ประกาศสำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่
เรื่อง การกำหนดหัวข้อร่างขอบเขตของงาน (Term of Reference: TOR)
โครงการบำรุงรักษาระบบป้องกันภัยเครือข่าย
คอมพิวเตอร์ มหาวิทยาลัยเชียงใหม่

1. หลักการและเหตุผล

ระบบเครือข่ายคอมพิวเตอร์และระบบอินเทอร์เน็ตเป็นโครงสร้างพื้นฐานที่สำคัญประการหนึ่งในการดำเนินงานต่างๆ ขององค์กรไม่ว่าจะขนาดเล็กหรือใหญ่ ประกอบกับการพัฒนาระบบเครือข่ายที่ก้าวหน้าไปอย่างไม่หยุดยั้ง ได้ก่อให้เกิดภัยคุกคามต่อระบบเครือข่ายในรูปแบบต่างๆ มากมายหลากหลายรูปแบบ ทั้งในเรื่องของการโจมตีเพื่อให้ระบบเครือข่ายไม่สามารถทำงานได้ หรือแม้กระทั่งการทำลายและขโมยข้อมูลที่สำคัญในระบบฯ ด้วยเหตุนี้ระบบเครือข่ายที่ดีและมีประสิทธิภาพ จึงต้องสามารถกำจัดภัยคุกคามเหล่านี้ให้ลดน้อยลงมากที่สุดเท่าที่จะเป็นไปได้ ดังนั้นองค์กรที่ตระหนักถึงความสำคัญของความปลอดภัยระบบเครือข่ายและมีข้อมูลที่สำคัญในระบบเครือข่าย จึงจำเป็นอย่างยิ่งที่จะต้องหาวิธีในการจัดการกับภัยคุกคามดังกล่าวด้วยเทคนิคและวิธีการต่างๆ

การรักษาความปลอดภัยระบบเครือข่ายคอมพิวเตอร์ (Network Security) เป็นสิ่งจำเป็นสำหรับกับการจัดการระบบเครือข่ายคอมพิวเตอร์ โดยการกำหนดนโยบายการรักษาความปลอดภัยการให้บริการต่างๆ ของระบบเครือข่ายฯ เช่น การอนุญาตหรือไม่อนุญาตให้ใช้บริการบางอย่างได้ เพื่อป้องกันการเข้าใช้งานที่อาจเกิดเป็นภัยคุกคามต่อระบบเครือข่ายคอมพิวเตอร์นั้น จำเป็นอย่างยิ่งที่จะต้องมีระบบป้องกันภัยคุกคามระบบเครือข่ายคอมพิวเตอร์ (Network IPS–Network Intrusion Prevention System) ในการช่วยตรวจสอบและป้องกันภัยคุกคามในรูปแบบต่างๆ เช่น การใช้งานระบบเครือข่ายฯ ที่ไม่ปกติ และการพยายามโจมตีระบบเครือข่ายคอมพิวเตอร์เพื่อให้ไม่สามารถใช้งานได้ตามปกติ เป็นต้น

ด้วยเหตุผลดังกล่าวข้างต้น มหาวิทยาลัยเชียงใหม่ จึงได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยระบบเครือข่ายคอมพิวเตอร์จึงจำเป็นอย่างยิ่ง ที่จะต้องทำการขยายเวลาการรับประกันอุปกรณ์เป็นระยะเวลา 3 ปี ของอุปกรณ์เดิมที่จัดซื้อ เมื่อปี 2553 และ 2555 เพื่อประหยัดงบประมาณในการจัดซื้ออุปกรณ์ระบบเครือข่าย และ เป็นการเตรียมการรับมือกับภัยคุกคามผ่านระบบเครือข่ายคอมพิวเตอร์ ด้วยการจัดหาระบบป้องกันภัยคุกคามระบบเครือข่าย (Network IPS – Network Intrusion Prevention System)และระบบเครือข่ายเสมือนส่วนตัว(Virtual Private Network:VPN)เพื่อให้บริการเครือข่ายงานวิจัย ที่มีประสิทธิภาพ เพื่อป้องกันระบบเครือข่ายของมหาวิทยาลัย ให้มีความปลอดภัยและปลอดจากภัยคุกคามต่างๆ

เพื่อให้บริการแก่หน่วยงานภายใน นักศึกษา และบุคลากรให้มีความปลอดภัยและมีประสิทธิภาพสูงสุด

2. วัตถุประสงค์

2.1 เพื่อให้การจัดการความปลอดภัยระบบเครือข่ายคอมพิวเตอร์เป็นไปด้วยความสะดวกและมีประสิทธิภาพ

2.2 เพื่อให้ระบบเครือข่ายของมหาวิทยาลัยปลอดภัยจากภัยคุกคามรูปแบบต่างๆ จากระบบเครือข่ายอินเทอร์เน็ต

2.3 เพื่อป้องกันเครื่องคอมพิวเตอร์ที่อยู่ภายในระบบเครือข่ายของมหาวิทยาลัยให้มีความปลอดภัยจากภัยคุกคาม และการโจมตีผ่านระบบเครือข่ายอินเทอร์เน็ต

2.4 เพื่อให้หน่วยงานภายใน นักศึกษา และบุคลากรของมหาวิทยาลัยมีความพึงพอใจและเกิดความเชื่อมั่นในการใช้งานระบบเครือข่ายของมหาวิทยาลัย

3. การพิจารณาทางเทคนิค

3.1 มหาวิทยาลัยเชียงใหม่จะพิจารณาราคาเฉพาะของผู้เข้าประกวดราคาที่ผ่านข้อเสนอทาง เทคนิคและผ่านข้อกำหนดเกี่ยวกับคุณสมบัติเท่านั้น นอกจากนี้ มหาวิทยาลัยเชียงใหม่ยังขอสงวนสิทธิ์ในการพิจารณาระบบป้องกันภัยคุกคามระบบเครือข่ายคอมพิวเตอร์ (Network IPS– Network Intrusion Prevention System) และระบบประกอบอื่นๆ ที่ผู้เข้าประกวดราคาเสนอซึ่งมีคุณสมบัติอื่นที่นอกเหนือไปจากคุณสมบัติที่จำเป็นและคุณสมบัติที่ควรมี และมหาวิทยาลัยสงวนสิทธิ์ที่จะพิจารณาผู้เข้าประกวดราคารายที่เสนอราคาอยู่ในวงเงิน และให้ประโยชน์แก่มหาวิทยาลัยมากที่สุดก่อน

3.2 ผู้เข้าประกวดราคามีหน้าที่แสดงเอกสารต่างๆ เพื่อยืนยันหรือแสดงให้เห็นถึงคุณสมบัติต่างๆ ที่จะต้องเป็นไปตามข้อกำหนดหรือมีคุณสมบัติที่ดีกว่าข้อกำหนด โดยเอกสารที่นำมาแสดงจะต้องเป็นเอกสารตัวจริงหรือเป็นเอกสารสำเนาที่เป็นทางการสามารถเชื่อถือได้ และเป็นที่ยอมรับโดยทั่วไป ซึ่งผู้เข้าประกวดราคามีหน้าที่จะต้องเปรียบเทียบข้อกำหนดที่มหาวิทยาลัยกำหนดในแต่ละข้อกับคุณสมบัติของตนเองและของอุปกรณ์ต่างๆ ที่เสนอ โดยจะต้องระบุให้ชัดเจนว่าเอกสารที่นำมาเสนอ ข้อความในประโยคใดที่ใช้ยืนยันข้อกำหนดหมายเลขใดของมหาวิทยาลัย โดยผู้เข้าประกวดราคามีหน้าที่ทำสัญลักษณ์แสดงบนข้อความในประโยคที่ใช้ยืนยัน ได้แก่ การขีดเส้นใต้ หรือการระบายสี พร้อมระบุหมายเลขลำดับของข้อกำหนดที่จะทำการยืนยันให้เห็นชัดเจน

ซึ่งหากผู้เข้าประกวดราคาขาดเอกสารยืนยัน หรือขาดการทำสัญลักษณ์แสดงบนข้อความในประโยคที่ใช้ยืนยัน หรือแสดงเอกสารไม่ชัดเจนทำให้ขาดข้อกำหนดหนึ่งใดในข้อกำหนดของมหาวิทยาลัย ให้ถือว่าผู้เข้าประกวดราคาไม่ผ่านการพิจารณาทางด้านเทคนิค

3.3 ให้จัดทำรายละเอียดข้อเสนอด้านเทคนิคของระบบงานที่เสนอ ในรูปแบบดังต่อไปนี้

หัวข้อ	คุณลักษณะที่กำหนด	คุณลักษณะที่เสนอ	เอกสารอ้างอิง (หน้า, ข้อ)
ระบุหัวข้อให้ตรงกับที่กำหนดในเอกสารนี้	ให้คัดลอกจากข้อกำหนดที่กำหนดในเอกสารนี้	ให้ระบุความสามารถหรือคุณลักษณะเฉพาะของระบบที่เสนอ	ให้ระบุหรืออ้างอิงถึงเอกสารในข้อเสนอที่เกี่ยวข้อง และทำสัญลักษณ์แสดงข้อความในประโยคของเอกสารหรือในแคตตาล็อกนั้นให้ชัดเจน

3.4 ผู้เข้าประกวดราคาจะต้องเสนอรายละเอียดการบำรุงรักษาอุปกรณ์และระบบตามที่มหาวิทยาลัยได้ระบุไว้ใน ตารางที่ 1 เท่านั้น ซึ่งหากผู้เข้าประกวดราคาได้เสนอรายการอุปกรณ์อื่นใดที่นอกเหนือไปจากข้อกำหนดดังกล่าว มหาวิทยาลัยขอสงวนสิทธิ์ในการเปลี่ยนแปลงคุณสมบัติรายการอุปกรณ์และระบบที่เสนอดังกล่าวได้ในภายหลัง เพื่อให้ระบบสามารถใช้งานได้อย่างมีประสิทธิภาพ

4. กำหนดระยะเวลาการดำเนินการ

ผู้ชนะการการประกวดราคาต้องส่งมอบกำหนดการเข้าบำรุงรักษาระบบป้องกันภัยคุกคามระบบเครือข่ายคอมพิวเตอร์ (Network IPS–Network Intrusion Prevention System) และอุปกรณ์ประกอบอื่นๆ ถ้ามีทั้งหมดภายในระยะเวลา 60 วัน นับจากวันลงนามในสัญญาจ้าง ซึ่งหากเกินกว่าระยะเวลาดังกล่าว ผู้ชนะการประกวดราคาต้องถูกปรับในอัตราวันละ 5,000 บาท (ห้าพันบาทถ้วน)

5. ขอบเขตการบำรุงรักษาระบบป้องกันภัยเครือข่ายคอมพิวเตอร์

การบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ (Network IPS–Network Intrusion Prevention System) อุปกรณ์ให้บริการระบบเครือข่ายเสมือนส่วนตัว(Virtual Private Network:VPN) และอุปกรณ์ประกอบอื่นๆ จะต้องเป็นไปตามข้อกำหนด ในภาคผนวก ของ TOR ให้ครบตามข้อกำหนด ทั้งนี้อาคารที่จะทำการบำรุงรักษา ระบบป้องกันภัยคุกคามระบบเครือข่ายคอมพิวเตอร์ (Network IPS–Network Intrusion Prevention System) ตามแต่อุปกรณ์ที่ติดตั้งทั่วมหาวิทยาลัย อุปกรณ์ให้บริการระบบเครือข่ายเสมือนส่วนตัว(Virtual Private Network:VPN) และอุปกรณ์ประกอบอื่นๆ นั้นให้ติดตั้ง ณ อาคารสำนักบริการเทคโนโลยีสารสนเทศ

6. ข้อกำหนดการดำเนินการบำรุงรักษา

ข้อกำหนดการติดตั้งโดยทั่วไป

6.1 ก่อนที่ผู้ชนะการประกวดราคาจะเข้าดำเนินการใดๆ ผู้ชนะการประกวดราคาจะต้องทำจดหมายแจ้งให้กับมหาวิทยาลัยรับทราบก่อนจะเข้าดำเนินการจริงอย่างน้อย 5 วันทำการ และจะต้องรอให้ได้รับการอนุมัติจากมหาวิทยาลัยก่อน จึงจะสามารถดำเนินการใดๆ ได้ ซึ่งหากผู้ชนะการประกวดราคาเข้าทำการติดตั้งระบบใดๆ โดยไม่ได้รับการอนุมัติจากมหาวิทยาลัย มหาวิทยาลัยมีสิทธิที่จะให้บริษัทดำเนินการรื้อถอนระบบๆ ต่างที่ได้ติดตั้งไปแล้ว โดยให้ถือเป็นความผิดและความรับผิดชอบของผู้ชนะการประกวดราคา

6.2 ชนะการประกวดราคาต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น เนื่องจากการติดตั้งอุปกรณ์หรือความเสียหายใดที่เกิดขึ้นเนื่องจากการปฏิบัติงานของผู้ชนะการประกวดราคา ผู้ชนะการประกวดราคาจะต้องดำเนินการซ่อมแซมแก้ไขให้อยู่ในสภาพเดิมโดยเร็วและยินยอมชดใช้ค่าเสียหายที่เกิดขึ้นให้กับมหาวิทยาลัย

6.3 ผู้ชนะการประกวดราคาต้องเป็นผู้จัดหาสายหรืออุปกรณ์เพิ่มเติมอื่นๆ ที่จำเป็นสำหรับการติดตั้งอุปกรณ์ระบบป้องกันภัยคุกคามระบบเครือข่ายคอมพิวเตอร์ (Network IPS–Network Intrusion Prevention System) และอุปกรณ์ประกอบอื่นๆ ที่ทางผู้ชนะการประกวดราคาเสนอมาให้สามารถทำงานได้อย่างมีประสิทธิภาพ

6.4 การติดตั้งอุปกรณ์ระบบป้องกันภัยคุกคามระบบเครือข่ายคอมพิวเตอร์ (Network IPS–Network Intrusion Prevention System) และอุปกรณ์ประกอบอื่นๆ ที่ผู้ชนะการประกวดราคาได้เสนอ หรือติดตั้งอุปกรณ์และระบบอื่นใดเพิ่มเติม ซึ่งหากไม่ได้ระบุไว้ในข้อกำหนดของมหาวิทยาลัย ให้อยู่ในดุลยพินิจของมหาวิทยาลัยที่จะเป็นผ

กำหนดลักษณะและรูปแบบของการติดตั้ง โดยขึ้นอยู่กับความจำเป็นและสภาพการใช้งานจริง เพื่อให้ระบบสามารถใช้งานได้อย่างมีประสิทธิภาพเป็นสำคัญ

6.5 สายสัญญาณเชื่อมต่อ (Patch cable) ที่จะนำมาใช้กับอุปกรณ์ระบบป้องกันภัยคุกคามระบบเครือข่ายคอมพิวเตอร์จะต้องเป็นสายที่เป็นชนิดที่เหมาะสม ซึ่งมีความยาวของสายและจำนวนที่จำเป็นต้องใช้งานจริง โดยเป็นสายที่มีคุณภาพมาตรฐานและผลิตสำเร็จรูปจากโรงงาน

7. รายการที่มหาวิทยาลัยต้องการให้บำรุงรักษา

มหาวิทยาลัยเชียงใหม่มีความต้องการจะบำรุงรักษาป้องกันภัยคุกคามระบบเครือข่ายคอมพิวเตอร์ (Network IPS–Network Intrusion Prevention System) อุปกรณ์ให้บริการระบบเครือข่ายเสมือนส่วนตัว(Virtual Private Network:VPN) และอุปกรณ์ประกอบอื่นๆ ที่เกี่ยวข้องดังรายการต่อไปนี้ โดตามที่กำหนดใน ภาคผนวก

8. การตรวจรับการบำรุงรักษา

8.1 ผู้ชนะการประกวดราคาต้องจัดเตรียมเอกสารต่างๆ สำหรับการส่งมอบและการตรวจรับอย่างเหมาะสมให้กับทางมหาวิทยาลัยเชียงใหม่พิจารณา

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

8.3 มหาวิทยาลัยจะทำการการตรวจรับโครงการทั้งหมด เมื่อระบบและอุปกรณ์ทั้งหมดที่ได้ทำการติดตั้งโดยผู้ชนะการประกวดราคาจะต้องสามารถเชื่อมต่อกับระบบเครือข่ายเดิมของมหาวิทยาลัยที่มีอยู่แล้วได้อย่างมีประสิทธิภาพ ตามคุณลักษณะของระบบและอุปกรณ์ที่กำหนดไว้

8.4 ผู้ชนะการประกวดราคาต้องจัดทำป้ายประจำอุปกรณ์สำหรับอุปกรณ์ทุกชิ้นที่ส่งมอบที่สามารถติดป้ายได้ โดยป้ายประจำอุปกรณ์ต้องมีข้อความประกอบด้วย ชื่ออุปกรณ์ หมายเลขประจำอุปกรณ์ ชื่อผู้ขาย วันที่ติดตั้ง เบอร์โทรศัพท์ติดต่อแจ้งซ่อม และวันหมดรับประกัน เป็นอย่างน้อย

8.5 ผู้ชนะการประกวดราคาต้องทำหนังสือแจ้งการส่งมอบระบบทั้งหมดเพื่อตรวจรับให้ทางมหาวิทยาลัยเชียงใหม่ทราบอย่างน้อย 5 วันทำการ ก่อนการส่งมอบ ผู้ชนะการประกวดราคาต้องจัดทำเอกสารระบุอุปกรณ์ คู่มือ หรือสิ่งอื่นใดที่จะทำการ

ตรวจรับ โดยระบุ ชนิด ยี่ห้อ รุ่น หมายเลขประจำอุปกรณ์ (serial number) สถานที่ติดตั้งหรือรายละเอียดอื่นใดที่จำเป็นในการตรวจรับให้มหาวิทยาลัยเชียงใหม่

9. **การดูแลรักษาและการรับประกันภายหลังการติดตั้ง**

9.1 อุปกรณ์และระบบต่างๆ ที่ผู้ชนะการประกวดราคาได้เสนอให้กับมหาวิทยาลัยจะต้องรับประกันถึงความเสียหายของอุปกรณ์และระบบเป็นเวลาไม่น้อยกว่า 3 ปี โดยหากเกิดความเสียหายใดๆ ขึ้นกับอุปกรณ์หรือระบบ ผู้ชนะการประกวดราคาจะต้องดำเนินการแก้ไขให้กับมหาวิทยาลัยโดยไม่คิดค่าใช้จ่ายใดๆ ในการดำเนินการ

9.2 ผู้ชนะการประกวดราคาจะต้องทำการซ่อมบำรุงระบบ ทำความสะอาดอุปกรณ์และอัพเดตรุ่นของซอฟต์แวร์ (Preventive Maintenance) ทั้งหมดที่ได้ทำการติดตั้งให้กับมหาวิทยาลัย ตามระยะเวลาที่รับประกันอุปกรณ์ โดยจะต้องทำการซ่อมบำรุงระบบทุกๆ 6 เดือน นับจากวันที่เริ่มรับประกัน และจะต้องจัดทำรายงานผลของการทำการซ่อมบำรุงระบบให้กับมหาวิทยาลัยทราบทุกครั้ง ซึ่งหากไม่มีการดำเนินการซ่อมบำรุงระบบและส่งผลรายงานภายใน 14 วันนับจากวันที่ครบกำหนดแต่ละรอบ มหาวิทยาลัยจะดำเนินการปรับเป็นรายครั้งในอัตราครั้งละ 10,000 (หนึ่งหมื่นบาทถ้วน)

9.3 หากเกิดความเสียหายกับอุปกรณ์ใดๆ ที่ผู้ชนะการประกวดราคาได้เสนอ ผู้ชนะการประกวดราคาจะต้องดำเนินการแก้ไขให้อุปกรณ์ที่เสียหายให้สามารถใช้งานได้ตามปกติ หรือจัดหาอุปกรณ์อื่นใดที่มีคุณสมบัติเท่าเทียมหรือดีกว่ามาทดแทนเพื่อให้ระบบสามารถใช้งานได้ตามปกติ ภายในระยะเวลา 24 ชั่วโมงหลังจากได้รับแจ้งจากมหาวิทยาลัยผ่านทางโทรศัพท์ หรือทางโทรสาร หรือทางจดหมายอิเล็กทรอนิกส์ ซึ่งในกรณีที่ผู้ชนะการประกวดราคาไม่สามารถแก้ไขให้ระบบทำงานได้ตามกำหนด ผู้ชนะการประกวดราคาต้องถูกปรับในอัตราชั่วโมงละ 1,000 บาท (หนึ่งพันบาทถ้วน) โดยเศษของชั่วโมงนับเป็นหนึ่งชั่วโมง

9.4 หากผู้ชนะการประกวดราคานิ่งเฉยไม่ดำเนินการใดๆ ที่จะแก้ไขความเสียหายของอุปกรณ์ที่เป็นของผู้ชนะการประกวดราคาภายหลังจาก 48 ชั่วโมง นับจากที่มหาวิทยาลัยได้แจ้งให้ผู้ชนะการประกวดราคาผ่านทางจดหมายหรือโทรสาร มหาวิทยาลัยมีสิทธิ์ที่จะดำเนินการจัดหา จัดซื้อ จัดจ้าง หรือดำเนินการใดๆ เพื่อแก้ไขให้อุปกรณ์ที่เสียหายสามารถใช้งานได้เป็นปกติ และมหาวิทยาลัยสามารถเรียกเก็บค่าใช้จ่ายในการดำเนินการทั้งหมดจากผู้ชนะการประกวดราคา

10. ระยะเวลาในการดำเนินการ 60 วัน นับจากวันลงนามในสัญญา

11. ระยะเวลาส่งมอบ 60 วัน

12. **วงเงินในการจัดหา 2,500,000บาท (สองล้านห้าแสนบาทถ้วน)**

13. **ในการประกวดราคาจัดซื้อจัดจ้างด้วยระบบอิเล็กทรอนิกส์**

ผู้เสนอราคาจะต้องเสนอราคาลดขั้นต่ำ (Minimum Bid) ไม่น้อยกว่าครั้งละ 5,000 บาท จากราคาสูงสุดในการประกวดราคาและการเสนอราคาครั้งถัดไปต้องเสนอราคาครั้งละไม่น้อยกว่า 5,000 บาท จากราคาครั้งสุดท้ายที่เสนอลดแล้ว

14. **สถานที่ติดต่อเพื่อขอทราบข้อมูลเพิ่มเติมหรือเสนอแนะวิจารณ์หรือแสดงความคิดเห็นโดยเปิดเผยตัว**

งานการเงินการคลังและพัสดุ
สำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่
เลขที่ 239 ถนนห้วยแก้ว ตำบลสุเทพ อำเภอเมือง จังหวัดเชียงใหม่ 50200
โทรศัพท์ 053-94-3807
โทรสาร 053-94-3825
E-mail : benjaporn.pong@cmu.ac.th / opas.m @cmu.ac.th

ภาคผนวก ก

คุณสมบัติเฉพาะของผู้เข้าประกวดราคา

1. คุณสมบัติของผู้เข้าประกวดราคา

1.1 มีเงินทุนจดทะเบียนไม่ต่ำกว่า 1 ล้านบาท

1.2 จดทะเบียนทำธุรกิจด้านระบบเครือข่ายคอมพิวเตอร์ในประเทศไทยไม่น้อยกว่า 1 ปี

1.3 ผู้เข้าประกวดราคาต้องเป็นผู้ที่ไม่มีชื่ออยู่ในหนังสือแจ้งเวียนทิ้งงานของทางราชการ

1.4 ผู้เข้าประกวดราคาต้องไม่เป็นผู้ที่ได้รับเอกสิทธิ์หรือความคุ้มครองทางการทูต ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่สละสิทธิ์หรือความคุ้มครองทางการทูต

ภาคผนวก ข

<u>คุณสมบัติการขยายระยะเวลารับประกันอุปกรณ์รักษาความปลอดภัย VPN</u>

1. บริษัทฯ ต้องทำการขยายเวลารับประกันอุปกรณ์รักษาความปลอดภัย VPN ยี่ห้อ DellSonicwall รุ่น EX6000 ซึ่งมีหมายเลขเครื่อง 0017C543CA36 ตามสัญญาเลขที่ 018/2555 ออกไปอีกเป็นเวลา 3 ปี โดยเริ่มนับจากวันที่หมดสัญญา
2. รองรับจำนวนผู้เข้าใช้งานในเวลาเดียวกันได้ไม่น้อยกว่า 100 User และสามารถขยายเพิ่มภายหลังรวมได้ไม่น้อยกว่า 250 User โดยไม่ต้องมีการเปลี่ยนอุปกรณ์
3. เป็นซอฟต์แวร์ที่มหาวิทยาลัยมีสิทธิ์ใช้งานได้อย่างถูกต้องตามกฎหมาย และมหาวิทยาลัยสามารถที่จะปรับปรุงรุ่น (Upgrade) ได้ตลอดระยะเวลารับประกัน
4. รองรับมาตรฐานการเข้ารหัสแบบ DES, 3DES, RC4, AES และ MD5, SHA Hash ได้
5. สามารถทำการ Query ไปยัง LDAP/AD แบบอ้างอิง Dynamic groups ได้
6. สามารถตรวจสอบเครื่อง End Point บนแพลตฟอร์ม Windows, Windows Mobile, Macintosh และ Linux ก่อนเข้าใช้งาน
7. สามารถป้องกันการโจรกรรม ชื่อผู้ใช้/รหัสผ่าน จากโปรแกรมประเภท Keylogger โดยใช้ Virtual Keyboard
8. สามารถกำหนด Quarantine Zone สำหรับกักและแจ้งผู้ใช้งาน จาก Client ที่มีคุณสมบัติไม่ครบตามที่กำหนด
9. สามารถกำหนด Deny Zone สำหรับป้องกันการเข้าใช้งาน จาก Client ที่มีคุณสมบัติตามที่กำหนด
10. สนับสนุนระบบปฏิบัติการต่างๆอย่างน้อยดังนี้ Windows8, Windows 7, Windows Vista, Windows XP, Macintosh OS X, Linux, Web–enabled mobile devices
11. สนับสนุนเวบบราวเซอร์ต่างๆ อย่างน้อยดังนี้ Internet Explorer, Mozilla Firefox, Safari, Chrome
12. สนับสนุนการเชื่อมต่อไปยัง Client/Server แอพพลิเคชั่น ผ่านโปรโตคอลต่างๆอย่างน้อยได้ดังนี้ TCP, UDP, ICMP, VoIP, Reverse–connection, Bi–directional
13. สนับสนุน Traffic Redirection ทั้งแบบ Split และ Redirect All สำหรับการเชื่อมต่อแบบ Tunnel
14. มีโปรแกรม SSLVPN Client สำหรับใช้เชื่อมต่อโดยไม่ผ่านเวบบราวเซอร์ บนแพลตฟอร์ม Windows, Macintosh และ Linux
15. มีโปรแกรม SSLVPN Client ชนิดทำงานเป็น Windows Service

16. มีระบบบริหารจัดการตัวอุปกรณ์แบบ Web-based และ Command line
17. สามารถดูรายชื่อผู้ที่กำลังเชื่อมต่อรวมถึงสามารถตัดออกจากระบบได้
18. สามารถแสดงข้อมูลกราฟสรุปค่าสถานะของอุปกรณ์ เช่น CPU/Memory/Swap Utilization, Network Bandwidth, Active Users ในช่วงระยะเวลาต่างๆได้
19. สามารถส่งข้อมูล Log ไปยัง Syslog server ได้
20. ผู้เสนอราคาต้องได้รับการแต่งตั้งเป็นตัวแทนจำหน่ายจากเจ้าของผลิตภัณฑ์ในการเสนอราคาครั้งนี้พร้อมการรับประกัน Hardware และ Software ไม่น้อยกว่า 3 ปี

ภาคผนวก ค.

รายละเอียดของการบำรุงรักษาอุปกรณ์

1. บริษัทฯ ต้องทำการขยายเวลารับประกันอุปกรณ์ Sourcefire รุ่น SF 3D8250 ซึ่งมีหมายเลขเครื่อง 11121600400095-A และระบบจัดการ (Defense Center) รวมถึงอุปกรณ์ประกอบอื่นๆ ตามสัญญาเลขที่ 011/2555 ออกไปอีกเป็นเวลา 3 ปี ทุกอุปกรณ์โดยเริ่มนับจากวันที่หมดสัญญา
2. อุปกรณ์ต้องยังคงมีความสามารถดังต่อไปนี้
   2.1 มีความสามารถในการตรวจจับ(IPS Throughput) ไม่น้อยกว่า 10Gbps และรองรับการขยายความสามารถในการตรวจจับได้สูงสุดไม่น้อยกว่า 40Gbps
   2.2 อุปกรณ์ต้องสามารถทำ Hardware Bypass ในกรณี Hardware/Software เกิดปัญหารวมถึงกรณีไฟฟ้าดับ โดยสามารถเลือกแบบ Fail-open หรือ Fail-Close ในแต่ละ segment ได้
   2.3 สามารถทำงานได้ทั้งแบบ IDS Mode สูงสุดเป็นจำนวน 10 ports หรือสูงสุด 5 segment ในโหมด In-line IPS
   2.4 ป้องกันการโจมตีแบบ Denial of Service (DoS) Attack และ DDoS ได้
   2.5 ป้องกันการบุกรุกแบบ Vulnerability Exploit, Reconnaissance (port scan/sweep)
   2.6 ป้องกันได้ตั้งแต่ระดับ Layer 2 (ARP) Attacks
   2.7 ป้องกันเครือข่ายและสามารถตรวจจับวิธีการบุกรุกดังนี้ Overflow, Backdoor Program, Trojan Horse ได้
3. สามารถแจ้งเตือนและโต้ตอบการโจมตีด้วยวิธีต่อไปนี้
   3.1 Drop
   3.2 Drop เมื่อเกิดเหตุการถึงจำนวนที่ตั้งไว้ (Threshold)
   3.3 ติดต่อกับอุปกรณ์ภายนอกเพื่อป้องกันข้อมูลไม่ให้วิ่งผ่าน (external remediation) โดยสามารถ ทำงานร่วมกับอุปกรณ์เครือข่าย เช่น เราเตอร์ได้
4. สามารถบริหารจัดการอุปกรณ์ได้ผ่าน Command-line หรือ GUI โดยผ่าน Web แบบ HTTPS
5. สามารถใช้งานมาตรฐาน IPv6 ทั้งการจัดการ IPS และการตรวจสอบข้อมูลการโจมตี
6. ระบบการจัดการ (Management) โดยมีความสามารถดังต่อไปนี้

6.1 สามารถจัดการจัดเก็บ Log และสามารถส่ง Log ไปที่ระบบ
จัดเก็บ Log ศูนย์กลาง (Centralized Log Management)

6.2 สามารถบริหารจัดการนโยบายเรื่องความปลอดภัย และส่งไปยังอุปกรณ์ได้ โดยจะต้องไม่มีผลกระทบต่อการตรวจสอบการโจมตีระหว่างที่มีการติดตั้งนโยบายความปลอดภัยชุดใหม่

6.3 สามารถแสดงสถานะการทำงานของอุปกรณ์ (Dashboard) โดยสามารถแสดงถึงสถานะการถูกโจมตีของระบบเครือข่าย และสามารถเลือกแสดงในระดับความรุนแรงที่สนใจได้ โดยสามารถเลือกแสดงเฉพาะการโจมตีที่มีผลกระทบอย่างรุนแรงกับเครือข่ายที่กำหนดได้

6.4 สามารถปรับแต่งการแสดงผลของ Dashboard โดยกำหนดเงื่อนไขที่ต้องการแสดง (search criteria) ได้เอง รวมถึงสามารถปรับช่วงเวลาการแสดงข้อมูลได้อย่างน้อยเป็น ชั่วโมง หรือ วัน

6.5 สามารถกำหนดให้มีการดึงข้อมูล (signature/rule) จากผู้ผลิตได้อัตโนมัติ

6.6 อนุญาตให้ผู้ใช้สามารถสร้างรูปแบบการตรวจสอบเองได้ (custom signature/rule) โดยมีเครื่องมือ หรือ GUI เพื่อช่วยในการสร้าง

6.7 สามารถนำเสนอข้อมูลที่ผ่านระบบตามแอพพลิเคชั่นทั้งในลักษณะจำนวน flow หรือปริมาณข้อมูล (KB/s) ได้

6.8 สามารถจัดเก็บข้อมูลที่มีการโจมตี (Packet Capture) และสามารถเรียกดูได้โดยตรงจากอุปกรณ์บริหาร จัดการ

6.9 สามารถแสดงชื่อผู้ใช้งานบนระบบเครือข่ายได้ โดยสามารถทำงานร่วมกับระบบไดเรกทอรีเช่น LDAP และ สามารถกำหนดให้ตรวจสอบชื่อผู้ใช้จากโปรโตคอลที่ไม่มีการเข้ารหัส เช่น POP3 ได้

7. ระบบจะต้องสามารถให้คำแนะนำและปรับแต่งนโยบายเรื่องความปลอดภัยได้อย่างอัตโนมัติ โดยอาศัยข้อมูลได้ทั้งจากการทำ Passive Scan หรือ Active Scan
8. ผู้เสนอราคาต้องได้รับการแต่งตั้งเป็นตัวแทนจำหน่ายจากเจ้าของผลิตภัณฑ์ในการเสนอราคาครั้งนี้พร้อมการรับประกัน Hardware และ Software ไม่น้อยกว่า 3 ปี

ขอรับรองว่าการกำหนดคุณลักษณะของพัสดุ ข้างต้นเป็นไปตามข้อกำหนด ในมติคณะรัฐมนตรีตามหนังสือที่ นร 0203/ว157 ลงวันที่ 27 ธันวาคม 2519

ประกาศ ณ วันที่ 21 มีนาคม 2557

(ลงนาม) ถนอมพร เลาหจรัสแสง

(รองศาสตราจารย์ ดร.ถนอมพร เลาหจรัสแสง)

ผู้อำนวยการสำนักบริการเทคโนโลยีสารสนเทศ

ตารางแสดงการบันทึกรายละเอียดประกาศร่าง TOR

รายการข้อมูล	คำอธิบาย
1. ชื่อหน่วยงาน	สำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่
2. ชื่อเรื่องร่าง TOR	**โครงการบำรุงรักษาระบบป้องกันภัยเครือข่ายคอมพิวเตอร์ มหาวิทยาลัยเชียงใหม่**
3. วงเงินงบประมาณ (บาท)	2,500,000 บาท (สองล้านห้าแสนบาทถ้วน)
4. ราคากลาง (บาท)	2,500,000 บาท (สองล้านห้าแสนบาทถ้วน)
5. ราคาสูงสุดที่พึงรับได้ (บาท)	2,500,000 บาท (สองล้านห้าแสนบาทถ้วน)
6. วันที่ประกาศ	21 มีนาคม 2557
7. จำนวนวันที่สิ้นสุดรับฟังข้อวิจารณ์	25มีนาคม 2557
8. อีเมล์แอดเดรส	benpjit@chiangmai.ac.th /opas@cm.ac.th
9. ที่อยู่โครงการ	สำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่ เลขที่ 239 ถ.ห้วยแก้ว ต.สุเทพ อ.เมือง จ.เชียงใหม่
10. จังหวัด	เชียงใหม่