**ร่าง ขอบเขตของงาน (Terms of Reference: TOR)**
**ปรับปรุงประสิทธิภาพการเฝ้าระวังภัยคุกคามและความปลอดภัยของข้อมูล ระยะที่ 1**
**สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน กระทรวงศึกษาธิการ**

## 1. หลักการและเหตุผล

ปัจจุบันภัยคุกคามทางไซเบอร์มีความรุนแรงและซับซ้อนเพิ่มมากขึ้น ส่งผลต่อการรักษาความปลอดภัยทางสารสนเทศที่จำเป็นต้องปรับเปลี่ยนและพัฒนาอย่างสม่ำเสมอ เพื่อให้ตอบสนองต่อภัยคุกคามที่เพิ่มมากขึ้น รวมถึงหน่วยงานภาครัฐต้องปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และการเก็บข้อมูลจราจรทางคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งจำเป็นต้องดำเนินการพัฒนาขีดความสามารถในด้านความปลอดภัยไซเบอร์ให้สามารถตรวจพบ (Detect) ป้องกัน (Protect) และตอบสนอง (Response) ภัยคุกคามที่ส่งผลกระทบต่อความปลอดภัยของระบบเทคโนโลยีสารสนเทศ เป็นการเพิ่มประสิทธิภาพการป้องกันภัยคุกคามลดความเสี่ยงของข้อมูลที่รั่วไหลจากภัยคุกคามทางไซเบอร์ เพื่อให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ดังนั้น สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน จำเป็นต้องเสริมสร้างความพร้อมในการรับมือภัยคุกคาม โดยการปรับปรุงประสิทธิภาพระบบเฝ้าระวังภัยคุกคามและความปลอดภัยของข้อมูลให้มีความพร้อมในการตอบสนองภัยคุกคามใหม่ได้อย่างมีประสิทธิภาพสูงสุด รวมถึงระบบที่สามารถป้องกันการสูญหายของข้อมูลได้

## 2. วัตถุประสงค์

2.1 เพื่อเพิ่มสมรรถนะด้านความปลอดภัยทางไซเบอร์ ลดความเสี่ยงและผลกระทบจากภัยคุกคามทางด้านไซเบอร์ที่จะส่งผลต่อการดำเนินงานของหน่วยงาน

2.2 เพื่อเพิ่มสมรรถนะด้านความปลอดภัยทางไซเบอร์ ในการรับมือและตอบสนองภัยคุกคามทางด้านไซเบอร์ที่เกิดขึ้นในปัจจุบันได้อย่างรวดเร็ว

2.3 เพื่อรักษาความลับของข้อมูลและป้องกันความเสี่ยงที่เกิดจากการรั่วไหลของข้อมูลหรือการละเมิดข้อมูลส่วนบุคคล

## 3. คุณสมบัติผู้เสนอราคา

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

1.....2.....3.....4.....
5.....6.....7.....8.....
9.....10.....11.....12.....
13.....

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นนิติบุคคลผู้มีอาชีพขายพัสดุที่ประกวดราคาซื้อด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทยเว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

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

3.11 ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ต้องมีคุณสมบัติดังนี้

3.11.1 กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงระหว่างผู้เข้าร่วมค้าจะต้องมีการกำหนดสัดส่วนหน้าที่และความรับผิดชอบในปริมาณงาน สิ่งของหรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

3.11.2 กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

3.11.3 สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

3.11.4 กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอ ในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

3.11.5 สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

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

5..... 6..... 7..... 8.....

9..... 10..... 11..... 12.....

13.....

3.12 ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

3.12.1 กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า 1 ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก 1 ปีสุดท้ายก่อนวันยื่นข้อเสนอ

3.12.2 กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ดังนี้ ต้องมีทุนจดทะเบียนไม่ต่ำกว่า 8 ล้านบาท

3.12.3 กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียนหรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง (สินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์ และประกอบธุรกิจค้าประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรองหรือที่สำนักงานสาขารับรอง (กรณีที่ได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอนับถึงวันยื่นข้อเสนอไม่เกิน 90 วัน

3.12.4 กรณีตาม (3.12.1) - (3.12.4) ยกเว้นสำหรับกรณีดังต่อไปนี้

3.12.4.1 กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ

3.12.4.2 นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย (ฉบับที่ 10) พ.ศ. 2561

3.13 ผู้ยื่นข้อเสนอต้องเป็นนิติบุคคลที่มีผลงานประเภทเดียวกันในการจัดหาครั้งนี้หรือเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ หรือจัดหาระบบเฝ้าระวังและรักษาความมั่งคงปลอดภัยไซเบอร์ โดยเป็นผลงานที่เสร็จสมบูรณ์แล้วอย่างน้อย 1 สัญญา และมีวงเงินต่อสัญญาไม่น้อยกว่า 20 ล้านบาท รวมภาษีมูลค่าเพิ่มแล้ว และเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับส่วนราชการ หน่วยงานตามกฎหมายว่าด้วยระเบียบบริหารราชการส่วนท้องถิ่น รัฐวิสาหกิจ หน่วยงานอื่นของรัฐ หรือหน่วยงานเอกชนที่น่าเชื่อถือและตรวจสอบได้ โดยผู้เสนอราคาต้องแนบสำเนาหลักฐานสัญญาโครงการ หรือหนังสือรับรองผลงาน โดยให้ยื่นขณะเข้าเสนอราคา

3.14 ผู้ยื่นข้อเสนอต้องได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่ายจากผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทย โดยให้ยื่นขณะเข้าเสนอราคา ตามข้อ 4.1 และ 4.2

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

5..... 6..... 7..... 8.....

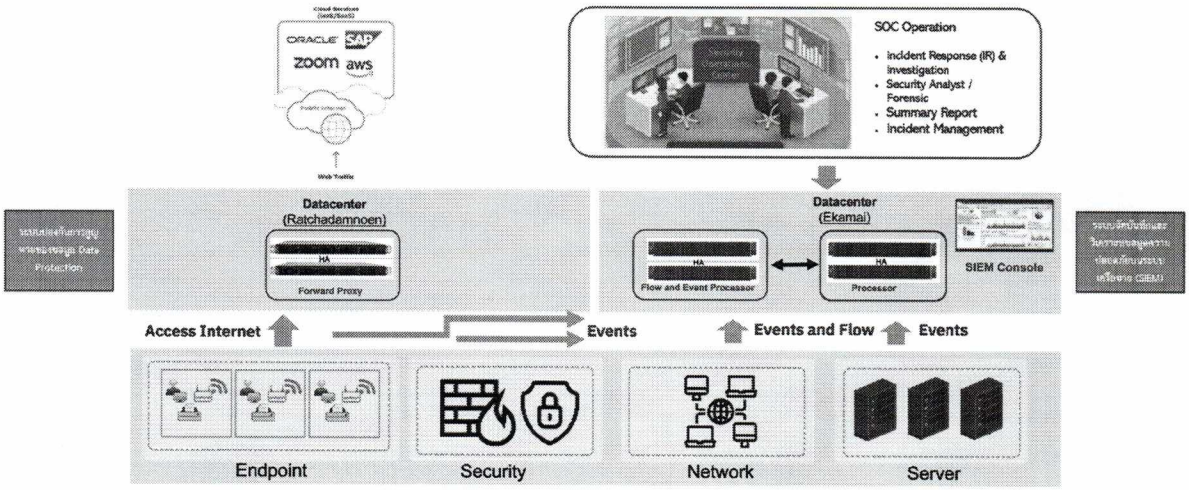
9..... 10..... 11..... 12.....

13.....

## 4. รายการครุภัณฑ์

| ลำดับ | รายการและคุณลักษณะ | จำนวน/หน่วยนับ | ราคาต่อหน่วย | ราคารวม |
|---|---|---|---|---|
| 4.1 | ระบบป้องกันการสูญหายของข้อมูล Data Protection | 1 ระบบ | 17,655,000 | 17,655,000 |
| 4.2 | ระบบจัดเก็บบันทึกและวิเคราะห์ข้อมูลความปลอดภัยบนระบบเครือข่าย (SIEM) | 1 ระบบ | 25,293,000 | 25,293,000 |
| **รวมทั้งสิ้น** | | | | **42,948,000** |

## 5. รายละเอียดคุณลักษณะ



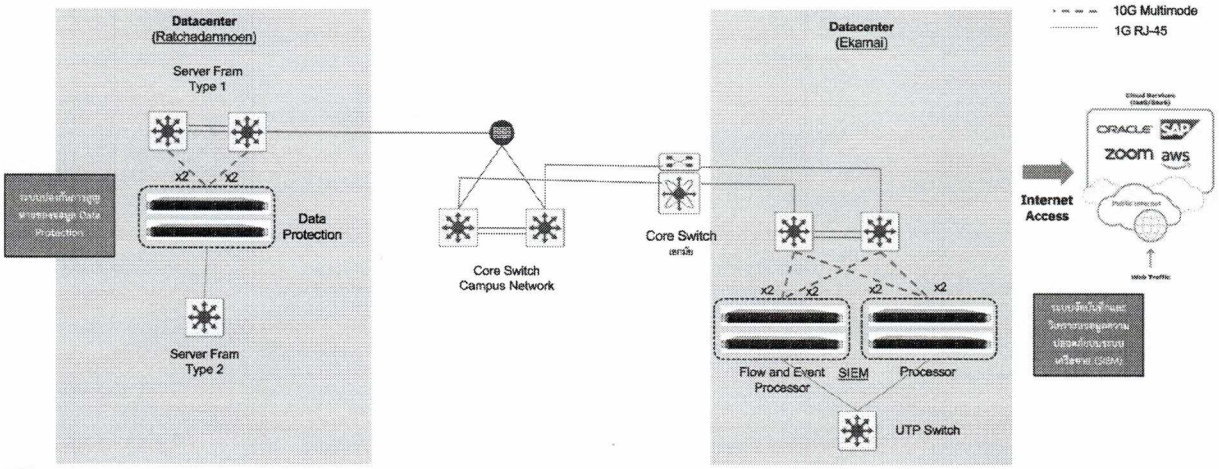

ภาพกรอบความคิด อุปกรณ์ของโครงการ

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

5.....6.....7.....8.....

9.....10.....11.....12.....

13.....




**การเชื่อมโยงอุปกรณ์ของโครงการกับระบบหรืออุปกรณ์ที่เกี่ยวข้อง**

5.1 ระบบป้องกันการสูญหายของข้อมูล Data Protection จำนวน 1 ระบบ มีคุณสมบัติ อย่างน้อยดังนี้

5.1.1 เป็นอุปกรณ์แบบ Hardware Appliance จำนวนไม่น้อยกว่า 2 ชุด และรองรับการทำงานแบบ Redundancy แบบ Active/Standby หรือ Active/Active โดยอุปกรณ์แต่ละชุด มีคุณสมบัติอย่างน้อยดังนี้

5.1.1.1 เป็น Hardware Appliance ที่ถูกออกแบบมาสำหรับการใช้งานเป็น Secure Web Gateway โดยเฉพาะ และมีหน่วยประมวลผลกลาง (CPU) รวมไม่น้อยกว่า 12 แกนหลัก (12 Core)

5.1.1.2 มีหน่วยความจำหลัก (Memory) ชนิด DDR5 ขนาดไม่น้อยกว่า 64 GB

5.1.1.3 มีหน่วยจัดเก็บข้อมูล (Hard Disk) ชนิด SSD หรือดีกว่า ขนาดความจุไม่น้อยกว่า 960 GB จำนวนไม่น้อยกว่า 2 หน่วย

5.1.1.4 มีช่องเชื่อมต่อระบบเครือข่าย แบบ 1 GbE (RJ-45) หรือดีกว่า จำนวนไม่น้อยกว่า 4 ช่อง

5.1.1.5 มีช่องเชื่อมต่อระบบเครือข่าย แบบ 10 GbE (Fiber Optic Short Range) หรือดีกว่า พร้อม Module Transceiver จำนวนไม่น้อยกว่า 4 Module

5.1.1.6 มี Throughput ไม่น้อยกว่า 5,000 Mbps

5.1.1.7 มีหน่วยจ่ายกระแสไฟฟ้าภายในเครื่อง (Power Supply Unit) จำนวนไม่น้อยกว่า 2 หน่วย ที่มีคุณสมบัติทำงานทดแทนกันได้โดยอัตโนมัติ (Redundant) และสามารถถอดเปลี่ยนได้ทันที (Hot-Swap)

5.1.2 มีลิขสิทธิ์การใช้งาน (Software License) จำนวนไม่น้อยกว่า 5,000 License

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

5..... 6..... 7..... 8.....

9..... 10..... 11..... 12.....

13.....

5.1.3 สามารถทำ URL Filtering หรือ Web Filtering ตามประเภทของเว็บไซต์ (Categories) โดยใช้ Categories ที่สามารถปรับปรุงให้ทันสมัยอยู่เสมอโดยผู้ผลิตได้ และมีจำนวน Category ไม่น้อยกว่า 80 Categories

5.1.4 สามารถป้องกันการเข้าสู่เว็บไซต์ที่มีอันตราย (Web Threat) โดยการตรวจสอบค่าความน่าเชื่อถือของเว็บ (Web Reputation) ได้

5.1.5 สามารถป้องกัน Malware โดยใช้การตรวจสอบแบบ Signature Based ได้เป็นอย่างน้อย

5.1.6 สามารถตรวจจับ Zero-day Malware โดยใช้เทคนิค Behavior Emulation หรือ Sandboxing Technology ได้

5.1.7 สามารถทำ Data Protection หรือ Data Loss Prevention (DLP) แบบ Web DLP และรองรับการสร้าง Classification เพื่อตรวจจับและป้องกันข้อมูลรั่วไหล

5.1.8 สามารถทำ SSL Inspection หรือ SSL Decryption เพื่อตรวจสอบการใช้งานเว็บที่ผ่านการเข้ารหัสแบบ SSL ได้

5.1.9 สามารถติดตั้งและทำงานแบบ Explicit Proxy และ Transparent Proxy ได้เป็นอย่างน้อย

5.1.10 สามารถทำการเข้ารหัสข้อมูลของผู้ใช้งานในกรณีที่มีการ Upload ไฟล์ไปเก็บไว้ที่ Cloud Storage และสามารถถอดรหัสข้อมูลในกรณีที่มีการ Download ไฟล์จาก Cloud Storage ได้

5.1.11 รองรับการทำงานร่วมกับโปรโตคอล Web Cache Communication Protocol (WCCP), Internet Content Adaptation Protocol (ICAP/ICAPS) และ WebSocket Protocol (SOCKS) ได้เป็นอย่างน้อย

5.1.12 รองรับการพิสูจน์ตัวตน (Authentication) กับ NTLM, LDAP, Kerberos ได้เป็นอย่างน้อย

5.1.13 สามารถใช้ Active Directory/LDAP User Group ในการทำ Authentication

5.2 ระบบจัดเก็บบันทึกและวิเคราะห์ข้อมูลความปลอดภัยบนระบบเครือข่าย (SIEM) จำนวน 1 ระบบ มีคุณสมบัติ อย่างน้อยดังนี้

5.2.1 สามารถรับข้อมูลจราจรทางคอมพิวเตอร์ (Log) หรือเหตุการณ์ด้านความปลอดภัย (Event) สำหรับทำงานด้าน SIEM จำนวนไม่น้อยกว่า 7,500 EPS (Event per Second)

5.2.2 มีฟีเจอร์หรือฟังก์ชัน Threat Intelligence ภายใต้เครื่องหมายการค้าเดียวกันกับระบบ SIEM

5.2.3 สามารถจัดเก็บและประมวลผล Log หรือ Event จาก Firewall, Network Devices, Operating System, Database ได้เป็นอย่างน้อย

5.2.4 รองรับการติดตั้ง (Installation) แบบ Appliance หรือ Virtual Appliance ได้เป็นอย่างน้อย

5.2.5 สามารถทำงานได้ในลักษณะ All-In-One หรือ Distributed ได้

5.2.6 รองรับการทำงานผ่านระบบเครือข่ายด้วย IPv4 และ IPv6 ได้

5.2.7 รองรับการเก็บข้อมูล Network Flow ในรูปแบบ Net Flow, J-Flow, S-Flow ได้เป็นอย่างน้อย

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

5.....6.....7.....8.....

9.....10.....11.....12.....

13.....

5.2.8 สามารถรับข้อมูล Log จากอุปกรณ์ต่าง ๆ (Log Source) ในรูปแบบอย่างน้อยดังนี้

5.2.8.1 Syslog ทั้ง TCP และ UDP

5.2.8.2 Database หรือ ODBC หรือ SQL

5.2.8.3 FTP หรือ File Transfer

5.2.8.4 OPSEC หรือ LEA Protocol

5.2.8.5 SDEE Protocol

5.2.9 มีรูปแบบความสัมพันธ์ (Correlation Rules) สำหรับใช้วิเคราะห์ข้อมูลภัยคุกคามแบบ Near Real-Time หรือดีกว่า

5.2.10 ระบบฐานข้อมูลเกี่ยวกับภัยคุกคาม (Threat Intelligence) ที่มาพร้อมระบบ SIEM ต้องสามารถตรวจสอบความเสี่ยงจาก IP, File, Application และ MD5 ได้เป็นอย่างน้อย

5.2.11 สามารถวิเคราะห์พฤติกรรมผู้ใช้งาน User Behavior Analytics (UBA) ได้ไม่น้อยกว่า 40,000 ผู้ใช้งาน และสามารถเพิ่มหน่วยความจำหรือหน่วยประมวลผลหรืออุปกรณ์อื่น ๆ เพื่อรองรับผู้ใช้งานได้สูงสุด 220,000 ผู้ใช้งาน

5.2.12 มี Machine Learning Model มาให้พร้อมใช้งานได้ไม่น้อยกว่า 15 Models โดยสามารถ Custom Model โดยใช้รูปแบบภาษา Ariel Query Language (AQL) หรือ Regular Expressions (Regex) ได้ และสามารถวิเคราะห์แบบทุกชั่วโมง (Hour to Hour Analytics) ได้

5.2.13 มี Rule สำหรับใช้ในการวิเคราะห์พฤติกรรมผู้ใช้งาน เช่น Access and Authentication, Accounts and Privileges, Browsing Behavior, DNS Analyzer, Geography และ Threat Intelligence

5.2.14 มี Predefined Rules มาพร้อมระบบที่เสนอเพื่อวิเคราะห์พฤติกรรมการใช้งานของผู้ใช้ด้วยข้อมูลจาก Threat Intelligence Platform เช่น Detect IOCs For Locky, Detect IOCs for WannaCry, Shell Bags Modified By Ransomware, User Accessing Risky IP Anonymization และ Multiple Sessions to Monitored Log Sources (NIS Directive)

5.2.15 สามารถจัดรูปแบบของ Events หรือ Logs ที่ได้รับจากอุปกรณ์ต้นทาง ให้อยู่ในรูปแบบเดียวกันเพื่อที่ระบบจะสามารถทำการวิเคราะห์ได้ (Parsed/Normalized)

5.2.16 สามารถยืนยันความถูกต้องของข้อมูล Log หรือ Event ที่เก็บรักษาว่าไม่มีการถูกเปลี่ยนแปลงแก้ไข (Data Integrity) ด้วย Hashing Algorithm แบบ SHA-1 หรือ SHA-256 หรือเทียบเท่าหรือดีกว่า

5.2.17 สามารถบริหารจัดการผ่าน Web Interface หรือ GUI ได้เป็นอย่างน้อย

5.2.18 สามารถประมวลผลและวิเคราะห์ข้อมูล Log หรือ Event ในแบบแยกเป็นรายหน่วยงาน หรือสามารถทำงานแบบ Multi-Tenanted ได้

5.2.19 สามารถจัดเก็บบันทึก Logging ที่เกิดขึ้นได้ไม่น้อยกว่า 90 วัน

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

5..... 6..... 7..... 8.....

9..... 10..... 11..... 12.....

13.....

5.2.20 มี Framework หรือ Extension ในการทำ Compliance หรือ Reporting ที่มาพร้อมกับระบบได้ เช่น General Data Protection Regulation (GDPR), Good Practice Guide 13 (GPG13), Gramm-Leach-Bliley Act (GLBA) และ Payment Card Industry (PCI)

5.2.21 สามารถแสดงรายงานในรูปแบบตาราง Bar Chart, Pie Chart และออกรายงานในรูปแบบ HTML หรือ PDF ได้เป็นอย่างน้อย

5.2.22 ผลิตภัณฑ์ต้องถูกจัดอันดับให้อยู่ในกลุ่ม Leader จากการจัดอันดับของ Gartner Magic Quadrant for SIEM (Security Information and Event Management) สำหรับปี 2024 หรือปีล่าสุด

5.2.23 ระบบจัดเก็บบันทึกและวิเคราะห์ข้อมูลความปลอดภัยบนระบบเครือข่าย (SIEM) ที่เสนอต้องมาพร้อมกับเครื่องคอมพิวเตอร์แม่ข่าย โดยมีคุณสมบัติ อย่างน้อยดังนี้

5.2.23.1 เครื่องคอมพิวเตอร์แม่ข่ายสำหรับประมวลข้อมูลของระบบจัดเก็บบันทึกและวิเคราะห์ข้อมูลความปลอดภัยบนระบบเครือข่าย (SIEM) จำนวน 2 เครื่อง โดยแต่ละเครื่องมีคุณสมบัติ อย่างน้อยดังนี้

1) มีหน่วยประมวลผลกลาง (Processor) ที่มี Core ไม่น้อยกว่า 12 Core หรือดีกว่า จำนวนไม่น้อยกว่า 2 หน่วย โดยแต่ละหน่วยมีความเร็วสัญญาณนาฬิกา (Clock Speed) ไม่ต่ำกว่า 2.0 GHz
2) มีหน่วยความจำแบบ Cache Memory รวมในระดับ (Level) เดียวกันขนาดไม่น้อยกว่า 30 MB
3) มีหน่วยความจำ (Memory) ชนิด DDR5 ที่มีขนาด 64 GB จำนวน 2 Slot เป็นอย่างน้อย และรองรับการขยายขนาดหน่วยความจำ (Memory) โดยมีจำนวน Slots รวมได้ไม่น้อยกว่า 30 Slots
4) มีหน่วยควบคุมในการจัดการ RAID ชนิดที่รองรับการทำ RAID 0, 1, 10, 5, 50, 6 และ 60 ได้เป็นอย่างน้อย พร้อม Flash cache ขนาดไม่น้อยกว่า 2 GB
5) มีหน่วยเก็บข้อมูลแบบ Hot-Swap ชนิด SSD หรือดีกว่า มีขนาดความจุไม่น้อยกว่า 3.84 TB จำนวนไม่น้อยกว่า 22 หน่วย
6) มีส่วนเชื่อมต่อกับระบบเครือข่าย แบบ 1 GbE จำนวนไม่น้อยกว่า 4 Ports
7) มีส่วนเชื่อมต่อกับระบบเครือข่าย แบบ 10/25 GbE จำนวนไม่น้อยกว่า 4 Ports พร้อม Module Transceiver 10 GbE จำนวนไม่น้อยกว่า 4 Module
8) มีหน่วยจ่ายกระแสไฟฟ้าภายในเครื่อง (Power Supply Unit) จำนวนไม่น้อยกว่า 2 หน่วย ที่มีคุณสมบัติทำงานทดแทนกันได้โดยอัตโนมัติ (Redundant) และสามารถถอดเปลี่ยนได้ทันที (Hot-Swap)
9) มีระบบบริหารจัดการเครื่องคอมพิวเตอร์แม่ข่ายจากระยะไกล โดยสามารถตรวจเช็คสถานะของเครื่อง เปิด-ปิดเครื่องคอมพิวเตอร์แม่ข่าย ควบคุมหน้าจอเครื่องคอมพิวเตอร์แม่ข่าย Mapping ISO File จากเครื่องคอมพิวเตอร์

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

5..... 6..... 7..... 8.....

9..... 10..... 11..... 12.....

13.....

ลูกข่ายได้ Mount ISO หรือ Image File ผ่าน HTTPS, SFTP, CIFS และ NFS ได้เป็นอย่างน้อย

10) เครื่องคอมพิวเตอร์แม่ข่ายที่เสนอ ต้องผ่านมาตรฐาน FCC (Class A), UL หรือ CSA และ Energy Star เป็นอย่างน้อย

5.2.23.2 เครื่องคอมพิวเตอร์แม่ข่ายสำหรับรับส่งข้อมูลจราจรคอมพิวเตอร์ เพื่อส่งข้อมูลไปประมวลผลสำหรับระบบจัดเก็บบันทึกและวิเคราะห์ข้อมูลความปลอดภัยบนระบบเครือข่าย (SIEM) จำนวน 2 เครื่อง โดยแต่ละเครื่องมีคุณสมบัติ อย่างน้อยดังนี้

1) มีหน่วยประมวลผลกลาง (Processor) ที่มี Core ไม่น้อยกว่า 12 Core หรือดีกว่า จำนวนไม่น้อยกว่า 1 หน่วย โดยแต่ละหน่วยมีความเร็วสัญญาณนาฬิกา (Clock Speed) ไม่ต่ำกว่า 2.0 GHz
2) มีหน่วยความจำแบบ Cache Memory รวมในระดับ (Level) เดียวกันขนาดไม่น้อยกว่า 30 MB
3) มีหน่วยความจำ (Memory) ชนิด DDR5 ที่มีขนาด 32GB จำนวน 2 Slot เป็นอย่างน้อย และรองรับการขยายขนาดหน่วยความจำ (Memory) โดยมีจำนวน Slots รวมได้ไม่น้อยกว่า 30 Slots
4) มีหน่วยควบคุมในการจัดการ RAID ชนิดที่รองรับการทำ RAID 0, 1, 10, 5, 50, 6 และ 60 ได้เป็นอย่างน้อย พร้อม Flash Cache ขนาดไม่น้อยกว่า 2 GB
5) มีหน่วยเก็บข้อมูลสำรอง (Hard Disk) แบบ Hot-Swap SSD ซึ่งมีขนาดความจุไม่น้อยกว่า 1.92 TB จำนวนไม่น้อยกว่า 4 หน่วย
6) มีส่วนเชื่อมต่อกับระบบเครือข่าย แบบ 1 GbE จำนวนไม่น้อยกว่า 4 Ports
7) มีส่วนเชื่อมต่อกับระบบเครือข่าย แบบ 10/25 GbE จำนวนไม่น้อยกว่า 4 Ports พร้อม Module Transceiver 10GbE จำนวนไม่น้อยกว่า 4 Module
8) มีหน่วยจ่ายกระแสไฟฟ้าภายในเครื่อง (Power Supply Unit) จำนวนไม่น้อยกว่า 2 หน่วย ที่มีคุณสมบัติทำงานทดแทนกันได้โดยมอัตโนมัติ (Redundant) และสามารถถอดเปลี่ยนได้ทันที (Hot-Swap)
9) มีระบบบริหารจัดการเครื่องคอมพิวเตอร์แม่ข่ายจากระยะไกล โดยสามารถตรวจเช็คสถานะของเครื่อง เปิด-ปิดเครื่องคอมพิวเตอร์แม่ข่าย ควบคุมหน้าจอเครื่องคอมพิวเตอร์แม่ข่าย Mapping ISO File จากเครื่องคอมพิวเตอร์

1..... 2..... 3..... 4.....
5..... 6..... 7..... 8.....
9..... 10..... 11..... 12.....
13.....

ลูกข่ายได้ Mount ISO หรือ Image File ผ่าน HTTPS, SFTP, CIFS และ NFS ได้เป็นอย่างน้อย

10) เครื่องคอมพิวเตอร์แม่ข่ายที่เสนอ ต้องผ่านมาตรฐาน FCC (Class A), UL หรือ CSA และ Energy Star เป็นอย่างน้อย

**6. การติดตั้งระบบ**

6.1 ผู้ขายต้องออกแบบและจัดทำ Standard Use Case รวมทั้งกำหนดประเภทข้อมูล (Log) ที่ใช้ในการวิเคราะห์ จำนวนไม่น้อยกว่า 5 Standard Use Case

6.2 ผู้ขายต้องออกแบบและจัดทำการแสดงผล Dashboard ให้สอดคล้องกับ Standard Use Case

6.3 ผู้ขายต้องออกแบบและจัดทำรูปแบบของ Report ให้สอดคล้องกับ Standard Use Case

6.4 ผู้ขายต้องออกแบบ Customized Use Case เพิ่มเติมจาก Standard Use Case

6.5 ผู้ขายต้องดูแลให้คำแนะนำของอุปกรณ์ที่จัดซื้อตามข้อ 4 เพื่อให้การดำเนินงานการเฝ้าระวังตรวจสอบการถูกบุกรุกและตอบสนองต่อภัยคุกคามทางไซเบอร์ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานเป็นไปอย่างมีประสิทธิภาพ

6.6 ผู้ขายต้องจัดทำเอกสารการออกแบบติดตั้ง และเอกสารคู่มือการใช้งานเป็นภาษาไทย

6.7 ผู้ขายต้องสนับสนุน ช่วยเหลือ และแก้ไข (Emergency Incident Response Support) จากผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศในรูปแบบ Onsite อย่างน้อย 2 ครั้ง

6.8 กรณีที่ผู้ขายดำเนินการติดตั้งพร้อมตั้งค่าระบบอุปกรณ์ หากต้องมีการจัดหาอุปกรณ์ส่วนเสริมเพิ่มเติมที่จำเป็นสำหรับติดตั้งอุปกรณ์เพื่อให้สามารถทำงานได้อย่างมีประสิทธิภาพ ผู้ขายต้องจัดหาเพิ่มเติมโดยไม่คิดค่าใช้จ่ายเพิ่มเติม

**7. เงื่อนไขอื่น ๆ**

ผู้ขายต้องจัดทำแผนการฝึกอบรมและจัดฝึกอบรมให้กับบุคลากรและเจ้าหน้าที่ตามที่สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานกำหนด จำนวนไม่น้อยกว่า 10 คน โดยผู้ขายเป็นผู้รับผิดชอบค่าใช้จ่ายในการฝึกอบรมทั้งหมด

**8. ระยะเวลาดำเนินงาน**

ระยะเวลาในการดำเนินการ 240 วัน นับถัดจากวันลงนามในสัญญา

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

5..... 6..... 7..... 8.....

9..... 10..... 11..... 12.....

13.....

**9. หลักเกณฑ์ในการพิจารณาข้อเสนอ**

การพิจารณาผลการยื่นข้อเสนอครั้งนี้ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานจะใช้หลักเกณฑ์พิจารณาตัดสินโดยใช้เกณฑ์ราคา

**10. งบประมาณโครงการ**

งบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. 2568 จำนวนทั้งสิ้น 42,948,000 บาท

**11. การส่งมอบงาน และการจ่ายเงิน**

11.1 งวดที่ 1 ภายใน 30 วัน นับถัดจากวันที่ลงนามในสัญญา เบิกจ่ายเงินร้อยละ 20 ของวงเงินงบประมาณตามสัญญา และคณะกรรมการตรวจรับพัสดุได้ทำการตรวจรับเรียบร้อยแล้ว โดยผู้ขายต้องส่งมอบเอกสาร อย่างน้อยดังนี้

11.1.1 แผนการบริหารโครงการ (Project Management Plan)

11.1.2 แผนการดำเนินการโครงการ (Implementation Plan)

11.2 งวดที่ 2 ภายใน 120 วัน นับถัดจากวันที่ลงนามในสัญญา เบิกจ่ายเงินร้อยละ 30 ของวงเงินวงเงินงบประมาณตามสัญญา และคณะกรรมการตรวจรับพัสดุได้ทำการตรวจรับเรียบร้อยแล้ว โดยผู้ขายต้องส่งมอบอุปกรณ์ ตามข้อกำหนดข้อ 5

11.3 งวดที่ 3 ภายใน 240 วัน นับถัดจากวันที่ลงนามในสัญญา เบิกจ่ายเงินร้อยละ 50 ของวงเงินวงเงินงบประมาณตามสัญญา และคณะกรรมการตรวจรับพัสดุได้ทำการตรวจรับเรียบร้อยแล้ว โดยผู้ขายต้องติดตั้งอุปกรณ์ทั้งหมดและทดสอบการทำงานภาพรวม รวมถึงการฝึกอบรม เอกสารการออกแบบติดตั้งและเอกสารคู่มือการใช้งานเป็นภาษาไทย ตามข้อ 6.6 พร้อมจัดส่งแผนการบำรุงรักษาในช่วงการรับประกัน ตามข้อ 13.1

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

**12. อัตราค่าปรับ**

12.1 กรณีที่ผู้ขายไม่ส่งมอบงานงวดสุดท้ายให้เป็นไปตามกำหนดระยะเวลาการส่งมอบงาน สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานจะดำเนินการปรับเป็นรายวัน ในอัตราร้อยละ 0.2 ของวงเงินงบประมาณตามสัญญานับถัดจากวันที่กำหนดแล้วเสร็จตามสัญญา จนถึงวันที่ผู้ขายปฏิบัติตามสัญญาถูกต้องครบถ้วนและสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานได้ตรวจรับงานแล้ว

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

5.....6.....7.....8.....

9.....10.....11.....12.....

13.....

12.2 ในระหว่างระยะเวลารับประกัน หากมีการชำรุดบกพร่องหรือข้อขัดข้องอันเนื่องมาจากการใช้งานตามปกติ ผู้ขายจะต้องจัดเจ้าหน้าที่เข้ามาซ่อมแซมและแก้ไขภายใน 4 ชั่วโมงหลังจากที่ได้รับแจ้งจากผู้ดูแลระบบและแก้ไขให้แล้วเสร็จภายใน 8 ชั่วโมงโดยไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้น ทั้งนี้ หากไม่สามารถดำเนินการให้แล้วเสร็จภายใน 8 ชั่วโมง ผู้ขายต้องยินยอมให้ผู้ซื้อคิดค่าปรับในอัตราร้อยละ 0.1 ต่อวันของเงินประกันผลงาน

**13. รายละเอียดการรับประกัน**

13.1 ผู้ขายต้องจัดทำแผนการบำรุงรักษาเชิงป้องกัน (Preventive Maintenance: PM) และการบำรุงรักษาเชิงแก้ไข (Corrective Maintenance: CM) ในช่วงระยะเวลาการรับประกัน โดยจัดส่งให้สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

13.2 ผู้ขายต้องจัดทำรายงานประจำเดือน (Monthly Report) ที่สรุปเหตุการณ์ภัยคุกคามด้านเทคโนโลยีสารสนเทศและไซเบอร์ในระหว่างระยะเวลารับประกัน อย่างน้อยดังนี้

13.2.1 รายงานสรุปการตอบรับเหตุการณ์ เพื่อนำเสนอให้สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานทราบถึงสาเหตุการบุกรุก จุดอ่อน และแนวทางแก้ไขป้องกัน รวมถึงการเรียนรู้เพื่อไม่เกิดปัญหาซ้ำ (Problem Learning)

13.2.2 รายงานสรุปผู้บริหาร (Executive Summary) เพื่อรายงานผลการเฝ้าระวังเหตุคุกคามทางไซเบอร์ในแต่ละเดือน

13.2.3 สรุปข่าวสารด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security News) พร้อมทั้งให้คำแนะนำ เพื่อหาแนวทางในการแก้ปัญหาร่วมกับสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

13.3 ผู้ขายต้องบำรุงรักษา และรับประกันการใช้งานฮาร์ดแวร์และซอฟต์แวร์ที่นำเสนอ ตลอดจนจะต้องรับผิดชอบดูแลแก้ไขปัญหาต่าง ๆ ที่เกิดขึ้นในระบบ รวมทั้งปรับแต่งระบบให้สามารถใช้งานได้อย่างมีประสิทธิภาพ โดยมีระยะเวลาการรับประกันทั้งสิ้น 1 ปี โดยนับถัดจากวันที่คณะกรรมการตรวจรับพัสดุตรวจรับงานงวดสุดท้ายเรียบร้อยแล้ว หากมีการชำรุดบกพร่องหรือข้อขัดข้องอันเนื่องมาจากการใช้งานตามปกติ ผู้ขายจะต้องจัดเจ้าหน้าที่เข้ามาซ่อมแซมและแก้ไขภายใน 4 ชั่วโมงหลังจากที่ได้รับแจ้งจากผู้ดูแลระบบและแก้ไขให้แล้วเสร็จภายใน 8 ชั่วโมง โดยไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้น

13.4 ผู้ขายต้องรักษาความลับและไม่นำเนื้อหาข้อมูล รูปภาพ และข้อมูลใด ๆ ของสำนักงาคณะกรรมการการศึกษาขั้นพื้นฐาน ไปเผยแพร่

**14. หน่วยงานที่รับผิดชอบ**

สำนักเทคโนโลยีเพื่อการเรียนการสอน สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

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

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

5.....6.....7.....8.....

9.....10.....11.....12.....

13.....