ขอบเขตงาน
(Terms of Reference: TOR)
โครงการปรับปรุงระบบ IT

1. ความเป็นมา

ปัจจุบัน คณะสถาปัตยกรรมศาสตร์และการผังเมือง มหาวิทยาลัยธรรมศาสตร์ มีการนำเทคโนโลยีสารสนเทศมาใช้สนับสนุนการบริหารจัดการ การปฏิบัติงานของบุคลากร และการจัดการเรียนการสอน โดยมีระบบเครื่องแม่ข่าย ระบบเครือข่าย ระบบบริหารจัดการบัญชีผู้ใช้งาน ระบบจัดเก็บและแบ่งปันข้อมูล รวมถึงระบบบริการสารสนเทศต่างๆ ซึ่งเป็นโครงสร้างพื้นฐานที่สำคัญในการดำเนินงานของคณะฯ อย่างไรก็ตาม ระบบเครื่องแม่ข่ายและอุปกรณ์เทคโนโลยีสารสนเทศบางส่วนมีอายุการใช้งานยาวนาน ใช้ระบบปฏิบัติการรุ่นเก่าที่ไม่สามารถปรับปรุงด้านความมั่นคงปลอดภัยได้อย่างต่อเนื่อง และเกิดข้อขัดข้องในการให้บริการ ส่งผลให้มีความเสี่ยงต่อความปลอดภัยของข้อมูลและความต่อเนื่องในการให้บริการ

ดังนั้น คณะสถาปัตยกรรมศาสตร์และการผังเมือง จึงมีความจำเป็นต้องดำเนินโครงการปรับปรุงระบบ IT เพื่อพัฒนาและทดแทนระบบเดิมให้มีความทันสมัย เพิ่มประสิทธิภาพและความมั่นคงปลอดภัยของระบบเครื่องแม่ข่าย ระบบจัดเก็บและสำรองข้อมูล ตลอดจนปรับปรุงระบบเครือข่ายไร้สาย เพื่อรองรับการปฏิบัติงานของบุคลากรและการจัดการเรียนการสอนให้มีประสิทธิภาพและต่อเนื่องในระยะยาว

2. วัตถุประสงค์

2.1 เพื่อปรับปรุงระบบเครือข่ายคอมพิวเตอร์และระบบเซิร์ฟเวอร์ของคณะสถาปัตยกรรมศาสตร์และการผังเมือง ที่ใช้งานมาเป็นระยะเวลานาน ให้มีความเสถียรและปลอดภัยตามมาตรฐานสากล

2.2 เพื่อเพิ่มประสิทธิภาพและความมั่นคงปลอดภัยของโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศให้สามารถรองรับการปฏิบัติงานและการให้บริการของคณะสถาปัตยกรรมศาสตร์และการผังเมืองได้อย่างต่อเนื่องและมีประสิทธิภาพ

2.3 เพื่อพัฒนาและเตรียมความพร้อมของระบบเทคโนโลยีสารสนเทศให้สามารถรองรับปริมาณการใช้งานที่เพิ่มขึ้นและการขยายตัวของระบบในอนาคต สอดคล้องกับแนวทางการบริหารจัดการองค์กรอย่างมีประสิทธิภาพและยั่งยืน

2.4 เพื่อจัดหาและติดตั้งอุปกรณ์กระจายสัญญาณไร้สาย (Wireless Access Point) มาตรฐาน Wi-Fi 6E ทดแทนอุปกรณ์เดิม จำนวน 50 ชุด พร้อมระบบบริหารจัดการส่วนกลาง (Wireless Controller หรือ Centralized Management System) และเชื่อมต่อระบบยืนยันตัวตนของคณะฯ และมหาวิทยาลัยได้อย่างสมบูรณ์

3. คุณสมบัติผู้ยื่นข้อเสนอ

3.1 ผู้ยื่นข้อเสนอต้องมีความสามารถตามกฎหมาย

3.2 ผู้ยื่นข้อเสนอต้องไม่เป็นบุคคลล้มละลาย

3.3 ผู้ยื่นข้อเสนอต้องไม่อยู่ระหว่างเลิกกิจการ

3.4 ผู้ยื่นข้อเสนอต้องไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการ

ตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ผู้ยื่นข้อเสนอต้องไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 ผู้ยื่นข้อเสนอต้องมีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 ผู้ยื่นข้อเสนอต้องเป็นนิติบุคคลผู้มีอาชีพขายหรือรับจ้างงานตามที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8 ผู้ยื่นข้อเสนอไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่คณะสถาปัตยกรรมศาสตร์และการผังเมือง มหาวิทยาลัยธรรมศาสตร์ ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ผู้ยื่นข้อเสนอไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

3.10 ผู้ยื่นข้อเสนอต้องลงทะเบียนที่มีข้อมูลถูกต้องครบถ้วนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e-GP) ของกรมบัญชีกลางที่เว็บไซต์ศูนย์ข้อมูลจัดซื้อจัดจ้างภาครัฐ

3.11 ผู้ยื่นข้อเสนอต้องได้รับการแต่งตั้งเป็นตัวแทนจำหน่ายสำหรับโครงการนี้จากเจ้าของผลิตภัณฑ์หรือตัวแทนจำหน่ายที่ได้รับการแต่งตั้งโดยตรงจากเจ้าของผลิตภัณฑ์ในประเทศไทย สำหรับอุปกรณ์กระจายสัญญาณไร้สาย (Access Point) โดยต้องมีหนังสือรับรองหรือหนังสือแต่งตั้งตัวแทนจำหน่ายที่ระบุชื่อโครงการและหน่วยงานอย่างชัดเจนมาแสดงในวันยื่นข้อเสนอ

4. ข้อกำหนดรายละเอียดคุณลักษณะและขอบเขตการดำเนินงาน

ผู้รับจ้างต้องดำเนินการสำรวจระบบเดิม จัดทำแผนดำเนินงาน ติดตั้งหรือปรับปรุงระบบ จัดหาอุปกรณ์และซอฟแวร์ลิขสิทธิ์ตามรายการ ทดสอบการทำงาน ส่งมอบเอกสาร และถ่ายทอดความรู้ โดยต้องประสานงานกับผู้ดูแลระบบของคณะฯ ก่อนเปลี่ยนแปลงระบบที่ให้บริการจริง และต้องวางแผนลดผลกระทบต่อการปฏิบัติงานและการเรียนการสอน โดยมีรายละเอียดคุณลักษณะและขอบเขตงาน ดังต่อไปนี้

4.1 ผู้รับจ้างต้องจัดซื้อพร้อมติดตั้งซอฟต์แวร์ระบบปฏิบัติการแม่ข่ายสำหรับระบบ Active Directory และ DNS Server ทดแทนระบบเดิม รายละเอียดดังนี้

4.1.1 จัดหาลิขสิทธิ์ระบบปฏิบัติการ Windows Server 2025 Standard แบบถูกต้องตามกฎหมาย (Volume Licensing หรือเทียบเท่า) สำหรับติดตั้งบนเครื่องแม่ข่าย จำนวน 2 ระบบ ประกอบด้วยเครื่องแม่ข่ายหลัก (Primary Domain Controller) และเครื่องแม่ข่ายสำรอง (Secondary Domain Controller) พร้อมลิขสิทธิ์การเข้าใช้งาน Windows Server Client Access License (CAL) ประเภท User CAL จำนวนไม่น้อยกว่า 150

Licenses เพื่อรองรับผู้ใช้งานของคณะฯ โดยห้ามใช้ระบบปฏิบัติการรุ่นทดลองใช้งาน (Evaluation Edition)

4.1.2 ดำเนินการติดตั้งระบบปฏิบัติการบนเครื่องแม่ข่ายเสมือน (Virtual Machine) โดยมีทรัพยากรขั้นต่ำไม่น้อยกว่า 4 vCPU หน่วยความจำ RAM ขนาด 8 GB และพื้นที่จัดเก็บข้อมูลขนาด 150 GB พร้อมกำหนดหมายเลขไอพีแอดเดรสแบบคงที่ (Static IP Address) และตั้งค่าการซิงโครไนซ์เวลามาตรฐานกับ NTP Server ภายนอก เช่น time.nist.gov หรือ pool.ntp.org

4.1.3 ติดตั้งบทบาท Active Directory Domain Services (AD DS) และดำเนินการเลื่อนระดับเครื่องแม่ข่าย (Promote) ให้เป็น Domain Controller พร้อมกำหนดชื่อ Domain Name, NetBIOS Name, Forest Functional Level และ Domain Functional Level ตามที่คณะฯ กำหนด

4.1.4 กำหนดบทบาท Flexible Single Master Operations (FSMO Roles) ทั้ง 5 บทบาท ได้แก่ Schema Master, Domain Naming Master, PDC Emulator, RID Master และ Infrastructure Master รวมถึงกำหนด Global Catalog บนเครื่องแม่ข่าย Domain Controller ให้เหมาะสมตามหลักวิศวกรรมระบบเครือข่ายและระบบสารสนเทศ

4.1.5 กำหนดรหัสผ่าน Directory Services Restore Mode (DSRM) สำหรับใช้ในการกู้คืนระบบ และส่งมอบรหัสผ่านดังกล่าวในซองปิดผนึกให้แก่ผู้ดูแลระบบของคณะฯ

4.1.6 ติดตั้งบทบาท DNS Server และสร้าง Forward Lookup Zone ในรูปแบบ Active Directory-integrated เพื่อให้สามารถจำลองและปรับปรุงข้อมูล (Replication) ระหว่างเครื่องแม่ข่าย Domain Controller ได้โดยอัตโนมัติ

4.1.7 สร้าง Reverse Lookup Zone ตามวงจรเครือข่ายย่อย (Subnet) ที่คณะฯ กำหนด พร้อมกำหนดค่า External DNS Forwarder ไปยังผู้ให้บริการ DNS ที่คณะฯ เลือกใช้ และเปิดใช้งานฟังก์ชัน Aging และ Scavenging สำหรับบริหารจัดการและลบระเบียนข้อมูล DNS ที่หมดอายุหรือไม่ใช้งานแล้ว

4.1.8 ออกแบบและจัดทำโครงสร้าง Organizational Unit (OU) ให้สอดคล้องกับโครงสร้างองค์กรของคณะฯ โดยรองรับการแบ่งโครงสร้างตามหน่วยงานย่อย สถานที่ หรือการผสมผสานทั้งสองรูปแบบตามที่คณะฯ กำหนด

4.1.9 ดำเนินการนำเข้าบัญชีผู้ใช้งาน (User Accounts) จากไฟล์ CSV ที่คณะฯ จัดเตรียมให้ โดยต้องรองรับเขตข้อมูลอย่างน้อย ได้แก่ sAMAccountName, mail, displayName, givenName, surname, department, title, telephoneNumber, manager และ Target OU

4.1.10 ดำเนินการสร้างกลุ่มความปลอดภัย (Security Group) และกลุ่มการแจกจ่าย (Distribution Group) พร้อมกำหนดสมาชิกเริ่มต้นของแต่ละกลุ่มตามที่คณะฯ กำหนด

4.1.11 ดำเนินการสร้างบัญชีผู้ใช้สำหรับบริการ (Service Account) เพื่อรองรับการเชื่อมต่อกับระบบประยุกต์อื่นๆ เช่น Mail Server, Antivirus, ERP, ระบบจัดการการเข้าถึงเครือข่าย (IAM/IAG), Wireless Authentication หรือ LDAP-bound Applications โดยกำหนด

คุณสมบัติรหัสผ่านแบบไม่หมดอายุ (Password Never Expires) และจำกัดสิทธิ์การเข้าถึงระบบตามหลักการให้สิทธิ์เท่าที่จำเป็น (Least Privilege)

4.1.12 ดำเนินการทดสอบความสมบูรณ์และความพร้อมใช้งานของระบบ โดยใช้คำสั่ง dcdiag /v และ repadmin /replsummary รวมถึงทดสอบการแปลงชื่อโดเมน (DNS Resolution Test) การซิงโครไนซ์เวลามาตรฐาน (Time Synchronization Test) และตรวจสอบความพร้อมใช้งานของโฟลเดอร์ SYSVOL และ NETLOGON

4.1.13 เปิดใช้งานระบบตรวจจับและติดตามสถานะการให้บริการ (Service Health Monitoring / Process Monitoring) โดยทำการติดตั้งระบบ Monitoring / Incident Management และระบบจะต้องสามารถแสดง สถานะการทำงาน Monitoring/Incident Management ได้ภายใน Dashboard เดียวกันแบบเวลาจริง (Real-time)

4.2 ผู้รับจ้างต้องจัดหาพร้อมติดตั้งและกำหนดค่าระบบบริการหมายเลขไอพีอัตโนมัติ (DHCP Server) ด้วยระบบปฏิบัติการแบบเปิด (Open-Source) ทดแทนระบบเดิม จำนวน 1 ระบบ

4.2.1 การติดตั้งและปรับแต่งระบบปฏิบัติการ (OS Installation & Security Hardening)

4.2.1.1 ติดตั้งระบบปฏิบัติการ Linux ตระกูล Debian รุ่นที่ 13 (Trixie) ชนิด 64-bit Server Edition หรือรุ่นเสถียรล่าสุดที่ไม่มีค่าใช้จ่ายด้านลิขสิทธิ์ บนเครื่องแม่ข่ายเป้าหมาย

4.2.1.2 ดำเนินการปรับปรุงระบบให้เป็นปัจจุบัน โดยติดตั้งแพตช์ความปลอดภัย (Security Patches) และแพ็กเกจระบบ รวมถึงปรับแต่งเคอร์เนล (Kernel) เพื่อให้ระบบมีเสถียรภาพและความปลอดภัยสูงสุด

4.2.1.3 กำหนดค่าระบบไฟร์วอลล์ เช่น UFW หรือ nftables เพื่อปิดพอร์ตและบริการที่ไม่จำเป็น โดยเปิดเฉพาะพอร์ตที่จำเป็นต่อการให้บริการ DHCP (UDP Port 67/68) และพอร์ตสำหรับการดูแลระบบ (SSH) เท่านั้น

4.2.1.4 กำหนดวิธีการพิสูจน์ตัวตนในการเข้าดูแลระบบแม่ข่ายด้วยกุญแจเข้ารหัส (SSH Key-based Authentication) และปิดการเข้าสู่ระบบโดยตรงด้วยบัญชี Root ผ่านช่องทาง SSH

4.2.2 การติดตั้งและกำหนดค่าบริการ DHCP (DHCP Service Setup)

4.2.2.1 ติดตั้งซอฟต์แวร์ให้บริการ DHCP ตามมาตรฐานสากล เช่น Kea DHCP Server หรือ ISC DHCP Server

4.2.2.2 กำหนดค่าขอบเขตการแจกจ่ายหมายเลขไอพี (Scope / Subnet / IP Range) โดยอ้างอิงโครงสร้างเครือข่ายและ VLAN จากระบบเดิมของคณะฯ

4.2.2.3 กำหนดค่าตัวเลือกพื้นฐาน (DHCP Options) ที่จำเป็น ได้แก่ Subnet Mask, Default Gateway, Primary/Secondary DNS Servers, Domain Name และ NTP Server

4.2.2.4 กำหนดระยะเวลาการเช่าใช้หมายเลขไอพี (Lease Time) ให้เหมาะสมกับประเภทอุปกรณ์ของแต่ละเครือข่าย เช่น เครื่องคอมพิวเตอร์สำนักงาน เครือข่ายไร้สายสำหรับผู้มาติดต่อ และอุปกรณ์ IoT

4.2.2.5 กำหนดค่าการจองหมายเลขไอพีแบบคงที่ตามหมายเลข MAC Address (Static DHCP Reservation) สำหรับอุปกรณ์สำคัญ เช่น เครื่องพิมพ์เครือข่าย กล้องวงจรปิด หรือเครื่องแม่ข่าย

4.2.3 การบันทึกข้อมูลจราจรและการเชื่อมโยงระบบ (Logging, Monitoring & Integration)

4.2.3.1 จัดทำระบบบันทึกประวัติการแจกจ่ายหมายเลขไอพี (Lease History / Audit Logs) โดยต้องสามารถระบุข้อมูล MAC Address, Assigned IP, Hostname และวันเวลา (Timestamp) ได้อย่างชัดเจน

4.2.3.2 กำหนดค่าการจัดส่งข้อมูลบันทึก (Log) ไปยังระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ส่วนกลาง (Centralized Log Server / Syslog) ของคณะฯ เพื่อให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

4.2.3.3 เปิดใช้งานระบบตรวจจับและติดตามสถานะการให้บริการ (Service Health Monitoring / Process Monitoring) โดยทำการติดตั้งระบบ Monitoring / Incident Management และระบบจะต้องสามารถแสดง สถานะการทำงาน Monitoring/Incident Management ได้ภายใน Dashboard เดียวกันแบบเวลาจริง (Real-time)

4.2.4 การทดสอบระบบ (System Testing)

4.2.4.1 ทดสอบการขอรับหมายเลขไอพีอัตโนมัติจากเครื่องลูกข่ายในแต่ละ VLAN / Subnet รวมถึงทดสอบการทำงานของ DHCP Relay

4.2.4.2 ทดสอบการจองหมายเลขไอพีแบบคงที่ (Reservation Test) และทดสอบการจัดการกรณีหมายเลขไอพีเต็มหรือหมดอายุการถือครอง

4.3 ผู้รับจ้างต้องจัดซื้อพร้อมติดตั้งและอัปเกรดระบบปฏิบัติการแม่ข่ายสำหรับระบบบันทึกเวลาปฏิบัติงานและระบบจัดการลิขสิทธิ์โปรแกรมเพื่อการเรียนการสอน จำนวน 1 ระบบ

4.3.1 จัดหาลิขสิทธิ์ระบบปฏิบัติการ Windows Server 2025 Standard (Core-based License) แบบถูกต้องตามกฎหมาย จำนวน 1 ชุด โดยมีจำนวนลิขสิทธิ์สอดคล้องกับจำนวนคอร์ของเครื่องแม่ข่ายตามที่คณะฯ กำหนด เพื่อรองรับการทำงานของซอฟต์แวร์บันทึกเวลาปฏิบัติงานและซอฟต์แวร์จัดการลิขสิทธิ์โปรแกรมเพื่อการเรียนการสอนเดิม ซึ่งพัฒนาขึ้นสำหรับระบบปฏิบัติการ Windows

4.3.2 ดำเนินการติดตั้งหรืออัปเกรดระบบปฏิบัติการของเครื่องแม่ข่ายที่ให้บริการระบบบันทึกเวลาเข้า-ออกงาน และระบบบริการจัดการลิขสิทธิ์ซอฟต์แวร์เพื่อการเรียนการสอน (License Server) ให้เป็นระบบปฏิบัติการรุ่นปัจจุบัน โดยต้องสามารถรองรับข้อมูลและบริการเดิมให้ทำงานได้อย่างต่อเนื่อง

4.3.3 ดำเนินการกำหนดค่าความปลอดภัยพื้นฐาน (Security Hardening) กำหนดการเชื่อมต่อกับระบบโดเมน ตั้งค่าไฟร์วอลล์ ปรับแต่งประสิทธิภาพการทำงานของระบบ (Performance Tuning) และติดตั้งแพตช์ความปลอดภัยให้เป็นปัจจุบัน

4.3.4 เปิดใช้งานระบบตรวจจับและติดตามสถานะการให้บริการ (Service Health Monitoring / Process Monitoring) โดยทำการติดตั้งระบบ Monitoring / Incident Management

และระบบจะต้องสามารถแสดง สถานะการทำงาน Monitoring/Incident Management ได้ภายใน Dashboard เดียวกันแบบเวลาจริง (Real-time)

4.4 ผู้รับจ้างต้องจัดซื้อพร้อมติดตั้งระบบแม่ข่ายแบ่งปันไฟล์สำหรับสำนักงาน (Office Share File Server) จำนวน 1 ระบบ

4.4.1 จัดหาลิขสิทธิ์ระบบปฏิบัติการ Windows Server 2025 Standard (Core-based License) แบบถูกต้องตามกฎหมาย จำนวน 1 ชุด เพื่อรองรับการทำงานร่วมกับระบบ Active Directory ของคณะฯ

4.4.2 ดำเนินการติดตั้งและปรับแต่งระบบปฏิบัติการ พร้อมเปิดใช้งานบทบาท File and Storage Services ซึ่งรองรับโปรโตคอล SMB 3.1.1 เพื่อรองรับการเข้าใช้งานของบุคลากรภายในคณะฯ จำนวนไม่น้อยกว่า 150 ผู้ใช้งาน

4.4.3 กำหนดค่าการเชื่อมต่อระบบพิสูจน์ตัวตนเข้ากับ Active Directory Domain Services (AD DS) ของคณะฯ เพื่อให้บุคลากรสามารถใช้บัญชีผู้ใช้งานโดเมนในการเข้าถึงโฟลเดอร์และข้อมูลตามสิทธิ์ที่ได้รับ

4.4.4 จัดทำโครงสร้างโฟลเดอร์ที่ใช้ร่วมกัน (Shared Folder) โดยแบ่งแยกตามหน่วยงานหรือฝ่ายงานภายในคณะฯ รวมถึงโฟลเดอร์ส่วนกลาง พร้อมกำหนดสิทธิ์การเข้าถึงข้อมูลอย่างละเอียด (NTFS Permissions / Access Control Lists : ACLs) และเปิดใช้งานคุณสมบัติ Access-Based Enumeration (ABE) เพื่อแสดงเฉพาะโฟลเดอร์ที่ผู้ใช้งานมีสิทธิ์เข้าถึงเท่านั้น

4.4.5 ติดตั้งบทบาท File Server Resource Manager (FSRM) เพื่อกำหนดโควตาพื้นที่จัดเก็บข้อมูล (Quota Management) และกำหนดนโยบายคัดกรองไฟล์ต้องห้าม (File Screening) เช่น ไฟล์สคริปต์ที่อาจเป็นอันตราย (.exe, .bat, .vbs) หรือไฟล์ที่มีความเสี่ยงต่อไวรัสเรียกค่าไถ่ (Ransomware)

4.4.6 กำหนดนโยบายความปลอดภัยของระบบ (Security Hardening) และเปิดใช้งานระบบบันทึกประวัติการเข้าถึงและการแก้ไขไฟล์สำคัญ (Audit Logging) เพื่อรองรับการตรวจสอบย้อนหลัง

4.4.7 เปิดใช้งานบริการ Volume Shadow Copy Service (VSS) เพื่อให้สามารถกู้คืนไฟล์รุ่นก่อนหน้า (Previous Versions) ได้ รวมถึงกำหนดค่าการสำรองข้อมูลอัตโนมัติไปยังอุปกรณ์จัดเก็บข้อมูลสำรองส่วนกลาง และดำเนินการทดสอบการกู้คืนข้อมูล

4.4.8 เปิดใช้งานระบบตรวจจับและติดตามสถานะการให้บริการ (Service Health Monitoring / Process Monitoring) โดยทำการติดตั้งระบบ Monitoring / Incident Management และระบบจะต้องสามารถแสดง สถานะการทำงาน Monitoring/Incident Management ได้ภายใน Dashboard เดียวกันแบบเวลาจริง (Real-time)

4.5 ผู้รับจ้างต้องจัดซื้อพร้อมติดตั้งระบบแม่ข่ายแบ่งปันไฟล์สำหรับห้องเรียนและงานบริการไอที (Classroom & IT Service Share File Server) จำนวน 1 ระบบ

4.5.1 จัดหาลิขสิทธิ์ระบบปฏิบัติการ Windows Server 2025 Standard (Core-based License) แบบถูกต้องตามกฎหมาย จำนวน 1 ชุด

4.5.2 ดำเนินการติดตั้งและกำหนดค่าระบบปฏิบัติการ พร้อมเปิดใช้งานบทบาท File and Storage Services ซึ่งรองรับโปรโตคอล SMB 3.1.1 กำหนดค่าความปลอดภัยของระบบ (Security Hardening) และติดตั้งแพตช์ความปลอดภัยให้เป็นปัจจุบัน

4.5.3 กำหนดค่าระบบการเข้าถึงไฟล์สำหรับห้องปฏิบัติการคอมพิวเตอร์ โดยไม่ต้องผ่านการพิสูจน์ตัวตนด้วยระบบ Active Directory ส่วนกลางของบุคลากร ทั้งนี้ ให้ใช้การจัดการบัญชีผู้ใช้งานระดับเครื่องแม่ข่ายหรือกลุ่มผู้ใช้งานเฉพาะห้องเรียนตามที่คณะฯ กำหนด เพื่อให้เกิดความคล่องตัวในการจัดการเรียนการสอนและแยกส่วนการรักษาความปลอดภัยออกจากเครือข่ายสำนักงาน

4.5.4 จัดทำโครงสร้างโฟลเดอร์สำหรับการเรียนการสอน โดยแบ่งแยกตามรายวิชาหรือห้องปฏิบัติการ ประกอบด้วยโฟลเดอร์สำหรับแจกจ่ายเอกสารประกอบการสอน ซึ่งกำหนดสิทธิ์ให้อ่านได้อย่างเดียว (Read Only) และโฟลเดอร์สำหรับส่งงานของนักศึกษา (Submit / Drop-box Folder) โดยต้องกำหนดสิทธิ์เพื่อป้องกันไม่ให้นักศึกษาสามารถเปิดดู แก้ไข หรือลบไฟล์งานของนักศึกษารายอื่นได้ พร้อมจัดทำสคริปต์สำหรับลบไฟล์ชั่วคราวโดยอัตโนมัติ (Automated Cleanup Script) เมื่อสิ้นสุดภาคการศึกษาหรือตามระยะเวลาที่คณะฯ กำหนด

4.5.5 จัดทำโครงสร้างโฟลเดอร์คลังข้อมูลสำหรับงานบริการเทคโนโลยีสารสนเทศ (IT Service & Asset Repository) เพื่อใช้จัดเก็บไฟล์ติดตั้งซอฟต์แวร์ ไดรเวอร์ อิมเมจระบบปฏิบัติการ และเอกสารคู่มือทางเทคนิค โดยกำหนดสิทธิ์การแก้ไขข้อมูลให้เฉพาะเจ้าหน้าที่ผู้ดูแลระบบเทคโนโลยีสารสนเทศเท่านั้น

4.5.6 ติดตั้งบทบาท File Server Resource Manager (FSRM) เพื่อกำหนดโควตาพื้นที่จัดเก็บข้อมูล (Quota) ตามรายวิชา กำหนดนโยบายบล็อกไฟล์ต้องห้าม (File Screening) เปิดใช้งานบริการ Volume Shadow Copy Service (VSS) และกำหนดค่าระบบสำรองข้อมูลโดยอัตโนมัติ

4.5.7 เปิดใช้งานระบบตรวจจับและติดตามสถานะการให้บริการ (Service Health Monitoring / Process Monitoring) โดยทำการติดตั้งระบบ Monitoring / Incident Management และระบบจะต้องสามารถแสดง สถานะการทำงาน Monitoring/Incident Management ได้ภายใน Dashboard เดียวกันแบบเวลาจริง (Real-time)

4.6 ผู้รับจ้างต้องจัดซื้อพร้อมติดตั้งระบบสำรองข้อมูลและอุปกรณ์จัดเก็บข้อมูลบนเครือข่าย (Network Attached Storage : NAS) จำนวน 1 ระบบ

4.6.1 คุณลักษณะเฉพาะของอุปกรณ์จัดเก็บข้อมูลบนเครือข่าย (NAS) จำนวน 1 เครื่อง

4.6.1.1 เป็นอุปกรณ์จัดเก็บข้อมูลบนเครือข่ายชนิดตั้งโต๊ะ (Desktop NAS) ที่มีช่องใส่ฮาร์ดดิสก์แบบถอดเปลี่ยนได้ทันที (Hot-Swappable Bays) รองรับฮาร์ดดิสก์ขนาด 3.5 นิ้ว หรือ 2.5 นิ้ว แบบ SATA ได้ไม่น้อยกว่า 4 ช่อง (4-Bay) และมีสล็อต M.2 NVMe SSD สำหรับทำระบบแคชไม่น้อยกว่า 2 ช่อง

4.6.1.2 มีหน่วยประมวลผลกลาง (CPU) แบบ 4-Core ความเร็วพื้นฐานไม่น้อยกว่า 2.0 GHz และรองรับความเร็วสูงสุดแบบ Burst ไม่น้อยกว่า 2.7 GHz