**ประกาศคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่**

**เรื่อง การกำหนดหัวข้อร่างขอบเขตของงาน (TOR)**

**รายการ ระบบป้องกันการบุกรุกทางเครือข่ายคอมพิวเตอร์ จำนวน ๑ ระบบ**

---

**๑. ความเป็นมา**

การขยายตัวในการใช้งานระบบสารสนเทศทางด้านต่าง ๆ ของคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่นับวันยิ่งทวีความสำคัญยิ่งขึ้นอันเนื่องมาจากความสะดวก รวดเร็ว สืบค้นข้อมูลย้อนหลังได้ง่าย รวมถึงการลดระยะเวลาทำงานโดยรวม แต่ทั้งนี้การเตรียมตัวเพื่อรับมือกับภัยคุกคามทางระบบเครือข่ายคอมพิวเตอร์ก็ยังต้องทำพร้อม ๆ กันไปเพื่อเป็นการรับประกันว่าสนเทศที่ใช้งานในระบบมีความปลอดภัยเพียงพอตามมาตรฐานและตามสมควร

**๒. วัตถุประสงค์ในการใช้งานของโครงการ**

๒.๑ เพื่อทดแทนระบบป้องกันการบุกรุกทางเครือข่าย (Firewall) เดิมซึ่งมีขีดความสามารถจำกัด

๒.๒ เพื่อรองรับมาตรฐานของระบบการรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ให้เป็นไปตามมาตรฐานสากล

**๓. คุณสมบัติของผู้เสนอราคา**

๓.๑. เป็นนิติบุคคลที่จดทะเบียนเพื่อประกอบกิจการในระบบที่เสนอ มีทุนจดทะเบียนไม่น้อยกว่า ๓ ล้านบาท และจดทะเบียนมาแล้วไม่น้อยกว่า ๕ ปี

๓.๒. มีหนังสือรับรองอย่างเป็นทางการ ในการสนับสนุนทางเทคนิค และสำรองอะไหล่อย่างน้อย ๕ ปี จากบริษัทเจ้าของผลิตภัณฑ์ หรือบริษัทสาขาของบริษัทผู้ผลิตฯ ที่ประจำในประเทศไทย ซึ่งออกให้สำหรับโครงการนี้

๓.๓ ไม่เป็นผู้ที่ถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานของทางราชการและได้แจ้งเวียนชื่อแล้ว

๓.๔ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้เสนอราคาได้มีคำ สั่งให้สละสิทธิ์ความคุ้มกันเช่นว่านั้น

๓.๕ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้เสนอราคารายอื่นที่เข้าเสนอราคาให้แก่มหาวิทยาลัย และไม่เป็นผู้มีผลประโยชน์ร่วมกันระหว่างผู้เสนอราคากับผู้ให้บริการตลาดกลางอิเล็กทรอนิกส์ ณ วันประกาศประมูลซื้อด้วยระบบอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรมในการประมูลซื้อด้วยระบบอิเล็กทรอนิกส์

๓.๖ ต้องเป็นผู้ปฏิบัติตามประกาศคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ เรื่อง หลักเกณฑ์และวิธีการจัดทำและแสดงบัญชีรายการรับจ่ายของโครงการที่บุคคลหรือนิติบุคคลเป็นคู่สัญญากับหน่วยงานของรัฐ พ.ศ.๒๕๕๔ ดังนี้

๓.๖.๑ บุคคลหรือนิติบุคคลที่จะเข้าเป็นคู่สัญญาต้องไม่อยู่ในฐานะเป็นผู้ไม่แสดงบัญชีรายรับรายจ่ายหรือแสดงบัญชีรายรับรายจ่ายไม่ถูกต้องครบถ้วนในสาระสำคัญ

๓.๖.๒ บุคคลหรือนิติบุคคลที่จะเข้าเป็นคู่สัญญากับหน่วยงานของรัฐซึ่งได้ดำเนินการจัดซื้อจัดจ้างด้วยระบบอิเล็กทรอนิกส์ (e-Government Procurement : e-GP) ต้องลงทะเบียนในระบบอิเล็กทรอนิกส์ของกรมบัญชีกลางที่เว็บไซต์ศูนย์ข้อมูลจัดซื้อจัดจ้างภาครัฐ

๓.๖.๓ คู่สัญญาต้องรับจ่ายเงินผ่านบัญชีเงินฝากกระแสรายวัน เว้นแต่การรับจ่ายเงินแต่ละครั้ง ซึ่งมีมูลค่าไม่เกินสามหมื่นบาทคู่สัญญาอาจรับจ่ายเป็นเงินสดก็ได้

**๔. แบบรูปรายการ หรือคุณลักษณะเฉพาะ**
**ซึ่งมีคุณสมบัติทางเทคนิคขั้นต่ำหรือเทียบเท่า ดังต่อไปนี้**

**๔.๑. ระบบควบคุมและกำหนดนโยบายการเข้าถึงระบบเครือข่าย**
(Network Access Control) **จำนวนไม่น้อยกว่า ๑ ระบบ**
**มีคุณลักษณะเฉพาะขั้นต่ำอย่างน้อยดังต่อไปนี้**

๔.๑.๑. มีโครงสร้างเป็น Appliance ที่ได้รับการออกแบบมาโดยเฉพาะ สามารถตรวจจับและควบคุมเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่มาเชื่อมต่อกับระบบเครือข่ายพร้อมกันได้ไม่น้อยกว่า ๒,๕๐๐ ชุดภายในเวลาเดียวกัน

๔.๑.๒. มีพอร์ตสามารถรองรับการเชื่อมต่อกับเครือข่ายแบบ ๑๐/๑๐๐/๑๐๐๐Base-T จำนวนไม่น้อยกว่า ๔ พอร์ต โดยสามารถทำหน้าที่ตรวจจับพฤติกรรมที่น่าสงสัยจากการ SPAN Network Traffic มาที่อุปกรณ์ NAC และรองรับมาตรฐาน ๘๐๒.๑Q

๔.๑.๓. สามารถรองรับการเชื่อมต่อและควบคุมป้องกันการบุกรุกระบบเครือข่ายได้อย่างน้อย ๔๐๙๖ VLANs

๔.๑.๔. รองรับการทำงานแบบ Active / Standby ได้

๔.๑.๕. สามารถทำหน้าที่เป็น IPS ได้

๔.๑.๖. ป้องกันการโจมตีแบบ ARP Spoofing หรือทำงานร่วมกับ Switch โดยสามารถทำ Quarantine VLAN ได้

๔.๑.๗. อุปกรณ์สามารถทำงานได้ในแบบ Agentless เป็นอย่างน้อย โดยสามารถทำการ Allow, Deny Traffic ต่างๆ ตาม Source IP/Port, Destination IP/Port และทำ HTTP Redirection หรือ ทำงานร่วมกับ Switch ที่รองรับ ๘๐๒.๑X และ ACL (Access Control List) เพื่อให้ง่ายต่อการติดตั้ง และควบคุมการเข้าถึงข้อมูลของผู้ใช้งานและอุปกรณ์ต่างๆ

๔.๑.๘. ตรวจสอบการโจมตีของเครื่องคอมพิวเตอร์ที่ติด Virus หรือ Worm ทางเครือข่าย แล้วหยุดการโจมตีได้ โดยไม่จำเป็นมีการ Update Virus/ Worm signature หรือมี NAC Agent ในการช่วยควบคุมและเฝ้าระวังเครื่องคอมพิวเตอร์ที่ติด Virus หรือ Worm ทางเครือข่าย

๔.๑.๙. มีความสามารถในการให้บริการ Web Login แก่ผู้ใช้งานในระบบโดยทำงานร่วมกับอุปกรณ์เชื่อมต่อภายในเครือข่าย เพื่อทำการยืนยันตัวตนก่อนใช้งานได้ โดยตรวจสอบความถูกต้องของข้อมูลผู้ใช้งานผ่านทาง Directory Service เช่น LDAP หรือ Active Directory ได้

๔.๑.๑๐. สามารถทำ Certificate-based Authentication ได้ โดยมี Built-in CA ภายในระบบ NAC ที่นำเสนอ

๔.๑.๑๑. สามารถควบคุม Guest ได้ โดยมี Portal สำหรับให้ Guest ทำการลงทะเบียนด้วยตนเองได้

๔.๑.๑๒. สามารถกำหนด Policy การใช้งานของเครื่องคอมพิวเตอร์ในเครือข่ายได้

๔.๑.๑๓. รองรับการทำงานร่วมกับมาตรฐาน ๘๐๒.๑X ได้

๔.๑.๑๔. มีวิธีการในการหยุดการใช้งานเครือข่ายของเครื่องคอมพิวเตอร์ที่สร้างปัญหาในระบบเครือข่ายได้ หรือมี NAC Agent ในการช่วยควบคุมและเฝ้าระวังเครื่องคอมพิวเตอร์ที่สร้างปัญหาในระบบเครือข่าย

๔.๑.๑๕. รองรับการควบคุมฟังก์ชั่นพื้นฐานของ Switch ได้แก่ การสั่ง Shutdown Port และการเปลี่ยน VLAN ได้

๔.๑.๑๖. สามารถควบคุมการใช้งานระบบเครือข่ายของผู้ใช้งานแบบ Real time ได้ โดยไม่จำเป็นต้องสร้าง Policy ใหม่ หรือมี NAC Agent ในการช่วยควบคุมและเฝ้าระวังเครื่องคอมพิวเตอร์

๔.๑.๑๗. สามารถสร้าง Virtual Firewall ได้เป็นอย่างน้อย หรือรองรับการทำงานร่วมกับ Switch ผ่าน ACL (Access Control List)

๔.๑.๑๘. สามารถทำระบบประกาศข่าวสารแก่ผู้ใช้งานได้ หรือมีระบบ Notification/Alerting ผ่านทาง Email

๔.๑.๑๙. สามารถตรวจสอบการใช้งานโปรแกรม Anti Virus ในเครื่องคอมพิวเตอร์ของผู้ใช้งาน และกำหนดให้มีการ Update ฐานข้อมูลของโปรแกรม Anti Virus ได้

๔.๑.๒๐. สามารถ Scan หาจุดบกพร่องของเครื่องคอมพิวเตอร์ภายในเครือข่าย เพื่อแจ้งเตือนให้ทำการ Update Patch ของระบบปฏิบัติการได้

๔.๑.๒๑. ระบบ Dashboard สามารถแสดงข้อมูลได้อย่างน้อยดังต่อไปนี้

- ๔.๑.๒๑.๑. System Summary
- ๔.๑.๒๑.๒. Endpoint Compliance Issues
- ๔.๑.๒๑.๓. Application by Category
- ๔.๑.๒๑.๔. Network Authentications
- ๔.๑.๒๑.๕. Managed Devices
- ๔.๑.๒๑.๖. Discovered Devices
- ๔.๑.๒๑.๗. Vulnerability by Severity
- ๔.๑.๒๑.๘. Vulnerability by Category
- ๔.๑.๒๑.๙. Indicators of Compromise

๔.๑.๒๒. สามารถตรวจสอบการใช้งาน USB Thumb Drive ได้ และสามารถหยุดยั้งไม่ให้ข้อมูลภายใน Thumb Drive นั้นเข้าสู่ระบบได้ หรือมี NAC Agent ที่สามารถตรวจจับการใช้งาน USB Thumb Drive

๔.๑.๒๓. สามารถตรวจสอบการใช้งานโปรแกรมประเภท Chat และ Peer-to-Peer ได้

๔.๑.๒๔. เมื่ออุปกรณ์มีปัญหาหรือไม่สามารถใช้งานได้ จะต้องสามารถ Bypass เพื่อให้ผู้ใช้สามารถใช้งานระบบเครือข่ายได้โดยอัตโนมัติ

๔.๑.๒๕. สามารถตรวจจับและควบคุมอุปกรณ์เครือข่ายแบบเคลื่อนที่ (Mobile Device) ที่เชื่อมต่อเข้ามาในระบบเครือข่ายแบบ real-time ได้ และสามารถจำแนกชนิดของอุปกรณ์ เช่น iPhone/iPad, Blackberry, Android และ Windows ได้

๔.๑.๒๖. สามารถแสดงรายการของแอพพลิเคชั่นที่ติดตั้งในระบบ (Android และ IOS) ได้ และสามารถทำการลบหรือติดตั้งแอพพลิเคชั่นเพิ่มเติมได้จากการบริหารจากส่วนกลาง

๔.๑.๒๗. มีหน้าจอ GUI ที่สามารถแสดงข้อมูลต่างๆ ของผู้ใช้งาน และ Policy ที่ถูกใช้กับผู้ใช้งานทุกคนพร้อมกันได้

๔.๑.๒๘. สามารถแสดงรายงานในรูปแบบของ PDF และ HTML ได้

๔.๑.๒๙. มีความสามารถในการส่ง remote log กับระบบ syslog ได้

๔.๑.๓๐. มีความสามารถในการส่ง e-mail เพื่อแจ้งเตือนผู้ดูแลระบบได้

๔.๑.๓๑. ได้รับการรับรองมาตรฐานความปลอดภัย Common Criteria EAL๔+ หรือเป็นผลิตภัณฑ์ที่อยู่ใน Gartner Market Guide for NAC ปี ๒๐๑๗ เป็นอย่างน้อย

๔.๑.๓๒. อุปกรณ์มีขนาดมาตรฐาน สามารถติดตั้งในตู้ RACK ขนาด ๑๙ นิ้ว

๔.๑.๓๓. มี Redundant Power Supply

๔.๑.๓๔. ผู้เสนอราคามีหนังสือรับรองจากเจ้าของผลิตภัณฑ์ หรือสาขาประจำประเทศไทยของผู้ผลิตโดยตรง ว่าอุปกรณ์ที่เสนอในโครงการนี้เป็นของใหม่ ยังอยู่ในสายการผลิต และยินดีสนับสนุนด้านเทคนิคและบริการหลังการขาย

**๔.๒. อุปกรณ์ป้องกันและรักษาความปลอดภัยทางเครือข่าย (Firewall) สำหรับ Demilitarized Zone (DMZ) จำนวนไม่น้อยกว่า ๑ ชุด มีคุณลักษณะเฉพาะขั้นต่ำอย่างน้อยดังต่อไปนี้**

๔.๒.๑. เป็นอุปกรณ์ Appliance ซึ่งได้รับการออกแบบมาเพื่อทำหน้าที่รักษาความปลอดภัยของเครือข่ายโดยเฉพาะ

๔.๒.๒. มีพอร์ต ๑๐ Gigabit Ethernet แบบ SFP+ ไม่น้อยกว่า ๖ พอร์ต หรือดีกว่า

๔.๒.๓. มีพอร์ต Gigabit Ethernet แบบ RJ๔๕ ไม่น้อยกว่า ๓๐ พอร์ต หรือดีกว่า

๔.๒.๔. มีพอร์ต Gigabit Ethernet แบบ RJ๔๕ สำหรับ Management หรือ HA ไม่น้อยกว่า ๒ พอร์ต

๔.๒.๕. มีความเร็วในการทำงานของ Firewall Throughput ที่ ๖๔ bytes ได้ไม่ต่ำกว่า ๕๐ Gbps หรือดีกว่า และได้รับการรองรับตามมาตรฐานของ ICSA ด้าน Firewall

๔.๒.๖. สามารถรองรับการเชื่อมต่อพร้อมๆกัน (concurrent Sessions) ได้ไม่น้อยกว่า ๑๖,๐๐๐,๐๐๐ การเชื่อมต่อ หรือดีกว่า และรองรับการเชื่อมต่อใหม่ (New Sessions / Second) ได้ด้วยความเร็วไม่ต่ำกว่า ๔๐๐,๐๐๐ การเชื่อมต่อ (sessions) ต่อวินาที หรือดีกว่า

๔.๒.๗. มีความสามารถในการตรวจจับและป้องกันไวรัสคอมพิวเตอร์ในโปรโตคอล FTP, HTTP, IMAP, IMAPS, POP๓, POP๓S, SMTP และ SMTPS และต้องสามารถ update ฐานข้อมูลไวรัสฯ (virus signature) ผ่านเครือข่าย Internet ได้เองโดยอัตโนมัติตลอดระยะของการรับประกันอุปกรณ์ และได้รับการรองรับตามมาตรฐานของ ICSA ด้าน Anti Virus

๔.๒.๘. มีความสามารถในการป้องกันการบุกรุก (Intrusion Prevention) ได้ไม่น้อยกว่า ๑๐ Gbps หรือดีกว่า (Enterprise MIX Traffic) โดยสามารถ update ฐานข้อมูลการบุกรุก (attack signature) ผ่านเครือข่าย Internet ได้เองโดยอัตโนมัติตลอดระยะของการรับประกัน และได้รับการรองรับตามมาตรฐานของ ICSA ด้าน IPS

๔.๒.๙. สามารถเข้ารหัสเพื่อการส่งข้อมูลด้วยวิธีการ VPN โดยมีใช้วิธีการเข้ารหัสแบบ ๓DES/AES IPSec และ SSL-VPN เพื่อความปลอดภัยในการติดต่อจากระยะไกลได้

๔.๒.๑๐. สามารถทำ IPSec VPN โดยมีความเร็วในการทำงาน IPSec VPN ได้ไม่ต่ำกว่า ๔๐ Gbps หรือดีกว่า และ VPN Gateway-to-Gateway Tunnel ได้ไม่น้อยกว่า ๘,๐๐๐ Tunnels หรือดีกว่า และได้รับการรองรับตามมาตรฐานของ ICSA ด้าน IPsec VPN

๔.๒.๑๑. สามารถทำ SSL VPN และรองรับผู้ใช้งานได้ไม่น้อยกว่า ๕,๐๐๐ ผู้ใช้งาน หรือดีกว่า และได้รับการรองรับตามมาตรฐานของ ICSA ด้าน SSL VPN

๔.๒.๑๒. สามารถทำ Routing Protocol แบบ RIPng, OSPFv๓, NAT๔๖, NAT๖๔, IS-IS และ BGP ได้เป็นอย่างน้อย

๔.๒.๑๓. สามารถทำงานในลักษณะ Content Filtering หรือ Web Filtering หรือ URL Filtering ได้ โดยสามารถกำหนดให้อุปกรณ์ป้องกันการเข้าถึง URL หรือ Web site ที่ต้องห้ามได้

๔.๒.๑๔. สามารถป้องกันการเข้าถึง Web site โดยกำหนดแยกตามประเภทของ Web site (Web Categories) ได้ โดยมีสิทธิในการเข้าตรวจสอบฐานข้อมูลประเภทของ Web site ได้ตลอดระยะของการรับประกัน

๔.๒.๑๕. สามารถทำงานในลักษณะของไฟล์วอลล์เสมือน Virtual Domain Firewall หรือ Virtual System เป็นจำนวนอย่างน้อย ๑๐ Virtual และสามารถขยายได้ไม่น้อยกว่า ๒๕๐ Virtual หรือดีกว่า

๔.๒.๑๖. สามารถทำ User Authentication แบบ Captive Portal ได้

๔.๒.๑๗. รองรับการตรวจสอบผู้ใช้ (User Authentication) กับ RADIUS, LDAP และ SSO (Single Sign On) กับ Windows Active Directory และ RADIUS ได้เป็นอย่างน้อย

๔.๒.๑๘. สามารถระบุชนิดและควบคุมการใช้งาน Application ต่างๆ ได้ และมี Application Control หรือ Application Firewall Throughput ไม่น้อยกว่า ๑๒ Gbps หรือดีกว่า

๔.๒.๑๙. มีความสามารถในการทำ High Availability (HA) แบบ Active-Active โดยไม่ต้องเสียค่าใช้จ่ายเพิ่ม

๔.๒.๒๐. มีระบบจ่ายไฟ (Power supply) ไม่น้อยกว่า ๒ ชุด

๔.๒.๒๑. อุปกรณ์ต้องได้รับรองมาตรฐาน FCC และ UL เป็นอย่างน้อย

๔.๒.๒๒. ผลิตภัณฑ์ที่เสนอต้องจัดอยู่ในกลุ่ม Challengers หรือ Leaders ของ Magic Quadrant For Enterprise Network Firewalls ปี ๒๐๑๖ หรือปีปัจจุบัน

๔.๒.๒๓. ผู้เสนอราคาต้องมีหนังสือแต่งตั้งการเป็นตัวแทนจำหน่ายและได้รับการรับรองจากผู้ผลิตสาขาในประเทศไทยโดยตรงว่าอุปกรณ์ที่เสนอเป็นอุปกรณ์ใหม่ ไม่เคยใช้งานมาก่อนและยังอยู่ในสายการผลิต

**๔.๓. อุปกรณ์ป้องกันและรักษาความปลอดภัยทางเครือข่าย**

**(Internet Network Firewall)** **จำนวนไม่น้อยกว่า ๑ ชุด**

**มีคุณลักษณะเฉพาะขั้นต่ำอย่างน้อยดังต่อไปนี้**

๔.๓.๑. เป็นอุปกรณ์ Appliance ซึ่งได้รับการออกแบบมาเพื่อทำหน้าที่รักษาความปลอดภัยของเครือข่ายโดยเฉพาะ

๔.๓.๒. มีพอร์ต ๑๐ Gigabit Ethernet แบบ SFP+ ไม่น้อยกว่า ๖ พอร์ต หรือดีกว่า

๔.๓.๓. มีพอร์ต Gigabit Ethernet แบบ RJ๔๕ ไม่น้อยกว่า ๓๐ พอร์ต หรือดีกว่า

๔.๓.๔. มีพอร์ต Gigabit Ethernet แบบ RJ๔๕ สำหรับ Management หรือ HA ไม่น้อยกว่า ๒ พอร์ต

๔.๓.๕. มีความเร็วในการทำงานของ Firewall Throughput ที่ ๖๔ bytes ได้ไม่ต่ำกว่า ๕๐ Gbps หรือดีกว่า และได้รับการรองรับตามมาตรฐานของ ICSA ด้าน Firewall

๔.๓.๖. สามารถรองรับการเชื่อมต่อพร้อมๆกัน (concurrent Sessions) ได้ไม่น้อยกว่า ๑๖,๐๐๐,๐๐๐ การเชื่อมต่อ หรือดีกว่า และรองรับการเชื่อมต่อใหม่ (New Sessions / Second) ได้ด้วยความเร็วไม่ต่ำกว่า ๔๐๐,๐๐๐ การเชื่อมต่อ (sessions) ต่อวินาที หรือดีกว่า

๔.๓.๗. มีความสามารถในการตรวจจับและป้องกันไวรัสคอมพิวเตอร์ในโปรโตคอล FTP, HTTP, IMAP, IMAPS, POP๓, POP๓S, SMTP และ SMTPS และต้องสามารถ update ฐานข้อมูล

ไวรัสฯ (virus signature) ผ่านเครือข่าย Internet ได้เองโดยอัตโนมัติตลอดระยะของการรับประกันอุปกรณ์ และได้รับการรองรับตามมาตรฐานของ ICSA ด้าน Anti Virus

๔.๓.๘. มีความสามารถในการป้องกันการบุกรุก (Intrusion Prevention) ได้ไม่น้อยกว่า ๑๐ Gbps หรือดีกว่า (Enterprise MIX Traffic) โดยสามารถ update ฐานข้อมูลการบุกรุก (attack signature) ผ่านเครือข่าย Internet ได้เองโดยอัตโนมัติตลอดระยะของการรับประกัน และได้รับการรองรับตามมาตรฐานของ ICSA ด้าน IPS

๔.๓.๙. สามารถเข้ารหัสเพื่อการส่งข้อมูลด้วยวิธีการ VPN โดยมีใช้วิธีการเข้ารหัสแบบ ๓DES/AES IPSec และ SSL-VPN เพื่อความปลอดภัยในการติดต่อจากระยะไกลได้

๔.๓.๑๐. สามารถทำ IPSec VPN โดยมีความเร็วในการทำงาน IPSec VPN ได้ไม่ต่ำกว่า ๔๐ Gbps หรือดีกว่า และ VPN Gateway-to-Gateway Tunnel ได้ไม่น้อยกว่า ๘,๐๐๐ Tunnels หรือดีกว่า และได้รับการรองรับตามมาตรฐานของ ICSA ด้าน IPsec VPN

๔.๓.๑๑. สามารถทำ SSL VPN และรองรับผู้ใช้งานได้ไม่น้อยกว่า ๕,๐๐๐ ผู้ใช้งาน หรือดีกว่า และได้รับการรองรับตามมาตรฐานของ ICSA ด้าน SSL VPN

๔.๓.๑๒. สามารถทำ Routing Protocol แบบ RIPng, OSPFv๓, NAT๔๖, NAT๖๔, IS-IS และ BGP ได้เป็นอย่างน้อย

๔.๓.๑๓. สามารถทำงานในลักษณะ Content Filtering หรือ Web Filtering หรือ URL Filtering ได้ โดยสามารถกำหนดให้อุปกรณ์ป้องกันการเข้าถึง URL หรือ Web site ที่ต้องห้ามได้

๔.๓.๑๔. สามารถป้องกันการเข้าถึง Web site โดยกำหนดแยกตามประเภทของ Web site (Web Categories) ได้ โดยมีสิทธิในการเข้าตรวจสอบฐานข้อมูลประเภทของ Web site ได้ตลอดระยะของการรับประกัน

๔.๓.๑๕. สามารถทำงานในลักษณะของไฟล์วอลล์เสมือน Virtual Domain Firewall หรือ Virtual System เป็นจำนวนอย่างน้อย ๑๐ Virtual และสามารถขยายได้ไม่น้อยกว่า ๒๕๐ Virtual หรือดีกว่า

๔.๓.๑๖. สามารถทำ User Authentication แบบ Captive Portal ได้

๔.๓.๑๗. รองรับการตรวจสอบผู้ใช้ (User Authentication) กับ RADIUS, LDAP และ SSO (Single Sign On) กับ Windows Active Directory และ RADIUS ได้เป็นอย่างน้อย

๔.๓.๑๘. สามารถระบุชนิดและควบคุมการใช้งาน Application ต่างๆ ได้ และมี Application Control หรือ Application Firewall Throughput ไม่น้อยกว่า ๑๒ Gbps หรือดีกว่า

๔.๓.๑๙. มีความสามารถในการทำ High Availability (HA) แบบ Active-Active โดยไม่ต้องเสียค่าใช้จ่ายเพิ่ม

๔.๓.๒๐. มีระบบจ่ายไฟ (Power supply) ไม่น้อยกว่า ๒ ชุด

๔.๓.๒๑. อุปกรณ์ต้องได้รับรองมาตรฐาน FCC และ UL เป็นอย่างน้อย

๔.๓.๒๒. ผลิตภัณฑ์ที่เสนอต้องจัดอยู่ในกลุ่ม Challengers หรือ Leaders ของ Magic Quadrant For Enterprise Network Firewalls ปี ๒๐๑๖ หรือ ปีปัจจุบัน

๔.๓.๒๓. ผู้เสนอราคาต้องมีหนังสือแต่งตั้งการเป็นตัวแทนจำหน่ายและได้รับการรับรองจากผู้ผลิตสาขาในประเทศไทยโดยตรงว่าอุปกรณ์ที่เสนอเป็นอุปกรณ์ใหม่ ไม่เคยใช้งานมาก่อนและยังอยู่ในสายการผลิต

**๔.๔. ระบบวิเคราะห์ภัยคุกคามและความปลอดภัยเครือข่าย**

**(Security Information and Even Management) จำนวนไม่น้อยกว่า ๑ ระบบ**

**มีคุณลักษณะเฉพาะขั้นต่ำอย่างน้อยดังต่อไปนี้**

๔.๔.๑. เป็นอุปกรณ์สำเร็จรูป (appliance) หรือ Server ที่ประกอบด้วย hardware, software อยู่ในเครื่องเดียวกัน โดยทำหน้าที่เป็นทั้ง Log Management และ SIEM

๔.๔.๒. มี Hard disk อย่างน้อย ๒๐ TB และมีหน่วยความจำไม่น้อยกว่า ๑๒๘ GB

๔.๔.๓. รองรับการต่อเชื่อมกับ External storage ในรูปแบบ SAN, NFS, หรือ iSCSI

๔.๔.๔. มีพอร์ตเชื่อมต่อเครือข่ายในแบบ ๑๐/๑๐๐/๑๐๐๐ อย่างน้อย ๒ พอร์ต

๔.๔.๕. รองรับการใช้งาน IPV๖

๔.๔.๖. ผู้ใช้และผู้ดูแลระบบสามารถใช้งานผ่านหน้าจอ web console ได้

๔.๔.๗. สามารถรวบรวม Log ในรูปแบบรวมศูนย์ Centralized Log หรือ Log Archiving

๔.๔.๘. สามารถรวบรวม Log ได้ทั้งแบบที่ติดตั้งตั้งซอฟต์แวร์ (Agent) และ ไม่ติดตั้งซอฟต์แวร์ (Agentless) ที่ระบบปลายทาง

๔.๔.๙. สามารถบีบอัดข้อมูลได้โดยอัตโนมัติเพื่อเพิ่มพื้นที่ในการเก็บข้อมูล

๔.๔.๑๐. สามารถรวบรวม Log จากหลายๆ Operating System เช่น Windows, Linux, HP, Solaris, AS/๔๐๐ และออกแบบรายงานในรูปแบบแสดงรายละเอียดการเข้าใช้ (User Monitoring)

๔.๔.๑๑. สามารถรวบรวม Log จากหลายๆ Database เช่น DB๒, Oracle, MS SQL Server and Sybase system และออกแบบรายงานในรูปแบบแสดงรายละเอียดการเข้าใช้ (User Monitoring)

๔.๔.๑๒. สามารถรวบรวม Log จากหลายๆ Application เช่น Microsoft Exchange, WebSphere Application Server และออกแบบรายงานในรูปแบบแสดงรายละเอียดการเข้าใช้ (User Monitoring)

๔.๔.๑๓. สามารถรวบรวม Log อุปกรณ์ Network Devices และ Security Devices ได้

๔.๔.๑๔. สามารถกำหนดนโยบายการใช้งานของผู้ใช้ในระดับต่างๆ และสามารถกำหนดเงื่อนไขการเข้าดู (access) Log ต่างๆ ที่รวบรวมได้ในระดับอุปกรณ์ (device level)

๔.๔.๑๕. สามารถแสดงข้อมูลการเข้าถึงของผู้ใช้งานระดับต่างๆ ในรูปแบบ Dashboard ได้

๔.๔.๑๖. สามารถปรับเปลี่ยนรูปแบบ (Customization) ของหน้าจอการแสดงข้อมูล (Dashboard) ได้

๔.๔.๑๗. สามารถแสดงรายงานบอกปริมาณของเหตุการณ์ที่เข้ามา รวมถึงการตรวจสอบกับนโยบายที่กำหนดไว้ได้โดยอัตโนมัติ

๔.๔.๑๘. มี Regulation ที่ช่วยในการทำ Compliance กับมาตรฐานดังต่อไปนี้ ได้ คือ ISO๒๗๐๐๑, PCI-DSS, HIPAA, Sarbanes Oxley เป็นอย่างน้อย

๔.๔.๑๙. สามารถตรวจสอบความถูกต้องของข้อมูล Log (Integrity Check) ตามมาตรฐาน Log Management Standard สากล NIST ๘๐๐-๙๒ SHA-๑ Hash Algorithm

๔.๔.๒๐. ระบบสามารถแสดงรายงานในรูปแบบต่าง ๆ โดยเป็น Template ที่กำหนดมาให้ และผู้ปฏิบัติงานสามารถ Customize report ได้ตามการ

๔.๔.๒๑. สามารถค้นหาข้อมูล (Log Searching) และระบุบอกรายละเอียดของข้อมูลที่ต้องการค้นหา โดยสามารถบอก ชื่อผู้ใช้ หรือ IP Address วันเวลา ลักษณะการเข้าถึงทรัพยากร (activity) เครื่องต้นทาง และปลายทางได้

๔.๔.๒๒. สามารถทำ Complex Search เพื่อรองรับการค้นหาข้อมูลอย่างรวดเร็ว และรองรับการค้นหาข้อมูลสำหรับ Big Data ในอนาคต

๔.๔.๒๓. สามารถทำรายงาน และ Export รายงานในรูปแบบ HTML, PDF หรือ CSV ได้

๔.๔.๒๔. สามารถจัดการกำหนดสิทธิ์ของผู้ที่มาใช้งานในบทบาทที่ต่างกันได้

๔.๔.๒๕. สามารถแสดงสถานะการรวบรวม Log ในรูปแบบกราฟฟิก และออกรายงานไปยังผู้ที่เกี่ยวข้องได้

๔.๔.๒๖. สามารถแจ้งเตือนผ่านระบบ email , syslog, หรือ SNMP ได้

๔.๔.๒๗. ข้อมูล Log ที่มีการเก็บบันทึกมีการทำ Indexing เพื่อความสะดวกและรวดเร็วในการค้นหาข้อมูลย้อนหลัง

๔.๔.๒๘. สามารถเก็บข้อมูลของ Network flow ในรูปแบบ Net flow ได้โดยไม่เพิ่มเติมอุปกรณ์

๔.๔.๒๙. สามารถรวบรวมข้อมูล Log และวิเคราะห์จัดการในรูปแบบของ incident management ได้

๔.๔.๓๐. สามารถเก็บข้อมูล และเรียกดูข้อมูล Log ของอุปกรณ์ต่างๆที่อยู่ภายในระบบได้

๔.๔.๓๑. อุปกรณ์ที่เสนอจะต้องรวมลิขสิทธิ์การใช้งานที่สามารถรองรับการเก็บ log ได้อย่างน้อย ๒๕ แหล่งข้อมูล (sources device) เช่น Network & Security Device และ Log จากเครื่องแม่ข่าย

## ๕. การติดตั้ง

๕.๑. ผู้ชนะการประกวดราคาต้องทำการเสนอรายชื่อทีมงานและผู้ดูแลโครงการที่จะทำการติดตั้งระบบและคอยให้บริการกรณีเกิดปัญหากับโครงการ ตลอดจนคอยประสานงานต่างๆ ในโครงการให้เป็นไปอย่างเรียบร้อย โดยผู้ดูแลโครงการที่เสนอรายชื่อมา คณะฯ จะต้องสามารถติดต่อได้กรณีเกิดปัญหากับระบบที่ทำการติดตั้งหรือปรับปรุง

๕.๒. จะต้องทำการเสนอแผนงานและขั้นตอนการทำงานโดยละเอียด รวมทั้งระบุถึงวิธีการติดตั้ง ทดสอบ ปรับปรุง ระยะเวลา ช่วงเวลาที่ใช้ และเครื่องมือที่ใช้ติดตั้งและหรือปรับปรุงระบบทั้งหมดเพื่อประกอบการพิจารณา

๕.๓. ผู้เสนอราคาต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นเนื่องจากการติดตั้งอุปกรณ์หรือความเสียหายใดๆ ที่เกิดขึ้นเนื่องจากการปฏิบัติงานของผู้เสนอราคา ผู้เสนอราคาจะต้องดำเนินการซ่อมแซมแก้ไขให้อยู่ในสภาพเดิมโดยเร็ว

๕.๔. การติดตั้งระบบในข้อ ๔.๑ (Network Access Control)

๕.๔.๑. กำหนดให้ติดตั้งในลักษณะแบบมี Agent หรือ Agentless จำนวนไม่น้อยกว่า ๕๐ อุปกรณ์ เพื่อกำหนดนโยบายการเข้าใช้งานระบบเครือข่ายไม่น้อยกว่า ๓ นโยบาย

๕.๔.๒. ออกแบบให้สามารถรองรับการเพิ่มนโยบายการใช้งานได้ในภายหลัง

๕.๔.๓. กำหนดให้สร้างระบบการยืนยันตัวตน (Authentication) ของผู้เข้าใช้งานระบบเครือข่ายเพื่อทดแทนระบบเดิมของคณะฯ

๕.๕. การติดตั้งอุปกรณ์ในข้อ ๔.๒ (Firewall) สำหรับ Demilitarized Zone

๕.๕.๑. กำหนดให้สร้างนโยบายการใช้งานให้สอดคล้องกับการใช้งานจริงของเครื่องแม่ข่ายของทางคณะฯ

๕.๕.๒. การวางตำแหน่งอุปกรณ์เป็นการวางขวางหรือวางคู่ขนานกับระบบเดิม

๕.๕.๓. กำหนดให้เปิดการทำงานของ IPS

๕.๖. การติดตั้งอุปกรณ์ในข้อ ๔.๓ (Internet Network Firewall)

๕.๖.๑. ให้อ้างอิงค่าการทำงานของอุปกรณ์ Firewall หลักเดิมของคณะฯ

๕.๖.๒. กำหนดให้เปิดการทำงานของ Antivirus

๕.๖.๓. กำหนดให้ทำการ Migration ค่าการทำงานเดิมของคณะฯ แล้วนำเข้าสู่ระบบใหม่โดยที่หากค่าการทำงานใดไม่ได้ใช้งานให้ทำการข้ามการบังคับใช้ไปก่อน หากจะนำมาใช้ภายหลังต้องสามารถนำกลับมาใช้ใหม่ได้

๕.๗. การติดตั้งระบบในข้อ ๔.๔ (Security Information Event Management)

กำหนดให้ระบบทำการรับค่า log จากอุปกรณ์เครือข่ายของคณะฯ ดังต่อไปนี้เป็นอย่างน้อย

๕.๗.๑. Active Directory

๕.๗.๒. Network Management ( Omni vista )

๕.๗.๓. Firewall

๕.๗.๔. Wireless controller

๕.๗.๕. IPS

๕.๗.๖. Radius Server

๕.๗.๗. กำหนดให้ทำการออกรายงานการตรวจวิเคราะห์ได้ดังต่อไปนี้เป็นอย่างน้อย

๕.๗.๗.๑. Top ๕ Application

๕.๗.๗.๒. Top ๕ IP Source

๕.๗.๗.๓. Top ๕ IP Destination

๕.๘. กำหนดให้ออกแบบระบบรักษาความปลอดภัยระบบเครือข่ายใหม่ตามสถาปัตยกรรมและเทคโนโลยีในปัจจุบันเพื่อรองรับการใช้งานของทางคณะฯ โดยนำเสนอการออกแบบให้คณะกรรมการพิจารณาก่อนการติดตั้งจริง

๕.๙. จะต้องส่งมอบรายละเอียดรายการอุปกรณ์ที่ติดตั้งทั้งหมด ซึ่งจะต้องมีข้อมูลดังต่อไปนี้เป็นอย่างน้อย ได้แก่ ชื่ออุปกรณ์ รุ่นอุปกรณ์ ชนิดอุปกรณ์ ชื่อบริษัทผู้ผลิตอุปกรณ์ หมายเลขประจำตัวอุปกรณ์ (Serial No.) หมายเลขประจำตัวอุปกรณ์ย่อย ฯลฯ ตามข้อมูลของอุปกรณ์ที่มีจริง วันที่รับประกัน วันที่หมดอายุ (ถ้ามี)

๕.๑๐. ให้จัดทำคู่มือการติดตั้งส่งมอบแก่คณะฯ ในวันส่งมอบงานโดยจัดทำเป็นเอกสารพิมพ์ ๑ ชุด และ soft copy บรรจุในแผ่น CD จำนวน ๒ ชุด

## ๖. การฝึกอบรม

๖.๑. ผู้เสนอราคาจะต้องถ่ายทอดความรู้ทางด้านอุปกรณ์ที่เสนอ ให้เจ้าหน้าที่ของทางคณะฯ ที่ได้รับมอบหมายอย่างน้อย ๔ คน โดยมีวิทยากรให้ความรู้เบื้องต้นในหัวข้อต่อไปนี้

๖.๑.๑. ความรู้พื้นฐานเกี่ยวกับระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์

๖.๑.๒. ความรู้เกี่ยวกับอุปกรณ์ทั้งหมดที่ทำการติดตั้งในระบบ

๖.๑.๓. ความรู้เกี่ยวกับการ setup และการตั้งค่า configuration ของอุปกรณ์ที่เสนอ

**๗. การรับประกัน**

๗.๑. การรับประกัน การสนับสนุนทางเทคนิคและการบริการหลังการขาย ไม่น้อยกว่า ๓ ปี

**๘. เงื่อนไขเฉพาะ**

๘.๑. รายการที่เสนอในข้อ ๔.๑-๔.๔ ผู้เสนอราคาจะต้องมีหนังสือรับรองว่าจะให้การสนับสนุนทางเทคนิค จากเจ้าของผลิตภัณฑ์หรือสาขาประจำประเทศไทยสำหรับโครงการนี้

**๙. ระยะเวลาในการส่งมอบ** กำหนดส่งมอบภายใน ๑๒๐ วัน นับถัดจากวันลงนามในสัญญาซื้อขาย

**๑๐. งบประมาณวงเงินในการจัดหา** ๑๙,๐๙๔,๑๐๐.- บาท (สิบเก้าล้านเก้าหมื่นสี่พันหนึ่งร้อยบาทถ้วน) ในการเสนอราคาผู้เสนอราคาต้องเสนอลดราคา ขั้นต่ำ (Minimum Bid) ไม่น้อยกว่าครั้งละ ๓๐,๐๐๐.-บาท จากราคาสูงสุดของการประกวดราคาฯและ การเสนอราคาครั้งถัด ๆ ไป ต้องเสนอลดราคาครั้งละ ไม่น้อยกว่า ๓๐,๐๐๐.-บาท จากครั้งสุดท้ายที่เสนอลดแล้ว

**๑๑. หน่วยงานรับผิดชอบดำเนินการ** คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่

สถานที่ติดต่อเพื่อขอทราบข้อมูลเพิ่มเติม หรือเสนอแนะวิจารณ์ หรือแสดงความคิดเห็นเป็นลายลักษณ์อักษรโดยเปิดเผยตัว ระบุชื่อ นามสกุลจริง พร้อมที่อยู่และหมายเลขโทรศัพท์ที่สามารถติดต่อได้ตามช่องทางดังต่อไปนี้.-

๑๑.๑ หน่วยจัดหาพัสดุ งานพัสดุ คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่

๑๑๐ ถนนอินทวโรรส ต.สุเทพ อ.เมือง จ.เชียงใหม่ ๕๐๒๐๐

๑๑.๒ จดหมายอิเล็กทรอนิกส์ Email Address : medpurch@cmu.ac.th

๑๑.๓ โทรสารหมายเลข : ๐๕๓-๙๓๖๑๘๙

ทั้งนี้ภายใน ๓ วันทำการ นับตั้งแต่คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ ได้เผยแพร่ลง Website เพื่อคณะแพทยศาสตร์ จะได้นำข้อคิดเห็นหรือข้อเสนอแนะมาพิจารณาต่อไป

ประกาศ ณ วันที่ ๑๑ เดือน สิงหาคม พ.ศ. ๒๕๖๐

(ศาสตราจารย์ นายแพทย์บรรณกิจ โชติมากิจกุล)

คณบดีคณะแพทยศาสตร์