

## มคอ.3 รายละเอียดรายวิชา (Course Specification)

รหัส-ชื่อรายวิชา: IMI62-332 ความมั่นคงสารสนเทศทางการแพทย์ (Medical Information Security)

ภาคการศึกษา: 2/2568

หลักสูตร: นวัตกรรมสารสนเทศทางการแพทย์

สังกัด: มหาวิทยาลัยวลัยลักษณ์

ผู้รับผิดชอบรายวิชา: ผู้ช่วยศาสตราจารย์ ดร.ชนันท์ภรณ์ จันแดง

# หมวดที่ 1 ข้อมูลทั่วไป

## 1.1 รหัสและชื่อรายวิชา

- รหัสรายวิชา: IMI62-332
- ชื่อรายวิชา (ไทย): ความมั่นคงสารสนเทศทางการแพทย์
- ชื่อรายวิชา (อังกฤษ): Medical Information Security

## 1.2 จำนวนหน่วยกิต

3(3-0-6)

- บรรยาย 3 ชั่วโมง
- ศึกษาด้วยตนเอง 6 ชั่วโมง/สัปดาห์

## 1.3 รายวิชาที่ต้องเรียนมาก่อน (Pre-requisite)

- IMI62-232 เครือข่ายคอมพิวเตอร์

## หมวดที่ 2 จุดมุ่งหมายและวัตถุประสงค์ของรายวิชา

### 2.1 จุดมุ่งหมายรายวิชา

รายวิชานี้มุ่งสร้างความรู้ความเข้าใจเกี่ยวกับความมั่นคงสารสนเทศในระบบสาธารณสุข การวิเคราะห์ ภัยคุกคามต่อข้อมูลสุขภาพ การออกแบบมาตรการควบคุมความปลอดภัยข้อมูล ตลอดจนการปฏิบัติ ตามกฎหมายและจริยธรรมด้านข้อมูลผู้ป่วย

## 2.2 วัตถุประสงค์การเรียนรู้ (CLOs) – ตามกรอบ KSEC + Bloom's Taxonomy

CLO	รายละเอียด	หมวด KSEC	ระดับ Bloom's
CLO1	อธิบายหลักการความมั่นคงสารสนเทศทางการแพทย์	Knowledge (K)	Understand
CLO2	วิเคราะห์ภัยคุกคาม ช่องโหว่ และความเสี่ยงในระบบสุขภาพ	Skills (S)	Analyze
CLO3	ประเมินและออกแบบมาตรการควบคุมตามมาตรฐานสากลด้านความมั่นคง	Competency (C)	Evaluate / Create
CLO4	ปฏิบัติตามกฎหมาย จริยธรรม และแนวปฏิบัติด้านข้อมูลสุขภาพ	Ethics (E)	Apply

## หมวดที่ 3 การเชื่อมโยง CLO กับ PLO (CLO-PLO Mapping)

CLO	PLO1	PLO2	PLO3	PLO4	PLO5	PLO6
CLO1	✓					
CLO2		✓	✓			
CLO3		✓	✓	✓		
CLO4						✓

# หมวดที่ 4 เนื้อหารายวิชาและแผนการสอน

## 4.1 เนื้อหารายวิชา (8 บท)

1. บทนำสู่ความมั่นคงสารสนเทศทางการแพทย์
2. ระบบสารสนเทศสุขภาพ (HIS/EHR/EMR/HIE)
3. ความมั่นคงของการสื่อสารข้อมูลสุขภาพ
4. ภัยคุกคาม ช่องโหว่ และการโจมตีไซเบอร์ในระบบสุขภาพ
5. ความมั่นคงของอุปกรณ์การแพทย์ (IoMT Security)
6. การประเมินความเสี่ยงและการคุ้มครองข้อมูลสุขภาพ
7. การตอบสนองเหตุการณ์และ Forensic เบื้องต้น
8. กฎหมาย มาตรฐาน และจริยธรรมด้านข้อมูลสุขภาพ

## 4.2 แผนการสอนรายสัปดาห์ (12 สัปดาห์) – ตารางสมบูรณ์

สัปดาห์	เนื้อหา	กิจกรรมการเรียนรู้ (TLA)	การประเมินผล	CLO
1	บทนำความมั่นคงสารสนเทศ	บรรยาย / ถาม-ตอบ	Quiz 1	CLO1
2	ภัยคุกคามในระบบสุขภาพ	วิเคราะห์ข่าว / Case Ransomware	Worksheet 1	CLO1, CLO2
3	HIS/EHR/EMR/HIE	บรรยาย / วิเคราะห์ระบบจริง	Quiz 2	CLO1
4	ความมั่นคงการสื่อสารข้อมูลสุขภาพ	สาธิต HL7/FHIR / วิเคราะห์การดักฟัง	Quiz 3	CLO1, CLO2
5	ภัยคุกคามและช่องโหว่	Workshop วิเคราะห์	Class	CLO2

# หมวดที่ 5 วิธีการสอนและสื่อการเรียนรู้

## 5.1 วิธีการสอน (Teaching and Learning Activities)

- การบรรยาย (Lecture)
- การอภิปราย (Discussion)
- การวิเคราะห์เหตุการณ์ (Case Study Analysis)
- การจำลองเหตุการณ์ (Tabletop Exercise)
- การทำ Workshop
- รายงานและการนำเสนอ

## 5.2 สื่อการสอน

- Lecture Notes รายสัปดาห์
- เอกสารมาตรฐาน: PDPA, HIPAA, ISO/IEC 27001



## หมวดที่ 6 การประเมินผลการเรียนรู้

รายการประเมิน	สัดส่วน	รายละเอียด	CLO
แบบทดสอบรายบท (Quiz)	30%	ทดสอบความเข้าใจรายสัปดาห์	CLO1, CLO2
รายงานวิเคราะห์ เหตุการณ์	10%	วิเคราะห์เหตุการณ์จริงด้านความมั่นคง สุขภาพ	CLO3
การมีส่วนร่วมในชั้นเรียน	25%	อภิปราย / กิจกรรม / Workshop	CLO1-4
สอบกลางภาค	15%	บทที่ 1-4	CLO1, CLO2
สอบปลายภาค	20%	บทที่ 5-8	CLO3, CLO4

# หมวดที่ 7 ทรัพยากรการเรียนรู้

## 7.1 หนังสือและเอกสารหลัก

- NIST SP 800 Series
- ISO/IEC 27001 & ISO 27799
- HIPAA Security Rule
- WHO & HC3 Threat Reports

## 7.2 เอกสารประกอบ

- Lecture Notes
- บทความวิจัยด้าน IoMT Security
- เอกสาร PDPA ด้านสุขภาพ

## หมวดที่ 8 นโยบายรายวิชา

- ต้องเข้าชั้นเรียนไม่น้อยกว่า 80%
- ไม่อนุญาตให้ทุจริตการสอบหรือคัดลอกงานผู้อื่น
- ส่งงานตามกำหนดเวลา
- เคารพหลักจริยธรรมและความเป็นส่วนตัวของข้อมูลผู้ป่วย
- ปฏิบัติตาม PDPA และกฎระเบียบของหน่วยงานด้านสาธารณสุข

