ขอบเขตของงาน (Terms of Reference : TOR)
โครงการยกระดับความปลอดภัยไซเบอร์ และป้องกันการรั่วไหลของข้อมูล

๑. ความเป็นมา

ด้วยกระทรวงการคลัง เป็นหน่วยงานกลางทางด้านเศรษฐกิจการเงินการคลังที่สำคัญของประเทศ มีข้อมูลสำคัญๆ เพื่อการบริหารจัดการ การกำหนดกรอบนโยบาย อาทิเช่น ข้อมูลในระบบบริหารงานการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ (GFMIS) เพื่อบริหารงบประมาณ การรับและนำส่งรายได้ การเบิกจ่าย การจัดซื้อจัดจ้าง การบัญชีทรัพย์สิน ให้กับส่วนราชการทุกกระทรวง กรม ทั่วประเทศ องค์กรปกครองส่วนท้องถิ่น รัฐวิสาหกิจ กองทุนและหน่วยงานอิสระ รวมหน่วยเบิกจ่ายทั้งสิ้นประมาณ ๑๖,๐๐๐ หน่วยงาน มีจำนวน Transaction ที่เกิดขึ้นในระบบมากกว่า ๔๐ ล้านรายการต่อปี โดยระบบ GFMIS ถูกกำหนดให้เป็นบริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ตามประกาศของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔ ด้วย นอกจากนี้ กระทรวงการคลังโดยสำนักงานปลัดกระทรวงการคลัง ยังทำหน้าที่บริหารจัดการฐานข้อมูลของประชาชนผู้ลงทะเบียนโครงการลงทะเบียนเพื่อสวัสดิการแห่งรัฐ ภายใต้พระราชบัญญัติการจัดประชารัฐสวัสดิการเพื่อเศรษฐกิจฐานรากและสังคม พ.ศ. ๒๕๖๒ ซึ่งมีผู้ผ่านสิทธิในโครงการลงทะเบียนเพื่อสวัสดิการแห่งรัฐ ปี ๒๕๖๕ จำนวนทั้งสิ้นประมาณ ๑๕ ล้านคนอีกด้วย ดังนั้นการรักษาความปลอดภัยของข้อมูลดังกล่าว จึงเป็นภารกิจที่สำคัญของสำนักงานปลัดกระทรวงการคลังซึ่งจะช่วยให้สามารถรับมือกับภัยคุกคามที่เกิดขึ้นในปัจจุบันและอนาคตได้อย่างมีประสิทธิภาพ ลดผลกระทบต่อภารกิจสำคัญของกระทรวงการคลัง และเสริมสร้างความเชื่อมั่นในระบบการบริหารจัดการของรัฐต่อไป

จากความก้าวหน้าของเทคโนโลยีดิจิทัลปัจจุบัน ภัยคุกคามทางไซเบอร์ได้ทวีความรุนแรง และซับซ้อนมากยิ่งขึ้น ไม่ว่าจะเป็นการโจมตีจากมัลแวร์ การเข้าถึงระบบเครือข่ายโดยมิชอบ หรือการรั่วไหลของข้อมูลที่สำคัญ ซึ่งหากเกิดเหตุการณ์ดังกล่าวอาจส่งผลกระทบต่อความมั่นคงทางการเงินของประเทศ ทำให้ข้อมูลทางการเงินที่สำคัญถูกเปิดเผยหรือนำไปใช้ในทางที่มิชอบ ส่งผลให้เกิดความเสียหายทางเศรษฐกิจ และกระทบต่อความเชื่อมั่นของประชาชนและผู้มีส่วนได้ส่วนเสียในระบบการบริหารจัดการของรัฐ ทั้งนี้ ความเสี่ยงที่ข้อมูลสำคัญอาจถูกโจมตีและนำไปใช้เพื่อประโยชน์ในทางมิชอบ เช่น การฉ้อโกง การทุจริต หรือการนำข้อมูลไปใช้ในการบ่อนทำลายความมั่นคงของประเทศ ยังเป็นเรื่องที่ไม่อาจมองข้ามได้ ด้วยเหตุนี้ สำนักงานปลัดกระทรวงการคลังจึงเล็งเห็นถึงความจำเป็นในการยกระดับมาตรการความปลอดภัยทางไซเบอร์และการป้องกันการรั่วไหลของข้อมูลเพื่อเสริมสร้างความมั่นคงในการดำเนินงาน และลดความเสี่ยงที่อาจเกิดขึ้น ศูนย์สารสนเทศและการสื่อสารสำนักงานปลัดกระทรวงการคลัง จึงได้จัดทำโครงการยกระดับความปลอดภัยไซเบอร์ และป้องกันการรั่วไหลของข้อมูล

๒. วัตถุประสงค์

๒.๑. เพื่อเพิ่มความปลอดภัยของข้อมูลที่สำคัญและลดความเสี่ยงจากการรั่วไหลของข้อมูล เนื่องจากข้อมูลที่กระทรวงการคลังรับผิดชอบเป็นข้อมูลที่มีความละเอียดอ่อน

๒.๒. เพื่อเพิ่มศักยภาพการป้องกันและตรวจจับการโจมตีทางไซเบอร์สนับสนุนการปฏิบัติงานของหน่วยงานภายใต้กระทรวงการคลัง

๒.๓. เพื่อปฏิบัติตามข้อกำหนดและมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๒๒ ซึ่งเป็นมาตรฐานสากลสำหรับระบบการจัดการความปลอดภัยของข้อมูล

๒.๔. เพื่อเพิ่มความมั่นคงของระบบเทคโนโลยีสารสนเทศในการป้องกันภัยคุกคาม โดยครอบคลุมถึงการป้องกัน การตรวจจับ และการตอบสนองต่อเหตุการณ์ที่อาจเกิดขึ้น ซึ่งเป็นการลดความเสี่ยงที่ข้อมูลสำคัญจะถูกโจมตีหรือถูกเข้าถึงโดยไม่ได้รับอนุญาต

๒.๕. เพื่อเสริมสร้างความรู้และทักษะด้านความปลอดภัยทางไซเบอร์ให้กับเจ้าหน้าที่ในสำนักงานปลัดกระทรวงการคลัง ให้สามารถปฏิบัติงานได้อย่างมั่นใจและมีประสิทธิภาพ

๒.๖. เพื่อเพิ่มความเชื่อมั่นในระบบการจัดการข้อมูลของกระทรวงการคลัง โดยสร้างความมั่นใจให้กับผู้มีส่วนได้ส่วนเสีย ว่าข้อมูลสำคัญได้รับการปกป้องและจัดการอย่างเหมาะสม

๓. เป้าหมาย

๓.๑. สำนักงานปลัดกระทรวงการคลังมีระบบที่สามารถรับมือกับภัยคุกคามที่เกิดขึ้นในปัจจุบันและอนาคต ได้อย่างมีประสิทธิภาพ ลดผลกระทบต่อภารกิจสำคัญของกระทรวงการคลังและเสริมสร้างความเชื่อมั่น ในระบบการบริหารจัดการของรัฐต่อไป

๓.๒. เจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารที่ปฏิบัติงานประจำภายในอาคารที่ทำการใหม่ สามารถปฏิบัติงานได้อย่างมั่นใจและมีประสิทธิภาพ

๔. คุณสมบัติผู้ยื่นข้อเสนอ

๔.๑. มีความสามารถตามกฎหมาย

๔.๒. ไม่เป็นบุคคลล้มละลาย

๔.๓. ไม่อยู่ระหว่างเลิกกิจการ

๔.๔. ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบ ที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศ ของกรมบัญชีกลาง

๔.๕. ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงาน ของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วน ผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๔.๖. มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุ ภาครัฐกำหนดในราชกิจจานุเบกษา

๔.๗. เป็นนิติบุคคล ผู้มีอาชีพขายพัสดุที่ประกวดราคาซื้อด้วยวิธีการทางอิเล็กทรอนิกส์

๔.๘. ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงานปลัดกระทรวงการคลัง ณ วันยื่นข้อเสนอ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในครั้งนี้

๔.๙. ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอ ได้มีคำสั่งให้สละเอกสิทธิ์ความคุ้มกันเช่นว่านั้น

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

๔.๑๑. ผู้ยื่นข้อเสนอต้องมีผลงานในการขายหรือติดตั้ง ระบบเครื่องคอมพิวเตอร์ หรือ ระบบเครือข่าย หรือ ระบบรักษาความมั่นคงปลอดภัย หรือ ระบบสนับสนุนศูนย์คอมพิวเตอร์ หรือการพัฒนาระบบคอมพิวเตอร์ โดยมีผลงานในการขายหรือติดตั้งสำเร็จมาแล้วให้กับหน่วยงานของรัฐ ภายในระยะเวลา ๕ ปี นับจาก วันแล้วเสร็จจนถึงวันยื่นข้อเสนอ ซึ่งมีมูลค่าไม่น้อยกว่า ๓๐,๐๐๐,๐๐๐.- บาท (สามสิบล้านบาทถ้วน) ต่อหนึ่งสัญญา ทั้งนี้ ให้แนบสำเนาสัญญาและสำเนาหนังสือรับรองผลงาน มาพร้อมการยื่นข้อเสนอ ทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์

๔.๑๒. ผู้ยื่นข้อเสนอซึ่งเป็นผู้ประกอบการ SMEs แสดงสำเนาใบขึ้นทะเบียนผู้ประกอบการวิสาหกิจขนาดกลาง และขนาดย่อม (SMEs) เป็น SME-GP (ถ้ามี) มาพร้อมการยื่นข้อเสนอทางระบบจัดซื้อจัดจ้างภาครัฐ ด้วยอิเล็กทรอนิกส์

๔.๑๓. ผู้ยื่นข้อเสนอที่เป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า ๑ ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ โดยแสดงสำเนาเอกสารหรือหลักฐานมาพร้อมการยื่นข้อเสนอทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์

๔.๑๔. ผู้ยื่นข้อเสนอที่เป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า จะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอไม่ต่ำกว่า ๒๐ ล้านบาท โดยแสดงสำเนาเอกสารหรือหลักฐานมาพร้อมการยื่นข้อเสนอทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์

๔.๑๕. กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียนหรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง (สินเชื่อที่ธนาคารภายในประเทศหรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้าประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรองหรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอนับถึงวันยื่นข้อเสนอไม่เกิน ๙๐ วัน) โดยแสดงสำเนาแบบหนังสือรับรองวงเงินสินเชื่อ (ตามแบบที่กรมบัญชีกลางกำหนด) มาพร้อมการยื่นข้อเสนอทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์

๔.๑๖. กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ หรือ เป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย (ฉบับที่ ๑๐) พ.ศ. ๒๕๖๑ ไม่ต้องยื่นเอกสารข้อเสนอตามข้อ ๔.๑๓ – ๔.๑๕

๕. แบบรูปรายการหรือคุณลักษณะเฉพาะ

สำนักงานปลัดกระทรวงการคลังมีความต้องการจัดซื้ออุปกรณ์ในโครงการยกระดับความปลอดภัยไซเบอร์และป้องกันการรั่วไหลของข้อมูล เพื่อจัดหาและติดตั้งอุปกรณ์ระบบเครือข่ายสำหรับยกระดับมาตรการความปลอดภัยทางไซเบอร์และการป้องกันการรั่วไหลของข้อมูลของกระทรวงการคลัง โดยต้องมีคุณลักษณะเฉพาะอย่างน้อยตามเอกสารแนบท้าย แบบรูปรายการหรือคุณลักษณะเฉพาะ ประกอบด้วยรายการดังต่อไปนี้

๕.๑	อุปกรณ์คัดกรองข้อมูลระบบเครือข่าย (TAP Aggregator)	จำนวน ๓ ชุด
๕.๒	ระบบตรวจสอบการทำงานและช่องโหว่ของระบบเครือข่าย สำหรับ Data Center	จำนวน ๒ ชุด
๕.๓	ระบบตรวจสอบการทำงานและช่องโหว่ของระบบเครือข่าย สำหรับ Campus	จำนวน ๑ ชุด
๕.๔	อุปกรณ์วิเคราะห์ข้อมูลภัยคุกคามระบบเครือข่าย	จำนวน ๑ ชุด
๕.๕	ระบบป้องกันข้อมูลรั่วไหลสำหรับเครื่องคอมพิวเตอร์ลูกข่าย	จำนวน ๑ ชุด

๖. ระยะเวลาดำเนินการ

ภายในระยะเวลา ๒๗๐ วัน นับถัดจากวันลงนามในสัญญา

๗. ระยะเวลาส่งมอบงาน

ผู้ชนะการประกวดราคาจะต้องส่งมอบงาน ดังต่อไปนี้

งวดที่ ๑ ภายใน ๓๐ วัน นับถัดจากวันลงนามในสัญญา

๑. แผนการดำเนินงานโครงการ และโครงสร้างการบริหารโครงการ

๒. ร่างแผนผังระบบเครือข่าย (Network Diagram)

๓. ร่างแผนผังแสดงอุปกรณ์ในตู้ Rack (Rack Layout)

๔. เอกสารจำนวน ๒ ชุด และในรูปแบบอิเล็กทรอนิกส์ซึ่งบันทึกลงใน Thumb Drive จำนวน ๖ ชุด

งวดที่ ๒ ภายใน ๑๘๐ วัน นับถัดจากวันลงนามในสัญญา

๑. ส่งมอบครุภัณฑ์ทั้งหมดในโครงการ และผลการทดสอบตามคุณลักษณะที่กำหนด

๒. ส่งมอบงานติดตั้งอุปกรณ์ รายการที่ ๕.๑ - ๕.๔ และรายงานผลการทดสอบอุปกรณ์

๓. คู่มือการใช้งานของอุปกรณ์ในโครงการ

๔. เอกสารจำนวน ๒ ชุด และในรูปแบบอิเล็กทรอนิกส์ซึ่งบันทึกลงใน Thumb Drive จำนวน ๖ ชุด

งวดสุดท้าย ภายใน ๒๗๐ วัน นับถัดจากวันลงนามในสัญญา

๑. แผนผังระบบเครือข่าย (Network Diagram) และแผนผังแสดงอุปกรณ์ในตู้ Rack (Rack Layout)

๒. ส่งมอบงานติดตั้งซอฟต์แวร์ รายการที่ ๕.๕

๓. เอกสารสรุปการติดตั้งอุปกรณ์และซอฟต์แวร์ทั้งหมดในโครงการ

๔. ส่งมอบผลการฝึกอบรมในลักษณะ On The Job Training ในโครงการทั้งหมด

๕. ส่งมอบงานอื่น ๆ ทั้งหมดในโครงการ

๖. เอกสารจำนวน ๒ ชุด และในรูปแบบอิเล็กทรอนิกส์ซึ่งบันทึกลงใน Portable Harddisk จำนวน ๖ ชุด

๘. เงื่อนไขการชำระเงิน

งวดที่ ๑ ชำระเงินในอัตราร้อยละ ๕ ของจำนวนเงินตามสัญญา เมื่อคณะกรรมการตรวจรับพัสดุได้ตรวจรับการส่งมอบงานงวดที่ ๑ เรียบร้อยแล้ว

งวดที่ ๒ ชำระเงินในอัตราร้อยละ ๗๐ ของจำนวนเงินตามสัญญา เมื่อคณะกรรมการตรวจรับพัสดุได้ตรวจรับการส่งมอบงานงวดที่ ๒ เรียบร้อยแล้ว

งวดสุดท้าย ชำระเงินในอัตราร้อยละ ๒๕ ของจำนวนเงินตามสัญญา เมื่อคณะกรรมการตรวจรับพัสดุได้ตรวจรับการส่งมอบงานงวดสุดท้าย เรียบร้อยแล้ว

๙. อัตราค่าปรับ

ผู้ชนะการประกวดราคาหรือผู้ขายต้องดำเนินการตามขอบเขตของงานที่กำหนดให้มีความถูกต้องครบถ้วน และหากไม่สามารถดำเนินการได้ครบถ้วนหรือถูกต้อง ผู้ชนะการประกวดราคาหรือผู้ขายยินยอมให้สำนักงานปลัดกระทรวงการคลังปรับเป็นรายวันในอัตราร้อยละ ๐.๒๐ (ศูนย์จุดสองศูนย์) ของราคาสิ่งของที่ยังไม่ได้ส่งมอบ จนกว่าจะดำเนินการแล้วเสร็จ หรือสำนักงานปลัดกระทรวงการคลังใช้สิทธิบอกเลิกสัญญา

๑๐. การรับประกันความชำรุดบกพร่อง

ผู้ชนะการประกวดราคาหรือผู้ขายต้องรับประกันความชำรุดบกพร่องของอุปกรณ์และระบบทั้งหมดที่ส่งมอบในโครงการยกระดับความปลอดภัยไซเบอร์ และป้องกันการรั่วไหลของข้อมูล เป็นระยะเวลา ๓ ปี นับถัดจากวันที่คณะกรรมการตรวจรับพัสดุได้ตรวจรับการส่งมอบพัสดุงวดสุดท้ายเรียบร้อยแล้ว โดยมีรายละเอียดตามขอบเขตของงานที่กำหนด

๑๑. วงเงินในการจัดหา

วงเงินในการจัดหาเป็นเงินทั้งสิ้น ๗๐,๐๐๐,๐๐๐.- บาท (เจ็ดสิบล้านบาทถ้วน) ซึ่งเป็นวงเงินที่รวมภาษีมูลค่าเพิ่ม และค่าใช้จ่ายอื่นใดทั้งปวงไว้ด้วยแล้ว โดยเบิกจ่ายจากเงินงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. ๒๕๖๗ งบกลาง รายการเงินสำรองจ่ายเพื่อกรณีฉุกเฉินหรือจำเป็น

๑๒. หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

ใช้เกณฑ์ราคาในการคัดเลือกผู้ที่เสนอราคาต่ำสุดเป็นผู้ชนะการซื้อหรือจ้างหรือเป็นผู้ได้รับการคัดเลือก โดยกรณีดำเนินการจัดซื้อโดยวิธีประกวดราคาอิเล็กทรอนิกส์ (Electronic Bidding : e - Bidding) และใช้เกณฑ์ราคาในการพิจารณาคัดเลือกผู้ชนะ ให้พิจารณาให้แต้มต่อในการยื่นข้อเสนอ ดังนี้

(๑) หากผู้ยื่นข้อเสนอซึ่งเป็นผู้ประกอบการ SMEs เสนอราคาสูงกว่าราคาต่ำสุดของผู้ยื่นข้อเสนอรายอื่นที่ไม่เกินร้อยละ ๑๐ ให้จัดซื้อจากผู้ประกอบการ SMEs ดังกล่าว โดยจัดเรียงลำดับผู้ยื่นข้อเสนอซึ่งเป็นผู้ประกอบการ SMEs ซึ่งเสนอราคาสูงกว่าราคาต่ำสุดของผู้ยื่นข้อเสนอรายอื่นไม่เกินร้อยละ ๑๐ ที่จะเรียกมาทำสัญญาไม่เกิน ๓ ราย

(๒) หากผู้ยื่นข้อเสนอได้เสนอพัสดุที่เป็นพัสดุที่ผลิตภายในประเทศ ที่ได้รับการรับรองและออกเครื่องหมายสินค้าที่ผลิตภายในประเทศไทย (Made in Thailand) จากสภาอุตสาหกรรมแห่งประเทศไทย เสนอราคาสูงกว่าราคาต่ำสุดของผู้ยื่นข้อเสนอรายอื่นไม่เกินร้อยละ ๕ ให้จัดซื้อจัดจ้างจากผู้ยื่นข้อเสนอที่เสนอพัสดุที่เป็นพัสดุที่ผลิตภายในประเทศที่ได้รับการรับรองและออกเครื่องหมายสินค้าที่ผลิตภายในประเทศไทยฯ

สำหรับการประกวดราคาอิเล็กทรอนิกส์ ที่มีการเสนอราคาหลายรายการและกำหนดเงื่อนไขเป็นกรณีการพิจารณาราคารวม หากผู้ยื่นข้อเสนอได้เสนอพัสดุที่เป็นพัสดุที่ผลิตภายในประเทศ ที่ได้รับการรับรองและออกเครื่องหมายสินค้าที่ผลิตภายในประเทศไทยฯ มีสัดส่วนมูลค่าตั้งแต่ร้อยละ ๖๐ ขึ้นไป ให้ได้แต้มต่อในการเสนอราคาตามวรรคหนึ่ง

อนึ่ง หากในการเสนอราคาครั้งนั้น ผู้ยื่นข้อเสนอรายใดมีคุณสมบัติทั้ง (๑) และ (๒) ให้ผู้ยื่นข้อเสนอรายนั้นได้แต้มต่อในการเสนอราคาสูงกว่าผู้ประกอบการรายอื่นไม่เกินร้อยละ ๑๕

(๓) หากผู้ยื่นข้อเสนอซึ่งมิใช่ผู้ประกอบการ SMEs แต่เป็นบุคคลธรรมดาที่ถือสัญชาติไทยหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยเสนอราคาสูงกว่าราคาต่ำสุดของผู้ยื่นข้อเสนอซึ่งเป็นบุคคลธรรมดาที่มิได้ถือสัญชาติไทยหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายของต่างประเทศไม่เกินร้อยละ ๓ ให้จัดซื้อหรือจัดจ้างจากผู้ยื่นข้อเสนอซึ่งเป็นบุคคลธรรมดาที่ถือสัญชาติไทยหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย

๑๓. ข้อตกลงในการเก็บรักษาความลับข้อมูลหรือเอกสาร

๑๓.๑) เอกสารทั้งหมดที่จัดทำขึ้น ถือเป็นลิขสิทธิ์ของสำนักงานปลัดกระทรวงการคลัง ผู้ขายหรือผู้รับจ้างจะต้องไม่เผยแพร่เอกสาร และ/หรือข้อมูลใด ๆ ที่จัดทำขึ้นทั้งหมด โดยไม่ได้รับความเห็นชอบอย่างเป็นลายลักษณ์อักษรจากสำนักงานปลัดกระทรวงการคลัง รวมทั้งจะต้องไม่แสวงหา หรือยินยอมให้บุคคลอื่นแสวงหาประโยชน์ใด ๆ จากข้อมูลและ/หรือ เอกสารดังกล่าวทั้งในทางพาณิชย์ หรือในกรณีอื่นอันอาจก่อให้เกิดความเสียหายแก่สำนักงานปลัดกระทรวงการคลังด้วยประการใดทั้งสิ้น

๑๓.๒) ข้อตกลงนี้ให้ถือเป็นส่วนหนึ่งของสัญญา อันเป็นเงื่อนไขที่สำนักงานปลัดกระทรวงการคลัง บอกเลิกสัญญาเรียกค่าเสียหายหรือปรับสินไหม รวมทั้งการดำเนินคดีทั้งในทางแพ่งและอาญาทุกประเภท

๑๓.๓) ข้อมูลต่าง ๆ ที่ผู้ขายหรือผู้รับจ้างได้รับทราบจากสำนักงานปลัดกระทรวงการคลังให้ถือเป็นความลับและลิขสิทธิ์ในเอกสารทุกฉบับและผลงานทุกชิ้น ซึ่งผู้ขายหรือผู้รับจ้างได้จัดทำขึ้น ให้ตกเป็นกรรมสิทธิ์ของสำนักงานปลัดกระทรวงการคลัง ผู้ขายหรือผู้รับจ้างจะนำไปเผยแพร่มิได้ โดยจะต้องปฏิบัติต่อข้อมูลดังกล่าวในชั้นข้อมูลลับของทางสำนักงานปลัดกระทรวงการคลัง เว้นแต่นำไปใช้เพื่อการศึกษาหรือขอผลงานทางวิชาการ (กรณีเป็นสถาบันการศึกษา)

๑๓.๔) ในการเก็บรักษาความลับของสำนักงานปลัดกระทรวงการคลัง ผู้ขายหรือผู้รับจ้างต้องระมัดระวังในการดูแลรักษาและปกป้องมิให้บุคคลอื่นที่ไม่เกี่ยวข้องกับการปฏิบัติงานตามสัญญาซื้อหรือจ้างได้ล่วงรู้ถึงข้อมูล หรือนำข้อมูลไปใช้หาประโยชน์ในการใด ๆ รวมถึงการเผยแพร่ต่อสาธารณะโดยมิได้รับอนุญาตจากสำนักงานปลัดกระทรวงการคลัง ยกเว้นในกรณีดังต่อไปนี้ ให้แจ้งสำนักงานปลัดกระทรวงการคลังทุกครั้ง กล่าวคือ

(๑) เป็นการเปิดเผยเพื่อประโยชน์ หรือความจำเป็นในการทำหน้าที่ตามสัญญาซื้อหรือจ้าง

(๒) เป็นกรณีจำเป็นต้องเปิดเผยตามกฎหมายหรือคำสั่งศาล

๑๓.๕) ผู้ขายหรือผู้รับจ้างต้องส่งมอบข้อมูล พร้อมทั้งข้อมูลที่ได้ทำซ้ำซึ่งสำเนาในทุกรูปแบบที่อาจสื่อความหมายถึงข้อมูลได้คืนแก่สำนักงานปลัดกระทรวงการคลังเมื่อเสร็จสิ้นงานซื้อหรือจ้าง หรือทำลายสำเนาข้อมูลเหล่านั้นเพื่อไม่ให้สามารถสื่อข้อความต่อไปได้อีก

๑๓.๖) ผู้ขายหรือผู้รับจ้างต้องรับผิดชอบในการดูแลรักษาความมั่นคงปลอดภัยข้อมูลให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และกฎหมายที่เกี่ยวข้องอย่างเคร่งครัด

๑๔. หน่วยงานผู้รับผิดชอบดำเนินการ

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง

๑๕. ข้อสงวนสิทธิในการยื่นข้อเสนอและอื่น ๆ

๑๕.๑) การจัดซื้อหรือการจัดจ้างครั้งนี้จะมีการลงนามในสัญญาหรือข้อตกลงเป็นหนังสือได้ต่อเมื่อพระราชบัญญัติงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. ๒๕๖๗ มีผลใช้บังคับ และได้รับจัดสรรงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. ๒๕๖๗ งบกลาง รายการเงินสำรองจ่ายเพื่อกรณีฉุกเฉินหรือจำเป็นจากสำนักงบประมาณแล้ว สำหรับกรณีที่ไม่ได้รับการจัดสรรงบประมาณรายจ่ายเพื่อการจัดหาในครั้งนี้ ส่วนราชการสามารถยกเลิกจัดหาได้

๑๕.๒) หากข้อความใดในขอบเขตของงานมีความขัดแย้งกัน ให้ยึดถือตามข้อกำหนดที่เป็นประโยชน์กับสำนักงานปลัดกระทรวงการคลัง

ท่านสามารถเสนอแนะวิจารณ์ หรือแสดงความคิดเห็นโดยเปิดเผย

๑. ทางไปรษณีย์ ส่ง คณะกรรมการจัดทำร่างขอบเขตของงานหรือรายละเอียดคุณลักษณะเฉพาะของพัสดุที่จะซื้อและกำหนดราคากลาง โครงการยกระดับความปลอดภัยไซเบอร์ และป้องกันการรั่วไหลของข้อมูล
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง
ถนนพระรามที่ ๖ แขวงพญาไท เขตพญาไท กรุงเทพมหานคร ๑๐๔๐๐

๒. ทาง e-Mail tor-mof๖๗_ndr-dlp@mof.go.th

๓. ทางโทรศัพท์ **หมายเลข ๐ ๒๑๒๖ ๕๙๐๐ ต่อ ๓๖๑๒ , ๓๖๑๔ , ๓๐๓๐๐ , ๓๐๓๐๑**

๔. ทางโทรสาร **หมายเลข ๐ ๒๒๗๓ ๙๗๙๐**

ทั้งนี้ โปรดแจ้ง ชื่อ ที่อยู่ พร้อมหมายเลขโทรศัพท์ติดต่อกลับด้วย

แบบรูปรายการหรือคุณลักษณะเฉพาะ

๑. ข้อกำหนดและเงื่อนไขในการยื่นข้อเสนอ

ผู้ยื่นข้อเสนอจะต้องปฏิบัติตามข้อกำหนดและเงื่อนไขในการยื่นข้อเสนอให้ครบถ้วนถูกต้อง รวมทั้งต้องปฏิบัติดังต่อไปนี้

๑.๑. ผู้ยื่นข้อเสนอต้องเป็นผู้ได้รับหนังสือแต่งตั้งให้เป็นตัวแทนจำหน่าย รวมทั้งการสนับสนุนอุปกรณ์ อะไหล่ การซ่อมแซมแก้ไข ผลิตภัณฑ์ที่เสนอจากผู้ผลิต หรือสาขาของผู้ผลิต หรือตัวแทนจำหน่ายในประเทศไทย โดยเป็นหนังสือที่แต่งตั้งสำหรับโครงการที่เสนอโดยเฉพาะ ยื่นมาพร้อมกับการยื่นข้อเสนอของผลิตภัณฑ์ดังต่อไปนี้

๑) อุปกรณ์คัดกรองข้อมูลระบบเครือข่าย (TAP Aggregator)

๒) ระบบตรวจสอบการทำงานและช่องโหว่ของระบบเครือข่าย สำหรับ Data Center

๓) ระบบตรวจสอบการทำงานและช่องโหว่ของระบบเครือข่าย สำหรับ Campus

๔) อุปกรณ์วิเคราะห์ข้อมูลภัยคุกคามระบบเครือข่าย

๕) ระบบป้องกันข้อมูลรั่วไหลสำหรับเครื่องคอมพิวเตอร์ลูกข่าย

๑.๒. ผู้ยื่นข้อเสนอต้องระบุยี่ห้อ รุ่น (Model) อุปกรณ์ที่เสนอทุกรายการในเอกสารรายการพัสดุ หรือเอกสารข้อกำหนดทางเทคนิค (Technical Proposal) ให้ชัดเจน พร้อมแคตตาล็อกของอุปกรณ์ที่เสนอ โดยต้องทำตารางเปรียบเทียบคุณลักษณะเฉพาะพร้อมอ้างอิงแค็ตตาล็อก มาพร้อมการยื่นข้อเสนอ

๑.๓. อุปกรณ์ทุกชิ้นที่เสนอต้องเป็นของแท้ ของใหม่ไม่เคยใช้งานมาก่อน ไม่เป็นของเก่าเก็บ ต้องอยู่ในสภาพที่ใช้งานได้ทันทีและต้องมีคุณสมบัติเฉพาะตรงตามที่กำหนดไว้ หรือดีกว่าข้อกำหนด

๒. คุณลักษณะเฉพาะของอุปกรณ์หรือระบบของโครงการยกระดับความปลอดภัยไซเบอร์ และป้องกันการรั่วไหลของข้อมูล ประกอบด้วยรายละเอียดดังต่อไปนี้

๒.๑. อุปกรณ์คัดกรองข้อมูลระบบเครือข่าย (TAP Aggregator) จำนวน ๓ ชุด โดยแต่ละชุดมีรายละเอียดคุณลักษณะเฉพาะอย่างน้อยดังต่อไปนี้

๑) มีช่องเชื่อมต่อแบบ ๑๐Gbps (SFP/SFP+) จำนวน ๔๐ ช่อง เสนอพร้อม Module Transceiver แบบ SFP+ จำนวน ๒๐ หน่วย

๒) มีช่องเชื่อมต่อระบบเครือข่ายแบบ ๔๐/๑๐๐ GE QSFP๑๐๐ จำนวน ๖ ช่อง

๓) สามารถตั้งค่า IEEE๘๐๒.๑Q VLAN Tagging และ VXLAN ได้

๔) สามารถเก็บ MAC Address ได้ไม่น้อยกว่า ๓๘๔,๐๐๐ MAC Address

๕) รองรับการให้บริการ Layer ๓ เช่น OSPF, OSPFv๓, BGP, MP-BGP ได้

๖) สามารถบริหารจัดการแบบ SSH และ Telnet ได้

๗) สามารถกรองข้อมูล (Filtering) การจราจรเครือข่ายที่ต้องการได้

๘) สามารถทำ Packet replication ผ่านพอร์ตในอุปกรณ์ได้

๙) มีความสามารถในการตัดข้อมูลการจราจรเครือข่ายที่ไม่ต้องการได้ (packet truncation)

๑๐) สามารถกรองข้อมูล (Filtering) ได้ในระดับ L๒/L๓/L๔ โดยใช้ DPI ได้

๑๑) สามารถในการทำงานร่วมกันกับระบบ Monitoring ด้วย OpenConfig, SNMP v๓, Syslog ได้

๑๒) มีลิขสิทธิ์การใช้งานครบทุกพอร์ตเชื่อมต่อ

๑๓) เป็นผลิตภัณฑ์ที่สามารถทำงานร่วมกับระบบตรวจสอบการทำงานและช่องโหว่ของระบบเครือข่าย หรืออุปกรณ์วิเคราะห์ข้อมูลภัยคุกคามระบบเครือข่าย ได้

๒.๒. ระบบตรวจสอบการทำงานและช่องโหว่ของระบบเครือข่าย สำหรับ Data Center จำนวน ๒ ชุด โดยแต่ละชุดมีรายละเอียดคุณลักษณะเฉพาะอย่างน้อยดังต่อไปนี้

๑) เป็นอุปกรณ์แบบ Hardware Appliance

๒) มีหน่วยประมวลผลกลาง (CPU) จำนวนรวมไม่น้อยกว่า ๖๔ Cores

๓) มีหน่วยจัดเก็บข้อมูล (Hard Disk) ความจุต่อหน่วยไม่น้อยกว่า ๖ TB จำนวนไม่น้อยกว่า ๑๒ หน่วย

๔) มีหน่วยความจำ (Memory) ขนาดรวมไม่น้อยกว่า ๕๑๒ GB

๕) สามารถทำงานในรูปแบบ Mirror/Span ได้

๖) รองรับการขยายในลักษณะ Scale-Out หรือเป็นสถาปัตยกรรมแบบกระจาย (Distributed Architecture)

๗) มี Throughput รวมแล้วไม่น้อยกว่า ๕ Gbps

๘) มีช่องเชื่อมต่อเครือข่ายแบบ ๑๐G (SFP+) จำนวนไม่น้อยกว่า ๔ ช่อง พร้อมโมดูล

๙) มีช่องเชื่อมต่อเครือข่าย (Network Interface) แบบ ๑G Base-T หรือดีกว่า จำนวนไม่น้อยกว่า ๒ ช่อง

๑๐) มีช่องเชื่อมต่อเครือข่าย (Network Interface) สำหรับทำหน้าที่บริหารจัดการ (Management) จำนวนไม่น้อยกว่า ๑ ช่อง

๑๑) มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน ๒ หน่วย

๑๒) สามารถเก็บข้อมูลจราจรเครือข่าย (Network Traffic) ในรูปแบบ PCAP

๑๓) มีความสามารถในการตรวจจับภัยคุกคามได้ตาม MITRE ATT & CK เช่น Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact เป็นต้น

๑๔) การตรวจจับภัยคุกคามระบบเครือข่ายเป็นลิขสิทธิ์แบบไม่จำกัดจำนวนอุปกรณ์

๑๕) สามารถบริหารจัดการผ่าน GUI หรือ Web Browser

๑๖) เป็นผลิตภัณฑ์ภายใต้เครื่องหมายการค้าเดียวกันกับอุปกรณ์วิเคราะห์ข้อมูลภัยคุกคามระบบเครือข่าย

๒.๓. ระบบตรวจสอบการทำงานและช่องโหว่ของระบบเครือข่าย สำหรับ Campus จำนวน ๑ ชุด โดยมีรายละเอียดคุณลักษณะเฉพาะอย่างน้อยดังต่อไปนี้

๑) เป็นอุปกรณ์แบบ Hardware Appliance

๒) มีหน่วยประมวลผลกลาง (CPU) จำนวนรวมไม่น้อยกว่า ๓๒ Cores

๓) มีหน่วยจัดเก็บข้อมูล (Hard disk) ความจุต่อหน่วยไม่น้อยกว่า ๑๐ TB จำนวนไม่น้อยกว่า ๔ หน่วย

๔) มีหน่วยความจำ (Memory) ขนาดรวมไม่น้อยกว่า ๕๑๒ GB

๕) สามารถทำงานในรูปแบบ Mirror/Span ได้

๖) รองรับการขยายในลักษณะ Scale-Out หรือเป็นสถาปัตยกรรมแบบกระจาย (Distributed Architecture)

๗) มี Throughput รวมแล้วไม่น้อยกว่า ๑ Gbps

๘) มีช่องเชื่อมต่อเครือข่ายแบบ ๑๐G (SFP+) จำนวนไม่น้อยกว่า ๔ ช่อง พร้อมโมดูล

๙) มีช่องเชื่อมต่อเครือข่าย (Network Interface) แบบ ๑G Base-T หรือดีกว่า จำนวนไม่น้อยกว่า ๒ ช่อง

๑๐) มีช่องเชื่อมต่อเครือข่าย (Network Interface) สำหรับทำหน้าที่บริหารจัดการ (Management) จำนวนไม่น้อยกว่า ๑ ช่อง

๑๑) มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน ๒ หน่วย

๑๒) สามารถเก็บข้อมูลจราจรเครือข่าย (Network Traffic) ในรูปแบบ PCAP

๑๓) มีความสามารถในการตรวจจับภัยคุกคามได้ตาม MITRE ATT & CK เช่น Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact เป็นต้น

๑๔) การตรวจจับภัยคุกคามระบบเครือข่ายเป็นลิขสิทธิ์แบบไม่จำกัดจำนวนอุปกรณ์

๑๕) สามารถบริหารจัดการผ่าน GUI หรือ Web Browser

๑๖) เป็นผลิตภัณฑ์ภายใต้เครื่องหมายการค้าเดียวกันกับอุปกรณ์วิเคราะห์ข้อมูลภัยคุกคามระบบเครือข่าย

๒.๔. อุปกรณ์วิเคราะห์ข้อมูลภัยคุกคามระบบเครือข่าย จำนวน ๑ ชุด โดยมีรายละเอียดคุณลักษณะเฉพาะอย่างน้อยดังต่อไปนี้

๑) เป็นอุปกรณ์แบบ Hardware Appliance

๒) มีหน่วยประมวลผลกลาง (CPU) จำนวนรวมไม่น้อยกว่า ๙๖ Cores

๓) มีหน่วยจัดเก็บข้อมูล (Hard disk) ความจุต่อหน่วยไม่น้อยกว่า ๘ TB จำนวนไม่น้อยกว่า ๑๐ หน่วย

๔) มีหน่วยจัดเก็บข้อมูล แบบ SSD ความจุต่อหน่วยไม่น้อยกว่า ๔๘๐ GB จำนวนไม่น้อยกว่า ๒ หน่วย

๕) มีหน่วยจัดเก็บข้อมูล แบบ Nvme ความจุต่อหน่วยไม่น้อยกว่า ๓.๒ TB จำนวนไม่น้อยกว่า ๒ หน่วย

๖) มีหน่วยความจำ (Memory) ขนาดรวมไม่น้อยกว่า ๑ TB

๗) มี Throughput รวมแล้วไม่น้อยกว่า ๑๐ Gbps

๘) มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน ๒ หน่วย

๙) สามารถวิเคราะห์ภัยคุกคามจากระบบเครือข่าย โดยเป็นลิขสิทธิ์แบบไม่จำกัดจำนวนอุปกรณ์

๑๐) มีความสามารถในการวิเคราะห์ข้อมูลจากระบบเครือข่ายได้ตาม MITRE ATT & CK เช่น Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact เป็นต้น

๑๑) สามารถเก็บข้อมูลจราจรเครือข่าย (Network Traffic) ได้ตั้งแต่ Layer ๒ ถึง Layer ๗ ได้

๑๒) มี AI (Artificial Intelligent) ในการวิเคราะห์ข้อมูลจราจรเครือข่าย (Network Traffic) เช่น Supervised, Unsupervised, Deep Neural Networks

๑๓) สามารถระบุ (Identifying) และทำ Profiling ของอุปกรณ์โดยนำข้อมูลจากพฤติกรรม เช่น Kerberos Name การใช้งานของอุปกรณ์

๑๔) สามารถค้นหาชื่อผู้ใช้งาน (User) หรือชื่ออุปกรณ์ (Device) ได้

๑๕) สามารถระบุข้อมูลการเข้าถึงโดเมน (Domains) จากระบบเครือข่ายได้

๑๖) สามารถระบุข้อมูลโดเมน (Domains) จากฐานข้อมูล https://Who.is หรือฐานข้อมูลอื่นได้

๑๗) สามารถตรวจจับภัยคุกคามจากข้อมูลที่ถูกเข้ารหัสได้โดยใช้เทคนิค Encrypted Traffic Analysis (ETA) หรือ SSL/TLS Fingerprinting

๑๘) สามารถตรวจจับการโจรกรรมข้อมูล (Data Exfiltration) โดยวิธี DNS tunneling และ ICMP tunneling ได้

๑๙) สามารถตรวจจับการโจมตีโดยการใช้เครื่องมือ (Tools) PSExec, PowerShell และ WMI ได้

๒๐) มีหน้าจอแสดงผลหรือ Dashboard แสดงการทำงานของ MITRE ATT&CK เพื่อระบุขอบเขตการโจมตี (Coverage)

๒๑) สามารทำงานร่วมกันกับอุปกรณ์ด้านความปลอดภัย เช่น อุปกรณ์ Firewall, ระบบวิเคราะห์ข้อมูล (SIEM) เป็นต้น

๒๒) สามารถบริหารจัดการผ่าน GUI หรือ Web Browser

๒๓) เป็นผู้ผลิตที่ถูกจัดอันดับเป็น Leader และ Outperformer อยู่ใน Gigaom Radar หัวข้อ NDR ปี ๒๐๒๓ หรือปีล่าสุด

๒.๕. ระบบป้องกันข้อมูลรั่วไหลสำหรับเครื่องคอมพิวเตอร์ลูกข่าย จำนวน ๑ ชุด โดยมีรายละเอียดคุณลักษณะเฉพาะอย่างน้อยดังต่อไปนี้

๒.๕.๑ มีลิขสิทธิ์รองรับการป้องกันข้อมูลรั่วไหลสำหรับเครื่องคอมพิวเตอร์ลูกข่าย จำนวนไม่น้อยกว่า ๕๐๐ สิทธิ์การใช้งาน โดยมีคุณลักษณะเฉพาะอย่างน้อยดังต่อไปนี้

๑) เป็นระบบที่ออกแบบมาเพื่อป้องกันการรั่วไหลของข้อมูล (Data Protection) ผ่านแหล่งที่มาของการรั่วไหลจากเครื่องคอมพิวเตอร์ลูกข่าย (Endpoint DLP)

๒) จะต้องมีซอฟต์แวร์ Agent ที่สามารถติดตั้งได้บนระบบระบบปฏิบัติการ Windows และ macOS ได้เป็นอย่างน้อย

๓) มี AI/ML เพื่อช่วยในการทำความเข้าใจพฤติกรรมข้อมูลผู้ใช้ได้อย่างรวดเร็วจากการใช้งานผ่านคอมพิวเตอร์ลูกข่าย เช่น พื้นที่เก็บข้อมูลแบบถอดได้ (Removable Storages), Local File Share และเครื่องพิมพ์ (Printer)

๔) มอนิเตอร์ข้อมูลที่ละเอียดอ่อนผ่านกิจกรรมต่าง ๆ บนเครื่องคอมพิวเตอร์ลูกข่าย เช่น การสั่งพิมพ์ (printing), การบันทึกไฟล์ลงบนพื้นที่เก็บข้อมูลแบบถอดได้ (saving to removable storage), การบันทึกไฟล์ลงบนเน็ตเวิร์คแชร์ (saving to network shares) และการอัปโหลดไฟล์ไปยังพื้นที่เก็บข้อมูลส่วนตัวบนคลาวน์ของผู้ใช้งาน (uploading to personal cloud storage accounts)

๕) ป้องกันข้อมูลรั่วไหลผ่าน personal cloud storage ได้แก่ Dropbox, OneDrive, iCloud, Box และ Google Drive

๖) สามารถตั้งนโยบายในการควบคุมข้อมูลรั่วไหลโดยตั้งเงื่อนไขที่แตกต่างกันจาก user, groups, DLP engine, departments, file type และ data size ได้

๗) สามารถกำหนด Action ได้อย่างน้อยดังต่อไปนี้ Allow (Permit), Block, Confirm, Protect หรือ Encrypt ไฟล์ (สำหรับ Removable storage) ได้

๘) สามารถเข้ารหัสไฟล์ที่มีข้อมูลละเอียดอ่อนเมื่อไฟล์ถูกคัดลอกจากเครื่องลูกข่ายไปยังที่เก็บข้อมูลแบบถอดได้เพื่อการแชร์ที่ปลอดภัยยิ่งขึ้น

๙) สามารถตั้งเงื่อนไขการควบคุม removable storage device ที่แตกต่างกัน โดยใช้ข้อมูลจาก Vendor ID, Product ID และ Serial Number ของ removable storage devices ได้

๑๐) สามารถตั้งเงื่อนไขการควบคุม printer ที่แตกต่างกัน โดยใช้ข้อมูลจาก Printer Name, Domain และ IP Address ของ printer ได้

๑๑) สามารถตั้งเงื่อนไขการควบคุม network share ที่แตกต่างกัน โดยเลือกจากทุกไฟล์และไดเรกทอรีในเครื่องแม่ข่าย หรือเฉพาะไฟล์ในไดเรกทอรี/ซับไดเรกทอรีที่กำหนดได้

๑๒) มี password ป้องกันไม่ให้ผู้ใช้ Logout จาก agent และ Uninstall agent ที่เป็นลักษณะ One Time Password (OTP) สำหรับผู้ใช้งานแต่ละคนได้

๑๓) มี password เฉพาะสำหรับผู้ดูแลระบบเพื่อปิดการทำงานของ Endpoint DLP, Logout จาก agent และ Uninstall agent สำหรับใช้ในการแก้ไขปัญหาได้

๑๔) ทำการขอ Exemption หรือ Bypass การตรวจสอบ Endpoint DLP ในกรณีที่ต้องการส่งออกข้อมูลนั้นชั่วคราว โดยจะได้รับ Password ที่เป็น One-Time Password (OTP) จากผู้ดูแลระบบเพื่อปิดการใช้งานชั่วคราวได้ และสามารถทำงานได้ขณะเครื่องลูกข่ายนั้นอยู่ใน offline mode

๑๕) สามารถตั้งค่า end user notification เพื่อแสดงบนเครื่องลูกข่ายเมื่อเกิดเหตุการณ์ที่สอดคล้องกับการรั่วไหลของข้อมูล และสามารถ custom ข้อความตามต้องการได้

๑๖) สามารถส่งอีเมลเมื่อเกิดเหตุการรั่วไหลของข้อมูลไปให้ auditor ได้

๑๗) สามารถป้องกันข้อมูลรั่วไหลได้ ทั้งในกรณีเครื่องคอมพิวเตอร์ลูกข่ายเชื่อมต่อกับอินเทอร์เน็ต และ offline mode

๒.๕.๒ ระบบสามารถป้องกันข้อมูลรั่วไหลจากการใช้งานอินเทอร์เน็ตแอปพลิเคชัน โดยมีคุณลักษณะเฉพาะอย่างน้อยดังต่อไปนี้

๑) เป็นระบบที่ออกแบบมาเพื่อป้องกันการรั่วไหลของข้อมูล (data protection) ผ่านแหล่งที่มาของการรั่วไหลการใช้งานอินเทอร์เน็ตแอปพลิเคชัน (Inline DLP)

๒) มี AI/ML เพื่อช่วยในการทำความเข้าใจพฤติกรรมข้อมูลผู้ใช้ได้อย่างรวดเร็วจากการใช้งานอินเตอร์เน็ตแอปพลิเคชัน

๓) สามารถมอนิเตอร์ข้อมูลที่ละเอียดอ่อนโดยแสดงข้อมูลผู้ใช้, แอปพลิเคชัน และประเภทเนื้อหา (content type) โดยเลือกแสดงผลตามกรอบเวลา (time frame) ที่ต้องการเพื่อช่วยในการวิเคราะห์การรั่วไหลของข้อมูลที่เกิดขึ้นได้

๔) สามารถกำหนดนโยบายในการควบคุมข้อมูลรั่วไหลโดยตั้งเงื่อนไขที่แตกต่างกันจาก user, groups, DLP engine, departments, URL categories, Cloud Applications, file type, data size และ time ได้

๕) รองรับการทำงานร่วมกับ Microsoft Information Protection (MIP) Labels เพื่อป้องกันการรั่วไหลของข้อมูลได้

๖) รองรับการกำหนด Action ได้อย่างน้อยดังต่อไปนี้ Allow, Block และส่งอีเมลเมื่อเกิดเหตุการรั่วไหลของข้อมูลไปให้ auditor ได้

๗) สามารถตั้งค่า end user notification เพื่อแสดงบนเครื่องลูกข่ายเมื่อเกิดเหตุการณ์ที่สอดคล้องกับการรั่วไหลของข้อมูล และสามารถแก้ไข (custom) ข้อความตามที่ต้องการได้

๘) มี password ป้องกันไม่ให้ผู้ใช้งานปิดการทำงาน, Logout จาก agent และ Uninstall agent ที่เป็นลักษณะ One Time Password (OTP) สำหรับผู้ใช้งานแต่ละคนได้

๙) มี password เฉพาะสำหรับผู้ดูแลระบบเพื่อปิดการทำงาน, Logout จาก agent และ Uninstall agent สำหรับใช้ในการแก้ไขปัญหาได้

๒.๕.๓ ระบบสามารถตรวจจับเอกสารสำคัญ และการอ่านข้อความจากภาพถ่าย โดยมีคุณลักษณะเฉพาะอย่างน้อยดังต่อไปนี้

๑) ระบบที่นำเสนอจะต้องมี Predefined dictionary หรือสามารถทำ custom dictionary ที่สามารถตรวจสอบข้อมูลลักษณะดังต่อไปนี้ได้เป็นอย่างน้อย

๑.๑) สามารถตรวจสอบข้อมูลระบุตัวตน Personally identifiable information (PII) เช่น หมายเลขบัตรประจำตัวประชาชนประเทศไทย (Thailand Identity Card Number) ได้

๑.๒) สามารถตรวจสอบข้อมูลบัตรเครดิต ดังต่อไปนี้ได้ American Express, Amex, JCB, Master card และ Visa เป็นต้น

๑.๓) สามารถตรวจสอบจับข้อมูล Source Code เช่น Python, Perl, Ruby, Visual Basic, และ C ได้

๑.๔) รองรับการตรวจจับ Passport และ Driver License ได้

๑.๕) วิธีการจำแนกหรือตรวจสอบข้อมูลที่มีความละเอียดอ่อน ด้วยวิธีการดังต่อไปนี้

- Predefined dictionaries จากระบบ
- Patterns หรือการกำหนดรูปแบบหรือกลุ่มคำ (Regular Expression)
- Phrases, ข้อความ หรือ keyword
- Indexed Document Match (IDM) เพื่อทำตรวจจับลายนิ้วมือเอกสารสำคัญที่มีข้อมูลละเอียดอ่อน (fingerprint)
- Exact Data Match (EDM) เพื่อตรวจสอบข้อมูลที่มีโครงสร้าง (structured data) ตามเกณฑ์ที่กำหนดไว้ล่วงหน้า เช่น อนุญาตให้พนักงานแชร์ข้อมูล PII ของตนเองโดยการใช้อีเมลส่วนตัวได้
- Optical Character Recognition (OCR) ป้องกันข้อมูลรั่วไหล จากการสแกนหาข้อความ text ที่ละเอียดอ่อนจากการส่งไฟล์รูปภาพผ่าน inline DLP ได้

๒) สามารถทำ content inspection เพื่อตรวจสอบการรั่วไหลของข้อมูล โดยรองรับไฟล์ที่มีขนาดใหญ่สูงสุดที่ ๔๐๐ MB ได้เป็นอย่างน้อย

๓) สามารถสร้าง DLP Engine โดยการกำหนด Expression ระหว่าง DLP Dictionaries ด้วยการใช้ Operator ได้แก่ All (AND), Any (OR), Exclude (AND NOT) และ Sum เพื่อกำหนดนโยบายในการตรวจสอบข้อมูลรั่วไหลได้สอดคล้องกับความต้องการที่กำหนด

๔) สามารถเลือกระดับความแม่นยำ (match accuracy) หรือเปอร์เซ็นต์ของความคล้ายคลึงกันของเอกสารที่มีการทำ Indexed Document Match (IDM) เช่นใกล้เคียงในระดับ Low, Medium และ High ได้

๕) มีเครื่องมือในการสร้างเทมเพลตของ Indexed Document Match (IDM) และ Exact Data Match (EDM) เพื่อไม่ให้เอกสารต้นฉบับรั่วไหลออกภายนอก

๒.๕.๔ ระบบสามารถบริหารจัดการกับเหตุการณ์ข้อมูลรั่วไหลที่ตรวจจับ โดยมีคุณลักษณะเฉพาะอย่างน้อยดังต่อไปนี้

๑) สามารถเรียกดูรายละเอียดเหตุการณ์ที่เกิดขึ้น (Incident) ประกอบด้วย วัน, เวลา, ชื่อผู้ที่ทำการละเมิด, Device name, Device OS, Department, ประเภทของ Source DLP (inline, endpoint), Client IP, นโยบายที่ละเมิด, DLP dictionaries, ชื่อของ manager, แอปพลิเคชัน หรือ URL, ช่องทางการรั่วไหลของข้อมูล (Channel), ชื่อไฟล์, ประเภทของไฟล์, ค่า hash ของไฟล์ และขนาดของไฟล์

๒) ทำ Notify แจ้งผู้ใช้งานที่เกี่ยวข้องกับ DLP incident ผ่านช่องทาง Email, Slack และ Teams ได้

๓) สามารถปรับเปลี่ยน priority หรือ incident severity และ Incident status เช่น Close incident, notify user, Escalate, Investigating, Assign DLP Admin, Ticket, Label และ Delete ได้

๔) สามารถทำการ Escalate DLP incident ไปยัง manager ของผู้ใช้งานเพื่อขออนุมัติได้

๕) สามารถระบุ note หรือ ข้อมูลเพิ่มเติมเกี่ยวกับ DLP incident ได้

๖) สามารถกำหนด DLP admin เพื่อจัดการกับ incident ที่ตรวจพบได้

๗) รองรับการสร้าง ticket โดยการทำงานร่วมกับ ServiceNow หรือ Jira ได้

๘) สามารถกำหนด Label ให้กับ DLP incident ได้

๙) สามารถลบ incident ที่ผ่านการตรวจสอบแล้วได้

๑๐) สามารถ Reopen เพื่อเปลี่ยนสถานะของ incident จาก resolved เป็น investigating ได้

๒.๕.๕ ระบบสามารถป้องกันภัยคุกคามทางไซเบอร์จากการใช้งานอินเทอร์เน็ต โดยมีคุณลักษณะเฉพาะอย่างน้อยดังต่อไปนี้

๑) สามารถทำ SAML และ SCIM ร่วมกับ Microsoft Entra ID (Azure AD) หรือ Microsoft Active Directory หรือ Okta ในการทำ user authentication และ provisioning หรือ Synchronize ข้อมูลผู้ใช้งานจาก Lightweight Directory Access Protocol (LDAP) ได้

๒) สามารถทำงานร่วมกับ Identity providers (IDPs) ได้ ๑๖ IdPs พร้อม ๆ กัน โดยไม่มีค่าใช้จ่ายเพิ่มเติม

๓) สามารถทำ SAML authentication ร่วมกับ Microsoft Entra ID (Azure AD) หรือ Okta หรือ สร้างผู้ใช้งานสำหรับกลุ่ม Administrators เพิ่มในระบบเพื่อใช้ในการบริหารจัดการระบบได้

๔) สามารถบริหารจัดการและควบคุมนโยบายการตรวจสอบ Data Loss Protection (DLP) ได้จากส่วนกลาง ในการทำ Data Discovery, Endpoint DLP policy, Inline DLP policy และการจัดการกับ DLP incident รวมทั้งรองรับการทำงานเป็น CASB เพื่อป้องกันข้อมูลรั่วไหลของข้อมูลผ่าน SaaS application ในอนาคตได้

๕) มีรายงาน (Reports) ที่แสดงจำนวนการใช้งาน sanctioned และ unsanctioned applications ตามการใช้งานของ users โดยแสดง application categories, risk index และการผ่านการรับรอง certifications ของแต่ละ application มากกว่า ๕๐,๐๐๐ cloud applications ได้

๖) สามารถ inspect SSL/TLS traffic โดยไม่มีปัญหาการเสื่อมประสิทธิภาพ (performance degradation) และไม่ต้องมีกระบวนการ manual ในการติดตั้ง SSL certificate บนเครื่องของผู้ใช้งาน

๗) รองรับการทำ File control เพื่อ block หรือ allow การดาวน์โหลด หรือ อัปโหลดไฟล์ไปยัง cloud application โดยควบคุมจาก user, group และ department ได้เป็นอย่างน้อย

๘) สามารถควบคุมนโยบายการเข้าถึงกลุ่ม cloud applications เช่น AI & ML, File sharing, Finance, Productivity & CRM, Instant Messaging, Webmail และ Social media เป็นต้น โดยสามารถควบคุมในระดับฟังก์ชันการใช้งานได้ เช่น อนุญาตให้ chat กับ instant messaging แต่ไม่อนุญาตให้ส่ง file และสามารถควบคุมการใช้งานได้จาก user, group, department, location และ time ได้เป็นอย่างน้อย

๙) มี Advanced Threat Protection ในการป้องกันภัยคุกคาม ได้แก่ phishing site, spyware, adware, botnets (command & control traffic), malware (virus, worm และ trojan), cryptomining, browser exploits, Cross Site Scripting (XSS) หรือ cookie stealing, P๒P file sharing และ unauthorized communication ได้

๑๐) สามารถป้องกันการเข้าถึง Website อันตราย หรือมีความเสี่ยงด้านความปลอดภัยได้ เช่น Computer Hacking, Copyright Infringement, Spyware/Adware, Weapons/Bombs และ Gambling เป็นต้น

๑๑) สามารถทำ tenancy restriction เพื่อจำกัดการเข้าถึง business และ personal accounts ของ cloud applications เช่น Microsoft, YouTube, Dropbox และ Google ได้

๑๒) สามารถจัดการกับ zero-day infections หรือ unknown threats สำหรับ file types ที่เป็น EXE และ DLL ได้

๑๓) มี password ป้องกันไม่ให้ผู้ใช้ปิดการทำงาน, Logout จาก agent และ Uninstall agent ที่เป็นลักษณะ One Time Password (OTP) สำหรับผู้ใช้งานแต่ละคนได้

๑๔) มี password เฉพาะสำหรับผู้ดูแลระบบเพื่อปิดการทำงาน, Logout จาก agent และ Uninstall agent สำหรับใช้ในการแก้ไขปัญหาได้

๑๕) การ update policy จากระบบจะต้องทำแล้วเสร็จทันที (หลักวินาที) โดยไม่ต้องมีการอัปเดต manual ใด ๆ จากผู้ใช้งาน

๑๖) สามารถเก็บ logs ในการใช้งานไว้ได้เป็นระยะเวลาอย่างน้อย ๖ เดือน หรือ ๑๘๐ วัน โดยที่ไม่มีค่าใช้จ่ายเพิ่มเติมได้

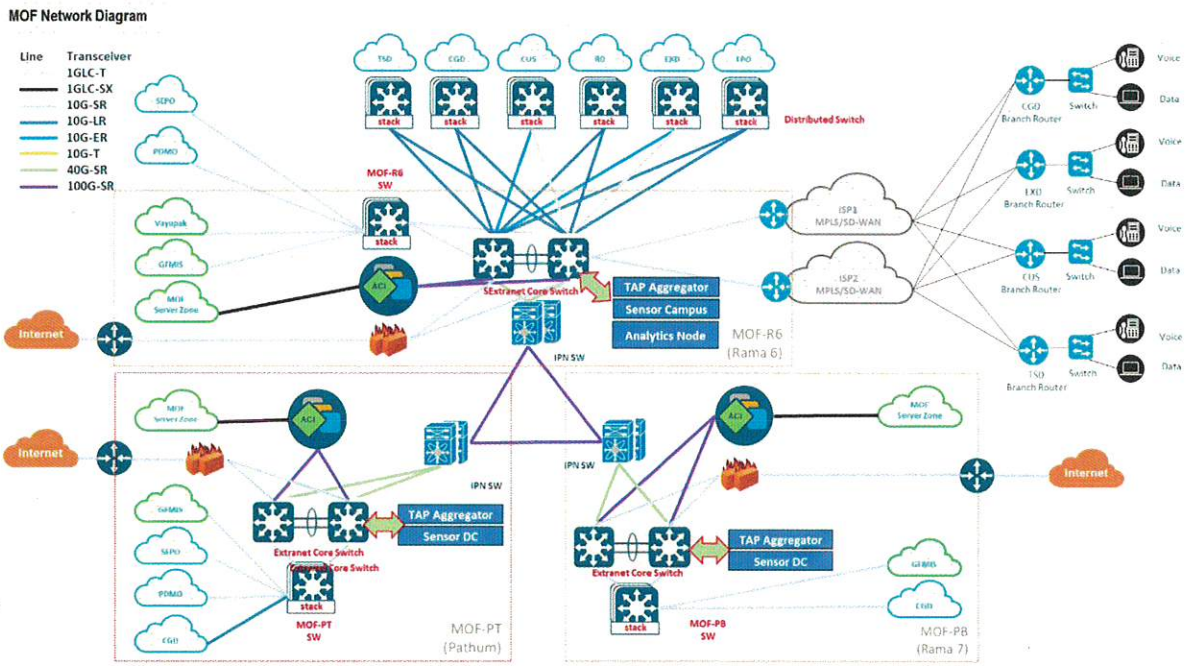
๑๗) ระบบจะต้องมี certificate เพื่อความน่าเชื่อถือ และตอบโจทย์มาตรฐานระดับสากลประกอบด้วย ISO ๒๗๐๐๑, ISO ๒๗๗๐๑, ISO ๒๗๐๑๘, ISO ๒๗๐๑๗, SOC ๒, CSA Star, FedRAMP High, NIST ๘๐๐-๖๓C, PCI/DSS, HIPAA และ GDPR เป็นอย่างน้อย

๑๘) มีรายงาน (reports) เพื่อดูรายละเอียดต่าง ๆ ได้แก่ Interactive reports , CIO report, CSO report, Executive insights report, Shadow IT report หรือ SaaS Security report, Quarterly business review (QBR) report และทำ Scheduling reports ได้

๑๙) ผลิตภัณฑ์ที่นำเสนอต้องอยู่ในกลุ่ม Leader ในการทำ Security Service Edge (SSE) จาก Gartner Magic Quadrant ปี ๒๐๒๔ หรือฉบับล่าสุดเท่านั้น

๓. แบบร่างแผนผังของระบบเครือข่ายสำหรับใช้ประกอบการออกแบบหรือการติดตั้งอุปกรณ์หรือระบบของโครงการยกระดับความปลอดภัยไซเบอร์ และป้องกันการรั่วไหลของข้อมูล

๓.๑. แบบร่าง System Diagram Architecture ที่เป็นความต้องการเบื้องต้นสำหรับให้ผู้ชนะการประกวดราคาใช้ประกอบการพิจารณาปรับปรุงหรือนำไปออกแบบให้เหมาะสมกับอุปกรณ์ที่เสนอเพื่อให้ระบบสามารถใช้งานได้อย่างมีประสิทธิภาพ



แผนภาพแสดง แนวทางการเชื่อมโยงระบบเครือข่ายสื่อสารข้อมูลกลางกระทรวงการคลัง

รายละเอียดการดำเนินงาน การติดตั้งและการทดสอบ

๑. การติดตั้งและสถานที่ติดตั้งอุปกรณ์ระบบคอมพิวเตอร์และเครือข่ายสื่อสาร

๑.๑. ต้องดำเนินการส่งมอบอุปกรณ์และติดตั้งพร้อมเดินสายสัญญาณหรือระบบไฟฟ้าในโครงการยกระดับความปลอดภัยไซเบอร์ และป้องกันการรั่วไหลของข้อมูล

๑.๒. ต้องส่งมอบอุปกรณ์หรืองานทั้งหมดตามโครงการ ณ อาคาร ๑๕๐ ปี กระทรวงการคลัง และนำไปติดตั้งที่อาคาร ๑๕๐ ปี กระทรวงการคลัง และศูนย์คอมพิวเตอร์กระทรวงการคลังที่เกี่ยวข้อง หรือตามที่คณะกรรมการตรวจรับพัสดุกำหนด

๑.๓. การเดินสายสัญญาณหรือสายไฟฟ้า (Cabling) ณ สถานที่ติดตั้ง ผู้ชนะการประกวดราคาต้องจัดหาราง หรือท่อหรือเฟล็กซ์ หรืออุปกรณ์อื่น ๆ ตามความจำเป็น สำหรับใช้ติดตั้งสายสัญญาณหรือสายไฟฟ้าตามโครงการและจัดให้เป็นระเบียบเรียบร้อย หรือเป็นไปตามมาตรฐานสากล

๒. การบริหารจัดการและเงื่อนไขในการดำเนินงาน

๒.๑. ผู้ชนะการประกวดราคาต้องเสนอโครงสร้างการบริหารโครงการและแผนการดำเนินงาน เพื่อให้คณะกรรมการตรวจรับพัสดุพิจารณาก่อนดำเนินงาน โดยแผนการดำเนินงานต้องระบุความรับผิดชอบในส่วนของผู้ชนะการประกวดราคา หรือบริษัทเจ้าของผลิตภัณฑ์ หรือส่วนของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง

๒.๒. ผู้ชนะการประกวดราคา ต้องจัดทำแผนการดำเนินงานหลัก (Master Plan) และแผนการดำเนินงานในรายละเอียด (Action Plan) และแผนการดำเนินงานอื่นๆ ที่ประกอบด้วยตารางการปฏิบัติงาน ขั้นตอนในการดำเนินการ/ขั้นตอนในการปฏิบัติงาน ผู้รับผิดชอบงานแต่ละขั้นตอน ผลงานที่จะส่งมอบ ระยะเวลาที่ใช้ในแต่ละขั้นตอน เพื่อใช้ในการบริหารและติดตามผลการดำเนินงานให้ครอบคลุมการดำเนินงานทั้งหมด

๒.๓. ผู้ชนะการประกวดราคาต้องจัดให้มีบุคลากรผู้เชี่ยวชาญที่มีประสบการณ์ในการทำงาน ประกอบด้วย

๑) ผู้บริหารโครงการ (Project Manager) จำนวน ๑ คน มีความชำนาญและประสบการณ์ในการควบคุมและบริหารโครงการมาแล้วไม่น้อยกว่า ๓ ปี

๒) Project Coordinator จำนวน ๑ คน โดยมีประสบการณ์ด้านการดูแล ประสานงาน และบริหารจัดการด้านงานเอกสาร ไม่น้อยกว่า ๒ ปี

๓) Network Engineer จำนวน ๒ คน โดยมีประสบการณ์ด้านการดูแลแก้ไขระบบเครือข่าย ไม่น้อยกว่า ๒ ปี และต้องมี Certificate CCNA หรือ Certificate CompTIA Network+ โดย Certificate ที่ยื่นเสนอมาจะต้องไม่หมดอายุ ในวันยื่นประกวดราคา

๔) System Engineer จำนวน ๒ คน โดยมีประสบการณ์ด้านระบบรักษาความปลอดภัยไม่น้อยกว่า ๒ ปี และต้องมี Certificate CompTIA Security+ โดย Certificate ที่ยื่นเสนอมา จะต้องไม่หมดอายุในวันยื่นประกวดราคา

๕) Support Engineer จำนวน ๑ คน โดยมีประสบการณ์ด้านการดูแลระบบคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศ ไม่น้อยกว่า ๒ ปี

๖) ต้องดำเนินการตรวจสอบหรือปฏิบัติงานเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ณ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือสถานที่ที่กำหนด หลังส่งมอบงานงวดสุดท้ายเสร็จสมบูรณ์ จำนวนอย่างน้อย ๑ คน โดยเข้าปฏิบัติงานเวลาทำการ ๐๘.๓๐ - ๑๖.๓๐ น. (ยกเว้นวันหยุดราชการ) ตลอดระยะเวลาการรับประกัน และต้องจัดทำรายงานผลการปฏิบัติงานตามที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง กำหนด

๗) ต้องดำเนินการตรวจสอบหรือปฏิบัติงานเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศแบบ Online หรือ Remote Support หลังส่งมอบงานงวดสุดท้ายเสร็จสมบูรณ์ จำนวนอย่างน้อย ๑ คน โดยปฏิบัติงานเวลาทำการ ๐๘.๓๐ - ๑๖.๓๐ น. (ยกเว้นวันหยุดราชการ) ตลอดระยะเวลาการรับประกัน และต้องจัดทำรายงานผลการปฏิบัติงานตามที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง กำหนด

๘) บุคลากรด้านอื่นๆ ที่เห็นว่าจำเป็นต่อการดำเนินโครงการ (ถ้ามี)

๒.๔. ต้องเสนอจำนวนบุคลากรตามที่กำหนดหรือสามารถเสนอเพิ่มให้เพียงพอที่จะทำงานในด้านต่าง ๆ ได้ทันตามกำหนดเวลา และต้องระบุหน้าที่ความรับผิดชอบ ประวัติการศึกษา ประวัติการทำงาน ประสบการณ์ ตำแหน่งหน้าที่ หรือผลงานของบุคลากรแต่ละคน พร้อมสำเนาหลักฐานที่แสดงว่า ได้ผ่านการฝึกอบรมเกี่ยวกับระบบที่เสนอ หรือการพัฒนาระบบในลักษณะเดียวกับระบบที่เสนอมาแล้วจากผู้ผลิตโดยตรง หรือสถาบันการฝึกอบรมที่ผ่านการรับรอง

๒.๕. ในกรณีที่คณะกรรมการตรวจรับพัสดุและ/หรือผู้แทนของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง เห็นว่าบุคลากรตามเสนอมา มีคุณสมบัติไม่เหมาะสมหรือทำงานไม่มีประสิทธิภาพ ผู้ชนะการประกวดราคาต้องดำเนินการปรับเปลี่ยนโดยทันทีที่ได้รับแจ้ง ทั้งนี้ ผู้ชนะการประกวดราคาจะอ้างการปรับเปลี่ยนนี้นำมาเป็นเหตุของการล่าช้าของงานไม่ได้

๒.๖. กรณีที่บุคลาการตามที่กำหนดไม่สามารถเข้าปฏิบัติงานได้ ผู้ชนะการประกวดราคาต้องจัดหาบุคลากรเพื่อมาปฏิบัติงานทดแทน พร้อมแจ้งชื่อผู้มาปฏิบัติงานแทนล่วงหน้าอย่างน้อย ๑ วัน ยกเว้นกรณีฉุกเฉิน

๒.๗. ผู้ชนะการประกวดราคาต้องเสนอรายงานความก้าวหน้าการดำเนินงานให้คณะกรรมการตรวจรับพัสดุและ/หรือผู้แทน ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลังทราบอย่างน้อยเดือนละครั้ง จนกว่างานจะแล้วเสร็จ

๓. การทดสอบและตรวจรับ

๓.๑. ผู้ชนะการประกวดราคาต้องส่งมอบอุปกรณ์ให้คณะกรรมการตรวจรับพัสดุ ณ สถานที่ติดตั้งที่คณะกรรมการตรวจรับพัสดุกำหนด โดยส่งมอบให้สำนักงานปลัดกระทรวงการคลังตามงวดงานที่กำหนดในเอกสารขอบเขตของงาน (TOR)

๓.๒. ผู้ชนะการประกวดราคาต้องติดตั้งและทดสอบการทำงานของอุปกรณ์และระบบทุกอย่างที่เสนอได้อย่างถูกต้องครบถ้วนสมบูรณ์

๓.๓. ผู้ชนะการประกวดราคาต้องเสนอเอกสารซึ่งประกอบด้วย รายละเอียดของอุปกรณ์ Configuration Diagram ทั้งหมด ข้อมูลวิธีการและขั้นตอนการตรวจรับของแต่ละอุปกรณ์โดยละเอียด

๓.๔. ผู้ชนะการประกวดราคาต้องจัดเตรียมอุปกรณ์สำหรับใช้งานหรือสนับสนุนการ Configuration และการทดสอบระบบ ในช่วงระยะเวลาของการติดตั้ง ทดสอบ ฝึกอบรม บำรุงรักษา และนำกลับคืนเมื่อเสร็จสิ้นการใช้งาน โดยต้องเสนอรายละเอียดของอุปกรณ์ให้คณะกรรมการตรวจรับพัสดุร่วมพิจารณาก่อนนำมาใช้

๓.๕. ผู้ชนะการประกวดราคาต้องออกแบบและจัดทำห้องศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Security Operation Center : SOC) และห้องประชุม ณ พื้นที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง หรือตามที่คณะกรรมการตรวจรับพัสดุกำหนด สำหรับให้เจ้าหน้าที่ของผู้ชนะการประกวดราคาหรือเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเข้าปฏิบัติงานร่วมกันเพื่อเฝ้าระวังและบริหารจัดการระบบรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของกระทรวงการคลัง ในช่วงระยะเวลาการรับประกัน โดยดำเนินการดังนี้

๑) ออกแบบและปรับปรุงห้องประชุมเดิมเพื่อจัดสรรพื้นที่สำหรับการปฏิบัติงานของเจ้าหน้าที่ และสำหรับการประชุมบริหารจัดการหรือแก้ไขปัญหาด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

๒) จัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานหรือการประชุม เช่น โต๊ะหรือเก้าอี้ ตามความจำเป็น (ถ้ามี) หรือตามที่คณะกรรมการตรวจรับพัสดุกำหนด

๓) จัดหาอุปกรณ์หรือระบบจอแสดงภาพสำหรับนำเสนอ หรือทำการย้ายระบบจอแสดงภาพ (Video Wall) เดิมเพื่อให้ห้อง SOC และห้องประชุมพร้อมใช้งาน ตามที่คณะกรรมการตรวจรับพัสดุกำหนด

๔) จัดหาสิ่งอำนวยความสะดวกที่จำเป็นสำหรับสนับสนุนการปฏิบัติงานในห้อง SOC และห้องประชุม ประกอบด้วย Notebook หรือ Tablet หรืออุปกรณ์อื่น ๆ ที่จำเป็น รวมจำนวนอย่างน้อย ๑๕ ชุด โดยต้องเสนอคุณลักษณะเฉพาะให้คณะกรรมการตรวจรับพัสดุพิจารณาก่อนจัดหาและต้องสามารถใช้งานได้ตลอดระยะเวลาการรับประกัน

๓.๖. ผู้ชนะการประกวดราคาต้องจะต้องถ่ายทอดความรู้ในการบริหารจัดการระบบให้กับเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง และบุคลากรที่เกี่ยวข้อง เพื่อให้สามารถใช้งานอุปกรณ์หรือระบบในโครงการได้อย่างมีประสิทธิภาพ

๓.๗. คณะกรรมการตรวจรับพัสดุและ/หรือผู้แทนของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และ/หรือผู้แทนสำนักงานปลัดกระทรวงการคลัง ที่เข้าร่วมดูแลการติดตั้งจะดำเนินการตรวจรับงานเฉพาะในเวลาทำการปกติ คือ ๐๘.๓๐ - ๑๖.๓๐ น. เว้นวันเสาร์ - อาทิตย์ และวันหยุดราชการ ในกรณีที่ผู้ชนะการประกวดราคามีความจำเป็นต้องตรวจรับงานนอกเหนือจากเวลาดังกล่าวจะต้องแจ้งให้สำนักงานปลัดกระทรวงการคลังทราบ พร้อมทั้งจะต้องรับผิดชอบค่าใช้จ่ายในการปฏิบัติงาน (ถ้ามี)

๓.๘. คณะกรรมการตรวจรับพัสดุและ/หรือผู้แทนของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และ/หรือผู้แทนสำนักงานปลัดกระทรวงการคลัง สงวนสิทธิที่จะเข้าทดสอบและตรวจสอบการทำงานของอุปกรณ์หรือระบบที่ติดตั้ง ตามสถานที่ที่กำหนด เพื่อดำเนินการตรวจรับงาน โดยผู้ชนะการประกวดราคาจะต้องอำนวยความสะดวกในการเดินทางหรือรับผิดชอบในค่าใช้จ่ายในการปฏิบัติงาน (ถ้ามี)

๓.๙. สำนักงานปลัดกระทรวงการคลัง สามารถที่จะนำอุปกรณ์ และ/หรือ งานในส่วนที่ส่งมอบแล้วไปใช้งานตามที่สำนักงานปลัดกระทรวงการคลังเห็นสมควร โดยที่ไม่กระทบกระเทือนหรือเป็นอุปสรรคในการทำงานของผู้ชนะการประกวดราคา โดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลังเพียงแต่แจ้งให้ผู้ชนะการประกวดราคาทราบ แต่หากการทดสอบอุปกรณ์/ระบบ ไม่ผ่านเงื่อนไขและเป็นเหตุให้ต้องเลิกสัญญาอันเนื่องมาจากความผิดพลาดของผู้ชนะการประกวดราคา ผู้ชนะการประกวดราคาไม่มีสิทธิเรียกร้องค่าใช้จ่ายหรือค่าเสียหายใดๆ จากสำนักงานปลัดกระทรวงการคลัง

๓.๑๐. หากมีข้อความใดในข้อกำหนดฉบับนี้ที่มีความขัดแย้งกัน ให้ยึดถือตามข้อกำหนดที่เป็นประโยชน์กับสำนักงานปลัดกระทรวงการคลัง

รายละเอียดการฝึกอบรมและคู่มือการใช้งาน

๑. รายละเอียดการฝึกอบรม

ผู้ชนะการประกวดราคาจะต้องจัดให้มีการฝึกอบรมทั้งภาคทฤษฎีและภาคปฏิบัติให้กับบุคลากรด้านต่าง ๆ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง เพื่อรองรับการปฏิบัติงานได้อย่างมีประสิทธิภาพ โดยต้องทำตามข้อกำหนดอย่างน้อย ดังนี้

๑.๑. ผู้ชนะการประกวดราคาต้องจัดฝึกอบรมเกี่ยวกับอุปกรณ์ที่ส่งมอบตามโครงการ และการบริหารระบบสำหรับผู้ดูแลระบบ โดยมีผู้เข้าอบรมอย่างน้อย ๕ คน ให้ผู้เข้าอบรมได้ใช้อุปกรณ์แบบ Hands on และมีเนื้อหาในด้านการทำงานของระบบ การใช้งาน การบำรุงรักษา เพื่อให้ผู้เข้าอบรมสามารถใช้งานอุปกรณ์ได้เป็นอย่างดี ดังนี้

๑) หลักสูตรด้าน IT Support เช่น CompTIA A+ พร้อมสอบใบรับรอง Certificate หรือตามที่คณะกรรมการตรวจรับพัสดุพิจารณา

๒) หลักสูตรอื่น ๆ ที่เกี่ยวเนื่องกับอุปกรณ์หรือซอฟต์แวร์ที่ส่งมอบตามโครงการ โดยรูปแบบการอบรมในลักษณะ On The Job Training

๒.๑.) ระบบตรวจสอบการทำงานและช่องโหว่ของระบบเครือข่าย

๒.๒.) อุปกรณ์วิเคราะห์ข้อมูลภัยคุกคามระบบเครือข่าย

๒.๓.) อุปกรณ์คัดกรองข้อมูลระบบเครือข่าย (TAP Aggregator)

๒.๔.) การใช้งานหรือการแก้ปัญหา ระบบป้องกันการรั่วไหลของข้อมูล (Data Leakage Prevention)

๒.๕.) หลักสูตรอื่นๆ ที่เห็นว่าเป็นประโยชน์ในการปฏิบัติงาน (ถ้ามี)

๑.๒. ผู้ชนะการประกวดราคาต้องจัดทำแผนการฝึกอบรมเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร พร้อมหัวข้อการฝึกอบรมแต่ละหลักสูตร ให้คณะกรรมการตรวจรับพัสดุพิจารณาก่อนดำเนินการ โดยที่หัวข้อการฝึกอบรมต้องครอบคลุมเนื้อหาทั้งหมดที่เกี่ยวกับการใช้งานระบบและการดูแลรักษาอย่างละเอียด ซึ่งผู้เข้าอบรมจะสามารถใช้งานระบบดังกล่าวได้เป็นอย่างดี และเนื้อหาในเอกสารการฝึกอบรมต้องเป็นของอุปกรณ์ที่ส่งมอบตามโครงการ

๑.๓. ผู้ชนะการประกวดราคาต้องเสนอและจัดทำแผนการฝึกอบรม ก่อนที่จะดำเนินการฝึกอบรม โดยมีรายละเอียดไม่น้อยกว่าที่กำหนดอย่างน้อยดังนี้

๑) ชื่อวิชา (Title)

๒) เนื้อหา (Content)

๓) กลุ่มผู้เรียน (Target Group)

๔) กำหนดวันที่จะฝึกอบรม (Timing)

๕) ระยะเวลาที่จะต้องใช้ (Duration)

๖) วิธีการสอน (เช่น Workshop, การบรรยาย)

๗) สถานที่ทำการสอน (Location)

๘) จำนวนคนในชั้น (ClassSize)

๙) Training Course Material เช่น คู่มือ เป็นต้น

๑.๔. คณะกรรมการตรวจรับพัสดุขอสงวนสิทธิที่จะเลือกหรือปรับปรุงเนื้อหา หัวข้อการฝึกอบรมแต่ละหลักสูตร และกำหนดการที่จัดอบรม โดยจะหารือกับผู้ชนะการประกวดราคาก่อนการอบรม

๑.๕. ผู้ชนะการประกวดราคาต้องจัดเตรียมอุปกรณ์ อาหารและเครื่องดื่ม พาหนะรับส่ง อุปกรณ์สำหรับการสาธิตและภาคปฏิบัติ และเอกสารฝึกอบรม

๑.๖. ผู้ชนะการประกวดราคาต้องรับผิดชอบในการจัดการฝึกอบรมในหลักสูตรเดิมหรือหลักสูตรใหม่ ทั้งหมดหรือบางส่วนของหลักสูตรอีกครั้ง หากคณะกรรมการตรวจรับพัสดุ หรือผู้แทนจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลัง เห็นว่าผลการฝึกอบรมที่ผ่านมานั้นมีเนื้อหาไม่ครอบคลุมเพียงพอหรือการถ่ายทอดไม่ครบถ้วนตรงตามหลักสูตรที่ได้ตกลงไว้

๑.๗. การจัดฝึกอบรมต้องดำเนินการให้แล้วเสร็จภายในระยะเวลาส่งมอบงานหรือระยะเวลาการรับประกันผลงาน ตามความเหมาะสมที่คณะกรรมการตรวจรับพัสดุพิจารณา

๒. คู่มือการใช้งาน

๒.๑. ผู้ชนะการประกวดราคาต้องจัดหาหรือจัดทำและส่งมอบคู่มือการใช้งานอุปกรณ์หรือระบบที่มีการติดตั้งและใช้งานในโครงการทั้งหมด ให้กับผู้ซื้อในวันที่ส่งมอบโครงการหรืองานงวดสุดท้าย

๒.๒. ผู้ชนะการประกวดราคาต้องส่งมอบคู่มือ Technical Manual, Systems Administrator Manual, Operation Manual และวิธีการแก้ปัญหาในลักษณะ (Troubleshooting) ที่เกี่ยวข้องกับระบบคอมพิวเตอร์ Hardware และ Software ในโครงการนี้ (ภาษาไทยหรือภาษาอังกฤษ) ในรูปแบบเอกสารกระดาษ (Hard Copy) จำนวน ๑ ชุด และเอกสารอิเล็กทรอนิกส์ (Soft file) โดยบันทึกใน Thumb Drive จำนวน ๑ ชุด

๒.๓. ผู้ชนะการประกวดราคาต้องจัดทำคู่มือการฝึกอบรม (Operational and Training Document) ในรูปแบบภาษาไทยหรือภาษาอังกฤษให้ถูกต้องและง่ายต่อการเข้าใจ สำหรับใช้ในการฝึกอบรม ในรูปแบบเอกสารกระดาษ (Hard Copy) จำนวน ๑ ชุด ต่อผู้เข้ารับการอบรม ๑ คน และส่งในรูปแบบเอกสารอิเล็กทรอนิกส์ (Soft file) ประเภท PDF โดยบันทึกใน Thumb Drive จำนวน ๑ ชุด

๒.๔. ผู้ชนะการประกวดราคาต้องปรับปรุงเอกสารหรือคู่มือการใช้งานอุปกรณ์หรือระบบ ในกรณีที่ระบบมีการปรับปรุงหรือปรับเปลี่ยนการทำงานของอุปกรณ์หรือระบบ เพื่อให้ได้เอกสารหรือคู่มือการใช้งานอุปกรณ์หรือระบบ ที่มีความทันสมัยและเป็นปัจจุบัน โดยไม่คิดค่าใช้จ่ายเพิ่มจากผู้ซื้อ

เงื่อนไขการรับประกันผลงานและความชำรุดบกพร่องและการบำรุงรักษาและซ่อมแซมแก้ไข

ผู้ชนะการประกวดราคาต้องบำรุงรักษา ซ่อมแซมแก้ไขหรือเปลี่ยนทดแทนอุปกรณ์ที่ส่งมอบในโครงการทั้งหมด เป็นระยะเวลา ๓ ปี นับตั้งแต่คณะกรรมการตรวจรับพัสดุได้ตรวจรับงานงวดสุดท้ายเสร็จสมบูรณ์ โดยต้องปฏิบัติตามเงื่อนไขดังต่อไปนี้

๑. การบำรุงรักษาแบบป้องกัน (Preventive Maintenance)

ผู้ชนะการประกวดราคาต้องเสนอแผน และทำการบำรุงรักษา (Preventive Maintenance) ดังนี้

๑.๑. ผู้ชนะการประกวดราคาต้องทำการบำรุงรักษา (Preventive Maintenance) อุปกรณ์และระบบที่ส่งมอบในโครงการ อย่างน้อย ๓ ครั้ง ตลอดระยะเวลารับประกัน เพื่อให้ระบบอยู่ในสภาพที่ใช้งานได้อย่างมีประสิทธิภาพตลอดเวลา โดยทำการบำรุงรักษาในช่วงระยะเวลาที่ไม่ส่งผลกระทบต่อการปฏิบัติงานของสำนักงานปลัดกระทรวงการคลัง และจะต้องแจ้งให้ทราบล่วงหน้าอย่างน้อย ๕ วันทำการ ในทุกครั้งที่เข้าดำเนินการบำรุงรักษา

๑.๒. เมื่อมีการเปลี่ยนแปลง แก้ไข ปรับปรุงเพิ่มเติม Software ในลักษณะการ Upgrade หรือออก Version ใหม่ของอุปกรณ์ในโครงการให้ทันสมัยขึ้น ผู้ชนะการประกวดราคาต้องแจ้งให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการคลังทราบ และทำการปรับปรุงเมื่อสำนักงานปลัดกระทรวงการคลังร้องขอให้มาติดตั้ง โดยไม่คิดค่าใช้จ่ายใด ๆ พร้อมทั้งนำเอกสารและคู่มือประกอบการใช้งาน (ถ้ามี) มามอบให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และต้องทำการอบรมให้เจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ถ้าเป็นสิ่งที่กระทบกับสภาพการดำเนินงานหรือมีผลให้การปฏิบัติงานเปลี่ยนไป

๒. การซ่อมแซมแก้ไข

๒.๑. หากอุปกรณ์หรือระบบชำรุด บกพร่อง หรือใช้งานไม่ได้ ถึงแม้ว่าจะติดตั้งอยู่ ณ สถานที่ใดตามที่กำหนดในสัญญา และความชำรุดนี้มิได้เกิดจากความผิดของสำนักงานปลัดกระทรวงการคลัง ผู้ชนะการประกวดราคาต้องเริ่มดำเนินการซ่อมแซมแก้ไขให้อยู่ในสภาพดีได้ดังเดิมโดยไม่คิดค่าใช้จ่ายใด ๆ จากสำนักงานปลัดกระทรวงการคลัง ภายใน ๔ ชม. (ในเวลาทำการ ๘.๓๐-๑๖.๓๐) นับตั้งแต่ได้รับแจ้ง

๒.๒. ในการซ่อมแซมแก้ไข หากผู้ชนะการประกวดราคาคาดว่าไม่สามารถดำเนินการได้แล้วเสร็จภายใน ๑๒ ชั่วโมง (ในเวลาทำการ ๘.๓๐-๑๖.๓๐) นับแต่เริ่มทำการซ่อมแซมแก้ไข ผู้ชนะการประกวดราคาสามารถนำเครื่องหรืออุปกรณ์สำรองที่มีประสิทธิภาพทัดเทียมกัน ที่สามารถทำให้การใช้งานเป็นปกติดังเดิม ซึ่งจะไม่ถือว่าเป็นเวลาที่เกิดเหตุขัดข้อง แต่ผู้ชนะการประกวดราคาต้องเร่งดำเนินการแก้ไขเครื่องหรืออุปกรณ์ ให้สามารถใช้งานได้ตามปกติ และนำมาเปลี่ยนทดแทน โดยเร็ว

๒.๓. สำนักงานปลัดกระทรวงการคลังยอมให้อุปกรณ์และระบบที่ส่งมอบในโครงการขัดข้องได้ไม่เกินเดือนละ ๔๘ ชั่วโมง (ในเวลาทำการ ๘.๓๐-๑๖.๓๐) โดยเริ่มนับเวลาตั้งแต่ที่เริ่มซ่อมแซมแก้ไขจนถึงเวลาที่ทำการซ่อมแซมแล้วเสร็จสมบูรณ์หรือเวลาที่ทำให้ระบบสามารถกลับมาทำงานได้ตามปกติ ถ้าการขัดข้องดังกล่าว มีระยะเวลาเกินเกณฑ์ที่กำหนด ผู้ชนะการประกวดราคาต้องถูกปรับในอัตราร้อยละ ๐.๐๒๕ ของราคาตามสัญญาต่อชั่วโมง เศษของชั่วโมง ให้นับเป็น ๑ ชั่วโมง

๓. การบริการและการสนับสนุน

ผู้ชนะการประกวดราคาจะต้องดำเนินการบริการและการสนับสนุน ตลอดระยะเวลารับประกัน โดยต้องปฏิบัติดังต่อไปนี้

๓.๑. จัดเจ้าหน้าที่ของผู้ชนะการประกวดราคามาปฏิบัติงานที่สำนักงานปลัดกระทรวงการคลัง ตามที่สำนักงานปลัดกระทรวงการคลังร้องขอ (On call) โดยไม่คิดค่าใช้จ่ายใด ๆ

๓.๒. ให้ความช่วยเหลือแก่ผู้บริหารจัดการระบบ (Administrator) และเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ตามที่สำนักงานปลัดกระทรวงการคลังร้องขอ (On call) โดยไม่คิดค่าใช้จ่ายใด ๆ

๓.๓. ให้คำปรึกษาแนะนำความรู้ในลักษณะของการถ่ายทอดเทคนิคและวิธีการปฏิบัติงานของระบบที่มีรายละเอียดเพิ่มเติมตามความต้องการของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้สามารถบริหารจัดการระบบเครือข่ายต่อไปได้ภายหลังติดตั้ง