ขอบเขตการดำเนินงาน (TOR)
การกำหนดคุณลักษณะ ราคากลาง และกำหนดหลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ
การจัดซื้อพร้อมติดตั้งระบบรักษาความปลอดภัยของเครือข่ายคอมพิวเตอร์ (Firewall) จำนวน 1 ระบบ
เป็นจำนวนเงิน 1,675,000 บาท
มหาวิทยาลัยราชภัฏพระนครศรีอยุธยา

1. ความต้องการทั่วไป

1.1. ผู้เสนอราคาต้องเป็นนิติบุคคลตามกฎหมายที่จดทะเบียนในประเทศไทย โดยมีวัตถุประสงค์ในการประกอบธุรกิจ เกี่ยวกับการค้า ระบบสื่อสาร หรือ ระบบคอมพิวเตอร์ หรือระบบโทรคมนาคมหรือที่เกี่ยวข้อง

1.2. ผู้เสนอราคาต้องเป็นบริษัทที่มีทุนจดทะเบียน ซึ่งมีมูลค่าไม่ต่ำกว่า 1,000,000 บาท

1.3. ผู้เสนอราคาต้องไม่เป็นผู้ที่ถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานของทางราชการและได้แจ้งเวียนชื่อแล้ว หรือไม่เป็นผู้ที่ได้รับผลของการสั่งให้นิติบุคคลหรือบุคคลอื่นเป็นผู้ทิ้งงานตามระเบียบของทางราชการ

1.4. ผู้เสนอราคาต้องไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้เสนอราคาได้มีคำสั่งให้สละสิทธิความคุ้มกันเช่นว่านั้น

1.5. ผู้เสนอราคาต้องเป็นบริษัทที่เคยมีผลงานด้าน การวางระบบเครือข่ายหรือระบบคอมพิวเตอร์หรือระบบเครือข่ายกล้องวงจรปิดแบบไอพี ซึ่งมีมูลค่าไม่น้อยกว่า 900,000 บาทจำนวนไม่น้อยกว่า 1 งาน และมีหลักฐานการจัดซื้อหรือจัดจ้าง เป็นสำเนาหนังสือรับรองผลงานหรือสำเนาคู่สัญญาแนบมาด้วย

1.6. เพื่อป้องกันสินค้านำเข้าอย่างผิดกฎหมายและการรับประกันสินค้า อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) ต้องมีเอกสารรับรองสินค้าและรับรองการการสนับสนุนข้อมูลทางเทคนิคและการสำรองอะไหล่ให้กับบริษัทที่ยื่นเสนอราคาสำหรับงานนี้โดยระบุเลขที่งาน ซึ่งออกโดยบริษัทผู้ผลิตหรือสาขาของผู้ผลิตภายในประเทศเพื่อประโยชน์ในการบริการหลังการขายและสำรองอะไหล่

1.7. ผู้เสนอราคาต้องเสนอรายละเอียดเอกสารทางเทคนิคของ อุปกรณ์ต่าง ๆ ที่ใช้ในการติดตั้งให้คณะกรรมการพิจารณา

1.8. ผู้ขายจะต้องรับประกันความชำรุดบกพร่องของอุปกรณ์เครือข่ายที่นำเสนอสำหรับงานที่เกิดขึ้นอันเนื่องจากการใช้งานตามปกติเป็นเวลาอย่างน้อย 1 ปี ในลักษณะ On - Site Support นับแต่วันที่ตรวจรับงานของหน่วยงาน

1.9. ภายในระยะเวลาดังกล่าว อุปกรณ์เครือข่ายที่นำเสนอ ชำรุดบกพร่องหรือใช้งานไม่ได้ทั้งหมดหรือแต่เพียงบางส่วน และความชำรุดบกพร่องนั้นมิใช่ความผิดของทางหน่วยงาน ผู้รับจ้างจะต้องจัดการซ่อมแซมแก้ไขให้อยู่ในสภาพใช้งานได้ดังเดิม นับแต่เวลาที่ได้รับแจ้งจากหน่วยงานฯ โดยไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้น จากหน่วยงาน

1.10. ในระหว่างการดำเนินการซ่อมแซมแก้ไขการชำรุดหรือขัดข้องของอุปกรณ์ผู้รับจ้างจะต้องจัดหาอุปกรณ์ที่มีคุณภาพเทียบเท่าอุปกรณ์ที่ชำรุดมาใช้งานทดแทนจนกว่า จะส่งคืนอุปกรณ์ที่นำไปซ่อมแซมแก้ไขแล้วเสร็จ

2. รายละเอียดและจำนวนครุภัณฑ์มีรายละเอียดดังนี้

2.1 อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) จำนวน 1 เครื่อง

<u>คุณลักษณะทางเทคนิค</u>

1. **อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) จำนวน 1 เครื่อง** มีรายละเอียดดังนี้
   - 1.1 เป็นอุปกรณ์ Firewall ชนิด Next Generation Firewall แบบ Appliance
   - 1.2 มี Firewall Throughput ไม่น้อยกว่า 30 Gbps
   - 1.3 มีช่องเชื่อมต่อเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T หรือดีกว่าจำนวนไม่น้อยกว่า 12 ช่อง และมีช่องสำหรับใส่ transceiver แบบ 25GE SFP28/10GE SFP+ ไม่น้อยกว่า 4 ช่อง พร้อมเสนอ Transceiver แบบ 10G SR มาครบทุกช่องและมีช่องสำหรับใส่ transceiver แบบ 40GE QSFP+ ไม่น้อยกว่า 2 ช่อง ได้ในอนาคต
   - 1.4 มี IPsec VPN Throughput ไม่น้อยกว่า 42 Gbps
   - 1.5 รองรับการสร้าง IPsec Tunnels แบบ Gateway to Gateway ได้อย่างน้อย 18,000 Tunnels และ แบบ Client to Gateway ได้อย่างน้อย 90,000 Tunnels
   - 1.6 มี Threat Protection Throughput ไม่น้อยกว่า 7 Gbps (เปิดใช้งาน Firewall, IPS, Application control และ Malware protection)
   - 1.7 ระบบที่เสนอสามารถทำ Two-Factor Authentication (2FA) กับการใช้งาน VPN ได้ในลักษณะ Mobile Token โดยมีลิขสิทธิ์การใช้งานเริ่มต้น 2 licenses เป็นอย่างน้อยหรือเสนอระบบเพิ่มเติมได้
   - 1.8 สามารถทำงานในลักษณะ Virtual Firewall ได้ 10 ระบบเป็นอย่างน้อย
   - 1.9 รองรับ Concurrent Session ได้อย่างน้อย 7,600,000 Sessionsและ New Sessions/Sec ได้อย่างน้อย 420,000 Sessions/Sec
   - 1.10 รองรับการทำ SSL Inspection Throughput ไม่น้อยกว่า 7 Gbps หรือมี SSL Inspection Concurrent/SSL Concurrent Decryption session ไม่น้อยกว่า 400,000 sessions
   - 1.11 สามารถควบคุม Application ใช้งานผ่าน WAN link ตามค่า SLA ที่กำหนดจาก Latency, Jitter, Packet loss ได้เป็นอย่างน้อย และสามารถทำ Fail-over link ได้แบบอัตโนมัติ หรือเสนอระบบเพิ่มเติมได้
   - 1.12 มีคุณสมบัติ DLP เพื่อตรวจจับไฟล์ และข้อมูลสำคัญ โดยกำหนดเงื่อนไขแบบ File Type, File Size, Regular Expression, ได้เป็นอย่างน้อย หรือเสนอระบบเพิ่มเติมได้
   - 1.13 สามารถตรวจสอบและป้องกันการบุกรุกรูปแบบต่าง ๆ อย่างน้อย ดังนี้ Syn Flood, UFlood, ICMP Flood, IP Address Spoofing, Port Scan, DoS or DDoS, Teardrop Attack, Land Attack,IP Fragment, ICMP Fragment เป็นต้นได้
   - 1.14 สามารถกำหนด IP Address และ Service Port แบบ Network Address Translation (NAT) และ Port Address Translation (PAT) ได้
   - 1.15 สามารถทำงานลักษณะ Transparent Mode ได้
   - 1.16 สามารถ Routing แบบ Static, Dynamic Routing ได้
   - 1.17 มี Power Supply แบบ Redundant หรือ มีคุณสมบัติ Hot Swap จำนวน 2 หน่วย
   - 1.18 สามารถบริหารจัดการอุปกรณ์ตามมาตรฐาน HTTPS หรือ SSH ได้เป็นอย่างน้อย
   - 1.19 สามารถทำ DNS Filtering หรือ DNS Security เพื่อป้องกันการ DNS request ไปยัง Botnet C&C domain และควบคุม DNS Safe search กับ search engine เช่น Google, Bing ได้หรือเสนอระบบเพิ่มเติมได้
   - 1.20 อุปกรณ์สามารถ Update Services ได้ IPS, Web Filtering, Sandbox Cloud, Antivirus และ Signature ได้ตลอดระยะเวลาของการรับประกัน

1.21 สามารถเก็บ และส่งรายละเอียด และตรวจสอบการใช้งาน (Logging/Monitoring) ในรูปแบบ Syslog ได้

1.22 สามารถใช้งานตามมาตรฐาน IPv6 ได้

1.23 แบรนด์ผลิตภัณฑ์ที่เสนอต้องอยู่ในกลุ่ม Recommended จาก NSS Labs ด้าน Next Generation Firewall (NGFW) ปี 2017- 2019

1.24 แบรนด์ผลิตภัณฑ์ที่เสนอต้องอยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant for Enterprise Network Firewalls ปี 2017-2018 และ Networks Firewall ปี 2019 หรือปีปัจจุบัน

1.25 อุปกรณ์ที่เสนอต้องเป็นของใหม่ ไม่เคยผ่านการใช้งานมาก่อนโดยมีหนังสือรับรองซึ่งออกโดยบริษัทผู้ผลิตหรือบริษัทสาขาในประเทศ ที่ใช้ชื่อบริษัทเดียวกับสินค้าที่เสนอราคาโดยระบุงาน

3. งานติดตั้งอุปกรณ์ป้องกันเครือข่าย มีรายละเอียดดังนี้

3.1 ผู้เสนอจะต้องออกแบบงานติดตั้งอุปกรณ์ป้องกันเครือข่ายที่เสนอโดยให้สามารถใช้งานร่วมกับระบบเดิมของหน่วยงานให้สามารถใช้งานได้อย่างมีประสิทธิภาพนำเสนอให้กับหน่วยงานเพื่ออนุมัติการติดตั้ง

4. การรับประกันผลงานและความชำรุดบกพร่อง มีรายละเอียดดังนี้

4.1 ผู้ขายจะต้องรับประกันการใช้งานของระบบงานที่เสนอ เป็นเวลาไม่น้อยกว่า 1 ปี นับถัดจากวันที่หน่วยงานได้ตรวจรับงานทั้งหมดแล้ว โดยต้องมีหน้าที่บำรุงรักษาและซ่อมแซมแก้ไข ให้อยู่ในสภาพที่ใช้งานได้ดีอยู่เสมอ

4.2 หน่วยงานหรือผู้แทนของหน่วยงาน อาจแจ้งปัญหา/ข้อผิดพลาดของระบบงาน สภาพของการชำรุดบกพร่องเบื้องต้นของระบบที่เสนอไปยังผู้ขายโดยทางโทรศัพท์ หรือโทรศัพท์เคลื่อนที่ หรือไปรษณีย์อิเล็กทรอนิกส์ (E-mail) ได้ทุกวันไม่เว้นวันหยุด และตลอด 24 ชั่วโมง และผู้ขายจะต้องตอบรับทราบภายใน 4 ชั่วโมง นับตั้งแต่เวลาที่ได้รับแจ้งโดยทางโทรศัพท์ โทรศัพท์เคลื่อนที่ หรือไปรษณีย์อิเล็กทรอนิกส์ (E-mail)

4.3 ผู้ขายจะต้องรับประกันความชำรุดบกพร่องของอุปกรณ์เครือข่ายที่นำเสนอสำหรับงานที่เกิดขึ้นอันเนื่องจากการใช้งานตามปกติเป็นเวลาอย่างน้อย 1 ปี ในลักษณะ On - Site Support นับแต่วันที่ตรวจรับงานของหน่วยงาน

4.4 ภายในระยะเวลาดังกล่าวอุปกรณ์เครือข่ายที่นำเสนอชำรุดบกพร่องหรือใช้งานไม่ได้ทั้งหมดหรือแต่เพียงบางส่วนและความชำรุดบกพร่องนั้นมิใช่ความผิดของทางหน่วยงานผู้รับจ้างจะต้องจัดการซ่อมแซมแก้ไขให้อยู่ในสภาพใช้งานได้ดังเดิมนับแต่เวลาที่ได้รับแจ้งจากหน่วยงานฯ โดยไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้นจากหน่วยงาน

4.5 ในระหว่างการดำเนินการซ่อมแซมแก้ไขการชำรุด หรือขัดข้องของอุปกรณ์ผู้รับจ้างจะต้องจัดหาอุปกรณ์ที่มีคุณภาพเทียบเท่าอุปกรณ์ที่ชำรุดมาใช้งานทดแทน จนกว่าจะส่งคืนอุปกรณ์ที่นำไปซ่อมแซมแก้ไขแล้วเสร็จ

5. ผู้เสนอราคาต้องแสดงตารางเปรียบเทียบคุณลักษณะที่มหาวิทยาลัยกำหนด และคุณลักษณะที่บริษัทเสนอพร้อมทั้งระบุว่าตรงกับแคตตาล็อกที่บริษัทเสนอข้อใดโดยทำเครื่องหมายกำกับในแต่ละข้อให้ชัดเจน

6. กำหนดส่งมอบพัสดุภายใน 90 วัน นับถัดจากวันที่ลงนามในสัญญา