ใบงานที่ 1

การวิเคราะห์กรณีศึกษา: ความมั่นคงปลอดภัยข้อมูลสุขภาพในโรงพยาบาล

รายวิชา: Introduction to Medical Information Security

หัวข้อ: CIA Triad, People–Process–Technology, Health Data Flow

> **รูปแบบ:** ทำงานเป็นกลุ่ม (4–6 คน) ภายในเวลา 60 นาที

วัตถุประสงค์ของใบงาน

เมื่อทำใบงานนี้เสร็จ นักศึกษาควรสามารถ

1. อธิบายและประเมินเหตุการณ์ด้านความมั่นคงปลอดภัยข้อมูลสุขภาพ โดยใช้กรอบคิด **CIA Triad**
2. วิเคราะห์เหตุการณ์ในมุมมองของ **People–Process–Technology (PPT Model)**
3. ระบุจุดเสี่ยงใน **กระบวนการไหลของข้อมูลสุขภาพ (Health Data Flow)** ในโรงพยาบาล
4. เสนอแนวทางควบคุมและป้องกันที่เหมาะสมกับบริบทของสถานพยาบาล

คำแนะนำสำหรับการทำงานเป็นกลุ่ม

- จัดกลุ่มละ **4–6 คน**
- เลือก **หัวหน้ากลุ่ม** 1 คน เพื่อสรุปคำตอบ และติดต่อกับผู้สอน
- เลือก **ผู้นำเสนอ** 1–2 คน สำหรับนำเสนอผลงานกลุ่ม
- ใช้ใบงานนี้เป็น “เอกสารกลาง” ของกลุ่ม และส่งคืนตามที่อาจารย์กำหนด

> **หมายเหตุ:** ให้ทุกคนมีส่วนร่วมในการคิด วิเคราะห์ และอภิปรายภายในกลุ่ม

ข้อความกรณีศึกษา (Case Study)

> **เหตุการณ์: Ransomware ในโรงพยาบาลศูนย์จังหวัด**
>
> โรงพยาบาลศูนย์จังหวัดแห่งหนึ่งมีระบบ EMR, LIS, PACS และระบบการเงินเชื่อมต่อกันมาหลายปี โดยยังมี **legacy system** บางส่วนที่ไม่ได้อัปเดตแพตช์สม่ำเสมอ บุคลากรทางการแพทย์จำนวนมากใช้ LINE ส่วนตัวในการส่งภาพผลตรวจและข้อมูลผู้ป่วยเพื่อความรวดเร็วในงานเวร
>
> วันหนึ่ง โรงพยาบาลถูกโจมตีด้วย **ransomware** ผ่านอีเมล phishing ที่เจ้าหน้าที่เวชระเบียนเปิดไฟล์แนบโดยคิดว่าเป็นไฟล์จากหน่วยงานรัฐ มัลแวร์ค่อย ๆ กระจายผ่านเครือข่ายภายใน

ข้อความกรณีศึกษา (Case Study)

> ผลคือ
>
> - ระบบ EMR และ PACS ถูกเข้ารหัส ใช้งานไม่ได้
> - ห้องฉุกเฉิน (ER) ไม่สามารถเข้าถึงประวัติแพ้ยาและประวัติการรักษาเดิม
> - หน่วยรังสีไม่สามารถเปิดดูภาพ CT/MRI ได้ ต้องใช้ระบบสำรองที่ล้าสมัยและข้อมูลไม่ครบ
> - พบว่าข้อมูลผู้ป่วยบางส่วนถูกส่งออกไปยังเซิร์ฟเวอร์ภายนอกก่อนถูกเข้ารหัส
> - โรงพยาบาลต้องปิดระบบเชื่อมต่ออินเทอร์เน็ตชั่วคราว ส่งผลให้การส่งเคลมประกันล่าช้า
>
> เหตุการณ์นี้ถูกสื่อมวลชนรายงาน ทำให้เกิดคำถามจากสาธารณะต่อมาตรการคุ้มครองข้อมูลผู้ป่วยและการปฏิบัติตาม PDPA ของโรงพยาบาล

ภารกิจของกลุ่ม

กลุ่มของท่านต้องทำภารกิจต่อไปนี้ให้ครบถ้วน

1. วิเคราะห์ผลกระทบของเหตุการณ์ในมุมมอง **CIA Triad**
2. วาดและอธิบาย **Health Data Flow** พร้อมระบุ “จุดเสี่ยง” ที่สำคัญ
3. วิเคราะห์สาเหตุและช่องโหว่ในมุมมอง **People–Process–Technology (PPT)**
4. เสนอ “ชุดมาตรการ” เพื่อป้องกันและลดความเสี่ยงในอนาคต

> ให้เขียนคำตอบลงในสไลด์ต่อไปนี้ให้ชัดเจนและกระชับ

ภารกิจที่ 1

วิเคราะห์เหตุการณ์ตามกรอบ CIA Triad

ภารกิจที่ 1: CIA Triad (1/2)

ให้กลุ่มของท่านวิเคราะห์ว่า เหตุการณ์ในกรณีศึกษามีผลกระทบต่อ

- **Confidentiality (C)**
- **Integrity (I)**
- **Availability (A)**

อย่างไรบ้าง

คำสั่ง

1. ระบุอย่างน้อย **2 เหตุการณ์** ต่อองค์ประกอบของ CIA
2. อธิบายสั้น ๆ ว่าเหตุการณ์นั้นกระทบ CIA องค์ประกอบใด และอย่างไร

ภารกิจที่ 1: CIA Triad (2/2) – พื้นที่สำหรับเขียนคำตอบ

ตารางที่ 1: การวิเคราะห์ตาม CIA Triad

องค์ประกอบ CIA	เหตุการณ์ในกรณีศึกษา	ผลกระทบ / คำอธิบาย (ย่อ)
C: Confidentiality		
C: Confidentiality		
I: Integrity		
I: Integrity		
A: Availability		
A: Availability		

> แนะนำ: พยายามเชื่อมโยงผลกระทบกับ “ผู้ป่วย” และ “องค์กร” ทั้งสองมิติ

ภารกิจที่ 2

วาด Health Data Flow และระบุจุดเสี่ยง

ภารกิจที่ 2: Health Data Flow (1/2)

ในกรณีนี้ ข้อมูลสุขภาพของผู้ป่วยไหลผ่านหลายระบบและหลายหน่วยงาน

ตัวอย่างจุดที่เกี่ยวข้อง เช่น

- ผู้ป่วย (Patient)
- ห้องตรวจ OPD / ER
- ระบบ EMR/EHR
- ห้องปฏิบัติการ (LIS)
- รังสีวินิจฉัย / PACS
- แพทย์ผู้รักษา
- ระบบการเงิน / ประกัน (Billing/Insurance)
- ระบบภายนอก / หน่วยงานภาครัฐ

ภารกิจที่ 2: Health Data Flow (2/2) – พื้นที่สำหรับเขียนคำตอบ

คำสั่ง

1. วาดแผนภาพ **กระบวนการไหลของข้อมูลสุขภาพ (Health Data Flow)** ที่เกี่ยวข้องกับกรณีนี้
2. ทำเครื่องหมาย (เช่น วงกลม หรือ ★) ที่ **3 จุด** ที่กลุ่มเห็นว่า “เสี่ยงที่สุด”
3. เขียนอธิบายด้านล่างอย่างน้อย 1–2 บรรทัดต่อจุด ว่าทำไมจึงเป็นจุดเสี่ยง

ภารกิจที่ 3

วิเคราะห์ด้วย People–Process–Technology (PPT Model)

ภารกิจที่ 3: PPT Model

ให้วิเคราะห์ว่าปัญหาในกรณีศึกษานี้เกิดจากช่องโหว่ในมิติใดบ้าง

- **People (บุคลากร)**
- **Process (กระบวนการ/นโยบาย)**
- **Technology (เทคโนโลยี/ระบบ)**

คำสั่ง

1. ระบุอย่างน้อย **2 ตัวอย่าง** ต่อมิติ (People, Process, Technology)
2. เขียนคำอธิบายสั้น ๆ ว่าทำไมจึงมองว่าเป็นช่องโหว่หรือปัญหา

ภารกิจที่ 3: PPT Model – พื้นที่สำหรับเขียนคำตอบ

ตารางที่ 2: การวิเคราะห์ช่องโหว่ตาม PPT Model

มิติ	ตัวอย่างช่องโหว่ / ปัญหา	คำอธิบาย (ย่อ)
People		
People		
Process		
Process		
Technology		
Technology		

> พิจารณาทั้งเรื่องการใช้ LINE ส่วนตัว, การเปิดไฟล์ phishing, การดูแลระบบ legacy, นโยบายภายใน ฯลฯ

ภารกิจที่ 4

เสนอชุดมาตรการป้องกันและลดความเสี่ยง

ภารกิจที่ 4: ข้อเสนอแนวทางควบคุมและป้องกัน

ให้กลุ่มของท่านเสนอ “ชุดมาตรการ” ที่คิดว่าสำคัญและเหมาะสมกับโรงพยาบาลในกรณีนี้

คำสั่ง

1. เลือกเสนอ **3–5 มาตรการ**
2. ระบุสำหรับแต่ละมาตรการว่า
    - เป็นมาตรการด้าน **People / Process / Technology**
    - เน้นปกป้อง **C / I / A** ใดเป็นหลัก
    - (ถ้าเป็นไปได้) มีความเกี่ยวข้องกับกรอบ/กฎหมายใด เช่น PDPA, ISO 27001, NIST CSF

ภารกิจที่ 4 – พื้นที่สำหรับเขียนคำตอบ

ตารางที่ 3: ชุดมาตรการที่เสนอ

มาตรการที่เสนอ	ประเภท (People / Process / Technology)	เน้นปกป้อง (C/I/A)	เชื่อมโยงกรอบ/กฎหมาย (ถ้ามี)

> ให้เลือกมาตรการที่ “เป็นไปได้จริง” ในบริบทโรงพยาบาล ไม่ใช่เพียงแนวคิดในเชิงทฤษฎีเท่านั้น

ส่วนสำหรับการเตรียมนำเสนอ (กลุ่ม)

การเตรียมนำเสนอผลงานกลุ่ม

ให้กลุ่มของท่านเตรียมสรุปเพื่อนำเสนอภายในเวลา **ประมาณ 3 นาที** โดยเน้น

1. **จุดเสี่ยงสำคัญที่สุด** ใน Health Data Flow (1–2 จุด)
2. **มาตรการที่คิดว่าสำคัญที่สุด** 1–2 ข้อ พร้อมเหตุผล
3. เชื่อมโยงให้เห็นว่า ทำไมกรณีนี้จึงเป็นปัญหาทั้งในมุม
    - ความปลอดภัยของผู้ป่วย
    - ความเชื่อมั่นของสังคม
    - การปฏิบัติตามกฎหมาย (เช่น PDPA)

> ให้ผู้นำเสนอทั้งกลุ่มเข้าใจภาพรวมของคำตอบ ไม่ใช่จำเฉพาะคนเดียว

คำถามสะท้อนคิด (สำหรับสมาชิกแต่ละคน)

ให้สมาชิกแต่ละคนลองตอบในใจ หรือจดสั้น ๆ

> หากคุณอยู่ในบทบาทใดบทบาทหนึ่งต่อไปนี้
>
> - เจ้าหน้าที่ไอที
> - แพทย์
> - พยาบาล
> - ผู้บริหารโรงพยาบาล
>
> **สิ่งแรกที่คุณจะผลักดันหรือเปลี่ยนแปลง** เกี่ยวกับความมั่นคงปลอดภัยข้อมูลสุขภาพในโรงพยาบาลคืออะไร เพราะเหตุใด?

คำตอบของคุณจะเป็นประเด็นที่ดีสำหรับการอภิปรายในชั้นเรียนต่อไป

สิ้นสุดใบงานที่ 1

ส่งใบงานตามรูปแบบที่ผู้สอนกำหนด

> โปรดตรวจสอบว่ากลุ่มของท่าน
>
> - เขียนคำตอบครบทุกภารกิจ
> - ระบุชื่อกลุ่ม/สมาชิกครบถ้วน
> - พร้อมสำหรับการนำเสนอ/อภิปรายในชั้นเรียน