

(ร่าง) ขอบเขตของงาน (Terms of Reference: TOR)
จ้างเหมาบริการยกระดับศักยภาพของระบบความมั่นคงปลอดภัยทางไซเบอร์อย่างยั่งยืน
สำหรับสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

1. หลักการและเหตุผล

จากแผนแม่บทภายใต้ยุทธศาสตร์ชาติ (พ.ศ. 2566 - 2580) ฉบับปรับปรุง ในประเด็นเรื่องความมั่นคง ซึ่งมีเป้าหมายแผนแม่ทอย่อย เรื่องปัญหาความมั่นคงที่มีอยู่ในปัจจุบัน (เช่น ปัญหายาเสพติด ความมั่นคงทางไซเบอร์ การค้ามนุษย์ ฯลฯ) และมีตัวชี้วัด เรื่องดัชนีความปลอดภัยจากภัยคุกคาม อันสอดคล้องกันกับมาตรา 44 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 สำหรับหน่วยงานภาครัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 ประกอบด้วย (1) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก และ (2) แผนการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งการรับมือภัยคุกคามทางไซเบอร์ โดยมุ่งเน้นการตรวจสอบควบคุมความปลอดภัยของข้อมูล ป้องกัน ฝ่าละอองและการตอบสนอง พร้อมทั้งการแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์ รวมถึงการบริหารจัดการนโยบายและมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ ตั้งแต่ปีงบประมาณ พ.ศ. 2566 - 2568 สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ได้มีการดำเนินการให้สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยมีการศึกษา วิเคราะห์ ออกแบบ จัดทำสถาปัตยกรรมและดำเนินงานให้สอดคล้องกับมาตรฐานสากล ในการฝ่าละออง บริหารจัดการ ติดตาม และวิเคราะห์ผลที่ได้จากระบบด้านความมั่นคงปลอดภัยทางไซเบอร์ เพื่อยกระดับศักยภาพความมั่นคงปลอดภัยไซเบอร์ (Security Maturity Uplift) ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

โดยปีงบประมาณ พ.ศ. 2568 สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ได้มีการดำเนินการออกแบบสถาปัตยกรรมความมั่นคงปลอดภัยทางไซเบอร์ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน (Enterprise Security Architecture Blueprint) ให้มีความปลอดภัยอย่างยั่งยืน สามารถป้องกันภัยคุกคามทางไซเบอร์แบบเชิงรุกและสามารถป้องกันก่อนที่จะเกิดเหตุภัยคุกคามได้ มีการตรวจสอบภัยคุกคามผ่านบริการข่าวกรองภัยคุกคามทางไซเบอร์ (Threat Intelligence) มีบริการตรวจจับและป้องกันภัยคุกคามทางไซเบอร์ (Extended Detection and Response of Cyber Security) สามารถป้องกันการโจมตีเครื่องคอมพิวเตอร์แม่ข่ายที่มีข้อมูลสำคัญ และมีการจัดเตรียมผู้เชี่ยวชาญในการฝ่าละออง บริหารจัดการ ติดตาม และวิเคราะห์ผล รวมถึงการจัดตั้งศูนย์ปฏิบัติการการรักษาความมั่นคงปลอดภัยทางไซเบอร์จากภายนอก (External Cybersecurity Operation Center) ในการตรวจสอบการถูกบุกรุก (Compromise Assessment) การตอบสนอง และการกำจัดภัยคุกคามทางไซเบอร์ (Incident Response)

ดังนั้น ในปีงบประมาณ พ.ศ. 2569 สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน จึงมีความจำเป็นต้องดำเนินการเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์อย่างต่อเนื่องและเพิ่มเติมให้สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ในการปรับปรุงและพัฒนานโยบาย มาตรฐาน และกระบวนการให้สอดคล้องกับหลักการทางไซเบอร์ในปัจจุบัน ในส่วนต่าง ๆ ทั้งในด้านการตรวจสอบมาตรฐานความปลอดภัยทางสารสนเทศขององค์กรในเชิงรุก ด้านการระบุและตรวจจับโดยใช้เทคโนโลยีที่ทันสมัยด้านการฝึกอบรมเพื่อสร้างความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์เพื่อลดโอกาสการหลอกลวงทางไซเบอร์ (Social Engineering)

1.  2.  3.  4.  5.  6. 
7.  8.  9.  10.  11. 

และมีผู้เชี่ยวชาญที่มีความรู้และประสบการณ์ ในการตอบสนองต่อภัยคุกคาม และการมีศูนย์ปฏิบัติการการรักษาความมั่นคงปลอดภัยทางไซเบอร์จากภายนอก (External Cybersecurity Operation Center) ทำให้การบริหารจัดการความเสี่ยงทางไซเบอร์มีประสิทธิภาพ

2. วัตถุประสงค์

2.1 เพื่อจัดทำและทบทวนมาตรฐาน นโยบาย และกระบวนการในการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ ให้มีความสอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และตามข้อกำหนดของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

2.2 เพื่อให้ผู้เชี่ยวชาญให้คำแนะนำ และแก้ไขปัญหาด้านการบริหารจัดการนโยบายและมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์

2.3 เพื่อเพิ่มประสิทธิภาพและความต่อเนื่องในการตรวจจับความเสี่ยงของระบบสารสนเทศจากภัยคุกคามทางไซเบอร์ที่มาจากภายนอก (Attack Surface Management)

2.4 เพื่อตรวจสอบและยกระดับมาตรฐานความปลอดภัยทางข้อมูลสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานในเชิงรุก (Proactive Security Assessment)

2.5 เพื่อเพิ่มประสิทธิภาพในการตรวจจับและป้องกันภัยคุกคามทางไซเบอร์ (Extended Detection and Response of Cyber Security) และการตรวจจับภัยคุกคามขั้นสูง (Advance Persistence Threat) กับระบบคอมพิวเตอร์แม่ข่ายที่ติดตั้งภายในศูนย์ข้อมูล (Data Center) ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

2.6 เพื่อตรวจสอบภัยคุกคามผ่านบริการข่าวกรองภัยคุกคามทางไซเบอร์ (Threat Intelligence) ที่เข้ามาโจมตีระบบเทคโนโลยีดิจิทัลและสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

2.7 เพื่อเฝ้าระวัง บริหารจัดการ ติดตาม และวิเคราะห์ผลที่ได้จากบริการความมั่นคงปลอดภัยทางไซเบอร์ ให้สามารถดำเนินการได้อย่างมีประสิทธิภาพ

2.8 เพื่อจัดตั้งศูนย์ปฏิบัติการการรักษาความมั่นคงปลอดภัยทางไซเบอร์จากภายนอก (External Cybersecurity Operation Center) ซึ่งมีผู้เชี่ยวชาญควบคุมและดูแล

2.9 เพื่อปรับปรุงแก้ไขเอกสารนโยบาย มาตรฐาน และกระบวนการที่เกี่ยวข้อง ให้เป็นปัจจุบันและสอดคล้องกับพระราชบัญญัติฯ

2.10 เพื่อพัฒนาบุคลากรส่วนกลางที่รับผิดชอบงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้มีความรู้และทักษะเกี่ยวกับการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ให้มีความต่อเนื่องและยั่งยืน

3. คุณสมบัติผู้เสนอราคา

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

1.  2.  3.  4.  5.  6. 
7.  8.  9.  10.  11. 

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทำงาน และได้แจ้งเวียนชื่อให้เป็นผู้ทำงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทำงานเป็นหุ้นส่วน ผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นนิติบุคคลผู้มีอาชีพรับจ้างงานที่ประกวดราคาด้วยวิธีการทางอิเล็กทรอนิกส์ดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้เสนอราคารอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้รับเอกลิทธิหรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้เสนอราคาได้มีคำสั่งให้สละเอกลิทธิความคุ้มกันเช่นนั้น

3.10 ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ “กิจการร่วมค้า” ต้องมีคุณสมบัติดังนี้

3.10.1 การกำหนดสัดส่วนการเข้าร่วมค้าของคู่สัญญา

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงฯ จะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

3.10.2 กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

3.10.3 การยื่นข้อเสนอของกิจการร่วมค้า

3.10.3.1 กรณีที่ข้อตกลงฯ กำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

3.10.3.2 การยื่นข้อเสนอด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e - bidding) ให้ผู้เข้าร่วมค้าที่ได้รับมอบหมายหรือมอบอำนาจตามข้อ 3.10.3.1 ดำเนินการซื้อเอกสารประกวดราคาอิเล็กทรอนิกส์ กรณีที่มีการจำหน่ายเอกสารซื้อหรือจ้าง

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

3.12 ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

3.12.1 กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งตามกฎหมายไทยหรือต่างประเทศซึ่งได้จดทะเบียนเกินกว่า 1 ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก 1 ปีสุดท้ายก่อนวันที่ยื่นข้อเสนอ งบแสดงฐานะการเงิน 1 ปีสุดท้ายก่อนวันยื่นข้อเสนอ หมายถึง งบแสดงฐานะการเงินย้อนไปก่อนวันที่หน่วยงานของรัฐกำหนดให้เป็นวันยื่นข้อเสนอ 1 ปีปฏิทิน เว้นแต่กรณีนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย

1.  2.  3.  4.  5.  6. 
7.  8.  9.  10.  11. 

หากวันยื่นข้อเสนอเป็นช่วงระยะเวลาที่กรมพัฒนาธุรกิจการค้ากำหนดให้นิติบุคคลยื่นงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ซึ่งจะอยู่ในช่วงเดือนมกราคม - เดือนพฤษภาคม ของทุกปี โดยนิติบุคคลที่เป็นผู้ยื่นข้อเสนออยู่นั้นยังอยู่ในช่วงของการยื่นงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า คือ ช่วงเดือนมกราคม - เดือนพฤษภาคม กรณีนี้ให้สามารถยื่นงบแสดงฐานะการเงินย้อนหลังไปอีก 1 ปี ได้

3.12.2 กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีกรารายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า หรือกรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศซึ่งยังไม่มีกรารายงานงบแสดงฐานะการเงิน ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียนโดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอไม่ต่ำกว่า 3 ล้านบาท

3.12.3 กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ สามารถดำเนินการได้ดังนี้

3.12.3.1 กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุน หรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้าประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทย แจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน 90 วัน

3.12.3.2 กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุน หรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้าประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ หรือเป็นสินเชื่อที่ธนาคารต่างประเทศ หรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้าประกันตามประกาศของธนาคารกลางต่างประเทศนั้น ตามรายชื่อบริษัทที่ธนาคารกลางต่างประเทศนั้นแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน 90 วัน

3.12.4 กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศที่มีได้ถือสัญชาติไทย ตามข้อ 3.12.2 และข้อ 3.12.3.2 มูลค่าจะต้องเป็นไปตามอัตราแลกเปลี่ยนเงินตราตามประกาศที่ธนาคารแห่งประเทศไทยกำหนด ในช่วงระหว่างวันที่เผยแพร่ประกาศและเอกสารเชิญชวนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (e - GP) หรือมีหนังสือเชิญชวน จนถึงวันเสนอราคา

ทั้งนี้ ผู้ยื่นข้อเสนอจะต้องยื่นเอกสารที่แสดงให้เห็นถึงข้อมูลเกี่ยวกับมูลค่าสุทธิของกิจการแล้วแต่กรณี ประกอบกับเอกสารดังกล่าวจะต้องผ่านการรับรองตามระเบียบกระทรวงการต่างประเทศว่าด้วยการรับรองเอกสาร พ.ศ. 2539 และที่แก้ไขเพิ่มเติม กำหนด โดยจะต้องยื่นเอกสารดังกล่าวในวันยื่นข้อเสนอ หากผู้ยื่นข้อเสนอไม่ได้มีการยื่นเอกสารดังกล่าวมาพร้อมกับการยื่นข้อเสนอให้ถือว่าผู้ยื่นข้อเสนอรายนั้นยื่นเอกสารไม่ครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารประกวดราคา

1.  2.  3.  4.  5.  6. 
7.  8.  9.  10.  11. 

3.12.5 กรณีตามข้อ 3.12.1 – ข้อ 3.12.4 ไม่ใช่บังคับกับกรณีดังต่อไปนี้

3.12.5.1 กรณีผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐภายในประเทศ

3.12.5.2 นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย พ.ศ. 2483 และที่แก้ไขเพิ่มเติม

3.13 ผู้ยื่นข้อเสนอต้องมีผลงานประเภทเดียวกันในการจัดทำครั้งนี้ โดยเป็นผลงานที่แล้วเสร็จในสัญญาเดียว มีมูลค่าของผลงานไม่น้อยกว่า 9,500,000 บาท (เก้าล้านห้าแสนบาทถ้วน) และเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับหน่วยงานของรัฐหรือหน่วยงานเอกชนที่สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานเชื่อถือโดยให้ยื่นเอกสารหนังสือรับรองผลงานและสำเนาสัญญาขณะเข้าเสนอราคา ทั้งนี้ คณะกรรมการพิจารณาผลขอสงวนสิทธิ์ในการที่จะดำเนินการตรวจสอบเอกสารหนังสือรับรองผลงานและสำเนาสัญญาไปยังหน่วยงานที่ออกเอกสาร

4. ขอบเขตการดำเนินงาน

ผู้รับจ้างต้องดำเนินการให้ครอบคลุมตามขอบเขตการดำเนินงาน โดยมีรายละเอียด อย่างน้อยดังนี้

4.1 การจัดทำแผนการบริหารโครงการ แผนการดำเนินการโครงการ และประชุมเริ่มโครงการ (Kick-off Meeting) อย่างน้อยดังนี้

4.1.1 จัดทำแผนการบริหารโครงการและแผนการดำเนินการโครงการ โดยกำหนดระยะเวลาในการดำเนินการแต่ละกิจกรรมอย่างชัดเจน เพื่อให้คณะกรรมการตรวจรับพัสดุ พิจารณออนุมัติก่อนเริ่มดำเนินการ ประกอบด้วย

4.1.1.1 แผนการบริหารโครงการ (Project Management Plan)

4.1.1.2 แผนการดำเนินการโครงการ (Implementation Plan) ประกอบด้วยรายละเอียดดังนี้

- 1) บริการบริหารความเสี่ยงระบบสารสนเทศของหน่วยงานจากเครือข่ายภายนอก (Attack Surface Management)
- 2) บริการตรวจจับการโจมตีและตอบสนองภัยคุกคาม (Extended Detection and Response: XDR)
- 3) บริการป้องกันไวรัส (Antivirus)
- 4) บริการข่าวกรองภัยคุกคามทางไซเบอร์ (Threat Intelligence)
- 5) การบำรุงรักษาเชิงป้องกัน (Preventive Maintenance) บริการข่าวกรองภัยคุกคามทางไซเบอร์ (Threat Intelligence)
- 6) บริการตรวจสอบและรายงานช่องโหว่ของระบบปฏิบัติการและแอปพลิเคชัน (Vulnerability Assessment Tool)
- 7) การบำรุงรักษาเชิงป้องกัน (Preventive Maintenance) บริการตรวจสอบและรายงานช่องโหว่ของระบบปฏิบัติการและแอปพลิเคชัน (Vulnerability Assessment Tool)

1.  2.  3.  4.  5.  6. 
7.  8.  9.  10.  11. 

4.1.2 จัดประชุมเริ่มโครงการ (Kick-off Meeting) และนำเสนอแผนการดำเนินการโครงการให้สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานทราบ

4.2 จัดบุคลากรให้คำแนะนำ ทบทวน และ/หรือจัดทำเอกสาร โดยมีรายละเอียดการดำเนินงานอย่างน้อยดังนี้

4.2.1 ทบทวน และ/หรือจัดทำเอกสารตามกรอบมาตรฐานทางไซเบอร์ (NIST Cybersecurity Framework) ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ในส่วนของการกำกับดูแลการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Govern) โดยประกอบไปด้วยเอกสารดังนี้

4.2.1.1 บริบทองค์กร (Organizational Context)

4.2.1.2 ข้อกำหนดบทบาทหน้าที่ในด้านความมั่นคงปลอดภัยทางไซเบอร์ภายในองค์กร และวัตถุประสงค์ด้านความมั่นคงปลอดภัยทางไซเบอร์ให้สอดคล้องกับแผนกลยุทธ์ด้านสารสนเทศ (Roles, Responsibilities, and Authorities)

4.2.1.3 นโยบายด้านความมั่นคงปลอดภัยไซเบอร์ (Policy)

4.2.1.4 แนวทางบริหารจัดการความเสี่ยงไซเบอร์ (Risk Management Strategy)

4.2.1.5 มาตรฐานการบริหารความเสี่ยงของห่วงโซ่อุปทาน (Cybersecurity Supply Chain Risk Management Standard)

4.2.2 ทบทวน และ/หรือจัดทำเอกสารตามกรอบมาตรฐานทางไซเบอร์ (NIST Cybersecurity Framework Assessment) ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ในส่วนของการระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify) โดยมีเอกสารการจัดการทรัพย์สิน (Asset Management) ดังนี้

4.2.2.1 ทบทวน และ/หรือจัดทำแผนภาพแสดงการไหลของข้อมูล (Data Flow Diagram) ของระบบสารสนเทศที่มีความสำคัญ (Critical IT System)

4.2.2.2 ทบทวน และ/หรือจัดทำทะเบียนทรัพย์สินอย่างน้อยปีละ 1 ครั้ง

4.2.2.3 ประเมินระดับความสำคัญของทรัพย์สินในหน่วยงาน

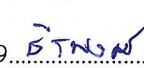
4.2.2.4 ทบทวน และ/หรือจัดทำนโยบายหรือกระบวนการในการจัดการทรัพย์สินขององค์กร (IT Asset Management)

4.2.2.5 ทบทวน และ/หรือจัดทำข้อกำหนดตัวชี้วัดในการรวบรวมทรัพย์สินและแนวทางการแก้ไขปรับปรุงการจัดการทรัพย์สินและตัวชี้วัด

4.2.3 ทบทวน และ/หรือจัดทำเอกสารตามกรอบมาตรฐานทางไซเบอร์ (NIST Cybersecurity Framework Assessment) ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ในส่วนของการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect) โดยประกอบไปด้วยเอกสาร อย่างน้อยดังนี้

4.2.3.1 การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศ (Access Control)

ทบทวน และ/หรือจัดทำนโยบายการเข้าถึงระบบสารสนเทศ (Access Control) และดำเนินการสื่อความให้ผู้เกี่ยวข้องรับทราบ

1.  2.  3.  4.  5.  6. 
7.  8.  9.  10.  11. 

4.2.3.2 การจัดทำแผนและหลักสูตรการฝึกอบรมด้านความมั่นคงปลอดภัยทางไซเบอร์ ให้สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน พิจารณาเห็นชอบก่อนดำเนินการฝึกอบรม และจัดฝึกอบรมในรูปแบบ Onsite พร้อมทั้งจัดทำสื่อการเรียนรู้ ดังนี้

- 1) ความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Awareness Training) ให้กับบุคลากรของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน จำนวนไม่น้อยกว่า 40 คน และมีระยะเวลาไม่น้อยกว่า 6 ชั่วโมง
- 2) ด้านความมั่นคงปลอดภัยสารสนเทศให้กับเจ้าหน้าที่ที่เกี่ยวข้อง ผู้เข้าอบรมจำนวนไม่น้อยกว่า 5 คน และมีระยะเวลาไม่น้อยกว่า 6 ชั่วโมง ในแต่ละด้าน ดังนี้
 - 2.1) อบรมด้าน Secure Coding ให้กับทีม Developer
 - 2.2) อบรมด้าน Security Monitoring ให้กับทีม Security
 - 2.3) อบรมด้าน General Security Awareness
- 3) จัดทำสื่อการเรียนรู้ในรูปแบบวิดีโอสั้น (Clip Video) ไม่น้อยกว่า 3 เรื่อง

4.2.3.3 การรักษาความปลอดภัยด้านข้อมูล (Data Security)

ทบทวน และ/หรือจัดทำนโยบายการปกป้องข้อมูลทั้งที่จัดเก็บภายในองค์กร (Data-at-rest) และที่ส่งต่อไปบนเครือข่ายสาธารณะ (Data-in-transit)

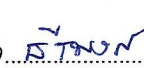
4.2.3.4 กระบวนการรักษาความปลอดภัยของข้อมูล (Information Protection Processes and Procedures)

- 1) ทบทวน และ/หรือจัดทำข้อกำหนดตั้งค่ามาตรฐาน (Configuration Baseline) ของอุปกรณ์ระบบสารสนเทศ ตามมาตรฐานความมั่นคงปลอดภัย CIS Baseline
- 2) ทบทวน และ/หรือจัดทำกระบวนการพัฒนาระบบอย่างมั่นคงปลอดภัย (Secure SDLC)
- 3) ทบทวน และ/หรือจัดทำนโยบายการบริหารจัดการช่องโหว่ของระบบ เทคโนโลยีสารสนเทศขององค์กร
- 4) ทบทวน และ/หรือจัดทำนโยบายควบคุมการเปลี่ยนแปลงของระบบ เทคโนโลยีสารสนเทศ (Change Management)
- 5) ทบทวน และ/หรือจัดทำนโยบายการสำรองและกู้คืนข้อมูลสารสนเทศ

4.2.3.5 การดูแลรักษา (Maintenance) ทบทวน และ/หรือจัดทำนโยบายบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศ

4.2.3.6 เทคโนโลยีที่ใช้ป้องกันภัยคุกคาม (Protective Technology)

- 1) ทบทวน และ/หรือจัดทำนโยบายการรักษาความปลอดภัยด้านเครือข่ายองค์กร (Network Security Policy & Standard)
- 2) ทบทวน และ/หรือจัดทำนโยบายการรักษาความปลอดภัยเครื่องคอมพิวเตอร์แม่ข่าย/เครื่องคอมพิวเตอร์ลูกข่าย (Endpoint Security Policy & Standard)

1.  2.  3.  4.  5.  6. 
 7.  8.  9.  10.  11. 

- 3) ทบทวน และ/หรือจัดทำนโยบายการบริหารจัดการความปลอดภัยทางไซเบอร์ (Security Monitoring Policy & Standard)
- 4) ทบทวน และ/หรือจัดทำนโยบายการจัดการอุปกรณ์ไอทีเคลื่อนที่ (Mobile Device) และอุปกรณ์ไอทีส่วนตัว (BYOD)

4.2.4 ทบทวน และ/หรือจัดทำเอกสารตามกรอบมาตรฐานทางไซเบอร์ (NIST Cybersecurity Framework Assessment) ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ในส่วนของมาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect) โดยประกอบไปด้วยเอกสาร อย่างน้อยดังต่อไปนี้

4.2.4.1 เหตุการณ์ผิดปกติ (Anomalies and Events)

- 1) กระบวนการตรวจสอบและวิเคราะห์เหตุการณ์ผิดปกติโดยสามารถระบุและจัดประเภทภัยคุกคามทางไซเบอร์
- 2) กระบวนการสำหรับวิเคราะห์เหตุการณ์ผิดปกติสามารถเกณฑ์แจ้งเตือนไปยังผู้เกี่ยวข้อง

4.2.4.2 การเฝ้าระวังอย่างต่อเนื่อง (Security Continuous Monitoring)

- 1) กระบวนการตรวจสอบกิจกรรมที่ไม่ได้รับอนุญาตโดยบุคคลที่ไม่มีสิทธิ
- 2) กระบวนการตรวจสอบและติดตามเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศจากผู้ให้บริการภายนอก

4.2.4.3 กระบวนการตรวจจับ (Detection Process)

ทบทวน และ/หรือจัดทำแผนการสื่อสารเหตุการณ์ด้านความมั่นคงปลอดภัยที่ตรวจจับได้ ไปยังผู้ที่เกี่ยวข้อง

4.2.5 ทบทวน และ/หรือจัดทำเอกสารตามกรอบมาตรฐานทางไซเบอร์ (NIST Cybersecurity Framework Assessment) ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ในส่วนของมาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond) โดยประกอบไปด้วยเอกสารดังนี้

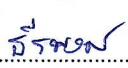
4.2.5.1 แผนการตอบสนองต่อภัยคุกคามทางไซเบอร์ (Response Planning) โดยจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan: CIRP) และสื่อสารให้ผู้เกี่ยวข้องรับทราบ

4.2.5.2 การสื่อสารด้านการตอบสนองต่อภัยคุกคามทางไซเบอร์ (Response Communications) โดยจัดทำแผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan) และสื่อสารให้ผู้เกี่ยวข้องรับทราบ

4.2.5.3 การวิเคราะห์ (Analysis) โดยจัดทำนโยบายการจัดเก็บและพิสูจน์หลักฐานอิเล็กทรอนิกส์ (Forensics) ที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์และดำเนินการกำหนดระดับผลกระทบของเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์และจัดลำดับความสำคัญของเหตุการณ์ที่เกิดขึ้น

4.2.5.4 การบรรเทาความเสี่ยง (Mitigation)

- 1) ทบทวน และ/หรือจัดทำนโยบายในการควบคุมและจำกัดเหตุการณ์ไม่ปกติเพื่อป้องกันภัยที่อาจจะเกิดขึ้นในอนาคต
- 2) ทบทวน และ/หรือจัดทำกระบวนการในการแจ้งเตือนผลกระทบที่อาจจะเกิดขึ้นจากเหตุการณ์ไม่ปกติไปยังหน่วยงานภายนอก

1.  2.  3.  4.  5.  6. 
7.  8.  9.  10.  11. 

- 3) ทบทวน และ/หรือจัดทำกลยุทธ์หรือขั้นตอนในการควบคุมความเหตุการณ์ ความมั่นคงปลอดภัยไซเบอร์ประเภทต่างๆ เช่น การรับมือ Ransomware

4.2.6 ทบทวน และ/หรือจัดทำเอกสารตามกรอบมาตรฐานทางไซเบอร์ (NIST Cybersecurity Framework Assessment) ที่จัดทำขึ้นตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ในส่วนของมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดขึ้นจากภัยคุกคามทางไซเบอร์ (Recover) โดยประกอบไปด้วยเอกสารดังนี้

4.2.6.1 การวางแผนด้านการกู้คืนระบบ (Recovery Planning)

- 1) เอกสารการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis)
- 2) เอกสารและนโยบายกำหนดระยะเวลาที่สำคัญในการกู้คืนระบบ ประกอบด้วย RTO, RPO และ MTPD
- 3) แผน BCP และ DRP สำหรับระบบงานสำคัญ

4.2.6.2 การสื่อสารด้านการกู้คืนระบบ (Recovery Communications) โดยจัดทำแผนการสื่อสารการกู้คืนระบบ (Recovery Communication Plan)

4.2.6.3 การพัฒนาปรับปรุงการกู้คืนระบบ (Recovery Improvement) โดยการทดสอบแผน BCP และ DRP สำหรับระบบงานที่สำคัญ และกำหนดตัวชี้วัดเพื่อวัดผลประสิทธิภาพของแผน

4.3 จัดเตรียมบริการบริหารความเสี่ยงระบบสารสนเทศของหน่วยงานจากเครือข่ายภายนอก (Attack Surface Management) ในรูปแบบซอฟต์แวร์พร้อมใช้งาน (Software-as-a-service) อย่างน้อยดังนี้

4.3.1 ออกแบบและจัดเตรียมบริการบริหารความเสี่ยงระบบสารสนเทศของหน่วยงานจากเครือข่ายภายนอก (Attack Surface Management) ตามแผนที่ได้เสนอไว้กับสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

4.3.2 ตั้งค่า (Configuration) บริการบริหารความเสี่ยงระบบสารสนเทศของหน่วยงานจากเครือข่ายภายนอก (Attack Surface Management) ตามรูปแบบที่ได้ศึกษา ออกแบบ และได้รับการอนุมัติ ในการดำเนินการตามที่สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานกำหนด

4.3.3 จัดเตรียมสิทธิการใช้งานบริการบริหารความเสี่ยงระบบสารสนเทศของหน่วยงานจากเครือข่ายภายนอก (Attack Surface Management) ในรูปแบบซอฟต์แวร์พร้อมใช้งาน (Software-as-a-service) จำนวน 1,000 ทรัพย์สินด้านสารสนเทศ (Digital Asset Inventory)

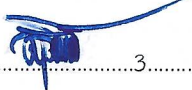
4.3.4 ตรวจสอบบริการบริหารความเสี่ยงระบบสารสนเทศของหน่วยงานจากเครือข่ายภายนอก (Attack Surface Management) ให้พร้อมใช้งานแบบ 24 ชั่วโมง 7 วัน

4.3.5 ประสานงานหน่วยงานที่เกี่ยวข้องกับสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน เพื่อแก้ไขช่องโหว่และความเสี่ยงที่ตรวจพบจากบริการบริหารความเสี่ยงระบบสารสนเทศของหน่วยงานจากภายนอก (Attack Surface Management)

4.3.6 สรุปรายงานรายเดือน (Monthly Report) ให้แก่สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน โดยครอบคลุมรายละเอียด อย่างน้อยดังนี้

4.3.6.1 คะแนนการป้องกันความเสี่ยง (Security Score) ที่เพิ่มขึ้นหรือลดลง โดยมีการเปรียบเทียบให้เห็นการเปลี่ยนแปลงในช่วงเวลาที่ผ่านมา

4.3.6.2 ช่องโหว่และความเสี่ยง (Vulnerabilities & Issues) ที่เพิ่มขึ้นและลดลง โดยมีการเปรียบเทียบให้เห็นการเปลี่ยนแปลงในช่วงเวลาที่ผ่านมา

1.  2.  3.  4.  5.  6. 
7.  8.  9.  10.  11. 

4.3.6.2 ช่องโหว่และความเสี่ยง (Vulnerabilities & Issues) ที่เพิ่มขึ้นและลดลง โดยมีการเปรียบเทียบให้เห็นการเปลี่ยนแปลงในช่วงเวลาที่ผ่านมา

4.3.6.3 ทรัพย์สินด้านสารสนเทศ (Digital Asset Inventory) ที่เพิ่มขึ้นและลดลง โดยมีการเปรียบเทียบให้เห็นการเปลี่ยนแปลงในช่วงเวลาที่ผ่านมา

4.3.6.4 ผลวิเคราะห์และแนวทางการแก้ไขเพื่อปิดช่องโหว่ (Gap Analysis)

4.3.6.5 ความคืบหน้าและสถานะการแก้ไขช่องโหว่และการปิดความเสี่ยง (Gap Closing)

4.4 จัดเตรียมบริการตรวจจัดการโจมตีและตอบสนองภัยคุกคาม (Extended Detection and Response: XDR) และบริการป้องกันไวรัส (Antivirus) โดยมีรายละเอียด อย่างน้อยดังนี้

4.4.1 ออกแบบและจัดเตรียมบริการตรวจจัดการโจมตีและตอบสนองภัยคุกคาม (Extended Detection and Response: XDR) และบริการป้องกันไวรัส (Antivirus) ตามแผนที่ได้เสนอไว้กับสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน โดยครอบคลุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และในรูปแบบ VM Server จำนวนไม่น้อยกว่า 300 เครื่อง

4.4.2 ตั้งค่า (Configuration) บริการตรวจจัดการโจมตีและตอบสนองภัยคุกคาม (Extended Detection and Response: XDR) ตามรูปแบบที่ได้ศึกษา ออกแบบ และได้รับการอนุมัติในการดำเนินการตามที่สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานกำหนด

4.4.3 ตรวจสอบบริการตรวจจัดการโจมตีและตอบสนองภัยคุกคาม (Extended Detection and Response: XDR) ให้พร้อมใช้งานแบบ 24 ชั่วโมง 7 วัน

4.4.4 สรุปรายงานรายเดือน (Monthly Report) ให้แก่สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน โดยครอบคลุมรายละเอียดดังนี้

4.4.4.1 สถานะความพร้อมใช้งานของระบบ (Availability Level)

4.4.4.2 รายงานภัยคุกคามที่ตรวจพบและสถานะการดำเนินการ (Action)

4.4.4.3 รายงานการอัปเดตซิกเนเจอร์ของระบบ (Signature Update)

4.4.5 การบำรุงรักษาเชิงป้องกัน (Preventive Maintenance) อย่างน้อยปีละ 2 ครั้ง

4.5 จัดเตรียมบริการข่าวกรองภัยคุกคามทางไซเบอร์ (Threat Intelligence) ในรูปแบบซอฟต์แวร์พร้อมใช้งาน (Software-as-a-Service) ดังนี้

4.5.1 ออกแบบและจัดเตรียมบริการข่าวกรองภัยคุกคามทางไซเบอร์ (Threat Intelligence) ตามแผนที่ได้เสนอไว้กับสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

4.5.2 ตั้งค่า (Configuration) บริการข่าวกรองภัยคุกคามทางไซเบอร์ (Threat Intelligence) ตามรูปแบบที่ได้ศึกษา ออกแบบ และได้รับการอนุมัติในการดำเนินการตามที่สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานกำหนด

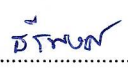
4.5.3 ตรวจสอบบริการข่าวกรองภัยคุกคามทางไซเบอร์ (Threat Intelligence) ให้พร้อมใช้งานแบบ 24 ชั่วโมง 7 วัน

4.5.4 สรุปรายงานรายเดือน (Monthly Report) ให้แก่สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน โดยครอบคลุมรายละเอียดดังนี้

4.5.4.1 สถานะความพร้อมใช้งานของระบบ (Availability Level)

4.5.4.2 รายงานข้อมูลข่าวกรองที่ตรวจพบจากระบบ (Threat Intelligence Information)

4.5.5 การบำรุงรักษาเชิงป้องกัน (Preventive Maintenance) อย่างน้อยปีละ 2 ครั้ง

1.  2.  3.  4.  5.  6. 
7.  8.  9.  10.  11. 

4.6 จัดเตรียมบริการตรวจสอบและรายงานช่องโหว่ของระบบปฏิบัติการและแอปพลิเคชัน (Vulnerability Assessment Tool) โดยครอบคลุมขั้นตอนดังนี้

4.6.1 ออกแบบและจัดเตรียมบริการตรวจสอบและรายงานช่องโหว่ของระบบปฏิบัติการและแอปพลิเคชัน (Vulnerability Assessment Tool) ตามกำหนดการที่ได้พิจารณาร่วมกับสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

4.6.2 ตั้งค่า (Configuration) บริการตรวจจับความเสี่ยงการให้บริการตรวจสอบและรายงานช่องโหว่ของระบบปฏิบัติการและแอปพลิเคชัน (Vulnerability Assessment Tool) ตามรูปแบบที่ได้ศึกษาออกแบบและได้รับการอนุมัติในการดำเนินการตามที่สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานกำหนด

4.6.3 ตรวจสอบบริการตรวจสอบและรายงานช่องโหว่ของระบบปฏิบัติการและแอปพลิเคชัน (Vulnerability Assessment Tool) ให้พร้อมใช้งานแบบ 24 ชั่วโมง 7 วัน

4.6.4 การบำรุงรักษาเชิงป้องกัน (Preventive Maintenance) อย่างน้อยปีละ 2 ครั้ง

4.7 ประเมินความเสี่ยงเพื่อหาช่องโหว่เชิงรุก (Proactive Security Assessment) โดยให้ครอบคลุมทุกระดับตั้งแต่ Network, System, Storage และ Database ของเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์ในระบบเครือข่าย (Network Equipment) และอุปกรณ์ในระบบรักษาความปลอดภัยสารสนเทศ (Security Device) ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน โดยครอบคลุมขั้นตอน อย่างน้อยดังนี้

4.7.1 ตรวจประเมินความเสี่ยง/ผลกระทบที่อาจจะเกิดขึ้นจากการดำเนินการประเมินความเสี่ยงเพื่อหาช่องโหว่เชิงรุก (Proactive Security Assessment) ร่วมกับสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

4.7.2 กำหนดเป้าหมายอุปกรณ์ที่จะประเมินความเสี่ยงเพื่อหาช่องโหว่เชิงรุก (Proactive Security Assessment) จำนวนไม่น้อยกว่า 300 IP Address

4.7.3 จัดทำแผนการดำเนินการ โดยระบุวัน เวลา และสถานที่ที่ดำเนินการประเมินความเสี่ยงเพื่อหาช่องโหว่เชิงรุก (Proactive Security Assessment)

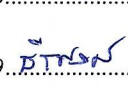
4.7.4 จัดทำรายละเอียดของซอฟต์แวร์สำหรับการดำเนินการประเมินความเสี่ยงเพื่อหาช่องโหว่เชิงรุก (Proactive Security Assessment)

4.7.5 ประเมินความเสี่ยงเพื่อหาช่องโหว่เชิงรุก (Proactive Security Assessment) โดยมีรายละเอียด อย่างน้อยดังนี้

4.7.5.1 ประเมินความเสี่ยงเพื่อหาช่องโหว่เชิงรุก (Proactive Security Assessment) ผ่าน IP Address ของอุปกรณ์ Network, System, Storage และ Database ของเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์ในระบบเครือข่าย (Network Equipment) และอุปกรณ์ในระบบรักษาความปลอดภัยสารสนเทศ (Security Device) ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน จำนวนไม่น้อยกว่า 300 IP Address

4.7.5.2 วิเคราะห์ จัดลำดับความเสี่ยง และจัดทำข้อเสนอแนะแนวทางจากผลของการดำเนินการประเมินความเสี่ยงเพื่อหาช่องโหว่เชิงรุก (Proactive Security Assessment)

4.7.5.3 ร่วมดำเนินการกับผู้ดูแลระบบของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน เพื่อปิดช่องโหว่ตามผลของการดำเนินการประเมินความเสี่ยงเพื่อหาช่องโหว่เชิงรุก (Proactive Security Assessment) ให้สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

1.  2.  3.  4.  5.  6. 
7.  8.  9.  10.  11. 

4.8 จัดทำและเสนอเอกสารการประเมินและวิเคราะห์ความปลอดภัยเชิงรุก ผลการประเมินความเสี่ยง และคำแนะนำการปรับปรุงแก้ไขข้อบกพร่องต่าง ๆ จากการประเมินความเสี่ยงเพื่อหาช่องโหว่เชิงรุก (Proactive Security Assessment) อย่างน้อยดังนี้

4.8.1 จัดทำรายงาน โดยมีเนื้อหา ครอบคลุมถึง ผลการประเมินต่าง ๆ พร้อมผลการวิเคราะห์ ผลกระทบจากความเสี่ยง และคำแนะนำในการแก้ไขปัญหาที่ค้นพบเพื่อปรับปรุงความมั่นคงปลอดภัยทางไซเบอร์

4.8.2 จัดทำรายงานสรุปผลการประเมิน และคำแนะนำสำหรับผู้บริหาร (Executive Summary)

4.8.3 เสนอผลการประเมินต่าง ๆ พร้อมคำแนะนำและวิธีดำเนินการในการแก้ไขปัญหา เพื่อปรับปรุงความมั่นคงปลอดภัยทางไซเบอร์ให้แก่ผู้บริหาร และเจ้าหน้าที่ของสำนักงานคณะกรรมการ การศึกษาขั้นพื้นฐานตามที่กำหนด

4.9 จัดให้มีผู้ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์จากเครือข่ายภายนอก (External Cyber Security Operation Center) เพื่อให้บริการครอบคลุมการทำงาน อย่างน้อยดังต่อไปนี้

4.9.1 เผื่อระวังและตอบสนองต่อความเสี่ยงทางไซเบอร์ที่ตรวจพบจากบริการบริหารความเสี่ยง ระบบสารสนเทศของหน่วยงานจากเครือข่ายภายนอก (Attack Surface Management) บริการตรวจจับการ โจมตีและตอบสนองภัยคุกคาม (Extended Detection and Response: XDR) บริการข่าวกรองภัยคุกคาม ทางไซเบอร์ (Threat Intelligence) แบบ 24 ชั่วโมง 7 วัน โดยจำแนกระดับความเสี่ยงและระยะเวลา ที่ต้องดำเนินการ

5. คุณสมบัติทางเทคนิค (Technical Specification)

ตามภาคผนวก 2 คุณสมบัติทางเทคนิค (Technical Specification) มีรายละเอียดดังนี้

5.1 บริการบริหารความเสี่ยงระบบสารสนเทศของหน่วยงานจากเครือข่ายภายนอก (Attack Surface Management)

5.2 บริการตรวจสอบและรายงานช่องโหว่ของระบบปฏิบัติการและแอปพลิเคชัน (Vulnerability Assessment Tool)

5.3 บริการตรวจจับการโจมตีและตอบสนองภัยคุกคาม (Extended Detection and Response: XDR)

5.3.1 บริการความปลอดภัยสำหรับเครื่องคอมพิวเตอร์แม่ข่าย (Endpoint Detection and Response: EDR)

5.3.2 บริการตรวจจับการโจมตีและตอบสนองภัยคุกคาม (Extended Detection and Response: XDR) และบริการวิเคราะห์การจราจรบนระบบเครือข่าย (Network Traffic Analysis: NTA หรือ Network Detection and Response: NDR)

5.3.3 บริการป้องกันไวรัส (Antivirus)

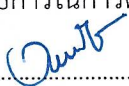
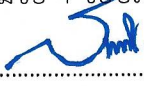
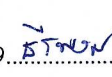
5.4 บริการข่าวกรองภัยคุกคามทางไซเบอร์ (Threat Intelligence)

6. ระยะเวลาดำเนินงาน

ระยะเวลาในการดำเนินการ 360 วัน นับถัดจากวันลงนามในสัญญา

7. หลักเกณฑ์ในการพิจารณาข้อเสนอ

7.1 ผู้ยื่นข้อเสนอต้องยื่นเอกสารเกี่ยวกับการศึกษาวิเคราะห์ ออกแบบ และขั้นตอนกระบวนการ วิธีการในการดำเนินการในแต่ละขอบเขตงานให้ชัดเจน ตามข้อ 4 ขอบเขตการดำเนินงาน

1.  2.  3.  4.  5.  6. 
7.  8.  9.  10.  11. 

7.2 การพิจารณาผลการยื่นข้อเสนอครั้งนี้ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานจะใช้หลักเกณฑ์การประเมินค่าประสิทธิภาพต่อราคา (Price Performance) โดยพิจารณาจากราคารวมตามปัจจัยหลักและน้ำหนักที่กำหนด ดังนี้

7.2.1 ราคาที่ยื่นข้อเสนอ (Price) กำหนดค่าน้ำหนักเท่ากับร้อยละ 20

7.2.2 คุณภาพและคุณสมบัติ (Performance) ที่เป็นประโยชน์ต่อทางราชการกำหนดน้ำหนักเท่ากับร้อยละ 80 โดยกำหนดหลักเกณฑ์การให้คะแนนข้อเสนอด้านเทคนิคในการพิจารณารูปแบบของงานเกณฑ์การตัดสินข้อเสนอด้านเทคนิค จะคัดเลือกจากผู้ได้รับคะแนนรวมแล้วไม่ต่ำกว่าร้อยละ 75 (75 คะแนน จาก 100 คะแนน) ดังต่อไปนี้

ลำดับ	เกณฑ์การพิจารณา	เกณฑ์ย่อย	คะแนนเต็ม
1. ผลงานและประสบการณ์ และบุคลากรหลัก คะแนนเต็ม 40 คะแนน			
1.1	ผลงานหรือประสบการณ์ของผู้ยื่นข้อเสนอ (พิจารณาจากหนังสือรับรองผลงานหรือสำเนาสัญญาโครงการที่แล้วเสร็จแล้วเท่านั้น)	ผลงานหรือประสบการณ์ตามข้อ 3.13 ในสัญญา เดี่ยวคะแนนเต็ม 15 คะแนน มีเกณฑ์การพิจารณา ดังนี้ 1) ผลงานหรือประสบการณ์เกี่ยวกับการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์กับการบริหารความเสี่ยงระบบสารสนเทศของหน่วยงานจากเครือข่ายภายนอก (Attack Surface Management) ได้ 5 คะแนน 2) ผลงานหรือประสบการณ์เกี่ยวกับการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์กับตรวจจับการโจมตีและตอบสนองภัยคุกคาม (Extended Detection and Response: XDR) ได้ 5 คะแนน 3) ผลงานหรือประสบการณ์เกี่ยวกับการดำเนินงานด้านจัดทำกรอบมาตรฐานทางไซเบอร์ (NIST Cybersecurity Framework Assessment) ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ได้ 5 คะแนน	15
1.2	วุฒิการศึกษา ประสบการณ์ และจำนวนของบุคลากรหลัก	พิจารณาจากวุฒิการศึกษา ประสบการณ์ จำนวนบุคลากรหลัก ตามข้อ 11 มีเกณฑ์พิจารณา ดังนี้ (คะแนนเต็ม 10 คะแนน) 1) มีวุฒิการศึกษา และประสบการณ์ และจำนวนบุคลากรตรงตามข้อกำหนดทั่วไป ได้ 2 คะแนน	10

1. 2. 3. 4. 5. 6.
7. 8. 9. 10. 11.

ลำดับ	เกณฑ์การพิจารณา	เกณฑ์ย่อย	คะแนนเต็ม
		2) มีวุฒิการศึกษา หรือประสบการณ์ หรือจำนวนบุคลากรสูงกว่าข้อกำหนดทั่วไป จำนวน 1 ตำแหน่ง ได้ 4 คะแนน 3) มีวุฒิการศึกษา หรือประสบการณ์ หรือจำนวนบุคลากรสูงกว่าข้อกำหนดทั่วไป จำนวน 2 ตำแหน่ง ได้ 6 คะแนน 4) มีวุฒิการศึกษา หรือประสบการณ์ หรือจำนวนบุคลากรสูงกว่าข้อกำหนดทั่วไป จำนวน 3 ตำแหน่ง ได้ 8 คะแนน 5) มีวุฒิการศึกษา หรือประสบการณ์ หรือจำนวนบุคลากรสูงกว่าข้อกำหนดทั่วไป จำนวน 4 ตำแหน่ง ได้ 10 คะแนน	
1.3	ใบเอกสารรับรอง (Certificate) ที่เกี่ยวข้องกับด้านความมั่นคงปลอดภัยไซเบอร์ ดังนี้ 1) CompTIA Cybersecurity Analyst (CySA+) 2) ISO/IEC 27001:2022 Internal Auditor 3) CompTIA Advanced Security Practitioner (CASP+) 4) Offensive Security Certified Professional (OSCP) 5) Certified in Cybersecurity (CC) 6) Certified Information Security Manager (CISM)	ใบเอกสารรับรอง (Certificate) ที่เกี่ยวข้องกับด้านความมั่นคงปลอดภัยไซเบอร์ คะแนนเต็ม 15 คะแนน มีเกณฑ์การพิจารณา ดังนี้ 1) มีใบเอกสารรับรองจำนวน 10 - 11 รายการ ได้ 5 คะแนน 2) มีใบเอกสารรับรองจำนวน 12 - 13 รายการ ได้ 7 คะแนน 3) มีใบเอกสารรับรองจำนวน 14 - 15 รายการ ได้ 9 คะแนน 4) มีใบเอกสารรับรองจำนวน 16 - 17 รายการ ได้ 11 คะแนน 5) มีใบเอกสารรับรองจำนวน 18 - 19 รายการ ได้ 13 คะแนน 6) มีใบเอกสารรับรองครบ 20 รายการ ได้ 15 คะแนน	15

1.  2.  3.  4.  5.  6. 
 7.  8.  9.  10.  11. 

ลำดับ	เกณฑ์การพิจารณา	เกณฑ์ย่อย	คะแนนเต็ม
	7) Cisco Certified Network Professional (CCNP) – Enterprise 8) eLearn Certified Digital Forensics Professional 9) Certified Red Team Professional (CRTP) 10) GIAC Certified Incident Handler (GCIH) 11) CompTIA Secure Infrastructure Expert (CSIE) 12) Attack Surface Management Certificate ของเครื่องมือหรือผลิตภัณฑ์ที่นำเสนอในโครงการนี้ 13) Threat Intelligence Certificate ของเครื่องมือหรือผลิตภัณฑ์ที่นำเสนอในโครงการนี้ 14) EDR Expert Certificate ของผลิตภัณฑ์ที่นำเสนอในโครงการนี้ 15) ISA/IEC 62443 CFS 16) Certified Cyber Defender (CCD) 17) Certified Information Systems Security Professional (CISSP) 18) Burp Suite Certified Practitioner (BSCP) 19) Information Security Management System (ISMS): Implementing ISO/IEC 27001:2022		

1. 2. 3. 4. 5. 6.

7. 8. 9. 10. 11.

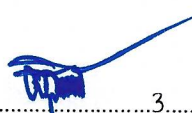
ลำดับ	เกณฑ์การพิจารณา	เกณฑ์ย่อย	คะแนนเต็ม
	(20) Certified Blue Team Level 1 (BLT1)		
2. ด้านความน่าเชื่อถือของเครื่องมือหรือผลิตภัณฑ์ที่นำเสนอและความร่วมมือกับองค์กรด้านความมั่นคงปลอดภัยไซเบอร์ในระดับสากล คะแนนเต็ม 40 คะแนน ³²			
2.1	ความน่าเชื่อถือของเครื่องมือหรือผลิตภัณฑ์	ความน่าเชื่อถือของเครื่องมือหรือผลิตภัณฑ์ คะแนนเต็ม 25 คะแนน มีเกณฑ์การพิจารณา ดังนี้ 1) เอกสารรับรองจากเจ้าของเครื่องมือหรือผลิตภัณฑ์ในส่วนของบริการบริหารความเสี่ยงระบบสารสนเทศของหน่วยงานจากเครือข่ายภายนอก (Attack Surface Management) และบริการข่าวกรองภัยคุกคามทางไซเบอร์ (Threat Intelligence) ต้องได้รับการรับรองมาตรฐาน ISO 27001 หรือ SOC2 TYPE-2 ได้ 5 คะแนน 2) เอกสารรับรองจากเจ้าของเครื่องมือหรือผลิตภัณฑ์ในส่วนของทีมตอบสนองต่อภัยคุกคามทางไซเบอร์โดยเจ้าของเครื่องมือหรือผลิตภัณฑ์บริการบริหารความเสี่ยงระบบสารสนเทศของหน่วยงานจากเครือข่ายภายนอก (Attack Surface Management) และบริการข่าวกรองภัยคุกคามทางไซเบอร์ (Threat Intelligence) ที่นำเสนอต้องได้รับการให้คะแนนหรือได้รับการจัดลำดับให้อยู่ในกลุ่ม SPARK Leaders ของ SPARK Matrixtm : Digital Forensics and Incident Response Services, Q4 2024 หรือปีล่าสุด ได้ 10 คะแนน 3) เอกสารรับรองจากเจ้าของเครื่องมือหรือผลิตภัณฑ์ในส่วนของทีมรับมือสถานการณ์ฉุกเฉิน (Computer Emergency Response Team: CERT) โดยเจ้าของเครื่องมือหรือผลิตภัณฑ์บริการบริหารความเสี่ยงระบบสารสนเทศของหน่วยงานจากเครือข่ายภายนอก (Attack Surface Management) และบริการข่าวกรองภัยคุกคามทางไซเบอร์	25

1. 2. 3. 4. 5. 6.
7. 8. 9. 10. 11.

ลำดับ	เกณฑ์การพิจารณา	เกณฑ์ย่อย	คะแนนเต็ม
		(Threat Intelligence) ที่นำเสนอต้องมี CERT เป็นของตัวเองและเป็นสมาชิกสมาคม CERT ระดับภูมิภาคอย่างน้อย 2 ภูมิภาค ได้ 10 คะแนน	
2.2	การเป็นสมาชิกหรือพันธมิตรกับองค์กรสากลที่เกี่ยวข้องกับการตอบสนองต่อภัยคุกคามทางไซเบอร์ (Security & Incident Response) ในแต่ละด้าน ดังนี้ 1) องค์กรหรือสมาคมด้าน Incident Response ระดับสากล (Global) 2) องค์กรหรือสมาคมด้านการป้องกัน Fraud และ Identity Theft 3) องค์กรหรือสมาคมด้านการทำ Security Incident Clearinghouse 4) องค์กรด้านการสืบสวนอาชญากรรมไซเบอร์ระหว่างประเทศ อย่างน้อย 3 หน่วยงาน	การเป็นสมาชิกหรือพันธมิตรกับองค์กรสากลที่เกี่ยวข้องกับการตอบสนองต่อภัยคุกคามทางไซเบอร์ (Security & Incident Response) คะแนนเต็ม 15 คะแนน มีเกณฑ์การพิจารณา โดยมีเอกสารรับรอง ดังนี้ 1) การเป็นสมาชิกหรือพันธมิตรองค์กรอย่างน้อย 1 ด้าน ได้ 4 คะแนน 2) การเป็นสมาชิกหรือพันธมิตรองค์กรอย่างน้อย 2 ด้าน ได้ 8 คะแนน 3) การเป็นสมาชิกหรือพันธมิตรองค์กรอย่างน้อย 3 ด้าน ได้ 12 คะแนน 4) การเป็นสมาชิกหรือพันธมิตรองค์กรครบตามที่กำหนด ได้ 15 คะแนน	15
3. วิธีการบริหารและวิธีปฏิบัติงาน คะแนนเต็ม 20 คะแนน			
3.1	วิธีการบริหารและวิธีปฏิบัติงานที่ชัดเจนและสอดคล้องกับขอบเขตการดำเนินงาน ตามข้อ 4	วิธีการบริหารและวิธีปฏิบัติงานที่ชัดเจน คะแนนเต็ม 20 คะแนน มีเกณฑ์การพิจารณา ดังนี้ 1) วิธีการบริหาร คะแนนเต็ม 5 คะแนน มีเกณฑ์การพิจารณา ดังนี้ 1.1) มีโครงสร้างทีมงาน ได้ 1 คะแนน 1.2) มีการจัดบุคลากรการทำงานตามขอบเขตงานในแต่ละตำแหน่ง ได้ 1 คะแนน 1.3) ผู้จัดการโครงการที่มีใบรับรองด้านความมั่นคงปลอดภัยไซเบอร์ดังต่อไปนี้ ได้ 3 คะแนน	20

1. 2. 3. 4. 5. 6.
7. 8. 9. 10. 11.

ลำดับ	เกณฑ์การพิจารณา	เกณฑ์ย่อย	คะแนนเต็ม
		- มีใบรับรอง Certified Information Systems Security Professional (CISSP) ได้ 1 คะแนน - มีใบรับรอง Certified Ethical Hacker (CEH) ได้ 1 คะแนน - มีใบรับรอง DevSecOps Foundation (DSOF) หรือ Certified DevSecOps Professional (CDP) ได้ 1 คะแนน 2) วิธีปฏิบัติงานที่สอดคล้องกับขอบเขตการดำเนินงาน ตามข้อ 4 คะแนนเต็ม 10 คะแนน มีเกณฑ์การพิจารณา ดังนี้ 2.1) มีแนวคิด และทฤษฎีที่เกี่ยวข้อง เพื่อแสดงความเข้าใจที่มีต่อสถานการณ์ปัจจุบันของระบบความมั่นคงปลอดภัยทางไซเบอร์ที่สอดคล้องกับภารกิจของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ได้ 3 คะแนน 2.2) มีการศึกษา และวิเคราะห์แนวโน้มภัยคุกคามทางไซเบอร์ (Cyber Trends) ที่อาจจะเกิดขึ้นในอนาคต ที่เกี่ยวข้องกับสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ได้ 3 คะแนน 2.3) มีกรอบการดำเนินการตามวัตถุประสงค์ของโครงการ และขั้นตอนการปฏิบัติงาน ได้ 2 คะแนน 2.4) มีการวิเคราะห์สถาปัตยกรรมความมั่นคงปลอดภัยทางไซเบอร์ ขององค์กร (Enterprise Cybersecurity Architecture & Diagram) ที่สอดคล้องกับสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ได้ 2 คะแนน	

1.  2.  3.  4.  5.  6. 

7.  8.  9.  10.  11. 

ลำดับ	เกณฑ์การพิจารณา	เกณฑ์ย่อย	คะแนนเต็ม
		3) ผู้ยื่นข้อเสนอต้องได้รับมาตรฐาน ISO/IEC 27001:2022 โดยพิจารณาจากเอกสารรับรองมาตรฐาน ISO/IEC 27001:2022 ได้ 5 คะแนน	
คะแนนรวมทั้งหมด			100

หมายเหตุ กรณีที่ไม่ได้ส่งเอกสารหรือไม่มีข้อมูลรายละเอียดตามเกณฑ์การพิจารณาในแต่ละข้อ จะไม่ได้รับคะแนนในข้อนั้น ๆ

7.3 หากผู้ยื่นข้อเสนอรายใด มีคุณสมบัติผู้ยื่นข้อเสนอและเงื่อนไขการเสนอราคาไม่ถูกต้อง หรือไม่ครบถ้วนคณะกรรมการพิจารณาผลการประกวดราคาจะไม่รับพิจารณาราคาของผู้ยื่นข้อเสนอรายนั้น

7.4 การตัดสินใจของคณะกรรมการพิจารณาผลการประกวดราคา สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน มีสิทธิ์ให้ผู้ยื่นข้อเสนอชี้แจงข้อเท็จจริง สภาพ ฐานะ หรือ ข้อเท็จจริงอื่นใดที่เกี่ยวข้องกับผู้ยื่นข้อเสนอ ได้มีสิทธิ์ที่จะไม่รับ ข้อเสนอไม่รับราคา หรือไม่ทำสัญญา หากหลักฐานดังกล่าวไม่มีความเหมาะสมหรือไม่ถูกต้อง

7.5 สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ทรงไว้ซึ่งสิทธิ์ที่จะไม่รับราคาต่ำสุด หรือราคาหนึ่งราคาใด หรือราคาที่เสนอทั้งหมดก็ได้ หรืออาจจะยกเลิกการประกวดราคาค้างนี้ ทั้งนี้ เพื่อประโยชน์ของทางราชการเป็นสำคัญและให้ถือว่า การตัดสินใจของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน เป็นเด็ดขาด ผู้ยื่นข้อเสนอจะเรียกร้องค่าเสียหายใด ๆ มิได้ รวมทั้ง สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน จะพิจารณายกเลิกการจ้าง หากมีเหตุที่เชื่อถือได้ว่า การยื่นข้อเสนอกระทำการโดยไม่สุจริต เช่น การเสนอเอกสารอันเป็นเท็จ หรือใช้ข้อมูลบุคคลธรรมดา หรือนิติบุคคลอื่น มาเสนอราคาแทน เป็นต้น

7.6 กรณีที่ปรากฏข้อเท็จจริงภายหลังจากการพิจารณาข้อเสนอว่าผู้ยื่นข้อเสนอที่มีสิทธิ์ได้รับการคัดเลือกเป็นผู้ยื่นข้อเสนอที่มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่น ณ วันยื่นข้อเสนอ หรือเป็นผู้ยื่นข้อเสนอที่กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน มีอำนาจที่จะตัดรายชื่อผู้ยื่นข้อเสนอรายดังกล่าวออก

8. งบประมาณโครงการ

วงเงินงบประมาณ จำนวนทั้งสิ้น 19,040,700.00 บาท (สิบเก้าล้านสี่หมื่นเจ็ดร้อยบาทถ้วน)

หมายเหตุ ราคากลางเป็นราคาที่ได้จากการอ้างอิงตามหลักเกณฑ์ราคากลางการจ้างที่ปรึกษา (มีนาคม 2569) สำนักงานบริหารหนี้สาธารณะ และการสืบราคาจากท้องตลาด

9. การส่งมอบงาน ค่าจ้าง และการจ่ายเงิน

9.1 งวดงานที่ 1 เบิกจ่ายร้อยละ 10 ของวงเงินตามสัญญาจ้าง หลังจากคณะกรรมการตรวจรับพัสดุได้ตรวจรับงานดังกล่าวเรียบร้อยแล้ว โดยผู้รับจ้างต้องส่งมอบงานภายในระยะเวลา 30 วัน นับถัดจากวันลงนามในสัญญา อย่างน้อยดังต่อไปนี้

9.1.1 หลักฐานการจัดประชุมเริ่มโครงการ (Kick-off Project) ตามข้อ 4.1.2

9.1.2 แผนการดำเนินโครงการ (Project Planning) ซึ่งอธิบายถึง กิจกรรมการดำเนินงาน ระยะเวลาการดำเนินงาน และกรรมวิธีการดำเนินงานโครงการ รวมถึงสิ่งส่งมอบงานในโครงการ ตามข้อ 4.1.1

1.  2.  3.  4.  5.  6. 
 7.  8.  9.  10.  11. 

9.2 งวดงานที่ 2 เบิกจ่ายร้อยละ 20 ของวงเงินตามสัญญาจ้าง หลังจากคณะกรรมการตรวจรับพัสดุได้ตรวจรับงานดังกล่าวเรียบร้อยแล้ว โดยผู้รับจ้างต้องส่งมอบงานภายในระยะเวลา 90 วัน นับถัดจากวันลงนามในสัญญา อย่างน้อยดังต่อไปนี้

9.2.1 รายงานบริการบริหารความเสี่ยงระบบสารสนเทศของหน่วยงานจากเครือข่ายภายนอก (Attack Surface Management) ตามข้อ 4.3

9.2.2 รายงานบริการข่าวกรองภัยคุกคามทางไซเบอร์ (Threat Intelligence) ตามข้อ 4.5

9.2.3 รายงานบริการตรวจสอบและรายงานช่องโหว่ของระบบปฏิบัติการและแอปพลิเคชัน (Vulnerability Assessment Tool) ตามข้อ 4.6

9.2.4 รายงานบริการความปลอดภัยสำหรับเครื่องคอมพิวเตอร์แม่ข่าย (Endpoint Detection and Response: EDR) บริการตรวจจับการโจมตีและตอบสนองภัยคุกคาม (Extended Detection and Response: XDR) และบริการวิเคราะห์การจราจรบนระบบเครือข่าย (Network Traffic Analysis: NTA หรือ Network Detection and Response: NDR) และบริการป้องกันไวรัส (Antivirus) ตามข้อ 4.4

9.3 งวดงานที่ 3 เบิกจ่ายร้อยละ 20 ของวงเงินตามสัญญาจ้าง หลังจากคณะกรรมการตรวจรับพัสดุได้ตรวจรับงานดังกล่าวเรียบร้อยแล้ว โดยผู้รับจ้างต้องส่งมอบงานภายในระยะเวลา 150 วัน นับถัดจากวันลงนามในสัญญา อย่างน้อยดังต่อไปนี้

9.3.1 เอกสารตามกรอบมาตรฐานทางไซเบอร์ (NIST Cybersecurity Framework) ที่จัดทำหรือทบทวนตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ในส่วนของการกำกับดูแลการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Govern) ตามข้อ 4.2.1

9.3.2 เอกสารตามกรอบมาตรฐานทางไซเบอร์ (NIST Cybersecurity Framework) ที่จัดทำหรือทบทวนตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ในส่วนของการระบุความเสี่ยงที่อาจเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify) ตามข้อ 4.2.2

9.3.3 รายงานผลการฝึกอบรมด้านความมั่นคงปลอดภัยทางไซเบอร์ ตามข้อ 4.2.3.2

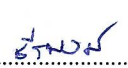
9.3.4 จัดให้มีผู้ปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์จากภายนอก (External Cybersecurity Operation Center) ตามข้อ 4.9

9.4 งวดงานที่ 4 เบิกจ่ายร้อยละ 20 ของวงเงินตามสัญญาจ้าง หลังจากคณะกรรมการตรวจรับพัสดุได้ตรวจรับงานดังกล่าวเรียบร้อยแล้ว โดยผู้รับจ้างต้องส่งมอบงานภายในระยะเวลา 210 วัน นับถัดจากวันลงนามในสัญญา อย่างน้อยดังนี้

9.4.1 เอกสารการประเมินและวิเคราะห์ความปลอดภัยเชิงรุก (Proactive Security Assessment) ตามข้อ 4.7 และข้อ 4.8

9.4.2 เอกสารตามกรอบมาตรฐานทางไซเบอร์ (NIST Cybersecurity Framework) ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ในส่วนของการป้องกันความเสี่ยงที่อาจเกิดขึ้น (Protect) ตามข้อ 4.2.3

9.5 งวดงานที่ 5 เบิกจ่ายร้อยละ 15 ของวงเงินตามสัญญาจ้าง หลังจากคณะกรรมการตรวจรับพัสดุได้ตรวจรับงานดังกล่าวเรียบร้อยแล้ว โดยผู้รับจ้างต้องส่งมอบเอกสารตามกรอบมาตรฐานทางไซเบอร์ (NIST Cybersecurity Framework) ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

1.  2.  3.  4.  5.  6. 
7.  8.  9.  10.  11. 

ในส่วนของการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect) ตามข้อ 4.2.4 ภายในระยะเวลา 270 วัน นับถัดจากวันลงนามในสัญญา

9.6 งวดงานที่ 6 เบิกจ่ายร้อยละ 15 ของวงเงินตามสัญญาจ้าง หลังจากคณะกรรมการตรวจรับพัสดุได้ตรวจรับงานดังกล่าวเรียบร้อยแล้ว โดยผู้รับจ้างต้องส่งมอบงานภายในระยะเวลา 360 วัน นับถัดจากวันลงนามในสัญญา อย่างน้อยดังต่อไปนี้

9.6.1 เอกสารตามกรอบมาตรฐานทางไซเบอร์ (NIST Cybersecurity Framework Assessment) ที่จัดทำขึ้นตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ในส่วนของการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond) ตามข้อ 4.2.5

9.6.2 เอกสารตามกรอบมาตรฐานทางไซเบอร์ (NIST Cybersecurity Framework Assessment) ที่จัดทำขึ้นตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ในส่วนของการรักษาและฟื้นฟูความเสียหายที่เกิดขึ้นจากภัยคุกคามทางไซเบอร์ (Recover) ตามข้อ 4.2.6

หมายเหตุ ผู้รับจ้างต้องส่งมอบเอกสารในแต่ละงวดงาน ในรูปแบบสื่อสิ่งพิมพ์ อย่างน้อย 3 ชุด พร้อมไฟล์อิเล็กทรอนิกส์ที่สามารถแก้ไขได้ และ PDF พร้อมบันทึกลงใน Flash Drive หรือ External Hard Disk

10. อัตราค่าปรับ

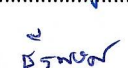
ผู้รับจ้างต้องดำเนินการให้บริการยกระดับศักยภาพของระบบความมั่นคงปลอดภัยทางไซเบอร์ตามระยะเวลาของโครงการที่กำหนดไว้ หากไม่สามารถดำเนินงานตามขอบเขตการดำเนินงาน ข้อ 4 ผู้ว่าจ้างมีสิทธิคิดค่าปรับจากผู้รับจ้างในอัตราร้อยละ 0.1 ต่อวันของวงเงินค่าจ้างทั้งหมดตามสัญญา จนกว่าจะดำเนินการครบถ้วนตามสัญญา

11. ข้อกำหนดทั่วไป

11.1 ผู้รับจ้างต้องจัดหาบุคลากรสำหรับจ้างเหมาบริการยกระดับระบบความมั่นคงปลอดภัยทางไซเบอร์สำหรับสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ที่มีคุณสมบัติ ความรู้ ประสบการณ์ และคุณสมบัติเฉพาะของตำแหน่งสอดคล้องกับตาราง ดังนี้

ลำดับที่	ตำแหน่ง	วุฒิการศึกษา	ประสบการณ์ไม่น้อยกว่า (ปี)	จำนวน (คน)
บุคลากรหลัก				
1	ผู้จัดการโครงการ (Project Manager)	ปริญญาโท ด้านคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ หรือสื่อสารโทรคมนาคม หรือวิศวกรรมไฟฟ้า หรือด้านอื่น ๆ ที่เกี่ยวข้อง	11	1
2	ผู้เชี่ยวชาญด้านมาตรฐานความปลอดภัยทางไซเบอร์ (Cyber Security Specialist)	ปริญญาเอก ด้านคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ หรือสื่อสารโทรคมนาคม หรือวิศวกรรมไฟฟ้า หรือด้านอื่น ๆ ที่เกี่ยวข้อง	10	1

1.  2.  3.  4.  5.  6. 

7.  8.  9.  10.  11. 

ลำดับที่	ตำแหน่ง	วุฒิการศึกษา	ประสบการณ์ ไม่น้อยกว่า (ปี)	จำนวน (คน)
3	นักวิเคราะห์ระบบรักษาความปลอดภัยสารสนเทศ (IT security Analyst - ASM)	ปริญญาตรี ด้านคอมพิวเตอร์ หรือ เทคโนโลยีสารสนเทศ หรือสื่อสารโทรคมนาคม หรือวิศวกรรมไฟฟ้า หรือด้านอื่น ๆ ที่เกี่ยวข้อง	3	1
4	นักวิเคราะห์ช่องโหว่ระบบสารสนเทศ (VA Engineer)	ปริญญาตรี ด้านคอมพิวเตอร์ หรือ เทคโนโลยีสารสนเทศ หรือสื่อสารโทรคมนาคม หรือวิศวกรรมไฟฟ้า หรือด้านอื่น ๆ ที่เกี่ยวข้อง	3	1
5	นักวิเคราะห์ระบบรักษาความปลอดภัยสารสนเทศ (IT Security Analyst - XDR)	ปริญญาตรี ด้านคอมพิวเตอร์ หรือ เทคโนโลยีสารสนเทศ หรือสื่อสารโทรคมนาคม หรือวิศวกรรมไฟฟ้า หรือด้านอื่น ๆ ที่เกี่ยวข้อง	3	1
6	นักวิเคราะห์ด้านข่าวกรองภัยคุกคามทางไซเบอร์ (Threat Intelligence Analyst - TI)	ปริญญาตรี ด้านคอมพิวเตอร์ หรือ เทคโนโลยีสารสนเทศ หรือสื่อสารโทรคมนาคม หรือวิศวกรรมไฟฟ้า หรือด้านอื่น ๆ ที่เกี่ยวข้อง	3	1
บุคลากรสนับสนุน				
1	เลขานุการโครงการ	ปริญญาตรี	1	1

หลักฐานการแสดงความรู้และความสามารถของบุคลากรปฏิบัติงานในโครงการนี้ ตามแบบฟอร์ม (ภาคผนวก 1)

11.2 ผู้รับจ้างต้องจัดเตรียมเครื่องมือและสภาพแวดล้อมที่เกี่ยวข้องสำหรับการติดตั้งบริการที่นำเสนอในโครงการ โดยผู้รับจ้างเป็นผู้รับผิดชอบค่าใช้จ่ายทั้งหมด

11.3 ผู้ยื่นข้อเสนอต้องมีหนังสือรับรองสิทธิการใช้งานที่ถูกต้องตามกฎหมายจากเจ้าของเครื่องมือหรือผลิตภัณฑ์ หรือสาขาเจ้าของเครื่องมือหรือผลิตภัณฑ์ในประเทศไทย หรือตัวแทนจำหน่ายในประเทศไทย โดยให้ยื่นขณะเข้าเสนอราคา ตามภาคผนวก 2

12. หน่วยงานที่รับผิดชอบ

สำนักเทคโนโลยีเพื่อการเรียนการสอน สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน
อีเมล obecict@obec.go.th โทรศัพท์ 02-288-5906

1. 2. 3. 4. 5. 6.
7. 8. 9. 10. 11.