	คู่มือการปฏิบัติงาน	วันที่เริ่มใช้ 1 ต.ค. 69
	หน่วยงาน : สำนักยุทธศาสตร์และแผน	รวม 21 กระบวนงาน
	กลุ่มงาน : 6. ศูนย์ข้อมูลและสารสนเทศ	รวม 7 กระบวนงาน
	กระบวนงาน : การพัฒนาระบบสารสนเทศ	ลำดับที่ 6.3/21

1. วัตถุประสงค์

1.1 เพื่อกำหนดแนวทางและขั้นตอนการปฏิบัติงานด้านการพัฒนาและบริหารจัดการระบบเทคโนโลยีสารสนเทศของศูนย์ข้อมูลและสารสนเทศให้เป็นมาตรฐานเดียวกัน

1.2 เพื่อให้การดำเนินงานด้านการพัฒนาระบบ การปรับปรุงระบบ การบริหารจัดการเว็บไซต์ และการบริหารจัดการฐานข้อมูล เป็นไปอย่างเป็นระบบ มีประสิทธิภาพ และสามารถตรวจสอบได้

1.3 เพื่อกำหนดบทบาทหน้าที่ของบุคลากรที่เกี่ยวข้องในการดำเนินงานด้านเทคโนโลยีสารสนเทศอย่างชัดเจน

1.4 เพื่อใช้เป็นแนวทางในการปฏิบัติงานสำหรับเจ้าหน้าที่ผู้ปฏิบัติงาน และเป็นเอกสารอ้างอิงสำหรับการถ่ายทอดองค์ความรู้ให้แก่เจ้าหน้าที่ใหม่

1.5 เพื่อสนับสนุนการบริหารจัดการระบบสารสนเทศของหน่วยงานให้มีความต่อเนื่อง มีความมั่นคงปลอดภัย และตอบสนองต่อภารกิจของหน่วยงาน

2. ขอบเขต

คู่มือการปฏิบัติงานฉบับนี้ครอบคลุมกระบวนการดำเนินงานของศูนย์ข้อมูลและสารสนเทศ ในส่วนของกลุ่มงานพัฒนาระบบเทคโนโลยีสารสนเทศ ซึ่งประกอบด้วยกระบวนงานหลัก ดังนี้

- การพัฒนาระบบสารสนเทศใหม่ของหน่วยงาน
- การปรับปรุงและแก้ไขระบบสารสนเทศที่มีอยู่เดิม
- การบริหารจัดการเว็บไซต์ของหน่วยงาน
- การบริหารจัดการฐานข้อมูลของระบบสารสนเทศ

โดยครอบคลุมตั้งแต่ขั้นตอนการรับเรื่อง การวิเคราะห์ความต้องการ การดำเนินการพัฒนา การทดสอบระบบ การนำระบบไปใช้งาน ตลอดจนการติดตามผลการดำเนินงาน

3. คำจำกัดความ

- **ระบบสารสนเทศ (Information System)**
  ระบบที่ประกอบด้วยซอฟต์แวร์ ฮาร์ดแวร์ ข้อมูล และกระบวนการทำงาน เพื่อสนับสนุนการดำเนินงานของหน่วยงาน
- **การพัฒนาระบบ (System Development)**
  กระบวนการออกแบบ สร้าง และพัฒนาระบบสารสนเทศใหม่ เพื่อสนับสนุนการดำเนินงานของหน่วยงาน
- **การปรับปรุงระบบ (System Enhancement / Maintenance)**
  การแก้ไข ปรับปรุง หรือเพิ่มเติมฟังก์ชันการทำงานของระบบสารสนเทศเดิมให้สามารถใช้งานได้อย่างมีประสิทธิภาพ
- **เว็บไซต์ของหน่วยงาน (Website Management)**
  ระบบเว็บไซต์ที่ใช้เผยแพร่ข้อมูล ข่าวสาร และบริการของหน่วยงานผ่านเครือข่ายอินเทอร์เน็ต
- **การบริหารจัดการฐานข้อมูล (Database Management)**
  กระบวนการดูแล บำรุงรักษา สำรองข้อมูล ปรับปรุงโครงสร้าง และบริหารจัดการข้อมูลของระบบสารสนเทศ
- **MA (Maintenance Agreement)**
  สัญญาการบำรุงรักษาระบบสารสนเทศกับผู้รับจ้างหรือผู้พัฒนาระบบ

4. หน้าที่ความรับผิดชอบ

4.1 ผู้ใช้งานระบบ (User)

- แจ้งปัญหาหรือความต้องการใช้งานระบบ
- ให้ข้อมูลรายละเอียดเกี่ยวกับปัญหาหรือความต้องการของระบบ
- ทดสอบการใช้งานระบบหลังจากมีการพัฒนา หรือปรับปรุง

4.2 นักวิชาการคอมพิวเตอร์ / ผู้พัฒนาระบบ (Developer)

- วิเคราะห์ความต้องการของระบบ
- ออกแบบ พัฒนา และปรับปรุงระบบสารสนเทศ
- ตรวจสอบและทดสอบระบบก่อนนำไปใช้งานจริง
- ดูแลและบริหารจัดการฐานข้อมูลของระบบ
- บริหารจัดการเว็บไซต์ของหน่วยงาน

4.3 หัวหน้าหน่วยงาน / ผู้บังคับบัญชา

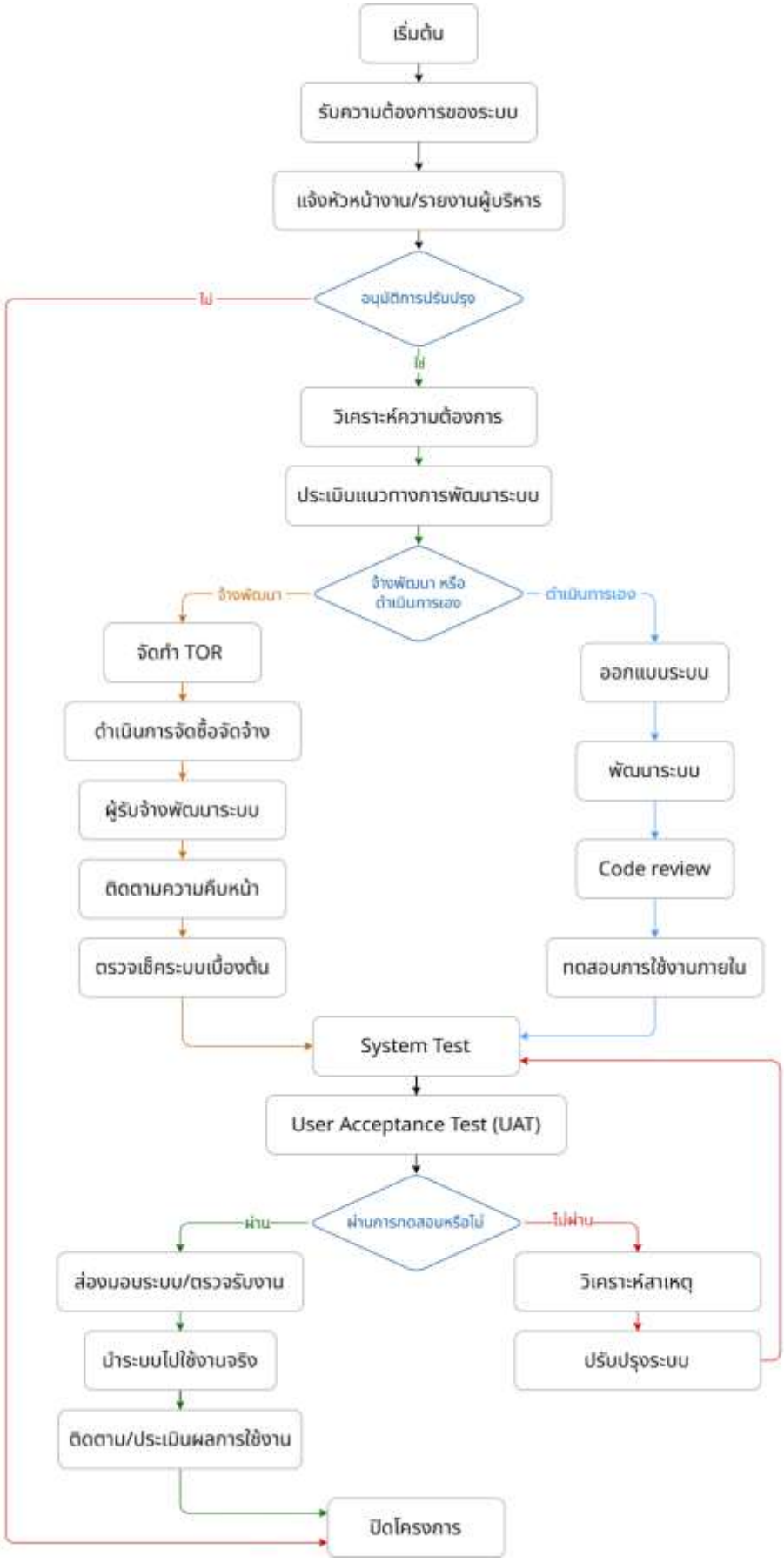
- พิจารณาอนุมัติแนวทางการดำเนินงาน
- กำกับดูแลและติดตามการดำเนินงานของเจ้าหน้าที่
- พิจารณาแนวทางแก้ไขปัญหาในกรณีที่เกิดข้อจำกัดในการดำเนินงาน

4.4 ผู้รับจ้างพัฒนาระบบ (กรณีมีสัญญาจ้าง)

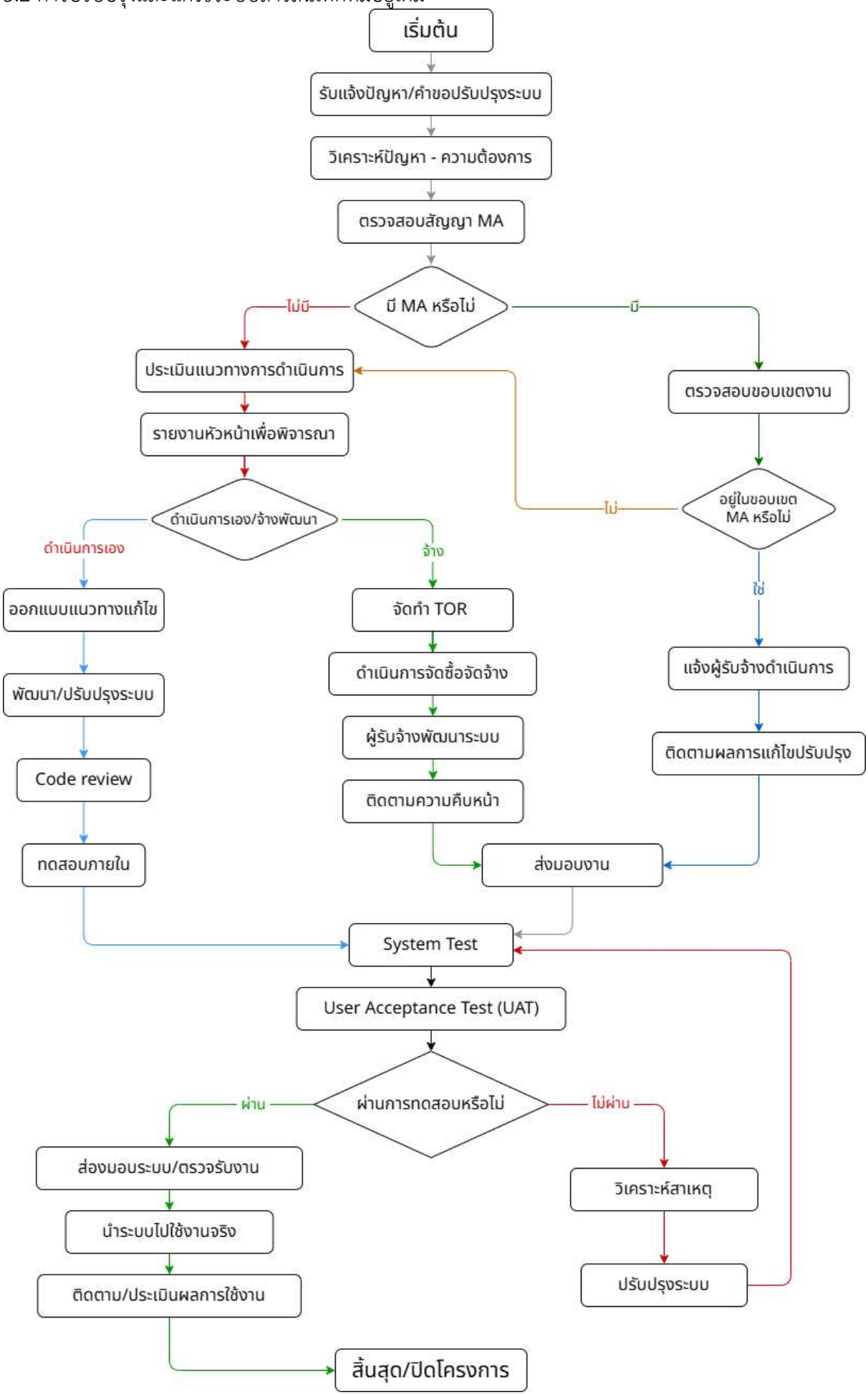
- ดำเนินการพัฒนาหรือปรับปรุงระบบตามขอบเขตของสัญญา
- แก้ไขข้อผิดพลาดของระบบภายใต้สัญญาบำรุงรักษา (MA)
- สนับสนุนการดำเนินงานด้านเทคนิคตามที่หน่วยงานร้องขอ

5. แผนผังการปฏิบัติงาน (Work Flow)

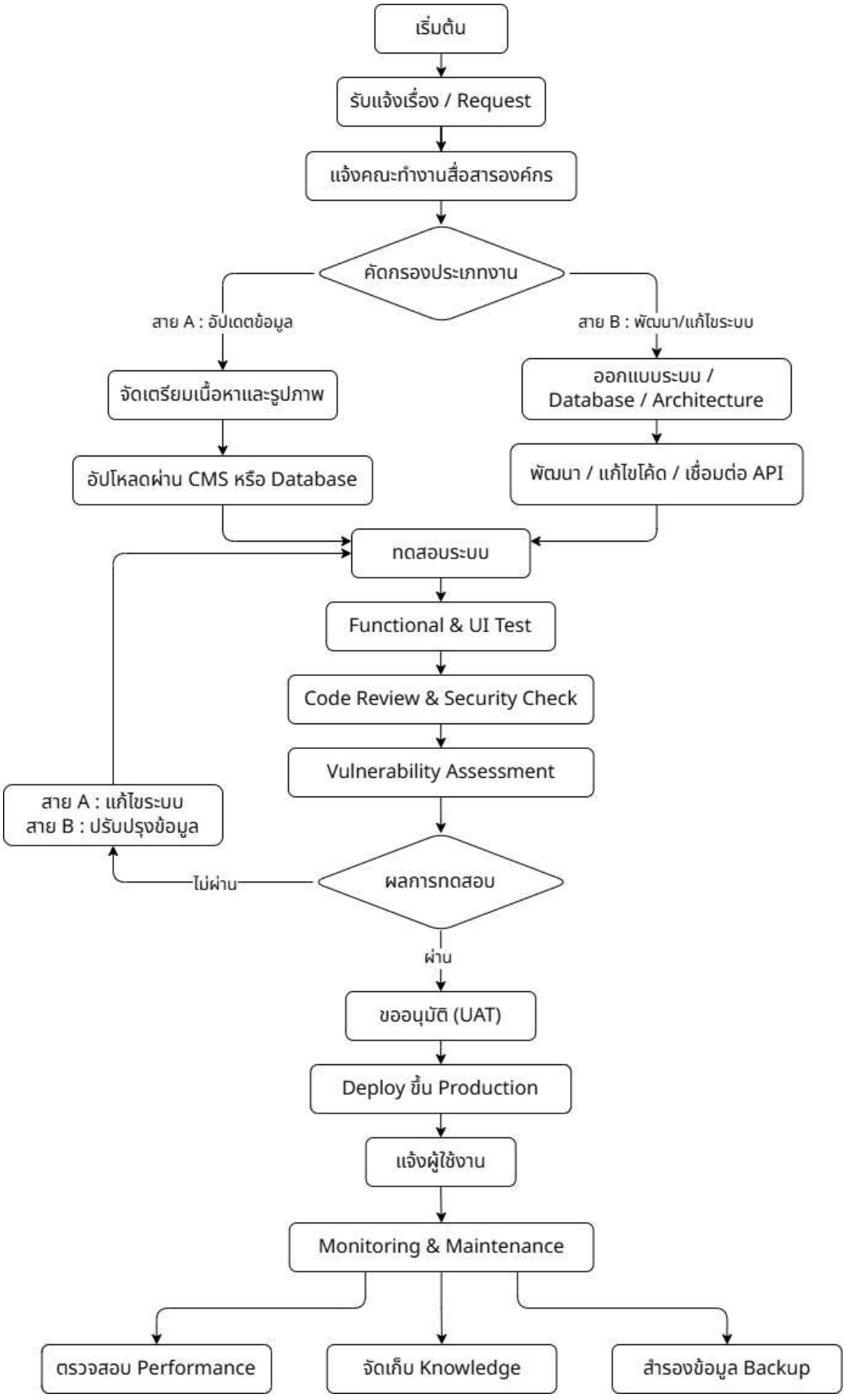
5.1 การพัฒนาระบบสารสนเทศใหม่ของหน่วยงาน



5.2 การปรับปรุงและแก้ไขระบบสารสนเทศที่มีอยู่เดิม



5.3 การบริหารจัดการเว็บไซต์ของหน่วยงาน



5.4 การบริหารจัดการฐานข้อมูลของระบบสารสนเทศ

6. ขั้นตอนการปฏิบัติงาน

6.1 กระบวนการพัฒนาระบบใหม่

14 ขั้นตอน · ตั้งแต่รับความต้องการจนถึงปิดโครงการ

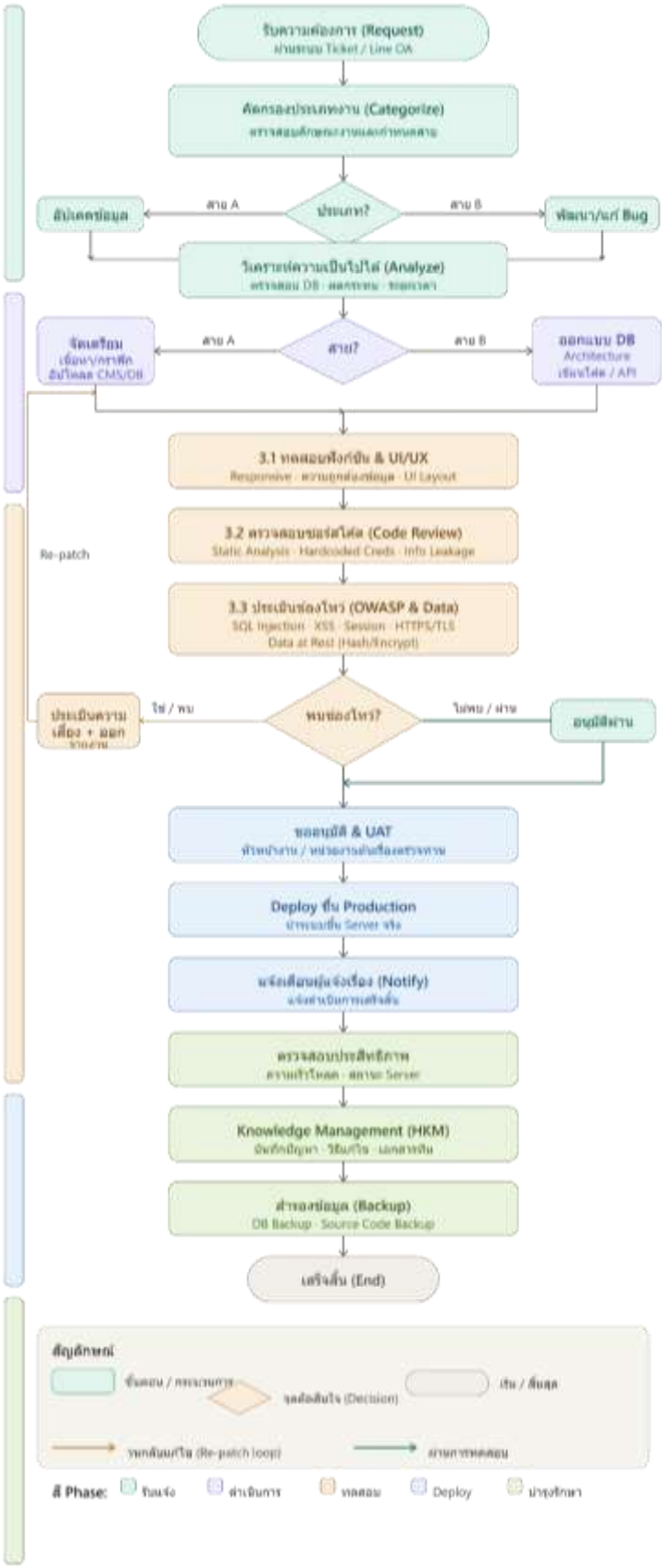
ลำดับ	ขั้นตอน	รายละเอียด
1	รับความต้องการระบบ	รับความต้องการจากหน่วยงานผู้ใช้งาน ทั้งการแจ้งความต้องการ การประชุมหารือ หรือเอกสารเสนอ เพื่อใช้เป็นข้อมูลเบื้องต้น
2	วิเคราะห์ความต้องการ	วิเคราะห์รายละเอียด (Requirement Analysis) ศึกษากระบวนการทำงาน ปัญหา และวัตถุประสงค์ เพื่อกำหนดขอบเขตและแนวทางพัฒนา
3	จัดทำ Requirement Document	จัดทำเอกสารความต้องการระบบ ประกอบด้วยฟังก์ชันการทำงาน ขอบเขต โครงสร้างข้อมูล และข้อกำหนดอื่น ๆ เพื่อใช้เป็นเอกสารอ้างอิง
4	ประเมินแนวทางการพัฒนา	พิจารณาความเหมาะสม ระหว่างพัฒนาเองหรือจ้างผู้พัฒนาภายนอก โดยพิจารณาจากความซับซ้อน ระยะเวลา งบประมาณ และทรัพยากร
5	รายงานหัวหน้าหน่วยงาน	เสนอผลวิเคราะห์และแนวทางพัฒนาต่อหัวหน้าหน่วยงานเพื่อพิจารณาให้ความเห็นชอบ
เลือกแนวทางดำเนินการ: จ้างพัฒนา (ข้อ 6) พัฒนาเอง (ข้อ 7)		
6	กรณีจ้างพัฒนาระบบจ้างภายนอก	6.1จัดทำเอกสารขอบเขตงาน (TOR) 6.2ดำเนินการจัดซื้อจัดจ้างตามระเบียบ 6.3ผู้รับจ้างดำเนินการพัฒนาตาม TOR 6.4ติดตามความคืบหน้าการดำเนินงาน 6.5ตรวจรับงานตามเงื่อนไขสัญญา
7	กรณีพัฒนาเองทีมงานภายใน	7.1ออกแบบระบบ (System Design) - โครงสร้าง ฐานข้อมูลหน้าจอ 7.2พัฒนาโปรแกรมตามแบบที่ออกแบบ 7.3ตรวจสอบคุณภาพโค้ด (Code Review) 7.4ทดสอบระบบภายใน (Internal Test)
8	ทดสอบระบบ (System Test)	ทดสอบระบบเพื่อตรวจสอบความถูกต้องของการทำงานให้เป็นไปตาม Requirement Document
9	ทดสอบการยอมรับ (UAT)	ให้ผู้ใช้งานทดสอบระบบ เพื่อยืนยันว่าระบบตอบสนองต่อความต้องการและสามารถใช้งานได้จริงตามวัตถุประสงค์
ผลการทดสอบ: ผ่าน ☐ ดำเนินการต่อ ไม่ผ่าน ☐ ข้อ 10		
10	กรณีทดสอบไม่ผ่าน	วิเคราะห์สาเหตุปัญหา ปรับปรุงแก้ไขระบบ และทำการทดสอบใหม่จนกว่าจะผ่าน จากนั้นกลับไปขั้นตอนที่ 8
11	ส่งมอบระบบ	ส่งมอบระบบให้หน่วยงานผู้ใช้งาน พร้อมจัดทำเอกสารประกอบการใช้งาน (ถ้ามี)
12	นำระบบไปใช้งานจริง	ติดตั้งและนำระบบขึ้น Production Environment
13	ติดตามผลการใช้งาน	ติดตามผลหลังนำระบบไปใช้งานจริง เพื่อรับข้อเสนอแนะหรือแก้ไขปัญหาที่อาจเกิดขึ้น
14	ปิดโครงการ	เมื่อระบบใช้งานได้ตามวัตถุประสงค์และไม่มีประเด็นคงค้าง สรุปผลการดำเนินงานและปิดโครงการ

6.2 กระบวนการปรับปรุงและแก้ไขระบบงานเดิม

6 ขั้นตอนหลัก · ตั้งแต่รับแจ้งปัญหาจนถึงส่งมอบงาน

ลำดับ	ขั้นตอน	รายละเอียด
1	รับแจ้งปัญหาหรือคำขอปรับปรุง	รับแจ้งจากผู้ใช้งานหรือหน่วยงานที่เกี่ยวข้อง ผ่านระบบรับแจ้ง หนังสือราชการ หรือช่องทางการสื่อสารของหน่วยงาน
2	วิเคราะห์ปัญหาและความต้องการ	วิเคราะห์สาเหตุปัญหา ผลกระทบที่เกิดขึ้น และขอบเขตของการปรับปรุงระบบ
3	ตรวจสอบสัญญา MA	ตรวจสอบเงื่อนไขสัญญาการบำรุงรักษาระบบ (Maintenance Agreement) ว่าปัญหาหรือการปรับปรุงที่แจ้งอยู่ในขอบเขตสัญญาหรือไม่
ผลตรวจสอบสัญญา: อยู่ในสัญญา MA (ข้อ 4) ไม่อยู่ในสัญญา MA (ข้อ 5)		
4	กรณีระบบอยู่ในสัญญา MA มีสัญญา MA	4.1แจ้งผู้รับจ้างตามสัญญาให้ดำเนินการแก้ไขหรือปรับปรุง 4.2ติดตามความคืบหน้าการดำเนินงาน 4.3ผู้รับจ้างแก้ไข/ปรับปรุง และส่งมอบงานให้หน่วยงาน
5	กรณีระบบไม่อยู่ในสัญญา MA ไม่มีสัญญา MA	5.1ประเมินแนวทางการดำเนินการแก้ไข/ปรับปรุง 5.2รายงานหัวหน้าหน่วยงานเพื่อพิจารณาแนวทาง 5.3พิจารณาวิธีดำเนินการ: แก้ไขเอง (ข้อ 6) จัดจ้างเพิ่มเติม
6	กรณีแก้ไขระบบเอง ทีมงานภายใน	6.1ออกแบบแนวทางการแก้ไข/ปรับปรุง 6.2ดำเนินการพัฒนาและปรับปรุงระบบ 6.3ตรวจสอบคุณภาพโค้ด (Code Review) 6.4ทดสอบระบบภายใน (Internal Test)
7	**กรณีจ้างผู้พัฒนาระบบ**	7.1 จัดทำเอกสารขอบเขตงาน (TOR) หรือรายละเอียดงาน 7.2 ดำเนินการจัดซื้อจัดจ้างตามระเบียบของหน่วยงาน 7.3 ผู้รับจ้างดำเนินการแก้ไขหรือปรับปรุงระบบ 7.4 ติดตามความคืบหน้าการดำเนินงานของผู้รับจ้าง 7.5 ผู้รับจ้างส่งมอบงานให้หน่วยงาน
8	**ทดสอบระบบ (System Test)**	ดำเนินการทดสอบระบบเพื่อตรวจสอบความถูกต้องของการทำงานของระบบหลังจากมีการแก้ไขหรือปรับปรุง
9	**ทดสอบการยอมรับระบบโดยผู้ใช้งาน (User Acceptance Test : UAT)**	ให้ผู้ใช้งานระบบดำเนินการทดสอบระบบ เพื่อยืนยันว่าระบบสามารถทำงานได้ถูกต้องและตรงตามความต้องการ
10	**กรณีทดสอบไม่ผ่าน**	หากผลการทดสอบพบข้อผิดพลาดหรือระบบไม่สามารถทำงานได้ตามที่กำหนด ให้ดำเนินการวิเคราะห์สาเหตุ ปรับปรุงแก้ไขระบบ และทำการทดสอบใหม่จนกว่าจะผ่านการทดสอบ
11	**ส่งมอบงานให้ผู้ใช้งาน**	เมื่อระบบผ่านการทดสอบเรียบร้อยแล้ว ให้ดำเนินการแจ้งผู้ใช้งานและส่งมอบงานที่ได้ปรับปรุงแก้ไข
12	**ติดตามผลการใช้งาน**	ติดตามผลการใช้งานระบบหลังจากดำเนินการแก้ไขหรือปรับปรุง เพื่อให้มั่นใจว่าระบบสามารถทำงานได้อย่างถูกต้อง
13	**ปิดงาน**	เมื่อการดำเนินการแก้ไขหรือปรับปรุงระบบเสร็จสิ้นและไม่มีปัญหาคงค้าง ให้ดำเนินการสรุปผลการดำเนินงานและปิดงาน

6.3 Flowchart: การบริหารจัดการเว็บไซต์ สวพส.



Flowchart ครบทั้ง 5 ระยะ โครงสร้างที่ใช้มีดังนี้

สีแต่ละ Phase

- □ เขียวน้ำทะเล = ระยะ 1 รับแจ้ง & ประเมิน
- □ ม่วง = ระยะ 2 ดำเนินการ
- □ เหลืองทอง = ระยะ 3 ทดสอบ & ความปลอดภัย
- □ น้ำเงิน = ระยะ 4 Deploy
- □ เขียว = ระยะ 5 บำรุงรักษา

จุดพิเศษใน Flow

- **Diamond สาย A / สาย B** (ระยะ 1) แยกเส้นทาง แล้ว merge กลับก่อนเข้า phase 2
- **Diamond สาย A / สาย B** (ระยะ 2) แยกขั้นตอนดำเนินการ แล้ว merge เข้าสู่การทดสอบ
- **Diamond พบช่องโหว่?** (3.4) มี **Re-patch loop** วนกลับไปแก้ไขที่ระยะ 2 โดยเส้นสีส้มด้านซ้าย และ เส้นสีเขียว "ผ่าน" ที่ด้านขวา

6.4 การบริหารจัดการฐานข้อมูลของระบบสารสนเทศ

1. เตรียมการและออกแบบ (Preparation & Design)

- รับความต้องการหรือโครงการใหม่จากหน่วยงานที่เกี่ยวข้อง
- กำหนดวัตถุประสงค์ของการจัดเก็บข้อมูลให้ชัดเจน ว่าจะนำข้อมูลไปใช้เพื่ออะไร และมีข้อมูลประเภทใดบ้าง
- **จัดประเภทข้อมูล (Data Classification)**
    - แบ่งระดับข้อมูล เช่น Public / Internal / Confidential / Sensitive
    - ใช้กำหนดระดับมาตรการรักษาความปลอดภัย
- **ประเมินความเสี่ยงด้านข้อมูลส่วนบุคคล (DPIA)**
    - วิเคราะห์ว่าข้อมูลเป็นข้อมูลทั่วไปหรือข้อมูลอ่อนไหว
    - ประเมินผลกระทบต่อเจ้าของข้อมูล
    - จัดทำบันทึกรายการประมวลผลข้อมูล (ROPA)
- **กำหนดระยะเวลาการจัดเก็บข้อมูล (Data Retention Policy)**
    - ระบุระยะเวลาที่ต้องจัดเก็บข้อมูลแต่ละประเภท
    - กำหนดเงื่อนไขการลบหรือทำลายข้อมูล
- **ออกแบบระบบตามหลัก Privacy by Design**
    - จัดเก็บข้อมูลเท่าที่จำเป็น (Data Minimization)
    - แยกข้อมูลระบุตัวตน (Anonymization / Pseudonymization)
    - ใช้การเข้ารหัสข้อมูลทั้งขณะจัดเก็บและส่งผ่าน (Encryption)

2. การจัดเก็บและประมวลผล (Storage & Processing)

- **การจัดการสิทธิ์ (IAM)**
    - ใช้หลัก Least Privilege
    - กำหนดสิทธิ์ตามบทบาท (Role-based Access)
    - ใช้ Multi-Factor Authentication (MFA)
- **การจัดเก็บข้อมูลอย่างปลอดภัย**
    - เข้ารหัสข้อมูลสำคัญในฐานข้อมูล
    - แยกการจัดเก็บ Encryption Key (Key Management)
    - มีการหมุนเวียน Key (Key Rotation)
- **ระบบบันทึกการใช้งาน (Audit Trail & Logging)**
    - บันทึกการเข้าถึงและการแก้ไขข้อมูล
    - สามารถตรวจสอบย้อนหลังได้
- **ความปลอดภัยของ API (API Security)**
    - ใช้ Token / OAuth
    - มี Rate Limiting
    - ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
- **การสำรองข้อมูล (Backup)**
    - สำรองข้อมูลอย่างสม่ำเสมอ
    - เข้ารหัสไฟล์สำรอง
- **การจัดการความยินยอม (Consent Management)**
    - แจ้ง Privacy Policy
    - ขอ Consent ตามกฎหมาย
    - รองรับการถอนความยินยอม

3. การบำรุงรักษาและติดตาม (Maintenance & Monitoring)

- **การตรวจสอบและเฝ้าระวัง (Monitoring & Auditing)**
    - ตรวจสอบ Log เพื่อหาความผิดปกติ
    - รวม Log ไว้ในระบบกลาง (Log Centralization)
- **การทดสอบความปลอดภัย**
    - Vulnerability Assessment
    - Penetration Testing
- **การตรวจสอบประสิทธิภาพ (Performance Monitoring)**
    - ตรวจสอบ CPU / Memory / Response Time
    - ตรวจสอบ Query ที่ช้า
- **ระบบแจ้งเตือนและจัดการเหตุการณ์ (Alert & Incident Response)**
    - ตั้ง Alert เมื่อพบพฤติกรรมผิดปกติ
    - มี Incident Response Plan
- **การจัดการเหตุละเมิดข้อมูล (Data Breach Management)**
    - แจ้ง DPO ทันทีเมื่อพบเหตุ
    - แจ้งหน่วยงานกำกับ (ภายใน 72 ชั่วโมง)
    - แจ้งเจ้าของข้อมูล
- **การทบทวนและปรับปรุงระบบ**
    - ปรับปรุงนโยบายความปลอดภัย
    - ปรับปรุงระบบตามความเสี่ยงใหม่

4. การทำลายและสิ้นสุด (Destruction & Termination)

- ตรวจสอบว่าข้อมูลหมดความจำเป็นหรือครบกำหนด
- **การจัดเก็บระยะยาว (Data Archiving)**
    - ย้ายข้อมูลที่ยังจำเป็นไปยังระบบ Archive
- **การทำลายข้อมูล (Secure Data Destruction)**
    - ใช้วิธีที่ไม่สามารถกู้คืนได้
- **การตรวจสอบหลังการลบ (Deletion Verification)**
    - ตรวจสอบว่าข้อมูลถูกลบจริง
    - ไม่มีข้อมูลตกค้างในระบบ
- จัดทำบันทึกการทำลายข้อมูล
- ปิดโครงการหรือยุติการใช้งานระบบ

6.5 การบริหารจัดการฐานข้อมูลของระบบสารสนเทศ 4 ระยะ

1. เตรียมการและออกแบบ (Preparation & Design)

กำหนดวัตถุประสงค์ · จัดประเภทข้อมูล · ออกแบบตามหลัก Privacy by Design

กิจกรรม	รายละเอียด	มาตรการ / เครื่องมือ
รับความต้องการ	รับความต้องการหรือโครงการใหม่จากหน่วยงานที่เกี่ยวข้อง กำหนดวัตถุประสงค์การจัดเก็บและประเภทข้อมูลให้ชัดเจน	Project Initiation
จัดประเภทข้อมูล Data Classification	แบ่งระดับข้อมูลเพื่อใช้กำหนดระดับมาตรการรักษาความปลอดภัย	PublicInternalConfidentialSensitive
ประเมินความเสี่ยง PDPA DPIA	วิเคราะห์ว่าข้อมูลเป็นข้อมูลทั่วไปหรืออ่อนไหว ประเมินผลกระทบต่อเจ้าของข้อมูล	• จัดทำบันทึกรายการประมวลผล (ROPA) • ประเมินผลกระทบต่อความเป็นส่วนตัว
Data Retention Policy ระยะเวลาจัดเก็บ	ระบุระยะเวลาจัดเก็บข้อมูลแต่ละประเภท และกำหนดเงื่อนไขการลบหรือทำลาย	Retention Schedule
Privacy by Design	ออกแบบระบบโดยคำนึงถึงความเป็นส่วนตัวตั้งแต่ต้น	• Data Minimization — จัดเก็บเท่าที่จำเป็น • Anonymization / Pseudonymization • Encryption ทั้งขณะจัดเก็บและส่งผ่าน

2. การจัดเก็บและประมวลผล (Storage & Processing)

AM · Encryption · Audit Trail · API Security · Backup · Consent

กิจกรรม	รายละเอียด	มาตรการ / เครื่องมือ
การจัดการสิทธิ์ IAM	ควบคุมการเข้าถึงตามบทบาทและหลัก Least Privilege	Least PrivilegeRBACMFA
การจัดเก็บข้อมูลปลอดภัย Secure Storage	เข้ารหัสข้อมูลสำคัญในฐานข้อมูล แยกการจัดเก็บ Key และหมุนเวียน Key อย่างสม่ำเสมอ	• Encryption at Rest • Key Management • Key Rotation
บันทึกการใช้งาน Audit Trail & Logging	บันทึกการเข้าถึงและแก้ไขข้อมูลทุกครั้ง เพื่อให้สามารถตรวจสอบย้อนหลังได้	Audit Log System
ความปลอดภัย API API Security	ป้องกันการเข้าถึง API โดยไม่ได้รับอนุญาต พร้อมควบคุมปริมาณคำขอ	Token / OAuthRate Limiting
สำรองข้อมูล Backup	สำรองข้อมูลอย่างสม่ำเสมอ และเข้ารหัสไฟล์สำรองข้อมูล	• Regular Backup Schedule • Encrypted Backup Files
จัดการความยินยอม Consent Management	แจ้ง Privacy Policy ขอ Consent ตามกฎหมาย และรองรับการถอนความยินยอม	Privacy PolicyConsent FormWithdrawal Right

3. การบำรุงรักษาและติดตาม (Maintenance & Monitoring)

Monitoring · Security Test · Performance · Incident Response · Data Breach

กิจกรรม	รายละเอียด	มาตรการ / เครื่องมือ
ตรวจสอบและเฝ้าระวัง Monitoring & Auditing	ตรวจสอบ Log เพื่อหาความผิดปกติ และรวม Log ไว้ในระบบกลาง	• Log Analysis • Log Centralization (SIEM)
ทดสอบความปลอดภัย Security Testing	ทดสอบระบบเพื่อค้นหาช่องโหว่และตรวจสอบความแข็งแกร่งของระบบ	Vulnerability AssessmentPenetration Testing
ตรวจสอบประสิทธิภาพ Performance Monitoring	ตรวจสอบทรัพยากรระบบและ Query ที่ใช้เวลานานเพื่อป้องกันคอขวด	• CPU / Memory / Response Time • Slow Query Analysis
แจ้งเตือนและจัดการเหตุ Alert & Incident Response	ตั้ง Alert เมื่อพบพฤติกรรมผิดปกติ และมีแผนรับมือเหตุการณ์	Alert RulesIncident Response Plan
จัดการเหตุละเมิดข้อมูล Data Breach Management	เมื่อพบเหตุละเมิด ต้องแจ้งหน่วยงานกำกับภายใน 72 ชั่วโมง และแจ้งเจ้าของข้อมูล	• แจ้ง DPO ทันที • แจ้งหน่วยงานกำกับ ภายใน 72 ชม. • แจ้งเจ้าของข้อมูล
ทบทวนและปรับปรุง Review & Improvement	ปรับปรุงนโยบายความปลอดภัยและระบบตามความเสี่ยงใหม่ที่พบ	Policy ReviewRisk-based Update

4. การทำลายและสิ้นสุด (Destruction & Termination)

Archive · Secure Deletion · Verification · ปิดโครงการ

กิจกรรม	รายละเอียด	มาตรการ / เครื่องมือ
ตรวจสอบความจำเป็น	ตรวจสอบว่าข้อมูลหมดความจำเป็นหรือครบกำหนดตาม Retention Policy แล้วหรือยัง	Retention Check
จัดเก็บระยะยาว Data Archiving	ย้ายข้อมูลที่ยังจำเป็นแต่ไม่ได้ใช้งานบ่อยไปยังระบบ Archive	Archive System
ทำลายข้อมูล Secure Data Destruction	ใช้วิธีทำลายข้อมูลที่ไม่สามารถกู้คืนได้ เพื่อป้องกันการรั่วไหลภายหลัง	Secure WipeCryptographic Erasure
ตรวจสอบหลังลบ Deletion Verification	ตรวจสอบให้มั่นใจว่าข้อมูลถูกลบจริงและไม่มีข้อมูลตกค้างในระบบใด ๆ	• ตรวจสอบ DB / Backup / Log • ยืนยันไม่มีข้อมูลตกค้าง
บันทึกและปิดโครงการ	จัดทำบันทึกการทำลายข้อมูลเป็นหลักฐาน และดำเนินการปิดโครงการหรือยุติการใช้งานระบบ	Destruction RecordProject Closure

7. มาตรฐานงาน

มาตรฐานของงานในคู่มือฉบับนี้กำหนดขึ้นเพื่อให้การดำเนินงานด้านเทคโนโลยีสารสนเทศของศูนย์ข้อมูลและสารสนเทศ สวพส. มีคุณภาพและประสิทธิภาพในระดับที่กำหนด สามารถตรวจสอบและวัดผลได้ โดยครอบคลุมกระบวนงานทั้ง 4 ด้าน ตั้งแต่กระบวนการพัฒนาระบบ (6.1) การปรับปรุงระบบ (6.2) การบริหารจัดการเว็บไซต์ (6.3) และการบริหารจัดการฐานข้อมูล (6.4)

7.1 ตัวชี้วัดมาตรฐาน (KPI)

ตารางต่อไปนี้กำหนดตัวชี้วัดหลักสำหรับการประเมินคุณภาพการปฏิบัติงาน เพื่อให้ผู้ปฏิบัติงานและผู้บังคับบัญชาสามารถติดตามผลการดำเนินงานได้อย่างเป็นระบบ:

ที่	ตัวชี้วัด (KPI)	เกณฑ์มาตรฐาน	หน่วย	เชื่อมโยงกับ
1	การพัฒนาระบบเสร็จตามกำหนด	≥ 90%	ร้อยละ	6.1 พัฒนาระบบใหม่
2	ระบบผ่าน UAT รอบแรก	≥ 80%	ร้อยละ	6.1 / 6.2
3	ข้อบกพร่อง Critical ได้รับการแก้ไขภายใน 24 ชม.	100%	ร้อยละ	6.2 ปรับปรุงระบบ
4	เว็บไซต์ออนไลน์ (Uptime)	≥ 99.5%	ร้อยละ	6.3 บริหารเว็บไซต์
5	เนื้อหาเว็บไซต์ได้รับการอัปเดตตามกำหนด	≥ 95%	ร้อยละ	6.3 บริหารเว็บไซต์
6	ช่องโหว่ระดับสูง (High) ได้รับการแก้ไขภายใน 72 ชม.	100%	ร้อยละ	6.3 / 6.4
7	มีการสำรองข้อมูลสำเร็จตามกำหนด	≥ 99%	ร้อยละ	6.4 บริหารฐานข้อมูล
8	ข้อมูลส่วนบุคคลได้รับการประเมิน DPIA ก่อนจัดเก็บ	100%	ร้อยละ	6.4 บริหารฐานข้อมูล
9	ตอบสนองรายงานเหตุละเมิดข้อมูลภายใน 72 ชม.	100%	ร้อยละ	6.4 บริหารฐานข้อมูล

7.2 มาตรฐานความปลอดภัยสารสนเทศ

การดำเนินงานด้านระบบสารสนเทศและฐานข้อมูลต้องเป็นไปตามมาตรฐานและกรอบงานด้านความปลอดภัยดังต่อไปนี้ โดยเฉพาะกระบวนงาน 6.3 (เว็บไซต์) และ 6.4 (ฐานข้อมูล):

ที่	มาตรฐาน / กรอบงาน	รายละเอียด	เชื่อมโยงกระบวนงาน
1	OWASP Top 10	ป้องกัน SQL Injection, XSS, CSRF และช่องโหว่พื้นฐาน	6.3 / 6.4
2	PDPA (พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)	จัดทำ DPIA, ROPA, ขอ Consent, จัดการ Data Breach	6.4
3	HTTPS / TLS 1.2+	การส่งผ่านข้อมูลต้องเข้ารหัสทั้งหมด	6.3 / 6.4
4	ISO/IEC 27001 (แนวทาง)	การจัดการความมั่นคงสารสนเทศ	6.1 – 6.4
5	Least Privilege / RBAC	กำหนดสิทธิ์ขั้นต่ำตามบทบาท	6.4

7.3 มาตรฐานกระบวนการทำงาน

นอกจากตัวชี้วัดเชิงปริมาณแล้ว กระบวนการทำงานยังต้องปฏิบัติตามมาตรฐานเชิงคุณภาพ ดังนี้:

- เอกสารประกอบการทำงาน: ทุกกระบวนการต้องมีเอกสารบันทึกผลการดำเนินงานอย่างครบถ้วน
- การทดสอบก่อนใช้งานจริง: ระบบทุกระบบต้องผ่านการทดสอบ (System Test + UAT) ก่อน Deploy
- การสำรองข้อมูล: ต้องมีการสำรองข้อมูลก่อนดำเนินการเปลี่ยนแปลงระบบที่สำคัญทุกครั้ง
- การควบคุมการเข้าถึง: บุคคลทุกคนต้องได้รับสิทธิ์เข้าถึงระบบตามหลัก Least Privilege เท่านั้น
- การบันทึก Log: ระบบทุกระบบต้องมี Audit Trail ที่สามารถตรวจสอบย้อนหลังได้
- การทบทวนนโยบาย: ต้องทบทวนและปรับปรุงนโยบายความปลอดภัยอย่างน้อยปีละ 1 ครั้ง

8. ระบบติดตามและประเมินผล

- ติดตามสถานะการดำเนินงานของระบบสารสนเทศอย่างสม่ำเสมอ
- ตรวจสอบประสิทธิภาพของระบบหลังจากการพัฒนา หรือปรับปรุง
- ประเมินความพึงพอใจของผู้ใช้งานระบบ
- บันทึกและจัดเก็บข้อมูลการดำเนินงานเพื่อใช้ในการวิเคราะห์และปรับปรุงระบบในอนาคต
- รายงานผลการดำเนินงานต่อผู้บังคับบัญชาเป็นระยะ

9. เอกสารอ้างอิง

คู่มือการปฏิบัติงานฉบับนี้อ้างอิงกฎหมาย ระเบียบ มาตรฐาน และแนวปฏิบัติดังต่อไปนี้ เพื่อให้การดำเนินงานเป็นไปอย่างถูกต้องตามกรอบกฎหมายและมาตรฐานสากล:

ที่	รายการเอกสาร	ฉบับ/ปี	เชื่อมโยง
1	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)	พ.ศ. 2562	6.4
2	พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม	พ.ศ. 2560	6.1–6.4
3	ระเบียบสถาบันวิจัยและพัฒนาพื้นที่สูงว่าด้วยการจัดซื้อจัดจ้าง	ปัจจุบัน	6.1 / 6.2
4	แนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศ สวพส.	ปัจจุบัน	6.1–6.4
5	OWASP Top 10 (2021)	2021	6.3 / 6.4
6	ISO/IEC 27001:2022 — Information Security Management	2022	6.1–6.4
7	NIST SP 800-53 Rev. 5 — Security and Privacy Controls	2020	6.4
8	W3C Web Content Accessibility Guidelines (WCAG 2.1)	2018	6.3
9	Thailand National Cybersecurity Act (พ.ร.บ. ไซเบอร์ พ.ศ. 2562)	พ.ศ. 2562	6.3 / 6.4
10	คู่มือแนวทางการพัฒนาระบบสารสนเทศภาครัฐ สำนักงาน ก.พ.ร.	ปัจจุบัน	6.1 / 6.2

หมายเหตุ: เอกสารอ้างอิงที่อาจมีการปรับปรุงแก้ไข ผู้ปฏิบัติงานควรตรวจสอบฉบับปัจจุบันจากแหล่งข้อมูลทางการเสมอ

10. แบบฟอร์มที่ใช้

แบบฟอร์มประกอบคู่มือการปฏิบัติงาน

กลุ่มงานพัฒนาระบบสารสนเทศ

ศูนย์ข้อมูลและสารสนเทศ สำนักยุทธศาสตร์และแผน

สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)

รหัส	ชื่อแบบฟอร์ม	เชื่อมโยงกระบวนงาน
IT-F-01	แบบฟอร์มแจ้งความต้องการระบบสารสนเทศ	6.1 / 6.2 — พัฒนาระบบใหม่ / ปรับปรุงระบบ
IT-F-02	เอกสารความต้องการของระบบ (Requirement Document)	6.1 — พัฒนาระบบใหม่
IT-F-03	แบบฟอร์มขอบเขตงาน (TOR)	6.1 / 6.2 — กรณีจ้างผู้พัฒนาภายนอก
IT-F-04	แบบฟอร์มรายงานผลการทดสอบระบบ (Test Report)	6.1 / 6.2 — System Test
IT-F-05	แบบฟอร์มทดสอบการยอมรับ (UAT)	6.1 / 6.2 — User Acceptance Test
IT-F-06	แบบฟอร์มส่งมอบระบบ (Delivery Record)	6.1 — ส่งมอบระบบ
IT-F-07	แบบฟอร์มรับแจ้งปัญหา (Incident Report)	6.2 / 6.3 — ปรับปรุงระบบ / เว็บไซต์
IT-F-08	แบบบันทึกรายการประมวลผลข้อมูล (ROPA)	6.4 — บริหารจัดการฐานข้อมูล (PDPA)
IT-F-09	แบบประเมินผลกระทบความเป็นส่วนตัว (DPIA)	6.4 — บริหารจัดการฐานข้อมูล (PDPA)
IT-F-10	แบบบันทึกการทำลายข้อมูล (Destruction Record)	6.4 — สิ้นสุดการจัดเก็บข้อมูล

จัดทำโดย	กลุ่มงานพัฒนาระบบ	**เวอร์ชัน**	1.0 / ปี 2569

แบบฟอร์มแจ้งความต้องการระบบสารสนเทศ

ศูนย์ข้อมูลและสารสนเทศ สำนักยุทธศาสตร์และแผน
สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)

รหัสแบบฟอร์ม	IT-F-01	เวอร์ชัน	1.0
ชื่อแบบฟอร์ม	**แบบฟอร์มแจ้งความต้องการระบบสารสนเทศ**	วันที่บังคับใช้	2568
วัตถุประสงค์	บันทึกความต้องการของผู้ใช้งานระบบ	กระบวนงาน	6.1 / 6.2

ส่วนที่ 1 : สำหรับผู้ขอรับบริการ (User Section)

ชื่อ-นามสกุล		ตำแหน่ง	
สำนัก / ฝ่าย / กลุ่มงาน		เบอร์โทร / อีเมล	
วันที่แจ้งความต้องการ		ความเร่งด่วน	☐ ด่วนมาก ☐ ด่วน ☐ ปกติ

ส่วนที่ 2 : รายละเอียดความต้องการ (System Requirements)

ประเภทคำขอ	☐ พัฒนาระบบสารสนเทศใหม่ ☐ ปรับปรุงระบบเดิม ☐ อื่นๆ ระบุ .....
ชื่อระบบ	
วัตถุประสงค์ / ปัญหา	
รายละเอียดที่ต้องการ	
รูปแบบข้อมูลเดิม	☐ Excel/Sheets ☐ กระดาษ ☐ ระบบเดิม (ระบุ.....) ☐ อื่นๆ
ระยะเวลาที่ต้องการ	

(.....)
ผู้ขอรับบริการ
วันที่ ...../...../.....

(.....)
หัวหน้ากลุ่มงานผู้รับบริการ
วันที่ ...../...../.....

ส่วนที่ 3 : สำหรับเจ้าหน้าที่กลุ่มพัฒนาระบบสารสนเทศ (IT Only)

ความเห็นเจ้าหน้าที่	
แนวทางดำเนินการ	☐ พัฒนาเอง ☐ จ้างผู้พัฒนาภายนอก ☐ รอพิจารณา
วันที่รับเรื่อง	

(.....)
ผู้รับผิดชอบดำเนินการ
วันที่ ...../...../.....

(.....)
หัวหน้าศูนย์ข้อมูลและสารสนเทศ
วันที่ ...../...../.....

แบบฟอร์มเอกสารความต้องการของระบบ

ศูนย์ข้อมูลและสารสนเทศ สำนักยุทธศาสตร์และแผน
สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)

รหัสแบบฟอร์ม	IT-F-02	เวอร์ชัน	1.0
ชื่อแบบฟอร์ม	เอกสารความต้องการของระบบ (Requirement Document)	วันที่บังคับใช้	2568
วัตถุประสงค์	กำหนดขอบเขตและรายละเอียดการพัฒนาระบบสารสนเทศ	กระบวนงาน	6.1

ส่วนที่ 1 : ข้อมูลโครงการ

ชื่อระบบ / โครงการ		รหัสโครงการ	
ผู้รับผิดชอบ (IT)		ผู้ประสานงาน (User)	
วันที่จัดทำ		เวอร์ชันเอกสาร	

ส่วนที่ 2 : ภาพรวมระบบ (System Overview)

วัตถุประสงค์ระบบ	
กลุ่มผู้ใช้งาน	
ขอบเขตของระบบ	
ระบบที่เชื่อมต่อ	

ส่วนที่ 3 : ฟังก์ชันการทำงาน (Functional Requirements)

ลำดับ	ฟังก์ชัน	รายละเอียด	ลำดับความสำคัญ
1			
2			
3			
4			
5			

ส่วนที่ 4 : โครงสร้างข้อมูล (Data Structure)

ตารางข้อมูลหลัก	
ข้อกำหนดอื่นๆ	

(.....)
ผู้จัดทำ (นักวิชาการคอมพิวเตอร์)
วันที่ ...../...../.....

(.....)
ผู้อนุมัติ (หัวหน้าศูนย์ข้อมูลฯ)
วันที่ ...../...../.....

แบบฟอร์มขอบเขตงาน

ศูนย์ข้อมูลและสารสนเทศ สำนักยุทธศาสตร์และแผน
สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)

รหัสแบบฟอร์ม	IT-F-03	เวอร์ชัน	1.0
ชื่อแบบฟอร์ม	แบบฟอร์มขอบเขตงาน (TOR - Terms of Reference)	วันที่บังคับใช้	2568
วัตถุประสงค์	ใช้สำหรับจัดทำสัญญาจ้างผู้พัฒนาระบบภายนอก	กระบวนงาน	6.1 / 6.2

ส่วนที่ 1 : ข้อมูลโครงการจ้าง	
ชื่อโครงการ	
วงเงินงบประมาณ	
ระยะเวลาดำเนินการ	
รูปแบบการจัดซื้อจัดจ้าง	☐ วิธีเฉพาะเจาะจง ☐ ประกวดราคา (e-bidding) ☐ คัดเลือก

ส่วนที่ 2 : ขอบเขตการดำเนินงาน	
วัตถุประสงค์	
ขอบเขตงานที่จ้าง	
งานที่ไม่รวมในขอบเขต	

ส่วนที่ 3 : คุณสมบัติผู้รับจ้าง	
คุณสมบัติทั่วไป	
คุณสมบัติด้านเทคนิค	
ผลงานที่ผ่านมา	

ส่วนที่ 4 : เงื่อนไขการส่งมอบ (Deliverables)

งวด	รายการส่งมอบ	กำหนดส่ง	% งวดเงิน
1			
2			
3			

(.....)
ผู้จัดทำ TOR (นักวิชาการคอมพิวเตอร์)
วันที่ ...../...../.....

(.....)
ผู้อนุมัติ TOR (หัวหน้าศูนย์ข้อมูลฯ)
วันที่ ...../...../.....

แบบฟอร์มรายงานผลการทดสอบระบบ

ศูนย์ข้อมูลและสารสนเทศ สำนักยุทธศาสตร์และแผน
สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)

รหัสแบบฟอร์ม	IT-F-04	**เวอร์ชัน**	1.0
ชื่อแบบฟอร์ม	**แบบฟอร์มรายงานผลการทดสอบระบบ (Test Report)**	**วันที่บังคับใช้**	2568
วัตถุประสงค์	บันทึกผล System Test ก่อนนำระบบไปใช้งานจริง	**กระบวนงาน**	6.1 / 6.2

ส่วนที่ 1 : ข้อมูลการทดสอบ

ชื่อระบบ		**เวอร์ชัน**	
วันที่ทดสอบ		**ผู้ทดสอบ**	
ประเภทการทดสอบ	☐ System Test ☐ Integration Test ☐ Regression Test	**สภาพแวดล้อม**	☐ Development ☐ UAT ☐ Production

ส่วนที่ 2 : รายการทดสอบ (Test Cases)

TC#	Module	รายการทดสอบ	ผลที่คาดหวัง	ผลจริง	Pass/Fail
1					
2					
3					
4					
5					

ส่วนที่ 3 : สรุปผลการทดสอบ

รายการ	จำนวนทั้งหมด	ผ่าน	ไม่ผ่าน	อัตราผ่าน (%)
Test Cases				

ข้อบกพร่องที่พบ	
ข้อเสนอแนะ	
สรุปผล	☐ ผ่านการทดสอบ ☐ ไม่ผ่าน ต้องแก้ไข ☐ ผ่านแบบมีเงื่อนไข

(.....)
ผู้ทดสอบ (นักวิชาการคอมพิวเตอร์)
วันที่ ...../...../.....

(.....)
หัวหน้าศูนย์ข้อมูลและสารสนเทศ
วันที่ ...../...../.....

แบบฟอร์มทดสอบการยอมรับระบบโดยผู้ใช้งาน

ศูนย์ข้อมูลและสารสนเทศ สำนักยุทธศาสตร์และแผน
สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)

รหัสแบบฟอร์ม	IT-F-05	เวอร์ชัน	1.0
ชื่อแบบฟอร์ม	**แบบฟอร์มทดสอบการยอมรับระบบโดยผู้ใช้งาน (UAT)**	วันที่บังคับใช้	2568
วัตถุประสงค์	ยืนยันว่าระบบตอบสนองต่อความต้องการของผู้ใช้งาน	กระบวนงาน	6.1 / 6.2

ส่วนที่ 1 : ข้อมูลการทดสอบ

ชื่อระบบ		เวอร์ชัน	
วันที่ทดสอบ		สถานที่ทดสอบ	
ผู้จัด (IT)		ผู้ประสานงาน (User)	

ส่วนที่ 2 : ผู้เข้าร่วมทดสอบ

ลำดับ	ชื่อ-สกุล	ตำแหน่ง	สำนัก / ฝ่าย	ลายมือชื่อ
1				
2				
3				
4				
5				

ส่วนที่ 3 : รายการทดสอบโดยผู้ใช้งาน

ลำดับ	สถานการณ์ทดสอบ (Scenario)	ผลที่คาดหวัง	ผลจริง	ผ่าน/ไม่ผ่าน
1				
2				
3				
4				
5				

ส่วนที่ 4 : ความเห็นผู้ใช้งานและสรุปผล

ปัญหา / ข้อเสนอแนะ	
ผลการทดสอบ (UAT)	☐ ผ่าน UAT พร้อม Deploy ☐ ไม่ผ่าน ต้องปรับปรุง ☐ ผ่านแบบมีเงื่อนไข

(.....)
ตัวแทนผู้ใช้งาน (User)
วันที่ ...../...../.....

(.....)
ผู้รับผิดชอบระบบ (IT)
วันที่ ...../...../.....

แบบฟอร์มส่งมอบระบบ

ศูนย์ข้อมูลและสารสนเทศ สำนักยุทธศาสตร์และแผน
สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)

รหัสแบบฟอร์ม	IT-F-06	เวอร์ชัน	1.0
ชื่อแบบฟอร์ม	แบบฟอร์มส่งมอบระบบ (System Delivery Record)	วันที่บังคับใช้	2568
วัตถุประสงค์	บันทึกการส่งมอบระบบสารสนเทศที่พัฒนาหรือปรับปรุงเสร็จสิ้น	กระบวนงาน	6.1

ส่วนที่ 1 : ข้อมูลระบบที่ส่งมอบ

ชื่อระบบ		เวอร์ชัน	
วันที่ส่งมอบ		รหัสโครงการ	
ผู้ส่งมอบ (IT)		ผู้รับมอบ (User)	
สภาพแวดล้อม	☐ Production Server URL:	ประเภทระบบ	☐ ระบบใหม่ ☐ ปรับปรุงระบบเดิม

ส่วนที่ 2 : รายการสิ่งที่ส่งมอบ (Deliverables Checklist)

ลำดับ	รายการ	ส่งมอบ	หมายเหตุ
1	Source Code (ซอร์สโค้ด)	☐ ใช่ ☐ ไม่มี	
2	ระบบบน Production Server	☐ ใช่ ☐ ไม่มี	
3	คู่มือผู้ใช้งาน (User Manual)	☐ ใช่ ☐ ไม่มี	
4	คู่มือผู้ดูแลระบบ (Admin Manual)	☐ ใช่ ☐ ไม่มี	
5	เอกสาร Requirement Document	☐ ใช่ ☐ ไม่มี	
6	เอกสาร Test Report	☐ ใช่ ☐ ไม่มี	
7	ผล UAT	☐ ใช่ ☐ ไม่มี	
8	รหัสผ่าน / Credentials ระบบ	☐ ใช่ ☐ ไม่มี	
9	สิทธิ์การเข้าถึง Database	☐ ใช่ ☐ ไม่มี	

ส่วนที่ 3 : การรับประกันและการบำรุงรักษา

ระยะเวลารับประกัน	
เงื่อนไขการรับประกัน	
ผู้ดูแลระบบ (IT)	
ช่องทางแจ้งปัญหา	

(.....)
ผู้ส่งมอบ (นักวิชาการคอมพิวเตอร์)
วันที่ ...../...../.....

(.....)
ผู้รับมอบ (หัวหน้าหน่วยงาน/ผู้ใช้งาน)
วันที่ ...../...../.....

แบบฟอร์มรับแจ้งปัญหา

ศูนย์ข้อมูลและสารสนเทศ สำนักยุทธศาสตร์และแผน
สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)

รหัสแบบฟอร์ม	IT-F-07	เวอร์ชัน	1.0
ชื่อแบบฟอร์ม	แบบฟอร์มรับแจ้งปัญหา (Incident Report)	วันที่บังคับใช้	2568
วัตถุประสงค์	บันทึกปัญหาที่เกิดขึ้นกับระบบสารสนเทศหรือเว็บไซต์	กระบวนงาน	6.2 / 6.3

ส่วนที่ 1 : ข้อมูลผู้แจ้งปัญหา

ชื่อ-สกุล		วันที่แจ้ง	
สำนัก / ฝ่าย		เบอร์โทร / อีเมล	
ช่องทางแจ้ง	☐ โทรศัพท์ ☐ อีเมล ☐ Line OA ☐ ระบบ Ticket ☐ อื่นๆ	เวลาที่แจ้ง	

ส่วนที่ 2 : รายละเอียดปัญหา

ระบบที่มีปัญหา	
ประเภทปัญหา	☐ ระบบล่ม/ใช้งานไม่ได้ ☐ ข้อมูลผิดพลาด ☐ ขอปรับปรุง ☐ ปัญหาด้านความปลอดภัย ☐ อื่นๆ
ระดับความรุนแรง	☐ Critical (ระบบหยุดทำงาน) ☐ High ☐ Medium ☐ Low
รายละเอียดปัญหา	
ขั้นตอนที่ทำให้เกิดปัญหา	
ผลกระทบ	

ส่วนที่ 3 : การดำเนินการแก้ไข (IT Section)

ผู้รับผิดชอบแก้ไข		วันที่รับเรื่อง	
วิธีการแก้ไข		มี MA หรือไม่	☐ มี ☐ ไม่มี
รายละเอียดการแก้ไข			
วันที่แก้ไขเสร็จ			
สถานะ	☐ แก้ไขเสร็จ ☐ อยู่ระหว่างดำเนินการ ☐ รอดำเนินการ ☐ ส่งต่อผู้รับจ้าง MA		

(.....)
ผู้แจ้งปัญหา
วันที่ ...../...../.....

(.....)
ผู้รับผิดชอบ (นักวิชาการคอมพิวเตอร์)
วันที่ ...../...../.....

แบบบันทึกรายการกิจกรรมการประมวลผลข้อมูล

ศูนย์ข้อมูลและสารสนเทศ สำนักยุทธศาสตร์และแผน
สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)

รหัสแบบฟอร์ม	IT-F-08	เวอร์ชัน	1.0
ชื่อแบบฟอร์ม	แบบบันทึกรายการกิจกรรมการประมวลผลข้อมูล (ROPA)	วันที่บังคับใช้	2568
วัตถุประสงค์	บันทึกรายการประมวลผลข้อมูลส่วนบุคคล ตาม พ.ร.บ. PDPA พ.ศ. 2562	กระบวนงาน	6.4

⚠ แบบฟอร์มนี้จัดทำตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) — ต้องจัดทำก่อนการประมวลผลข้อมูลส่วนบุคคลทุกครั้ง

ส่วนที่ 1 : ข้อมูลระบบ / กิจกรรม

ชื่อระบบ / กิจกรรม	
ผู้ควบคุมข้อมูล	
ผู้ประมวลผลข้อมูล	
DPO ที่รับผิดชอบ	
วันที่จัดทำ / ปรับปรุง	

ส่วนที่ 2 : ประเภทข้อมูลส่วนบุคคลที่ประมวลผล

ลำดับ	ประเภทข้อมูล	วัตถุประสงค์การประมวลผล	ฐานทางกฎหมาย	ระดับความอ่อนไหว
1	ข้อมูลประจำตัว (ชื่อ, รหัส)		☐ ฉันทามติ ☐ สัญญา ☐ กฎหมาย	☐ ทั่วไป ☐ อ่อนไหว
2	ข้อมูลการติดต่อ (เบอร์, อีเมล)		☐ ฉันทามติ ☐ สัญญา ☐ กฎหมาย	☐ ทั่วไป ☐ อ่อนไหว
3	ข้อมูลการใช้งานระบบ		☐ ฉันทามติ ☐ สัญญา ☐ กฎหมาย	☐ ทั่วไป ☐ อ่อนไหว
4	อื่นๆ (ระบุ)		☐ ฉันทามติ ☐ สัญญา ☐ กฎหมาย	☐ ทั่วไป ☐ อ่อนไหว

ส่วนที่ 3 : การจัดเก็บและส่งต่อข้อมูล

สถานที่จัดเก็บข้อมูล	☐ Server ภายในองค์กร ☐ Cloud (ระบุ .....) ☐ อื่นๆ
ระยะเวลาจัดเก็บ	
การส่งข้อมูลให้บุคคลอื่น	☐ ไม่มี ☐ มี (ระบุผู้รับ / วัตถุประสงค์: .....)
มาตรการรักษาความปลอดภัย	☐ Encryption ☐ Access Control ☐ Audit Log ☐ MFA ☐ อื่นๆ

(.....)
ผู้จัดทำ ROPA (นักวิชาการคอมพิวเตอร์)
วันที่ ...../...../.....

(.....)
เจ้าหน้าที่คุ้มครองข้อมูล (DPO)
วันที่ ...../...../.....

แบบประเมินผลกระทบความเป็นส่วนตัว

ศูนย์ข้อมูลและสารสนเทศ สำนักยุทธศาสตร์และแผน
สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)

รหัสแบบฟอร์ม	IT-F-09	เวอร์ชัน	1.0
ชื่อแบบฟอร์ม	แบบประเมินผลกระทบความเป็นส่วนตัว (DPIA)	วันที่บังคับใช้	2568
วัตถุประสงค์	ประเมินความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคลก่อนพัฒนาหรือปรับปรุงระบบ	กระบวนงาน	6.4

⚠ DPIA ต้องดำเนินการก่อนประมวลผลข้อมูลส่วนบุคคลทุกโครงการ ตาม มาตรา 39 PDPA

ส่วนที่ 1 : ข้อมูลโครงการ

ชื่อโครงการ / ระบบ	
ผู้รับผิดชอบ	
วันที่ประเมิน	
วัตถุประสงค์การประมวลผล	

ส่วนที่ 2 : การคัดกรอง (Screening) — ต้องทำ DPIA หรือไม่

ลำดับ	เกณฑ์การพิจารณา	ใช่	ไม่ใช่
1	มีการประมวลผลข้อมูลส่วนบุคคลในปริมาณมาก	☐	☐
2	มีข้อมูลอ่อนไหว (สุขภาพ, ชีวภาพ, ศาสนา ฯลฯ)	☐	☐
3	มีการเชื่อมโยงข้อมูลจากหลายแหล่ง	☐	☐
4	มีการประมวลผลข้อมูลของเด็กหรือผู้เปราะบาง	☐	☐
5	มีการส่งข้อมูลไปต่างประเทศ	☐	☐
6	มีการตัดสินใจอัตโนมัติ (AI/Algorithm)	☐	☐

ส่วนที่ 3 : การระบุและประเมินความเสี่ยง

ลำดับ	ความเสี่ยงที่ระบุ	ผลกระทบ (H/M/L)	โอกาสเกิด (H/M/L)	มาตรการลดความเสี่ยง
1				
2				

ส่วนที่ 4 : สรุปผลและการอนุมัติ

ระดับความเสี่ยงรวม	☐ สูง (High) ☐ ปานกลาง (Medium) ☐ ต่ำ (Low)
มาตรการที่จะนำไปใช้	
ผลการพิจารณา	☐ อนุมัติดำเนินการ ☐ อนุมัติแบบมีเงื่อนไข ☐ ไม่อนุมัติ

(.....)
ผู้ประเมิน (นักวิชาการคอมพิวเตอร์)
วันที่ ...../...../.....

(.....)
เจ้าหน้าที่คุ้มครองข้อมูล (DPO)
วันที่ ...../...../.....

แบบบันทึกการทำลายข้อมูล

ศูนย์ข้อมูลและสารสนเทศ สำนักยุทธศาสตร์และแผน
สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)

รหัสแบบฟอร์ม	IT-F-10	เวอร์ชัน	1.0
ชื่อแบบฟอร์ม	แบบบันทึกการทำลายข้อมูล (Data Destruction Record)	วันที่บังคับใช้	2568
วัตถุประสงค์	เอกสารหลักฐานการลบหรือทำลายข้อมูลอย่างปลอดภัย ตาม Data Retention Policy	กระบวนงาน	6.4

⚠ แบบฟอร์มนี้เป็นหลักฐานการทำลายข้อมูล ต้องเก็บรักษาไว้ไม่น้อยกว่า 3 ปี ตาม PDPA และนโยบายองค์กร

ส่วนที่ 1 : ข้อมูลการดำเนินการ

ชื่อระบบ / ฐานข้อมูล		วันที่ทำลาย	
ผู้ดำเนินการทำลาย		ผู้ตรวจสอบ	
เหตุผลในการทำลาย	☐ ครบกำหนด Retention Policy ☐ ยุติการใช้งานระบบ ☐ คำร้องเจ้าของข้อมูล ☐ อื่นๆ		

ส่วนที่ 2 : รายการข้อมูลที่ทำลาย

ลำดับ	ชื่อฐานข้อมูล / ตาราง / ไฟล์	ประเภทข้อมูล	ปริมาณข้อมูล	วิธีการทำลาย	หมายเหตุ
1					
2					
3					
4					

ส่วนที่ 3 : วิธีการทำลายข้อมูล

วิธีการที่ใช้	
เครื่องมือ / ซอฟต์แวร์	

ส่วนที่ 4 : การตรวจสอบยืนยัน (Deletion Verification)

ลำดับ	รายการตรวจสอบ	ผล	หมายเหตุ
1	ตรวจสอบข้อมูลถูกลบจาก Database แล้ว	☐ ผ่าน ☐ ไม่ผ่าน	
2	ตรวจสอบข้อมูลถูกลบจาก Backup แล้ว	☐ ผ่าน ☐ ไม่ผ่าน	
3	ตรวจสอบข้อมูลถูกลบจาก Log แล้ว	☐ ผ่าน ☐ ไม่ผ่าน	
4	ไม่พบข้อมูลตกค้างในระบบใดๆ	☐ ผ่าน ☐ ไม่ผ่าน	
5	บันทึก Destruction Record เรียบร้อย	☐ ผ่าน ☐ ไม่ผ่าน	

(.....)
ผู้ดำเนินการทำลายข้อมูล
วันที่ ...../...../.....

(.....)
ผู้ตรวจสอบ / เจ้าหน้าที่คุ้มครองข้อมูล (DPO)
วันที่ ...../...../.....

11. ภาคผนวก

ภาคผนวกต่อไปนี้ประกอบด้วยเอกสารสนับสนุนการปฏิบัติงานตามกระบวนการที่กำหนดไว้ในข้อ 6.1 ถึง 6.4 แบบฟอร์มและตารางในภาคผนวกสามารถนำไปใช้งานจริงได้โดยตรง

ภาคผนวก ก: รายการแบบฟอร์มและเอกสารประกอบการปฏิบัติงาน

แบบฟอร์มต่อไปนี้ใช้สนับสนุนกระบวนการทำงานตามข้อ 6.1–6.4 โดยเจ้าหน้าที่ต้องกรอกและจัดเก็บในระบบจัดการเอกสารของหน่วยงาน:

รหัสแบบฟอร์ม	ชื่อแบบฟอร์ม	วัตถุประสงค์	เชื่อมโยงกระบวนงาน
IT-F-01	แบบฟอร์มแจ้งความต้องการระบบสารสนเทศ	บันทึกความต้องการผู้ใช้	6.1 / 6.2
IT-F-02	เอกสารความต้องการของระบบ (Requirement Document)	กำหนดขอบเขตการพัฒนา	6.1
IT-F-03	แบบฟอร์มขอบเขตงาน (TOR)	สัญญาจ้างผู้พัฒนา	6.1 / 6.2
IT-F-04	แบบฟอร์มรายงานผลการทดสอบระบบ (Test Report)	บันทึกผล System Test	6.1 / 6.2
IT-F-05	แบบฟอร์มทดสอบการยอมรับ (UAT)	ยืนยันระบบโดยผู้ใช้	6.1 / 6.2
IT-F-06	แบบฟอร์มส่งมอบระบบ (Delivery Record)	บันทึกการส่งมอบ	6.1
IT-F-07	แบบฟอร์มรับแจ้งปัญหา (Incident Report)	บันทึกปัญหาเว็บ/ระบบ	6.2 / 6.3
IT-F-08	แบบบันทึกรายการประมวลผลข้อมูล (ROPA)	ปฏิบัติตาม PDPA	6.4
IT-F-09	แบบประเมินผลกระทบความเป็นส่วนตัว (DPIA)	ประเมินความเสี่ยง PDPA	6.4
IT-F-10	แบบบันทึกการทำลายข้อมูล (Destruction Record)	เอกสารหลักฐานการลบ	6.4

ภาคผนวก ข: อภิธานศัพท์และคำย่อ (Glossary)

ตารางต่อไปนี้รวบรวมคำย่อและศัพท์เทคนิคที่ใช้ในคู่มือฉบับนี้ เพื่อให้ผู้ปฏิบัติงานและผู้ที่เกี่ยวข้องเข้าใจความหมายตรงกัน:

คำย่อ / ศัพท์	ชื่อเต็ม	ความหมาย	ปรากฏใน
MA	Maintenance Agreement	สัญญาการบำรุงรักษาระบบสารสนเทศ	6.2
UAT	User Acceptance Test	การทดสอบระบบโดยผู้ใช้งาน	6.1 / 6.3
TOR	Terms of Reference	เอกสารขอบเขตงาน	6.1 / 6.2
PDPA	Personal Data Protection Act	พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	6.4
DPIA	Data Protection Impact Assessment	การประเมินผลกระทบด้านการคุ้มครองข้อมูล	6.4
ROPA	Records of Processing Activities	บันทึกรายการกิจกรรมการประมวลผลข้อมูล	6.4
DPO	Data Protection Officer	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	6.4
IAM	Identity and Access Management	การบริหารจัดการตัวตนและการเข้าถึง	6.4
MFA	Multi-Factor Authentication	การยืนยันตัวตนหลายปัจจัย	6.4
OWASP	Open Worldwide Application Security Project	กรอบมาตรฐานความปลอดภัยเว็บแอปพลิเคชัน	6.3 / 6.4
SIEM	Security Information & Event Management	ระบบจัดการข้อมูลเหตุการณ์ความปลอดภัย	6.4
TLS	Transport Layer Security	โปรโตคอลเข้ารหัสการส่งข้อมูล	6.3 / 6.4
CMS	Content Management System	ระบบจัดการเนื้อหาเว็บไซต์	6.3
XSS	Cross-Site Scripting	การโจมตีโดยการฝังโค้ดในหน้าเว็บ	6.3 / 6.4
RBAC	Role-Based Access Control	การควบคุมสิทธิ์ตามบทบาท	6.4

ภาคผนวก ค: Data Classification Matrix

ตารางจัดประเภทข้อมูลต่อไปนี้ใช้เป็นแนวทางในการกำหนดมาตรการรักษาความปลอดภัยตามระดับความอ่อนไหวของข้อมูล สอดคล้องกับกระบวนงาน 6.4 (การบริหารจัดการฐานข้อมูล):

ระดับข้อมูล	ตัวอย่างข้อมูล	มาตรการรักษาความปลอดภัย	การเข้าถึง	Retention
Public (สาธารณะ)	ข่าวประชาสัมพันธ์ เอกสารเผยแพร่	HTTPS · Integrity Check	ทุกคน	ตามนโยบาย
Internal (ภายใน)	ข้อมูลพนักงาน รายงานภายใน	HTTPS · Role-based Access	บุคลากร สวพส.	5 ปี
Confidential (ลับ)	ข้อมูลโครงการวิจัย สัญญา	Encryption + MFA Audit Trail	เฉพาะผู้มีสิทธิ์	7 ปี
Sensitive (ข้อมูลส่วนบุคคล)	ชื่อ-สกุล ที่อยู่ ข้อมูลสุขภาพ	PDPA · Encrypt at Rest DPIA · Consent	DPO + ผู้รับผิดชอบ	ตาม PDPA

ภาคผนวก ง: Incident Response Timeline

แผนผังระยะเวลาการตอบสนองต่อเหตุการณ์ความปลอดภัย (Incident Response) สำหรับกระบวนงาน 6.3 และ 6.4 โดยเฉพาะกรณีเหตุละเมิดข้อมูลส่วนบุคคลตาม PDPA:

ระยะเวลา	ขั้นตอน	การดำเนินการ	ผู้รับผิดชอบ	เชื่อมโยง
0 – 1 ชม.	**ตรวจจับ (Detect)**	รับแจ้ง / ระบบแจ้งเตือน ตรวจสอบและยืนยันเหตุการณ์	นักวิชาการคอมพิวเตอร์	6.3 / 6.4
1 – 4 ชม.	**ควบคุม (Contain)**	จำกัดขอบเขตผลกระทบ แยก System ที่ได้รับผลกระทบ	นักวิชาการคอมพิวเตอร์	6.4
4 – 24 ชม.	**แจ้ง DPO (หากเกี่ยวข้อง PDPA)**	ประเมินว่าเป็น Data Breach หรือไม่ แจ้ง DPO ทันที	นักวิชาการคอมพิวเตอร์ + DPO	6.4
ภายใน 72 ชม.	**แจ้งหน่วยงานกำกับ**	แจ้ง สำนักงาน PDPC ตามกฎหมาย (Data Breach)	DPO	6.4
72 ชม. ขึ้นไป	**กู้คืน (Recovery)**	คืนระบบสู่สภาวะปกติ ตรวจสอบข้อมูลสมบูรณ์	นักวิชาการคอมพิวเตอร์	6.3 / 6.4
หลังเหตุการณ์	**ทบทวน (Lessons Learned)**	สรุปบทเรียน ปรับปรุงแผน บันทึกในระบบ HKM	ทีมงาน	6.3 / 6.4

ภาคผนวก จ: บันทึกการปรับปรุงคู่มือ (Document History)

บันทึกการเปลี่ยนแปลงและปรับปรุงคู่มือการปฏิบัติงานฉบับนี้:

ฉบับที่	วันที่	รายการปรับปรุง	ผู้จัดทำ	ผู้อนุมัติ
1.0	2568	จัดทำคู่มือครั้งแรก ครอบคลุมกระบวนงาน 6.1–6.4	นักวิชาการคอมพิวเตอร์	หัวหน้าศูนย์ข้อมูลฯ
–	–	*(สำหรับการปรับปรุงครั้งถัดไป)*	–	–