แผนการพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ

(IT Infrastructure Development Plan)

ประจำปี 2566 - 2570

1. บทสรุป (Executive Summary)

แผนการพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศฉบับนี้ เป็นแผนกลยุทธ์ระยะ **5 ปี** ที่มีวัตถุประสงค์เพื่อยกระดับขีดความสามารถทางเทคโนโลยีของสำนักหอสมุด มหาวิทยาลัยเกษตรศาสตร์ ให้มีความทันสมัย มั่นคงปลอดภัย และสามารถสนับสนุนการให้บริการอย่างเต็มศักยภาพ

ปัจจุบัน องค์กรกำลังเผชิญความท้าทายจากระบบเดิมที่เริ่มล้าสมัย, ขาดความยืดหยุ่น และมีความเสี่ยงด้านความปลอดภัยสูง แผนนี้จึงมุ่งเน้นการปรับเปลี่ยนสถาปัตยกรรมหลัก (Core Architecture Transformation) ผ่านโครงการสำคัญ ได้แก่ **การปรับปรุงเครื่องแม่ข่ายสู่เทคโนโลยี Containerization (Docker)** เพื่อเพิ่มความเร็วและประสิทธิภาพ, **การเปลี่ยนอุปกรณ์เครือข่ายหลัก (Switches/Wi-Fi)** เพื่อรองรับปริมาณข้อมูลที่สูงขึ้น และ **การยกระดับความปลอดภัยด้วย Next-Generation Firewall ร่วมกับระบบ Endpoint Detection and Response (EDR)** เพื่อการป้องกันเชิงรุก

ด้วยงบประมาณที่ได้มาจากงบ ICT และปรับงบเงินรายได้บางส่วน แผนพัฒนานี้จะส่งผลให้องค์กรมีระบบที่คล่องตัว, มีความมั่นคงปลอดภัยสูง และพร้อมรองรับการทำงานในทุกรูปแบบ การลงทุนครั้งนี้จึงเป็นการสร้างรากฐานทางเทคโนโลยีที่แข็งแกร่งเพื่อเพิ่มขีดความสามารถในการแข่งขันขององค์กร และการให้บริการในระยะยาว

2. หลักการและเหตุผล (Principles and Rationale)

- **วิสัยทัศน์และพันธกิจขององค์กร:** เป็นศูนย์การเรียนรู้และพัฒนาที่ยั่งยืน

  แผนยุทธศาสตร์ที่ 3

  การเพิ่มประสิทธิภาพการดำเนินงานตามภารกิจและส่งเสริมให้เป็นองค์กรแห่งความสุข

  กลยุทธ์ที่ 1

  พัฒนาระบบเทคโนโลยีสารสนเทศที่สนับสนุนการดำเนินงาน

- **ความท้าทายทางเทคโนโลยี:**

  ปัจจัยภายนอก: การแข่งขัน, กฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA), เทรนด์เทคโนโลยี (AI, Cloud, Hybrid Work)

  ปัจจัยภายใน: การพัฒนาแบบรวมศูนย์, ความต้องการของพนักงาน, ปัญหาที่พบจากการทำงานในปัจจุบัน

- **วัตถุประสงค์ของแผน (Objectives):** กำหนดวัตถุประสงค์ที่ชัดเจนและวัดผลได้ (SMART Goals)

  เพื่อเพิ่มความเร็วในการ Deploy แอปพลิเคชันขึ้น 50% ด้วย Docker

  เพื่อเพิ่มความพร้อมใช้งาน (Availability) ของระบบหลักให้ได้ 99.50%

  เพื่อลดเวลาในการตรวจจับและตอบสนองต่อภัยคุกคาม (Mean Time to Respond) ลง 70%

  เพื่อสร้างระบบเครือข่ายที่รองรับการทำงานแบบ Hybrid Work ได้อย่างเต็มรูปแบบ

3. การวิเคราะห์โครงสร้างพื้นฐานปัจจุบัน (As-Is: Current State Analysis)

3.1 ระบบเครือข่าย (Network Infrastructure)

3.2 เซิร์ฟเวอร์และศูนย์ข้อมูล (Servers & Data Center)

3.3 ระบบคลาวด์ (Cloud Services)

3.4 คอมพิวเตอร์และอุปกรณ์ผู้ใช้งาน (End-User Computing)

3.5 ระบบความปลอดภัย (Security Infrastructure)

3.6 ซอฟต์แวร์และแอปพลิเคชัน (Software & Applications)

4. สถาปัตยกรรมเป้าหมายในอนาคต (To-Be: Target Architecture)

(ส่วนนี้ถูกปรับปรุงตามเทคโนโลยีใหม่ที่คุณระบุ)

- **4.1 ระบบเครือข่าย (Network Infrastructure):**

  Switches: เปลี่ยนอุปกรณ์ Core Switch และ Distribution Switch เป็นรุ่นที่รองรับความเร็ว 10GbE - 40 10GbE เพื่อลดปัญหาความเร็วของเครือข่ายและลดความเสี่ยงของอุปกรณ์เดิมที่หมดอายุการใช้งาน

  Wireless: อัปเกรดอุปกรณ์ Access Point ทั้งหมดเป็นมาตรฐาน Wi-Fi 6/6E เพื่อรองรับอุปกรณ์จำนวนมากและความเร็วสูง

- **4.2 เซิร์ฟเวอร์และศูนย์ข้อมูล (Servers & Data Center):**

  Containerization: ปรับเปลี่ยนสถาปัตยกรรมหลักจากการใช้ Virtual Machine (VM) แบบเดิม ไปสู่ **Docker Container** บนเครื่องแม่ข่ายชุดใหม่ เพื่อเพิ่มความเร็วในการพัฒนาและติดตั้ง (CI/CD), ลดการใช้ทรัพยากร และบริหารจัดการได้ง่ายขึ้น

  Legacy System: สำหรับระบบเก่าที่ไม่สามารถย้ายไป Docker ได้ จะทำการประเมินเพื่อย้ายขึ้นคลาวด์ (Cloud Migration) หรือคงไว้บน VM เท่าที่จำเป็น

- **4.3 ระบบความปลอดภัย (Security Infrastructure):**

  Perimeter Security: จัดหา **Next-Generation Firewall (NGFW)** ที่มีความสามารถในการจำแนกแอปพลิเคชัน, ป้องกันการบุกรุก (IPS) และกรองเนื้อหาเว็บ และลดความเสี่ยงจากอุปกรณ์เดิมที่หมดอายุการใช้งาน

  Endpoint Security: นำระบบ **Endpoint Detection and Response (EDR)** มาใช้กับเครื่องคอมพิวเตอร์และเซิร์ฟเวอร์ เพื่อตรวจจับ, สอบสวน และตอบสนองต่อภัยคุกคามขั้นสูงที่ไม่สามารถป้องกันได้ด้วย Antivirus ทั่วไป

  Security Posture: บังคับใช้ Multi-Factor Authentication (MFA) และใช้แนวทาง Zero Trust ในการเข้าถึงระบบสารสนเทศควบคู่กับทางสำนักบริการคอมพิวเตอร์

Physical Security (CCTV): ปรับปรุงระบบกล้องวงจรปิดเป็นแบบ IP Camera ที่มีความละเอียดสูง สามารถบริหารจัดการและเฝ้าระวังได้จากส่วนกลาง เพื่อเพิ่มความปลอดภัยทางกายภาพให้กับพื้นที่สำคัญ

- **4.4 คอมพิวเตอร์และอุปกรณ์ผู้ใช้งาน (End-User Computing):**

  กำหนดรอบการเปลี่ยนเครื่องทุก 4 ปี หรือจัดหาเครื่องในการให้บริการผู้ใช้ เพื่อควบคุมความปลอดภัย

5. แผนการดำเนินงาน (Implementation Roadmap)

(ปรับปรุงโครงการให้สอดคล้องกับสถาปัตยกรรมเป้าหมาย)

ระยะที่ 1: สร้างรากฐานความปลอดภัยและเครือข่าย (0-12 เดือน)

1. จัดหาและติดตั้ง NGFW + EDR

เปลี่ยน Firewall เดิม และติดตั้ง Agent EDR ชุดแรก

ฝ่ายเทคโนโลยีสารสนเทศ| **อยู่ระหว่างจัดซื้อ**

2. อัปเกรด Core Switch |

เปลี่ยน Core Switch เป็น 10GbE และปรับตั้งค่า VLAN

นางสาวศศินพร นาคเกษม เป็นผู้ดำเนินการ ร่วมกับทางบริษัทแลสำนักบริการคอมพิวเตอร์ **เสร็จสิ้น**

3. อัปเกรด Wi-Fi (Phase 1)

ติดตั้ง AP Wi-Fi 6 ในพื้นที่หนาแน่น

นางสาวศศินพร นาคเกษม เป็นผู้ดำเนินการ **เสร็จสิ้น**

4. จัดตั้ง Docker Host Cluster

จัดหาเครื่องแม่ข่ายและติดตั้งแพลตฟอร์ม Docker

นายอภิยศ เหรียญวิพัฒน์ เป็นผู้ดำเนินการ **เสร็จสิ้น**

5. ปรับปรุงระบบกล้องวงจรปิด (CCTV) |

จัดหาและติดตั้งระบบ CCTV ใหม่ทดแทนระบบเดิม |

นายประจักษ์ สุขอร่าม เป็นผู้ดำเนินการ **เสร็จสิ้น**

ระยะที่ 2: การปรับเปลี่ยนสู่สถาปัตยกรรมใหม่ (12-24 เดือน)

5. โครงการย้ายแอปพลิเคชันสู่ Docker |

เริ่มย้ายแอปพลิเคชัน In-house จาก VM ไปยัง Container **เสร็จสิ้น**

ทีม System/Dev ในฝ่ายเทคโนโลยีสารสนเทศ

6. อัปเกรด Wi-Fi (Phase 2)

ขยายการติดตั้ง AP Wi-Fi 6 ให้ครอบคลุม

นางสาวศศินพร นาคเกษม เป็นผู้ดำเนินการ **เสร็จสิ้น**

7. ขยายการติดตั้ง EDR ทั่วองค์กร

ติดตั้ง Agent EDR บนอุปกรณ์ที่เหลือและปรับจูน Policy

ทีม Security **ยังไม่เริ่ม**

ระยะที่ 3: การเพิ่มประสิทธิภาพและนวัตกรรม (24-36 เดือน)

8. จัดทำระบบ Centralized Log & SIEM รวบรวม Log เพื่อวิเคราะห์และตรวจจับภัยคุกคาม

Security นายอภิยศ เหรียญวิพัฒน์ ,นางสาวพนารัตน์ สร้อยศรีเมือง เป็นผู้ดำเนินงาน **เสร็จสิ้น**

9. นำ CI/CD Pipeline มาใช้

สร้าง Automation สำหรับการทดสอบและติดตั้งแอปบน Docker

นายอภิยศ เหรียญวิพัฒน์ เป็นผู้ดำเนินการ **เสร็จสิ้น**

6. ตัวชี้วัดความสำเร็จ (Success Metrics / KPIs)

6.1 ด้านการดำเนินงาน (Operational KPIs)

- **System Uptime:** ความพร้อมใช้งานของระบบบริการหลัก (เช่น ระบบห้องสมุดอัตโนมัติ, เว็บไซต์) ต้องไม่ต่ำกว่า 99.50%
- **Application Deployment Time:** ลดระยะเวลาในการติดตั้งและอัปเดตแอปพลิเคชันลง 50% หลังจากใช้ Docker อย่างเต็มรูปแบบ

- **Infrastructure-related Incidents:** จำนวนปัญหาที่เกิดจากโครงสร้างพื้นฐาน (เช่น เครือข่ายล่ม, เซิร์ฟเวอร์หยุดทำงาน) ลดลง 30%

6.2 ด้านความปลอดภัย (Security KPIs)

- **Mean Time to Respond (MTTR):** ลดระยะเวลาเฉลี่ยในการตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์ลง 70%
- **Critical Security Incidents:** จำนวนเหตุการณ์ด้านความปลอดภัยระดับวิกฤต (เช่น ข้อมูลรั่วไหล, Ransomware) ต้องเป็นศูนย์
- **MFA Adoption Rate:** อัตราการเปิดใช้งาน Multi-Factor Authentication สำหรับบุคลากรและระบบสำคัญต้องเป็น 100%
- **Vulnerability Patching Time:** ลดระยะเวลาเฉลี่ยในการอัปเดตแพตช์ความปลอดภัยสำหรับช่องโหว่ระดับวิกฤตให้เหลือไม่เกิน 7 วัน

6.3 ด้านการเงิน (Financial KPIs)

- **Cost Savings:** สามารถแสดงให้เห็นถึงการประหยัดค่าใช้จ่ายด้านการบำรุงรักษา (Maintenance) อุปกรณ์เก่าได้อย่างน้อย 15% ต่อปี

6.4 ด้านผู้ใช้งานและบริการ (User & Service KPIs)

- **User Satisfaction Score:** คะแนนความพึงพอใจของบุคลากรและผู้ใช้บริการต่อประสิทธิภาพของระบบ IT (เช่น ความเร็ว Wi-Fi, ความเสถียรของระบบ) ต้องมากกว่า 8/10 จากการสำรวจ
- **Network Performance:** ความเร็วในการใช้งานเครือข่ายไร้สาย (Wi-Fi Speed Test) ในพื้นที่ให้บริการต้องมีค่าเฉลี่ยสูงกว่า 300 Mbps

https://www.lib.ku.ac.th/api/it_plan.html