ขอบเขตของงาน (Terms of Reference : TOR)

ชื่อรายการพัสดุ โครงการจัดหาการเช่าให้อุปกรณ์รักษาความปลอดภัยและป้องกันภัยคุกคามเว็บไซต์ (Web Application Firewall) มหาวิทยาลัยราชภัฏเพชรบุรี จำนวน 2 รายการ

1. ความเป็นมา

ศูนย์เทคโนโลยีดิจิทัล มหาวิทยาลัยราชภัฏเพชรบุรี เป็นหน่วยงานภาครัฐที่ได้นำระบบคอมพิวเตอร์มาช่วยอำนวยความสะดวกในการให้บริการแก่นักศึกษาแบบ Online และสนับสนุนการใช้งานด้านคอมพิวเตอร์ให้แก่บุคลากรภายในหน่วยงานของมหาวิทยาลัย ซึ่งการนำระบบเทคโนโลยีสารสนเทศเข้ามาประยุกต์ใช้งานภายในมหาวิทยาลัย ส่งผลให้เกิดการพัฒนาในรูปแบบต่างๆทั้งในแง่ของประสิทธิภาพและประสิทธิผลที่เกิดขึ้นไม่ว่าจะเป็น การขับเคลื่อนนวัตกรรมการเรียนรู้ให้แก่นักศึกษา การปฏิบัติงานของเจ้าหน้าที่ภายในมหาวิทยาลัย รวมไปถึงการให้บริการแก่ภาคประชาชน แต่สิ่งที่มาพร้อมกับเทคโนโลยีนั่นคือ ภัยคุกคามทางด้านไซเบอร์ ที่ปัจจุบันเพิ่มขึ้นอย่างรวดเร็ว ด้วยวิธีการหลากหลายรูปแบบ มีความซับซ้อนมากขึ้นและมีวัตถุประสงค์ที่แตกต่างกันไปไม่ว่าจะเป็นการทำลายระบบ (Destroy) , การขโมยข้อมูล (Data Theft) , การหลอกลวง (Phishing) และการเรียกค่าไถ่ (Ransomware) ซึ่งภัยคุกคามทางด้านไซเบอร์เหล่านี้ ได้สร้างความเสียหายและทำลายความมั่นคงต่อระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย ส่งผลกระทบโดยตรงต่อการดำเนินงานให้สอดคล้องกับวิสัยทัศน์และพันธกิจของศูนย์เทคโนโลยีดิจิทัล

การโจมตีเว็บไซต์ก็เป็นอีกรูปแบบหนึ่งที่ปัจจุบันหน่วยงานราชการหลายแห่งกำลังโดนโจมตี ทั้งในรูปแบบโจมตีทางไซเบอร์ที่มุ่งทำให้เว็บไซต์หรือบริการออนไลน์ไม่สามารถใช้งานได้ (DDos Attack) หรือการเจาะเข้าเว็บไซต์เพื่อขโมยข้อมูลสำคัญ เป็นต้น

อย่างไรก็ตามถึงแม้ศูนย์เทคโนโลยีดิจิทัลจะมีการนำระบบหรืออุปกรณ์รักษาความปลอดภัยทางด้านไซเบอร์เข้ามาใช้งานภายในมหาวิทยาลัยเพื่อป้องกันและปกป้องระบบเทคโนโลยีสารสนเทศจากภัยคุกคามทางด้านไซเบอร์ตามหลักการความมั่นคงปลอดภัยทางไซเบอร์ แต่ยังมีข้อจำกัดทางด้านความสามารถหรือศักยภาพในการเฝ้าระวัง วิเคราะห์ ตรวจจับ และตอบสนองต่อภัยคุกคามทางด้านไซเบอร์ที่เกิดขึ้นกับเว็บไซต์ของมหาวิทยาลัย ทำให้ศูนย์เทคโนโลยีดิจิทัลจำเป็นต้องมีการปรับปรุงเพิ่มเติมระบบรักษาความปลอดภัยทางด้านไซเบอร์ที่ป้องกันการบุกรุกเว็บไซต์ให้มีความทันสมัยมากขึ้นเพื่อการตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์ที่เกิดขึ้นได้อย่างมีประสิทธิภาพ

ศูนย์เทคโนโลยีดิจิทัล ในฐานะหน่วยงานที่มีบทบาทในการเป็นศูนย์กลางด้านเทคโนโลยีสารเทศและการสื่อสารของมหาวิทยาลัย จึงมีความจำเป็นต้องจัดหาเทคโนโลยีเพื่อมาช่วยเพิ่มความมั่นคง

..... กรรมการ .....กรรมการ .....กรรมการ.....กรรมการ

27 มี.ค. 2569

ปลอดภัยให้กับระบบเครือข่ายของมหาวิทยาลัยให้สามารถรองรับภัยคุกคามรูปแบบใหม่ๆได้อย่างประสิทธิภาพ

2. วัตถุประสงค์

2.1 จัดหาเช่าใช้อุปกรณ์รักษาความปลอดภัยและป้องกันภัยคุกคามเว็บไซต์ (Web Application Firewall) จำนวน 1เครื่อง

2.2 จัดหาเช่าใช้อุปกรณ์จัดเก็บข้อมูล (Log/Events) ระบบเครือข่าย จำนวน 1 เครื่อง

3. คุณสมบัติของผู้ยื่นข้อเสนอ

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วน ผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นนิติบุคคล ผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอราคารายอื่นที่เข้ายื่นข้อเสนอให้แก่มหาวิทยาลัย ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม ในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งสละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

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

..... กรรมการ .....กรรมการ .....กรรมการ.....กรรมการ

27 มี.ค. 2569

4. ขอบเขตของงาน

4.1 รายละเอียดคุณลักษณะ จัดหาการเช่าใช้อุปกรณ์รักษาความปลอดภัยและป้องกันภัยคุกคามเว็บไซต์ (Web Application Firewall) จำนวน 1 เครื่อง ระยะเวลา 12 เดือน โดยมีคุณสมบัติเฉพาะดังนี้

4.1.1 เป็นอุปกรณ์แบบ Appliance สำหรับทำหน้าที่เป็น Web Application Firewall (WAF) โดยเฉพาะ และไม่มีลักษณะเป็นคุณสมบัติส่วนหนึ่งของอุปกรณ์ Firewall หรือ อุปกรณ์ application delivery control โดยสามารถป้องกัน Web Application จากภัยคุกคามทางไซเบอร์ได้

4.1.2 สามารถทำงานได้โดยไม่จำกัดสิทธิ์ของจำนวน Application ที่ใช้งาน (Unlimited Application Licenses)

4.1.3 มีช่องการเชื่อมต่อระบบเครือข่าย (Network Interfaces) 10/100/1000 (RJ45) จำนวนไม่น้อยกว่า 4 พอร์ต และช่องใส่ Transceiver แบบ 1000BaseX (SFP) จำนวนไม่น้อยกว่า 4 ช่อง หรือดีกว่า

4.1.4 มีหน่วยเก็บข้อมูล Storage แบบ SSD ขนาด 480 GB จำนวนไม่น้อยกว่า 1 หน่วย

4.1.5 สามารถรองรับ Throughput ได้ไม่น้อยกว่า 500 Mbps และมีค่าความหน่วง (Latency) น้อยกว่า 5 ms

4.1.6 รองรับการใช้งานในลักษณะ Administrative Domains ได้ไม่น้อยกว่า 32 Domains

4.1.7 สามมารถป้องกันการโจมตีผ่านทางเว็บแอพพลิเคชั่นได้ตาม OWASP Top 10 รวมถึง Cross Site Scripting, SQL Injection, Cross Site Request Forgery และ Session Hijacking ได้เป็นอย่างน้อย

4.1.8 สามารถป้องกันการโจมตีผ่านทาง API ได้ เช่น XML and JSON protocol conformance, Machine Learning Based API Discovery and Protection และ Web Services Signatures เป็นต้น

4.1.9 มีคุณสมบัติรองรับการใช้งานด้านความปลอดภัย เช่น Protocol validation, Brute force protection, Cookie signing and encryption, Data Leak Prevention, DoS Prevention, Virtual Patching, Malware Detection และ Operating system intrusion signatures เป็นอย่างน้อย

4.1.10 มีความสามารถในการเฝ้าระวังการเปลี่ยนแปลงเว็บไซต์ (Web Defacement) และสามารถ restore website content จากส่วนที่ backup ไว้ ได้โดยอัตโนมัติ

4.1.11 มีความสามารถในการตรวจสอบ IP Reputation เพื่อป้องกัน Botnets, Spammers, Anonymous Proxies, Malicious Sources ได้

4.1.12 สามารถแสดงข้อมูลการโจมตีที่เกิดขึ้น (Geo IP Analytics) และตั้งค่าการป้องกันตามประเทศ (IP Address Geolocation) ได้

4.1.13 มีคุณสมบัติรองรับการใช้งานในรูปแบบ Reverse proxy, Inline Transparent, Span (Offline Sniffing) และ WCCP ได้เป็นอย่างน้อย4.1.14 สามารถตรวจสอบช่องโหว่ของเว็บแอพพลิเคชั่น (Vulnerability Scan) จากตัวอุปกรณ์ได้ และรองรับการทำงานร่วมกับ 3rd Party vulnerability scanner เช่น Acunetix, HP WebInspect, IBM AppScan, Qualys ได้เป็นอย่างน้อย

..... กรรมการ .....กรรมการ .....กรรมการ.....กรรมการ

27 มี.ค. 2569

4.1.15 สามารถทำรายงาน (Report) เป็นรายชั่วโมง รายวัน รายสัปดาห์ ได้เป็นอย่างน้อย โดยเลือกเป็นรูปแบบ PDF, HTML และ MS Word ได้เป็นอย่างน้อย

4.1.16 อุปกรณ์ที่เสนอต้องผ่านการรับรองมาตรฐานด้านความปลอดภัยจาก FCC, VCCI และ CE เป็นอย่างน้อย

4.1.17 ผลิตภัณฑ์ที่เสนอมีเครื่องหมายการค้าหรือระบบปฏิบัติการที่อยู่ในกลุ่มผู้นำ (Leader) ของ KuppinggerCole – Leadership Compass ด้าน Web Application Firewall ประจำปี 2024 หรือปีล่าสุด หรือ GigaOM - Application and API Security ประจำปี 2024 หรือปีล่าสุด

4.1.18 อุปกรณ์ต้องสามารถทำการปรับปรุงฐานข้อมูลภัยคุกคาม (Signature) เป็นระยะเวลา อย่างน้อย 1 ปี

4.1.19 ผู้เสนอราคาต้องได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่ายจากผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทย โดยให้ยื่นขณะเข้าเสนอราคา

4.2 รายละเอียดคุณลักษณะเฉพาะ จัดหาการเช่าใช้อุปกรณ์จัดเก็บข้อมูล (Logs/Events) ระบบเครือข่าย จำนวน 1 ระบบ ระยะเวลา 12 เดือน โดยมีคุณสมบัติเฉพาะดังนี้

4.2.1 เป็นอุปกรณ์ Hardware Appliance ที่สามารถเก็บรวบรวมเหตุการณ์ (Logs or Events) ที่เกิดขึ้นบนอุปกรณ์รักษาความปลอดภัยและป้องกันภัยคุกคามเว็บไซต์ (Web Application Firewall) ที่เสนอมาในโครงการนี้ได้และอยู่ภายใต้เครื่องหมายการค้าเดียวกันกับอุปกรณ์รักษาความปลอดภัยและป้องกันภัยคุกคามเว็บไซต์ (Web Application Firewall) ที่เสนอ

4.2.2 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 1 GE จำนวนไม่น้อยกว่า 4 พอร์ต

4.2.3 มี Storage ขนาด 7 TB และต้องสามารถจัดเก็บข้อมูลจารจรทางคอมพิวเตอร์ (Log) ได้ไม่น้อยกว่า 90 วัน

4.2.4 มีอัตราความสามารถในการจัดเก็บข้อมูลเพื่อวิเคราะห์ได้ไม่น้อยกว่า 3,500 Logs/Events persecond และสามารถรองรับจำนวน log ได้ไม่น้อยกว่า 150 GB ต่อวัน

4.2.5 สามารถแสดงข้อมูล Log เช่น Date, Time, Source IP, User, Destination IP และ Services ได้เป็นอย่างน้อย

4.2.6 มีรูปแบบรายงาน (Report templates) มาให้อย่างน้อย 30 รูปแบบ และสามารถแสดงรายงานในรูปแบบของ PDF, HTML และ CSV ได้เป็นอย่างน้อย

4.2.7 อุปกรณ์ต้องสามารถทำการปรับปรุงระบบปฏิบัติการ (Firmware) ได้เป็นระยะเวลาอย่างน้อย 1 ปี

5. กำหนดเวลาส่งมอบงาน

กำหนดเวลาส่งมอบงานแล้วเสร็จภายใน 90 วัน นับถัดจากวันลงนามในสัญญา

..... กรรมการ .....กรรมการ .....กรรมการ.....กรรมการ

27 มี.ค. 2569

6. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

ในการการพิจารณาคัดเลือกข้อเสนอครั้งนี้ มหาวิทยาลัยจะพิจารณาตัดสินโดยใช้หลักเกณฑ์ ราคา

7. วงเงินงบประมาณ 1,800,000 (หนึ่งล้านแปดแสนบาทถ้วน)

8. งวดงานและการจ่ายเงิน

มหาวิทยาลัยจะจ่ายเงินชำระให้แก่ผู้รับจ้างจำนวน 1 งวด เป็นจำนวนเงินร้อยละ 100 ของค่าจ้างซึ่งได้รวมภาษีมูลค่าเพิ่มตลอดจนภาษีอากรอื่นๆ และค่าใช้จ่ายทั้งปวงแล้ว เมื่อผู้รับจ้างส่งมอบงานดังกล่าวถูกต้องและครบถ้วนตามสัญญาให้กับมหาวิทยาลัย

9. อัตราค่าปรับ

ผู้รับจ้างต้องดำเนินการตามของเขตงานและเงื่อนไขที่กำหนดไว้ในสัญญา ในกรณีที่เกิดความล่าช้าอันเนื่องจากการกระทำของผู้รับจ้างเป็นเหตุให้การส่งมอบล่าช้ากว่าระยะเวลาที่กำหนดในสัญญาผู้รับจ้างจะต้องชดใช้ค่าปรับให้กับผู้ว่าจ้าง ในอัตราร้อยละ 0.1 ของวงเงินค่างานจ้าง นับถัดจากวันครบกำหนดตามสัญญาจนถึงวันที่ผู้รับจ้างส่งมอบให้แก่ผู้ซื้อจนถูกต้องครบถ้วนตามสัญญา

10. การรับประกันความชำรุดบกพร่อง

ผู้รับจ้างต้องรับประกันความชำรุดบกพร่องเป็นเวลา 1 ปี นับแต่วันที่มหาวิทยาลัยฯ ได้รับมอบพัสดุภายในกำหนดเวลาดังกล่าว หากสิ่งของเกิดชำรุดบกพร่อง หรือขัดข้องผู้รับจ้างจะต้องจัดการซ่อมแซม แก้ไขให้อยู่ในสภาพใช้การได้ดีดังเดิม หรือนำอุปกรณ์ทดแทนที่มีคุณสมบัติเทียบเท่าหรือดีกว่ามาติดตั้ง เพื่อให้ระบบสามารถกลับมาใช้งานได้ตามปกติภายในวันทำการถัดไป หรือภายในเวลาไม่เกิน ภายใน 24 ชั่วโมง นับแต่วันที่ได้รับแจ้งจากมหาวิทยาลัยฯ โดยไม่คิดค่าใช้จ่ายใดๆทั้งสิ้น

11. อื่น ๆ

11.1 ผู้รับจ้างต้องรับผิดชอบในการติดตั้ง ตั้งค่า และดำเนินการปรับจูนระบบร่วมกับเจ้าหน้าที่ของมหาวิทยาลัย เพื่อให้ระบบ Web Application Firewall สามารถป้องกันภัยคุกคามได้อย่างมีประสิทธิภาพสูงสุดและลดผลกระทบของการบล็อกผู้ใช้งานปกติที่ผิดพลาด

..... กรรมการ .....กรรมการ .....กรรมการ.....กรรมการ

27 มี.ค. 2569

11.2 ผู้รับจ้างต้องจัดการถ่ายทอดเทคโนโลยีหรือฝึกอบรมการใช้งาน การตั้งค่าระบบ และการออกรายงานเบื้องต้น ให้กับบุคลากรของมหาวิทยาลัยราชภัฏเพชรบุรี จำนวนไม่น้อยกว่า 1 วันทำการ

11.3 เมื่อสิ้นสุดสัญญาเช่าใช้ 12 เดือน ผู้รับจ้างต้องดำเนินการลบและทำลายข้อมูลจราจรทางคอมพิวเตอร์ (Log) และการตั้งค่าของมหาวิทยาลัยที่ค้างอยู่ในอุปกรณ์ทั้งหมด และต้องส่งมอบหนังสือรับรองการทำลายข้อมูลอย่างปลอดภัยให้แก่มหาวิทยาลัยก่อนนำอุปกรณ์กลับคืน

11.4 กรณี Web Application Firewall ไม่ทำงาน Web Server ยังคงทำงานได้ปกติ ไม่ส่งผลกระทบต่อการทำงานของ Web Server

..... กรรมการ .....กรรมการ .....กรรมการ.....กรรมการ

27 มี.ค. 2569