

รายละเอียดคุณลักษณะเฉพาะ
จ้างเหมาบำรุงรักษาศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์
(Ministry Security Operation Center : MSOC) ประจำปีงบประมาณ พ.ศ. 2570

1. หลักการและเหตุผล

สำนักงานปลัดกระทรวงแรงงานเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศซึ่งมีหน้าที่ต้องปฏิบัติตามเพื่อให้สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 และต้องมีมาตรฐานในการรักษาความมั่นคงปลอดภัยเพื่อให้สอดคล้องกับกฎหมายอื่น ๆ ที่เกี่ยวข้อง เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ (ฉบับที่ 2) พ.ศ. 2560 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม เป็นต้น ซึ่งเป็นความจำเป็นที่สำนักงานปลัดกระทรวงแรงงานจะต้องดำเนินการพัฒนาขีดความสามารถในด้านความมั่นคงปลอดภัยไซเบอร์ให้สามารถป้องกัน (Protect) ตรวจจับ (Detect) และตอบสนอง (Response) ต่อภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของบริการดิจิทัลและข้อมูลในการดำเนินงานของสำนักงานปลัดกระทรวงแรงงานในการให้บริการประชาชนได้อย่างมีประสิทธิภาพ และส่งผลกระทบต่อการดำเนินงานหลักของสำนักงานปลัดกระทรวงแรงงานน้อยที่สุด

ในปีงบประมาณ พ.ศ. 2567 สำนักงานปลัดกระทรวงแรงงานได้ดำเนินการโครงการ ศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Ministry Security Operation Center : MSOC) โดยมีระบบป้องกันตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์ และระบบเครือข่าย (End-Point Protection and Network Protection) ระบบเฝ้าระวังและตอบสนองภัยคุกคามทางไซเบอร์ (Extended Detection and Response) ระบบตรวจประเมินความเสี่ยงความมั่นคงปลอดภัยไซเบอร์เพื่อค้นหาช่องโหว่และความเสี่ยงที่อาจเกิดขึ้นสำหรับระบบเครือข่าย เครื่องคอมพิวเตอร์แม่ข่าย เว็บแอปพลิเคชัน ระบบบริหารจัดการภัยคุกคามที่เกี่ยวข้อง และจัดตั้งห้องศูนย์ปฏิบัติการ MSOC เพื่อวางรากฐานด้านการป้องกันและตรวจจับภัยคุกคามทางไซเบอร์

ดังนั้น สำนักงานปลัดกระทรวงแรงงาน จึงมีความจำเป็นต้องดำเนินการจ้างเหมาบำรุงรักษาศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Ministry Security Operation Center : MSOC) เพื่อให้สามารถป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของบริการดิจิทัลและข้อมูลในการดำเนินงานของสำนักงานปลัดกระทรวงแรงงานในการให้บริการประชาชนได้อย่างมีประสิทธิภาพ

2. วัตถุประสงค์

2.1 เพื่อให้ระบบเครือข่ายและระบบสารสนเทศของกระทรวงแรงงานใช้งานได้อย่างต่อเนื่องและมั่นคงปลอดภัย เพื่อช่วยเฝ้าระวัง ตรวจจับ และตอบสนองต่อภัยคุกคามทางไซเบอร์ได้ทุกวันตลอด 24 ชั่วโมง

2.2 เพื่อให้การปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานเป็นไปอย่างต่อเนื่อง ลดความเสี่ยงจากเหตุขัดข้องในการเฝ้าระวัง ตรวจจับ วิเคราะห์ และตอบสนองต่อภัยคุกคาม ซึ่งอาจส่งผลกระทบต่อระบบสารสนเทศและการดำเนินงานของสำนักงานปลัดกระทรวงแรงงาน

2.3 เพื่อให้การบริหารจัดการเหตุการณ์ (Incident Response) มีความรวดเร็วและเป็นมาตรฐานโดยมีผู้เชี่ยวชาญคอยสนับสนุนเมื่อเกิดเหตุ รวมถึงช่วยวิเคราะห์ค้นหาต้นตอที่แท้จริงของปัญหา (Root Cause) การเก็บรักษา ค้นหา และวิเคราะห์หลักฐานเบื้องต้น และให้คำแนะนำเชิงเทคนิคได้อย่างถูกต้อง

3. คุณสมบัติของผู้ยื่นข้อเสนอ

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ในระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระงับชื่อไว้ในบัญชีรายชื่อผู้ทำงาน และได้แจ้งเวียนชื่อให้เป็นผู้ทำงานของหน่วยงานรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทำงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นนิติบุคคล ผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนออื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงานปลัดกระทรวงแรงงาน ณ วันยื่นข้อเสนอ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม ในการประกวดราคาอิเล็กทรอนิกส์ ครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นนั้น

3.10 ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ต้องมีคุณสมบัติ ดังนี้

(1) การกำหนดสัดส่วนในการเข้าร่วมค้าของคู่สัญญา

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงฯ จะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

(2) กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้น ต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

(3) การยื่นข้อเสนอของกิจการร่วมค้า

(3.1) กรณีที่ข้อตกลงฯ กำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่ง เป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

(3.2) การยื่นข้อเสนอด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding) ให้ผู้เข้าร่วมค้าที่ได้รับมอบหมายหรือมอบอำนาจตามข้อ (3.1) ดำเนินการซื้อเอกสารประกวดราคาอิเล็กทรอนิกส์ กรณีที่มีการจำหน่ายเอกสารซื้อหรือจ้าง

3.11 ผู้ยื่นข้อเสนอต้องลงทะเบียน ในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement: e-GP) ของกรมบัญชีกลาง

3.12 ผู้ยื่นข้อเสนอซึ่งเป็นผู้ประกอบการ SMEs แสดงสำเนาใบขึ้นทะเบียนผู้ประกอบการวิสาหกิจขนาดกลางและขนาดย่อม (SMEs) (ถ้ามี) มาพร้อมการยื่นข้อเสนอทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์

3.13 ผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า 1 ปี ต้องมีมูลค่าสุทธิของกิจการจากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สุทธิ ที่ปรากฏ งบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก 1 ปี สุดท้ายก่อนวันยื่นข้อเสนอ โดยแสดงสำเนาเอกสารหรือหลักฐานมาพร้อมการยื่นข้อเสนอของระบบจัดซื้อจัดจ้างด้วยอิเล็กทรอนิกส์

3.14 ผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งยังไม่มีกิจการรายงาน งบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้าให้พิจารณา การกำหนดมูลค่า ของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่ได้ชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ไม่ต่ำกว่า 2 ล้านบาท โดยแสดงสำเนาเอกสารหรือหลักฐานมาพร้อมการยื่นข้อเสนอของระบบจัดซื้อจัดจ้างด้วยอิเล็กทรอนิกส์

3.15 กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง (สินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุน หรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์ และประกอบธุรกิจค้าประกัน ตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคาร แห่งประเทศไทยแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อ ที่สำนักงานใหญ่รับรองหรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันที่ยื่นข้อเสนอไม่เกิน 90 วัน) โดยแสดงสำเนาแบบหนังสือรับรองวงเงินสินเชื่อ (ตามแบบที่กรมบัญชีกลางกำหนด) มาพร้อมการยื่นข้อเสนอของระบบจัดซื้อจัดจ้างด้วยอิเล็กทรอนิกส์

3.16 ผู้ยื่นข้อเสนอจะต้องเป็นผู้มีประสบการณ์ในการให้บริการหรือดูแลศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ให้กับหน่วยงานราชการ หรือ รัฐวิสาหกิจ หรือหน่วยงานเอกชน มีผลงานอย่างน้อยจำนวน 1 ผลงาน มูลค่าผลงานไม่น้อยกว่า 3.5 ล้านบาท พร้อมทั้งแนบสำเนาหนังสือรับรองผลงาน หรือสำเนาสัญญาจ้าง หรือ สำเนาใบสั่งซื้อกับหน่วยงานราชการ หรือ รัฐวิสาหกิจ หรือหน่วยงานเอกชน แสดงให้สำนักงานปลัดกระทรวงแรงงาน พิจารณาในวันยื่นเสนอราคา (ผลงานที่นำมาอ้างอิงนี้จะต้องเป็นผลงานของผู้ยื่นข้อเสนอโดยตรง ที่สิ้นสุดแล้ว)

4. ขอบเขตเอกสารข้อเสนอ

4.1 ผู้ยื่นข้อเสนอจะต้องทำตารางเปรียบเทียบรายละเอียดของข้อกำหนดจ้างเหมาบำรุงรักษาศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ Ministry Security Operation Center : MSOC ประจำปีงบประมาณ พ.ศ. 2570 ที่เสนอเป็นรายข้อ ตั้งแต่ข้อ 5 ถึงข้อสุดท้าย รวมถึงภาคผนวก โดยใช้ตัวอย่างแบบฟอร์มการเปรียบเทียบตามตารางที่ 1 ในการเปรียบเทียบรายการดังกล่าว หากมีกรณีที่ต้องมีการอ้างอิงข้อความหรือเอกสารในส่วนอื่นที่จัดทำเสนอมา ผู้ยื่นข้อเสนอต้องระบุให้เห็นอย่างชัดเจน สามารถตรวจสอบได้โดยง่ายไว้ในเอกสารเปรียบเทียบด้วยว่า สิ่งที่ต้องการอ้างอิงถึงนั้น อยู่ในส่วนใดตำแหน่งใดของเอกสารอื่นๆ ที่จัดทำเสนอมา สำหรับเอกสารที่อ้างอิงถึง ให้หมายเหตุหรือขีดเส้นใต้หรือระบายสีพร้อมเขียนหัวข้อกำกับไว้ เพื่อให้สามารถตรวจสอบกับเอกสารเปรียบเทียบได้ง่ายและตรงกันด้วย ทั้งนี้ผู้ยื่นข้อเสนอต้องส่งเอกสารเปรียบเทียบพร้อมเอกสารอ้างอิงทั้งหมด หากผู้ยื่นข้อเสนอไม่ดำเนินการตามข้อนี้คณะกรรมการฯ ขอสงวนสิทธิ์ในการไม่พิจารณาข้อเสนอของผู้ยื่นข้อเสนอ

ตารางที่ 1 ตารางเปรียบเทียบคุณสมบัติข้อกำหนดและรายละเอียดข้อเสนอ

อ้างอิงข้อ	ข้อกำหนด/อุปกรณ์ที่ต้องการ	ข้อกำหนด/อุปกรณ์ที่นำเสนอ	เปรียบเทียบ	เอกสารอ้างอิง
ระบุหัวข้อให้ตรงกับหัวข้อที่ระบุในเอกสารประกวดราคา	ให้คัดลอกคุณลักษณะเฉพาะที่สำนักงานปลัดกระทรวงแรงงานกำหนดมากรอกในช่องนี้	ให้ระบุคุณลักษณะเฉพาะที่ผู้ยื่นข้อเสนอเสนอ	ตรงตามข้อกำหนด/ดีกว่าข้อกำหนด	ระบุหมายเลขหน้าของเอกสารอ้างอิงของผู้ยื่นข้อเสนอ

4.2 ราคาที่เสนอ ต้องเป็นราคารวมทั้งโครงการ ทั้งนี้ต้องรวมภาษีมูลค่าเพิ่มและภาษีต่าง ๆ

4.3 ระบบงานที่ปรับปรุงหรือพัฒนาขึ้นทั้งหมดจะต้องเป็นลิขสิทธิ์ของสำนักงานปลัดกระทรวงแรงงานและผู้ยื่นข้อเสนอต้องไม่เปิดเผยข้อมูลที่เกิดขึ้นจากการดำเนินงานตามโครงการของสำนักงานปลัดกระทรวงแรงงาน

5. ขอบเขตงาน

ผู้รับจ้างจะต้องให้บริการดูแลบำรุงรักษาศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Ministry Security Operation Center : MSOC) ของสำนักงานปลัดกระทรวงแรงงาน โดยมีรายละเอียดดังนี้

5.1 คำนิยาม

5.1.1 ศูนย์ปฏิบัติการ MSOC หมายถึง ศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Ministry Security Operation Center : MSOC) ของสำนักงานปลัดกระทรวงแรงงาน

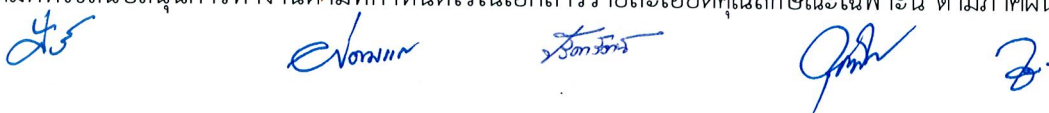
5.1.2 สิทธิการใช้งานซอฟต์แวร์ (License) หมายถึง สิทธิที่เจ้าของลิขสิทธิ์หรือผู้มีสิทธิในซอฟต์แวร์อนุญาตให้ผู้ใช้งานสามารถใช้ซอฟต์แวร์ได้ตามจำนวน ระยะเวลา และเงื่อนไขที่กำหนด โดยต้องเป็นสิทธิการใช้งานที่ถูกต้องตามกฎหมาย และมีผลตลอดระยะเวลาของสัญญา รวมถึงการต่ออายุสิทธิการใช้งานหรือ Software Subscription ตามที่กำหนด ไว้ในเอกสารรายละเอียดคุณลักษณะเฉพาะนี้

5.1.3 ฮาร์ดแวร์ (Hardware) หมายถึง ครุภัณฑ์ อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย และอุปกรณ์ที่เกี่ยวข้องกับศูนย์ปฏิบัติการ MSOC รวมถึงเครื่องคอมพิวเตอร์แม่ข่ายพร้อมซอฟต์แวร์บริหารจัดการคอมพิวเตอร์เสมือน อุปกรณ์กระจายสัญญาณ และอุปกรณ์อื่นที่ใช้สนับสนุนการทำงานตามที่กำหนดไว้ในเอกสารรายละเอียดคุณลักษณะเฉพาะนี้ ตามภาคผนวก ก

5.1.4 ซอฟต์แวร์ (Software) หมายถึง ระบบป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์และระบบเครือข่าย (Endpoint Protection and Network Protection) ระบบเฝ้าระวัง และตอบสนองต่อภัยคุกคามทางไซเบอร์ (Extended Detection and Response: XDR) และระบบตรวจประเมินความเสี่ยงความมั่นคงปลอดภัยไซเบอร์เพื่อค้นหาช่องโหว่และความเสี่ยงที่อาจเกิดขึ้นสำหรับระบบเครือข่าย เครื่องคอมพิวเตอร์แม่ข่าย และเว็บแอปพลิเคชัน รวมถึงซอฟต์แวร์ที่เกี่ยวข้องตามที่กำหนดไว้ในเอกสารรายละเอียดคุณลักษณะเฉพาะนี้ ตามภาคผนวก ก

5.1.5 การบำรุงรักษา หมายถึง การบำรุงรักษาเพื่อป้องกัน (Preventive Maintenance : PM) การบำรุงรักษาเพื่อซ่อมแซมแก้ไข (Corrective Maintenance : CM) การบำรุงรักษาเพื่อปรับเปลี่ยนตามความเปลี่ยนแปลง (Adaptive Maintenance) รวมถึงการบำรุงรักษา การปรับปรุง การอัปเดต และการดำเนินการอื่นใดที่เกี่ยวข้องตามที่กำหนดไว้ในเอกสารรายละเอียดคุณลักษณะเฉพาะนี้

5.1.6 ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์ฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ทั้งหมดที่ใช้สนับสนุนการทำงานตามที่กำหนดไว้ในเอกสารรายละเอียดคุณลักษณะเฉพาะนี้ ตามภาคผนวก ก



5.2 ผู้รับจ้างจะต้องส่งแผนการดำเนินงาน ภายใน 7 วัน นับจากวันเริ่มดำเนินงานตามสัญญา เพื่อให้คณะกรรมการตรวจรับพัสดุพิจารณาให้ความเห็นชอบแผนการดำเนินงาน จำนวน 1 ชุด ประกอบด้วย

5.2.1 แผนการดำเนินงานการบำรุงรักษาศูนย์ปฏิบัติการ MSOC ที่มีรายละเอียดอย่างน้อยดังนี้
กรอบแนวทางการดำเนินงาน แผนการดำเนินงาน กิจกรรมหลัก กิจกรรมย่อย ระยะเวลาการทำงาน

5.2.2 แผนการจัดสรรบุคลากร พร้อมโครงสร้างการทำงานของบุคลากร ที่ระบุชื่อ นามสกุล ตำแหน่ง ความรับผิดชอบ ช่องทางการติดต่อ และแนบเอกสารสัญญาไม่เปิดเผยข้อมูลที่เป็นความลับ (NDA) ทั้งนี้ กรณีมีการเปลี่ยนแปลงบุคลากรระหว่างการดำเนินงานต้องส่งให้คณะกรรมการตรวจรับพัสดุ พิจารณาให้ความเห็นชอบก่อนเริ่มดำเนินงาน

5.3 ผู้รับจ้างจะต้องดูแลบำรุงรักษาศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Ministry Security Operation Center : MSOC) ตามภาคผนวก ก ให้สามารถใช้งานได้ทุกวันตลอด 24 ชั่วโมง (ในเวลา 7 วัน x 24 ชั่วโมง) ตลอดระยะเวลาสัญญาจ้างเหมาบำรุงรักษา โดยมีระบบตรวจจับภัยคุกคามทางไซเบอร์และประเมินความเสี่ยงระบบสารสนเทศ ประกอบด้วย

5.3.1 ระบบป้องกัน ตรวจจับและตอบสนองต่อภัยคุกคาม (End-Point Protection, Network Protection, IPS, Agent Software) ประกอบด้วย

- (1) ระบบตรวจจับและป้องกันการโจมตีระบบเครือข่าย (Intrusion Prevention System)
- (2) Agent Software สำหรับป้องกันและตรวจจับภัยคุกคามในระดับเครื่องผู้ใช้ (Endpoint Sensor)
- (3) Agent Software สำหรับป้องกันและตรวจจับภัยคุกคามในระดับเครื่องแม่ข่าย (Server Sensor)

5.3.2 ระบบเฝ้าระวังและตอบสนองภัยคุกคาม (Extended Detection and Response, SOC Platform) ประกอบด้วย

- (1) ระบบตรวจจับภัยคุกคามขั้นสูงทางไซเบอร์บนระบบเครือข่าย
- (2) ระบบเฝ้าระวังและตอบสนองภัยคุกคามทางไซเบอร์ (Extended Detection and Response)
- (3) ระบบบริการผู้เชี่ยวชาญสำหรับค้นหาภัยคุกคามเชิงรุกและตอบสนองต่อภัยคุกคามอัตโนมัติ (SOC as a service)
- (4) ระบบตรวจประเมินความเสี่ยงความมั่นคงปลอดภัยไซเบอร์เพื่อค้นหาช่องโหว่และความเสี่ยงที่อาจเกิดขึ้นสำหรับระบบเครือข่าย เครื่องคอมพิวเตอร์แม่ข่าย และเว็บแอปพลิเคชัน

5.3.3 ระบบตรวจประเมินความเสี่ยง (Network Sensor, Attack Surface Risk Management) ประกอบด้วย

- (1) ระบบบริหารจัดการอุปกรณ์ตรวจจับป้องกันภัยคุกคามบนระบบเครือข่าย (Network Sensor)

5.4 ผู้รับจ้างจะต้องจัดให้มีบริการผู้เชี่ยวชาญสำหรับค้นหาภัยคุกคามเชิงรุกและตอบสนองต่อภัยคุกคามอัตโนมัติ (SOC as a Service) ทุกวันตลอด 24 ชั่วโมง (ในเวลา 7 วัน x 24 ชั่วโมง) ตลอดระยะเวลาสัญญาจ้างเหมาบำรุงรักษา

5.5 การบำรุงรักษาซอฟต์แวร์ (Software Maintenance) ครอบคลุมถึง License of Software Release upgrades หรือ License of Software version, Patches/Fixes, Software media, Document และตลอดระยะเวลาของสัญญานี้ สำนักงานปลัดกระทรวงแรงงานสามารถขอ Upgrade System Software และ Application Software ของระบบต่างๆ ที่สามารถทำงานบนฮาร์ดแวร์ (Hardware) เดิมได้ โดยไม่ต้องเสียค่าใช้จ่ายเพิ่มเติม ตามสิทธิประโยชน์ที่สำนักงานปลัดกระทรวงแรงงานพึงมีได้ และไม่ขัดต่อมาตรฐานของผลิตภัณฑ์นั้นๆ ทั้งนี้รวมถึง Software Subscription



5.6 กรณีที่สำนักงานปลัดกระทรวงแรงงาน มีความประสงค์จะปรับแต่งระบบ ให้มีประสิทธิภาพมากขึ้น รวมถึงการเคลื่อนย้ายเครื่องและอุปกรณ์สนับสนุนทั้งหมดที่อยู่ภายใต้ศูนย์ปฏิบัติการ MSOC เพื่อเพิ่มประสิทธิภาพดังกล่าว โดยค่าใช้จ่ายที่เกิดขึ้นทั้งหมดให้ถือเป็นภาระรับผิดชอบของผู้รับจ้าง

5.7 ผู้รับจ้างต้องรับประกันการชำรุดบกพร่องของการทำงานของระบบ ไม่ว่าจะเป็น Hardware หรือ Software กรณีที่มีค่าใช้จ่ายใด ๆ เกิดขึ้นในการบำรุงรักษา โดยค่าใช้จ่ายที่เกิดขึ้นทั้งหมดให้ถือเป็นภาระรับผิดชอบของผู้รับจ้าง

5.8 การดำเนินการใด ๆ ไม่ว่าจะเป็นส่วนของระบบ Hardware หรือ Software ที่มีผู้รับจ้างมีหน้าที่ดูแล หากมีปัญหาเกี่ยวกับลิขสิทธิ์ ผู้รับจ้างจะต้องดำเนินการขออนุญาตหรือทำข้อตกลงหรือทำสัญญาหรือทำการอย่างอื่นใดกับเจ้าของลิขสิทธิ์ เพื่อให้สามารถใช้สิทธิ์นั้น ๆ ได้อย่างถูกต้องตามกฎหมาย โดยให้ถือเป็นภาระและหน้าที่ของผู้รับจ้างเพียงฝ่ายเดียว

5.9 การซ่อมแซมแบบ Corrective Maintenance (CM) ดังนี้

5.9.1 หากระบบคอมพิวเตอร์ภายใต้ศูนย์ปฏิบัติการ MSOC ไม่สามารถใช้งานได้ตามปกติ ไม่ว่าจะเป็นกรณีปัญหาบางส่วนหรือทั้งระบบ ในเวลา 7 วัน x 24 ชั่วโมง (ตลอด 24 ชั่วโมงของทุกวันไม่เว้นวันหยุดราชการ) ผู้รับจ้างจะต้องจัดให้มีช่างที่มีความรู้ความชำนาญจัดการซ่อมแซมแก้ไขให้อยู่ในสภาพที่ใช้งานได้ดีตามปกติ และจะต้องซ่อมแซมโดยใช้อะไหล่แท้ ที่เป็นของใหม่เท่านั้น ที่มีคุณสมบัติเทียบเท่า หรือดีกว่า

5.9.2 กรณีระบบคอมพิวเตอร์ เกิดชำรุดเสียหายไม่สามารถใช้งานได้ตามปกติ ผู้รับจ้างต้องเข้ามาดำเนินการตรวจสอบ วิเคราะห์ และแก้ไขปัญหาของระบบ ต้องดำเนินการแก้ไขให้แล้วเสร็จให้อยู่ในสภาพที่สามารถใช้งานได้ตามปกติ นับตั้งแต่เวลาที่ได้รับแจ้งผ่านทางจดหมายอิเล็กทรอนิกส์ (E-Mail) หรือแจ้งให้ทราบทางวาจาหรือ ทางโทรศัพท์ ไม่ว่าวิธีใดวิธีหนึ่ง เป็นเวลาเริ่มต้น เพื่อใช้ในการคำนวณระยะเวลาในการเข้ามาดำเนินการแก้ไข เวลาที่ใช้ในการคำนวณค่าปรับจะเริ่มตั้งแต่เวลาที่พ้นกำหนดการตอบสนอง จนถึงเวลาที่ผู้รับจ้างได้ดำเนินการซ่อมแซมแก้ไขแล้วเสร็จ และระบบคอมพิวเตอร์ สามารถใช้งานได้ตามปกติ ที่มีรายละเอียดดังนี้

ระดับความรุนแรงของปัญหา	สถานการณ์	ช่องทางการให้บริการ	ระยะเวลาการตอบสนองและแก้ไขปัญหา
ระดับ 1 : สูง	ระบบหรืออุปกรณ์ไม่สามารถให้บริการได้ และส่งผลกระทบต่อการทำงาน ป้องกัน ตรวจสอบ แจ้งระวัง หรือตอบสนองภัยคุกคาม	Remote Access / Onsite	ตอบสนองภายใน 2 ชั่วโมง และแก้ไขภายใน 8 ชั่วโมง
ระดับ 2 : ปานกลาง	ระบบหรืออุปกรณ์บางส่วนขัดข้อง แต่ระบบโดยรวมยังสามารถให้บริการได้	Remote Access / Onsite	ตอบสนองภายใน 4 ชั่วโมง และแก้ไขภายใน 16 ชั่วโมง
ระดับ 3 : ต่ำ	ระบบยังสามารถใช้งานได้ตามปกติ และเป็นการขอคำแนะนำ ตรวจสอบ หรือปรับตั้งค่าระบบ	Remote Access / Onsite / ประสานงาน	ตอบสนองภายใน 24 ชั่วโมง และแก้ไขภายใน 7 วันทำการ

หากผู้รับจ้างไม่สามารถดำเนินการแก้ไขระบบคอมพิวเตอร์ให้สามารถใช้งานได้ตามปกติ ผู้รับจ้างจะต้องจัดหาระบบคอมพิวเตอร์ที่มีประสิทธิภาพเทียบเท่าหรือดีกว่ามาทดแทนให้กับสำนักงานปลัดกระทรวงแรงงานใช้งานจนกว่าจะสามารถซ่อมแซมแก้ไขได้แล้วเสร็จ พร้อมทั้งแจ้งให้เจ้าหน้าที่ของสำนักงานปลัดกระทรวงแรงงานผู้มีหน้าที่รับผิดชอบทราบในทันที

5.9.3 กรณีอุปกรณ์ระบบและอุปกรณ์สนับสนุนต่าง ๆ ในโครงการฯ ขาดหรือเสียหายจำเป็นจะต้องนำกลับไปซ่อมแซมแก้ไข ผู้รับจ้างต้องนำระบบและอุปกรณ์ใหม่ที่มีประสิทธิภาพเทียบเท่าหรือสูงกว่ามาทดแทนให้กับสำนักงานปลัดกระทรวงแรงงานใช้งานจนกว่าจะสามารถซ่อมแซมแก้ไขได้แล้วเสร็จ

5.9.4 กรณีผู้รับจ้างมีความจำเป็นต้องระบบและอุปกรณ์สนับสนุนต่าง ๆ ในโครงการฯ กลับไปซ่อม ผู้รับจ้างจะต้องซ่อมแซมโดยใช้อะไหล่แท้ที่เป็นของใหม่ และให้แล้วเสร็จ ไม่เกิน 30 วัน นับถัดจากวันที่นำระบบและอุปกรณ์สนับสนุนไปซ่อม หากผู้รับจ้างไม่สามารถซ่อมแซมให้แล้วเสร็จตามระยะเวลาที่กำหนด สำนักงานปลัดกระทรวงแรงงานจะคำนวณค่าปรับเป็นรายวันตามข้อ 6.3.2 และหากจำเป็นต้องซ่อมแซมระบบและอุปกรณ์สนับสนุนที่เสียหายเกิน 30 วัน ผู้รับจ้างต้องแจ้งสำนักงานปลัดกระทรวงแรงงานเป็นลายลักษณ์อักษร

5.9.5 หากผู้รับจ้างไม่ปฏิบัติตามสัญญา หรือข้อตกลงที่กำหนดไว้ และก่อให้เกิดความเสียหายต่อการทำงานของสำนักงานปลัดกระทรวงแรงงาน ผู้รับจ้างจะต้องรับผิดชอบค่าใช้จ่ายทั้งหมดอันจะเกิดจากการที่สำนักงานปลัดกระทรวงแรงงาน ต้องดำเนินการแก้ไขปัญหาดังกล่าว

5.9.6 ผู้รับจ้างต้องสรุปปัญหา และจัดทำเอกสารสรุปรายงานปัญหาที่เกิดขึ้นพร้อมทั้งแสดงขั้นตอนการซ่อมแซมแก้ไข และวิธีการแก้ไขโดยละเอียดทุกขั้นตอนให้กับสำนักงานปลัดกระทรวงแรงงาน

5.10 การซ่อมแซมแบบ Preventive Maintenance (PM) ดังนี้

5.10.1 ผู้รับจ้างจะต้องจัดเจ้าหน้าที่ที่มีความชำนาญเข้าทำการตรวจสอบและบำรุงรักษา (Preventive Maintenance) ณ ศูนย์ปฏิบัติการ MSOC ในรูปแบบ Onsite Service โดยการตรวจสอบสภาพการทำงานของอุปกรณ์ต่างๆ ของระบบคอมพิวเตอร์ในโครงการฯ ทั้งในส่วนของฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ทุกๆ 4 เดือนตลอดระยะเวลารับประกัน/สัญญา

5.10.2 ผู้รับจ้างต้องตรวจสอบสถานะระบบ (System Status & Log Check) ดังนี้

- 1) ตรวจสอบสถานะการทำงานของระบบปฏิบัติการ (OS), Virtualization, ปริมาณการใช้ทรัพยากร (CPU, Memory, Disk Space) และการเก็บรวบรวม Logfile
- 2) ตรวจสอบการเชื่อมต่อและการทำงานของ Agent Software EDR บนเครื่องผู้ใช้งาน

5.10.3 ผู้รับจ้างต้องการอัปเดตระบบและฐานข้อมูลภัยคุกคาม

- 1) ดำเนินการอัปเดตข้อมูล Threat Intelligence, Pattern Signatures และ Rules/Policies ของระบบ IPS, EDR, NDR, XDR และ ASM ให้เป็นเวอร์ชันล่าสุด
- 2) ติดตั้งการอัปเดตเวอร์ชันซอฟต์แวร์ (Software Release Upgrades / Software Version) และลงแพตช์แก้ไขข้อผิดพลาด (Patches / Fixes) ของซอฟต์แวร์ต่างๆ ในโครงการตามความเหมาะสมโดยไม่มีค่าใช้จ่าย

5.10.4 ผู้รับจ้างต้องจัดทำและส่งมอบเอกสารต่อคณะกรรมการ/เจ้าหน้าที่ผู้รับผิดชอบ ดังต่อไปนี้

- 1) เอกสารรายงานการบำรุงรักษา (Service Report): ระบุรายละเอียดผลการตรวจสอบปัญหาที่พบ และการแก้ไข
- 2) รายการตรวจเช็ค (Logbook / Checklist): เอกสารบันทึกการตรวจสอบตามหัวข้อบำรุงรักษาจริงที่ลงนามโดยช่างผู้ปฏิบัติงานและเจ้าหน้าที่ผู้รับตรวจ
- 3) รายงานประวัติการซ่อมบำรุง (Maintenance History Report): รวบรวมประวัติการบำรุงรักษา และการแก้ไขปัญหาสะสมตลอดระยะเวลาสัญญา เพื่อใช้อ้างอิงกรณีเกิดปัญหาระบบ

5.11 ผู้รับจ้างจะต้องจัดให้มีเจ้าหน้าที่คอยสนับสนุนการปฏิบัติงานภายในศูนย์ปฏิบัติการ MSOC ตามภาคผนวก ข เริ่มเข้าปฏิบัติงานที่ศูนย์ปฏิบัติการ MSOC ตามที่กำหนด และรายงานผลการปฏิบัติงานของบุคลากร พร้อมใบบันทึกการเข้า-ออกการปฏิบัติงาน

5.12 ผู้รับจ้างและบุคลากรของผู้รับจ้างต้องรักษาข้อมูลของทางราชการ ข้อมูลการดำเนินงาน และข้อมูลจราจรทางคอมพิวเตอร์ไว้เป็นความลับอย่างเคร่งครัด โดยต้องจัดทำและลงนามใน "สัญญาไม่เปิดเผยข้อมูลที่เป็นความลับ (NDA)" ให้แก่สำนักงานปลัดกระทรวงแรงงาน

6. การคิดค่าปฏิบัติงานในโครงการ

6.1 การให้บริการซ่อมแซม

6.1.1 ในกรณีที่ไม่สามารถซ่อมแซมได้ภายในเวลาที่กำหนด ระยะเวลาอุปกรณ์ต่างๆ ในระบบ ชัดข้อรวมตามเกณฑ์การคำนวณนับไม่เกินเดือนละ 36 ชั่วโมง หรือร้อยละ 5 (ห้า) ของเวลา ใช้งานทั้งหมดของอุปกรณ์ต่างๆ ของอุปกรณ์ของเดือนนั้น ในระบบแล้วแต่ตัวเลขใดจะมากกว่ากัน มิฉะนั้นผู้รับจ้างจะต้องยอมให้สำนักงานปลัดกระทรวงแรงงาน คิดค่าปรับเวลาที่ไม่สามารถใช้งานอุปกรณ์ต่างๆ ในระบบในส่วนที่เกินกำหนดข้างต้นเป็นชั่วโมง ในอัตราร้อยละ 0.035 (ศูนย์จุดศูนย์สามห้า) ของวงเงินค่าจ้างบำรุงรักษา (รายงวด) ตามสัญญาฯ คุณจำนวนชั่วโมง คุณค่าตัวถ่วงตามภาคผนวก ค โดยเฉพาะของชั่วโมงให้คิดเป็นหนึ่งชั่วโมง

6.1.2 กรณีบุคลากรตามภาคผนวก ข ไม่สามารถปฏิบัติงานได้ครบเวลาตามที่กำหนดไว้ในข้อกำหนดทางด้านบุคลากรและพัฒนาศูนย์ฯ สำนักงานปลัดกระทรวงแรงงานจะคิดค่าปรับเป็นรายชั่วโมง ในอัตราร้อยละ 0.035 (ศูนย์จุดศูนย์สามห้า) ของวงเงินค่าจ้างบำรุงรักษา (รายงวด) ตามสัญญาฯ คุณจำนวนชั่วโมง คุณค่าตัวถ่วงตามภาคผนวก ค โดยเฉพาะของชั่วโมงให้คิดเป็นหนึ่งชั่วโมง

6.2 ผู้รับจ้างจะต้องเข้าดำเนินงาน Preventive Maintenance (PM) ตามระยะเวลาที่กำหนดในข้อ 5.10 และแผนการดำเนินงานตามข้อ 5.2 หากผู้รับจ้างไม่สามารถดำเนินการได้ ภายหลังจากครบระยะเวลาที่กำหนดไว้ข้างต้น จะคิดค่าปรับตามข้อ 6.3.2

6.3 กรณีการคำนวณคิดค่าปรับ

6.3.1 ค่าปรับรายชั่วโมง = จำนวนชั่วโมงที่เกินเวลาที่กำหนด โดยเฉพาะของชั่วโมงให้คิดเป็น 1 ชั่วโมง x (ร้อยละ 0.035 x วงเงินค่าจ้างบำรุงรักษา (รายงวด) ตามสัญญาฯ) x ค่าตัวถ่วง (ภาคผนวก ค)

6.3.2 ค่าปรับรายวัน = จำนวนวันที่เกินเวลาที่กำหนด x ร้อยละ 0.1 x วงเงินค่าจ้างบำรุงรักษา (รายงวด) ตามสัญญาฯ x ค่าตัวถ่วง (ภาคผนวก ค)

7. การฝึกอบรม

7.1 ผู้รับจ้างจะต้องจัดทำแผนการฝึกอบรม และเอกสารหลักสูตรฝึกอบรมเพิ่มพูนทักษะด้านการดูแลรักษาระบบคอมพิวเตอร์และการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยกำหนดระยะเวลาในการดำเนินการแต่ละกิจกรรมอย่างชัดเจน ภายใน 30 วันนับถัดจากวันเริ่มดำเนินงานตามสัญญา เพื่อให้คณะกรรมการตรวจรับพัสดุในโครงการฯ พิจารณออนุมัติก่อนเริ่มดำเนินการ และผู้รับจ้างจะต้องดำเนินการอบรมตามแผนการฝึกอบรมวิชาการที่ได้รับการอนุมัติให้ดำเนินการแล้ว โดยประกอบด้วยสาระสำคัญ ประกอบด้วย

- (1) หลักสูตรการฝึกอบรมที่เสนอ
- (2) วัตถุประสงค์ในการอบรมแต่ละหลักสูตร
- (3) ระยะเวลา และช่วงเวลาในการฝึกอบรม
- (4) วิธีการฝึกอบรม
- (5) จำนวนผู้เข้าอบรมในแต่ละหลักสูตร
- (6) คุณสมบัติพื้นฐานของผู้เข้ารับการอบรมแต่ละหลักสูตร
- (7) สถานที่ฝึกอบรม

โดยหลักสูตรฝึกอบรมที่เสนอดังกล่าว จำนวน 2 หลักสูตร ดังนี้

(1) หลักสูตรระดับผู้ดูแลระบบ (Admin) จำนวนไม่น้อยกว่า 10 คน เป็นเวลาไม่น้อยกว่า 18 ชั่วโมง ในรูปแบบ Onsite

(2) หลักสูตรระดับผู้ดูแลระบบ (User) จำนวนไม่น้อยกว่า 80 คน เป็นเวลาไม่น้อยกว่า 6 ชั่วโมง ในรูปแบบ Online

ทั้งนี้ผู้รับจ้างจะต้องรับผิดชอบค่าใช้จ่ายที่ใช้ในการฝึกอบรมทั้งหมดให้กับผู้เข้ารับการอบรมและเจ้าหน้าที่ ได้แก่ ค่าอาหารว่างพร้อมเครื่องดื่ม ค่าอาหารกลางวัน ค่าวิทยากร ค่าเช่าสถานที่ ค่ากระเป๋าเอกสาร และค่าอุปกรณ์เครื่องมือเครื่องใช้ที่จำเป็นต่อการฝึกอบรมทั้งหมด ยกเว้นค่าเดินทาง ในกรณี Onsite

7.2 สำนักงานปลัดกระทรวงแรงงานขอสงวนสิทธิ์ในการคัดลอกหรือทำซ้ำเอกสารและคู่มือต่างๆ เพื่อใช้งานในกิจการของสำนักงานปลัดกระทรวงแรงงาน หากเอกสารและคู่มือรายการใดไม่สามารถคัดลอกหรือทำซ้ำได้ ให้ผู้รับจ้างแจ้งสำนักงานปลัดกระทรวงแรงงานทราบเป็นลายลักษณ์อักษร

กรณีผู้รับจ้างไม่แจ้งให้สำนักงานปลัดกระทรวงแรงงานทราบ จะถือว่าผู้รับจ้างอนุญาตให้คัดลอกหรือทำซ้ำได้ ทั้งนี้หากมีบุคคลภายนอกกล่าวอ้างหรือใช้สิทธิ์เรียกร้องใดๆ ว่ามีการละเมิดลิขสิทธิ์เกี่ยวกับเอกสารและคู่มือที่สำนักงานปลัดกระทรวงแรงงานคัดลอกหรือทำซ้ำเพื่อใช้งานในกิจการของสำนักงานปลัดกระทรวงแรงงาน ผู้รับจ้างต้องดำเนินการทั้งปวงเพื่อให้การกล่าวอ้างหรือการเรียกร้องดังกล่าวระงับสิ้นไปโดยเร็ว โดยผู้รับจ้างต้องเป็นผู้ชำระค่าเสียหายและค่าใช้จ่ายต่างๆ ที่เกิดขึ้นทั้งหมด

8. หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

ในการพิจารณาผลการยื่นข้อเสนอครั้งนี้ สำนักงานปลัดกระทรวงแรงงานจะพิจารณาตัดสินโดยใช้หลักเกณฑ์การพิจารณาจากราคา

9. ระยะเวลาดำเนินการและส่งมอบงาน

ผู้รับจ้างต้องให้บริการจ้างเหมาบำรุงรักษาศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Ministry Security Operation Center : MSOC) และสำนักงานปลัดกระทรวงแรงงานจะจ่ายค่าจ้างโดยแบ่งการส่งมอบงานและการชำระเงินเป็น 12 งวด งวดละเท่าๆ กัน เมื่อคณะกรรมการตรวจรับพัสดุฯ ได้ทำการตรวจรับงานเสร็จเรียบร้อยแล้ว โดยจะต้องส่งมอบงานเป็นรายงวด ภายใน 1 วันนับถัดจากวันครบกำหนดรายงวด หากงวดใดวันครบกำหนดส่งมอบงานตรงกับวันหยุดราชการให้ส่งมอบงานในวันทำการถัดไป หากผู้รับจ้างไม่สามารถส่งมอบงานได้จะคิดค่าปรับเป็นรายวันที่เกินระยะเวลาที่กำหนดตามข้อ 6.3.2 ซึ่งมีรายละเอียดการส่งมอบงาน ดังนี้

หากงวดใดวันครบกำหนดส่งมอบงานตรงกับวันหยุดราชการให้ส่งมอบงานในวันทำการถัดไป หากผู้รับจ้างไม่สามารถส่งมอบงานได้จะคิดค่าปรับเป็นรายวันที่เกินระยะเวลาที่กำหนดตามข้อ 6.3.2 ซึ่งมีรายละเอียดการส่งมอบงานดังนี้

งวดที่ 1 ประกอบด้วย

- 1) ส่งแผนการดำเนินงาน
- 2) รายงานสรุปผลการเฝ้าระวังภัยคุกคามทางไซเบอร์
- 3) รายงาน Corrective Maintenance
- 4) รายงานผลการปฏิบัติงานของบุคลากร พร้อมใบบันทึกการเข้า-ออกการปฏิบัติงาน

งวดที่ 2 - 3 ประกอบด้วย

- 1) รายงานสรุปผลการเฝ้าระวังภัยคุกคามทางไซเบอร์
- 2) รายงาน Corrective Maintenance
- 3) รายงานผลการปฏิบัติงานของบุคลากร พร้อมใบบันทึกการเข้า-ออกการปฏิบัติงาน

งวดที่ 4 ประกอบด้วย

- 1) รายงานสรุปผลการเฝ้าระวังภัยคุกคามทางไซเบอร์
- 2) รายงาน Corrective Maintenance
- 3) รายงานผลการทำ Preventive Maintenance (PM)
- 4) รายงานผลการปฏิบัติงานของบุคลากร พร้อมใบบันทึกการเข้า-ออกการปฏิบัติงาน

งวดที่ 5 - 7 ประกอบด้วย

- 1) รายงานสรุปผลการเฝ้าระวังภัยคุกคามทางไซเบอร์
- 2) รายงาน Corrective Maintenance
- 3) รายงานผลการปฏิบัติงานของบุคลากร พร้อมใบบันทึกการเข้า-ออกการปฏิบัติงาน

งวดที่ 8 ประกอบด้วย

- 1) รายงานสรุปผลการเฝ้าระวังภัยคุกคามทางไซเบอร์
- 2) รายงาน Corrective Maintenance
- 3) รายงานผลการทำ Preventive Maintenance (PM)
- 4) รายงานผลการฝึกอบรม
- 5) รายงานผลการปฏิบัติงานของบุคลากร พร้อมใบบันทึกการเข้า-ออกการปฏิบัติงาน

งวดที่ 9 - 11 ประกอบด้วย

- 1) รายงานสรุปผลการเฝ้าระวังภัยคุกคามทางไซเบอร์
- 2) รายงาน Corrective Maintenance
- 3) รายงานผลการปฏิบัติงานของบุคลากร พร้อมใบบันทึกการเข้า-ออกการปฏิบัติงาน

งวดที่ 12 ประกอบด้วย

- 1) รายงานสรุปผลการเฝ้าระวังภัยคุกคามทางไซเบอร์
- 2) รายงาน Corrective Maintenance
- 3) รายงานผลการทำ Preventive Maintenance (PM)
- 4) รายงานสรุปภาพรวมเหตุการณ์ผลการเฝ้าระวังภัยคุกคามทางไซเบอร์ตลอดสัญญา
- 5) รายงานผลการปฏิบัติงานของบุคลากร พร้อมใบบันทึกการเข้า-ออกการปฏิบัติงาน

ส.ร.

ด.ม.ก.

วิ.ร.ร.

ก.ร.ร.

อ.ร.

10. ระยะเวลาดำเนินงาน

ดำเนินการให้บริการบำรุงรักษาศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Ministry Security Operation Center : MSOC) ระยะเวลา 12 เดือน (1 ตุลาคม 2569 – 30 กันยายน 2570) ทั้งนี้ ขอสงวนสิทธิ์ในการเปลี่ยนแปลงระยะเวลาและค่าจ้างในการจ้างตามที่ให้บริการจริง

11. วงเงินในการจัดหา

เป็นวงเงินทั้งสิ้น 6,610,000 บาท (หกล้านหกแสนหนึ่งหมื่นบาทถ้วน) ซึ่งเป็นราคาที่รวมภาษีมูลค่าเพิ่มและอื่นๆ เรียบร้อยแล้ว ทั้งนี้ ขอสงวนสิทธิ์ในการเปลี่ยนแปลงระยะเวลาและค่าใช้จ่ายในการจ้างตามที่ให้บริการจริง

12. หน่วยงานผู้รับผิดชอบดำเนินการ

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงแรงงาน



ภาคผนวก ก
รายการระบบและอุปกรณ์ศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์
(Ministry Security Operation Center : MSOC)

1. รายการดูแลบำรุงรักษาระบบตรวจจับภัยคุกคามทางไซเบอร์และประเมินความเสี่ยงระบบสารสนเทศ

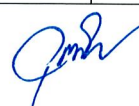
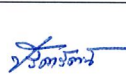
1.1 ระบบป้องกัน ตรวจจับและตอบสนองต่อภัยคุกคาม (End-Point Protection, Network Protection, IPS, Agent Software)

ฮาร์ดแวร์ (Hardware)

ลำดับ	รายการ	แบบ/รุ่น	จำนวน	หน่วยนับ
1	อุปกรณ์ตรวจจับและป้องกันการโจมตีระบบเครือข่าย (Intrusion Prevention System)	TippingPoint 5500TX	2	เครื่อง

ซอฟต์แวร์ (Software)

ลำดับ	รายการ	แบบ/รุ่น	จำนวน	หน่วยนับ
1	ระบบตรวจจับและป้องกันการโจมตีระบบเครือข่าย (Intrusion Prevention System)	TippingPoint 3Gbps TPS Inspection License + Threat DV + TLS inspection	2	ชุด
2	Agent Software สำหรับป้องกันและตรวจจับภัยคุกคามในระดับเครื่องผู้ใช้งาน (Endpoint Sensor)	Trendmicro Vision One Endpoint Security Essentials	1,800	ลิขสิทธิ์
3	Agent Software สำหรับป้องกันและตรวจจับภัยคุกคามในระดับเครื่องแม่ข่าย (Server Sensor)	Trendmicro Vision One Endpoint Security Pro	260	ลิขสิทธิ์



1.2 ระบบเฝ้าระวังและตอบสนองภัยคุกคาม (Extended Detection and Response, SOC Platform)

ฮาร์ดแวร์ (Hardware)

ลำดับ	รายการ	แบบ/รุ่น	จำนวน	หน่วยนับ
1	อุปกรณ์ตรวจจับภัยคุกคามขั้นสูงทางไซเบอร์บนระบบเครือข่าย	Deep Discovery Inspector 4000 Appliance	1	เครื่อง

ซอฟต์แวร์ (Software)

ลำดับ	รายการ	แบบ/รุ่น	จำนวน	หน่วยนับ
1	ระบบตรวจจับภัยคุกคามขั้นสูงทางไซเบอร์บนระบบเครือข่าย	Deep Discovery Inspector 4000 Software with 4 Gbps	1	ชุด
2	ระบบเฝ้าระวังและตอบสนองภัยคุกคามทางไซเบอร์ (Extended Detection and Response)	Trend Micro Vision One Credits	1	ชุด
3	ระบบบริการผู้เชี่ยวชาญสำหรับค้นหาภัยคุกคามเชิงรุกและตอบสนองต่อภัยคุกคามอัตโนมัติ (SOC as a service)	Trend micro vision one SOC service essential	1	ชุด
4	ระบบตรวจประเมินความเสี่ยงความมั่นคงปลอดภัยไซเบอร์เพื่อค้นหาช่องโหว่และความเสี่ยงที่อาจเกิดขึ้นสำหรับระบบเครือข่าย, เครื่องแม่ข่าย และเว็บแอปพลิเคชัน	Trend Vision One Attack Surface Risk Management	1	ชุด



1.3 ระบบตรวจประเมินความเสี่ยง (Network Sensor, Attack Surface Risk Management)

ฮาร์ดแวร์ (Hardware)

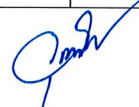
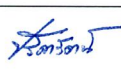
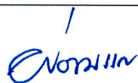
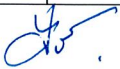
ลำดับ	รายการ	แบบ/รุ่น	จำนวน	หน่วยนับ
1	อุปกรณ์บริหารจัดการอุปกรณ์ ตรวจจับป้องกันภัยคุกคามบน ระบบเครือข่าย (Network Sensor)	Tippingpoint SMS H4 XL	1	เครื่อง

ซอฟต์แวร์ (Software)

ลำดับ	รายการ	แบบ/รุ่น	จำนวน	หน่วยนับ
1	ระบบบริหารจัดการอุปกรณ์ ตรวจจับป้องกันภัยคุกคามบน ระบบเครือข่าย (Network Sensor)	Tippingpoint SMS H4 XL	1	ชุด

2. เครื่องคอมพิวเตอร์แม่ข่ายพร้อมซอฟต์แวร์บริหารจัดการคอมพิวเตอร์เสมือน อุปกรณ์กระจายสัญญาณ

ลำดับ	รายการ	แบบ/รุ่น	จำนวน	หน่วยนับ
1	เครื่องคอมพิวเตอร์แม่ข่าย พร้อม ชุดซอฟต์แวร์ระบบแม่ข่าย คอมพิวเตอร์เสมือน	H3C รุ่น UniServer R4700 G5 / VMware	2	ชุด
2	อุปกรณ์กระจายสัญญาณ (Switch)	Juniper รุ่น EX4100-48T	2	ชุด
3	อุปกรณ์กระจายสัญญาณ ขนาด 24 ช่อง	Juniper รุ่น EX2300-24T	1	ชุด



3. รายการดูแลบำรุงรักษาอุปกรณ์และระบบพื้นฐานที่จำเป็นสำหรับห้องศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์

ลำดับ	รายการ	แบบ/รุ่น	จำนวน	หน่วยนับ
1	กล้องโทรทัศน์วงจรปิด	Hikvision รุ่น DS-2CD2125FHWD-I(S)	4	ชุด
2	อุปกรณ์บันทึกภาพผ่านเครือข่าย (Network Video Recorder) แบบ 8 ช่อง	Hikvision รุ่น DS-7608NI-M2/8P	1	ชุด
3	ระบบการบริหารจัดการ การเข้า-ออกประตู พร้อมเครื่องบันทึก	Hikvision รุ่น DS-K1T673TDX	1	ระบบ
4	จอแสดงผลภาพแบบวิดีโอวอลล์ (Video Wall)	Samsung รุ่น VM55B-U	8	จอ
5	ตู้ควบคุมและจัดการจอแสดงผลภาพแบบวิดีโอวอลล์ (VideoWall Controller)	BRWALL รุ่น BR40	1	ชุด
6	จอแสดงผลภาพสำหรับสื่อสาร ประชุมหรืออบรม	Hisense รุ่น 65MR6DE-E	1	จอ
7	เครื่องคอมพิวเตอร์ตั้งโต๊ะและจอแสดงผลภาพ ขนาด 23.8 นิ้ว	HP รุ่น HP Pro Tower 400 G9	5	ชุด
8	จอแสดงผลภาพขนาด 23.8 นิ้ว	HP รุ่น HP P24h G5 FHD Monitor	5	จอ
9	เครื่องปรับอากาศขนาด 24,000 BTU	GREE รุ่น GULD-24T1/A-S	2	ชุด
10	เครื่องสำรองไฟฟ้า ขนาด 10 kVA (ระบบไฟฟ้า 3 เฟส)	APC รุ่น Smart-UPS SRT 10000VA 230	1	ชุด
11	เครื่องพิมพ์ Multifunction เลเซอร์	HP รุ่น Color LaserJet Pro MFP M282nw	1	ชุด
12	เครื่องทำลายเอกสาร	OA-STAR รุ่น NT-10M	1	ชุด
13	โต๊ะทำงาน		5	ชุด
14	เก้าอี้สำนักงาน		10	ชุด
15	โต๊ะประชุม		1	ชุด
16	ตู้จัดเก็บเอกสารประเภทซอง ขนาด 9 ช่อง		1	ตู้



ภาคผนวก ข

รายละเอียดและคุณสมบัติบุคลากรปฏิบัติงานในศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์
(Ministry Security Operation Center)

1. ผู้จัดการศูนย์ปฏิบัติการ (SOC Manager) ปฏิบัติหน้าที่ ในวันเวลาทำการ อย่างน้อยเดือนละ 1 วัน ตั้งแต่ เวลา 08.30 น. – 16.30 น. จำนวน 1 คน โดยมีภาระหน้าที่ และคุณสมบัติดังต่อไปนี้

ภาระหน้าที่

- 1) ให้คำปรึกษา แนะนำ ร่วมวางแผนออกแบบและพัฒนากระบวนการปฏิบัติงานในศูนย์ปฏิบัติการ MSOC และการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานปลัดกระทรวงแรงงาน
- 2) ควบคุม ดูแลและจัดการจัดตารางงานของทีมงานให้มีประสิทธิภาพ
- 3) ควบคุม ดูแลจัดการการทำงานและประเมิน ปรับปรุงการปฏิบัติงาน อย่างต่อเนื่อง
- 4) ติดตามและอัปเดตข้อมูลของอุปกรณ์ที่ใช้ในศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อปรับปรุงและพัฒนาการใช้งานอย่างต่อเนื่อง
- 5) รายงานสรุปผลการเฝ้าระวังภัยคุกคามทางไซเบอร์

คุณสมบัติ

- 1) วุฒิการศึกษาระดับปริญญาตรีขึ้นไป ในสาขาวิชาคอมพิวเตอร์, เทคโนโลยีสารสนเทศ (IT), วิศวกรรมคอมพิวเตอร์, วิทยาการคอมพิวเตอร์ หรือสาขาอื่นที่เกี่ยวข้อง
- 2) มีประสบการณ์การทำงานด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Cybersecurity) อย่างน้อย 10 ปี
- 3) มีใบรับรอง (Certificate) GMON หรือ CISSP หรือ CISM หรือ CISA

2. ตำแหน่งเจ้าหน้าที่วิเคราะห์ภัยคุกคามฯ ระบบ ระดับ 1 (Cyber Security Analyst : Tier 1) เข้าปฏิบัติหน้าที่ในวันเวลาทำการ ตั้งแต่เวลา 08.30 น. – 16.30 น. จำนวน 1 คน มีคุณสมบัติดังต่อไปนี้

ภาระหน้าที่

- 1) ดำเนินการตรวจสอบวิเคราะห์และรายงานการแจ้งเตือนด้านความปลอดภัยและข้อมูลเหตุการณ์ ในวันเวลาทำการ ตั้งแต่เวลา 08.30 น. – 16.30 น.
- 2) ตรวจสอบและระบุเหตุการณ์ผิดปกติที่อุปกรณ์รักษาความปลอดภัยตรวจพบในเชิงบวกและจัดทำ รายงาน
- 3) วิเคราะห์เหตุการณ์ภัยคุกคามทางไซเบอร์ที่ได้รับการแจ้งเตือนยืนยันความถูกต้องของ เหตุการณ์ จัดลำดับความสำคัญของเหตุการณ์และบันทึกเหตุการณ์
- 4) ทำการบันทึกการตรวจสอบและบันทึกกิจกรรมที่ไม่เหมาะสมหรือผิดกฎหมาย ซึ่งรวมถึงการ ตรวจสอบอุปกรณ์เครือข่าย เครื่องแม่ข่ายและเครื่องลูกข่าย เพื่อรายงานเหตุการณ์กับทางสำนักงาน ปลัดกระทรวงแรงงาน
- 5) ให้คำแนะนำเบื้องต้นในการแก้ไขเหตุการณ์ภัยคุกคามทางไซเบอร์ หากไม่สามารถดำเนินการ แก้ไข ได้ด้วยตนเอง ต้องส่งต่อเหตุการณ์ไปยังเจ้าหน้าที่เฝ้าระวังภัยคุกคามทางไซเบอร์ระดับ 2 (Tier 2)
- 6) ทำรายงานสรุปรายวัน รายสัปดาห์และรายงานสรุปรายเดือนของภัยคุกคามและการวิเคราะห์ เหตุการณ์ความปลอดภัย



คุณสมบัติ

- 1) วุฒิการศึกษาระดับปริญญาตรีขึ้นไป ในสาขาวิชาคอมพิวเตอร์, เทคโนโลยีสารสนเทศ (IT), วิศวกรรมคอมพิวเตอร์, วิทยาการคอมพิวเตอร์ หรือสาขาอื่นที่เกี่ยวข้อง
- 2) มีประสบการณ์การทำงานด้านเฝ้าระวังและวิเคราะห์ข้อมูลความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Security Operation Center) อย่างน้อย 3 ปี
- 3) มีใบรับรอง (Certificate) CompTIA Security+

3. เจ้าหน้าที่วิเคราะห์ภัยคุกคามฯ ระดับ 2 (Cyber Security Analyst : Tier 2) เข้าปฏิบัติหน้าที่ ในวันเวลาทำการ ตั้งแต่เวลา 08.30 น. – 16.30 น. จำนวน 1 คน โดยมีภาระหน้าที่ และคุณสมบัติดังต่อไปนี้

ภาระหน้าที่

- 1) วิเคราะห์เหตุการณ์ความปลอดภัยคอมพิวเตอร์ที่ได้รับการประสานจาก เจ้าหน้าที่เฝ้าระวังภัยคุกคามทางไซเบอร์ระดับ 1 (Tier 1) เพื่อตอบสนองและการสนับสนุนการตรวจจับภัยคุกคามที่เกิดขึ้น
- 2) ให้คำแนะนำในการแก้ไขปัญหา และดำเนินการร่วมกับเจ้าหน้าที่สำนักงานปลัดกระทรวงแรงงาน ในการแก้ไขเหตุการณ์ภัยคุกคามทางไซเบอร์
- 3) ดูแลรับผิดชอบในการตรวจพบเหตุการณ์และ/หรือเหตุการณ์ที่เกิดขึ้นและตอบสนองต่อการปฏิบัติตามกระบวนการ ที่กำหนดไว้
- 4) จัดทำสรุปผลการเฝ้าระวังภัยคุกคามทางไซเบอร์

คุณสมบัติ

- 1) วุฒิการศึกษาระดับปริญญาตรี วิศวกรรมศาสตร์ หรือวิทยาศาสตร์ หรือเทคโนโลยีสารสนเทศ หรือเทียบเท่า
- 2) มีประสบการณ์การทำงานติดตั้ง ปรับปรุง หรือเฝ้าระวังและวิเคราะห์ข้อมูลความมั่นคงปลอดภัยระบบเทคโนโลยี สารสนเทศ (Security Operation Center) อย่างน้อย ๕ ปี
- 3) มีใบรับรอง (Certificate) ระดับ Professional ของผลิตภัณฑ์ที่นำเสนอมาในโครงการ หรือ CompTIA Security+ และ CompTIA CySA+

4. เจ้าหน้าที่ IT Support จำนวน 1 คน โดยมีภาระหน้าที่ และคุณสมบัติดังต่อไปนี้

ภาระหน้าที่

- 1) ติดตามเหตุการณ์ความปลอดภัยคอมพิวเตอร์ที่ได้รับการประสานจากเจ้าหน้าที่เฝ้าระวังภัยคุกคามทางไซเบอร์ระดับ 1 (Tier 1) และระดับ 2 (Tier 2) เพื่อตอบสนองและการสนับสนุนการตรวจจับภัยคุกคามที่เกิดขึ้น
- 2) ประสานงานและเข้าแก้ไขปัญหาด้านเทคนิคเบื้องต้น และดำเนินการร่วมกับเจ้าหน้าที่สำนักงานปลัดกระทรวงแรงงาน เมื่อเกิดเหตุการณ์คุกคามหรือความผิดปกติทางไซเบอร์
- 3) ให้คำแนะนำ ความช่วยเหลือ และประสานงานกับผู้ใช้งานหรือหน่วยงานที่เกี่ยวข้องเกี่ยวกับมาตรการความปลอดภัยทางไซเบอร์

คุณสมบัติ

- 1) วุฒิการศึกษาระดับปริญญาตรีขึ้นไป ในสาขาวิชาคอมพิวเตอร์, เทคโนโลยีสารสนเทศ (IT), วิศวกรรมคอมพิวเตอร์, วิทยาการคอมพิวเตอร์ หรือสาขาอื่นที่เกี่ยวข้อง
- 2) มีประสบการณ์ด้านเทคโนโลยีสารสนเทศ ระบบเครือข่าย หรือระบบความมั่นคงปลอดภัยไซเบอร์ ไม่น้อยกว่า 2 ปี

ภาคผนวก ค
ตารางกำหนดตัวถ่วงของคอมพิวเตอร์

ลำดับ	รายการ	ค่าตัวถ่วง
1	ห้องศูนย์ปฏิบัติการและประสานงานกลางด้านความมั่นคงปลอดภัยไซเบอร์ พร้อมระบบคอมพิวเตอร์และซอฟต์แวร์	0.1
2	ระบบป้องกันตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์และระบบเครือข่าย (End-Point Protection and Network Protection)	0.1
3	ระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามทางไซเบอร์ (Extended Detection and Response)	0.3
4	ระบบตรวจประเมินความเสี่ยงความมั่นคงปลอดภัยไซเบอร์เพื่อค้นหาช่องโหว่และความเสี่ยงอาจเกิดขึ้นสำหรับระบบเครือข่าย, เครื่องแม่ข่าย และเว็บแอปพลิเคชัน	0.3
5	ระบบเครื่องคอมพิวเตอร์แม่ข่ายพร้อมซอฟต์แวร์บริหารจัดการ และอุปกรณ์กระจายสัญญาณ	0.1
6	บุคลากรตามภาคผนวก ข	0.1

