ขอบเขตการดำเนินงาน (Term of Reference)
จ้างเหมาบริการเฝ้าระวังและป้องกันภัยคุกคามทางเครือข่ายสารสนเทศสำหรับ Cloud
ระยะเวลา 12 เดือน

1. <u>หลักการและเหตุผล</u>

ความมั่นคงปลอดภัยทางเครือข่ายเป็นหนึ่งในปัจจัยสำคัญขององค์กรที่จะช่วยป้องกันความเสียหายที่เกิดจากผู้ไม่หวังดี ปัจจุบันการโจมตีทางเครือข่ายมีความหลากหลายมากขึ้นตามเทคโนโลยีที่มีการพัฒนาอย่างต่อเนื่อง โดยเฉพาะการโจมตีของผู้ไม่หวังดีที่มีเป้าหมายที่จะโจมตีสำนักงาน เป็นรูปแบบการโจมตีที่โปรแกรมป้องกันไวรัสบางส่วนไม่สามารถตรวจจับได้ เพราะผู้โจมตีมักใช้โปรแกรมทั่วไปที่ไม่อันตรายและไม่ถือว่าเป็นอันตรายนำมาใช้ผิดวิธี จนเกิดผลเสียต่อองค์กรได้

สำนักงานจึงมีความจำเป็นต้องจัดหาบริการเฝ้าระวังและป้องกันภัยคุกคามทางเครือข่าย เพื่อตรวจสอบพฤติกรรมที่น่าสงสัยจากผู้ไม่หวังดีจากข้อมูลจราจรทางอิเล็กทรอนิกส์ของสำนักงานตลอด 24 ชั่วโมง เพื่อให้สามารถตอบสนองต่อเหตุการณ์ทางด้านความมั่นคงปลอดภัยสารสนเทศได้ทันท่วงที ซึ่งจำเป็นต้องมีบุคลากรที่มีความรู้ความสามารถด้านนี้เฉพาะด้านประกอบกับระบบสารสนเทศที่ใช้ในการติดตามวิเคราะห์เฝ้าระวังและป้องกันภัยคุกคามดังกล่าว ซึ่งปัจจุบันสำนักงานยังขาดบุคลากรที่มีความชำนาญดังกล่าว แม้จะสามารถจัดหาระบบสารสนเทศในการวิเคราะห์จัดการได้ แต่ด้วยขนาดของระบบเครือข่ายสำนักงานเป็นขนาดกลางอาจไม่คุ้มค่าต่อการลงทุนระบบที่ต้องคอยดำเนินการปรับปรุงให้มีความทันสมัยตามภัยคุกคามที่มีการพัฒนาตลอดเวลา การจ้างเหมาผู้เชี่ยวชาญภายนอกพร้อมระบบบริหารจัดการภัยคุกคามจึงเป็นทางเลือกที่จะมีประสิทธิภาพที่สุดในขณะนี้

2. <u>วัตถุประสงค์</u>

2.1 เพื่อจัดหาบริการเฝ้าระวังภัยคุกคามทางไซเบอร์ เช่น การระบาดของไวรัส หรือการบุกรุกจากภายนอกเข้าสู่ระบบ หรือการขโมยข้อมูลโดยผู้ไม่ประสงค์ดี

2.2 เพื่อจัดหาบริการตรวจสอบช่องโหว่ทางด้านความมั่นคงปลอดภัยของระบบด้วยเครื่องมือ Vulnerability Assessment พร้อมแนะนำแนวทางในการแก้ไขช่องโหว่ของระบบ

2.3 เพื่อจัดหาโปรแกรมป้องกันและกำจัดภัยคุกคามบนเครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์แม่ข่ายแบบเสมือน ที่อยู่ในสภาพแวดล้อมคลาวด์รูปแบบ IaaS

2.4 เพื่อป้องกันภัยความเสียหายของระบบงานสารสนเทศและข้อมูล และให้มีความมั่นคงปลอดภัยจากภัยคุกคามและโปรแกรมไม่พึงประสงค์ เช่น Viruses, Spyware, Trojans และ Worms เป็นต้น

2.5 เพื่อให้เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์แม่ข่ายแบบเสมือน ได้รับการป้องกันจากโปรแกรมไม่พึงประสงค์ และให้สามารถทำงานได้อย่างมีประสิทธิภาพและต่อเนื่อง

3. <u>คุณสมบัติผู้ยื่นข้อเสนอ</u>

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบ ที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลที่ซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วน ผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นนิติบุคคลผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงาน ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทยเว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

3.10 ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ต้องมีคุณสมบัติดังนี้

(1) การกำหนดสัดส่วนในการเข้าร่วมค้าของคู่สัญญา

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงฯ จะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

(2) กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลักกิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

(3) การยื่นข้อเสนอของกิจการร่วมค้า

(3.1) กรณีที่ข้อตกลงฯ กำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

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

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

3.12 ผู้เสนอราคาต้องมีมูลค่าสุทธิของกิจการ ดังนี้

(1) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย/กฎหมายต่างประเทศ ซึ่งได้จดทะเบียนเกินกว่า 1 ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ของ 1 ปีสุดท้ายก่อนวันยื่นข้อเสนอ ซึ่งจะต้องแสดงค่าเป็นบวก

(2) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย/กฎหมายต่างประเทศ ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ไม่ต่ำกว่า 1,000,000 บาท

(3) กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดาถือสัญชาติไทย/บุคคลธรรมดาที่มิได้ถือสัญชาติไทยให้พิจารณาจากหนังสือรับรองบัญชีเงินฝาก โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่าไม่น้อยกว่า 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้งและหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือก จะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าว อีกครั้งหนึ่งในวันลงนามในสัญญา ทั้งนี้ หนังสือรับรองบัญชีเงินฝากซึ่งธนาคารออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอหรือวันลงนามในสัญญา ไม่เกิน 90 วัน

(4) กรณีที่ผู้ยื่นข้อเสนอมีคุณสมบัติไม่เป็นไปตามข้อ (1) - (3)

ผู้ยื่นข้อเสนอสามารถขอหนังสือรับรองวงเงินสินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และ ประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ หรือเป็นสินเชื่อที่ธนาคารต่างประเทศ หรือบริษัทเงินทุน หรือบริษัทเงินทุนหลักทรัพย์ ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารกลางของประเทศนั้นตามรายชื่อบริษัทเงินทุนที่ธนาคารกลางของประเทศนั้นแจ้งเวียนให้ทราบโดยพิจารณาจากยอดเงินรวม ของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจ จากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอนับถึงวันยื่นข้อเสนอไม่เกิน 90 วัน โดยต้องมีวงเงินสินเชื่อจากธนาคารไม่น้อยกว่า 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอ ในแต่ละครั้ง ทั้งนี้ สำหรับธนาคารภายในประเทศหนังสือรับรองวงเงินสินเชื่อให้เป็นไปตามแบบที่กำหนด

(5) กรณีนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศและบุคคลธรรมดาที่มิได้ถือสัญชาติไทยตามข้อ (2)-(4) มูลค่าจะต้องเป็นไปตามอัตราแลกเปลี่ยนเงินตราตามประกาศที่ ธนาคารแห่งประเทศไทยกำหนดในช่วงระหว่างวันที่เผยแพร่ประกาศและเอกสารเชิญชวนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (e - GP) หรือมีหนังสือเชิญชวน จนถึงวันเสนอราคา

(6) กรณีตามข้อ (1)-(4) ใช้บังคับกับการจัดซื้อจัดจ้างโดยวิธีประกาศเชิญชวนทั่วไปวิธีคัดเลือก และวิธีเฉพาะเจาะจง ตามหมวด 6 งานจ้างที่ปรึกษา ตามหมวด 7 และงานจ้างออกแบบหรือควบคุมงานก่อสร้างตามหมวด 8 แห่งพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 เว้นแต่ในกรณีดังต่อไปนี้

(6.1) กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ

(6.2) นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการ ตามพระราชบัญญัติล้มละลาย พ.ศ. 2483 และที่แก้ไขเพิ่มเติม

(6.3) งานจ้างก่อสร้างที่กรมบัญชีกลางได้ขึ้นทะเบียนผู้ประกอบการงานก่อสร้างแล้ว และงานจ้างก่อสร้างที่หน่วยงานของรัฐที่ได้มีการจัดทำบัญชีผู้ประกอบการงานก่อสร้างที่มีคุณสมบัติ เบื้องต้นไว้แล้วก่อนวันที่พระราชบัญญัติการจัดซื้อจัดจ้างฯ มีผลใช้บังคับ

(6.4) การจัดซื้อจัดจ้างตามมาตรา 56 วรรคหนึ่ง (2) (ข) และ (ค) แห่งพระราชบัญญัติการจัดซื้อจัดจ้างฯ

(6.5) การซื้ออสังหาริมทรัพย์และการเช่าอสังหาริมทรัพย์

(6.6) กรณีงานจ้างบริการหรืองานจ้างเหมาบริการกับบุคคลธรรมดา เช่น จ้างพนักงาน ขับรถ ครูชาวต่างชาติ พนักงานเก็บขยะ พนักงานบันทึกข้อมูล เป็นต้น

3.13 ผู้เสนอราคาต้องมีมูลค่าสุทธิของกิจการ เป็นไปตามหนังสือคณะกรรมการวินิจฉัยปัญหาการจัดซื้อจัดจ้างและบริหารพัสดุภาครัฐด่วนที่สุด ที่ กค (กวจ) 0405.2/ว 48 ลงวันที่ 20 มกราคม 2568

4. <u>เงื่อนไขข้อเสนอด้านเทคนิค</u>

ผู้ยื่นข้อเสนอต้องแสดงเอกสารให้สำนักงานคณะกรรมการส่งเสริมการลงทุน พิจารณาดังนี้

4.1 ตารางเปรียบเทียบรายละเอียดคุณลักษณะเฉพาะของรายละเอียดงานข้อ 7 และ ข้อ 8 ที่สำนักงานต้องการจัดหา เป็นรายข้อทุกข้อ (Statement of Compliance) โดยมีรายละเอียดดังต่อไปนี้

ลำดับที่	รายละเอียดที่กำหนด	รายละเอียดที่เสนอ	หน้าที่อ้างอิง
ระบุหัวข้อให้ตรงกับหัวข้อที่ระบุในเอกสารที่ยื่นเสนอราคา	ระบุคุณลักษณะเฉพาะที่สำนักงานกำหนด	ระบุคุณลักษณะเฉพาะที่บริษัทนำเสนอ	ระบุหมายเลขหน้าของเอกสารอ้างอิง

1) ต้องเปรียบเทียบรายละเอียดที่กำหนดของสำนักงานกับรายละเอียดที่เสนอ ให้ชัดเจนไม่คลุมเครือ โดยต้องระบุยี่ห้อ รุ่น ขนาด อย่างละเอียดชัดเจนเป็นรายข้อทุกข้อ (ไม่ควรระบุว่า ไม่น้อยกว่า ไม่ต่ำกว่า มากกว่า สูงกว่า ดีกว่า)

2) ต้องอ้างอิงถึงรายละเอียดใน Catalog หรือ Data Sheet ของเจ้าของผลิตภัณฑ์ ว่าได้แสดงอยู่ในหน้าใด และใน Catalog หรือ Data Sheet ต้องแสดงหมายเลขของรายการที่อ้างอิงถึง พร้อมทำแถบสีหรือเน้นข้อความที่อ้างอิงถึงให้เห็นอย่างชัดเจน

4.2 เอกสารด้านเทคนิคที่เสนอทั้งหมด จะต้องมีเลขหน้ากำกับทุกหน้า

4.3 เอกสารรับรองผู้เชี่ยวชาญที่ผ่านการอบรมหรือ Certificate เฉพาะทางด้านที่เกี่ยวข้องกับการใช้งาน หรือการแก้ไขปัญหา หรือการดูแลรักษาของผลิตภัณฑ์ที่นำเสนอ

4.4 กรณีที่มีการเสนอรายละเอียดอื่นใดแตกต่างไปจากข้อกำหนดของสำนักงาน ผู้ยื่นข้อเสนอจะต้องจัดทำเอกสารอธิบายในรายละเอียดที่แตกต่างนั้นทุกรายการ พร้อมเปรียบเทียบความเทียบเท่าหรือดีกว่า ทั้งในเชิงเทคนิคและประสิทธิภาพ และข้อดี-ข้อเสีย ให้ชัดเจนเป็นภาษาไทยพร้อมหลักฐานที่เชื่อถือได้ ประกอบทุกรายการ ทั้งนี้ สำนักงานขอสงวนสิทธิ์ในการเรียกผู้ยื่นข้อเสนอเข้ามาชี้แจงรายละเอียดเพิ่มเติมตามวันและเวลาที่สำนักงานกำหนด

4.5 หากผู้ยื่นข้อเสนอไม่ดำเนินการตามที่กำหนด ในข้อ 4.1 - 4.3 หรือไม่สามารถพิสูจน์รายละเอียดที่แตกต่างไปจากข้อกำหนดของสำนักงานได้ชัดเจน และสำนักงานไม่อาจค้นหาข้อมูลที่อ้างอิงถึงได้ ผู้ยื่นข้อเสนอจะอ้างว่าข้อมูลที่เสนอหรือที่อ้างอิงถึง มีครบถ้วนอยู่ในเอกสารที่เสนอมาแล้วไม่ได้ และหากไม่มีการอ้างอิงหรืออ้างอิงไม่ถูกต้อง หรือไม่มีข้อมูล หรือมีข้อมูลขัดแย้งไม่ตรงกัน หรือมีการจัดทำเอกสารอธิบายรายละเอียดที่แตกต่างไปจากข้อกำหนดของสำนักงาน ไม่ชัดเจนหรือคลุมเครือ และ/หรือ จำเป็นต้องใช้วิธีการพิสูจน์ทราบจากการทดสอบเป็นระยะเวลาเกินกว่า 3 วัน สำนักงานจะถือว่าการเสนอราคาในครั้งนี้ผิดเงื่อนไข ไม่ผ่านการพิจารณาข้อเสนอด้านเทคนิค

5. <u>ขอบข่ายการให้บริการ</u>

ผู้ยื่นข้อเสนอจะต้องดำเนินการจัดการบริการและอุปกรณ์ต่าง ๆ ที่เกี่ยวข้องนำมาให้บริการแก่สำนักงาน ดังนี้

5.1 ให้บริการเฝ้าระวังและป้องกันภัยคุกคามทางเครือข่ายสารสนเทศจากการวิเคราะห์ Log ของอุปกรณ์จากเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายของสำนักงาน

5.2 ผู้ยื่นข้อเสนอต้องดำเนินการและให้การสนับสนุนในการติดตั้งระบบหรืออุปกรณ์ Hardware Appliance หรือ Software ทั้งหมดที่เกี่ยวข้องกับการให้บริการเฝ้าระวังเหตุการณ์ภัยคุกคามทางไซเบอร์ และการส่งข้อมูล Log รายละเอียดตามที่สำนักงานกำหนด

5.3 ให้บริการตรวจจับข้อมูลองค์กรที่รั่วไหล โดยตรวจจับการพูดคุยของแฮกเกอร์ เพื่อระบุ ข้อมูลบัญชีหรือข้อมูลรับรอง (Credentials) ที่อาจถูกขโมยและถูกเผยแพร่ในหมู่แฮกเกอร์ และประเมินว่าองค์กรมีความอ่อนไหวต่อการโจมตีแบบเจาะจงเป้าหมาย (Targeted Attack) มากน้อยเพียงใดได้ และตรวจสอบระบบเครือข่ายองค์กรว่ามีพอร์ตที่ตั้งค่าไม่ปลอดภัยอาจถูกใช้เป็นช่องทางให้ผู้โจมตีได้

5.4 ให้บริการผู้เชี่ยวชาญทางไซเบอร์ดำเนินการให้คำแนะนำทางการตอบสนอง ระงับเหตุภัยคุกคาม พร้อมคำปรึกษาทางเทคนิคอื่นๆ ที่เกี่ยวข้อง (Incident Respond and Retainer / IRR) แบบไม่จำกัดชั่วโมง โดยผู้ให้บริการจะต้องประเมินจำนวนชั่วโมงให้ผู้ใช้บริการรับทราบและอนุมัติก่อนดำเนินการ

6. <u>รายละเอียดการติดตั้ง Log Collector สำหรับส่งข้อมูล</u>

6.1 ผู้ยื่นข้อเสนอจะติดตั้งและกำหนดค่า log collector บน VM ในรูปแบบ IaaS (Infrastructure as Service) โดยใช้ทรัพย์ยากรของผู้ว่าจ้างจัดเตรียมไว้ เช่น vCPU, Memory, Storage, Network Security Group ตามข้อกำหนดด้านความปลอดภัยสารสนเทศขององค์กร

7. <u>รายละเอียด/ข้อกำหนดคุณลักษณะเฉพาะด้าน</u>

7.1 ระบบเฝ้าระวังและป้องกันภัยคุกคามทางเครือข่ายสารสนเทศ

7.1.1 ผู้ยื่นข้อเสนอต้องให้บริการระบบจัดเก็บบันทึกข้อมูล (Log Collector) จากเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยที่ให้บริการอยู่ในระบบคลาวด์ประเภท IaaS เช่น System Log, Application Log, Security Log, Transaction Log เป็นอย่างน้อย สำหรับนำมาวิเคราะห์เพื่อการเฝ้าระวังและป้องกันภัยคุกคามทางไซเบอร์โดยผู้ยื่นข้อเสนอจะต้องเป็นผู้ติดตั้ง Software Log Collector บน Virtual Machine ที่สำนักงานจัดเตรียมไว้

7.1.2 ผู้ยื่นข้อเสนอจะต้องใช้ผลิตภัณฑ์ระบบเฝ้าระวังภัยคุกคามทางไซเบอร์ SIEM ที่อยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant for Security Information and Event Management (SIEM) ปี 2024 หรือปีล่าสุด ซึ่งสามารถรองรับการบูรณาการข้อมูลจากบริการคลาวด์

7.1.3 ผู้ยื่นข้อเสนอจะต้องสามารถวิเคราะห์ข้อมูลจากระบบคลาวด์ที่มีขนาด 100 GB/Day ได้เป็นอย่างน้อย

7.1.4 ผู้ยื่นข้อเสนอจะต้องจัดเก็บข้อมูล Log โดยมีพื้นที่จัดเก็บข้อมูลได้ไม่น้อยกว่า 90 วัน

7.1.5 ระบบจัดเก็บบันทึกข้อมูลของผู้ยื่นข้อเสนอจะต้องสามารถรองรับข้อมูล Log จากระบบปฏิบัติการ Window, Linux และแหล่งข้อมูลบนคลาวด์ได้เป็นอย่างน้อย

7.1.6 ผู้ยื่นข้อเสนอจะต้องช่วยเหลือการปรับแต่งค่าการส่งข้อมูล Log จากเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยที่ให้บริการอยู่ในระบบคลาวด์ประเภท IaaS ไปยัง Log Server ของผู้ยื่นข้อเสนอ ทั้งนี้ ระหว่างสัญญา สำนักงานคณะกรรมการส่งเสริมการลงทุนขอสงวนสิทธิ์ในการปรับเปลี่ยน เพิ่ม/ลด Log Source ได้ตามความต้องการ

7.1.7 ผู้ยื่นข้อเสนอจะต้องมีระบบ SIEM (Security Information and Event Management) ในการวิเคราะห์ภัยคุกคามทางไซเบอร์ด้วยเทคนิค Correlation, Security Analytic และการใช้ข้อมูลจากแหล่ง Threat Intelligence ในการตรวจจับภัยคุกคามทางไซเบอร์

7.1.8 ผู้ยื่นข้อเสนอจะต้องเฝ้าระวังเหตุการณ์และแจ้งเตือนภัยคุกคามทางไซเบอร์ โดยทำการวิเคราะห์ข้อมูล Log จากอุปกรณ์ที่ได้ทำการจัดเก็บ

7.1.9 ผู้ยื่นข้อเสนอจะต้องดำเนินการตอบสนองต่อภัยคุกคามทางไซเบอร์ ด้วยการวิเคราะห์หาสาเหตุ แนะนำวิธีการแก้ไข จนไปถึงประสานเพื่อแก้ไขหรือยับยั้งภัยคุกคามที่เกิดขึ้นผ่านทางอีเมลให้แก่สำนักงาน

7.1.10 ผู้ยื่นข้อเสนอต้องมีศูนย์ข้อมูล (Data Center) ที่ได้รับมาตรฐานความปลอดภัยสำหรับระบบคลาวด์ CSA STAR (Security, Trust & Assurance Registry)

7.2 ซอฟต์แวร์ป้องกันและกำจัดภัยคุกคามทางเครือข่ายสารสนเทศในรูปแบบ Endpoint Detection and Response (EDR) on Cloud

- สำหรับเครื่องคอมพิวเตอร์แม่ข่ายหรือเครื่องคอมพิวเตอร์แม่ข่ายแบบเสมือน จำนวนไม่น้อยกว่า 40 License

7.2.1 สามารถวิเคราะห์ (Analysis), ตรวจจับ (Detect), ป้องกัน (Protect), แจ้งเตือน (Alert) ภัยคุกคามจากโปรแกรมไม่พึงประสงค์ (Malware) และตอบสนอง (Response) ต่ออันตรายจากภัยคุกคามต่าง ๆ บนเครื่องคอมพิวเตอร์ปลายทาง (Endpoint) เช่น Virus, Spyware, Trojan, Phishing, Rootkit, Backdoors, Worm, Ransomware ได้เป็นอย่างน้อย

7.2.2 สามารถตรวจจับ, ป้องกัน และแจ้งเตือนอันตรายภัยต่าง ๆ จากโปรแกรมไม่พึงประสงค์ (Malware) โดยใช้เทคนิค Signature Base, Cloud Reputation หรือ Behavior Base ได้เป็นอย่างน้อย

7.2.3 สามารถติดตั้ง Agent บนเครื่องคอมพิวเตอร์ปลายทาง (Endpoint) ได้เป็นอย่างน้อยดังนี้

- Windows 10, Windows 11
- Windows Server 2008R2 SP1, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022
- Linux: AlmaLinux, Rocky Linux, RHEL, Debian, Ubuntu, Fedora, SUSE

7.2.4 สามารถจัดลำดับความรุนแรงของภัยคุกคาม (Severity) และแสดงรายละเอียดของภัยคุกคามพร้อมทั้งสรุปผลที่เกิดขึ้นโดยรองรับ MITRE ATT&CK framework ได้เป็นอย่างน้อย

7.2.5 มีระบบปัญญาประดิษฐ์ (AI) หรือ Playbook หรือ workflow เพื่อช่วยสำหรับการตรวจสอบรวบรวมสรุปผลของภัยคุกคามที่เกิดขึ้นและแสดงหลักฐานจากแหล่งต่าง ๆ ได้โดยอัตโนมัติ

7.2.6 สามารถอัพเดตฐานข้อมูลของ Malware หรือ Machine Learning ได้จากเครื่อง Centralized Management, Internet หรือ Cloud console

7.2.7 สามารถแสดงข้อมูลรายละเอียดของภัยคุกคามในรูปแบบของกราฟโดยแสดงถึงความสัมพันธ์ของการโจมตีต่าง ๆ ได้

7.2.8 สามารถย้อนกลับการเปลี่ยนแปลงที่ทำโดย Malware และส่งคืนระบบกลับสู่สถานะปกติบนเครื่องคอมพิวเตอร์ลูกข่ายโดยอัตโนมัติได้ หรือ ทำการ Connect to host เพื่อทำการ response ปัญหาจากทางระยะไกลได้

7.2.9 สามารถทำการค้นหาและตรวจสอบข้อมูลบนเครื่องคอมพิวเตอร์แม่ข่ายจากศูนย์กลาง เช่น File Hash, Process, Registry, Service, Network Connection, WMI Activity ได้

7.2.10 สามารถทำการค้นหาและตรวจสอบข้อมูลภัยคุกคามที่เกิดขึ้นบนเครื่องคอมพิวเตอร์แม่ข่ายจากศูนย์กลางแบบย้อนหลัง (Historical) ได้ไม่น้อยกว่า 90 วัน

7.2.11 สามารถสั่งให้เครื่องคอมพิวเตอร์แม่ข่ายปฏิบัติตามคำสั่งที่ต้องการจากศูนย์กลางได้ เช่น Remove file, Kill Process, Reboot OS, User Logoff ได้

7.2.12 สามารถสั่งกักกันเครื่องคอมพิวเตอร์ที่มีความเสี่ยงจากภัยคุกคามออกจากระบบเครือข่าย (Quarantine) เพื่อป้องกันและควบคุมการแพร่กระจายของ Unknown malware ได้

7.2.13 มีระบบ Threat Intelligence หรือทำงานร่วมกับระบบอื่นๆ เพื่อให้สามารถแจ้งเตือนถึงภัยคุกคามที่เกิดขึ้นได้โดยอัตโนมัติได้

7.2.14 ระบบต้องสามารถตรวจสอบ hash ต้องสงสัยที่ detect ได้กับ Threat Intelligent ภายนอก เช่น Virus Total ได้เป็นอย่างน้อย

7.2.15 สามารถแสดงการทำงานของ Malware ในรูปแบบของกราฟได้ โดยแสดงถึงจุดเริ่มต้น ช่วงระยะเวลาและรายละเอียดของการทำงานเพื่อให้ผู้ดูแลระบบทำความเข้าใจกับการคุกคามและตอบสนองได้เร็วขึ้น

7.2.16 สามารถควบคุมการใช้งานอุปกรณ์ต่อพ่วง (Device Control) เช่น Removable drive และ USB Drives

7.2.17 มีระบบตรวจสอบอุปกรณ์ที่ติดตั้ง Agent ในระบบ หรือ อุปกรณ์ที่ไม่มี Agent ในระบบ (Rogue System Detection)

7.2.18 สามารถทำการเปรียบเทียบนโยบาย (Comparison Policy) หรือ สามารถย้อนกลับนโยบาย Revert policy ได้จากหน้าบริหารจัดการ หรือ สามารถตรวจสอบ Prevention Policy หรือ สามารถตรวจสอบ Policy ได้จากหน้า Management Console

7.2.19 สามารถบริหารจัดการนโยบายของระบบที่เสนอได้จากจุดเดียว (Centralized Management) และสามารถส่งคำสั่งลบ โปรแกรมป้องกันความปลอดภัย หรือ Agent หรือ ส่งคำสั่ง Power Shell ไปยัง เครื่องปลายทางได้

7.2.20 ระบบ EDR ต้องสามารถติดตั้ง Agent บนเครื่อง VM หรือ Instance ที่อยู่ในสภาพแวดล้อมคลาวด์รูปบบ IaaS ได้

7.2.21 ผลิตภัณฑ์ที่นำเสนอต้องได้รับการจัดอันดับให้อยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant ในกลุ่มผลิตภัณฑ์ Endpoint Protection Platform (EEP) ประจำปี 2025

7.3 ศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยสารสนเทศ (Security Operation Center: SOC)
ผู้ยื่นข้อเสนอต้องจัดให้มีศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยสารสนเทศ (SOC) โดยมีคุณสมบัติอย่างน้อยดังนี้

7.3.1 ต้องให้บริการเฝ้าระวังและวิเคราะห์ความเชื่อมโยงของเหตุการณ์ภัยคุกคามทางไซเบอร์จากข้อมูล Log ของ Log Source ต่างๆ ของ สำนักงานคณะกรรมการส่งเสริมการลงทุนตลอด 24x7

7.3.2 ต้องมีห้องเฉพาะ (Dedicated Room) สำหรับเป็นศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยสารสนเทศ (Cybersecurity Operations Center) ที่ผ่านการรับรองตามมาตรฐานสากล ISO/IEC 27001:2022

7.3.3 ต้องได้รับการรับรองตามมาตรฐานการบริหารความต่อเนื่องทางธุรกิจ ISO 22301 Business Continuity Management Systems

7.3.4 ต้องได้รับรองตามมาตรฐานระบบการจัดการงานบริการด้านเทคโนโลยีสารสนเทศ ISO 20000-1 Service Management System

7.3.5 ต้องมีระบบ Biometric Access Control สำหรับควบคุมการเข้า-ออก ของเจ้าหน้าที่และมีการเก็บวันเวลาเข้า - ออก ไม่น้อยกว่า 90 วัน

7.3.6 ต้องมีระบบ CCTV สามารถบันทึกและดูภาพย้อนหลังได้ไม่น้อยกว่า 90 วัน

7.4 ผู้เชี่ยวชาญด้าน Cyber Security จำนวน 6 คน

ผู้ยื่นข้อเสนอต้องมีทีมผู้เชี่ยวชาญด้าน Cyber Security โดยมีคุณสมบัติอย่างน้อย ดังนี้

7.4.1 ผู้จัดการโครงการ จำนวน 1 คน มีคุณสมบัติ ดังนี้

7.4.1.1 มีประสบการณ์ในตำแหน่งผู้จัดการโครงการที่เกี่ยวกับศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางด้านความปลอดภัยสารสนเทศ หรือตำแหน่งที่เกี่ยวข้อง ไม่น้อยกว่า 5 ปี

7.4.1.2 คุณวุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรีในสาขาเทคโนโลยีสารสนเทศ หรือวิศวกรรมคอมพิวเตอร์ หรือที่เกี่ยวข้อง

7.4.1.3 ได้รับประกาศนียบัตรรับรองคุณวุฒิด้านความปลอดภัยสารสนเทศ Certified Information Systems Security Professional (CISSP) หรือ Certified Information Security Manager (CISM)

7.4.2 ผู้บัญชาการหรือหัวหน้าหน่วยงานศูนย์เฝ้าระวังภัยคุกคาม (CSOC Lead) จำนวน 1 คน มีคุณสมบัติดังนี้

7.4.2.1 คุณวุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรีในสาขาเทคโนโลยีสารสนเทศ หรือวิศวกรรมคอมพิวเตอร์ หรือที่เกี่ยวข้อง

7.4.2.2 มีประสบการณ์ทำงานในศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางด้านความปลอดภัยสารสนเทศในตำแหน่ง Security Analyst หรือสูงกว่ามาแล้วไม่น้อยกว่า 3 ปี

7.4.2.3 ได้รับประกาศนียบัตรรับรองคุณวุฒิมีประกาศนียบัตรด้านความปลอดภัยสารสนเทศ GIAC Certified Incident Handler Certification (GCIH) หรือ Assessing Information Security Risk using the OCTAVE Approach หรือ Certified Information Security Manager (CISM)

7.4.3 ผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยต่อภัยคุกคามไซเบอร์ ระดับ 3 จำนวน 1 คน มีคุณสมบัติ ดังนี้

7.4.3.1 มีประสบการณ์ทำงานในศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางด้านความปลอดภัยสารสนเทศในตำแหน่ง Security Analyst หรือ Digital forensic ปฏิบัติหน้าที่ทำการวิเคราะห์ Root cause analysis และ Digital forensic มาแล้วไม่น้อยกว่า 3 ปี

7.4.3.2 คุณวุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรีในสาขาเทคโนโลยีสารสนเทศ หรือวิศวกรรมคอมพิวเตอร์ หรือที่เกี่ยวข้อง

7.4.3.3 ได้รับประกาศนียบัตรรับรองคุณวุฒิด้านความปลอดภัยสารสนเทศ GIAC Certified Forensic Analyst (GCFA) หรือ EC-Council: CEH (Certified Ethical Hacker)

7.4.4 ผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยต่อภัยคุกคามไซเบอร์ ระดับ 2 จำนวน 1 คน มีคุณสมบัติ ดังนี้

7.4.4.1 มีประสบการณ์ทำงานในศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางด้านความปลอดภัยสารสนเทศในตำแหน่ง Security Analyst มาแล้วไม่น้อยกว่า 3 ปี

7.4.4.2 คุณวุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรีในสาขาเทคโนโลยีสารสนเทศ หรือวิศวกรรมคอมพิวเตอร์ หรือที่เกี่ยวข้อง

7.4.4.3 ได้รับประกาศนียบัตรรับรองคุณวุฒิด้านความปลอดภัยสารสนเทศ EC-Council Certified Security Analyst (ECSA) หรือ Certified CompTIA Cybersecurity Analyst (CySA+) หรือ CompTIA Advanced Security Practitioner (CASP+) หรือ Certified Ethical Hacker (CEH)

7.4.5 ผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยต่อภัยคุกคามไซเบอร์ ระดับ 1 จำนวนไม่น้อยกว่า 2 คน มีคุณสมบัติ ดังนี้

7.4.5.1 คุณวุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรีในสาขาเทคโนโลยีสารสนเทศ หรือวิศวกรรมคอมพิวเตอร์ หรือที่เกี่ยวข้อง

7.4.5.2 มีประสบการณ์ทำงานในศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางด้านความปลอดภัยสารสนเทศในตำแหน่ง Security Analyst มาแล้วไม่น้อยกว่า 2 ปี

7.4.5.3 ได้รับประกาศนียบัตรรับรองคุณวุฒิด้านความปลอดภัยสารสนเทศ Certified CompTIA Security + หรือ ISC2: Certified in Cybersecurity Certification (CC) หรือเทียบเท่า

7.4.5.4 เจ้าหน้าที่ปฏิบัติงาน ณ ศูนย์เฝ้าระวังภัยคุกคาม (CSOC) ของผู้ยื่นข้อเสนอตลอด 24 ชั่วโมง

7.4.6 เอกสารหลักฐาน ตารางเปรียบเทียบ เพื่อยืนยันว่ามีผู้เชี่ยวชาญด้าน Cyber Security ที่มีคุณสมบัติตรงตามขอบเขตงาน (Term of Reference: TOR) ข้อ 7.4.1-7.4.5 โดยไม่ระบุรายชื่อของผู้เชี่ยวชาญ

ตัวอย่าง :

เจ้าหน้าที่ปฏิบัติงาน	คุณสมบัติ	บริษัท ตัวอย่าง จำกัด
1. ผู้จัดการโครงการ จำนวน 1 คน	- มีประสบการณ์ในตำแหน่งผู้จัดการโครงการที่เกี่ยวกับศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางด้านความปลอดภัยสารสนเทศ หรือตำแหน่งที่เกี่ยวข้อง ไม่น้อยกว่า 5 ปี - คุณวุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรีในสาขาเทคโนโลยีสารสนเทศ หรือวิศวกรรมคอมพิวเตอร์ หรือที่เกี่ยวข้อง - ได้รับประกาศนียบัตรรับรองคุณวุฒิด้านความปลอดภัยสารสนเทศ Certified Information Systems Security Professional (CISSP) หรือ Certified Information Security Manager (CISM)	ยืนยันสามารถทำตามขอบเขตงานได้
2.		

7.5 การตรวจสอบช่องโหว่ (Vulnerability Assessment : VA Scan) เพื่อตรวจสอบหาช่องโหว่ที่เกิดขึ้นกับระบบ โดยมีรายละเอียดในบริการ VA Scan อย่างน้อยดังนี้

7.5.1 ให้บริการตรวจสอบช่องโหว่สำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการอยู่ในระบบคลาวด์ประเภท IaaS ได้ไม่น้อยกว่า 5 IP ได้เป็นอย่างน้อย

7.5.2 ต้องใช้โปรแกรมที่มีลิขสิทธิ์ถูกกฎหมาย ในการทำ Vulnerability Assessment

7.5.3 สามารถตรวจสอบช่องโหว่ของอุปกรณ์บนระบบเครือข่ายได้ทั้งเครือข่ายสาธารณะ (Public) และเครือข่ายภายใน (Private)

7.5.4 สามารถตรวจสอบช่องโหว่ของระบบปฏิบัติการหรือบริการด้านระบบเครือข่ายได้อย่างน้อยดังนี้ ระบบปฏิบัติการด้านคอมพิวเตอร์ (Operating System) เช่น Windows OS หรือ Linux OS

7.5.5 รองรับการ scan ทั้งแบบ Non Credential Scan และ Credential Scan ได้

7.5.6 สามารถสร้างรายงานได้หลายรูปแบบ เช่น Executive Summary หรือ แบบแยกตาม Host หรือ Plugin

7.5.7 จัดทำรายงานผลการวิเคราะห์และตรวจสอบช่องโหว่ ในรูปแบบเอกสารไฟล์ดิจิทัล โดยมีรายละเอียดของรายงานอย่างน้อยดังนี้

(1) รายงานสรุปภาพรวมของการตรวจสอบ

(2) ระบุการจัดระดับความรุนแรง (Severity) หรือผลกระทบที่อาจจะเกิดจากช่องโหว่ที่พบ

(3) รายละเอียดช่องโหว่ที่ตรวจสอบพบของแต่ละอุปกรณ์ โดยจัดเรียงตามระดับความรุนแรงหรือผลกระทบที่อาจจะเกิดจากช่องโหว่ดังกล่าว

(4) คำแนะนำและขั้นตอนในการแก้ไข (Action & Recommendation)

(5) รายงานจะต้องมีการอ้างอิงกับ CVSS และ CVE และมีการระบุ Severity ของช่องโหว่ที่พบ

8. รายละเอียด/ข้อกำหนดคุณลักษณะอื่นๆ

8.1 ผู้ยื่นข้อเสนอต้องซ่อมแซม/ปรับปรุงสิ่งก่อสร้างของสำนักงานที่ได้รับผลกระทบ หรือเกิดความเสียหายจากการดำเนินงานของผู้ยื่นข้อเสนอให้กลับคืนสู่สภาพดีดังเดิม โดยค่าใช้จ่ายที่เกิดขึ้นทั้งหมดผู้ยื่นข้อเสนอต้องเป็นผู้รับผิดชอบ

8.2 ค่าจ้างเหมาเฝ้าระวังและป้องกันภัยคุกคามทางเครือข่ายสารสนเทศตามขอบเขตงานนี้ ให้ครอบคลุมถึงค่าแรงงาน ค่าอะไหล่ ค่าอุปกรณ์สิ่งของที่ต้องเปลี่ยน ค่าเดินสายสัญญาณใหม่ ค่าปรับปรุงการตั้งค่าอุปกรณ์ โดยสำนักงานจะไม่เสียค่าใช้จ่ายใด ๆ เพิ่มเติม

8.3 ผู้ยื่นข้อเสนอต้องทำการเฝ้าระวัง วิเคราะห์ และแจ้งเตือนภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ พร้อมให้บริการคำปรึกษา แนะนำวิธีการแก้ไข จนไปถึงประสานงานเพื่อแก้ไขหรือยับยั้งภัยคุกคามที่เกิดขึ้นตลอด 24 ชั่วโมง ผ่านทางโทรศัพท์หรืออีเมล เป็นอย่างน้อย

8.4 ผู้ยื่นข้อเสนอต้องดำเนินการแจ้งเตือนเมื่อเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ตาม Service Level Agreement (SLA) ที่ สำนักงานคณะกรรมการส่งเสริมการลงทุน กำหนด รวมทั้งให้คำแนะนำทางเทคนิค

ในการรับมือตอบสนองเหตุการณ์ภัยคุกคามดังกล่าวแก่ สำนักงานคณะกรรมการส่งเสริมการลงทุน ตลอดระยะเวลาสัญญา ตามเงื่อนไข SLA ดังนี้

ระดับความรุนแรง	ผลกระทบ	เวลาในการแจ้งเตือน นับจากเกิดเหตุ	เวลาในการให้คำแนะนำแก้ไขปัญหา นับจากเกิดเหตุ
สูงมาก (Critical)	การดำเนินการหยุดชะงัก และจำเป็นต้องแก้ไขอย่างเร่งด่วนที่สุด	ภายใน 15 นาที	ภายใน 30 นาที
สูง (High)	ธุรกิจไม่สามารถดำเนินการได้อย่างมีประสิทธิภาพ และจำเป็นต้องแก้ไขอย่างเร่งด่วน	ภายใน 30 นาที	ภายใน 2 ชั่วโมง
ปานกลาง (Medium)	กระทบต่อการดำเนินธุรกิจ และมีความจำเป็นต้องแก้ไขอย่างทันท่วงที	ภายใน 2 ชั่วโมง	ภายใน 6 ชั่วโมง
ต่ำ (Low)	ไม่กระทบต่อประสิทธิภาพการทำงานทั่วไป และ ไม่มีผลกระทบต่อการดำเนินธุรกิจโดยภาพรวม	ภายใน 6 ชั่วโมง	ภายใน 24 ชั่วโมง

8.5 การแจ้งเตือนเหตุการณ์ภัยคุกคามทางไซเบอร์ตาม SLA ต้องครอบคลุมเนื้อหาอย่างน้อยดังนี้

(1) กำหนดหมายเลขเหตุการณ์ภัยคุกคาม (Incident Number)

(2) ระบุประเภทของภัยคุกคาม

(3) วัน-เวลา เริ่มต้นและสิ้นสุดของภัยคุกคาม

(4) ระบุต้นทาง (Source หรือ Attacker) และปลายทาง (Destination หรือ Target)

(5) ระดับความรุนแรงตาม SLA (Severity)

(6) รายละเอียดเหตุการณ์และพฤติกรรม

(7) ระบุตัวบ่งชี้การโจมตี (Indicator of Attack : IOA) หรือตัวบ่งชี้การถูกโจมตี (Indicator of Compromise : IOC) (ถ้ามี)

(8) สิ่งที่ควรดำเนินการเป็นลำดับแรก (First Action)

9. <u>เงื่อนไขอื่น ๆ</u>

ผู้ยื่นข้อเสนอต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ นโยบายคุ้มครองข้อมูลส่วนบุคคล และประมวลแนวทางปฏิบัติและกรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานคณะกรรมการส่งเสริมการลงทุน รวมถึงกฎหมาย นโยบาย คำสั่งและขั้นตอนปฏิบัติอื่น ๆ ที่เกี่ยวข้อง

10. <u>หลักเกณฑ์ในการพิจารณาผล</u>

10.1 สำนักงานจะพิจารณาโดยใช้เกณฑ์ราคา (Price)

10.2 ผู้ยื่นข้อเสนอจะต้องยื่นเอกสารหลักฐานตาม TOR ดังต่อไปนี้

- ข้อ 7.1.2 ผู้ยื่นข้อเสนอจะต้องใช้ผลิตภัณฑ์ระบบเฝ้าระวังภัยคุกคามทางไซเบอร์ SIEM ที่อยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant for Security Information and Event Management (SIEM) ปี 2024 หรือปีล่าสุด ซึ่งสามารถรองรับการบูรณาการข้อมูลจากบริการคลาวด์

- ข้อ 7.1.10 ผู้ยื่นข้อเสนอต้องมีศูนย์ข้อมูล (Data Center) ที่ได้รับมาตรฐานความปลอดภัยสำหรับระบบคลาวด์ CSA STAR (Security, Trust & Assurance Registry)

- ข้อ 7.2.21 ผลิตภัณฑ์ที่นำเสนอต้องได้รับการจัดอันดับให้อยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant ในกลุ่มผลิตภัณฑ์ Endpoint Protection Platform (EEP) ประจำปี 2025

- ข้อ 7.3.2 ต้องมีห้องเฉพาะ (Dedicated Room) สำหรับเป็นศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยสารสนเทศ (Cybersecurity Operations Center) ที่ผ่านการรับรองตามมาตรฐานสากล ISO/IEC 27001:2022

- ข้อ 7.3.3 ต้องได้รับการรับรองตามมาตรฐานการบริหารความต่อเนื่องทางธุรกิจ ISO 22301 Business Continuity Management Systems

- ข้อ 7.3.4 ต้องได้รับรองตามมาตรฐานระบบการจัดการงานบริการด้านเทคโนโลยีสารสนเทศ ISO 20000-1 Service Management System

10.3 กรณีที่ผู้ยื่นข้อเสนอยื่นเอกสารไม่ถูกต้องหรือไม่ครบถ้วนตามข้อกำหนด TOR สำนักงานขอสงวนสิทธิ์ไม่รับพิจารณาเอกสารของผู้ยื่นข้อเสนอรายนั้น เว้นแต่เป็นข้อผิดพลาดหรือผิดหลงเพียงเล็กน้อย หรือที่ผิดไปจากเงื่อนไขและขอบเขตของงานตามเอกสารนี้ ในส่วนที่มิใช่สาระสำคัญ ทั้งนี้ เฉพาะในกรณีที่พิจารณาเห็นว่าเป็นประโยชน์ต่อทางราชการเท่านั้น

10.4 ผู้ยื่นข้อเสนอจะต้องผ่านการพิจารณารายละเอียดทางด้านเทคนิคครบถ้วน จึงจะสามารถได้รับสิทธิในการพิจารณาด้านราคา

10.5 สำนักงานคงไว้ซึ่งสิทธิ์ที่จะยกเลิกข้อเสนอโดยไม่พิจารณาจัดจ้างก็ได้หรือเจรจาต่อรองสอบถามรายละเอียดเพิ่มเติมก็ได้ ทั้งนี้เพื่อประโยชน์ของทางราชการเป็นสำคัญและให้ถือว่าการตัดสินของสำนักงาน เป็นที่สิ้นสุด

10.6 สำนักงานมีสิทธิ์พิจารณายกเลิกการยื่นข้อเสนอ และลงโทษผู้ยื่นข้อเสนอเสมือนเป็นผู้ทิ้งงาน หากมีเหตุที่เชื่อได้ว่าการยื่นข้อเสนอกระทำไปโดยไม่สุจริต หรือมีการสมยอมกันในการยื่นข้อเสนอ

10.7 ในกรณีที่ผู้ยื่นข้อเสนอ เสนอราคาต่ำจนคาดหมายว่าไม่อาจดำเนินงานตามสัญญาได้ สำนักงานจะให้ผู้รับจ้างนั้น ชี้แจงและแสดงหลักฐานที่ทำให้เชื่อได้ว่า ผู้ยื่นข้อเสนอสามารถดำเนินงานตามโครงการนี้ได้เสร็จสมบูรณ์ หากคำชี้แจงไม่มีเหตุผลที่อาจรับฟังได้ สำนักงานมีสิทธิ์ที่จะไม่รับราคาของผู้ยื่นข้อเสนอและลงโทษผู้เสนอราคาเสมือนเป็นผู้ทิ้งงาน

11. <u>การส่งมอบงานและการตรวจรับ</u>

11.1 ผู้ยื่นข้อเสนอจะต้องเฝ้าระวังและป้องกันภัยคุกคามทางเครือข่ายสารสนเทศพร้อมทั้งจัดทำรายงานสรุปเหตุการณ์ภัยคุกคามทางไซเบอร์เป็นประจำทุกเดือนตลอดอายุสัญญาในรูปแบบไฟล์ PDF จำนวน 1 ชุด ผ่านทางอีเมลล์ ภายในวันที่ 15 ของเดือนถัดไป

11.2 ผู้ยื่นข้อเสนอจะต้องจัดทำรายงานตรวจสอบการทำงานของระบบป้องกันและกำจัดไวรัสเป็นประจำทุกเดือนตลอดอายุสัญญาในรูปแบบไฟล์ PDF จำนวน 1 ชุด ผ่านทางอีเมลล์ ภายในวันที่ 15 ของเดือนถัดไป ดังรายการดังต่อไปนี้

11.2.1 รายงานการตรวจสอบรายการเครื่องคอมพิวเตอร์และอุปกรณ์ที่เชื่อมต่อเข้ากับระบบควบคุมโปรแกรมป้องกันไวรัสแบบรวมศูนย์ หากพบเครื่องคอมพิวเตอร์หรืออุปกรณ์ ที่ไม่อยู่ในสถานะ Active หรือ Error หรืออื่นๆ ให้ดำเนินการตรวจสอบแก้ไขให้อยู่ในสถานะพร้อมใช้งานเป็นประจำทุกเดือน

11.2.2 รายงาน Version ของโปรแกรมป้องกันไวรัส โดยระบุถึง Version ล่าสุด ณ เดือนนั้นๆ ของโปรแกรม และจำนวนของโปรแกรมป้องกันไวรัสที่ได้มีการติดตั้งบนเครื่องคอมพิวเตอร์ โดยระบุถึง Version ที่ใช้งานอยู่

11.2.3 รายงานสรุปผลจำนวน Malware ที่โจมตีและเครื่องคอมพิวเตอร์ที่ติด Malware ภายใน 15 วัน ของเดือนถัดไป ตามรูปแบบที่สำนักงานกำหนด

11.3 ผู้ยื่นข้อเสนอจะต้องส่งมอบรายงานรูปแบบเอกสารตรวจรับตามงวดงานจำนวน 1 ชุด โดยประกอบด้วยรายงานประจำเดือนตามงวดงาน ตามข้อ 11.1 และ 11.2 ภายใน 15 วันของเดือนถัดไป หรือตามที่สำนักงานกำหนด

12. <u>การจ่ายเงิน</u>

สำนักงานจะชำระเงินค่าจ้างทั้งหมด 4 งวด โดยต้องส่งมอบเอกสารหลักฐานการปฏิบัติงานภายใน 15 วัน นับถัดจากวันครบกำหนดในแต่ละงวดงานให้กับสำนักงานและคณะกรรมการตรวจรับพัสดุได้รวจรับเรียบร้อยแล้ว ดังนี้

<u>งวดที่ 1</u> จำนวนร้อยละ 25% ของราคาจ้างทั้งหมด ภายใน 3 เดือนนับถัดจากวันลงนามในสัญญา โดยมีรายละเอียดดัง ข้อ 11. การส่งมอบงานและการตรวจรับ

<u>งวดที่ 2</u> จำนวนร้อยละ 25% ของราคาจ้างทั้งหมด ภายใน 6 เดือนนับถัดจากวันลงนามในสัญญา โดยมีรายละเอียดดัง ข้อ 11. การส่งมอบงานและการตรวจรับ

<u>งวดที่ 3</u> จำนวนร้อยละ 25% ของราคาจ้างทั้งหมด ภายใน 9 เดือนนับถัดจากวันลงนามในสัญญา โดยมีรายละเอียดดัง ข้อ 11. การส่งมอบงานและการตรวจรับ

<u>งวดที่ 4</u> จำนวนร้อยละ 25% ของราคาจ้างทั้งหมด ภายใน 12 เดือนนับถัดจากวันลงนามในสัญญา โดยมีรายละเอียดดัง ข้อ 11. การส่งมอบงานและการตรวจรับ

13. <u>วงเงินในการจัดหา</u>

วงเงินในการจัดจ้างจำนวน 1,940,000 บาท (หนึ่งล้านเก้าแสนสี่หมื่นบาทถ้วน)

14. <u>การส่งเสริมหรือสนับสนุนผู้ประกอบการวิสาหกิจขนาดกลางและขนาดย่อม (SMEs) และพัสดุที่ผลิตภายในประเทศ</u>

14.1 สำเนาใบทะเบียนผู้ประกอบวิสาหกิจขนาดกลางและขนาดย่อม (SMEs) (ถ้ามี)

14.2 ผู้ยื่นข้อเสนอที่เป็นผู้ชนะการเสนอราคาต้องจัดทำแผนการใช้พัสดุที่ผลิตภายในประเทศ โดยยื่นให้สำนักงานภายใน 60 วันนับถัดจากวันลงนามในสัญญา

15. <u>ค่าปรับ</u>

15.1 ในกรณีเกิดเหตุขัดข้องจากโปรแกรมป้องกันไวรัสจนไม่สามารถใช้งานได้ ผู้ยื่นข้อเสนอจะต้องแก้ไขให้สามารถกลับมาใช้งานภายใต้ระดับความรุนแรง ตามรายละเอียดดังนี้

15.1.1 เกิดข้อผิดพลาด/บกพร่องของระบบขั้นรุนแรงมาก และส่งผลกระทบต่อการทำงานของบริการอื่นๆ ต้องหยุดชะงักหรือไม่สามารถให้บริการได้ ซึ่งจำเป็นต้องได้รับการแก้ไขโดยด่วนที่สุด อาทิ โปรแกรม Antivirus ส่งสัญญาณทราฟฟิคจำนวนมากจนส่งผลให้ไม่สามารถใช้งานระบบ Internet ของสำนักงานได้ จะต้องมีการ Response time ภายในระยะเวลา 30 นาที และ Recovery time ภายในระยะเวลา 4 ชั่วโมง

15.1.2 เกิดข้อผิดพลาด/บกพร่องของระบบขั้นรุนแรงปานกลาง และส่งผลกระทบต่อกิจกรรมที่สำคัญและจำเป็นต่อการดำเนินธุรกิจ ส่งผลให้ธุรกิจไม่สามารถดำเนินการได้อย่างมีประสิทธิภาพ และจำเป็นจะต้องแก้ไขอย่างเร่งด่วน อาทิ เครื่องคอมพิวเตอร์ลูกข่ายหรือเครื่องคอมพิวเตอร์แม่ข่ายที่ติดตั้งโปรแกรม Antivirus อยู่ไม่สามารถทำงานได้ จะต้องมีการ Response time ภายในระยะเวลา 2 ชั่วโมง และ Recovery time ภายในระยะเวลา 8 ชั่วโมง

15.1.3 เกิดข้อผิดพลาด/บกพร่องของระบบขั้นต่ำ แต่ไม่มีผลกระทบต่อการดำเนินธุรกิจโดยภาพรวม อาทิ ระบบการทำงานของโปรแกรม Antivirus ทำงานไม่เสถียร (ไม่มีผลต่อการให้บริการ) จะต้องมีการ Response time ภายในระยะเวลา 4 ชั่วโมง และ Recovery time ภายในระยะเวลา 12 ชั่วโมง

15.2 เมื่อพ้นกำหนด Recovery time ตามข้อ 15.1 แล้ว สำนักงานขอสงวนสิทธิ์ในการปรับต่อวัน ในอัตราร้อยละ 0.10 ของราคาทั้งหมดตามสัญญา (โดยเศษของชั่วโมงให้นับเป็นหนึ่งวัน)

15.3 กรณีที่ไม่สามารถติดตั้งระบบควบคุมโปรแกรมป้องกันไวรัสแบบรวมศูนย์ และโปรแกรมป้องกันไวรัส ตามข้อ 15.1 ได้ทันตามเวลาที่กำหนด สำนักงานขอสงวนสิทธิ์ในการปรับต่อวัน ในอัตราร้อยละ 0.10 ของราคาทั้งหมดตามสัญญา (โดยเศษของชั่วโมงให้นับเป็นหนึ่งวัน)

15.4 กรณีผู้ยื่นข้อเสนอไม่ส่งมอบงานภายในระยะเวลาที่สำนักงานกำหนด จะปรับในอัตราร้อยละ 0.10 ต่อวัน จากราคาทั้งหมดตามสัญญา ไปจนกระทั่งผู้ยื่นข้อเสนอส่งมอบงาน

15.5 ในกรณีที่เกิดเหตุขัดข้องจนเป็นเหตุให้ไม่สามารถให้บริการได้ ผู้ยื่นข้อเสนอจะต้องดำเนินการตรวจสอบและแก้ไขข้อขัดข้องให้อยู่ในสภาพใช้งานได้ดีตามเดิมภายในระยะเวลา 4 ชั่วโมง นับตั้งแต่ได้รับแจ้งเหตุขัดข้องจากสำนักงาน โดยดำเนินการแก้ไขระบบหรืออุปกรณ์หรือวงจรสื่อสาร หากไม่สามารถแก้ไขได้ภายในเวลาที่กำหนด สำนักงานจะปรับในอัตราร้อยละ 0.10 ต่อวัน จากราคาทั้งหมดตามสัญญา โดยเศษของวันให้นับเป็น 1 วัน ไปจนกว่าจะแก้ไขข้อขัดข้องให้อยู่ในสภาพใช้งานได้ดีตามเดิม

15.6 กรณีอื่นๆ ที่ไม่ได้กล่าวถึงค่าปรับในที่นี้ หากคณะกรรมการพิจารณาแล้วเห็นว่า ผู้เสนอราคาไม่ปฏิบัติตามรายละเอียดที่ระบุไว้ในสัญญาและก่อให้เกิดความเสียหายกับสำนักงาน สำนักงานขอสงวนสิทธิ์ในการปรับต่อวัน ในอัตราร้อยละ 0.10 ของราคาทั้งหมดตามสัญญา (โดยเศษของชั่วโมงให้นับเป็นหนึ่งวัน) ไปจนกว่าจะดำเนินการได้ถูกต้องตามที่กำหนด

15.7 สำนักงานมีสิทธิหักค่าปรับจากเงินงวดที่สำนักงานยังไม่ได้จ่าย ไม่ว่าพฤติการณ์ที่ก่อให้เกิดค่าปรับ จะเป็นค่าปรับของเงินงวดที่ค้างหรือไม่ก็ได้

16. <u>เอกสารที่ผู้รับจ้างต้องส่งมอบก่อนลงนามในสัญญา</u>

ผู้ยื่นข้อเสนอต้องส่งรายชื่อผู้เชี่ยวชาญด้าน Cyber Security ที่มีคุณสมบัติตรงตามขอบเขตงาน (Term of Reference: TOR) ข้อ 7.4 ผู้เชี่ยวชาญด้าน Cyber Security จำนวน 6 คน และจัดทำรายชื่อของผู้เชี่ยวชาญรายละเอียดด้านการศึกษา ประสบการณ์ทำงาน รวมถึงหลักฐานต่างๆ ที่เกี่ยวข้อง และส่งมอบให้สำนักงานก่อนลงนามในสัญญา

17. <u>ระยะเวลาในการทำงาน</u>

12 เดือน นับถัดจากวันลงนามในสัญญา หรือวันที่ได้รับแจ้งจากสำนักงานให้เริ่มดำเนินงาน

18. <u>แผนการทำงาน</u>

"คู่สัญญาต้องจัดทำแผนการทำงานมาให้ภายใน 10 วัน นับถัดจากวันลงนามในสัญญา" เว้นแต่เป็นกรณีการเช่า หรือสัญญาอายุไม่เกิน 90 วัน หรือกรณีการซื้อซึ่งสัญญากำหนดส่งงานงวดเดียว หรือกรณีการซื้อ การเช่า การจ้าง และการจ้างก่อสร้าง ซึ่งสัญญาหรือบันทึกข้อตกลงเป็นหนังสือมีวงเงินไม่เกิน 500,000.00 บาท โดยจัดทำแผนการทำงานตามสิ่งที่ส่งมาด้วย ทั้งนี้ แผนการทำงานดังกล่าวให้ถือเป็นเอกสารส่วนหนึ่งของสัญญา

19. <u>การสงวนสิทธิ์</u>

กรณีมีปัญหาใดๆ เกิดขึ้น ทั้งในช่วงการพิจารณาข้อเสนอ และดำเนินงานต่าง ๆ ภายหลังจากได้ทำสัญญากับผู้ยื่นข้อเสนอแล้ว สำนักงานสงวนสิทธิ์ในการตัดสินวินิจฉัยชี้ขาดปัญหาที่เกิดขึ้นดังกล่าว และให้ถือว่าคำวินิจฉัยของสำนักงานข้างต้นเป็นที่สิ้นสุดเด็ดขาดแล้ว ผู้ยื่นข้อเสนอต้องยอมรับคำวินิจฉัยดังกล่าวโดยจะไม่โต้แย้ง หรือมีข้อแม้ใดๆ ทั้งสิ้น

ทั้งนี้สำนักงานจะถือว่าผู้ยื่นข้อเสนอได้รับทราบ เข้าใจ และยอมรับในรายละเอียดต่าง ๆ ที่สำนักงานกำหนดในเอกสารขอบเขตของงาน (TOR) เป็นที่เรียบร้อยแล้ว

20. <u>สถานที่ติดต่อสอบถามข้อมูลเพิ่มเติม</u>

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ชั้น 2 สำนักงานคณะกรรมการส่งเสริมการลงทุน 555 ถนนวิภาวดีรังสิต แขวงจตุจักร เขตจตุจักร กรุงเทพมหานคร 10900 โทรศัพท์ 0 2553 8111 ต่อ 8395 หรือ 8492 E-Mail: pongpon@boi.go.th และ nattapat@boi.go.th