โครงการติดตั้งอุปกรณ์ระบบป้องกันภัยคุกคาม ระบบเครือข่ายคอมพิวเตอร์ มหาวิทยาลัยเชียงใหม่

๑. หลักการและเหตุผล

ระบบเครือข่ายคอมพิวเตอร์และระบบอินเทอร์เน็ตเป็นโครงสร้างพื้นฐานที่สำคัญประการหนึ่งในการดำเนินงานต่างๆ ขององค์กรไม่ว่าจะขนาดเล็กหรือใหญ่ ประกอบกับการพัฒนาระบบเครือข่ายที่ก้าวหน้าไปอย่างไม่หยุดยั้ง ได้ก่อให้เกิดภัยคุกคามต่อระบบเครือข่ายในรูปแบบต่างๆ มากมายหลากหลายรูปแบบ ทั้งในเรื่องของการโจมตีเพื่อให้ระบบเครือข่ายไม่สามารถทำงานได้ หรือแม้กระทั่งการทำลายหรือโจรกรรมข้อมูลที่สำคัญในระบบฯ ด้วยเหตุนี้ระบบเครือข่ายที่ดีและมีประสิทธิภาพ จึงต้องสามารถกำจัดภัยคุกคามเหล่านี้ให้ลดน้อยลงมากที่สุดเท่าที่จะเป็นไปได้ ดังนั้นองค์กรที่ตระหนักถึงความสำคัญของความปลอดภัยระบบเครือข่ายและมีข้อมูลที่สำคัญในระบบเครือข่าย จึงจำเป็นอย่างยิ่งที่จะต้องหาวิธีในการจัดการกับภัยคุกคามดังกล่าวด้วยเทคนิคและวิธีการต่างๆ

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

ด้วยเหตุผลดังกล่าวข้างต้น มหาวิทยาลัยเชียงใหม่ได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยระบบเครือข่ายคอมพิวเตอร์เป็นอย่างยิ่ง ทำให้ต้องมีการเตรียมการรับมือกับภัยคุกคามผ่านระบบเครือข่ายคอมพิวเตอร์ ด้วยการจัดหาระบบป้องกันภัยคุกคามระบบเครือข่าย (Network IPS – Network Intrusion Prevention System) ที่มีประสิทธิภาพเพื่อป้องกันระบบเครือข่ายของมหาวิทยาลัย ให้มีความปลอดภัยและปลอดจากภัยคุกคามต่างๆ เพื่อให้การดำเนินงานระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย ที่ได้ให้บริการแก่หน่วยงานภายใน นักศึกษา และบุคลากรมีความปลอดภัยและมีประสิทธิภาพสูงสุด

๒. วัตถุประสงค์

๒.๑ เพื่อให้การจัดการความปลอดภัยระบบเครือข่ายคอมพิวเตอร์เป็นไปด้วยความสะดวกและมีประสิทธิภาพ

๒.๒ เพื่อให้ระบบเครือข่ายของมหาวิทยาลัยปลอดภัยจากภัยคุกคามรูปแบบต่างๆ จากระบบเครือข่ายอินเทอร์เน็ต

๒.๓ เพื่อป้องกันเครื่องคอมพิวเตอร์ที่อยู่ภายในระบบเครือข่ายของมหาวิทยาลัยให้มีความปลอดภัยจากภัยคุกคาม และการโจมตีผ่านระบบเครือข่ายอินเทอร์เน็ต

๒.๔ เพื่อให้หน่วยงานภายใน, นักศึกษา และบุคลากรของมหาวิทยาลัยมีความพึงพอใจและเกิดความเชื่อมั่นในการใช้งานระบบเครือข่ายของมหาวิทยาลัย

๓. เป้าหมายและแนวทางการใช้ประโยชน์

โครงการนี้มีเป้าหมายและแนวทางการสร้างผลสัมฤทธิ์จากโครงการให้เกิดประโยชน์ดังต่อไปนี้

๓.๑ ระบบเครือข่ายของมหาวิทยาลัยมีระบบการจัดการระบบรักษาความปลอดภัยที่สามารถบริหารและจัดการได้อย่างมีประสิทธิภาพ, ข้อมูลของระบบรักษาความปลอดภัยมีความทันสมัยอยู่เสมอ และสามารถป้องกันภัยคุกคามระบบเครือข่ายคอมพิวเตอร์ที่หลากหลายรูปแบบอย่างมีประสิทธิภาพสูงสุด

๓.๒ ระบบเครือข่ายของมหาวิทยาลัยปลอดภัยจากภัยคุกคามระบบเครือข่ายคอมพิวเตอร์จากระบบอินเทอร์เน็ต

๓.๓ เครื่องคอมพิวเตอร์ที่อยู่ภายในระบบเครือข่ายของมหาวิทยาลัยปลอดภัยจากการโจมตีจากระบบเครือข่ายอินเทอร์เน็ต โดยมีอัตราการถูกภัยคุกคามน้อยที่สุด

๓.๔ หน่วยงานภายใน, นักศึกษา และบุคลากรของมหาวิทยาลัยมีความมั่นใจในการใช้งานระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยในแง่ของความปลอดภัยในการใช้งานระบบอินเทอร์เน็ต

๔. ระบบป้องกันภัยคุกคามระบบเครือข่ายคอมพิวเตอร์ที่ต้องการ

มหาวิทยาลัยเชียงใหม่มีความประสงค์ที่จะประกวดราคาเพื่อติดตั้งระบบป้องกันภัยคุกคามระบบเครือข่าย (IPS-Network Intrusion Prevention System) และอุปกรณ์ประกอบอื่นๆ ที่สามารถเชื่อมโยงและใช้งานร่วมกับระบบเครือข่ายและระบบป้องกันภัยคุกคามระบบเครือข่าย (IPS-Network Intrusion Prevention System) เดิมของมหาวิทยาลัยได้อย่างมีประสิทธิภาพ

๕. การพิจารณาทางเทคนิค

๕.๑ มหาวิทยาลัยเชียงใหม่จะพิจารณาราคาเฉพาะของ**ผู้เข้าประกวดราคาที่ผ่านข้อเสนอทางเทคนิคและผ่านข้อกำหนดเกี่ยวกับคุณสมบัติเท่านั้น** นอกจากนี้มหาวิทยาลัยเชียงใหม่ยังขอสงวนสิทธิ์ในการพิจารณาระบบป้องกันภัยคุกคามระบบเครือข่ายคอมพิวเตอร์ (Network IPS- Network Intrusion Prevention System) และระบบประกอบอื่นๆ ที่ผู้เข้าประกวดราคาเสนอซึ่งมีคุณสมบัติอื่นที่นอกเหนือไปจากคุณสมบัติที่จำเป็นและคุณสมบัติที่ควรมี และมหาวิทยาลัยสงวนสิทธิ์ที่จะพิจารณาผู้เข้าประกวดราคารายที่เสนอราคาอยู่ในวงเงิน และให้ประโยชน์แก่มหาวิทยาลัยมากที่สุดก่อน

๕.๒ ผู้เข้าประกวดราคามีหน้าที่แสดงเอกสารต่างๆ เพื่อยืนยันหรือแสดงให้เห็นถึงคุณสมบัติต่างๆ ที่จะต้องเป็นไปตามข้อกำหนดหรือมีคุณสมบัติที่ดีกว่าข้อกำหนด โดยเอกสารที่นำมาแสดงจะต้องเป็นเอกสารตัวจริงหรือเป็นเอกสารสำเนาที่เป็นทางการ สามารถเชื่อถือได้ และเป็นที่ยอมรับโดยทั่วไป ซึ่งผู้เข้าประกวดราคามีหน้าที่จะต้องเปรียบเทียบข้อกำหนดที่มหาวิทยาลัยกำหนดในแต่ละข้อกับคุณสมบัติของตนเองและของอุปกรณ์ต่างๆ ที่เสนอ โดยจะต้องระบุให้ชัดเจนว่าเอกสารที่นำมาเสนอ ข้อความในประโยคใดที่ใช้ยืนยันข้อกำหนดหมายเลขใดของมหาวิทยาลัย โดยผู้เข้า

ประกวดราคามีหน้าที่ทำสัญลักษณ์แสดงบนข้อความในประโยคที่ใช้ยืนยัน ได้แก่ การขีดเส้นใต้ หรือการระบายสี พร้อมระบุหมายเลขลำดับของข้อกำหนดที่จะทำการยืนยันให้เห็นชัดเจน ซึ่ง**หากผู้เข้า**ประกวดราคาขาดเอกสารยืนยัน หรือขาดการทำสัญลักษณ์แสดงบนข้อความในประโยคที่ใช้ยืนยัน หรือแสดงเอกสารไม่ชัดเจนทำให้ขาดข้อกำหนดหนึ่งใดในข้อกำหนดของมหาวิทยาลัย ให้ถือว่าผู้เข้าประกวดราคาไม่ผ่านการพิจารณาทางด้านเทคนิค

๕.๓ ให้จัดทำรายละเอียดข้อเสนอด้านเทคนิคของระบบงานที่เสนอ ในรูปแบบดังต่อไปนี้

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

๕.๔ **ผู้เข้าประกวดราคาจะต้องเสนออุปกรณ์และระบบเฉพาะที่มหาวิทยาลัยได้ระบุไว้ใน**ตารางที่ ๑ เท่านั้น ซึ่งหากผู้เข้าประกวดราคาได้เสนอรายการอุปกรณ์อื่นใดที่นอกเหนือไปจากข้อกำหนดดังกล่าว มหาวิทยาลัยขอสงวนสิทธิ์ในการเปลี่ยนแปลงคุณสมบัติรายการอุปกรณ์และระบบที่เสนอดังกล่าวได้ในภายหลัง เพื่อให้ระบบสามารถใช้งานได้อย่างมีประสิทธิภาพ

๖. กำหนดระยะเวลาการติดตั้ง

ผู้เข้าประกวดราคาต้องส่งมอบระบบป้องกันภัยคุกคามระบบเครือข่ายคอมพิวเตอร์ (Network IPS-Network Intrusion Prevention System) และอุปกรณ์ประกอบอื่นๆ ทั้งหมดภายในระยะเวลา ๖๐ วัน นับจากวันลงนามในสัญญาจ้าง ซึ่งหากเกินกว่าระยะเวลาดังกล่าว ผู้ชนะการประกวดราคาต้องถูกปรับในอัตราวันละ ๕,๐๐๐ บาท (ห้าพันบาทถ้วน)

๗. ขอบเขตการติดตั้งระบบป้องกันภัยคุกคามระบบเครือข่ายคอมพิวเตอร์

การติดตั้งระบบป้องกันภัยคุกคามระบบเครือข่ายคอมพิวเตอร์ (Network IPS-Network Intrusion Prevention System) และอุปกรณ์ประกอบอื่นๆ จะต้องเป็นไปตามข้อกำหนด มาตรฐานความปลอดภัย มาตรฐานการติดตั้งอุปกรณ์และสายสัญญาณของผู้ผลิต และมาตรฐานสากลอื่นๆ ที่เกี่ยวข้อง ทั้งนี้ผู้เข้าประกวดราคาจะต้องเป็นผู้รับผิดชอบค่าใช้จ่ายทั้งหมดในการติดตั้ง ตลอดจนค่าใช้จ่ายในการปรับปรุงและซ่อมแซมส่วนที่ได้รับผลกระทบจากการติดตั้งดังกล่าว ทั้งนี้อาคารที่จะทำการติดตั้งระบบป้องกันภัยคุกคามระบบเครือข่ายคอมพิวเตอร์ (Network IPS-Network Intrusion Prevention System) และอุปกรณ์ประกอบอื่นๆ นั้นให้ติดตั้ง ณ อาคารสำนักบริการเทคโนโลยีสารสนเทศ

8. ข้อกำหนดการติดตั้งระบบป้องกันภัยคุกคามระบบเครือข่ายคอมพิวเตอร์และอุปกรณ์ประกอบอื่นๆ

ข้อกำหนดการติดตั้งโดยทั่วไป

๘.๑ก่อนที่ผู้ชนะการประกวดราคาจะเข้าดำเนินการใดๆ ผู้ชนะการประกวดราคาจะต้องทำจดหมายแจ้งให้กับมหาวิทยาลัยรับทราบก่อนจะเข้าดำเนินการจริงอย่างน้อย ๕ วันทำการ และจะต้องรอให้ได้รับการอนุมัติจากมหาวิทยาลัยก่อน จึงจะสามารถดำเนินการใดๆ ได้ ซึ่งหากผู้ชนะการประกวดราคาเข้าทำการติดตั้งระบบใดๆ โดยไม่ได้รับการอนุมัติจากมหาวิทยาลัย มหาวิทยาลัยมีสิทธิที่จะให้บริษัทดำเนินการรื้อถอนระบบๆ ต่างที่ได้ติดตั้งไปแล้ว โดยให้ถือเป็นความผิดและความรับผิดชอบของผู้ชนะการประกวดราคา

๘.๒ผู้ชนะการประกวดราคาต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น เนื่องจากการติดตั้งอุปกรณ์หรือความเสียหายใดที่เกิดขึ้นเนื่องจากการปฏิบัติงานของผู้ชนะการประกวดราคา ผู้ชนะการประกวดราคาจะต้องดำเนินการซ่อมแซมแก้ไขให้อยู่ในสภาพเดิมโดยเร็ว และยินยอมชดใช้ค่าเสียหายที่เกิดขึ้นให้กับมหาวิทยาลัย

๘.๓ผู้ชนะการประกวดราคาต้องเป็นผู้จัดหาสายหรืออุปกรณ์เพิ่มเติมอื่นๆ ที่จำเป็นสำหรับการติดตั้งอุปกรณ์ระบบป้องกันภัยคุกคามระบบเครือข่ายคอมพิวเตอร์ (Network IPS-Network Intrusion Prevention System) และอุปกรณ์ประกอบอื่นๆ ที่ทางผู้ชนะการประกวดราคาเสนอมาให้สามารถทำงานได้อย่างมีประสิทธิภาพ

๘.๔การติดตั้งอุปกรณ์ระบบป้องกันภัยคุกคามระบบเครือข่ายคอมพิวเตอร์ (Network IPS-Network Intrusion Prevention System) และอุปกรณ์ประกอบอื่นๆ ที่ผู้ชนะการประกวดราคาได้เสนอ หรือติดตั้งอุปกรณ์และระบบอื่นใดเพิ่มเติม ซึ่งหากไม่ได้ระบุไว้ในข้อกำหนดของมหาวิทยาลัย ให้อยู่ในดุลยพินิจของมหาวิทยาลัยที่จะเป็นผู้กำหนดลักษณะและรูปแบบของการติดตั้ง โดยขึ้นอยู่กับความจำเป็นและสภาพการใช้งานจริง เพื่อให้ระบบสามารถใช้งานได้อย่างมีประสิทธิภาพเป็นสำคัญ

๘.๕สายสัญญาณเชื่อมต่อ (Patch cable) ที่จะนำมาใช้กับอุปกรณ์ระบบป้องกันภัยคุกคามระบบเครือข่ายคอมพิวเตอร์จะต้องเป็นสายที่เป็นชนิดที่เหมาะสม ซึ่งมีความยาวของสายและจำนวนที่จำเป็นต้องใช้งานจริง โดยเป็นสายที่มีคุณภาพมาตรฐานและผลิตสำเร็จรูปจากโรงงาน

๙. รายการอุปกรณ์ที่มหาวิทยาลัยต้องการ

มหาวิทยาลัยเชียงใหม่มีความต้องการติดตั้งระบบป้องกันภัยคุกคามระบบเครือข่ายคอมพิวเตอร์ (Network IPS-Network Intrusion Prevention System) และอุปกรณ์ประกอบอื่นๆ ที่เกี่ยวข้องดังรายการต่อไปนี้ โดยจะกำหนดคุณสมบัติเฉพาะของอุปกรณ์ในภาคผนวก ก

ตารางที่ ๑ แสดงรายการอุปกรณ์ที่ต้องการจัดซื้อ

ลำดับ	รายการอุปกรณ์	จำนวน	หน่วย	สถานที่ติดตั้ง
๑	อุปกรณ์ Network IPS (Network Intrusion Prevention System)	๑	ชุด	อาคารสำนักบริการเทคโนโลยีสารสนเทศ

๑๐. การตรวจรับอุปกรณ์และการรับประกัน

๑๐.๑ ผู้ชนะการประกวดราคาต้องจัดเตรียมเอกสารต่างๆ สำหรับการส่งมอบและการตรวจรับอย่างเหมาะสมให้กับทางมหาวิทยาลัยเชียงใหม่พิจารณา โดยประกอบด้วยข้อมูลดังต่อไปนี้เป็นอย่างน้อย ได้แก่ ชื่ออุปกรณ์ รุ่นอุปกรณ์ ชนิดอุปกรณ์ ชื่อบริษัทผู้ผลิตอุปกรณ์ หมายเลขประจำตัวอุปกรณ์ (Serial No), หมายเลขประจำตัวอุปกรณ์ย่อย (ถ้ามี) วันที่รับประกัน วันที่หมดรับประกัน ฯลฯ

๑๐.๒ มหาวิทยาลัยจะทำการการตรวจรับโครงการทั้งหมด เมื่อระบบและอุปกรณ์ทั้งหมดที่ได้ทำการติดตั้งโดยผู้ชนะการประกวดราคาจะต้องสามารถเชื่อมต่อกับระบบเครือข่ายเดิมของมหาวิทยาลัยที่มีอยู่แล้วได้อย่างมีประสิทธิภาพ ตามคุณลักษณะของระบบและอุปกรณ์ที่กำหนดไว้

๑๐.๓ ผู้ชนะการประกวดราคาต้องจัดทำป้ายประจำอุปกรณ์สำหรับอุปกรณ์ทุกชิ้นที่ส่งมอบที่สามารถติดป้ายได้ โดยป้ายประจำอุปกรณ์ต้องมีข้อความประกอบด้วย ชื่ออุปกรณ์ หมายเลขประจำอุปกรณ์ ชื่อผู้ขาย วันที่ติดตั้ง เบอร์โทรศัพท์ติดต่อแจ้งซ่อมและวันหมดรับประกัน เป็นอย่างน้อย

๑๐.๔ ผู้ชนะการประกวดราคาต้องทำหนังสือแจ้งการส่งมอบระบบทั้งหมดเพื่อตรวจรับให้ทางมหาวิทยาลัยเชียงใหม่ทราบอย่างน้อย ๕ วันทำการ ก่อนการส่งมอบ ผู้ชนะการประกวดราคาต้องจัดทำเอกสารระบุอุปกรณ์ คู่มือ หรือสิ่งอื่นใดที่จะทำการตรวจรับโดยระบุ ชนิด ยี่ห้อ รุ่น หมายเลขประจำอุปกรณ์ (serial number) สถานที่ติดตั้งหรือรายละเอียดอื่นใดที่จำเป็นในการตรวจรับให้มหาวิทยาลัยเชียงใหม่

๑๐.๕ ชิ้นส่วนอุปกรณ์จะต้องรับประกันถึงความเสียหายเป็นเวลาไม่น้อยกว่า ๒ ปี โดยหากเกิดความเสียหายใดๆ ขึ้นกับชิ้นส่วนอุปกรณ์ ผู้ชนะการประกวดราคาจะต้องดำเนินการแก้ไขให้กับมหาวิทยาลัยโดยไม่คิดค่าใช้จ่ายใดๆ ในการดำเนินการ

๑๐.๖ หากเกิดความเสียหายกับชิ้นส่วนอุปกรณ์ที่ผู้ชนะการประกวดราคาได้เสนอ ผู้ชนะการประกวดราคาจะต้องดำเนินการแก้ไขให้อุปกรณ์ที่เสียหายให้สามารถใช้งานได้ตามปกติ หรือจัดหาอุปกรณ์อื่นใดที่มีคุณสมบัติเท่าเทียมหรือดีกว่ามาทดแทนเพื่อให้ระบบสามารถใช้งานได้ตามปกติ ภายในระยะเวลา ๒๔ ชั่วโมงหลังจากได้รับแจ้งจากมหาวิทยาลัยผ่านทางโทรศัพท์ หรือทางโทรสาร หรือทางจดหมายอิเล็กทรอนิกส์ ซึ่งในกรณีที่ผู้ชนะการประกวดราคาไม่สามารถแก้ไขให้ระบบทำงานได้ตามกำหนด ผู้ชนะการประกวดราคาต้องถูกปรับในอัตราชั่วโมงละ ๑,๐๐๐ บาท (หนึ่งพันบาทถ้วน) โดยเศษของชั่วโมงนับเป็นหนึ่งชั่วโมง

๑๑. ระยะเวลาในการดำเนินการ ๖๐ วันนับจากวันลงนามในสัญญา

๑๒. ระยะเวลาในการส่งมอบ ๖๐ วัน

๑๓. วงเงินในการจัดหา ๕,๐๐๐,๐๐๐ บาท (ห้าล้านบาทถ้วน)

ขอรับรองว่าการกำหนดคุณลักษณะของพัสดุ ข้างต้นเป็นไปตามข้อกำหนดในมติคณะรัฐมนตรีตาม
หนังสือที่ นร. ๐๒๐๓/ว๑๕๗ ลงวันที่ ๒๗ ธันวาคม ๒๕๑๙

ประกาศ ณ วันที่ ๔ เมษายน ๒๕๕๕

(ลงนาม) ถนอมพร เลาหจรัสแสง
(รองศาสตราจารย์ ดร. ถนอมพร เลาหจรัสแสง)
ผู้อำนวยการสำนักบริการเทคโนโลยีสารสนเทศ

ภาคผนวก ก

คุณสมบัติเฉพาะของผู้เข้าประกวดราคาและอุปกรณ์ระบบต่างๆ ที่มหาวิทยาลัยต้องการ ซึ่งทั้งหมดจะต้องมีคุณสมบัติดังต่อไปนี้เป็นอย่างน้อย

๑. คุณสมบัติของผู้เข้าประกวดราคา

๑.๑มีเงินทุนจดทะเบียนไม่ต่ำกว่า ๑ ล้านบาท

๑.๒ จดทะเบียนทำธุรกิจด้านระบบเครือข่ายคอมพิวเตอร์ในประเทศไทยไม่น้อยกว่า ๑ ปี

๑.๓ ผู้เข้าประกวดราคาต้องเป็นผู้ที่ไม่มีชื่ออยู่ในหนังสือแจ้งเวียนทิ้งงานของทางราชการ

๑.๔ ผู้เข้าประกวดราคาต้องไม่เป็นผู้ที่ได้รับเอกสิทธิ์หรือความคุ้มครองทางการทูต ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่สละสิทธิ์หรือความคุ้มครองทางการทูต

๑.๕ ผู้เข้าประกวดราคาต้องมีบุคลากรประจำที่มีความรู้ความเข้าใจเกี่ยวกับอุปกรณ์ระบบป้องกันภัยคุกคามระบบเครือข่ายคอมพิวเตอร์ (Network IPS-Network Intrusion Prevention System) ที่เสนอ ซึ่งสามารถให้ความช่วยเหลือกับมหาวิทยาลัยเชียงใหม่ได้ โดยผู้เข้าประกวดราคาจะต้องส่งรายชื่อของบุคลากรประจำ ซึ่งจ้างงานมาไม่น้อยกว่า ๔ เดือน และจบการศึกษาระดับปริญญาตรีหรือสูงกว่าทางด้านวิศวกรรมคอมพิวเตอร์หรือวิทยาการคอมพิวเตอร์ จำนวนรวมไม่น้อยกว่า ๑ คน โดยแนบประวัติการศึกษา การฝึกอบรม ใบประกาศที่เกี่ยวข้อง และเอกสารการจ้างงาน ซึ่งขณะดำเนินการติดตั้งอุปกรณ์ให้กับมหาวิทยาลัยจะต้องมีบุคลากรที่เสนอร่วมอยู่ด้วยจำนวนไม่น้อยกว่า ๑ คน

๑.๖ มีหนังสือรับรองจากบริษัทผู้ผลิตว่าให้การสนับสนุนการประกวดราคาในครั้งนี้

๒. คุณสมบัติของอุปกรณ์ที่ต้องการ

อุปกรณ์ตรวจจับและป้องกันการบุกรุกบนระบบเครือข่าย(Intrusion Prevention System)

๒.๑ เป็นอุปกรณ์แบบ Hardware Appliance ที่ออกแบบมาเพื่อทำหน้าที่ป้องกันการบุกรุกบนระบบเครือข่าย (IPS) โดยเฉพาะ โดยไม่ใช่อุปกรณ์แบบ UTM หรืออุปกรณ์ Firewall ที่ทำงานแบบ IPS โดยมีผลการทดสอบจากหน่วยงานที่เชื่อถือได้ เช่น ICSA และ NSS Labs โดยได้รับการประเมินจากหน่วยงานที่น่าเชื่อถือให้เป็นผู้นำในกลุ่มตลาดอุปกรณ์ IPS เช่น Gartner IPS Magic Quadrant เป็นต้น

๒.๒ มีความสามารถในการตรวจจับ (IPS Throughput) ไม่น้อยกว่า ๑๐ Gbps และรองรับการขยายความสามารถในการตรวจจับได้สูงสุดไม่น้อยกว่า ๔๐ Gbps

๒.๓ มี Network Interface แบบ ๑ Gbps Copper ไม่น้อยกว่า ๘ พอร์ต, ๑๐ Gbps แบบ SR ไม่น้อยกว่า ๒ พอร์ต โดยรองรับการขยายจำนวนพอร์ตเพิ่มเติมในอนาคตอีกไม่น้อยกว่า ๖ พอร์ต (๓x๑๐ Gbps segment) เพื่อรองรับ IPS Throughput ๔๐Gbps ตามข้อ ๒.๒ ทั้งนี้ทางผู้เสนอราคาต้องจัดเตรียม Module ๑๐ Gbps แบบ SR จำนวน ๒ พอร์ต เพื่อใช้เชื่อมต่อระหว่างอุปกรณ์ IPS กับอุปกรณ์ Router ของทางมหาวิทยาลัย และอุปกรณ์ IPS กับอุปกรณ์สลับสัญญาณหลัก (Core Switch) ของมหาวิทยาลัยมาในการเสนอราคาครั้งนี้ด้วย

๒.๔ มีพอร์ตสำหรับบริหารจัดการอุปกรณ์แบบ ๑๐/๑๐๐ Ethernet หรือดีกว่า อย่างน้อย ๑ พอร์ต และ Serial Port อย่างน้อย ๑ port (Out of band management)

๒.๕ อุปกรณ์ต้องสามารถทำ Hardware Bypass ในกรณี Hardware/Software เกิดปัญหารวมถึงกรณีไฟฟ้าดับ โดยสามารถเลือกแบบ Fail-open หรือ Fail-Close ในแต่ละ segment ได้

๒.๖ สามารถทำงานได้ทั้งแบบ IDS Mode สูงสุดเป็นจำนวน ๑๐ ports หรือสูงสุด ๕ segment ในโหมด In-line IPS

๒.๗ สามารถป้องกันการโจมตีและการบุกรุกเครือข่ายได้อย่างน้อยดังนี้

๒.๗.๑ ป้องกันการระบาดของ Virus และ Worm

๒.๗.๒ ป้องกันการโจมตีแบบ Denial of Service (DoS) Attack และ DDoS ได้

๒.๗.๓ ป้องกันการบุกรุกแบบ Vulnerability Exploit, Reconnaissance (port scan/sweep)

๒.๗.๔ ป้องกันเทคนิคการหลบซ่อนการโจมตีแบบ IP Defragmentation, TCP Stream Segmentation, RPC Fragmentation, URL Obfuscation, HTML Obfuscation, HTML Evasion และ FTP Evasion ได้

๒.๗.๕ ป้องกันได้ตั้งแต่ระดับ Layer ๒ (ARP) Attacks

๒.๗.๖ ป้องกันเครือข่ายและสามารถตรวจจับวิธีการบุกรุกดังนี้ Overflow, Backdoor Program, Trojan Horse และ Spy ware

๒.๘ สามารถแจ้งเตือนและโต้ตอบการโจมตีด้วยวิธีต่อไปนี้

๒.๘.๑ Drop

๒.๘.๒ Drop เมื่อเกิดเหตุการณ์ถึงจำนวนที่ตั้งไว้ (Threshold)

๒.๘.๓ ติดต่อกับอุปกรณ์ภายนอกเพื่อป้องกันข้อมูลไม่ให้วิ่งผ่าน (external remediation) โดยสามารถทำงานร่วมกับอุปกรณ์เครือข่าย เช่น เร้าเตอร์ได้

๒.๙ อุปกรณ์ IPS จะต้องถูกออกแบบมาเพื่อให้มีความน่าเชื่อถือสูง โดยจะต้องมีระบบ Redundant Power Supply และใช้อุปกรณ์เก็บข้อมูลแบบ SSD (Solid State Disk) แทนฮาร์ดดิสก์ในการเก็บข้อมูล

๒.๑๐ สามารถบริหารจัดการอุปกรณ์ได้ผ่าน Command-line หรือ GUI โดยผ่าน Web แบบ HTTPS

๒.๑๑ สามารถใช้งานมาตรฐาน IPv๖ ทั้งการจัดการ IPS และการตรวจสอบข้อมูลการโจมตี

๒.๑๒ ได้รับมาตรฐาน ความปลอดภัย FCC , UL หรือ CE เป็นอย่างน้อย

๒.๑๓ อุปกรณ์ที่เสนอต้องสามารถติดตั้งบน Rack ขนาด ๑๙ นิ้วได้

๒.๑๔ อุปกรณ์ที่เสนอต้องมาพร้อมกับระบบการจัดการ (Management) โดยมีความสามารถอย่างน้อยดังต่อไปนี้

๒.๑๔.๑ สามารถจัดการจัดเก็บ Log และสามารถส่ง Log ไปที่ระบบจัดเก็บ Log ศูนย์กลาง (Centralized Log Management)

๒.๑๔.๒ สามารถบริหารจัดการนโยบายเรื่องความปลอดภัย และส่งไปยังอุปกรณ์ได้ โดยจะต้องไม่มีผลกระทบต่อการตรวจสอบการโจมตีระหว่างที่มีการติดตั้งนโยบายความปลอดภัยชุดใหม่

๒.๑๔.๓ สามารถแสดงสถานะการทำงานของอุปกรณ์ (Dashboard) โดยสามารถแสดงถึงสถานะการถูกโจมตีของระบบเครือข่าย และสามารถเลือกแสดงในระดับความรุนแรงที่สนใจได้ โดยสามารถเลือกแสดงเฉพาะการโจมตีที่มีผลกระทบอย่างรุนแรงกับเครือข่ายที่กำหนดได้

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

๒.๑๔.๕ สามารถกำหนดให้มีการดึงข้อมูล (signature/rule) จากผู้ผลิตได้อัตโนมัติ

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

๒.๑๔.๗ สามารถนำเสนอข้อมูลที่ผ่านระบบตามแอพพลิเคชั่นทั้งในลักษณะจำนวน flow หรือปริมาณข้อมูล (KB/s) ได้

๒.๑๔.๘ สามารถจัดเก็บข้อมูลที่มีการโจมตี (Packet Capture) และสามารถเรียกดูได้โดยตรงจากอุปกรณ์บริหารจัดการ

๒.๑๔.๙ สามารถแสดงชื่อผู้ใช้งานบนระบบเครือข่ายได้ โดยสามารถทำงานร่วมกับระบบไดเรกทอรีเช่น LDAP และ สามารถกำหนดให้ตรวจสอบชื่อผู้ใช้จากโปรโตคอลที่ไม่มีการเข้ารหัส เช่น POP๓ ได้

๒.๑๕ ระบบจะต้องสามารถให้คำแนะนำและปรับแต่งนโยบายเรื่องความปลอดภัยได้อย่างอัตโนมัติ โดยอาศัยข้อมูลได้ทั้งจากการทำ Passive Scan หรือ Active Scan

๒.๑๖ รองรับการรับข้อมูลจากอุปกรณ์ภายนอก เช่น ระบบ Vulnerability Management หรือข้อมูลจากระบบเครือข่ายเช่น Netflow เพื่อนำมาใช้ในการประเมินความเสี่ยงของระบบได้

๒.๑๗ ผู้เสนอราคาจะต้องดำเนินการจัดการอบรมให้แก่ผู้ดูแลระบบของมหาวิทยาลัย โดยหลักสูตรดังกล่าวต้องเป็นหลักสูตรอย่างเป็นทางการจากเจ้าของผลิตภัณฑ์ จำนวนไม่น้อยกว่า ๒ คน และระยะเวลาในการอบรมไม่น้อยกว่า ๓ วัน โดยค่าใช้จ่ายในการอบรมทั้งหมดผู้เสนอราคาต้องเป็นผู้รับผิดชอบ

๒.๑๘ ผู้เสนอราคาต้องได้รับการแต่งตั้งเป็นตัวแทนจำหน่ายจากเจ้าของผลิตภัณฑ์ในการเสนอราคาครั้งนี้ และจะต้องนำเสนออุปกรณ์พร้อมการรับประกัน Hardware และ Software ไม่น้อยกว่า ๒ ปี

ตารางแสดงการบันทึกรายละเอียดประกาศร่าง TOR

รายการข้อมูล	คำอธิบาย
๑. ชื่อหน่วยงาน	สำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่
๒. ชื่อเรื่องร่าง TOR	โครงการติดตั้งอุปกรณ์ระบบป้องกันภัยคุกคาม ระบบเครือข่ายคอมพิวเตอร์
๓. วงเงินงบประมาณ (บาท)	๕,๐๐๐,๐๐๐ บาท (ห้าล้านบาทถ้วน)
๔. ราคากลาง (บาท)	๕,๐๐๐,๐๐๐ บาท (ห้าล้านบาทถ้วน)
๕. ราคาสูงสุดที่พึงรับได้ (บาท)	๕,๐๐๐,๐๐๐ บาท (ห้าล้านบาทถ้วน)
๖. วันที่ประกาศ	๔ เมษายน ๒๕๕๕
๗. จำนวนวันที่สิ้นสุดรับฟังข้อวิจารณ์	๑๐ เมษายน ๒๕๕๕
๘. อีเมล์แอดเดรส	benjaporn.pong@cmu.ac.th/ opas.m@cmu.ac.th
๙.ที่อยู่โครงการ	สำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่ เลขที่ ๒๓๙ ถนนห้วยแก้ว ต.สุเทพ อ.เมือง จ.เชียงใหม่
๑๐. จังหวัด	เชียงใหม่