R0Cyber

CYBER LAW & STANDARDS · 2.2 ตอนที่ 3

นโยบายความปลอดภัย การรายงานเหตุ และการประสานงาน

เปลี่ยนข้อกำหนดของกฎหมายหลายฉบับ ให้เป็นนโยบายเดียวขององค์กร และขั้นตอนรายงานเหตุที่ทุกคนทำตามได้

Policy | Reporting matrix | RACI

CYBER ACT	พ.ร.บ.ไซเบอร์ 2562 · CII	สกมช.
COMPUTER	พ.ร.บ.คอมพิวเตอร์	ม.5–14, 26
PDPA	คุ้มครองข้อมูลส่วนบุคคล	สคส.
POLICY	นโยบายความปลอดภัยองค์กร	ISO 27001
REPORT	รายงานเหตุ · ประสานงาน	72 ชม.
EXERCISE	Tabletop · ซ้อมตัดสินใจ	Workshop

CYBER LAW · POLICY · RESPONSE

อ้างอิง พ.ร.บ.ไซเบอร์ 2562 · พ.ร.บ.คอมพิวเตอร์ 2550/2560 · PDPA 2562 · เนื้อหาเพื่อการศึกษา ไม่ใช่คำปรึกษาทางกฎหมาย

R0Cyber

ตอนนี้มี 5 หัวข้อ

01	นโยบายความปลอดภัย	ลำดับชั้นเอกสาร · นโยบายที่ต้องมี · ทำให้ใช้ได้จริง
02	การรายงานเหตุภายใน	ระดับความรุนแรง · ช่องทาง · แบบฟอร์ม
03	การรายงานภายนอก	ใครต้องแจ้งใคร ภายในเมื่อไร
04	การประสานงาน	บทบาท · RACI · การสื่อสาร · ตัวชี้วัด
05	ทบทวนและสรุป	Quick check · สรุปตอน

R0Cyber

ลำดับชั้นเอกสารความปลอดภัย

นโยบาย (Policy) — ทิศทางและหลักการ · ผู้บริหารสูงสุดอนุมัติ · เปลี่ยนไม่บ่อย

มาตรฐาน (Standard) — ข้อกำหนดที่วัดได้ เช่น รหัสผ่าน ≥ 12 ตัว + MFA

ขั้นตอน (Procedure) — ทำอะไร ทีละขั้น ใครทำ เช่น ขั้นตอนเพิ่ม/ถอนสิทธิ์

แนวปฏิบัติ / คู่มือ (Guideline) — คำแนะนำและตัวอย่าง ช่วยให้ทำได้ถูก

หลัก: ยิ่งลงล่าง ยิ่งละเอียดและเปลี่ยนบ่อย — นโยบายบอก "อะไร/ทำไม" ขั้นตอนบอก "อย่างไร" · ทุกฉบับต้องมีเจ้าของและวันทบทวน

POLICY SET

R0Cyber

นโยบายที่องค์กรควรมี และกฎหมายที่รองรับ

นโยบายความมั่นคงปลอดภัยสารสนเทศ

แม่บท · ISO 27001

การใช้งานที่ยอมรับได้

อีเมล อินเทอร์เน็ต อุปกรณ์ · การเฝ้าระวัง

การควบคุมการเข้าถึง

สิทธิ์ · MFA · ทบทวนสิทธิ์

การจัดชั้นและจัดการข้อมูล

ลับ/ภายใน/สาธารณะ · PDPA

การรับมือเหตุและรายงานเหตุ

PDPA 72 ชม. · พ.ร.บ.ไซเบอร์

ความต่อเนื่องทางธุรกิจ (BCP/DR)

สำรอง · กู้คืน · ซ้อม

ผู้ให้บริการภายนอก

DPA · สิทธิตรวจสอบ · ห่วงโซ่อุปทาน

การเก็บ log

≥ 90 วัน · พ.ร.บ.คอมพิวเตอร์

ความเป็นส่วนตัว

Privacy notice · สิทธิ · ROPA

นโยบายที่ดีไม่ต้องยาว — แต่ต้องโยงกับกฎหมาย มาตรฐาน และความเสี่ยงจริงขององค์กร

MAKE IT REAL

R0Cyber

ทำนโยบายให้ใช้ได้จริง ไม่ใช่แค่เอกสารในแฟ้ม

1

โยงกับข้อกำหนด

ทุกข้อบอกได้ว่ารองรับกฎหมาย/มาตรฐานข้อใด

2

ผู้บริหารอนุมัติ

ประกาศใช้อย่างเป็นทางการ มีงบรองรับ

3

สื่อสารและรับทราบ

อบรม · ลงชื่อรับทราบ · พนักงานใหม่

4

วัดผล

ตัวชี้วัด · ตรวจสอบภายใน

5

ทบทวนทุกปี

และเมื่อกฎหมายหรือระบบเปลี่ยน

มีกระบวนการขอข้อยกเว้น

ใครอนุมัติ หมดอายุเมื่อไร มีมาตรการชดเชยอะไร

วัดได้จริง

เช่น % พนักงานผ่านอบรม · บัญชีที่ไม่มี MFA · log ครบ 90 วัน

R0Cyber

การรายงานเหตุภายใน: เร็ว ง่าย ไม่กล่าวโทษ

ระดับ	ตัวอย่าง	แจ้งใคร · ภายใน
P1 วิกฤติ	แรนซัมแวร์ · ข้อมูลลูกค้ารั่วจำนวนมาก · ระบบหลักล่ม	ทีมรับมือ + ผู้บริหาร + DPO · ทันที
P2 สูง	บัญชีผู้ดูแลถูกยึด · มัลแวร์หลายเครื่อง	ทีมรับมือ + หัวหน้า · ภายใน 1 ชม.
P3 กลาง	ส่งอีเมลผิดคน · โน้ตบุ๊กหาย	ทีมความปลอดภัย + DPO · วันเดียวกัน
P4 ต่ำ	อีเมลฟิชชิงที่ถูกบล็อก · สแกนจากภายนอก	บันทึกในระบบ · ทบทวนรายสัปดาห์

หัวใจ: ช่องทางเดียวที่ทุกคนรู้ (อีเมล/โทร/ปุ่มรายงาน) · รายงานเร็วดีกว่ารายงานครบ · ไม่ลงโทษคนที่รายงาน

นาฬิกา 72 ชม. ของ PDPA เริ่มเมื่อองค์กร "ทราบเหตุ" — การรายงานภายในที่ช้า กินเวลาของทั้งองค์กร

R0Cyber

เมทริกซ์การรายงานภายนอก: ใคร แจ้งใคร เมื่อไร

เมื่อเกิด	แจ้ง	กรอบเวลา	ผู้รับผิดชอบ
ข้อมูลส่วนบุคคลรั่ว (มีความเสี่ยง)	สคส.	ภายใน 72 ชม. นับแต่ทราบเหตุ	DPO
ข้อมูลรั่ว (ความเสี่ยงสูง)	เจ้าของข้อมูล	โดยไม่ชักช้า พร้อมแนวทางเยียวยา	DPO + สื่อสาร
ภัยคุกคามต่อ CII	สกมช. + หน่วยงานควบคุมฯ	ตามประกาศ กกม./หน่วยงานควบคุม	CISO
ธุรกิจภายใต้หน่วยงานกำกับ	ธปท. · ก.ล.ต. · คปภ. ฯลฯ	ตามเกณฑ์ของแต่ละหน่วยงาน	Compliance
มีการกระทำความผิด	ตำรวจ (แจ้งความ)	โดยเร็ว · หลังเก็บหลักฐาน	กฎหมาย
กระทบลูกค้าองค์กร/คู่สัญญา	คู่สัญญา	ตามสัญญา/DPA	เจ้าของสัญญา

ทำให้เป็นของจริง: ใส่ชื่อ เบอร์ ช่องทาง และกรอบเวลาจริงตามประกาศที่ใช้กับองค์กรคุณ — ทบทวนทุกครั้งที่มีประกาศใหม่

R0Cyber

รายงานเหตุต้องมีอะไรบ้าง

incident_report.txt

```
รหัสเหตุ      : INC-2026-0142
ทราบเหตุเมื่อ  : 2026-11-07 22:10 (ผู้แจ้ง: SOC)
ลักษณะเหตุ    : ransomware + exfiltration
ระบบที่กระทบ   : order-db, file-server
ข้อมูลที่เกี่ยว : ลูกค้า ~50,000 ราย (มีข้อมูลสุขภาพ)
สถานะ        : กักกันแล้ว 23:05 · กำลังประเมิน
ผลกระทบ      : ระบบสั่งซื้อหยุด · เสี่ยงถูกหลอกลวง
มาตรการ      : ตัดเครือข่าย · รีเซ็ตรหัส · แจ้ง DPO
ผู้ประสานงาน   : DPO / CISO (เบอร์ 24 ชม.)
```

หลักการเขียน

- แยกข้อเท็จจริง กับสิ่งที่ยังไม่ทราบ
- ใช้เวลาที่ชัดเจน (วัน เวลา โซนเวลา)
- รายงานเท่าที่ทราบก่อน แล้วอัปเดต
- ห้ามคาดเดาผู้กระทำในรายงานทางการ
- เก็บทุกเวอร์ชันไว้เป็นหลักฐาน

แบบฟอร์มเดียวกัน ใช้ได้ทั้งรายงานผู้บริหาร แจ้ง สคส. และแจ้ง สกมช. — ลดเวลาเขียนใหม่ทุกครั้ง

COORDINATION

R0Cyber

บทบาทในการรับมือเหตุ: ใครทำอะไร

ผู้บัญชาการเหตุ (IC)

ตัดสินใจ จัดลำดับงาน คุมเวลา

ทีมไอที/SOC

กักกัน วิเคราะห์ กู้คืน เก็บหลักฐาน

DPO + ฝ่ายกฎหมาย

ประเมินหน้าที่ตามกฎหมาย แจ้งหน่วยงาน

สื่อสารองค์กร

ข้อความถึงลูกค้า สื่อ พนักงาน

ผู้บริหาร

อนุมัติการตัดสินใจสำคัญและงบ

ภายนอก

ผู้เชี่ยวชาญ IR · ประกันภัยไซเบอร์ · ผู้ให้บริการ

เตรียมไว้ก่อน: รายชื่อติดต่อ 24 ชม. · ช่องทางสื่อสารสำรองนอกระบบที่ถูกโจมตี · ห้องประชุมเหตุการณ์ · สัญญากับผู้เชี่ยวชาญภายนอก

บทเรียนบ่อย: ใช้อีเมลบริษัทคุยเรื่องเหตุ ทั้งที่อีเมลอาจถูกผู้โจมตีอ่านอยู่

R0Cyber

วัดผลและปรับปรุงอย่างต่อเนื่อง

เวลาในการตรวจพบ

MTTD · ตั้งแต่เกิดเหตุถึงรู้ตัว

เวลาในการรับมือ

MTTR · ตั้งแต่รู้ถึงกลับมาปกติ

แจ้งทันเวลา

% เหตุที่แจ้งหน่วยงานภายในกำหนด

ความพร้อมของคน

% ผ่านอบรม · ซ้อมกี่ครั้ง/ปี

ทบทวนหลังเหตุทุกครั้ง (Lessons learned)

อะไรได้ผล อะไรช้า ต้องแก้นโยบาย ขั้นตอน หรือมาตรการทางเทคนิคใด — แล้วนำไปซ้อมใน Tabletop รอบถัดไป

ตอนที่ 4 Workshop: ลงมือทำ Data flow · Compliance checklist · Incident reporting flow · Tabletop exercise

QUICK CHECK

R0Cyber

ทบทวนสั้น ๆ: จริงหรือไม่จริง?

1. นโยบายควรละเอียดทุกขั้นตอน เปลี่ยนทุกเดือน	✗ ไม่จริง	ขั้นตอนต่างหากที่ละเอียด
2. นาฬิกา 72 ชม. ของ PDPA เริ่มเมื่อองค์กรทราบเหตุ	✓ จริง	รายงานภายในต้องเร็ว
3. ระหว่างเหตุ ควรใช้ช่องทางสื่อสารสำรองนอกระบบที่ถูกโจมตี	✓ จริง	ผู้โจมตีอาจอ่านอีเมล
4. ทุกเหตุต้องแจ้ง สกมช. เสมอ ไม่ว่าองค์กรใด	✗ ไม่จริง	บังคับสำหรับ CII

SUMMARY · ตอนที่ 3

สรุป: นโยบายและการรายงานเหตุ

- ✓ นโยบาย ⟶ มาตรฐาน ⟶ ขั้นตอน ⟶ แนวปฏิบัติ
- ✓ นโยบายต้องโยงกฎหมาย มีเจ้าของ วัดผล ทบทวนทุกปี
- ✓ รายงานภายใน: ระดับ P1–P4 · ช่องทางเดียว · ไม่กล่าวโทษ
- ✓ เมทริกซ์รายงานภายนอก: สคส. 72 ชม. · สกมช. · หน่วยงานกำกับ · ตำรวจ
- ✓ บทบาทชัด + ช่องทางสำรอง + ทบทวนหลังเหตุ

ทำแบบทดสอบท้ายตอน แล้วพบกันในตอนถัดไป

ตอนถัดไป

ตอนที่ 4

Workshop: Data flow ⟶ Tabletop

- วิเคราะห์ Data flow
- Compliance checklist
- Incident reporting flow
- Tabletop exercise