ประกาศสำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่
เรื่องกำหนดหัวข้อร่างขอบเขตของงาน (Term of Reference: TOR)
โครงการจัดซื้อระบบรักษาความปลอดภัยผ่านระบบเครือข่าย
มหาวิทยาลัยเชียงใหม่

1. หลักการและเหตุผล

ระบบเครือข่ายคอมพิวเตอร์และระบบอินเทอร์เน็ตเป็นโครงสร้างพื้นฐานที่สำคัญประการหนึ่งในการดำเนินงานต่างๆ ขององค์กร ไม่ว่าจะขนาดเล็กหรือใหญ่ ประกอบกับการพัฒนาระบบเครือข่ายที่ก้าวหน้าไปอย่างไม่หยุดยั้ง ได้ก่อให้เกิดภัยคุกคามต่อระบบเครือข่ายในรูปแบบต่างๆ มากมายหลากหลายรูปแบบ ทั้งในเรื่องของการโจมตีเพื่อให้ระบบเครือข่ายไม่สามารถทำงานได้ หรือแม้กระทั่งการทำลายและขโมยข้อมูลที่สำคัญในระบบฯ ด้วยเหตุนี้ระบบเครือข่ายที่ดีและมีประสิทธิภาพ จึงต้องสามารถกำจัดภัยคุกคามเหล่านี้ให้ลดน้อยลงมากที่สุดเท่าที่จะเป็นไปได้ ดังนั้นองค์กรที่ตระหนักถึงความสำคัญของความปลอดภัยระบบเครือข่ายและมีข้อมูลที่สำคัญในระบบเครือข่าย จึงจำเป็นอย่างยิ่งที่จะต้องหาวิธีในการจัดการกับภัยคุกคามดังกล่าวด้วยเทคนิคและวิธีการต่างๆ

ด้วยเหตุผลดังกล่าวข้างต้น มหาวิทยาลัยเชียงใหม่ได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยระบบเครือข่ายคอมพิวเตอร์และความปลอดภัยของข้อมูลเป็นอย่างยิ่ง ทำให้ต้องมีการเตรียมการรับมือกับภัยคุกคามผ่านระบบเครือข่ายคอมพิวเตอร์ดังกล่าว ด้วยการจัดหาระบบรักษาความปลอดภัยด้วยเทคโนโลยี VPN (Virtual Private Network) ที่มีประสิทธิภาพเพื่อป้องกันระบบเครือข่ายคอมพิวเตอร์และข้อมูลสารสนเทศที่สำคัญของมหาวิทยาลัย ให้มีความปลอดภัยและปลอดจากภัยคุกคามต่างๆ เพื่อให้การดำเนินงานระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย ที่ได้ให้บริการแก่หน่วยงานภายใน นักศึกษา และบุคลากรมีความปลอดภัยและมีประสิทธิภาพสูงสุด

2. วัตถุประสงค์

2.1 เพื่อให้การจัดการความปลอดภัยระบบเครือข่ายคอมพิวเตอร์เป็นไปด้วยความสะดวกและมีประสิทธิภาพ

2.2 เพื่อให้ระบบเครือข่ายคอมพิวเตอร์และข้อมูลสารสนเทศที่สำคัญของของมหาวิทยาลัยปลอดภัยจากภัยคุกคามรูปแบบต่างๆ จากระบบเครือข่ายอินเทอร์เน็ต

2.3 เพื่อให้ผู้ใช้งานของมหาวิทยาลัยที่ใช้งานผ่านระบบเครือข่ายอินเทอร์เน็ตสามารถเข้าถึงระบบเครือข่ายอินทราเน็ตได้อย่างปลอดภัย

2.4 เพื่อให้หน่วยงานภายใน นักศึกษา และบุคลากรของมหาวิทยาลัยมีความพึงพอใจและเกิดความเชื่อมั่นในการใช้งานระบบเครือข่ายของมหาวิทยาลัย

2.5 เพื่อให้แก่นักศึกษาและบุคลากรสามารถเข้าถึงระบบเครือข่ายงานวิจัยได้อย่างสะดวกและปลอดภัย

3. เป้าหมายและแนวทางการใช้ประโยชน์

โครงการนี้มีเป้าหมายและแนวทางการสร้างผลสัมฤทธิ์จากโครงการให้เกิดประโยชน์ดังต่อไปนี้

3.1 ผู้ใช้งานของมหาวิทยาลัยที่ใช้งานผ่านระบบเครือข่ายอินเทอร์เน็ตสามารถเข้าถึงระบบเครือข่ายอินทราเน็ตได้อย่างปลอดภัย

3.2 ระบบเครือข่ายของมหาวิทยาลัยมีระบบการจัดการระบบรักษาความปลอดภัยที่สามารถบริหารและจัดการได้อย่างมีประสิทธิภาพ

3.3 ระบบเครือข่ายของมหาวิทยาลัยปลอดภัยจากภัยคุกคามระบบเครือข่ายคอมพิวเตอร์จากระบบอินเทอร์เน็ต

3.4 นักศึกษาและบุคลากรสามารถเข้าถึงระบบเครือข่ายงานวิจัยได้อย่างสะดวกและปลอดภัย

4. ระบบรักษาความปลอดภัยระบบเครือข่ายคอมพิวเตอร์ที่ต้องการ

มหาวิทยาลัยเชียงใหม่มีความประสงค์ที่จะประกวดราคาเพื่อติดตั้งระบบรักษาความปลอดภัยระบบเครือข่ายคอมพิวเตอร์ด้วยเทคโนโลยี VPN (Virtual Private Network) และอุปกรณ์ประกอบอื่นๆ ที่สามารถเชื่อมโยงและใช้งานร่วมกับระบบเครือข่ายคอมพิวเตอร์และระบบรักษาความปลอดภัยแบบ VPN เดิมของมหาวิทยาลัยได้อย่างมีประสิทธิภาพ ทั้งนี้อุปกรณ์รักษาความปลอดภัยระบบเครือข่าย และอุปกรณ์ประกอบอื่นๆ ทั้งหมดที่ได้ทำการติดตั้งดังกล่าวต้องสามารถทำงานได้อย่างมีประสิทธิภาพตามวัตถุประสงค์และเป้าหมายของโครงการ

ระบบรักษาความปลอดภัยระบบเครือข่ายที่ต้องการประกอบไปด้วยเทคโนโลยีระบบรักษาความปลอดภัยแบบ VPN (Virtual Private Network) ซึ่งมีคุณสมบัติไม่ด้อยกว่าคุณสมบัติที่กำหนดและใช้เทคโนโลยีแบบ Ethernet ที่สามารถเชื่อมโยงและใช้งานร่วมกับระบบเครือข่ายหลัก และระบบอื่นๆ เดิมของมหาวิทยาลัยได้อย่างมีประสิทธิภาพ

5. การพิจารณาทางเทคนิค

5.1 มหาวิทยาลัยเชียงใหม่จะพิจารณาราคาเฉพาะของ**ผู้เข้าประกวดราคาที่ผ่านข้อเสนอทางเทคนิคและผ่านข้อกำหนดเกี่ยวกับคุณสมบัติเท่านั้น** นอกจากนี้มหาวิทยาลัยเชียงใหม่ยังขอสงวน

สิทธิ์ในการพิจารณาระบบรักษาความปลอดภัยแบบ VPN (Virtual Private Network) และระบบประกอบอื่นๆ ที่ผู้เข้าประกวดราคาเสนอซึ่งมีคุณสมบัติอื่นที่นอกเหนือไปจากคุณสมบัติที่จำเป็นและคุณสมบัติที่ควรมี และมหาวิทยาลัยสงวนสิทธิ์ที่จะพิจารณาผู้เข้าประกวดราคารายที่เสนอราคาอยู่ในวงเงิน และให้ประโยชน์แก่มหาวิทยาลัยมากที่สุดก่อน

5.2 ผู้เข้าประกวดราคามีหน้าที่แสดงเอกสารต่างๆ เพื่อยืนยันหรือแสดงให้เห็นถึงคุณสมบัติต่างๆ ที่จะต้องเป็นไปตามข้อกำหนดหรือมีคุณสมบัติที่ดีกว่าข้อกำหนด พร้อมทั้งแสดงให้เห็นอย่างชัดเจนว่าได้เสนออุปกรณ์หรือระบบของผู้ผลิตรายใด รุ่นใด จำนวนเท่าใด และมีคุณสมบัติอย่างไร โดยเอกสารที่นำมาแสดงจะต้องเป็นเอกสารตัวจริงหรือเป็นเอกสารสำเนาที่เป็นทางการ สามารถเชื่อถือได้ และเป็นที่ยอมรับโดยทั่วไป ซึ่งผู้เข้าประกวดราคามีหน้าที่จะต้องเปรียบเทียบข้อกำหนดที่มหาวิทยาลัยกำหนดในแต่ละข้อกับคุณสมบัติของตนเองและของอุปกรณ์ต่างๆ ที่เสนอ โดยจะต้องระบุให้ชัดเจนว่าเอกสารที่นำมาเสนอ ข้อความในประโยคใดที่ใช้ยืนยันข้อกำหนดหมายเลขใดของมหาวิทยาลัย โดยผู้เข้าประกวดราคามีหน้าที่ทำสัญลักษณ์แสดงบนข้อความในประโยคที่ใช้ยืนยัน ได้แก่ การขีดเส้นใต้ หรือ การระบายสี พร้อมระบุหมายเลขลำดับของข้อกำหนดที่จะทำการยืนยันให้เห็นชัดเจน ซึ่ง**หากผู้เข้าประกวดราคาขาดเอกสารยืนยัน หรือขาดการทำสัญลักษณ์แสดงบนข้อความในประโยคที่ใช้ยืนยัน หรือแสดงเอกสารไม่ชัดเจนทำให้ขาดข้อกำหนดหนึ่งใดในข้อกำหนดของมหาวิทยาลัย ให้ถือว่าผู้เข้าประกวดราคาไม่ผ่านการพิจารณาทางด้านเทคนิค**

5.3 ให้จัดทำรายละเอียดข้อเสนอด้านเทคนิคของระบบงานที่เสนอ ในรูปแบบดังต่อไปนี้

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

5.4 ผู้เข้าประกวดราคาจะต้องเสนออุปกรณ์และระบบเฉพาะที่มหาวิทยาลัยได้ระบุไว้ในตารางที่ 1 เท่านั้น ซึ่งหากผู้เข้าประกวดราคาได้เสนอรายการอุปกรณ์อื่นใดที่นอกเหนือไปจากข้อกำหนดดังกล่าว มหาวิทยาลัยขอสงวนสิทธิ์ในการเปลี่ยนแปลงคุณสมบัติรายการอุปกรณ์และระบบที่เสนอดังกล่าวได้ในภายหลัง เพื่อให้ระบบสามารถใช้งานได้อย่างมีประสิทธิภาพ

6. กำหนดระยะเวลาการติดตั้ง

ผู้เข้าประกวดราคาต้องส่งมอบระบบรักษาความปลอดภัยแบบ VPN (Virtual Private Network) และอุปกรณ์ประกอบอื่นๆ ทั้งหมดภายในระยะเวลา 60 วัน นับจากวันลงนามในสัญญา ซึ่งหากเกินกว่าระยะเวลาดังกล่าว ผู้ชนะการประกวดราคาต้องถูกปรับในอัตราวันละ 2,000 บาท (สองพันบาทถ้วน)

7. ขอบเขตการติดตั้งระบบรักษาความปลอดภัยระบบเครือข่ายคอมพิวเตอร์

การติดตั้งระบบรักษาความปลอดภัยแบบ VPN (Virtual Private Network) และอุปกรณ์ประกอบอื่นๆ จะต้องเป็นไปตามข้อกำหนด มาตรฐานความปลอดภัย มาตรฐานการติดตั้งอุปกรณ์และสายสัญญาณของผู้ผลิต และมาตรฐานสากลอื่นๆ ที่เกี่ยวข้อง ทั้งนี้ผู้เข้าประกวดราคาจะต้องเป็นผู้รับผิดชอบค่าใช้จ่ายทั้งหมดในการติดตั้ง ตลอดจนค่าใช้จ่ายในการปรับปรุงและซ่อมแซมส่วนที่ได้รับผลกระทบจากการติดตั้งดังกล่าว ทั้งนี้อาคารที่จะทำการติดตั้งระบบรักษาความปลอดภัยแบบ VPN (Virtual Private Network) และอุปกรณ์ประกอบอื่นๆ นั้นให้ติดตั้ง ณ อาคารสำนักบริการเทคโนโลยีสารสนเทศ

8. ข้อกำหนดการติดตั้งระบบรักษาความปลอดภัยระบบเครือข่ายคอมพิวเตอร์และอุปกรณ์ประกอบอื่นๆ

ข้อกำหนดการติดตั้งโดยทั่วไป

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

8.2 ผู้ชนะการประกวดราคาต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น เนื่องจากการติดตั้งอุปกรณ์หรือความเสียหายใดที่เกิดขึ้นเนื่องจากการปฏิบัติงานของผู้ชนะการประกวดราคา ผู้ชนะการประกวดราคาจะต้องดำเนินการซ่อมแซมแก้ไขให้อยู่ในสภาพเดิมโดยเร็วและยินยอมชดใช้ค่าเสียหายที่เกิดขึ้นให้กับมหาวิทยาลัย

8.3 ผู้ชนะการประกวดราคาต้องเป็นผู้จัดหาสายหรืออุปกรณ์เพิ่มเติมอื่นๆ ที่จำเป็นสำหรับการติดตั้งอุปกรณ์รักษาความปลอดภัยแบบ VPN (Virtual Private Network) และอุปกรณ์ประกอบอื่นๆ ที่ทางผู้ชนะการประกวดราคาเสนอมาให้สามารถทำงานได้อย่างมีประสิทธิภาพ

8.4 การติดตั้งอุปกรณ์รักษาความปลอดภัยแบบ VPN (Virtual Private Network) และอุปกรณ์ประกอบอื่นๆ ที่ผู้ชนะการประกวดราคาได้เสนอ หรือติดตั้งอุปกรณ์และระบบอื่นใดเพิ่มเติม ซึ่งหากไม่ได้ระบุไว้ในข้อกำหนดของมหาวิทยาลัย ให้อยู่ในดุลยพินิจของมหาวิทยาลัยที่จะเป็นผู้กำหนดลักษณะและรูปแบบของการติดตั้ง โดยขึ้นอยู่กับความจำเป็นและสภาพการใช้งานจริง เพื่อให้ระบบสามารถใช้งานได้อย่างมีประสิทธิภาพเป็นสำคัญ

8.5 สายสัญญาณเชื่อมต่อ (Patch cable) ที่จะนำมาใช้กับอุปกรณ์รักษาความปลอดภัยแบบ VPN (Virtual Private Network) จะต้องเป็นสายที่เป็นชนิดที่เหมาะสม ซึ่งมีความยาวของสายและจำนวนที่จำเป็นต้องใช้งานจริง โดยเป็นสายที่มีคุณภาพมาตรฐานและผลิตสำเร็จรูปจากโรงงาน

9. รายการอุปกรณ์ที่มหาวิทยาลัยต้องการ

มหาวิทยาลัยเชียงใหม่มีความต้องการติดตั้งระบบรักษาความปลอดภัยแบบ VPN (Virtual Private Network) และอุปกรณ์ประกอบอื่นๆ ที่เกี่ยวข้องดังรายการต่อไปนี้ โดยจะกำหนดคุณสมบัติเฉพาะของอุปกรณ์ในภาคผนวก ก

ตารางที่ 1 แสดงรายการอุปกรณ์ที่ต้องการจัดซื้อ

ลำดับ	รายการอุปกรณ์	จำนวน	หน่วย	สถานที่ติดตั้ง
1	อุปกรณ์รักษาความปลอดภัย VPN	1	ชุด	สำนักบริการเทคโนโลยีสารสนเทศ
2	โมดูลช่องสัญญาณ Firewall	1	ชุด	สำนักบริการเทคโนโลยีสารสนเทศ
3	ลิขสิทธิ์การใช้งาน Firewall	1	ปี	สำนักบริการเทคโนโลยีสารสนเทศ
4	เครื่องคอมพิวเตอร์ลูกข่าย	3	ชุด	สำนักบริการเทคโนโลยีสารสนเทศ

10. การตรวจรับอุปกรณ์และระบบ

10.1 ผู้ชนะการประกวดราคาต้องจัดเตรียมเอกสารต่างๆ สำหรับการส่งมอบและการตรวจรับอย่างเหมาะสมให้กับทางมหาวิทยาลัยเชียงใหม่พิจารณา

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

10.3 มหาวิทยาลัยจะทำการการตรวจรับโครงการทั้งหมด เมื่อระบบและอุปกรณ์ทั้งหมดที่ได้ทำการติดตั้งโดยผู้ชนะการประกวดราคาจะต้องสามารถเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์และระบบรักษาความปลอดภัยเดิมของมหาวิทยาลัยที่มีอยู่แล้วได้อย่างมีประสิทธิภาพ ตามคุณลักษณะของระบบและอุปกรณ์ที่กำหนดไว้

10.4 ผู้ชนะการประกวดราคาต้องจัดทำป้ายประจำอุปกรณ์สำหรับอุปกรณ์ทุกชิ้นที่ส่งมอบที่สามารถติดป้ายได้ โดยป้ายประจำอุปกรณ์ต้องมีข้อความประกอบด้วย ชื่ออุปกรณ์ หมายเลขประจำอุปกรณ์ ชื่อผู้ขาย วันที่ติดตั้ง เบอร์โทรศัพท์ติดต่อแจ้งซ่อม และวันหมดรับประกัน เป็นอย่างน้อย

10.5 ผู้ชนะการประกวดราคาต้องทำหนังสือแจ้งการส่งมอบระบบทั้งหมดเพื่อตรวจรับให้ทางมหาวิทยาลัยเชียงใหม่ทราบอย่างน้อย 5 วันทำการ ก่อนการส่งมอบ ผู้ชนะการประกวดราคาต้องจัดทำเอกสารระบุอุปกรณ์ คู่มือ หรือสิ่งอื่นใดที่จะทำการตรวจรับ โดยระบุ ชนิด ยี่ห้อ รุ่น หมายเลขประจำอุปกรณ์ (serial number) สถานที่ติดตั้งหรือรายละเอียดอื่นใดที่จำเป็นในการตรวจรับให้มหาวิทยาลัยเชียงใหม่

10.6 ผู้ชนะการประกวดราคาต้องส่งมอบคู่มือการใช้งาน และโปรแกรมประกอบการใช้งานของอุปกรณ์ทุกชิ้นให้กับมหาวิทยาลัย

11. การดูแลรักษา การรับประกัน และการฝึกอบรมภายหลังการติดตั้ง

11.1 ผู้ชนะการประกวดราคาจะต้องทำการซ่อมบำรุงระบบ ทำความสะอาดอุปกรณ์ และอัพเดตรุ่นของซอฟแวร์ (Preventive Maintenance) ทั้งหมดที่ได้ทำการติดตั้งให้กับมหาวิทยาลัย ตามระยะเวลาที่รับประกันอุปกรณ์ โดยจะต้องทำการซ่อมบำรุงระบบทุกๆ 6 เดือน นับจากวันที่เริ่มรับประกัน และจะต้องจัดทำรายงานผลของการทำการซ่อมบำรุงระบบให้กับมหาวิทยาลัยทราบทุกครั้ง ซึ่งหากไม่มีการดำเนินการซ่อมบำรุงระบบและส่งผลรายงานภายใน 14 วันนับจากวันที่ครบกำหนดแต่ละรอบ มหาวิทยาลัยจะดำเนินการปรับเป็นรายครั้งในอัตราครั้งละ 30,000 (สามหมื่นบาทถ้วน)

11.2 ผู้ชนะการประกวดราคาจะต้องรับประกันถึงความเสียหายและดูแลรักษาอุปกรณ์และระบบทั้งที่เป็นฮาร์ดแวร์และซอฟต์แวร์ทั้งหมดเป็นระยะเวลา 3 ปี นับจากวันที่ส่งมอบของโครงการเป็นที่เรียบร้อยแล้ว ซึ่งหากเกิดความเสียหายใดๆ ผู้ชนะการประกวดราคาจะต้องดำเนินการแก้ไขให้กับมหาวิทยาลัยในทันที โดยไม่คิดค่าใช้จ่ายใดๆ ในการดำเนินการ

11.3 การรับประกันจะต้องครอบคลุมถึงความคุ้มครองต่อความสูญเสีย หรือเสียหาย จากผลโดยตรง หรือโดยอ้อม อันเนื่องมาจากสาเหตุ ไฟไหม้ ฟ้าผ่า ภัยระเบิด ภัยน้ำท่วม ภัยลมพายุ ภัยเนื่องจากน้ำ ภัยจากยวดยานพาหนะ ภัยจากอากาศ ภัยจากควัน ภัยลูกเห็บ ภัยแผ่นดินไหว ภัยจลาจลและนัดหยุดงาน ภัยจากการกระทำอันป่าเถื่อนและเจตนาร้าย ภัยจากการโจรกรรมที่ปรากฏร่องรอยการงัดแงะ ภัยต่อเครื่องไฟฟ้า (Electrical Injury) และภัยจากอุบัติเหตุทางกายภาพอื่นๆ

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

11.5 หากผู้ชนะการประกวดราคานิ่งเฉยไม่ดำเนินการใดๆ ที่จะแก้ไขความเสียหายของอุปกรณ์ที่เป็นของผู้ชนะการประกวดราคาภายหลังจาก 48 ชั่วโมง นับจากที่มหาวิทยาลัยได้แจ้งให้ผู้ชนะการประกวดราคาผ่านทางจดหมายหรือโทรสาร มหาวิทยาลัยมีสิทธิ์ที่จะดำเนินการจัดหา จัดซื้อ จัดจ้าง หรือดำเนินการใดๆ เพื่อ

แก้ไขให้อุปกรณ์ที่เสียหายสามารถใช้งานได้เป็นปกติ และมหาวิทยาลัยสามารถเรียกเก็บค่าใช้จ่ายในการดำเนินการทั้งหมดจากผู้ชนะการประกวดราคา

11.6 ผู้ชนะการประกวดราคาต้องจัดหลักสูตรฝึกอบรมให้กับบุคลากรของมหาวิทยาลัยเชียงใหม่จำนวนไม่น้อยกว่า 2 คน เพื่อให้สามารถใช้งานและดูแลอุปกรณ์รักษาความปลอดภัย VPN ที่เสนอได้ โดยต้องเป็นหลักสูตรตามมาตรฐานของผู้ผลิตอุปกรณ์ที่เสนอ จำนวนไม่น้อยกว่า 3 วัน ทั้งนี้ผู้ชนะการประกวดราคาจะต้องเสนอหลักสูตรในการอบรมให้กับมหาวิทยาลัยพิจารณา ซึ่งทางมหาวิทยาลัยขอสงวนสิทธิ์ในการพิจารณาเลือกหลักสูตรและสถานที่ฝึกอบรมในภายหลัง และผู้ชนะการประกวดราคาจะต้องเป็นผู้รับผิดชอบค่าใช้จ่ายที่เกิดขึ้นทั้งหมด รวมถึงเบี้ยเลี้ยงของบุคลากรที่ไปร่วมฝึกอบรมนี้ทั้งหมด

11.7 ผู้ชนะการประกวดราคาต้องจัดฝึกอบรมให้กับบุคลากรของมหาวิทยาลัยเชียงใหม่ในการใช้งานอุปกรณ์รักษาความปลอดภัย VPN ในเบื้องต้น และการใช้งานซอฟต์แวร์ระบบรักษาความปลอดภัย Firewall ในเบื้องต้น ตามที่เสนอ จำนวนไม่น้อยกว่า 8 คน จำนวนรวมไม่น้อยกว่า 4 วัน วันละไม่น้อยกว่า 6 ชั่วโมง โดยผู้ชนะการประกวดราคาจะต้องเสนอรายชื่อ พร้อมทั้งประวัติ และเอกสารแสดงการฝึกอบรมหรือการรับรองความรู้ของผู้ที่จะมาเป็นวิทยากรในการอบรมให้กับมหาวิทยาลัยพิจารณา ซึ่งหากวิทยากรที่เสนอขาดความรู้ความสามารถหรือขาดความเหมาะสมตามดุลยพินิจของมหาวิทยาลัย ผู้เข้าประกวดราคาจะต้องจัดหา จัดจ้าง และเสนอรายชื่อวิทยากรใหม่ให้กับมหาวิทยาลัยพิจารณาอีกครั้ง จนกว่าจะผ่านการพิจารณาของมหาวิทยาลัย

12. การเปลี่ยนแปลง การเพิ่ม การลดอุปกรณ์และอุปกรณ์ประกอบ

ในกรณีจำเป็นมหาวิทยาลัยสามารถขอเพิ่ม ลด หรือเปลี่ยนแปลงอุปกรณ์ต่างๆ ให้แตกต่างจากที่ระบุไว้ในเอกสารนี้ได้ เพื่อให้อุปกรณ์และระบบต่างๆ ที่เสนอสามารถทำงานร่วมกับระบบเครือข่ายและระบบคอมพิวเตอร์ทั้งหมดของมหาวิทยาลัยได้อย่างมีประสิทธิภาพ โดยผู้ชนะการประกวดราคาจะต้องปฏิบัติตามที่มหาวิทยาลัยกำหนดและจะต้องเสนอมูลค่าของปริมาณงานที่เพิ่มขึ้นหรือลดลงให้มหาวิทยาลัยพิจารณาก่อนที่ผู้ชนะการประกวดราคาจะดำเนินการ ซึ่งมหาวิทยาลัยจะชำระหรือขอคืนเงินดังกล่าวให้กับผู้ชนะการประกวดราคาเมื่อมหาวิทยาลัยได้ทำการตรวจรับและเบิกจ่ายต่อไป ทั้งนี้มหาวิทยาลัยขอสงวนสิทธิ์ที่จะพิจารณาจัดหาผู้ดำเนินการรายอื่นแทนผู้ชนะการประกวดราคาได้ หากพบว่ามูลค่าของปริมาณงานที่เพิ่มขึ้นหรือลดลงนั้น เป็นราคาที่ไม่เป็นธรรมต่อทางราชการและอาจก่อให้เกิดความเสียหายต่อราชการได้

13. ระยะเวลาในการดำเนินการ 60 วัน นับจากวันลงนามในสัญญา

14. ระยะเวลาส่งมอบ 60 วัน

15. วงเงินในการจัดหา 2,500,000 บาท (สองล้านห้าแสนบาทถ้วน)

ขอรับรองว่าการกำหนดคุณลักษณะของพัสดุ ข้างต้นเป็นไปตามข้อกำหนด ในมติคณะรัฐมนตรีตามหนังสือที่ นร 0203/ว157 ลงวันที่ 27 ธันวาคม 2519

ประกาศ ณ วันที่ 25 สิงหาคม 2553

(ลงนาม) รัฐสิทธิ์ สุขะหุต
(ผู้ช่วยศาสตราจารย์ ดร.รัฐสิทธิ์ สุขะหุต)
รองผู้อำนวยการ รักษาการแทน
ผู้อำนวยการสำนักบริการเทคโนโลยีสารสนเทศ

ภาคผนวก ก

คุณสมบัติเฉพาะของผู้เข้าประกวดราคาและอุปกรณ์ระบบต่างๆ ที่มหาวิทยาลัยต้องการ ซึ่งทั้งหมดจะต้องมีคุณสมบัติดังต่อไปนี้เป็นอย่างน้อย

1. คุณสมบัติของผู้เข้าประกวดราคา

1.1 มีเงินทุนจดทะเบียนไม่ต่ำกว่า 1 ล้านบาท

1.2 จดทะเบียนทำธุรกิจด้านระบบเครือข่ายคอมพิวเตอร์หรือระบบรักษาความปลอดภัยคอมพิวเตอร์ในประเทศไทยไม่น้อยกว่า 1 ปี

1.3 ผู้เข้าประกวดราคาต้องเป็นผู้ที่ไม่มีชื่ออยู่ในหนังสือแจ้งเวียนทิ้งงานของทางราชการ

1.4 ผู้เข้าประกวดราคาต้องไม่เป็นผู้ที่ได้รับเอกสิทธิ์หรือความคุ้มครองทางการทูต ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่สละสิทธิ์หรือความคุ้มครองทางการทูต

1.5 อุปกรณ์รักษาความปลอดภัยแบบ VPN ในลำดับที่ 1 ของตารางที่ 1 และลิขสิทธิ์การใช้งาน Firewall ในลำดับที่ 3 ตารางที่ 1 ผู้เข้าประกวดราคาต้องมีหนังสือรับรองจากบริษัทผู้ผลิตว่าให้การสนับสนุนการประกวดราคาในครั้งนี้

1.6 ผู้เข้าประกวดราคาต้องมีบุคลากรที่มีความรู้ความเข้าใจเกี่ยวกับอุปกรณ์รักษาความปลอดภัยต่างๆ ที่เสนอ ซึ่งสามารถให้ความช่วยเหลือกับมหาวิทยาลัยเชียงใหม่ได้ โดยผู้เข้าประกวดราคาจะต้องส่งรายชื่อของบุคลากร และจบการศึกษาระดับปริญญาตรีหรือสูงกว่าทางด้านวิศวกรรมหรือวิทยาการคอมพิวเตอร์ จำนวนรวมไม่น้อยกว่า 1 คน โดยแนบประวัติการศึกษา การฝึกอบรม ใบประกาศที่เกี่ยวข้อง ซึ่งขณะดำเนินการติดตั้งอุปกรณ์ให้กับมหาวิทยาลัยจะต้องมีบุคลากรที่เสนอร่วมอยู่ด้วยจำนวนไม่น้อยกว่า 1 คน

2. คุณสมบัติของอุปกรณ์และรายละเอียดต่างๆ ดังต่อไปนี้เป็นอย่างน้อย

2.1 อุปกรณ์รักษาความปลอดภัย VPN (รายการที่ 1 ตารางที่ 1) จำนวน 1 ชุด

<u>ฮาร์ดแวร์และซอฟต์แวร์</u>

2.1.1 อุปกรณ์ต้องมีลักษณะการออกแบบเฉพาะสำหรับใช้งาน SSL VPN เป็นสำคัญ

2.1.2 มีพอร์ต Gigabit Ethernet รวมกันจำนวนไม่น้อยกว่า 4 พอร์ต

2.1.3 มีระบบ Load-balancing แบบ Active/Active Stateful authentication failover ในตัวอุปกรณ์เอง

2.1.4 รองรับจำนวนผู้เข้าใช้งานในเวลาเดียวกันได้ไม่น้อยกว่า 100 User และสามารถขยายเพิ่มภายหลังรวมได้ไม่น้อยกว่า 250 User โดยไม่ต้องมีการเปลี่ยนอุปกรณ์

2.1.5 เป็นซอฟต์แวร์ที่มหาวิทยาลัยมีสิทธิ์ใช้งานได้อย่างถูกต้องตามกฎหมาย และมหาวิทยาลัยสามารถที่จะปรับปรุงรุ่น (Upgrade) ได้ตลอดระยะเวลารับประกัน

<u>ระบบความปลอดภัย</u>

2.1.6 รองรับมาตรฐานการเข้ารหัสแบบ DES, 3DES, RC4, AES และ MD5, SHA Hash ได้

2.1.7 รองรับระบบการพิสูจน์ตัวตนแบบต่างๆได้อย่างน้อยดังนี้

2.1.7.1 Username/password

2.1.7.2 Digital Certificates แบบ Client-side และ Server-side

2.1.7.3 Digital Certificates แบบเก็บใน LDAP

2.1.7.4 RSA SecurID รวมถึง One-Time Password Tokens อื่นๆ

2.1.7.5 Microsoft Active Directory

2.1.7.6 LDAP (Active Directory, Sun iPlanet, etc.)

2.1.7.7 Radius

2.1.7.8 Certificate Revocation Lists (CRL)

2.1.7.9 One-Time Password ในตัวอุปกรณ์เอง

2.1.8 สามารถทำการ Query ไปยัง LDAP/AD แบบอ้างอิง Dynamic groups ได้

2.1.9 สามารถแจ้งเตือนผู้ใช้ในกรณีที่รหัสผ่านกำลังจะหมดอายุและอนุญาตให้ผู้ใช้เปลี่ยนรหัสผ่านได้

2.1.10 สามารถกำหนด Access control ได้ทั้งจาก User ไป Resource, จาก Resource ไป User และจาก User ไป User จากค่าต่างๆได้อย่างน้อยดังนี้

2.1.10.1 User and group

2.1.10.2 Source IP and network

2.1.10.3 Destination network

2.1.10.4 Service/Port

2.1.10.5 Day, date, time and range

2.1.10.6 Browser encryption key length

2.1.10.7 Policy Zones

2.1.10.8 File system

2.1.11 สามารถตรวจสอบเครื่อง End Point บนแพลตฟอร์ม Windows, Windows Vista, Windows Mobile, Macintosh และ Linux ก่อนเข้าใช้งาน และสามารถระบุช่วงเวลาในการตรวจซ้ำระหว่างการใช้งาน จากค่าต่างๆได้อย่างน้อยดังนี้

2.1.11.1 Directory/File name โดยสามารถระบุค่า Size, Last modified(Absolute, Relative) และ File Integrity โดยใช้ MD5, SHA-1 hash หรือ Windows catalog fileได้

2.1.11.2 Register keys

2.1.11.3 Running processes

2.1.11.4 Device Watermarks

2.1.11.5 Windows domain

2.1.11.6 Windows version

2.1.11.7 International Mobile Equipment Identity (IMEI)

2.1.12 มีระบบ Data Protection ที่ทำงานได้บนแพลตฟอร์ม Windows XP, Windows Vista, Macintosh และ Linux โดยสามารถลบข้อมูลที่เกิดขึ้นระหว่างการเชื่อมต่อหลังจากผู้ใช้งานออกจากระบบได้ดังนี้

2.1.12.1 Browser history

2.1.12.2 Browser cache

2.1.12.3 Browser username and password

2.1.12.4 Browser URL AutoComplete list

2.1.12.5 Windows index.dat

2.1.12.6 Temporary storage

2.1.13 สามารถป้องกันการโจรกรรม ชื่อผู้ใช้/รหัสผ่าน จากโปรแกรมประเภท Keylogger โดยใช้ Virtual Keyboard

2.1.14 สามารถกำหนด Quarantine Zone สำหรับกักและแจ้งผู้ใช้งาน จาก Client ที่มีคุณสมบัติไม่ครบตามที่กำหนด

2.1.15 สามารถกำหนด Deny Zone สำหรับป้องกันการเข้าใช้งาน จาก Client ที่มีคุณสมบัติตามที่กำหนด

2.1.16 รองรับการทำ Single Sign-On แบบต่างๆอย่างน้อยได้ดังนี้

2.1.16.1 Forms-Based Single Sign-On

2.1.16.2 Basic Authentication Forwarding

2.1.16.3 NTLM Authentication Forwarding

2.1.16.4 RSA ClearTrust

<u>การเชื่อมต่อและการสนับสนุนแอพพลิเคชั่น</u>

2.1.17 รองรับการเชื่อมต่อผ่านเวบบราวเซอร์แบบไม่มีการติดตั้ง SSLVPN Add-on/Agent โดยสามารถใช้งาน Resources ประเภท Web-based และ Web file access (SMB/CIFS, DFS) ได้

2.1.18 สนับสนุนระบบปฏิบัติการต่างๆอย่างน้อยดังนี้ Windows Vista, Windows XP, Macintosh OS X, Linux, Web-enabled mobile devices

2.1.19 สนับสนุนเวบบราวเซอร์ต่างๆ อย่างน้อยดังนี้ Internet Explorer, Mozilla Firefox, Safari

2.1.20 ผู้ใช้งานสามารถสร้าง Bookmark ส่วนตัวได้

2.1.21 สนับสนุนการเชื่อมต่อไปยัง Client/Server แอพพลิเคชั่น ผ่านโปรโตคอลต่างๆ อย่างน้อยได้ดังนี้ TCP, UDP, ICMP, VoIP, Reverse-connection, Bi-directional

2.1.22 สนับสนุน Traffic Redirection ทั้งแบบ Split และ Redirect All สำหรับการเชื่อมต่อแบบ Tunnel

2.1.23 สนับสนุนรูปแบบการกำหนด IP Address ให้ผู้ใช้งานแบบ Tunnel ได้อย่างน้อยดังนี้

2.1.23.1 Translated Address Pools(Source NAT)

2.1.23.2 Routed Address Pools (DHCP)

2.1.23.3 RADIUS-Assigned Address Pools

2.1.23.4 Static Address Pools

2.1.24 มีระบบป้องกันปัญหาการซ้ำกันของ Routing และ IP Address บนเครื่องผู้ใช้งาน

2.1.25 มีโปรแกรม SSLVPN Client สำหรับใช้เชื่อมต่อโดยไม่ผ่านเวบบราวเซอร์ บนแพลตฟอร์ม Windows Vista, Windows XP, Windows 2003, Macintosh, Linux

2.1.26 มีโปรแกรม SSLVPN Client ชนิดทำงานเป็น Windows Service

2.1.27 โปรแกรม SSLVPN Client สามารถทำการตรวจสอบ, ดาวน์โหลด รวมถึง อัพเดทตัวเอง ในกรณีที่มีเวอร์ชั่นที่ใหม่กว่าบนตัวอุปกรณ์ SSLVPN ได้

2.1.28 สามารถระบุให้เครื่องผู้ใช้งานรัน Script หลังจากเชื่อมต่อได้

2.1.29 สามารถระบุ SSLVPN ตัวสำรอง ในกรณีที่ตัวหลักไม่สามารถทำงานได้ โปรแกรม SSLVPN Client จะทำการเชื่อมต่อ ไปยังตัวสำรองโดยอัตโนมัติ

2.1.30 สามารถคงสถานะการเชื่อมต่อ ในกรณีที่ผู้ใช้มีการเคลื่อนที่ไปยังเครือข่าย/สถานที่อื่น โดยไม่ต้องป้อนชื่อผู้ใช้/รหัสผ่านใหม่

2.1.31 สามารถกำหนดค่า Session length ได้

2.1.32 สามารถกำหนดค่า Client inactivity timer ได้

<u>ระบบบริหารจัดการ</u>

2.1.33 มีระบบบริหารจัดการตัวอุปกรณ์แบบ Web-based และ Command line

2.1.34 มีระบบ Role-based administration

2.1.35 รูปแบบการกำหนด Policy เป็นแบบ Object-based ทำให้สามารถบริหารจัดการได้ง่ายและรวดเร็ว

2.1.36 สามารถสร้างและออกแบบหน้า Portal ให้เหมาะสมสำหรับแต่ละกลุ่มผู้ใช้ และอุปกรณ์ Mobile device ที่มีขนาดจอแสดงผลเล็กเช่น Mobile phone, Smartphone, PDA เป็นต้น

2.1.37 รองรับการใช้อักขระประเภท Extended/Double-byte ในการกำหนดค่าต่างๆเช่น ชื่อผู้ใช้, รหัสผ่าน, Resources, Access control เป็นต้น

2.1.38 สามารถดูรายชื่อผู้ที่กำลังเชื่อมต่อรวมถึงสามารถตัดออกจากระบบได้

2.1.39 สามารถกำหนดจำนวน Sessions สูงสุดของผู้ใช้รายบุคคล/กลุ่ม ที่สามารถเข้าใช้งานได้ในเวลาเดียวกัน

2.1.40 สามารถแสดงข้อมูลกราฟสรุปค่าสถานะของอุปกรณ์ เช่น CPU/Memory/Swap Utilization, Network Bandwidth, Active Users ในช่วงระยะเวลาต่างๆได้

<u>Auditing และ Logging</u>

2.1.41 สนับสนุนข้อมูล Radius auditing และ accounting

2.1.42 สามารถเรียกดู, ค้นหา, คัดกรองข้อมูล Log จากระบบบริหารจัดการ โดยมีการเก็บค่าต่างๆอย่างน้อยดังนี้

2.1.42.1 Date/Time

2.1.42.2 Source IP/Port

2.1.42.3 Destination IP/Port

2.1.42.4 Username

2.1.42.5 Authentication method

2.1.42.6 Connection status/duration

2.1.42.7 Bytes received/sent

2.1.43 สามารถส่งข้อมูล Log ไปยัง Syslog server ได้

2.1.44 สนับสนุนข้อมูล SNMP MIB

2.1.45 ผ่านการรับรองมาตรฐาน FCC, ICES, CE, VCCI และ TUV/GS, UL, CB Scheme เป็นอย่างน้อย

2.2 โมดูลช่องสัญญาณ Firewall (รายการที่ 2 ตารางที่ 1) จำนวน 1 ชุด

2.2.1 เป็นโมดูลที่มีช่องสัญญาณแบบ 10Gbps จำนวนไม่น้อยกว่า 2 พอร์ต ซึ่งเป็นแบบ 10GBase-SR หรือดีกว่า

2.2.2 สามารถติดตั้งบนอุปกรณ์ระบบรักษาความปลอดภัยเดิม (Firewall) ของมหาวิทยาลัยได้อย่างมีประสิทธิภาพ และเป็นผลิตภัณฑ์ภายใต้ผู้ผลิตเดียวกับอุปกรณ์

2.3 ลิขสิทธิ์การใช้งาน Firewall (รายการที่ 3 ตารางที่ 1) จำนวน 1 ปี

2.3.1 มีลิขสิทธิ์การใช้งานของระบบรักษาความปลอดภัยเดิม (Firewall) ของมหาวิทยาลัยเพิ่มเติมอย่างถูกต้องตามกฎหมาย

2.4 เครื่องคอมพิวเตอร์ลูกข่าย (รายการที่ 4 ตารางที่ 1) จำนวน 3 ชุด

2.4.1 เป็นเครื่องคอมพิวเตอร์ที่ถูกออกแบบมาเพื่อใช้งานในลักษณะแบบ Small Form Factor Desktop

2.4.2 มีหน่วยประมวลผล Intel Core i5 หรือดีกว่า ความเร็วไม่น้อยกว่า 2.66 GHz และมี Chipset Intel Q57 หรือดีกว่า

2.4.3 มีหน่วยความจำหลักแบบ DDR3-SDRAM หรือดีกว่า ขนาดรวมกันไม่น้อยกว่า 8 GB และสามารถขยายได้สูงสุดรวมไม่น้อยกว่า 16 GB

2.4.4 มี Hard Disk ชนิด SATA หรือดีกว่า ความเร็วไม่น้อยกว่า 7,200 รอบต่อนาที (rpm) ขนาดไม่น้อยกว่า 1 TB

2.4.5 มีช่องสัญญาณ Ethernet แบบ Gigabit Ethernet จำนวนไม่น้อยกว่า 1 พอร์ต

2.4.6 มีจอภาพสี (Monitor) แบบ LCD ความละเอียดไม่น้อยกว่า 1680 x 1050 ขนาดไม่น้อยกว่า 22 นิ้ว จำนวนไม่น้อยกว่า 1 จอ

2.4.7 มีหน่วยควบคุมการแสดงผล NVIDIA Quadro NVS290 หรือดีกว่า ซึ่งมีหน่วยความจำขนาดไม่น้อยกว่า 256 MB

2.4.8 มีแป้นพิมพ์ (Keyboard) ชนิด USB แบบไม่น้อยกว่า 104 keys ซึ่งมีทั้งอักษรภาษาไทยและภาษาอังกฤษ โดยพิมพ์ติดถาวรลงบนแป้นพิมพ์ จำนวนไม่น้อยกว่า 1 หน่วย

2.4.9 มีเมาส์ (Mouse) USB แบบ Optical Scroll พร้อมแผ่นรองเมาส์ จำนวนไม่น้อยกว่า 1 หน่วย

2.4.10 มี SuperMulti LightScribe Drive หรือดีกว่า จำนวนไม่น้อยกว่า 1 หน่วย

2.4.11 รองรับระบบปฏิบัติการ Microsoft Windows XP และ Microsoft Windows 7 ได้เป็นอย่างน้อย

2.4.12 ชิ้นส่วนและอุปกรณ์ทั้งหมดอยู่ภายใต้เครื่องหมายการค้าของผู้ผลิตรายเดียวกัน

ตารางแสดงการบันทึกรายละเอียดประกาศร่าง TOR

รายการข้อมูล	คำอธิบาย
1. ชื่อหน่วยงาน	สำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่
2. ชื่อเรื่องร่าง TOR	โครงการจัดซื้อระบบรักษาความปลอดภัยผ่านระบบเครือข่าย
3. วงเงินงบประมาณ (บาท)	2,500,000 บาท (สองล้านห้าบาทถ้วน)
4. ราคากลาง (บาท)	2,500,000 บาท (สองล้านห้าบาทถ้วน)
5. ราคาสูงสุดที่พึงรับได้ (บาท)	2,500,000 บาท (สองล้านห้าบาทถ้วน)
6. วันที่ประกาศ	25 สิงหาคม 2553
7. จำนวนวันที่สิ้นสุดรับฟังข้อวิจารณ์	28 สิงหาคม 2553
8. อีเมล์แอดเดรส	benpjit@chiangmai.ac.th / sajja@cm.edu
9.ที่อยู่โครงการ	สำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่ เลขที่ 239 ถนนห้วยแก้ว ต.สุเทพ อ.เมือง จ.เชียงใหม่
10. จังหวัด	เชียงใหม่