ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)

ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการจัดซื้อ/จัดจ้าง งานเช่าซื้ออุปกรณ์ป้องกันเครือข่าย อุปกรณ์ระบบเครือข่ายไร้สาย และซอฟต์แวร์ระบบตรวจสอบการทำงานของเครือข่ายคอมพิวเตอร์
/หน่วยงานเจ้าของโครงการ ฝ่ายเทคโนโลยีสารสนเทศ

2. วงเงินงบประมาณที่ได้รับจัดสรร 2,000,000 บาท

3. วันที่กำหนดราคากลาง (ราคาอ้างอิง) 12 ก.พ. 2561
เป็นเงิน 2,070,806.67 บาท ราคา/หน่วย (ถ้ามี) - บาท

4. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)
4.1 บริษัท ไอที เอสเซนเชียล (ไทยแลนด์) จำกัด
4.2 บริษัท ทีจีเอส เอ็นเตอร์ไพรส์ เน็ตเวิร์ค จำกัด
4.3 บริษัท เจ ซีสเทม แอนด์ โซลูชั่น จำกัด

5. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน นายคมสัน วรกุล

ขอบเขตของงาน (Terms of Reference : TOR)
การเช่าซื้ออุปกรณ์ป้องกันเครือข่าย อุปกรณ์ระบบเครือข่ายไร้สาย และซอฟต์แวร์ระบบตรวจสอบการทำงานของเครือข่ายคอมพิวเตอร์ สถาบันวิจัยและพัฒนาอัญมณีและเครื่องประดับแห่งชาติ (องค์การมหาชน)

---

1. ความเป็นมา

ปัจจุบันข้อมูล (Data) และสารสนเทศ (Information) เปรียบเสมือนสินทรัพย์ที่มีมูลค่าและมีบทบาทสำคัญต่อการบริหารจัดการองค์กร ดังนั้น องค์กรต่างๆ จึงเริ่มตระหนักถึงการปกป้องรักษาข้อมูลและสารสนเทศที่สำคัญอันนำมาซึ่งความท้าทายในการบริหารความมั่นคงปลอดภัยของสารสนเทศอย่างเป็นมาตรฐานและมีประสิทธิภาพคุ้มค่ากับการลงทุนเพื่อให้ผู้ใช้ข้อมูลและสารสนเทศมีความเชื่อมั่นว่าข้อมูลและสารสนเทศดังกล่าวมีความปลอดภัย สถาบันวิจัยและพัฒนาอัญมณีและเครื่องประดับแห่งชาติ (องค์การมหาชน) เห็นความสำคัญของการรักษาความมั่นคงปลอดภัยของข้อมูลและสารสนเทศดังกล่าว จึงได้จัดทำระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 ขึ้น ตั้งแต่ปี พ.ศ. 2558 โดยมีวัตถุประสงค์เพื่อสร้างความปลอดภัยให้กับโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและระบบสารสนเทศของสถาบันฯ ตามมาตรฐานสากล ตลอดจนสามารถสร้างความเชื่อมั่นให้กับลูกค้าหรือผู้ใช้บริการโครงสร้างพื้นฐานฯ และระบบสารสนเทศดังกล่าว แต่เนื่องจากอุปกรณ์โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่ให้บริการอยู่ในปัจจุบัน อันได้แก่ อุปกรณ์ป้องกันเครือข่าย (Firewall) และอุปกรณ์ระบบเครือข่ายไร้สาย (Wireless Network Devices) มีอายุการใช้งานมากกว่า 6 ปี ซึ่งเป็นระยะเวลาที่เกินกว่าอายุของผลิตภัณฑ์ (Lifetime) ส่งผลให้ สถาบันฯ ไม่สามารถปรับปรุง Firmware ของอุปกรณ์เป็นรุ่นปัจจุบันหรือใกล้เคียงรุ่นปัจจุบันได้ อันจะทำให้เกิดความเสี่ยงต่อการถูกโจมตีผ่านทางช่องโหว่ของ Firmware รุ่นเก่าที่ไม่ได้รับการปรับปรุง (Update) ประกอบกับ อุปกรณ์ฯ จะไม่สามารถรองรับความต้องการใช้งานจากเจ้าหน้าที่และลูกค้าของสถาบันฯ ที่เพิ่มขึ้นหลายเท่าตัวในปี พ.ศ. 2561 ตลอดจน ไม่สามารถเชื่อมต่อกับอุปกรณ์สื่อสาร อันได้แก่ Smart Phone, Tablet Computer ที่ใช้มาตรฐานการเชื่อมต่อใหม่ได้ สถาบันฯ จึงมีความจำเป็นต้องจัดหาอุปกรณ์ป้องกันเครือข่ายและอุปกรณ์ระบบเครือข่ายไร้สายใหม่ อันประกอบด้วย อุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย (Access Point: AP) และอุปกรณ์ควบคุมและจัดการอุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย (AP Controller) ทดแทนอุปกรณ์ฯ เดิม รวมทั้ง จัดหาซอฟต์แวร์ระบบตรวจสอบการทำงานของเครือข่ายคอมพิวเตอร์ (Computer Network Monitoring Software) เพื่อเพิ่มประสิทธิภาพการบริการด้านเครือข่ายคอมพิวเตอร์แก่เจ้าหน้าที่และลูกค้าของสถาบันฯ ให้สามารถใช้งานเครือข่ายคอมพิวเตอร์ของสถาบันฯ ได้อย่างสะดวก รวดเร็ว และมั่นคงปลอดภัย อันจะส่งผลต่อประสิทธิภาพและประสิทธิผลของงาน รวมทั้งความพึงพอใจต่อบริการของสถาบันฯ ตามลำดับ

/2. วัตถุประสงค์...

2. วัตถุประสงค์

จัดหาอุปกรณ์ป้องกันเครือข่าย อุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย อุปกรณ์ควบคุมและจัดการอุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย ทดแทนอุปกรณ์ฯ เดิม รวมทั้ง จัดหาซอฟต์แวร์ระบบตรวจสอบการทำงานของเครือข่ายคอมพิวเตอร์ เพื่อเพิ่มประสิทธิภาพและความมั่นคงปลอดภัยของการบริการด้านเครือข่ายคอมพิวเตอร์ตามระบบมาตรฐาน ISO/IEC 27001 แก่เจ้าหน้าที่และลูกค้าของสถาบันฯ

3. คุณสมบัติของผู้เสนอราคาและข้อปฏิบัติของผู้เสนอราคา

3.1 ผู้เสนอราคาจะต้องมีหนังสือรับรองผลงานเกี่ยวกับการจำหน่ายและติดตั้งอุปกรณ์ป้องกันเครือข่าย อุปกรณ์ระบบเครือข่ายไร้สาย และซอฟต์แวร์ระบบตรวจสอบการทำงานของเครือข่ายคอมพิวเตอร์ พร้อมสำเนาสัญญาผลงานที่กล่าวอ้างซึ่งเป็นวงเงินไม่น้อยกว่า 1,000,000 บาท (หนึ่งล้านบาทถ้วน) ต่อหนึ่งสัญญา ภายในระยะเวลา 3 ปี นับจากวันที่งานแล้วเสร็จจนถึงวันที่ยื่นข้อเสนอด้านราคา และเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับหน่วยงานราชการ รัฐวิสาหกิจ หรือหน่วยงานเอกชนที่สถาบันฯ เชื่อถือได้

3.2 ผู้เสนอราคาต้องเป็นนิติบุคคลไทยที่ได้รับจดทะเบียนประกอบธุรกิจในประเทศไทย ทั้งนี้ผู้เสนอราคาจะต้องนำส่งเอกสารดังต่อไปนี้ให้กับสถาบันฯ เพื่อประกอบการพิจารณา

3.2.1 สำเนาหนังสือรับการจดทะเบียนนิติบุคคล

3.2.2 สำเนาหนังสือบริคณห์สนธิ

3.2.3 บัญชีรายชื่อกรรมการผู้จัดการ

3.2.4 บัญชีรายชื่อผู้ถือหุ้นรายใหญ่/สำเนาบัญชีรายชื่อผู้ถือหุ้นทั้งหมด

3.2.5 ใบทะเบียนภาษีมูลค่าเพิ่ม (ภ.พ.๒๐)

กรณีที่ผู้เสนอราคามอบอำนาจให้บุคคลอื่นลงนามในใบเสนอราคาแทน ผู้เสนอราคาต้องจัดทำหนังสือมอบอำนาจติดอากรแสตมป์ตามกฎหมายให้ครบถ้วนและนำส่งให้กับสถาบันฯ

3.3 ผู้เสนอราคาต้องไม่เป็นผู้ที่ถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานของทางราชการและได้แจ้งเวียนชื่อแล้ว หรือไม่เป็นผู้ที่ได้รับผลการสั่งให้นิติบุคคลอื่นเป็นผู้ทิ้งงานตามระเบียบของทางราชการ

3.4 ผู้เสนอราคาต้องไม่เป็นผู้มีประโยชน์ร่วมกับผู้เสนอราคารายอื่นหรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรมในการจัดซื้อในครั้งนี้

3.5 ผู้เสนอราคาต้องไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้เสนอราคาได้มีคำสั่งให้สละสิทธิ์และความคุ้มกันเช่นว่านั้น

/3.6 ผู้เสนอราคา...

3.6 ผู้เสนอราคาต้องมีผู้ควบคุมและดำเนินงานอย่างน้อย 1 คน ที่ได้รับใบประกาศนียบัตร (Certificate) จากเจ้าของผลิตภัณฑ์หรือตัวแทนเจ้าของผลิตภัณฑ์ และมีประสบการณ์ในการติดตั้ง (1) อุปกรณ์ป้องกันเครือข่าย (Firewall) (2) อุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย (Access Point: AP) (3) อุปกรณ์ควบคุมและจัดการอุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย (AP Controller) และ (4) ซอฟต์แวร์ระบบตรวจสอบการทำงานของเครือข่ายคอมพิวเตอร์ (Computer Network Monitoring Software) ที่มีความสอดคล้องกับระบบมาตรฐานด้านความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001 โดยจะต้องแนบสำเนาใบประกาศนียบัตรและเอกสารแสดงผลงานการติดตั้งอุปกรณ์และซอฟต์แวร์ดังกล่าวมาพร้อมกับข้อเสนอด้านเทคนิค และจะต้องสามารถแสดงใบประกาศนียบัตรฉบับจริงได้ทันทีที่สถาบันฯ ร้องขอ

3.7 ผู้เสนอราคาต้องเสนอราคาครบทุกรายการตามคุณลักษณะเฉพาะที่กำหนดไว้

3.8 ผู้เสนอราคาต้องจัดทำเอกสารแสดงตารางเปรียบเทียบทางเทคนิคระหว่างข้อกำหนดและรายละเอียดของซอฟต์แวร์และอุปกรณ์ที่เสนอกับข้อกำหนดและรายละเอียดของซอฟต์แวร์และอุปกรณ์ซึ่งถูกกำหนดโดยสถาบันฯ เป็นรายข้อตามแบบรูปรายการหรือคุณลักษณะเฉพาะทุกข้อ ณ วันที่ยื่นซองข้อเสนองาน สำหรับผู้เสนอราคาที่มีการอ้างอิงถึงข้อความ ภาพ หรือข้อมูลที่ปรากฏในเอกสารแสดงรายการสินค้า (Catalog) หรือเอกสารอื่นใดที่เกี่ยวข้องกับสินค้า ผู้เสนอราคาจะต้องระบุหน้าและตำแหน่งของข้อความ ภาพ หรือข้อมูลในเอกสารที่อ้างอิงนั้นให้ชัดเจน ส่วนในเอกสารประกอบที่ถูกนำมาอ้างอิง ให้ผู้เสนอราคาทำเครื่องหมายขีดเส้นใต้หรือระบายสี และเขียนหัวข้อกำกับไว้ในเอกสารอ้างอิงให้ตรงกับหมายเลขของข้อกำหนด เพื่อให้คณะกรรมการจัดซื้อตรวจสอบได้อย่างชัดเจน **ทั้งนี้ หากผู้เสนอราคาไม่ดำเนินการตามข้อนี้ คณะกรรมการฯ ขอสงวนสิทธิในการไม่พิจารณาข้อเสนอของผู้เสนอราคา**

4. สถานที่ติดตั้งและส่งมอบงาน

สถานที่ที่ผู้เสนอราคาจะติดตั้ง ปรับแต่ง และส่งมอบอุปกรณ์ป้องกันเครือข่าย อุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย อุปกรณ์ควบคุมและจัดการอุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย และซอฟต์แวร์ระบบตรวจสอบการทำงานของเครือข่ายคอมพิวเตอร์ อยู่ที่ชั้นที่ 1-4 และชั้นที่ 6 ห้องชุดเลขที่ 140, 140/1, 140/2, 140/3 และ 140/5 อาคารชุดไอทีเอฟ-ทาวเวอร์ ถนนสีลม แขวงสุริยวงศ์ เขตบางรัก กรุงเทพมหานคร

5. แบบรูปรายการและคุณลักษณะเฉพาะ

รายละเอียดตามเอกสารแนบ (จำนวน 7 หน้า)

/6. วิธีการ...

6. วิธีการรับ-ส่งซองข้อเสนองาน

ผู้เสนอราคาต้องยื่นข้อเสนองานตามแบบที่กำหนดไว้ในเอกสารการจัดซื้อด้วยวิธีคัดเลือก โดยไม่มีเงื่อนไขใดๆ ทั้งสิ้น และจะต้องกรอกข้อมูลให้ถูกต้องครบถ้วนพร้อมลงลายมือชื่อของผู้เสนอราคาให้ชัดเจน โดยผู้เสนอราคาต้องแยกซองแต่ละรายการถึงคณะกรรมการจัดซื้อ ดังนี้

6.1 ซองข้อเสนอด้านเทคนิค (ปิดผนึกซองให้เรียบร้อย) จำนวน 3 ชุด

6.2 ซองข้อเสนอด้านราคา (ปิดผนึกซองให้เรียบร้อย) จำนวน 1 ชุด พร้อมสำเนา 2 ชุด

7. หลักเกณฑ์ในการพิจารณา

สถาบันฯ จะเปิดซองพิจารณาเฉพาะข้อเสนอด้านเทคนิคก่อน สำหรับการเปิดซองข้อเสนอด้านราคา คณะกรรมการจัดซื้อจะเปิดซองข้อเสนอด้านราคาเฉพาะรายที่ผ่านการพิจารณาคัดเลือกด้านเทคนิคแล้วเท่านั้น หลักเกณฑ์การพิจารณาข้อเสนอด้านเทคนิค สถาบันฯ จะพิจารณาให้คะแนนตามหมวดต่างๆ ดังนี้

7.1	คุณสมบัติและเอกสารหลักฐานของผู้เสนอราคา	20	คะแนน
7.2	รูปแบบรายการ แนวคิด แผนงาน เทคนิค เทคโนโลยี เครื่องมืออุปกรณ์	40	คะแนน
7.3	ประวัติการดำเนินงานและผลงานของบุคลากร (คุณวุฒิและประสบการณ์)	30	คะแนน
7.4	ระยะเวลาดำเนินงานและข้อเสนออื่นๆ ที่เป็นประโยชน์ต่อสถาบันฯ	10	คะแนน
	รวมคะแนน	100	คะแนน

สถาบันฯ จะเปิดซองข้อเสนอด้านราคาเฉพาะรายที่ได้คะแนนสูงสุดจากการพิจารณาด้านเทคนิคเป็นลำดับแรก ถ้าปรากฏว่า ผู้เสนอราคาลำดับแรกเสนอราคาเกินกว่าวงเงินงบประมาณและคณะกรรมการจัดซื้อไม่สามารถต่อรองราคาให้อยู่ในวงเงินงบประมาณได้ คณะกรรมการฯ จะพิจารณาข้อเสนอของผู้เสนอราคาที่ได้คะแนนข้อเสนอด้านเทคนิคในลำดับถัดไปแทน ทั้งนี้ การตัดสินของคณะกรรมการฯ ถือเป็นที่สิ้นสุดและสถาบันฯ สงวนสิทธิในการโต้แย้ง

คณะกรรมการฯ สงวนสิทธิในการตัดสินใจดำเนินการใดๆ ระหว่างการพิจารณาคัดเลือกผู้เสนอราคา เพื่อให้เกิดประโยชน์สูงสุดต่อสถาบันฯ

8. ระยะเวลาดำเนินการและการส่งมอบ

ผู้เสนอราคาต้องส่งมอบอุปกรณ์ป้องกันเครือข่าย อุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย อุปกรณ์ควบคุมและจัดการอุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย และซอฟต์แวร์ระบบตรวจสอบการทำงานของเครือข่ายคอมพิวเตอร์ พร้อมติดตั้งให้สามารถใช้งานได้ทั้งหมดภายใน 120 วัน นับแต่วันที่ลงนามในสัญญา โดยผู้เสนอราคาจะต้องจัดทำแผนการส่งมอบพร้อมติดตั้ง และแจ้งเป็นหนังสือให้สถาบันฯ ทราบก่อนดำเนินงานภายใน 15 วัน นับแต่วันที่ลงนามในสัญญา

/9. การ...

9. การชำระเงิน

9.1 เงินงวดที่ 1 ในอัตราร้อยละ 70 ของราคาที่ตกลงจัดซื้อ โดยชำระภายใน 30 วัน นับแต่วันที่สถาบันฯ ได้รับส่งมอบอุปกรณ์และซอฟต์แวร์ตามข้อ 5. ทุกรายการ และคณะกรรมการตรวจรับได้ดำเนินการตรวจรับเรียบร้อยแล้ว

9.2 เงินงวดที่ 2 ภายหลังจากการชำระเงินงวดที่ 1 เป็นระยะเวลา 30 วัน ในอัตราร้อยละ 10 ของราคาที่ตกลงจัดซื้อ โดยจะชำระภายใน 30 วัน นับแต่วันที่สถาบันฯ ได้รับมอบรายงานการบำรุงรักษาอุปกรณ์และซอฟต์แวร์ตามข้อ 5. ครั้งที่ 1 และคณะกรรมการตรวจรับได้ดำเนินการตรวจรับเรียบร้อยแล้ว

9.3 เงินงวดที่ 3 ภายหลังจากการชำระเงินงวดที่ 2 เป็นระยะเวลา 30 วัน ในอัตราร้อยละ 10 ของราคาที่ตกลงจัดซื้อ โดยจะชำระภายใน 30 วัน นับแต่วันที่สถาบันฯ ได้รับมอบรายงานการบำรุงรักษาอุปกรณ์และซอฟต์แวร์ตามข้อ 5. ครั้งที่ 2 และคณะกรรมการตรวจรับได้ดำเนินการตรวจรับเรียบร้อยแล้ว

9.4 เงินงวดที่ 4 ภายหลังจากการชำระเงินงวดที่ 3 เป็นระยะเวลา 30 วัน ในอัตราร้อยละ 10 ของราคาที่ตกลงจัดซื้อ โดยจะชำระภายใน 30 วัน นับแต่วันที่สถาบันฯ ได้รับมอบรายงานการบำรุงรักษาอุปกรณ์และซอฟต์แวร์ตามข้อ 5. ครั้งที่ 3 และคณะกรรมการตรวจรับได้ดำเนินการตรวจรับเรียบร้อยแล้ว

10. ระยะเวลารับประกัน

10.1 ผู้เสนอราคาต้องรับประกันรายการอุปกรณ์และซอฟต์แวร์ตามข้อ 5. เป็นระยะเวลาไม่น้อยกว่า 3 ปี นับจากวันที่คณะกรรมการตรวจรับได้ดำเนินการตรวจรับการส่งมอบงานเรียบร้อยแล้ว ในกรณีที่รายการอุปกรณ์และซอฟต์แวร์ใดๆ ตามข้อ 5. เกิดข้อขัดข้องจนไม่สามารถใช้งานได้ ผู้เสนอราคาต้องเข้ามาแก้ไขและซ่อมแซม ณ สถานที่ส่งมอบ ตามที่ระบุไว้ในข้อ 4. (On-site Services) ภายในระยะเวลาไม่เกิน 4 ชั่วโมง หลังจากที่ได้รับแจ้งปัญหาทางใดทางหนึ่ง เช่น โทรศัพท์ อีเมล ฯลฯ

10.2 ผู้เสนอราคาที่ได้รับคัดเลือกในการจัดซื้อด้วยวิธีการคัดเลือกนี้ จะต้องทำสัญญาซื้อขายตามแบบสัญญาที่สถาบันฯ กำหนด และจะต้องวางหลักประกันการปฏิบัติตามสัญญาเป็นจำนวนเงินเท่ากับร้อยละ 5 ของราคาที่ตกลงซื้อขาย ให้สถาบันฯ ยึดถือไว้ในขณะทำสัญญา โดยใช้หลักประกันอย่างหนึ่งอย่างใด ดังต่อไปนี้

(1) เงินสด

(2) แคชเชียร์เช็คที่ธนาคารสั่งจ่ายให้แก่ สถาบันวิจัยและพัฒนาอัญมณีและเครื่องประดับแห่งชาติ (องค์การมหาชน) โดยเป็นเช็คลงวันที่ที่ทำสัญญาหรือก่อนหน้านั้นไม่เกิน 3 วันทำการ

(3) หนังสือค้ำประกันของธนาคารภายในประเทศ

10.3 ผู้เสนอราคาซึ่งสถาบันฯ ได้คัดเลือกแล้วไม่ไปทำสัญญา หรือข้อตกลงภายในเวลาที่สถาบันฯ กำหนด สถาบันฯ อาจพิจารณาเรียกร้องให้ชดใช้ความเสียหายอื่นๆ (ถ้ามี) รวมทั้งจะพิจารณาให้เป็นผู้ทิ้งงาน

10.4 สถาบันฯ สงวนสิทธิที่จะแก้ไขเพิ่มเติมเงื่อนไขหรือข้อกำหนดในแบบสัญญาให้เหมาะสมได้

/11. ค่าปรับ...

11. ค่าปรับกรณีผู้เสนอราคามิได้ปฏิบัติตามสัญญา

เมื่อครบกำหนดการส่งมอบอุปกรณ์ป้องกันเครือข่าย อุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย อุปกรณ์ควบคุมและจัดการอุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย ซอฟต์แวร์ระบบตรวจสอบการทำงานของเครือข่ายคอมพิวเตอร์ พร้อมติดตั้ง ตามระยะเวลาการส่งมอบที่กำหนดไว้ในสัญญา แต่ผู้เสนอราคายังไม่ได้ส่งมอบ หรือส่งมอบไม่ถูกต้องครบถ้วน หรือส่งมอบทั้งหมดแต่ใช้งานไม่ได้ตามที่กำหนดไว้ในข้อ 5. ให้ถือว่าผู้เสนอราคายังไม่ได้ส่งมอบงานนั้นเลย และผู้เสนอราคาจะต้องชำระค่าปรับให้กับสถาบันฯ เป็นรายวันในอัตราร้อยละ 0.20 ของมูลค่างานทั้งหมด

12. หน่วยงานรับผิดชอบดำเนินการ

สถานที่ติดต่อเพื่อขอทราบข้อมูลเพิ่มเติม สถาบันวิจัยและพัฒนาอัญมณีและเครื่องประดับแห่งชาติ (องค์การมหาชน) ชั้น 6 อาคารชุดไอทีเอฟ-ทาวเวอร์ ถนนสีลม แขวงสุริยวงศ์ เขตบางรัก กรุงเทพมหานคร

(1) ฝ่ายเทคโนโลยีสารสนเทศ โทรศัพท์ 0 2634 4999 ต่อ 434 โทรสาร 0 2634 4970

(2) ส่วนงานจัดซื้อและพัสดุฯ โทรศัพท์ 0 2634 4999 ต่อ 617 โทรสาร 0 2634 4970

แบบรูปรายการและคุณลักษณะเฉพาะ
งานปรับปรุงโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ

---

1. ข้อมูลความต้องการ

1.1 ผู้เสนอราคาที่ได้รับการคัดเลือกต้องดำเนินการจัดหาและติดตั้งอุปกรณ์และซอฟต์แวร์ดังรายการต่อไปนี้

1.1.1 อุปกรณ์ป้องกันเครือข่าย (Firewall) จำนวน 2 ชุด โดยติดตั้งแทนที่อุปกรณ์เดิม

1.1.2 อุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย (Access Point: AP) จำนวน 15 ชุด โดยติดตั้งแทนที่อุปกรณ์เดิม จำนวน 8 ชุด และติดตั้งพร้อมเดินสายสัญญาณใหม่ จำนวน 7 ชุด ตามจุดที่สถาบันฯ กำหนด

1.1.3 อุปกรณ์ควบคุมและจัดการอุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย (AP Controller) จำนวน 1 ชุด โดยติดตั้งแทนที่อุปกรณ์เดิม

1.1.4 ซอฟต์แวร์ระบบตรวจสอบการทำงานของเครือข่ายคอมพิวเตอร์ (Computer Network Monitoring Software) จำนวน 1 ชุด

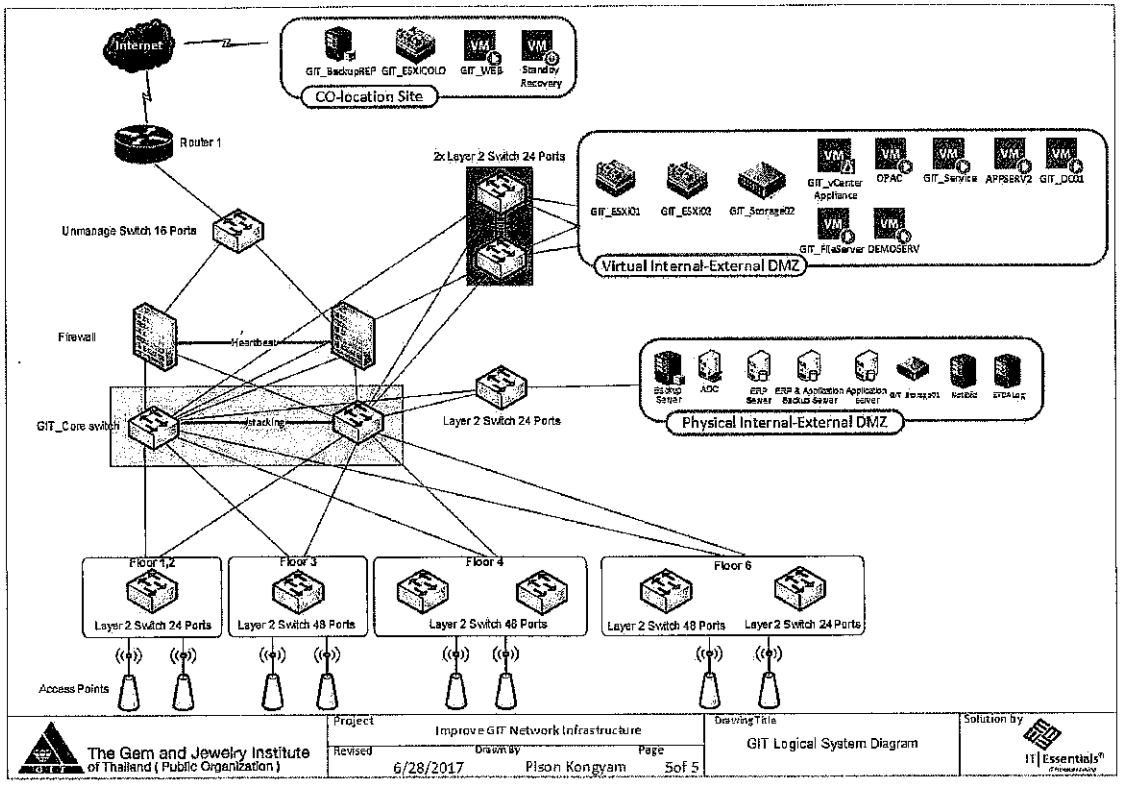
1.2 ผู้เสนอราคาที่ได้รับการคัดเลือกต้องดำเนินการกำหนดค่าหรือตั้งค่า (Configure) อุปกรณ์และซอฟต์แวร์ในข้อ 1.1.1 ถึง 1.1.4 ให้สามารถเชื่อมต่อและทำงานร่วมกัน ตลอดจนทำงานร่วมกับระบบเครือข่ายปัจจุบันของสถาบันฯ ดังรูปที่ 1 ได้

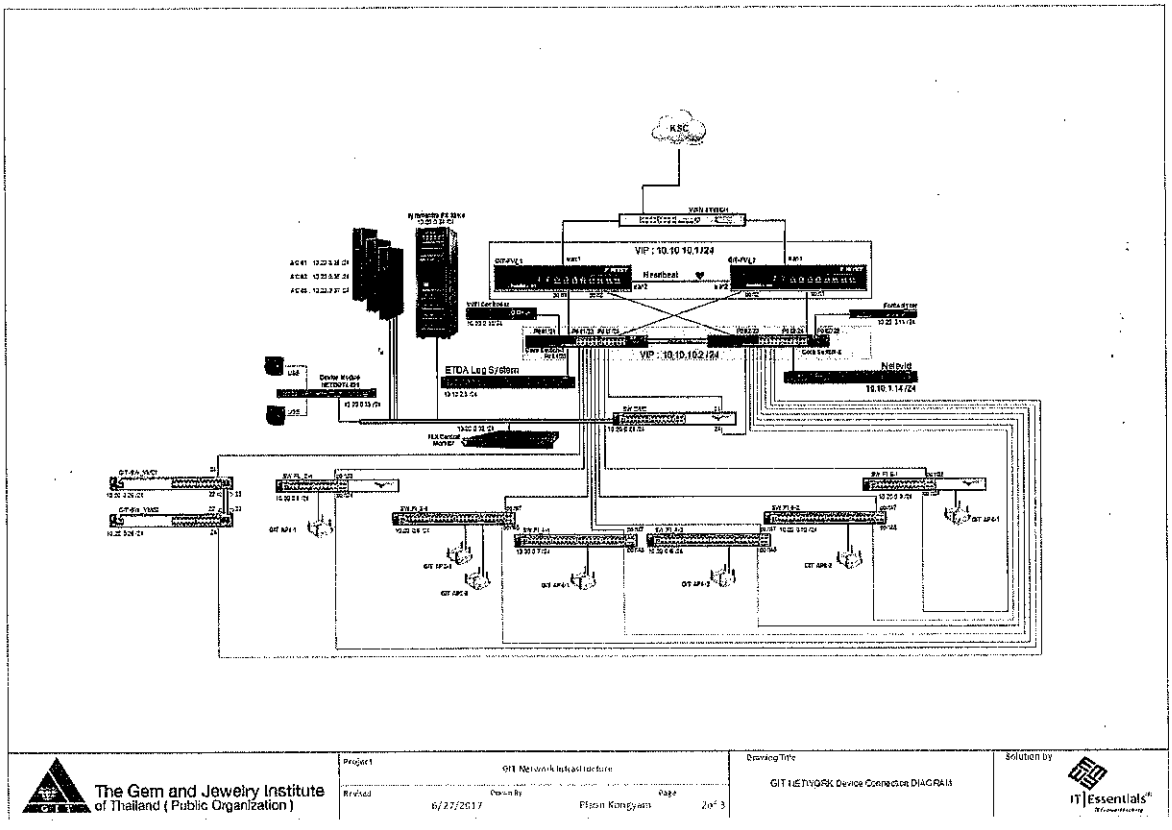
1.3 ผู้เสนอราคาที่ได้รับการคัดเลือกต้องจัดอบรมแก่เจ้าหน้าที่ของหน่วยงานด้านเทคโนโลยีสารสนเทศของสถาบันฯ จำนวนไม่น้อยกว่า 2 คน ในแต่ละหลักสูตรดังต่อไปนี้เป็นอย่างน้อย ณ สำนักงานของสถาบันฯ

1.3.1 หลักสูตรจัดการและบำรุงรักษาอุปกรณ์ป้องกันเครือข่าย (Firewall)

1.3.2 หลักสูตรจัดการและบำรุงรักษาอุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย (Access Point: AP) และอุปกรณ์ควบคุมและจัดการอุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย (AP Controller)

1.3.3 หลักสูตรการใช้งานซอฟต์แวร์ระบบตรวจสอบการทำงานของเครือข่ายคอมพิวเตอร์





รูปที่ 1 แสดงระบบเครือข่ายปัจจุบันของสถาบันฯ (Production Network)

2. คุณลักษณะทั่วไป

2.1 อุปกรณ์ที่นำเสนอต้องเป็นรุ่นที่ยังมีการผลิตอยู่ในสายการผลิตปัจจุบัน และเป็นของใหม่ซึ่งยังไม่เคยถูกใช้งานมาก่อน

2.2 อุปกรณ์ที่นำเสนอต้องมีเอกสารรับรองจากผู้ผลิตที่ได้มาตรฐานเป็นที่เชื่อถือได้ และต้องเป็นผลิตภัณฑ์ที่มีตัวแทนจำหน่ายในประเทศไทยซึ่งได้รับการรับรองอย่างถูกต้องตามกฎหมาย

2.3 อุปกรณ์ทุกชิ้นต้องสามารถทำงานกับระบบไฟฟ้าในประเทศไทยซึ่งเป็นแบบ 220/230 VAC 50 Hz ได้

2.4 ซอฟต์แวร์ทั้งหมดรวมทั้งซอฟต์แวร์ที่ถูกติดตั้งมากับอุปกรณ์ต้องได้รับลิขสิทธิ์อนุญาตถูกต้องตามกฎหมาย

3. ข้อกำหนดทางเทคนิค

3.1 <u>อุปกรณ์ป้องกันเครือข่าย (Firewall)</u>

3.1.1 เป็นอุปกรณ์ Appliance ที่มีหน่วยประมวลผลแบบ Multicore และได้รับการออกแบบมาเพื่อทำหน้าที่รักษาความปลอดภัยของระบบเครือข่ายโดยเฉพาะ

3.1.2 มีตัวเครื่องเป็นแบบยึดเข้ากับตู้สำหรับจัดเก็บอุปกรณ์ขนาดมาตรฐานและมีความสูงไม่เกิน 2U

3.1.3 มีช่อง (Port) สำหรับเชื่อมต่อระบบเครือข่ายแบบ 10/100/1000 Ethernet (RJ-45) ไม่น้อยกว่า 6 ช่อง และทุกช่องต้องสามารถกำหนดขอบเขต (Zone) ให้เป็นได้ทั้ง LAN/WAN/DMZ หรือขอบเขต (Zone) ที่ผู้ดูแลระบบกำหนดขึ้นมาเอง นอกจากนั้น ทุกช่องยังสามารถเป็น HA Dedicate Port ได้

3.1.4 ทำงานโดยไม่จำกัดสิขสิทธิ์จำนวนผู้ใช้ (Unlimited Concurrent User Licenses)

3.1.5 มีความสามารถในการทำงานเป็น Stateful Inspection Firewall และได้รับการรองรับตามมาตรฐานของ ICSA ด้าน Firewall หรือเทียบเท่า

3.1.6 มีความเร็วในการทำงานของ Firewall (Throughput) ไม่น้อยกว่า 18,000 Mbps

3.1.7 สามารถรองรับการเชื่อมต่อพร้อมกัน (Concurrent Sessions) ได้ไม่น้อยกว่า 8,000,000 Sessions

3.1.8 สามารถรองรับการเชื่อมต่อใหม่ (New Sessions) ได้ด้วยความเร็วไม่น้อยกว่า 140,000 Sessions ต่อวินาที

3.1.9 สามารถทำงานในลักษณะ Transparent Mode และ NAT/ROUTE Mode ได้

3.1.10 รองรับ Dynamic Routing อันได้แก่ RIP v1, RIP v2, OSPF, BGP และ Multicast

3.1.11 รองรับโปรโตคอล H.323 และ SIP

3.1.12 รองรับ NAT (Network Address Translation), VIP (Virtual IP) และ PAT (Port Address Translation)

3.1.13 รองรับ HA (High Availability) ทั้งในแบบ Active-active และ Active-passive

3.1.14 สามารถตั้งค่า Link Aggregation ตามมาตรฐาน IEEE802.3ad ได้อย่างน้อย 24 กลุ่ม

3.1.15 สามารถกรองเนื้อหาและสร้างนโยบาย (Policy) ผสมผสานกันระหว่างผู้ใช้งาน และ IP Address

3.1.16 สามารถควบคุมการเข้าถึงโดยผ่านวิธีการระบุตัวตนผู้ใช้งาน ขอบเขตต้นทาง (Source Zone) ขอบเขตปลายทาง (Destination Zone) และ IP Address

3.1.17 ,สามารถควบคุมหรือจำกัดการเชื่อมต่อระบบเครือข่ายที่เกิดจากการใช้งานโปรแกรมประเภท Peer-to-peer เช่น Bit Torrent, eDonkey, Gnutella, Kazaa, Keylogger ฯลฯ

3.1.18 สามารถทำงานในลักษณะ Content Filtering โดยสามารถกำหนดให้อุปกรณ์ป้องกันการเข้าถึง URL หรือเว็บไซต์ต้องห้าม (URL/Website Blocking) ได้

3.1.19 สามารถตรวจจับและป้องกัน Malware ในโปรโตคอล HTTP, FTP, IMAP, POP3 และ SMTP โดยได้รับการรองรับตามมาตรฐานของ ICSA ด้านการป้องกัน Malware หรือเทียบเท่า

3.1.20 สามารถตรวจสอบและป้องกันการบุกรุก (Intrusion Prevention) และมีความเร็วในการทำงาน (Throughput) ไม่น้อยกว่า 4 Gbps

3.1.21 สามารถป้องกัน Spam Mail โดยกรองข้อมูลจากหัวจดหมาย (Header) ขนาด (Size) ผู้ส่ง (Sender) และ ผู้รับ (Recipient) ได้

3.1.22 มีระบบป้องกัน Web Application (Web Application Firewall) ที่สามารถป้องกันการโจมตี Web Server จากภายในและภายนอก โดยป้องกันได้ทั้ง HTTP, HTTPS รวมทั้งสามารถป้องกันการโจมตีแบบ SQL Injections, Cross-Site Scripting, Session Hijacking, URL Tempering ได้เป็นอย่างน้อย

3.1.23 สามารถปรับปรุง (Update) ฐานข้อมูล Malware (Malware Signature) และฐานข้อมูลการบุกรุก (Attack Signature) ผ่านเครือข่ายอินเทอร์เน็ต (Internet) ได้โดยอัตโนมัติ

3.1.24 รองรับการจัดการแบนด์วิดท์ (Bandwidth Management: QoS) โดยการสร้างนโยบายสำหรับกลุ่มผู้ใช้งาน หรือเฉพาะผู้ใช้งาน รวมถึง Application โดยสามารถกำหนดปริมาณแบนด์วิดท์ต่ำสุดและสูงสุดในช่วงเวลาใดเวลาหนึ่งได้

3.1.25 สามารถเลือกตั้งค่าเวลาของอุปกรณ์โดยใช้ Network Time Protocol (NTP) หรือกำหนดเวลาเองได้

3.1.26 รองรับการตรวจสอบผู้ใช้งาน (User Authentication) กับฐานข้อมูลผู้ใช้งานภายในอุปกรณ์, Active Directory (AD) หรือ RADIUS และสามารถทำงานแบบ Single Sign-on กับฐานข้อมูลบัญชีผู้ใช้งานบน Active Directory หรือ RADIUS ได้

3.1.27 รองรับ MAC Address Authenticated Users และ MAC Address Filtering

3.1.28 สามารถแบ่งระดับของผู้ดูแลระบบได้หลายระดับเพื่อความปลอดภัยของการจัดการอุปกรณ์ และรองรับการสร้างบัญชีผู้ใช้งาน (User Account) ประเภท Guest หรือ Temp อย่างไม่จำกัด รวมทั้ง สร้างรหัสผ่านสำหรับผู้ใช้งานแบบสุ่ม (Random Password) และสามารถพิมพ์บัญชีผู้ใช้งานดังกล่าวในรูปแบบตั๋ว (Ticket) ได้

3.1.29 สามารถกำหนดช่วงเวลาในการเข้าใช้งานหรือไม่ใช้งาน (Time-based Policies) ที่ลงละเอียดถึงผู้ใช้งาน IP Address และสามารถกำหนดโควตา (Quota) แบบ Access Time, Time Quota, Data Quota และ Schedule ของแต่ละผู้ใช้งาน กลุ่มผู้ใช้งาน หรือ IP Address

3.1.30 สามารถเข้ารหัสการส่งข้อมูลด้วยวิธี VPN (Virtual Private Network) โดยเข้ารหัสแบบ IPSec ซึ่งมีความเร็วในการทำงานไม่น้อยกว่า 1,500 Mbps และได้รับการรับรองตามมาตรฐานของ ICSA ด้าน IPSec หรือเทียบเท่า

3.1.31 รองรับการกำหนด VPN สำหรับผู้ใช้งาน แยกจาก VPN สำหรับผู้ดูแลระบบ

3.1.32 VPN Client ที่สนับสนุนการทำงานบนระบบปฏิบัติการ Microsoft Windows 7 เป็นอย่างน้อย

3.1.33. สามารถจัดการอุปกรณ์ผ่าน Console และโปรแกรม Web Browser ได้

3.1.34 สามารถแจ้งเตือนผู้ดูแลระบบผ่านทาง e-mail ได้

3.1.35 สามารถจัดเก็บข้อมูลจราจรทางอิเล็กทรอนิกส์ที่มีคุณสมบัติตามที่พระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ กำหนด รวมทั้ง รายงานผล (Report) และการวิเคราะห์ข้อมูลที่ถูกจัดเก็บได้

3.1.36 สามารถเก็บรายละเอียดและตรวจสอบการใช้งาน (Logging/Monitoring) ทั้งแบบจัดเก็บภายในอุปกรณ์ และจัดเก็บที่ SysLog Server และสามารถแสดงผลได้ในรูปแบบของ HTML, PDF และ Excel format รวมทั้ง สามารถพิมพ์ผลข้อมูลผ่านทางเครื่องพิมพ์ได้

3.1.37 สามารถตั้งเวลาในการส่งรายงาน (Report) ให้ผู้ดูแลระบบได้เป็นรายวัน หรือรายสัปดาห์

3.1.38 สามารถแจ้งเตือนผู้ดูแลระบบ หากมีการโจมตีเครือข่ายคอมพิวเตอร์ ตลอดจนรายงานผลและแสดงข้อมูลการถูกโจมตีในรูปแบบ Dashboard ได้

3.1.39 ได้รับการรับรองมาตรฐานดังต่อไปนี้

3.1.39.1 มาตรฐานการแผ่กระจายคลื่นแม่เหล็กไฟฟ้า FCC หรือเทียบเท่า และ

3.1.39.2 มาตรฐานความปลอดภัย UL หรือเทียบเท่า

3.2 <u>อุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย (Access Point: AP)</u>

3.2.1 เป็นอุปกรณ์ที่ใช้คลื่นความถี่วิทยุในการรับส่งข้อมูลโดยใช้งานย่านความถี่ 2.4 GHz และ 5.0 GHz เป็นอย่างน้อย

3.2.2 มีอุปกรณ์สำหรับยึดติดกับกำแพง ผนัง หรือฝ้าเพดาน

3.2.3 มีช่อง (Port) สำหรับเชื่อมต่อระบบเครือข่าย แบบ 10/100/1000 Ethernet (RJ-45) อย่างน้อย 1 ช่อง

3.2.4 รองรับการใช้งานที่อุณหภูมิ 0 ถึง 50 องศาเซลเซียส

3.2.5 รองรับมาตรฐาน IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n และ IEEE 802.11ac รวมทั้ง มาตรฐาน IEEE 802.3af (PoE)

3.2.6 รองรับเทคโนโลยี 2x2 MIMO

3.2.7 สามารถเข้ารหัสข้อมูลโดยใช้ Advanced Encryption Standard (AES) และ Temporal Key Integrity Protocol (TKIP) ได้เป็นอย่างน้อย

3.2.8 สนับสนุนการทำ Authentication ตามมาตรฐาน IEEE 802.1X และสามารถรองรับการตรวจสอบ MAC Address (MAC Address Authentication) กับฐานข้อมูล MAC Address ภายในตัวอุปกรณ์ได้

3.2.9 สนับสนุนมาตรฐานความปลอดภัย WPA และ WPA2

3.2.10 สามารถรองรับการทำงานแบบ Multiple SSIDs ได้ไม่น้อยกว่า 8 SSIDs โดยสามารถกำหนดค่า QoS ที่แตกต่างกันในแต่ละ SSID ได้

3.2.11 สามารถจัดการอุปกรณ์ผ่าน Console และโปรแกรม Web Browser ได้

3.2.12 สามารถทำงานร่วมกับอุปกรณ์ป้องกันเครือข่าย (Firewall) ในข้อ 3.1 ได้เป็นอย่างดี

3.2.13 สามารถทำงานร่วมกับอุปกรณ์ควบคุมและจัดการอุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย (AP Controller) ในข้อ 3.3 ได้เป็นอย่างดี และต้องมีเครื่องหมายการค้าเดียวกัน

3.2.14 ได้รับการรับรองมาตรฐานดังต่อไปนี้

3.2.14.1 มาตรฐานการแผ่กระจายคลื่นแม่เหล็กไฟฟ้า FCC หรือเทียบเท่า และ

3.2.14.2 มาตรฐานความปลอดภัย UL, EN หรือเทียบเท่า

3.3 <u>อุปกรณ์ควบคุมและจัดการอุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย (AP Controller)</u>

3.3.1 เป็นอุปกรณ์ที่ออกแบบมาเพื่อทำหน้าที่ควบคุมและจัดการอุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย (Access Point: AP) ในข้อ 3.2 ตามมาตรฐาน IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n และ IEEE 802.11ac

3.3.2 สามารถควบคุมอุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย (AP) ได้ไม่น้อยกว่า 15 เครื่อง

3.3.3 มีช่อง (Port) สำหรับเชื่อมต่อระบบเครือข่าย แบบ 10/100/1000 Ethernet (RJ-45) อย่างน้อย 4 ช่อง

3.3.4 สนับสนุนการทำ Authentication ตามมาตรฐาน IEEE 802.1X และสามารถตรวจสอบสิทธิ์ผู้ใช้งานโดยทำงานร่วมกับ Active Directory (AD) ได้

3.3.5 รองรับการทำ Authentication ผ่าน RADIUS, TACACS และ Web-based

3.3.6 รองรับการสร้าง Guest Account และสามารถให้บริการ Guest Access Users ได้พร้อมกันไม่น้อยกว่า 200 Users

3.3.7 รองรับการสร้างหน้าเว็บ Authentication แบบ Internal Captive Portal และ External Captive Portal

3.3.8 รองรับการทำงานตามมาตรฐาน IEEE 802.1Q VLAN Tagging และ IEEE 802.1ad Link Aggregation หรือ LACP

3.3.9 รองรับการกำหนด VLAN ได้ไม่น้อยกว่า 500 VLANs

3.3.10 สามารถกำหนด Bandwidth Contract สำหรับผู้ใช้แต่ละคนได้

3.3.11 สนับสนุนมาตรฐานความปลอดภัย WPA และ WPA2

3.3.12 สามารถเข้ารหัสข้อมูลโดยใช้ Advanced Encryption Standard (AES) และ Temporal Key Integrity Protocol (TKIP) ได้เป็นอย่างน้อย

3.3.13 สามารถตรวจจับอุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย (AP) แปลกปลอมได้ (Rogue Detection)

3.3.14 สามารถตรวจพบระบบปฏิบัติการ (OS) ของอุปกรณ์ที่เชื่อมต่อระบบเครือข่ายไร้สายได้

3.3.15 รองรับการ Roaming ในลักษณะ Layer 2 และ Layer 3

3.3.16 สามารถจัดการอุปกรณ์ผ่าน Console และโปรแกรม Web Browser ได้

3.3.17 สามารถทำงานร่วมกับอุปกรณ์ป้องกันเครือข่าย (Firewall) ในข้อ 3.1 ได้เป็นอย่างดี

3.3.18 สามารถทำงานร่วมกับอุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย (AP) ในข้อ 3.2 ได้เป็นอย่างดี และต้องมีเครื่องหมายการค้าเดียวกัน

3.3.19 ได้รับการรับรองมาตรฐานดังต่อไปนี้

3.3.19.1 มาตรฐานการแผ่กระจายคลื่นแม่เหล็กไฟฟ้า FCC หรือเทียบเท่า และ

3.3.19.2 มาตรฐานความปลอดภัย UL, CSA, EN หรือเทียบเท่า

3.4 <u>ซอฟต์แวร์ระบบตรวจสอบการทำงานของเครือข่ายคอมพิวเตอร์</u>

3.4.1 สามารถตรวจสอบการทำงานของอุปกรณ์เครือข่าย รวมทั้ง เครื่องแม่ข่ายทั้งแบบ Physical และ Virtual Machine ซึ่งทำงานบนระบบปฏิบัติการ Windows Server 2008 R2 ขึ้นไปได้

3.4.2 สามารถตรวจสอบการทำงานของ Application ดังต่อไปนี้ ได้เป็นอย่างน้อย

3.4.2.1 Microsoft Active Directory

3.4.2.2 Microsoft IIS Server 7

3.4.2.3 Microsoft SQL Server 2008

3.4.3 สามารถแสดงสถานะการทำงานที่เกิดขึ้นของระบบปฏิบัติการและ Application รวมทั้งองค์ประกอบต่างๆ โดยใช้สัญลักษณ์สีได้

3.4.4 สามารถตรวจสอบการทำงานของเครื่องแม่ข่าย อุปกรณ์เครือข่าย และ Application ผ่าน Console และโปรแกรม Web Browser ได้

3.4.5 สามารถกำหนดสิทธิ์การเข้าใช้งานระบบเป็นรายบุคคลหรือกลุ่มบุคคลได้

3.4.6 สามารถแสดงแผนผังความสัมพันธ์ระหว่าง Application ที่ต้องการตรวจสอบกับส่วนประกอบของระบบเครือข่ายในรูปแบบ Graphical Interface รวมทั้ง สร้าง Network Diagram ที่สามารถแสดงผลได้บนหน้าจอคอมพิวเตอร์และอุปกรณ์สื่อสารแบบพกพา

3.4.7 รองรับการแจ้งเตือนผู้ดูแลระบบทาง email

3.4.8 สามารถให้ผู้ดูแลระบบเลือกวิธีการตรวจสอบการทำงานของเครื่องแม่ข่ายในรูปแบบ Agent หรือ Agentless ได้

3.4.9 สามารถแสดงการใช้งานทรัพยากรของเครื่องแม่ข่ายและอุปกรณ์เครือข่าย (Performance) แบบ Real Time

3.4.10 สามารถเก็บสถิติและจัดทำรายงานข้อมูลที่เกิดขึ้นในระหว่างช่วงเวลาที่กำหนดได้ตลอดจน รองรับการสร้างรายงานโดยผู้ดูแลระบบ

3.4.11 สามารถกรองข้อมูลเพื่อให้ได้รายงานที่แสดงถึงสภาวะการทำงาน รวมทั้ง การใช้ทรัพยากร (Utilization & Performance) ของเครื่องแม่ข่ายและอุปกรณ์เครือข่าย ตามสภาวะความเป็นจริง

3.4.12 รองรับการตั้งค่า Self-Tuning Threshold เพื่อป้องกัน False Alarm

3.4.13 สามารถจัดเก็บเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Event) โดยจัดเก็บจาก Security Log ในระบบปฏิบัติการบนเครื่องแม่ข่าย

3.4.14 มี Maintenance Mode สำหรับการป้องกันการแจ้งเตือนในกรณีที่เครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายหยุดให้บริการเนื่องจากการบำรุงรักษา