ร่าง ข้อกำหนดขอบเขตงาน (Terms of Reference : TOR)
การปรับปรุงระบบการรักษาความปลอดภัย (Security System)
และการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log System)
ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

1. หลักการและเหตุผล

การติดต่อสื่อสารผ่านระบบเครือข่ายคอมพิวเตอร์ได้เข้ามามีบทบาทและมีความสำคัญต่อการทำงานและการดำเนินชีวิตของทุก ๆ คนเพิ่มมากขึ้น ในขณะเดียวกันปัญหาของภัยคุกคามที่เกิดจากโปรแกรมที่ถูกสร้างขึ้นมาเพื่อประสงค์ร้ายต่อเครื่องคอมพิวเตอร์และเพื่อมาล้วงข้อมูลสำคัญไปจากผู้ใช้งานคอมพิวเตอร์ โดยมัลแวร์ที่เรารู้จักกันดีก็คือ ไวรัส (Virus) เวิร์ม (Worm) โทรจัน (Trojan Horse) สปายแวร์ (Spyware) คีย์ล็อกเกอร์ (Key Logger) คุ้กกี้ (Cookie) และการ Malicious Mobile Code (MMC) ที่อาศัยช่องโหว่ของโปรแกรมอินเทอร์เน็ตบราวเซอร์ เช่น การแสดงโฆษณาในลักษณะของการ Pop-Up หน้าต่างโฆษณาออกมาเป็นระยะ เราเรียกโปรแกรมประเภทนี้ว่า แอ็ดแวร์ (Adware) ซึ่งภัยเหล่านี้ได้เพิ่มขึ้นอย่างรวดเร็ว ซึ่งอาจจะเกิดผลกระทบแก่ผู้ใช้งานได้ เป็นต้น

ปัจจุบันสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน มักประสบปัญหาเกี่ยวกับการบริหารจัดการและควบคุมการใช้งานอินเทอร์เน็ต และการแพร่ระบาดของภัยร้ายจากมัลแวร์เป็นอย่างมาก เนื่องจากระบบและอุปกรณ์ที่ใช้งานอยู่มีการใช้งานมากกว่า 7 ปีแล้ว และไม่รองรับรูปแบบของภัยคุมคามใหม่ ๆ ที่เกิดขึ้น เช่น รูปแบบการโจมตีระบบเครือข่ายคอมพิวเตอร์ หรือการเรียกค่าไถ่ จากเครื่องคอมพิวเตอร์ลูกข่ายที่ติดมัลแวร์ รวมทั้งการเข้าใช้งานเว็บไซต์ที่ไม่เหมาะสม และไม่สามารถจัดจ้างเพื่อทำการบำรุงรักษาต่อไปได้

สำหรับปัญหาของภัยคุกคามต่าง ๆ สามารถป้องกันและแก้ไขได้ หากมีระบบรักษาความปลอดภัยที่ดีและมีประสิทธิภาพ ครอบคลุมระบบเครือข่ายคอมพิวเตอร์ทุก ๆ ส่วน อาทิเช่น ส่วนของระบบเครือข่ายคอมพิวเตอร์ ส่วนของเครื่องคอมพิวเตอร์ลูกข่าย ตลอดจนส่วนที่ให้บริการการออกอินเทอร์เน็ต รวมถึงสามารถตรวจสอบการใช้งานของผู้ใช้งานทั้งภายในเครือข่าย และการใช้งานอินเทอร์เน็ต

2. วัตถุประสงค์

2.1. เพื่อจัดหาระบบรักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์ และระบบรักษาความปลอดภัยบนเครื่องคอมพิวเตอร์ลูกข่าย ทดแทนระบบรักษาความปลอดภัยเดิมที่ด้อยประสิทธิภาพ และใช้งานมานานกว่า 7 ปี

2.2. เพื่อป้องกันภัยจากการแพร่ระบาดของมัลแวร์ (Malware) บนเครื่องคอมพิวเตอร์ลูกข่าย

2.3. เพื่อป้องกันและแก้ไขปัญหาของการแพร่ระบาดของมัลแวร์ (Malware) ประเภทต่าง ๆ บนเครือข่ายคอมพิวเตอร์ ที่ส่งผลให้การใช้งานระบบเครือข่ายคอมพิวเตอร์และการใช้งานอินเทอร์เน็ตไม่มีประสิทธิภาพ

2.4. เพื่อการกำหนดนโยบาย (Policy) ในการใช้งานระบบงานภายในเครือข่าย การใช้งานอินเทอร์เน็ต และการป้องกันการบุกรุกโจมตีจากภายนอกเครือข่าย

2.5. เพื่อเก็บข้อมูลการใช้งานข้อมูลจราจรคอมพิวเตอร์ในระบบเครือข่ายคอมพิวเตอร์ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน และให้เป็นไปตามข้อกำหนดของ พ.ร.บ. คอมพิวเตอร์ 2560

3. คุณสมบัติผู้เสนอราคา

3.1. มีความสามารถตามกฎหมาย

3.2. ไม่เป็นบุคคลล้มละลาย

3.3. ไม่อยู่ระหว่างเลิกกิจการ

3.4. ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5. ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วน ผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6. มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7. เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8. ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9. ไม่เป็นผู้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทยเว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

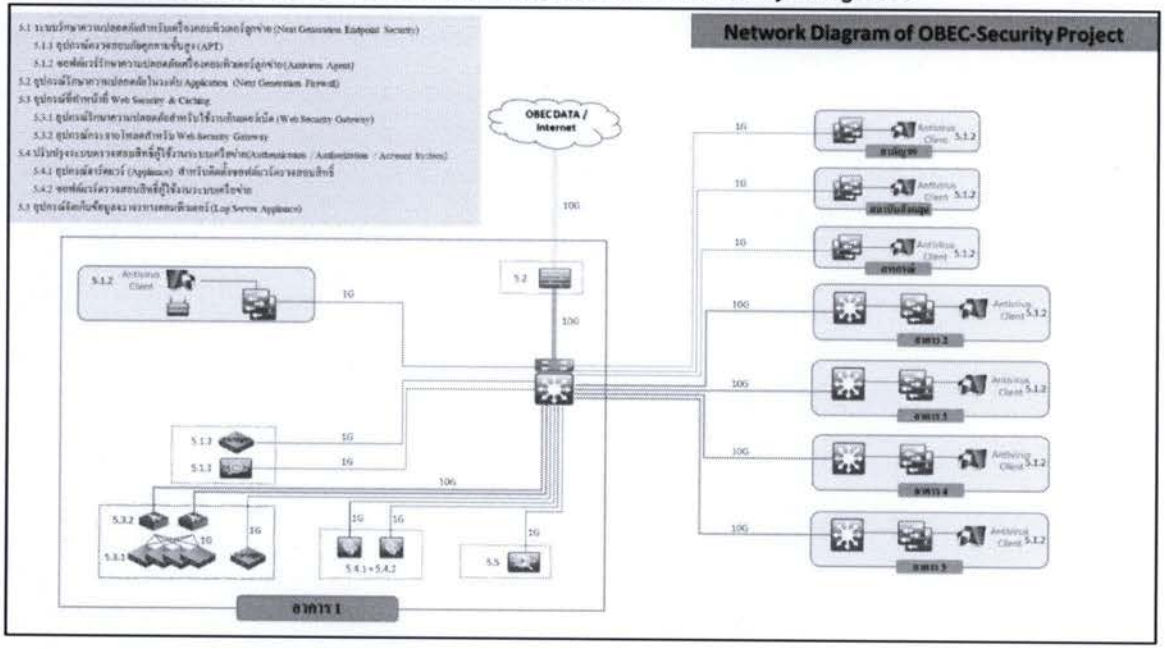
3.10. ผู้ยื่นข้อเสนอต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e - GP) ของกรมบัญชีกลาง

3.11. ผู้ยื่นข้อเสนอซึ่งได้รับคัดเลือกเป็นคู่สัญญาต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e - GP) ของกรมบัญชีกลาง ตามที่คณะกรรมการ ป.ป.ช. กำหนด

3.12. ผู้ยื่นข้อเสนอต้องไม่อยู่ในฐานะเป็นผู้ไม่แสดงบัญชีรายรับรายจ่าย หรือแสดงบัญชีรายรับรายจ่าย ไม่ถูกต้องครบถ้วนในสาระสำคัญ ตามที่คณะกรรมการ ป.ป.ช. กำหนด

3.13. ผู้ยื่นข้อเสนอซึ่งได้รับคัดเลือกเป็นคู่สัญญาต้องรับและจ่ายเงินผ่านบัญชีธนาคาร เว้นแต่การจ่ายเงินแต่ละครั้งซึ่งมีมูลค่าไม่เกินสามหมื่นบาทคู่สัญญาอาจจ่ายเป็นเงินสดก็ได้ ตามที่คณะกรรมการ ป.ป.ช. กำหนด

4. แผนผังการเชื่อมโยงระบบรักษาความปลอดภัยเครือข่าย (Security Diagram)



5. คุณลักษณะของอุปกรณ์

ที่	รายการ	จำนวน	งบประมาณ
5.1	ระบบรักษาความปลอดภัยสำหรับเครื่องคอมพิวเตอร์ลูกข่าย (Next Generation Endpoint Security)	1 ระบบ	6,500,000
5.2	อุปกรณ์รักษาความปลอดภัยในระดับ Application (Next Generation Firewall)	1 ชุด	6,500,000
5.3	อุปกรณ์ที่ทำหน้าที่ Web Security & Caching	1 ระบบ	15,000,000
5.4	ปรับปรุงระบบตรวจสอบสิทธิ์ผู้ใช้งานระบบเครือข่าย (Authentication / Authorization / Account System)	1 ระบบ	3,500,000
5.5	อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log Server Appliance)	1 ชุด	2,500,000
รวมทั้งสิ้น			**34,000,000**

5.1. ระบบรักษาความปลอดภัยสำหรับเครื่องคอมพิวเตอร์ลูกข่าย (Next Generation Endpoint Security) จำนวน 1 ระบบ ประกอบด้วยดังนี้

5.1.1. อุปกรณ์ตรวจสอบภัยคุกคามขั้นสูง Advanced Persistent Threat (APT) ที่เป็นผลิตภัณฑ์ภายใต้บริษัทเดียวกันกับซอฟต์แวร์รักษาความปลอดภัยเครื่องคอมพิวเตอร์ลูกข่าย (Endpoint Protection) และทำงานร่วมกันได้ โดยมีคุณสมบัติอย่างน้อยดังต่อไปนี้

5.1.1.1. เป็นระบบตรวจจับและค้นหาการโจมตี แบบ APT (Advanced Persistent Threats), Zero-day Malware และการโจมตีโดยใช้ Document Exploits ได้

5.1.1.2. เป็นอุปกรณ์ Appliance มี Interface แบบ 10/100/1000 (RJ45) อย่างน้อย 3 พอร์ต หรือดีกว่า และมี Management Port แบบ 10/100/1000 (RJ45) อย่างน้อย 1 พอร์ต

5.1.1.3. สามารถตรวจจับ Zero-day & UnKnown Malware ได้ด้วยวิธี Sandboxing และสร้าง Dynamic Signature และ Blacklisting เพื่อหยุดยั้งภัยคุกคามที่ตรวจพบและป้องกัน C&C Communication ของ Malware ที่ Endpoint ได้

5.1.1.4. ใช้เทคนิค Sandbox Analysis เพื่อตรวจจับ/ป้องกัน Advance Malware โดยมีอย่างน้อย 60 Virtual Sandbox หรือรองรับ Capacity ได้อย่างน้อย 20,000 Samples ต่อวัน สามารถเสนออุปกรณ์เพิ่มเติมได้เพื่อให้จำนวน Virtual Sandbox/Capacity ครบถ้วนได้

5.1.1.5. มี Redundant Power Supply

5.1.2. ซอฟต์แวร์รักษาความปลอดภัยเครื่องคอมพิวเตอร์ลูกข่าย (Endpoint Protection) โดยมีคุณสมบัติอย่างน้อยดังต่อไปนี้

5.1.2.1. สามารถติดตั้ง Agent ได้ไม่น้อยกว่า 3,000 เครื่อง และสามารถ Update Signature ได้ตลอดระยะเวลา 1 ปี โดยรองรับการทำงานบนระบบปฏิบัติการอย่างน้อย ดังนี้

5.1.2.1.1. Microsoft Windows Server 2012 หรือรุ่นที่ดีกว่า (64 บิต)

5.1.2.1.2. Microsoft Windows 8.1 หรือรุ่นที่ดีกว่า (32 บิต และ 64 บิต)

5.1.2.1.3. macOS 10.9.5 หรือรุ่นที่ใหม่กว่า

5.1.2.1.4. Linux

5.1.2.1.5. Android 8 หรือรุ่นที่ใหม่กว่า

5.1.2.1.6. iOS 10 หรือรุ่นที่ใหม่กว่า

5.1.2.2. สามารถทำงานได้ในทั้งรูปแบบ On-premise และ as a Service สำหรับเครื่องลูกข่ายบนระบบปฏิบัติการ Windows และ Mac โดยมีระบบบริหารจัดการนโยบายจากส่วนกลาง (Policy Management) ผ่าน Web Console หรือ GUI ได้ และสามารถทำรายงานสรุปให้ผู้ดูแลระบบและผู้บริหารได้

5.1.2.3. สามารถทำการป้องกันอันตรายที่มาจากทางเว็บไซต์ต่าง ๆ (Web Threats) โดยใช้ Web Reputation ได้

5.1.2.4. สามารถตรวจพบไวรัสคอมพิวเตอร์ได้อย่างน้อย โดยวิธีการตรวจสอบข้อมูลจาก Definition หรือ Signature ของไวรัส นอกจากนั้นสามารถใช้เทคนิคการตรวจจับไวรัสหรือมัลแวร์ได้หลากหลายวิธี อย่างน้อยดังนี้ File Reputation, Behavioral Analysis, Machine Learning และสามารถทำงานร่วมกับระบบ Sandbox ได้ หรือเสนอระบบอื่นเพิ่มเติมเพื่อทำงานเทียบเท่าหรือดีกว่า

5.1.2.5. มีความสามารถ Ransomware Protection และสามารถกู้คืนเอกสารที่ถูกโจมตี โดย Ransomware ได้

5.1.2.6. กรณีที่ตรวจพบไวรัสคอมพิวเตอร์ และไม่สามารถกำจัดได้ในช่วงเวลานั้น จะต้องมีระบบที่กักกัน (Quarantines) ไม่ให้ไวรัสแพร่ระบาดออกไปได้

5.1.2.7. สามารถหยุดการทำงาน และถอดถอนการติดตั้งของระบบรักษาความปลอดภัย โดยรองรับการใช้รหัสผ่านได้ หรือวิธีอื่นได้

5.1.2.8. สามารถกำหนดสิทธิ์ของผู้ดูแลระบบในระดับที่แตกต่างกัน ด้วยสิทธิ์ที่ต่างกันได้ (Role-based Administration)

5.1.2.9. มีระบบการติดตั้งใช้งานในระบบเครือข่าย และปรับปรุงข้อมูลไวรัสคอมพิวเตอร์ให้ทันสมัย ซึ่งสามารถทำงานได้ในลักษณะติดตั้งผ่านเครื่องแม่ข่ายส่วนกลาง

5.1.2.10. สามารถทำการป้องกันโปรแกรมประยุกต์ที่ไม่ได้รับอนุญาตและไม่ต้องการให้ติดตั้ง (Lockdown, Blacklist) ไปยังเครื่องลูกข่ายได้ และสามารถกำหนด Rule โดยใช้เงื่อนไขได้อย่างน้อย ดังนี้

5.1.2.10.1. Path Expression

5.1.2.10.2. File Signatures (SHA-1)

5.1.2.10.3. Certificate

5.1.2.10.4. Application Reputation List

5.1.2.11. มีระบบการป้องกันข้อมูลเมื่อเกิดการโจรกรรมอุปกรณ์ได้โดยการสั่งล็อคหรือล้างข้อมูลได้จากระยะไกล (Reset Password) จากส่วนกลางรวมไปถึงสามารถกำหนดนโยบายการใช้พาสเวิร์ดและปิดการใช้งานความสามารถบางอย่างของอุปกรณ์ได้ เช่น กล้องถ่ายรูปบน Android และ iOS ได้เป็นอย่างน้อย หรือเสนอระบบอื่นเพิ่มเติมเพื่อทำงานเทียบเท่าได้หรือดีกว่า

5.1.2.12. สามารถป้องกันข้อมูลรั่วไหล (Data Loss Prevention) โดยกำหนดนโยบาย ให้ตรวจสอบไฟล์หรือข้อมูลตามลักษณะ Keyword หรือแบบ Regular Expression ผ่านทาง FTP, HTTP, Web Mail โดยใช้เงื่อนไขได้แก่ File Attributes, Keywords, Regular Expressions หรือเสนอระบบอื่นเพิ่มเติมเทียบเท่าหรือดีกว่า

5.1.2.13. สามารถทำการเข้ารหัสข้อมูลในเครื่องคอมพิวเตอร์ได้ในรูปแบบทั้ง Full Disk Encryption และ File and Folder Encryption ได้

5.1.2.14. มีความสามารถในการกำหนดสิทธิ์การใช้งาน ได้แก่ Full Access, Read, Read and Execute, Modify, List Content ให้กับอุปกรณ์ USB Storage Devices ได้ และสามารถอนุญาตให้ใช้งาน USB Storage ได้เป็นรายยี่ห้อ (Vendor ID) และ Serial Number ที่มีการลงทะเบียนในระบบเท่านั้น

5.1.2.15. สามารถหยุดการทำงานของ Scheduled Scan ได้โดยอัตโนมัติเมื่อใช้เวลาในการทำ Scan นานเกินกว่าที่กำหนด

5.1.2.16. ผลิตภัณฑ์ที่นำเสนอต้องอยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant ของ Endpoint Protection Platforms ปี 2018 หรือใหม่กว่า

5.1.3. ผู้เสนอราคาต้องได้รับหนังสือแต่งตั้งให้เป็นตัวแทนจำหน่ายจากผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทย พร้อมแนบหนังสือรับรอง ประกอบการพิจารณา

5.2. อุปกรณ์รักษาความปลอดภัยในระดับ Application (Next Generation Firewall) จำนวน 1 ชุด โดยมีคุณสมบัติอย่างน้อยดังนี้

5.2.1. เป็นอุปกรณ์เฉพาะ Hardware Appliance ที่ทำหน้าที่ Next Generation Firewall โดยแยกหน่วยประมวลผลสำหรับบริหารจัดการ Management/Control Plane และ

หน่วยประมวลผลสำหรับ Data Plane ออกจากกัน หรือสามารถเสนอระบบบริหารจัดการแยกภายนอกได้

5.2.2. มี Throughput ของการใช้งานระดับ Application Firewall หรือ Application Control หรือ Production Performance ไม่น้อยกว่า 39 Gbps

5.2.3. สามารถทำงานป้องกันการบุกรุกและโจมตี (Intrusion Prevention/ Detection) ได้ โดยมี Throughput สูงสุดไม่น้อยกว่า 20 Gbps และได้รับการอัพเดทอัตโนมัติเป็นเวลาอย่างน้อย 1 ปี

5.2.4. รองรับการเชื่อมต่อ (Concurrent Sessions หรือ Concurrent Connections) ได้ไม่น้อยกว่า 8,000,000 (Sessions หรือ Connections) และรองรับการเชื่อมต่อได้ไม่น้อยกว่า 348,000 New Sessions per Second

5.2.5. สามารถทำ VPN ตามมาตรฐาน IPSec โดยรองรับการใช้ Key Exchange แบบ IKEv1/v2 และรองรับการทำ Encryption แบบ 3DES, AES (128-bit, 192-bit, 256-bit) ได้เป็นอย่างน้อย โดยมี VPN Throughput สูงสุดไม่น้อยกว่า 16 Gbps

5.2.6. รองรับการใช้งาน Client VPN (Remote Access) บนโปรโตคอล IPSec และ SSL ได้จำนวนผู้ใช้ได้ไม่น้อยกว่า 5,000 ผู้ใช้ รวมทั้งสามารถทำงานกับระบบปฏิบัติการ Windows (ทั้ง 32 และ 64 bits) ได้เป็นอย่างน้อย หรือนำเสนอระบบภายนอกได้

5.2.7. มีพอร์ตแบบ 100/1000/10G (RJ-45) จำนวนไม่น้อยกว่า 4 พอร์ต

5.2.8. มีพอร์ตรองรับแบบ 1/10G (SFP/SFP+) จำนวนไม่น้อยกว่า 16 พอร์ต

5.2.9. มีพอร์ตรองรับแบบ 40G (QSFP+) จำนวนไม่น้อยกว่า 4 พอร์ต พร้อมเสนอโมดูลแบบ 10GBASE-SR จำนวน 2 โมดูล และโมดูลแบบ 10GBASE-ER จำนวน 2 โมดูล

5.2.10. มีพอร์ต Management Interface แบบ 10/100/1000 อย่างน้อย 1 พอร์ต

5.2.11. อุปกรณ์ต้องมี HDD หรือระบบ External Storage สำหรับเก็บ Log ขนาดไม่น้อยกว่า 2 TB หลังทำ RAID-1

5.2.12. สามารถทำ NAT (Network Address Translation) และ PAT (Port Address Translation) ได้

5.2.13. สามารถใช้กับระบบเครือข่ายแบบ VLAN ผ่าน Protocol 802.1Q ได้

5.2.14. สามารถทำงานแบบ Route Mode และ Transparent (Layer 2) Mode Firewall ได้

5.2.15. สามารถทำ Dynamic Routing Protocol ได้แก่ RIP, OSPF และ BGP ได้เป็นอย่างน้อย

5.2.16. สามารถป้องกันภัยคุกคามประเภท Virus, Exploit และ Spyware ได้ โดยสามารถอัพเดท Signature ใหม่ ๆ แบบอัตโนมัติได้

5.2.17. มีระบบตรวจจับ Advanced Malware แบบ Cloud-Based และใช้เทคโนโลยีแบบ Sandbox เพื่อใช้ระบุ Malware ประเภทใหม่ (Zero-Day Malware) ซึ่งไม่มีในฐานข้อมูลการบุกรุกโจมตีได้ รวมถึงสามารถสร้างรูปแบบการโจมตี (Signature) ดังกล่าวขึ้นมาเพื่อใช้ป้องกันระบบเครือข่ายได้โดยอัตโนมัติ หรือสามารถเสนอระบบแยกภายนอกที่สามารถทำงานร่วมกับระบบนี้ได้

5.2.18. สามารถกำหนดนโยบายการเข้าถึง Website (Web Filtering) สามารถติดตามและควบคุมการเข้าถึงเว็บได้ตาม Category, Block List, Allow List ที่กำหนดได้ และต้องมีการจัด Category ให้กับแต่ละ Website ไม่น้อยกว่า 2 Category หรือเสนอ

อุปกรณ์เพิ่มเติมเพื่อให้ทำได้ตามข้อกำหนด โดยอุปกรณ์ที่เสนอเพิ่มเติมต้องมี Throughput ไม่น้อยกว่า Firewall Throughput

5.2.19. สามารถทำการตรวจสอบทราฟฟิคที่เข้ารหัส SSL ด้วยการทำ SSL Decryption (ทั้งแบบ Inbound และ Outbound) รวมทั้งการทำ SSH Decryption ได้ หรือนำเสนอระบบเพิ่มเติมเพื่อให้ทำงานได้ตามข้อกำหนด

5.2.20. สามารถทำงานร่วมกับระบบการพิสูจน์ตัวตน (Authentication Systems) ได้แก่ Active Directory, LDAP เพื่อทำการติดตามผู้ใช้ได้เป็นอย่างน้อย

5.2.21. สามารถควบคุมประเภทของไฟล์ที่อนุญาตให้ดาวน์โหลดและอัพโหลดแต่ละ Applications ได้ รวมทั้งสามารถป้องกันการรั่วไหลของข้อมูล (Data Filtering) ออกจากระบบเครือข่าย เช่น หมายเลขบัตรเครดิต ได้เป็นอย่างน้อย

5.2.22. สามารถรับ Syslog จากระบบที่มีอยู่ได้ เพื่อใช้ในการยืนยันตัวตนของ User ที่ใช้งาน โดยรองรับทั้ง User Log-in และ User Log-out หรือนำเสนอระบบเพิ่มเติม โดยมี License ครอบคลุมการใช้งาน

5.2.23. สามารถส่ง Syslog ไปยังระบบภายนอกโดยมีการเข้ารหัสแบบ SSL หรือ TLS ได้ เพื่อความปลอดภัยของระบบ

5.2.24. สามารถเรียกดูข้อมูลสรุปในรูปแบบของ GUI ได้ โดยสามารถปรับแต่งรายงานตามความต้องการ (Custom Report) และส่งออก (Export) ให้อยู่ในรูปแบบ PDF ได้เป็นอย่างน้อย พร้อมทั้งตั้งเวลาส่งรายงานผ่านทาง Email แบบอัตโนมัติได้ หรือสามารถเสนอระบบแยกภายนอกได้

5.2.25. มีระบบจ่ายไฟสำรอง Redundancy Power Supply และ Fan แบบ Hot Swap

5.2.26. กรณีที่มีอุปกรณ์ 2 Units ต้องรองรับการติดตั้งเพื่อทำ High Availability (HA) แบบ Active/Passive และ Active/Active ได้

5.2.27. ผลิตภัณฑ์ที่นำเสนอจะต้องอยู่ใน Leader Quadrant ของ Gartner Magic Quadrant ด้าน Enterprise Network Firewalls ปี 2018 หรือใหม่กว่า

5.2.28. ผู้เสนอราคาต้องได้รับหนังสือแต่งตั้งให้เป็นตัวแทนจำหน่ายจากผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทย พร้อมแนบหนังสือรับรอง ประกอบการพิจารณา

5.3. อุปกรณ์ที่ทำหน้าที่ Web Security & Caching จำนวน 1 ระบบ ประกอบด้วยดังนี้

5.3.1. อุปกรณ์รักษาความปลอดภัยสำหรับใช้งานอินเตอร์เน็ต (Web Security Gateway) โดยมีคุณสมบัติอย่างน้อยดังต่อไปนี้

5.3.1.1. เป็นแบบ Virtual Appliance หรือ Appliance ที่ถูกออกแบบมาเพื่อทำหน้าที่ Web Security หรือ Secure Web Gateway โดยเฉพาะ

5.3.1.2. มี License รองรับผู้ใช้งานทั้งด้าน Web Security Gateway ไม่น้อยกว่า 3,000 ผู้ใช้งาน เป็นระยะเวลา 1 ปี

5.3.1.3. สามารถรองรับ Internet Throughput ได้ไม่น้อยกว่า 3 Gbps โดยสามารถเสนอระบบแบบ Virtual Appliance หรือ Appliance มากกว่า 1 หน่วยได้ ดังนี้

5.3.1.3.1. กรณีที่เสนอเป็นแบบ Virtual Appliance อุปกรณ์ที่เสนอแต่ละเครื่องต้องมีคุณสมบัติอย่างน้อยดังต่อไปนี้

5.3.1.3.1.1. มีหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า 2 หน่วย

5.3.1.3.1.2. มี Hard Disk ความจุ 600 GB ไม่น้อยกว่า 4 หน่วย

5.3.1.3.1.3. มีหน่วยความจำอย่างน้อย 256 GB

5.3.1.3.1.4. มีพอร์ต 1/10 Gigabit Ethernet ไม่น้อยกว่า 2 พอร์ต

5.3.1.3.1.5. มี Power Supply ไม่น้อยกว่า 2 หน่วย แบบ Hot Swap หรือ Hot-Pluggable

5.3.1.3.2. กรณีที่เสนอเป็นแบบ Appliance อุปกรณ์ที่เสนอแต่ละเครื่องมีคุณสมบัติอย่างน้อยดังต่อไปนี้

5.3.1.3.2.1. มีหน่วยประมวลผลกลาง (CPU) จำนวนไม่น้อยกว่า 2 หน่วย

5.3.1.3.2.2. มีพื้นที่ใช้งานของ Hard Disk รวมกันไม่น้อยกว่า 4 TB

5.3.1.3.2.3. มีหน่วยความจำไม่น้อยกว่า 64 GB

5.3.1.3.2.4. มีพอร์ต 1000 Base-T ไม่น้อยกว่า 4 Ports

5.3.1.3.2.5. มี Power Supply ไม่น้อยกว่า 2 หน่วย แบบ Hot Swap หรือ Hot-Pluggable

5.3.1.4. มีระบบบริหารจัดการจากศูนย์กลาง (Centralized Management) มีคุณสมบัติอย่างน้อยดังต่อไปนี้

5.3.1.4.1. สามารถบริหาร และจัดการ Configuration ระบบ หรืออุปกรณ์ Secure Web Gateway ที่เสนอทั้งหมดได้ โดยเป็นผลิตภัณฑ์ยี่ห้อเดียวกับ Secure Web Gateway ที่นำเสนอ

5.3.1.4.2. สามารถสร้างและส่งรายงานโดยอัตโนมัติตามระยะเวลาที่กำหนดผ่านทาง e-Mail ได้

5.3.1.4.3. สามารถออกรายงานในรูปแบบ HTML หรือ PDF ได้ โดยสามารถออกรายงานแบบ Top Users, Top Categories และ Top Web Sites หรือ Top Domain และรองรับการ Customizable Reports ได้

5.3.1.4.4. สามารถควบคุมผ่านทาง Browser-based Management แบบ HTTPS ได้

5.3.1.5. สามารถทำงานได้ทั้ง IPv4 และ IPv6

5.3.1.6. สามารถรองรับโปรโตคอล WCCP ได้ทั้งแบบ GRE และ Layer2

5.3.1.7. สามารถกำหนดนโยบายการใช้งานให้กับผู้ใช้แบบบุคคลหรือกลุ่มจาก Directory Services และ LDAP ได้

5.3.1.8. มีฐานข้อมูล Web Category ไม่น้อยกว่า 80 Categories ได้บนอุปกรณ์

5.3.1.9. สามารถกำหนดสิทธิการใช้งานเว็บไซต์ โดยกำหนดจากผู้ใช้ กลุ่มของผู้ใช้ และ IP Address ได้

5.3.1.10. สามารถกำหนดนโยบายการใช้งานเว็บไซต์ในรูปแบบต่าง ๆ อย่างน้อยดังนี้ Allow, Block และการ Block File Type ตามเวลาที่กำหนดได้

5.3.1.11. สามารถตรวจสอบภัยคุกคามต่างๆ แบบ Real-Time โดยใช้เทคโนโลยี WebPulse หรือ Advanced Classification Engine (ACE) หรือ Talos Security Intelligence

5.3.1.12. สามารถทำงานเป็น Web Proxy ทั้งแบบ Transparent Mode และ Explicit Mode ได้

5.3.1.13. สามารถวิเคราะห์และตรวจสอบข้อมูลที่ถูกเข้ารหัสประเภท HTTPS ได้ (SSL Inspection)

5.3.1.14. สามารถกำหนดให้ยกเว้นการถอดรหัส (SSL Decryption By Pass) โดยกำหนดเป็นบางหมวดหมู่ (Category) ได้ เพื่อป้องกันการละเมิดสิทธิส่วนบุคคลของผู้ใช้ได้

5.3.1.15. สามารถตรวจสอบและป้องกัน Virus, Malware และ Spyware รวมทั้ง Malicious Code ที่มากับเว็บไซต์ โดยการวิเคราะห์ Package แบบ Real-time ได้ โดยมี License รองรับ ไม่น้อยกว่า 3,000 ผู้ใช้งาน เป็นระยะเวลา 1 ปี

5.3.1.16. ผลิตภัณฑ์ที่นำเสนอต้องได้รับการยอมรับให้เป็น Leader หรือ Challenger ด้านอุปกรณ์รักษาความปลอดภัยเว็บ (Secure Web Gateway) จาก Gartner ในปี 2018 หรือใหม่กว่า

5.3.2. อุปกรณ์กระจายโหลดสำหรับ Web Security Gateway จำนวน 2 ชุด โดยแต่ละชุดมีคุณบัติอย่างน้อยดังนี้

5.3.2.1. มี Layer 7 Throughput ไม่น้อยกว่า 20 Gbps

5.3.2.2. รองรับ Layer 4 HTTP Request/Sec ได้ไม่น้อยกว่า 2,000,000 Requests Per Second (RPS)

5.3.2.3. มี Network Interface แบบ 1 Gigabit Ethernet ไม่น้อยกว่า 5 พอร์ต

5.3.2.4. มี Network Interface แบบ 10 Gigabit Ethernet (SFP+) ไม่น้อยกว่า 2 พอร์ต พร้อมเสนอ Transceiver Module แบบ 10GBase-SR ไม่น้อยกว่า 2 โมดูล

5.3.2.5. รองรับ SSL Bulk Throughput ไม่น้อยกว่า 9 Gbps

5.3.2.6. รองรับ Layer 4 Concurrent Sessions ไม่น้อยกว่า 32,000,000 Sessions

5.3.2.7. รองรับการทำ Layer 7 Application Persistence และ HTTP Acceleration and Optimization ได้

5.3.2.8. สามารถทำ Load Balance โดยใช้ Method แบบ Round Robin, Least Connections ได้เป็นอย่างน้อย

5.3.2.9. สามารถทำ Virtualization ในระดับ Layer 3 ไม่น้อยกว่า 32 Instances

5.3.2.10. สามารถทำงานด้านความปลอดภัย เช่น Web Application Firewall (WAF) และ DNS Application Firewall (DAF) ได้ หรือนำเสนออุปกรณ์อื่นเพิ่มเติม เพื่อให้ทำงานได้

5.4. ปรับปรุงระบบตรวจสอบสิทธิ์ผู้ใช้งานระบบเครือข่าย(Authentication / Authorization / Account System) จำนวน 1 ระบบ ประกอบด้วย

5.4.1. อุปกรณ์ฮาร์ดแวร์ (Appliance) สำหรับติดตั้งซอฟต์แวร์ตรวจสอบสิทธิ์ผู้ใช้งานระบบเครือข่าย จำนวน 2 ชุด โดยมีคุณสมบัติอย่างน้อยดังต่อไปนี้

5.4.1.1. มีหน่วยประมวลผลกลาง (CPU) ขนาดไม่น้อยกว่า 2.0 GHz, 12-cores จำนวนไม่น้อยกว่า 1 หน่วย

5.4.1.2. มีหน่วยความจำ (Memory) ขนาดไม่น้อยกว่า 96 GB

5.4.1.3. มี Hard Disk ขนาดไม่น้อยกว่า 600 GB แบบ SAS 10K RPM จำนวนไม่น้อยกว่า 4 หน่วย

5.4.1.4. มีพอร์ต 1 Gigabit Ethernet จำนวนไม่น้อยกว่า 4 พอร์ต และพอร์ต 10 Gigabit Ethernet จำนวนไม่น้อยกว่า 2 พอร์ต

5.4.1.5. มีแหล่งจ่ายไฟไม่น้อยกว่า 2 ชุด แบบ Hot-Swappable หรือ Hot-Pluggable ที่สามารถถอดเปลี่ยนได้ขณะทำงาน

5.4.2. ซอฟต์แวร์ตรวจสอบสิทธิ์ผู้ใช้งานระบบเครือข่ายที่เสนอต้องถูกออกแบบสำหรับควบคุมนโยบายขององค์กรแบบครบวงจร สำหรับการเข้าถึงเครือข่ายแบบสาย (Wire) แบบไร้สาย (Wireless) และแบบเสมือน (VPN) โดยมีคุณสมบัติอย่างน้อยดังนี้

5.4.2.1. มีลิขสิทธิ์สำหรับใช้งานเพื่อพิสูจน์ตัวตน (Authentication) ดังนี้

5.4.2.1.1. กรณีที่ระบบที่นำเสนอสามารถใช้งานร่วมกับ Cisco ISE Base License ของ สพฐ. เดิมที่มีอยู่จำนวน 2,500 licenses ให้เสนอ License จำนวนไม่น้อยกว่า 500 License

5.4.2.1.2. กรณีที่ระบบที่นำเสนอไม่สามารถใช้งานร่วมกับ Cisco ISE Base License ของ สพฐ. เดิมที่มีอยู่จำนวน 2,500 licenses ให้เสนอ License ใหม่ จำนวนไม่น้อยกว่า 3,000 License

5.4.2.2. มีลิขสิทธิ์สำหรับการทำ Self-service Device Onboarding โดยการนำอุปกรณ์ส่วนตัวมาใช้ในองค์กรไม่น้อยกว่า 2,000 Licenses

5.4.2.3. สามารถทำ Authentication, Authorization และ Accounting ตามมาตรฐาน RADIUS (Remote Access Dial-In User Service) ได้

5.4.2.4. สามารถกำหนด และอนุญาตให้ผู้ใช้งานภายนอก (Guest) เข้าใช้งานเครือข่าย โดยมีการจำกัดการเข้าถึง หรือการให้บริการเฉพาะอินเทอร์เน็ตสำหรับบุคคลภายนอกเท่านั้น

5.4.2.5. สามารถทำการเชื่อมต่อกับฐานข้อมูลของผู้ใช้งานจากภายนอก (External User Databases) ได้แก่ Microsoft Active Directory (AD), Lightweight Directory Access Protocol (LDAP), RADIUS, RSA One-time Password (OTP), Certificate Authorities และ Open Database Connectivity (ODBC) ได้เป็นอย่างน้อย

5.4.2.6. ต้องสามารถทำงานร่วมกับระบบเครือข่ายแบบไร้สาย (Wireless LAN System) ที่สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานใช้งานอยู่ได้

5.4.2.7. ต้องสามารถทำงานในลักษณะ High Availability (HA) เพื่อให้ระบบตรวจสอบสิทธิ์ผู้ใช้งานสามารถทำงานได้อย่างต่อเนื่อง

5.4.2.8. ต้องรองรับการโอนย้ายสิทธิ์ในการใช้งาน Cisco ISE Base License จำนวน 2,500 Licenses จากระบบตรวจสอบสิทธิ์ผู้ใช้งานของ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน เดิมที่มีการใช้งานได้

5.4.2.9. ระบบหรืออุปกรณ์ที่นำเสนอทั้งหมดต้องเป็นเวอร์ชันล่าสุดยังไม่ถูกประกาศวันยุติการใช้งาน (End-of-Life และ End-of-Sale) และได้รับการสนับสนุนทางด้านเทคนิคหลังการขายจากผู้ผลิต หรือสาขาประเทศไทย

5.4.2.10. ผู้เสนอราคาต้องได้รับหนังสือแต่งตั้งให้เป็นตัวแทนจำหน่ายจากผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทย พร้อมแนบหนังสือรับรองประกอบการพิจารณา

5.5. อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log Server Appliance) จำนวน 1 ชุด โดยมีคุณสมบัติอย่างน้อยดังนี้

5.5.1. เป็นอุปกรณ์ Appliance หรือ Software ที่ติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่สามารถเก็บรวบรวมเหตุการณ์ (Logs or Events) ที่มาจากกลุ่มของ Network, Network Security และ Systems ได้ไม่น้อยกว่า 200 อุปกรณ์ โดยสามารถแสดงผลอยู่ภายใต้รูปแบบ (Format) เดียวกันได้

5.5.2. มีหน่วยประมวลผลกลาง (CPU) แบบ 6 Cores หรือดีกว่า จำนวนไม่น้อยกว่า 2 หน่วย

5.5.3. มีหน่วยความจำหลัก (Memory) ขนาดไม่น้อยกว่า 32 GB

5.5.4. มีช่องสัญญาณสำหรับเชื่อมต่อเครือข่ายแบบ 10/100/1000Base-TX หรือดีกว่า จำนวนไม่น้อยกว่า 2 พอร์ต

5.5.5. มีส่วนควบคุม RAID แบบ RAID 10 หรือ RAID 5 หรือ RAID 6 พร้อม Hard Disk ขนาดไม่น้อยกว่า 2 TB จำนวนไม่น้อยกว่า 8 หน่วย

5.5.6. สามารถจัดเก็บข้อมูลเหตุการณ์ต่อวินาที (Events Per Seconds) ได้ไม่น้อยกว่า 41,000 eps

5.5.7. มีระบบการเข้ารหัสข้อมูลเพื่อใช้ยืนยันความถูกต้องของข้อมูลที่จัดเก็บตามมาตรฐาน MD5 หรือ SHA-1 หรือดีกว่า

5.5.8. สามารถเก็บ Log File ในรูปแบบ Syslog ของอุปกรณ์ เช่น Router, Switch, Firewall, VPN, Server เป็นต้น ได้

5.5.9. สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS, Command Line Interface และ SSH ได้

5.5.10. สามารถจัดเก็บ Log File ได้ถูกต้อง ตรงตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ฉบับที่มีผลบังคับใช้ โดยการเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ต้องเป็นไปตามมาตรฐานศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ มศอ. 4003.1-2560 หรือดีกว่า

5.5.11. สามารถสำรองข้อมูล (Data Backup) ไปยังอุปกรณ์จัดเก็บข้อมูล ได้แก่ Tape หรือ DVD หรือ Storage

5.5.12. สามารถแจ้งเตือน (Alert) ไปยังผู้ดูและระบบเมื่อมีเหตุการณ์ตรงตามเงื่อนไขที่สร้างไว้ หรือเหตุการณ์ผิดปกติของตัวอุปกรณ์ผ่าน e-Mail ได้

5.5.13. สามารถบีบอัดข้อมูลบนพื้นที่จัดเก็บได้อย่างน้อย 15 : 1

5.5.14. สามารถทำการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ในลักษณะของ Centralized และ Forwarder Mode ได้

5.5.15. สามารถปรับเปลี่ยนรูปแบบรายงาน (Custom Report) ได้

5.5.16. สามารถตรวจสอบสถานะของอุปกรณ์ที่ส่ง Log เข้ามาว่ายังทำงานอยู่ได้ หรือเสนออุปกรณ์เพิ่มเติม

5.5.17. สามารถบอกวันสุดท้ายของ Log ที่ส่งเข้ามายังระบบได้

5.5.18. สามารถแยกการเก็บ Log ตามหน่วยงานและแยกสิทธิ์การเข้าถึงได้ หรือเสนออุปกรณ์เพิ่มเติม

5.5.19. สามารถค้นหาข้อมูล Log จากอุปกรณ์ที่ส่ง Log ผ่านทาง IPv4 และ IPv6 ได้

5.5.20. ผู้เสนอราคาต้องได้รับหนังสือแต่งตั้งให้เป็นตัวแทนจำหน่ายจากผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทย พร้อมแนบหนังสือรับรอง ประกอบการพิจารณา

6. ขอบเขตการดำเนินโครงการ

6.1. ผู้ขายจะต้องจัดทำแผนการดำเนินโครงการในภาพรวมทั้งหมด เพื่อให้คณะกรรมการตรวจรับพัสดุและผู้เกี่ยวข้องสามารถติดตามการดำเนินโครงการได้

6.2. ส่งมอบอุปกรณ์ต่าง ๆ ในโครงการ

6.3. ติดตั้งอุปกรณ์ต่าง ๆ ในโครงการ พร้อมตั้งค่าอุปกรณ์ และทดสอบการใช้งานร่วมกับระบบเครือข่ายเดิมของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

7. การฝึกอบรม

ผู้ขายต้องดำเนินการจัดฝึกอบรมโดยผู้เชี่ยวชาญในหลักสูตรสำหรับผู้ดูแลระบบ (Admin) จำนวนไม่น้อยกว่า 5 คน โดยผู้ขายเป็นผู้รับผิดชอบค่าใช้จ่ายทั้งหมดในการจัดฝึกอบรม

8. การบำรุงรักษาและซ่อมแซมแก้ไข

8.1. ผู้ขายจะต้องบำรุงรักษา และรับประกันการใช้งานระบบฯ รวมทั้งฮาร์ดแวร์และซอฟแวร์ที่นำเสนอ ตลอดจนจะต้องรับผิดชอบดูแลแก้ไขปัญหาต่าง ๆ ที่เกิดขึ้นในระบบ รวมทั้งปรับแต่งระบบให้สามารถใช้งานได้อย่างมีประสิทธิภาพ โดยมีระยะเวลาการรับประกันทั้งสิ้น 1 ปี โดยนับตั้งแต่วันที่ส่งมอบและตรวจรับ ได้รับมอบงานไว้ใช้งานโดยสมบูรณ์ หากมีการชำรุดบกพร่องหรือข้อขัดข้องอันเนื่องมาจากการใช้งานตามปกติ ผู้ขายจะต้องจัดเจ้าหน้าที่เข้ามาซ่อมแซมและแก้ไข โดยไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้น

8.2. ผู้ขายจะต้องรักษาความลับและไม่นำเนื้อหาข้อมูล รูปภาพ และข้อมูลใด ๆ ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานไปเผยแพร่

8.3. ผู้ขายจะต้องให้บริการติดตั้ง Bug-fix (Patch) และให้บริการ Upgrade Version ของระบบฯ ตามประกาศของเจ้าของผลิตภัณฑ์ (ตาม Patch ที่มีอยู่ ณ ปัจจุบัน) ซึ่งต้องไม่กระทบต่อการทำงานของระบบฯ โดยต้องได้รับความเห็นชอบร่วมกันระหว่างสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานกับผู้ขาย

8.4. ผู้ขายต้องจัดให้มี Help Desk ซึ่งสามารถให้บริการช่วยเหลือผู้ใช้งานระบบฯ โดยจะต้องสามารถติดต่อ ประสานงาน แจ้งปัญหา และ/หรือร้องขอความช่วยเหลือ ให้คำปรึกษา และแก้ไขปัญหาได้ในวันและเวลาทำการ ยกเว้น กรณีที่เกิดเหตุขัดข้องเร่งด่วนต้องสามารถติดต่อได้นอกเวลาทำการ

9. ระยะเวลาการดำเนินงาน

ผู้ขายจะต้องส่งมอบงานทั้งหมดภายใน 120 วัน นับถัดจากวันที่ลงนามในสัญญา

10. การส่งมอบงาน

ผู้ขายจะต้องส่งมอบงานตามขอบเขตการดำเนินงานทั้งหมด ภายในระยะเวลาที่กำหนดในสัญญา และต้องจัดให้มีการประชุมเพื่อสรุปผลความคืบหน้าของการดำเนินงานให้แก่คณะกรรมการตรวจรับพัสดุได้รับทราบในแต่ละงวดงาน ดังนี้

งวดงานที่ 1 ภายใน 30 วันนับถัดจากวันลงนามในสัญญา ส่งมอบงานตามข้อ 6.1

งวดงานที่ 2 ภายใน 60 วันนับถัดจากวันลงนามในสัญญา ส่งมอบงานตามข้อ 6.2

งวดงานที่ 3 ภายใน 90 วันนับถัดจากวันลงนามในสัญญา ส่งมอบงานตามข้อ 6.3

งวดงานที่ 4 ภายใน 120 วันนับถัดจากวันลงนามในสัญญา ส่งมอบงานตามข้อ 7

11. สถานที่ติดตั้ง

สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน (สพฐ.)

12. งบประมาณ

วงเงินค่าใช้จ่ายทั้งสิ้น 34,000,000 บาท (สามสิบสี่ล้านบาทถ้วน)

13. เงื่อนไขการชำระเงิน

ผู้จ้างจะแบ่งจ่ายเงินออกเป็น 4 งวด เมื่อผู้ขายส่งมอบงานตามรายละเอียดดังนี้

งวดเงินที่ 1 ชำระเงินเป็นจำนวน 10% ของจำนวนเงินตามสัญญา เมื่อผู้ขายได้ส่งมอบงวดงานที่ 1 และคณะกรรมการตรวจรับพัสดุได้ดำเนินการตรวจรับถูกต้องครบถ้วนเรียบร้อยแล้ว

งวดเงินที่ 2 ชำระเงินเป็นจำนวน 30% ของจำนวนเงินตามสัญญา เมื่อผู้ขายได้ส่งมอบงวดงานที่ 2 และคณะกรรมการตรวจรับพัสดุได้ดำเนินการตรวจรับถูกต้องครบถ้วนเรียบร้อยแล้ว

งวดเงินที่ 3 ชำระเงินเป็นจำนวน 30% ของจำนวนเงินตามสัญญา เมื่อผู้ขายได้ส่งมอบงวดงานที่ 3 และคณะกรรมการตรวจรับพัสดุได้ดำเนินการตรวจรับถูกต้องครบถ้วนเรียบร้อยแล้ว

งวดเงินที่ 4 ชำระเงินเป็นจำนวน 30% ของจำนวนเงินตามสัญญา เมื่อผู้ขายได้ส่งมอบงวดงานที่ 4 และคณะกรรมการตรวจรับพัสดุได้ดำเนินการตรวจรับถูกต้องครบถ้วนเรียบร้อยแล้ว

14. หน่วยงานที่รับผิดชอบ

สำนักเทคโนโลยีเพื่อการเรียนการสอน สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

อีเมล์ obecict@obecmail.obec.go.th

โทรศัพท์ 02-288-5906 โทรสาร 02-280-3804