มคอ. 3 รายละเอียดของรายวิชา

Course Specification

0214336 ความปลอดภัยบนเครือข่ายคอมพิวเตอร์

Security in Computer Networks

รายวิชานี้เป็นส่วนหนึ่งของหลักสูตรวิทยาศาสตรบัณฑิต

สาขาวิชาวิทยาการคอมพิวเตอร์

หลักสูตรปรับปรุง พ.ศ. 2560

คณะวิทยาศาสตร์และนวัตกรรมดิจิทัล

มหาวิทยาลัยทักษิณ

สารบัญ

หมวด		หน้า
หมวดที่ 1	ข้อมูลทั่วไป	2
หมวดที่ 2	จุดมุ่งหมายและวัตถุประสงค์	4
หมวดที่ 3	ลักษณะการดำเนินการ	5
หมวดที่ 4	การพัฒนาผลการเรียนรู้ของนิสิต	6
หมวดที่ 5	แผนการสอนและการประเมินผล	11
หมวดที่ 6	ทรัพยากรประกอบการเรียนการสอน	20
หมวดที่ 7	การประเมินและปรับปรุงการดำเนินการของรายวิชา	21

รายละเอียดของรายวิชา

หมวดที่ 1 ข้อมูลทั่วไป

1. รหัส ชื่อรายวิชา จำนวนหน่วยกิต รายวิชาที่ต้องเรียนมาก่อน รายวิชาที่เรียนพร้อมกัน และคำอธิบายรายวิชา

0214336 ความปลอดภัยบนเครือข่ายคอมพิวเตอร์ 3(3-0-6)

Security in Computer Networks

บุรพวิชา : -

ควบคู่ : -

แนวคิดเกี่ยวกับความปลอดภัยเครือข่ายคอมพิวเตอร์ การเกิดภัยพิบัติด้านต่างๆของระบบงานคอมพิวเตอร์ การสร้างความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ การระบุตัวตน การตรวจสอบสิทธิ เทคนิคการเข้ารหัสข้อมูลแบบต่างๆ ลายมือชื่อดิจิตอล ไฟร์วอลล์ ระบบการป้องกัน ระบบการตรวจจับการบุกรุก การฟื้นฟูระบบเครือข่ายจากภัยพิบัติ

Computer network security concepts; threads and attacks; security in network system development; identifications and authentications; encryption and cryptography; digital signature; firewalls; intrusions; detection system; security network system disaster recovery

2. หลักสูตรและประเภทของรายวิชา

☑ วิชาเอกเลือก

3. อาจารย์ผู้รับผิดชอบรายวิชาและอาจารย์ผู้สอน

อาจารย์ผู้รับผิดชอบรายวิชา/อาจารย์ผู้สอนรายวิชา อาจารย์ ดร.ณภัทร แก้วภิบาล

4. ภาคการศึกษา/ ชั้นปีที่เรียน

ภาคการศึกษาที่ 2 ปีการศึกษา 2565 นิสิตชั้นปีที่ 3 สาขาวิชาวิทยาการคอมพิวเตอร์

5. สถานที่เรียน

วันจันทร์ เวลา 16.10 - 17.10 น. ห้อง SC1304 และ

วันศุกร์ เวลา 13.00 - 15.00 น. ห้อง SC1443

มหาวิทยาลัยทักษิณ วิทยาเขตพัทลุง

ช่องทางการเรียนออนไลน์ (สามารถเลือกได้มากกว่า 1 ช่องทาง)

- ☐ Webex
- ☑ TSU MOOC
- ☐ Google Classroom
- ☐ อื่นๆ โปรดระบุ.....

6. วันที่จัดทำหรือปรับปรุงรายละเอียดของรายวิชาครั้งล่าสุด

13 พฤศจิกายน 2566

หมวดที่ 2 จุดมุ่งหมายและวัตถุประสงค์

1. จุดมุ่งหมายของรายวิชา / ผลลัพธ์การเรียนรู้ของรายวิชา (Courses Learning Outcome :CLOs) ที่สอดคล้องกับ Programme Learning Outcome, PLOs และ Curriculum Mapping (ซึ่งตรงกับ มคอ.2)

เพื่อให้นิสิตเกิดการเรียนรู้/มีความสามารถ/มีสมรรถนะที่ต้องการด้านต่าง ๆ

CLO1 เข้าใจหลักการหลักการความปลอดภัยในเครือข่ายคอมพิวเตอร์และระบบสารสนเทศได้

CLO2 ระบุลักษณะของภัยคุกคามในเครือข่ายคอมพิวเตอร์และระบบสารสนเทศได้

CLO3 อธิบายเทคนิคการเข้ารหัสข้อมูลแบบสมมาตรและอสมมาตรได้ถูกต้อง

CLO4 สามารถนำเทคนิคการเข้ารหัสข้อมูลไปใช้ในการรักษาความปลอดภัยของข้อมูลในระบบสารสนเทศได้อย่างถูกต้องและเหมาะสม

CLO5 อธิบายความสำคัญของการระบุตัวตน การตรวจสอบสิทธิ และการใช้งานลายมือดิจิทัลในการรักษาความปลอดภัยของเครือข่ายและระบบสารสนเทศ

CLO6 อธิบายความสำคัญของระบบตรวจจับ ป้องกันการบุกรุก และไฟร์วอลล์ในระบบเครือข่าย

CLO7 เข้าใจหลักการและวิธีการฟื้นฟูระบบเครือข่ายจากสถานการณ์ฉุกเฉิน

CLO8 มีจรรยาบรรณทางวิชาการและวิชาชีพในการรักษาความปลอดภัยของเครือข่ายและระบบสารสนเทศ

2. วัตถุประสงค์ของรายวิชา

2.1 เพื่อให้ผู้เรียนมีมีความรู้และความเข้าใจหลักการความปลอดภัยในเครือข่ายคอมพิวเตอร์และระบบสารสนเทศในองค์กร การใช้งานเครื่องสำหรับการจัดการความปลอดภัยในเครือข่าย ความปลอดภัยของสารสนเทศ การติดตามสถานการณ์ภัยคุกคามทางเครือข่ายคอมพิวเตอร์

2.2 เพื่อนำความรู้และทักษะการรักษาความปลอดภัยในเครือข่ายคอมพิวเตอร์ เพื่อแก้ไขปัญหาทางคอมพิวเตอร์ ซึ่งสอดคล้องกับการเติบโตของเทคโนโลยีและตลาดแรงงานด้านวิทยาการคอมพิวเตอร์ โดยพัฒนาให้เป็นไปตามกรอบมาตรฐานคุณวุฒิระดับอุดมศึกษา พ.ศ. 2552

หมวดที่ 3 ลักษณะการดำเนินการ

1. จำนวนชั่วโมงที่ใช้ต่อภาคการศึกษา

บรรยาย	สอนเสริม	การฝึกปฏิบัติ/การฝึกงานภาคสนาม	การศึกษาด้วยตนเอง
3 ชั่วโมงต่อสัปดาห์ x 15 สัปดาห์ = 45 ชั่วโมง	ตามความต้องการของนิสิต	ไม่มี	6 ชั่วโมงต่อสัปดาห์ x 15 สัปดาห์ = 90 ชั่วโมง

คำชี้แจง ภาคการศึกษาจะต้องไม่น้อยกว่า 15 สัปดาห์

2. จำนวนชั่วโมงต่อสัปดาห์ที่ และช่องทางในการให้คำปรึกษาแนะนำทางวิชาการแก่นิสิตเป็นรายบุคคล

อาจารย์จัดเวลาให้คำปรึกษาเป็นรายบุคคลหรือรายกลุ่มตามความต้องการ ประมาณ 1 ชั่วโมงต่อสัปดาห์ (เฉพาะรายที่ต้องการ) ผ่านทางช่องทางติดต่อสื่อสารให้คำปรึกษาต่อไปนี้

- ❑ ห้องทำงาน SC1407
- ❑ E-mail: naphat.k@tsu.ac.th
- ❑ เบอร์โทรศัพท์ 088-7607910
- ❑ Line ID: pingnaphat
- ❑ Line Group: 66-2-NetworkSec.CS

หมวดที่ 4 การพัฒนาผลการเรียนรู้ของนิสิต

1. แผนที่การกระจายความรับผิดชอบ (นำข้อมูลจาก ข้อ 3 หมวดที่ 4 ในเล่ม มคอ.2)

ระบุวิธีการประเมินผลการเรียนรู้หัวข้อย่อยแต่ละหัวข้อตามที่ปรากฏในแผนที่แสดงการกระจายความรับผิดชอบของรายวิชา (Curriculum Mapping) ตามที่กำหนดใน เล่ม มคอ.2 สัปดาห์ที่ประเมิน และสัดส่วนของการประเมิน

1. ด้านคุณธรรม จริยธรรม							2. ด้านความรู้								3. ด้านทักษะทางปัญญา				4. ด้านทักษะความสัมพันธ์ระหว่างบุคคลและความรับผิดชอบ						5. ด้านทักษะการวิเคราะห์เชิงตัวเลข การสื่อสาร และการใช้เทคโนโลยีสารสนเทศ			
1.1	1.2	1.3	1.4	1.5	1.6	1.7	2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8	3.1	3.2	3.3	3.4	4.1	4.2	4.3	4.4	4.5	4.6	5.1	5.2	5.3	5.4
						●	●	●	●	●			●		●		●											
ELO 6							ELO 1 2 3 4 5								ELO 2 3													

หมายเหตุ ELO1 สามารถอธิบายทฤษฎีพื้นฐานทางวิทยาการคอมพิวเตอร์ได้

ELO2 สามารถวิเคราะห์ และแก้ปัญหาโดยใช้วิธีการทางวิทยาการคอมพิวเตอร์ได้อย่างถูกต้อง

ELO3 สามารถใช้ทักษะ เทคนิคปัจจุบัน และเครื่องมือที่จำเป็นในการแก้ปัญหาทางคอมพิวเตอร์

ELO4 สามารถออกแบบระบบคอมพิวเตอร์และระบบสารสนเทศที่ถูกต้องตามความต้องการ

ELO5 สามารถพัฒนาระบบคอมพิวเตอร์ และระบบสารสนเทศที่มีประสิทธิภาพอย่างสร้างสรรค์ จากการประยุกต์เครื่องมือและเทคโนโลยีสมัยใหม่

ELO6 มีจรรยาบรรณเชิงวิชาการ และวิชาชีพ ไม่คัดลอกงานผู้อื่น และมีการอ้างอิงแหล่งที่มา

ผลการเรียนรู้	ELOs	CLOs	วิธีการสอน	วิธีการประเมินผล
1. ด้านคุณธรรม จริยธรรม				
1.1 ตระหนักในคุณธรรมจริยธรรม			1. บรรยายและยกตัวอย่าง พร้อมสอดแทรกคุณธรรมและจริยธรรมที่เกี่ยวข้องกับความปลอดภัยในเครือข่าย	1. ประเมินจากการสังเกตพฤติกรรมการตรงต่อเวลาในการเข้าชั้นเรียนและการส่งงานตามกำหนดเวลา 2. ประเมินจากการใส่อ้างอิงแหล่งที่มาของการสืบค้นข้อมูลได้ถูกต้อง
1.2 มีวินัย ตรงต่อเวลา และความรับผิดชอบต่อตนเอง วิชาชีพและสังคม				
1.3 มีภาวะความเป็นผู้นำและผู้ตามในการทำงานเป็นทีม				

ผลการเรียนรู้	ELOs	CLOs	วิธีการสอน	วิธีการประเมินผล
1.4 เคารพสิทธิและรับฟังความคิดเห็นของผู้อื่น			2. มอบหมายชิ้นงานให้ทำงานในชั้นเรียนและนอกชั้นเรียน 3. มอบหมายงานให้ศึกษาค้นคว้าข้อมูลพร้อมทั้งสอดแทรกความสำคัญของการใส่อ้างอิงแหล่งที่มา	3. ประเมินจากความรับผิดชอบ และไม่คัดลอกงานของผู้อื่น
1.5 เคารพกฎระเบียบและข้อบังคับต่าง ๆ ขององค์กรและสังคม				
1.6 สามารถวิเคราะห์ผลกระทบจากการใช้คอมพิวเตอร์ต่อบุคคล องค์กร และสังคม				
● 1.7 มีจรรยาบรรณทางวิชาการและวิชาชีพ	6	8		
2. ด้านความรู้				
● 2.1 มีความรู้และความเข้าใจเกี่ยวกับหลักการและทฤษฎีที่ที่สำคัญในเนื้อหาสาขาวิชาวิทยาการคอมพิวเตอร์	1	1, 3, 5, 6, 7	1. การบรรยายในชั้นเรียน การยกตัวอย่างปัญหาของเครือข่ายคอมพิวเตอร์และระบบสารสนเทศและการแก้ไขปัญหาด้วยความรู้ด้วยความปลอดภัยในเครือข่าย 2. มอบหมายงานให้นิสิตศึกษาค้นคว้านอกชั้นเรียน เพื่อให้นิสิตวิเคราะห์ปัญหาและแก้ไขปัญหาด้วยการใช้เครื่องมือที่เหมาะสม 3. เปิดโอกาสให้นิสิตได้มีส่วนร่วมในการวิเคราะห์ปัญหาและร่วมแก้ไขปัญหาตาม	1. ประเมินจากงานที่มอบหมายงานทั้งในและนอกชั้นเรียน 2. ประเมินจากผลการสอบวัดความรู้กลางภาคและปลายภาค 3. ประเมินจากคุณภาพของรายงานการศึกษาค้นคว้า
● 2.2 สามารถวิเคราะห์ปัญหาและอธิบายความต้องการทางคอมพิวเตอร์ รวมทั้งประยุกต์ความรู้ ทักษะและการใช้เครื่องมือที่เหมาะสมกับการแก้ไขปัญหา	2	5, 6, 7		
● 2.3 สามารถวิเคราะห์ ออกแบบ พัฒนา บำรุงรักษา และ/หรือประเมินระบบคอมพิวเตอร์ให้ตรงตามข้อกำหนด	2, 3	4, 5, 6, 7		
● 2.4 สามารถติดตามความก้าวหน้าทางวิชาการและวิวัฒนาการคอมพิวเตอร์เพื่อการนำไปประยุกต์	4, 5	2, 3, 4, 6		
2.5 รู้ เข้าใจและสนใจพัฒนาความรู้ ความชำนาญทางคอมพิวเตอร์อย่างต่อเนื่อง				

ผลการเรียนรู้	ELOs	CLOs	วิธีการสอน	วิธีการประเมินผล
2.6 มีความรู้ในแนวกว้างของสาขาวิชาวิทยาการคอมพิวเตอร์ เล็งเห็นการเปลี่ยนแปลง และเข้าใจผลกระทบของเทคโนโลยีใหม่ ๆ ที่เกี่ยวข้อง			โจทย์ที่ได้รับมอบหมาย	
● 2.7 มีประสบการณ์ในการพัฒนา และ/หรือการประยุกต์ซอฟต์แวร์และฮาร์ดแวร์ที่ใช้งานได้จริง	3, 4, 5	4, 6		
2.8 สามารถบูรณาการความรู้ในสาขาวิชาวิทยาการคอมพิวเตอร์กับความรู้ในศาสตร์อื่น ๆ ที่เกี่ยวข้อง				
3. ด้านทักษะทางปัญญา				
● 3.1 สามารถคิดอย่างมีวิจารณญาณและอย่างเป็นระบบ	2	2, 4, 5, 6	1. กำหนดโจทย์ปัญหาและให้นิสิตร่วมศึกษา วิเคราะห์ และแสดงความคิดเห็น อภิปรายกลุ่ม และร่วมคิดวิธีการแก้ปัญหาอย่างเป็นระบบ 2. กำหนดกรณีศึกษา เพื่อให้นิสิตนำความรู้เทคนิคการรักษาความปลอดภัยมาใช้แก้ปัญหาทางคอมพิวเตอร์ได้ถูกต้อง	1. ประเมินจากงานที่มอบหมายงานทั้งในและนอกชั้นเรียน 2. ประเมินจากผลการสอบวัดความรู้กลางภาคและปลายภาค
3.2 สามารถสืบค้น ตีความ และประเมินสารสนเทศ เพื่อใช้ในการแก้ไขปัญหาอย่างสร้างสรรค์				
● 3.3 สามารถรวบรวม ศึกษา วิเคราะห์ และสรุปประเด็นปัญหาและความต้องการ	2, 3	2, 3, 5		
3.4 สามารถประยุกต์ความรู้และทักษะกับการแก้ไขปัญหาทางคอมพิวเตอร์ได้อย่างเหมาะสม				

ผลการเรียนรู้	ELOs	CLOs	วิธีการสอน	วิธีการประเมินผล
			3. เปิดโอกาสให้นิสิตร่วมอภิปราย/แสดงความคิดเห็น	
4. ทักษะความสัมพันธ์ระหว่างบุคคลและความรับผิดชอบ				
4.1 สามารถสื่อสารกับกลุ่มคนหลากหลายโดยใช้ภาษาไทยได้อย่างมีประสิทธิภาพ				
4.2 สามารถให้ความช่วยเหลือและอำนวยความสะดวกแก่การแก้ปัญหาสถานการณ์ต่าง ๆ ในกลุ่มทั้งในบทบาทของผู้นำ หรือในบทบาทของผู้ร่วมทีมทำงาน				
4.3 สามารถใช้ความรู้ด้านวิทยาการคอมพิวเตอร์มาชี้นำสังคมในประเด็นที่เหมาะสม				
4.4 มีความรับผิดชอบในการกระทำของตนเองและรับผิดชอบงานในกลุ่ม				
4.5 สามารถเป็นผู้ริเริ่มแสดงประเด็นในการแก้ไขสถานการณ์ทั้งส่วนตัวและส่วนรวม พร้อมทั้งแสดงจุดยืนอย่างพอเหมาะทั้งของตนเองและของกลุ่ม				
4.6 มีความรับผิดชอบการพัฒนาการเรียนรู้ทั้งของตนเองและทางวิชาชีพอย่างต่อเนื่อง				
5. ด้านทักษะการวิเคราะห์เชิงตัวเลข การสื่อสาร และการใช้เทคโนโลยีสารสนเทศ				
5.1 มีทักษะในการใช้เครื่องมือที่จำเป็นที่มีอยู่ในปัจจุบันในการทำงานที่เกี่ยวกับคอมพิวเตอร์				

ผลการเรียนรู้	ELOs	CLOs	วิธีการสอน	วิธีการประเมินผล
5.2 สามารถแนะนำประเด็นการแก้ไขปัญหาโดยใช้สารสนเทศทางคณิตศาสตร์หรือการแสดงสถิติประยุกต์ต่อปัญหาที่เกี่ยวข้องอย่างสร้างสรรค์				
5.3 สามารถสื่อสารอย่างมีประสิทธิภาพทั้งปากเปล่าและการเขียน พร้อมทั้ง เลือกใช้รูปแบบของสื่อการนำเสนออย่างเหมาะสม				
5.4 สามารถใช้สารสนเทศและเทคโนโลยีสื่อสารได้อย่างเหมาะสม				

หมวดที่ 5 แผนการสอนและการประเมินผล

1. แผนการสอน

ระบุหัวข้อ/รายละเอียด สัปดาห์ที่สอน จำนวนชั่วโมงการสอน (ซึ่งต้องสอดคล้องกับจำนวนหน่วยกิต) กิจกรรมการเรียนการสอนและสื่อที่ใช้ รวมทั้งอาจารย์ผู้สอน ในแต่ละหัวข้อ/รายละเอียดของรายวิชา สามารถแยกชั่วโมงบรรยายและชั่วโมงปฏิบัติ

สัปดาห์ที่/วันที่	บท/หัวข้อย่อยที่สำคัญ	CLO	จำนวนชั่วโมง		กิจกรรมการเรียนการสอน/สื่อที่ใช้	ผู้สอน
			บรรยาย	ปฏิบัติ		
1	**บทที่ 1 ความรู้เบื้องต้นของความปลอดภัยในเครือข่ายและระบบสารสนเทศ** 1.1 ปัญหาความปลอดภัยของเครือข่ายในองค์กร 1.2 ภัยคุกคามในระบบเครือข่าย **บทที่ 2 หลักการด้านการรักษาความปลอดภัย (CIAAAAPDR)** 2.1 แนวคิดและหลักการด้านความปลอดภัยในเครือข่าย 2.2 คุณสมบัติที่เกี่ยวข้องกับการรักษาความปลอดภัยในเครือข่ายและระบบสารสนเทศ	CLO 1, 2	3	0	- ชี้แจงรายละเอียดวิชา - แนะนำหนังสือและแหล่งค้นคว้าข้อมูลเพิ่มเติม - บรรยายสอนแบบ Case-based Learning โดยใช้ PowerPoint	อ.ดร.ณภัทร
2	**บทที่ 3 ปัญหาด้านความปลอดภัยที่เกิดขึ้นในเครือข่ายและภัยคุกคามในปัจจุบัน**	CLO 1, 2	3	0	- บรรยาย ยกตัวอย่างโดยใช้ PowerPoint - **การสอนแบบ Active Learning** ให้นิสิตศึกษาค้นคว้า	อ.ดร.ณภัทร

สัปดาห์ที่/วันที่	บท/หัวข้อย่อยที่สำคัญ	CLO	จำนวนชั่วโมง		กิจกรรมการเรียนการสอน/สื่อที่ใช้	ผู้สอน
			บรรยาย	ปฏิบัติ		
	3.1 โปรโตคอลเครือข่าย ช่องโหว่ และแนวทางป้องกัน 3.2 TCP/UDP/ ICMP 3.3 การโจมตีรูปแบบอื่น ๆ 3.4 ช่องโหว่อื่น ๆ ในเว็บไซต์และระบบสารสนเทศ				ภัยคุกคาม วิเคราะห์สาเหตุ ปัญหา และนำเสนอแนวทางป้องกัน 10 คะแนน คิดเป็น 5%	
3 - 5	**บทที่ 4 เทคนิคการเข้ารหัสข้อมูล** 4.1 ความสำคัญของการรักษาความลับของข้อมูลและความถูกต้องของข้อมูล 4.2 การเข้ารหัสข้อมูลแบบสมมาตรและไม่สมมาตร 4.3 การประยุกต์ใช้การเข้ารหัสในเครือข่ายและระบบสารสนเทศ	**CLO 2, 3, 4**	**9**	**0**	- บรรยายโดยใช้ PowerPoint - ยกตัวอย่างกรณีศึกษา การประยุกต์ใช้เทคนิคการเข้ารหัสข้อมูล - **การสอนแบบ Active Learning** ให้นิสิตศึกษาเทคนิคการเข้ารหัสข้อมูล 10 คะแนน คิดเป็น 5%	อ.ดร.ณภัทร
6	**บทที่ 5 การระบุตัวตน** 5.1 หลักการและแนวคิดการระบุตัวต้น 5.2 วิธีการระบุตัวตนแบบต่าง ๆ เช่น Password-based, Token-based, Biometric เป็นต้น	**CLO 5**	**3**	**0**	- บรรยายแบบ Case-based Learning โดยใช้ PowerPoint - อภิปรายการสร้าง Token เพื่อนำไปใช้ในการระบุตัวตนบนเว็บไซต์ - ทดสอบย่อย	อ.ดร.ณภัทร

สัปดาห์ที่/วันที่	บท/หัวข้อย่อยที่สำคัญ	CLO	จำนวนชั่วโมง		กิจกรรมการเรียนการสอน/สื่อที่ใช้	ผู้สอน
			บรรยาย	ปฏิบัติ		
	5.3 การประยุกต์ใช้ Token-based ในการระบุตัวตนบนเว็บไซต์					
7	**บทที่ 6 การตรวจสอบสิทธิ์และการเข้าถึงข้อมูล** 6.1 ความสำคัญของการตรวจสอบสิทธิ์ในระบบเครือข่ายและระบบสารสนเทศ 6.2 การกำหนดสิทธิ์การเข้าถึงข้อมูลในระบบเครือข่าย 6.3 เรียนรู้การกำหนดสิทธิ์ในระบบไฟล์	CLO 4	3	0	- บรรยายแบบ Case-based Learning โดยใช้ PowerPoint - ทดสอบย่อย	อ.ดร.ณภัทร
8	**บทที่ 7 ลายมือดิจิทัล** 7.1 หลักการทำงานและความสำคัญของลายมือดิจิทัล 7.2 การสร้างและประยุกต์ใช้งานลายมือดิจิทัล	CLO 4	3	0	- บรรยายแบบ Case-based Learning โดยใช้ PowerPoint - **การสอนแบบ Active Learning** ให้นิสิตศึกษาวิธีการสร้าง SSL และติดตั้งบนเว็บไซต์ - 10 คะแนน คิดเป็น 5% - ทดสอบย่อย	อ.ดร.ณภัทร
9	**บทที่ 8 ไฟร์วอลล์** 8.1 หลักการทำงานของ Firewall	CLO 5	3	0	- บรรยาย โดยใช้ PowerPoint - **การสอนแบบ Active Learning** ให้นิสิตศึกษาการ	อ.ดร.ณภัทร

สัปดาห์ที่/วันที่	บท/หัวข้อย่อยที่สำคัญ	CLO	จำนวนชั่วโมง		กิจกรรมการเรียนการสอน/สื่อที่ใช้	ผู้สอน
			บรรยาย	ปฏิบัติ		
	8.2 ความสามารถของ Firewall รูปแบบต่าง ๆ และการประยุกต์ใช้งาน				ติดตั้งระบบ Firewall ในเครือข่ายคอมพิวเตอร์ 10 คะแนน คิดเป็น 5%	
10	**บทที่ 9 ระบบตรวจจับและป้องกันการบุกรุก** 9.1 หลักการทำงานของระบบ IDS/IPS 9.2 ความสามารถของระบบ IDS/IPS และการประยุกต์ใช้งาน	CLO 5	3	0	- บรรยาย โดยใช้ PowerPoint - **การสอนแบบ Active Learning** ให้นิสิตศึกษาการติดตั้งระบบ IDS/IPS ในเครือข่าย 10 คะแนน คิดเป็น 5%	อ.ดร.ณภัทร
11-13	**บทที่ 10 การสร้างความปลอดภัยของระบบเครือข่ายและระบบสารสนเทศ** 10.1 ปัญหาความปลอดภัยของเว็บแอปพลิเคชัน และเครือข่าย 10.2 ลักษณะการโจมตีแบบ CSRF 10.3 โปรโตคอลด้านความปลอดภัย 10.4 เทคโนโลยีด้านความปลอดภัยในเครือข่ายและระบบสารสนเทศ	CLO 2, 3, 4, 5	9	0	- บรรยาย ยกตัวอย่างกรณีศึกษา โดยใช้ PowerPoint - **การสอนแบบ Active Learning** ให้นิสิตศึกษาและออกแบบความปลอดภัยในระบบเครือข่ายและระบบสารสนเทศด้วยเทคโนโลยีที่มีอยู่ปัจจุบัน 10 คะแนน คิดเป็น 5%	อ.ดร.ณภัทร
14	**บทที่ 11 การฟื้นฟูระบบเครือข่ายจากสถานการณ์ฉุกเฉิน**	CLO 6	3	0	- บรรยายสอนแบบ Case-based	อ.ดร.ณภัทร

สัปดาห์ที่/วันที่	บท/หัวข้อย่อยที่สำคัญ	CLO	จำนวนชั่วโมง		กิจกรรมการเรียนการสอน/สื่อที่ใช้	ผู้สอน
			บรรยาย	ปฏิบัติ		
	11.1 การจัดการความเสี่ยงและการประเมินภัยคุกคาม 11.2 ขั้นตอนการรับมือกับสถานการณ์ฉุกเฉินไม่คาดคิด 11.3 การฟื้นฟูระบบเครือข่ายและระบบสารสนเทศ				Learning โดยใช้ PowerPoint - ยกตัวอย่างกรณีศึกษา การจัดทำแผนฟื้นฟูระบบเครือข่ายในสถานการณ์ฉุกเฉิน	
15	**ประเด็นแนวโน้มเทคโนโลยีความปลอดภัยในเครือข่ายและมาตรฐานความมั่นคงปลอดภัยไซเบอร์**	CLO 1, 7	3	0	- อภิปรายและตอบคำถามในชั้นเรียน - มอบหมายงานให้นิสิตศึกษาและนำเสนอเทคโนโลยีความปลอดภัยในเครือข่ายและมาตรฐานความมั่นคงปลอดภัยไซเบอร์	อ.ดร.ณภัทร
17-18	สอบปลายภาค					
รวม			45	0		

หมายเหตุ : กิจกรรมการเรียนการสอนควรจะเขียนให้หลากหลายเหมาะสมในแต่ละบท

- มีสัดส่วนของ Active learning ร้อยละ 30

2. แผนการประเมินผลการเรียนรู้

ลำดับ	ผลการเรียนรู้ (TQF)	ผลลัพธ์การเรียนรู้ (CLO)	วิธีการประเมิน	สัปดาห์ที่ประเมิน/วันที่	สัดส่วนของการประเมินผล
1	2.1 2.2 2.3 2.4 3.1 3.3	1, 4, 5, 6	สอบปลายภาค	สัปดาห์ที่ 17-18	**30%**
2	2.1 2.2 2.3 2.4	1, 4	การทดสอบย่อย	สัปดาห์ที่ 6-8	**10%**

ลำดับ	ผลการเรียนรู้ (TQF)	ผลลัพธ์การเรียนรู้ (CLO)	วิธีการประเมิน	สัปดาห์ที่ประเมิน/วันที่	สัดส่วนของการประเมินผล
	3.1 3.3				
3	1.1 1.2 1.7 2.1 2.2 2.3 2.4	1, 2, 3, 5, 7	กิจกรรม Active Learning	สัปดาห์ที่ 2, 3, 9, 10, 13	30%
4	1.1 1.2 1.7 2.1 2.2 2.3 2.4 3.1 3.3	1, 2, 3, 5, 7	งานที่ได้รับมอบหมาย	ตลอดภาคเรียน	20%
5	2.1 2.2 2.3 2.4	7	รายงานและการนำเสนอ	15	10%
รวม					**100%**

เกณฑ์การประเมินผลการเรียน

80.00 – 100.00	ได้เกรด A	53.00 – 60.99	ได้เกรด C
74.00 – 79.99	ได้เกรด B+	47.00 – 52.99	ได้เกรด D+
68.00 – 73.99	ได้เกรด B	41.00 – 46.99	ได้เกรด D
61.00 – 67.99	ได้เกรด C+	0.00 – 40.99	ได้เกรด F

เกณฑ์การให้คะแนนรายงาน คะแนนเต็ม 10 คะแนน

เกณฑ์พิจารณา	สัดส่วน	ระดับคะแนน			
		ปรับปรุง	ดี	ดีมาก	ยอดเยี่ยม
ความครบถ้วนสมบูรณ์ของเนื้อหา	5	0-1.24 - รายงานมีความถูกต้องครบถ้วนของเนื้อหาน้อยกว่า 30%	1.25-2.49 - รายงานมีความถูกต้องครบถ้วนของเนื้อหามากกว่า 30% แต่ไม่เกิน 60% - มีการพิมพ์ผิดพลาดจำนวนมาก	2.50-3.74 - รายงานมีความถูกต้องครบถ้วนของเนื้อหามากกว่า 60% แต่ไม่เกิน 85% - มีการพิมพ์ผิดพลาดบางส่วน	3.75-5.00 - รายงานมีความถูกต้องครบถ้วนของเนื้อหามากกว่า 85% - มีการพิมพ์ผิดพลาดบางส่วน การจัดเรียบร้อย
การเรียบเรียงเนื้อหา	2	0-0.49 - มีคำสะกดผิดจำนวนมาก - ไม่มีการเรียบเรียงเนื้อหาเข้าใจยาก - ไม่มีการอธิบายเนื้อหาหรือรูปภาพชัดเจน	0.50-0.99 - มีคำสะกดผิดบางส่วน - มีการเรียบเรียงเนื้อหาบางส่วนแต่อ่านไม่เข้าใจ - ไม่มีการอธิบายเนื้อหาหรือรูปภาพชัดเจน	1.00-1.49 - ไม่มีคำสะกดผิด - มีการเรียบเรียงเนื้อหาค่อนข้างดีเข้าใจง่าย - ไม่มีการอธิบายเนื้อหาหรือรูปภาพชัดเจน	1.50-2.00 - ไม่มีคำสะกดผิด - เรียบเรียงเนื้อหาต่อเนื่องดี - อธิบายเนื้อหาได้ดี รูปภาพชัดเจน
รูปแบบรายงานถูกต้อง	2	0-0.49 - ไม่มีการจัดรูปแบบกั้นหน้ากั้นหลังตามรูปแบบที่กำหนด	0.50-0.99 - มีการจัดรูปแบบกั้นหน้ากั้นหลังตามรูปแบบที่กำหนดน้อยกว่า 50%	1.00-1.49 - มีการจัดรูปแบบกั้นหน้ากั้นหลังตามรูปแบบที่กำหนดมากกว่า	1.50-2.00 - มีการจัดรูปแบบกั้นหน้ากั้นหลังตามรูปแบบที่กำหนดมากกว่า 80%

เกณฑ์พิจารณา	สัดส่วน	ระดับคะแนน			
		ปรับปรุง	ดี	ดีมาก	ยอดเยี่ยม
				50% แต่ไม่เกิน 80%	
เอกสารอ้างอิง	1	0-0.24 - ไม่มีอ้างอิง - ไม่มีการ Citation - ไม่จัดรูปแบบตามกำหนด	0.25-0.49 - มีการใส่อ้างอิงหรือมีการ Citation อย่างใดอย่างหนึ่ง - จัดรูปแบบตามกำหนดน้อยกว่า 50%	0.50-0.74 - มีการใส่อ้างอิงและ Citation - จัดรูปแบบตามกำหนดมากกว่า 50% แต่ไม่เกิน 80%	0.74-1.00 - มีการใส่อ้างอิงและ Citation - จัดรูปแบบตามกำหนดมากกว่า 80%

เกณฑ์การให้คะแนนการนำเสนอ คะแนนเต็ม 5 คะแนน

เกณฑ์พิจารณา	สัดส่วน	ระดับคะแนน			
		ปรับปรุง	ดี	ดีมาก	ยอดเยี่ยม
การนำเสนอและสื่อประกอบการนำเสนอ (PowerPoint)	3	0-0.74 - นำเสนอเนื้อหาไม่ถูกต้องครบถ้วน หรือใช้เวลาน้อยหรือมากเกินไป - สื่อประกอบนำเสนอไม่สวยงามและไม่น่าสนใจ	0.75-1.49 - นำเสนอเนื้อหาส่วนใหญ่ได้ถูกต้องครบถ้วนตามเวลาที่กำหนด - สื่อประกอบนำเสนอค่อนข้างน่าสนใจ	1.50-2.24 - นำเสนอเนื้อหาถูกต้องครบถ้วน แต่ใช้เวลานำเสนอน้อยหรือมากเกินไป - สื่อประกอบนำเสนอสวยงามน่าสนใจ	2.25-3.00 - นำเสนอเนื้อหาถูกต้องครบถ้วนตามเวลาที่กำหนด - สื่อประกอบนำเสนอสวยงามน่าสนใจ
การตอบคำถาม	2	0-0.49	0.50-0.99	1.00-1.49	1.50-2.00

เกณฑ์พิจารณา	สัดส่วน	ระดับคะแนน			
		ปรับปรุง	ดี	ดีมาก	ยอดเยี่ยม
		- ตอบคำถามไม่ถูกต้อง ไม่ตรงประเด็น - ไม่เข้าใจเนื้อหาที่นำเสนอ	- ตอบคำถามได้เพียงบางคำถาม - เข้าใจเนื้อหาที่นำเสนอเพียงบางส่วน	- ตอบคำถามได้ถูกต้อง ตรงประเด็น - เข้าใจเนื้อหาที่นำเสนอส่วนใหญ่	- ตอบคำถามถูกต้อง ตรงประเด็น - เข้าใจเนื้อหาที่นำเสนอเป็นอย่างดี

หมวดที่ 6 ทรัพยากรประกอบการเรียนการสอน

1. ตำรา เอกสารหลัก และข้อมูลสำคัญ

1. William Stallings. Network Security Essential: Application & Standards, 4th edition, Prentice Hall, 2011.
2. James F. Kurose and Keith W. Ross, Computer Networking: A Top-Down Approach, Seventh Edition, Pearson, 2017

2. เอกสารและข้อมูลแนะนำ

- วิดีโอ YouTube การใช้งานคำสั่งใน Kali Linux

หมวดที่ 7 การประเมินและปรับปรุงการดำเนินการของรายวิชา

1. กลยุทธ์การประเมินประสิทธิผลของรายวิชาโดยนิสิต

แบบประเมินรายวิชาของมหาวิทยาลัย

2. กลยุทธ์การประเมินการสอน

แบบประเมินผลการสอน ซึ่งเป็นแบบประเมินผลการสอนของมหาวิทยาลัย ที่กำหนดให้มีการประเมินการสอนของอาจารย์ผู้สอน โดยนิสิต ทุกภาคการศึกษา

3. การปรับปรุงการสอน

อาจารย์ผู้สอนทบทวนและปรับปรุงวิธีการสอนจากผลการประเมินประสิทธิผลของรายวิชา จัดทำรายงานผลการดำเนินการของรายวิชา (มคอ. 5) ทุกภาคการศึกษา

4. การทวนสอบมาตรฐานผลสัมฤทธิ์ของนิสิตในรายวิชา

กรรมการพัฒนาหลักสูตรและมาตรฐานการศึกษาทำหน้าที่ทวนสอบผลสัมฤทธิ์ของนักศึกษาในรายวิชา โดยประเมินคุณภาพของข้อสอบและความเหมาะสมของการให้คะแนน ตลอดจนพิจารณาระดับคะแนนในรายวิชา

5. การดำเนินการทบทวนและการวางแผนปรับปรุงประสิทธิผลของรายวิชา

นำผลการประเมินและทวนสอบผลสัมฤทธิ์ประสิทธิผลรายวิชามาวางแผนการปรับปรุงการสอน และรายละเอียดวิชาเพื่อให้เกิดคุณภาพมากขึ้นโดยมีการปรับปรุงรายวิชาทุก 2 ปี

ชื่ออาจารย์ผู้รับผิดชอบรายวิชา : ความปลอดภัยบนเครือข่ายคอมพิวเตอร์

ลงชื่อ ณภัทร แก้วภิบาล

(อาจารย์ ดร.ณภัทร แก้วภิบาล)

วันที่ 13 พฤศจิกายน 2566