รายละเอียดคุณลักษณะเฉพาะ

โครงการศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์

(Ministry Security Operation Center : MSOC)

๑. ความเป็นมาหลักการและเหตุผล

สำนักงานปลัดกระทรวงแรงงานนำระบบเทคโนโลยีสารสนเทศมาใช้ในการปฏิบัติงานภายในองค์กร รวมถึงการให้บริการข้อมูลข่าวสารในด้านนโยบายและรายงานด้านสถิติต่างๆ ให้แก่ หน่วยงานในสังกัด หน่วยงานภายนอกและประชาชนทั่วไป ปัจจุบันมีระบบงานสำคัญหลายระบบ อาทิเช่น ระบบบริหารจัดการเว็บไซด์กระทรวง ระบบที่เกี่ยวข้องกับผู้มีรายได้น้อยที่ลงทะเบียนสวัสดิการแห่งรัฐ ระบบติดตามผลการปฏิบัติงานในโครงการต่างๆ ของสำนักงานปลัดกระทรวงแรงงาน รวมถึงระบบบริหารงานภายใน เพื่อเป้าหมายในการเพิ่มศักยภาพด้านแรงงานและผู้ประกอบการ การคุ้มครองและเสริมสร้างความมั่นคง การบริหารจัดการด้านแรงงานระหว่างประเทศ ระบบสารสนเทศของสำนักงานปลัดกระทรวงแรงงานในปัจจุบันถือว่าเป็นส่วนสำคัญหลักอันหนึ่งในการดำเนินงานให้บรรลุวัตถุประสงค์ของหน่วยงาน ซึ่งหากเกิดปัญหาไม่สามารถทำงานได้ทั้งหมดหรือบางส่วน จะส่งผลต่อการทำงานทั้งงานประจำและงานด้านนโยบาย รวมถึงงานบริการด้านข้อมูลให้แก่ประชาชนและหน่วยงานอื่นๆที่เกี่ยวข้อง จึงมีความจำเป็นอย่างยิ่งในการทำให้ระบบสารสนเทศมีเสถียรภาพ พร้อมใช้งานและสามารถให้บริการระบบงานได้อย่างต่อเนื่อง ซึ่งปัจจุบันภัยคุกคามทางไซเบอร์มีโอกาสเกิดและมีความรุนแรงมากขึ้น เนื่องจากการพัฒนาทางด้านเทคโนโลยีสารสนเทศที่มีการปรับเปลี่ยนอยู่เสมอ เพื่อให้รองรับกับความต้องการใช้งานบริการดิจิทัล ซึ่งสอดคล้องกับการพัฒนาการให้บริการภาครัฐผ่านระบบดิจิทัลในปัจจุบัน ส่งผลให้บริการดิจิทัลของสำนักงานปลัดกระทรวงแรงงานมีโอกาสเป็นเป้าหมายในการโจมตีจากผู้ไม่หวังดี และเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ขึ้นได้ โดยอาจส่งผลกระทบทั้งด้านการรักษาความลับ การรักษาความถูกต้อง และการสามารถในการให้บริการดิจิทัล รวมถึงส่งผลกระทบต่อภาพลักษณ์ของสำนักงานปลัดกระทรวงแรงงาน ในด้านการให้บริการภาครัฐผ่านระบบดิจิทัลเป็นอย่างมาก

อีกทั้งสำนักงานปลัดกระทรวงแรงงานเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศซึ่งมีหน้าที่ต้องปฏิบัติตามเพื่อให้สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และต้องมีมาตรฐานในการรักษาความมั่นคงปลอดภัยเพื่อให้สอดคล้องกับกฎหมายอื่น ๆ ที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ เป็นต้น ซึ่งเป็นความจำเป็นที่สำนักงานปลัดกระทรวงแรงงานจะต้องดำเนินการพัฒนาขีดความสามารถในด้านความมั่นคงปลอดภัยไซเบอร์ให้สามารถป้องกัน (Protect) ตรวจพบ (Detect) และตอบสนอง (Response) ต่อภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของบริการดิจิทัลและข้อมูลในการดำเนินงานของสำนักงานปลัดกระทรวง

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

แรงงานในการให้บริการประชาชนได้อย่างรวดเร็ว มีประสิทธิภาพ และส่งผลกระทบต่อการดำเนินงานหลักของสำนักงานปลัดกระทรวงแรงงานน้อยที่สุด

ดังนั้น สำนักงานปลัดกระทรวงแรงงาน จึงจำเป็นอย่างยิ่งที่ต้องเสริมสร้างความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ต่อบริการดิจิทัลของหน่วย ที่ยิ่งมีการปรับเปลี่ยนและพัฒนาอย่างไม่หยุดนิ่ง โดยการพัฒนาศูนย์ประสานงานกลางในการเฝ้าระวังและรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานสำคัญทางเทคโนโลยีของสำนักงานปลัดกระทรวงแรงงาน รวมทั้งวิเคราะห์ภัยคุกคามทางไซเบอร์และปฏิบัติการเชิงรุกด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ จึงมีความจำเป็นต้องจัดทำโครงการพัฒนาศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เพื่อให้มีขีดความสามารถในการเฝ้าระวังและรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานทางเทคโนโลยีให้บริการดิจิทัลของสำนักงานปลัดกระทรวงแรงงานที่ต้องตอบสนองต่อความต้องการใช้ที่เพิ่มมากขึ้นในอนาคตได้อย่างมีประสิทธิภาพและมีความพร้อมต่อการให้บริการประชาชน ซึ่งถือเป็นภารกิจของภาครัฐต่อการตอบสนองการให้บริการเพื่อให้เกิดความพึงพอใจของประชาชนสูงสุดตรงตามภารกิจของกระทรวงแรงงานที่ได้รับนโยบายจากทางรัฐบาล

๒. วัตถุประสงค์ของโครงการ

๒.๑ เพื่อพัฒนางานเฝ้าระวัง รักษาความมั่นคงปลอดภัย จัดการและตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัย ไซเบอร์ของสำนักงานปลัดกระทรวงแรงงานและหน่วยงานในสังกัด

๒.๒ เพื่อวิเคราะห์ภัยคุกคามทางไซเบอร์และปฏิบัติการเชิงรุกด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

๒.๓ เพื่อให้สามารถตอบสนองต่อเหตุการณ์หรืออุบัติการณ์ที่เกิดจากภัยคุกคามทางไซเบอร์ได้อย่างรวดเร็วและมีประสิทธิภาพ ส่งผลให้ระบบที่ให้บริการแก่ประชาชนสามารถให้บริการได้อย่างต่อเนื่อง

๒.๔ เพื่อลดความเสี่ยงต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศและระบบที่ให้บริการแก่ประชาชน ในกรณีที่ถูกบุกรุกหรือโจมตีจากภัยคุกคามทางไซเบอร์

๒.๕ เพื่อให้สำนักงานปลัดกระทรวงแรงงานซึ่งเป็นหน่วยงานที่มีโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สามารถดำเนินการได้สอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และการรักษา ความมั่นคงปลอดภัยสารสนเทศได้อย่างครบถ้วน

๒.๖ เพื่อพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและความเป็นส่วนบุคคลของสำนักงานปลัดกระทรวงแรงงาน ให้สอดคล้องเป็นไปตามมาตรฐานสากล

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

๓. เงื่อนไขการเสนอราคา

๓.๑ ขอบเขตเอกสารข้อเสนอโครงการ

ผู้ยื่นข้อเสนอจะต้องทำการเปรียบเทียบรายละเอียดและเงื่อนไขเฉพาะต่อข้อกำหนดและรายละเอียดคุณลักษณะ (Specification) เป็นรายข้อตั้งแต่ข้อ ๔ ถึงข้อสุดท้าย รวมถึงภาคผนวก โดยใช้ตัวอย่างแบบฟอร์มการเปรียบเทียบตามตารางที่ ๑ ในการเปรียบเทียบรายการดังกล่าว หากมีกรณีที่ต้องมีการอ้างอิงข้อความหรือเอกสารในส่วนอื่นที่จัดทำเสนอมา ผู้ยื่นข้อเสนอต้องระบุให้เห็นอย่างชัดเจน สามารถตรวจสอบได้โดยง่ายไว้ในเอกสารเปรียบเทียบด้วยว่าสิ่งที่ต้องการอ้างอิงถึงนั้น อยู่ในส่วนใดตำแหน่งใดของเอกสารอื่น ๆ ที่จัดทำเสนอมา สำหรับเอกสารที่อ้างอิงถึงให้หมายเหตุหรือขีดเส้นใต้หรือระบายสีพร้อมเขียนหัวข้อกำกับไว้ เพื่อให้สามารถตรวจสอบกับเอกสารเปรียบเทียบได้ง่ายและตรงกันด้วย ทั้งนี้ ผู้ยื่นข้อเสนอต้องส่งเอกสารเปรียบเทียบพร้อมเอกสารอ้างอิงทั้งหมด หากผู้ยื่นข้อเสนอไม่ดำเนินการตามข้อนี้ สำนักงานปลัดกระทรวงแรงงาน ขอสงวนสิทธิ์ในการไม่พิจารณาข้อเสนอของผู้ยื่นข้อเสนอ

ตารางที่ ๑ ตารางเปรียบเทียบคุณสมบัติข้อกำหนดและรายละเอียดข้อเสนอโครงการ

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

๓.๒ ราคาที่เสนอ ต้องเป็นราคารวมทั้งโครงการ ทั้งนี้ต้องรวมภาษีมูลค่าเพิ่มและภาษีต่าง ๆ

๓.๓ ระบบงานที่ปรับปรุงหรือพัฒนาขึ้นทั้งหมดจะต้องเป็นลิขสิทธิ์ของสำนักงานปลัดกระทรวงแรงงานและผู้ยื่นข้อเสนอต้องไม่เปิดเผยข้อมูลที่เกิดขึ้นจากการดำเนินงานตามโครงการของสำนักงานปลัดกระทรวงแรงงาน

๔. คุณสมบัติของผู้ยื่นข้อเสนอ

๔.๑ มีความสามารถตามกฎหมาย

๔.๒ ไม่เป็นบุคคลล้มละลาย

๔.๓ ไม่อยู่ในระหว่างเลิกกิจการ

๔.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอ หรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

๔.๕ ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงาน และได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วน ผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๔.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๔.๗ เป็นบุคคล หรือ นิติบุคคลผู้มีอาชีพขายพัสดุที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

๔.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนออื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงานปลัดกระทรวงแรงงาน ณ วันยื่นข้อเสนอ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม ในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๔.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอ ได้มีคำสั่งให้สละสิทธิ์ความคุ้มกันเช่นว่านั้น

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

๔.๑๑ ผู้ยื่นข้อเสนอจะต้องมีหนังสือรับรองการแต่งตั้งเป็นตัวแทนจำหน่ายจากผู้ผลิต หรือตัวแทนจำหน่ายในประเทศไทย โดยให้ยื่นขณะเข้าเสนอราคา เพื่อให้การสนับสนุนแก่ผู้ยื่นข้อเสนอในกรณีที่เกี่ยวข้องกับผลิตภัณฑ์ตามข้อกำหนด โดยผลิตภัณฑ์ซอฟต์แวร์ต้องมีลิขสิทธิ์ถูกต้องตามกฎหมาย ตามรายการครุภัณฑ์ภาคผนวก ค ข้อ ๒.๑ โดยให้แนบเอกสารดังกล่าวมาในวันที่ยื่นข้อเสนอและเอกสารหลักฐานดังกล่าวต้องมีอายุครอบคลุมถึงวันที่เสนอราคา

๔.๑๒ ผู้ยื่นข้อเสนอต้องมีผลงานการขายพร้อมการติดตั้งอุปกรณ์ระบบรักษาความมั่นคงปลอดภัยเครือข่าย ให้กับส่วนราชการ รัฐวิสาหกิจ บริษัทเอกชน หรือธนาคาร จำนวนอย่างน้อย ๑ ผลงาน โดยมีมูลค่ารวมในสัญญาเดียวกันไม่น้อยกว่า ๒๐,๐๐๐,๐๐๐ บาท (ยี่สิบล้านบาทถ้วน) ย้อนหลังไม่เกิน ๕ ปี นับถึงวันที่ยื่นเอกสารประกวดราคา โดยแนบหนังสือรับรองผลงานและสำเนาสัญญา มาพร้อมกับเอกสารการประกวดราคา ทั้งนี้ สำนักงานปลัดกระทรวงแรงงานขอสงวนสิทธิที่จะตรวจสอบข้อเท็จจริงที่เสนอ

๔.๑๓ ผู้ยื่นข้อเสนอต้องมีบุคลากรหลักและบุคลากรผู้เชี่ยวชาญในตำแหน่งต่างๆ ที่มีความรู้ ความชำนาญในตำแหน่ง หน้าที่ความรับผิดชอบ โดยเสนอรายละเอียดประวัติการศึกษา ผลงาน ประสบการณ์ ของบุคลากรที่จะเข้ามาดำเนินงานโดยยื่นรายละเอียดเป็นเอกสารหลักฐานตามที่กำหนดในภาคผนวก ก รวมทั้งบุคลากรที่เสนอต้องแสดงหลักฐาน ยืนยันการเข้าร่วมปฏิบัติงานโครงการฯ เพื่อประกอบการพิจารณา โดยยกเว้นบุคลากรในภาคผนวก ข ให้จัดส่งรายชื่อตามคุณสมบัติที่กำหนดเพื่อเข้าปฏิบัติงานโครงการฯ ตามงวดงานที่ ๒

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

๔.๑๔ ผู้ยื่นข้อเสนอที่เสนอราคาในรูปแบบของ “กิจการร่วมค้า” ต้องมีคุณสมบัติดังนี้

(๑) กรณีที่กิจการร่วมค้าได้จดทะเบียนเป็นนิติบุคคลใหม่ กิจการร่วมค้าจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารประกวดราคา และการเสนอราคาให้เสนอราคาในนาม “กิจการร่วมค้า” ส่วนคุณสมบัติด้านผลงาน กิจการร่วมค้าร่วมดังกล่าวสามารถนำผลงานของผู้เข้าร่วมค้ามาใช้แสดงเป็นผลงานของกิจการร่วมค้าที่เข้าประกวดราคาได้

(๒) กรณีที่กิจการร่วมค้าไม่ได้จดทะเบียนเป็นนิติบุคคลใหม่ นิติบุคคลแต่ละนิติบุคคลที่เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารประกวดราคา เว้นแต่ในกรณีที่กิจการร่วมค้า ได้มีข้อตกลงระหว่างผู้เข้าร่วมค้าเป็นลายลักษณ์อักษร กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้รับผิดชอบหลัก ในการเข้าเสนอราคากับหน่วยงานของรัฐ และแสดงหลักฐานดังกล่าวมาพร้อมการยื่นข้อเสนอประกวดราคาทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ กิจการร่วมค้านั้นสามารถใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอได้

ทั้งนี้ “กิจการร่วมค้าที่จดทะเบียนเป็นนิติบุคคลใหม่” หมายความว่า กิจการร่วมค้าที่จดทะเบียน เป็นนิติบุคคลต่อกรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์

๔.๑๕ ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

(๑) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า ๑ ปี ต้องมีมูลค่าสุทธิของกิจการจากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สุทธิที่ปรากฏ งบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก ๑ ปี สุดท้ายก่อนวันยื่นข้อเสนอ

(๒) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งยังไม่มีการรายงาน งบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้าให้พิจารณา การกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่ได้ชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอไม่ต่ำกว่า ๒๐ ล้านบาท

(๓) สำหรับการจัดซื้อจัดจ้าง ครั้งหนึ่งที่มีวงเงินเกิน ๕๐๐,๐๐๐ บาทขึ้นไป กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดา โดยพิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน ๙๐ วัน ก่อนวัน ยื่นข้อเสนอ โดยต้องมีเงินฝากคงเหลือในการบัญชีธนาคารเป็นมูลค่า ๑ ใน ๔ ของมูลค่า งบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้งและหากเป็นผู้ชนะการจัดซื้อจัดจ้าง หรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝาก ที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

(๔) กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง (สินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุน หรือบริษัทเงินทุนหลักทรัพย์

ลงชื่อ ..... ประธานกรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ

ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์ และประกอบธุรกิจค้ำประกัน ตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคาร แห่งประเทศไทยแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อ ที่สำนักงานใหญ่รับรองหรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันที่ยื่นข้อเสนอไม่เกิน ๙๐ วัน)

๔.๑๖ ผู้ยื่นข้อเสนอซึ่งเป็นผู้ประกอบการ SMEs แสดงสำเนาใบขึ้นทะเบียนผู้ประกอบการวิสาหกิจขนาดกลางและขนาดย่อม (SMEs) (ถ้ามี) มาพร้อมการยื่นข้อเสนอทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์

๕. หลักเกณฑ์การพิจารณาคัดเลือก

ในการพิจารณาผล สำนักงานปลัดกระทรวงแรงงาน จะพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ โดยใช้หลักเกณฑ์ราคาประกอบเกณฑ์อื่น โดยพิจารณาให้คะแนนตามปัจจัยหลักและน้ำหนักที่กำหนด ดังนี้

๕.๑ ราคาที่ยื่นข้อเสนอ (Price) กำหนดน้ำหนักเท่ากับร้อยละ ๓๐ (สามสิบ)

๕.๒ คุณภาพและคุณสมบัติที่เป็นประโยชน์ต่อทางราชการ กำหนดน้ำหนักรวม เท่ากับร้อยละ ๗๐ (เจ็ดสิบ) โดยมีรายละเอียดตามภาคผนวก ง เกณฑ์คุณภาพและคุณสมบัติที่เป็นประโยชน์ต่อทางราชการ

ผู้ยื่นข้อเสนอจะต้องศึกษาข้อกำหนดการสาธิตการทดสอบ (Proof of Concept : POC) ตามภาคผนวก ง เกณฑ์คุณภาพและคุณสมบัติที่เป็นประโยชน์ต่อทางราชการ เพื่อเตรียมการจัดทำระบบสารสนเทศ เพื่อการสาธิตการทดสอบระบบ และทำการติดตั้งให้พร้อมสำหรับการทดสอบ ณ สถานที่ที่สำนักงานปลัดกระทรงแรงงานกำหนด โดยคณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์ จะจัดให้มีการอธิบายขั้นตอนและวิธีการสาธิตการทดสอบระบบก่อนการทดสอบ ผู้ยื่นข้อเสนอจะต้องจัดเตรียมระบบสารสนเทศ รวมทั้งอุปกรณ์คอมพิวเตอร์ (Hardware & Software) ที่มีขีดความสามารถเพียงพอในการสาธิตการทดสอบตามเกณฑ์การทดสอบที่กำหนด ทั้งนี้ ผู้ยื่นข้อเสนอทุกรายจะต้องทำการทดสอบให้เสร็จสิ้นตามวันเวลาที่กำหนด โดยมีคณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์ และ/หรือเจ้าหน้าที่เทคนิคที่ได้รับมอบหมายร่วมทำการทดสอบตลอดระยะเวลาการทดสอบ และเมื่อสิ้นเสร็จการทดสอบแล้ว จะพิจารณาคะแนนผลการทดสอบตามที่กำหนดต่อไป

๖. ขอบเขตการดำเนินงาน

๖.๑ ผู้ขายจะต้องจัดทำแผนดำเนินการ หรือแผนการติดตั้งอุปกรณ์ในโครงการฯ โดยกำหนดระยะเวลาในการดำเนินการแต่ละกิจกรรมอย่างชัดเจน เพื่อให้คณะกรรมการตรวจรับพัสดุ พิจารณาอนุมัติก่อนเริ่มดำเนินการ ภายใน ๓๐ วัน นับถัดจากวันลงนามในสัญญา

๖.๒ ผู้ขายจะต้องเข้าสำรวจสถานที่ติดตั้งอุปกรณ์ที่ใช้ในโครงการฯ โดยจะต้องทำการออกแบบสถานที่และการเชื่อมต่ออุปกรณ์ทั้งหมดที่ใช้ในโครงการฯ ให้สามารถใช้งานได้อย่างมีประสิทธิภาพ โดยมีรายละเอียดดังต่อไปนี้

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ	ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ	ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ	ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ	ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการและเลขานุการ	

๖.๒.๑ กล้องโทรทัศน์วงจรปิดชนิดเครือข่าย แบบมุมมองคงที่สำหรับติดตั้งภายในสำนักงาน จำนวน ๔ ชุด

๖.๒.๒ อุปกรณ์บันทึกภาพผ่านเครือข่าย (Network Video Recorder) แบบ ๘ ช่อง จำนวน ๑ ชุด

๖.๒.๓ อุปกรณ์การบริหารจัดการ การเข้า-ออกประตู พร้อมเครื่องบันทึก ๑ ระบบ

๖.๒.๔ จอแสดงผลภาพแบบวิดีโอวอล (Video Wall) จำนวน ๔ จอ

๖.๒.๕ ตู้ควบคุมและจัดการจอแสดงภาพแบบวิดีโอวอล (Video Wall Controller) จำนวน ๑ ชุด

๖.๒.๖ จอแสดงผลภาพสำหรับสื่อสาร ประชุมหรืออบรมภายในห้อง SOC พร้อมอุปกรณ์เชื่อมต่อการแสดงผล จำนวน ๑ จอ

๖.๒.๗ เครื่องคอมพิวเตอร์ตั้งโต๊ะ สำหรับงานวิเคราะห์และตอบสนองภัยคุกคามชั้นสูง จำนวน ๕ ชุด

๖.๒.๘ จอแสดงภาพขนาดไม่น้อยกว่า ๒๑.๕ นิ้ว สำหรับเจ้าหน้าที่ปฏิบัติงาน จำนวน ๕ จอ

๖.๒.๙ เครื่องสำรองไฟฟ้า ขนาด ๑๐ kVA (ระบบไฟฟ้า ๓ เฟส) จำนวน ๑ ชุด

๖.๒.๑๐ เครื่องปรับอากาศขนาดไม่เกิน ๒๔,๐๐๐ BTU พร้อมติดตั้งจำนวน ๒ ชุด

๖.๒.๑๑ เครื่องพิมพ์ Multifunction เลเซอร์หรือ LED สี จำนวน ๑ ชุด

๖.๒.๑๒ เครื่องทำลายเอกสาร ๑ ชุด

๖.๒.๑๓ ตู้เก็บของ (ล็อคเกอร์) ๑ ชุด

๖.๒.๑๔ อุปกรณ์สำนักงาน ประกอบด้วย

๖.๒.๑๔.๑ โต๊ะทำงาน ๕ ชุด

๖.๒.๑๔.๒ เก้าอี้สำนักงาน ๕ ชุด

๖.๒.๑๔.๓ กระดานไวท์บอร์ด ๑ ชุด

๖.๒.๑๔.๔ กระดาษและหมึกพริ้นท์ ๑ ชุด

๖.๒.๑๔.๕ โต๊ะประชุม อย่างน้อย ๕ ที่นั่ง ๑ ชุด

๖.๒.๑๕ อุปกรณ์สำนักงานจิปาถะอื่น ๆ เช่น ปากกา สีไฮไลท์ ปากกาเขียนกระดานไวท์บอร์ด เป็นต้น

๖.๒.๑๖ งานปรับปรุงพื้นที่ รายละเอียดดังนี้

๖.๒.๑๖.๑ งานรื้อถอนและขนเศษวัสดุทิ้ง

๖.๒.๑๖.๒ งานฝ้าเพดานฉาบเรียบทาสี

๖.๒.๑๖.๓ งานผนังเบาฉาบเรียบทาสี

๖.๒.๑๖.๔ งานประตูบานสวิงกระจกเทมเปอร์

๖.๒.๑๖.๕ งานย้ายประตูบานเลื่อน

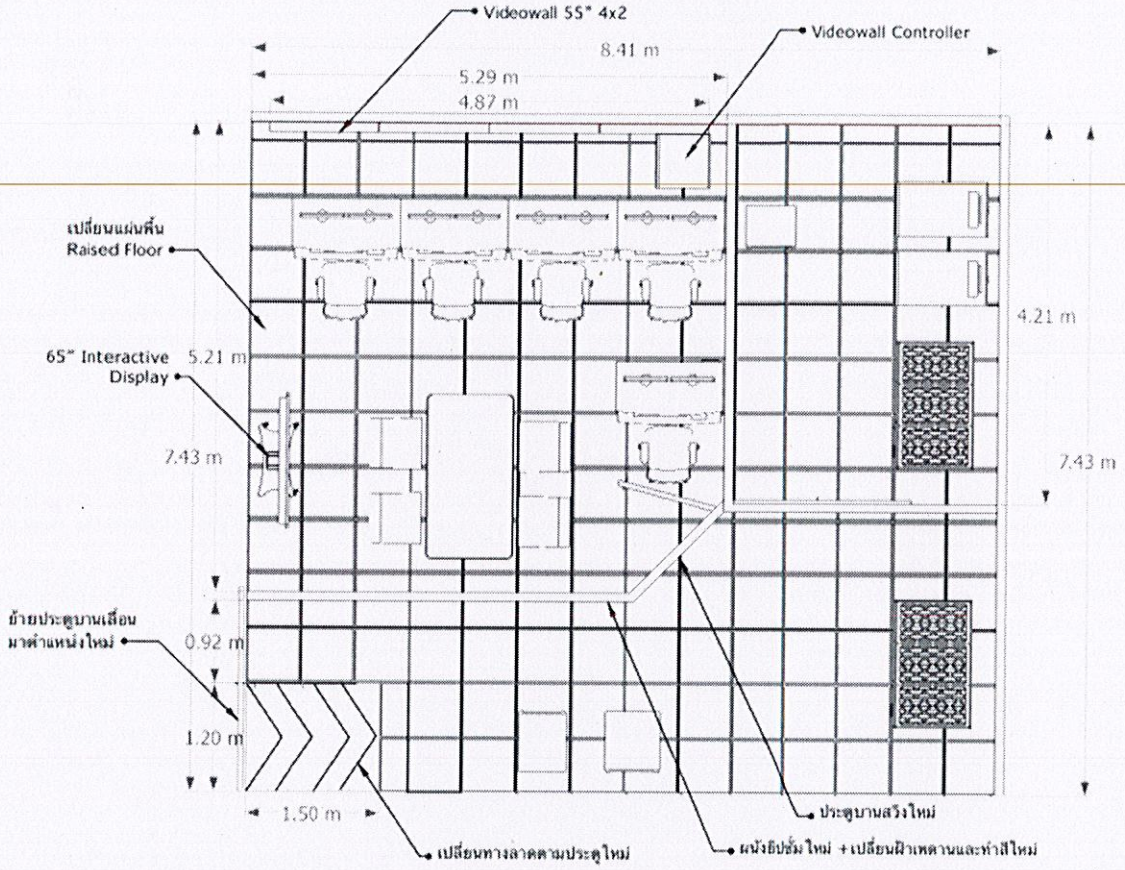
๖.๒.๑๖.๖ งานซ่อมแซมผนังมุมห้อง

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ	ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ	ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ	ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ	ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการและเลขานุการ	

๖.๒.๑๖.๗ ส่วนงานพื้น Raised Floor

แบบร่างงานปรับปรุงห้อง MSOC



๖.๓ การรื้อถอน ผู้ขายจะต้องจัดหาวัสดุปกคลุมบริเวณพื้นที่ปรับปรุงและการรื้อถอนไม่ให้เกิดการชำรุดเสียหาย หากเกิดความชำรุดเสียหายต่อทรัพย์สินของผู้ว่าจ้าง ผู้ขายจะต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นทั้งหมด โดยผู้ว่าจ้างไม่ต้องเสียค่าใช้จ่ายใด ๆ ในการนี้ทั้งสิ้น

๖.๔ ผู้ขายต้องทำการส่งคืนวัสดุ อุปกรณ์ และครุภัณฑ์ ที่มีมูลค่าซึ่งได้จากการรื้อถอน พร้อมจัดทำรายละเอียดการส่งคืนให้คณะกรรมการตรวจรับพัสดุทราบ และทำการทิ้งวัสดุที่ไม่มีมูลค่าให้แก่สำนักงานปลัดกระทรวงแรงงาน

๖.๕ ผู้ขายจะต้องดำเนินการติดตั้งอุปกรณ์ทั้งหมดที่ใช้ในโครงการฯ ทั้งการตั้งค่า (Configuration) การปรับแต่งระบบ (Customization) รวมไปถึงการทดสอบการทำงานที่เป็นการทดสอบสภาวะการทำงานของอุปกรณ์ ที่นำเสนอใน

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ

โครงการ (Equipment Testing) ซึ่งการดำเนินการติดตั้งทุกขั้นตอนจะต้องดำเนินการร่วมกับเจ้าหน้าที่ผู้รับผิดชอบของสำนักงานปลัดกระทรวงแรงงาน

๖.๖ ผู้ขายจะต้องจัดหาเครื่องมือที่จำเป็น ที่ต้องใช้สำหรับการติดตั้งอุปกรณ์ทั้งหมดที่ใช้ในโครงการฯ ให้สามารถใช้งานได้อย่างสมบูรณ์ตามที่สำนักงานปลัดกระทรวงแรงงานกำหนด โดยผู้ขายต้องเป็นผู้ออกค่าใช้จ่ายเองทั้งสิ้น

๖.๗ ผู้ขายจะต้องจัดทำหรือติดตั้งระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามทางไซเบอร์ (Extended Detection and Response) เพื่อรวบรวมและแสดงเหตุการณ์ ความเสี่ยง แสดงในรูปแบบ Dashboard สำหรับป้องกันและตรวจจับภัยคุกคามในระดับเครื่องผู้ใช้งาน (Client) และเครื่องแม่ข่าย (Server) และอุปกรณ์ตรวจจับและป้องกันการโจมตีระบบเครือข่าย (Intrusion Prevention System) หรือ อุปกรณ์ตรวจจับ, วิเคราะห์และเฝ้าระวังภัยคุกคามบนระบบเครือข่าย (Network Sensor) ในโครงการให้อยู่ในระบบเดียวกัน (Single Console) ได้

๖.๘ ผู้ขายจะต้องจัดทำหรือติดตั้งระบบตรวจประเมินความเสี่ยงความมั่นคงปลอดภัยไซเบอร์เพื่อค้นหาช่องโหว่และความเสี่ยงที่อาจเกิดขึ้นสำหรับระบบเครือข่าย, เครื่องแม่ข่าย และเว็บแอพพลิเคชั่น เพื่อรวบรวมและแสดงเหตุการณ์ความเสี่ยง แสดงในรูปแบบ Dashboard สำหรับป้องกันและตรวจจับภัยคุกคามในระดับเครื่องผู้ใช้งาน (Client) และเครื่องแม่ข่าย (Server) และอุปกรณ์ตรวจจับและป้องกันการโจมตีระบบเครือข่าย (Intrusion Prevention System) หรือ อุปกรณ์ตรวจจับ, วิเคราะห์และเฝ้าระวังภัยคุกคามบนระบบเครือข่าย (Network Sensor) ในโครงการให้อยู่ในระบบเดียวกัน (Single Console) ได้

๖.๙ ผู้ขายจะต้องพัฒนากระบวนการทำงานภายในศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ สำนักงานปลัดกระทรวงแรงงานให้สอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และการรักษาความมั่นคงปลอดภัยสารสนเทศ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และเป็นไปตามมาตรฐานสากล ISO/IEC 27001 โดยมีรายละเอียดดังนี้

(๑) ศึกษา วิเคราะห์สภาพทั่วไปของบริบทขององค์กร รวมถึงระบบงานต่าง ๆ ที่เกี่ยวข้องกับการปฏิบัติภารกิจของหน่วยงาน รวมถึงขอบเขตการให้บริการและสภาพแวดล้อมต่าง ๆ ที่เกี่ยวข้องกับการทำงานของศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์

(๒) ให้คำแนะนำในการจัดตั้งคณะกรรมการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศภายในเพื่อศึกษาและดำเนินการให้ศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นไปตามมาตรฐานสากล ISO/IEC 27001 อย่างละเอียด

(๓) รายงานผลการศึกษาพร้อมประเมินความต้องการเบื้องต้น และกำหนดขอบเขตของระบบบริหารจัดการด้านความ มั่นคงปลอดภัยสารสนเทศ รวมทั้งรายงานผลการทำงานในภาพรวม

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

(๔) ออกแบบระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศสำหรับการปฏิบัติงานในศูนย์ปฏิบัติการรักษา ความมั่นคงปลอดภัยไซเบอร์และโครงสร้างพื้นฐานที่สนับสนุน ให้แก่สำนักงานปลัดกระทรวงแรงงาน ให้สอดคล้องกับมาตรฐาน ISO/IEC 27001

(๕) จัดทำแผนการจัดทำระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ

๕.๑ ดำเนินการร่วมกับคณะทำงานในการจัดทำบัญชีรายการทรัพย์สิน (Asset Inventory) ตามขอบเขตที่กำหนดและร่วมดำเนินการในการพัฒนากระบวนการหรือระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ในการประเมินและวิเคราะห์ความเสี่ยงตามรายการทรัพย์สินที่จัดทำขึ้น

๕.๒ จัดทำแผนบริหารจัดการความเสี่ยงด้านสารสนเทศ

๕.๓ จัดเตรียมแนวทางการนำระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศไปปฏิบัติ เพื่อเป็นมาตรการป้องกันความเสี่ยงและแนวทางการถ่ายทอดความรู้และแนวปฏิบัติที่ถูกต้อง

๕.๔ จัดเตรียมแนวทางในการเฝ้าระวังและทบทวนสำหรับการวัดผลของมาตรการควบคุมความเสี่ยงที่ใช้ควบคุม ดูแลองค์กร รวมถึงความถี่ในการเฝ้าระวังต้องสอดคล้องกับความเสี่ยงเพื่อให้มั่นใจว่าหากเกิดเหตุการณ์ที่เกี่ยวข้องกับ ความมั่นคงปลอดภัย หน่วยงานสามารถมีกระบวนการรายงานผลได้ทันเวลา

๕.๕ จัดเตรียมแนวทางในการรักษามาตรฐานและการพัฒนาปรับปรุงกระบวนการ เพื่อป้องกันปัญหาที่อาจเกิดขึ้นซ้ำซ้อนในอนาคตรวมถึงแนวทางในการปรับปรุงระบบบริหารจัดการ ด้านความมั่นคงปลอดภัยสารสนเทศให้มีประสิทธิภาพยิ่งขึ้นกว่าเดิม

๕.๖ จัดเตรียมเอกสาร Statement of Applicability (SOA) ตาม Annex A ของ มาตรฐานสากล ISO/IEC27001 และตัวอย่างของมาตรการควบคุมความเสี่ยง เช่น นโยบาย ขั้นตอนการปฏิบัติ และแบบฟอร์มเพื่อบันทึกการทำงาน เป็นต้น เพื่อให้มีความถูกต้องและเป็นไปตามมาตรฐานสากล

(๖) กำหนดแนวทางในการคัดเลือกทีมงานตรวจสอบภายในและดำเนินการตรวจสอบระบบ บริหารจัดการความมั่นคงปลอดภัยตามมาตรฐานสากล ISO/IEC 27001 ร่วมกับทีมงานตรวจสอบภายใน รวมทั้งพัฒนารายงานการตรวจสอบภายใน (Internal Audit) เพื่อให้ทราบถึงผลลัพธ์และเตรียมนำสู่การยื่นขอใบรับรองมาตรฐานสากล ISO/IEC 27001

(๗) จัดทำรายงานเสนอผู้บริหารระดับสูงเพื่อพิจารณาเกี่ยวกับแผนและแนวทางการพัฒนาระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

๗. การส่งมอบงาน แบ่งออกเป็น ๔ งวดงาน ดังนี้

งวดงานที่ ๑ ผู้ขายจะต้องดำเนินการให้แล้วเสร็จสมบูรณ์ภายในระยะเวลา ๖๐ วัน นับถัดจากวันลงนามในสัญญา ประกอบด้วย

๑. จัดทำแผนดำเนินการโครงการฯ พร้อมรายละเอียดในการดำเนินการแต่ละกิจกรรมอย่างชัดเจน โดยจัดส่งเอกสารเสนอคณะกรรมการตรวจรับพัสดุ

๒. ดำเนินการสำรวจ วิเคราะห์ ความต้องการเบื้องต้น เพื่อออกแบบศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (Ministry Security Operation Center) พร้อมทั้งจัดทำรายงาน และจัดส่งเอกสารเสนอคณะกรรมการตรวจรับพัสดุ

งวดงานที่ ๒ ผู้ขายจะต้องดำเนินการให้แล้วเสร็จสมบูรณ์ภายในระยะเวลา ๒๗๐ วัน นับถัดจากวันลงนามในสัญญา ประกอบด้วย

๑. ส่งมอบงานด้านอุปกรณ์ทั้งหมดในโครงการตามข้อกำหนดทางด้านระบบตรวจจับภัยคุกคามทางไซเบอร์และประเมินความเสี่ยงระบบสารสนเทศ

๑.๑ ส่งมอบเอกสารแสดงลิขสิทธิ์การใช้งาน (License) ถูกต้องจากเจ้าของลิขสิทธิ์ในรายการอุปกรณ์ที่ติดตั้งทั้งหมด

๑.๒ ส่งมอบเอกสารคู่มือการใช้งานของอุปกรณ์ (User manual) และคู่มือการดูแลอุปกรณ์ (Admin user manual) โดยจัดส่งในรูปแบบสื่ออิเล็กทรอนิกส์

๑.๓ ส่งมอบงานปรับปรุงห้องศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์

๑.๔ ส่งมอบงานติดตั้ง อุปกรณ์ทั้งหมดที่ใช้ในโครงการฯ ตามข้อกำหนดทางด้านเทคนิค และจัดทำรายงานผลการติดตั้ง และทดสอบอุปกรณ์

๑.๕ ส่งมอบและจัดทำรายงานผลการทดสอบสภาวะการทำงานของอุปกรณ์ (Equipment Testing)

๑.๖ ส่งมอบงานตามข้อกำหนดทางด้านบุคลากรและงานพัฒนาศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (ตามภาคผนวก ก) ในส่วนงานดังนี้

๑.๖.๑ ที่ปรึกษาด้านการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์และผู้เชี่ยวชาญด้านมาตรฐาน ISO/IEC 27001 เข้าร่วมทำงานเพื่อพัฒนากระบวนการปฏิบัติงานในศูนย์ฯ ติดตาม ควบคุม กำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานปลัดกระทรวงแรงงานอย่างต่อเนื่อง พร้อมส่งมอบรายงานสรุปผลการดำเนินงาน ดังนี้

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

๑.๖.๑.๑ รายงานผลการออกแบบระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศสำหรับการปฏิบัติงานในศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์และโครงสร้างพื้นฐานที่สนับสนุน ให้แก่สำนักงานปลัดกระทรวงแรงงาน ที่สอดคล้องกับมาตรฐาน ISO/IEC 27001

๑.๖.๑.๒ รายงานแนวทางในการคัดเลือกทีมงานตรวจสอบภายในและดำเนินการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัยตามมาตรฐานสากล ISO/IEC 27001

๑.๖.๒ ทีมมาตรฐาน ISO/IEC 27001 พัฒนากระบวนการปฏิบัติงานภายในศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ สำนักงานปลัดกระทรวงแรงงานให้สอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และเป็นไปตามมาตรฐานสากล ISO/IEC 27001 พร้อมส่งมอบรายงานสรุปผลการดำเนินงาน ดังนี้

๑.๖.๒.๑ บัญชีรายการทรัพย์สิน (Asset Inventory) ตามขอบเขตที่กำหนดและร่วมดำเนินการในการพัฒนากระบวนการหรือระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

๑.๖.๒.๒ รายงานแนวทางการนำระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศไปปฏิบัติ แนวทางในการเฝ้าระวังและทบทวนสำหรับการวัดผลของมาตรการควบคุมความเสี่ยงที่ใช้ควบคุมดูแลองค์กร และแนวทางในการรักษามาตรฐานและการพัฒนาปรับปรุงกระบวนการ

๑.๗ ผู้ขายจะต้องจัดส่งรายชื่อบุคลากรเพื่อเตรียมปฏิบัติงานในศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (Ministry Security Operation Center) ตามภาคผนวก ข

งวดงานที่ ๓ ผู้ขายจะต้องดำเนินการให้แล้วเสร็จสมบูรณ์ภายในระยะเวลา ๓๓๐ วัน นับถัดจากวันลงนามในสัญญา ประกอบด้วย

๑. จัดฝึกอบรมเจ้าหน้าที่ให้มีความตระหนักรู้ถึงด้านความมั่นคงปลอดภัยสารสนเทศ และมีความเข้าใจด้านการปฏิบัติการด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบริการ ดิจิทัล ข้อมูลสารสนเทศ และโครงสร้างพื้นฐานสารสนเทศของสำนักงานปลัดกระทรวงแรงงานสำหรับเจ้าหน้าที่แบบ online จำนวนไม่น้อยกว่า ๑๒๐ คน เป็นเวลาไม่น้อยกว่า ๖ ชั่วโมง พร้อมรายงานสรุปผลและจัดส่งเอกสารเสนอคณะกรรมการตรวจรับพัสดุ

๒. ส่งมอบงานตามข้อกำหนดทางด้านบุคลากรและงานพัฒนาศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ในส่วนงานดังนี้

๒.๑ ทีมมาตรฐาน ISO/IEC 27001 พัฒนากระบวนการปฏิบัติงานภายในศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ สำนักงานปลัดกระทรวงแรงงานให้สอดคล้องตามพระราชบัญญัติการ

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ

รักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และเป็นไปตามมาตรฐานสากล ISO/IEC 27001 พร้อมส่งมอบรายงานสรุปผลการดำเนินงาน

๒.๑.๑ รายงานการตรวจสอบภายใน (Internal Audit) เพื่อให้ทราบถึงผลลัพธ์และเตรียมนำสู่การยื่นขอใบรับรองมาตรฐานสากล ISO/IEC 27001

๒.๑.๒ จัดทำรายงานเสนอผู้บริหารระดับสูงเพื่อพิจารณาเกี่ยวกับแผนและแนวทางการพัฒนาระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ

๒.๒ ที่ปรึกษาด้านการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์และผู้เชี่ยวชาญด้านมาตรฐาน ISO/IEC 27001 เข้าร่วมทำงานเพื่อพัฒนากระบวนการปฏิบัติงานในศูนย์ฯ และการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานปลัดกระทรวงแรงงานเพื่อให้มีความพร้อมในการเฝ้าระวังและรักษาความมั่นคงปลอดภัยไซเบอร์ และสอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และเป็นไปตามมาตรฐานสากล ISO/IEC 27001 พร้อมส่งมอบรายงานสรุปผล Statement of Applicability (SOA) ตาม Annex A ของ มาตรฐานสากล ISO/IEC27001 และตัวอย่างของมาตรการควบคุมความเสี่ยง

งวดงานที่ ๔ ผู้ขายจะต้องดำเนินการให้แล้วเสร็จสมบูรณ์ภายในระยะเวลา ๓๖๕ วัน นับถัดจากวันลงนามในสัญญา ประกอบด้วย

๑. จัดฝึกอบรมหลักสูตรสำหรับผู้ดูแลระบบที่เกี่ยวข้องกับโครงการ จำนวนไม่น้อยกว่า ๑๐ คน เป็นเวลาไม่ต่ำกว่า ๑๘ ชั่วโมง พร้อมรายงานสรุปผลและจัดส่งเอกสารเสนอคณะกรรมการตรวจรับพัสดุ

๒. ทีมมาตรฐาน ISO/IEC 27001 เข้าร่วมติดตามผลจากการปฏิบัติตามกรอบมาตรฐานและกระบวนการที่พัฒนาขึ้นในงวดงานที่ ๓ พร้อมทั้ง ตรวจทาน ให้คำแนะนำ และร่วมปรับปรุงแก้ไขกระบวนการและหรือเอกสารที่จำเป็นอย่างต่อเนื่อง พร้อมส่งมอบรายงานสรุปผลการดำเนินงาน (Final Report)

๘. เงื่อนไขการชำระเงิน

สำนักงานปลัดกระทรวงแรงงานจะทำการชำระตามสัญญา และผ่านการตรวจรับและเห็นชอบจากคณะกรรมการตรวจรับพัสดุเรียบร้อยแล้ว โดยจะทำการจ่ายเป็นจำนวน ๔ งวด ดังนี้

๘.๑ งวดที่ ๑ จ่ายเงินร้อยละ ๑๐ ของวงเงินตามสัญญา เมื่อส่งมอบงานงวดที่ ๑ เป็นที่เรียบร้อยและผ่านการตรวจรับและเห็นชอบจากคณะกรรมการตรวจรับพัสดุเรียบร้อยแล้ว

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ

๘.๒ งวดที่ ๒ จ่ายเงินร้อยละ ๔๐ ของวงเงินตามสัญญา เมื่อส่งมอบงานงวดที่ ๒ เป็นที่เรียบร้อยและผ่านการตรวจรับและเห็นชอบจากคณะกรรมการตรวจรับพัสดุเรียบร้อยแล้ว

๘.๓ งวดที่ ๓ จ่ายเงินร้อยละ ๔๐ ของวงเงินตามสัญญา เมื่อส่งมอบงานงวดที่ ๓ เป็นที่เรียบร้อยและผ่านการตรวจรับและเห็นชอบจากคณะกรรมการตรวจรับพัสดุเรียบร้อยแล้ว

๘.๔ งวดที่ ๔ จ่ายเงินร้อยละ ๑๐ ของวงเงินตามสัญญา เมื่อส่งมอบงานงวดที่ ๔ เป็นที่เรียบร้อยและผ่านการตรวจรับและเห็นชอบจากคณะกรรมการตรวจรับพัสดุเรียบร้อยแล้ว

๙. การคิดค่าปรับ กรณีดำเนินการไม่แล้วเสร็จตามระยะเวลา

๙.๑ ค่าปรับ รายวัน ในอัตราร้อยละ ๐.๒ (ศูนย์จุดสอง) ของราคาค่าพัสดุทั้งหมดที่ยังไม่ได้รับมอบ นับถัดจากวันที่สิ้นสุดสัญญาหรือวันที่สำนักงานปลัดกระทรวงแรงงานได้ขยายให้ จนถึงวันที่ทำงานแล้วเสร็จจริงและส่งผลงานที่แล้วเสร็จตามขอบเขตที่ระบุไว้ได้ครบถ้วนและถูกต้องแล้ว ถ้าไม่ถึงวันหรือเศษของวันให้คิดเป็นหนึ่งวัน

๙.๒ หากการส่งมอบดังกล่าวไม่ครบถ้วน ไม่สามารถใช้งานได้ ไม่แล้วเสร็จทันตามกำหนด สำนักงานปลัดกระทรวงแรงงานมีสิทธิเรียกค่าเสียหายใดๆ อันเนื่องมาจากผู้ขายไม่ปฏิบัติตามสัญญานี้ และถ้าสำนักงานปลัดกระทรวงแรงงานจัดซื้ออุปกรณ์รวมถึงการติดตั้งจากบุคคลอื่นเต็มจำนวนหรือเฉพาะจำนวนที่ขาดส่ง แล้วแต่กรณี ผู้ขายจะต้องชดใช้ราคาที่เพิ่มขึ้นจากราคาที่กำหนดไว้ในสัญญานี้ด้วย รวมทั้งค่าใช้จ่ายใดๆ ที่สำนักงานปลัดกระทรวงแรงงานต้องใช้จ่ายในการจัดหาผู้ขายรายใหม่ดังกล่าวด้วย

๙.๓ หากสำนักงานปลัดกระทรวงแรงงานเห็นว่าผู้ขายไม่อาจปฏิบัติตามสัญญาต่อไปได้ สำนักงานปลัดกระทรวงแรงงานจะใช้สิทธิบอกเลิกสัญญา และริบหรือบังคับจากหลักประกัน และถ้าสำนักงานปลัดกระทรวงแรงงานได้แจ้ง ข้อเรียกร้องให้ชำระค่าปรับไปยังผู้ขายเมื่อครบกำหนดส่งมอบแล้ว สำนักงานปลัดกระทรวงแรงงานมีสิทธิที่จะปรับผู้ขายจนถึงวันบอกเลิกสัญญาได้อีกด้วย

๑๐. การรับประกันผลงานและการให้บริการ

๑๐.๑ ผู้ขายจะต้องรับประกันการชำรุดบกพร่องของอุปกรณ์ระบบ เป็นระยะเวลา ๑ ปี ดังนี้

๑๐.๑.๑ ระบบคอมพิวเตอร์ ทั้งอุปกรณ์ฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ที่เสนอทั้งหมดในโครงการฯ

๑๐.๑.๒ อุปกรณ์ต่าง ๆ ทั้งหมดที่ใช้ทำการปรับปรุงพื้นที่ศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (Ministry Security Operation Center)

ทั้งนี้โดยวันที่เริ่มการรับประกันให้นับถัดจากวันที่ผู้ขายส่งมอบงานงวดสุดท้ายถูกต้องครบถ้วนตามสัญญาเรียบร้อย

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

๑๐.๒ ในช่วงระยะเวลาของการรับประกัน หากระบบคอมพิวเตอร์ ไม่สามารถใช้งานได้ตามปกติ ไม่ว่าจะเป็นกรณีปัญหาบางส่วนหรือทั้งระบบ ในเวลา ๗ วัน x ๒๔ ชั่วโมง (ตลอด ๒๔ ชั่วโมงของทุกวันไม่เว้นวันหยุดราชการ) ผู้ขายจะต้องจัดให้มีช่างที่มีความรู้ความชำนาญมาจัดการซ่อมแซมแก้ไขให้อยู่ในสภาพที่ใช้งานได้ดีตามปกติ และจะต้องซ่อมแซมโดยใช้อะไหล่แท้ ที่เป็นของใหม่เท่านั้น

๑๐.๓ กรณีระบบคอมพิวเตอร์ เกิดชำรุดเสียหายไม่สามารถใช้งานได้ตามปกติ ผู้ขายจะต้องเข้ามาดำเนินการตรวจสอบ วิเคราะห์ และแก้ไขปัญหาของระบบ ต้องดำเนินการแก้ไขให้แล้วเสร็จ ให้อยู่ในสภาพที่สามารถใช้งานได้ตามปกติภายใน ๔ ชั่วโมง นับตั้งแต่เวลาที่ได้รับแจ้งผ่านทางจดหมายอิเล็กทรอนิกส์ (E-Mail) หรือแจ้งให้ทราบทางวาจา หรือ ทางโทรศัพท์ ไม่ว่าวิธีใดวิธีหนึ่ง เป็นเวลาเริ่มต้น เพื่อใช้ในการคำนวณระยะเวลาในการเข้ามาดำเนินการแก้ไข จำนวนเวลาที่ใช้ในการคำนวณค่าปรับจะเริ่มตั้งแต่เวลาที่พ้นกำหนด ๔ ชั่วโมง จนถึงเวลาที่ผู้ขายได้ดำเนินการซ่อมแซมแก้ไขแล้วเสร็จและระบบคอมพิวเตอร์ ใช้งานได้ตามปกติ หากผู้ขายไม่สามารถดำเนินการแก้ไขระบบและอุปกรณ์ให้สามารถใช้งานได้ตามปกติ ผู้ขายจะต้องจัดหาอุปกรณ์ที่มีประสิทธิภาพเทียบเท่าหรือดีกว่ามาทดแทนให้กับสำนักงานปลัดกระทรวงแรงงานใช้งานจนกว่าจะสามารถซ่อมแซมแก้ไขได้แล้วเสร็จ พร้อมทั้งแจ้งให้เจ้าหน้าที่ของสำนักงานปลัดกระทรวงแรงงานผู้มีหน้าที่รับผิดชอบทราบในทันที

๑๐.๔ กรณีอุปกรณ์ระบบและอุปกรณ์สนับสนุนต่างๆ ในโครงการฯ ชำรุดเสียหายจำเป็นจะต้องนำกลับไปซ่อมแซมแก้ไข ผู้ขายจะต้องนำเครื่องและอุปกรณ์ประกอบใหม่ที่มีประสิทธิภาพเทียบเท่าหรือสูงกว่ามาทดแทนให้กับสำนักงานปลัดกระทรวงแรงงานใช้งานจนกว่าจะสามารถซ่อมแซมแก้ไขได้แล้วเสร็จ

๑๐.๕ กรณีผู้ขายมีความจำเป็นต้องนำเครื่องและอุปกรณ์สนับสนุนต่างๆ ในโครงการฯ กลับไปซ่อม ผู้ขายจะต้องซ่อมแซมโดยใช้อะไหล่แท้ที่เป็นของใหม่ และให้แล้วเสร็จภายในเวลา ไม่เกิน ๓๐ วัน นับถัดจากวันที่นำเครื่องและอุปกรณ์สนับสนุนไปซ่อม หากผู้ขายไม่สามารถซ่อมแซมให้แล้วเสร็จตามระยะเวลาที่กำหนดเวลาได้ ผู้ขายต้องทำการส่งมอบอุปกรณ์และทำหนังสือส่งมอบอุปกรณ์ที่นำมาทดแทน ให้เป็นทรัพย์สินของสำนักงานปลัดกระทรวงแรงงาน

๑๐.๖ กรณีที่ผู้ขายไม่ปฏิบัติตามสัญญาหรือข้อตกลงการรับประกันและก่อให้เกิดความเสียหาย ต่อการทำงานของสำนักงานปลัดกระทรวงแรงงาน ผู้ขายจะต้องรับผิดชอบค่าใช้จ่ายทั้งหมดอันจะเกิดจากการที่สำนักงานปลัดกระทรวงแรงงาน ต้องดำเนินการแก้ไขปัญหาดังกล่าว

๑๐.๗ ผู้ขายจะต้องจัดเจ้าหน้าที่ผู้มีความชำนาญเข้าทำการตรวจสอบและบำรุงรักษา (Preventive Maintenance) ณ ศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานปลัดกระทรวงแรงงาน ในรูปแบบ On site Service โดยการตรวจสอบสภาพการทำงานของอุปกรณ์ต่างๆ ของระบบคอมพิวเตอร์ที่เสนอในโครงการฯ ทั้งในส่วนของฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ทุกๆ ๔ เดือนภายในระยะเวลาการรับประกัน และจัดทำรายงานการตรวจสอบและบำรุงรักษา (Preventive Maintenance) ทุกครั้ง การบำรุงรักษาแต่ละครั้งจะต้อง

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ

มีเอกสารรายงานการบำรุงรักษา (Service Report) เป็นหลักฐานและจัดทำ Logbook/Check list ของงานที่ทำการบำรุงรักษาเก็บเป็นเอกสาร พร้อมกับรายงานประวัติการซ่อมบำรุงตลอดระยะเวลา เพื่อใช้อ้างถึงในกรณีที่มีข้อสงสัยเกี่ยวกับปัญหาที่เกิดขึ้น

๑๐.๘ การบำรุงรักษาแบบ 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

๑๐.๙ กรณีที่สำนักงานปลัดกระทรวงแรงงาน มีความประสงค์จะปรับแต่งระบบ ให้มีประสิทธิภาพมากขึ้น รวมถึงการเคลื่อนย้ายเครื่องและอุปกรณ์สนับสนุนทั้งหมดที่เสนอมาในโครงการฯ เพื่อเพิ่มประสิทธิภาพดังกล่าว ค่าใช้จ่ายที่เกิดขึ้นทั้งหมดให้ถือเป็นภาระรับผิดชอบของผู้ขาย

๑๐.๑๐ การสนับสนุนการปฏิบัติงานในศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์

ผู้ขายจะต้องจัดให้มีเจ้าหน้าที่คอยสนับสนุนการปฏิบัติงานภายในศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ตามภาคผนวก ข เริ่มเข้าปฏิบัติงานที่ศูนย์ฯ ตามข้อกำหนด และส่งมอบรายงานสรุปผลการเฝ้าระวังภัยคุกคามทางไซเบอร์สำหรับผู้บริหาร (Executive Reports) เป็นระยะเวลา ๑ ปี นับถัดจากวันที่ผู้ขายส่งมอบงานงวดสุดท้ายถูกต้องครบถ้วนตามสัญญาเรียบร้อย โดยมีรายละเอียดดังนี้

๑) ผู้จัดการศูนย์ปฏิบัติการ (SOC Manager) ควบคุมการปฏิบัติงานของ เจ้าหน้าที่ประจำศูนย์ฯ ในวันเวลาทำการอย่างน้อยสัปดาห์ละ ๒ วัน ตั้งแต่เวลา ๐๘.๓๐ น. – ๑๖.๓๐ น. จำนวนอย่างน้อย ๑ คน

๒) เจ้าหน้าที่วิเคราะห์ภัยคุกคามฯ ระบบ ระดับ ๑ (Cyber Security Analyst T1) เข้าปฏิบัติหน้าที่ประจำที่ศูนย์ฯ ในวันเวลาทำการ ตั้งแต่เวลา ๐๘.๓๐ น. – ๑๖.๓๐ น. จำนวน ๒ คน

๓) เจ้าหน้าที่วิเคราะห์ภัยคุกคามฯ ระบบ ระดับ ๒ (Cyber Security Analyst T2) เข้าปฏิบัติหน้าที่ประจำที่ศูนย์ฯ ในวันเวลาทำการ ตั้งแต่เวลา ๐๘.๓๐ น. – ๑๖.๓๐ น. จำนวนอย่างน้อย ๒ คน

ทั้งนี้ ให้ผู้ขายแสดงรายชื่อเจ้าหน้าที่และหมายเลขโทรศัพท์สำหรับการติดต่อ เพื่อการสนับสนุนหรือให้คำแนะนำตลอด ๒๔ ชั่วโมง

๑๐.๑๑ การคิดค่าปรับกรณีระบบขัดข้องในช่วงระยะเวลารับประกันดังนี้

๑) ในกรณีที่ไม่สามารถซ่อมแซมได้ภายในเวลาที่กำหนด ระยะเวลาอุปกรณ์ต่างๆ ในระบบขัดข้องรวมตามเกณฑ์การคำนวณนับไม่เกินเดือนละ ๓๖ ชั่วโมง หรือร้อยละ ๕ (ห้า) ของเวลา ใช้งานทั้งหมดของอุปกรณ์ต่างๆ ในระบบแล้วแต่ตัวเลขใดจะมากกว่ากัน มิฉะนั้นผู้ขายจะต้องยอมให้สำนักงานปลัดกระทรวงแรงงาน คิดค่าปรับเวลาที่ไม่สามารถ

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ	ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ	ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ	ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ	ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการและเลขานุการ	

ใช้งานอุปกรณ์ต่างๆ ในระบบในส่วนที่เกินกำหนดข้างต้นเป็นชั่วโมง ในอัตราร้อยละ ๐.๐๒๕ (ศูนย์จุดศูนย์สองห้า) ของวงเงินในสัญญาฯ คูณจำนวนชั่วโมง คูณค่าตัวถ่วงตามภาคผนวก จ โดยเศษของชั่วโมงให้คิดเป็นหนึ่งชั่วโมง

๒) กรณีบุคลากรตามภาคผนวก ข ไม่สามารถปฏิบัติงานได้ครบเวลาตามที่กำหนดไว้ในข้อกำหนดทางด้านบุคลากรและพัฒนาศูนย์ฯ สำนักงานปลัดกระทรวงแรงงานจะคิดค่าปรับเป็นรายชั่วโมง ในอัตราร้อยละ ๐.๐๒๕ (ศูนย์จุดศูนย์สองห้า) ของวงเงินในสัญญาฯ คูณจำนวนชั่วโมง คูณค่าตัวถ่วงตามภาคผนวก จ โดยเศษของชั่วโมงให้คิดเป็นหนึ่งชั่วโมง

๓) สำนักงานปลัดกระทรวงแรงงาน ขอสงวนสิทธิ์ที่จะยึดหลักค้ำประกันสัญญาในกรณีที่ผู้ขายไม่ปฏิบัติตามสัญญาหรือข้อตกลง หรือกระทำให้เกิดความเสียหายต่ออุปกรณ์ต่างๆ ในระบบของ สำนักงานปลัดกระทรวงแรงงาน หากสำนักงานปลัดกระทรวงแรงงาน พิจารณาแล้วว่าเกิดความเสียหายจริง ทั้งนี้ผู้ขายจะต้องรับผิดชอบค่าใช้จ่ายทั้งหมด อันจะเกิดจากการที่สำนักงานปลัดกระทรวงแรงงาน ต้องดำเนินการแก้ไขปัญหาระบบคอมพิวเตอร์ หรือจัดหาอะไหล่ หรือจัดหาอุปกรณ์ต่างๆ ในระบบใหม่ทดแทน

๔) ในระหว่างการดำเนินการ หากผู้ขายทำให้อุปกรณ์ต่างๆ ของสำนักงานปลัดกระทรวงแรงงาน ชำรุดเสียหายหรือ ทำให้สถานที่ส่วนใดส่วนหนึ่งของอาคารชำรุดเสียหาย ผู้ขายจะต้องแก้ไขปรับปรุงหรือทำขึ้นใหม่ให้คงเดิมและใช้งานได้ตามปกติ และผู้ขายเป็นผู้รับภาระค่าใช้จ่ายเองทั้งหมด

๑๐.๑๒ การดำเนินการใดๆ ไม่ว่าจะเป็นส่วนของฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ที่ผู้ขายดำเนินการติดตั้งในโครงการ หากมีปัญหาเกี่ยวกับลิขสิทธิ์ ผู้ขายจะต้องดำเนินการขออนุญาต ทำการตกลงอย่างอื่นอย่างใดกับบุคคลผู้เป็นเจ้าของลิขสิทธิ์ เพื่อให้สามารถใช้ลิขสิทธิ์นั้นๆ ได้อย่างถูกต้องตามกฎหมาย โดยให้ถือเป็นภาระหน้าที่ของผู้ขายเพียงฝ่ายเดียวและเป็นผู้รับภาระค่าใช้จ่ายเองทั้งหมด

๑๐.๑๓ ผู้ขายจะต้องจัดเก็บรักษาข้อมูลต่าง ๆ ที่เกี่ยวกับการดำเนินงานตามสัญญานี้ที่ผู้ขายได้รับจากผู้ว่าจ้าง ซึ่งรวมถึง ข้อมูลต่าง ๆ ที่ ผู้ว่าจ้างได้จัดทำขึ้นเนื่องจากการดำเนินงานนี้อย่างเป็นความลับ และ/หรือความลับทางการค้าของผู้ว่าจ้าง และผู้ขายต้องหามาตรการในการจัดเก็บข้อมูลที่เป็นความลับให้มิดชิดทั้งนี้ ผู้ขายจะต้องลงนามใน “สัญญาไม่เปิดเผย ข้อมูลที่เป็นความลับ” ภายใน ๑๕ วัน นับถัดจากวันลงนามในสัญญา

๑๑. การฝึกอบรมโครงการ

๑๑.๑ ผู้ขายจะต้องดำเนินการจัดฝึกอบรม และจัดทำคู่มือการฝึกอบรม ไม่น้อยกว่า ๒ หลักสูตร ประกอบด้วยหลักสูตร IT Security Awareness Training จำนวนไม่น้อยกว่า ๑๒๐ คน ระยะเวลาไม่น้อยกว่า ๖ ชั่วโมง และหลักสูตรการดูแลระบบสำหรับผู้ดูแลระบบ (Administrator) จำนวนไม่น้อยกว่า ๑๐ คน ระยะเวลาไม่ต่ำกว่า ๑๘ ชั่วโมง โดยเสนอแผนการฝึกอบรมต่อคณะกรรมการตรวจรับพัสดุและได้รับการอนุมัติให้ดำเนินการ โดยมีรายละเอียด ดังนี้

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ

(๑) ชื่อหลักสูตร

(๒) วัตถุประสงค์ของการฝึกอบรม

(๓) หัวข้อการฝึกอบรม

(๔) ระยะเวลาการฝึกอบรม

(๕) สถานที่ในการฝึกอบรม

(๖) จำนวนผู้เข้ารับการฝึกอบรม

ทั้งนี้ผู้ขายต้องรับผิดชอบค่าใช้จ่ายที่เกิดขึ้นจากการฝึกอบรม ได้แก่ ค่าเครื่องคอมพิวเตอร์และอุปกรณ์สำหรับการฝึกอบรม ค่าอาหารว่างและเครื่องดื่ม ค่าอาหารกลางวัน ค่าวิทยากร ค่าเอกสารประกอบการฝึกอบรม และค่าใช้จ่ายอื่น ๆ ที่เกี่ยวข้อง ผู้ขายจะต้องเป็นผู้รับผิดชอบทั้งหมด

๑๑.๒ สำนักงานปลัดกระทรวงแรงงานขอสงวนสิทธิ์ในการคัดลอกหรือทำซ้ำเอกสารและคู่มือต่างๆ เพื่อใช้งานในกิจการของสำนักงานปลัดกระทรวงแรงงาน หากเอกสารและคู่มือรายการใดไม่สามารถคัดลอกหรือทำซ้ำได้ ให้ผู้ขายแจ้งสำนักงานปลัดกระทรวงแรงงานทราบเป็นลายลักษณ์อักษร

กรณีผู้ขายไม่แจ้งให้สำนักงานปลัดกระทรวงแรงงานทราบ จะถือว่าผู้ขายอนุญาตให้คัดลอกหรือทำซ้ำได้ ทั้งนี้หากมีบุคคลภายนอกกล่าวอ้างหรือใช้สิทธิ์เรียกร้องใดๆ ว่ามีการละเมิดลิขสิทธิ์เกี่ยวกับเอกสารและคู่มือที่สำนักงานปลัดกระทรวงแรงงานคัดลอกหรือทำซ้ำเพื่อใช้งานในกิจการของสำนักงานปลัดกระทรวงแรงงาน ผู้ขายต้องดำเนินการทั้งปวงเพื่อให้การกล่าวอ้างหรือการเรียกร้องดังกล่าวระงับสิ้นไปโดยเร็ว โดยผู้ขายต้องเป็นผู้ชำระค่าเสียหายและค่าใช้จ่ายต่างๆ ที่เกิดขึ้นทั้งหมด

๑๒. วงเงินในการจัดหา

งบประมาณจำนวน ๗๓,๑๐๖,๓๐๐ บาท (เจ็ดสิบสามล้านหนึ่งแสนหกพันสามร้อยบาทถ้วน) ซึ่งเป็นราคาที่รวมภาษีมูลค่าเพิ่ม และค่าใช้จ่ายทั้งปวงแล้ว

๑๓. สถานที่/พื้นที่ดำเนินการ

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารสำนักงานปลัดกระทรวงแรงงาน

๑๔. ติดต่อสอบถามรายละเอียดเพิ่มเติมได้ที่

หน่วยงาน : ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารสำนักงานปลัดกระทรวงแรงงาน

โทรศัพท์ : ๐ ๒๒๓๒ ๑๒๒๔ , ๐ ๒๒๓๒ ๑๓๓๔

โทรสาร : ๐ ๒๒๔๘ ๔๑๔๑

E-mail Address : ictc@mol.mail.go.th

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ภาคผนวก ก

รายละเอียดและคุณสมบัติบุคลากร

งานจัดจ้างบุคลากรหลักและสนับสนุน งานพัฒนาศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์

๑. ผู้ยื่นข้อเสนอต้องจัดหาบุคลากรผู้เชี่ยวชาญ จัดทำแนวทาง กระบวนการ และคู่มือการปฏิบัติงานที่เป็นมาตรฐาน รวมถึงการปรับปรุงพื้นที่ห้องศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังนี้

๑.๑ ผู้จัดการโครงการ จำนวน ๑ คน โดยมีภาระหน้าที่และคุณสมบัติดังต่อไปนี้

ภาระหน้าที่

๑) บริหารจัดการโครงการโดยรวมให้เป็นไปตามข้อกำหนดในสัญญา

๒) สรุปและรายงานผลการดำเนินงานเพื่อนำเสนอและส่งมอบงานในแต่ละงวดงาน

คุณสมบัติ

๑) ปริญญาโท วิศวกรรมศาสตร์ หรือวิทยาศาสตร์ หรือเทคโนโลยีสารสนเทศ หรือเทียบเท่า

๒) มีประสบการณ์การทำงาน อย่างน้อย ๒๐ ปี

๑.๒ ที่ปรึกษาด้านการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Management Consultant) จำนวน ๑ คน โดยมีภาระหน้าที่และคุณสมบัติดังต่อไปนี้

ภาระหน้าที่

๑) ให้คำปรึกษาด้านการออกแบบและจัดวางระบบรักษาความมั่นคงปลอดภัยไซเบอร์

๒) ให้คำปรึกษาด้านการออกแบบและจัดวางระบบเฝ้าระวังภัยคุกคามไซเบอร์

๓) ให้คำปรึกษาด้านการเฝ้าระวัง วิเคราะห์และแจ้งเตือนภัยคุกคามไซเบอร์

๔) ให้คำปรึกษาด้านการบริหารจัดการศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์สำนักงานปลัดกระทรวงแรงงานให้สอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และเป็นไปตามมาตรฐานสากล ISO/IEC 27001

คุณสมบัติ

๑) ปริญญาตรี วิศวกรรมศาสตร์ หรือวิทยาศาสตร์ หรือเทคโนโลยีสารสนเทศ หรือเทียบเท่า

๒) มีใบรับรอง (Certificate) CISM หรือ CISA หรือ CISSP หรือ GCCC หรือ CompTIA CASP+

๓) มีประสบการณ์การทำงาน อย่างน้อย ๑๕ ปี

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

๒. ผู้ยื่นข้อเสนอต้องจัดเตรียมบุคลากรที่มีความรู้ความสามารถเพื่อเข้าดำเนินการพัฒนากระบวนการทำงานในศูนย์ ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัย ไซเบอร์ พ.ศ.๒๕๖๒ และเป็นไปตามมาตรฐานสากล ISO/IEC 27001 จำนวน ๒ คน ดังต่อไปนี้

๒.๑ ผู้เชี่ยวชาญด้านมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001 จำนวน ๑ คน โดยมีภาระหน้าที่และคุณสมบัติดังต่อไปนี้

ภาระหน้าที่

๑) ออกแบบระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศสำหรับการปฏิบัติงานในศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์และโครงสร้างพื้นฐานที่สนับสนุน ให้แก่สำนักงานปลัดกระทรวงแรงงาน ให้สอดคล้องกับมาตรฐาน ISO/IEC 27001

๒) กำหนดแนวทางในการคัดเลือกทีมงานตรวจสอบภายในและดำเนินการตรวจสอบระบบ บริหารจัดการความมั่นคงปลอดภัยตามมาตรฐานสากล ISO/IEC 27001 ร่วมกับทีมงานตรวจสอบภายใน รวมทั้งพัฒนารายงานการตรวจสอบภายใน (Internal Audit) เพื่อให้ทราบถึงผลลัพธ์และเตรียมนำสู่การยื่นขอใบรับรองมาตรฐานสากล ISO/IEC 27001

๓) จัดทำรายงานเสนอผู้บริหารระดับสูงเพื่อพิจารณาเกี่ยวกับแผนและแนวทางการพัฒนาระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ

คุณสมบัติ

๑) ปริญญาตรี วิศวกรรมศาสตร์ หรือวิทยาศาสตร์ หรือเทคโนโลยีสารสนเทศ หรือเทียบเท่า

๒) มีประสบการณ์การทำงาน อย่างน้อย ๑๕ ปี

๓) ผ่านการฝึกอบรม IRCA ISO/IEC 27001 Lead Auditor หรือ CISA หรือเทียบเท่า

๒.๒ เจ้าหน้าที่ปฏิบัติงานด้านมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001 จำนวน ๑ คน โดยมีภาระหน้าที่และคุณสมบัติดังต่อไปนี้

ภาระหน้าที่

๑) ดำเนินการร่วมกับคณะทำงานในการจัดทำบัญชีรายการทรัพย์สิน (Asset Inventory) ตามขอบเขตที่กำหนดและร่วมดำเนินการในการพัฒนากระบวนการหรือระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ในการประเมินและวิเคราะห์ความเสี่ยงตามรายการทรัพย์สินที่จัดทำขึ้น

๒) จัดเตรียมแนวทางการนำระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศไปปฏิบัติเพื่อเป็นมาตรการป้องกันความเสี่ยงและแนวทางการถ่ายทอดความรู้ และแนวปฏิบัติที่ถูกต้อง

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ

๓) จัดเตรียมแนวทางในการเฝ้าระวังและทบทวนสำหรับการวัดผลของมาตรการควบคุมความเสี่ยงที่ใช้ควบคุมดูแลองค์กรรวมถึงความถี่ในการเฝ้าระวังต้องสอดคล้องกับความเสี่ยงเพื่อให้มั่นใจว่าหากเกิดเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย หน่วยงานสามารถมีกระบวนการรายงานผลได้ทันเวลา

๔) จัดเตรียมแนวทางในการรักษามาตรฐานและการพัฒนาปรับปรุงกระบวนการ เพื่อป้องกันปัญหาที่อาจเกิดขึ้นซ้ำซ้อนในอนาคตรวมถึงแนวทางในการปรับปรุงระบบบริหารจัดการ ด้านความมั่นคงปลอดภัยสารสนเทศให้มีประสิทธิภาพยิ่งขึ้นกว่าเดิม

๕) จัดเตรียมเอกสาร Statement of Applicability (SOA) ตาม Annex A ของ มาตรฐานสากล ISO/IEC27001 และตัวอย่างของมาตรการควบคุมความเสี่ยง เช่น นโยบาย ขั้นตอนการปฏิบัติ และแบบฟอร์มเพื่อบันทึกการทำงาน เป็นต้น เพื่อให้มีความถูกต้องและเป็นไปตามมาตรฐานสากล

คุณสมบัติ

๑) ปริญญาตรี วิศวกรรมศาสตร์ หรือวิทยาศาสตร์ หรือเทคโนโลยีสารสนเทศ หรือเทียบเท่า

๒) มีประสบการณ์การทำงาน อย่างน้อย ๕ ปี

๓) ผ่านการฝึกอบรม IRCA ISO/IEC 27001 Lead Auditor หรือ Implementing ISO/IEC 27001 ISMS หรือ ITIL หรือ CISA หรือ GCCC หรือ เทียบเท่า

๓. เจ้าหน้าที่สนับสนุนโครงการ จำนวน ๑ คน โดยมีภาระหน้าที่ และคุณสมบัติดังต่อไปนี้

ภาระหน้าที่

๑) สนับสนุนการทำงานของผู้จัดการโครงการ

๒) ติดต่อ ประสานงานกับทีมงานต่าง ๆ ที่เกี่ยวข้อง

๓) ติดตามงาน สรุปและรายงานผลการดำเนินงานเพื่อนำเสนอและส่งมอบงานในแต่ละงวดงาน

คุณสมบัติ

๑) ปริญญาตรี วิศวกรรมศาสตร์ หรือวิทยาศาสตร์ หรือเทคโนโลยีสารสนเทศ หรือเทียบเท่า

๒) มีประสบการณ์การทำงานติดตั้ง ปรับปรุง อุปกรณ์ ความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ อย่างน้อย ๓ ปี

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ภาคผนวก ข

รายละเอียดและคุณสมบัติบุคลากรเพื่อปฏิบัติงานในศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (Ministry Security Operation Center) ดังนี้

๑. ผู้ยื่นข้อเสนอต้องจัดเตรียมบุคลากรเพื่อปฏิบัติงานในศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (Ministry Security Operation Center) รายละเอียดดังนี้

๑.๑ ผู้จัดการศูนย์ปฏิบัติการ (SOC Manager) เข้าปฏิบัติหน้าที่ ในวันเวลาทำการอย่างน้อยสัปดาห์ละ ๒ วัน ตั้งแต่เวลา ๐๘.๓๐ น. – ๑๖.๓๐ น. จำนวน ๑ คน โดยมีภาระหน้าที่ และคุณสมบัติดังต่อไปนี้

ภาระหน้าที่

๑) ร่วมวางแผนออกแบบและพัฒนากระบวนการปฏิบัติงานในศูนย์ฯ และการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานปลัดกระทรวงแรงงาน

๒) จัดการดำเนินงานในแต่ละวันโดยรวม มีหน้าที่รับผิดชอบในการตรวจพบเหตุการณ์และ / หรือเหตุการณ์ที่เกิดขึ้นและตอบสนองต่อการปฏิบัติตามกระบวนการ ที่กำหนดไว้

๓) ดูแลและจัดการจัดตารางงานของทีม ให้มีประสิทธิภาพ

๔) ดูแลจัดการการทำงานและประเมิน ปรับปรุงการปฏิบัติงาน อย่างต่อเนื่อง

๕) ติดตามและอัปเดตข้อมูลของอุปกรณ์ที่ใช้ในศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อปรับปรุงและพัฒนาการใช้งานอย่างต่อเนื่อง

๖) จัดประชุมสรุปผลการดำเนินการแก้ไขเหตุการณ์ภัยคุกคามทางไซเบอร์ ประจำเดือน

คุณสมบัติ

๑) ปริญญาตรี วิศวกรรมศาสตร์ หรือวิทยาศาสตร์ หรือเทคโนโลยีสารสนเทศ หรือเทียบเท่า

๒) มีประสบการณ์การทำงานด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Cybersecurity) อย่างน้อย ๑๕ ปี

๓) มีใบรับรอง (Certificate) GMON หรือ CISSP หรือ CISM หรือ CISA

๑.๒ เจ้าหน้าที่วิเคราะห์ภัยคุกคามฯ ระบบ ระดับ ๑ (Cyber Security Analyst T1) เข้าปฏิบัติหน้าที่ในวันเวลาทำการ ตั้งแต่เวลา ๐๘.๓๐ น. – ๑๖.๓๐ น. จำนวน ๒ คน มีคุณสมบัติดังต่อไปนี้

ภาระหน้าที่

๑) ดำเนินการตรวจสอบวิเคราะห์และรายงานการแจ้งเตือนด้านความปลอดภัยและข้อมูลเหตุการณ์ในวันเวลาทำการ ตั้งแต่เวลา ๐๘.๓๐ น. – ๑๖.๓๐ น.

๒) ตรวจสอบและระบุเหตุการณ์ผิดปกติที่อุปกรณ์รักษาความปลอดภัยตรวจพบในเชิงบวกและจัดทำรายงาน

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ

๓) วิเคราะห์เหตุการณ์ภัยคุกคามทางไซเบอร์ที่ได้รับการแจ้งเตือนยืนยันความถูกต้องของเหตุการณ์ จัดลำดับความสำคัญของเหตุการณ์และบันทึกเหตุการณ์

๔) ทำการบันทึกการตรวจสอบและบันทึกกิจกรรมที่ไม่เหมาะสมหรือผิดกฎหมาย ซึ่งรวมถึงการตรวจสอบอุปกรณ์เครือข่าย เครื่องแม่ข่ายและเครื่องลูกข่าย เพื่อรายงานเหตุการณ์กับทางสำนักงานปลัดกระทรวงแรงงาน

๕) ให้คำแนะนำเบื้องต้นในการแก้ไขเหตุการณ์ภัยคุกคามทางไซเบอร์ หากไม่สามารถดำเนินการแก้ไขได้ด้วยตนเอง ต้องส่งต่อเหตุการณ์ไปยังเจ้าหน้าที่เฝ้าระวังภัยคุกคามทางไซเบอร์ระดับ ๒ (Tier 2)

๖) ทำรายงานสรุปรายวัน รายสัปดาห์และรายงานสรุปรายเดือนของภัยคุกคามและการวิเคราะห์เหตุการณ์ความปลอดภัย

คุณสมบัติ

๑) ปริญญาตรี วิศวกรรมศาสตร์ หรือวิทยาศาสตร์ หรือเทคโนโลยีสารสนเทศ หรือเทียบเท่า

๒) มีประสบการณ์การทำงานด้านเฝ้าระวังและวิเคราะห์ข้อมูลความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Security Operation Center) อย่างน้อย ๓ ปี

๓) มีใบรับรอง (Certificate) CompTIA Security+

๑.๓ เจ้าหน้าที่วิเคราะห์ภัยคุกคามฯ ระดับ 2 (Cyber Security Analyst T2) เข้าปฏิบัติหน้าที่เป็นรอบ ในวันเวลาทำการ ตั้งแต่เวลา ๐๘.๓๐ น. – ๑๖.๓๐ น. จำนวน ๒ คน โดยมีภาระหน้าที่ และคุณสมบัติดังต่อไปนี้

ภาระหน้าที่

๑) วิเคราะห์การเหตุการณ์ความปลอดภัยคอมพิวเตอร์ที่ได้การประสานจาก เจ้าหน้าที่เฝ้าระวังภัยคุกคามทางไซเบอร์ระดับ ๑ (Tier 1) เพื่อตอบสนองและการสนับสนุนการตรวจจับภัยคุกคามที่เกิดขึ้น

๒) ให้คำแนะนำในการแก้ไขปัญหา และดำเนินการร่วมกับเจ้าหน้าที่สำนักงานปลัดกระทรวงแรงงานในการแก้ไขเหตุการณ์ภัยคุกคามทางไซเบอร์

คุณสมบัติ

๑) ปริญญาตรี วิศวกรรมศาสตร์ หรือวิทยาศาสตร์ หรือเทคโนโลยีสารสนเทศ หรือเทียบเท่า

๒) มีประสบการณ์การทำงานติดตั้ง ปรับปรุง หรือเฝ้าระวังและวิเคราะห์ข้อมูลความมั่นคงปลอดภัยระบบเทคโนโลยี สารสนเทศ (Security Operation Center) อย่างน้อย ๕ ปี

๓) มีใบรับรอง (Certificate) ระดับ Professional ของผลิตภัณฑ์ที่นำเสนอมาในโครงการ หรือ CompTIA Security+ และ CompTIA CySA+

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ภาคผนวก ค

รายละเอียดคุณลักษณะเฉพาะทางเทคนิค (Technical Specification)

งานจัดหาครุภัณฑ์ โครงการศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์

๑. งานห้องศูนย์ปฏิบัติการและประสานงานกลางด้านความมั่นคงปลอดภัยไซเบอร์ พร้อมระบบคอมพิวเตอร์และซอฟต์แวร์

ผู้ยื่นข้อเสนอต้องจะต้องเสนออุปกรณ์ และทำการปรับปรุงห้องศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ในพื้นที่ที่สำนักงานปลัดกระทรวงแรงงานจัดเตรียมไว้ โดยมีรายละเอียดดังนี้

๑.๑ อุปกรณ์และระบบพื้นฐานที่จำเป็นสำหรับเจ้าหน้าที่ศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ จะต้องประกอบด้วยอุปกรณ์อย่างน้อย ดังนี้

๑.๑.๑ อุปกรณ์กล้องโทรทัศน์วงจรปิดชนิดเครือข่าย แบบมุมมองคงที่สำหรับติดตั้งภายในสำนักงาน จำนวน 4 ชุด โดยมีคุณสมบัติอย่างน้อยเทียบเท่าหรือดีกว่า ดังต่อไปนี้

๑.๑.๑.๑ มีความละเอียดของภาพสูงสุดไม่น้อยกว่า 1,920 x 1,080 pixel หรือไม่น้อยกว่า 2,073,600 pixel

๑.๑.๑.๒ มี frame rate ไม่น้อยกว่า 30 ภาพต่อวินาที (frame per second)

๑.๑.๑.๓ ใช้เทคโนโลยี Infrared (IR) สำหรับการแสดงภาพในกรณีที่มีค่าความเข้มของแสง 0 LUX ได้

๑.๑.๑.๔ มีขนาดตัวรับภาพ (Image Sensor) ไม่น้อยกว่า 1/2.8 นิ้ว 2 MP

๑.๑.๑.๕ สามารถตรวจจับความเคลื่อนไหวอัตโนมัติ (Motion Detection) ได้

๑.๑.๑.๖ สามารถแสดงรายละเอียดของภาพที่มีความแตกต่างของแสงมาก (Wide Dynamic Range หรือ Super Dynamic Range หรือ Digital Wide Dynamic Range) ได้

๑.๑.๑.๗ สามารถส่งสัญญาณภาพ (Streaming) ไปแสดงได้อย่างน้อย 2 แหล่ง

๑.๑.๑.๘ สามารถส่งสัญญาณภาพได้ตามมาตรฐาน H.264 เป็นอย่างน้อย

๑.๑.๑.๙ สามารถใช้งานตามโปรโตคอล (Protocol) IPv4 ได้เป็นอย่างน้อย

๑.๑.๑.๑๐ มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100 Base-T หรือดีกว่า และสามารถทำงานได้ตามมาตรฐาน IEEE 802.3af หรือ IEEE 802.3at (Power over Ethernet) ในช่องเดียวกันได้

๑.๑.๑.๑๑ ตัวกล้องได้มาตรฐาน IP66 หรือติดตั้งอุปกรณ์เพิ่มเติมสำหรับหุ้มกล้อง (Housing) ที่ได้มาตรฐาน IP66 เป็นอย่างน้อย

๑.๑.๑.๑๒ สามารถทำงานได้ที่อุณหภูมิ -10 °C ถึง 50 °C เป็นอย่างน้อย

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ	ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ	ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ	ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ	ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการและเลขานุการ	

๑.๑.๑.๑๓สามารถใช้งานกับมาตรฐาน HTTP, “NTP หรือ SNTP”, RTSP ได้เป็นอย่างน้อย

๑.๑.๒ อุปกรณ์บันทึกภาพผ่านเครือข่าย (Network Video Recorder) แบบ 8 ช่อง จำนวน 1 ชุด โดยมีคุณสมบัติอย่างน้อยเทียบเท่าหรือดีกว่า ดังต่อไปนี้

๑.๑.๒.๑ เป็นอุปกรณ์ที่ผลิตมาเพื่อบันทึกภาพจากกล้องโทรทัศน์วงจรปิดโดยเฉพาะ

๑.๑.๒.๒ สามารถบันทึกและบีบอัดภาพได้ตามมาตรฐาน MPEG4 หรือ H.264 หรือดีกว่า

๑.๑.๒.๓ มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 1 ช่อง

๑.๑.๒.๔ สามารถทำงานได้ตามมาตรฐาน IEEE 802.3af หรือ IEEE 802.3at (Power over Ethernet) ในช่องเดียวกันได้ จำนวนไม่น้อยกว่า 8 ช่อง

๑.๑.๒.๕ สามารถบันทึกภาพและส่งภาพเพื่อแสดงผลที่ความละเอียดของภาพสูงสุดไม่น้อยกว่า 1,920 x 1,080 pixel หรือไม่น้อยกว่า 2,073,600 pixel

๑.๑.๒.๖ สามารถใช้งานกับมาตรฐาน “HTTP หรือ HTTPS”, SMTP, “NTP หรือ SNTP”, SNMP, RTSP ได้เป็นอย่างน้อย

๑.๑.๒.๗ มีหน่วยจัดเก็บข้อมูลสำหรับกล้องวงจรปิดโดยเฉพาะ (Surveillance Hard Disk) ชนิด SATA ขนาดความจุรวมไม่น้อยกว่า 8 TB

๑.๑.๒.๘ มีช่องเชื่อมต่อ (Interface) แบบ USB จำนวนไม่น้อยกว่า 1 ช่อง

๑.๑.๒.๙ สามารถใช้งานตามโปรโตคอล (Protocol) IPv4 และ IPv6 ได้

๑.๑.๒.๑๐ สามารถแสดงภาพที่บันทึกจากกล้องโทรทัศน์วงจรปิดผ่านระบบเครือข่ายได้

๑.๑.๓ ระบบการบริหารจัดการ การเข้า-ออกประตู พร้อมเครื่องบันทึก 1 ระบบ โดยมีคุณสมบัติอย่างน้อยเทียบเท่าหรือดีกว่า ดังต่อไปนี้

๑.๑.๓.๑ ระบบจะประกอบไปด้วยเครื่องตรวจจับใบหน้า 2 เครื่อง มีคุณสมบัติดังนี้

๑.๑.๓.๑.๑ ตัวอุปกรณ์ มีกล้องอย่างน้อย 2 MP

๑.๑.๓.๑.๒ ตัวอุปกรณ์สามารถวิเคราะห์ใบหน้าโดยไม่สามารถหลอกโดยใช้รูป หรือ วีดีโอ จากอุปกรณ์ต่างๆ ได้ (Face anti-spoofing)

๑.๑.๓.๑.๓ การตรวจจับใบหน้า และสามารถวิเคราะห์ใบหน้าได้โดยใช้เวลาไม่เกิน 0.2 s

๑.๑.๓.๑.๔ สามารถเพิ่มฐานข้อมูลใบหน้าได้ไม่ต่ำกว่า 50,000 ใบหน้า

๑.๑.๓.๑.๕ มีความแม่นยำในการตัวจับใบหน้า (Accuracy) สูงสุด 99%

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

๑.๑.๓.๑.๖ อุปกรณ์ต้องสามารถพัฒนาโปรแกรมต่อได้โดยมี ISAPI หรือ API หรือ SDK ให้เพื่อเชื่อมต่อกับระบบได้

๑.๑.๓.๑.๗ มี Network standard Ethernet port 10/100M อย่างน้อย1 ช่อง

๑.๑.๓.๑.๘ อุปกรณ์รองรับการส่งข้อมูลแบบ USB จำนวน 1 ช่อง, Wiegand จำนวน 1 ช่อง, RS485 จำนวน 1 ช่อง ได้เป็นอย่างน้อย

๑.๑.๓.๑.๙ อุปกรณ์ได้มาตรฐาน IP54 เป็นอย่างน้อย

๑.๑.๓.๑.๑๐ Magnetic Lock แรงดึงไม่น้อยกว่า 250 Kg 2 ชุด

๑.๑.๓.๒ Power Supply พร้อม Battery สำรองไฟขนาด 12 Volt และ Buzzer พร้อมกล่องสำหรับติดตั้งเหนือประตู 1 ชุด

๑.๑.๓.๓ Emergency Break glass สีเขียว 1 กล่อง

๑.๑.๔ จอแสดงผลภาพแบบวิดีโอวอล (Video Wall) จำนวน 4 จอ โดยมีคุณสมบัติอย่างน้อยเทียบเท่าหรือดีกว่า ดังต่อไปนี้

๑.๑.๔.๑ จอภาพผลมีขนาดไม่น้อยกว่า 54 นิ้ว (วัดตามแนวเส้นทแยงมุม)

๑.๑.๔.๒ จอภาพมีสัดส่วนภาพด้านกว้างต่อด้านยาว 16:9

๑.๑.๔.๓ แสดงผลภาพด้วยความละเอียด 1920 x 1080 Pixel

๑.๑.๔.๔ จอภาพมีขอบต่อชนกันขนาด Bezel to Bezel ไม่มากกว่า 3.5 mm

๑.๑.๔.๕ ความสว่างของจอภาพ (Brightness) ไม่น้อยกว่า 500 cd/m²(typ.)

๑.๑.๔.๖ มีช่องสัญญาณขาเข้า (Input) อย่างน้อย ดังนี้

๑.๑.๔.๖.๑ ช่องสัญญาณ HDMI 2.0 ไม่น้อยกว่า 2 ช่อง

๑.๑.๔.๖.๒ ช่องสัญญาณ DP ไม่น้อยกว่า 1 ช่อง

๑.๑.๔.๖.๓ ช่องสัญญาณ LAN ไม่น้อยกว่า 1 ช่อง

๑.๑.๔.๖.๔ ช่องสัญญาณ RS232 ไม่น้อยกว่า 1 ช่อง

๑.๑.๔.๖.๕ ช่องสัญญาณ IR ไม่น้อยกว่า 1 ช่อง

๑.๑.๔.๗ มีช่องต่อสัญญาณขาออก (Output)ในตัวเครื่อง ดังนี้

๑.๑.๔.๗.๑ ช่องสัญญาณ DP ไม่น้อยกว่า 1 ช่อง

๑.๑.๔.๗.๒ ช่องสัญญาณ RS232 ไม่น้อยกว่า 1 ช่อง

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

๑.๑.๔.๘ จอภาพสามารถรับสัญญาณเพื่อแสดงภาพได้ที่ความละเอียด 1920 x 1080 หรือ/และ 3840 x 2160 ได้เป็นอย่างน้อย

๑.๑.๕ ตู้ควบคุมและจัดการจอแสดงภาพแบบวิดีโอวอล (VideoWall Controller) จำนวน 1 ชุด โดยมีคุณสมบัติอย่างน้อยเทียบเท่าหรือดีกว่า ดังต่อไปนี้

๑.๑.๕.๑ ชุดควบคุมเป็นแบบ Pure-Hardware FPGA

๑.๑.๕.๒ มีช่องสัญญาณเข้าชนิด HDMI แบบ FullHD ไม่น้อยกว่า 8 ช่อง

๑.๑.๕.๓ มีช่องสัญญาณออกชนิด HDMI แบบ FullHD ไม่น้อยกว่า 8 ช่อง

๑.๑.๕.๔ รองรับการเปิดอย่างน้อย 4 windows ในแต่ละหน้าจอ

๑.๑.๕.๕ สามารถซ้อนทับภาพ,ขยายขนาด เข้า-ออกภาพ หรือ สลับหน้าต่างหลายภาพ และ/หรือ Picture in Picture หรือ Full Screen อย่างใดอย่างหนึ่ง

๑.๑.๕.๖ สามารถปรับแต่งความละเอียดสัญญาณออก (EDID) ตามความละเอียดทางกายภาพของระบบแสดงผลได้

๑.๑.๕.๗ สามารถสลับภาพแบบไร้รอยต่อ

๑.๑.๖ จอแสดงผลภาพสำหรับสื่อสาร ประชุมหรืออบรม จำนวน 1 จอ โดยมีคุณสมบัติอย่างน้อยเทียบเท่าหรือดีกว่า ดังต่อไปนี้

๑.๑.๖.๑ เป็นจอที่สร้างมาใช้งานแบบ Interactive ในลักษณะ Whiteboard ที่สามารถ วาด/เขียน/ลบ ด้วยการสัมผัสหรือใช้ปากกาได้

๑.๑.๖.๒ สามารถ รับ/ส่งการแชร์ภาพจากอุปกรณ์ต่างๆ ได้

๑.๑.๖.๓ เป็นจอแสดงผลชนิดใช้ Backlight แบบ LED ขนาด 65 นิ้ว

๑.๑.๖.๔ ความละเอียดของการแสดงผล (Resolution) ไม่น้อยกว่า 3,840 x 2,160 จุดหรือ 4K

๑.๑.๖.๕ ความสว่างของจอภาพ (Brightness) ไม่น้อยกว่า 350nits (cd/m²)

๑.๑.๖.๖ มีระบบปฏิบัติการภายในตัวเครื่องแบบ OS Android version 8.0 หรือสูงกว่า

๑.๑.๖.๗ มีช่องต่อสัญญาณขาเข้า แบบ HDMI จำนวน 2 ports เป็นอย่างน้อย และ ช่องต่อสัญญาณเข้า LAN จำนวน 1 port

๑.๑.๖.๘ มีช่องต่อสัญญาณออก Output แบบ HDMI จำนวน 1 ports เป็นอย่างน้อย

๑.๑.๖.๙ มี Touch Pen ไม่น้อยกว่า 2 อัน

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

๑.๑.๗ เครื่องคอมพิวเตอร์ตั้งโต๊ะและจอแสดงภาพขนาด 21.5 นิ้ว สำหรับงานวิเคราะห์และตอบสนองภัยคุกคามชั้นสูง จำนวน 5 ชุด โดยมีคุณสมบัติอย่างน้อยเทียบเท่าหรือดีกว่า ดังต่อไปนี้

๑.๑.๗.๑ มีหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า 10 แกนหลัก (10 core) และ 20 แกนเสมือน (20 Thread) โดยมีความเร็วสัญญาณนาฬิกาสูงสุด ไม่น้อยกว่า 4.3 GHz จำนวน 1 หน่วย

๑.๑.๗.๒ หน่วยประมวลผลกลาง (CPU) มีหน่วยความจำแบบ Cache Memory รวมในระดับ (Level) เดียวกัน ขนาดไม่น้อยกว่า 8 MB

๑.๑.๗.๓ มีหน่วยประมวลผลเพื่อแสดงภาพ โดยมีคุณลักษณะอย่างใดอย่างหนึ่ง หรือดีกว่า ดังนี้

๑) เป็นแผงวงจรเพื่อแสดงภาพแยกจากแผงวงจรหลักที่มีหน่วยความจำขนาดไม่น้อยกว่า 2 GB หรือ

๒) มีหน่วยประมวลผลเพื่อแสดงภาพติดตั้งอยู่ภายในหน่วยประมวลผลกลาง แบบ Graphics Processing Unit ที่สามารถใช้หน่วยความจำหลักในการแสดงภาพขนาดไม่น้อยกว่า 2 GB หรือ

๓) มีหน่วยประมวลผลเพื่อแสดงภาพที่มีความสามารถในการใช้หน่วยความจำหลักในการแสดงภาพ

๑.๑.๗.๔ มีหน่วยความจำหลัก (RAM) ชนิด DDR4 หรือดีกว่า มีขนาดไม่น้อยกว่า 16 GB

๑.๑.๗.๕ มีหน่วยจัดเก็บข้อมูล ชนิด SATA หรือดีกว่า ขนาดความจุไม่น้อยกว่า 2 TB หรือ ชนิด Solid State Drive ขนาดความจุไม่น้อยกว่า 480 GB จำนวน 1 หน่วย

๑.๑.๗.๖ มีช่องเชื่อมต่อ (Interface) แบบ USB 2.0 หรือดีกว่า ไม่น้อยกว่า 3 ช่อง

๑.๑.๗.๗ มีช่องเชื่อมต่อแบบ HDMI จำนวน 1 ช่อง

๑.๑.๗.๘ มีแป้นพิมพ์และเมาส์

๑.๑.๗.๙ มีซอฟท์แวร์ลิขสิทธิ์ระบบปฏิบัติการ Window 11 Pro

๑.๑.๗.๑๐ จอแสดงภาพขนาดไม่น้อยกว่า 21.5 นิ้ว

๑) รองรับความละเอียดการแสดงผลไม่น้อยกว่า 1,920 x 1,080 Pixel

๒) มี Refresh Rate ไม่น้อยกว่า 60 Hz

๓) มี Contrast Ratio ไม่น้อยกว่า 600 : 1

๑.๑.๘ จอแสดงภาพขนาดไม่น้อยกว่า 21.5 นิ้ว สำหรับเจ้าหน้าที่ปฏิบัติงาน จำนวน 5 จอ โดยมีคุณสมบัติอย่างน้อยเทียบเท่าหรือดีกว่า ดังต่อไปนี้

๑.๑.๘.๑ มีขนาดไม่น้อยกว่า 21.5 นิ้ว

๑.๑.๘.๒ รองรับความละเอียดการแสดงผลไม่น้อยกว่า 1,920 x 1,080 Pixel

๑.๑.๘.๓ มี Refresh Rate ไม่น้อยกว่า 60 Hz

๑.๑.๘.๔ มี Contrast Ratio ไม่น้อยกว่า 600 : 1

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

๑.๑.๙ เครื่องปรับอากาศขนาด 24,000 BTU พร้อมติดตั้ง จำนวน 2 ชุด โดยมีคุณสมบัติอย่างน้อยเทียบเท่าหรือดีกว่า ดังต่อไปนี้

๑.๑.๙.๑ ต้องเป็นระบบทำความเย็นแบบ Inverter

๑.๑.๙.๒ ต้องเป็นเครื่องปรับอากาศที่ประกอบสำเร็จรูปทั้งชุด ทั้งหน่วยส่งความเย็น และหน่วยระบายความร้อนต้องเป็นยี่ห้อเดียวกัน

๑.๑.๙.๓ สามารถใช้กับระบบไฟฟ้า 1 เฟส 220 โวลต์ 50 เฮิร์ท หรือ 3 เฟส 380 โวลต์ 50 เฮิร์ท ได้

๑.๑.๑๐ เครื่องสำรองไฟฟ้า ขนาด 10 kVA (ระบบไฟฟ้า 3 เฟส) จำนวน 1 ชุด โดยมีคุณสมบัติอย่างน้อยเทียบเท่าหรือดีกว่า ดังต่อไปนี้

๑.๑.๑๐.๑ มีกำลังไฟฟ้าขาออก (Output) ไม่น้อยกว่า 10 kVA (8,000 Watts)

๑.๑.๑๐.๒ มีช่วงแรงดันไฟฟ้า Input (VAC) แบบ 3 เฟส ไม่น้อยกว่า 380 +/-20%

๑.๑.๑๐.๓ มีช่วงแรงดันไฟฟ้า Output (VAC) ไม่มากกว่า 220 +/-1%

๑.๑.๑๐.๔ สามารถสำรองไฟฟ้าที่ Full Load ได้ไม่น้อยกว่า 10 นาที

๑.๑.๑๑ เครื่องพิมพ์ Multifunction เลเซอร์หรือ LED สี จำนวน 1 ชุด โดยมีคุณสมบัติอย่างน้อยเทียบเท่าหรือดีกว่า ดังต่อไปนี้

๑.๑.๑๑.๑ เป็นอุปกรณ์ที่มีความสามารถเป็น Printer, Copier และ Scanner ภายในเครื่องเดียวกัน

๑.๑.๑๑.๒ มีความละเอียดในการพิมพ์ไม่น้อยกว่า 600 x 600 dpi

๑.๑.๑๑.๓ มีความเร็วในการพิมพ์ขาวดำสำหรับกระดาษ A4 ไม่น้อยกว่า 20 หน้าต่อนาที (ppm)

๑.๑.๑๑.๔ มีความเร็วในการพิมพ์สีสำหรับกระดาษ A4 ไม่น้อยกว่า 20 หน้าต่อนาที (ppm)

๑.๑.๑๑.๕ มีหน่วยความจำ (Memory) ขนาดไม่น้อยกว่า 256 MB

๑.๑.๑๑.๖ สามารถสแกนเอกสาร ขนาด A4 (ขาวดำ และ สี) ได้

๑.๑.๑๑.๗ มีความละเอียดในการสแกนสูงสุด ไม่น้อยกว่า 1,200 x 1,200 dpi

๑.๑.๑๑.๘ สามารถถ่ายสำเนาเอกสารได้ทั้งสีและขาวดำ

๑.๑.๑๑.๙ สามารถทำสำเนาได้สูงสุดไม่น้อยกว่า 99 สำเนา

๑.๑.๑๑.๑๐ มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100 Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 1 ช่อง หรือ สามารถใช้งานผ่านเครือข่ายไร้สาย Wi-Fi (IEEE 802.11b, g, n) ได้

๑.๑.๑๑.๑๑ มีถาดใส่กระดาษได้รวมกันไม่น้อยกว่า 250 แผ่น

๑.๑.๑๑.๑๒ สามารถใช้ได้กับ A4, Letter, Legal และสามารถกำหนดขนาดของกระดาษเองได้

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

๑.๑.๑๒ เครื่องทำลายเอกสาร จำนวน 1 ชุด โดยมีคุณสมบัติอย่างน้อยเทียบเท่าหรือดีกว่า ดังต่อไปนี้

๑.๑.๑๒.๑ จำนวนเอกสารที่สามารถทำลายได้ 8 - 10 แผ่น/ครั้ง (A4)

๑.๑.๑๒.๒ ขนาดของเอกสารหลังการทำลาย 4 x 28 มม.หรือ เล็กกว่า

๑.๑.๑๒.๓ ระบบถอยหลังอัตโนมัติเมื่อกระดาษติด (Auto Reverse หรือ Antijam Techology)

๑.๑.๑๒.๔ ถังจุกระดาษไม่น้อยกว่า 20 ลิตร

๑.๑.๑๓ ตู้จัดเก็บเอนกประสงค์ จำนวน 1 ตู้ โดยมีคุณสมบัติอย่างน้อยเทียบเท่าหรือดีกว่า ดังต่อไปนี้

๑.๑.๑๓.๑ ขนาดไม่น้อยกว่า 9 ช่อง

๑.๑.๑๓.๒ ชนิดบานเปิดทึบประตูเดียว พร้อมกุญแจแบบแยกล็อก

๑.๑.๑๓.๓ มีมาตรฐานการผลิตที่ได้รับการยอมรับในระดับสากล

๑.๑.๑๔ ปรับปรุงพื้นที่

๑.๑.๑๔.๑ ผู้ยื่นข้อเสนอต้องปรับปรุงพื้นที่ห้องทำงาน (Control Room)

๑.๑.๑๔.๒ ผู้ยื่นข้อเสนอต้องจัดหาและติดตั้งติดตั้งฝ้าเพดานตกแต่ง พร้อมทำสี

๑.๑.๑๔.๓ ผู้ยื่นข้อเสนอต้องจัดหาและติดตั้งประตูกระจกชนิดเทมเปอร์ แบบสไลด์ จำนวน 1 ประตู

๑.๑.๑๕ อุปกรณ์สำนักงาน

๑.๑.๑๕.๑ ผู้ยื่นข้อเสนอต้องจัดหาโต๊ะทำงาน จำนวน 5 ชุด (แยกเป็นอุปกรณ์สำนักงาน)

๑.๑.๑๕.๒ ผู้ยื่นข้อเสนอต้องจัดหาเก้าอี้สำหรับเจ้าหน้าที่ จำนวน 5 ชุด

๑.๑.๑๕.๓ ผู้ยื่นข้อเสนอต้องจัดหาโต๊ะประชุมรองรับสำหรับ 5 ที่นั่ง พร้อมเก้าอี้สำนักงาน

๑.๑.๑๕.๔ กระดาษและหมึกปริ้นท์ อย่างละ 1 ชุด (และรองรับเครื่องปริ้น)

๑.๑.๑๕.๕ ปากกา สีไฮไลท์ 1 ชุด

๑.๑.๑๕.๖ กระดานไวท์บอร์ด และปากกาเขียนกระดานไวท์บอร์ด 1 ชุด

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

๒. ระบบตรวจจับภัยคุกคามทางไซเบอร์และประเมินความเสี่ยงระบบสารสนเทศ

๒.๑ ระบบป้องกัน ตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์ และระบบเครือข่าย (End-Point Protection and Network Protection) จำนวน 1 ระบบ ประกอบด้วย

๒.๑.๑ อุปกรณ์ตรวจจับและป้องกันการโจมตีระบบเครือข่าย (Intrusion Prevention System) จำนวน 2 ชุด โดยมีคุณสมบัติอย่างน้อยเทียบเท่าหรือดีกว่า ดังต่อไปนี้

๒.๑.๑.๑ เป็นอุปกรณ์ทำหน้าที่ป้องกันการบุกรุกและการโจมตี โดยอุปกรณ์ที่เสนอต้องถูกออกแบบมาเป็น IPS โดยเฉพาะ ไม่เป็นลักษณะ UTM (Unified Threat Management)

๒.๑.๑.๒ มี IPS Inspection Throughput ไม่น้อยกว่า 3 Gbps และสามารถรองรับการอัพเกรดเป็น 5 Gbps ได้โดยใช้อุปกรณ์เดิม หรือสามารถนำเสนออุปกรณ์รุ่นที่สูงกว่าได้

๒.๑.๑.๓ ต้องรองรับ Concurrent Session ได้ไม่น้อยกว่า 30,000,000 Concurrent Session และไม่น้อยกว่า 400,000 New Connection per Second

๒.๑.๑.๔ มี Interface 1 Gigabit Ethernet แบบ UTP จำนวนไม่น้อยกว่า 8 พอร์ต ทำงานได้อย่างน้อย 4 segments และ มี Interface 10 Gigabit Fiber แบบ SR จำนวนไม่น้อยกว่า 4 พอร์ต ทำงานได้อย่างน้อย 2 segments

๒.๑.๑.๕ สามารถทำ Hardware Bypass ได้ด้วยตัวอุปกรณ์เองในกรณี Hardware/Software เกิดปัญหารวมถึงกรณีไฟฟ้าดับ โดยสามารถเลือก Fail-open หรือ Fail-Close ในแต่ละ segment ได้ ในกรณีที่อุปกรณ์ที่เสนอไม่สามารถทำ Hardware Bypass ได้ด้วยตัวเอง สามารถเสนออุปกรณ์อื่นเพื่อช่วยในการ Bypass ได้

๒.๑.๑.๖ สามารถป้องกันการโจมตีจาก Worms, Viruses, Trojans, Phishing, Spyware, DDoS/DoS, Backdoors, Vulnerabilities, Protocol/Packet anomaly และ Statistical anomalies หรือ Application anomaly ได้

๒.๑.๑.๗ สามารถทำงานในลักษณะ Rate-Limit และ Block Unwanted traffic เช่น Peer-to-Peer และ Instant Messaging ได้

๒.๑.๑.๘ สามารถทำ SSL Inspection ได้ทั้งขาเข้าและขาออก โดยมี Throughput สำหรับ SSL Only Traffic (2k key) สูงสุดไม่น้อยกว่า 3.5 Gbps หรือสามารถเสนออุปกรณ์ SSL Inspection เพิ่มเติมเพื่อให้รองรับตามข้อกำหนดได้

๒.๑.๑.๙ มี Automatic policy tuning หรือ Recommendation มาจาก research lab ของเจ้าของผลิตภัณฑ์หรืออุปกรณ์เพื่อปรับ policy IPS ให้ทันสมัยและเหมาะสมกับการโจมตีต่างๆ

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ

ในช่วงแต่ละสัปดาห์ หรือ นำเสนอบริการแนะนำในการปรับแต่ง policy IPS จากเจ้าของผลิตภัณฑ์เพื่อให้ได้รับ policy ที่ทันสมัยตามข้อกำหนดได้

๒.๑.๑.๑๐ สามารถกำหนด Action ในการจัดการการบุกรุกได้อย่างน้อย ดังนี้ Block, Permit, Log, Alert

๒.๑.๑.๑๑ สามารถรองรับการทำงานในลักษณะ Active-Active หรือ Active-Standby High Availability ได้

๒.๑.๑.๑๒ สามารถทำงานใน Network แบบ Symmetric และ Asymmetric ได้

๒.๑.๑.๑๓ สามารถรองรับการตรวจจับการบุกรุกบน IPv6 ได้

๒.๑.๑.๑๔ มี Dual Power Supplies เพื่อรองรับในกรณีที่ Power Supply ตัวใดตัวหนึ่งไม่สามารถทำงานได้

๒.๑.๑.๑๕ สามารถบริหารการจัดการแบบ On-Box Web-based Management หรือ Command Line Interface

๒.๑.๑.๑๖ ได้รับการรับรองมาตรฐาน CSA, UL, IEC, EN เป็นอย่างน้อย

๒.๑.๑.๑๗ ผลิตภัณฑ์ที่นำเสนอต้องมีหน่วยงานเฉพาะที่ทำหน้าที่ในการติดตามความเคลื่อนไหวในวงการผู้รุกราน (Threat Researcher หรือเทียบเท่า) เพื่อจะได้สามารถปรับปรุงฐานข้อมูล ระบบ Threat Intelligence ในการรุกรานระบบได้อย่างต่อเนื่อง และสามารถ Update ผ่าน Internet ได้เมื่อมีการปรับปรุงฐานข้อมูลการรุกรานระบบ

๒.๑.๑.๑๘ ผลิตภัณฑ์ที่นำเสนอต้องได้รับการจัดอันดับให้อยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant ในกลุ่มผลิตภัณฑ์ Intrusion Detection and Prevention System โดยเป็นรายงานของปี 2018 หรือใหม่กว่า

๒.๑.๑.๑๙ ต้องรับประกันอีก 2 ปี หลังจากมีการตรวจรับพัสดุ

๒.๑.๒ อุปกรณ์บริหารจัดการอุปกรณ์ตรวจจับป้องกันภัยคุกคามบนระบบเครือข่าย (Network Sensor) จำนวน 1 ชุด โดยมีคุณสมบัติอย่างน้อยเทียบเท่าหรือดีกว่า ดังต่อไปนี้

๒.๑.๒.๑ อุปกรณ์ที่เสนอต้องรองรับการบริหารจัดการ IPS ได้อย่างน้อย 10 อุปกรณ์เพื่อรองรับการขยายในอนาคต

๒.๑.๒.๒ สามารถทำ Discovering, Monitoring, Configuring, Diagnosing และ Reporting ได้

๒.๑.๒.๓ สามารถสร้างและกำหนด Policies ต่างๆ ไปยังอุปกรณ์ หลายตัวในระบบได้

๒.๑.๒.๔ สามารถกำหนดให้ Download และปรับปรุง Filter/signature ไปยังอุปกรณ์ IPS ได้โดยอัตโนมัติ

๒.๑.๒.๕ อุปกรณ์ต้องสามารถทำ Automatic reporting และ Customize Report ได้

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ

๒.๑.๒.๖ มีหน่วยเก็บข้อมูลในรูปแบบของ HDD หรือ SSD (RAID1 หรือดีกว่า) และสามารถเก็บข้อมูลย้อนหลังได้ไม่น้อยกว่า 200 ล้านเหตุการณ์ หรือมีความจุไม่น้อยกว่า 2TB

๒.๑.๒.๗ มี Dual Power Supplies เพื่อรองรับในกรณีที่ Power Supply ตัวใดตัวหนึ่งไม่สามารถทำงานได้

๒.๑.๒.๘ ต้องรับประกันอีก 2 ปี หลังจากมีการตรวจรับพัสดุ

๒.๑.๓ Agent Software สำหรับป้องกันและตรวจจับภัยคุกคามในระดับเครื่องผู้ใช้งาน (Endpoint Sensor) จำนวนไม่น้อยกว่า 1,800 ลิขสิทธิ์ โดยมีคุณสมบัติอย่างน้อยเทียบเท่าหรือดีกว่า ดังต่อไปนี้

๒.๑.๓.๑ เป็นระบบรักษาความปลอดภัยที่สามารถทำงานบนระบบปฏิบัติการ Windows 8.1, Windows 10, Windows 11 และ MacOS 11 ได้เป็นอย่างน้อย

๒.๑.๓.๒ ต้องมีระบบบริหารจัดการเป็นแบบ Software as a Service (SaaS) หรือ Cloud Delivered หรือ Cloud Based ที่มี Web-Based Management เพื่อใช้ในการบริหารจัดการเครื่องลูกข่าย

๒.๑.๓.๓ มีความสามารถในการตรวจสอบมัลแวร์ (Malware) แบบอ้างอิงจากฐานข้อมูล (Signature) และแบบวิเคราะห์พฤติกรรม (Heuristic Technology) ได้อย่างน้อย ดังนี้

๒.๑.๓.๓.๑ Virtual Patching หรือ Intrusion Prevention (HIPS) หรือ Attack Surface Reduction หรือ Exploit Preventions

๒.๑.๓.๓.๒ Behavior Monitoring

๒.๑.๓.๓.๓ Machine Learning

๒.๑.๓.๔ รองรับ Ransomware Protection

๒.๑.๓.๕ สามารถป้องกันช่องโหว่ทางเครือข่ายของระบบปฏิบัติการ โดยที่ไม่จำเป็นต้องทำการติดตั้ง Patches บนระบบปฏิบัติการเหล่านั้นจริง (Virtual Patch) เพื่อป้องกันปัญหาที่อาจเกิดขึ้นจากการ Patches ได้ หรือ ทำ Exploit Protection ได้

๒.๑.๓.๖ ความสามารถในการกำหนดสิทธิ์การใช้งาน เช่น Full Access, Read, Read and Execute, Modify หรือ List Content ให้กับอุปกรณ์ USB Storage devices ได้ และสามารถอนุญาตให้ใช้งาน USB Storage ได้เป็นรายยี่ห้อ (Vendor ID) และ Serial Number ที่มีการลงทะเบียนในระบบเท่านั้น หรือเทียบเท่า

๒.๑.๓.๗ มีความสามารถในการป้องกันข้อมูลสำคัญขององค์กรไม่ให้รั่วไหลออกไปภายนอกองค์กร (Data loss prevention) ผ่านทาง FTP หรือ Network Share, HTTP หรือ Browser, Web Mail, Printer, Windows Clipboard, และ Removable Storage ได้ โดยใช้เงื่อนไข

ลงชื่อ ..... ประธานกรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการและเลขานุการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ

อย่างน้อยดังนี้ File Attributes, Keywords และ Regular Expressions หรือเสนอระบบเพิ่มเติมเพื่อให้คุณสมบัติดังกล่าว

๒.๑.๓.๘ สามารถทำการป้องกันโปรแกรมประยุกต์ที่ไม่ได้รับอนุญาต (Lockdown, Block และ Allow) และไม่ต้องการให้ติดตั้งบนเครื่องคอมพิวเตอร์ลูกข่ายได้ (Application Control) และสามารถกำหนด Rule โดยใช้เงื่อนไขต่าง ๆ ได้ หรือเสนอระบบอื่นเพิ่มเติมเพื่อให้สามารถทำ Application Control ได้

๒.๑.๓.๙ สามารถกำหนดนโยบายการอัพเดทให้เครื่องคอมพิวเตอร์ลูกข่ายที่ถูกกำหนดให้ทำหน้าที่แจกจ่าย Pattern ให้แก่เครื่องอื่น ๆ ในองค์กรได้ (Update Agent) หรือกำหนดนโยบายการอัพเดต agent ได้

๒.๑.๓.๑๐ สามารถออกรายงานการทำงานในรูปแบบ PDF หรือ CSV หรือ JSON ได้

๒.๑.๓.๑๑ ผลิตภัณฑ์ที่นำเสนอต้องได้รับการจัดอันดับให้อยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant ในกลุ่มผลิตภัณฑ์ Endpoint Protection Platforms ปี 2023 หรือใหม่กว่า และ ได้รับการจัดอันดับให้อยู่ในกลุ่ม Leader ของ Forrester Wave Endpoint Security ปี 2023 หรือใหม่กว่า

๒.๑.๓.๑๒ ต้องรับประกันอีก 2 ปี หลังจากมีการตรวจรับพัสดุ

๒.๑.๔ Agent Software สำหรับป้องกันและตรวจจับภัยคุกคามในระดับเครื่องแม่ข่าย จำนวนอย่างน้อย 260 ลิขสิทธิ์ โดยมีคุณสมบัติอย่างน้อยเทียบเท่าหรือดีกว่า ดังต่อไปนี้

๒.๑.๔.๑ เป็น Agent Software สำหรับรักษาความปลอดภัยที่สามารถทำงานบนระบบปฏิบัติการ Microsoft Windows Server 2008 R2, Microsoft Windows Server 2012, 2016, 2019 รวมถึงรองรับระบบปฏิบัติการอื่นๆ อาทิ เช่น Debian Linux 8, RedHat Enterprise Linux 6, 7, Ubuntu Linux (LTS), SUSE Enterprise Linux 11, 12 ได้เป็นอย่างน้อย

๒.๑.๔.๒ สามารถเชื่อมต่อกับ VMware vCenter หรือ AWS และ Microsoft Azure เพื่อค้นหา (discover) workload ที่ทำงานอยู่ได้

๒.๑.๔.๓ สามารถทำ agent self-protection เพื่อป้องกัน local user จากการ tampering agent เช่น uninstall และแก้ไขตัว agent ได้

๒.๑.๔.๔ มีความสามารถตรวจสอบ malware ด้วยเทคโนโลยี machine learning, behavior monitor เพื่อป้องกัน malware ที่เกิดใหม่ได้

๒.๑.๔.๕ รองรับ Ransomware protection ได้

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ

๒.๑.๔.๖ มีความสามารถในการป้องกัน malware และ ภัยคุกคามทางเว็ป ต่างๆ ด้วยเทคโนโลยี Reputation หรือระบบ Cloud ของเจ้าของผลิตภัณฑ์ได้ เพื่อเพิ่มประสิทธิภาพในการป้องกัน และตรวจจับ

๒.๑.๔.๗ มีความสามารถในการทำ Stateful Firewall ในลักษณะของ Host-based Firewall ที่สามารถตั้งนโยบายความปลอดภัยให้กับระบบปฏิบัติการแต่ละเครื่องได้โดยใช้นโยบายที่แตกต่างกัน

๒.๑.๔.๘ มีความสามารถในการป้องกันช่องโหว่ของระบบปฏิบัติการได้ โดยที่ไม่จำเป็นต้องทำการติดตั้ง patches หรือซอฟต์แวร์ใดๆ บนระบบปฏิบัติการเหล่านั้นจริง เพื่อป้องกันปัญหาที่อาจเกิดขึ้นจากการ patches โดยที่ยังไม่ได้ทำการทดสอบกับการใช้งานจริง

๒.๑.๔.๙ สามารถสแกนเครื่องคอมพิวเตอร์เพื่อหา vulnerable software แล้วจัดหาการตั้งค่า recommended security ที่เหมาะสมให้ หรือนำเสนอ vulnerability assessment tool ที่มีลิขสิทธิ์การทำงานถูกต้องตลอดอายุสัญญาเพื่อตรวจหา vulnerable software บนเครื่องคอมพิวเตอร์ปลายทางโดยต้องมีการอัพเดทฐานข้อมูลให้มีความทันสมัยตลอดอายุการใช้งานได้

๒.๑.๔.๑๐ มีความสามารถในการป้องกันการโจมตีในระดับ Application-Layer อาทิเช่น SQL injection และ cross-site script หรือสามารถเสนอ Web Application Firewall ที่มี throughput ไม่ต่ำกว่า 4 Gbps ได้ เพื่อรองรับการใช้งานของสำนักงานปลัดกระทรวงแรงงาน

๒.๑.๔.๑๑ สามารถถอดรหัส traffic ประเภท SSL/TLS บนระบบปฏิบัติการ Windows และ Linux ได้เพื่อป้องกันการโจมตีผ่านช่องโหว่ หรือนำเสนออุปกรณ์ SSL Decryption ที่มี throughput ไม่น้อยกว่า 4 Gbps ได้ เพื่อรองรับการใช้งานของสำนักงานปลัดกระทรวงแรงงาน

๒.๑.๔.๑๒ สามารถตรวจจับและป้องกันช่องโหว่ประเภท zero-day vulnerabilities ได้ โดยรวมถึง exploits ประเภทต่างๆ ด้วย

๒.๑.๔.๑๓ ระบบจะต้องทำการเฝ้าระวังการเปลี่ยนแปลง Files และ Registry ในระบบเสมือนได้เป็นอย่างน้อย

๒.๑.๔.๑๔ สามารถทำ Application Control เพื่อควบคุมการทำงานแอพพลิเคชั่นแปลกปลอมบนระบบปฏิบัติการณ์ Windows และ Linux ได้ หรือเสนอระบบอื่นเพิ่มเติม

๒.๑.๔.๑๕ สามารถวิเคราะห์ log file ของระบบปฏิบัติการณ์และแอพพลิเคชั่นต่างๆ หรือ user activity และ process monitoring และแจ้งเตือนถึงเหตุการณ์น่าสงสัย (suspicious

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ

activity) หรือเหตุการณ์เกี่ยวกับความปลอดภัยของระบบที่ใช้งานได้ หรือนำเสนอระบบจัดเก็บ Log สำหรับเครื่องแม่ข่ายเพิ่มเติม

๒.๑.๔.๑๖ สามารถทำ Device Control เพื่อควบคุมการใช้งาน external storage device บนแพลตฟอร์ม Windows ได้เป็นอย่างน้อย

๒.๑.๔.๑๗ สามารถออกรายงานการทำงานในรูปแบบ PDF หรือ CSV ได้

๒.๑.๔.๑๘ ต้องรับประกันอีก 2 ปี หลังจากมีการตรวจรับพัสดุ

๒.๑.๕ อุปกรณ์ตรวจจับภัยคุกคามขั้นสูงทางไซเบอร์บนระบบเครือข่าย จำนวน 1 ชุด โดยมีคุณสมบัติอย่างน้อยเทียบเท่าหรือดีกว่า ดังต่อไปนี้

๒.๑.๕.๑ เป็นระบบตรวจจับ ค้นหา แจ้งเตือน และรายงานอันตรายจากภัยคุกคามขั้นสูงในระบบเครือข่ายให้กับผู้ดูแลระบบได้

๒.๑.๕.๒ สามารถเชื่อมต่อกับระบบเครือข่ายสื่อสารข้อมูลของกระทรวงแรงงานได้ โดยรองรับ Interface 10 Gbps ไม่น้อยกว่า 4 Port และรองรับการวิเคราะห์ปริมาณการ รับ-ส่งข้อมูลได้ไม่น้อยกว่า 4 Gbps

๒.๑.๕.๓ สามารถรับข้อมูลจากระบบเครือข่ายสื่อสารข้อมูลของกระทรวงแรงงานได้ ด้วยวิธี Mirror Port หรือ Tap/Span ได้ และรองรับ Protocol CIFS/SMB, SMTP, HTTP ได้เป็นอย่างน้อย

๒.๑.๕.๔ สามารถวิเคราะห์พฤติกรรมของไฟล์ด้วย Virtual Analyzer หรือ Sandbox ได้ภายในตัวอุปกรณ์ โดยรองรับไฟล์ตระกูล Executables และ Microsoft Office เป็นอย่างน้อย และสามารถ Custom sandbox หรือสามารถ configure os และ application support เพื่อเพิ่มประสิทธิภาพในการตรวจจับให้สูงขึ้น ได้ หรือเสนออุปกรณ์เพิ่มเติม เพื่อให้ได้ความสามารถดังกล่าว โดยต้องสามารถวิเคราะห์ไฟล์ด้วยวิธี Sandbox ได้ไม่น้อยกว่า 6,000 ไฟล์ต่อวัน หรือวิเคราะห์พร้อมกัน 30 ไฟล์

๒.๑.๕.๕ สามารถทำ Network Analytics ด้วย Machine Learning เพื่อทำ Threat Correlation ในการโจมตี โดยเก็บรวบรวมข้อมูลย้อนหลังได้อย่างน้อย 6 เดือน หรือเก็บข้อมูลได้ย้อนหลังสำหรับการสืบค้นไม่น้อยกว่า 10TB

๒.๑.๕.๖ สามารถทำงานค้นหาร่องรอยการโจมตี (Sweeping / Hunting) จากข้อมูลที่บันทึก โดยมี Threat Intelligence จากเจ้าของผลิตภัณฑ์เองหรือสามารถเพิ่มแหล่งข้อมูลจาก STIX File หรือ TAXII Feeds ได้

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ

๒.๑.๕.๗ สามารถทำงานร่วมกับ agent software สำหรับป้องกันและตรวจจับภัยคุกคามในระดับเครื่องผู้ใช้งานในโครงการได้ โดยสามารถกำหนดให้ระบบส่งค่า Threat Intelligence เช่น File Hash และ IP ไปยัง agent software ดังกล่าวได้หรือเสนอระบบเพิ่มเติมเพื่อให้ได้ความสามารถดังกล่าว

๒.๑.๕.๘ ผลิตภัณฑ์ที่เสนอต้องได้รับการจัดอันดับให้อยู่ในกลุ่ม Leader ของ The Forrester Wave ในกลุ่มผลิตภัณฑ์ Network Analysis and Visibility ปี 2023 หรือใหม่กว่า

๒.๑.๕.๙ ต้องรับประกันอีก 2 ปี หลังจากมีการตรวจรับพัสดุ

๒.๑.๖ ระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามทางไซเบอร์ (Extended Detection and Response) จำนวน 1 ชุด โดยมีคุณสมบัติอย่างน้อยเทียบเท่าหรือดีกว่า ดังต่อไปนี้

๒.๑.๖.๑ สามารถตรวจจับและโต้ตอบต่อภัยคุกคามข้ามเลเยอร์ เพื่อการค้นหาและวิเคราะห์ภัยคุกคามที่มาจากหลายทิศทางแบบเชิงลึก (Extended Detection and Response; XDR)

๒.๑.๖.๒ สามารถทำงานโดยการแลกเปลี่ยนข้อมูลร่วมกับ Agent Software สำหรับป้องกันและตรวจจับภัยคุกคามในระดับเครื่องผู้ใช้งาน (Client) และเครื่องแม่ข่าย (Server) และอุปกรณ์ตรวจจับและป้องกันการโจมตีระบบเครือข่าย (Intrusion Prevention System) หรือ อุปกรณ์ตรวจจับ, วิเคราะห์และเฝ้าระวังภัยคุกคามบนระบบเครือข่าย (Network Sensor) ในโครงการได้ หรือเสนอระบบหรืออุปกรณ์เพิ่มเติมเพื่อให้สามารถเฝ้าระวังและตอบสนองต่อภัยคุกคามทั้งในระดับเครื่องลูกข่าย เครื่องแม่ข่าย และเครือข่ายได้

๒.๑.๖.๓ สามารถเก็บบันทึกรายละเอียดกิจกรรมของเครื่องแม่ข่ายและเครื่องลูกข่าย ได้แก่ Endpoint Name, IP address หรือข้อมูลเกี่ยวกับ Network, URL หรือ Browser ได้เป็นอย่างน้อย

๒.๑.๖.๔ สามารถทำการเก็บข้อมูลหลักฐานต่าง ๆ ของเครื่องคอมพิวเตอร์ (Telemetry หรือ Forensic Analysis) เพื่อตรวจสอบเหตุการณ์การทำงานของมัลแวร์ (malware) ย้อนหลังได้ไม่น้อยกว่า 90 วัน โดยมีการเก็บข้อมูลไว้บนบริการที่ได้รับมาตรฐาน ISO 27001 เป็นอย่างน้อย

๒.๑.๖.๕ สามารถดูการกระทำของภัยคุกคามที่เกิดขึ้นบนเครือข่าย เช่น Command and Control ได้

๒.๑.๖.๖ สามารถส่งคำสั่ง เช่น Isolate Endpoint, Remote Shell หรือ Real-Time Response หรือ Live Investigation, Collect File หรือ Delete File และ Add to Block List เพื่อตอบสนองต่อภัยคุกคามได้

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ

๒.๑.๖.๗ สามารถใช้ในการตอบสนองภัยคุกคามที่เกิดขึ้นแบบอัตโนมัติ (Security Playbooks) เพื่อลดภาระงานของผู้ดูแลระบบ โดยจะต้องมี Pre-defined Templates มาให้ และสามารถ Customize เพิ่มเติมได้

๒.๑.๖.๘ สามารถรวบรวมภัยคุกคามได้จากแหล่งข้อมูลภายในของเจ้าของผลิตภัณฑ์ และจากแหล่งข้อมูลภายนอก เช่น STIX file, CSV file และ TAXII Feeds เพื่อค้นหาการโจมตีที่เกิดขึ้นในองค์กรได้

๒.๑.๖.๙ มีหน้าจอแสดงการจัดลำดับความสำคัญและแจ้งเตือน เพื่อเพิ่มความสามารถในการมองเห็น ได้แก่ ดูรายละเอียดการดำเนินการเพิ่มเติม (Execution Profile), ระบุขอบเขตของผลกระทบ (Identify the Scope of Impact) และดำเนินการโต้ตอบ (Response Actions)

๒.๑.๖.๑๐ มี Public API เพื่อรองรับการทำงานร่วมกับ SIEM และ SOAR ได้

๒.๑.๖.๑๑ ระบบตรวจจับและโต้ตอบต่อภัยคุกคามข้ามเลเยอร์ (Extended Detection and Response) ที่เสนอจะต้องมีลิขสิทธิ์การใช้ร่วมกับระบบต่างๆ ดังนี้

๒.๑.๖.๑๑.๑ มีลิขสิทธิ์ถูกต้องสำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องลูกข่ายที่เสนอในโครงการ

๒.๑.๖.๑๑.๒ มีลิขสิทธิ์สำหรับอุปกรณ์เครือข่าย โดยมี Network Throughput รวมไม่น้อยกว่า 10 Gbps

๒.๑.๖.๑๒ เจ้าของผลิตภัณฑ์ต้องได้รับการจัดอันดับให้อยู่ในกลุ่ม Leader ของ The Forrester Wave ในกลุ่มผลิตภัณฑ์ Endpoint Detection and Response Providers ปี 2022 หรือใหม่กว่า

๒.๑.๖.๑๓ ต้องรับประกันอีก 2 ปี หลังจากมีการตรวจรับพัสดุ

๒.๑.๗ บริการผู้เชี่ยวชาญสำหรับค้นหาภัยคุกคามเชิงรุกและตอบสนองต่อภัยคุกคามอัตโนมัติ จำนวน 1 ระบบ โดยมีคุณสมบัติอย่างน้อยเทียบเท่าหรือดีกว่า ดังต่อไปนี้ (SOC as a service)

๒.๑.๗.๑ สามารถทำการตรวจจับภัยคุกคามเชิกรุก (Threat Hunting) ที่เสนอในโครงการได้ โดยจะต้องครอบคลุมทั้งในส่วนของ Endpoint, Server โดยจะต้องเป็นผู้เชี่ยวชาญมาให้บริการจากเจ้าของผลิตภัณฑ์ ที่นำเสนอ

๒.๑.๗.๒ สามารถทำการตรวจสอบ (Monitoring), เชื่อมโยงข้อมูล (Correlation) และจัดลำดับความสำคัญ (Prioritization) การแจ้งเตือนที่เกิดขึ้นได้ และสามารถทำการค้นหาสิ่ง

ลงชื่อ ..... ประธานกรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการและเลขานุการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ

ผิดปกติจากหลักฐานเชื่อมโยงที่มีอยู่ (Indicators of compromise) และหลักฐานจากรูปแบบการโจมตี (Indicators of attack) โดยอัตโนมัติ

๒.๑.๗.๓ สามารถทำการวิเคราะห์เชิงลึกที่ครอบคลุม (Comprehensive Analysis) โดยจัดทำแผนการตอบสนองต่อเหตุการณ์ที่เกิดขึ้นแบบละเอียด

๒.๑.๗.๔ สามารถทำ Threat Hunting ได้ และเชื่อมโยงข้อมูลที่เกี่ยวข้อง Threat Intelligence ได้ทั้งจากที่มาจากเจ้าของผลิตภัณฑ์ หรือ Government Agencies หรือ Third party เช่น TAXII feed, MISP feed

๒.๑.๗.๕ สามารถตรวจสอบและแจ้งเตือนเหตุการณ์โจมตีที่สำคัญผ่านทางโทรศัพท์หรือช่องทางที่กำหนดได้ตลอด 24/7 และช่วยวิเคราะห์ความเป็นไปได้ของแหล่งที่มาของการโจมตี (Initial compromise identification)

๒.๑.๗.๖ สามารถทำการค้นหาหลักฐานบ่งชี้ว่าถูกโจมตี (Indicator of compromise) ตาม Threat intelligence ที่สำคัญและแจ้งเตือนรายละเอียดหากตรวจพบ

๒.๑.๗.๗ สามารถบริหารจัดการ Case ที่เกิดขึ้นได้ โดยจะมีการวิเคราะห์, แจ้งเตือน แนะนำวิธีการแก้ไข และทำการปิด Case พร้อมระบุรายละเอียดเพิ่มเติมให้สำหรับ Case ที่เกิดขึ้น (Case Management) หรือมีช่องทางการสื่อสารกับนักวิเคราะห์ได้

๒.๑.๗.๘ สามารถออกแผนการตอบสนองต่อเหตุการณ์ภัยคุกคาม แบบ step-by-step เพื่อแก้ไขเหตุการณ์ที่เกิดขึ้น

๒.๑.๗.๙ สามารถออกรายงานประจำเดือน เพื่อสรุปเหตุการณ์ที่เกิดขึ้นทั้งหมดและให้คำแนะนำเพื่อปรับปรุงประสิทธิภาพในการป้องกันและตรวจสอบในช่วงที่ผ่านมา โดยรายงานทั้งหมดจะต้องมีอีเมล์แจ้งเตือนไปยังผู้ที่เกี่ยวข้องได้

๒.๑.๘ ระบบตรวจประเมินความเสี่ยงความมั่นคงปลอดภัยไซเบอร์เพื่อค้นหาช่องโหว่และความเสี่ยงที่อาจเกิดขึ้นสำหรับระบบเครือข่าย, เครื่องแม่ข่าย และเว็บแอพพลิเคชั่น จำนวน 1 ชุด ประกอบด้วย

๒.๑.๘.๑ ระบบบริหารจัดการความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Attack Surface Risk Management) จำนวน 1 ระบบ โดยมีคุณสมบัติอย่างน้อยเทียบเท่าหรือดีกว่าดังต่อไปนี้

๒.๑.๘.๑.๑ สามารถแสดงค่าความเสี่ยงขององค์กร (Risk Insight หรือ Risk Index) ในลักษณะของตัวเลขที่คำนวณหาค่าความเสี่ยงจากองค์ประกอบได้

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ

๒.๑.๘.๑.๒ ต้องสามารถค้นหาช่องทางที่มีความเสี่ยงจากภายในองค์กรและความเสี่ยงจากภายนอกองค์กร (Attack Surface Discovery) ไม่ว่าจะเป็น Devices, Internet-Facing Assets, Accounts (Identities) และ Cloud Apps ได้ หรือเสนอระบบอื่นเพิ่มเติมเพื่อคุณสมบัติดังกล่าว

๒.๑.๘.๑.๓ สามารถตรวจประเมินความเสี่ยงเครื่องแม่ข่ายและอุปกรณ์เครือข่ายภายในได้ไม่น้อยกว่า 4000 หมายเลขไอพี หรือ Asset

๒.๑.๘.๑.๔ สามารถตรวจประเมินความเสี่ยง Internet Facing Assets ได้ไม่จำกัดจำนวนไอพีแอดเดรสหรือเว็ปไซต์ไม่น้อยกว่า 10 โดเมน ด้วยวิธีการตรวจสอบ certificates, ports และ vulnerabilities

๒.๑.๘.๑.๕ สามารถนำข้อมูลจากต้นทาง (Data Source) จากเจ้าของผลิตภัณฑ์ และจากผลิตภัณฑ์อื่นๆ (3rd party) เช่น Azure AD, Active Directory (on-premises) หรือ Office 365 มาคำนวณค่าความเสี่ยง (Risk indicator) เพิ่มเติมได้หรือทำ Identity Protection ได้

๒.๑.๘.๑.๖ สามารถค้นหาและตรวจสอบช่องโหว่ของระบบปฏิบัติการ (OS) และ Application ของเครื่องลูกข่ายภายในองค์กรได้

๒.๑.๘.๑.๗ ระบบต้องมีความสามารถในการแนะนำแนวทางการแก้ไข ปรับปรุง เพื่อลดความเสี่ยงต่อภัยคุกคามขององค์กรได้ (Risk Reduction Measures)

๒.๑.๘.๑.๘ ต้องรับประกันอีก 2 ปี หลังจากมีการตรวจรับพัสดุ

๒.๒ ระบบเครื่องคอมพิวเตอร์แม่ข่ายพร้อมซอฟต์แวร์บริหารจัดการ และอุปกรณ์กระจายสัญญาณ จำนวน 1 ระบบ ประกอบด้วย

๒.๒.๑ เครื่องคอมพิวเตอร์แม่ข่าย พร้อมชุดซอฟต์แวร์ระบบแม่ข่ายคอมพิวเตอร์เสมือน จำนวน 2 ชุด โดยมีคุณสมบัติอย่างน้อยเทียบเท่าหรือดีกว่า ดังนี้

๒.๒.๑.๑ มีหน่วยประมวลผลกลาง (CPU) แบบ 16 แกนหลัก (16 core) หรือดีกว่า สำหรับคอมพิวเตอร์แม่ข่าย (Server) โดยเฉพาะและมีความเร็วสัญญาณนาฬิกาพื้นฐานไม่น้อยกว่า 2.8 GHz จำนวน 1 หน่วย

๒.๒.๑.๒ มีหน่วยความจำหลัก (RAM) ชนิด DDR4 หรือดีกว่า ขนาดไม่น้อยกว่า 64 GB

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ

๒.๒.๑.๓ มีหน่วยจัดเก็บข้อมูล (Hard Drive) ชนิด SATA หรือ SCSI หรือ SAS ที่มีความเร็วรอบไม่น้อยกว่า 10,000 รอบต่อนาที หรือ ชนิด Solid State Drive หรือดีกว่า และมีความจุรวมหลังทำ RAID ไม่น้อยกว่า 2 TB

๒.๒.๑.๔ ลิขสิทธิ์ของซอฟต์แวร์ระบบแม่ข่ายคอมพิวเตอร์เสมือนที่นำเสนอต้องเป็นซอฟต์แวร์ที่มีสิทธิการใช้งานแบบ Open License ที่สามารถย้ายลิขสิทธิ์ไปใช้งานกับ Server อื่นได้ โดยมีลิขสิทธิ์ถูกต้องตามจำนวน Processor Core รวมไม่น้อยกว่า 16 Cores

๒.๒.๒ อุปกรณ์กระจายสัญญาณ (Switch) 2 ชุด สำหรับใช้เชื่อมต่อภายในระบบตรวจจับภัยคุกคามทางไซเบอร์และประเมินความเสี่ยงระบบสารสนเทศ โดยมีคุณสมบัติอย่างน้อยเทียบเท่าหรือดีกว่า ดังนี้

๒.๒.๒.๑ เป็นอุปกรณ์ Ethernet Switch ที่ทำงานเป็น Layer 3 Switch

๒.๒.๒.๒ อุปกรณ์ต้องมี Packet Switching Capacity ไม่น้อยกว่า 250 Gbps และมี Forwarding Rate ไม่น้อยกว่า 190 Mpps

๒.๒.๒.๓ อุปกรณ์ต้องมีพอร์ทสำหรับเชื่อมต่อ อย่างน้อยดังต่อไปนี้

๒.๒.๒.๓.๑ พอร์ทความเร็ว 10/100/1000BASE-T ไม่น้อยกว่า 48 พอร์ท

๒.๒.๒.๓.๒ พอร์ทความเร็ว 1/10 Gbps แบบ Fiber (SFP/SFP+) ไม่น้อยกว่า 4 พอร์ท

๒.๒.๒.๔ มีหน่วยความจำ DRAM ขนาดไม่น้อยกว่า 2 GB และ Flash Memory หรือดีกว่าขนาดไม่น้อยกว่า 2 GB

๒.๒.๒.๕ มีพอร์ท Ethernet Management แบบ Fiber (SFP) หรือ 10/100/1000 BaseT (RJ45) จำนวนอย่างน้อย 1 พอร์ท

๒.๒.๒.๖ สามารถทำ Stacking หรือ Clustering พร้อมเสนอโมดูลสำหรับการทำ Stacking หรือ Clustering โดยให้เสนอสาย Stack มาให้พร้อมรองรับการทำ Stacking

๒.๒.๒.๗ รองรับจำนวน MAC Address รวมไม่น้อยกว่า 32,000 MAC Address

๒.๒.๒.๘ สามารถทำ Jumbo Frame ขนาดไม่น้อยกว่า 9,000 bytes

๒.๒.๒.๙ ต้องรองรับจำนวน VLAN ได้ไม่น้อยกว่า 4,090 VLAN

๒.๒.๒.๑๐ สามารถทำ Configuration Rollback ได้

๒.๒.๒.๑๑ ผลิตภัณฑ์ที่นำเสนอต้องได้รับการจัดอันดับให้อยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant ในกลุ่มผลิตภัณฑ์ Wired and Wireless Lan ในปี 2021 หรือใหม่กว่า

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

๒.๒.๓ อุปกรณ์กระจายสัญญาณ ขนาด 24 ช่อง จำนวน 1 ชุด โดยมีคุณสมบัติอย่างน้อยเทียบเท่าหรือดีกว่า ดังนี้

๒.๒.๓.๑ อุปกรณ์กระจายสัญญาณที่ทำงานเป็น Layer 2 และ Layer 3 Switch

๒.๒.๓.๒ อุปกรณ์ต้องมีพอร์ทสำหรับเชื่อมต่อ อย่างน้อยดังต่อไปนี้

๒.๒.๓.๒.๑ พอร์ทความเร็ว 10/100/1000BASE-T ไม่น้อยกว่า 24 พอร์ท

๒.๒.๓.๒.๒ พอร์ทความเร็ว 1/10 Gbps แบบ Fiber (SFP) ไม่น้อยกว่า 4 พอร์ท

๒.๒.๓.๓ อุปกรณ์ต้องมี Packet Switching Capacity ไม่น้อยกว่า 128 Gbps และมี Forwarding Rate ไม่น้อยกว่า 95 Mpps

๒.๒.๓.๔ มีหน่วยความจำ DRAM ขนาดไม่น้อยกว่า 2 GB และ Flash Memory หรือดีกว่าขนาดไม่น้อยกว่า 2 GB

๒.๒.๓.๕ ต้องรองรับจำนวน MAC Address รวมไม่น้อยกว่า 16,000 MAC Address

๒.๒.๓.๖ ต้องรองรับจำนวน VLAN ได้ไม่น้อยกว่า 4,090 VLAN

๒.๒.๓.๗ สามารถทำ Configuration Rollback ได้

๒.๒.๓.๘ ผลิตภัณฑ์ที่นำเสนอต้องได้รับการจัดอันดับให้อยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant ในกลุ่มผลิตภัณฑ์ Wired and Wireless Lan ในปี 2021 หรือใหม่กว่า

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

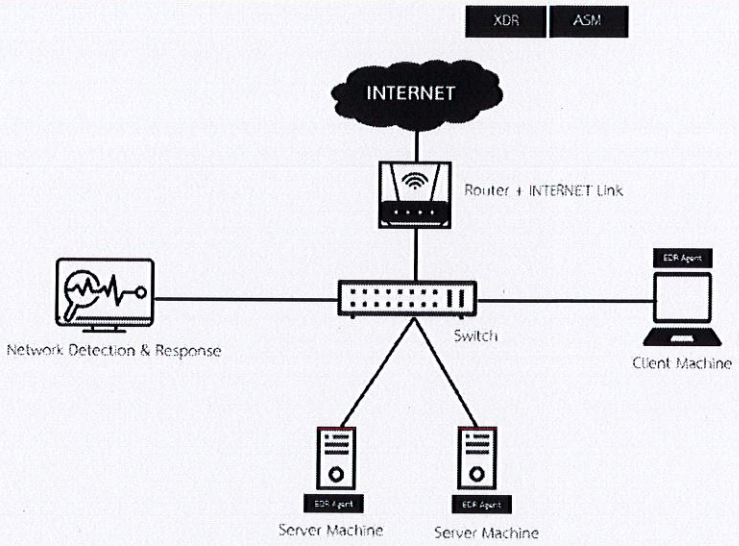
ภาคผนวก ง

เกณฑ์คุณภาพและคุณสมบัติที่เป็นประโยชน์ต่อทางราชการ

รายละเอียดการสาธิตการทดสอบ Proof of Concept (POC)

ผู้ยื่นข้อเสนอที่เข้าร่วมการทดสอบ POC ต้องมีความพร้อมในการดำเนินการทดสอบ POC โดยสำนักงานปลัดกระทรวงแรงงานกำหนดรายละเอียดการทดสอบ POC โดยมีรายละเอียดดังนี้

๑. **Logical Diagram**



รูปที่ 1 Logical Diagram สำหรับการทดสอบ

ผู้ยื่นข้อเสนอที่เข้าร่วมการทดสอบ POC จะต้องจัดเตรียมอุปกรณ์ พร้อมทั้งลิขสิทธิ์การใช้งานที่จะใช้ในการทดสอบเพื่อใช้ในการทดสอบตาม Logical Diagram อย่างน้อยดังนี้

๑. เครื่องคอมพิวเตอร์แม่ข่าย สำหรับติดตั้ง Software ที่ทำหน้าที่เป็น Web Server หรืออื่นๆ ตามเงื่อนไขการทดสอบ

๒. เครื่องคอมพิวเตอร์แม่ข่ายระบบปฏิบัติการวินโดว์สำหรับติดตั้งซอฟต์แวร์ EDR เพื่อจำลองเป็นเครื่องคอมพิวเตอร์แม่ข่ายของสำนักงานปลัดกระทรวงแรงงาน จำนวน ๒ เครื่อง สามารถนำมาเป็น Hardware หรือติดตั้งแบบ Virtual Machine

๓. เครื่องคอมพิวเตอร์ลูกข่ายสำหรับติดตั้งซอฟต์แวร์ EDR เพื่อจำลองเป็นเครื่องคอมพิวเตอร์ผู้ใช้งาน สามารถนำมาเป็น Hardware หรือติดตั้งแบบ Virtual Machine

๔. อุปกรณ์กระจายสัญญาณ (L2 Switch) ที่มีจำนวนพียงพอต่อการนำเสนอระบบ POC ของบริษัทผู้เข้าร่วมการทดสอบ POC

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ

๕. อุปกรณ์เพื่อใช้เชื่อมต่ออินเตอร์เน็ต

๖. อุปกรณ์อื่นๆ สนับสนุนการทดสอบและจัดส่งรายงาน

อุปกรณ์ต่าง ๆ ข้างต้นนี้ เป็นเพียงรายการอุปกรณ์เบื้องต้นเท่านั้น ผู้ยื่นข้อเสนอที่เข้าร่วมการทดสอบ POC สามารถปรับเปลี่ยนเพิ่มเติมรายการและจำนวนได้ตามความเหมาะสม

๒. ข้อกำหนดทั่วไปในการสาธิตการทดสอบ

๒.๑ ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอครบถ้วน ถูกต้อง และผ่านเกณฑ์คุณสมบัติตามที่สำนักงานปลัดกระทรวงแรงงานกำหนดไว้ในประกาศและเอกสารประกวดราคาอิเล็กทรอนิกส์เท่านั้นที่จะมีสิทธิ์เข้าทำการสาธิตการทดสอบระบบ

๒.๒ สำนักงานปลัดกระทรวงแรงงานจะกำหนดวันประชุมชี้แจงการสาธิตการทดสอบระบบ รวมทั้งกำหนดการและสถานที่ทำการสาธิตการทดสอบระบบ โดยสำนักงานปลัดกระทรวงแรงงานจะดำเนินการทดสอบให้แล้วเสร็จภายใน 5 วันทำการนับถัดจากวันยื่นข้อเสนอในระบบการจัดซื้อจัดจ้างภาครัฐ กรมบัญชีกลาง

๒.๓ ผู้ยื่นข้อเสนอที่เข้าร่วมการทดสอบ POC จะต้องส่งผู้แทนเข้าร่วมประชุมชี้แจงการสาธิตการทดสอบระบบตามวันเวลาและสถานที่ที่สำนักงานปลัดกระทรวงแรงงานกำหนด เพื่อรับทราบรายละเอียดการทดสอบ ขั้นตอนการทดสอบ ตลอดจนกำหนดการต่าง ๆ รวมทั้งสถานที่ทดสอบและรายละเอียดการเตรียมการด้านสถานที่และสิ่งอำนวยความสะดวกที่สำนักงานปลัดกระทรวงแรงงานจัดเตรียมไว้ โดยคณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์ จะชี้แจงรายละเอียด และตอบข้อซักถามเพื่อความเข้าใจโดยเท่าเทียมกัน

๒.๔ ผู้ยื่นข้อเสนอที่เข้าร่วมการทดสอบ POC ต้องดำเนินการส่งรายการอุปกรณ์และติดตั้งอุปกรณ์ในวันเวลาตามรายละเอียดที่กำหนดใน ตารางที่ ๒ แผนการทดสอบ POC โดยรายละเอียดในตารางที่ ๒ นี้ เป็นเพียงรายละเอียดเบื้องต้น คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์ สามารถปรับเปลี่ยนหรือเปลี่ยนแปลงได้ตามความเหมาะสม

๒.๕ การสาธิตการทดสอบระบบจะดำเนินการภายใต้การกำกับดูแลของคณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์ และตลอดระยะเวลาการสาธิตการทดสอบระบบ บุคลากรที่เข้าร่วมทุกคนต้องฝากอุปกรณ์สื่อสารและอุปกรณ์อิเล็กทรอนิกส์อื่น ๆ ไว้กับคณะกรรมการฯ หรือเจ้าหน้าที่เพื่อเก็บรักษาไว้จนกว่าจะเสร็จสิ้นการสาธิตการทดสอบระบบ

๒.๖ ห้ามมิให้บุคคลของผู้ยื่นข้อเสนอที่เข้าร่วมการทดสอบ POC คนหนึ่งคนใดออกจากห้องหรือพื้นที่การทดสอบโดยไม่ได้รับอนุญาต มิฉะนั้นจะถูกตัดสิทธิ์การกลับเข้าห้องหรือพื้นที่การทดสอบนั้นทันที กรณีมีความจำเป็นต้อง

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ขออนุญาตต่อคณะกรรมการฯ เพื่อพิจารณาอนุญาตออกนอกพื้นที่ และต้องอยู่ภายใต้การกำกับของกรรมการฯ หรือเจ้าหน้าที่ของสำนักงานปลัดกระทรวงแรงงานจนกว่าจะเสร็จสิ้นความจำเป็นและกลับเข้าพื้นที่เรียบร้อยแล้ว

๒.๗ ห้ามบุคคลใดของผู้ยื่นข้อเสนอที่เข้าร่วมการทดสอบ POC เปิดเผยรายละเอียดที่เกิดขึ้นระหว่างการสาธิตการทดสอบต่อบุคคลอื่นใด เว้นแต่กรณีจำเป็นและต้องได้รับความเห็นชอบในเนื้อหาที่จะเปิดเผยอย่างเป็นทางการจากสำนักงานปลัดกระทรวงแรงงานเท่านั้น บุคคลของผู้ยื่นข้อเสนอที่เข้าร่วมการทดสอบ POC ทุกคนที่เข้าทำการสาธิตการทดสอบระบบต้องลงนามในเอกสารหนังสือแสดงเจตนาไม่เปิดเผยข้อมูลของสำนักงานปลัดกระทรวงแรงงานและส่งมอบหนังสือแสดงเจตนาไม่เปิดเผยข้อมูลของสำนักงานปลัดกระทรวงแรงงานก่อนที่จะดำเนินการสาธิตการทดสอบระบบ

๒.๘ ระหว่างการสาธิตหากมีบุคคลใดของผู้มีสิทธิ์ทำการสาธิตการทดสอบระบบ มีพฤติกรรมส่อไปในทางไม่สุจริต ฝ่าฝืน หรือละเมิดกฎ กติกา ข้อปฏิบัติในการสาธิตการทดสอบระบบ หรือคำสั่งของสำนักงานปลัดกระทรวงแรงงาน บุคคลนั้นจะถูกตัดสิทธิ์ให้ออกจากการสาธิตการทดสอบระบบทันที

๒.๙ การจัดเตรียมวัสดุ อุปกรณ์ฮาร์ดแวร์ อุปกรณ์เครือข่ายต่าง ๆ รวมทั้งซอฟต์แวร์เพื่อใช้ในการสาธิตการทดสอบ ตลอดจนการศึกษารายละเอียดในภาคผนวกต่าง ๆ เพื่อเตรียมการระบบสารสนเทศให้พร้อมทำการสาธิตการทดสอบระบบ การจัดเตรียมทั้งหมดนี้ถือเป็นความรับผิดชอบของผู้ยื่นข้อเสนอที่เข้าร่วมการทดสอบ POC ในการจัดเตรียมอุปกรณ์ให้เพียงพอต่อการสาธิตการทดสอบตามเกณฑ์การทดสอบทุกข้อ โดยรายการทั้งหมดจะต้องสำแดงเป็นเอกสารขอนำเข้าพื้นที่โดยต้องแสดงรายละเอียดแต่ละรายการและจำนวนอย่างชัดเจนทุกรายการที่มีการนำเข้ามาในสถานที่ทดสอบ ทั้งนี้การติดตั้งอุปกรณ์ทั้งหมดให้เสร็จสิ้นพร้อมทำการสาธิตทดสอบระบบภายในวันเวลาและสถานที่ที่สำนักงานปลัดกระทรวงแรงงานกำหนด ค่าใช้จ่าย และค่าเสียหายใด ๆ (ถ้ามี) ที่เกิดขึ้นจากการจัดเตรียมและติดตั้งเพื่อการสาธิตการทดสอบระบบทั้งหมด ให้ถือเป็นความรับผิดชอบของผู้ยื่นข้อเสนอที่เข้าร่วมการทดสอบ POC ทั้งหมด จะเรียกร้องใด ๆ กับสำนักงานปลัดกระทรวงแรงงานไม่ได้

๒.๑๐ เมื่อผู้ยื่นข้อเสนอที่เข้าร่วมการทดสอบ POC ดำเนินการทดสอบ POC ตามรายละเอียดตารางที่ ๑ เกณฑ์การทดสอบและวิธีการให้คะแนนเสร็จสิ้นแล้ว คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์จะพิจารณาผลการทดสอบและให้คะแนนแต่ละหัวข้อตามรายละเอียดใน ตารางที่ ๑ เกณฑ์การทดสอบและวิธีการให้คะแนน โดยพิจารณาตามเอกสารผลการทดสอบที่นำส่งพร้อมลงลายมือชื่อแล้วของผู้ยื่นข้อเสนอที่เข้าร่วมการทดสอบ POC แต่ละราย พร้อมตรวจสอบการแสดงผลจากระบบของแต่ละราย โดยการพิจารณาให้คะแนนจะไม่มีการใช้ดุลพินิจใด ๆ ทั้งสิ้น

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ	ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ	ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ	ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ	ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการและเลขานุการ	

ตารางที่ ๑ เกณฑ์การทดสอบและวิธีการให้คะแนน

ลำดับที่	เกณฑ์การทดสอบ	วิธีการให้คะแนน
1.	ทดสอบพร้อมนำเสนอระบบป้องกันและตรวจจับภัยคุกคามในระดับเครื่องผู้ใช้งาน (EDR for Client) ที่สามารถป้องกันข้อมูลสำคัญขององค์กรไม่ให้รั่วไหลออกไปภายนอกองค์กร (Data loss prevention) ผ่านทาง HTTP และ Windows Clipboard ได้ **(10 คะแนน)**	**<u>ระดับที่ 4 (10 คะแนน)</u>** มีการนำเสนอด้วยวิธีการสาธิตจากระบบจริง โดยระบบป้องกันตรวจจับภัยคุกคามในระดับเครื่องผู้ใช้งาน ที่มีสามารถ ป้องกันข้อมูลรั่วไหล (DLP) ได้โดยมีรายละเอียดดังนี้ 1. ทำได้บน Agent Software ของ EDR for Client 2. สามารถป้องกันข้อมูลผ่านทาง HTTP และ Windows Clipboard ได้ครบถ้วนโดยวิธีการสาธิตจากระบบจริง **<u>ระดับที่ 3 (6 คะแนน)</u>** มีการนำเสนอด้วยวิธีการสาธิตจากระบบจริง โดยระบบป้องกันตรวจจับภัยคุกคามในระดับเครื่องผู้ใช้งาน ที่มีสามารถ ป้องกันข้อมูลรั่วไหล (DLP) ได้โดยเสนอระบบอื่นเพิ่มเติม โดยมีรายละเอียดดังนี้ 1. นำเสนอด้วยระบบอื่นเพิ่มเติม 2. สามารถป้องกันข้อมูลผ่านทาง HTTP, Windows Clipboard ได้ครบถ้วนโดยวิธีการสาธิตจากระบบจริง **<u>ระดับที่ 2 (3 คะแนน)</u>** นำเสนอด้วยวิธีการ นำเสนอเอกสารแสดงระบบ (Capture Screen) ระบบป้องกันตรวจจับภัยคุกคามในระดับเครื่องผู้ใช้งาน ที่มีสามารถ ป้องกันข้อมูลรั่วไหล (DLP) โดยมีรายละเอียดดังนี้ 1. นำเสนอด้วยระบบอื่นเพิ่มเติม หรือ Software ของระบบ EDR for Client 2. สามารถป้องกันข้อมูลผ่านทาง HTTP, Windows Clipboard ได้ครบถ้วน **<u>ระดับที่ 1 (0 คะแนน)</u>** นำเสนอไม่ครบถ้วนตามข้อกำหนด หรือไม่สามารถนำมาแสดงได้

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลำดับที่	เกณฑ์การทดสอบ	วิธีการให้คะแนน
2.	ทดสอบพร้อมนำเสนอระบบป้องกันและตรวจจับภัยคุกคามในระดับเครื่องแม่ข่ายในการป้องกันภัยคุกคามในระดับ Application ได้ **(10 คะแนน)**	**<u>ระดับที่ 4 (10 คะแนน)</u>** มีการนำเสนอระบบป้องกันภัยคุกคามในระดับเครื่องแม่ข่าย (Server) ที่สามารถป้องกันการโจมตีในระดับ Application ได้โดยมีรายละเอียดดังนี้ 1. สามารถป้องกัน SQL injection ได้ 2. สามารถป้องกัน Cross Site Script ได้ 3. ป้องกันได้ด้วย Agent ระบบป้องกันภัยคุกคามในระดับแม่ข่ายและนำเสนอการป้องกันโดยวิธีการสาธิตจากระบบจริง **<u>ระดับที่ 3 (6 คะแนน)</u>** มีการนำเสนอระบบป้องกันภัยคุกคามในระดับเครื่องแม่ข่าย (Server) ที่สามารถป้องกันการโจมตีในระดับ Application ได้โดยมีรายละเอียดดังนี้ 1. สามารถป้องกัน SQL injection หรือ Cross Site Script ได้แค่อย่างใดอย่างหนึ่ง 2. ป้องกันได้ด้วย Agent ระบบป้องกันภัยคุกคามในระดับแม่ข่าย ที่นำเสนอและนำเสนอการป้องกันโดยวิธีการสาธิตจากระบบจริง **<u>ระดับที่ 2 (3 คะแนน)</u>** มีการนำเสนอระบบป้องกันภัยคุกคามในระดับเครื่องแม่ข่าย (Server) ที่สามารถป้องกันการโจมตีในระดับ Application ได้โดยมีรายละเอียดดังนี้ 1. สามารถป้องกัน SQL injection หรือ Cross Site Script ได้แค่อย่างใดอย่างหนึ่ง 2. นำเสนอการป้องกันการโจมตีในระดับ Application ด้วยระบบอื่นเพิ่มเติมหรือนำเสนอการป้องกันด้วยวิธีการนำเสนอเอกสารแสดงระบบ (Capture Screen) **<u>ระดับที่ 1 (0 คะแนน)</u>** นำเสนอไม่ครบถ้วนตามข้อกำหนด หรือไม่สามารถนำมาแสดงได้

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ

ลำดับที่	เกณฑ์การทดสอบ	วิธีการให้คะแนน
3.	ทดสอบพร้อมนำเสนอระบบป้องกันและตรวจจับภัยคุกคามในระดับเครื่องแม่ข่ายที่สามารถตรวจสอบการสื่อสารที่มีการเข้ารหัสด้วย SSL/TLS ได้ **(10 คะแนน)**	**<u>ระดับที่ 4 (10 คะแนน)</u>** มีการนำเสนอระบบป้องกันภัยคุกคามในระดับเครื่องแม่ข่าย (Server) ที่สามารถตรวจสอบการสื่อสารที่มีการเข้ารหัสด้วย SSL/TLS ได้ โดยมีรายละเอียดดังนี้ 1. สามารถตรวจสอบและป้องกันการโจมตีที่มีการเข้ารหัสด้วย SSL/TLS ได้บนระบบปฏิบัติการทั้ง Window และ Linux 2. ตรวจสอบการสื่อสารได้ด้วย Agent ของระบบป้องกันภัยคุกคามในระดับแม่ข่าย 3. นำเสนอการตรวจสอบการสื่อสารโดยวิธีการสาธิตจากระบบจริง **<u>ระดับที่ 3 (6 คะแนน)</u>** มีการนำเสนอระบบป้องกันภัยคุกคามในระดับเครื่องแม่ข่าย (Server) ที่สามารถป้องกันการโจมตีในระดับ Application ได้โดยมีรายละเอียดดังนี้ 1. สามารถตรวจสอบและป้องกันการโจมตีที่มีการเข้ารหัสด้วย SSL/TLS ได้บนระบบปฏิบัติการ Window หรือ Linux อย่างใดอย่างหนึ่ง 2. ตรวจสอบการสื่อสารได้ด้วย Agent ระบบป้องกันภัยคุกคามในระดับแม่ข่าย 3. นำเสนอการตรวจสอบการสื่อสารโดยวิธีการสาธิตจากระบบจริง **<u>ระดับที่ 2 (3 คะแนน)</u>** มีการนำเสนอระบบป้องกันภัยคุกคามในระดับเครื่องแม่ข่าย (Server) ที่สามารถป้องกันการโจมตีในระดับ Application ได้โดยมีรายละเอียดดังนี้ 1. ตรวจสอบการสื่อสารได้ด้วยระบบอื่นเพิ่มเติมหรือนำเสนอการป้องกันด้วยวิธีการ นำเสนอเอกสารแสดงระบบ (Capture Screen) **<u>ระดับที่ 1 (0 คะแนน)</u>** นำเสนอไม่ครบถ้วนตามข้อกำหนด หรือไม่สามารถนำมาแสดงได้

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ

ลำดับที่	เกณฑ์การทดสอบ	วิธีการให้คะแนน
4.	ทดสอบพร้อมนำเสนอระบบตรวจจับภัยคุกคามทางไซเบอร์และประเมินความเสี่ยงระบบสารสนเทศที่สามารถบริหารจัดการแบบรวมศูนย์ได้ผ่านหน้าจอเดียว (Single Console) **(10 คะแนน)**	**<u>ระดับที่ 4 (10 คะแนน)</u>** มีการนำเสนอระบบตรวจจับภัยคุกคามทางไซเบอร์และประเมินความเสี่ยงระบบสารสนเทศที่สามารถบริหารจัดการแบบรวมศูนย์ได้ผ่านหน้าจอเดียว (Single Console) ได้ โดยมีรายละเอียดดังนี้ 1. สามารถแสดงผลการตรวจจับภัยคุกคามในระดับเครื่องคอมพิวเตอร์ผู้ใช้งานและแม่ข่ายได้ 2. สามารถแสดงผลการตรวจจับภัยคุกคามขั้นสูงทางไซเบอร์บนระบบเครือข่าย 3. สามารถประเมินความเสี่ยงของเครื่องผู้ใช้และเครื่องแม่ข่ายที่มี Agent ระบบป้องกันภัยคุกคามในระดับเครื่องคอมพิวเตอร์ได้ 4. สามารถทำข้อ 1-3 ได้ด้วยหน้าจอเดียว (Single Console) 5. นำเสนอโดยมีวิธีการสาธิตจากระบบจริง **<u>ระดับที่ 3 (6 คะแนน)</u>** มีการนำเสนอระบบตรวจจับภัยคุกคามทางไซเบอร์และประเมินความเสี่ยงระบบสารสนเทศที่สามารถบริหารจัดการแบบรวมศูนย์ได้ผ่านหน้าจอเดียว (Single Console) ได้ โดยมีรายละเอียดดังนี้ 1. สามารถแสดงผลการตรวจจับภัยคุกคามในระดับเครื่องคอมพิวเตอร์ผู้ใช้งานและแม่ข่ายได้ 2. สามารถแสดงผลการตรวจจับภัยคุกคามขั้นสูงทางไซเบอร์บนระบบเครือข่าย 2. สามารถประเมินความเสี่ยงของเครื่องผู้ใช้และเครื่องแม่ข่ายที่มี Agent ระบบป้องกันภัยคุกคามในระดับเครื่องคอมพิวเตอร์ได้ 3. สามารถทำข้อ 1-3 ได้ด้วยหลายหน้าจอ (Multiple Consoles) 4. นำเสนอโดยมีวิธีการสาธิตจากระบบจริง **<u>ระดับที่ 2 (3 คะแนน)</u>** มีการนำเสนอระบบตรวจจับภัยคุกคามทางไซเบอร์และประเมินความเสี่ยงระบบสารสนเทศที่สามารถบริหารจัดการแบบรวมศูนย์ได้ผ่านหน้าจอเดียว (Single Console) ได้ โดยมีรายละเอียดดังนี้

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ

ลำดับที่	เกณฑ์การทดสอบ	วิธีการให้คะแนน
		1. สามารถแสดงผลการตรวจจับภัยคุกคามในระดับเครื่องคอมพิวเตอร์ผู้ใช้งานและแม่ข่ายได้ 2. สามารถแสดงผลการตรวจจับภัยคุกคามขั้นสูงทางไซเบอร์บนระบบเครือข่าย ได้ 3. สามารถประเมินความเสี่ยงของเครื่องผู้ใช้และเครื่องแม่ข่ายที่มี Agent ระบบป้องกันภัยคุกคามในระดับเครื่องคอมพิวเตอร์ได้
		4. สามารถทำข้อ 1-3 ได้ด้วยหลายหน้าจอ (Multiple Consoles) 5. นำเสนอด้วยวิธีการนำเสนอเอกสารแสดงระบบ (Capture Screen) **<u>ระดับที่ 1 (0 คะแนน)</u>** นำเสนอไม่ครบถ้วนตามข้อกำหนด หรือไม่สามารถนำมาแสดงได้
5.	ทดสอบพร้อมนำเสนอระบบป้องกันและตรวจจับภัยคุกคามในระดับเครื่องแม่ข่ายที่สามารถแสกนหาช่องโหว่บนเครื่องคอมพิวเตอร์แต่ละเครื่องและปรับแต่งนโยบายเพื่อป้องกันการโจมตีที่ช่องโหว่ที่ถูกพบแบบอัตโนมัติ **(15 คะแนน)**	**<u>ระดับที่ 4 (15 คะแนน)</u>** มีการนำเสนอระบบป้องกันภัยคุกคามในระดับเครื่องแม่ข่าย (Server) ที่ตรวจสอบช่องโหว่ของเครื่องแม่ข่ายโดยมีรายละเอียดดังนี้ 1. สามารถแสกนหาช่องโหว่บนเครื่องคอมพิวเตอร์แม่ข่ายได้ 2. สามารถปรับแต่งนโยบายเพื่อป้องกันการโจมตีที่ช่องโหว่ที่ถูกพบแบบอัตโนมัติ 3. แสกนช่องโหว่และป้องกันการโจมตีที่ช่องโหว่ที่ถูกพบด้วย Agent ระบบป้องกันภัยคุกคามในระดับแม่ข่าย 4. นำเสนอโดยวิธีการสาธิตจากระบบจริง **<u>ระดับที่ 3 (10 คะแนน)</u>** มีการนำเสนอระบบป้องกันภัยคุกคามในระดับเครื่องแม่ข่าย (Server) ที่ตรวจสอบช่องโหว่ของเครื่องแม่ข่ายโดยมีรายละเอียดดังนี้ 1. สามารถแสกนหาช่องโหว่บนเครื่องคอมพิวเตอร์แม่ข่ายได้ 2. สามารถปรับแต่งนโยบายเพื่อป้องกันการโจมตีที่ช่องโหว่ที่ถูกพบได้โดยใช้บุคลากรจากทีมผู้ดูแลระบบ

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ

ลำดับที่	เกณฑ์การทดสอบ	วิธีการให้คะแนน
		3. แสกนช่องโหว่และป้องกันการโจมตีที่ช่องโหว่ที่ถูกพบด้วย Agent ระบบป้องกันภัยคุกคามในระดับแม่ข่าย 4. นำเสนอโดยวิธีการสาธิตจากระบบจริง **<u>ระดับที่ 2 (5 คะแนน)</u>** มีการนำเสนอระบบป้องกันภัยคุกคามในระดับเครื่องแม่ข่าย (Server) ที่ตรวจสอบช่องโหว่ของเครื่องแม่ข่ายโดยมีรายละเอียดดังนี้ 1. สามารถแสกนหาช่องโหว่บนเครื่องคอมพิวเตอร์แม่ข่ายได้ 2. สามารถปรับแต่งนโยบายเพื่อป้องกันการโจมตีที่ช่องโหว่ที่ถูกพบได้โดยใช้บุคลากรจากทีมผู้ดูแลระบบ 3. แสกนช่องโหว่และป้องกันการโจมตีที่ช่องโหว่ที่ถูกพบด้วยระบบอื่นเพิ่มเติม 4. นำเสนอด้วยวิธีการนำเสนอเอกสารแสดงระบบ (Capture Screen) หรือ วิธีการสาธิตจากระบบจริง **<u>ระดับที่ 1 (0 คะแนน)</u>** นำเสนอไม่ครบถ้วนตามข้อกำหนด หรือไม่สามารถนำมาแสดงได้
6.	ทดสอบพร้อมนำเสนอระบบป้องกันและตรวจจับภัยคุกคามในระดับเครื่องแม่ข่ายที่สามารถจัดทำรายงานประจำเดือนเพื่อสรุปเหตุการณ์ที่เกิดขึ้น **(15 คะแนน)**	**<u>ระดับที่ 4 (15 คะแนน)</u>** มีการนำเสนอระบบป้องกันภัยคุกคามในระดับเครื่องแม่ข่าย (Server) ที่สามารถจัดทำรายงานสรุปเหตุการณ์ของเครื่องแม่ข่ายโดยมีรายละเอียดดังนี้ 1. สามารถจัดทำรายงานประจำเดือนเพื่อสรุปเหตุการณ์ที่เกิดขึ้นแบบทันทีและตั้งเวลา 2. สามารถเข้ารหัสผ่านความปลอดภัย ด้วยรหัสผ่านจากภายในระบบที่นำเสนอโดยตรง 3. นำเสนอโดยมีวิธีการสาธิตจากระบบจริง **<u>ระดับที่ 3 (10 คะแนน)</u>** มีการนำเสนอระบบป้องกันภัยคุกคามในระดับเครื่องแม่ข่าย (Server) ที่สามารถจัดทำรายงานสรุปเหตุการณ์ของเครื่องแม่ข่ายโดยมีรายละเอียดดังนี้

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ

ลำดับที่	เกณฑ์การทดสอบ	วิธีการให้คะแนน
		1. สามารถจัดทำรายงานประจำเดือนเพื่อสรุปเหตุการณ์ที่เกิดขึ้นแบบทันทีหรือตั้งเวลา 2. สามารถเข้ารหัสผ่านความปลอดภัยด้วยรหัสผ่านจากภายในระบบที่นำเสนอโดยตรง 3. นำเสนอโดยนำเสนอเอกสารแสดงระบบ (Capture Screen)
		<u>ระดับที่ 2 (5 คะแนน)</u> มีการนำเสนอระบบป้องกันภัยคุกคามในระดับเครื่องแม่ข่าย (Server) ที่สามารถจัดทำรายงานสรุปเหตุการณ์ของเครื่องแม่ข่ายโดยมีรายละเอียดดังนี้ 1. สามารถจัดทำรายงานประจำเดือนเพื่อสรุปเหตุการณ์ที่เกิดขึ้นแบบทันทีหรือตั้งเวลา 2. ไม่สามารถเข้ารหัสผ่านความปลอดภัยได้ 3. นำเสนอด้วยวิธีการนำเสนอเอกสารแสดงระบบ (Capture Screen) หรือ วิธีการสาธิตจากระบบจริง **<u>ระดับที่ 1 (0 คะแนน)</u>** นำเสนอไม่ครบถ้วนตามข้อกำหนด หรือไม่สามารถนำมาแสดงได้

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ตารางที่ ๒ แผนการทดสอบ POC

กำหนดการทดสอบ POC

๑. ดำเนินการติดตั้งอุปกรณ์สำหรับการทดสอบ ตามเงื่อนไขที่สำนักงานปลัดกระทรวงแรงงานกำหนด			
สถานที่ติดตั้งอุปกรณ์	**เป็นไปตามสำนักงานปลัดกระทรวงแรงงานกำหนด**		
วันที่	.....	**เวลา**	.....
รายละเอียด			
▪ ผู้ยื่นข้อเสนอที่เข้าร่วมการทดสอบ POC ลงทะเบียนเพื่อเข้าดำเนินการทดสอบ POC ▪ ผู้ยื่นข้อเสนอที่เข้าร่วมการทดสอบ POC ส่งรายการอุปกรณ์ และรายละเอียดซอฟต์แวร์สำหรับใช้ในการทดสอบ POC ให้สำนักงานปลัดกระทรวงแรงงาน พิจารณา ▪ ผู้ยื่นข้อเสนอที่เข้าร่วมการทดสอบ POC ดำเนินการติดตั้งอุปกณ์ทั้งหมดตามรายการที่แจ้งไว้กับสำนักงานปลัดกระทรวงแรงงาน ณ สถานที่ ที่ สำนักงานปลัดกระทรวงแรงงาน กำหนด			
๒. ดำเนินการทำสอบตามเงื่อนไขที่กำหนด			
สถานที่ติดตั้งอุปกรณ์	**เป็นไปตามสำนักงานปลัดกระทรวงแรงงานกำหนด**		
วันที่	.....	**เวลา**	.....
รายละเอียด			
เวลา	ผู้ยื่นข้อเสนอที่เข้าร่วมการทดสอบ POC ลงทะเบียนเพื่อเข้าดำเนินการทดสอบ POC		
เวลา	ผู้ยื่นข้อเสนอที่เข้าร่วมการทดสอบ POC ดำเนินการติดตั้งอุปกณ์ทั้งหมดตามรายการที่แจ้งไว้กับสำนักงานปลัดกระทรวงแรงงาน ณ สถานที่ ที่ สำนักงานปลัดกระทรวงแรงงาน กำหนด		
เวลา	ผู้ยื่นข้อเสนอที่เข้าร่วมการทดสอบ POC เริ่มดำเนินการทดสอบ และนำเสนอต่อคณะกรรมการ		
	จัดส่งรายงานผลการทดสอบต่อคณะกรรมการ		

หมายเหตุ :

๑) กรณีผู้ยื่นข้อเสนอที่เข้าร่วมการทดสอบ POC ไม่มาลงทะเบียนเพื่อเข้าดำเนินการทดสอบ POC ตามวันเวลาที่กำหนด จะถือว่าผู้ยื่นข้อเสนอที่เข้าร่วมการทดสอบ POC สละสิทธิการเข้าร่วมการทดสอบ และได้คะแนนในการสาธิตการทดสอบเป็น 0 คะแนน

๒) ถ้าเกิดข้อผิดพลาดในขั้นตอนการสาธิต ให้ผู้ยื่นข้อเสนอที่เข้าร่วมการทดสอบ POC สามารถทำการแก้ไขระบบที่จะสาธิตได้ โดยมีระยะเวลาการแก้ไขรวมไม่เกิน ๓๐ นาที แล้วกลับมานำเสนอให้คณะกรรมการได้ใหม่เพียง ๑ ครั้ง

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ
ลงชื่อ ..... กรรมการ

ภาคผนวก จ

ตารางกำหนดตัวถ่วงของคอมพิวเตอร์

ชื่อรายการ	ค่าตัวถ่วง
๑.ห้องศูนย์ปฏิบัติการและประสานงานกลางด้านความมั่นคงปลอดภัยไซเบอร์ พร้อมระบบคอมพิวเตอร์และซอฟต์แวร์	๐.๑
๒.ระบบป้องกัน ตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์ และระบบเครือข่าย (End-Point Protection and Network Protection)	๐.๑
๓.ระบบเฝ้าระวังและตอบสนองต่อภัยคุกคามทางไซเบอร์ (Extended Detection and Response)	๐.๓
๔.ระบบตรวจประเมินความเสี่ยงความมั่นคงปลอดภัยไซเบอร์เพื่อค้นหาช่องโหว่และความเสี่ยง ที่อาจเกิดขึ้นสำหรับระบบเครือข่าย, เครื่องแม่ข่าย และเว็บแอพพลิเคชั่น	๐.๓
๕.ระบบเครื่องคอมพิวเตอร์แม่ข่ายพร้อมซอฟต์แวร์บริหารจัดการ และอุปกรณ์กระจายสัญญาณ	๐.๑
๖.บุคลากรตามภาคผนวก ข	๐.๑

คณะกรรมการจัดทำรายละเอียดคุณลักษณะเฉพาะฯ

ลงชื่อ ..... ประธานกรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการและเลขานุการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ

ลงชื่อ ..... กรรมการ