ทีม/ชื่อ: _____ วันที่: _____

Workshop: Data Flow · Compliance · Incident Reporting · Tabletop

ใช้คู่กับวิดีโอตอนที่ 4 · ทำเป็นทีม 4–6 คน · ใช้เวลาประมาณ 3.5 ชั่วโมง

ช่วง	กิจกรรม	เวลา	เอกสาร	ผลงาน
0	บรีฟโจทย์บริษัทเฮลธ์พลัส (สมมติ) และแบ่งบทบาท	15 นาที	หน้า 2	—
1	วิเคราะห์ Data flow และประเด็นกฎหมายรายเส้นทาง	30 นาที	Worksheet 1	ตาราง data flow
2	จัดทำ Compliance checklist (PDPA · พ.ร.บ.ไซเบอร์ · พ.ร.บ.คอมพิวเตอร์)	25 นาที	Worksheet 2	เช็กลิสต์พร้อมสถานะ
3	เหตุจำลอง ⟶ Incident reporting flow + เมทริกซ์การแจ้ง	30 นาที	Worksheet 3–4	flow + matrix
4	Tabletop exercise (inject 6 ใบ) + บันทึกการตัดสินใจ	90 นาที	Worksheet 5	decision log
5	ประเมินผลและทบทวนหลังการซ้อม	20 นาที	แบบประเมิน	แผนปรับปรุง

บทบาทในทีม: ผู้บัญชาการเหตุ (IC) · ไอที/SOC · DPO/กฎหมาย · สื่อสารองค์กร · ผู้บริหาร · (ผู้ดำเนินเกม 1 คนแยกจากทีม)
กติกา: ห้ามใช้ระบบจริงหรือข้อมูลจริง · ทุกการตัดสินใจต้องบันทึกเหตุผลและอ้างกฎหมาย/สัญญาที่เกี่ยวข้อง

SCENARIO

ทีม/ชื่อ: _____ วันที่: _____

โจทย์: บริษัท เฮลธ์พลัส (บริษัทสมมติ)

หัวข้อ	รายละเอียด
ธุรกิจ	แอปร้านยาออนไลน์ + ปรึกษาเภสัชกรผ่านวิดีโอ · ลูกค้า 200,000 ราย · คำสั่งซื้อวันละ 3,000 รายการ · 12 สาขามี Wi-Fi ให้ลูกค้า
ข้อมูล	ชื่อ ที่อยู่ เบอร์โทร เลขบัตรประชาชน · ใบสั่งยาและประวัติการใช้ยา (ข้อมูลสุขภาพ) · ข้อมูลชำระเงินผ่านผู้ให้บริการภายนอก
ระบบ	แอป/เว็บ ⟶ API บนคลาวด์ (สิงคโปร์) ⟶ ฐานข้อมูลคำสั่งซื้อ ⟶ บริษัทขนส่ง · ระบบอีเมลการตลาด · ผู้ให้บริการชำระเงิน · ระบบจ่ายยาของโรงพยาบาลรัฐคู่สัญญา
สัญญา	สัญญากับโรงพยาบาลรัฐกำหนดให้แจ้งเหตุที่กระทบบริการ "โดยเร็วที่สุด ไม่เกิน 24 ชม." และปฏิบัติตามมาตรฐานความปลอดภัยของโรงพยาบาล (สมมติ)
สถานะปัจจุบัน	มี DPO นอกเวลา · ROPA ทำไว้ 2 ปีก่อน · ยังไม่มี DPA กับบริษัทขนส่ง · log Wi-Fi เก็บ 7 วัน · ไม่เคยซ้อมแผนรับมือเหตุ

WORKSHEET 1

ทีม/ชื่อ: _____ วันที่: _____

วิเคราะห์ Data Flow

หนึ่งแถวต่อหนึ่งเส้นทาง (ลูกศร) · อ้างมาตราที่เกี่ยวข้องในช่องประเด็น

เส้นทาง (จาก ⟶ ถึง)	ข้อมูล	อ่อนไหว?	ฐานกฎหมาย	เข้ารหัส?	ข้ามประเทศ?	DPA?	เก็บนาน	ประเด็น / สิ่งที่ต้องทำ

WORKSHEET 2

ทีม/ชื่อ: _____ วันที่: _____

Compliance Checklist

สถานะ: ✓ มี · ◐ บางส่วน · ✗ ไม่มี · ระบุหลักฐานที่ตรวจสอบได้

กลุ่ม	ข้อกำหนด	สถานะ	หลักฐาน	ผู้รับผิดชอบ	กำหนดเสร็จ	ความเสี่ยง
PDPA	ROPA ครบและเป็นปัจจุบัน (ม.39)					
PDPA	ฐานทางกฎหมาย + ความยินยอมสำหรับข้อมูลสุขภาพ (ม.24, 26)					
PDPA	Privacy notice ในแอปและสาขา (ม.23)					
PDPA	DPA กับขนส่ง คลาวด์ ชำระเงิน อีเมลการตลาด (ม.40)					
PDPA	เกณฑ์ส่งข้อมูลไปต่างประเทศ (ม.28–29)					
PDPA	DPO และช่องทางติดต่อ (ม.41–42)					
PDPA	แผนแจ้งเหตุ สคส. 72 ชม. (ม.37(4))					
ไซเบอร์/สัญญา	มาตรฐานความปลอดภัยตามสัญญาโรงพยาบาล					
ไซเบอร์/สัญญา	ผู้ประสานงานด้านไซเบอร์ 24 ชม.					
ไซเบอร์/สัญญา	ประเมินความเสี่ยง/ตรวจสอบประจำปี					
คอมพิวเตอร์	log Wi-Fi และระบบ ≥ 90 วัน · ซิงก์เวลา (ม.26)					
คอมพิวเตอร์	ขั้นตอนเก็บหลักฐาน + แจ้งความ					
นโยบาย	นโยบายความปลอดภัย + การใช้งานที่ยอมรับได้ (ทบทวนในปีนี้)					
นโยบาย	แผนรับมือเหตุ + ซ้อมปีละครั้ง					

WORKSHEET 3

ทีม/ชื่อ: _____ วันที่: _____

เหตุจำลอง และ Incident Reporting Flow

อ่านไทม์ไลน์ แล้วเติมแต่ละขั้นของ flow ว่าใครทำอะไร เมื่อไร

ไทม์ไลน์เหตุ (สมมติ)
ศ. 22:10 SOC แจ้งเตือนการส่งออกข้อมูลจำนวนมากจาก order-db
ศ. 22:40 ไฟล์บน file-server ถูกเข้ารหัส พบข้อความเรียกค่าไถ่
ศ. 23:05 ตัดการเชื่อมต่อเครือข่ายเซิร์ฟเวอร์ที่ได้รับผล
ส. 08:00 ผู้โจมตีส่งตัวอย่างข้อมูลลูกค้า 100 ราย (มีใบสั่งยา)
ส. 10:00 ระบบจ่ายยาของโรงพยาบาลคู่สัญญาเชื่อมต่อไม่ได้
ส. 14:00 นักข่าวสอบถามผ่านเพจบริษัท

1. ตรวจพบ

ใคร: _____ เวลา: _____

2. คัดกรอง (ระดับ?)

ใคร: _____ เวลา: _____

3. กักกัน + หลักฐาน

ใคร: _____ เวลา: _____

4. ประเมิน (ข้อมูล/จำนวน/ความเสี่ยง)

ใคร: _____ เวลา: _____

5. แจ้ง (ดู Worksheet 4)

ใคร: _____ เวลา: _____

6. กู้คืน + ทบทวน

ใคร: _____ เวลา: _____

คำถาม	คำตอบของทีม
"ทราบเหตุ" เมื่อใด ⟶ ครบ 72 ชม. เมื่อใด	
ข้อมูลอะไร กี่ราย อ่อนไหวหรือไม่ ความเสี่ยงระดับใด	
หลักฐานใดต้องเก็บก่อนกู้คืน · ใครเก็บ	
ใครเป็น IC · ใครเป็นโฆษก · ช่องทางสื่อสารสำรองคืออะไร	

WORKSHEET 4

ทีม/ชื่อ: _____ วันที่: _____

เมทริกซ์การแจ้งหน่วยงานภายนอก

ระบุว่าต้องแจ้งหรือไม่ พร้อมฐานกฎหมาย/สัญญา และคำนวณเวลาครบกำหนดจริง

หน่วยงาน/ผู้รับแจ้ง	ต้องแจ้ง?	ฐานกฎหมาย/สัญญา	กรอบเวลา	ครบกำหนด (วัน เวลา)	ผู้แจ้ง	ช่องทาง	สถานะ
สคส.							
เจ้าของข้อมูล (ลูกค้า)							
โรงพยาบาลรัฐคู่สัญญา							
ตำรวจไซเบอร์							
ThaiCERT / สกมช.							
ผู้ให้บริการคลาวด์/ขนส่ง							
บริษัทประกันภัยไซเบอร์ (ถ้ามี)							
อื่น ๆ: _____							

WORKSHEET 5

ทีม/ชื่อ: _____ วันที่: _____

Tabletop Exercise: Inject และบันทึกการตัดสินใจ

ผู้ดำเนินเกมเปิด inject ทีละใบ · ทีมมีเวลา 10–15 นาทีต่อ inject

Inject	สถานการณ์	การตัดสินใจของทีม	ผู้ตัดสินใจ	อ้างอิงกฎหมาย/สัญญา	เวลา
T+0	SOC แจ้งเตือนการส่งออกข้อมูลผิดปกติ				
T+1 ชม.	ไฟล์ถูกเข้ารหัส พบข้อความเรียกค่าไถ่				
T+10 ชม.	ผู้โจมตีปล่อยตัวอย่างข้อมูลลูกค้า				
T+16 ชม.	นักข่าวถาม · ลูกค้าโพสต์ในโซเชียล				
T+40 ชม.	ผู้บริหารถามเรื่องค่าไถ่				
T+70 ชม.	ข้อมูลบางส่วนยังไม่ครบ ใกล้ครบ 72 ชม.				

EVALUATION

ทีม/ชื่อ: _____ วันที่: _____

แบบประเมินผลการซ้อม และทบทวนหลังการซ้อม

ผู้ดำเนินเกมให้คะแนน 1–3 ต่อเกณฑ์ (รวมเต็ม 15 · ผ่านเมื่อ ≥ 11)

เกณฑ์	ดี (3)	พอใช้ (2)	ต้องปรับ (1)	คะแนน
ความครบถ้วนทางกฎหมาย	ระบุทุกหน่วยงาน + เหตุผล	ขาด 1 หน่วยงาน	ขาดหลายหน่วยงาน	
ความทันเวลา	แจ้ง สคส. < 72 ชม. พร้อมบันทึก	ทันแต่ไม่มีบันทึก	เกิน 72 ชม.	
การตัดสินใจและบทบาท	IC ชัด ตัดสินใจเป็นลำดับ	บางจุดสับสน	ไม่มีผู้ตัดสินใจ	
การสื่อสาร	ถูกต้อง สอดคล้องทุกช่องทาง	ช้าหรือไม่สอดคล้อง	ขัดกันเอง	
หลักฐาน	เก็บก่อนกู้คืน มี hash	เก็บบางส่วน	ล้างระบบก่อนเก็บ	

ทบทวนหลังการซ้อม	รายการ	ผู้รับผิดชอบ	เสร็จภายใน
3 สิ่งที่ได้ผล			
3 สิ่งที่ต้องแก้			

แนวเฉลยสำหรับผู้สอน (ไม่ใช่เฉลยเดียว)

ให้คะแนนจากเหตุผลทางกฎหมายและความสมเหตุสมผล มากกว่าความตรงกับเฉลย

ประเด็น	แนวคำตอบ
Data flow ที่เสี่ยงสูง	ใบสั่งยา ⟶ คลาวด์ต่างประเทศ (ม.26, 28–29 + DPA) · ประวัติยา ⟶ อีเมลการตลาด (ม.21, 26: ตัดออก/ขอยินยอมแยก) · ขนส่งไม่มี DPA (ม.40) · log Wi-Fi 7 วัน (ขัด ม.26 พ.ร.บ.คอมพิวเตอร์)
เวลา 72 ชม.	นับอย่างระมัดระวังจาก ศ. 22:10 ⟶ ครบ จ. 22:10 · ถ้ายืนยันข้อมูลรั่วภายหลัง ให้บันทึกเหตุผลของจุดเริ่มนับ
ระดับความเสี่ยง	สูง: ข้อมูลสุขภาพ + เลขบัตร + มีหลักฐานผู้โจมตีถือข้อมูล ⟶ แจ้ง สคส. และลูกค้าพร้อมแนวทางเยียวยา (เช่น ระวังการหลอกลวง ช่องทางสอบถาม)
การแจ้งอื่น	โรงพยาบาลคู่สัญญา ≤ 24 ชม. ตามสัญญา (สมมติ) · แจ้งความตำรวจไซเบอร์หลังเก็บหลักฐาน · ขอความช่วยเหลือ ThaiCERT · แจ้งประกันภัยตามกรมธรรม์
หลักฐาน	แยกเครื่องแต่ไม่ปิด/ล้างทันที · เก็บ log, memory, disk image + hash · บันทึกห่วงโซ่การครอบครอง
ค่าไถ่	ไม่มีคำตอบเดียว: ประเมินกฎหมาย ความเสี่ยงที่ข้อมูลยังถูกเผยแพร่ ความพร้อมของสำรอง และให้ผู้มีอำนาจตัดสินใจพร้อมบันทึกเหตุผล — การจ่ายไม่ทำให้หน้าที่แจ้งเหตุหมดไป
การสื่อสาร	โฆษกคนเดียว · ข้อความยึดข้อเท็จจริง ไม่คาดเดา · ใช้ช่องทางสำรองระหว่างทีม