รายละเอียดคุณลักษณะ ราคากลาง และหลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอรายการซื้อพร้อมติดตั้งระบบรักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์ (Firewall) จำนวน 1 ระบบ มหาวิทยาลัยราชภัฏพระนครศรีอยุธยา

1. ความเป็นมา

การจัดหาระบบรักษาความปลอดภัยของเครือข่ายคอมพิวเตอร์ (Firewall) เพื่อทดแทนระบบเดิมสำหรับมหาวิทยาลัยมีหลักการและเหตุผลที่สำคัญในการเสริมสร้างความปลอดภัยให้กับเครือข่ายคอมพิวเตอร์ ซึ่งเป็นโครงสร้างพื้นฐานสำคัญในการให้บริการทางการศึกษาและการบริหารจัดการภายในมหาวิทยาลัย ในยุคปัจจุบันที่เทคโนโลยีและการใช้งานอินเทอร์เน็ตมีการพัฒนาอย่างรวดเร็ว การโจมตีทางไซเบอร์มีความซับซ้อนและหลากหลายมากขึ้น เช่น การโจมตีจากแฮกเกอร์ การแพร่กระจายของมัลแวร์ หรือการโจมตีแบบ DDoS (Distributed Denial of Service) ที่สามารถส่งผลกระทบต่อการทำงานของเครือข่ายและการเข้าถึงข้อมูลสำคัญของมหาวิทยาลัย ระบบ Firewall ที่ทันสมัยจะช่วยให้มหาวิทยาลัยสามารถกรองข้อมูลที่ไม่พึงประสงค์ ป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตจากภายนอก และป้องกันภัยคุกคามที่อาจเกิดจากภายในเครือข่ายได้อย่างมีประสิทธิภาพมากขึ้น ระบบเดิมที่มีอาจไม่สามารถรับมือกับภัยคุกคามที่มีความซับซ้อนในปัจจุบันหรือไม่สามารถรองรับการป้องกันที่มีประสิทธิภาพในระดับสูงได้ เนื่องจากอาจมีข้อจำกัดในเรื่องของฟังก์ชันหรือความสามารถในการตรวจจับและตอบสนองต่อการโจมตีที่เกิดขึ้น การทดแทนระบบ Firewall เก่าด้วยระบบที่ทันสมัยจะช่วยให้มหาวิทยาลัยสามารถรองรับการเติบโตของปริมาณข้อมูลและผู้ใช้งานในเครือข่ายได้ดียิ่งขึ้น โดยระบบใหม่สามารถรองรับการขยายเครือข่ายในอนาคต เช่น การเพิ่มอุปกรณ์ใหม่ การเชื่อมต่อกับระบบภายนอก หรือการรองรับการใช้งานของผู้ใช้ที่มากขึ้น โดยไม่กระทบต่อความเสถียรของระบบ นอกจากนี้ ระบบ Firewall ใหม่ยังมีฟังก์ชันที่ทันสมัย เช่น การตรวจจับภัยคุกคามในรูปแบบของการเรียนรู้จากพฤติกรรม (Behavioral Analysis) การป้องกันการโจมตีในระดับแอปพลิเคชัน (Application Layer) การจัดการและควบคุมการใช้งานเครือข่าย (Traffic Shaping) และฟังก์ชันอื่น ๆ ที่ช่วยเพิ่มความปลอดภัยในหลายมิติ ซึ่งจะทำให้การป้องกันข้อมูลสำคัญของมหาวิทยาลัย เช่น ข้อมูลส่วนบุคคลของนักศึกษา คณาจารย์ และบุคลากร เป็นไปอย่างมีประสิทธิภาพและปลอดภัยมากยิ่งขึ้น

อีกทั้งระบบ Firewall ที่ใหม่จะช่วยให้ฝ่ายเทคโนโลยีสารสนเทศของมหาวิทยาลัยสามารถตรวจสอบและจัดการความปลอดภัยของเครือข่ายได้อย่างรวดเร็วและแม่นยำมากขึ้น โดยการให้ข้อมูลและการแจ้งเตือนภัยที่มีความแม่นยำสูง รวมถึงการวิเคราะห์ข้อมูลจราจรที่เข้าและออกจากเครือข่ายเพื่อหาจุดเสี่ยงหรือช่องโหว่ที่อาจเกิดขึ้น ซึ่งจะช่วยให้ฝ่ายเทคโนโลยีสารสนเทศสามารถตอบสนองและดำเนินการแก้ไขได้ทันท่วงที ลดความเสี่ยงจากการถูกโจมตีที่อาจจะส่งผลกระทบต่อการดำเนินงานของมหาวิทยาลัย นอกจากนี้ ระบบ Firewall ที่มีฟังก์ชันการจัดการแบบศูนย์กลาง (Centralized Management) ยังช่วยให้การจัดการเครือข่ายเป็นไปได้อย่างสะดวกและรวดเร็ว ลดภาระงานของฝ่ายเทคโนโลยีสารสนเทศในการตรวจสอบและดูแลรักษาระบบ

ในด้านการปฏิบัติตามกฎหมายและข้อกำหนดต่าง ๆ ระบบ Firewall ที่ทันสมัยยังช่วยให้มหาวิทยาลัยสามารถปฏิบัติตามพระราชบัญญัติคอมพิวเตอร์ และข้อบังคับที่เกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูลได้อย่างถูกต้องและครบถ้วน การมีระบบที่สามารถควบคุมและตรวจสอบการเข้าถึงข้อมูลและแหล่งข้อมูลต่าง ๆ ได้อย่างรัดกุม เป็นการป้องกันการละเมิดสิทธิ์ส่วนบุคคลและการเผยแพร่ข้อมูลที่อาจจะผิดกฎหมาย โดยเฉพาะในกรณีที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของนักศึกษาและบุคลากรในมหาวิทยาลัย ซึ่งเป็นข้อมูลที่ต้องมีการคุ้มครองตามมาตรฐานความปลอดภัย

ด้วยเหตุนี้ การจัดหา ระบบ Firewall ที่ทันสมัยเพื่อทดแทนระบบเดิมจึงไม่เพียงแต่เป็นการปรับปรุงด้านความปลอดภัยของเครือข่าย แต่ยังเป็นการยกระดับการจัดการเครือข่ายคอมพิวเตอร์ให้ทันสมัยและรองรับการขยายตัวในอนาคต พร้อมทั้งสามารถตอบสนองต่อการโจมตีหรือภัยคุกคามในรูปแบบต่าง ๆ ได้อย่างมีประสิทธิภาพและรวดเร็ว รวมทั้งยังเป็นการปฏิบัติตามข้อกำหนดทางกฎหมายเพื่อปกป้องข้อมูลสำคัญของมหาวิทยาลัยอย่างเหมาะสม

2. วัตถุประสงค์

2.1 เพื่อเพิ่มความปลอดภัยของเครือข่ายคอมพิวเตอร์ เป็นการป้องกันการโจมตีทางไซเบอร์และการเข้าถึงข้อมูลที่ไม่ได้รับอนุญาตจากภายนอกและภายในเครือข่าย

2.2 เพื่อลดความเสี่ยงจากภัยคุกคาม ช่วยในการตรวจจับและป้องกันภัยคุกคามที่ซับซ้อน เช่น มัลแวร์ การโจมตี DDoS และการแฮ็ก

2.3 เพื่อรองรับการขยายเครือข่ายในอนาคต ให้สามารถรองรับการขยายตัวของเครือข่ายคอมพิวเตอร์และจำนวนผู้ใช้งานที่เพิ่มขึ้นได้อย่างมีประสิทธิภาพ

2.4 เพื่อปฏิบัติตามกฎหมายและข้อกำหนดด้านความปลอดภัย ช่วยให้มหาวิทยาลัยปฏิบัติตามพระราชบัญญัติคอมพิวเตอร์ และข้อกำหนดด้านความปลอดภัยข้อมูลส่วนบุคคล

2.5 เพื่อให้จัดการเครือข่ายมีประสิทธิภาพ ทำให้ฝ่ายเทคโนโลยีสารสนเทศ (IT) ของมหาวิทยาลัยสามารถจัดการ ตรวจสอบ และตอบสนองต่อปัญหาด้านความปลอดภัยได้อย่างรวดเร็วและมีประสิทธิภาพ

3. คุณสมบัติของผู้ยื่นข้อเสนอ

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบ ที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพขายพัสดุที่จะจัดซื้อ

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ มหาวิทยาลัย ณ วันยื่นข้อเสนอและเสนอราคา หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวาง การแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาล ของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

3.10 ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ต้องมีคุณสมบัติดังนี้

(1) การกำหนดสัดส่วนในการเข้าร่วมค้าของคู่สัญญา

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงฯ จะต้องมีการกำหนดสัดส่วนหน้าที่และความรับผิดชอบในปริมาณงาน สิ่งของหรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

(2) กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

(3) การยื่นข้อเสนอของกิจการร่วมค้า

(3.1) กรณีที่ข้อตกลงฯ กำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอ ในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

3.11 ผู้ยื่นข้อเสนอต้องลงทะเบียนที่มีข้อมูลถูกต้องครบถ้วนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e-GP) ของกรมบัญชีกลาง

3.12 ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

(1) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า 1 ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิ ที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก 1 ปีสุดท้ายก่อนวันยื่นข้อเสนอ

(2) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ให้พิจารณากำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ไม่ต่ำกว่า 1 ล้านบาท

(3) สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเงินเกิน 500,000 บาทขึ้นไป กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดา โดยพิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน 90 วัน ก่อนวันยื่นข้อเสนอ โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

(4) กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่างบประมาณที่ยื่นข้อเสนอในครั้งนั้น (สินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์ และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันที่ยื่นข้อเสนอไม่เกิน 90 วัน)

(5) กรณีตาม (1) - (4) ยกเว้นสำหรับกรณีดังต่อไปนี้

(5.1) กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ

(5.2) นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย (ฉบับที่ 10) พ.ศ. 2561

3.13 ผู้ยื่นข้อเสนอต้องจัดทำตารางเปรียบเทียบข้อกำหนดตามรายละเอียดคุณลักษณะเฉพาะที่มหาวิทยาลัยกำหนดกับคุณลักษณะที่เสนอ โดยอ้างอิงหัวข้อของเอกสารผลิตภัณฑ์พร้อมระบุหน้าที่ปรากฏใน Catalog ด้วย

4. รายละเอียดการบำรุงรักษาระบบรักษาความปลอดภัยของเครือข่ายคอมพิวเตอร์ (Firewall) จำนวน 1 ระบบ มีรายละเอียดดังนี้

4.1 เป็นอุปกรณ์ Next Generation Firewall แบบ Appliance ที่ใช้ตัวประมวลผลสำหรับงานเฉพาะทาง

4.2 มีช่องต่อ GE RJ45 ไม่น้อยกว่า 16 ช่อง ช่องต่อ 1GE SFP ไม่น้อยกว่า 8 ช่องต่อ 10GE SFP+ ไม่น้อยกว่า 4 ช่องและมีช่องต่อ 25GE SFP28 ไม่น้อยกว่า 4 ช่อง

4.3 มีประสิทธิภาพการทำงาน (Throughput) ของ Firewall ไม่น้อยกว่า 150 Gbps

4.4 รองรับการเชื่อมต่อพร้อมกัน (Concurrent Sessions) ไม่น้อยกว่า 16,000,000 การเชื่อมต่อและรองรับการเชื่อมต่อใหม่ (New Sessions) ไม่น้อยกว่า 720,000 การเชื่อมต่อวินาที

4.5 รองรับ Threat Protection Throughput ได้ไม่น้อยกว่า 30 Gbps (เปิดใช้งาน Firewall และ IPS และ Application Control และ Malware Protection)

4.6 มีหน่วยเก็บข้อมูล (Storage) ขนาดความจุไม่น้อยกว่า 480 GB จำนวนไม่น้อยกว่า 2 หน่วย หรือดีกว่า

4.7 มีประสิทธิภาพการทำงาน (Throughput) ของ IPSec VPN ได้ไม่น้อยกว่า 55 Gbps รองรับ IPSec VPN Tunnel แบบ Gateway-to-Gateway พร้อมกันได้ไม่น้อยกว่า 2,000 Tunnels

4.8 รองรับผู้ใช้ SSL VPN ได้ไม่น้อยกว่า 10,000 รายพร้อมกัน

4.9 ป้องกันการเข้าถึง Web ตาม Categories และตาม URL ที่กำหนดได้

4.10 สามารถตรวจรับ Application ได้ไม่น้อยกว่า 1,000 รายการ

4.11 สามารถทำงานในลักษณะ Virtual Domain ได้ 10 ระบบเป็นอย่างน้อย

4.12 มีความสามารถในการทำ Software-Defined Wan (SD-WAN) โดยตรวจสอบ WAN SLA Latency และ Jitter และ Packet Loss ได้

4.13 รองรับการทำ High Availability (HA) แบบ Active/Active และ Active/Passive ได้

4.14 มี Power Supply ทำงานในลักษณะ Redundant และ Hot Swap

4.15 ใช้งานกับไฟฟ้ากระแสสลับ (AC) ขนาด 220 Volts 50/60 Hz

4.16 สามารถพิสูจน์ตัวตนแบบ Two-Factor Authentication (2FA) ภายในตัวอุปกรณ์ พร้อมสิทธิ์ใช้งานอย่างน้อย 2 Token

4.17 สามารถพิสูจน์ตัวตน (Authentication) ผู้ใช้งานได้โดยรองรับฐานข้อมูลผู้ใช้แบบ Local และ LDAP และ RADIUS และมีคุณสมบัติ Guest Management ที่สามารถกำหนดระยะเวลาใช้งาน (Account Expire) และสร้าง User ID และรหัสผ่านแบบสุ่ม

4.18 เป็นอุปกรณ์ที่อยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant for SD-WAN ปี 2022 หรือใหม่กว่า

4.19 เป็นอุปกรณ์ที่อยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant for Network Firewall ปี 2022 หรือใหม่กว่า

4.20 เพื่อประโยชน์ในการการบริการหลังการขายและการสำรองอะไหล่ผู้เสนอราคาต้องมีหนังสือแต่งตั้งการเป็นตัวแทนจำหน่ายจากบริษัทเจ้าของผลิตภัณฑ์ที่มีสาขาในประเทศไทยโดยตรง และมีเอกสารรับรองว่าระบบที่เสนอเป็นระบบใหม่ ไม่เคยถูกใช้งานมาก่อน และยังอยู่ในสายการผลิต โดยระบุเลขที่เอกสารของหน่วยงาน

4.21 สามารถบริหารจัดการอุปกรณ์ผ่าน Console และ Web Browser เช่น Firefox หรือ Google Chrome ได้

4.22 สามารถตรวจจับและป้องกัน Virus ที่ผ่านมากับโปรโตคอล HTTP และ IMAPและ SMTP และ POP๓ และ MAPI และ FTP ได้

4.23 สามารถทำงานในลักษณะ SD-WAN ที่ควบคุมเส้นทางของ Traffic ต่อไปนี้ได้เป็นอย่างน้อย

4.24 สามารถป้องกัน SpamEmail ด้วยวิธี IP Address Check และ URL Check และ Email Checksum ได้

4.25 อุปกรณ์ต้องมีระบบป้องกัน Web Application (Web Application Firewall)

4.26 สามารถรองรับการทำงาน IPv๖ ได้ ดังนี้ Routing และ Firewall และ UTM และ NAT๖๔ และ NAT46 และ IPSec

4.27 สามารถส่งข้อมูลเข้าไประบบสอบสวนความเสี่ยงในระบบ Sandbox Cloud เพื่อตรวจสอบ Unknow Malware ได้

4.28 รองรับการตรวจสอบผู้ใช้งาน (User Authenticator) กับ Local User ภายในอุปกรณ์เอง LDAP และ Radius รวมถึงสามารถทำงานแบบ Single Sign-On กับฐานข้อมูลผู้ใช้งานบน Active Directory (AD) และ Radius ได้

4.29 ด้าน Data Security (ความปลอดภัยข้อมูล)

- 4.29.1 ระบบต้องรองรับ Antivirus (AV) สำหรับตรวจจับไวรัส มัลแวร์ โทรจัน และภัยคุกคามแบบไฟล์ (File-based Threats)
- 4.29.2 ต้องมีความสามารถด้าน Cloud Sandboxing (SBX) เพื่อวิเคราะห์ไฟล์หรือสคริปต์ต้องสงสัยในสภาพแวดล้อมจำลองที่ปลอดภัย
- 4.29.3 ระบบต้องรองรับ Virus Outbreak Service
- 4.29.4 ต้องมีระบบ Data Loss Prevention (DLP) เพื่อควบคุมและป้องกันการรั่วไหลของข้อมูลสำคัญผ่านช่องทางต่าง ๆ เช่น อีเมล เว็บ และไฟล์อัปโหลด

4.30 ด้าน Network Security (ความปลอดภัยเครือข่าย)

- 4.30.1 ระบบต้องรองรับ Intrusion Prevention System (IPS) สำหรับตรวจจับและป้องกันการโจมตีช่องโหว่ต่าง ๆ บนเครือข่าย
- 4.30.2 ระบบต้องรองรับเทคโนโลยี Next Generation Firewall (NGFW) เช่น Application Control และ User Identity และ Content Inspection
- 4.30.3 ต้องรองรับการบริหารจัดการทราฟฟิก เช่น Routing และ WAN Optimization และ SD-WAN

4.31 ด้าน Web Security (ความปลอดภัยเว็บและอินเทอร์เน็ต)

4.31.1 ระบบต้องมี DNS Security เพื่อบล็อกโดเมนฟิชชิง มัลแวร์ และโดเมนต้องสงสัย

4.31.2 ต้องรองรับข้อมูล IP Reputation เพื่อป้องกันทราฟฟิกที่มาจาก IP อันตราย

4.31.3 ต้องมีระบบกรองเว็บไซต์ URL Filtering ตามหมวดหมู่หรือ Policy ที่กำหนด

4.31.4 ต้องรองรับ ISDB Reputation เพื่อประเมินความน่าเชื่อถือของเว็บไซต์แบบอัตโนมัติ

4.31.5 ต้องมีฟังก์ชัน Botnet Protection ป้องกันทราฟฟิกบอตและการสั่งการจาก Command and Control

4.31.6 ระบบต้องรองรับ Video Filtering เพื่อตรวจสอบและป้องกันการใช้งานผ่าน YouTube Channel

4.32 ระบบยืนยันตัวตนหลายชั้น (Multifactor Authentication – MFA)

4.32.1 อุปกรณ์ต้องรองรับการยืนยันตัวตนหลายชั้น เพื่อเพิ่มระดับความปลอดภัยในการเข้าถึงระบบ

4.32.2 รองรับรูปแบบ MFA เช่น รหัสผ่าน (Password) ร่วมกับ อีเมล หรือ SMS OTP

4.32.3 สามารถกำหนดนโยบายบังคับใช้ MFA สำหรับผู้ดูแลระบบ (Administrator) และผู้ใช้งาน VPN ได้

4.33 การฝึกอบรม (Training)

4.33.1 ผู้ขายต้องจัดการฝึกอบรมการใช้งานระบบ Firewall ให้เจ้าหน้าที่ของหน่วยงานอย่างน้อย 1 ครั้ง

4.33.2 เนื้อหาการฝึกอบรมต้องครอบคลุม

- ความรู้พื้นฐานด้านความปลอดภัยเครือข่าย
- การกำหนดนโยบายรักษาความปลอดภัย (Security Policy)
- การตั้งค่า Firewall Rules และ NAT และ VPN และ MFA
- การตรวจสอบ Log และ รายงาน และ การวิเคราะห์ภัยคุกคาม
- วิธีตรวจสอบและแก้ไขปัญหาเบื้องต้น

4.33.3 ต้องมีเอกสารประกอบการอบรม เช่น คู่มือผู้ดูแลระบบ (Admin Manual) อย่างละเอียด

4.33.4 วิทยากรผู้ทำหน้าที่ถ่ายทอดความรู้เกี่ยวกับระบบรักษาความปลอดภัยเครือข่าย (Firewall) ต้องเป็นผู้เชี่ยวชาญเฉพาะด้าน และต้องมี ใบรับรองคุณวุฒิวิชาชีพ (Certificate) จากสถาบัน หรือผู้ผลิตอุปกรณ์ (Vendor) ที่เกี่ยวข้อง

4.33.5 แสดงใบรับรองหรือหลักฐานประกอบความเชี่ยวชาญให้หน่วยงานตรวจสอบก่อนการอบรม

4.34 อุปกรณ์ทดแทนในกรณีที่เครื่องมีปัญหา (Replacement Unit)

4.34.1 หากอุปกรณ์ชำรุดหรือไม่สามารถใช้งานได้ ผู้ขายต้องจัดหาอุปกรณ์ทดแทนให้ทันทีภายใน 1 วันทำการ (Next Business Day) หรือเร็วกว่า

4.34.2 อุปกรณ์ทดแทนต้องมีคุณสมบัติเทียบเท่าหรือดีกว่าอุปกรณ์หลัก

4.34.3 ผู้ขายต้องช่วยดำเนินการกู้คืนค่าเดิม (Configuration Restore) ให้ระบบกลับมาทำงานได้ตามปกติ

4.34.4 ต้องไม่คิดค่าใช้จ่ายเพิ่มเติมภายในระยะเวลารับประกัน

4.35 การบำรุงรักษาระบบ (Maintenance) ทุก 3 เดือน

4.35.1 ผู้ขายต้องให้บริการตรวจสอบและบำรุงรักษาเชิงป้องกัน (Preventive Maintenance) ทุก 3 เดือน

4.35.2 รายการตรวจสอบต้องประกอบด้วย

- ตรวจสอบสถานะฮาร์ดแวร์ เช่น อุณหภูมิ พัดลม แหล่งจ่ายไฟ
- ตรวจสอบปริมาณการใช้งานระบบ (CPU และ Memory และ Bandwidth)
- ตรวจสอบระบบ High Availability
- ตรวจสอบและอัปเดต Firmware และ Security Patch
- ตรวจสอบ Log พฤติกรรมผิดปกติ และสัญญาณภัยคุกคาม
- ทดสอบ MFA และการเชื่อมต่อ VPN

4.35.3 ผู้ขายต้องจัดทำรายงานสรุปผลการบำรุงรักษาเป็นลายลักษณ์อักษรทุกไตรมาส

4.35.4 ให้คำแนะนำเพื่อปรับปรุงนโยบายรักษาความปลอดภัยอย่างเหมาะสม

4.36 การรับประกันและการให้บริการสนับสนุน (Warranty & Support)

4.36.1 ผู้ขายต้องรับประกันอุปกรณ์ระบบรักษาความปลอดภัยบนเครือข่าย (Firewall) พร้อมทั้งซอฟต์แวร์และลิขสิทธิ์ที่เกี่ยวข้องเป็นระยะเวลา ไม่น้อยกว่า 3 ปี โดยการรับประกันต้องครอบคลุม

- ความเสียหายหรือความชำรุดของฮาร์ดแวร์ที่เกิดจากการใช้งานตามปกติ
- การอัปเดตซอฟต์แวร์ ระบบปฏิบัติการภายในอุปกรณ์ และแพตช์ความปลอดภัย
- การอัปเดตฐานข้อมูลภัยคุกคาม (Threat Intelligence) ตลอดอายุสัญญา
- การเปลี่ยนอุปกรณ์ส่วนที่ชำรุดโดยไม่คิดค่าใช้จ่ายภายในระยะเวลารับประกัน

4.36.2 ผู้ขายต้องรับผิดชอบให้อุปกรณ์สามารถทำงานได้อย่างต่อเนื่องและมีเสถียรภาพตลอดอายุการรับประกัน

4.36.3 ผู้ขายต้องจัดให้บริการแก้ไขปัญหาในวันจันทร์-อาทิตย์ 24 ชั่วโมง ไม่เว้นวันหยุดราชการ โดยจัดเตรียมเบอร์โทรศัพท์ให้สามารถแจ้งเหตุขัดข้องได้ (Telephone Support)

4.36.4 ผู้รับจ้างต้องดำเนินการตอบกลับ (Response Time) ภายใน 1 ชั่วโมง นับจากเวลาที่ได้รับแจ้งเหตุขัดข้อง

4.36.5 ผู้รับจ้างต้องดำเนินการวิเคราะห์ และแจ้งวิธีการแก้ไขปัญหาให้ผู้ดูแลระบบทราบและติดตามผลของการแก้ไขปัญหาจนแล้วเสร็จ ต้องรายงานเป็นลายลักษณ์อักษรให้ผู้ดูแลระบบรับทราบดังนี้

4.36.5.1 กรณีวิกฤต ระบบงานหลักหยุดทำงาน หรือถูกโจมตีทางไซเบอร์จนเสียหาย หรือข้อมูลรั่วไหลแจ้งวิธีการแก้ไข ภายใน 4 ชั่วโมง นับจากตรวจพบเหตุการณ์ รายงานความคืบหน้า ทุกๆ 2 ชั่วโมง จนกว่าระบบจะกลับมาใช้งานได้ ส่งรายงานฉบับสมบูรณ์ ภายใน 3 วันทำการ หลังจากแก้ไขจบ

4.36.5.2 กรณีความรุนแรงสูง ระบบยังทำงานได้แต่ติดขัดอย่างมาก หรืออุปกรณ์เสียหาย (ความเสี่ยงสูงขึ้น) หรือตรวจพบช่องโหว่ร้ายแรงที่ต้องรีบปิด แจ้งวิธีการแก้ไข ภายใน 8 - 12 ชั่วโมง รายงานความคืบหน้า วันละ 1 ครั้งจนกว่าจะแก้ไขเสร็จ ส่งรายงานฉบับสมบูรณ์ ภายใน 5 วันทำการ หลังจากแก้ไขจบ

4.36.5.3 กรณีความรุนแรงปานกลางหรือต่ำ ปัญหาการใช้งานทั่วไป หรือการขอปรับเปลี่ยนนโยบาย หรือการตั้งค่าที่ไม่กระทบความปลอดภัยโดยตรง แจ้งวิธีการแก้ไข ภายใน 2 วันทำการ รายงานความคืบหน้า ตามรอบการประชุมหรือเมื่อมีการเปลี่ยนแปลงส่งรายงานฉบับสมบูรณ์ ภายใน 15 วันทำการ (หรือสรุปในรายงานประจำเดือน)

4.37 ผู้เสนอราคาต้องยื่นเอกสาร ณ วันเสนอราคา

4.37.1 ผู้เสนอราคาต้องได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่ายจากผู้ผลิตในประเทศไทย โดยมีหนังสือรับรองจากผู้ผลิตมาแสดงในวันที่ยื่นเสนอราคา เพื่อประโยชน์ในการการบริการหลังการขายและการสำรองอะไหล่ผู้เสนอราคาต้องมีหนังสือแต่งตั้งการเป็นตัวแทนจำหน่ายจากบริษัทเจ้าของผลิตภัณฑ์ที่มีสาขาในประเทศไทยโดยตรง และมีเอกสารรับรองว่าระบบที่เสนอเป็นระบบใหม่ ไม่เคยถูกใช้งานมาก่อน และยังอยู่ในสายการผลิต โดยระบุเลขที่เอกสารของหน่วยงาน

4.37.2 ผู้เสนอราคาต้องแสดงหลักฐานหรือหนังสือรับรองคุณวุฒิวิชาชีพ (Certificate) จากสถาบันหรือผู้ผลิตอุปกรณ์ (Vendor) ที่เกี่ยวข้อง

5. กำหนดเวลาส่งมอบพัสดุ

60 วัน นับถัดจากวันลงนามในสัญญา

6. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

เกณฑ์ราคา

7. วงเงินงบประมาณ/วงเงินที่ได้รับจัดสรร

7.1 วงเงินงบประมาณ งบประมาณแผ่นดิน ประจำปีงบประมาณ พ.ศ. 2569 เป็นจำนวนเงิน 3,188,600 บาท (สามล้านหนึ่งแสนแปดหมื่นแปดพันหกร้อยบาทถ้วน)

7.2 วงเงินราคากลาง เป็นจำนวนเงิน 3,188,600 บาท (สามล้านหนึ่งแสนแปดหมื่นแปดพันหกร้อยบาทถ้วน)

8. **งวดงานและการจ่ายเงิน**

งวดที่ 1 (งวดสุดท้าย) จะจ่ายให้ 100% เมื่อผู้ขายได้ส่งมอบพัสดุครบถ้วนตามสัญญา และคณะกรรมการตรวจรับพัสดุได้ตรวจรับเรียบร้อยแล้ว

9. **อัตราค่าปรับ**

ในกรณีที่ผู้ขายปฏิบัติผิดสัญญา จะกำหนดค่าปรับเป็นรายวันเป็นจำนวนเงินตายตัวในอัตราร้อยละ 0.20 (ศูนย์จุดสองศูนย์) ของราคาของสิ่งของที่ยังไม่ได้รับมอบนับถัดจากครบกำหนดตามสัญญา จนถึงวันที่ผู้ขายได้นำสิ่งมาส่งมอบให้แก่ผู้ซื้อจนถูกต้องครบถ้วนตามสัญญา

10. **การกำหนดระยะเวลารับประกันความชำรุดบกพร่อง**

10.1 ผู้ขายจะต้องรับประกันการใช้งานของระบบงานที่เสนอ เป็นเวลาไม่น้อยกว่า 3 ปี นับถัดจากวันที่หน่วยงานได้ตรวจรับงานทั้งหมดแล้ว โดยต้องมีหน้าที่บำรุงรักษาและซ่อมแซมแก้ไข ให้อยู่ในสภาพที่ใช้งานได้ดีอยู่เสมอ

10.2 หน่วยงานหรือผู้แทนของหน่วยงาน อาจแจ้งปัญหาหรือข้อผิดพลาดของระบบงาน สภาพของการชำรุดบกพร่องเบื้องต้นของระบบที่เสนอไปยังผู้ขายโดยทางโทรศัพท์ หรือโทรศัพท์เคลื่อนที่ หรือไปรษณีย์อิเล็กทรอนิกส์ (E-mail) หรือแอปพลิเคชันไลน์ ได้ทุกวันไม่เว้นวันหยุด และตลอด 24 ชั่วโมง และผู้ขายจะต้องตอบรับทราบภายใน 4 ชั่วโมง นับตั้งแต่เวลาที่ได้รับแจ้งโดยทางโทรศัพท์ โทรศัพท์เคลื่อนที่ หรือไปรษณีย์อิเล็กทรอนิกส์ (E-mail) หรือแอปพลิเคชันไลน์

10.3 ผู้ขายจะต้องรับประกันความชำรุดบกพร่องของอุปกรณ์เครือข่ายที่นำเสนอสำหรับงานที่เกิดขึ้นอันเนื่องจากการใช้งานตามปกติเป็นเวลาอย่างน้อย 3 ปี ในลักษณะ On - Site Support นับถัดจากวันที่มหาวิทยาลัยได้รับมอบ

10.4 ภายในระยะเวลาดังกล่าวอุปกรณ์เครือข่ายที่นำเสนอชำรุดบกพร่องหรือใช้งานไม่ได้ทั้งหมดหรือแต่เพียงบางส่วนและความชำรุดบกพร่องนั้นมิใช่ความผิดของทางหน่วยงานผู้รับจ้างจะต้องจัดการซ่อมแซมแก้ไขให้อยู่ในสภาพใช้งานได้ดังเดิมนับแต่เวลาที่ได้รับแจ้งจากหน่วยงานฯ โดยไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้นจากหน่วยงาน