ขอบเขตงาน (Terms of Reference : TOR)

อุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System) แบบที่ 2 จำนวน 1 เครื่อง

สำนักวิชาการศึกษาทั่วไปและนวัตกรรมการเรียนรู้อิเล็กทรอนิกส์

มหาวิทยาลัยราชภัฏสวนสุนันทา

โดยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding)

เจ้าของโครงการ

สำนักวิชาการศึกษาทั่วไปและนวัตกรรมการเรียนรู้อิเล็กทรอนิกส์

มหาวิทยาลัยราชภัฏสวนสุนันทา

ขอบเขตงาน (Terms of Reference : TOR)
อุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System) แบบที่ 2 จำนวน 1 เครื่อง
สำนักวิชาการศึกษาทั่วไปและนวัตกรรมการเรียนรู้อิเล็กทรอนิกส์
มหาวิทยาลัยราชภัฏสวนสุนันทา
โดยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding)

.....

1. เหตุผลและความจำเป็น

สืบเนื่องจากมหาวิทยาลัยมีนโนบายในการขับเคลื่อนการปรับรูปแบบการจัดการเรียนการสอน ส่งเสริมให้เกิดการเรียนรู้ตลอดชีวิต (Lifelong learning) เพื่อรองรับการพลิกโฉมฉับพลันและวิกฤตการณ์โลกโดยได้วิเคราะห์สถานการณ์ของโลก เพื่อเพิ่มศักยภาพในการสอนของอาจารย์และเพิ่มผลสัมฤทธิ์การเรียนรู้ของนักศึกษาให้สูงขึ้น โดยสำนักวิชาการศึกษาทั่วไปและนวัตกรรมการเรียนรู้อิเล็กทรอนิกส์ เป็นหน่วยงานที่ดำเนินงานจัดการเรียนการสอน หมวดวิชาศึกษาทั่วไป ได้มีการทบทวนรูปแบบและกระบวนการการจัดการเรียนการสอนของสำนักฯ เพื่อให้สอดรับกับนโยบายและทิศทางของมหาวิทยาลัย จึงได้มีการคิดการจัดการเรียน การสอนแบบ HyFlex Learning รูปแบบการเรียนรู้ที่ยืดหยุ่นต่อผู้เรียน โดยผู้เรียนสามารถเลือกรูปแบบของการเรียนรู้ได้ตามความต้องการในทุกช่องทาง ไม่ว่าจะเป็นรูปแบบการเรียนรู้แบบเผชิญหน้า ณ เวลาเดียวกัน หรือ Face-to-Face Driving โดยมีสองรูปแบบให้ผู้เรียนได้เลือกตามความเหมาะสมของตนเอง ประกอบไปด้วย เข้าเรียนในชั้นเรียนปกติ (On Site - Synchronous) หรือเลือกเข้าชั้นเรียนเสมือน (Online - Remote Asynchronous) หรือรูปแบบการเรียนรู้แบบวิดีโอตามประสงค์ (Video On Demand) เพื่อเพิ่มโอกาสทางการเรียนรู้ในการเข้าถึงข้อมูลและเอื้อต่อเรียนรู้ของตัวผู้เรียนเอง

ดังนั้นเพื่อให้แนวทางการจัดการเรียนการสอนของสำนักวิชาการศึกษาทั่วไปและนวัตกรรมการเรียนรู้อิเล็กทรอนิกส์เป็นไปด้วยความเรียบร้อย จึงขอจัดซื้ออุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System) แบบที่ 2 จำนวน 1 เครื่อง เพื่อรองรับการปฏิบัติงานด้านการจัดการเรียนการสอนและการปฏิบัติงานของเจ้าหน้าที่ภายในสำนักงานได้อย่างมีประสิทธิภาพ

2. วัตถุประสงค์

2.1 เพื่อจัดหาอุปกรณ์ป้องกันและตรวจจับการบุกรุก ให้มีความปลอดภัยต่อการใช้งานระบบเครือข่ายคอมพิวเตอร์ของสำนักวิชาการศึกษาทั่วไปฯ มากยิ่งขึ้น

2.2 เพื่อให้ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ของสำนักวิชาการศึกษาทั่วไปฯ มีเครื่องมือในการบริหารจัดการการรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ทันสมัยได้อย่างมีประสิทธิภาพ

2.3 เพื่อให้สำนักวิชาการศึกษาทั่วไปฯ มีระบบที่น่าเชื่อถือและเกิดความเชื่อมั่นต่อการใช้งานระบบเครือข่ายคอมพิวเตอร์ของสำนักงาน

3. คุณสมบัติผู้เสนอราคา

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีคุณลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้าง และการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นนิติบุคคลผู้มีอาชีพขายพัสดุที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้อื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่มหาวิทยาลัยราชภัฏสวนสุนันทา ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้ได้รับสิทธิ์เอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทยเว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

3.10 ผู้ยื่นข้อเสนอต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e-GP) ของกรมบัญชีกลาง ที่เว็บไซต์ศูนย์ข้อมูลจัดซื้อจัดจ้างภาครัฐ กรณีผู้เสนอราคายังมิได้ทำการลงทะเบียน ณ วันที่ยื่นขอเสนอจะต้องดำเนินการลงทะเบียนให้เรียบร้อยก่อนการทำสัญญาหรือข้อตกลง

3.11 คู่สัญญาต้องรับจ่ายเงินผ่านบัญชีฝากกระแสรายวัน เว้นแต่การรับจ่ายเงินแต่ละครั้ง ซึ่งมีมูลค่าไม่เกินสามหมื่นบาทคู่สัญญาอาจรับจ่ายเป็นเงินสดก็ได้

4. คุณลักษณะรายละเอียดของอุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System) แบบที่ 2 จำนวน 1 เครื่อง

1. เป็นอุปกรณ์ (Hardware Appliance) ที่ออกแบบมาให้สามารถทำหน้าที่ป้องกันการบุกรุกทางเครือข่าย (Intrusion Prevention System)

2. อุปกรณ์ที่เสนอต้องสามารถติดตั้งใน Rack มาตรฐาน 19" ขนาดความสูงไม่เกิน 1U ได้

3. สามารถใช้งานเป็น Next Generation Firewall ได้อย่างมีประสิทธิภาพโดยไม่ต้องมีอุปกรณ์หรือระบบภายนอก โดยเป็นผลิตภัณฑ์ที่ผ่านการทดสอบหรือถูกบรรจุอยู่ใน Magic Quadrant ของ Gartner ด้านอุปกรณ์ Network Firewall ปี ค.ศ. 2022 หรือใหม่กว่า ในส่วนของ Leaders หรือ Visionaries หรือ Challengers เป็นอย่างน้อย

4. เป็นผลิตภัณฑ์ที่ได้รับการรับรองหรือทดสอบจาก Cyber Ratings ระดับ “AAA” หรือ“Recommended” รวมกันได้ไม่น้อยกว่า 2 ปีติดต่อกัน

5. ต้องสามารถใช้งานเป็น Web Application Firewall (WAF) ได้ โดยอ้างอิงจาก OWASP Top 10 web application security risks เป็นอย่างน้อยโดยไม่ต้องมีอุปกรณ์หรือระบบภายนอก

6. มีความสามารถตรวจสอบการเปิดพอร์ต, ช่องโหว่และสแกนรหัสผ่านที่ไม่รัดกุมในการป้องกันแรนซัมแวร์ ช่วยให้ผู้ดูแลระบบสร้างนโยบายด้านความปลอดภัยเพื่อป้องกันแรนซัมแวร์

7. มีความสามารถในการตรวจสอบช่องโหว่ของ Web Application และ Vulnerability ในรูปแบบ Real-time ได้

8. อุปกรณ์ที่เสนอต้องสามารถเลือกการทำงานได้อย่างน้อยใน 5 โหมด ได้แก่ Passive และ/หรือ In-Line และ/หรือ Routed (Layer 3) และ/หรือ Transparent/Bridge (Layer 2) และ/หรือ Virtual Wire และ/หรือ Bypass และ/หรือ Hybrid

9. สามารถทำการกำหนด IP Address และ Service Port แบบ Network Address Translate (NAT) และ Port Address Translate (PAT) ได้เป็นอย่างน้อย

10. สามารถตรวจจับวิธีการบุกรุกและป้องกันเครือข่ายได้หลากหลายอย่างน้อยดังนี้

    10.1 Signature Matching หรือ Signature Based

    10.2 Anomalies ต่างๆ ได้แก่ Protocol หรือ Packet หรือ Statistical หรือ Application หรือ HTTP Anomalies ได้

    10.3 SQL Injection, Cross-site Scripting (XSS), Web Shells, Buffer Overflow และ Brute-force ได้

    10.4 Worm, Virus, Backdoor Program และ Spyware ได้

    10.5 Packet Analysis หรือ APT (Advance Persistent Threat) หรือ Threat ด้วยเทคโนโลยี Cloud Sandbox Threat Analysis โดยใช้ตรวจจับ Botnet, Remote Access Trojan และ Malware ได้

10.6 IP และ Port Scanning, Syn Flood, UDP Flood, DOS, DDOS, Teardrop Attack, Land Attack และ IP Fragment ได้

10.7 IP Address Spoofing หรือ ARP Spoofing ได้

10.8 Vulnerability Protection และ Content Security ได้

11. สามารถทำงานได้อย่างน้อย 3 Segment ใน IPS Mode และสามารถทำงานแบบ Virtual Domain ได้สูงสุดไม่น้อยกว่า 10 Virtual Domains

12. สามารถเลือกการทำ Routing แบบ Static และ Dynamic ได้

13. มีหน่วยจัดเก็บข้อมูลในตัวแบบ Solid State Disk (SSD) หรือดีกว่าขนาดไม่น้อยกว่า 250 GB (ก่อนการ Format)

14. มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) ดังนี้

14.1 แบบ 10 Gigabit Ethernet ที่มีช่องสำหรับติดตั้ง Module Transceiver แบบ SFP+ หรือดีกว่าจำนวนไม่น้อยกว่า 6 ช่อง

14.2 แบบ 10/100/1000 Base-T ที่มี Interface การเชื่อมต่อแบบ RJ-45 จำนวนไม่น้อยกว่า 16 ช่อง

14.3 มี Slot หรือ Interface I/O จำนวนไม่น้อยกว่า 2 ช่อง สำหรับใส่การ์ดเพื่อเพิ่มพอร์ตสำหรับเชื่อมต่อระบบเครือข่ายในอนาคตได้

15. มีค่า Firewall Throughput ไม่น้อยกว่า 30 Gbps

16. มีค่าความเร็วในการตรวจจับ IPS Throughput แบบ 64k HTTP ไม่น้อยกว่า 7 Gbps และแบบ Enterprise Mix ไม่น้อยกว่า 5 Gbps

17. มีค่าความเร็วในการตรวจจับ Threat Prevention (เปิดฟังก์ชั่นการทำงาน Firewall, Application Control, Bandwidth Management, IPS และ Antivirus ให้ทำงานพร้อมกัน) Throughput แบบ 64k HTTP ไม่น้อยกว่า 3.5 Gbps และแบบ Enterprise Mix ไม่น้อยกว่า 3 Gbps

18. มีค่าความเร็วในการตรวจจับด้าน Web Application Firewall (เมื่อเปิดฟังก์ชั่นการทำงาน Firewall, Application Control, Bandwidth Management, IPS และ WAF ให้ทำงานพร้อมกัน) Throughput แบบ 64k HTTP ไม่น้อยกว่า 3 Gbps และแบบ Enterprise Mix ไม่น้อยกว่า 1.5 Gbps

19. สามารถรับ Concurrent Connection ไม่น้อยกว่า 4,000,000 Connections และต้องสามารถรับ New Connections ไม่น้อยกว่า 180,000 per Second

20. เมื่ออุปกรณ์เกิดปัญหาสามารถทำงานได้อย่างต่อเนื่อง (Bypass Traffic) โดยช่องสัญญาณ In-Line Mode หรือ Hardware Bypass จำนวนไม่น้อยกว่า 4 คู่

21. มีความสามารถในการตรวจสอบภัยคุกคามการโจมตีของผู้ไม่ประสงค์ดี โดยวิธีการวางเหยื่อล่อ (Decoy) ให้เสมือนอยู่ในสภาพแวดล้อมจริง เพื่อทำการเบี่ยงเบนหรือลวงผู้ไม่ประสงค์ดีให้ทำการเข้ามาโจมตีเหยื่อล่อ (Decoy) โดยมีลักษณะการทำงานอย่างน้อยดังนี้

21.1 สามารถแสดงข้อมูล Attack Stage, Attack Trend, Attack IP, Threat Level และ Deception Service เป็นต้น

21.2 สามารถกำหนด Deception Service เช่น FTP, Web Logic, Jenkins, PostgreSQL, MS SQL, SSH, Telnet และ RDP เป็นต้น

22. สามารถตรวจสอบ Malware บน Protocol ได้แก่ HTTP, HTTPS, FTP, SMB, SMTP, POP3 และ IMAP ได้เป็นอย่างน้อย

23. รองรับการทำงาน SSL Decryption บน TLS 1.3 หรือสูงกว่า

24. มีฟังก์ชั่นให้ตัวอุปกรณ์ทำหน้าที่เป็น Security Operation Center หรือ SOC เพื่อตรวจสอบและแสดงภัยคุกคามต่อระบบงาน (Business System) และเครื่องลูกข่าย (Client) รวมถึงระดับความรุนแรง (Severity), ประเภทภัยคุกคาม (Threat Type) และขั้นตอนการโจมตี (Attack Stage) ได้เป็นอย่างน้อย

25. มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน 2 หน่วย

26. สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน Web Browser หรือ HTTPS หรือ SSH ได้เป็นอย่างน้อย

27. สามารถเก็บและส่งรายละเอียดและตรวจสอบการใช้งาน (Logging/Monitor) ในรูปแบบ Syslog ได้ โดยผู้เสนอราคามีหน้าที่ตั้งค่าให้ส่ง Log ไปยัง Log Server ของทางหน่วยงาน

28. สามารถใช้งานตามมาตรฐาน IPv6 ได้

29. มีการรับประกันผลิตภัณฑ์เป็นระยะเวลาไม่น้อยกว่า 5 ปี

30. สามารถปรับปรุงฐานข้อมูลและอัพเดตให้เป็นเวอร์ชั่นล่าสุดได้ตลอดการรับประกัน มีลิขสิทธิ์อย่างน้อยดังต่อไปนี้

30.1 ลิขสิทธิ์ในการใช้งานและการปรับปรุงฐานข้อมูลและอัพเดตเฟิร์มแวร์ของตัวอุปกรณ์

30.2 ลิขสิทธิ์ในการใช้งานและการปรับปรุงฐานข้อมูลและอัพเดต IPS (Intrusion Prevention System)

30.3 ลิขสิทธิ์ในการใช้งานและการปรับปรุงฐานข้อมูลและอัพเดต Antivirus หรือ Anti-Malware

30.4 ลิขสิทธิ์ในการใช้งานและการปรับปรุงฐานข้อมูลและอัพเดตการทำงาน Web Application Firewall

31. ผู้เสนอราคาต้องได้รับการแต่งตั้งเป็นตัวแทนจำหน่ายโดยตรงจากบริษัทฯ เจ้าของผลิตภัณฑ์หรือบริษัทฯ สาขาของเจ้าของผลิตภัณฑ์ประจำประเทศไทย สำหรับผลิตภัณฑ์ที่เสนอในโครงการนี้โดยเฉพาะ และให้การสนับสนุนผลิตภัณฑ์ดังกล่าวในการเสนอราคานี้ โดยเฉพาะโดยมีเอกสารหรือหลักฐานแสดง ณ วันยื่นเอกสารประกวดราคาอิเล็กทรอนิกส์ เพื่อรองรับการให้บริการทางเทคนิคและบริการหลังการขายเป็นอย่างดี ที่ระบุชื่อโครงการ ชื่อหน่วยงานมหาวิทยาลัยราชภัฏสวนสุนันทาที่ชัดเจนและเอกสารต้องมีอายุไม่เกิน 30 วันนับจากวันที่ออกเอกสารจนถึงวันที่ยื่นเสนอราคา

32. ผู้เสนอราคาต้องได้รับการสนับสนุนทางเทคนิคและการบริการหลังการขายตลอดระยะเวลาการรับประกันโดยตรงจากบริษัทฯ เจ้าของผลิตภัณฑ์หรือบริษัทฯ สาขาของเจ้าของผลิตภัณฑ์ประจำประเทศไทย สำหรับผลิตภัณฑ์ที่เสนอในโครงการนี้โดยเฉพาะ และให้การสนับสนุนผลิตภัณฑ์ดังกล่าวในการเสนอราคานี้โดยเฉพาะและต้องรับรองว่าผลิตภัณฑ์ที่นำเสนอในครั้งนี้ต้องเป็นของใหม่ ยังอยู่ในสายการผลิต และมีเงื่อนไขทางเทคนิคตรงตามเอกสารโบรชัวร์ต่างๆ โดยมีเอกสารหรือหลักฐานแสดง ณ วันที่ยื่นเอกสารประกวดราคาอิเล็กทรอนิกส์

5. ระยะเวลาในการดำเนินการ

ระยะเวลาดำเนินการ 90 วัน นับจากวันที่ลงนามในสัญญาซื้อ

6. วงเงินในการจัดหา

วงเงินงบประมาณอุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System) แบบที่ 2 จำนวน 1 เครื่อง จำนวนเงินงบประมาณ 1,400,000 บาท (หนึ่งล้านสี่แสนบาทถ้วน)

7. รายละเอียดการส่งมอบงาน

ส่งมอบงาน 90 วัน นับถัดจากวันที่ลงนามในสัญญาซื้อ

บริษัทผู้เสนอราคาจะต้องดำเนินการติดตั้งและส่งมอบอุปกรณ์ที่กำหนดไว้ตามคุณลักษณะเฉพาะให้ถูกต้องครบถ้วน รวมทั้งเอกสารที่ต้องใช้ในการประกอบการตรวจรับ พร้อมทั้งทดสอบอุปกรณ์ทั้งหมดให้แล้วเสร็จภายในระยะเวลา 90 วัน นับถัดจากวันที่ลงนามในสัญญา

8. เงื่อนไขการชำระเงิน

การชำระจ่าย 1 งวด ตามกรอบวงเงินงบประมาณที่จัดสรรงบประมาณ

จำนวนเงิน 1,400,000 บาท (หนึ่งล้านสี่แสนบาทถ้วน)

9. ค่าปรับ

หากผู้ขายไม่สามารถทำงานให้แล้วเสร็จได้ในเวลาที่กำหนดไว้ในสัญญาและผู้ซื้อยังมิได้บอกเลิกในสัญญา ผู้ขายต้องชำระค่าปรับให้แก่ผู้ซื้อเป็นจำนวนร้อยละ 0.20 นับถัดจากวันที่ครบกำหนดเวลาแล้วเสร็จของงานตามสัญญา หรือวันที่ผู้ซื้อขอขยายเวลาทำงานให้จนถึงวันที่ทำงานแล้วเสร็จจริง นอกจากนั้นผู้ขายยอมให้ผู้ซื้อเรียกค่าเสียหายอันเกิดขึ้นจากการที่ผู้ขายทำงานล่าช้าเฉพาะส่วนที่เกินกว่าจำนวนค่าปรับดังกล่าวได้อีกด้วย

10. การรับประกัน

ผู้ขายจะต้องรับประกันความชำรุดบกพร่องของสิ่งของที่ซื้อขายที่เกิดขึ้นภายในระยะเวลา ไม่น้อยกว่า 5 ปีนับถัดจากวันที่ได้รับอุปกรณ์ หากอุปกรณ์ชำรุดบกพร่องไม่สามารถทำงานได้ปกติ ผู้ขายต้องดำเนินการแก้ไขหรือต้องหาอุปกรณ์ยี่ห้อเดียวกันรุ่นเดียวกัน หรือสูงกว่ามาทดแทน โดยเร่งดำเนินการแก้ไขให้แล้วเสร็จภายใน 24 ชั่วโมง นับจากเวลาที่ได้รับความชำรุดบกพร่อง ยกเว้นเหตุอันควรจำเป็นต้องใช้ระยะเวลาในการแก้ไขมากขึ้นตามความเห็นของมหาวิทยาลัยฯ

11. สถานที่ติดต่อเพื่อขอทราบข้อมูลเพิ่มเติม

สำนักวิชาการศึกษาทั่วไปและนวัตกรรมการเรียนรู้อิเล็กทรอนิกส์
มหาวิทยาลัยราชภัฏสวนสุนันทา เลขที่ 1 ถนนอู่ทองนอก เขตดุสิต กรุงเทพฯ 10300
หมายเลขโทรศัพท์ 02-1651265

งานจัดซื้อครุภัณฑ์นี้ มหาวิทยาลัยราชภัฏสวนสุนันทาสงวนสิทธิ์จะก่อหนี้ผูกพัน เมื่อได้รับอนุมัติเงินประจำงวดหรือมีเงินงบประมาณเพียงพอ โดยผู้ประมูลงานได้ ไม่มีสิทธิ์เรียกร้องค่าเสียหายใด ๆ ทั้งสิ้น

ลงชื่อ ..... ประธานกรรมการ
(นางสาวน้ำทิพย์ กลีบบัวบาน)

ลงชื่อ ..... กรรมการ
(นายสุภาส อมรฉันทนากร)

ลงชื่อ ..... กรรมการและเลขานุการ
(นางสาวภัททิยา ตรัยที่พึ่ง)