แนวปฏิบัติ PDPA และระบบสารสนเทศเพื่อการจัดการข้อมูลนักศึกษา.md

Add new file
jeerapol kumkeam authored just now

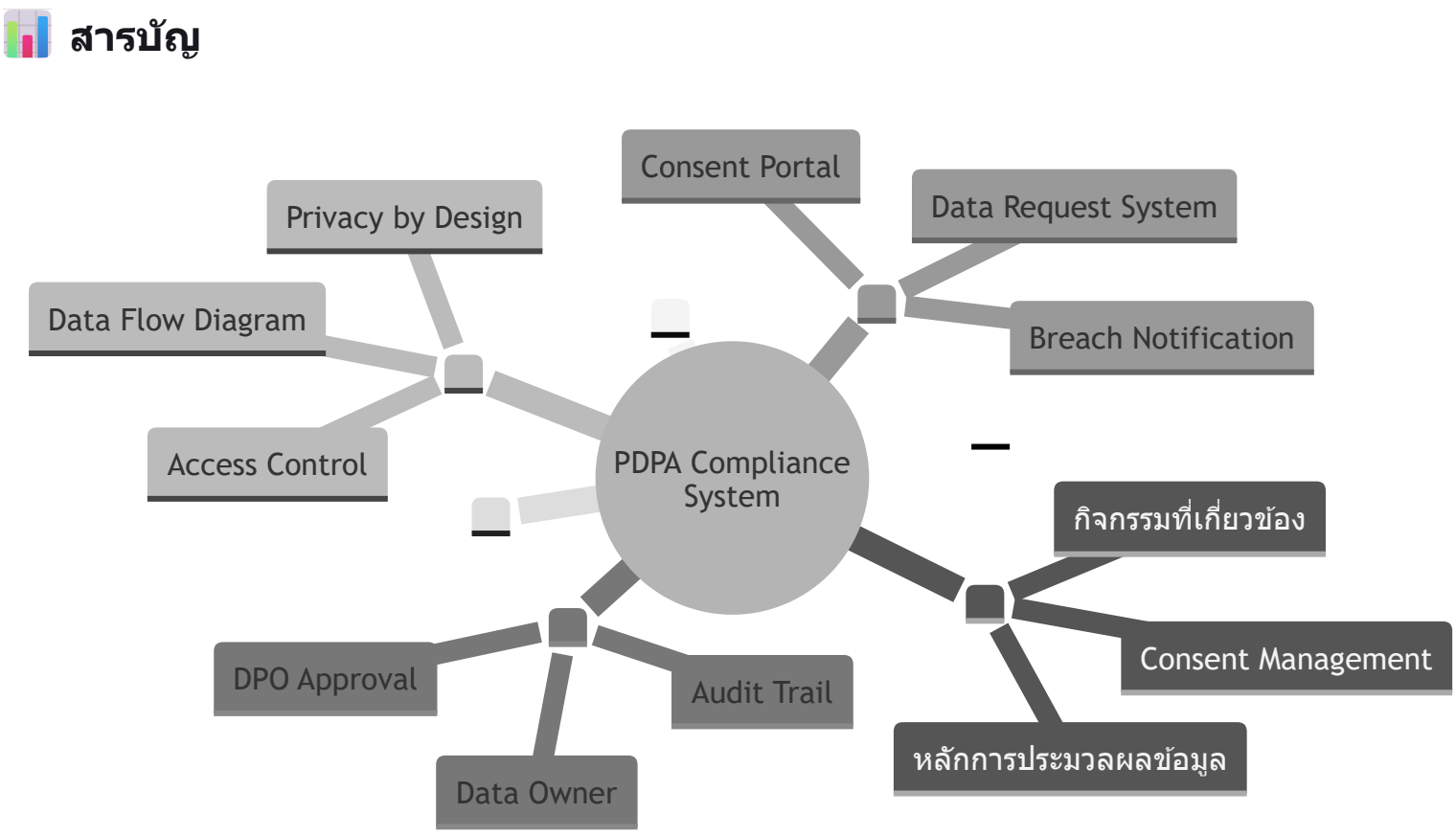
แนวปฏิบัติ PDPA และระบบสารสนเทศเพื่อการจัดการข้อมูลนักศึกษา.md 34.58 KiB

🛡️ แนวปฏิบัติ PDPA และระบบสารสนเทศเพื่อการจัดการข้อมูลนักศึกษา

ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

สำนักหอสมุดกลาง มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

📊 สารบัญ



---

1. บทสรุปผู้บริหาร

🎯 วัตถุประสงค์

เพื่อสร้างระบบการจัดการข้อมูลส่วนบุคคลของนักศึกษาที่สอดคล้องกับ **พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)** และลดความเสี่ยง **CL-RA-01 (Data Leakage)** และ **CL-RA-07 (ขาดความรู้ PDPA)** ตามแผนจัดการความเสี่ยง **CL-RTP-03** และ **CL-RTP-05**

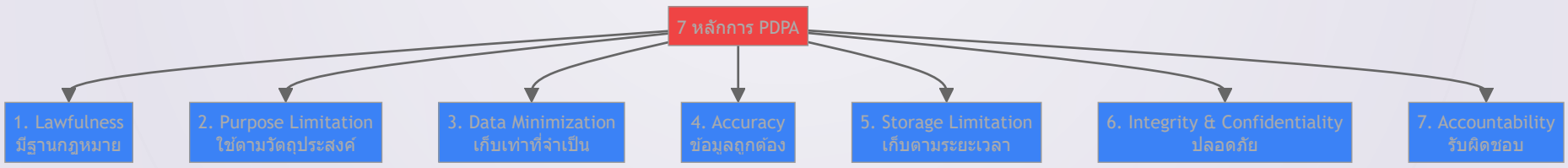
📋 กิจกรรมที่เกี่ยวข้องกับข้อมูลนักศึกษา

กิจกรรม	ข้อมูลที่เก็บ	ฐานกฎหมาย	ระยะเวลาเก็บ
การสมัครสมาชิกห้องสมุด	ชื่อ, รหัสนักศึกษา, คณะ, อีเมล	Contractual Necessity	ตลอดการเป็นสมาชิก + 5 ปี
การยืม-คืนทรัพยากร	ประวัติการยืม, ค่าปรับ	Contractual Necessity	3 ปี
Library Tour / กิจกรรม	รูปถ่าย, วิดีโอ, ชื่อ-สกุล	**Consent**	2 ปี
Smart Room Booking	ชื่อ, รหัสนักศึกษา, เวลาใช้งาน	Legitimate Interest	1 ปี
Virtual Tour (มีผู้ใช้จริง)	IP Address, Cookie	Consent	6 เดือน
Smart Curriculum Connect	หลักสูตร, วิชาที่ลงทะเบียน	Legitimate Interest	ตลอดการศึกษา
AI Jinny X Chatbot	คำถาม, IP Address	Consent	1 ปี
การวิจัย/สำรวจความพึงพอใจ	คำตอบแบบสำรวจ, Demographics	Consent	3 ปี

---

2. 📜 แนวปฏิบัติ PDPA สำหรับกิจกรรมต่างๆ

2.1 หลักการประมวลผลข้อมูลส่วนบุคคล (7 Principles)



2.2 แนวปฏิบัติสำหรับแต่ละกิจกรรม

📸 กิจกรรมที่ 1: การถ่ายภาพ/วิดีโอ (Library Tour, กิจกรรม)

ผู้รับผิดชอบ: นายคุณากร สุทธิกุล

ขั้นตอน	การปฏิบัติ	ฐานกฎหมาย
ก่อนถ่ายภาพ	1. แจ้งวัตถุประสงค์การใช้งาน 2. ขอความยินยอม (Consent Form) 3. แจ้งสิทธิ์ในการถอนความยินยอม	Consent
ระหว่างถ่ายภาพ	1. ถ่ายเฉพาะผู้ที่ให้ความยินยอม 2. หลีกเลี่ยงการถ่ายใบหน้าผู้ที่ปฏิเสธ	Consent
หลังถ่ายภาพ	1. เก็บไฟล์ในระบบที่ปลอดภัย (RBAC) 2. ลบไฟล์ที่ไม่ได้ใช้ภายใน 30 วัน 3. บันทึก Log การเข้าถึง	Storage Limitation
การเผยแพร่	1. ตรวจสอบว่าไม่ละเมิดสิทธิ์ 2. ไม่ใช้เพื่อการค้าโดยไม่ยินยอม 3. มี Watermark "KMUTNB Library"	Purpose Limitation

แบบฟอร์ม Consent Form:

```
แบบฟอร์มความยินยอมในการถ่ายภาพ/วิดีโอ
=====================================

ข้าพเจ้า .....
รหัสนักศึกษา .....
คณะ/สาขา .....

ยินยอม ☐ / ไม่ยินยอม ☐ ให้สำนักหอสมุดกลาง มจพ. ถ่ายภาพ/วิดีโอ
ของข้าพเจ้าในกิจกรรม .....

วัตถุประสงค์การใช้งาน:
☐ ประชาสัมพันธ์กิจกรรมของห้องสมุด
☐ ใช้ในเว็บไซต์/สื่อออนไลน์ของสำนักหอสมุดกลาง
☐ ใช้ในรายงานประจำปี/รายงาน TQA
☐ ใช้ในการวิจัย (ไม่เปิดเผยตัวตน)

ระยะเวลาเก็บข้อมูล: 2 ปี นับจากวันที่ถ่ายภาพ

สิทธิ์ของข้าพเจ้า:
1. ขอเข้าถึงข้อมูลส่วนบุคคล
2. ขอแก้ไขข้อมูลให้ถูกต้อง
3. ขอถอนความยินยอม (โดยส่งอีเมลถึง pdpa@lib.kmutnb.ac.th)
4. ร้องเรียนต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ลงชื่อ .....
วันที่ ...../...../.....
```

💻 กิจกรรมที่ 2: ระบบสารสนเทศ (Smart Lib Portal, Smart Room, Virtual Tour)

ผู้รับผิดชอบ: นายปิยะเดช กิจผดุง

ระบบ	ข้อมูลที่เก็บ	มาตรการคุ้มครอง
Smart Lib Portal	ชื่อ, รหัสนักศึกษา, ประวัติการยืม	- ใช้ HTTPS/TLS 1.3 - เข้ารหัสรหัสผ่าน (bcrypt) - RBAC (Role-Based Access Control) - Audit Log ทุกการเข้าถึง
Smart Room Booking	ชื่อ, รหัสนักศึกษา, เวลาใช้งาน	- ใช้ SSO (Single Sign-On) - ลบข้อมูลอัตโนมัติหลัง 1 ปี - ไม่เก็บ IP Address
Virtual Tour	IP Address, Cookie, User Agent	- Cookie Consent Banner - ไม่เก็บข้อมูลส่วนบุคคล - ใช้ Anonymous Analytics
AI Jinny X	คำถาม, Session ID	- ไม่เก็บข้อมูลส่วนบุคคลใน Chat Log - ลบ Log อัตโนมัติหลัง 1 ปี - ไม่ส่งข้อมูลไปยัง External API

📊 กิจกรรมที่ 3: การวิจัย/สำรวจความพึงพอใจ

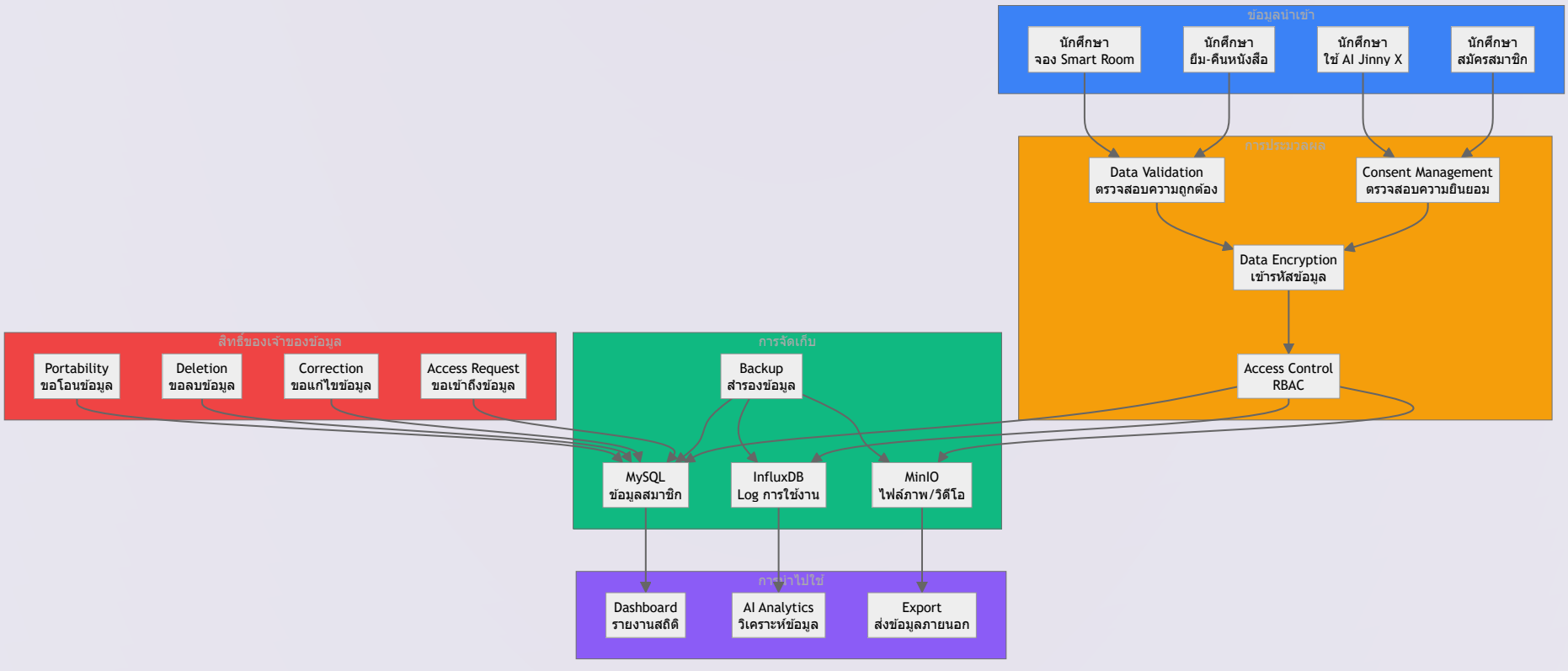
ผู้รับผิดชอบ: นายยุทธชัย สมมุติ

ขั้นตอน	การปฏิบัติ	ฐานกฎหมาย
ก่อนเก็บข้อมูล	1. แจ้งวัตถุประสงค์การวิจัย 2. ขอ Ethics Approval (ถ้าจำเป็น) 3. ขอ Consent จากผู้เข้าร่วม	Consent
ระหว่างเก็บข้อมูล	1. เก็บข้อมูลแบบ Anonymous (ถ้าเป็นไปได้) 2. เข้ารหัสไฟล์ข้อมูล 3. เก็บใน Server ที่ปลอดภัย	Data Minimization
หลังเก็บข้อมูล	1. ลบข้อมูลที่ระบุตัวตนหลังวิเคราะห์เสร็จ 2. เก็บเฉพาะข้อมูลสรุป (Aggregate Data) 3. ทำลายข้อมูลต้นฉบับหลัง 3 ปี	Storage Limitation
การเผยแพร่	1. นำเสนอในรูปแบบ Aggregate 2. ไม่เปิดเผยข้อมูลส่วนบุคคล 3. ระบุแหล่งที่มาอย่างชัดเจน	Purpose Limitation

---

3. 📐 สถาปัตยกรรมระบบสารสนเทศ PDPA Compliance

3.1 Data Flow Diagram

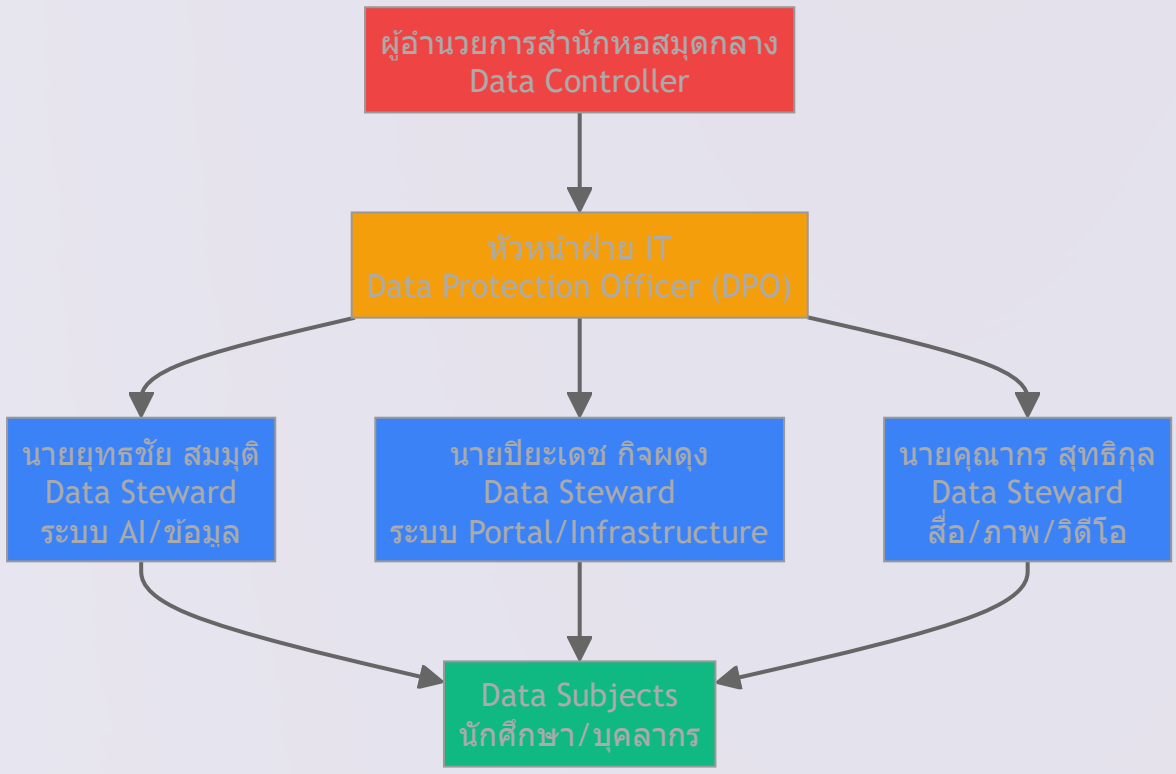


3.2 Privacy by Design

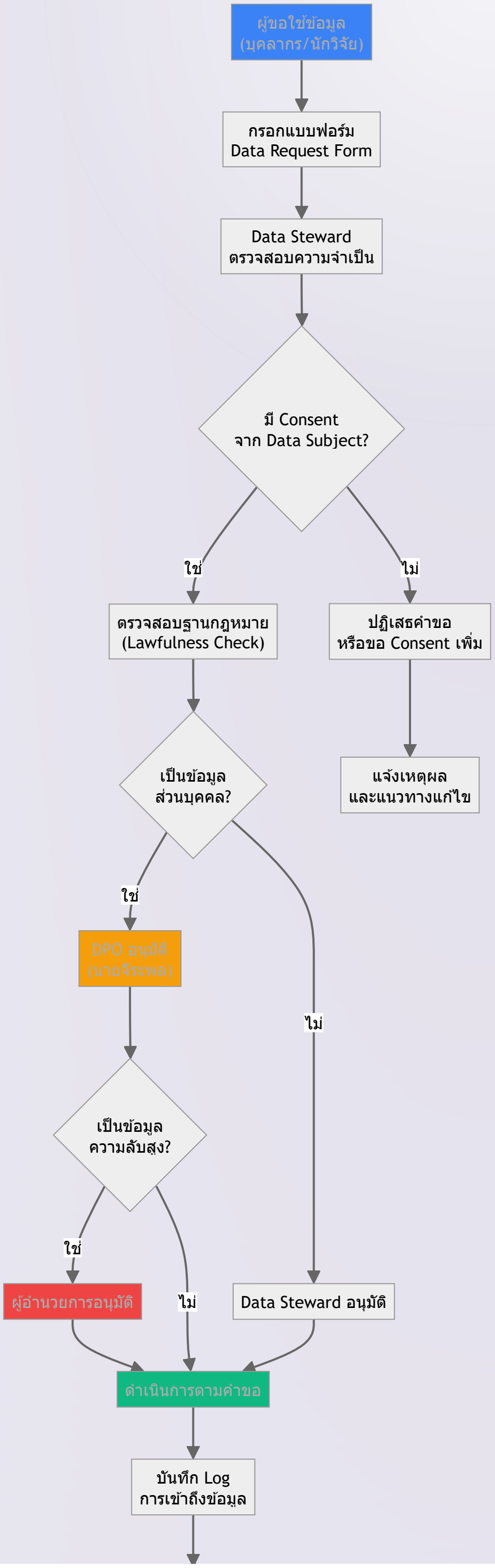
หลักการ	การนำไปใช้	ผู้รับผิดชอบ
Data Minimization	เก็บเฉพาะข้อมูลที่จำเป็นเท่านั้น (เช่น ไม่เก็บเลขบัตรประชาชน)	ปิยะเดช
Purpose Limitation	ใช้ข้อมูลตามวัตถุประสงค์ที่แจ้งไว้เท่านั้น	ยุทธชัย
Storage Limitation	ลบข้อมูลอัตโนมัติหลังครบระยะเวลา (Cron Job)	ปิยะเดช
Access Control	RBAC (Role-Based Access Control) สำหรับทุกระบบ	ปิยะเดช
Encryption	เข้ารหัสข้อมูลขณะพัก (AES-256) และขณะส่ง (TLS 1.3)	ปิยะเดช
Audit Trail	บันทึก Log ทุกการเข้าถึงข้อมูล (InfluxDB)	ปิยะเดช
Consent Management	ระบบจัดการความยินยอมแบบ Centralized	ยุทธชัย

4. 🔄 Flow การอนุมัติตามความรับผิดชอบ (Data Governance)

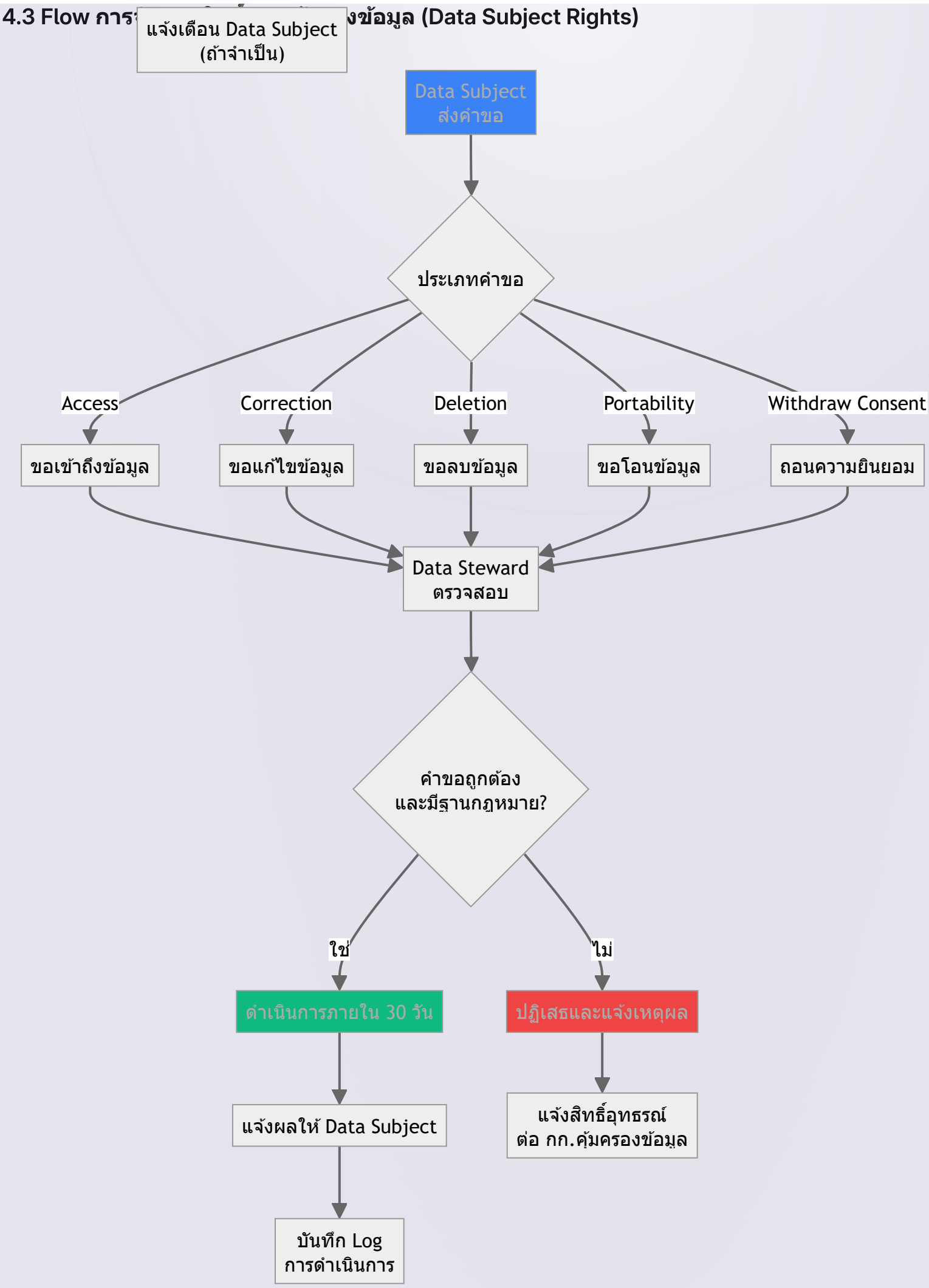
4.1 โครงสร้าง Data Governance



4.2 Flow การอนุมัติการเข้าถึง/ใช้ข้อมูล

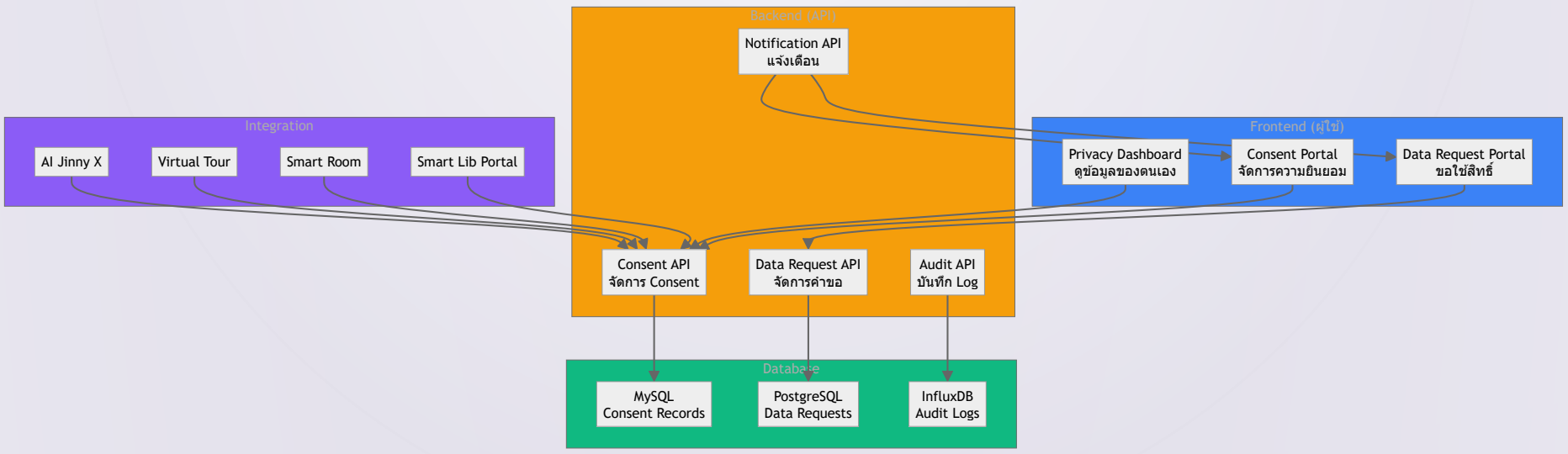

ผู้ขอใช้ข้อมูล (บุคลากร/นักวิจัย)
กรอกแบบฟอร์ม Data Request Form
Data Steward ตรวจสอบความจำเป็น
มี Consent จาก Data Subject?
ใช่
ไม่
ตรวจสอบฐานกฎหมาย (Lawfulness Check)
ปฏิเสธคำขอ หรือขอ Consent เพิ่ม
เป็นข้อมูลส่วนบุคคล?
แจ้งเหตุผลและแนวทางแก้ไข
ใช่
ไม่
DPO อนุมัติ (นายจีระพล)
เป็นข้อมูลความลับสูง?
ใช่
ไม่
ผู้อำนวยการอนุมัติ
Data Steward อนุมัติ
ดำเนินการตามคำขอ
บันทึก Log การเข้าถึงข้อมูล

4.3 Flow การ[illegible]งข้อมูล (Data Subject Rights)



5. 💻 ระบบสารสนเทศ PDPA Compliance

5.1 สถาปัตยกรรมระบบ



5.2 ฟีเจอร์หลักของระบบ

🎯 ฟีเจอร์ที่ 1: Consent Management System

ผู้รับผิดชอบ: นายยุทธชัย สมมุติ

```
-- ตัวอย่าง Database Schema
CREATE TABLE consent_records (
    id SERIAL PRIMARY KEY,
    student_id VARCHAR(20) NOT NULL,
    activity_type VARCHAR(50) NOT NULL,
    purpose TEXT NOT NULL,
    consent_given BOOLEAN NOT NULL,
    consent_date TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
    withdrawal_date TIMESTAMP NULL,
    data_retention_period INTERVAL DEFAULT '2 years',
    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
    updated_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP
);

CREATE INDEX idx_student_consent ON consent_records(student_id, activity_type);
```

API Endpoints:

```
POST /api/consent/give          # ให้ความยินยอม
POST /api/consent/withdraw      # ถอนความยินยอม
GET  /api/consent/status/:id    # ตรวจสอบสถานะ
GET  /api/consent/history/:id   # ประวัติความยินยอม
```

🎯 ฟีเจอร์ที่ 2: Data Request Management System

ผู้รับผิดชอบ: นายปิยะเดช กิจผดุง

```
CREATE TABLE data_requests (
    id SERIAL PRIMARY KEY,
    requester_id VARCHAR(20) NOT NULL,
    request_type VARCHAR(50) NOT NULL,  -- access, correction, deletion, portability
    data_subject_id VARCHAR(20) NOT NULL,
    description TEXT NOT NULL,
    status VARCHAR(20) DEFAULT 'pending',  -- pending, approved, rejected, completed
    approved_by VARCHAR(20) NULL,
    approval_date TIMESTAMP NULL,
    completion_date TIMESTAMP NULL,
    notes TEXT NULL,
    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP
);
```

Workflow:

1. ผู้ใช้ส่งคำขอผ่าน Portal
2. Data Steward ตรวจสอบและแนะนำ
3. DPO อนุมัติ (ถ้าจำเป็น)
4. ดำเนินการและแจ้งผล
5. บันทึก Log และแจ้งเตือน

🎯 ฟีเจอร์ที่ 3: Audit Trail & Monitoring

ผู้รับผิดชอบ: นายปิยะเดช กิจผดุง

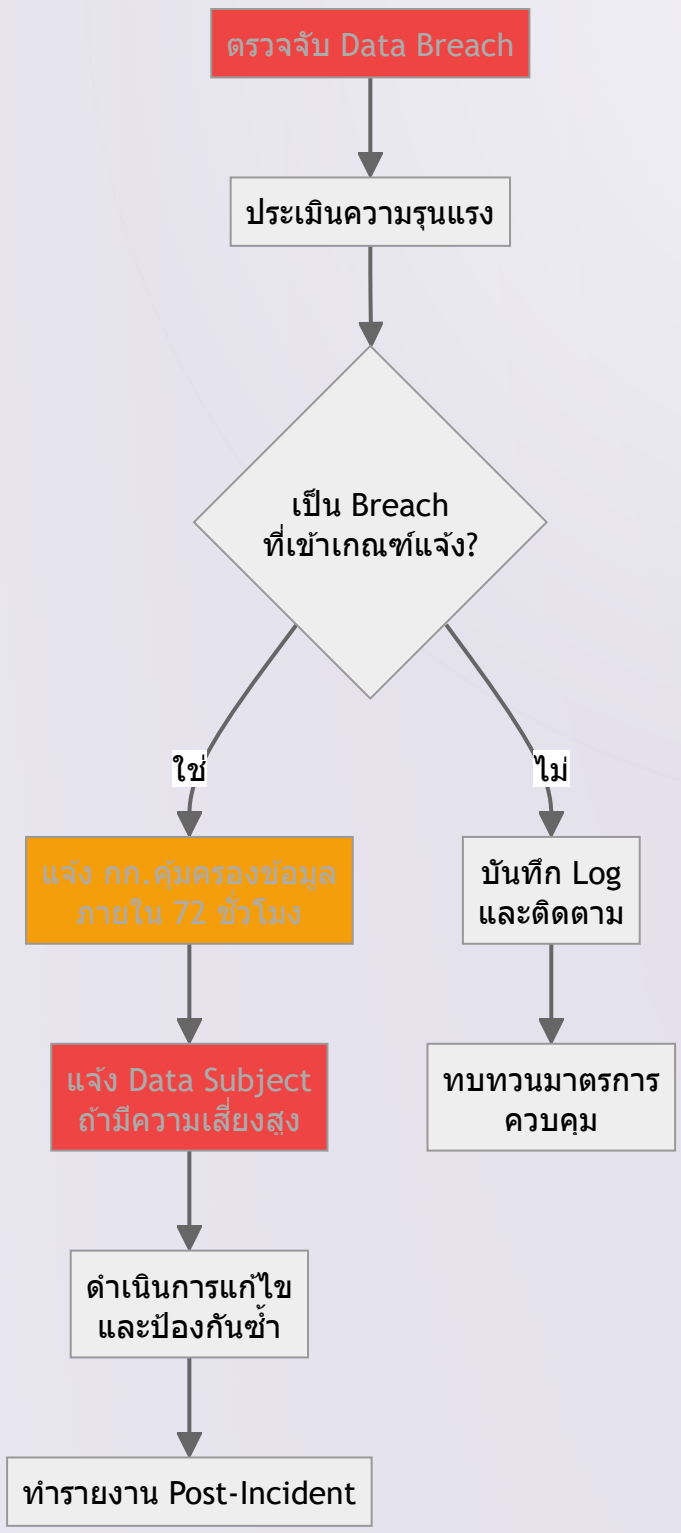
```
-- InfluxDB Schema
measurement: "data_access_log"
tags:
  - user_id
  - data_type
  - action
  - ip_address
fields:
  - timestamp
  - duration_ms
  - records_accessed
  - success (boolean)
```

Dashboard:

- แสดงจำนวนการเข้าถึงข้อมูลแบบ Real-time
- แจ้งเตือนเมื่อมีการเข้าถึงผิดปกติ (Anomaly Detection)
- รายงานการปฏิบัติตาม PDPA รายเดือน

🎯 ฟีเจอร์ที่ 4: Data Breach Notification System

ผู้รับผิดชอบ: นายจีระพล คุ่มเคี่ยม (หัวหน้าฝ่าย)



---

6. 🔗 การบูรณาการกับระบบเดิม

6.1 ระบบที่ต้องปรับปรุง

ระบบ	การปรับปรุง	ผู้รับผิดชอบ	ระยะเวลา
Smart Lib Portal	เพิ่ม Consent Banner, Privacy Policy Link	ปิยะเดช	Q1/2570
Smart Room Booking	เพิ่ม Consent Checkbox, Auto-Delete	ปิยะเดช	Q1/2570
Virtual Tour	เพิ่ม Cookie Consent, Anonymous Analytics	คุณากร	Q2/2570
AI Jinny X	เพิ่ม Privacy Notice, Auto-Delete Log	ยุทธชัย	Q2/2570
Library Tour	เพิ่ม Consent Form, Secure Storage	คุณากร	Q1/2570

6.2 ตัวอย่างการบูรณาการ Consent API

```javascript
// ตัวอย่างโค้ด JavaScript สำหรับ Smart Lib Portal
async function checkConsent(studentId, activityType) {
    const response = await fetch(`/api/consent/status/${studentId}?activity=${activityType}`);
    const data = await response.json();

    if (!data.consent_given) {
        showConsentModal(activityType);
        return false;
    }

    return true;
}
```

```
async function giveConsent(studentId, activityType, purpose) {
    const response = await fetch('/api/consent/give', {
        method: 'POST',
        headers: { 'Content-Type': 'application/json' },
        body: JSON.stringify({
            student_id: studentId,
            activity_type: activityType,
            purpose: purpose
        })
    });

    return await response.json();
}
```

7. 📂 Evidence Checklist สำหรับ TQA

📂 หมวด 1: การนำองค์กร (Leadership)

- [ ] **PDPA Policy:** นโยบายคุ้มครองข้อมูลส่วนบุคคลของสำนักหอสมุดกลาง
- [ ] **Data Governance Structure:** โครงสร้าง Data Governance (Data Controller, DPO, Data Stewards)
- [ ] **Privacy Notice:** ประกาศความเป็นส่วนตัวบนเว็บไซต์

📂 หมวด 2: กลยุทธ์ (Strategy)

- [ ] **Data Protection Impact Assessment (DPIA):** การประเมินผลกระทบสำหรับระบบใหม่
- [ ] **Risk Treatment Plan:** CL-RTP-03 (RBAC + Audit Log), CL-RTP-05 (อบรม PDPA)
- [ ] **Consent Management Strategy:** กลยุทธ์การจัดการความยินยอม

📂 หมวด 4: การวัดและวิเคราะห์ (Measurement)

- [ ] **Consent Management Dashboard:** Dashboard แสดงสถานะความยินยอม
- [ ] **Audit Trail Reports:** รายงานการเข้าถึงข้อมูล
- [ ] **Data Request Reports:** รายงานคำขอใช้สิทธิ์ของ Data Subjects

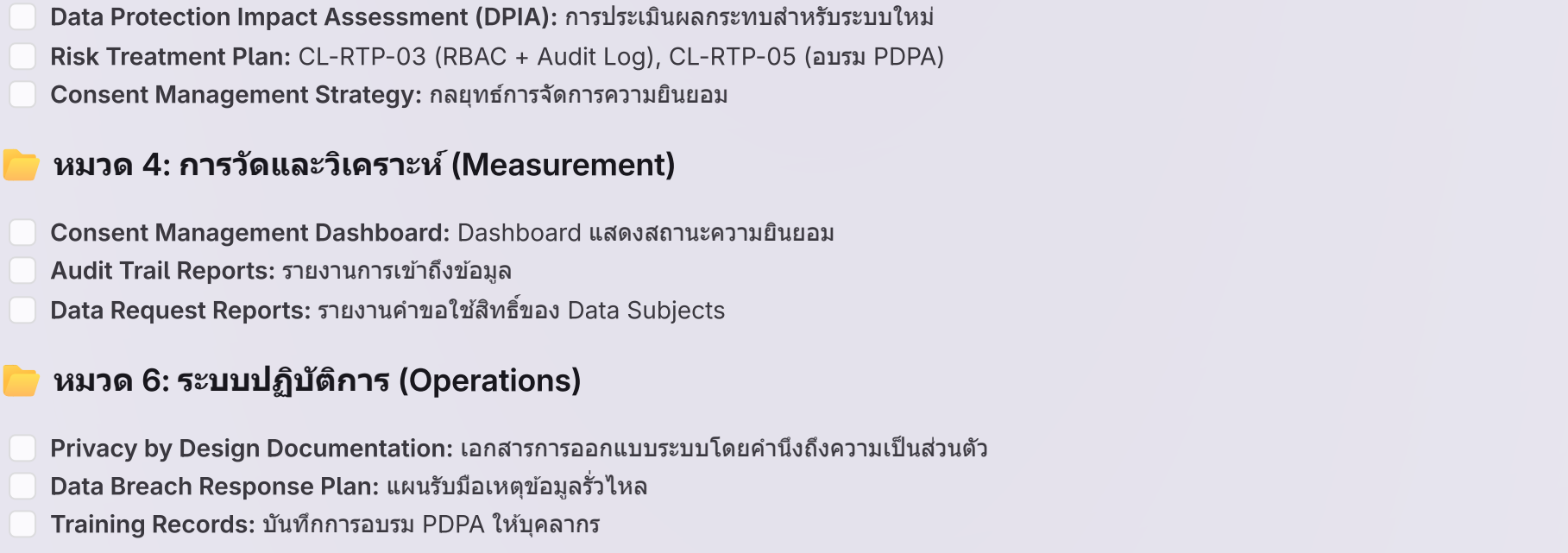
📂 หมวด 6: ระบบปฏิบัติการ (Operations)

- [ ] **Privacy by Design Documentation:** เอกสารการออกแบบระบบโดยคำนึงถึงความเป็นส่วนตัว
- [ ] **Data Breach Response Plan:** แผนรับมือเหตุข้อมูลรั่วไหล
- [ ] **Training Records:** บันทึกการอบรม PDPA ให้บุคลากร

📂 หมวด 7: ผลลัพธ์ (Results)

- [ ] **Consent Rate:** ร้อยละของการได้รับความยินยอม
- [ ] **Data Request Resolution Time:** ระยะเวลาเฉลี่ยในการจัดการคำขอ
- [ ] **Data Breach Incidents:** จำนวนเหตุการณ์ข้อมูลรั่วไหล (เป้าหมาย = 0)

8. 🗓️ แผนการดำเนินการ (Roadmap 2570)



9. 💡 ข้อแนะนำเชิงปฏิบัติ

9.1 สำหรับหัวหน้าฝ่าย (นายจีระพล)

1. **แต่งตั้ง DPO อย่างเป็นทางการ:** ออกประกาศแต่งตั้งนายจีระพลเป็น Data Protection Officer (DPO) ของสำนักหอสมุดกลาง
2. **จัดอบรม PDPA:** จัดอบรมเชิงปฏิบัติการให้บุคลากรทุกคนภายใน Q1/2570 (ตาม CL-RTP-05)
3. **ของบประมาณ:** ของบประมาณสำหรับพัฒนา Consent Management System และ Audit Trail Dashboard
4. **ทำ DPIA:** ดำเนินการ Data Protection Impact Assessment สำหรับระบบใหม่ทุกโครงการ

9.2 สำหรับทีมงาน IT

1. **นายยุทธชัย (Data Steward - AI/Data):**
   - พัฒนา Consent Management API
   - ปรับปรุง AI Jinny X ให้เป็น Privacy by Design
   - จัดทำ Privacy Notice สำหรับระบบ AI
2. **นายปิยะเดช (Data Steward - Infrastructure):**
   - พัฒนาระบบ Audit Trail (InfluxDB)
   - ปรับปรุง Smart Lib Portal และ Smart Room
   - จัดทำ RBAC Matrix สำหรับทุกระบบ
3. **นายคุณากร (Data Steward - Media):**
   - จัดทำ Consent Form สำหรับกิจกรรมถ่ายภาพ/วิดีโอ
   - ปรับปรุง Virtual Tour ให้มี Cookie Consent
   - จัดทำ Secure Storage สำหรับไฟล์ภาพ/วิดีโอ

9.3 Quick Wins (3 เดือนแรก)

- ✅ **อบรม PDPA ให้บุคลากรทุกคน** (ต.ค. 69)
- ✅ **ติดตั้ง Consent Banner** บนเว็บไซต์หลัก (พ.ย. 69)
- ✅ **พัฒนา Consent Form** สำหรับ Library Tour (ธ.ค. 69)
- ✅ **ติดตั้ง Audit Log** บน Smart Lib Portal (ธ.ค. 69)

---

10. 📊 ตัวชี้วัดความสำเร็จ (KPIs)

ตัวชี้วัด	ค่าเป้าหมาย 2570	วิธีการวัด
Consent Rate	≥ 95%	ร้อยละของกิจกรรมที่ได้รับความยินยอม
Data Request Resolution Time	≤ 30 วัน	ระยะเวลาเฉลี่ยในการจัดการคำขอ
Data Breach Incidents	0 ครั้ง	จำนวนเหตุการณ์ข้อมูลรั่วไหล
PDPA Training Coverage	100%	ร้อยละของบุคลากรที่ผ่านการอบรม
Audit Trail Coverage	100%	ร้อยละของระบบที่มี Audit Log
Privacy by Design Compliance	100%	ร้อยละของระบบใหม่ที่ผ่าน DPIA

---

11. 🔗 การเชื่อมโยงกับ Risk Management

Risk ID	ความเสี่ยง	มาตรการ PDPA	สถานะ
CL-RA-01	Data Leakage	RBAC + Audit Log + Encryption	🔄 กำลังดำเนินการ (CL-RTP-03)
CL-RA-07	ขาดความรู้ PDPA	อบรม PDPA เชิงปฏิบัติการ	📅 กำหนด ส.ค. 2569 (CL-RTP-05)
PDPA-NEW-01	ไม่ได้รับความยินยอม	Consent Management System	📅 กำหนด Q1/2570
PDPA-NEW-02	ไม่สามารถจัดการสิทธิ์ได้	Data Request Portal	📅 กำหนด Q2/2570

> **เอกสารนี้จัดทำในรูปแบบ Markdown + Mermaid รองรับ GitLab Native Rendering**
> **เวอร์ชัน:** 1.0 (PDPA Compliance System) | **วันที่:** ตุลาคม 2569
> **ผู้จัดทำ:** นายจีระพล คุ่มเคี่ยม | **หน่วยงาน:** ฝ่ายเทคโนโลยีสารสนเทศและนวัตกรรมทางการศึกษา
> **การทบทวนถัดไป:** หลังการอบรม PDPA เดือนตุลาคม 2569

💡 คำแนะนำสำหรับการอัปโหลด GitLab:

- คัดลอกโค้ดทั้งหมดไปวางในไฟล์ `.md` (เช่น `pdpa-compliance-system.md`)
- GitLab จะ render Mermaid diagram โดยอัตโนมัติ
- ใช้เอกสารนี้เป็น **Master Reference** สำหรับการใช้งาน PDPA ในสำนักหอสมุดกลาง

หากต้องการให้ผมจัดทำ **Template Consent Form** หรือ **Privacy Notice Template** สำหรับกิจกรรมต่างๆ แจ้งได้เลยครับ! 🎯