

ด้านล่างนี้คือ แผนการสอนรายสัปดาห์ (**Weekly Teaching Plan**) ฉบับสมบูรณ์ 12 สัปดาห์ จัดทำตามรูปแบบ มคอ.3 ที่ใช้ในสถาบันอุดมศึกษา พร้อมกิจกรรมการเรียนรู้ (TLA), วิธีประเมิน (Assessment), และ CLO ที่เชื่อมโยงในแต่ละสัปดาห์

แผนการสอนรายสัปดาห์ (12 สัปดาห์) – ฉบับสมบูรณ์

รายวิชา: **IMI62-332** ความมั่นคงสารสนเทศทางการแพทย์ (Medical Information Security)
ภาคการศึกษา 2/2568

สัปดาห์ที่ 1 — บทนำความมั่นคงสารสนเทศทางการแพทย์

เนื้อหา:

- ความหมาย ความสำคัญ และองค์ประกอบความมั่นคงสารสนเทศ
- บริบทด้านข้อมูลสุขภาพและระบบสาธารณสุข
- ลักษณะเฉพาะของข้อมูลสุขภาพ

กิจกรรมการสอน (TLA):

บรรยาย + ถาม-ตอบ + วิเคราะห์ตัวอย่างเบื้องต้น

งาน/การประเมินผล:

แบบทดสอบสั้น (Quiz 1)

CLO ที่เกี่ยวข้อง: CLO1

สัปดาห์ที่ 2 — ภัยคุกคามในระบบสุขภาพ

เนื้อหา:

- ประเภทภัยคุกคามไซเบอร์ในโรงพยาบาล
- ความเสี่ยงเชิงกระบวนการและปัจจัยมนุษย์ (Human Factors)
- แนวโน้มภัยคุกคามด้านสุขภาพระดับโลก

กิจกรรม:

อภิปรายข่าวจริง + วิเคราะห์เหตุการณ์ Ransomware

ประเมินผล:

แบบฝึกหัดวิเคราะห์ (Worksheet 1)

CLO: CLO1, CLO2

สัปดาห์ที่ 3 — ระบบสารสนเทศสุขภาพ (HIS/EHR/EMR/HIE)

เนื้อหา:

- โครงสร้าง HIS, EHR/EMR
- สถาปัตยกรรมระบบบริการสุขภาพ
- ความเสี่ยงเชิงสถาปัตยกรรมและการบูรณาการระบบ

กิจกรรม:

บรรยาย + ตัวอย่างโครงสร้าง EHR จริง

ประเมินผล:

Quiz 2

CLO: CLO1

สัปดาห์ที่ 4 — ความมั่นคงของการสื่อสารข้อมูลสุขภาพ

เนื้อหา:

- HL7, FHIR, DICOM
- Encryption, Secure Channel, Transport Security
- Network Threats ในบริการสุขภาพ

กิจกรรม:

เดโมการส่งข้อมูลสุขภาพ + วิเคราะห์การดักฟัง (concept demonstration)

ประเมินผล:

แบบทดสอบสั้น (Quiz 3)

CLO: CLO1, CLO2

สัปดาห์ที่ 5 — ภัยคุกคาม ช่องโหว่ และการโจมตี

เนื้อหา:

- ช่องโหว่ระบบสุขภาพ (Vulnerability Sources)
- Ransomware, MITM, Insider Threat, Supply Chain Attack
- แนวทางลดความเสี่ยง

กิจกรรม:

Workshop วิเคราะห์ช่องโหว่ (Vulnerability Scenario)

ประเมินผล:

การมีส่วนร่วมและวิเคราะห์เหตุการณ์

CLO: CLO2

****สัปดาห์ที่ 6 — สอบกลางภาค (Midterm Exam)**

เนื้อหาที่สอบ: บทที่ 1-4

สัดส่วน: 15%

CLO: CLO1, CLO2

สัปดาห์ที่ 7 — ความมั่นคงของอุปกรณ์ IoMT (IoMT Security)

เนื้อหา:

- ประเภทอุปกรณ์การแพทย์ที่เชื่อมต่อ
- การโจมตีอุปกรณ์ Critical Care
- มาตรการควบคุมด้าน IoMT

กิจกรรม:

Case Study: แยกเครื่อง Infusion Pump / Pacemaker

ประเมินผล:

Worksheet 2

CLO: CLO2

สัปดาห์ที่ 8 — การประเมินความเสี่ยง (Risk Assessment)

เนื้อหา:

- Risk Identification / Analysis / Mitigation
- Data Classification
- ความเสี่ยงเชิงเทคนิคและเชิงกระบวนการ

กิจกรรม:

Workshop จำลองการทำ Risk Assessment

ประเมินผล:

แบบฝึกวิเคราะห์ความเสี่ยง

CLO: CLO2, CLO3

สัปดาห์ที่ 9 — การคุ้มครองข้อมูลสุขภาพ (Data Protection)

เนื้อหา:

- Access Control / Authentication
- Encryption at rest & in transit
- Data Governance และแนวปฏิบัติในสถานพยาบาล

กิจกรรม:

กิจกรรมกลุ่ม: ออกแบบนโยบาย Data Protection

ประเมินผล:

รายงานกลุ่ม (10%)

CLO: CLO3

สัปดาห์ที่ 10 — การตอบสนองเหตุการณ์ (Incident Response)

เนื้อหา:

- โครงสร้าง Incident Response (NIST CSF / ISO 27035)
- Data Breach Handling
- Business Continuity (BCP) ในโรงพยาบาล

กิจกรรม:

จำลองเหตุการณ์โจมตี (Tabletop Exercise)

ประเมินผล:

การมีส่วนร่วม + การวิเคราะห์ผลการจำลอง

CLO: CLO3

สัปดาห์ที่ 11 — กฎหมาย มาตรฐาน และจริยธรรมข้อมูลสุขภาพ

เนื้อหา:

- PDPA, HIPAA, ISO/IEC 27001
- จริยธรรมข้อมูลสุขภาพ
- ความรับผิดชอบวิชาชีพ

กิจกรรม:

อภิปรายกรณีละเมิดข้อมูลผู้ป่วยในไทยและต่างประเทศ

ประเมินผล:

ส่งรายงานวิเคราะห์ (10%)

CLO: CLO4

สัปดาห์ที่ 12 — สรุปบททวนและเตรียมสอบปลายภาค

เนื้อหา:

- ทบทวนบทที่ 5–8
- ชักถามปัญหาและประเด็นสำคัญ
- แนวข้อสอบปลายภาค

กิจกรรม:

Open Q&A + การสรุปภาพรวมมาตรการความมั่นคง

ประเมินผล:

ประเมินผ่านความมีส่วนร่วม

CLO: CLO1–4

✓ แผนการสอนรายสัปดาห์ (12 สัปดาห์) สมบูรณ์แล้ว

หากต้องการผมสามารถจัดทำเพิ่มเติมได้ เช่น

- 📌 ทำแผนสอนรายคาบ (Lesson Plan)
- 📌 ออกแบบ Rubric การประเมินแต่ละกิจกรรม
- 📌 จัดทำเอกสารเป็นไฟล์ Word/ PDF
- 📌 จัดทำสไลด์ประกอบการสอน 12 สัปดาห์

แจ้งได้เลยครับ.