LIB-SOP-A03-2570.md



Add new file
jeerapol kumkeam authored just now

LIB-SOP-A03-2570.md 20.64 KiB

เอกสารมาตรฐานการปฏิบัติงาน (SOP) ฉบับเต็ม

รหัสเอกสาร: LIB-SOP-A03-2570
ชื่อเอกสาร: การพัฒนาและบริหารระบบดิจิทัล (Smart Digital System Development & Governance)
เวอร์ชัน: 1.0
วันที่บังคับใช้: 1 ตุลาคม 2569
วันที่ทบทวนถัดไป: 1 ตุลาคม 2570 (หรือเมื่อมีการเปลี่ยนแปลงระบบที่สำคัญ)
Process Owner: หัวหน้าฝ่ายเทคโนโลยีสารสนเทศและนวัตกรรมทางการศึกษา (นายจีระพล คุ่มเคี่ยม)
เชื่อมโยงยุทธศาสตร์: Library 5.0 • ยุทธศาสตร์ที่ 1 (Efficient Management) และที่ 3 (Smart Technology) • TQA หมวด 6.1, 6.2 • SC6 (Digital Portfolio) • SC7 (Cybersecurity & Resilience)

---

1. วัตถุประสงค์ (Outcome-Based Objective)

เพื่อพัฒนาและบริหารระบบดิจิทัลของสำนักหอสมุดกลาง (88 ระบบ ใน 6 Strategic Domains) ให้มีประสิทธิภาพ ปลอดภัย เชื่อมโยงกันเป็น **Integrated Smart Digital Ecosystem** รองรับ Library 5.0 และ TQC 2570 โดยมุ่งเน้น **User Value, System Resilience และ Cost Efficiency** มากกว่าการเพิ่มจำนวนระบบ ผ่านกระบวนการ **Digital Portfolio Review** ที่ทบทวนอย่างสม่ำเสมอ และหลัก **Sovereign Tech Stack** (Self-hosted, AI On-premise)

2. ขอบเขต (Scope)

ครอบคลุมวงจรชีวิตของระบบดิจิทัลทั้งหมด (System Lifecycle) ตั้งแต่การทบทวนพอร์ตโฟลิโอ การออกแบบและพัฒนา การทดสอบความปลอดภัย การนำขึ้นใช้งาน (Deploy) การติดตามผล และการปรับปรุง/ยกเลิก โดยแบ่งเป็น 6 Strategic Domains:

Domain	ตัวอย่างระบบ
1. Core Library & Digital Assets	Sierra, EBOOK, DigitalObject, WALAI AutoLib
2. Smart Operations & Facilities	SmartAccessControl, SmartHouseKeeper, SmartTransformer
3. AI & Smart Services	AI Jinny X, SmartTutor, Chatbot, Recommendation System
4. TQA, Strategy & UX	SmartTQA, SmartOKR, SmartVOC, Library Dashboard
5. Green & Sustainability	GreenLibNet2024, electricity_db, GLN
6. Knowledge & Workforce	SmartKM, SmartTraining, OPL Repository

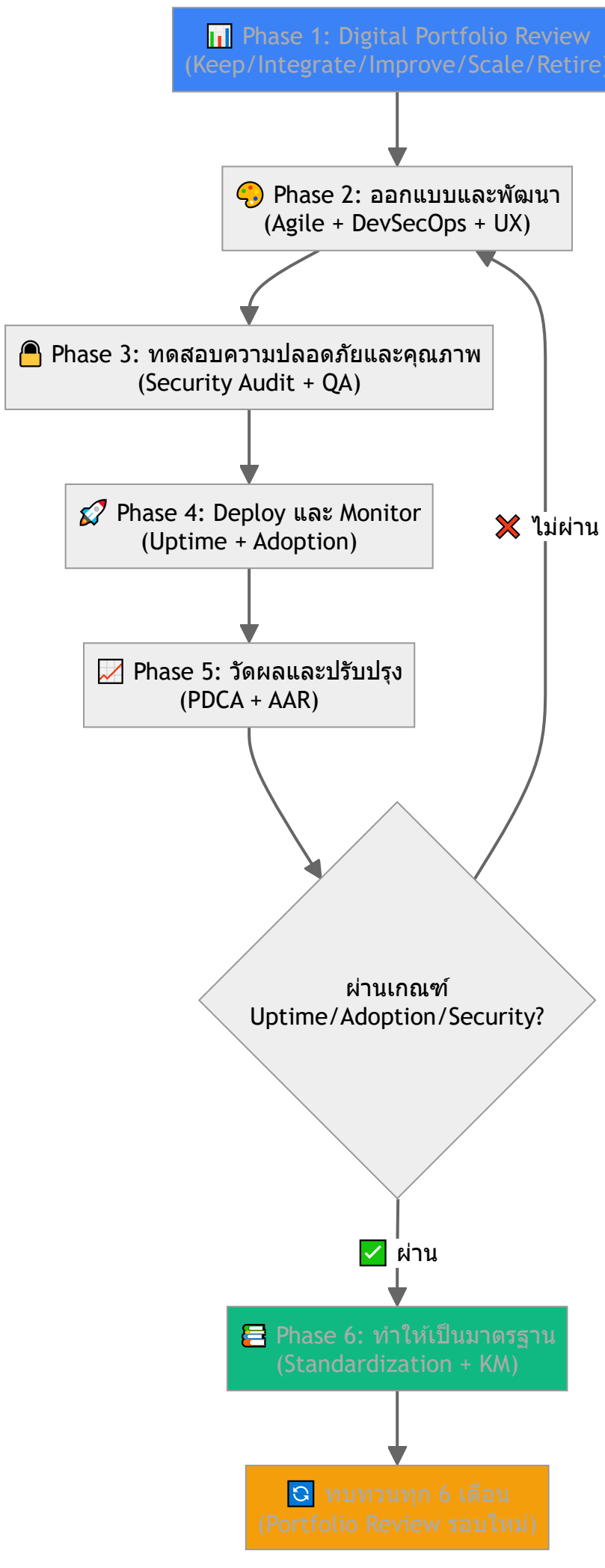
3. คำจำกัดความ (Definitions)

คำศัพท์	นิยาม
Digital Portfolio Review	การทบทวนระบบดิจิทัลอย่างสม่ำเสมอ เพื่อจัดประเภทเป็น **Keep / Integrate / Improve / Scale / Retire** ตามคุณค่า ความเสี่ยง และความคุ้มค่า
Sovereign Tech Stack	แนวทางการพัฒนาระบบที่เน้น Self-hosted และ On-premise AI (เช่น Ollama @ 192.168.5.191) เพื่อควบคุมข้อมูลและลดการพึ่งพาภายนอก
System Uptime	ร้อยละของเวลาที่ระบบพร้อมใช้งานตาม SLA (เป้าหมาย ≥99.9%)
MTTR (Mean Time to Resolve)	เวลาเฉลี่ยในการแก้ไขปัญหาตั้งแต่พบจนแก้ไขเสร็จ (เป้าหมาย ≤30 นาที สำหรับ Incident วิกฤต)
Adoption Rate	ร้อยละของกลุ่มเป้าหมายที่ใช้งานระบบจริงเทียบกับที่ตั้งเป้า
Zero Trust Security	แนวทางการรักษาความปลอดภัยที่ "ไม่เชื่อถือ任何人/ระบบใดโดยปริยาย" ต้องตรวจสอบทุกครั้ง
DevSecOps	การบูรณาการความปลอดภัย (Security) เข้าไปในทุกขั้นตอนของ DevOps

4. บทบาทและหน้าที่ (Roles & Responsibilities)

บทบาท	หน้าที่ความรับผิดชอบ
Process Owner (หน.ฝ่าย IT)	อนุมัติแผนพัฒนาระบบ ตัดสินใจบนฐาน Digital Portfolio Review ควบคุม Cybersecurity และทบทวน SOP
System Owner (แต่ละระบบ)	รับผิดชอบระบบที่ได้รับมอบหมาย รายงาน Adoption, Uptime, Incident และเสนอแผนปรับปรุง
Developer / DevOps Team	พัฒนาระบบตาม Agile + DevSecOps ดูแล CI/CD Pipeline และ Documentation
Security Officer	ดำเนินการ Cybersecurity Audit, PDPA Compliance, Penetration Test และ Incident Response
UX/UI Designer	ออกแบบประสบการณ์ผู้ใช้ ทำ Usability Test และวัด CES ของระบบ
Data Steward	ดูแล Data Quality, Data Governance และ API Integration ตามหลัก One Data One Truth

5. ขั้นตอนการดำเนินงาน (Procedure)



Phase 1: Digital Portfolio Review (ทุก 6 เดือน)

1. รวบรวมข้อมูลระบบทั้งหมดจาก **System Registry** (User Value, Adoption, Cost, Risk, Integration Status)
2. จัดประเภทแต่ละระบบตามเกณฑ์:
   - **Keep**: ระบบที่ทำงานได้ดี คงสถานะปัจจุบัน
   - **Integrate**: ระบบที่ซ้ำซ้อน ให้เชื่อมโยง/รวมกัน
   - **Improve**: ระบบที่ต้องการปรับปรุงประสิทธิภาพ/UX
   - **Scale**: ระบบที่มีศักยภาพ ขยายผลสู่ผู้ใช้มากขึ้น
   - **Retire**: ระบบที่ล้าสมัย/ใช้ต่ำ/เสี่ยงสูง วางแผนยกเลิก
3. เสนอแผนต่อคณะกรรมการ IT และกำหนด Owner ชัดเจน
4. 100% ของระบบสำคัญต้องผ่าน Review ทุก 6 เดือน

Phase 2: ออกแบบและพัฒนา (Agile + DevSecOps)

1. วิเคราะห์ความต้องการจาก **VOC, User Journey และ Pain Points**
2. ออกแบบด้วยหลัก **User-Centric Design** และ **Sovereign Tech Stack**
3. พัฒนาแบบ **Agile (Sprint 2-4 สัปดาห์)** พร้อม **CI/CD Pipeline**
4. บูรณาการ **Security by Design** ตั้งแต่ขั้นตอนออกแบบ (Threat Modeling)
5. ทำ **API Integration** ตามมาตรฐาน One Data One Truth

Phase 3: ทดสอบความปลอดภัยและคุณภาพ

1. **QA Testing**: Functional, Performance, Usability (CES ≥4.2)
2. **Security Testing**: Vulnerability Scan, Penetration Test, OWASP Top 10
3. **PDPA Compliance Check**: ตรวจสอบการเก็บ/ใช้/เปิดเผยข้อมูลส่วนบุคคล
4. **Accessibility Test**: รองรับผู้ใช้หลากหลาย (WCAG 2.1 Level AA)
5. ต้องผ่านเกณฑ์ก่อน Deploy ทุกครั้ง (Quality Gate)

Phase 4: Deploy และ Monitor

1. Deploy ผ่าน **Staging → Production** พร้อม Rollback Plan
2. ติดตาม **Real-time Monitoring** (Uptime, Response Time, Error Rate)
3. วัด **Adoption Rate** เทียบกับเป้าหมาย
4. มี **Incident Response Plan** (MTTR ≤30 นาที สำหรับ Incident วิกฤต)
5. ทำ **Backup & Disaster Recovery** Test ทุก 6 เดือน

Phase 5: วัดผลและปรับปรุง (PDCA + AAR)

1. วัดผล KPI ทุกเดือน (Uptime, Adoption, Security Incident, User Satisfaction)
2. ทำ **AAR (After Action Review)** หลังทุกโครงการ/Incident สำคัญ
3. นำผลการวัดไปปรับปรุงในรอบถัดไป (Learning Loop)
4. อัปเดต **Risk Register** และ **Improvement Portfolio**

Phase 6: ทำให้เป็นมาตรฐาน (Standardization + KM)

1. จัดทำ **OPL (One Point Lesson)** และ **Technical Documentation**
2. แชร์ความรู้ผ่าน **Knowledge Sharing Day** และ **SmartKM**
3. อัปเดต **KPI Dictionary** และ **System Registry**
4. นำ Best Practice ไปใช้กับระบบอื่น (Scale)

6. ตัวชี้วัดกระบวนการ (Process KPIs) - LeTCI Framework

KPI Name	นิยาม (Definition)	สูตรคำนวณ (Formula)	ค่าเป้าหมาย (Target)	แหล่งข้อมูล (Data Source)	ความถี่
System Uptime	ร้อยละของเวลาที่ระบบสำคัญพร้อมใช้งาน	(เวลาพร้อมใช้ / เวลาทั้งหมด) × 100	**≥99.9%**	Monitoring Dashboard	รายเดือน
Security Breach	จำนวนเหตุการณ์ด้านความปลอดภัยที่ส่งผลต่อข้อมูล/ระบบ	นับจำนวน Incident	**0 ครั้ง**	Security Log / Incident Log	รายปี
Adoption Rate	ร้อยละของกลุ่มเป้าหมายที่ใช้งานระบบจริง	(จำนวนผู้ใช้จริง / กลุ่มเป้าหมาย) × 100	**≥70%**	System Log	รายไตรมาส
MTTR (Critical Incident)	เวลาเฉลี่ยในการแก้ไขปัญหาวิกฤต	ผลรวมเวลาแก้ไข / จำนวน Incident	**≤30 นาที**	Incident Log	รายเดือน
Digital Portfolio Review	ร้อยละของระบบสำคัญที่ผ่าน Portfolio Review	(ระบบที่ผ่าน Review / ระบบสำคัญทั้งหมด) × 100	**100%**	Review Report	ทุก 6 เดือน

KPI Name	นิยาม (Definition)	สูตรคำนวณ (Formula)	ค่าเป้าหมาย (Target)	แหล่งข้อมูล (Data Source)	ความถี่
Integration Rate	ร้อยละของระบบสำคัญที่เชื่อมโยง API/Data กับระบบอื่น	(ระบบที่ Integrate / ระบบสำคัญ) × 100	**≥80%**	System Registry	รายปี
User Satisfaction (System)	ความพึงพอใจต่อระบบดิจิทัล	ค่าเฉลี่ยคะแนน (1-5)	**≥4.50**	UX Survey	ราย 6 เดือน

7. การบริหารความเสี่ยง (Risk Management)

ความเสี่ยง (Risk)	ผลกระทบ (Impact)	มาตรการควบคุม (Control Measure)
ระบบล้าสมัย/ซ้ำซ้อน (SC6, WT2)	สูญเสียงบประมาณ ผู้ใช้สับสน	**บังคับทำ Digital Portfolio Review** ทุก 6 เดือน พร้อมแผน Retire ที่ชัดเจน
Cybersecurity Breach (SC7, T1)	ข้อมูลรั่วไหล ระบบหยุดทำงาน เสียชื่อเสียง	**DevSecOps + Zero Trust + PDPA Compliance** + Pen Test รายปี + Incident Response Plan
ระบบพึ่งพา Vendor/Cloud ภายนอก	ถูก Lock-in ขาดความต่อเนื่อง	**Sovereign Tech Stack** (Self-hosted, Ollama On-premise) + Multi-source Strategy
พัฒนาระบบโดยไม่ฟังเสียงผู้ใช้	ระบบไม่ถูกใช้ Adoption ต่ำ	**บังคับทำ UX Research + Usability Test** ก่อน Deploy + วัด CES ทุกไตรมาส
บุคลากรมี Skill ไม่ทันเทคโนโลยี (SC5, T4)	พัฒนาระบบช้า มี Bug มาก	**Capability Matrix + IDP** + Training ≥20 ชม./คน/ปี + KM Sharing
ข้อมูลไม่เชื่อมโยง (Silo) (W1, SC2)	รายงานซ้ำซ้อน ตัดสินใจผิดพลาด	**One Data One Truth + API Standard + Data Governance**

8. เอกสารและบันทึกที่เกี่ยวข้อง (Documents & Records)

รหัสเอกสาร	ชื่อเอกสาร	หน้าที่จัดเก็บ	ระยะเวลาจัดเก็บ
LIB-FM-DPR-001	แบบฟอร์ม Digital Portfolio Review	ฝ่าย IT	5 ปี
LIB-FM-SEC-001	แบบฟอร์ม Security Audit & Pen Test Report	ฝ่าย IT	5 ปี
LIB-FM-INC-001	Incident Log & Response Report	ฝ่าย IT	3 ปี
LIB-FM-UX-001	แบบฟอร์ม Usability Test & CES Survey	ฝ่าย IT + ฝ่ายบริการ	3 ปี
LIB-FM-REG-001	System Registry & API Documentation	ฝ่าย IT	ตลอดอายุระบบ + 3 ปี
LIB-RPT-IT-001	รายงาน Monitoring Dashboard รายเดือน	ฝ่าย IT	5 ปี

9. ประวัติการแก้ไข (Revision History)

เวอร์ชัน	วันที่	รายละเอียดการแก้ไข	ผู้จัดทำ	ผู้อนุมัติ
1.0	01/10/2569	จัดทำฉบับแรก เพื่อรองรับ Library 5.0, Digital Portfolio และ TQC 2570	คณะทำงานยุทธศาสตร์	รศ.ดร.พยุง มีสัจ

💡 คำแนะนำสำหรับ Process Owner (นายจีระพล) ในการนำ SOP นี้ไปใช้จริง:

1. **Digital Portfolio Review คือหัวใจ:** ไม่ใช่แค่ "มีระบบอะไรบ้าง" แต่ต้องตอบให้ได้ว่า **"ระบบไหนควรอยู่ ระบบไหนควรไป"** ทุก 6 เดือน ต้องมีระบบที่ถูก Retire หรือ Integrate อย่างน้อย 5-10% เพื่อลด Technical Debt
2. **Security ไม่ใช่ Phase แต่เป็น Culture:** ฝัง **DevSecOps** เข้าไปใน DNA ของทีม Developer ทุก Commit ต้องผ่าน Security Scan อัตโนมัติ และทำ **Threat Modeling** ก่อนเริ่มโปรเจกต์ใหม่
3. **Sovereign Tech Stack คือความได้เปรียบ:** การใช้ Ollama On-premise และ Self-hosted Services ไม่ใช่แค่เรื่องเทคนิค แต่เป็น **Strategic Resilience** ที่ทำให้เราควบคุมข้อมูล ลดค่าใช้จ่ายระยะยาว และรองรับ AI ได้โดยไม่พึ่ง Vendor
4. **Adoption สำคัญกว่า Feature:** ระบบที่ดีไม่ใช่ระบบที่มี Feature เยอะ แต่คือระบบที่ **ผู้ใช้ใช้งานจริง** วัด Adoption Rate ทุกไตรมาส และถ้าต่ำกว่า 70% ต้องกลับไปดู UX หรือ Communication
5. **เชื่อมโยงกับ TQC 2570:** ทุกระบบต้องมี **Owner, KPI, SLA และ Evidence** ที่ตรวจสอบย้อนหลังได้ เพื่อรองรับการประเมิน TQA หมวด 6.1 และ 6.2

🎯 การเชื่อมโยงกับเกณฑ์ TQA และห้องสมุดดีเด่น (Evidence Packaging)

- **TQA หมวด 6.1 (การออกแบบกระบวนการ):** SOP นี้แสดงถึง Digital Portfolio Review, System Owner, และ DevSecOps ที่ชัดเจน
- **TQA หมวด 6.2 (การปฏิบัติการ):** KPI เรื่อง Uptime, MTTR และ Security Breach คือหลักฐานเชิงประจักษ์
- **TQA หมวด 7.2 (ผลลัพธ์ด้านปฏิบัติการ):** Adoption Rate และ Integration Rate สะท้อนประสิทธิภาพ
- **ห้องสมุดดีเด่น (ตัวชี้วัด 3.1):** ระบบ AI Jinny X, Smart Room, Smart Payment, Library Dashboard ล้วนพัฒนาจาก SOP นี้
- **SC6 & SC7 (Strategic Challenges):** SOP นี้ตอบโจทย์โดยตรงเรื่อง Digital Portfolio และ Cybersecurity

---

🔗 การเชื่อมโยงกับ SOP อื่น

SOP ที่เชื่อมโยง	ลักษณะการเชื่อมโยง
SOP-A01 (Service Design)	ระบบดิจิทัลที่พัฒนาต้องรองรับ Customer Journey ที่ออกแบบใน A01
SOP-A02 (Resource Management)	ระบบ Sierra, EBOOK, DigitalObject อยู่ภายใต้ Domain 1 ของ SOP นี้
SOP-A04 (Facilities)	ระบบ SmartAccessControl, SmartTransformer อยู่ภายใต้ Domain 2
SOP-B01 (One Data)	API และ Data Standard ต้องสอดคล้องกับ KPI Dictionary ของ B01
SOP-B03 (Risk Management)	Cybersecurity Risk ใน SOP นี้ต้องถูกนำเข้าสู่ Risk Register กลางของ B03

หากท่านต้องการให้ผมจัดทำ **แบบฟอร์ม Digital Portfolio Review Template**, **Incident Response Plan Template** หรือ **SOP ฉบับถัดไป (A04-A07)** แจ้งได้เลยครับ!