดได้ตามความเหมาะสม

หลักสูตรการอบรม	กลุ่มของผู้เข้ารับการอบรม	รูปแบบการอบรม	จำนวนผู้เข้าอบรม	ระยะเวลาการอบรม
๑) การติดตั้งและใช้งานเครื่องคอมพิวเตอร์แม่ข่ายสำหรับระบบฐานข้อมูล	ผู้ดูแลระบบ / เจ้าหน้าที่ทางเทคนิค (IT)	ห้องอบรมหรือออนไลน์ พร้อม VDO และสื่อการสอน	๑๐ คน	๑ วัน
๒) การติดตั้งและใช้งานอุปกรณ์สำหรับใช้งานเป็นเครื่องสำรองข้อมูลแบบเบ็ดเสร็จ (Backup Appliance)	ผู้ดูแลระบบ / เจ้าหน้าที่ทางเทคนิค (IT)	ห้องอบรมหรือออนไลน์ พร้อม VDO และสื่อการสอน	๑๐ คน	๑ วัน
๓) การทำงานของซอฟต์แวร์ระบบบริหารการเข้าถึงแบบรวมศูนย์ (Identity Management System)	ผู้ดูแลระบบ / เจ้าหน้าที่ทางเทคนิค (IT)	ห้องอบรมหรือออนไลน์ พร้อม VDO และสื่อการสอน	๑๐ คน	๑ วัน

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 คู่มือการสำรองข้อมูล (Backup & Recovery)

เอกสารแนบ ๔
การบำรุงรักษาและซ่อมแซมแก้ไข

ต้องดำเนินการบำรุงรักษา ซ่อมแซม แก้ไข หรือเปลี่ยนแทน สำหรับโครงการปรับปรุงและเพิ่มประสิทธิภาพระบบโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศของระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ใหม่ 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 รวมทั้งสามารถตรวจสอบสถานะความคืบหน้าของการให้บริการได้ และมีระบบฐานข้อมูลอุปกรณ์ครุภัณฑ์

คอมพิวเตอร์และอุปกรณ์ต่อพ่วงที่อยู่ในสัญญาบำรุงรักษาและซ่อมแซมแก้ไข 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

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