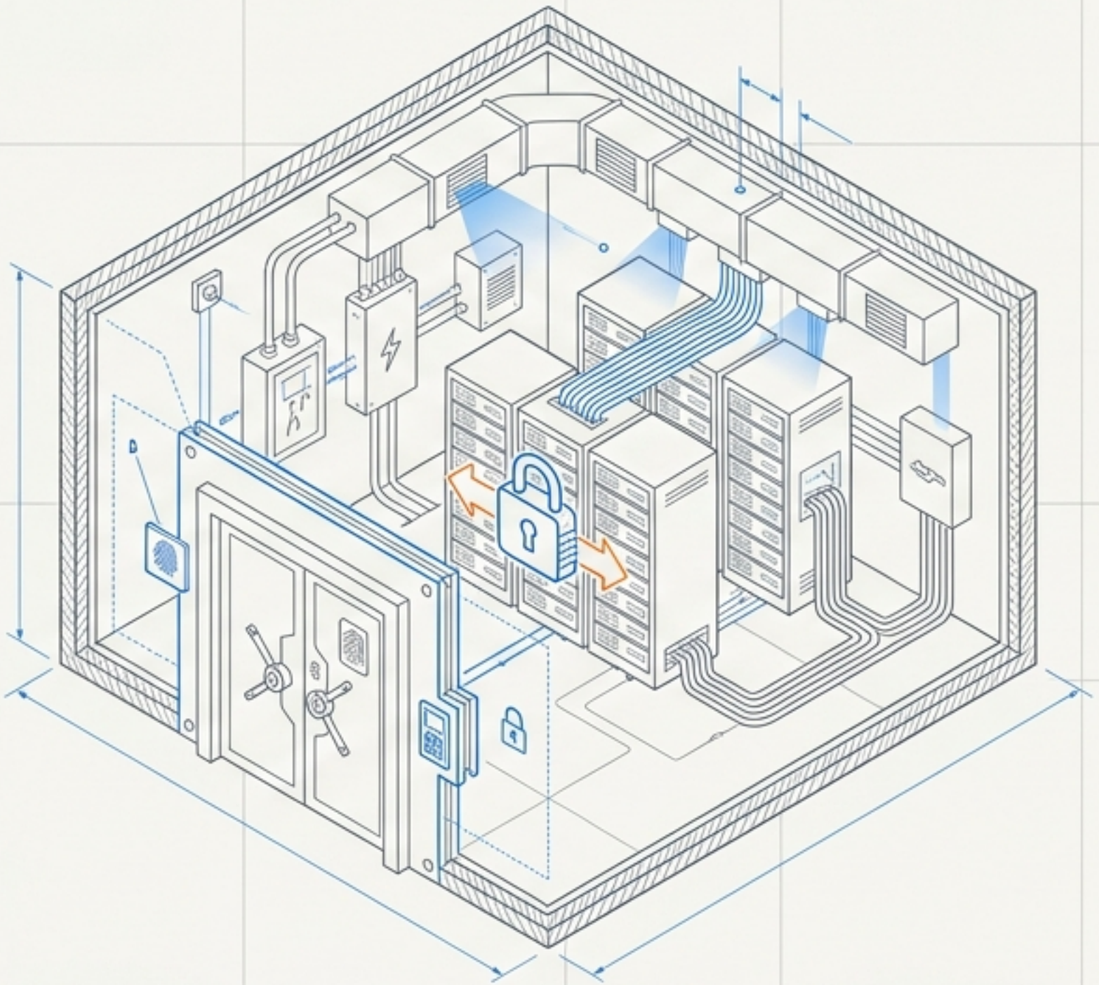
PDPA Master Checklist for IT Admins

เช็กลิสต์และข้อปฏิบัติเชิงเทคนิคเพื่อการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล



5 กฎเหล็กรายวัน: The Frontline Defense Protocol

แจ้งเหตุฉุกเฉิน (Report Breaches)

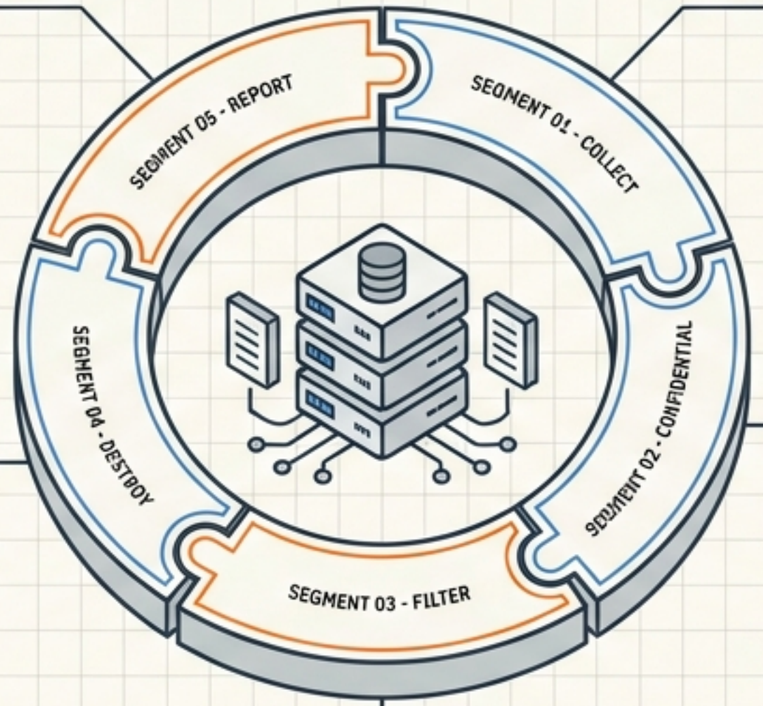
หากข้อมูลรั่วไหลหรือส่งผิด ต้องแจ้ง DPO หรือนิติกรภายใน 72 ชั่วโมง เพื่อระงับความเสียหายทันที

CRITICAL ALERT PATHWAY 05

รวบรวมเท่าที่จำเป็น (Collect Minimally)

จัดเก็บเฉพาะตามวัตถุประสงค์งาน ไม่เก็บข้อมูลส่วนเกิน และแจ้งสิทธิให้ทราบเสมอ

PATHWAY 01



ทำลายอย่างถูกวิธี (Proper Destruction)

ย่อยทำลายเอกสารเมื่อหมดความจำเป็น ห้ามทิ้งลงถังขยะปกติหรือขายเป็นกระดาษรีไซเคิลเด็ดขาด

DATA FLOW 01

รักษาความลับขั้นสุด (Strict Confidentiality)

ล็อกหน้าจอ เก็บรักษาพาสเวิร์ด ไม่แชร์บัญชีผู้ใช้ และห้ามใช้กระดาษ Reuse ที่มีข้อมูลส่วนตัว

DATA FLOW 02

DATA FLOW 03

คัดกรองก่อนส่งต่อ (Filter Before Forwarding)

ตรวจสอบความถูกต้องก่อนส่งอีเมลหรือไฟล์ในกลุ่ม Line ห้ามเผยแพร่แก่บุคคลภายนอกโดยพลการ

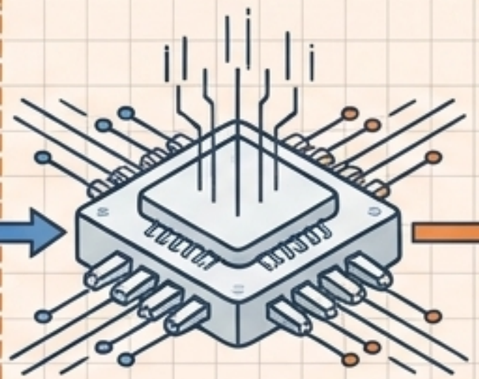
The 8-Pillar Implementation Blueprint

System Foundation
(โครงสร้างพื้นฐานและนโยบาย)

1. ด้านสัญญาและข้อตกลง

8. การบริหารจัดการภายใน

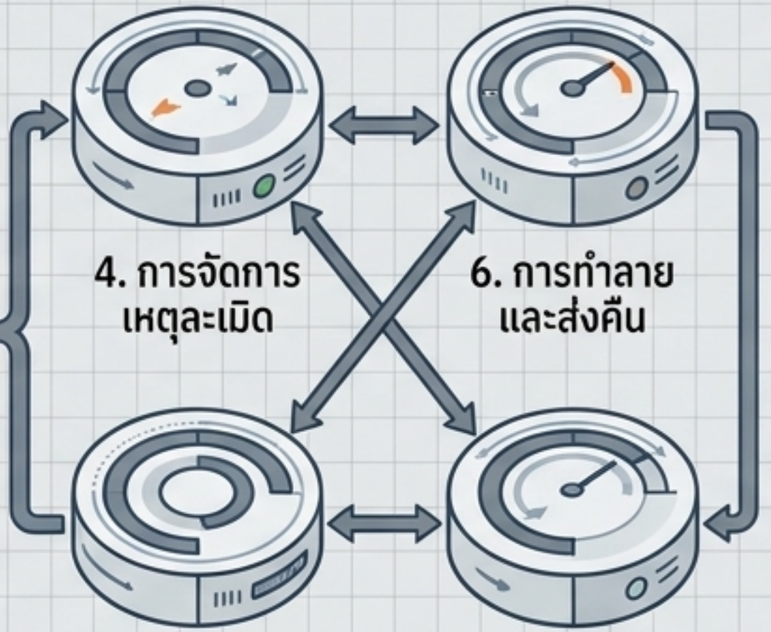
Active Operations
(การจัดการและปกป้องข้อมูล)



2. วิธีการจัดเก็บข้อมูล

3. มาตรการความปลอดภัย

Monitoring & Lifecycle
(การตรวจสอบและวงจรชีวิตข้อมูล)



4. การจัดการเหตุละเมิด

6. การทำลายและส่งคืน

5. การบันทึกรายการกิจกรรม (ROPA)

7. การจัดการสิทธิ

Foundation & Governance: ขอบเขตอำนาจหน้าที่

External Protocols (Contracts & DPA)

สัญญาเป็นลายลักษณ์อักษร:
ต้องมีข้อตกลง (DPA) กับผู้ควบคุมข้อมูลส่วนบุคคลที่ชัดเจน

ทำตามคำสั่งอย่างเคร่งครัด:
ห้ามนำข้อมูลไปใช้นอกเหนือจากที่ระบุในสัญญา ขอบเขตภาระงาน หรือวัตถุประสงค์ที่แจ้งไว้

การจ้างช่วง (Sub-contractors):
หากมีการว่าจ้างผู้ดูแลระบบช่วงต่อ ต้องได้รับความยินยอมจากผู้ควบคุมข้อมูลฯ ก่อนเสมอ

Internal Protocols (Governance)

รักษาความลับ (Confidentiality):
ถือปฏิบัติอย่างเคร่งครัดต่อข้อมูลส่วนบุคคลที่เข้าถึงตามหน้าที่

อัปเดตความรู้สม่ำเสมอ:
เข้ารับการอบรมด้าน PDPA และความปลอดภัยไซเบอร์เพื่อรับมือภัยคุกคามใหม่ๆ

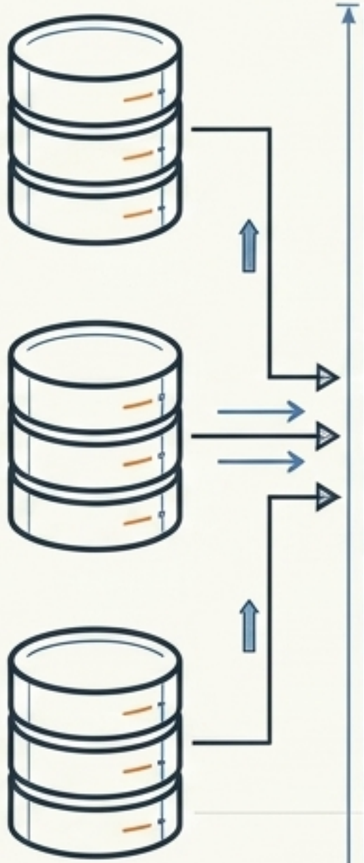
UNIFIED FOUNDATION

Storage Architecture & Data Segregation

Data Routing (Separation):
แยกฐานข้อมูล (Database) ตามแผนกหรือโครงการ ป้องกันการเข้าถึงข้ามส่วนงานโดยไม่มีอำนาจหน้าที่

Routing Hub

Data Routing (Separation):
แยกฐานข้อมูล (Database) ตามแผนกหรือโครงการ ป้องกันการเข้าถึงข้ามส่วนงานโดยไม่มีอำนาจหน้าที่

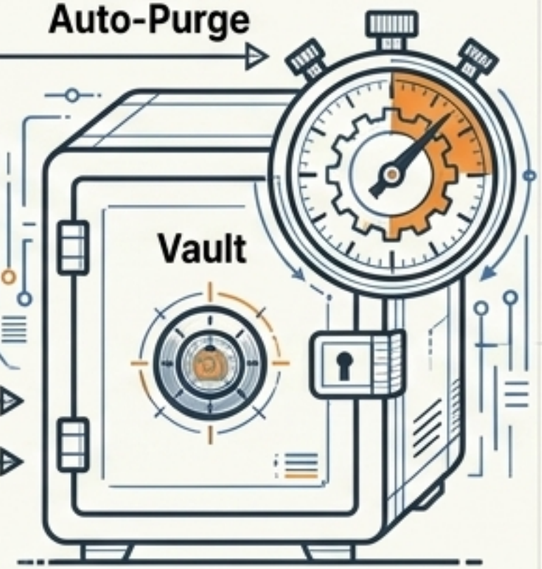


Server Standards (Cloud & On-Prem):

Server Standards (Cloud & On-Prem):

- **Cloud:** ตรวจสอบสถานที่ตั้ง Server และมาตรฐานรับรอง (PDPA/GDPR)
- **On-Premise:** ควบคุมการเข้าออกห้อง Server อย่างเข้มงวด (Key card/CCTV) และมีระบบป้องกันอัคคีภัย

Auto-Purge

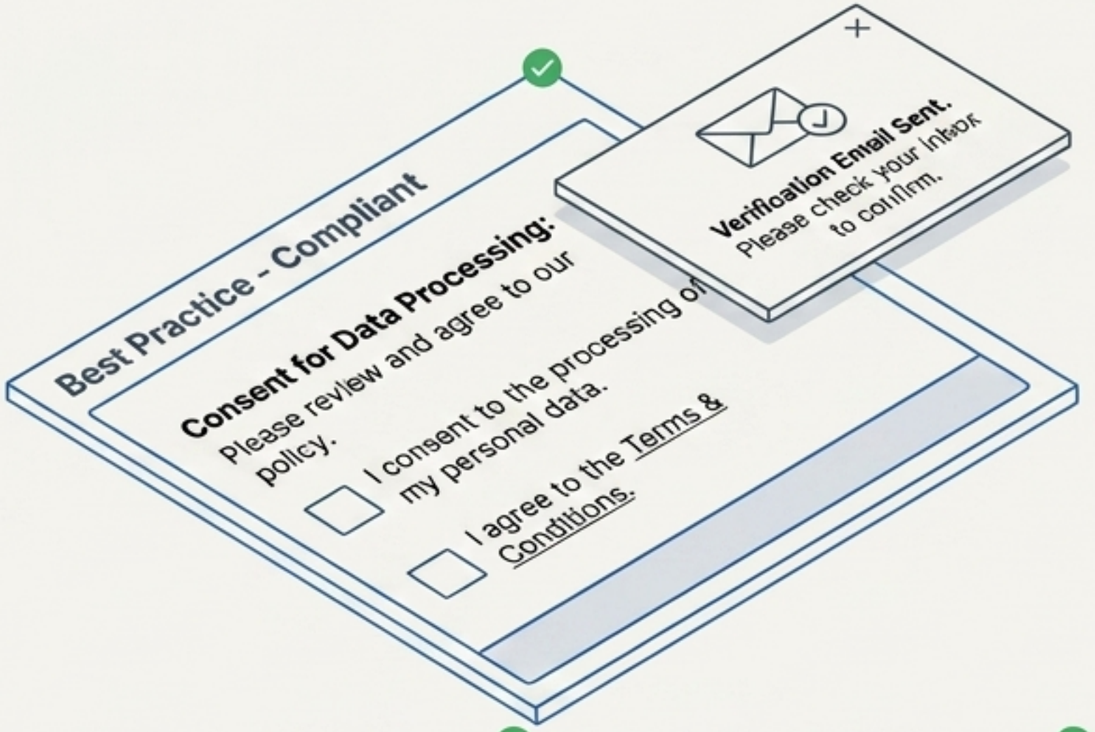


Lifecycle Rules:

- **Auto-purge:** ตั้งค่าระบบลบข้อมูลอัตโนมัติเมื่อครบกำหนดตามสัญญา
- **Secure Backup:** ข้อมูลสำรองต้องได้รับความคุ้มครองเท่าเทียมกัน และต้องถูกลบด้วยเมื่อมีการใช้สิทธิ Right to Erasure

Legal Consent Mechanisms in UI/UX

รูปแบบการขอความยินยอมที่ถูกต้องตามกฎหมาย

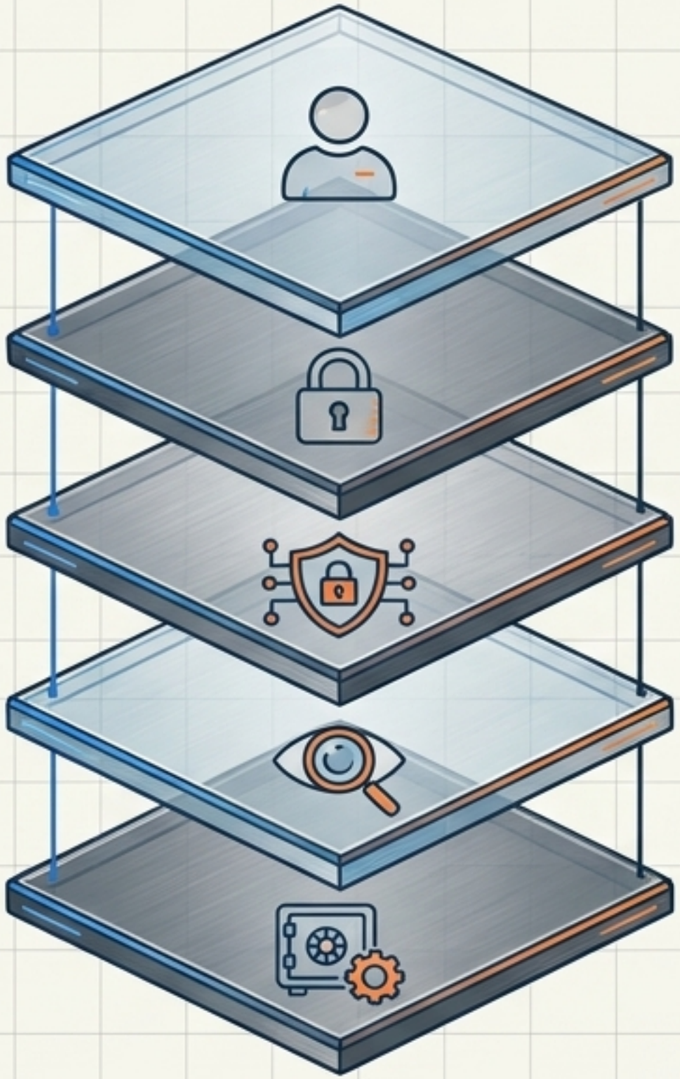


1. Click-to-Accept: เจ้าของข้อมูลต้องเป็นคนกดเลือกเองเท่านั้น

2. Double Opt-in: ส่งอีเมลยืนยันตัวตนอีกครั้งหลังสมัครในเว็บไซต์

3. Clear Separation: แยกส่วนความยินยอมออกจาก Terms & Conditions ชัดเจน ใช้ภาษาเข้าใจง่าย

The Security Measures Framework (SOC Stack)



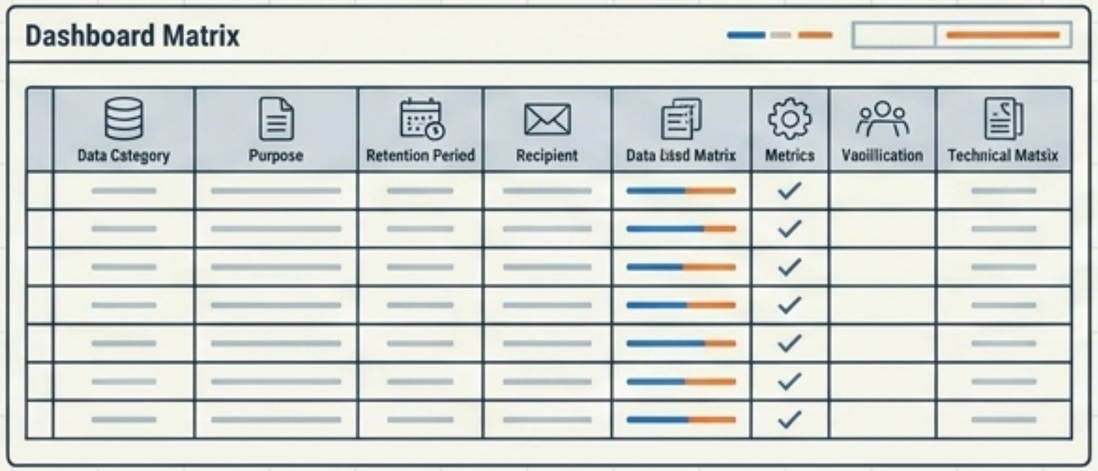
- **Layer 1: Authentication -** ใช้ระบบยืนยันตัวตนแบบ Multi-Factor Authentication (MFA) สำหรับการเข้าถึงระบบฐานข้อมูล
- **Layer 2: Access Control -** กำหนดสิทธิ์ตามหลัก Least Privilege (ให้สิทธิ์เฉพาะเท่าที่จำเป็นต่อการปฏิบัติงานเท่านั้น)
- **Layer 3: Encryption -** เข้ารหัสข้อมูลทั้งขณะรับส่งข้อมูล (In transit) และขณะจัดเก็บ (At rest)
- **Layer 4: Logging & Monitoring -** บันทึก Log files เพื่อตรวจสอบย้อนหลัง (ใคร, เข้าถึงอะไร, เมื่อใด)
- **Layer 5: Backup & Recovery -** สำรองข้อมูลสม่ำเสมอ และทดสอบแผนการกู้คืนเพื่อให้ระบบพร้อมใช้งาน (Availability) เสมอ

Active Monitoring: Breach Incident SOP & ROPA

Data Breach Management (SOP)

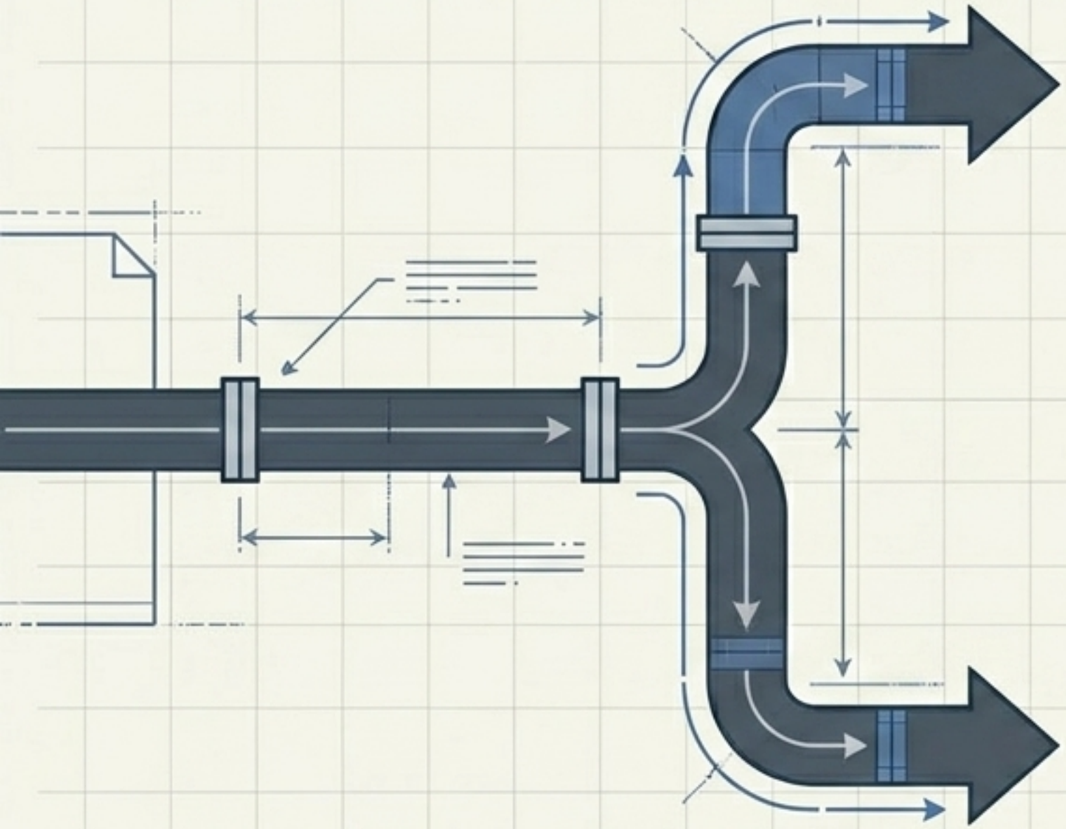
- จัดทำขั้นตอนการปฏิบัติงาน (SOP) สำหรับรับมือข้อมูลรั่วไหล
- เมื่อพบเหตุต้องสงสัย ต้องแจ้งผู้ควบคุมข้อมูลทันที (ภายใน 24-72 ชั่วโมง)

Record of Processing (ROPA)



- จัดทำและอัปเดตบัญชีรายการกิจกรรม (ROPA) ให้เป็นปัจจุบัน
- ระบุ: ประเภทข้อมูล, วัตถุประสงค์, และระยะเวลาจัดเก็บ
- Special Requirement: ข้อมูลอ่อนไหว/อาชญากรรม ต้องมีการบันทึกการประมวลผลเป็นหนังสือหรือระบบอิเล็กทรอนิกส์อย่างเคร่งครัด

Data Lifecycle Management & Subject Rights

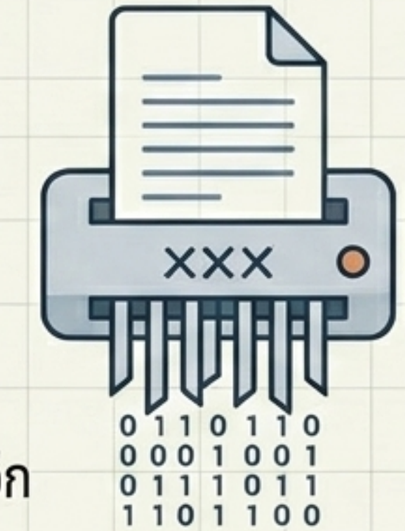


การจัดการสิทธิ (Data Subject Rights Readiness):

- เตรียมระบบให้พร้อมสนับสนุนผู้ควบคุมข้อมูล
- รองรับการขอใช้สิทธิของเจ้าของข้อมูล (เช่น ขอเข้าถึง, ขอระงับการใช้, ขอลบ) ภายในเวลาที่กฎหมายกำหนด

การทำลายและส่งคืน (Retention & Disposal):

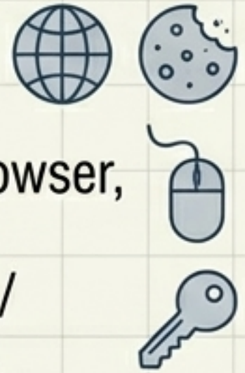
- เมื่อสิ้นสุดสัญญา/ภารกิจ ต้องลบ ทำลาย หรือส่งคืนข้อมูลทั้งหมด
- ใช้วิธี Data Sanitization ที่ได้มาตรฐาน เพื่อให้มั่นใจว่าไม่สามารถกู้คืนข้อมูลกลับมาได้อีก



The Data Asset Radar

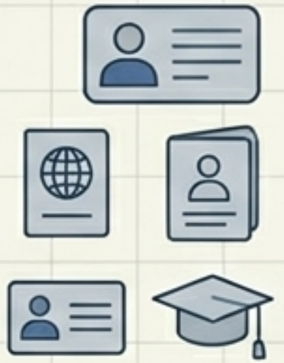
หมวดหมู่ข้อมูลที่ระบบ IT ต้องควบคุมดูแล

Quadrant 1: Digital Footprints (ร่องรอยดิจิทัล)



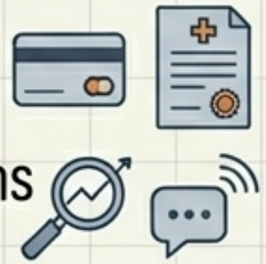
- หมายเลข IP Address, Cookies, Browser, Device ID, Time zone.
- การเข้าสู่ระบบ (Logins), Username/ Password, PIN, App activity logs.

Quadrant 2: Identity & Profile (ข้อมูลระบุตัวตนบุคคล)



- ข้อมูลรายละเอียดส่วนบุคคล และการระบุ/ยืนยันตัวตน.
- ข้อมูลการติดต่อ, การทำงาน, การศึกษา.

Quadrant 3: Behavioral & Commercial (พฤติกรรมและการทำธุรกรรม)



- ข้อมูลการเงิน และ การรับบริการ.
- ข้อมูลกรมธรรม์ประกันภัย.
- ข้อมูลวิจัยตลาด และ ข้อมูลการสื่อสาร (บันทึกสนทนา).

Quadrant 4: Highly Sensitive (ข้อมูลอ่อนไหว - ควบคุมพิเศษ)

ข้อมูลส่วนบุคคลประเภทอ่อนไหว (Sensitive Data) ต้องใช้มาตรการขั้นสูงสุดและบันทึก ROPA เสมอ.

Self-Audit Diagnostic Matrix

	ดำเนินการแล้ว (Done)	ยังไม่ได้ดำเนินการ (Not Done)
1. ทำสัญญา DPA และตรวจสอบเงื่อนไข Sub-processor แล้ว	☐	☐
2. แยก Database ตามแผนก และตั้งระบบลบอัตโนมัติ (Auto-purge)	☐	☐
3. UI/UX การขอความยินยอมไม่มีการติ๊กเลือกไว้ล่วงหน้า (No pre-tick)	☐	☐
4. Server และ Backup มีการเข้ารหัส (Encryption) และจำกัดการเข้าถึง (MFA)	☐	☐
5. มี SOP รับมือเหตุข้อมูลรั่วไหล และพร้อมแจ้งเหตุใน 72 ชม.	☐	☐
6. อัปเดต ROPA โดยเฉพาะการบันทึกข้อมูลประเภทอ่อนไหว	☐	☐
7. ระบบรองรับการลบ/ระงับข้อมูลตามสิทธิ (Data Subject Rights)	☐	☐
8. มีกระบวนการ Data Sanitization ที่กู้คืนไม่ได้เมื่อจบงาน	☐	☐

สถานะของระบบ IT ในปัจจุบันของคุณเป็นอย่างไร? นำเช็กลิสต์นี้ไปใช้ประเมินทันที