ร่าง

รายละเอียดคุณลักษณะเฉพาะ
ของโครงการจัดซื้อระบบรักษาความมั่นคงปลอดภัยสำหรับเครือข่ายสารสนเทศเพื่อการพัฒนาการศึกษา
ประจำปีงบประมาณ พ.ศ. 2567

---

1. ความเป็นมา

การดำเนินงานบริการสารสนเทศหรือยุคดิจิทัลในปัจจุบันนั้น ศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศถือเป็นสิ่งสำคัญและมีความจำเป็นอย่างยิ่งต่อองค์กรสำหรับการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยในโลกไซเบอร์ไม่ว่าจะเป็นผู้ให้บริการด้านโครงข่าย ผู้ให้บริการอินเทอร์เน็ต ผู้ให้บริการ Cloud ผู้ให้บริการดูแล Application และอื่นๆ ทั้งนี้เนื่องมาจากการทำงานขององค์กร ผู้ใช้งานตลอดจนลูกค้าขององค์กรมีความจำเป็นต้องอาศัยระบบคอมพิวเตอร์ อินเทอร์เน็ต เครือข่ายไร้สาย อุปกรณ์ประเภท Smartphone รวมทั้งอุปกรณ์ประเภท Internet of Things เหล่านี้ล้วนก่อให้เกิดความจำเป็นที่จะต้องมีการเฝ้าระวังและป้องกันระบบและอุปกรณ์ขององค์กรให้มีความมั่นคงปลอดภัยอย่างเพียงพอและตลอดเวลา

Security Operation Center หรือ SOC คือศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ที่ทำหน้าที่เฝ้าระวังและป้องกันระบบหรืออุปกรณ์สำคัญขององค์กรจากการถูกบุกรุกหรือการเข้าถึงโดยไม่ได้รับอนุญาต ซึ่งหากมีเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Incident) เกิดขึ้น เช่น ระบบถูกบุกรุก หรือการเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต SOC จะทำหน้าที่ประเมิน ตรวจสอบและแก้ไขเหตุการณ์ที่เกิดขึ้น เพื่อลดผลกระทบและความเสียหายที่อาจเกิดขึ้นกับองค์กรให้อยู่ในระดับที่ไม่รุนแรง

อีกทั้งปัจจุบันหน่วยงานต่างๆ ได้เริ่มให้ความสำคัญเป็นอย่างมากต่อการดูแลระบบเพื่อรักษาความมั่นคงปลอดภัยข้อมูลของระบบสารสนเทศ ซึ่งผู้ไม่ประสงค์ดีใช้อินเทอร์เน็ตเพื่อเข้ามาโจมตี โจรกรรม รวมถึงทำลายข้อมูล โดยผู้โจมตีมีการเปลี่ยนแปลงรูปแบบไปจากเดิมจากที่มักโจมตีโดย DDoS, Malware, Virus ก็ได้เปลี่ยนรูปแบบโจมตีมาเป็นแบบ Ransomware (มัลแวร์ประเภทหนึ่ง ที่โจมตีด้วยการเข้ารหัส หรือล็อกไฟล์ข้อมูลของเหยื่อ ทำให้เข้าถึงข้อมูลของตนเองไม่ได้ และเรียกค่าไถ่ต่อเหยื่อ ที่ต้องการกู้คืน และปลดล็อกข้อมูล) โดยการโจมตีเช่นนี้มุ่งเน้นและหวังผลในเรื่องของเงินมาเป็นอันดับแรก ซึ่งก่อความเสียหายแก่ผู้ใช้งานอินเทอร์เน็ต โดยผู้ไม่ประสงค์ดีสามารถโจมตีมาจากทั้งภายในและภายนอกประเทศ กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษาเป็นผู้ดำเนินการโครงการเครือข่ายสารสนเทศเพื่อพัฒนาการศึกษา โดยสำนักงานให้บริการอินเทอร์เน็ตเพื่อการศึกษาและวิจัย ให้แก่สถาบันการศึกษาต่าง ๆ และมีโครงข่ายเคเบิลใยแก้วนำแสงขึ้นเองเพื่อเชื่อมโยงไปยังสถาบันการศึกษาต่างๆ ทุกระดับ (ระดับอุดมศึกษา ระดับอาชีวศึกษา ระดับการศึกษาขั้นพื้นฐาน และอื่นๆ) จำนวน 10,702 แห่งทั่วประเทศ มีผู้ใช้งานเครือข่ายมากกว่า 5,000,000 คน ดังนั้นหากมีผู้ไม่ประสงค์ดีเข้ามาโจมตีหรือทำลายข้อมูลของผู้ใช้บริการเครือข่ายสารสนเทศเพื่อพัฒนาการศึกษา จะทำให้เกิดผลเสียอันจะพึงประเมินค่าไม่ได้ อีกทั้งนอกจากที่ผู้อื่นจะเข้ามาบุกรุกเราเพียงฝ่ายเดียวสมาชิกเครือข่ายของเราก็สามารถโจมตีไปยังเครือข่ายภายนอกได้เช่นเดียวกัน ซึ่งจะส่งผลให้เครือข่ายสารสนเทศเพื่อพัฒนาการศึกษาของเราขาดความน่าเชื่อถือและในที่สุดแล้วอาจถึงผลให้เครือข่ายอินเทอร์เน็ตทั่วโลกปิดกั้นการเข้าถึงข้อมูลจากเครือข่ายเพื่อพัฒนาการศึกษาของเราได้ ทั้งนี้ ณ ปัจจุบัน

เครือข่ายสารสนเทศเพื่อพัฒนาการศึกษาไม่มีเครื่องมือใดๆ ใช้งานเพื่อการเฝ้ามองความปลอดภัยบนเครือข่าย ดังนั้นเพื่อป้องกันไม่ให้เกิดปัญหาในขั้นต้น เครือข่ายสารสนเทศเพื่อพัฒนาการศึกษาจึงจำเป็นต้องมีระบบรักษาความมั่นคงปลอดภัยสำหรับเครือข่าย เมื่อเกิดเหตุฉุกเฉินหรือเมื่อเกิดเหตุการณ์เกี่ยวกับความมั่นคงและความปลอดภัยจะได้สามารถเตือนผู้ดูแลระบบของสมาชิกแต่ละหน่วยงานให้ดำเนินการแก้ไข ป้องกันปัญหาที่เกิดขึ้นได้อย่างทันท่วงที หากมีระบบเฝ้ามองและป้องกันระบบความมั่นคง ปลอดภัยด้านระบบสารสนเทศอย่างจริงจัง จะช่วยให้การใช้งานระบบเครือข่ายสารสนเทศของหน่วยงานสถาบันการศึกษาสามารถมีความปลอดภัยและมีประสิทธิภาพ

การดำเนินโครงการนี้ยังมีความจำเป็นเพื่อให้หน่วยงานสามารถปฏิบัติงานบริการสารสนเทศเป็นไปตามกฎหมาย/กฎระเบียบที่เกี่ยวข้อง เช่น พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยมีวัตถุประสงค์เพื่อกำหนดนโยบาย มาตรการ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานภาครัฐและภาคเอกชนที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ

2. วัตถุประสงค์

2.1 เพื่อเป็นเครื่องมือสำหรับรักษาความปลอดภัยบนเครือข่ายสารสนเทศและเฝ้าระวังการโจมตีทางไซเบอร์ของเครือข่ายสารสนเทศเพื่อพัฒนาการศึกษา พร้อมทั้งระบบบริการจัดการและระบบฐานข้อมูลภัยคุกคามอัจฉริยะ (Threats Intelligence) ในการเพิ่มประสิทธิภาพเชิงเฝ้าระวังและป้องกันภัยคุกคามทางด้านไซเบอร์ให้กับเครือข่ายเพื่อพัฒนาการศึกษาให้เป็นไปตามมาตรฐานสากล

2.2 เพื่อเพิ่มความสามารถเชิงความมั่นคงปลอดภัย (Network Security and Cybersecurity) ให้กับ Network Operation Center (NOC) ในการทำงานเชิงอัตโนมัติมากขึ้น เพื่อลดความเสี่ยงให้สมาชิกที่เชื่อมต่ออยู่บนเครือข่ายเพื่อพัฒนาการศึกษาจากภัยคุกคามต่าง ๆที่ผ่านทางเครือข่ายอินเทอร์เน็ต ในลักษณะ SOC (Security Operation Center)

2.3 หน่วยงานสามารถให้บริการสารสนเทศเป็นไป พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

3. คุณสมบัติของผู้เสนอราคา

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

1..... 2..... 3..... 4..... 5.....

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นนิติบุคคลผู้มีอาชีพขายงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

ผู้เสนอราคาที่เสนอราคาในรูปแบบของ "กิจการร่วมค้า" ต้องมีคุณสมบัติ ดังนี้

(1) กรณีที่กิจการร่วมค้าได้จดทะเบียนเป็นนิติบุคคลใหม่ กิจการร่วมค้าจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารประกวดราคา และการเสนอราคาให้เสนอราคาในนาม "กิจการร่วมค้า" ส่วนคุณสมบัติด้านผลงาน กิจการร่วมค้าดังกล่าวสามารถนำผลงานของผู้เข้าร่วมค้ามาใช้แสดงเป็นผลงานของกิจการร่วมค้าที่เข้าประกวดราคาได้

(2) กรณีที่กิจการร่วมค้าไม่ได้จดทะเบียนเป็นนิติบุคคลใหม่ นิติบุคคลแต่ละนิติบุคคลที่เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารประกวดราคา เว้นแต่ในกรณีที่กิจการร่วมค้าได้มีข้อตกลงระหว่างผู้เข้าร่วมค้าเป็นลายลักษณ์อักษรกำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้รับผิดชอบหลักในการเข้าเสนอราคากับหน่วยงานของรัฐ และแสดงหลักฐานดังกล่าวมาพร้อมการยื่นข้อเสนอประกวดราคาทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ กิจการร่วมค้านั้นสามารถใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นเสนอราคาได้

ทั้งนี้ "กิจการร่วมค้าที่จดทะเบียนเป็นนิติบุคคลใหม่" หมายความว่า กิจการร่วมค้าที่จดทะเบียนเป็นนิติบุคคลต่อกรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์

3.8 กรณีผู้เสนอราคาที่ยื่นในนามกิจการร่วมค้า (Joint venture) หรือกิจการค้าร่วม (Consortium) ในการทำสัญญาร่วมค้า หรือค้าร่วมกรณีที่มิได้จดทะเบียนเป็นนิติบุคคลขึ้นใหม่จะต้องมีข้อกำหนดความรับผิดชอบร่วมกันในลักษณะลูกหนี้ร่วมต่อ สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม และห้ามบุคคลหรือกิจการเข้าร่วมกลุ่มในกิจการร่วมค้า (Joint venture) หรือกิจการค้าร่วม (Consortium) มากกว่า 1 กลุ่มสำหรับคุณสมบัติของกิจการค้าร่วม (Consortium) ให้นำคุณสมบัติของผู้เสนอราคาที่เป็นกิจการร่วมค้า (Joint venture) มาใช้บังคับโดยอนุโลม

3.9 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ สป.อว. ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.10 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทยเว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

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

3.12 ผู้ยื่นข้อเสนอต้องมีผลงานเกี่ยวกับการขายและติดตั้งระบบเครือข่ายสารสนเทศ หรือระบบรักษาความมั่นคงปลอดภัย ต่อหนึ่งสัญญา/ข้อตกลง จำนวนอย่างน้อย 1 ผลงาน โดยแต่ละงาน/โครงการ มีวงเงินไม่ต่ำกว่า 35,000,000 บาท (สามสิบห้าล้านบาทถ้วน) ในสัญญาเดียว และได้ดำเนินการแล้วเสร็จโดยผลงานนั้นต้องมีระยะเวลาไม่เกิน 5 ปี นับถัดจากวันที่รับมอบไว้ใช้งานถึงวันที่ยื่นข้อเสนอ และเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับส่วนราชการ หน่วยงานตามกฎหมายว่าด้วยระเบียบบริหารราชการส่วนท้องถิ่น หน่วยงานอื่นซึ่งมีกฎหมายบัญญัติให้มีฐานะเป็นราชการบริหารส่วนท้องถิ่น รัฐวิสาหกิจ หรือหน่วยงานเอกชนที่สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม เชื่อถือ พร้อมเอกสารหลักฐานหรือหนังสือรับรองผลงานและสำเนาสัญญามาแสดง

3.13 ผู้เสนอราคาต้องได้รับการแต่งตั้งโดยตรงจากบริษัทผู้ผลิตหรือสาขาของบริษัทผู้ผลิตประจำประเทศไทย หรือผู้แทนจำหน่ายผลิตภัณฑ์นั้นโดยตรงภายในประเทศไทย สำหรับอุปกรณ์และระบบที่เสนอในโครงการให้เป็นผู้เสนอผลิตภัณฑ์และได้รับการสนับสนุนทางด้านเทคนิคในโครงการนี้ โดยแนบหนังสือแต่งตั้งต้นฉบับหรือหนังสือแต่งตั้งที่ได้จากระบบอิเล็กทรอนิกส์พร้อมลายเซ็นผู้มีอำนาจลงนามจากบริษัทผู้ผลิตหรือสาขาของบริษัทผู้ผลิตประจำประเทศไทย

4. ขอบเขตการดำเนินงาน (Scope of Works)

4.1 การดำเนินการติดตั้งระบบบริหารเหตุการณ์และข้อมูลการรักษาความมั่นคงปลอดภัย (Security Information and Event Management: SIEM จำนวน 5 เครื่อง

4.2 การดำเนินการติดตั้งระบบบริหารการตอบสนองภัยคุกคามแบบอัตโนมัติ จำนวน 1 เครื่อง

4.3 การดำเนินการติดตั้งอุปกรณ์ตรวจสอบและวิเคราะห์กระแสการรับส่งข้อมูลเครือข่าย (Network Traffic Flow) จำนวน 2 ระบบ

4.4 การดำเนินการติดตั้งอุปกรณ์ควบคุมดูแลและจำกัดภัยคุกคาม (Threat Mitigation System) ในรูปแบบการปฏิเสธการให้บริการแบบวงกว้าง (Distributed Denial of Service – DDoS) จำนวน 1 ระบบ

4.5 การดำเนินการติดตั้งอุปกรณ์กระจายสัญญาณ ขนาดไม่น้อยกว่า 48 ช่องสัญญาณ จำนวน 2 เครื่อง

4.6 ผู้เสนอราคาต้องดำเนินการดังต่อไปนี้ เพื่อให้อุปกรณ์ต่าง ๆ ซึ่งประกอบด้วยฮาร์ดแวร์ ซอฟต์แวร์และสิทธิการใช้งานต่าง ๆ ที่เสนอ <u>รวมทั้งอุปกรณ์ที่ผู้เสนอราคาอาจจะต้องจัดหาเพิ่มเติม (ถ้ามี)</u> ทำงานร่วมกันได้กับระบบเดิมได้เป็นอย่างดี ตามความต้องการโดยทั่วไป

4.6.1 ผู้เสนอราคาต้องดำเนินการจัดหาและติดตั้งอุปกรณ์ ณ สถานที่ที่สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรมกำหนด

4.6.2 ผู้เสนอราคาต้องดำเนินการพัฒนา ปรับแต่ง กำหนดค่าต่าง ๆ และปรับปรุงโยกย้ายระบบที่เสนอให้เหมาะสม และสามารถทำงานร่วมกันได้กับระบบเดิมได้สมบูรณ์

4.7 ผู้เสนอราคาต้องจัดประชุมร่วมระหว่างผู้เสนอราคากับเจ้าหน้าที่ของสำนักงานฯ และคณะกรรมการตรวจรับพัสดุ เพื่อเสนอแผนงานการดำเนินโครงการให้คณะกรรมการตรวจรับพัสดุอนุมัติภายใน 30 วัน นับถัดจากวันลงนามในสัญญา

4.8 ผู้เสนอราคาต้องจัดประชุมร่วมระหว่างผู้เสนอราคากับเจ้าหน้าที่ของสำนักงานฯ หรือคณะกรรมการตรวจรับพัสดุ เพื่อนำเสนอความก้าวหน้าของโครงการ (Progress Report) พร้อมทั้งจัดส่งรายงานประจำทุกเดือน

4.9 ผู้เสนอราคาต้องส่งรายชื่อคณะทำงานพร้อมประวัติการศึกษาและประสบการณ์การทำงาน (Resume) ที่ระบุระยะเวลาการทำงาน พร้อมแนบหลักฐาน Certificate ที่ยังไม่หมดอายุ ณ วันที่ยื่นเอกสารเสนอราคาและหนังสือรับรองการปฏิบัติงาน ของบุคลากรรับผิดชอบโครงการ มีหน้าที่ปฏิบัติงานจนกว่าผู้เสนอราคาจะส่งมอบงานแล้วเสร็จตามข้อกำหนด

4.9.1 ผู้เชี่ยวชาญประจำโครงการ อย่างน้อย 1 ท่าน เพื่อให้คำปรึกษาในเรื่องการใช้งานอุปกรณ์วิเคราะห์ ออกแบบระบบให้เหมาะสมกับโครงการ

4.9.1.1 เป็นบุคลากรที่เป็นพนักงานประจำ (Full Time) ของผู้เสนอราคา โดยแสดงหลักฐานเอกสารประกันสังคม ไม่น้อยกว่า 6 เดือน

4.9.1.2 เป็นผู้เชี่ยวชาญที่ผ่านการอบรมและได้รับประกาศนียบัตรระดับสูงสุด JNCIE หรือ HCIE หรือ CCIE ด้านรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ (Security) และผู้เชี่ยวชาญระบบเครือข่ายระดับสูงต้องมีประสบการณ์อย่างน้อย 5 ปี

4.9.2 วิศวกรเครือข่าย อย่างน้อย 1 ท่าน เพื่อให้คำปรึกษาในเรื่องการติดตั้ง และการแก้ไขปัญหา

4.9.2.1 เป็นบุคลากรที่เป็นพนักงานประจำ (Full Time) ของผู้เสนอราคา โดยแสดงหลักฐานเอกสารประกันสังคม ไม่น้อยกว่า 6 เดือน

4.9.2.2 เป็นผู้เชี่ยวชาญที่ผ่านการอบรมและได้รับประกาศนียบัตร CompTIA Security+ หรือ CCNA-Security หรือใบประกาศนียบัตรด้าน Security ในระดับเริ่มต้นเป็นอย่างน้อย และต้องมีประสบการณ์อย่างน้อย 3 ปี

4.11 ผู้เสนอราคาต้องมีเจ้าหน้าปฏิบัติงานประจำโครงการอย่างน้อย 2 คน ประจำที่สำนักงานฯ หลังจากส่งมอบงานเสร็จ เพื่อบริหารจัดการและแก้ไขปัญหาอุปกรณ์และระบบที่ติดตั้งในโครงการตลอดระยะเวลารับประกัน เป็นผู้เชี่ยวชาญที่ผ่านการอบรมและได้รับประกาศนียบัตร CompTIA Security+ หรือ CCNA-Security หรือใบประกาศนียบัตรด้าน Security ในระดับเริ่มต้นเป็นอย่างน้อย

4.10 ผู้เสนอราคาส่งมอบเอกสารทั้งหมดในรูปแบบเอกสารจำนวน 2 ชุด ในการส่งมอบงานในแต่ละงวดงาน ประกอบด้วย

4.10.1 เอกสารต้นฉบับ (สี) จำนวน 1 ชุดและเอกสารสำเนา (สี) จำนวน 1 ชุด

4.10.2 เอกสารรูปแบบไฟล์อิเล็กทรอนิกส์ที่สามารถแก้ไขได้ เช่น Word Excel Visio เป็นต้น จำนวน 1 ชุด

1..... 2..... 3..... 4..... 5.....

5. คุณสมบัติเฉพาะทางเทคนิค

คุณสมบัติโดยรายละเอียดที่ปรากฏตามข้อกำหนดนี้ถือเป็นคุณสมบัติและรายการขั้นต่ำ ดังนั้นกรณีจำเป็นต้องมีอุปกรณ์ (ฮาร์ดแวร์/ซอฟต์แวร์) อื่น ๆ ประกอบเพื่อทำให้ระบบสามารถทำงานได้ครบถ้วนตามข้อกำหนดนี้ ถือเป็นภาระหน้าที่ต้องดำเนินการจัดหาเพิ่มเติม โดยค่าใช้จ่ายที่เกิดขึ้นถือเป็นภาระของผู้เสนอราคา

5.1 ระบบบริหารเหตุการณ์และข้อมูลการรักษาความมั่นคงปลอดภัย (Security Information and Event Management: SIEM จำนวน 5 เครื่อง

5.1.1 ระบบสามารถทำการสืบค้นข้อมูลจราจรทางคอมพิวเตอร์ได้อย่างน้อย 90 วันในรูปแบบ Online ไม่ต้องทำการ Restore จากระบบ Archive หรือ Offline Storage

5.1.2 ระบบสามารถทำการ Forensic เหตุการณ์จากข้อมูลจราจรทางคอมพิวเตอร์ที่ได้รับจากอุปกรณ์ต่างๆ ได้ เช่นอุปกรณ์เครือข่าย, เครื่องคอมพิวเตอร์แม่ข่าย เป็นต้น

5.1.3 ระบบต้องทำการเข้ารหัส (Hash) ข้อมูลที่เก็บด้วย Algorithm เช่น SHA-256 ได้เป็นอย่างน้อย

5.1.4 ระบบต้องทำการ Encryption ข้อมูลด้วย AES-256 bits ได้เป็นอย่างน้อย เพื่อยืนยันว่าข้อมูลจะไม่มีการแก้ไขเปลี่ยนแปลง เมื่อส่งออกจากอุปกรณ์ (Data Integrity)

5.1.5 ระบบต้องสามารถย้ายและถ่ายโอนข้อมูลสำรอง (Archive) ไปยังหน่วยจัดเก็บข้อมูลภายนอกได้

5.1.6 ระบบต้องสามารถแสดง Map ของภัยคุกคามที่เกิดขึ้น แบบ Real Time และย้อนหลัง 6 หรือ12 หรือ 24 ชั่วโมงได้

5.1.7 ระบบต้องสามารถแสดงกราฟสรุปข้อมูลการโจมตี เช่น Top Attack, Top Target Port, Top Attacking Country เป็นต้น

5.1.8 มีระบบการแจ้งเตือนผ่านทาง Email โดยสามารถกำหนดรูปแบบการแจ้งเตือนที่ต่างกัน ตามเหตุการณ์ที่เกิดได้

5.1.9 มีหน้าจอในการแสดงข้อมูล (Dashboard) และสามารถปรับเปลี่ยนรูปแบบ (Customization) ของหน้าจอได้

5.1.10 สามารถออกรายงาน และมี Template ของรายงานอย่างน้อยดังนี้

5.1.10.1 ข้อมูลการโจมตีจากภายในองค์กรสูงสุด (Top Internal Attackers)

5.1.10.2 ข้อมูลการโจมตีสูงสุดในแต่ละเครือข่าย (Attacks Per Network) การโจมตีสูงสุดในแต่ละส่วนงาน (Per Department) และการโจมตีสูงสุดในแต่ละสาขา (Per Subsidiary)

5.1.10.3 ข้อมูลปริมาณการใช้งานเครือข่าย Bandwidth/Traffic Usage

5.1.10.4 รองรับการทำรายงานตามมาตราฐาน ISO 27001 และ PCI DSS ได้

5.1.11 สามารถสร้างรายงานแบบอัตโนมัติตามระยะเวลาที่กำหนด เช่น รายชั่วโมง,รายวัน, รายสัปดาห์, รายเดือน และกำหนดระยะเวลาเองได้

5.1.12 สามารถส่งรายงาน Audit Trail ไปยังผู้ตรวจสอบภายในซึ่งไม่มีสิทธิ์ในการเข้าใช้งานระบบนี้ได้

5.1.13 สามารถออกรายงานในรูปแบบ CSV, PDF และ Word ได้เป็นอย่างน้อย

5.1.14 สามารถกำหนดสิทธิผู้เข้าใช้งาน ได้อย่างน้อย 3 ระดับ

5.1.15 รับประกันของอุปกรณ์ระยะเวลาอย่างน้อย 3 ปี

5.2 ระบบบริหารการตอบสนองภัยคุกคามแบบอัตโนมัติ จำนวน 1 เครื่อง

5.2.1 เป็นระบบ SOAR ที่อยู่ในการจัดอันดับความน่าเชื่อถือของ Gartner ไม่ต่ำกว่าปี 2023

5.2.2 เป็นระบบที่สามารถรองรับระบบเพิ่มเติมเพื่อให้มีประสิทธิภาพมากขึ้นโดยสามารถใช้เครื่องมือเพิ่มเติมได้ เช่น Whois, Virus Total, Recorded Future, and MISP และต้องมีระบบการควบคุมความปลอดภัยแบบอัจฉริยะที่สามารถรองรับบูรณาการแบบ Out of the box ได้

5.2.3 ระบบสามารถรองรับ Use Case/Playbook Triggers แบบต่างๆ และรองรับ Use Case/Playbook Versioning and Testing ได้

5.2.4 ระบบสามารถรองรับ Automatic Playbook Recommendation และ Execution Based on Rules or Conditions ได้

5.2.5 ระบบสามารถรองรับ Use Case/Playbook Actions or Triggers แบบไม่จำกัดได้

5.2.6 ระบบสามารถรองรับ

5.2.6.1 Automatic Case Prioritization

5.2.6.2 Tasks Prioritization

5.2.6.3 Workload Reduction

5.2.6.4 Reduction of False Positives

5.2.6.5 Third Party Tools Automation

5.2.7 ระบบสามารถสร้าง Workflow/Playbook แบบ Codeless Processได้ โดยสามารถใช้ Interfaceของระบบได้เลยโดยไม่ต้องพัฒนาเพิ่มเติม และสามารถสร้าง Graphical User Interface โดยใช้วิธีแบบ Drag-and-Drop

5.2.8 ระบบสามารถแสดง Runtime View of Playbooks โดยใช้รูปแบบของ GUI โดยใช้รูปแบบเดียวกับ Playbook Design View และให้รายละเอียดแบบเต็มของ Task Executed, Input Parameters, Results, Output Parameters, Errors (ถ้ามี)

5.2.9 ระบบสามารถรองรับ Modular Playbooks ที่ครอบคลุมแผนธุรกิจและ Logic ประยุกต์แบบต่างๆ และ รองรับการทำงานแบบ Nested เพื่อรองรับการนำ Multiple Playbooks ไป ใช้ซ้ำ ในแบบต่างๆ ได้

5.2.10 ระบบสามารถปรับเปลี่ยน Augment Incident Playbooks ได้อย่างทันท่วงทีแบบ Real Time เพื่อสนับสนุนการทำงานแบบ Specific Incident Response Workflow

5.2.11 ระบบสามารถรองรับการจำลองเหตุการณ์และการประเมินความความเป็นไปได้, รองรับแผนการรับมือ ระบุช่องว่างในระบบและประเมินแผนการรองรับได้

5.2.12 ระบบสามาถแสดงตัวเลือกในการการรับมือ Data Breach Preparation, Assessment, Notification, และการจัดการขยายระบบในอนาคต การสร้าง Playbooks สามารถกำหนดการกำกับดูแลให้อยู่ภายในขอบเขตอย่างเคร่งครัด

5.2.13 ระบบสามารถแสดง Dashboard ได้หลายหน้าจอและสามารถกำหนดตามที่ผู้ใช้ระบุได้ตามที่ผู้ใช้ระบบได้กำหนด

5.2.14 ระบบสามารถแสดง Dashboard ได้แบบ Out-of-The-Box ได้แบบไม่จำกัดว่าเป็นแบบ Incident Over Time by Type, Open Incidents by Phase Close Incident by Duration

5.2.15 รับประกันของอุปกรณ์ระยะเวลาอย่างน้อย 3 ปี

5.3 อุปกรณ์ตรวจสอบและวิเคราะห์กระแสการรับส่งข้อมูลเครือข่าย (Network Traffic Flow) จำนวน 2 ระบบ

5.3.1 เป็นอุปกรณ์ที่ตรวจสอบและวิเคราะห์ Network Traffic จาก Flow บนอุปกรณ์ Network แบบ Appliance โดยทำงานในลักษณะเป็น Flow Data Collector และมีลิขสิทธิ์สำหรับเก็บและวิเคราะห์ข้อมูลจาก Router ได้ไม่น้อยกว่า 10 อุปกรณ์

5.3.2 มี Interface แบบ 1/10G Copper ไม่น้อยกว่า 2 Ports และรองรับ Interface แบบ 10G SFP+ ไม่น้อยกว่า 4 Ports ได้ในอนาคต

5.3.3 สามารถเก็บข้อมูลได้ ไม่น้อยกว่า 30,000 Flows/Sec จากอุปกรณ์ Router ที่ Monitor ได้ พร้อมทั้งรองรับการเก็บข้อมูลได้ไม่น้อยกว่า 280,000 flows/sec โดยไม่ต้องเปลี่ยนอุปกรณ์เพิ่มภายหลัง

5.3.4 สามารถรับข้อมูล Flow จากอุปกรณ์ Router ได้แก่ NetFlow, Cflowd, Sflow, Jflow, IPFIX และ Netstream ได้เป็นอย่างน้อย

5.3.5 สามารถเก็บข้อมูลของ Traffic ได้จาก NetFlow, SNMP และ BGP Routing Information จากอุปกรณ์ที่ Monitor ในโครงข่ายได้ พร้อมทั้งสามารถทำรายงานย้อนหลังได้

5.3.6 สามารถสร้าง Baselining ของ Network เพื่อใช้ในการส่ง Alert แจ้งเตือนในกรณีเกิดเหตุการณ์ผิดปกติได้

5.3.7 สามารถทำงานในลักษณะเป็น Real-time Detection and Mitigation ของ Securities Events ได้ โดย สามารถทำ Mitigation ร่วมกับ Router และอุปกรณ์ DDoS Mitigation ได้

5.3.8 สามารถตรวจจับความผิดปกติ ซึ่งเกิดจาก Bandwidth, Packet และ Protocol Anomalies จากอุปกรณ์ที่ถูก Monitor ได้

5.3.9 สามารถทำการตรวจสอบ IP address ที่จู่โจมระบบโดยใช้ WHOIS lookup ได้

5.3.10 รองรับ Dual Stack IPv4/IPv6 สำหรับการใช้งาน IPv6 Ping, Traceroute, SSH, HTTPS, Syslog, DNS, NTP และ SNMP ได้

5.3.11 มี Dashboards ที่แสดงผลการทำงานของระบบ และมี Web Monitoring หรือ Web-based GUI ที่รองรับ Web Browsers เช่น Google Chrome, Mozilla Firefox ได้เป็นอย่างน้อย

5.3.12 สามารถแสดงรายงาน Traffic Break Down โดย IP location เช่น Break Down โดย Countries, Regions, Cities ได้เป็นอย่างน้อย

5.3.13 สามารถทำการ Confirm ในการทำการเปลี่ยนแปลง Configuration (Configuration Commit) ทุกครั้งและสามารถ Revert ไปยัง Version ที่ถูก Save ไว้ก่อนหน้าที่จะมีการเปลี่ยนแปลงได้ และผู้ดูแลระบบต้องสามารถเพิ่ม Comment สำหรับ Audit Trail และดูรายละเอียด Configuration Change ก่อนการ Commit ได้

5.3.14 สามารถออก Report ในรูปแบบ PDF หรือ XML Format ได้

5.3.15 สามารถทำรายงานเพื่อให้ผู้ดูแลระบบเปรียบเทียบปริมาณ Traffic ของ Direct peering และ Non-direct peering เพื่อใช้หา New peering (peering evaluation) ได้

5.3.16 สามารถสร้าง Alert ให้ผู้ดูแลระบบทราบถึงความผิดปกติของระบบได้ เช่น System Error, Over-Load Condition ไม่ว่าจะเกิดจาก Process Error, CPU Load, High Memory Consumption

5.3.17 สามารถจัดการและ Modify Setup Parameters ของระบบผ่านทาง Command Line หรือ GUI ได้

5.3.18 มี Redundant Power Supply และสามารถติดตั้งใน Rack 19" ได้

5.3.19 อุปกรณ์สามารถทำงานและใช้ข้อมูลภัยคุกคามจาก Intelligence Feed ของผลิตภัณฑ์เพื่อเพิ่มความสามารถในการตรวจสอบ วิเคราะห์ Traffic ได้

5.3.20 รับประกันของอุปกรณ์ระยะเวลาอย่างน้อย 3 ปี

5.4 อุปกรณ์ควบคุมดูแลและจำกัดภัยคุกคาม (Threat Mitigation System) ในรูปแบบการปฏิเสธการให้บริการแบบวงกว้าง (Distributed Denial of Service – DDoS) จำนวน 1 ระบบ

5.4.1 เป็นอุปกรณ์ Appliance ที่ได้รับการออกแบบมาเพื่อทำ Surgical Mitigation โดยเฉพาะแบบ Stateless Architecture สำหรับทุกประเภทของการโจมตี DDoS (L3/4 และ application layer)

5.4.2 สามารถรองรับ Throughput ในการทำ Mitigation ได้ 5 Gbps ในระหว่าง Off-Ramp เพื่อบรรเทาการโจมตี (Active Mitigation) และรองรับการขยาย License เพื่อทำการ Mitigation ถึง 40 Gbps ได้ในอนาคต

5.4.3 สามารถรองรับขนาดของ Traffic ได้ไม่น้อยกว่า 37 Mpps

5.4.4 มี Interface แบบ 10 GE SFP+ พร้อม Transceiver แบบ 10GE LR Fiber จำนวนไม่น้อยกว่า 4 Ports และรองรับการเพิ่ม Interface แบบ 10 GE SFP+ ไม่น้อยกว่า 4 Ports และแบบ 1G SFP ไม่น้อยกว่า 8 Ports ได้ในอนาคต

5.4.5 สามารถตรวจสอบและคัดกรองข้อมูลที่เป็นการโจมตีออก (Remove Attack Traffic) แล้วส่งข้อมูลที่เหลือต่อไปยังปลายทาง (On-Ramp Traffic) ได้

5.4.6 สามารถแสดงสถิติของข้อมูลที่ส่งผ่าน (Passed) และคัดออก (Dropped) ระหว่างการบรรเทาปัญหา (Mitigation) ได้

5.4.7 ต้องอนุญาตให้สร้าง Mitigation Template ที่แตกต่างกันได้

5.4.8 สามารถกำหนดได้ว่าจะให้มีการทำ Mitigation แบบ Manual โดยผู้ดูแลระบบ หรือทำ Mitigation แบบอัตโนมัติจาก Alert ของระบบตรวจจับการโจมตี และวิเคราะห์ข้อมูลจราจรอุปกรณ์ตรวจสอบและวิเคราะห์ Network Traffic จาก Flow ภายใต้ผลิตภัณฑ์เดียวกัน

5.4.9 ต้องอนุญาตให้ผู้ใช้กำหนดเงื่อนไขการคัดกรอง (Filter Expression) ทำการระบุข้อมูลที่จะคัดออกเพื่อบรรเทาการโจมตี โดยสามารถระบุจากข้อมูล IP และข้อมูล Payload ได้

5.4.10 สามารถใช้เทคนิค Packet Content Filtering, Geo Location Report and Blocking, Multiple Anti-Spoofing ระหว่างการบรรเทาการโจมตี (Active Mitigation) ได้เป็นอย่างน้อย

5.4.11 สามารถทำ Mitigation สำหรับ Traffic ที่เป็น IPv4 และ IPv6 ได้

5.4.12 สามารถทำการ Update ฐานข้อมูลเกี่ยวกับการโจมตีจาก Website ของผู้ผลิตได้

5.4.13 สามารถทำงานร่วมกับอุปกรณ์ตรวจจับการโจมตี และวิเคราะห์ข้อมูลจราจร และสามารถบริหารจัดการแบบรวมศูนย์จากอุปกรณ์ตรวจจับการโจมตี และวิเคราะห์ข้อมูลจราจรที่นำเสนอได้

5.4.14 อุปกรณ์มี Redundant Power Supply

5.4.15 อุปกรณ์ติดตั้งใน Rack 19" ได้

5.4.16 รับประกันของอุปกรณ์ระยะเวลาอย่างน้อย 3 ปี

5.5 อุปกรณ์กระจายสัญญาณ ขนาดไม่น้อยกว่า 48 ช่องสัญญาณ

5.5.1 มีขนาดของ Switching Capacity หรือ Switching Throughput ไม่น้อยกว่า 4 Tbps และมี Forwarding Rate ไม่น้อยกว่า 1 Bpps

5.5.2 มีพอร์ตแบบ 1/10/25 Gigabit Ethernet จำนวนไม่น้อยกว่า 48 พอร์ต และมีพอร์ต 40/100 Gigabit Ethernet แบบ QSFP จำนวนไม่น้อยกว่า 8 พอร์ต โดยทุกพอร์ตสามารถทำงานแบบ Wire Speed หรือ Wire Rate หรือ Non-Blocking ได้ พร้อม Module ให้เพียงพอต่อการใช้งานทั้ง 2 ฝั่ง Uplink หรืออย่างน้อย 24 Port

5.5.3 มีขนาดของ System Memory หรือ DRAM ไม่น้อยกว่า 8 GB และมีขนาดของ Flash Memory หรือ SSD ไม่น้อยกว่า 8 GB

5.5.4 รองรับจำนวน MAC Address ได้ไม่น้อยกว่า 280,000 Addresses และสามารถทำ VLAN ตามมาตรฐาน 802.1Q ได้ไม่น้อยกว่า 4,000 VLANs

5.5.5 สามารถทำ Equal Cost Multipath Routing (ECMP) ได้ไม่น้อยกว่า 64 Ways

5.5.6 สามารถทำ IP Routing Protocol สำหรับ IPv4 และ IPv6 อย่างน้อย Static, OSPF และ BGP ได้ และรองรับจำนวน IPv4 Unicast Route ได้สูงสุดไม่น้อยกว่า 360,000 Routes

5.5.7 สามารถทำ Network Virtualization โดยใช้เทคโนโลยี Virtual Extensible LAN (VXLAN) แบบ VXLAN Bridging และ VXLAN Routing และสามารถทำ EVPN Control Plane ได้ หรือเทียบเท่า

5.5.8 สามารถตรวจสอบ (Monitor) และบันทึกข้อมูล (Log) ในกรณีเกิด Buffer Congestion บนตัวอุปกรณ์ได้ ในระดับ Real-Time โดยที่สามารถแสดงข้อมูลของ Latency ที่เกิดขึ้นจาก Congestion ได้เป็นอย่างน้อย

5.5.9 มีระบบ Redundant Power Supplies แบบ 1+1 เป็นอย่างน้อยและสามารถถอดเปลี่ยนได้โดยที่ไม่ต้องปิดตัวอุปกรณ์ (Hot Swappable) และรองรับการทำงานกับระบบไฟในประเทศไทยแบบ 220V 50Hz ได้

5.5.10 อุปกรณ์ต้องผ่านการรับรองตามมาตรฐานความปลอดภัย FCC, IEC, UL และ EN หรือเทียบเท่า

5.5.11 เป็นผลิตภัณฑ์ที่ต้องอยู่ใน Quadrant LEADERS ของ Gartner Magic Quadrant For Data Center and Cloud Networking ปี ค.ศ. 2020 หรือใหม่กว่า

5.5.12 รับประกันของอุปกรณ์ระยะเวลาอย่างน้อย 3 ปี

6. ข้อกำหนดทั่วไปของอุปกรณ์ระบบที่นำเสนอ

6.1 สิ่งแวดล้อมในขณะใช้งาน ระบบที่นำเสนอจะต้องสามารถออกแบบติดตั้งระบบที่เสนอได้อย่างเหมาะสม สะดวกต่อการปฏิบัติงานได้อย่างดี อุปกรณ์ทุกชนิดที่เสนอต้องสามารถทำงานได้อย่างสมบูรณ์ในสภาพอากาศของประเทศไทย ดังต่อไปนี้เป็นอย่างน้อย

6.1.1 ช่วงอุณหภูมิการใช้งานระหว่าง 10°c – 40°c

6.1.2 ความชื้นสัมพัทธ์ระหว่าง 15% - 80% (Non Condensing)

6.2 ระบบไฟฟ้าหลักและฟิวส์ อุปกรณ์ที่เสนอจะต้องสามารถทำงานได้กับแหล่งจ่ายไฟฟ้ากระแสสลับ 220V±10% 50 Hz ในกรณีไฟฟ้าหนึ่งเฟส หรือ 380V±10 % 50 Hz ในกรณีไฟฟ้าสามเฟส และมีระบบสายดิน (Ground) ตามมาตรฐานอุตสาหกรรมของประเทศไทย หรือมาตรฐานสากลอื่นซึ่งเป็นที่ยอมรับทั่วไป ตามหลักวิศวกรรมไฟฟ้าในตำแหน่งที่เหมาะสม

6.3 ระบบที่นำเสนอในโครงการต้องมีการป้องกันการรบกวนทางแม่เหล็กไฟฟ้าตามมาตรฐานสากลอื่นซึ่งเป็นที่ยอมรับทั่วไป

6.4 โปรแกรม (Software) ระบบงานต่าง ๆ ของโครงการที่นำเสนอนี้จะต้องใช้งานได้ และเป็นโปรแกรมที่ถูกต้องตามกฎหมายลิขสิทธิ์

6.5 เป็นอุปกรณ์ที่นำเข้ามาจำหน่ายในประเทศไทยโดยได้รับการสนับสนุนทางเทคนิคและบริการหลังการขายจากสำนักงานสาขาของเจ้าของผลิตภัณฑ์ในประเทศไทย

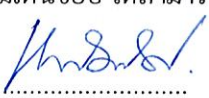
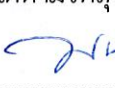
7. การฝึกอบรม

ผู้เสนอราคาจะต้องเสนอหลักสูตรการฝึกอบรมซึ่งประกอบด้วยภาคทฤษฎีและภาคปฏิบัติ สำหรับเจ้าหน้าที่ภายใต้กำกับของสำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม จนสามารถใช้งานได้อย่างมีประสิทธิภาพ โดยต้องดำเนินการฝึกอบรมให้แล้วเสร็จภายใน 180 วัน (หนึ่งร้อยแปดสิบ) วันนับถัดจากวันลงนามในสัญญา โดยไม่คิดค่าใช้จ่ายใด ๆ และต้องจัดส่งเอกสารสำหรับการฝึกอบรมพร้อม Data Sheets ของอุปกรณ์ในโครงการนี้ อยู่ในรูปแบบหนังสือคู่มือการใช้งานของระบบทั้งหมดที่นำเสนอ จำนวน 2 ชุด และในรูปแบบของอุปกรณ์สำหรับบันทึกข้อมูลจำนวน 2 ชุด โดยหลักสูตรอย่างน้อยให้ครอบคลุมระบบที่นำเสนอ ทั้งนี้ หลักสูตรการอบรม จำนวนผู้เข้ารับการอบรม ระยะเวลาการอบรม อาจจะเปลี่ยนแปลงได้ตามความเหมาะสมหรือเป็นตามการพิจารณาของคณะกรรมการตรวจรับพัสดุ ดังนี้

7.1 การทำงานร่วมกันของระบบ/อุปกรณ์ทั้งหมดที่ได้จากการจัดหาครั้งนี้ จำนวนผู้เข้ารับการอบรมไม่น้อยกว่า 5 คนต่อหลักสูตร อย่างน้อย 12 ชั่วโมง

8. การดำเนินการติดตั้งระบบ

8.1 การดำเนินการติดตั้งระบบ จะต้องดำเนินการติดตั้งตามแบบที่ได้ดำเนินการออกแบบไว้ตามที่คณะกรรมการตรวจรับพัสดุพิจารณาให้ความเห็นชอบ ให้สามารถใช้งานได้ตามวัตถุประสงค์ของขอบเขตของงาน

1..... 2.....  3.....  4.....  5..... 

8.2 วัสดุ อุปกรณ์ ระบบไฟฟ้า ระบบปรับอากาศหรืออื่น ๆ ที่จำเป็นต้องใช้เพิ่มเติมภายหลัง เพื่อให้ระบบสามารถทำงานได้ดีและมีประสิทธิภาพ ผู้เสนอราคาจะต้องเป็นผู้รับผิดชอบในการดำเนินการจัดหาและรับผิดชอบค่าใช้จ่ายที่เกิดขึ้น

8.3 ผู้เสนอราคาจะต้องเป็นผู้รับผิดชอบกรณีเกิดปัญหาแบบ end-to-end ระหว่างอุปกรณ์ที่เสนอและอุปกรณ์เดิมจะต้องทำงานร่วมกันได้อย่างมีประสิทธิภาพ โดยบริการทั้งหมดในเครือข่าย UniNet จะต้องสามารถทำงานได้อย่างปกติภายในระยะเวลาตามข้อกำหนดบำรุงรักษาของสำนักงานฯ

8.4 ผู้เสนอราคาจะต้องประสานงาน สำรวจสถานที่ติดตั้ง ตามสถานที่ที่จะต้องติดตั้งอุปกรณ์และระบบ

8.5 ผู้เสนอราคาจะต้องขออนุญาตเข้าพื้นที่เพื่อดำเนินการปรับปรุงสถานที่ การติดตั้งอุปกรณ์ หรือกรณีที่มีความจำเป็นต้องดำเนินงานนอกเวลาราชการ เพื่อไม่ให้กระทบการปฏิบัติงานของเจ้าหน้าที่อื่น ๆ ของหน่วยงาน/สถานที่ที่ติดตั้งล่วงหน้าไม่น้อยกว่า 5 วันทำการ

8.6 ผู้เสนอราคาจะต้องถ่ายภาพการดำเนินงานการติดตั้งระบบ ณ สถานที่ มาประกอบการส่งมอบงาน

9. การบำรุงรักษาและซ่อมแซมแก้ไขระบบ

ผู้เสนอราคาตกลงรับประกันความชำรุดบกพร่องหรือขัดข้องของคอมพิวเตอร์และการติดตั้งตามสัญญานี้เป็นเวลา 3 (สาม) ปี นับถัดจากวันที่ผู้ซื้อได้รับมอบคอมพิวเตอร์ทั้งหมดโดยถูกต้องครบถ้วนตามสัญญา ถ้าภายในระยะเวลาดังกล่าวคอมพิวเตอร์ชำรุดบกพร่องหรือขัดข้อง หรือใช้งานไม่ได้ทั้งหมดหรือแต่บางส่วนหรือเกิดความชำรุดบกพร่องหรือขัดข้องจากการติดตั้ง เว้นแต่ความชำรุดบกพร่องหรือขัดข้องดังกล่าวเกิดขึ้นจากความผิดของผู้ซื้อซึ่งไม่ได้เกิดจากการใช้งานตามปกติ ผู้เสนอราคาจะต้องจัดการซ่อมแซมแก้ไขให้อยู่ในสภาพใช้การได้ดีดังเดิม โดยต้องเริ่มจัดการซ่อมแซมแก้ไขภายใน 24 ชั่วโมง นับถัดจากเวลาที่ได้รับแจ้งจากผู้ซื้อโดยไม่คิดค่าใช้จ่ายใด ๆ จากผู้ซื้อทั้งสิ้น ถ้าผู้เสนอราคาไม่จัดการซ่อมแซมแก้ไขภายในกำหนดเวลาดังกล่าว ผู้ซื้อมีสิทธิที่จะทำการนั้นเองหรือจ้างผู้อื่นทำการนั้นแทนผู้เสนอราคา โดยผู้เสนอราคาต้องออกค่าใช้จ่ายทั้งสิ้นแทนผู้ซื้อ

9.1 ผู้เสนอราคามีหน้าที่บำรุงรักษาและซ่อมแซมแก้ไขคอมพิวเตอร์ให้อยู่ในสภาพใช้งานได้ดีอยู่เสมอตลอดระยะเวลาดังกล่าวในวรรคหนึ่งด้วยค่าใช้จ่ายของผู้เสนอราคา โดยมีเวลาคอมพิวเตอร์ขัดข้องรวมตามเกณฑ์การคำนวณเวลาขัดข้องไม่เกินเดือนละ 14 (สิบสี่) ชั่วโมง หรือร้อยละ 2 (สอง) ของเวลาใช้งานทั้งหมดของคอมพิวเตอร์ของเดือนนั้น แล้วแต่ตัวเลขใดจะมากกว่ากัน มิฉะนั้นผู้เสนอราคาต้องยอมให้ผู้ซื้อคิดค่าปรับเป็นรายชั่วโมง ในอัตราร้อยละ 0.025 (ศูนย์จุดศูนย์สองห้า) ของราคาทั้งหมดตามสัญญานี้ ในเวลาที่ไม่สามารถใช้คอมพิวเตอร์ได้ในส่วนที่เกินกว่ากำหนดเวลาขัดข้องข้างต้น

เกณฑ์การคำนวณเวลาขัดข้องของคอมพิวเตอร์ ให้เป็นดังนี้

- กรณีที่คอมพิวเตอร์เกิดขัดข้องพร้อมกันหลายหน่วย ให้นับเวลาขัดข้องของหน่วยที่มีตัวถ่วงมากที่สุดเพียงหน่วยเดียว

- กรณีความเสียหายอันสืบเนื่องมาจากความขัดข้องของคอมพิวเตอร์แตกต่างกัน เวลาที่ใช้ในการคำนวณค่าปรับจะเท่ากับเวลาขัดข้องของคอมพิวเตอร์หน่วยนั้นคูณด้วยตัวถ่วงซึ่งมีค่าต่างๆ ตามเอกสารแนบ

9.2 ผู้เสนอราคาต้องบำรุงรักษาซอฟต์แวร์ที่เกี่ยวข้องกับ “โครงการซื้อระบบรักษาความมั่นคงปลอดภัยสำหรับเครือข่ายสารสนเทศเพื่อการพัฒนาการศึกษา” ตลอดระยะเวลาการรับประกัน เมื่อมีการเปลี่ยนแปลง แก้ไข ปรับปรุง เพิ่มเติมซอฟต์แวร์ ในลักษณะการ Update, Release หรือ Version ใหม่ของระบบที่เสนอให้ทันสมัยขึ้นและเหมาะสม ผู้เสนอราคาต้องเข้าดำเนินการติดตั้งให้โดยไม่คิดค่าใช้จ่ายใด ๆ

1..... 2..... 3..... 4..... 5.....

9.3 ในระยะเวลารับประกันตามสัญญาผู้เสนอราคาต้องบำรุงรักษาเชิงป้องกัน (Preventive Maintenance) ทุกจุดที่ติดตั้งอย่างน้อย 4 ครั้งต่อปี (3 เดือนต่อครั้ง) เพื่อให้ระบบอยู่ในสภาพที่ใช้งานได้ตลอดระยะเวลา โดยบำรุงรักษาในเวลาที่ไม่กระทบกระเทือนต่อการปฏิบัติงาน พร้อมจัดทำรายงาน ดังนี้

- Attacks Report
- Malware Report
- Traffic Report
- Web activity Report
- Performance and Utilization Report

เป็นอย่างน้อย หากผู้เสนอราคาไม่ปฏิบัติตาม สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม มีสิทธิปรับตามเกณฑ์การคำนวณเป็นไปตามข้อ 12.2

10. การรับประกันคุณภาพ

ผู้เสนอราคารับรองว่าคอมพิวเตอร์ที่ขายให้ตามสัญญาเป็นของแท้ ของใหม่ ไม่ใช่เครื่องที่ใช้งานแล้วนำมาปรับปรุงสภาพขึ้นใหม่และมีคุณสมบัติไม่ต่ำกว่าที่กำหนดไว้ตามรายละเอียด และคุณลักษณะเฉพาะของอุปกรณ์ที่กำหนดไว้

11. ระยะเวลาในการดำเนินงาน/ระยะเวลาส่งมอบงาน

กำหนดระยะเวลาดำเนินการภายใน 180 วัน นับถัดจากวันลงนามในสัญญา สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม จะแบ่งการจ่ายเงินเป็นงวด ๆ และจ่ายเงินต่อเมื่อผู้เสนอราคาได้ปฏิบัติงานในงวดงานนั้น ๆ และคณะกรรมการตรวจรับพัสดุได้ทำการตรวจรับไว้เรียบร้อยแล้วดังนี้

งวดที่ 1 ในอัตราร้อยละ 5 ของราคาทั้งหมดตามสัญญา จะจ่ายเมื่อผู้เสนอราคาได้ดำเนินการดังต่อไปนี้ ถูกต้องครบถ้วนภายใน 60 วัน นับถัดจากวันลงนามในสัญญา

ลำดับ	การดำเนินงาน	เอกสารที่ต้องนำส่ง
1	ประชุมร่วมกับคณะกรรมการตรวจรับพัสดุและเจ้าหน้าที่ของสำนักงานบริหารเทคโนโลยีเพื่อพัฒนาการศึกษา (UniNet) เพื่อนำเสนอแผนดำเนินโครงการฯ	■ เอกสารสรุปรายงานการประชุม ■ แผนการการดำเนินโครงการ (Project Management Document)

1..... 2..... 3..... 4..... 5.....

ลำดับ	การดำเนินงาน	เอกสารที่ต้องนำส่ง
2	ประชุมร่วมกับคณะกรรมการตรวจรับพัสดุและเจ้าหน้าที่ของสำนักงานบริหารเทคโนโลยีเพื่อพัฒนาการศึกษา (UniNet) เพื่อออกแบบระบบ	■ เอกสารการออกแบบระบบและการใช้งานอุปกรณ์ที่จัดหาในโครงการ (Detail Design Document)
3	สำรวจจุดติดตั้งอุปกรณ์	■ เอกสารสำรวจพื้นที่ติดตั้งอุปกรณ์ (Shop Drawing and Site Preparation Document)
4	เสนอขั้นตอนการทดสอบคุณสมบัติอุปกรณ์	■ เอกสารขั้นตอนการทดสอบอุปกรณ์ (Test Plan Document)

งวดที่ 2 ในอัตราร้อยละ 95 ของราคาทั้งหมดตามสัญญา จะจ่ายเมื่อผู้เสนอราคาได้ดำเนินการดังต่อไปนี้ ถูกต้องครบถ้วนภายใน 180 วัน นับถัดจากวันลงนามในสัญญา

ลำดับ	การดำเนินงาน	เอกสารที่ต้องนำส่ง
1	ส่งมอบอุปกรณ์	■ เอกสารรายการอุปกรณ์พร้อมราคา
2	ทดสอบคุณสมบัติอุปกรณ์	■ เอกสารผลการทดสอบคุณสมบัติอุปกรณ์
3	ติดตั้งอุปกรณ์และการใช้งานระบบ	■ เอกสารรายงานผลการติดตั้งอุปกรณ์ทั้งหมด และ AS-Built Drawing
4	อบรมการใช้งานระบบ	■ เอกสารการจัดฝึกอบรมการใช้งานระบบ

1..... 2..... 3..... 4..... 5.....

ลำดับ	การดำเนินงาน	เอกสารที่ต้องนำส่ง
5	เสนอแผนขั้นตอนการบำรุงรักษา แผนการดำเนินการเข้าบำรุงรักษา	▪ เอกสารขั้นตอนการบำรุงรักษา แผนการดำเนินการเข้าบำรุงรักษา
6	เอกสารรายงานของระบบ	▪ Attacks Report ▪ Malware Report ▪ Traffic Report ▪ Web activity Report ▪ Performance and Utilization Report
7	สรุปโครงการ	▪ รายงานสรุปโครงการฉบับสมบูรณ์ (Final Report)

12. อัตราค่าปรับ

12.1 หากผู้เสนอราคาไม่สามารถส่งมอบงาน “โครงการซื้อระบบรักษาความมั่นคงปลอดภัยสำหรับเครือข่ายสารสนเทศเพื่อการพัฒนาการศึกษา” ภายในกำหนดระยะเวลาในสัญญา สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรมมีสิทธิปรับผู้เสนอราคาเป็นรายวันในอัตราร้อยละ 0.1 (ศูนย์จุดหนึ่ง) ของราคาทั้งหมดตามสัญญานับถัดจากวันครบกำหนดตามสัญญาจนถึงวันที่ผู้เสนอราคาได้นำสิ่งของมาส่งมอบพร้อมติดตั้งให้แก่ผู้ซื้อจนถูกต้องครบถ้วน

สูตรการคำนวณค่าปรับ

ค่าปรับ = (วงเงินตามสัญญา x 0.1/100) x (ระยะเวลาที่ใช้ในการคำนวณค่าปรับ)

ระยะเวลาที่ใช้ในการคำนวณค่าปรับ = วันที่ส่งงานงวดสุดท้ายเป็นที่ถูกต้องครบถ้วน – วันที่ครบกำหนดตามสัญญา

12.2 หากพ้นกำหนดเวลาในข้อ 9.3 ผู้เสนอราคาต้องชำระค่าปรับเป็นรายครั้ง ในอัตราร้อยละ 0.1 (ศูนย์จุดหนึ่ง) ของราคาทั้งหมดตามสัญญา

สูตรการคำนวณค่าปรับ

ค่าปรับ = (วงเงินตามสัญญา x 0.1/100) x (จำนวนครั้งที่ไม่เข้าดำเนินการ)

1..... 2..... 3..... 4..... 5.....

13. หลักเกณฑ์และสิทธิในการพิจารณาการเสนอราคา

13.1 ราคาของ "โครงการซื้อระบบรักษาความมั่นคงปลอดภัยสำหรับเครือข่ายสารสนเทศเพื่อการพัฒนาการศึกษา" ที่เสนอจะต้องรวมถึงการติดตั้ง การซ่อมแซมแก้ไขและปรับเปลี่ยนอะไหล่และ/หรืออุปกรณ์ และ/หรือส่วนหนึ่งส่วนใดของอุปกรณ์ระบบเครือข่าย และ/หรือวัสดุที่เกี่ยวข้องกับการทำงานของอุปกรณ์ ได้แก่ แบตเตอรี่หรือถ่านไฟฉายของอุปกรณ์ UPS, Main Board และ/หรือการปรับเปลี่ยนโยกย้ายอุปกรณ์ในระบบ เป็นต้น (ยกเว้นวัสดุสิ้นเปลืองประเภท กระดาษ-พิมพ์ ผงหมึก) ทั้งนี้ อุปกรณ์ใดๆ ในโครงการ หากเกิดการชำรุดเสียหายจนไม่อาจซ่อมแซมได้ และ/หรือกรณีซ่อมแซมแล้วแต่ไม่สามารถใช้งานได้ดีดังเดิม จะต้องจัดหาอุปกรณ์ระบบเครือข่ายเป็นของใหม่ที่มีมาตรฐานและความสามารถในการทำงานเทียบเท่าหรือคุณสมบัติไม่น้อยไปกว่าเดิม ตลอดจนสัมภาระทั้งหมดและเครื่องมือต่าง ๆ สำหรับใช้ทำการงานให้สำเร็จรวมถึงภาษีมูลค่าเพิ่ม ภาษีอากรอื่น ๆ และค่าใช้จ่ายทั้งปวงไว้ด้วยแล้ว มาทดแทนโดยไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้น

13.2 ในการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม จะพิจารณาตัดสินโดยใช้หลักเกณฑ์ราคาและจะพิจารณาจากราคารวม

14. ข้อกำหนดการทำเอกสารข้อเสนอ

14.1 ในการจัดทำข้อเสนองานซื้อ "โครงการซื้อระบบรักษาความมั่นคงปลอดภัยสำหรับเครือข่ายสารสนเทศเพื่อการพัฒนาการศึกษา" ที่เสนอให้จัดทำในรูปแบบ ดังนี้

หัวข้อ	ข้อกำหนดที่ต้องการ	ข้อเสนอของผู้เสนอราคา	เอกสารอ้างอิง (หน้า,ข้อ)
ระบุหัวข้อให้ตรงกับที่สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรมกำหนด	- หัวข้อ TOR ข้อ 3 คุณสมบัติของผู้เสนอราคา - หัวข้อ TOR ข้อ 4 ขอบเขตของการดำเนินงาน - หัวข้อ TOR ข้อ 5 คุณสมบัติเฉพาะทางเทคนิค (ให้คัดลอกข้อกำหนดของ สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม)	ให้ระบุข้อเสนอของงานที่เสนอ	ให้ระบุหรืออ้างถึงเอกสารในข้อเสนอที่เกี่ยวข้อง

14.2 นำเสนอเอกสารเพื่อสำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม ใช้ประกอบการพิจารณาผลการประกวดราคาอย่างน้อยต้องมีเอกสารดังต่อไปนี้

(1) จัดทำตารางแสดงรายการอุปกรณ์

1..... 2..... 3..... 4..... 5.....

(2) จัดทำขั้นตอนการดำเนินงานโดยสรุปตลอดระยะเวลาการดำเนินการโครงการในรูปแบบแผนภูมิเวลา (Gantt chart)

(3) จัดทำรายละเอียดของแบบรูปรายการ แค็ตตาล็อก และข้อกำหนดคุณลักษณะเฉพาะของอุปกรณ์และชิ้นส่วนต่าง ๆ ที่เสนอโดยต้องเน้นหรือทำเครื่องหมายกำกับคุณลักษณะที่ตรงกับข้อกำหนดฯ ที่ระบุไว้

(4) จัดทำรายละเอียดคุณลักษณะเฉพาะ (Specification) และอื่น ๆ อย่างน้อย ได้แก่ Compliance Statement, Equipment List or Bill of Quantities, Product Catalog เป็นต้น

(5) จัดทำข้อเสนออื่น ๆ ตามที่ผู้ประสงค์จะเสนอราคาจะนำเสนอและที่เป็นประโยชน์ต่อการพิจารณาของคณะกรรมการฯ (ถ้ามี)

(6) ผู้เสนอราคาต้องเสนอระบบ ประกอบด้วยฮาร์ดแวร์ ซอฟต์แวร์ และสิทธิการใช้งานที่จำเป็น เพื่อให้ระบบสามารถทำงานได้ตามข้อกำหนดนี้ พร้อมทั้งอธิบายและแสดงเอกสารประกอบที่จำเป็นเพื่อทำให้เชื่อได้ว่าระบบที่นำเสนอมีความสามารถตามข้อกำหนดนี้

(7) เอกสารหลักฐานหรือหนังสือรับรองผลงาน และสำเนาสัญญา ตามข้อ 3.12 และ ข้อ 3.13

15. วงเงินในการจัดหา

ใช้เงินจากจากเงินปีงบประมาณ พ.ศ.2566 ไปพลางก่อน แผนงานพื้นฐานด้านการพัฒนาเสริมสร้างศักยภาพทรัพยากรมนุษย์ ผลผลิตที่ 1 : สถาบันการศึกษาได้รับบริการเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา กิจจกรรม : บริการระบบเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา งบลงทุน ค่าครุภัณฑ์ ระบบรักษาความมั่นคงปลอดภัยสำหรับเครือข่ายสารสนเทศเพื่อพัฒนาการศึกษา และงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. 2567 ในงบรายจ่ายโครงการเดียวกัน เมื่อพระราชบัญญัติงบปประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. 2567 ประกาศบังคับใช้ และได้รับจัดสรรจากสำนักงบประมาณ วงเงิน 75,000,000.- บาท (เจ็ดสิบห้าล้านบาทถ้วน)

16. การรักษาความลับ

16.1 ผู้เสนอราคาต้องตกลงจะไม่เปิดเผยรายละเอียดเกี่ยวกับงาน (System Specification) และจะเก็บรักษาข้อมูล และหรือเอกสารอื่นใดที่เกี่ยวข้องกับโครงการนี้ไว้เป็นความลับ เว้นแต่เป็นการเปิดเผยเพื่อประโยชน์หรือความจำเป็นในการปฏิบัติตามสัญญาหรือเป็นกรณีจำเป็นต้องเปิดเผยตามกฎหมายหรือคำสั่งศาล หรือได้รับความยินยอมจากผู้ซื้อเป็นลายลักษณ์อักษรหรือเป็นข้อมูลและหรือเอกสารที่ได้เปิดเผยต่อสาธารณชนแล้ว

16.2 ผู้เสนอราคาต้องตกลงว่าบรรดาข้อมูล เอกสาร และความลับทางธุรกิจของผู้ซื้อทั้งปวงที่ติดต่อสื่อสารมาจากผู้ซื้อไม่ว่าลักษณะใด ๆ ที่เกี่ยวพันกับโครงการนี้ ไม่ว่าก่อนหรือหลังจากวันที่ลงนามในสัญญาฯ ถือว่าเป็นข้อมูลความลับของผู้ซื้อ ซึ่งผู้เสนอราคาจะต้องนำข้อมูลดังกล่าวไปใช้เพื่อให้บรรลุวัตถุประสงค์ตามสัญญาฯ ผู้เสนอราคามีหน้าที่รับผิดชอบในการควบคุมดูแลพนักงาน ลูกจ้าง ตัวแทนและหรือบุคลากรของผู้เสนอราคา ไม่ให้เปิดเผยข้อมูลความลับของผู้ซื้อให้แก่บุคคลที่สาม โดยปราศจากความยินยอมล่วงหน้าเป็นลายลักษณ์อักษรจากผู้ซื้อ

1.....  ..... 2.....  ..... 3.....  ..... 4.....  ..... 5.....  .....

16.3ผู้เสนอราคาเข้าใจและยอมรับว่าข้อมูลหรือเอกสารใด ๆ ที่เกี่ยวข้องกับการปฏิบัติงานตามสัญญาฉบับนี้เป็นทรัพย์สินของผู้ซื้อ ผู้เสนอราคาจะใช้ข้อมูลและหรือเอกสารดังกล่าว ในการปฏิบัติงานให้เป็นไปตามวัตถุประสงค์ของสัญญาฯ นี้เท่านั้นและจะต้องเก็บรักษาข้อมูลและหรือเอกสารดังกล่าวไว้เป็นความลับ โดยจะเปิดเผยต่อบุคคลอื่นไม่ได้เป็นอันขาด เว้นแต่จะได้รับความยินยอมจากผู้ซื้อเป็นลายลักษณ์อักษร และตกลงจะควบคุมดูแลให้บุคลากร พนักงาน ลูกจ้าง และหรือตัวแทนของผู้เสนอราคาปฏิบัติเช่นเดียวกันกับผู้เสนอราคาด้วย ในกรณีที่สัญญานี้สิ้นสุดลงไม่ว่าด้วยเหตุใด ๆ ผู้เสนอราคาต้องตกลงส่งมอบบรรดาข้อมูลและเอกสารดังกล่าวคืนให้แก่ผู้ซื้อทันที

16.4ผู้เสนอราคาตกลงจะเก็บรักษาข้อมูลใด ๆ ที่ได้รับมาเนื่องจากการปฏิบัติงานตามสัญญาฯ ไว้เป็นความลับตลอดไป แม้ว่าสัญญาฯ จะสิ้นสุดลงไม่ว่าด้วยเหตุใด ๆ ก็ตาม

17. การติดต่อสอบถามรายละเอียดเพิ่มเติม

สาธารณชนที่ต้องการเสนอแนะ วิจารณ์ หรือมีความเห็นเกี่ยวกับร่างขอบเขตงาน (Terms of Reference : TOR) และร่างเอกสารการประกวดราคาซื้อระบบรักษาความมั่นคงปลอดภัยสำหรับเครือข่ายสารสนเทศเพื่อการพัฒนาการศึกษา ในครั้งนี้ ให้แจ้งเป็นลายลักษณ์อักษร ไปยังหน่วยงานโดยเปิดเผยตัวในช่องทางดังต่อไปนี้

ชื่อ ผู้ติดต่อ นายกษิดิศ ศรีอำไพพร

(1) จดหมายลงทะเบียน (EMS)

(2) ไปรษณีย์อิเล็กทรอนิกส์ procurement@uni.net.th

ข้อมูลการติดต่อ : สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม
สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา (ฝ่ายบริหารระบบเครือข่าย)
เลขที่ 328 ถนนศรีอยุธยา แขวงทุ่งพญาไท
เขตราชเทวี กรุงเทพ 10400
โทรศัพท์ : 0 2232 4000

1..... 2..... 3..... 4..... 5.....

เอกสารแนบ

รายละเอียดการใช้ระบบรักษาความมั่นคงปลอดภัยสำหรับเครือข่ายสารสนเทศเพื่อการพัฒนาการศึกษา

ประจำปีงบประมาณ พ.ศ. 2567

ลำดับ	รายการ	ค่าตัวถ่วง
1	ระบบบริหารเหตุการณ์และข้อมูลการรักษาความมั่นคงปลอดภัย (Security Information and Event Management: SIEM จำนวน 5 เครื่อง	1
2	ระบบบริหารการตอบสนองภัยคุกคามแบบอัตโนมัติ จำนวน 1 เครื่อง	1
3	อุปกรณ์ตรวจสอบและวิเคราะห์กระแสการรับส่งข้อมูลเครือข่าย (Network Traffic Flow) จำนวน 2 ระบบ	1
4	อุปกรณ์ควบคุมดูแลและจำกัดภัยคุกคาม (Threat Mitigation System) ในรูปแบบการปฏิเสธการให้บริการแบบวงกว้าง (Distributed Denial of Service – DDoS) จำนวน 1 ระบบ	1
5	อุปกรณ์กระจายสัญญาณ ขนาดไม่น้อยกว่า 48 ช่องสัญญาณ จำนวน 2 เครื่อง	1

1..... 2..... 3..... 4..... 5.....