ข้อกำหนด และขอบเขตของงาน

จัดซื้ออุปกรณ์ป้องกันเครือข่ายแบบ Next Generation Firewall

---

1. หลักการและเหตุผล

กองระบบและบริหารข้อมูลเชิงยุทธศาสตร์การอุดมศึกษาวิทยาศาสตร์ วิจัยและนวัตกรรม (กรข.) สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม (สป.อว.) มีภารกิจหลักในการสนับสนุนการดำเนินงานด้านเทคโนโลยีสารสนเทศของ สป.อว. ทั้งด้านอุดมศึกษา และด้านวิทยาศาสตร์และนวัตกรรม ซึ่งมีการพัฒนาระบบโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ เพื่อรองรับการปฏิบัติงาน และประสานงานแลกเปลี่ยนข้อมูลผ่านระบบเครือข่ายคอมพิวเตอร์ทั้งภายในและภายนอกองค์กร ตามนโยบายและยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศและการสื่อสารของประเทศให้สามารถใช้งานได้ตลอดเวลา รวมถึงมีความมั่นคงปลอดภัยในการใช้งาน นั้น

ปัจจุบัน สป.อว. มีการนำอุปกรณ์ป้องกันเครือข่าย Next Generation Firewall มาใช้ควบคุมและป้องกันการเข้าถึงระบบเครือข่ายที่ไม่พึงประสงค์ตามนโยบายความปลอดภัยที่กำหนดไว้ เพื่อป้องกันภัยคุกคามจากภายนอกและภายในระบบ เช่น การโจมตีแบบแรนซัมแวร์ (Ransomware), การเจาะระบบ (Intrusion), การใช้แอปพลิเคชันที่ไม่พึงประสงค์ เป็นต้น แต่ด้วยอุปกรณ์มีอายุการใช้งานเกิน 5 ปี ทำให้ประสิทธิภาพลดลงและไม่สามารถรองรับฟังก์ชันหรือเทคโนโลยีใหม่ในยุคที่ภัยคุกคามทางไซเบอร์มีความซับซ้อนและเปลี่ยนแปลงรวดเร็ว รวมถึงการหยุดให้การสนับสนุนด้านเทคนิค อัปเดต และแพตช์ด้านความปลอดภัย สำหรับฟังก์ชันการใช้งานเครือข่ายเสมือน (VPN) บนอุปกรณ์ดังกล่าวจากบริษัทผู้ผลิต ซึ่งอาจส่งผลกระทบทำให้เกิดช่องโหว่บนเครือข่ายอย่างร้ายแรงได้

กรข. จึงจำเป็นต้องจัดซื้ออุปกรณ์ป้องกันเครือข่ายแบบ Next Generation Firewall ทดแทนอุปกรณ์เดิมที่ล้าสมัยและเริ่มเสื่อมสภาพ เพื่อเพิ่มประสิทธิภาพในการตรวจสอบ วิเคราะห์ การป้องกันภัยคุกคามได้แบบเรียลไทม์ และสามารถรองรับปริมาณข้อมูล (Network Throughput) ที่เพิ่มขึ้นได้อย่างเหมาะสม รวมถึงการเสริมสร้างระบบป้องกันภัยคุกคามทางไซเบอร์ที่หลากหลายและภัยคุกคามใหม่ๆ เช่น การโจมตีเว็บไซต์ ไวรัส มัลแวร์ และการเข้าถึงระบบเครือข่ายของหน่วยงานโดยไม่ได้รับอนุญาต เพื่อป้องกันการรั่วไหลของข้อมูลสำคัญ และรักษาความต่อเนื่องในการดำเนินงานของระบบสารสนเทศ รวมถึงสร้างความเชื่อมั่นให้กับประชาชนและผู้ใช้บริการ

2. วัตถุประสงค์

2.1 เพื่อจัดหาอุปกรณ์ป้องกันเครือข่ายแบบ Next Generation Firewall (NGFW) ทดแทนอุปกรณ์เดิมที่เสื่อมสภาพล้าสมัย

2.2 เพื่อเพิ่มประสิทธิภาพในการบริหารจัดการระบบเครือข่ายของหน่วยงานให้มีความมั่นคงปลอดภัยและสามารถป้องกันภัยคุกคามทางไซเบอร์ที่มีความซับซ้อนและเปลี่ยนแปลงอยู่ตลอดเวลา

2.3 เพื่อให้ระบบเครือข่ายสามารถรองรับปริมาณการใช้งานของข้อมูลที่เพิ่มขึ้นได้อย่างมีเสถียรภาพและต่อเนื่อง

2.4 เพื่อสนับสนุนการดำเนินงานและภารกิจของหน่วยงานให้สามารถให้บริการได้อย่างมีประสิทธิภาพ ปลอดภัย และเป็นไปตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศภาครัฐ

2.5 เพื่อให้สามารถบริหารจัดการ ควบคุม และติดตามการใช้งานระบบเครือข่ายได้อย่างเป็นระบบและมีประสิทธิภาพ

3. คุณสมบัติผู้ยื่นข้อเสนอ

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นนิติบุคคล ผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่ รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละสิทธิ์และความคุ้มกันเช่นว่านั้น

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

3.11 ผู้ยื่นข้อเสนอต้องได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่ายจากบริษัทผู้ผลิตหรือสาขาผู้ผลิตในประเทศไทยอย่างเป็นทางการ ให้มีสิทธิ์ในการจำหน่ายและบริการหลังการขายจากบริษัทผู้ผลิตหรือสาขาผู้ผลิตในประเทศไทยสำหรับโครงการนี้ โดยแนบเอกสารดังกล่าวในวันยื่นข้อเสนอด้วย

4. ข้อกำหนดทั่วไป

ต้องเป็นผลิตภัณฑ์จากผู้ผลิตที่ได้มาตรฐาน และยังมิได้ทำการติดตั้งใช้งาน ณ ที่ใดมาก่อน รวมถึงไม่เป็นอุปกรณ์ที่ถูกนำมาปรับปรุงสภาพใหม่ (Rebuilt) และยังอยู่ในสายการผลิต

5. รายละเอียดคุณลักษณะเฉพาะด้านเทคนิค

5.1 อุปกรณ์ป้องกันเครือข่ายแบบ Next Generation Firewall จำนวน 1 เครื่อง

5.1.1 เป็นอุปกรณ์ Firewall ชนิด Next Generation Firewall แบบ Appliance

5.1.2 มี Application Firewall Throughput หรือ Next Generation Firewall Throughput ไม่น้อยกว่า 50 Gbps แบบ Appmix หรือ Enterprise testing condition หรือ Enterprise traffic mix

5.1.3 มี Threat prevention/protection Throughput ไม่น้อยกว่า 35 Gbps ในแบบ Appmix หรือ Enterprise testing condition หรือ Enterprise traffic mix

5.1.4 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) อย่างน้อย ดังนี้

5.1.4.1 ช่องเชื่อมต่อแบบ 10/100/1000 Base-T หรือ 1G/2.5G/5G/10G (RJ45) หรือดีกว่าไม่น้อยกว่า 8 ช่อง

5.1.4.2 ช่องเชื่อมต่อแบบ 1G/10G SFP/SFP+ หรือดีกว่า ไม่น้อยกว่า 8 ช่อง

5.1.4.3 ช่องเชื่อมต่อแบบ 10G/25G SFP+/SFP28 หรือดีกว่า ไม่น้อยกว่า 4 ช่อง

5.1.5 สามารถตรวจสอบและป้องกันการบุกรุกรูปแบบต่างๆ อย่างน้อย ดังนี้ Syn Flood, UDP Flood, ICMP Flood, IP Address Spoofing, Port Scan, DoS or DDoS, Teardrop Attack, Land Attack, IP Fragment, ICMP Fragment เป็นต้นได้

5.1.6 สามารถทำการกำหนด IP Address และ Service Port แบบ Network Address Translation (NAT) และ Port Address Translation (PAT) ได้

5.1.7 สามารถทำงานลักษณะ Transparent Mode หรือ Transparent Inline ได้

5.1.8 สามารถ Routing แบบ Static, Dynamic Routing หรือ Policy Based Forwarding หรือ Policy based Routing ได้

5.1.9 มี Power Supply แบบ Redundant หรือ Hot Swap จำนวนอย่างน้อย 2 หน่วย

5.1.10 สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS หรือ SSH ได้เป็นอย่างน้อย

5.1.11 สามารถเก็บและส่งรายละเอียดและตรวจสอบการใช้งาน (Logging/Monitoring) ในรูปแบบ Syslog ได้

5.1.12 สามารถใช้งานตามมาตรฐาน IPv6 ได้

5.1.13 มีช่องเชื่อมต่อเครือข่าย (Network Interface) สำหรับทำ HA แบบ 10G SFP+ หรือดีกว่า ไม่น้อยกว่า 2 ช่อง

5.1.14 มีช่องเชื่อมต่อเครือข่าย แบบ 1G/10G SFP/SFP+ หรือดีกว่าสำหรับการบริหารจัดการโดยเฉพาะ (Out of Band Management) ไม่น้อยกว่า 1 ช่อง

5.1.15 มี storage ชนิด SSD สำหรับจัดเก็บข้อมูลระบบ (System Storage) ขนาดไม่น้อยกว่า 480GB หรือดีกว่า

5.1.16 สามารถทำการตรวจสอบ (Inspection/Decryption) ทราฟฟิคที่เข้ารหัส SSL หรือ TLS หรือ HTTPS หรือนำเสนอระบบอื่นๆเพิ่มเติม เพื่อให้สามารถทำได้ตามข้อกำหนด

5.1.17 สามารถทำงานร่วมกับระบบการพิสูจน์ตัวตน (Authentication Systems) ได้แก่ Active Directory, LDAP, Radius ได้เป็นอย่างน้อย

5.1.18 สามารถกำหนดนโยบายการเข้าถึง website (URL Filtering) สามารถติดตามและควบคุมการเข้าถึงเว็บได้ตาม Category ที่กำหนดได้

5.1.19 มีระบบตรวจจับ Advanced Malware/Threat/Attack โดยใช้เทคโนโลยี Sandbox, AI, ML หรือเทียบเท่าได้

5.1.20 สามารถแสดงข้อมูลสรุปหรือรายงานในรูปแบบ graphic หรือ chart ได้เป็นอย่างน้อย

5.1.21 สามารถทำการเชื่อมต่ออุปกรณ์คอมพิวเตอร์เข้าสู่เครือข่ายทรัพยากรภายในองค์กรอย่างปลอดภัยผ่าน Virtual Private Network (VPN) ได้

5.1.22 สามารถตรวจจับและจำแนกแอปพลิเคชัน รวมถึงเนื้อหาที่ใช้งานบนเครือข่ายได้ เช่น Facebook, YouTube, Dropbox และ BitTorrent เป็นต้น

5.1.23 ตรวจจับภัยคุกคามหรือพฤติกรรมที่ไม่ปลอดภัยที่อาจแฝงมากับทราฟฟิกได้

5.1.24 รองรับการติดตั้งเพื่อทำ High Availability แบบ Active-Active และ Active-Passive ได้

5.1.25 อุปกรณ์ต้องได้รับรองมาตรฐาน FCC, VCCI และ UL เป็นอย่างน้อย

5.1.26 มีลิขสิทธิ์การใช้งานถูกต้องตามกฎหมายและรับประกันอุปกรณ์เป็นระยะเวลาอย่างน้อย 3 ปี

5.1.27 สามารถทำ SSL Decryption Broker หรือ Network Packet Broker ได้ เพื่อให้สามารถส่งทราฟฟิคที่ถอดรหัสแล้วไปยังอุปกรณ์อื่นแบบ Inline ได้ หรือนำเสนอระบบอื่นๆเพิ่มเติมเพื่อให้สามารถทำได้ตามข้อกำหนด

5.1.28 สามารถกำหนดนโยบายการเข้าถึง website (URL Filtering) สามารถติดตามและควบคุมการเข้าถึงเว็บได้ตาม Category, Block list, Allow list ที่กำหนดได้ และต้องมีการจัด category ให้กับแต่ละ website ไม่น้อยกว่า 2 category (Multi-Category URL Filtering) และสามารถตรวจจับและป้องกันการเข้าถึงเว็บไซต์ Phishing ที่ยังไม่เป็นที่รู้จักได้ (Unknown Phishing) หรือนำเสนอระบบอื่นๆเพิ่มเติม เพื่อสามารถทำได้ตามข้อกำหนด โดยมี Throughput ไม่น้อยกว่า Firewall Throughput

5.1.29 สามารถตรวจจับและป้องกันเว็บไซต์ Phishing โดยการใช้ AI ในการวิเคราะห์รูปภาพ (image) บนหน้าเว็บไซต์ เพื่อตรวจสอบการลอกเลียนแบบเว็บไซต์ รวมทั้งสามารถป้องกันการส่งข้อมูลการเข้าถึงระบบเครือข่ายของผู้ใช้งาน (User Credential) ขององค์กร ไปยังเว็บไซต์ดังกล่าวได้แบบ Real-time หรือนำเสนอระบบอื่นๆเพิ่มเติม เพื่อสามารถทำได้ตามข้อกำหนด โดยมี Throughput ไม่น้อยกว่า Firewall Throughput

5.1.30 มีระบบตรวจจับ Advanced Malware แบบ Cloud-Based และใช้เทคโนโลยีแบบ Sandbox , Machine Learning ทั้งในรูปแบบของ Static Analysis และ Dynamic Analysis ด้วยเทคนิคการทำ API Hooking, Behavioral analysis, Recursive analysis รวมทั้ง Intelligent Runtime Memory Analysis เพื่อใช้ระบุ Malware ประเภทใหม่ (Zero-day Malware) ซึ่งไม่มีในฐานข้อมูลการบุกรุกโจมตีได้ รวมถึงสามารถสร้างรูปแบบการโจมตี (Signature) ดังกล่าวขึ้นมาเพื่อใช้ป้องกันระบบเครือข่ายได้โดยอัตโนมัติ

หรือนำเสนอระบบอื่นๆเพิ่มเติม เพื่อสามารถทำได้ตามข้อกำหนด โดยมี Throughput ไม่น้อยกว่า Firewall Throughput

5.1.31 สามารถตรวจจับ, วิเคราะห์ และ ป้องกัน การเข้าถึง Malicious Domain ภายในองค์กรได้แบบ Real-time (DNS Security) โดยต้องมีการใช้ระบบ Machine Learning หรือ AI ในการตรวจจับ Domain ที่ผิดปกติ เช่น DGA Domain, DNS Tunneling, Fast Flux Domain, Dangling DNS Attacks, Wildcard DNS ในรูปแบบของการทำงานแบบ Inline Protection เป็นอย่างน้อย หรือนำเสนอระบบอื่นๆเพิ่มเติม เพื่อสามารถทำได้ตามข้อกำหนด โดยระบบที่นำเสนอจะต้องมี Throughput ไม่น้อยกว่า Firewall Throughput ของอุปกรณ์

5.1.32 ผลิตภัณฑ์ที่นำเสนอในโครงการต้องได้รับการจัดอันดับให้อยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant 2025 หรือ Forrester Wave for Firewall 2024 ในกลุ่มผลิตภัณฑ์ Enterprise Network Firewalls

6. ระยะเวลาการส่งมอบ

ผู้ยื่นข้อเสนอต้องดำเนินการส่งมอบอุปกรณ์ที่นำเสนอในโครงการนี้ ภายในระยะเวลา 120 วัน นับถัดจากวันที่ลงนามในใบสั่งซื้อ

7. การอบรม

ผู้ยื่นข้อเสนอต้องจัดอบรมการใช้งาน และการแก้ปัญหาเบื้องต้นของอุปกรณ์ที่นำเสนอ ให้กับผู้ดูแลระบบ สป.อว. จำนวนไม่น้อยกว่า 5 คน ณ สป.อว. (อาคารพระจอมเกล้า) โดยผู้ยื่นข้อเสนอต้องเป็นผู้รับผิดชอบค่าใช้จ่ายทั้งหมด ในการจัดหาเอกสารประกอบการอบรมแต่ละหลักสูตรให้กับ สป.อว.

8. การรับประกัน

8.1. ผู้ยื่นข้อเสนอต้องรับประกันความชำรุดบกพร่อง หรือการขัดข้องของอุปกรณ์ที่นำเสนอทั้งหมด ในกรณีที่เกิดปัญหาอุปกรณ์ชำรุดบกพร่องหรือใช้งานไม่ได้แบบ 7 วัน x 24 ชั่วโมง โดยทาง สป.อว. สามารถแจ้งปัญหาทาง E-mail หรือทางโทรศัพท์ หรือผ่านช่องทาง Chat หรือหนังสือราชการ

8.2. ผู้ยื่นข้อเสนอจะต้องดำเนินการตรวจสอบลักษณะปัญหาและแก้ไขปัญหาเบื้องต้นผ่านทางโทรศัพท์ หรือผ่านช่องทาง Chat หรือด้วยวิธีการ Remote Desktop ซึ่งหากการแก้ไขปัญหาเบื้องต้นไม่เป็นผลสำเร็จ จะต้องจัดให้มีเจ้าหน้าที่ ที่มีความเชี่ยวชาญและมีประสบการณ์เดินทางเข้ามาแก้ไขปัญหาดังกล่าว ณ สป.อว. (อาคารพระจอมเกล้า) ภายใน 4 ชั่งโมงตลอดอายุสัญญา

8.3. ผู้ยื่นข้อเสนอต้องติดตั้งเครื่องหมายแสดงการรับประกันซึ่งต้องระบุชื่อบริษัทผู้รับประกันและระยะเวลารับประกันพร้อมเบอร์โทรศัพท์ หรือ E-Mail ไว้อย่างชัดเจน

9. การปฏิบัติตามนโยบายด้าน ICT ของ สป.อว.

9.1. ผู้ยื่นข้อเสนอจะต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของ สป.อว. และขั้นตอนปฏิบัติต่าง ๆ ตามนโยบาย ISO27001 รวมถึงคำสั่งและวิธีปฏิบัติที่เกี่ยวข้องอย่างเคร่งครัด

9.2. ผู้ยื่นข้อเสนอต้องมีกระบวนการขั้นตอนการประเมินความเสี่ยงและการควบคุมความเสี่ยงอย่างน้อย 3 ประการ คือ การรักษาความปลอดภัยและความลับของระบบงานและข้อมูล (Confidentiality) ,ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล (Integrity) และความพร้อมใช้เทคโนโลยีสารสนเทศที่ใช้บริการ (Availability)

9.3. ผู้ยื่นข้อเสนอจะต้องปฏิบัติตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล และกฎหมายอื่นๆ ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล รวมถึงนโยบาย คำสั่ง ระเบียบที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลของ สป.อว. ไม่ว่าจะเป็นการใช้ ประมวลผล การเก็บรักษา ตลอดถึงการส่งคืน และทำลายข้อมูล

9.4. ผู้ยื่นข้อเสนอต้องมีแผนการตอบสนองหรือขั้นตอนการจัดการและการรายงานในกรณีที่เกิดเหตุการณ์ละเมิดต่อความปลอดภัยของข้อมูลส่วนบุคคล ซึ่งเป็นการเข้าถึง ทำลาย สูญหาย เปลี่ยนแปลง เปิดเผย โอน ได้ไปซึ่งความครอบครอง หรือการกระทำใดๆ ที่มีลักษณะเป็นการเข้าถึงหรือประมวลผลข้อมูลส่วนบุคคล โดยไม่ชอบด้วยกฎหมาย รวมถึงมาตรการในการบริหารจัดการที่เกี่ยวข้องกับการละเมิดข้อมูลส่วนบุคคล ทั้งนี้ในกรณีที่เกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ให้แจ้งให้ สป.อว. ทราบภายใน 24 ชั่วโมง นับแต่ทราบเหตุการณ์ละเมิดข้อมูลส่วนบุคคล พร้อมกับแนวทางการเยียวยาโดยไม่ชักช้า

10. การปกปิดความลับทางด้านข้อมูล (Non-disclosure agreement)

ผู้ยื่นข้อเสนอหรือเจ้าหน้าที่ของผู้ยื่นข้อเสนอจะต้องดำเนินการลงนามการปกปิดความลับทางด้านข้อมูล (Non-disclosure agreement) ให้กับสำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัย และนวัตกรรม สำหรับโครงการนี้ เพื่อเป็นการรักษาความลับทางด้านข้อมูลไม่ให้รั่วไหลสู่สาธารณะโดยไม่ได้รับอนุญาต

11. เอกสารส่งมอบ

11.1. ผู้ยื่นข้อเสนอต้องจัดส่งเอกสารส่งมอบงาน ดังต่อไปนี้

1) ผังภาพรวมของโครงสร้างการเชื่อมต่ออุปกรณ์ที่นำเสนอเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ (Logical Diagram and Rack Diagram) ของ สป.อว. (อาคารพระจอมเกล้า) ทั้งหมดในโครงการนี้ พร้อมระบุรายละเอียดกำกับแต่ละรายการในผังภาพให้ชัดเจน
2) เอกสารคู่มือการติดตั้งอุปกรณ์ที่นำเสนอ
3) รายละเอียดการกำหนดค่าการใช้งานอุปกรณ์ (System Configuration)
4) เอกสารสิทธิ์การใช้งาน (License) และบัญชีผู้ใช้งาน (Account) ในโครงการนี้ทั้งหมด

11.2. ในกรณีที่เอกสารส่งมอบ ประกอบไปด้วยข้อมูลที่สำคัญของหน่วยงาน อาทิเช่น หมายเลข IP address ,เอกสารการกำหนดการตั้งค่าอุปกรณ์ ,เอกสารลิขสิทธิ์ (License) ของอุปกรณ์ ,ข้อมูลส่วนบุคคล รวมถึงบัญชีและรหัสผ่านของผู้ใช้งานระบบสารสนเทศ เป็นต้น ทางผู้ยื่นข้อเสนอต้องจัดทำป้ายแสดงระดับชั้นความลับ ให้มีตราหรือเครื่องหมาย หรือชื่อขององค์กร และมีข้อความระบุว่า “Confidential” หรือคำว่า “ลับ” จำนวน 1 ชุดบนเอกสาร และจัดทำเอกสารรูปแบบเฉพาะที่ปิดบังข้อมูลที่สำคัญของหน่วยงาน โดยมีข้อความว่า “Internal Use” หรือคำว่า “ใช้ภายใน” จำนวน 1 ชุดบนเอกสาร ที่จะจัดส่งให้กับทาง สป.อว. (รวมทั้งหมด 2 ชุด) และข้อมูลแบบ Electronic File (USB) ซึ่งต้องทำการเข้ารหัสข้อมูล (Encrypted) เพื่อป้องกันการเข้าถึงข้อมูลที่สำคัญ โดยต้องมีข้อความระบุว่า “Confidential” หรือคำว่า “ลับ” บนเอกสารซองเอกสารทึบแสงที่ปิดผนึกเรียบร้อยนำส่งมอบให้กับทาง สป.อว. จำนวน 2 ชุด พร้อมดำเนินการส่งรหัสผ่านให้กับผู้ดูแลระบบผ่านทางช่องตามที่ สป.อว.เป็นผู้กำหนด ด้วยโปรแกรม WinZip หรือ WinRAR หรือ 7Zip เป็นต้น

12. งบประมาณ

วงเงินงบประมาณ 5,000,000 บาท (ห้าล้านบาทถ้วน)

13. หลักเกณฑ์การพิจารณา

โดยใช้เกณฑ์ราคาในการคัดเลือกที่เสนอราคาต่ำสุดเป็นผู้ชนะการซื้อหรือเป็นผู้ได้รับการคัดเลือก

14. เงื่อนไขการชำระเงิน

ทาง สป.อว. จะชำระเงินเต็มจำนวนมูลค่า เมื่อผู้ขายได้ส่งมอบงานและอุปกรณ์ในโครงการนี้ทั้งหมดแล้วเสร็จและคณะกรรมการได้ตรวจรับเรียบร้อยแล้ว

15. ค่าปรับ

หากผู้ขายไม่สามารถส่งมอบครุภัณฑ์ให้แล้วเสร็จตามเวลาที่กำหนดไว้ในใบสั่งซื้อผู้ขายจะต้องชำระค่าปรับให้แก่ทาง สป.อว. เป็นรายวันอัตราร้อยละ 0.20 (ศูนย์จุดสองศูนย์) ของราคาสิ่งของที่ยังไม่ได้รับมอบ

16. กำหนดยืนราคา 120 วัน

17. สถานที่ส่งมอบพัสดุ

สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม เลขที่ 75/47 ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพมหานคร โทร. 0 2333 3840

(นายทวีศักดิ์ นาเมืองรักษ์)	(นางสาวศุภกร สาระวงศ์)	(นายกิติศักดิ์ วงศ์ธานุวัฒน์)
นักวิชาการคอมพิวเตอร์ชำนาญการ	เจ้าหน้าที่ระบบงานคอมพิวเตอร์	เจ้าหน้าที่ระบบงานคอมพิวเตอร์
ผู้กำหนดคุณลักษณะเฉพาะ	ผู้กำหนดคุณลักษณะเฉพาะ	ผู้กำหนดคุณลักษณะเฉพาะ