ประกาศคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่

เรื่อง การกำหนดหัวข้อร่างขอบเขตของงาน (TOR)

รายการ ระบบตรวจสอบและป้องกันเครือข่ายคอมพิวเตอร์ จำนวน ๑ ระบบ

---

๑. ความเป็นมา

เนื่องด้วย คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่มีนโยบายในการส่งเสริมการใช้ระบบเทคโนโลยีสารสนเทศในการสนับสนุนกระบวนการทำงานทางด้านต่างๆของทางคณะฯ เพื่อเป็นเพิ่มศักยภาพในการทำงานและการบริการด้านต่างๆให้รวดเร็วและมีประสิทธิภาพยิ่งขึ้น ส่งผลให้อุปกรณ์และระบบต่างๆทางด้านการรักษาความปลอดภัยเครือข่ายที่ใช้งานในปัจจุบันไม่อาจรองรับปริมาณงานที่เพิ่มขึ้นได้อย่างเพียงพอ จำเป็นต้องมีการหาอุปกรณ์มาทดแทนเพิ่มเติมเพื่อเป็นการเพิ่มขีดความสามารถในการรับมือกับปริมาณงานที่เพิ่มขึ้นรวมถึงการรับมือกับภัยคุกคามทางเครือข่ายคอมพิวเตอร์ซึ่งนับวันจะยิ่งรุนแรงและรวดเร็วกว่าในอดีต

๒. วัตถุประสงค์

๒.๑ เพื่อจัดหาอุปกรณ์ทดแทนของเดิมซึ่งหมดอายุการใช้งาน

๒.๒ เพื่อปรับปรุงระบบความปลอดภัยทางจดหมายอิเล็กทรอนิกส์ให้มีความน่าเชื่อถือ มั่นคง

๒.๓ เพื่อให้สามารถรองรับปริมาณงานทางสารสนเทศที่เพิ่มขึ้น

๓. คุณสมบัติของผู้เสนอราคา

๓.๑ ผู้เสนอราคาจะต้องเป็นนิติบุคคลที่ดำเนินกิจการทางด้านนี้และมีทุนจดทะเบียนไม่น้อยกว่า ๓,๐๐๐,๐๐๐ บาท และดำเนินกิจการมาไม่น้อยกว่า ๓ ปี

๓.๒ ผู้เสนอราคาต้องเป็นผู้ได้รับการแต่งตั้งอย่างเป็นทางการในการยื่นเสนออุปกรณ์ในข้อ ๔.๑ - ๔.๕ สำหรับโครงการนี้ โดยมีหนังสือแต่งตั้งจากเจ้าของผลิตภัณฑ์หรือสำนักงานสาขาในประเทศไทย เพื่อรับการสนับสนุนในการให้บริการหลังการขาย

๓.๓ ผู้ชนะการเสนอราคาจะต้องรับผิดชอบการดำเนินงานต่าง ๆ ทั้งหมดให้ถูกต้องตามข้อกำหนด รวมทั้งปฏิบัติตามระเบียบ กฎ ข้อบังคับ ของ คณะฯ โดยผู้ชนะการเสนอราคาจะอ้างเหตุไม่รับผิดชอบใดๆ จากความเข้าใจผิด ความไม่ทราบ ความผิดพลาด หรือความไม่สมบูรณ์ ของข้อมูลที่มีในข้อกำหนดนี้ไม่ได้ การดำเนินการใด ๆ ของผู้ชนะการเสนอราคา ที่ขัดกับระเบียบ กฎ ข้อบังคับ ที่เกี่ยวข้องกับการดำเนินงานตามข้อกำหนดและตามสัญญา ผู้ชนะการเสนอราคาจะต้องรับผิดชอบต่อผลที่จะเกิดขึ้น และแก้ไขให้ถูกต้อง

๓.๔ ผู้เสนอราคาต้องปฏิบัติในวันยื่นซองเสนอราคา

๓.๔.๑ ผู้เสนอราคาต้องยื่นรายการเปรียบเทียบ รายละเอียดระหว่างโปรแกรมและ อุปกรณ์ที่เสนอ กับคุณลักษณะเฉพาะที่กำหนดไว้ ว่าตรงกันหรือไม่ เพื่อประกอบการพิจารณา

๓.๔.๒ ในกรณีที่มีอุปกรณ์หลายรุ่น (Model) และ/หรือ Option ผู้เสนอราคาต้องระบุให้ชัดเจน โดยพิมพ์เป็นรายการว่าจะส่งมอบรุ่น หรือ Series ใด และ Option ใด

๓.๕ ผู้เสนอราคาต้องมีผลงานการติดตั้งระบบเครือข่ายคอมพิวเตอร์ให้กับสถาบันการศึกษาภาครัฐหรือหน่วยงานราชการที่เชื่อถือได้ โดยมีมูลค่างานไม่น้อยกว่า ๒ ล้านบาท จำนวนไม่น้อยกว่า ๑ สัญญา ภายในระยะเวลาย้อนหลังไม่เกิน ๕ ปี (นับถึงวันที่ยื่นซองประกวดราคา) โดยต้องยื่นหนังสือรับรองผลงานมาแสดงในวันยื่นซองประกวดราคา

๔. คุณลักษณะเฉพาะ

๔.๑ อุปกรณ์ตรวจสอบและป้องกันการบุกรุกทางเครือข่ายคอมพิวเตอร์ จำนวน ๑ ชุด มีคุณลักษณะเฉพาะดังนี้

๔.๑.๑เป็นอุปกรณ์ Appliance ที่มีหน่วยประมวลผลเป็นแบบ ASIC ซึ่งได้รับการออกแบบมาเพื่อทำหน้าที่รักษาความปลอดภัยของเครือข่ายโดยเฉพาะ

๔.๑.๒ มี Network Interface แบบ ๑๐/๑๐๐/๑๐๐๐ Ethernet (RJ-๔๕) อย่างน้อย ๑๒ ports และแบบ ๑๐G Ethernet พร้อม Connector ชนิด SR อย่างน้อย ๒ ports

๔.๑.๓ มีความเร็วในการทำงานของ Firewall ได้ไม่ต่ำกว่า ๒๐ Gbps และได้รับการรองรับตามมาตรฐานของ ICSA ด้าน Firewall

๔.๑.๔ สามารถรองรับการเชื่อมต่อพร้อมๆกัน (concurrent Sessions) ได้ไม่น้อยกว่า ๗,๐๐๐,๐๐๐ การเชื่อมต่อ และรองรับการเชื่อมต่อใหม่ (New Sessions / Second) ได้ด้วยความเร็วไม่ต่ำกว่า ๑๙๐,๐๐๐ การเชื่อมต่อ (sessions) ต่อวินาที

๔.๑.๕ มีความสามารถในการตรวจจับและป้องกันไวรัสคอมพิวเตอร์ในโปรโตคอล FTP, HTTP, IMAP, IMAPS, POP๓, POP๓S, SMTP และ SMTPS โดยได้รับการรองรับตามมาตรฐานของ ICSA ด้าน Antivirus และต้องสามารถ update ฐานข้อมูลไวรัสฯ (virus signature) ผ่านเครือข่าย Internet ได้เองโดยอัตโนมัติตลอดระยะของการรับประกันอุปกรณ์

๔.๑.๖ มีความสามารถในการป้องกันการบุกรุก (Intrusion Prevention) โดยสามารถ update ฐานข้อมูลการบุกรุก (attack signature) ผ่านเครือข่าย Internet ได้เองโดยอัตโนมัติตลอดระยะของการรับประกัน และได้รับการรับรองมาตรฐานจาก ICSA ด้าน Intrusion Prevention

๔.๑.๗ สามารถเข้ารหัสเพื่อการส่งข้อมูลด้วยวิธีการ VPN โดยมีใช้วิธีการเข้ารหัสแบบ ๓ DES/AES IPSec และ SSL-VPN เพื่อความปลอดภัยในการติดต่อจากระยะไกลได้ และได้รับการรับรองตามมาตรฐานของ ICSA ด้าน IPSec และ SSL-VPN

๔.๑.๘ มีความเร็วในการทำงาน IPSec VPN ได้ไม่ต่ำกว่า ๘ Gbps

๔.๑.๙ รองรับการเชื่อมโยงด้วย SSL VPN พร้อมๆ กันได้ไม่น้อยกว่า ๓,๐๐๐ users

๔.๑.๑๐ สามารถทำงาน WAN Optimization สำหรับโปรโตคอล FTP, CIFS และ HTTP ได้เป็นอย่างน้อย

๔.๑.๑๑ สามารถทำงานในลักษณะ Content Filtering ได้ โดยสามารถกำหนดให้อุปกรณ์ป้องกันการเข้าถึง URL หรือ Web site ที่ต้องห้ามได้ (URL blocking)

๔.๑.๑๒ สามารถป้องกันการเข้าถึง Web site โดยกำหนดแยกตามประเภทของ Web site (Web Categories) ได้ โดยมีสิทธิในการเข้าตรวจสอบฐานข้อมูลประเภทของ Web site ได้ตลอดระยะของการรับประกัน

๔.๑.๑๓ รองรับการตรวจสอบผู้ใช้ (User Authentication) กับฐานข้อมูลผู้ใช้ภายในตัวอุปกรณ์, ผู้ใช้ใน RADIUS, ใน LDAP และ Windows Active Directory ได้เป็นอย่างน้อย

๔.๑.๑๔ สามารถระบุชนิดและควบคุมการใช้งาน Application ต่างๆ ได้ไม่น้อยกว่า ๑๐๐๐ Applications โดยต้องมี Application ตามรายการต่อไปนี้ด้วย

๔.๑.๑๔.๑ Application Peer-to-Peer ได้แก่ Bit Torrent, eDonkey, Gnutella, Kazaa และ and WinNY

๔.๑.๑๔.๒ Instant Messaging ได้แก่ MSN, Yahoo IM, AOL-IM, ICQ

๔.๑.๑๔.๓ Facebook, Youtube และ MySpace

๔.๑.๑๕ มีความสามารถในการทำ High Availability (HA) แบบ Active-Active โดยไม่ต้องเสียค่าใช้จ่ายเพิ่ม

๔.๑.๑๖ มีสิทธิ์ในการ Upgrade firmware ตลอดอายุการรับประกัน

๔.๒ อุปกรณ์จัดเก็บและวิเคราะห์ข้อมูลจราจรคอมพิวเตอร์ จำนวน ๑ ชุด

มีคุณลักษณะเฉพาะ ดังนี้

๔.๒.๑ เป็นอุปกรณ์ประเภท hardware appliance ที่ได้รับการปรับปรุง firmware เพื่อปิดช่องโหว่ (hardened) เป็นที่เรียบร้อยแล้ว ผลิตโดยผู้ผลิตเดียวกันกับอุปกรณ์รักษาความปลอดภัยที่เสนอ หรือได้รับการรับรองจากผู้ผลิตอุปกรณ์รักษาความปลอดภัยที่เสนอมาว่าสามารถใช้งานร่วมกันได้

๔.๒.๒ รองรับการเก็บข้อมูลจราจรฯ โดยรูปแบบ syslog ได้

๔.๒.๓ มี Interface ชนิด Gigabit Ethernet แบบ RJ-๔๕ จำนวนไม่น้อยกว่า ๔ interface

๔.๒.๔ รองรับข้อมูลจราจรได้ไม่น้อยกว่า ๑,๐๐๐ log ต่อวินาที

๔.๒.๕ มีหน่วยจัดเก็บข้อมูล(Hard Disk) ความจุไม่น้อยกว่า ๒ TB

๔.๒.๖ รองรับการเก็บข้อมูลในรูปแบบ SQL ได้

๔.๒.๗ รองรับการทำ Forensic Analysis โดยการรวบรวมและคัดกรองเหตุการณ์จากข้อมูลต่อไปนี้ ได้เป็นอย่างน้อย

๔.๒.๗.๑ Username

๔.๒.๗.๒ Email Address

๔.๒.๗.๓ IM user

๔.๒.๘ การส่งและรับข้อมูลจราจรฯ กับอุปกรณ์รักษาความปลอดภัย สามารถกระทำโดยการเข้ารหัสได้ หรือผู้เสนอราคาต้องจัดการหรือจัดหาอุปกรณ์ให้มีการเข้ารหัสในการส่งและรับข้อมูลจราจรฯ นี้

๔.๒.๙ มีสิทธิในการรับข้อมูลจราจรฯ จากอุปกรณ์ประเภทเครือข่ายได้

๔.๒.๑๐ สามารถเก็บข้อมูลจราจรดังต่อไปนี้ได้เป็นอย่างน้อย

๔.๒.๑๐.๑ IP address ต้นทาง (source IP address)

๔.๒.๑๐.๒ IP address ปลายทาง (source IP address)

๔.๒.๑๐.๓ Service port ปลายทาง (destination port) เช่น tcp port ๘๐ เป็นต้น

๔.๒.๑๐.๔ วันและเวลาของการเชื่อมต่อชื่อของผู้ใช้งาน เมื่อมีการระบุตัวบุคคล (authentication)

๔.๒.๑๑ สามารถกำหนดสิทธิและระดับความสำคัญให้กับผู้ดูแลระบบฯ ที่จะเข้ามาใช้งานอุปกรณ์เก็บข้อมูลจราจรฯ นี้ได้ อย่างน้อยที่สุดต้องสามารถกำหนดได้ว่ามีสิทธิในการอ่านอย่างเดียวได้ (read-only administrator)

๔.๒.๑๒ สามารถ export ข้อมูลจราจรฯ ออกไปยัง FTP server เพื่อเก็บสำรองข้อมูลไว้ได้

๔.๒.๑๓ มีความสามารถในการวิเคราะห์การจราจรข้อมูลเครือข่าย(Network Analyzer) ได้อย่างน้อยดังนี้

๔.๒.๑๓.๑ Real-Time Traffic Viewer

๔.๒.๑๓.๒ Historical Traffic Viewer

๔.๒.๑๓.๓ Customizable Traffic Analyzer Log

๔.๒.๑๓.๔ Search Network Traffic Logs

๔.๒.๑๔ มีความสามารถในการวิเคราะห์พร้อมออกรายงานข้อมูลการจราจรคอมพิวเตอร์ที่บันทึกไว้อย่างน้อย ดังนี้

๔.๒.๑๔.๑ Automatic Log Watch

๔.๒.๑๔.๒ Profile-Base Reporting

๔.๒.๑๔.๓ การจัดการมุมมอง การค้นหา ข้อมูล Log ที่บันทึกไว้

๔.๒.๑๕ สามารถออกรายงานได้ไม่น้อยกว่า ๔๕๐ รูปแบบ ตามที่กำหนดไว้ เช่น

๔.๒.๑๕.๑ จำนวนสูงสุดไวรัสคอมพิวเตอร์ที่พบ

๔.๒.๑๕.๒ การรายงานเหตุการณ์ต่างๆที่เกิดขึ้นตามที่มีการกำหนดค่าการทำงานไว้

๔.๒.๑๕.๓ การใช้งานจดหมายอิเล็กทรอนิกส์

๔.๒.๑๕.๔ การใช้งาน Web

๔.๒.๑๕.๕ การใช้งาน Bandwidth ของระบบเครือข่าย

๔.๒.๑๕.๖ Protocol สูงสุดที่ใช้งาน

๔.๒.๑๖ มีความสามารถในการบริหารจัดการเขตกักกันแบบศูนย์กลาง

๔.๒.๑๖.๑ แสดงรายการที่ถูกกักกัน

๔.๒.๑๖.๒ รายงานสรุปแฟ้มข้อมูลที่ถูกกักกันแยกตามประเภทต่างๆ เช่น เหตุผลตรวจพบ เวลา เป็นต้น

๔.๒.๑๗ มีความสามารถในการจัดทำเหมืองข้อมูล หรือ DLP Archive

๔.๒.๑๘ สามารถแสดง Log แบบทันท่วงที ดังนี้

๔.๒.๑๘.๑ Web ๒.๐ Style

๔.๒.๑๘.๒ Historical & Custom log Views

๔.๒.๑๘.๓ Log Filtering

๔.๒.๑๘.๔ E-mail Traffic

๔.๒.๑๘.๕ FTP Traffic

๔.๒.๑๘.๖ สรุปอุปกรณ์รวม

๔.๓ อุปกรณ์รักษาความปลอดภัยระบบจดหมายอิเล็กทรอนิกส์ จำนวน ๑ ระบบ มีคุณสมบัติเฉพาะดังนี้

๔.๓.๑ เป็นอุปกรณ์ที่ถูกสร้างขึ้นเพื่อใช้ในการตรวจจับ SPAM และ ไวรัส ทาง e-mail ที่ทำงานบนระบบปฏิบัติการเฉพาะที่ทำการปิดช่องโหว่ของระบบมาเป็นที่เรียบร้อย (Hardened Operating System)

๔.๓.๒ สามารถทำงานได้หลายโหมดการทำงาน ได้แก่ Transparent Mode, Gateway Mode และ E-mail Server Mode

๔.๓.๓ มีความสามารถในการตรวจจับ SPAM ได้ไม่ต่ำกว่า ๑,๑๐๐,๐๐๐ ฉบับต่อชั่วโมง (messages/hour)

๔.๓.๔ มีความสามารถในการทำ E-mail Routing ได้ไม่ต่ำกว่า ๑,๑๐๐,๐๐๐ ฉบับต่อชั่วโมง (messages/hour)

๔.๓.๕ มี Ethernet Interface แบบ ๑๐/๑๐๐/๑๐๐๐ อย่างน้อย ๖ Interfaces

๔.๓.๖ มีความสามารถในการจัดเก็บข้อมูลบน Hard disk

๔.๓.๗ มีหน่วยจัดเก็บข้อมูล(Hard disk) ไม่น้อยกว่า ๒TB และสามารถขยายได้สูงสุดไม่น้อยกว่า ๖ TB ในภายหลัง โดยต้องรองรับการทำการในรูปแบบของ RAID (๑,๕,๑๐,๕๐) เป็นอย่างน้อย

๔.๓.๘ ระบบต้องรองรับการเชื่อมต่อกับหน่วยความจำภายนอกในรูปแบบของการทำงานร่วมกับ Network Attached Storage (NAS)

๔.๓.๙ รองรับการทำงานกับ e-mail หลายๆโดเมนพร้อมๆกันได้ (Multiple Email Domain support) เป็นจำนวนไม่น้อยกว่า ๕,๐๐๐ โดเมน

๔.๓.๑๐ สามารถสร้าง Profile ที ใช้ในการตรวจจับ SPAM, ใช้ในการตรวจจับ Virus, ใช้ในการทำ Authentication, ใช้ในการตรวจจับ Content อย่างน้อยไม่ต่ำกว่าประเภทละ ๕๕๐ profiles

๔.๓.๑๑ รองรับการทำงานในรูปแบบของ SMTP Mail Gateway สำหรับ e-mail server ในระบบ

๔.๓.๑๒ มีระบบการทำงานของ Policy-based mail routing และ Queue management

๔.๓.๑๓ มีระบบการทำงานของ Outbound Mail Relay เพื่อเพิ่มความปลอดภัยของระบบ e-mail ขาออก

๔.๓.๑๔ มีระบบการทำงานแบบ Granular Layered Detecting เพื่อป้องกัน ไวรัส และ SPAM

๔.๓.๑๕ สามารถทำการกักกัน (Spam Quarantining) และสามารถเพิ่มคำในหัวเรื่อง (Spam tagging) ใน E-mail ที่ถูกตรวจจับว่าเป็น SPAM ได้

๔.๓.๑๖ user ในระบบสามารถตรวจสอบ E-mail ที่ถูก Quarantine ไว้ได้ด้วยตัวเองเป็นรายบุคคลผ่านทาง Web Mail และ POP๓ โดยทำการยืนยันการเข้าถึง Quarantine ได้ด้วย Username และ Password จาก LDAP, Radius, SMTP, POP๓ และ IMAP

๔.๓.๑๗ รองรับการทำงานในรูปแบบของ Sender Policy Framework (SPF), DomainKeys และ DomainKeys Indentified Mail (DKIM)

๔.๓.๑๘ สามารถทำการจัดเก็บ E-mail ทุกฉบับ (E-mail Achieving) ที่ต้องการจะตรวจสอบได้จากการกำหนดเงื่อนไขต่างๆ อาทิเช่น Sender Address, Recipient Address, Subject, Attachment และ อื่นๆ

๔.๓.๑๙ รองรับการทำ SMTP Authentication ผ่านทาง LDAP, Radius, POP๓ และ IMAP

๔.๓.๒๐ สามารถตรวจสอบถึงความน่าเชื่อถือของ Server และ Client ที่ส่ง E-mail เข้ามาในระบบ (Sender Reputation) โดยให้คะแนนจาก E-mail ในรูปแบบต่างๆที่ส่งผ่านเข้ามายังระบบ อาทิเช่น Number of Viruses Sent, Amount of SPAM Sent, No. of bad Recipients และอื่นๆ พร้อมทั้งสามารถตั้งค่าการกระทำให้กับคะแนนในระดับต่างๆกัน

๔.๓.๒๑ สามารถทำการป้องกันการโจมตีในรูปแบบของ Denial of Service ต่างๆได้ อาทิเช่น Denial of Service (Mail Bombing), Recipient address attack, Email rate limiting และ Reverse DNS check (Anti-spoofing) เป็นอย่างน้อย

๔.๓.๒๒ สามารถกำหนดวิธีการจัดการกับ E-mail ที่ตรวจจับได้ว่าเป็น SPAM ได้ดังนี้ คือ Quarantine, Tag E-mail Header, Tag E-mail Subject Line, Reject และ Discard

๔.๓.๒๓ สามารถควบคุมขนาดของ E-mail ที่จะถูกส่งผ่านเข้าไปยังผู้ใช้งานในระบบได้ (email size control)

๔.๓.๒๔ สามารถทำรายงานสรุปจำนวน SPAM ที่ได้รับในแต่ละวันส่งให้ User แต่ละคนได้โดยอัตโนมัติ (Daily Quarantine Summaries)

๔.๓.๒๕ ระบบการตรวจสอบเนื้อหาในการตรวจจับ SPAM ต้องผ่านกระบวนต่างๆ อย่างน้อย ดังนี้

๔.๓.๒๕.๑ ตรวจสอบ SPAM ได้ทั้งจาก E-mail ขอเข้าและ ขาออก พร้อมๆกัน

๔.๓.๒๕.๒ ตรวจสอบจากการให้คะแนน Heuristic SPAM Filtering

๔.๓.๒๕.๓ ตรวจสอบจากไฟล์ และเนื้อหาที่ถูกแนบมากับ E-mail (Attachment/ Content Filtering)

๔.๓.๒๕.๔ ตรวจสอบจากรูปภาพที่ถูกแนบมาในเนื้อหาของ E-mail (Image Analysis Scanning)

๔.๓.๒๕.๕ ตรวจสอบจาก Header ของ E-mail (Email Header Inspection)

๔.๓.๒๕.๖ ตรวจสอบจาก Database ที่สามารถเรียนรู้ได้เองจากการทำงาน และจาก user ในระบบ (Bayesian Filtering)

๔.๓.๒๕.๗ ตรวจสอบจากแหล่งที่มาโดยดูจาก Database ภายนอก อาทิเช่น Real-time Blackhole List (RBL) filtering และ Spam URI RBL (SURBL) เป็นอย่างน้อย

๔.๓.๒๕.๘ ตรวจสอบจากรายชื่อของ Black/white List ที่สามารถถูกสร้างขึ้นในลักษณะของ รายบุคคล และ ภาพรวมทั้งหมด (Per user/ Global)

๔.๓.๒๕.๙ ตรวจหา IP address ของ Domain ผู้ส่งเพื่อเปรียบเทียบกับ IP address แหล่งที่มาของ E-mail แต่ละฉบับ (Forged IP Checking)

๔.๓.๒๕.๑๐ Greylist Checking

๔.๓.๒๕.๑๑ Bounce Verification

๔.๓.๒๖ สามารถทำการตรวจสอบไวรัส และ Spy ware ที่แฝงมากับ E-mail ได้

๔.๓.๒๖.๑ สามารถตรวจสอบหา Virus บน e-mail ที่ส่งผ่านโปรโตคอล SMTP ได้

๔.๓.๒๖.๒ สามารถแทรกข้อความแจ้งเตือนลงไปภายใน E-mail ได้ (Replacement message notification)

๔.๓.๒๖.๓ สามารถกรองไฟล์ที่แนบมาด้วยการแยก block ตามประเภทของไฟล์ (File type) ได้

๔.๓.๒๖.๔ สามารถตรวจสอบเพื่อป้องกันไฟล์ที่ถูกแนบมากับ e-mail ได้โดยดูจากรูปแบบและ นามสกุล (Extension) ของ File เหล่านั้น

๔.๓.๒๗ สามารถให้บริการเป็น E-mail Server สำหรับเข้าใช้งานในรูปแบบของ POP๓, SMTP และ IMAP ได้อย่างน้อยดังนี้

๔.๓.๒๗.๑ รองรับการทำงานในรูปแบบของ E-mail Server สำหรับ ๓๐๐๐ Mailboxes เป็นอย่างน้อย

๔.๓.๒๗.๒ รองรับการให้บริการ SMTP ผ่านทาง SSL (SMTP over SSL)

๔.๓.๒๗.๓ สามารถกำหนดปริมาณขนาดของเนื้อที่เพื่อให้บริการแก่ผู้ใช้งานแต่ละรายได้ (Disk Quota Policy)

๔.๓.๒๗.๔ สามารถให้บริการผ่านทาง Web Mail ได้

๔.๓.๒๗.๕ สามารถให้บริการการเชื่อมต่อเข้าใช้งาน E-mail ผ่านทาง Secure WebMail

๔.๓.๒๗.๖ สามารถแบ่งกลุ่มการใช้งานเป็นแบบ User, Group หรือ Alias ได้

๔.๓.๒๗.๗ สามารถให้บริการตรวจสอบการเข้าใช้แบบใช้ User บนตัวระบบหรือส่งผ่านไปตรวจสอบยัง LDAP (LDAP Authentication) ได้

๔.๓.๒๗.๘ สามารถแยกส่วนของ Bulk Folder ออกมาเพื่อใช้แยกการจัดเก็บ SPAM ได้

๔.๓.๒๘ มีระบบการทำ E-mail monitoring, Logging และ Reporting ได้อย่างน้อยดังนี้

๔.๓.๒๘.๑ การเก็บข้อมูลเหตุการณ์เมื่อมีการเปลี่ยนแปลงค่าการทำงานต่างๆภายในระบบ (Configuration change and management event)

๔.๓.๒๘.๒ รองรับการส่ง log ของข้อมูลต่างไปเก็บยัง Syslog ภายในอุปกรณ์หรือภายนอกอุปกรณ์ (External or Local Syslog)

๔.๓.๒๘.๓ สามารถทำการแจ้งเตือน (Alert) เมื่อมีเหตุการณ์ที่สำคัญ หรือการตรวจพบไวรัสเกิดขึ้น (Critical events and virus incident alerting)

๔.๓.๒๘.๔ สามารถทำ Report ได้ไม่น้อยกว่า ๑๐๐ ประเภท โดยสามารถแสดงผลออกมาในรูปแบบของ HTML และ PDF เป็นอย่างน้อย และสามารถตั้งเวลาให้การสั่งทำรายงานได้โดยอัตโนมัติ

๔.๓.๒๘.๕ สามารถออก Report โดยใช้ข้อมูล MSISDN ได้ อาทิเช่น Top Client MSISDN, Top Sender MSISDN, Top SPAM MSISDN และ Top Virus MSISDN

๔.๓.๒๙ การบริหารจัดการสามารถทำได้ผ่านทาง Console Port, HTTP, HTTPS, Telnet และ SSH เป็นอย่างน้อย

๔.๓.๓๐ สามารถทำงานร่วมกับ Dynamic DNS (DDNS)

๔.๓.๓๑ สามารถทำงานร่วมกับ MSISDN ได้ทั้งในด้านการทำ Anti-Spam และ Report อาทิเช่น MSISDN Logging & Reporting, MSISDN Reputation และ MSISDN Blacklisting & Whitelisting

๔.๓.๓๒ สามารถแบ่งการบริหารจัดการ E-mail แต่ละ Domain ให้ผูกกับ Administrator account ที่ต้องการอย่างเฉพาะเจาะจงได้ (Tiered Administration Domains) อย่างน้อย ๕๐ admin accounts

๔.๓.๓๓ เป็นอุปกรณ์ที่พร้อมรองรับการทำ HA ในแบบ Active – Passive ทั้งในระบบการทำงานแบบ Gateway (Relay) Mode และ Transparent Mode

๔.๓.๓๔ มี Redundant Power Supplies แบบ Hot Swappable

๔.๓.๓๕ มีลิขสิทธิ์การตรวจจับป้องกันไวรัสคอมพิวเตอร์ และ Spam mail แบบไม่จำกัดจำนวนผู้ใช้งานมาพร้อมกับอุปกรณ์ (Unlimited Licensed)

๔.๓.๓๖ อุปกรณ์ต้องสามารถตรวจสอบ Spam mail จากฐานข้อมูลของผู้ผลิตผ่านเครือข่าย Internet ได้ตลอดอายุการรับประกัน

๔.๓.๓๗ อุปกรณ์ต้องสามารถ update Anti-Virus Definition ได้อัตโนมัติ ตลอดอายะการรับประกัน

๔.๓.๓๘ อุปกรณ์ต้องได้รับการรับรองมาตรฐานผลิตภัณฑ์ อย่างน้อยดังต่อไปนี้ ICSA ด้าน Anti-Spam, VBspam Platinum , FCC ClassA, UL/CB/CUL, VCCI และ C-Tick เป็นอย่างน้อย

๔.๔ อุปกรณ์สลับสัญญาณแบบที่ ๑ จำนวน ๑ ชุด

มีคุณสมบัติเฉพาะดังนี้

๔.๔.๑ เป็นอุปกรณ์ที่มีสถาปัตยกรรมเป็นแบบ Stackable LAN Switch ที่รองรับการทำ Stack ได้ไม่น้อยกว่า ๘ ชุดและเป็นอุปกรณ์ที่สามารถทำงานในระดับ Layer ๒ และ Layer ๓ เป็นอย่างน้อย

๔.๔.๒ มีขนาด Switch Fabric รวมไม่น้อยกว่า ๑๔๔ Gbps และมี Throughput หรือ Forwarding Rate รวมสูงสุดได้ไม่น้อยกว่า ๙๕ Mpps

๔.๔.๓ มีพอร์ต Gigabit Ethernet แบบ ๑๐/๑๐๐/๑๐๐๐ BaseTX จำนวนไม่น้อยกว่า ๒๐ พอร์ต

๔.๔.๔ มีพอร์ต Gigabit Ethernet แบบ SFP หรือ GBIC ไม่น้อยกว่า ๔ พอร์ต พร้อมเสนอ Transceiver แบบ ๑๐๐๐Base-LX หรือ ๑๐๐๐Base-SX ตามจำนวนใช้งาน

๔.๔.๕ รองรับระบบจ่ายไฟสำรอง (Redundant Power Supply) โดยสามารถติดตั้งเพิ่มเติมได้ภายหลัง

๔.๔.๖ สนับสนุนจำนวน MAC Address ได้สูงสุดไม่น้อยกว่า ๑๒,๐๐๐ Address

๔.๔.๗ สามารถทำ VLAN ตามมาตรฐาน IEEE๘๐๒.๑q ได้ไม่น้อยกว่า ๑,๐๐๐ VLAN และ VLAN Stacking (Q-in-Q) ได้

๔.๔.๘ สามารถทำ User Authentication แบบ IEEE๘๐๒.๑X, MAC-based และ Web-based หรือ Captive Portal ได้เป็นอย่างน้อย โดยต้องสามารถกำหนด VLAN ให้กับผู้ใช้งานได้หลังจากทำ Authentication (VLAN Assignment)

๔.๔.๙ สามารถทำงานตามมาตรฐาน IEEE๘๐๒.๑d, IEEE๘๐๒.๑w, IEEE๘๐๒.๑s, IEEE๘๐๒.๑p, IEEE๘๐๒.๑q และ IEEE๘๐๒.๑ab (LLDP) ได้เป็นอย่างน้อย

๔.๔.๑๐ สามารถทำ IPv๔ routing protocol ได้แก่ RIPv๑, RIP๒, Policy Based Routing และรองรับการทำ OSPF, IS-IS, BGP๔, Virtual Routing Forwarding (VRF) โดยการ upgrade license

๔.๔.๑๑ สามารถทำ IP Multicast protocol ได้แก่ IGMPv๓ ได้เป็นอย่างน้อย และรองรับการทำ IP Multicast Routing Protocol แบบ PIM-SM, PIM-DM, DVMRP โดยการ upgrade license

๔.๔.๑๒ สามารถทำ IPv๖ routing protocol ได้แก่ RIPng และ ๖to๔ Tunneling ได้เป็นอย่างน้อย

๔.๔.๑๓ สามารถทำ WCCPv๒ หรือ Load Balance Proxy Server แบบ Weighted Round Robin หรือ Round Robin หรือ Weighted Least Connections

๔.๔.๑๔ เป็นอุปกรณ์ที่สามารถทำงานแบบ Port Trunking หรือ Link Aggregation ได้ไม่น้อยกว่า ๓๒ Groups

๔.๔.๑๕ สามารถกำหนดคุณภาพการให้บริการ โดยทำ Packet classification Layer ๒ – Layer ๔ พร้อมการทำ Marking และ Re-marking ระหว่างค่า QoS และสามารถกำหนดการป้องกันการส่งผ่านข้อมูลด้วย Access Control List (ACL) ในระดับ Layer ๒-๔, IPv๖ ได้ไม่น้อยกว่า ๑,๐๐๐ รายการ

๔.๔.๑๖ สามารถทำ NetFlow หรือ sFlow ได้ โดยมีรูปแบบของข้อมูลการใช้งานแบบ VLAN, Source IP / Destination IP, TCP/UDP port ได้เป็นอย่างน้อย

๔.๔.๑๗ สามารถทำ Mac address security หรือ Learn port security, DHCP snooping, IP source guard หรือ IP source filtering, Dynamic ARP Inspection หรือ ARP spoof protection และ STP root guard ได้

๔.๔.๑๘ มี Module Traffic Anomaly Detector หรือสามารถทำ Traffic Anomaly Detection โดยต้องสามารถ Shutdown port หรือ Filter IP address หรือ Filter MAC address หรือ Filter Bad Traffic ได้ หรือเสนอระบบ Network Access Control ที่สามารถป้องกันการโจมตีเพื่อทำงานทดแทนโดยระบบที่เสนอต้องสามารถรองรับผู้ใช้งานทั้งหมดในระบบ

๔.๔.๑๙ สามารถทำ SLA Monitoring โดยการ Simulate Traffic เช่น HTTP หรือ FTP หรือ Ping เป็นต้น เพื่อตรวจหา Latency หรือ RTT, Jitter, Packet Loss หรือ Packet Sent/Receive ได้เป็นอย่างน้อย

๔.๔.๒๐ สามารถทำ SPAN Port หรือ Port Mirroring ทั้งแบบ one-to-one, many-to-one และ RSPAN Port หรือ Remote Port Mirroring ได้

๔.๔.๒๑ สามารถเข้าไปบริหารและจัดการอุปกรณ์ด้วย CLI, Telnet, SSHv๒, NTPv๓, Syslog, SNMPv๓, RMON และ Embedded WEB management ได้

๔.๕ อุปกรณ์สลับสัญญาณแบบที่ ๒ จำนวน ๔ ชุด

มีคุณสมบัติเฉพาะดังนี้

๔.๕.๑ อุปกรณ์จะต้องได้รับการออกแบบให้มีลักษณะเป็น Stackable หรือ Virtual Chassis โดยรองรับการทำ Stacking หรือ Virtual Chassis ได้ไม่น้อยกว่า ๘ ตัว และเป็นพอร์ตในการทำ Stacking หรือ Virtual Chassis โดยเฉพาะ

๔.๕.๒ มีพอร์ต USB จำนวนไม่น้อยกว่า ๑ พอร์ต เพื่อรองรับการทำ Recovery หรือ Upgrade

๔.๕.๓ มีขนาดของ Switching Fabric หรือ Switching Capacity รวมไม่น้อยกว่า ๘๘ Gbps และมี Throughput หรือ Forwarding Rate รวมไม่น้อยกว่า ๖๕ Mpps

๔.๕.๔ รองรับระบบจ่ายไฟที่มีการสำรองไฟแบบสมบูรณ์ (Redundancy Power Supply)

๔.๕.๕ มีพอร์ต Gigabit Ethernet แบบ ๑๐/๑๐๐/๑๐๐๐BaseT ไม่น้อยกว่า ๒๔ พอร์ต

๔.๕.๖ มีพอร์ต Gigabit Ethernet แบบ ๑๐๐๐BaseX (GBIC หรือ SFP) ไม่น้อยกว่า ๒ พอร์ต พร้อมเสนอพอร์ตแบบ ๑๐๐๐Base-SX, ๑๐๐๐Base-LX ตามจำนวนใช้งาน

๔.๕.๗ รองรับพอร์ต ๑๐Gigabit Ethernet ไม่น้อยกว่า ๒ พอร์ต โดยการเพิ่ม Module หรือ License บนอุปกรณ์ Access Switch

๔.๕.๘ รองรับจำนวน MAC Addresses ได้ไม่น้อยกว่า ๑๒,๐๐๐ Addresses

๔.๕.๙ สามารถทำ VLAN ตามมาตรฐาน IEEE๘๐๒.๑q ได้ไม่น้อยกว่า ๑,๐๐๐ VLAN

๔.๕.๑๐ เป็นอุปกรณ์ที่สามารถทำงานแบบ Port Trunking หรือ Link Aggregation ตามมาตรฐาน IEEE๘๐๒.๓ad ได้ไม่น้อยกว่า ๓๒ Groups, Uni-Directional Link Detection (UDLD) และสามารถทำ Link Protection without STP แบบ Flex Link หรือ Dual-home Link หรือ Ethernet Ring Protection หรือเทียบเท่าได้

๔.๕.๑๑ สามารถทำ SPAN Port หรือ Port Mirroring ทั้งแบบ one-to-one, many-to-one และ RSPAN Port หรือ Remote Port Mirroring ได้

๔.๕.๑๒ สามารถทำ User Authentication แบบ IEEE ๘๐๒.๑x, MAC Based และ Web-based ได้

๔.๕.๑๓ สามารถทำ IP Routing Protocol ได้แก่ Policy Base Routing (PBR), VRRP, RIPv๑/v๒ และ RIPng ได้เป็นอย่างน้อย

๔.๕.๑๔ สามารถจัดการข้อมูลประเภท Multicast ด้วย Internet Group Management Protocol แบบ IGMPv๓ และ MLD ได้

๔.๕.๑๕ สามารถทำฟังก์ชั่น DHCP snooping, IP source guard หรือ IP source filtering, Dynamic ARP Inspection หรือ Dynamic ARP Protection, STP root guard, BPDU guard หรือ BPDU shutdown port, Loop Guard หรือ Loopback Detection และ Port security ได้

๔.๕.๑๖ สามารถทำ Quality of Service (QoS) ได้ ตามมาตรฐาน IEEE ๘๐๒.๑p, ToS, DSCP และมี Queue ไม่น้อยกว่า ๘ Queues ต่อพอร์ต (Hardware Based)

๔.๕.๑๗ สามารถควบคุมการส่งผ่านข้อมูลด้วย Access Control List (ACL) แบบ Source/ Destination IP address, Source/Destination MAC address, VLAN, IP Protocol, TCP/UDP port และ IPv๖ ได้ไม่น้อยกว่า ๑,๐๐๐ รายการ

๔.๕.๑๘ มีความสามารถทำ NetFlow หรือ sFlow หรือ J-Flow ได้อย่างน้อย ๑ โปรโตคอล

๔.๕.๑๙ สามารถทำ Network Timing Protocol (NTP) โดยสามารถ Sync ระบบเวลากับอุปกรณ์ NTP Server ในระบบเครือข่าย หรือ NTP server ของการสื่อสารได้ๆ

๔.๕.๒๐ สนับสนุนระบบ Network Management ตามมาตรฐาน SNMPv๓, RMON ๔ group, Secure Shell และ มี Web Based Management หรือ GUI Software

๔.๕.๒๑ อุปกรณ์ผ่านการรับรองตามมาตรฐานความปลอดภัย IEC, FCC, UL เป็นอย่างน้อย

๔.๖ เครื่องคอมพิวเตอร์แม่ข่ายแบบที่ ๑ จำนวน ๑ เครื่อง

มีคุณลักษณะเฉพาะ ดังนี้

๔.๖.๑ มีหน่วยประมวลผลกลาง (CPU) แบบ RISC สำหรับเครื่องคอมพิวเตอร์แม่ข่าย (Server) มีความเร็วสัญญาณนาฬิกาไม่น้อยกว่า ๓.๖ GHz จำนวนไม่น้อยกว่า ๔ Processor core

๔.๖.๒ CPU รองรับการประมวลผลแบบ ๖๔ bit และมีหน่วยความจำแบบ Cache Memory รวมไม่น้อยกว่า ๓๒ MB

๔.๖.๓ มีหน่วยความจำหลัก (RAM) ชนิด ECC DDR๓ หรือดีกว่า มีขนาดรวมไม่น้อยกว่า ๓๒ GB และ รองรับการขยายได้สูงสุดไม่น้อยกว่า ๖๔ GB

๔.๖.๔ มีช่องสำหรับเชื่อมต่ออุปกรณ์เพิ่มเติมแบบ PCI-E หรือดีกว่า จำนวนไม่น้อยกว่า ๔ ช่อง

๔.๖.๕ มีหน่วยจัดเก็บข้อมูล (Hard Disk) SAS หรือดีกว่า ขนาดความจุไม่น้อยกว่า ๓๐๐ GB จำนวนไม่น้อยกว่า ๒ หน่วย

๔.๖.๖ มี FC Adapter แบบ ๒-port ความเร็วไม่น้อยกว่า ๘Gb จำนวนไม่น้อยกว่า ๒ หน่วย

๔.๖.๗ มี DVD-RAM หรือดีกว่า จำนวน ๑ หน่วย

๔.๖.๘ มีช่องเชื่อมต่อระบบเครือข่าย แบบ ๑๐/๑๐๐/๑๐๐๐ Mbps หรือ Gigabit Ethernet จำนวนไม่น้อยกว่า ๔ ช่อง

๔.๖.๙ มี Redundant Power Supply แบบ Hot Plug หรือ Hot Swap

๔.๖.๑๐ ติดตั้งซอฟต์แวร์ระบบปฏิบัติการ Redhat Linux แบบ ๖๔ bit ในข้อ ๔.๘ พร้อมใช้งาน โดยมีลิขสิทธิ์ถูกต้องตามกฎหมาย

๔.๖.๑๑ สนับสนุนการแบ่ง Virtualization Server (Partition หรือ Domain) จำนวนไม่น้อยกว่า ๔ Virtualization Server (Partition หรือ Domain)

๔.๗ เครื่องคอมพิวเตอร์แม่ข่ายแบบที่ ๒ จำนวน ๑ ชุด

มีคุณลักษณะเฉพาะ ดังนี้

๔.๗.๑ เป็นเครื่องคอมพิวเตอร์ที่ได้รับการออกแบบมาเพื่อทำงานเป็นเครื่องแม่ข่าย Server โดยเฉพาะ

๔.๗.๒ มี BIOS แบบ UEFI ที่มีลิขสิทธิ์ถูกต้องตามกฎหมายและได้รับการออกแบบให้ใช้กับเครื่องแม่ข่าย

๔.๗.๓ มีหน่วยประมวลผลกลาง(Processor) ชนิด Intel Xeon Quad-Core ซึ่งทำงานที่ความถี่สัญญาณนาฬิกา (Clock Speed) ไม่น้อยกว่า ๒.๔ GHz หรือดีกว่า จำนวนไม่น้อยกว่า ๑ หน่วย รองรับการขยายได้ไม่น้อยกว่า ๒ หน่วย

๔.๗.๔ หน่วยประมวลผลกลางมี Cache ขนาดไม่น้อยกว่า ๑๐ MB หรือดีกว่า

๔.๗.๕ มีหน่วยความจำแบบ DDR๓ RDIMMs หรือดีกว่า โดยมีขนาดหน่วยความจำ ไม่น้อยกว่า ๑๒ GB และสามารถรองรับการขยายรวมได้สูงสุดในภายหลัง ไม่น้อยกว่า ๓๖๘ GB และสามารถรองรับการทำงานแบบ Memory Mirroring และ Memory Sparing หรือเทียบเท่าได้เป็นอย่างน้อย

๔.๗.๖ มีหน่วยควบคุมในการจัดการ RAID แบบ SAS/SATA หรือดีกว่า สามารถทำ RAID ๐, ๑ , ๕ ได้เป็นอย่างน้อย

๔.๗.๗ มีหน่วยเก็บข้อมูลสำรอง (Hard Disk) แบบ Hot-Swap/Hot-Plug SAS/SATA หรือดีกว่าที่มีขนาด ๒.๕ นิ้วซึ่งมีขนาดความจุก่อนการ format ไม่น้อยกว่า ๓๐๐ GB ที่มีความเร็วในการทำงานไม่น้อยกว่า ๑๐,๐๐๐ รอบต่อนาที(rpm) จำนวนไม่น้อยกว่า ๓ หน่วย และสามารถรองรับการเพิ่มขยายในอนาคตรวมได้สูงสุดไม่น้อยกว่า ๘ หน่วย

๔.๗.๘ มีหน่วยอ่านเขียนข้อมูลแผ่นแบบ DVD-RW drive หรือดีกว่าจำนวนไม่น้อยกว่า ๑ หน่วย

๔.๗.๙ มีหน่วยควบคุมแสดงภาพ (Video Controller) ที่มีหน่วยความจำไม่น้อยกว่า ๑๖ MB

๔.๗.๑๐ มีส่วนเชื่อมต่อกับระบบเครือข่าย (Network Controller) แบบ Gigabit Ethernet หรือดีกว่า ที่ติดตั้งลงในแผงวงจรหลัก (Module) จำนวนไม่น้อยกว่า ๔ พอร์ต หรือดีกว่า และ สามารถเพิ่มขยายส่วนเชื่อมต่อแบบ ๑๐ Gb Ethernet จำนวนไม่น้อยกว่า ๒ พอร์ต

โดยยังคงมีช่องต่ออุปกรณ์เพิ่มขยาย (Expansion slots) แบบ PCIe จำนวนไม่น้อยกว่า ๒ slots

๔.๗.๑๑ ตัวเครื่องมีพอร์ตหรือช่องสัญญาณสำหรับการเชื่อมต่อกับอุปกรณ์ภายนอก ดังต่อไปนี้

๔.๗.๑๒ พอร์ตอนุกรม (Serial port แบบ ๙ pin) จำนวนไม่น้อยกว่า ๑ port

๔.๗.๑๓ มีพอร์ต USB (USB ๒.๐) ด้านหน้า จำนวนไม่น้อยกว่า ๒ ports

๔.๗.๑๔ มีพอร์ต USB (USB ๒.๐) ด้านหลัง จำนวนไม่น้อยกว่า ๔ ports

๔.๗.๑๕ มีพอร์ต USB แบบ Internal จำนวนไม่น้อยกว่า ๑ ports

๔.๗.๑๖ ตัวเครื่องคอมพิวเตอร์แม่ข่ายที่นำเสนอต้องสามารถรองรับเทคโนโลยี IPMI ๒.๐ และ TPM ๑.๒ ได้เป็นอย่างน้อย

๔.๗.๑๗ มีหน่วยจ่ายกระแสไฟฟ้าภายในเครื่อง (Power Supply) ขนาดไม่ต่ำกว่า ๕๕๐ Watt. จำนวนไม่น้อยกว่า ๒ หน่วย ที่มีคุณสมบัติทำงานทดแทนกันได้โดยอัตโนมัติ (Redundant) และสามารถถอดเปลี่ยนได้ทันทีแม้ไม่เกิดปัญหาใดๆ (Hot-swap)

๔.๗.๑๘ มีระบบพัดลมระบายความร้อนภายในเครื่อง (Fan) ที่มีคุณสมบัติสามารถถอดเปลี่ยนได้ทันทีแม้ไม่เกิดปัญหาใดๆ (Hot-swap)

๔.๗.๑๙ มีระบบ Light Path Diagnostics หรือเทียบเท่า เพื่อดูข้อผิดพลาดและวิเคราะห์อาการเสียของอุปกรณ์ต่าง ๆภายในตัวเครื่องคอมพิวเตอร์แม่ข่าย

๔.๗.๒๐ มีระบบการเตือนถึงความเป็นไปได้ในการชำรุดเสียหายของอุปกรณ์ล่วงหน้า (Predictive Failure Analysis หรือเทียบเท่า) สำหรับ Processor(s), Memory, Disk (s), Power Supply และพัดลมได้เป็นอย่างน้อย

๔.๗.๒๑ เป็นคอมพิวเตอร์แม่ข่ายที่ได้รับการออกแบบสำหรับติดตั้งกับตู้อุปกรณ์สื่อสารมาตรฐาน (๑๙" Rack) โดยเฉพาะและมีขนาด ๑U พร้อมอุปกรณ์ Rack ในการติดตั้ง

๔.๗.๒๒ เครื่องคอมพิวเตอร์แม่ข่ายที่เสนอ ต้องได้รับการรับรองตามมาตรฐาน FCC, UL และ VCCI (Class A) เป็นอย่างน้อย

๔.๗.๒๓ ต้องมีการรับประกันแบบ On-site Service เป็นระยะเวลาอย่างน้อย ๓ ปี แบบ ๒๔ x ๗

๔.๗.๒๔ อุปกรณ์รุ่นที่เสนอ ต้องเป็นเครื่องใหม่ที่ยังมิได้ทำการติดตั้งใช้งาน ณ ที่ใดมาก่อน และไม่เป็นเครื่องที่ถูกนำมาปรับปรุงสภาพใหม่ (Reconditioned หรือ Rebuilt) โดยมีหนังสือรับรองจากเจ้าของผลิตภัณฑ์ (สาขาในประเทศไทย) โดยตรง

๔.๘ ระบบปฏิบัติการสำหรับเครื่องแม่ข่าย

มีคุณลักษณะเฉพาะ ดังนี้

๔.๘.๑ ระบบปฏิบัติการ Windows sever ๒๐๑๒ จำนวน ๑ ชุด

๔.๘.๒ ระบบปฏิบัติการ Linux Red hat จำนวน ๔ ชุด

๔.๘.๓ มีลิขสิทธิ์การใช้งานถูกต้องตามกฎหมาย

๕. การรับประกัน

การรับประกันอุปกรณ์ทั้งหมด ๓ ปี

๖. การติดตั้ง

๖.๑.๑ ผู้ชนะการประกวดราคาต้องศึกษาระเบียบข้อบังคับการเข้าทำงานในส่วนที่เกี่ยวข้องกับคณะฯ เสนอเอกสารและ นำเสนอรายละเอียดต่างๆให้กับงานเทคโนโลยีสารเทศรับทราบภายใน ๑๕ วัน นับตั้งแต่วันที่ลงนามในสัญญา ซึ่งเอกสารที่เสนอจะต้องประกอบด้วย

๖.๑.๑.๑ แผนการติดตั้งขั้นตอนการทำงานโดยละเอียดรวมทั้งระบุถึงวิธีการติดตั้ง ทดสอบปรับปรุง ระยะเวลา ช่วงเวลาที่ใช้ และเครื่องมือที่ใช้ติดตั้งและ/หรือปรับปรุงระบบทั้งหมด

๖.๑.๑.๒ ส่งรายชื่อ ตำแหน่ง หมายเลขโทรศัพท์ที่ทำงาน หมายเลขโทรศัพท์เคลื่อนที่ หมายเลขโทรสาร และ e-mail ทั้งหมดของทีมงาน

๖.๑.๒ ก่อนที่ผู้ชนะการประกวดราคาจะเข้าดำเนินการใดๆ ผู้เสนอราคาจะต้องทำหนังสือชี้แจงพร้อมรายละเอียดของวัสดุอุปกรณ์ที่จะใช้งาน แจ้งให้กับงานเทคโนโลยีสารสนเทศรับทราบก่อนจะเข้าดำเนินการจริงและ และ ต้องรอให้ได้รับการอนุมัติจากผู้ควบคุมการติดตั้งก่อน จึงจะสามารถดำเนินการได้ หากบริษัทฯไม่ปฏิบัติตามบริษัทฯต้องดำเนินการรื้อถอนระบบต่างๆที่ได้ติดตั้งไปแล้ว โดยให้ถือเป็นความผิดและความรับผิดชอบของผู้ชนะการประกวดราคา

๖.๑.๓ ผู้ชนะการประกวดราคาต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น เนื่องจากการติดตั้งอุปกรณ์หรือความเสียหายใดที่เกิดขึ้นเนื่องจากการปฏิบัติงานของผู้ชนะการประกวดราคา ผู้ชนะการประกวดราคาจะต้องดำเนินการซ่อมแซมแก้ไขให้อยู่ในสภาพเดิมโดยเร็ว

๖.๑.๔ ติดตั้งอุปกรณ์ข้อ ๔.๑ – ๔.๘ ณ ศูนย์ข้อมูล (Data Center Site)อาคารศรีพัฒน์ ชั้น ๖

๖.๑.๕ ให้บริการในการปรับปรุง (Upgrade) ความสามารถของ Software, Firmware ตลอดอายุการรับประกัน โดยแจ้งให้ทางคณะฯพิจารณาก่อนดำเนินการ

๖.๑.๖ ผู้ชนะการประกวดราคาจะต้องจัดทำสรุปคู่มือการติดตั้งและคู่มือการใช้งานเบื้องต้นโดยละเอียดทั้งหมดที่เสนอในรูปแบบ Soft copy ๒ ชุด และ Hard copy ๑ ชุด ในวันส่งมอบงาน

๖.๑.๗ ผู้ชนะการประกวดราคาจะต้องส่งมอบรายละเอียดรายการอุปกรณ์ที่ติดตั้งทั้งหมด ซึ่งจะต้องมีข้อมูลดังต่อไปนี้เป็นอย่างน้อย ได้แก่ ชื่ออุปกรณ์ รุ่นอุปกรณ์ ชนิดอุปกรณ์ ชื่อบริษัทผู้ผลิตอุปกรณ์ หมายเลขประจำตัวอุปกรณ์ (Serial No) หมายเลขประจำตัวอุปกรณ์ย่อย (ถ้ามี) วันที่รับประกัน วันที่หมดรับประกัน ฯลฯ ตามข้อมูลของอุปกรณ์ที่มีจริง

๖.๑.๘ การติดตั้งอุปกรณ์ทั้งหมดที่ผู้ชนะการประกวดราคาได้เสนอ หรือติดตั้งอุปกรณ์และระบบอื่นใดเพิ่มเติม ซึ่งหากไม่ได้ระบุไว้ในข้อกำหนดของคณะฯ ให้อยู่ในดุลยพินิจของคณะฯที่จะเป็นผู้กำหนดลักษณะและรูปแบบของการติดตั้ง โดยขึ้นอยู่กับความจำเป็นและสภาพการใช้งานจริง เพื่อให้ระบบสามารถใช้งานได้อย่างมีประสิทธิภาพเป็นสำคัญ

๖.๒ การฝึกอบรม

ผู้ชนะการประกวดราคาต้องจัดการฝึกอบรมเชิงปฏิบัติการให้กับบุคลากรของคณะฯ จำนวนไม่น้อยกว่า ๓ คน ในการใช้งานอุปกรณ์ จำนวนไม่น้อยกว่า ๔ ชั่วโมง ดังนี้

๖.๒.๑ อุปกรณ์ในข้อ ๔.๑–๔.๓ จำนวนไม่น้อยกว่า ๓ คน เป็นเวลาไม่น้อยกว่า ๒ วัน โดยวันละไม่น้อยกว่า ๔ ชั่วโมง

๖.๒.๒ อุปกรณ์ในข้อ ๔.๖ จำนวนไม่น้อยกว่า ๓ คน จำนวนไม่น้อยกว่า ๔ ชั่วโมง

โดยผู้ชนะการประกวดราคาจะต้องเสนอรายชื่อ พร้อมทั้งประวัติ และเอกสารแสดงการฝึกอบรมหรือการรับรองความรู้ของผู้ที่จะมาเป็นวิทยากรในการอบรมให้กับคณะฯ พิจารณา ซึ่งหากวิทยากรที่เสนอขาดความรู้ความสามารถหรือขาดความเหมาะสมตามดุลยพินิจของคณะฯ ผู้ชนะการประกวดราคาจะต้องจัดหา จัดจ้าง และเสนอรายชื่อวิทยากรใหม่ ให้กับคณะฯ พิจารณาอีกครั้ง จนกว่าจะผ่านการพิจารณาของคณะฯ

๖.๓ เงื่อนไขเฉพาะ

๖.๓.๑ เป็นผลิตภัณฑ์ของแท้ ของใหม่ทั้งหมด ไม่เคยใช้งานมาก่อน

๖.๓.๒ มีศูนย์บริการของบริษัทเจ้าของผลิตภัณฑ์ในจังหวัดเชียงใหม่สำหรับอุปกรณ์ในข้อ ๔.๖ และ ๔.๗

๖.๓.๓ ผู้เสนอราคาต้องเป็นผู้ได้รับการแต่งตั้งอย่างเป็นทางการในการยื่นเสนออุปกรณ์ในข้อ ๔.๑ - ๔.๕ สำหรับโครงการนี้ โดยมีหนังสือแต่งตั้งจากเจ้าของผลิตภัณฑ์หรือสำนักงานสาขาในประเทศไทย เพื่อรับการสนับสนุนในการให้บริการหลังการขาย

๖.๓.๔ วิศวกรระบบเครือข่ายต้องสามารถปรับเปลี่ยนค่า configuration ของระบบได้ตามความต้องการของคณะฯ

๖.๔ ข้อกำหนดทั่วไปของอุปกรณ์ที่เสนอ

๖.๔.๑ อุปกรณ์ต้องสามารถเชื่อมต่อใช้งานกับระบบคอมพิวเตอร์และระบบสื่อสารข้อมูลที่คณะฯ มีอยู่เดิมได้ ตรงตามมาตรฐานสากลของการรับส่งข้อมูล

๖.๔.๒ อุปกรณ์สื่อสารต้องผลิตขึ้นมาตามมาตรฐานผลิตภัณฑ์อุตสาหกรรมด้านต่างๆ ที่เกี่ยวข้อง ซึ่งรวมถึงด้านไฟฟ้า โทรคมนาคม ความปลอดภัย และการจำกัดคลื่นรบกวน (RFI) และระบุหมายเลขรองรับ การผ่านการทดสอบตามมาตรฐาน FCC และ/หรือ UL และ/หรือ มาตรฐานอื่นๆ ที่เกี่ยวข้อง (ถ้ามี)

๖.๔.๓ อุปกรณ์ต้องสามารถใช้งานกับไฟฟ้า ๒๒๐ VAC ๕๐Hz ตามมาตรฐานของไทยได้ โดยไม่ต้องใช้อุปกรณ์แปลงระบบไฟฟ้า

๖.๔.๔ ขนาดหน่วยความจำ (RAM, ROM, BIOS, FLASH, FIRMWARE) นั้นคิดที่ ๑K = ๑,๐๒๔ bytes; ๑M = ๑,๐๒๔ K; ๑G =๑,๐๒๔ M

๖.๔.๕ ความเร็วในการรับ-ส่งข้อมูลผ่านเครือข่าย ความจุของจานแม่เหล็ก (formatted-capacity) และเทปเก็บข้อมูล (uncompressed-capacity) แบบต่าง ๆ นั้นคิดที่ ๑K = ๑,๐๐๐ bytes; ๑M = ๑,๐๐๐ K; ๑G = ๑,๐๐๐ M

๖.๔.๖ อุปกรณ์และซอฟต์แวร์ทุกส่วนจะต้องสามารถทำงานที่การคำนวณและแสดงผลวันที่ วันและเวลาถึงปี ค.ศ. ๒๐๒๐ ได้โดยไม่มีปัญหาใดๆ ทั้งสิ้น

๗. ระยะเวลาการส่งมอบ

กำหนดส่งมอบภายใน ๑๒๐ วัน นับถัดจากวันลงนามในสัญญา

๘. งบประมาณวงเงินในการจัดหา

๕,๕๕๐,๐๐๐.- บาท (ห้าล้านห้าแสนห้าหมื่นบาทถ้วน) ในการเสนอราคาผู้เสนอราคาต้องเสนอลดราคาขั้นต่ำ (Minimum Bid) ไม่น้อยกว่าครั้งละ ๑๐,๐๐๐.- บาท จากราคาสูงสุดของการประกวดราคาฯ และ การเสนอราคาครั้งถัด ๆ ไป ต้องเสนอลดราคาครั้งละไม่น้อยกว่า ๑๐,๐๐๐.-บาท จากครั้งสุดท้ายที่เสนอลดแล้ว

๙. หน่วยงานรับผิดชอบดำเนินการ คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่

สถานที่ติดต่อเพื่อขอทราบข้อมูลเพิ่มเติม หรือเสนอแนะวิจารณ์ หรือแสดงความคิดเห็นเป็นลายลักษณ์อักษรโดยเปิดเผยตัว ระบุชื่อ นามสกุลจริง พร้อมที่อยู่และหมายเลขโทรศัพท์ที่สามารถติดต่อได้ตามช่องทางดังต่อไปนี้.-

๙.๑ หน่วยจัดหาพัสดุ งานพัสดุ คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ ๑๑๐ ถนนอินทวโรรส ต. สุเทพ อ.เมือง จ.เชียงใหม่ ๕๐๒๐๐

๙.๒ จดหมายอิเล็กทรอนิกส์ Email Address : medpurch@mail.med.cmu.ac.th

๙.๓ โทรสารหมายเลข : ๐๕๓-๒๑๐๑๓๖

ทั้งนี้ภายใน ๓ วันทำการ นับตั้งแต่คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ ได้เผยแพร่ลง Website เพื่อคณะแพทยศาสตร์ จะได้นำข้อคิดเห็นหรือข้อเสนอแนะมาพิจารณาต่อไป

ประกาศ ณ วันที่ ๕ เดือน มิถุนายน พ.ศ.๒๕๕๖

(รองศาสตราจารย์ นายแพทย์วัฒนา นาคเจริญ)
คณบดีคณะแพทยศาสตร์