

รายละเอียดของรายวิชา

มหาวิทยาลัยเอเชียอาคเนย์ SOUTHEAST ASIA UNIVERSITY
คณะ/หลักสูตร/สาขาวิชา คณะศิลปศาสตร์และวิทยาศาสตร์ ☐ หลักสูตร..... ☒ สาขาวิชาเทคโนโลยีดิจิทัลและนวัตกรรม ☐ หมวดวิชาศึกษาทั่วไป

หมวดที่ 1 ข้อมูลทั่วไป

1.1 รหัสและชื่อรายวิชา รหัสวิชา 832209 ชื่อรายวิชา ความมั่นคงของระบบคอมพิวเตอร์ (ภาษาอังกฤษ) (Computer Security)
1.2 จำนวนหน่วยกิต 3 หน่วยกิต (3-0-6)
1.3 ประเภทของรายวิชา ระดับปริญญาตรี ☐ กำหนดให้เรียนโดยไม่นับหน่วยกิต ☐ วิชาเฉพาะ กลุ่มวิชา ☐ แกน ☒ เอกบังคับ ☐ เอกเลือก ☐ วิชาเลือกเสรี ☐ หมวดวิชาศึกษาทั่วไป กลุ่ม ☐ ทักษะทางปัญญา ☐ ทักษะการมีปฏิสัมพันธ์ ☐ ทักษะการเป็นผู้นำตนเอง ☐ ทักษะทางด้านดิจิทัล ระดับปริญญาโท และระดับปริญญาเอก ☐ หมวดวิชาเสริมพื้นฐาน ☐ หมวดวิชาบังคับ ☐ หมวดกลุ่มวิชา.....
1.4 อาจารย์ผู้รับผิดชอบรายวิชา 1) อาจารย์ผู้รับผิดชอบรายวิชา อ.สิทธิ สิตไทย 2) อาจารย์ผู้สอน อ.สิทธิ สิตไทย
1.5 ภาคการศึกษา/ ชั้นปีที่เรียน (ตามแผนการศึกษาของหลักสูตร) ปีการศึกษาที่ xxxx ภาคการศึกษาที่ x ชั้นปีที่เรียน x
1.6 รายวิชาบังคับก่อน (Pre-requisite) (ถ้ามี) รหัสวิชา.....ชื่อรายวิชา.....
1.7 รายวิชาที่ต้องเรียนพร้อมกัน (Co-requisites) (ถ้ามี) รหัสวิชา..... ชื่อรายวิชา.....
1.8 สถานที่เรียน ☒ Onsite ห้อง บรรยาย 1 อาคารพลฤๅณ ประโมทะกะ มหาวิทยาลัยเอเชียอาคเนย์ ☐ Online หลักสูตร (ระบบการศึกษาทางไกลทางอินเทอร์เน็ต)
1.9 วันที่จัดทำหรือปรับปรุงรายละเอียดของรายวิชาครั้งล่าสุด วันที่ 15 กรกฎาคม 2568

หมวดที่ 2 จุดมุ่งหมายและวัตถุประสงค์

2.1 จุดมุ่งหมายของรายวิชา 1) เพื่อให้ผู้เรียนเข้าใจหลักการและเทคนิคด้านความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และเครือข่าย 2) เพื่อให้ผู้เรียนสามารถวิเคราะห์ความเสี่ยง ช่องโหว่ และเปรียบเทียบมาตรการป้องกันเพื่อการตัดสินใจ 3) เพื่อให้ผู้เรียนประยุกต์ใช้เทคนิคการเข้ารหัส การพิสูจน์ตัวตน และการควบคุมการเข้าถึง 4) เพื่อปลูกฝังความรับผิดชอบตนเองและสังคมและการเรียนรู้ต่อเนื่องด้านความมั่นคงปลอดภัยตามแนวทาง OBE
2.2 วัตถุประสงค์ในการพัฒนา/ปรับปรุงรายวิชา ปรับปรุงให้สอดคล้องกับ PLOs (PLO1, PLO2, PLO5) ตามแนวทาง OBE และ AUN-QA โดยเพิ่มปฏิบัติการวิเคราะห์ความมั่นคงปลอดภัยและกรณีศึกษาภัยคุกคามที่ทันสมัย พร้อมการประเมินตามสภาพจริง

ผลลัพธ์การเรียนรู้ของหลักสูตรและผลลัพธ์การเรียนรู้ระดับรายวิชา

ผลลัพธ์การเรียนรู้ของหลักสูตร (PLOs)	ผลลัพธ์การเรียนรู้ 4 ด้าน (ไม่จำเป็นต้องเลือกทุกช่อง)				ผลลัพธ์การเรียนรู้ระดับรายวิชา (CLOs)
PLO1 สามารถสืบค้นและวิเคราะห์ประเด็นปัญหาด้วยการบูรณาการความรู้ทางวิชาการอย่างเป็นระบบ	K ✓	S	E	C	CLO1: สืบค้น วิเคราะห์และบูรณาการความรู้ด้านความมั่นคงของระบบคอมพิวเตอร์และเครือข่ายได้อย่างเป็นระบบเพื่ออธิบายหลักการและออกแบบแนวทางในการพัฒนาแผนและระบบรักษาความมั่นคงปลอดภัยอย่างมีเหตุผล

ผลลัพธ์ การ เรียนรู้ ของ หลักสูตร ร (PLOs)	ผลลัพธ์การ เรียนรู้ 4 ด้าน (ไม่จำเป็นต้อง เลือกทุกช่อง)				ผลลัพธ์การเรียนรู้ระดับรายวิชา (CLOs)
เพื่อ พัฒนา โครงงาน น เทคโนโลยี ดิจิทัล และ นวัตกรรม อย่างมี เหตุผล					
PLO2 สามารถ วิเคราะห์ ห์ เปรียบเทียบ ข้อมูล เชิง ตัวเลข เพื่อการ ตัดสินใจ ที่ น่าเชื่อถือ ด้วย ทักษะ ปัญหา เพื่อ สร้างสร	K	S ✓	E	C	CLO2: วิเคราะห์และเปรียบเทียบข้อมูล/ทางเลือกเชิงเทคนิคของความมั่นคงของระบบคอมพิวเตอร์แ ละเครือข่ายเพื่อการตัดสินใจที่น่าเชื่อถือ และลงมือสร้างสรรค์แผนและระบบรักษาความมั่นคงปลอดภัยด้วยเครื่องมือดิจิทัล

ผลลัพธ์ การ เรียนรู้ ของ หลักสูตร ร (PLOs)	ผลลัพธ์การ เรียนรู้ 4 ด้าน (ไม่จำเป็นต้อง เลือกทุกช่อง)				ผลลัพธ์การเรียนรู้ระดับรายวิชา (CLOs)
รศ ผลงาน โครงงาน น เทคโนโลยี ดิจิทัล และ นวัตกรรม					
PLO5 แสดงออก ถึง ทัศนคติ เชิงบวก ยอมรับ ฟังความ คิดเห็น ของ ผู้อื่น รับผิดชอบ ต่อ ตนเอง และ สังคม เพื่อ พัฒนา การ เรียนรู้	K	S	E	C	CLO3: แสดงออกถึงทัศนคติเชิงบวก ยอมรับฟังความคิดเห็นของผู้อื่น รับผิดชอบต่อตนเองและสังคม และพัฒนาการเรียนรู้ของตนเองอย่างต่อเนื่องในการเรียนรู้ความมั่นคงของระบบคอมพิวเตอร์ และเครือข่าย
				✓	

ผลลัพธ์ การเรียนรู้ ของ หลักสูตร (PLOs)	ผลลัพธ์การ เรียนรู้ 4 ด้าน (ไม่จำเป็นต้อง เลือกทุกช่อง)	ผลลัพธ์การเรียนรู้ระดับรายวิชา (CLOs)			
ของ ตนเอง อย่าง ต่อเนื่อง					

หมวดที่ 3 ลักษณะและการดำเนินการ

● 3.1 คำอธิบายรายวิชา (Course Description)

เทคนิคการวิเคราะห์ความปลอดภัยและความมั่นคงในระดับต่าง ๆ ของเครือข่ายแบบเปิด เทคโนโลยีด้านความปลอดภัยของเครือข่ายคอมพิวเตอร์ เทคนิคการเข้ารหัส การรับรองความถูกต้อง (Authentication), การควบคุมการเข้าถึง (Access Control), การจัดการช่องโหว่ (Vulnerability Management), และการรักษาความปลอดภัยในระบบคลาวด์ ความปลอดภัยในเครือข่ายอินเทอร์เน็ต ไวรัส เวิร์ม ไฟล์วอลล์ การบริหารความปลอดภัยเทคโนโลยีสารสนเทศ การป้องกันการโจมตีทางไซเบอร์ เช่น การโจมตีแบบฟิชซิง (Phishing), มัลแวร์ (Malware), และการโจมตี DDoS

Principles of network security on various levels of open systems. Technology on computer network security. Cryptosystem techniques, authentication, access control, vulnerability management, and cloud security. Security on Internet systems. Virus, worm, and firewall. Security management on information technology. How to defend against cyberattacks such as phishing, malware, and DDoS attacks.

3.2 จำนวนชั่วโมงที่ใช้ต่อภาคการศึกษา

บรรยาย	สอนเสริม (ถ้ามี)	การฝึกปฏิบัติ/งานภาคสนาม/ การฝึกงาน	การศึกษาด้วยตนเอง
-	-	80 ชั่วโมงต่อภาคการศึกษา	45 ชั่วโมงต่อภาคการศึกษา

3.3 จำนวนชั่วโมงต่อสัปดาห์ที่อาจารย์ให้คำปรึกษาและแนะนำทางวิชาการแก่นักศึกษาเป็นรายบุคคล

ให้คำปรึกษาและคำแนะนำทางวิชาการแก่นักศึกษาเป็นรายบุคคล โดยนัดล่วงหน้าเพื่อพบปะอาจารย์ผู้สอน และใช้สื่อเทคโนโลยีต่าง ๆ ได้แก่ E-mail: sitthai@sau.ac.th

หมวดที่ 4 การพัฒนาผลการเรียนรู้ของนักศึกษา

การพัฒนาผลการเรียนรู้ในมาตรฐานผลการเรียนรู้แต่ละด้านที่มุ่งหวัง ซึ่งต้องสอดคล้องกับที่ระบุไว้ในรายละเอียดของหลักสูตร โดยมาตรฐานการเรียนรู้แต่ละด้าน ให้แสดงข้อมูลต่อไปนี้

- 1) สรุปล้น ๆ เกี่ยวกับความรู้ หรือทักษะที่รายวิชามุ่งหวังที่จะพัฒนานักศึกษา
- 2) คำอธิบายเกี่ยวกับวิธีการสอนที่จะใช้ในรายวิชาเพื่อพัฒนาความรู้ หรือทักษะในข้อ 1
- 3) วิธีการที่จะใช้วัดและประเมินผลการเรียนรู้ของนักศึกษาในรายวิชานี้เพื่อประเมินผลการเรียนรู้ในมาตรฐานการเรียนรู้ แต่ละด้านที่เกี่ยวข้อง

กลยุทธ์การพัฒนานักศึกษาตามผลลัพธ์การเรียนรู้ที่คาดหวังของรายวิชา

ผลลัพธ์การเรียนรู้ที่คาดหวังของรายวิชา (CLOs)	ผลลัพธ์การเรียนรู้ที่คาดหวังของหลักสูตร (PLOs) ที่รายวิชารับผิดชอบ	กลยุทธ์การสอน ตาม CLOs	กลยุทธ์สำหรับวิธีการวัดและประเมินผล ตาม CLOs
CLO1: สืบค้น วิเคราะห์ และบูรณาการความรู้ด้านความมั่นคงของระบบคอมพิวเตอร์และเครือข่ายได้อย่างเป็นระบบ เพื่ออธิบายหลักการและออกแบบแนวทางในการพัฒนาแผนและระบบรักษาความมั่นคงปลอดภัยอย่างมีเหตุผล	PLO1	จัดการเรียนรู้แบบบรรยายเชิงปฏิสัมพันธ์ (Interactive Lecture) ร่วมกับการเรียนรู้โดยใช้ปัญหาเป็นฐาน (Problem-based Learning) การอภิปรายกรณีศึกษา และมอบหมายให้สืบค้น วิเคราะห์ และสังเคราะห์องค์ความรู้อย่างเป็นระบบ เพื่อบูรณาการความรู้สู่การพัฒนาโครงงาน	ประเมินจากการสอบข้อเขียน (สอบกลางภาค/ปลายภาค) แบบทดสอบย่อย และรายงานการวิเคราะห์/ สืบค้น โดยใช้เกณฑ์การให้คะแนน แบบรูบริก (Rubric)
CLO2: วิเคราะห์และเปรียบเทียบข้อมูล/ทางเลือกเชิงเทคนิคของความมั่นคงของระบบคอมพิวเตอร์และเครือข่ายเพื่อการตัดสินใจที่น่าเชื่อถือ และลงมือสร้างสรรค์แผนและระบบรักษาความมั่นคงปลอดภัยด้วยเครื่องมือดิจิทัล	PLO2	จัดการเรียนรู้โดยการสาธิต และฝึกปฏิบัติในห้องปฏิบัติการ (Demonstration & Hands-on Lab) การเรียนรู้โดยใช้โครงงานเป็นฐาน (Project-based Learning) และการฝึกวิเคราะห์เปรียบเทียบทางเลือก/ข้อมูลเชิงตัวเลขเพื่อการตัดสินใจเชิงเท	ประเมินจากผลงานปฏิบัติและโครงงาน ใบงาน และการสอบปฏิบัติ ด้วยการประเมินตามสภาพจริง (Authentic Assessment) และเกณฑ์รูบริกเชิงสมรรถนะ

		เทคนิคในการสร้างสรรค์ผลงาน	
CLO3: แสดงออกถึงทัศนคติเชิงบวก ยอมรับฟังความคิดเห็นของผู้อื่น รับผิดชอบต่อตนเองและสังคม และพัฒนาการเรียนรู้ของตนเองอย่างต่อเนื่องในการเรียนรู้ความมั่นคงของระบบคอมพิวเตอร์และเครือข่าย	PLO5	จัดการเรียนรู้แบบสะท้อนคิด (Reflective Learning) ส่งเสริมการทำงานกลุ่มที่เปิดรับฟังความคิดเห็นของผู้อื่น การเรียนรู้ด้วยตนเองอย่างต่อเนื่อง และการรับผิดชอบต่อตนเองและสังคม	ประเมินจากการสะท้อนคิด การมีส่วนร่วมในชั้นเรียน การยอมรับฟังความคิดเห็นและการพัฒนาตนเอง ด้วยแบบประเมินตนเองและการประเมินโดยเพื่อน (Self & Peer Assessment)

4.1 แผนที่แสดงการกระจายความรับผิดชอบ PLOs ของหลักสูตรฯ ต่อรายวิชา

รายวิชา	Program Learning Outcome (PLOs)				
	PLO1	PLO2	PLO3	PLO4	PLO5
832209 ความมั่นคงของระบบคอมพิวเตอร์	An	An			Ap

Bloom's Taxonomy: **R** = Remembering; **U** = Understanding; **AP** = Applying; **AN** = Analyzing; **E** = Evaluating; **C** = Creating

หมายเหตุ 1. PLOs Curriculum Mapping ให้หลักสูตรมีรายวิชาที่กระจายความรับผิดชอบต่อผลลัพธ์การเรียนรู้แต่ละด้านให้ครบทุกข้อ
2. ระบุแนวคิด Bloom's Taxonomy ลงในช่องว่าง ให้มีความสัมพันธ์และเชื่อมโยงกับผลลัพธ์การเรียนรู้ระดับรายวิชา (Course Learning Outcomes: CLOs) และรายละเอียดผลลัพธ์การเรียนรู้ 4 ด้านดังนี้

R = Remember หมายถึง มีความสามารถในการจดจำ/รับรู้

Ap = Apply หมายถึง มีความสามารถนำไปใช้ในการแก้ปัญหาหรือปรับใช้ได้

E = Evaluate หมายถึง ประเมินและสามารถนำมาใช้ในการตัดสินใจได้

U = Understand หมายถึง มีความสามารถในการจับสาระสำคัญ และแสดงออกให้เห็นได้

An = Analyze หมายถึง วิเคราะห์ แยกแยะได้

C = Create หมายถึง สร้างสรรค์ คิดค้น พัฒนา

หมวดที่ 5 แผนการสอนและการประเมินผล

5.1 แผนการสอน

ภาคบรรยาย/ภาคปฏิบัติ							
สัปดาห์ที่	หัวข้อ/ รายละเอียด	CLOs	จำนวน ชั่วโมง	กิจกรรม การเรียนรู้ การสอน	สื่อที่ใช้/ แหล่งการ เรียนรู้	ผลลัพธ์ (Output)	ผู้สอน
1	แนะนำรายวิชา แนวคิดความ มั่นคงปลอดภัยและหลัก CIA (Confidentiality/Integrity/Availability)	CLO1	5	บรรยายเชิงปฏิสัมพันธ์ อภิปราย และวิเคราะห์กรณีศึกษา (Interactive Lecture & Case Discussion)	เอกสารประกอบการสอน/ สไลด์, ระบบ e-Learning (sau.ac.th), เครื่องมือวิเคราะห์ความมั่นคงปลอดภัย (Wireshark/Nmap/Kali Linux) และเครื่องมือเข้ารหัส/ทดสอบเจาะระบบ, บทความ/สื่อออนไลน์ และแหล่งเรียนรู้เปิด	สรุปหลักความมั่นคงปลอดภัย	อ.สิทธิ
2	ภัยคุกคาม การโจมตีและการประเมินความเสี่ยง	CLO1	5	บรรยายเชิงปฏิสัมพันธ์ อภิปราย และวิเคราะห์กรณีศึกษา (Interactive Lecture & Case Discussion)	เอกสารประกอบการสอน/ สไลด์, ระบบ e-Learning (sau.ac.th), เครื่องมือวิเคราะห์ความมั่นคงปลอดภัย (Wireshark/Nmap/Kali Linux) และเครื่องมือเข้ารหัส/ทดสอบ	รายงานวิเคราะห์ภัยคุกคาม	อ.สิทธิ

					ออบจาระบบ , บทความ/สื่อ ออนไลน์ และแหล่งเรีย ไขข้อมูล		
3	พื้นฐานวิทยา การเข้ารหัส (Cryptograp hy)	CLO1, CLO2	5	สาธิตและฝึก ปฏิบัติในห้อง ปฏิบัติการพร ้อมใบงาน (Demonstra tion & Hands-on Lab)	เอกสารประก อบการสอน/ สไลด์, ระบบ e-Learning (sau.ac.th), เครื่องมือวิเค าะห์ความม ั่นคงปลอดภัย (Wireshark/ Nmap/Kali Linux) และเครื่องมือ เข้ารหัส/ทดส ออบจาระบบ , บทความ/สื่อ ออนไลน์ และแหล่งเรีย ไขข้อมูล	ใบงานการเข้า รหัส	อ.สิทธิ์
4	การเข้ารหัสแ ขงสมมาตรแ ละอสมมาตร	CLO1, CLO2	5	สาธิตและฝึก ปฏิบัติในห้อง ปฏิบัติการพร ้อมใบงาน (Demonstra tion & Hands-on Lab)	เอกสารประก อบการสอน/ สไลด์, ระบบ e-Learning (sau.ac.th), เครื่องมือวิเค าะห์ความม ั่นคงปลอดภัย (Wireshark/ Nmap/Kali Linux) และเครื่องมือ เข้ารหัส/ทดส ออบจาระบบ	โปรแกรมเข้า รหัส/ถอดรหั ส	อ.สิทธิ์

					, บทความ/สื่อ ออนไลน์ และแหล่งเรีย เรียนรู้เปิด		
5	ฟังก์ชันแฮชแ ละลายเซ็นดิ จิทัล	CLO1, CLO2	5	สาธิตและฝึก ปฏิบัติในห้อง ปฏิบัติการพร อมใบงาน (Demonstra tion & Hands-on Lab)	เอกสารประก อบการสอน/ สไลด์, ระบบ e-Learning (sau.ac.th), เครื่องมือวิเค าะห์ความม้ นคงปลอดภัย (Wireshark/ Nmap/Kali Linux) และเครื่องมือ เข้ารหัส/ทดสอบ เจาะระบบ , บทความ/สื่อ ออนไลน์ และแหล่งเรีย เรียนรู้เปิด	ตัวอย่างแฮชแ ละลายเซ็นดิ จิทัล	อ.สิทธิ
6	การพิสูจน์ตัว ตน (Authentica tion)	CLO1, CLO2	5	สาธิตและฝึก ปฏิบัติในห้อง ปฏิบัติการพร อมใบงาน (Demonstra tion & Hands-on Lab)	เอกสารประก อบการสอน/ สไลด์, ระบบ e-Learning (sau.ac.th), เครื่องมือวิเค าะห์ความม้ นคงปลอดภัย (Wireshark/ Nmap/Kali Linux) และเครื่องมือ เข้ารหัส/ทดสอบ เจาะระบบ ,	ระบบพิสูจน์ตัว ตนตัวอย่าง	อ.สิทธิ

					บทความ/สื่อออนไลน์ และแหล่งเรียนรู้เปิด		
7	การควบคุมการเข้าถึง (Access Control)	CLO1, CLO2	5	การเรียนรู้โดยใช้ปัญหา/โครงงานเป็นฐาน และเวิร์กช็อปกลุ่ม (Problem/Project-based Workshop)	เอกสารประกอบการสอน/สไลด์, ระบบ e-Learning (sau.ac.th), เครื่องมือวิเคราะห์ความมั่นคงปลอดภัย (Wireshark/Nmap/Kali Linux) และเครื่องมือเข้ารหัส/ทดสอบเจาะระบบ , บทความ/สื่อออนไลน์ และแหล่งเรียนรู้เปิด	นโยบายควบคุมการเข้าถึง	อ.สิทธิ
8				สอบกลางภาค			
9	ความมั่นคงปลอดภัยของเครือข่ายแบบเปิด	CLO1, CLO2	5	สาธิตและฝึกปฏิบัติในห้องปฏิบัติการพร้อมใบงาน (Demonstration & Hands-on Lab)	เอกสารประกอบการสอน/สไลด์, ระบบ e-Learning (sau.ac.th), เครื่องมือวิเคราะห์ความมั่นคงปลอดภัย (Wireshark/Nmap/Kali Linux) และเครื่องมือเข้ารหัส/ทดสอบเจาะระบบ ,	รายงานวิเคราะห์ทราฟฟิกเครือข่าย	อ.สิทธิ

					บทความ/สื่อออนไลน์และแหล่งเรียนรู้เปิด		
10	การจัดการช่องโหว่ (Vulnerability Management)	CLO1, CLO2	5	สาธิตและฝึกปฏิบัติในห้องปฏิบัติการพร้อมใบงาน (Demonstration & Hands-on Lab)	เอกสารประกอบการสอน/สไลด์, ระบบ e-Learning (sau.ac.th), เครื่องมือวิเคราะห์ความมั่นคงปลอดภัย (Wireshark/Nmap/Kali Linux) และเครื่องมือเข้ารหัส/ทดสอบเจาะระบบ, บทความ/สื่อออนไลน์และแหล่งเรียนรู้เปิด	รายงานสแกนช่องโหว่	อ.สิทธิ
11	ความมั่นคงปลอดภัยของเว็บไซต์และแอปพลิเคชัน (OWASP)	CLO1, CLO2	5	การเรียนรู้โดยใช้ปัญหา/โครงงานเป็นฐาน และเวิร์กช็อปกลุ่ม (Problem/Project-based Workshop)	เอกสารประกอบการสอน/สไลด์, ระบบ e-Learning (sau.ac.th), เครื่องมือวิเคราะห์ความมั่นคงปลอดภัย (Wireshark/Nmap/Kali Linux) และเครื่องมือเข้ารหัส/ทดสอบเจาะระบบ, บทความ/สื่อ	รายงานทดสอบความปลอดภัยเว็บ	อ.สิทธิ

					ออนไลน์ และแหล่งเรียนรู้อื่นๆ		
12	มัลแวร์และการป้องกัน	CLO1, CLO2	5	สาธิตและฝึกปฏิบัติในห้องปฏิบัติการพร้อมใบงาน (Demonstration & Hands-on Lab)	เอกสารประกอบการสอน/สไลด์, ระบบ e-Learning (sau.ac.th), เครื่องมือวิเคราะห์ความมั่นคงปลอดภัย (Wireshark/Nmap/Kali Linux) และเครื่องมือเข้ารหัส/ทดสอบเจาะระบบ, บทความ/สื่อออนไลน์ และแหล่งเรียนรู้อื่นๆ	รายงานวิเคราะห์มัลแวร์	อ.สิทธิ
13	การเฝ้าระวังและระบบตรวจจับการบุกรุก (IDS/IPS)	CLO1, CLO2	5	สาธิตและฝึกปฏิบัติในห้องปฏิบัติการพร้อมใบงาน (Demonstration & Hands-on Lab)	เอกสารประกอบการสอน/สไลด์, ระบบ e-Learning (sau.ac.th), เครื่องมือวิเคราะห์ความมั่นคงปลอดภัย (Wireshark/Nmap/Kali Linux) และเครื่องมือเข้ารหัส/ทดสอบเจาะระบบ, บทความ/สื่อออนไลน์	การตั้งค่าระบบตรวจจับการบุกรุก	อ.สิทธิ

					และแหล่งเรียนรู้เปิด		
14	นโยบายมาตรฐานกฎหมายและจริยธรรมด้านความมั่นคงปลอดภัย	CLO1, CLO2	5	การเรียนรู้โดยใช้ปัญหา/โครงงานเป็นฐาน และเวิร์กช็อปกลุ่ม (Problem/Project-based Workshop)	เอกสารประกอบการสอน/สไลด์, ระบบ e-Learning (sau.ac.th), เครื่องมือวิเคราะห์ความมั่นคงปลอดภัย (Wireshark/Nmap/Kali Linux) และเครื่องมือเข้ารหัส/ทดสอบเจาะระบบ, บทความ/สื่อออนไลน์ และแหล่งเรียนรู้เปิด	ร่างนโยบายความมั่นคงปลอดภัย	อ.สิทธิ์
15	ปฏิบัติการทดสอบเจาะระบบ (Penetration Testing) ในสภาพแวดล้อมจำลอง	CLO1, CLO2	5	การเรียนรู้โดยใช้ปัญหา/โครงงานเป็นฐาน และเวิร์กช็อปกลุ่ม (Problem/Project-based Workshop)	เอกสารประกอบการสอน/สไลด์, ระบบ e-Learning (sau.ac.th), เครื่องมือวิเคราะห์ความมั่นคงปลอดภัย (Wireshark/Nmap/Kali Linux) และเครื่องมือเข้ารหัส/ทดสอบเจาะระบบ, บทความ/สื่อออนไลน์	รายงานผลการทดสอบเจาะระบบ	อ.สิทธิ์

					และแหล่งเรียนรู้เปิด		
16	เวิร์กช็อปโครงการความมั่นคงปลอดภัยและการนำเสนอ/สรุปรายวิชา	CLO2, CLO3	5	นำเสนอผลงาน อภิปราย และสะท้อนผลการเรียนรู้ร่วมกัน (Presentation & Reflection)	เอกสารประกอบการสอน/สไลด์, ระบบ e-Learning (sau.ac.th), เครื่องมือวิเคราะห์ความมั่นคงปลอดภัย (Wireshark/Nmap/Kali Linux) และเครื่องมือเข้ารหัส/ทดสอบเจาะระบบ, บทความ/สื่อออนไลน์ และแหล่งเรียนรู้เปิด	โครงงานและสไลด์นำเสนอ	อ.สิทธิ์
	รวม	80					
คำอธิบาย ควรมีช่วงเวลาสำหรับชี้แจงนักศึกษาให้ทราบถึงจุดมุ่งหมายของรายวิชา คำอธิบายรายวิชา ผลลัพธ์การเรียนรู้ระดับรายวิชา วิธีการเรียนการสอน และวิธีการวัดและประเมินผล							

5.2 แผนการประเมินตามผลลัพธ์การเรียนรู้ที่คาดหวังของรายวิชา				
การวัดผล				
ที่	ผลลัพธ์การเรียนรู้ที่คาดหวังของรายวิชา (CLOs)	วิธีการประเมินผลการเรียนรู้ของผู้เรียน	สัปดาห์ที่ประเมิน	สัดส่วนของการประเมินผล (รวม 100%)
1	CLO1, CLO2	ความรับผิดชอบต่อการเรียน การสอบกลางภาค	8	30
2	CLO2, CLO3	งานมอบหมาย การนำเสนอ	ตลอดภาคการศึกษา (สัปดาห์ที่ 3-15)	30
3	CLO1, CLO2	คะแนนสอบปลายภาค	17	40
เกณฑ์การประเมินผลรายวิชา				

1) องค์ประกอบของการประเมินผลการเรียน

ระดับคะแนน	ช่วงระดับคะแนน
A	80%ขึ้นไป
B+	75-79%
B	70-74%
C+	65-69%
C	60-64%
D+	55-59%
D	50-54%
F	ต่ำกว่า 50%

2) ระบบการประเมินผลการเรียน ซึ่งมีรายละเอียดดังนี้

เนื้อหาที่ประเมิน	เกณฑ์การประเมิน
การประเมินหลังการเรียน	เป็นไปตามเกณฑ์ที่กำหนดโดยอาจารย์ผู้สอนในแต่ละส่วนของเนื้อหารายวิชา
การประเมินผลจาก “กรณีศึกษา” ที่อาจารย์ผู้สอนยกตัวอย่าง	เป็นไปตามเกณฑ์ที่กำหนดโดยอาจารย์ผู้สอนในแต่ละส่วนของเนื้อหารายวิชา
การนำเสนอ	ประเมินโดยใช้ Scoring Rubric สำหรับการทำงานกลุ่ม โดยใช้เกณฑ์การประเมินการนำเสนอ แบ่งออกเป็น 1) เนื้อหา 2) วิธีการพุดนำเสนอ 3) เวลาที่ใช้ในการนำเสนอ 4) การใช้เทคโนโลยีในการนำเสนอและการให้คะแนนการเข้าร่วมฟังการนำเสนอ

คำอธิบาย * ระบุผลการเรียนรู้หัวข้อย่อยตามที่ปรากฏในแผนที่แสดงการกระจายความรับผิดชอบของรายวิชา (Curriculum Mapping) ของรายละเอียดหลักสูตร (แบบ SAU-OBE-02)

* วิธีการประเมิน เช่น ประเมินจากการเขียนรายงานหรือโครงงานหรือการทดสอบ

3) ในกรณีที่มีข้อสงสัย นักศึกษาสามารถขอตรวจสอบผลการเรียนของรายวิชานี้ได้ โดยยื่นคำร้องไปยังหัวหน้าสาขาวิชา/ผู้อำนวยการหลักสูตร ภายในระยะเวลา 1 สัปดาห์

หมวดที่ 6 ทรัพยากรประกอบการเรียนการสอน

6.1 ตำราและเอกสารหลักที่ใช้ประกอบการเรียน (ระบุตำรา และเอกสารหลักหรือข้อมูลที่เป็นประโยชน์อื่น ๆ ที่ใช้ในการเรียนการสอน) เอกสารประกอบการสอนความมั่นคงของระบบคอมพิวเตอร์. และ Stallings, W. Cryptography and Network Security. Pearson.
6.2 อุปกรณ์การสอนอื่น ๆ (ถ้ามี) (ระบุเอกสารสำคัญอื่น ๆ ที่ใช้ประกอบการเรียนการสอน เช่น สื่ออิเล็กทรอนิกส์ หรือแหล่งสืบค้นอื่นๆ) สื่ออิเล็กทรอนิกส์บนระบบ e-Learning (sau.ac.th), เอกสารมาตรฐาน (NIST, OWASP), แหล่งเรียนรู้และห้องปฏิบัติการจำลองด้านความมั่นคงปลอดภัย
6.3 ทรัพยากรหรือวิธีการใช้ในการพัฒนาทักษะภาษาอังกฤษของนักศึกษา (ถ้ามี) -
6.4 การบรรยายโดยผู้มีประสบการณ์ทางวิชาการหรือวิชาชีพจากหน่วยงานหรือชุมชนภายนอก (ถ้ามี) -
6.5 การดูงานนอกสถานที่ในรายวิชา (ถ้ามี) -

หมวดที่ 7 การประเมินและปรับปรุงการดำเนินการของรายวิชา

7.1 กลยุทธ์การประเมินประสิทธิผลของรายวิชาโดยนักศึกษา 1) การประเมินผลการดำเนินการตามแผนการสอน 2) การประเมินผลการศึกษาของผู้เรียนตามด้านการพัฒนาผลการเรียนรู้ของนักศึกษา 3) การประเมินการประเมินการสอนของอาจารย์โดยนักศึกษาจากระบบ sau.ac.th
7.2 กลยุทธ์การประเมินการสอน 1) การปรับเนื้อหาการสอนให้สอดคล้องกับผลการเรียนรู้ที่คาดหวังของหลักสูตรตามที่ระบุใน SAU-OBE-02 2) การปรับกิจกรรมการเรียนรู้ของรายวิชาให้สอดคล้องกับผลการเรียนรู้ที่คาดหวังของหลักสูตรตามที่ระบุใน SAU-OBE-02
7.3 การปรับปรุงการสอน (อธิบายกลไกและวิธีการปรับปรุงการสอนว่ามีกลไกและวิธีการปรับปรุงการสอนไว้อย่างไรบ้าง) ตัวอย่างเช่น 1) บันทึกข้อมูลและสัมภาษณ์นักศึกษาที่ลงทะเบียนในรายวิชา 2) ปรับปรุงการสอนผ่านการสัมมนาอาจารย์ผู้สอนเมื่อสิ้นภาคการศึกษา
7.4 การทวนสอบมาตรฐานผลสัมฤทธิ์รายวิชาของนักศึกษา (อธิบายกระบวนการที่ใช้ในการทวนสอบมาตรฐานผลสัมฤทธิ์ของนักศึกษาตามมาตรฐานผลการเรียนรู้ของรายวิชา) 1) ทวนสอบจากคะแนนข้อสอบ หรืองานที่มอบหมาย

2) ทวนสอบมาตรฐานผลสัมฤทธิ์ของนักศึกษาโดยระบบคณะกรรมการบริหารหลักสูตร 3) ในระหว่างกระบวนการสอนรายวิชา เปิดโอกาสให้นักศึกษาสะท้อน (feed back) และมีการทวนสอบผลสัมฤทธิ์ในรายหัวข้อตามที่คาดหวังจากการเรียนรู้ในรายวิชา อาจได้จากการสอบถามหรือการสุ่มตรวจผลงานของนักเรียน รวมถึงพิจารณาจากการทดสอบย่อยและหลังจากการออกผลการเรียนรายวิชาหรือการวิเคราะห์ข้อสอบ
7.5 การดำเนินการทบทวนและการวางแผนปรับปรุงประสิทธิผลของรายวิชา (อธิบายกระบวนการในการนำข้อมูลที่ได้จากการประเมินเพื่อปรับปรุงคุณภาพ) นำผลการประเมินประสิทธิผลของรายวิชาโดยนักศึกษา ผลสัมฤทธิ์การเรียนรู้ตามผลลัพธ์การเรียนรู้ที่คาดหวัง และผลการทวนสอบมาตรฐานผลสัมฤทธิ์ มาวิเคราะห์ร่วมกันในการสัมมนาอาจารย์ผู้สอนเมื่อสิ้นภาคการศึกษา เพื่อปรับปรุงเนื้อหา กิจกรรมการเรียนรู้แบบ Active Learning สื่อการสอน และวิธีการวัดและประเมินผลให้สอดคล้องกับผลลัพธ์การเรียนรู้ระดับรายวิชา (CLOs) และของหลักสูตร (PLOs) ตามวงจรคุณภาพ PDCA แล้วจัดทำรายงานผลการดำเนินการของรายวิชา (แบบ SAU-OBE-04/มคอ.5) เสนอต่อคณะกรรมการบริหารหลักสูตร เพื่อวางแผนพัฒนาและปรับปรุงในปีการศึกษาถัดไป

ลงชื่อ: อ.สิทธิ สิตไทย อาจารย์ผู้รับผิดชอบรายวิชา วันที่ 15 กรกฎาคม 2568	
ระดับปริญญาตรี ลงชื่อ: หัวหน้าสาขาวิชา วันที่.....	หลักสูตรระดับปริญญาโท/ปริญญาเอก ลงชื่อ: ผู้อำนวยการหลักสูตร วันที่.....
	หลักสูตรระดับปริญญาโท/ปริญญาเอก ลงชื่อ: คณบดี วันที่.....