(ร่าง) ขอบเขตของงาน (Terms of Reference: TOR)
จ้างเหมาบริการเพิ่มประสิทธิภาพการป้องกันและการรักษาความปลอดภัยของข้อมูล
พร้อมปรับปรุงความปลอดภัยตามมาตรฐาน ISO/IEC 27001:2022 และ ISO/IEC 27701:2019

1. หลักการและเหตุผล

จากแผนแม่บทภายใต้ยุทธศาสตร์ชาติ (พ.ศ. 2566 - 2580) ฉบับปรับปรุง และนโยบายการศึกษาของกระทรวงศึกษาธิการ ประจำปีงบประมาณ พ.ศ. 2568 - 2569 เพื่อให้เกิดประโยชน์สูงสุดต่อผู้เรียนและประชาชน โดยมีแนวทางการลดภาระนักเรียนและผู้ปกครองด้วยการส่งเสริมให้มีกระบวนการสร้างความปลอดภัยให้กับผู้เรียน อีกทั้งตามนโยบายของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ประจำปีงบประมาณ พ.ศ. 2568 – 2569 ว่าด้วยเรื่อง "พัฒนาระบบบริหารจัดการให้มีประสิทธิภาพ ถูกต้อง รวดเร็ว ประโยชน์ ประหยัด โปร่งใส และตรวจสอบได้" ซึ่งมีแนวทางในการ "จัดหาโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัลที่มีความปลอดภัย ให้กับหน่วยงานและสถานศึกษาในสังกัด" สอดคล้องกับ มาตรา 44 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 สำหรับหน่วยงานภาครัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 ประกอบด้วย (1) แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (2) การประเมินความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และ (3) แผนการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งรับมือกับภัยคุกคามทางไซเบอร์ โดยการมุ่งเน้นการตรวจสอบควบคุมความปลอดภัยของข้อมูล ป้องกัน การเฝ้าระวังและการตอบสนองและแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์ อีกทั้งมาตรา 54 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 สำหรับหน่วยงานภาครัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และดำเนินการให้สอดคล้องกับแนวปฏิบัติการรักษาความมั่นคงปลอดภัยเว็บไซต์ (Website Security Guideline) ตามที่มีประกาศจากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

ปัจจุบัน สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน (สพฐ.) รวมถึงสำนักงานเขตพื้นที่การศึกษาตกเป็นเป้าหมายการโจมตีจากกลุ่มผู้ไม่หวังดีที่มีเป้าหมายเพื่อสร้างความเสียหายและสร้างความเสื่อมเสียของชื่อเสียงด้วยวิธีการโจมตีทางหน้าเว็บไซต์ การยิงการจราจรทางคอมพิวเตอร์จำนวนมากจากหลายที่ (Distributed Denial of Service: DDoS) และการฝังสคริปต์เว็บพนันออนไลน์ (Gambling) รวมไปถึงการเปลี่ยนแปลงหน้าเว็บไซต์เป็นเนื้อหาอื่น (Web Defacement) อ้างอิงข้อมูลสถิติจาก ThaiCERT ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ปี 2568 พบว่าหน่วยงานทางการศึกษาตกเป็นเป้าหมายการถูกโจมตีทางไซเบอร์สูงเป็นอับดับแรก ส่วนใหญ่เป็นการปลอมแปลงหน้าเว็บไซต์และฝั่งเว็บพนันออนไลน์ ซึ่งสอดคล้องกับสภาพปัจจุบันของหน่วยงาน ก่อให้เกิดการเข้าใจผิดและความเสียหายแก่หน่วยงานและผู้รับบริการ อีกทั้ง สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานมีการให้บริการระบบสารสนเทศที่สำคัญ ประกอบด้วย ข้อมูลนักเรียน ข้อมูลบุคลากร และข้อมูลอื่น ๆ ที่เกี่ยวข้องกับด้านการศึกษา เป็นจำนวนมาก ดังนั้น เพื่อให้ระบบสารสนเทศดังกล่าวรวมถึงระบบสำคัญของหน่วยงานมีความมั่นคงปลอดภัย สามารถให้บริการได้อย่างต่อเนื่อง จึงจำเป็นต้องมีการกำหนดมาตรฐานกระบวนการในการปฏิบัติงาน เพื่อสร้างความน่าเชื่อถือของระบบที่ให้บริการแก่ผู้เรียนและประชาชนต่อไปในอนาคต

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

7.....8.....9.....10.....11.....

ดังนั้น สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน จึงมีความจำเป็นต้องเพิ่มประสิทธิภาพการป้องกันและการรักษาความปลอดภัยของข้อมูลพร้อมปรับปรุงความปลอดภัยตามมาตรฐาน ISO/IEC 27001:2022 และ ISO/IEC 27701:2019 เพื่อป้องกันการถูกโจมตีที่ทำให้เกิดความเข้าใจผิด สร้างความเสื่อมเสีย และความเสียหาย ด้วยการค้นหาและแก้ไขช่องโหว่อย่างต่อเนื่อง และทำให้เว็บแอปพลิเคชันมีความปลอดภัย รวมถึงมีการตรวจสอบและยกระดับความปลอดภัยของระบบเว็บไซต์ของสำนักงานเขตพื้นที่การศึกษา เพื่อทำให้การบริหารความเสี่ยงทางไซเบอร์มีประสิทธิภาพ อ้างอิงตามกรอบแนวปฏิบัติ NIST Cybersecurity Framework 2.0 ในส่วนการป้องกันภัยคุกคามทางไซเบอร์ (Protect) พร้อมจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ตามมาตรฐาน ISO/IEC 27001:2022 และระบบบริหารจัดการข้อมูลส่วนบุคคล (Privacy Information Management System: PIMS) ตามมาตรฐาน ISO/IEC 27701:2019 รวมถึงการกำกับดูแล (Govern) อีกทั้งเตรียมบุคลากรในการดำเนินการตอบสนองและกำจัดภัยคุกคาม (Incident Response) เมื่อเกิดเหตุการณ์การละเมิดเกิดขึ้น

2. วัตถุประสงค์

2.1 เพื่อตรวจสอบมาตรฐานความปลอดภัยของเว็บแอปพลิเคชัน โดยมุ่งหวังให้สามารถค้นหาช่องโหว่หรือจุดอ่อนที่อาจถูกผู้ไม่หวังดีใช้เป็นช่องทางในการโจมตีระบบของสำนักงานเขตพื้นที่การศึกษา (Web Application Security Scan)

2.2 เพื่อจัดให้มีผู้เชี่ยวชาญในการเสนอแนะแนวทางแก้ไขช่องโหว่หรือจุดอ่อนที่พบจากการตรวจสอบมาตรฐานความปลอดภัยของระบบสารสนเทศเว็บแอปพลิเคชัน รวมถึงเสนอแนะแนวทางการตั้งค่าระบบอย่างปลอดภัย (System Hardening) สำหรับระบบสารสนเทศเว็บแอปพลิเคชันของสำนักงานเขตพื้นที่การศึกษา

2.3 เพื่อเพิ่มความสามารถในการป้องกันการโจมตีในระดับเว็บแอปพลิเคชัน (Web Application Firewall) สำหรับระบบสารสนเทศเว็บแอปพลิเคชันของสำนักงานเขตพื้นที่การศึกษา

2.4 เพื่อเพิ่มความสามารถในการป้องกันการโจมตีประเภทที่ทำให้ระบบเว็บแอปพลิเคชันไม่สามารถใช้งานได้ (Web Application DDoS Protection) สำหรับระบบสารสนเทศเว็บแอปพลิเคชันของสำนักงานเขตพื้นที่การศึกษา

2.5 เพื่อทำการตอบสนองและกำจัดภัยคุกคาม (Incident Response) ของระบบที่พบว่าถูกโจมตีและมีแผนปรับปรุงเพื่อป้องกันไม่ให้เกิดเหตุการณ์ซ้ำเดิม สำหรับเครื่องคอมพิวเตอร์แม่ข่ายที่ Data Center เอกมัยและราชดำเนินของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

2.6 เพื่อให้โครงสร้างพื้นฐานและการดำเนินงานของศูนย์ข้อมูล (Data Center) ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน มีระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศเป็นไปตามมาตรฐานสากล ISO/IEC 27001:2022 (Information Security Management System: ISMS)

2.7 เพื่อให้การดำเนินงานด้านการบริหารการจัดการข้อมูลส่วนบุคคลของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานเป็นไปตามมาตรฐานสากล ISO/IEC 27701:2019 (Privacy Information Management System: PIMS)

2.8 เพื่อป้องกันการโจมตีและเข้าถึงระบบฐานข้อมูลโดยไม่ได้รับอนุญาตด้วยระบบรักษาความปลอดภัยสำหรับฐานข้อมูล (Database Firewall)

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

7.....8.....9.....10.....11.....

3. คุณสมบัติผู้ยื่นข้อเสนอ

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงาน และได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นนิติบุคคลผู้มีอาชีพรับจ้างงานตามขอบเขตงานนี้

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนออื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ณ วันยื่นข้อเสนอ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการยื่นข้อเสนอครั้งนี้

3.9 ไม่เป็นผู้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์ความคุ้มกันเช่นว่านั้น

3.10 ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ต้องมีคุณสมบัติดังนี้

3.10.1 การกำหนดสัดส่วนการเข้าร่วมค้าของคู่สัญญา

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลง ฯ จะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงานสิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

3.10.2 กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

3.10.3 การยื่นข้อเสนอของกิจการร่วมค้า

3.10.3.1 กรณีที่ข้อตกลงฯ กำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอ ในนามกิจการร่วมค้า

3.10.3.2 การยื่นข้อเสนอด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e - bidding) ให้ผู้เข้าร่วมค้าที่ได้รับมอบหมายหรือมอบอำนาจตามข้อ 3.10.3.1 ดำเนินการซื้อเอกสารประกวดราคาอิเล็กทรอนิกส์ กรณีที่มีการจำหน่ายเอกสารซื้อหรือจ้าง

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

7.....8.....9.....10.....11.....

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

3.12 ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

3.12.1 กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยหรือต่างประเทศซึ่งได้จดทะเบียนเกินกว่า 1 ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก 1 ปีสุดท้ายก่อนวันยื่นข้อเสนอ งบแสดงฐานะการเงิน 1 ปีสุดท้ายก่อนวันยื่นข้อเสนอ หมายถึง งบแสดงฐานะการเงินย้อนไปก่อนวันที่หน่วยงานของรัฐกำหนดให้เป็นวันยื่นข้อเสนอ 1 ปีปฏิทิน เว้นแต่กรณีนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยหากวันยื่นข้อเสนอเป็นช่วงระยะเวลาที่กรมพัฒนาธุรกิจการค้ากำหนดให้นิติบุคคลยื่นงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ซึ่งจะอยู่ในช่วงเดือนมกราคม - เดือนพฤษภาคม ของทุกปี โดยนิติบุคคลที่เป็นผู้ยื่นข้อเสนอนั้นยังอยู่ในช่วงของการยื่นงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า คือ ช่วงเดือนมกราคม - เดือนพฤษภาคม กรณีนี้ให้สามารถยื่นงบแสดงฐานะการเงินย้อนหลังไปอีก 1 ปี ได้

3.12.2 กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า หรือกรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงิน ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียนโดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอไม่ต่ำกว่า 8 ล้านบาท

3.12.3 กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ สามารถดำเนินการได้ดังนี้

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

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

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

7.....8.....9.....10.....11.....

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

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

3.12.5 กรณีตามข้อ 3.12.1 – ข้อ 3.12.4 ไม่ใช้บังคับกับกรณีดังต่อไปนี้

3.12.5.1 กรณีผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐภายในประเทศ

3.12.5.2 นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติ ล้มละลาย พ.ศ. 2483 และที่แก้ไขเพิ่มเติม

3.13 ผู้ยื่นข้อเสนอต้องมีผลงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเป็นผลงานที่แล้วเสร็จในสัญญาเดียว และมีมูลค่าของผลงานไม่น้อยกว่า 20 ล้านบาท (ยี่สิบล้านบาทถ้วน) และเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับหน่วยงานของรัฐหรือหน่วยงานเอกชนที่สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานเชื่อถือ โดยต้องยื่นหนังสือรับรองผลงานจากคู่สัญญาและสำเนาสัญญาพร้อมรับรองสำเนาถูกต้อง ให้ยื่นขณะเข้าเสนอราคา ทั้งนี้คณะกรรมการพิจารณาผลขอสงวนสิทธิ์ในการที่จะดำเนินการตรวจสอบเอกสารหนังสือรับรองผลงานและสำเนาสัญญา ไปยังหน่วยงานที่ออกเอกสาร

3.14 ผู้ยื่นข้อเสนอต้องได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่ายจากผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทย โดยให้ยื่นขณะเข้าเสนอราคา ตามข้อ 5.1 – 5.4

4. ขอบเขตการดำเนินงาน

ผู้รับจ้างต้องดำเนินการตามขอบเขตของงาน อย่างน้อยดังต่อไปนี้

4.1 การจัดทำแผนและการบริหารโครงการ (Project Plan) และประชุมเปิดตัวโครงการ (Kick-off Meeting) อย่างน้อยดังต่อไปนี้

4.1.1 จัดทำแผนและการบริหารโครงการ (Project Plan) โดยกำหนดระยะเวลาในการดำเนินการแต่ละกิจกรรม เพื่อให้คณะกรรมการตรวจรับพัสดุ พิจารณาอนุมัติก่อนเริ่มดำเนินการ ประกอบด้วย

4.1.1.1 แผนการบริหารโครงการ (Project Management Plan)

4.1.1.2 แผนการดำเนินการโครงการ (Implementation Plan) ประกอบด้วยรายละเอียดดังต่อไปนี้

1) การติดตั้งระบบตรวจสอบช่องโหว่และมาตรฐานความปลอดภัยของเว็บแอปพลิเคชัน (Web Application Security Scanner) ของสำนักงานเขตพื้นที่การศึกษา

2) บริการติดตั้งการป้องกันการโจมตีระดับเว็บแอปพลิเคชัน (Web Application Firewall)

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

7.....8.....9.....10.....11.....

3) บริการติดตั้งการป้องกันการโจมตีประเภทที่ทำให้ระบบเว็บแอปพลิเคชัน (Web Application DDoS Protection) ไม่สามารถใช้งานได้

4) การตรวจสอบช่องโหว่และมาตรฐานความปลอดภัยของเว็บแอปพลิเคชัน (Web Application Security Scan) ของสำนักงานเขตพื้นที่การศึกษาและประเมินแนวทางการตั้งค่าระบบอย่างปลอดภัย (System Hardening)

5) การดำเนินการตอบสนองและกำจัดภัยคุกคาม (Incident Response)

6) การจัดทำเอกสาร กระบวนการ และเตรียมความพร้อมในการขอรับรองมาตรฐาน ISO/IEC 27001:2022 (Information Security Management System: ISMS) ของศูนย์ข้อมูล (Data Center) สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานพร้อมจัดบุคลากรให้คำแนะนำ

7) การจัดทำเอกสาร กระบวนการ และเตรียมความพร้อมในการขอรับรองมาตรฐาน ISO/IEC 27701:2019 (Privacy Information Management System: PIMS) ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

8) การติดตั้งระบบรักษาความปลอดภัยสำหรับระบบฐานข้อมูล (Database Firewall)

4.1.1.3 จัดประชุมเปิดตัวโครงการ (Kick-off Meeting) และนำเสนอแผนการดำเนินการโครงการให้สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

4.2 จัดเตรียมบริการตรวจสอบช่องโหว่และมาตรฐานความปลอดภัยของเว็บแอปพลิเคชัน (Web Application Security Scanner) ของสำนักงานเขตพื้นที่การศึกษา ในรูปแบบซอฟต์แวร์พร้อมใช้งาน (Software-as-a-Service) โดยครอบคลุมขั้นตอนดังต่อไปนี้

4.2.1 ศึกษา วิเคราะห์ ออกแบบ และติดตั้งบริการตรวจสอบช่องโหว่และมาตรฐานความปลอดภัยของเว็บแอปพลิเคชัน (Web Application Security Scanner) ของสำนักงานเขตพื้นที่การศึกษาตามที่สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานกำหนด

4.2.2 ตั้งค่าเครื่องมือตรวจสอบช่องโหว่และมาตรฐานความปลอดภัยของเว็บแอปพลิเคชัน (Web Application Security Scanner) ของสำนักงานเขตพื้นที่การศึกษา ตามที่ได้จากการศึกษา วิเคราะห์ ออกแบบ และได้รับการอนุมัติจากสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

4.2.3 ทดสอบเครื่องมือตรวจสอบช่องโหว่และมาตรฐานความปลอดภัยของเว็บแอปพลิเคชัน (Web Application Security Scanner) ของสำนักงานเขตพื้นที่การศึกษา ให้พร้อมใช้งาน

4.3 จัดเตรียมบริการป้องกันการโจมตีในระดับเว็บแอปพลิเคชัน (Web Application Firewall) สำหรับเว็บแอปพลิเคชันของสำนักงานเขตพื้นที่การศึกษา ในรูปแบบซอฟต์แวร์พร้อมใช้งาน (Software-as-a-Service) ดังต่อไปนี้

4.3.1 ศึกษา วิเคราะห์ ออกแบบ และติดตั้งบริการป้องกันการโจมตีในระดับเว็บแอปพลิเคชัน (Web Application Firewall) สำหรับเว็บแอปพลิเคชันของสำนักงานเขตพื้นที่การศึกษา ตามแผนที่ได้เสนอไว้กับสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

4.3.2 ตั้งค่าเครื่องมือป้องกันการโจมตีในระดับเว็บแอปพลิเคชัน (Web Application Firewall) สำหรับเว็บแอปพลิเคชันของสำนักงานเขตพื้นที่การศึกษา ตามที่ได้จากการศึกษา วิเคราะห์ ออกแบบ และได้รับการอนุมัติจากสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

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

7.....8.....9.....10.....11.....

4.3.3 ทดสอบเครื่องมือป้องกันการโจมตีในระดับเว็บแอปพลิเคชัน (Web Application Firewall) สำหรับเว็บแอปพลิเคชันของสำนักงานเขตพื้นที่การศึกษา ให้พร้อมใช้งาน

4.4 จัดเตรียมบริการป้องกันการโจมตีประเภทที่ทำให้ระบบเว็บแอปพลิเคชันไม่สามารถใช้งานได้ (Web Application DDoS Protection) สำหรับเว็บแอปพลิเคชันของสำนักงานเขตพื้นที่การศึกษา ในรูปแบบซอฟต์แวร์พร้อมใช้งาน (Software-as-a-Service) ดังต่อไปนี้

4.4.1 ศึกษา วิเคราะห์ ออกแบบ และติดตั้งบริการป้องกันการโจมตีประเภทที่ทำให้ระบบเว็บแอปพลิเคชันไม่สามารถใช้งานได้ (Web Application DDoS Protection) สำหรับเว็บแอปพลิเคชันของสำนักงานเขตพื้นที่การศึกษาตามแผนที่ได้เสนอไว้กับสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

4.4.2 ตั้งค่าเครื่องมือป้องกันการโจมตีประเภทที่ทำให้ระบบเว็บแอปพลิเคชันไม่สามารถใช้งานได้ (Web Application DDoS Protection) สำหรับเว็บแอปพลิเคชันของสำนักงานเขตพื้นที่การศึกษา ตามที่ได้จากการศึกษา วิเคราะห์ ออกแบบ และได้รับการอนุมัติจากสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

4.4.3 ทดสอบเครื่องมือป้องกันการโจมตีประเภทที่ทำให้ระบบเว็บแอปพลิเคชันไม่สามารถใช้งานได้ (Web Application DDoS Protection) สำหรับเว็บแอปพลิเคชันของสำนักงานเขตพื้นที่การศึกษา ให้พร้อมใช้งาน

4.5 การตรวจสอบช่องโหว่และมาตรฐานความปลอดภัยของเว็บแอปพลิเคชันของสำนักงานเขตพื้นที่การศึกษา (Web Application Security Scan) และประเมินแนวทางการตั้งค่าระบบอย่างปลอดภัย (System Hardening) โดยครอบคลุมขั้นตอน อย่างน้อยดังต่อไปนี้

4.5.1 กำหนดเป้าหมาย Web Application ที่จะตรวจสอบช่องโหว่และมาตรฐานความปลอดภัยของเว็บแอปพลิเคชันของสำนักงานเขตพื้นที่การศึกษา (Web Application Security Scan) และประเมินแนวทางการตั้งค่าระบบอย่างปลอดภัย (System Hardening) จำนวนไม่น้อยกว่า 245 URLs

4.5.2 จัดทำแผนการดำเนินการ โดยระบุวัน และเวลา ที่จะตรวจสอบช่องโหว่และมาตรฐานความปลอดภัยของเว็บแอปพลิเคชันของสำนักงานเขตพื้นที่การศึกษา (Web Application Security Scan)

4.5.3 ตรวจสอบช่องโหว่และมาตรฐานความปลอดภัยของเว็บแอปพลิเคชัน (Web Application Security Scan) ของสำนักงานเขตพื้นที่การศึกษา โดยมีรายละเอียด อย่างน้อยดังนี้

4.5.3.1 ตรวจสอบช่องโหว่และมาตรฐานความปลอดภัยของเว็บแอปพลิเคชันของสำนักงานเขตพื้นที่การศึกษา (Web Application Security Scan) จำนวนไม่น้อยกว่า 245 URLs

4.5.3.2 วิเคราะห์ จัดลำดับความเสี่ยง จากผลของการตรวจสอบช่องโหว่และมาตรฐานความปลอดภัยของเว็บแอปพลิเคชันของสำนักงานเขตพื้นที่การศึกษา (Web Application Security Scan)

4.5.3.3 ประเมินความเสี่ยง/ผลกระทบที่อาจจะเกิดขึ้นจากการตรวจสอบช่องโหว่และมาตรฐานความปลอดภัยของเว็บแอปพลิเคชัน (Web Application Security Scan) ของสำนักงานเขตพื้นที่การศึกษา ร่วมกับสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

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

7.....8.....9.....10.....11.....

4.5.4 จัดทำและนำเสนอเอกสารการตรวจสอบช่องโหว่และมาตรฐานความปลอดภัยของเว็บแอปพลิเคชัน (Web Application Security Scan) ของสำนักงานเขตพื้นที่การศึกษา และกำหนดแนวทางการตั้งค่าระบบให้มีความปลอดภัย (System Hardening) อย่างน้อยดังต่อไปนี้

4.5.4.1 จัดทำรายงาน โดยมีเนื้อหา ครอบคลุมถึง ผลการประเมินต่าง ๆ พร้อมผลการวิเคราะห์ผลกระทบจากความเสี่ยง และเสนอแนะแนวทางแก้ไขปัญหา และช่องโหว่ที่พบจากการตรวจสอบมาตรฐานความปลอดภัยของระบบสารสนเทศเว็บแอปพลิเคชัน รวมถึงเสนอแนะแนวทางการตั้งค่าระบบอย่างปลอดภัย (System Hardening) สำหรับเว็บแอปพลิเคชันของสำนักงานเขตพื้นที่การศึกษา

4.5.4.2 สรุปผลการประเมิน และคำแนะนำสำหรับผู้บริหาร (Executive Summary)

4.6 ตอบสนองต่อภัยคุกคามทางไซเบอร์ (Incident Response) ที่ตรวจพบภายในศูนย์ข้อมูล (Data Center) ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน โดยผู้รับจ้างต้องดำเนินการอย่างน้อยดังต่อไปนี้

4.6.1 ประสานงานและดำเนินการร่วมกับเจ้าหน้าที่ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานในการจำกัดขอบเขตความเสียหาย (Containment) และการแพร่กระจายของมัลแวร์ในระบบสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

4.6.2 ประสานงานและดำเนินการร่วมกับเจ้าหน้าที่ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานในการกำจัดภัยคุกคามทางไซเบอร์ (Remediation) ที่เกิดขึ้นออกจากระบบสารสนเทศของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

4.6.3 เก็บหลักฐานทางดิจิทัล (Digital Evidence Collection) โดยเก็บข้อมูลอย่างน้อยดังนี้

4.6.3.1 ข้อมูลเหตุการณ์ต่าง ๆ หรือการจราจรของข้อมูล (Event or Communication Logs)

4.6.3.2 ข้อมูลของไฟล์ดัมพ์หน่วยความจำข้อมูล (Memory Dump)

4.6.3.3 ข้อมูลเหตุการณ์ต่าง ๆ จากอุปกรณ์รักษาความปลอดภัย (Security Tools and SIEM System)

4.6.3.4 ข้อมูลอื่น ๆ ที่เกี่ยวข้องกับเหตุการณ์ (Other Related Incident Data)

4.6.4 ประสานงานและดำเนินการร่วมกับเจ้าหน้าที่ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานในการเก็บรักษาสถานะของหลักฐานทางดิจิทัล (Evidence Preservation) สำหรับการวิเคราะห์เหตุการณ์บุกรุก

4.6.5 เก็บข้อมูลเครื่องคอมพิวเตอร์แม่ข่ายที่ถูกผู้ไม่ประสงค์ดีหรือแฮคเกอร์ (Threat Actor) โจมตี ที่อยู่ภายในศูนย์ข้อมูล (Data Center) ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานเพื่อวิเคราะห์ข้อมูล (Collection of Data for Analysis)

4.6.6 ประสานงานและดำเนินการร่วมกับเจ้าหน้าที่ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ในการแยกเครื่องคอมพิวเตอร์แม่ข่ายที่ถูกโจมตี ให้อยู่คนละระบบเครือข่าย กับเครื่องคอมพิวเตอร์แม่ข่ายปกติ (Network Segmentation and Isolation)

4.6.7 วิเคราะห์ข้อมูลเพื่อสรุปเหตุการณ์การโจมตี (Analysis of Data Collected in order to Reconstruct the Attack Lifecycle)

4.6.8 ดำเนินการทำวิศวกรรมผันกลับเพื่อระบุมัลแวร์ที่ถูกใช้งาน (Reverse Engineering Identified Malware) โดยระบุมัลแวร์ที่เกี่ยวข้องกับเหตุการณ์และข้อมูลอื่น ๆ ที่เกี่ยวข้อง เช่น ตัวชี้วัดภัยคุกคาม (Indicator of Compromise) ไอพีแอดเดรสของเครื่องคอมพิวเตอร์แม่ข่ายที่ควบคุมมัลแวร์ (Malware C&C Servers) เป็นต้น

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

7.....8.....9.....10.....11.....

4.6.9 วิเคราะห์มัลแวร์ที่ตรวจพบ (Malware Analysis) เพื่อสรุปพฤติกรรมของมัลแวร์

4.6.10 สรุปตัวชี้วัดภัยคุกคาม (Producing Indicators of Compromise and Indicators of Attack)

4.6.11 ประสานงานและร่วมดำเนินการกับเจ้าหน้าที่ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน เพื่อดำเนินการค้นหา (Scanning) ว่ายังมีภัยคุกคามดังกล่าวในระบบเครือข่ายและโครงสร้างพื้นฐาน (Network and Infrastructure) หรือไม่

4.6.12 วิเคราะห์ช่องทางและรูปแบบการโจมตีของกลุ่มผู้ไม่หวังดี (Incident Root Cause Analysis) โดยมีการค้นหาข้อมูลครอบคลุมรายละเอียดอย่างน้อยดังต่อไปนี้

4.6.12.1 ตรวจสอบรูปแบบการโจมตีของกลุ่มผู้ไม่หวังดี (Threat Actor Analysis Information Platform) เพื่อตรวจสอบดูว่าหน่วยงานมีข้อมูลที่รั่วไหลหรือถูกประกาศบนเว็บมืด (Dark Web) ที่กลุ่มผู้ไม่หวังดีใช้เป็นเครื่องมือในการเข้าถึงระบบสารสนเทศและบัญชีผู้ใช้งานหรือไม่ โดยครอบคลุมรายละเอียดดังต่อไปนี้

1) ข้อมูลรั่วไหล (Compromises) อย่างน้อยดังนี้
   - ข้อมูลผู้ใช้รั่วไหล (Accounts)
   - ข้อมูลฐานข้อมูลที่รั่วไหล (Breached DB)
   - ข้อมูลรั่วไหลจากสาธารณะ (Public Leaks)
   - ข้อมูลรั่วไหลจาก Git (GIT Leaks)
2) ข้อมูลกลุ่มผู้ไม่หวังดี (Threat Actor) อย่างน้อยดังนี้
   - ข้อมูลรูปแบบการโจมตี (Tactics Technique Procedure: TTP)
   - ประวัติการโจมตีของกลุ่มผู้ไม่หวังดี (Brief history and timeline)
3) ข้อมูลมัลแวร์ (Malware) อย่างน้อยดังนี้
   - ข้อมูลทั่วไป (Information)
   - ข้อมูล MITRE ATT&CK
   - ข้อมูล Signatures
   - ข้อมูล Net indicators
   - ข้อมูล Files
   - ข้อมูล Configs
4) ข้อมูลไอพีต้องสงสัย (Suspicious IP) อย่างน้อยดังนี้
   - The Onion Router
   - Open Proxy
   - Socks Proxy
   - Scanning IP
   - VPN
5) วิเคราะห์และกำหนด Hunting Rules แบบไม่จำกัดจำนวน (Unlimited Number of Hunting Rules)

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

7.....8.....9.....10.....11.....

6) ผู้รับจ้างต้องใช้เครื่องมือประเภท Threat Actor Analysis Information Platform ที่ได้รับการรับรองจาก SPARK Matrix™: Digital Threat Intelligence Management ปี 2025 หรือปีล่าสุด ในระดับ SPARK Leaders

4.6.12.2 ตรวจสอบช่องทางการเข้าถึงระบบสารสนเทศองค์กรจากภายนอก (External Attack Surface) โดยครอบคลุมรายละเอียดดังต่อไปนี้

1) วิเคราะห์ผลการประเมินความเสี่ยงในส่วนของช่องโหว่ (Vulnerability) โดยตรวจสอบการใช้งานระบบปฏิบัติงาน (Operating System) เซอร์วิสที่ใช้งาน (Services) แอปพลิเคชัน (Application) ซอฟต์แวร์ (Software) และฮาร์ดแวร์ (Hardware) จากฐานข้อมูลที่เก็บข้อมูลเกี่ยวกับช่องโหว่ด้านความปลอดภัยของซอฟต์แวร์และระบบคอมพิวเตอร์ (Common Vulnerabilities Exposure: CVE) โดยจะดำเนินการตรวจสอบช่องโหว่ครอบคลุมตามรายละเอียด อย่างน้อยดังนี้

- ฐานข้อมูลที่มีการเปิดการเข้าถึงจากอินเทอร์เน็ต (Open Databases)
- ระบบเก็บข้อมูลที่มีการเปิดการเข้าถึงจากอินเทอร์เน็ต (Buckets of File Storages)
- ระบบไดเร็กทอรี่ที่มีการเปิดการเข้าถึงจากอินเทอร์เน็ต (Open Listings of Directories)
- การตั้งค่าระบบสารสนเทศที่ไม่ถูกต้องอื่น ๆ (Potential Misconfigurations)

2) วิเคราะห์ผลการประเมินความเสี่ยงความปลอดภัยด้านระบบเครือข่าย (Network Security) ซึ่งตรวจสอบโดยการค้นหา (Scanning) ผ่านระบบอินเทอร์เน็ตไปยังที่อยู่เครือข่ายย่อย (Subnet) ภายในสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน โดยดำเนินการตรวจสอบครอบคลุมตามรายละเอียด อย่างน้อยดังนี้

- การเปิดการเข้าถึงระยะไกลของผู้ดูแลระบบ (Remote Administrative Services)
- การใช้งานเซอร์วิสผ่านอินเทอร์เน็ต (Open Ports)
- การเข้ารหัสเว็บไซต์ที่ไม่ปลอดภัย (Insecure Service Headers)
- การใช้งานพร็อกซี (Proxy Node)
- การเป็นเป้าหมายของการโจมตีด้วยการส่งคำขอเข้าไปเป็นจำนวนมากทำให้เว็บไซต์ไม่สามารถใช้งานได้ (DDoS Attack)

3) วิเคราะห์ผลการประเมินความเสี่ยงในส่วนของความปลอดภัยด้านข้อมูลรั่วไหล (Leaked Credentials) ตรวจสอบครอบคลุมตามรายละเอียด อย่างน้อยดังนี้

- ข้อมูลรั่วไหลจากการเป็นเป้าหมายการบุกรุก (Targeted Data Breaches) โดยข้อมูลลักษณะนี้จะมาจากแหล่งของเว็บมืด (Dark Web)
- ข้อมูลรั่วไหลจากเว็บไซต์สาธารณะ (Public Available Data Breaches) โดยข้อมูลลักษณะนี้จะมาจากเว็บไซต์สาธารณะ

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

7.....8.....9.....10.....11.....

4) วิเคราะห์ผลการประเมินความเสี่ยงในส่วนของความปลอดภัยด้านมัลแวร์ (Malware Security) ตรวจสอบครอบคลุมตามรายละเอียด อย่างน้อยดังนี้

- การตกเป็นเหยื่อของการปลอมแปลงหน้าเว็บไซต์ (Phishing Content)
- การตกเป็นเหยื่อของการแพร่กระจายมัลแวร์ (Malware Distribution)
- การตกเป็นเหยื่อของการฝังมัลแวร์ (Malware Embedded)

5) วิเคราะห์ผลการประเมินความเสี่ยงในส่วนของความปลอดภัย ที่ปรากฏบนเว็บมืด (Dark Web Mention) โดยตรวจสอบครอบคลุมในส่วนของการถูกพูดถึงบนเว็บมืด การรั่วไหลหรือการตกเป็นเป้าหมายการโจมตีของผู้ไม่หวังดี

6) วิเคราะห์ผลการประเมินความเสี่ยงในส่วนของความปลอดภัยการเข้ารหัสเว็บไซต์ (SSL/TLS Security) ตรวจสอบครอบคลุมตามรายละเอียด ดังนี้

- การเข้ารหัสที่ไม่ปลอดภัย (Insecure SSL/TLS)
- การใช้งานการเข้ารหัสที่จะหมดอายุ (Expired Certificate)
- การใช้งานมาตรฐานการเข้ารหัสที่ไม่มีความปลอดภัย (Insecure Standard)
- การใช้งานเซอร์วิสที่มีความเสี่ยงในการเข้าถึง (Insecure Ports)

7) วิเคราะห์ผลการประเมินความเสี่ยงในส่วนของความปลอดภัยการใช้งานอีเมล (Email Security) โดยตรวจสอบครอบคลุมในส่วนของการตั้งค่าความปลอดภัยของอีเมลหน่วยงานเพื่อป้องกันการสวมรอย

8) วิเคราะห์ผลการประเมินความเสี่ยงในส่วนของความปลอดภัยทางด้านการใช้งานโดเมน (Domain & DNS Security) โดยตรวจสอบครอบคลุมในส่วนของการตั้งค่าความปลอดภัยของโดเมนหน่วยงาน (DNSSEC)

9) ผู้รับจ้างต้องใช้เครื่องมือประเภท External Attack Surface Management (EASM) ที่เจ้าของผลิตภัณฑ์อยู่ใน Frost Radar TM Report ประเภท External Attack Surface Management ในระดับ Leader ปี 2024 หรือปีล่าสุด และอยู่ใน Frost Radar TM Report ประเภท Cyber Threat Intelligence ในระดับ Leader ปี 2024 หรือปีล่าสุด

4.6.13 สรุปรายงานการตอบสนองต่อภัยคุกคามทางไซเบอร์ (Report with Information about the Work Performed) ครอบคลุมรายละเอียดอย่างน้อยดังต่อไปนี้

4.6.13.1 ช่วงเวลาการเกิดเหตุการณ์ (Timeline)

4.6.13.2 รายละเอียดช่องทางและรูปแบบการโจมตีของกลุ่มผู้ไม่หวังดี (Incident Root Cause Analysis)

4.6.13.3 รายละเอียดของมัลแวร์ (Malware) ที่ถูกใช้งานและกลุ่มผู้ไม่หวังดีที่โจมตีเข้ามาในระบบสารสนเทศ

4.6.13.4 รายงานความเสียหาย (Impact Analysis) ที่เกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่ายในขอบเขตที่ถูกผู้ไม่หวังดี (Threat Actor) โจมตี

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

7.....8.....9.....10.....11.....

4.6.13.5 ข้อเสนอแนะสำหรับการจำกัดขอบเขตความเสียหาย (Containment)

4.6.13.6 ข้อเสนอแนะสำหรับการกำจัดภัยคุกคามทางไซเบอร์ (Remediation)

4.6.13.7 ข้อเสนอแนะสำหรับการป้องกันไม่ให้เกิดเหตุการณ์เดิมในอนาคต (Preventive Guideline)

4.7 จัดทำเอกสาร กระบวนการ และเตรียมความพร้อมในการขอรับรองมาตรฐาน ISO/IEC 27001:2022 (Information Security Management System: ISMS) และมาตรฐาน ISO/IEC 27701:2019 (Privacy Information Management System: PIMS) สำหรับศูนย์ข้อมูล (Data Center) สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน โดยมีรายละเอียดการดำเนินงาน อย่างน้อยดังต่อไปนี้

4.7.1 ดำเนินงานตามมาตรฐาน ISO/IEC 27001:2022 และ ISO/IEC 27701:2019 อย่างน้อยดังต่อไปนี้

4.7.1.1 กำหนดกิจกรรม และจัดทำแผนการดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS/PIMS Project Plan) โดยระบุกิจกรรมทั้งหมดที่ต้องดำเนินการให้ครบถ้วน

4.7.1.2 ทบทวนและติดตามผลการดำเนินงานของรายการความไม่สอดคล้องทั้งหมดจากการตรวจประเมินรอบปีที่ผ่านมา และจัดทำรายงานสรุปสถานการณ์ดำเนินงานพร้อมข้อแนะนำ

4.7.1.3 ทบทวนและปรับปรุง ISMS/PIMS Scope ให้ครอบคลุมขอบเขตงานที่กำหนด

4.7.1.4 ประเมิน ISMS/PIMS Gap Analysis ให้เป็นไปตามมาตรฐานและสามารถเชื่อมโยงกับแนวทางปฏิบัติงานตามมาตรฐานปัจจุบันที่สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

4.7.1.5 ดำเนินการทบทวนปรับปรุงรายการกฎหมาย ข้อบังคับ นโยบาย ที่เกี่ยวข้อง (Regulatory Compliance List) พร้อมทั้งให้ข้อเสนอแนะ โดยให้ปรับปรุงเอกสารทุกครั้งที่มีการเปลี่ยนแปลงของรายการกฎหมาย ข้อบังคับ นโยบาย

4.7.1.6 ทบทวนนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ และด้านความปลอดภัยของข้อมูลส่วนบุคคล (ISMS/PIMS Policy)

4.7.1.7 จัดทำ ISMS/PIMS Manual ให้ครอบคลุมขอบเขตงานที่กำหนด รวมถึงมาตรการเกี่ยวกับ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และกฎหมายลำดับรองที่เกี่ยวข้อง

4.7.1.8 จัดทำเอกสาร Statement of Applicability (SOA)

4.7.1.9 ทบทวนบัญชีรายชื่อเอกสาร (Document Master List) และทบทวน/ปรับปรุงเอกสารตามบัญชีรายชื่อเอกสาร โดยสาระสำคัญต้องเป็นไปตามมาตรฐาน ISO/IEC 27001:2022 (Data Center) และ ISO/IEC 27701:2019 (ระบบการบริหารบุคลากรภายใน ที่มีการจัดเก็บข้อมูลเจ้าหน้าที่หรือบุคคลภายนอก) ให้สอดคล้องกับหลักปฏิบัติที่เหมาะสมของ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน พร้อมจัดทำเอกสารเพิ่มเติมอื่น ๆ ที่เกี่ยวข้อง

4.7.1.10 ทบทวนและปรับปรุงรายการซอฟต์แวร์ (Software List) ที่อนุญาตให้ติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่าย

4.7.1.11 จัดทำทะเบียนควบคุม (ISMS และ PIMS Record Tracking) ประกอบด้วย

1) รายการที่กำหนดให้มีการทบทวน/ปรับปรุง
2) กิจกรรมตามแผนการจัดการความเสี่ยง
3) กิจกรรมการวัดประสิทธิผล

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

7.....8.....9.....10.....11.....

4) กิจกรรมตามแผนการสื่อสาร

5) การดำเนินการตามกฎหมายที่เกี่ยวข้อง

6) รายการการเปลี่ยนแปลง (Change) และรายการเหตุการณ์ละเมิด (Incident) ที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ และข้อมูลส่วนบุคคล

4.7.1.12 สำรวจความคิดเห็นจากผู้มีส่วนได้ส่วนเสียหรือผู้ที่มีส่วนเกี่ยวข้อง (Feedback from Interested Parties) ในขอบเขตงานตามข้อกำหนดของมาตรฐาน พร้อมจัดทำรายงาน ผลการสำรวจความคิดเห็น

4.7.2 การดำเนินงานสำหรับส่วนเฉพาะของมาตรฐาน ISO/IEC 27701:2019

4.7.2.1 ทบทวนปรับปรุง Data Mapping และ Record of Processing Activities ให้เป็นปัจจุบัน

4.7.2.2 ทบทวนและปรับปรุงเอกสารเกี่ยวกับการบริหารจัดการข้อมูลส่วนบุคคล ให้สอดคล้องตามกฎหมาย อย่างน้อยดังนี้

1) สัญญาการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA)

2) สัญญารักษาความลับ (Non-Disclosure Agreement: NDA)

3) ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (Data Sharing Agreement: DSA)

4) ขั้นตอนการประเมินผลกระทบการใช้ข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA)

5) จัดทำแผนการสื่อสาร แนวทางดำเนินการและประเมินผลการสื่อสาร

4.7.3 กิจกรรมการบริหารจัดการความเสี่ยง วางแผนและดำเนินงานบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management) โดยใช้หลักการ ISO/IEC 27001:2022 และดำเนินงานบริหารจัดการความเสี่ยงด้านการบริหารจัดการข้อมูลส่วนบุคคล (PII Risk Assessment and Data Privacy Impact Analysis) ผลการดำเนินงานครอบคลุม ดังนี้

4.7.3.1 จัดทำแผนดำเนินการของกิจกรรมประเมินความเสี่ยงและการจัดการความเสี่ยง และระบุส่วนงานที่เกี่ยวข้องกับกิจกรรมต่าง ๆ อย่างน้อยดังนี้

1) วิเคราะห์ผู้มีส่วนได้ส่วนเสียของกระบวนการบริหารจัดการความเสี่ยง

2) ระบุความเสี่ยง จัดทำทะเบียนความเสี่ยง วิเคราะห์ความเสี่ยงและโอกาสในการเกิดของผู้มีส่วนได้ส่วนเสีย และของระบบงานที่เกี่ยวข้อง และนำมาเป็นส่วนหนึ่งในการกำหนด ตัวชี้วัดความเสี่ยง (Key Risk Indicator: KRI)

3) จัดทำแผนการสื่อสารให้กับผู้มีส่วนได้ส่วนเสียและดำเนินการสื่อสารกระบวนการบริหารความเสี่ยง และประเมินผลการรับรู้ของกิจกรรมการบริหารความเสี่ยง

4) กำหนดเกณฑ์การวัดประสิทธิผลของการบริหารความเสี่ยง

5) จัดทำตัวชี้วัดความเสี่ยง (Key Risk Indicator: KRI) ของการบริหารความเสี่ยง และประเมินประสิทธิผล ที่มีรายละเอียดการวัด ตัววัดผลลัพธ์ (outcome) การติดตาม วิเคราะห์ประเมินของกระบวนการที่เกี่ยวข้องกับการดำเนินธุรกิจให้สอดคล้องกับความสำคัญของเทคโนโลยีสารสนเทศแต่ละระบบงาน

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

7.....8.....9.....10.....11.....

6) จัดทำบริบทของการบริหารจัดการความเสี่ยง (Context Establishment) ประกอบด้วยหัวข้อต่อไปนี้

(1) ขอบเขตการดำเนินการ

(2) Basic Criteria ประกอบด้วย

- Risk management approach
- Risk evaluation criteria
- Impact criteria
- Risk acceptance criteria

(3) โครงสร้างการบริหารจัดการความเสี่ยง

7) ระบุรายละเอียดของความเสี่ยง (Risk Identification) ประกอบด้วย

(1) ทบทวนและปรับปรุงรายการทรัพย์สิน (Asset Inventory) และประเมินมูลค่าของทรัพย์สิน (Asset Valuation)

(2) ระบุและจัดทำPII Inventory

(3) ระบุรายชื่อเจ้าของความเสี่ยง (Risk Owner)

(4) จัดทำและทบทวนทะเบียนความเสี่ยงและผลกระทบ (Risk Profile)

(5) จัดทำและทบทวนทะเบียนภัยคุกคาม (List of Threat)

(6) ระบุมาตรการควบคุมที่บังคับใช้

(7) จัดทำและทบทวนทะเบียนช่องโหว่

8) ทบทวนคู่มือวิธีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2022 และคู่มือวิธีการประเมินความเสี่ยงด้านการบริหารจัดการข้อมูลส่วนบุคคล

9) ประเมินความเสี่ยง (Risk Analysis and Evaluation) คัดเลือกวิธีการจัดการความเสี่ยง และวางแผนดำเนินการจัดการความเสี่ยง

10) จัดทำรายงานผลการประเมินความเสี่ยง (Risk Assessment Report) ตามรูปแบบที่สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานกำหนด

11) จัดทำคู่มือการปฏิบัติเพื่อควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ พร้อมรูปแบบแผนจัดการความเสี่ยง

12) จัดทำรายงานผลการทบทวนปรับปรุงกระบวนการหรือวิธีการประเมินความเสี่ยง และแนวทางปรับปรุงกระบวนการทำงาน

4.7.4 กิจกรรมการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan)

4.7.4.1 ทบทวนแผนการบริหารความต่อเนื่องทางธุรกิจ ให้ครอบคลุมขอบเขตงานที่กำหนด

4.7.4.2 กรณีมีการซักซ้อมแผนฉุกเฉิน เพื่อบริหารความต่อเนื่องทางธุรกิจ ให้จัดทำรายงานผลการซ้อมแผนฉุกเฉินเพื่อบริหารความต่อเนื่องทางธุรกิจ

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

7.....8.....9.....10.....11.....

4.7.5 จัดอบรมหลักสูตรที่เกี่ยวข้องกับมาตรฐาน ISO/IEC27001:2022 และISO/IEC27701:2019 ให้แก่บุคลากรของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานและผู้เกี่ยวข้อง ณ สถานที่ตามที่สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานกำหนด โดยมีหลักสูตรดังต่อไปนี้

4.7.5.1 หลักสูตรมาตรฐานความมั่นคงปลอดภัยข้อมูลสารสนเทศ ISO/IEC 27001:2022 และความมั่นคงปลอดภัยข้อมูลส่วนบุคคล ISO/IEC27701:2019 จำนวนไม่น้อยกว่า 5 คน ระยะเวลาอบรมไม่น้อยกว่า 5 ชั่วโมง

4.7.5.2 หลักสูตรการตรวจประเมินภายในมาตรฐานความมั่นคงปลอดภัยข้อมูลสารสนเทศ ISO/IEC27001:2022 และความมั่นคงปลอดภัยข้อมูลส่วนบุคคล ISO/IEC27701:2019 จำนวนไม่น้อยกว่า 5 คน ระยะเวลาอบรมไม่น้อยกว่า 5 ชั่วโมง

4.7.6 สนับสนุนให้สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ผ่านการตรวจรับรองเพื่อให้ได้ Certificate ตามมาตรฐาน ISO/IEC 27001:2022 และ ISO/IEC 27701:2019 ตามขอบเขตงานที่กำหนด โดยครอบคลุมขั้นตอน อย่างน้อยดังต่อไปนี้

4.7.6.1 การตรวจประเมินภายใน

1) วิเคราะห์ผู้มีส่วนได้ส่วนเสียของกระบวนการตรวจประเมินภายใน

2) จัดทำขั้นตอนการตรวจประเมินภายใน

3) กำหนดหลักเกณฑ์ และวางแผนการวัดประสิทธิผลของการตรวจประเมินภายใน

4) จัดทำแผนการสื่อสารกิจกรรมการตรวจประเมินภายใน และวัดผลการสื่อสาร

5) จัดทำแผนการตรวจประเมินภายใน (Internal Audit Plan) ทั้งนี้ต้องส่งแผนให้สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ทราบล่วงหน้าก่อนวันตรวจจริง อย่างน้อย 1 เดือน

6) มีโปรแกรมการตรวจประเมินภายใน (Internal Audit Program) พร้อมกำหนดหัวข้อตรวจประเมินภายใน (Internal Audit Checklist)

7) เข้าร่วมดำเนินการกับสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานในการดำเนินการตรวจประเมินภายใน (Internal Auditor) ให้ครอบคลุมขอบเขตงานที่กำหนด พร้อมทั้งสรุปประเด็นให้สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

8) จัดทำรายงานผลการตรวจประเมินภายใน (Internal Audit Report)

9) สนับสนุนและให้ข้อเสนอแนะในการแก้ไขข้อบกพร่อง (Non Conformity: NC) ที่ตรวจพบจากการตรวจประเมินภายใน

10) วัดประสิทธิผลของกิจกรรมตรวจประเมินภายใน และรายงานผล

4.7.6.2 การตรวจรับรอง

1) จัดหาผู้ตรวจรับรอง (Certification Body: CB) เพื่อทำการตรวจรับรองมาตรฐาน ISO/IEC 27001:2022 และ ISO/IEC 27701:2019 ภายใต้ขอบเขตงานที่กำหนด โดยผู้รับจ้างเป็นผู้รับผิดชอบค่าใช้จ่าย

2) กำหนดหลักเกณฑ์ และวางแผนการวัดประสิทธิผลของการตรวจรับรอง

3) วางแผนการสื่อสารกิจกรรมการตรวจรับรอง และวัดผลการสื่อสาร

4) เตรียมความพร้อมและซักซ้อมผู้เกี่ยวข้องก่อนการตรวจรับรอง สำหรับมาตรฐาน ISO/IEC 27001:2022 และ ISO/IEC 27701:2019

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

7.....8.....9.....10.....11.....

5) ร่วมสังเกตการณ์การตรวจรับรอง

6) ติดตามผลการตรวจรับรอง

7) สนับสนุนและให้ข้อเสนอแนะในการแก้ไขข้อบกพร่อง (Non Conformity: NC) ที่ตรวจพบจากการตรวจรับรอง

8) จัดทำเอกสารและหลักฐานเพื่อประกอบการแก้ไขข้อบกพร่อง

9) วัดประสิทธิผลของกิจกรรมตรวจรับรอง และรายงานผล

4.8 จัดเตรียมบริการรักษาความปลอดภัยสำหรับระบบฐานข้อมูล (Database Firewall) ของแอปพลิเคชันในศูนย์ข้อมูล (Data Center) สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน โดยครอบคลุมขั้นตอนดังต่อไปนี้

4.8.1 ศึกษา วิเคราะห์ ออกแบบและติดตั้งระบบรักษาความปลอดภัยสำหรับระบบฐานข้อมูล (Database Firewall) ของแอปพลิเคชันในศูนย์ข้อมูล (Data Center) สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ตามแผนที่ได้เสนอไว้กับสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

4.8.2 ตั้งค่าเครื่องมือรักษาความปลอดภัยสำหรับระบบฐานข้อมูล (Database Firewall) ของแอปพลิเคชันในศูนย์ข้อมูล (Data Center) สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ตามรูปแบบที่ได้ศึกษา ออกแบบ และได้รับการอนุมัติในการดำเนินการตามที่สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานกำหนด

4.8.3 ทดสอบเครื่องมือรักษาความปลอดภัยสำหรับระบบฐานข้อมูล (Database Firewall) ของแอปพลิเคชันในศูนย์ข้อมูล (Data Center) สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ให้พร้อมใช้งาน

5. คุณสมบัติของบริการ

5.1 บริการตรวจสอบช่องโหว่และมาตรฐานความปลอดภัยของเว็บแอปพลิเคชัน (Web Application Security Scanner) โดยมีคุณสมบัติอย่างน้อยดังต่อไปนี้

5.1.1 บริการที่เสนอต้องได้รับการจัดลำดับให้อยู่ในกลุ่ม Leaders ของ Gartner Magic Quadrant สำหรับ Application Security Testing ปี 2023 หรือปีล่าสุด และอยู่ในกลุ่ม Leaders ของ The Forrester Wave สำหรับ Software Composition Analysis ปี 2024 หรือปีล่าสุด

5.1.2 สามารถตรวจหาช่องโหว่ Web Application ตาม Signature หรือ ฐานข้อมูล Security Vulnerabilities อย่างน้อยตาม OWASP Top 10 2021 หรือปีล่าสุด

5.1.3 สามารถเลือกวิธีการสแกน Web Application ด้วยการใช้ CRAWLER

5.1.4 สามารถตรวจสอบช่องโหว่ของ Web Application ไม่น้อยกว่า 245 URLs

5.1.5 สามารถตรวจสอบช่องโหว่ของ Web Application เช่น Cross-Site Scripting, SQL Injections, PHP code injection (หรือ Local File Inclusion), Log4j Log4Shell (CVE-2021-42287), Open redirection, Server-Side Request Forgery, Operating system command injection ได้เป็นอย่างน้อย

5.1.6 สามารถปรับแต่งการตั้งค่าโปรไฟล์ (Custom Profile) ในการสแกนได้

5.1.7 สามารถดำเนินการทำ Schedule Scan ได้

5.1.8 สามารถสั่ง Scan, Pause, Resume, หรือ Stop การตรวจสอบช่องโหว่ได้

5.1.9 สามารถกำหนดช่องโหว่กับผู้ใช้งานระบบได้ (Assign vulnerabilities to a team member)

5.1.10 มี Scanning Agent สำหรับการตรวจสอบช่องโหว่ที่อยู่ในระบบเครือข่ายภายในได้

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

7.....8.....9.....10.....11.....

5.1.11 สามารถจัดทำรายงานผลของการตรวจสอบช่องโหว่แบ่งเป็น PCI-DSS v.4.0.1 and v.3.2.1, OWASP Top 10, ISO 27001, HIPAA ได้เป็นอย่างน้อย

5.1.12 สามารถจัดทำรายงานในรูปแบบ PDF/DOCX ได้เป็นอย่างน้อย

5.2 บริการป้องกันการโจมตีในระดับเว็บแอพพลิเคชั่น (Web Application Firewall) โดยมีคุณสมบัติอย่างน้อยดังต่อไปนี้

5.2.1 บริการที่นำเสนอต้องได้รับการจัดลำดับให้อยู่ในกลุ่ม Leaders ของ The Forrester Wave สำหรับ Web Application Firewall Solutions ปี 2025 หรือปีล่าสุด และอยู่ในกลุ่ม Leader ของ GIGAOM Radar Report สำหรับ Content Delivery Network ปี 2024 หรือปีล่าสุด

5.2.2 ให้บริการบนระบบ Cloud แบบ Software as a Service (SaaS) และสามารถใช้งานได้ไม่น้อยกว่า 245 URLs

5.2.3 รองรับการใช้งานแบบ Data Transfer ไม่น้อยกว่า 1 TB ต่อเดือน

5.2.4 ต้องมี Node หรือ Point of Presence (POPs) จำนวนไม่น้อยกว่า 250 แห่งทั่วโลก และมีจำนวนไม่น้อยกว่า 6 แห่ง ในประเทศไทย โดยแต่ละแห่งต้องมีความสามารถในการทำ Web Application Firewall (WAF) และ Content Delivery Network (CDN)

5.2.5 ต้องได้รับการรับรองมาตรฐาน ISO 27001 และ SOC Type II เป็นอย่างน้อย

5.2.6 สามารถป้องกันการโจมตีผ่านทางเว็บไซต์ตาม OWASP Top 10 เช่น SQL injection, Broken Authentication, Cross-site Scripting ได้

5.2.7 สามารถกำหนดค่า IP Firewall ด้วยเงื่อนไข Source IP Address, Source IP Address Range, Autonomous System Number (ASN) และระบุประเทศได้

5.2.8 สามารถตั้งค่า Web Application Firewall (WAF) และสามารถแก้ไข เพิ่ม Custom WAF Rules ได้ไม่น้อยกว่า 1,000 Rules

5.2.9 สามารถกำหนด Action ของ Rule ที่สร้างขึ้นมาเองได้ เช่น Log, Manage Challenge และ Block

5.2.10 สามารถทำ Delivery Policy หรือ Request Header Transform เพื่อ Rewrite Request ได้ เช่น Redirect URL, Rewrite Request URL, Rewrite Request Header และ Remove Request Header

5.2.11 สามารถ Cache Content ที่เป็น Static Content หรือ Dynamic Content และสามารถทำ Custom Cache Rule ได้

5.2.12 สามารถทำ Tiered Caching หรือ Cache Shield ได้

5.2.13 สามารถลดขนาดของรูปภาพได้โดยสามารถเลือกได้ทั้งแบบ Lossless และ Lossy รวมถึงรองรับ WebP

5.2.14 มีระบบ Always Online ที่สามารถทำการแสดง Static Content ในกรณีที่ Server ต้นทางไม่สามารถใช้งานได้

5.2.15 มี Real-Time Dashboard โดยต้องสามารถแสดงข้อมูล ปริมาณ Requests, Cached Request, Response Time, Top Sources, Top URL ได้เป็นอย่างน้อย

5.2.16 รองรับการส่ง Raw Log ผ่านทาง Logpull หรือ REST API หรือ Logpush ไปยังอุปกรณ์หรือระบบ SIEM ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานได้

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

7.....8.....9.....10.....11.....

5.2.17 สามารถสรุปการใช้งานแบบรายสัปดาห์ หรือ แบบรายเดือน

5.2.18 สามารถทำการแจ้งเตือนผู้ดูแลระบบ เมื่อมีเหตุการณ์ที่เกิดขึ้นตามเงื่อนไขที่กำหนด ผ่านทาง Email ได้เป็นอย่างน้อย

5.2.19 สามารถบริหารจัดการปริมาณผู้ใช้งานเว็บไซต์ โดยมีฟังก์ชัน Waiting Room เพื่อควบคุมจำนวนผู้เข้าใช้งานพร้อมกันได้

5.2.20 มี Waiting Room ที่สามารถปรับแต่งรูปแบบการแสดงผลได้ และรองรับการตอบกลับแบบ JSON

5.2.21 รองรับการเข้ารหัสข้อมูลแบบ End-to-End ด้วยการเข้ารหัสแบบ Post-Quantum โดยใช้ Hybrid Key Exchange สำหรับการเชื่อมต่อในทั้งเส้นทางอย่างน้อยดังนี้

5.2.21.1 การเชื่อมต่อจากผู้ใช้งานมายังเครือข่ายผู้ให้บริการ (Visitor to Edge)

5.2.21.2 การเชื่อมต่อภายในเครือข่ายหลักของผู้ให้บริการ (Edge to Edge)

5.2.21.3 การเชื่อมต่อไปยัง Origin Server (Edge to Origin)

5.2.22 สามารถกำหนดสิทธิผู้ใช้งาน (Role-Based Access Control) และยืนยันตัวตนด้วยวิธี Two-Factor Authentication ได้

5.2.23 บริการที่นำเสนอต้องเป็นผลิตภัณฑ์ที่เป็นเครื่องหมายการค้าเดียวกันกับระบบป้องกันการโจมตีประเภทที่ทำให้ระบบเว็บแอพพลิเคชั่นไม่สามารถใช้งานได้ (Web Application DDoS Protection) ในข้อ 5.3 และต้องสามารถเข้าได้งานได้จากหน้าบริหารจัดการเดียวกัน (Management Console)

5.3 บริการป้องกันการโจมตีประเภทที่ทำให้เว็บแอปพลิเคชันไม่สามารถใช้งานได้ (Web Application DDoS Protection) โดยมีคุณสมบัติอย่างน้อยดังต่อไปนี้

5.3.1 บริการที่นำเสนอต้องได้รับการจัดลำดับให้อยู่ในกลุ่ม Technology Leaders ของ SPARK Matrix™สำหรับ DDoS Mitigation ปี 2024 หรือปีล่าสุด และอยู่ในกลุ่ม Technology Leaders ของ SPARK Matrix™ สำหรับ Bot Management ปี 2024 หรือปีล่าสุด

5.3.2 ให้บริการบนระบบ Cloud แบบ Software as a Service (SaaS) และสามารถใช้งานได้ไม่น้อยกว่า 245 URLs

5.3.3 ต้องมี Node หรือ Point of Presence (POPs) จำนวนไม่น้อยกว่า 250 แห่งทั่วโลก และมีจำนวนไม่น้อยกว่า 6 แห่ง ในประเทศไทย โดยแต่ละแห่งต้องรองรับการให้บริการ DDoS Mitigation

5.3.4 ต้องได้รับการรับรองมาตรฐาน ISO 27001 และ SOC Type II ได้เป็นอย่างน้อย

5.3.5 สามารถป้องกันการโจมตี DDoS Attack Layer 3, Layer 4 และ Layer 7 ได้อัตโนมัติ โดยไม่มีผลกระทบต่อผู้ใช้งานปกติ

5.3.6 มีระบบป้องกัน Web DDoS attacks ที่ทำงานแบบอัตโนมัติ ไม่จำกัดจำนวนครั้ง (Unlimited DDOS Protection) และสามารถรองรับการโจมตีแบบ DDoS Volumetric Attacks ได้อย่างน้อย 245 Tbps และมีความสามารถในการป้องกันการโจมตีจากในระดับเครือข่าย (DDoS) ขนาด 405 Tbps เป็นอย่างน้อยโดยไม่ส่งผลกระทบต่อผู้ใช้งานปกติขณะเปิดระบบป้องกัน และไม่มีการคิดค่าบริการจากปริมาณการรับ-ส่งข้อมูลที่เกิดขึ้นจากการโจมตี

5.3.7 มี Real-Time Dashboard โดยต้องสามารถแสดงข้อมูล ปริมาณ Requests, Cached Request, Response Time, Top Sources, Top URL ได้เป็นอย่างน้อย

5.3.8 ระบบต้องสามารถป้องกันการโจมตีแบบ Requests From Known Botnet ได้

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

7.....8.....9.....10.....11.....

5.3.9 ผู้ให้บริการต้องมีการรับประกันความพร้อมใช้งานของระบบ (Service Level Agreement: SLA) สำหรับการให้บริการป้องกันการโจมตีแบบ DDoS

5.3.10 มี Dashboard ช่วยผู้ใช้วิเคราะห์ Traffic ว่าเป็นมนุษย์หรือ Bot ด้วยวิธีการ Machine Learning และ Heuristic ได้

5.3.11 รองรับการส่ง Raw Log ผ่านทาง Logpull หรือ REST API หรือ Logpush ไปยังอุปกรณ์หรือระบบ SIEM ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานได้

5.3.12 ผู้ให้บริการต้องให้บริการ Authoritative DNS Services สำหรับโดเมนสาธารณะ

5.3.13 สามารถสรุปการใช้งานแบบรายสัปดาห์ หรือ แบบรายเดือน

5.3.14 สามารถทำการแจ้งเตือนผู้ดูแลระบบ เมื่อมีเหตุการณ์ที่เกิดขึ้นตามเงื่อนไขที่กำหนดไว้ผ่านทาง Email ได้เป็นอย่างน้อย

5.3.15 สามารถกำหนดสิทธิผู้ใช้งาน (Role-based Access Control) และยืนยันตัวตนด้วยวิธี Two-Factor Authentication ได้

5.4 บริการรักษาความปลอดภัยสำหรับระบบฐานข้อมูล (Database Firewall) โดยมีคุณสมบัติอย่างน้อยดังต่อไปนี้

5.4.1 เป็นซอฟต์แวร์ที่ออกแบบมาเพื่อตรวจสอบ ควบคุมและป้องกันการโจมตีฐานข้อมูลเพื่อให้สามารถใช้ข้อมูลจากฐานข้อมูลให้มีความปลอดภัย

5.4.2 มีสิทธิ์ในการใช้งานไม่น้อยกว่า 3 กลุ่มฐานข้อมูล (Database Cluster) ที่สามารถรองรับไม่น้อยกว่า 25 ฐานข้อมูล (Database Instance) หรือเทียบเท่า

5.4.3 สามารถตรวจสอบและป้องกันการโจมตีฐานข้อมูลดังต่อไปนี้ได้เป็นอย่างน้อย ได้แก่ PostgreSQL, MySQL, MS SQL Server, IBM DB2, MongoDB

5.4.4 สามารถตรวจสอบและ Monitor การใช้งานฐานข้อมูลได้แบบ Real-Time

5.4.5 มีหน้าจอหรือ Dashboard ที่สามารถ Monitor ข้อมูลดังต่อไปนี้ได้เป็นอย่างน้อย ได้แก่ Query Recognizer, Audit, Traffic, Free Space, Memory, Traffic Buffers, Queues, Query Cache Rate และ Audit Storage Info

5.4.6 สามารถป้องกันการโจมตีฐานข้อมูลด้วยเทคนิค SQL Injection, DDoS Attack, Brute-force รวมถึง Unauthorize Query ได้เป็นอย่างน้อย

5.4.7 สามารถเก็บ Log การใช้งานของผู้ใช้ที่มีการเข้าถึงข้อมูลในฐานข้อมูล โดยจัดเก็บ Query และผลลัพธ์ที่ได้ เช่น ตลอดจนข้อมูลอื่น ๆ ที่เกี่ยวข้องกับผู้ใช้ เช่น IP Address, Username, Client Application Name เป็นต้น

5.4.8 สามารถสร้าง Policy เพื่อควบคุมการเข้าถึงฐานข้อมูล โดยใช้เงื่อนไข อย่างน้อยดังนี้

- Database Name หรือ DB
- User IP Address หรือ Host
- Client Application หรือ Application
- Query หรือ Regular Expression

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

7.....8.....9.....10.....11.....

5.4.9 สามารถทำ Data Masking เพื่อให้ข้อมูลมีความปลอดภัย โดยต้องรองรับเทคนิคดังต่อไปนี้

- Dynamic Data Masking
- Static Data Masking
- In-place Data Masking

5.4.10 สามารถเข้ารหัสข้อมูลและคงรูปแบบเดิมของข้อมูลไว้ได้ (Format-Preserving Encryption)

5.4.11 สามารถตรวจสอบและค้นหาข้อมูล Sensitive หรือ Confidential Information ในฐานข้อมูลได้

5.4.12 สามารถเขียนสคริปต์ด้วยภาษา Lua เพื่อช่วยในการค้นหาข้อมูล Sensitive โดยมีตัวแปรอย่างน้อยที่สามารถใช้งานได้ คือ AttributeID, ColumnName, FullColumnType, ColumnSize, ColumnValue และ ColumnType

5.4.13 สามารถวิเคราะห์พฤติกรรมการใช้งานของผู้ใช้ (User Behavior) และแจ้งเตือนหากพบพฤติกรรมการใช้งานที่ผิดปกติ

5.4.14 สามารถติดตั้งและทำงานทั้งในรูปแบบของ Sniffer Mode และ Proxy Mode และ Trailing DB Audit Logs ได้

5.4.15 สามารถ Compliance ได้ตามมาตรฐาน HIPAA, GDPR, PCI DSS, SOX และ ISO 27001 เป็นอย่างน้อย

5.4.16 สามารถตรวจสอบข้อมูลช่องโหว่หรือ Patch ล่าสุดเกี่ยวกับฐานข้อมูล เพื่อ Update ให้มีความปลอดภัย

5.4.17 สามารถสร้างรายงาน รวมถึง Export รายงานในรูปแบบ PDF และ CSV ได้ดังต่อไปนี้

- Audited Applications
- Masked Applications
- Blocked Applications
- Audited Application Users
- Blocked Application Users
- Masked Application Users

5.4.18 สามารถสร้าง Schedule Task หรือ Periodic Task เพื่อให้ระบบทำงานอัตโนมัติได้อย่างน้อยดังต่อไปนี้

- Backup Dictionary
- Clean Audit Data
- System Health Check
- User Suspicious Behavior Detection

5.4.19 รองรับการเชื่อมต่อกับระบบ SIEM ได้เป็นอย่างน้อย

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

7.....8.....9.....10.....11.....

6. ระยะเวลาดำเนินงาน

ระยะเวลาในการดำเนินการ 300 วัน นับถัดจากวันลงนามในสัญญา

7. หลักเกณฑ์ในการพิจารณาข้อเสนอ

7.1 ผู้ยื่นข้อเสนอต้องยื่นเอกสารเกี่ยวกับการศึกษาวิเคราะห์ ออกแบบ และขั้นตอนกระบวนการวิธีการในการดำเนินการในแต่ละขอบเขตงานให้ชัดเจน ตามข้อ 4 ขอบเขตการดำเนินงาน

7.2 การพิจารณาผลการยื่นข้อเสนอครั้งนี้ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานจะใช้หลักเกณฑ์การประเมินค่าประสิทธิภาพต่อราคา (Price Performance) โดยพิจารณาจากราคารวมตามปัจจัยหลักและน้ำหนักที่กำหนด ดังนี้

7.2.1 ราคาที่ยื่นข้อเสนอ (Price) กำหนดค่าน้ำหนักเท่ากับร้อยละ 20

7.2.2 คุณภาพและคุณสมบัติ (Performance) ที่เป็นประโยชน์ต่อทางราชการกำหนดน้ำหนักเท่ากับร้อยละ 80 โดยกำหนดหลักเกณฑ์การให้คะแนนข้อเสนอด้านเทคนิคในการพิจารณารูปแบบของงาน เกณฑ์การตัดสินข้อเสนอด้านเทคนิค จะคัดเลือกจากผู้ได้รับคะแนนรวมแล้วไม่ต่ำกว่าร้อยละ 75 (75 คะแนนจาก 100 คะแนน) ดังต่อไปนี้

ลำดับ	เกณฑ์การพิจารณา	เกณฑ์ย่อย	คะแนนเต็ม
1. ผลงานและประสบการณ์ และบุคลากรหลัก คะแนนเต็ม 50 คะแนน			
1.1	ผลงานหรือประสบการณ์ของผู้ยื่นข้อเสนอ *(พิจารณาจากหนังสือรับรองผลงานหรือสำเนาสัญญาโครงการที่แล้วเสร็จแล้วเท่านั้น)*	มีผลงานหรือประสบการณ์ คะแนนเต็ม 20 คะแนน มีเกณฑ์การพิจารณา ดังนี้ 1) ผลงานหรือประสบการณ์เกี่ยวกับจัดทำกรอบมาตรฐานทางไซเบอร์ (NIST Cybersecurity Framework) ได้ 5 คะแนน 2) ผลงานหรือประสบการณ์เกี่ยวกับการติดตั้งระบบรักษาความมั่นคงปลอดภัยไซเบอร์ ได้ 5 คะแนน 3) ผลงานหรือประสบการณ์เกี่ยวกับการดำเนินงานด้านการประเมินการถูกบุกรุก (Compromise Assessment) และการตอบสนองและกำจัดภัยคุกคาม (Incident Response) ได้ 5 คะแนน 4) ผลงานหรือประสบการณ์เกี่ยวกับการจัดหาระบบเฝ้าระวังของศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัย (Security Operation Center: SOC) ได้ 5 คะแนน	20
1.2	ประสบการณ์และจำนวนของบุคลากรหลัก	ประสบการณ์และจำนวนของบุคลากรหลัก คะแนนเต็ม 10 คะแนน มีเกณฑ์การพิจารณา ดังนี้ 1) บุคลากรหลักมีประสบการณ์ ตามข้อ 11 คะแนนเต็ม 5 คะแนน มีเกณฑ์การพิจารณา ดังนี้ 1.1) ตรงตามข้อกำหนด ได้ 3 คะแนน 1.2) สูงกว่าข้อกำหนด ได้ 5 คะแนน	10

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

7.....8.....9.....10.....11.....

ลำดับ	เกณฑ์การพิจารณา	เกณฑ์ย่อย	คะแนนเต็ม
		2) บุคลากรหลักที่มีคุณสมบัติตรงตามข้อกำหนดและจำนวนบุคลากร ตามข้อ 11 คะแนนเต็ม 5 คะแนน มีเกณฑ์การพิจารณา ดังนี้ 2.1) คุณสมบัติและจำนวนบุคลากรตรงตามข้อกำหนด ได้ 3 คะแนน 2.2) คุณสมบัติและจำนวนบุคลากรสูงกว่าข้อกำหนด ได้ 5 คะแนน	
1.3	ใบเอกสารรับรอง (Certificate) ที่เกี่ยวข้องกับด้านความมั่นคงปลอดภัยไซเบอร์ ดังนี้ 1) CompTIA Cybersecurity Analyst (CySA+) 2) Computer Hacking Forensic Investigator (CHFI) 3) EC-Council Certified Incident Handler (ECIH) 4) EC-Council Certified Security Specialist (ECSS) 5) Certified in Cybersecurity (CC) 6) ISO/IEC 27001:2022 Auditor Transition 7) Information Security Management System (ISMS): Implementing ISO/IEC 27001:2022 8) Certified Information Privacy Professional/Europe (CIPP/E) 9) CompTIA Advanced Security Practitioner (CASP+) 10) Certified Information Security Auditor (CISA) 11) Web Application Firewall และ Web Application DDoS Protection Certificate ของเครื่องมือหรือผลิตภัณฑ์ที่นำเสนอในโครงการนี้ 12) Web Application Security Scanner ของเครื่องมือหรือผลิตภัณฑ์ที่นำเสนอในโครงการนี้	มีเอกสารรับรอง (Certificate) ที่เกี่ยวข้องกับด้านความมั่นคงปลอดภัยไซเบอร์ คะแนนเต็ม 20 คะแนน มีเกณฑ์การพิจารณา ดังนี้ 1) มีเอกสารรับรองจำนวน 10 - 11 รายการ ได้ 10 คะแนน 2) มีเอกสารรับรองจำนวน 12 - 13 รายการ ได้ 12 คะแนน 3) มีเอกสารรับรองจำนวน 14 - 15 รายการ ได้ 14 คะแนน 4) มีเอกสารรับรองจำนวน 16 - 17 รายการ ได้ 16 คะแนน 5) มีเอกสารรับรองจำนวน 18 - 19 รายการ ได้ 18 คะแนน 6) มีเอกสารรับรองครบ 20 รายการ ได้ 20 คะแนน	20

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

7.....8.....9.....10.....11.....

ลำดับ	เกณฑ์การพิจารณา	เกณฑ์ย่อย	คะแนนเต็ม
	13) Database Firewall Certificate ของเครื่องมือหรือผลิตภัณฑ์ที่นำเสนอในโครงการนี้ 14) ISO 27001:2022 Lead Auditor 15) ISA/IEC 62443 CFS 16) Certified Information Security Manager (CISM) 17) Certified Information Systems Security Professional (CISSP) 18) ISO 27001:2022 Lead Implementer 19) Project Management Professional (PMP)® Certification 20) DevSecOps Foundation (DSOF) Certification		
2. ด้านความน่าเชื่อถือของเครื่องมือและผลิตภัณฑ์ที่นำเสนอ คะแนนเต็ม 20 คะแนน			
	ความน่าเชื่อถือของเครื่องมือหรือผลิตภัณฑ์	ความน่าเชื่อถือของเครื่องมือหรือผลิตภัณฑ์คะแนนเต็ม 20 คะแนน มีเกณฑ์การพิจารณา ดังนี้ 1) มีเอกสารรับรองจากเจ้าของเครื่องมือหรือผลิตภัณฑ์ในส่วนของระบบ Web Application Firewall ที่นำเสนอต้องเป็นสมาชิกหน่วยงาน FS-ISAC Critical Provider และต้องมีเอกสารรับประกันความพร้อมใช้งานของระบบโดยพิจารณาจากจำนวนจุดให้บริการ (Point of Presence –POP) ที่รองรับการให้บริการ WAF และ CDN ในประเทศไทย คะแนนเต็ม 5 คะแนน มีเกณฑ์การพิจารณา ดังนี้ 1.1) เป็นสมาชิก FS-ISAC Critical Provider และมีจุดให้บริการในประเทศไทยอย่างน้อย 6 แห่ง ได้ 1 คะแนน 1.2) เป็นสมาชิก FS-ISAC Critical Provider และมีจุดให้บริการในประเทศไทยอย่างน้อย 8 แห่ง ได้ 3 คะแนน 1.3) เป็นสมาชิก FS-ISAC Critical Provider และมีจุดให้บริการในประเทศไทยอย่างน้อย 10 แห่ง ได้ 5 คะแนน	20

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

7.....8.....9.....10.....11.....

ลำดับ	เกณฑ์การพิจารณา	เกณฑ์ย่อย	คะแนนเต็ม
		2) มีเอกสารรับรองจากเจ้าของเครื่องมือหรือผลิตภัณฑ์ในส่วนของระบบ Web Application DDoS Protection ที่นำเสนอต้องได้รับการรับรอง Cyber Essentials Certificate of Assurance และ EU Cloud Code of Conduct ได้ 5 คะแนน 3) มีเอกสารรับรองจากเจ้าของเครื่องมือหรือผลิตภัณฑ์ในส่วนของระบบ Web Application Security Scanner ที่นำเสนอต้องได้รับการรับรอง ISO27001 ISO27017 SOC 2 – TYPE II และเป็นสมาชิกองค์กร OpenSSF (Open Source Security Foundation) ได้ 5 คะแนน 4) มีเอกสารรับรองจากเจ้าของเครื่องมือหรือผลิตภัณฑ์ในส่วนของระบบ Database Firewall นำเสนอต้องได้รับการให้คะแนนหรือได้รับการจัดลำดับให้อยู่ในกลุ่ม Product Leader ของ KuppingerCole Leadership Compass สำหรับ Data Security Platform ปี 2025 หรือปีล่าสุด ได้ 5 คะแนน	
3. วิธีการบริหารและวิธีปฏิบัติงาน คะแนนเต็ม 30 คะแนน			
3.1	วิธีการบริหารและวิธีปฏิบัติงานที่ชัดเจนและสอดคล้องกับขอบเขตการดำเนินงานตามข้อ 4	วิธีการบริหารและวิธีปฏิบัติงานที่ชัดเจน คะแนนเต็ม 30 คะแนน มีเกณฑ์การพิจารณา ดังนี้ 1) วิธีการบริหาร คะแนนเต็ม 10 คะแนน มีเกณฑ์การพิจารณา ดังนี้ 1.1) มีโครงสร้างทีมงาน ได้คะแนน 2 คะแนน 1.2) มีการจัดบุคลากรการทำงานตามขอบเขตงานในแต่ละตำแหน่ง ได้คะแนน 2 คะแนน 1.3) ผู้จัดการโครงการที่มีใบรับรองด้านความมั่นคงปลอดภัยไซเบอร์คะแนนเต็ม 6 คะแนน มีเกณฑ์การพิจารณา ดังนี้ - มี Certified Information Systems Security Professional (CISSP) ได้ 1 คะแนน - มี Computer Hacking Forensic Investigator (CHFI) ได้ 1 คะแนน - มี ISO/IEC 27701:2019 Implementation ได้ 1 คะแนน - มี ISO/IEC 27001:2022 Auditor Transition ได้ 1 คะแนน	30

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

7.....8.....9.....10.....11.....

ลำดับ	เกณฑ์การพิจารณา	เกณฑ์ย่อย	คะแนนเต็ม
		- มี Information Security Management System (ISMS): Implementing ISO/IEC 27001:2022 ได้ 1 คะแนน - มี ISO/IEC 27701:2019 Internal Auditor ได้ 1 คะแนน 2) วิธีปฏิบัติงานที่สอดคล้องกับขอบเขตการดำเนินงาน ตามข้อ 4 คะแนนเต็ม 15 คะแนน มีเกณฑ์การพิจารณา ดังนี้ 2.1) มีแนวคิดและทฤษฎีที่เกี่ยวข้อง เพื่อแสดงความเข้าใจที่มีต่อสถานภาพปัจจุบันของระบบความมั่นคงปลอดภัยทางไซเบอร์ที่สอดคล้องกับภารกิจของสำนักงานเขตพื้นที่การศึกษา 245 เขต ได้ 5 คะแนน 2.2) มีการศึกษาและวิเคราะห์แนวโน้มภัยคุกคามทางไซเบอร์ (Cyber Trends) ที่อาจจะเกิดขึ้นในอนาคต ที่เกี่ยวข้องกับสำนักงานเขตพื้นที่การศึกษา 245 เขต ได้ 5 คะแนน 2.3) มีกรอบการดำเนินการตามวัตถุประสงค์ของโครงการ และขั้นตอนการปฏิบัติงาน ได้ 5 คะแนน 3) ผู้ยื่นข้อเสนอต้องได้รับมาตรฐาน ISO/IEC 27001:2022 ขอบเขต Attack Surface Management และ Threat Intelligence โดยพิจารณาจากเอกสารรับรองมาตรฐาน ISO/IEC 27001:2022 ได้ 5 คะแนน	
คะแนนรวมทั้งหมด			100

<u>หมายเหตุ</u> กรณีที่ไม่ได้ส่งเอกสารหรือไม่มีข้อมูลรายละเอียดตามเกณฑ์การพิจารณาในแต่ละข้อ จะไม่ได้รับคะแนนในข้อนั้น ๆ

7.3 หากผู้ยื่นข้อเสนอรายใด มีคุณสมบัติผู้ยื่นข้อเสนอและเงื่อนไขการเสนอราคาไม่ถูกต้อง หรือไม่ครบถ้วนคณะกรรมการพิจารณาผลการประกวดราคาจะไม่รับพิจารณาราคาของผู้ยื่นข้อเสนอรายนั้น

7.4 การตัดสินของคณะกรรมการพิจารณาผลการประกวดราคา สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน มีสิทธิ์ให้ผู้ยื่นข้อเสนอชี้แจงข้อเท็จจริง สภาพ ฐานะ หรือ ข้อเท็จจริงอื่นใดที่เกี่ยวข้องกับผู้ยื่นข้อเสนอได้ มีสิทธิ์ที่จะไม่รับ ข้อเสนอไม่รับราคา หรือไม่ทำสัญญา หากหลักฐานดังกล่าวไม่มีความเหมาะสมหรือไม่ถูกต้อง

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

7.....8.....9.....10.....11.....

7.5 สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ทรงไว้ซึ่งสิทธิ์ที่จะไม่รับราคาต่ำสุด หรือราคาหนึ่งราคาใด หรือราคาที่เสนอทั้งหมดก็ได้ หรืออาจจะยกเลิกการประกวดราคาครั้งนี้ ทั้งนี้ เพื่อประโยชน์ของทางราชการเป็นสำคัญและให้ถือว่าการตัดสินของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน เป็นเด็ดขาดผู้ยื่นข้อเสนอจะเรียกร้องค่าเสียหายใด ๆ มิได้ รวมทั้ง สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน จะพิจารณายกเลิกการจ้าง หากมีเหตุที่เชื่อถือได้ว่า การยื่นข้อเสนอกระทำการโดยไม่สุจริต เช่น การเสนอเอกสารอันเป็นเท็จ หรือใช้ชื่อบุคคลธรรมดา หรือนิติบุคคลอื่น มาเสนอราคาแทน เป็นต้น

7.6 กรณีที่ปรากฏข้อเท็จจริงภายหลังจากการพิจารณาข้อเสนอว่าผู้ยื่นข้อเสนอที่มีสิทธิ์ได้รับการคัดเลือกเป็นผู้ยื่นข้อเสนอที่มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่น ณ วันยื่นข้อเสนอ หรือเป็นผู้ยื่นข้อเสนอ ที่กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน มีอำนาจที่จะตัดรายชื่อผู้ยื่นข้อเสนอรายดังกล่าวออก

8. งบประมาณโครงการ

วงเงินงบประมาณ จำนวนทั้งสิ้น 40,000,000.00 (สี่สิบล้านบาทถ้วน)

<u>หมายเหตุ</u> ราคากลางเป็นราคาที่ได้จากการอ้างอิงจากหลักเกณฑ์ อัตราค่าใช้จ่าย และแนวทางการพิจารณางบประมาณรายจ่ายประจำปีของสำนักงบประมาณ ธันวาคม 2567 และสืบราคาจากท้องตลาด

9. การส่งมอบงาน ค่าจ้าง และการจ่ายเงิน

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

9.1.1 หลักฐานการจัดประชุมเปิดโครงการ (Kick-off Project)

9.1.2 แผนการดำเนินโครงการ (Project Planning) ซึ่งอธิบายถึง กิจกรรมการดำเนินงาน ระยะเวลาการดำเนินงาน และกรรมวิธีการดำเนินงานโครงการ รวมถึงสิ่งส่งมอบงานในโครงการ ตามข้อ 4.1

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

9.2.1 รายงานความพร้อมใช้งานของบริการตรวจสอบช่องโหว่และมาตรฐานความปลอดภัยของเว็บแอปพลิเคชันของสำนักงานเขตพื้นที่การศึกษา (Web Application Security Scanner) ตามข้อ 4.2

9.2.2 รายงานความพร้อมใช้งานของบริการป้องกันการโจมตีในระดับเว็บแอปพลิเคชัน (Web Application Firewall) สำหรับเว็บแอปพลิเคชันของสำนักงานเขตพื้นที่การศึกษา ตามข้อ 4.3

9.2.3 รายงานความพร้อมใช้งานของบริการป้องกันการโจมตีประเภทที่ทำให้ระบบเว็บแอปพลิเคชัน (Web Application DDoS Protection) ไม่สามารถใช้งานได้ สำหรับเว็บแอปพลิเคชันของสำนักงานเขตพื้นที่การศึกษา ตามข้อ 4.4

9.2.4 รายงานผล ISMS/PIMS Gap Analysis Report ตามข้อ 4.7

9.2.5 รายงานความพร้อมใช้งานของบริการรักษาความปลอดภัยสำหรับระบบฐานข้อมูล (Database Firewall) ของแอปพลิเคชันในศูนย์ข้อมูล (Data Center) สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ตามข้อ 4.8

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

7.....8.....9.....10.....11.....

9.3 งวดงานที่ 3 เบิกจ่ายร้อยละ 20 ของวงเงินตามสัญญาจ้าง หลังจากคณะกรรมการตรวจรับพัสดุได้ตรวจรับงานดังกล่าวเรียบร้อยแล้ว โดยผู้รับจ้างต้องส่งมอบงานภายในระยะเวลา 180 วัน นับถัดจากวันลงนามในสัญญา อย่างน้อยดังต่อไปนี้

9.3.1 เอกสารการตรวจสอบช่องโหว่และมาตรฐานความปลอดภัยของเว็บแอปพลิเคชันของสำนักงานเขตพื้นที่การศึกษา (Web Application Security Scan) และประเมินแนวทางการตั้งค่าระบบอย่างปลอดภัย (System Hardening) ตามข้อ 4.5

9.3.2 บัญชีรายชื่อเอกสาร (Document Master List) เอกสารตามบัญชีรายชื่อ และเอกสารเพิ่มเติมที่เกี่ยวข้อง ตามข้อ 4.7

9.4 งวดงานที่ 4 เบิกจ่ายร้อยละ 30 ของวงเงินตามสัญญาจ้าง หลังจากคณะกรรมการตรวจรับพัสดุได้ตรวจรับงานดังกล่าวเรียบร้อยแล้ว โดยผู้รับจ้างต้องส่งมอบงานภายในระยะเวลา 240 วัน นับถัดจากวันลงนามในสัญญา อย่างน้อยดังต่อไปนี้

9.4.1 รายงานผลการดำเนินการตอบสนองต่อภัยคุกคามทางไซเบอร์ (Incident Response) ที่ตรวจพบของศูนย์ข้อมูล (Data Center) สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ตามข้อ 4.6

9.4.2 เอกสารผลการดำเนินการจัดทำเอกสาร กระบวนการ และเตรียมความพร้อมในการขอรับรอง มาตรฐาน ISO/IEC 27001:2022 (Information Security Management System: ISMS) ของศูนย์ข้อมูล (Data Center) สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน และมาตรฐาน ISO/IEC 27701:2019 (Privacy Information Management System: PIMS) ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน รวมถึงเอกสารที่เกี่ยวข้อง ตามข้อ 4.7

9.4.3 งวดงานที่ 5 เบิกจ่ายร้อยละ 20 ของวงเงินตามสัญญาจ้าง ภายในระยะเวลา 300 วัน นับถัดจากวันลงนามในสัญญา หลังจากคณะกรรมการตรวจรับพัสดุ ได้ตรวจรับงานดังกล่าวเรียบร้อยแล้ว โดยผู้รับจ้างต้องส่งมอบเอกสารผ่านการรับรองมาตรฐาน มาตรฐาน ISO/IEC 27001:2022 (Information Security Management System: ISMS) ของศูนย์ข้อมูล (Data Center) สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน และมาตรฐาน ISO/IEC 27701:2019 (Privacy Information Management System: PIMS) ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน จากผู้ตรวจรับรองมาตรฐาน (Certified Body) ตามข้อ 4.7

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

10. อัตราค่าปรับ

ผู้รับจ้างต้องสามารถให้บริการได้ ภายในระยะเวลาของโครงการที่กำหนดไว้ หากเกิดความล่าช้าไปจากแผนงานด้วยสาเหตุจากผู้รับจ้าง ผู้ว่าจ้างมีสิทธิคิดค่าปรับจากผู้รับจ้างในอัตราร้อยละ 0.1 ต่อวันของวงเงินค่าจ้างทั้งหมดตามสัญญา ยกเว้นกรณีที่ล่าช้าเกิดจากผู้ว่าจ้าง ผู้ว่าจ้างและผู้รับจ้างจะทำการเจรจาเพื่อกำหนดระยะเวลาของแผนงานที่เหมาะสมโดยไม่ถือว่าระยะเวลาที่ยืดออกไปเป็นสาเหตุความล่าช้าจากผู้รับจ้าง

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

7.....8.....9.....10.....11.....

11. ข้อกำหนดทั่วไป

11.1 ผู้รับจ้างต้องจัดหาบุคลากรสำหรับโครงการจ้างเหมาบริการเพิ่มประสิทธิภาพการป้องกันและการรักษาความปลอดภัยของข้อมูลพร้อมปรับปรุงความปลอดภัยตามมาตรฐาน ISO/IEC 27001:2022 และ ISO/IEC 27701:2019 ที่มีคุณสมบัติ ความรู้ ประสบการณ์ และคุณสมบัติเฉพาะของตำแหน่งสอดคล้องกับตาราง ดังนี้

ลำดับที่	ตำแหน่ง	วุฒิการศึกษา	ประสบการณ์ไม่น้อยกว่า (ปี)	จำนวน (คน)
1	ผู้จัดการโครงการ (Project Manager)	ปริญญาโท ด้านคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ หรือสื่อสารโทรคมนาคม หรือวิศวกรรมไฟฟ้า หรือด้านอื่น ๆ ที่เกี่ยวข้อง	10	1
2	ผู้ชำนาญด้านช่องโหว่หรือจุดอ่อน (System Hardening Expert)	ปริญญาตรี ด้านคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ หรือสื่อสารโทรคมนาคม หรือวิศวกรรมไฟฟ้า หรือด้านอื่น ๆ ที่เกี่ยวข้อง	5	1
3	ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ (Information Technology Specialist)	ปริญญาเอก ด้านคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ หรือสื่อสารโทรคมนาคม หรือวิศวกรรมไฟฟ้า หรือด้านอื่น ๆ ที่เกี่ยวข้อง	10	1
4	ผู้ชำนาญด้านเทคโนโลยีสารสนเทศ (Information Technology Expert)	ปริญญาโท ด้านคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ หรือสื่อสารโทรคมนาคม หรือวิศวกรรมไฟฟ้า หรือด้านอื่น ๆ ที่เกี่ยวข้อง	10	1
5	ผู้เชี่ยวชาญด้านการบริหารจัดการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ	ปริญญาโท ด้านคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ หรือสื่อสารโทรคมนาคม หรือวิศวกรรมไฟฟ้า หรือด้านอื่น ๆ ที่เกี่ยวข้อง	5	1
6	ที่ปรึกษาด้านการบริหารจัดการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (ISO 27001)	ปริญญาตรี ด้านคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ หรือสื่อสารโทรคมนาคม หรือวิศวกรรมไฟฟ้า หรือด้านอื่น ๆ ที่เกี่ยวข้อง	10	1
7	ที่ปรึกษาด้านการคุ้มครองข้อมูลส่วนบุคคล (ISO 27701)	ปริญญาตรี ด้านคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ หรือสื่อสารโทรคมนาคม หรือวิศวกรรมไฟฟ้า หรือด้านอื่น ๆ ที่เกี่ยวข้อง	10	1

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

7.....8.....9.....10.....11.....

ลำดับที่	ตำแหน่ง	วุฒิการศึกษา	ประสบการณ์ไม่น้อยกว่า (ปี)	จำนวน (คน)
8	หัวหน้าทีมด้านการตอบสนองต่อภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Responder Lead)	ปริญญาโท ด้านคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ หรือสื่อสารโทรคมนาคม หรือวิศวกรรมไฟฟ้า หรือด้านอื่น ๆ ที่เกี่ยวข้อง	5	1
9	วิศวกรด้านการตอบสนองต่อภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Responder Engineer)	ปริญญาตรี ด้านคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ หรือสื่อสารโทรคมนาคม หรือวิศวกรรมไฟฟ้า หรือด้านอื่น ๆ ที่เกี่ยวข้อง	5	1
10	เลขานุการโครงการ	ปริญญาตรี	1	1

หลักฐานการแสดงความรู้และความสามารถของบุคลากรปฏิบัติงานในโครงการนี้ ตามแบบฟอร์ม (ภาคผนวก 1)

11.2 ผู้รับจ้างต้องเป็นผู้รับผิดชอบค่าใช้จ่ายที่เกิดขึ้นทั้งหมด ในการดำเนินการจัดประชุมสำหรับคณะกรรมการพิจารณาตรวจสอบเอกสารมาตรฐานที่เกี่ยวข้องในโครงการนี้ จำนวนไม่น้อยกว่า 2 ครั้ง แต่ละครั้งไม่น้อยกว่า 3 วัน โดยมีผู้เข้าร่วมประชุมไม่น้อยกว่า 25 คนต่อครั้ง สถานที่จัดประชุมตามที่สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานกำหนด

12. หน่วยงานที่รับผิดชอบ

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

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

ภาคผนวก 1 แบบฟอร์มประวัติบุคลากรที่เสนอ
จ้างเหมาบริการเพิ่มประสิทธิภาพการป้องกันและการรักษาความปลอดภัยของข้อมูล
พร้อมปรับปรุงความปลอดภัยตามมาตรฐาน ISO/IEC 27001:2022 และ ISO/IEC 27701:2019

ประวัติส่วนตัว

ชื่อ – นามสกุล.....

ตำแหน่งที่เสนอในโครงการ.....

ที่อยู่ปัจจุบัน.....

.....

ประวัติการศึกษา

1. ปริญญาตรี : มหาวิทยาลัย..... คณะ .....
   สาขา..... ปีที่สำเร็จ .....
2. ปริญญาโท : มหาวิทยาลัย..... คณะ .....
   สาขา..... ปีที่สำเร็จ .....
3. ปริญญาเอก : มหาวิทยาลัย..... คณะ .....
   สาขา..... ปีที่สำเร็จ .....

ประวัติการทำงาน (ปัจจุบัน ถึง อดีต)

1. ระบุปี ถึง ปัจจุบัน ตำแหน่ง..... หน่วยงาน.....
   รายละเอียด.....
2. ระบุปี ถึง ปัจจุบัน ตำแหน่ง..... หน่วยงาน.....
   รายละเอียด.....
3. ระบุปี ถึง ปัจจุบัน ตำแหน่ง..... หน่วยงาน.....
   รายละเอียด.....

การฝึกอบรม (ปัจจุบัน ถึง อดีต)

1. ปี.....หลักสูตร.....
2. ปี.....หลักสูตร.....
3. ปี.....หลักสูตร.....

เอกสารประกอบ

1. สำเนาใบรายงานผลการศึกษา (Transcript) พร้อมลงนามรับรองสำเนาถูกต้อง (ถ้ามี)
2. สำเนาใบรับรองการฝึกอบรม (Certification) พร้อมลงนามรับรองสำเนาถูกต้อง (ถ้ามี)