รายละเอียดคุณลักษณะ ราคามาตรฐานและกำหนดหลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ
การจัดซื้อพร้อมติดตั้งครุภัณฑ์อุปกรณ์บริหารจัดการระบบเครือข่าย (Authen)
จำนวน 1 เครื่อง เป็นจำนวนเงิน 729,419 บาท
มหาวิทยาลัยราชภัฏพระนครศรีอยุธยา

1. ความเป็นมา

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ เป็นหน่วยงานที่ดูแลรับผิดชอบด้านสารสนเทศ ของมหาวิทยาลัยราชภัฏพระนครศรีอยุธยา มีภารกิจหลักในการวางโครงสร้างพื้นฐาน และให้บริการด้านระบบสารสนเทศ ระบบคอมพิวเตอร์ และเครือข่ายให้กับนักศึกษา อาจารย์ บุคลากร และหน่วยงานภายในมหาวิทยาลัย ให้สามารถใช้งานระบบสารสนเทศและระบบเครือข่ายได้อย่างต่อเนื่องและมีประสิทธิภาพ

เพื่อรองรับการใช้งานระบบสารสนเทศและระบบเครือข่ายที่เพิ่มสูงขึ้น การใช้งานระบบคอมพิวเตอร์และเครือข่ายภายในมหาวิทยาลัย จำเป็นที่ต้องมีระบบตรวจสอบผู้ใช้ (login) ที่สามารถตรวจสอบได้ถึงรายละเอียดของผู้ใช้งานระบบเครือข่ายได้ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ให้รองรับการตรวจสอบผู้ใช้เครือข่ายที่เพิ่มมากขึ้น สามารถให้บริการระบบสารสนเทศและเครือข่ายให้กับนักศึกษา อาจารย์ และบุคลากรอย่างต่อเนื่องและมีประสิทธิภาพ ดังนี้

2. วัตถุประสงค์

2.1 เพื่อปรับปรุงประสิทธิภาพระบบตรวจสอบผู้ใช้ (Login) ให้รองรับเครือข่ายขนาด 10 G

2.2 เพื่อพิสูจน์ตัวตนสำหรับการเข้าใช้งานอินเทอร์เน็ต ให้สามารถตรวจสอบการใช้งานตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

3. รายละเอียดทั่วไป

3.1 ผู้ยื่นเสนอราคาต้องมีผลงานด้านระบบเครือข่ายคอมพิวเตอร์ ซึ่งมีวงเงินสัญญา ไม่น้อยกว่า 360,000 บาท (สามแสนหกหมื่นบาทถ้วน)

3.2 ผู้ยื่นเสนอราคาต้องมีเจ้าหน้าที่หลัก (Single Contact Point) ไม่น้อยกว่า 1 คน เพื่อรับแจ้งปัญหาและประสานงานด้านต่าง ๆ ที่เกี่ยวข้อง

3.3 ผู้ยื่นข้อเสนอต้องมีบุคลากรผู้เชี่ยวชาญด้านระบบคอมพิวเตอร์ ทั้งฮาร์ดแวร์ซอฟต์แวร์ System และ Application Software และระบบเครือข่าย คอมพิวเตอร์ทั้งอุปกรณ์สื่อสาร อุปกรณ์คอมพิวเตอร์ และอุปกรณ์ที่เกี่ยวข้อง และมีประสบการณ์ไม่น้อยกว่า 1 ปี โดยผู้เสนอราคาจะต้องแนบหลักฐานในวันที่ยื่นเสนอราคา

3.4 ผู้ยื่นเสนอราคาต้องจัดทำตารางการเปรียบเทียบรายละเอียด คุณลักษณะเฉพาะของครุภัณฑ์ตามข้อกำหนดของมหาวิทยาลัย กับที่เสนอเป็นข้อ ๆ ในแต่ละรายการอย่างละเอียดโดย พิมพ์เป็นเอกสารประกอบการนำเสนอ พร้อมทั้งบ่งชี้ในแต่ละรายการ และในแคตาล็อกอย่างครบถ้วนและชัดเจน โดยไม่อนุญาตให้มีการขอส่งเอกสารเพิ่มเติมในภายหลังไม่ว่ากรณีใด ๆ นับจากวันให้ยื่นเสนอราคา

4. รายละเอียดคุณสมบัติของอุปกรณ์ มีคุณสมบัติดังนี้

ครุภัณฑ์อุปกรณ์บริหารจัดการระบบเครือข่าย (Authen) จำนวน 1 เครื่อง ซึ่งมีคุณลักษณะดังนี้

4.1 เป็นอุปกรณ์ Hardware appliance ที่ถูกออกแบบมาเพื่อรองรับการพิสูจน์ตัวตนโดยเฉพาะ

4.2 มีพอร์ตการเชื่อมต่อระบบเครือข่าย (Network Interfaces) แบบ 10/100/1000 (RJ-45) จำนวนไม่น้อยกว่า 2 พอร์ต และแบบ 10G SFP+ ไม่น้อยกว่า 2 ช่อง

4.3 ซีพียูสถาปัตยกรรม Multi-core

4.4 หน่วยความจำหลักความจุไม่น้อยกว่า 64 กิกะไบต์

4.5 หน่วยความจำสำรองความจุไม่น้อยกว่า 8 เทระไบต์

4.6 มีแหล่งจ่ายไฟ (Power Supply) จำนวน 2 หน่วย ทำงานร่วมกันแบบ Redundant

4.7 สามารถทำการพิสูจน์ตัวตนของผู้ใช้งานได้อย่างน้อย 10,000 users โดยไม่ต้องซื้ออุปกรณ์อื่นเพิ่มเติม

4.8 สามารถสร้างกลุ่มผู้ใช้งาน (User group) บนตัวเองได้ 800 กลุ่มผู้ใช้งานเป็นอย่างน้อย

4.9 สามารถพิสูจน์ตัวตน (User Authentication) และตรวจสอบสิทธิ์ (User Authorization) ของผู้ใช้งานระบบเครือข่ายได้เป็นอย่างน้อย

4.10 สามารถทำ Single Sign-on ร่วมกับ Active directory, LDAP server, RADIUS server และ SAML ได้เป็นอย่างน้อย

4.11 สามารถพิสูจน์ตัวตนผู้ใช้งาน ได้ทั้งการเชื่อมต่อผ่านระบบเครือข่ายแบบ Wired LAN และ Wireless LAN ตามมาตรฐาน IEEE 802.1X ได้

4.12 รองรับการทำงาน High availability (HA) แบบ Active-Passive ได้เป็นอย่างน้อย

4.13 สามารถบริหารจัดการผ่านทาง Console CLI และ HTTPS ได้เป็นอย่างน้อย

4.14 ทำงานผ่านเว็บบราวเซอร์โดยมีฟังก์ชันให้ผู้ดูแลระบบบริหารจัดการระบบ

4.15 มีหน้าจอ GUI เพื่อใช้บริหารจัดการระบบ ดังนี้

4.15.1 ใช้ควบคุมและปรับตั้งค่าระบบตรวจสอบการยืนยันตัวบุคคล

4.15.2 ใช้ควบคุมและปรับตั้งค่า Captive Portal

4.15.3 แสดงสถานะระบบ โดยแสดงค่าการใช้ซีพียู หน่วยความจำ และฮาร์ดดิส

4.15.4 สร้าง ลบ แก้ไข บัญชีผู้ดูแลระบบ

4.15.5 เปลี่ยนรหัสผ่านของผู้ดูแลระบบ

4.15.6 การกำหนดกลุ่มผู้ดูแลระบบ และกำหนดสิทธิ์ที่แตกต่างกันแต่ละกลุ่ม

4.15.7 กำหนดไอพีแอดเดรสของคอมพิวเตอร์ไคลเอ็นต์ที่อนุญาตให้เข้าปรับแต่งระบบ

4.15.8 กำหนดไอพีแอดเดรสหรือกลุ่มของไอพีแอดเดรส IPv4/IPv6 ของเครื่องลูกข่ายที่ผ่านเครือข่ายได้ โดยไม่ต้องยืนยันตัวบุคคล (Bypass List)

4.15.9 กำหนดไอพีแอดเดรส IPv4/IPv6 ของเครื่องแม่ข่ายที่ผ่านเครือข่ายได้ โดยไม่ต้องยืนยันตัวบุคคล

4.16 มีฟังก์ชันการบริหารจัดการการยืนยันตัวบุคคล ดังนี้

4.16.1 กำหนดการยืนยันตัวตนด้วยชื่อบัญชีและรหัสผ่าน เพื่อให้ไอพีแอดเดรสของเครื่องไคลเอ็นต์ที่ใช้สามารถเข้าสู่อินเทอร์เน็ต

4.16.2 ทำ Dual Authentication เพียงครั้งเดียว หากเครื่องไคลเอ็นต์ที่ใช้เป็น Dual Stack ที่มี IPv4 และ IPv6 อยู่ในขณะเดียวกัน

4.16.3 กำหนดรายการยืนยันชื่อบัญชีรหัสผ่านด้วย LDAP และ Active Directory และ Local Guest User ได้

4.16.4 มีส่วนแสดงรายการข้อมูลชื่อบัญชี ไอพีแอดเดรสทั้ง IPv4 และ IPv6 และวันเวลาที่เข้าใช้

4.16.5 สร้างบัญชีผู้ใช้เครือข่ายชั่วคราว (Guest User Account) เป็นรายบุคคล โดยไม่จำกัดจำนวน

4.16.6 กำหนดกลุ่มบัญชีผู้ใช้ชั่วคราว เพื่อออกบัญชีชั่วคราวหลายคนแบบอัตโนมัติ

4.16.7 ออกรายงานชื่อบัญชีและรหัสผ่านผู้ใช้ชั่วคราวได้

4.16.8 กำหนดวันสิ้นสุดสิทธิ์ใช้งานของผู้ใช้ชั่วคราวทั้งแบบรายบุคคลและรายกลุ่มได้

4.17 มีฟังก์ชันบริหารจัดการโควต้าเครือข่าย ดังนี้

4.17.1 การตั้งนโยบายการใช้โควตาแบบรายกลุ่มและรายบุคคล

4.17.2 การเพิ่ม ลด และแก้ไขรายละเอียดโควตาแบบรายกลุ่มและรายบุคคล

4.17.3 การกำหนดอัตราการใช้ช่องสัญญาณสูงสุดรายกลุ่มต่อช่วงเวลา

4.17.4 การกำหนดเพดานการใช้ช่องสัญญาณเมื่อใช้เกินโควตา

4.17.5 การกำหนดอัตราการใช้ช่องสัญญาณรายบุคคลแบบสิทธิ์เฉพาะ พร้อมวันสิ้นสุดสิทธิ์เฉพาะ

4.18 มีระบบรายงานการใช้โควต้าดังนี้

4.18.1 รายงานการใช้ช่องสัญญาณตามชื่อบัญชีรายบุคคล โดยรวมปริมาณการใช้ประจำวันจากทุกเครื่องของผู้ใช้งาน

4.18.2 รายงานการใช้ช่องสัญญาณประกอบด้วยข้อมูล IPv4 และ IPv6 ทั้งขาเข้าและขาออก รวมทั้งรายละเอียดการใช้โดยแยกเป็นปริมาณการใช้รวมทั้งขาเข้าและขาออก ปริมาณการใช้รวมขาเข้า และปริมาณการใช้รวมขาออก เป็นอย่างน้อย

4.18.3 การเรียงลำดับผู้ใช้ตามปริมาณการใช้งานรวมทั้งแบบน้อยไปมาก และมากไปน้อยได้

4.18.4 รายงานในรูปกราฟแสดงปริมาณการใช้ช่องสัญญาณทั้งขาเข้าและขาออก

4.18.5 จำนวนผู้ใช้รวมรายวัน

4.18.6 การสืบค้นผลโดยเลือกวันเวลาได้

4.19 มีฟังก์ชันบริหารจัดการ Captive Portal โดยสามารถปรับตั้งค่าได้ ดังนี้

4.19.1 การสร้างหน้าจอล็อกอินที่สามารถปรับตั้ง ชื่อหน่วยงาน, โลโก้หน่วยงาน และ พื้นหลัง (background) ของหน้าเว็บ

4.19.2 การสร้างหน้าจอ Keep Alive

4.19.3 การสร้างหน้าจอรายงานข้อมูลพื้นฐาน

4.19.4 การสร้างหน้าจอ Logout

4.19.5 การกำหนดคุณสมบัติการ Login โดยให้มีระบบ Captcha และการอนุญาตให้ Login อัตโนมัติได้เป็นอย่างน้อย

4.20 มีฟังก์ชันรายงาน Session การยืนยันตัวตนของผู้ใช้รายบุคคลดังนี้

4.20.1 ชื่อบัญชีผู้ใช้งาน

4.20.2 ชื่อโดเมนที่ผู้ใช้สังกัด

4.20.3 ไอพีแอดเดรส IPv4 และ/หรือ IPv6 ที่ใช้ยืนยันตัวตน

4.20.4 MAC Address ในกรณีที่ยืนยันตัวตนผ่าน 802.1x

4.20.5 วันเวลาการยืนยันตัวตน และระยะเวลาตั้งแต่เข้าระบบ

4.20.6 ข้อมูลสรุปการใช้ช่องสัญญาณทั้งขาเข้าและขาออก ตามประเภท IPv4 และ/หรือ IPv6 โดยสามารถแสดงปริมาณข้อมูลที่ใช้และจำนวนแพคเก็ตเป็นอย่างน้อย

4.20.7 การสั่งยกเลิก Session ยืนยันตัวตนเป็นรายบุคคล

4.21 สามารถบันทึกข้อมูลจราจรเครือข่าย HTTP และ HTTPS ได้ โดยมีข้อมูลที่เก็บดังนี้

4.21.1 เวลาที่ใช้งาน

4.21.2 ชื่อบัญชีผู้ใช้งาน

4.21.3 ไอพีแอดเดรสเครื่องต้นทาง

4.21.4 ไอพีแอดเดรสเครื่องปลายทาง

4.21.5 โปรโตคอล

4.21.6 หมายเลขพอร์ตเครื่องต้นทาง

4.21.7 หมายเลขพอร์ตเครื่องปลายทาง

4.21.8 ชื่อเครื่องปลายทาง

4.21.9 Path ของ URL กรณีที่เรียกใช้ผ่าน HTTP

4.22 สามารถบันทึกข้อมูลจราจรเครือข่ายแบบ Flow ได้ โดยมีข้อมูลที่เก็บดังนี้

4.22.1 เวลาที่เริ่มใช้งาน

4.22.2 ชื่อบัญชีผู้ใช้งาน

4.22.3 ไอพีแอดเดรสเครื่องต้นทาง

4.22.4 ไอพีแอดเดรสเครื่องปลายทาง

4.22.5 โปรโตคอล

4.22.6 หมายเลขพอร์ตเครื่องต้นทาง

4.22.7 หมายเลขพอร์ตเครื่องปลายทาง

4.23 สามารถบันทึกข้อมูลการยืนยันตัวตนเข้าระบบโดยมีข้อมูลที่เก็บดังนี้

4.23.1 เวลาเข้าระบบ

4.23.2 เวลาออกจากระบบ

4.23.3 ชื่อบัญชีผู้ใช้

4.23.4 ไอพีแอดเดรสเครื่องที่เข้าระบบทั้ง IPv4 และ IPv6

4.23.5 วิธีเข้าระบบ และวิธีออกจากระบบ

4.24 มีฟังก์ชันสืบค้นข้อมูลจราจรเครือข่ายดังนี้

4.24.1 ระบุวันที่ และเวลาเริ่มต้นและสิ้นสุดของข้อมูลที่ต้องการสืบค้นได้โดยสามารถระบุช่วงเวลาเป็นหน่วยนาทีได้

4.24.2 ระบุชื่อบัญชีผู้ใช้งาน ไอพีแอดเดรสต้นทาง หรือ ไอพีแอดเดรสปลายทางได้

4.24.3 การทำสำเนาข้อมูลที่สืบค้นในรูปของไฟล์

4.25 สามารถติดตั้งในตู้แร็คมาตรฐาน 19 นิ้ว

4.26 ได้รับการรับรองตามมาตรฐาน FCC, CE, และ UL เป็นอย่างน้อย

4.27 มีการรับประกันอุปกรณ์ (Hardware warranty) เป็นระยะเวลาไม่น้อยกว่า 2 ปี

4.28 ผู้เสนอราคาต้องมีหนังสือแต่งตั้งการเป็นตัวแทนจำหน่ายจากบริษัทเจ้าของผลิตภัณฑ์

5. การรับประกันคุณภาพ

5.1 ผู้ชนะการเสนอราคาต้องรับประกันคุณภาพของอุปกรณ์บริหารจัดการระบบเครือข่าย (Authen) ที่นำเสนอในโครงการนี้ เป็นระยะเวลา 2 ปี นับจากวันตรวจรับระบบเสร็จสมบูรณ์ทั้งหมด โดยที่มหาวิทยาลัยราชภัฏพระนครศรีอยุธยาไม่ต้องรับผิดชอบค่าใช้จ่ายใด ๆ ทั้งสิ้น

5.2 ผู้ชนะการเสนอราคาต้องมีการจัดฝึกอบรมการใช้งานระบบให้กับเจ้าหน้าที่ดูแลระบบของมหาวิทยาลัย รวมถึงการแก้ไขปัญหาของระบบ จำนวน 1 วัน พร้อมทั้งมีคู่มือการใช้งานระบบ จำนวนไม่น้อยกว่า 5 เล่ม

5.3 หากระบบชำรุด บกพร่อง หรือใช้งานไม่ได้ตามที่กำหนดในสัญญา ผู้ชนะการเสนอราคาจะต้องมีการตอบสนอง (Response Time) ภายในระยะเวลา 4 ชั่วโมง หลังจากได้รับแจ้งเหตุผิดปกติจากมหาวิทยาลัยฯ พร้อมทั้งดำเนินการแก้ไขให้แล้วเสร็จสามารถใช้งานได้ปกติภายใน 8 ชั่วโมง ในกรณีที่ไม่สามารถซ่อมแซมอุปกรณ์เครือข่ายคอมพิวเตอร์ ให้ใช้งานได้เป็นปกติ ภายใน 24 ชั่วโมง หลังการรับแจ้ง บริษัทจะต้องจัดหาอุปกรณ์เครือข่ายคอมพิวเตอร์ยี่ห้อเดียวกัน ที่มีคุณลักษณะไม่ด้อยกว่าอุปกรณ์เดิมมาให้ใช้ทดแทน ทั้งนี้จะต้องมีหนังสือแจ้งการเปลี่ยนแปลงเป็นลายลักษณ์อักษร ให้ผู้ว่าจ้างพิจารณารายการที่ต้องเปลี่ยนแปลงอุปกรณ์คอมพิวเตอร์ก่อนทุกครั้ง โดยรูปแบบการให้บริการแบบ 5x8

5.4 หากผู้ชนะการเสนอราคานิ่งเฉยไม่ดำเนินการใด ๆ ที่จะแก้ไขความเสียหายของอุปกรณ์ หรือระบบที่เป็นของผู้ชนะการเสนอราคาภายหลังจาก 24 ชั่วโมง นับจากที่มหาวิทยาลัยราชภัฏพระนครศรีอยุธยาแจ้งให้ทราบผ่านทางโทรศัพท์ หรือทางโทรสาร หรือทางจดหมายอิเล็กทรอนิกส์ มหาวิทยาลัยราชภัฏพระนครศรีอยุธยา มีสิทธิ์ที่จะดำเนินการจัดหา จัดซื้อ จัดจ้าง หรือดำเนินการใด ๆ เพื่อแก้ไขให้อุปกรณ์หรือระบบที่เสียหายสามารถใช้งานได้เป็นปกติ และ มหาวิทยาลัยราชภัฏพระนครศรีอยุธยา สามารถเรียกเก็บค่าใช้จ่าย ในการดำเนินการทั้งหมดจากผู้ชนะการเสนอราคา

6. กำหนดส่งมอบพัสดุภายใน 120 วัน นับถัดจากวันที่ลงนามในสัญญา