ROCyber

CYBER LAW & STANDARDS · PDPA ตอนที่ 5

การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

มาตรการขั้นต่ำที่กฎหมายกำหนด และวิธีแปลงเป็นการควบคุมจริงในระบบสารสนเทศขององค์กร

CIA | มาตรการขั้นต่ำ | ISO 27001

COLLECT	เก็บรวบรวม · ฐานทางกฎหมาย	ม.19–26
USE	ใช้ · ตามวัตถุประสงค์ที่แจ้ง	ม.21
DISCLOSE	เปิดเผย · ส่งต่อ · ต่างประเทศ	ม.27–29
PROTECT	รักษาความมั่นคงปลอดภัย	ม.37
RESPOND	แจ้งเหตุละเมิดภายใน 72 ชม.	ม.37(4)
ERASE	ลบ · ทำลาย · ทำให้ระบุตัวไม่ได้	ม.33

PERSONAL DATA LIFECYCLE · PDPA

อ้างอิง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศคณะกรรมการฯ · เนื้อหาเพื่อการศึกษา ไม่ใช่คำปรึกษาทางกฎหมาย

R0Cyber

กฎหมายกำหนดให้มี "มาตรการที่เหมาะสม"

ประกาศ สคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูล พ.ศ. 2565: กำหนดมาตรการขั้นต่ำที่ทุกองค์กรต้องมี

Confidentiality

ความลับ: เฉพาะผู้มีสิทธิเข้าถึงได้

Integrity

ความถูกต้องครบถ้วน: ไม่ถูกแก้ไขโดยมิชอบ

Availability

ความพร้อมใช้: ใช้ได้เมื่อจำเป็น ไม่สูญหาย

ตามความเสี่ยง	เข้มข้นตามความเสี่ยงของข้อมูลและกิจกรรม — ข้อมูลอ่อนไหวต้องเข้มกว่า
ทุกรูปแบบ	ครอบคลุมทั้งข้อมูลอิเล็กทรอนิกส์และเอกสารกระดาษ
ทบทวนเสมอ	ทบทวนเมื่อจำเป็น หรือเมื่อเทคโนโลยีเปลี่ยน

R0Cyber

มาตรการสามด้าน: บริหาร · เทคนิค · กายภาพ

ด้านบริหารจัดการ

- นโยบายและผู้รับผิดชอบ
- ประเมินความเสี่ยง
- กำหนดสิทธิ์ตามหน้าที่
- อบรมพนักงาน
- จัดการผู้ให้บริการ

ด้านเทคนิค

- ยืนยันตัวตน · MFA
- เข้ารหัสข้อมูล
- บันทึกและเฝ้าระวัง (log)
- สำรองข้อมูล
- แพตช์และป้องกันมัลแวร์

ด้านกายภาพ

- ควบคุมการเข้าห้องเซิร์ฟเวอร์
- ตู้เอกสารมีกุญแจ
- นโยบายโต๊ะสะอาด
- ทำลายเอกสารและสื่อบันทึก
- ป้องกันอุปกรณ์สูญหาย

ทั้งสามด้านต้องไปด้วยกัน — ระบบเข้ารหัสอย่างดี ก็ไร้ผลถ้าพนักงานพิมพ์รายชื่อลูกค้าแล้ววางทิ้งไว้

R0Cyber

องค์ประกอบที่ประกาศ สคส. ปี 2565 กำหนด

ควบคุมการเข้าถึง	ข้อมูล อุปกรณ์จัดเก็บ และอุปกรณ์ประมวลผล — ตามความจำเป็นและสิทธิ์
กำหนดสิทธิ์ผู้ใช้	ใครเข้าถึง แก้ไข ลบข้อมูลได้แค่ไหน
บริหารการเข้าถึงของผู้ใช้	เพิ่ม · ทบทวน · ถอนสิทธิ์ เมื่อย้ายงานหรือลาออก
หน้าที่ของผู้ใช้	ป้องกันการเข้าถึง เปิดเผย ลักลอบทำสำเนา หรือขโมยอุปกรณ์
ตรวจสอบย้อนหลังได้	บันทึกว่าใครเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูล
สร้างความตระหนักรู้	แจ้งนโยบายและฝึกอบรมบุคลากรที่เกี่ยวข้อง

ครบวงจร: ระบุความเสี่ยง ⟶ ป้องกัน ⟶ ตรวจจับ ⟶ ตอบสนอง ⟶ กู้คืน (สอดคล้องกับ NIST CSF)

R0Cyber

การควบคุมการเข้าถึง: เท่าที่จำเป็นต่อหน้าที่

สิทธิ์น้อยที่สุด (Least privilege)

ฝ่ายขายเห็นข้อมูลลูกค้าของตน ไม่เห็นข้อมูลเงินเดือน

ยืนยันตัวตนหลายปัจจัย (MFA)

บังคับใช้กับอีเมล ระบบผู้ดูแล และการเข้าถึงจากภายนอก

ทบทวนสิทธิ์ทุกรอบ

เช่น ทุกไตรมาส · ถอนสิทธิ์ทันทีเมื่อลาออก

บัญชีสิทธิ์สูง

แยกบัญชีผู้ดูแล · บันทึกทุกการใช้งาน

ปัญหาที่พบบ่อย: บัญชีที่ใช้ร่วมกัน · รหัสผ่านอ่อน · บัญชีพนักงานที่ลาออกแล้วยังใช้ได้

บทเรียนปี 2568: รหัสผ่านอ่อนและไม่ประเมินความเสี่ยง เป็นเหตุให้ระบบของหน่วยงานรัฐถูกเจาะ และถูกปรับ

R0Cyber

ปกป้องตัวข้อมูล: เข้ารหัส ปิดบัง สำรอง



เข้ารหัส

ระหว่างส่ง (TLS) และขณะจัดเก็บ · จัดการกุญแจแยกจากข้อมูล



ปิดบังข้อมูล

แสดงเลขบัตรแค่ 4 หลักท้าย · ใช้ข้อมูลปลอมในระบบทดสอบ



สำรองข้อมูล

หลัก 3-2-1 · มีสำเนาที่แก้ไขไม่ได้ · ทดสอบกู้คืนจริง



แพตช์ · EDR

ปิดช่องโหว่ตามรอบ · ตรวจจับมัลแวร์บนเครื่อง



ป้องกันข้อมูลรั่ว

DLP · จำกัด USB · ควบคุมการแชร์ลิงก์คลาวด์



ทำลายอย่างปลอดภัย

ล้างดิสก์ก่อนทิ้ง · ทำลายเอกสาร

ข้อดีทางกฎหมาย: ข้อมูลที่เข้ารหัสอย่างเหมาะสมเมื่อรั่วไหล มีความเสี่ยงต่อเจ้าของข้อมูลต่ำกว่ามาก — มีผลต่อการประเมินเหตุละเมิด

R0Cyber

บันทึกและเฝ้าระวัง: รู้ทันเหตุ และพิสูจน์ได้

audit_trail.log

```
2026-11-07 09:12 user=somchai  READ   customer#10233
2026-11-07 09:13 user=somchai  EXPORT customers.csv (5,000 rows)
2026-11-07 23:47 user=svc_api  READ   customer#*  (12,880) # ผิดปกติ
2026-11-08 02:05 user=admin2 DELETE audit_log      # ต้องแจ้งเตือน
```

ตั้งการแจ้งเตือนเมื่อ

- ส่งออกข้อมูลจำนวนมาก
- เข้าถึงนอกเวลาทำงาน
- ล็อกอินล้มเหลวซ้ำ ๆ
- มีการลบหรือปิด log

เก็บรักษา log: ผู้ให้บริการต้องเก็บข้อมูลจราจรคอมพิวเตอร์ไม่น้อยกว่า 90 วัน (พ.ร.บ.คอมพิวเตอร์) · ป้องกัน log ไม่ให้ถูกแก้ไข

log เองก็เป็นข้อมูลส่วนบุคคล — ต้องจำกัดสิทธิ์ผู้ดูและกำหนดระยะเวลาเก็บเช่นกัน

R0Cyber

ออกแบบความเป็นส่วนตัวตั้งแต่เริ่มต้น

Privacy by Design & by Default

- คิดเรื่องข้อมูลตั้งแต่เริ่มออกแบบระบบ ไม่ใช่ตอนจะเปิดใช้
- ค่าเริ่มต้นเก็บน้อยที่สุด · เปิดเผยน้อยที่สุด
- ลบข้อมูลอัตโนมัติเมื่อพ้นระยะ

ประเมินผลกระทบ (DPIA)

- ทำก่อนเริ่มโครงการที่เสี่ยงสูง เช่น ระบบใบหน้า หรือรวมข้อมูลจำนวนมาก
- ระบุความเสี่ยง · มาตรการลดความเสี่ยง · ผู้อนุมัติ
- เป็นแนวปฏิบัติที่ดีและใช้เป็นหลักฐาน

เช็กลิสต์ก่อนเปิดระบบใหม่: ฐานทางกฎหมาย · Privacy notice · สิทธิ์การเข้าถึง · เข้ารหัส · log · ระยะเวลาเก็บ · DPA กับผู้ให้บริการ

R0Cyber

จุดอ่อนที่มักถูกลืม: คน กระดาษ และผู้ให้บริการ

คน

อบรมเป็นประจำ · ซ้อมรับมืออีเมลหลอกลวง · รู้ช่องทางรายงานเหตุ

กระดาษ

ตู้มีกุญแจ · ทำลายด้วยเครื่องทำลายเอกสาร · ไม่นำเอกสารลูกค้ากลับบ้าน

ผู้ให้บริการ

ตรวจก่อนจ้าง · DPA · ทบทวนเป็นระยะ · ถอนสิทธิ์เมื่อจบงาน

บทเรียนปี 2568: เวชระเบียนผู้ป่วยกว่า 1,000 รายการ ถูกนำไปใช้ห่อขนม

โรงพยาบาลเอกชนถูกปรับ 1.21 ล้านบาท และผู้รับจ้างทำลายเอกสารถูกปรับด้วย — การทำลายเอกสารต้องมีการควบคุมและตรวจสอบ

มาตรการที่ดีที่สุดบนกระดาษ คือการไม่พิมพ์ข้อมูลที่ไม่จำเป็นตั้งแต่แรก

R0Cyber

มาตรฐานที่ช่วยพิสูจน์ว่ามาตรการ "เหมาะสม"

มาตรฐาน	เน้นเรื่อง	ใช้กับ PDPA อย่างไร
ISO/IEC 27001	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS)	โครงมาตรการ ม.37(1) ครบทั้งสามด้าน
ISO/IEC 27701	ส่วนขยายด้านความเป็นส่วนตัว (PIMS)	บทบาท Controller/Processor · สิทธิ · ROPA
NIST CSF 2.0	Govern · Identify · Protect · Detect · Respond · Recover	วัดระดับความพร้อมและวางแผนปรับปรุง
CIS Controls	มาตรการทางเทคนิคเรียงตามลำดับความสำคัญ	เริ่มต้นได้เร็วสำหรับองค์กรขนาดกลาง

ข้อควรรู้: มาตรฐานไม่ใช่ข้อบังคับของ PDPA แต่เป็นหลักฐานที่ดีว่าองค์กรมีมาตรการที่เหมาะสม

หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ยังมีหน้าที่ตาม พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ 2562 เพิ่มเติม

QUICK CHECK

R0Cyber

ทบทวนสั้น ๆ: จริงหรือไม่จริง?

1. มาตรการความปลอดภัยต้องครอบคลุมเอกสารกระดาษด้วย	✓ จริง	ทุกรูปแบบ
2. MFA และทบทวนสิทธิ์ เป็นส่วนหนึ่งของการควบคุมการเข้าถึง	✓ จริง	ตามประกาศ 2565
3. ได้ ISO 27001 แล้ว ไม่ต้องทำอะไรเพิ่มตาม PDPA	✗ ไม่จริง	ยังต้องทำหน้าที่อื่นด้วย
4. log การเข้าถึงข้อมูลไม่ใช่ข้อมูลส่วนบุคคล	✗ ไม่จริง	มีชื่อผู้ใช้และ IP

SUMMARY · ตอนที่ 5

สรุป: การรักษาความปลอดภัยข้อมูล

- ✓ ม.37(1) + ประกาศ สคส. 2565: มาตรการขั้นต่ำ
- ✓ รักษา CIA ตามความเสี่ยง ทุกรูปแบบข้อมูล
- ✓ บริหาร · เทคนิค · กายภาพ ต้องไปด้วยกัน
- ✓ สิทธิ์น้อยที่สุด · MFA · เข้ารหัส · log
- ✓ ISO 27001/27701 ช่วยพิสูจน์ความเหมาะสม

ทำแบบทดสอบท้ายตอน แล้วพบกันในตอนถัดไป

R0Cyber

Cyber Law & Standards · learn.r0cyber.com

ตอนถัดไป

ตอนที่ 6

การแจ้งเหตุละเมิดและบทลงโทษ

- เหตุละเมิดคืออะไร
- แจ้ง สคส. ภายใน 72 ชม.
- ขั้นตอนรับมือเหตุ
- บทลงโทษและกรณีจริง