มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

คณะบริหารธุรกิจ

ประมวลรายวิชา ความมั่นคงของระบบสารสนเทศ
(Course Syllabus of Information System Security)

1. รหัสวิชาและชื่อวิชา 05-510-409 ความมั่นคงของระบบสารสนเทศ

2. จำนวนหน่วยกิต 3(2-2-5)

3. หลักสูตรและประเภทของรายวิชา

หลักสูตรบริหารธุรกิจบัณฑิต สาขาวิชาคอมพิวเตอร์ธุรกิจ วิชาชีพบังคับ (หลักสูตรปรับปรุงปี 2562)

4. อาจารย์ผู้รับผิดชอบรายวิชาและอาจารย์ผู้สอน

อาจารย์ผู้รับผิดชอบรายวิชา รองศาสตราจารย์ ดร. สุรีรัตน์ อินทร์หม้อ

อาจารย์ผู้สอน รองศาสตราจารย์ ดร. สุรีรัตน์ อินทร์หม้อ

5. ภาคการศึกษา/ชั้นปีที่เรียน

ภาคการศึกษาที่ 2/2566

6. รายวิชาที่ต้องเรียนมาก่อน (Pre-requisite) (ถ้ามี)

ไม่มี

7. คำอธิบายของรายวิชา

หลักการเบื้องต้นด้านความมั่นคงปลอดภัย ประเภทของภัยรุกราน การโจมตีระบบและการป้องกัน นโยบายและแบบจำลองเพื่อความมั่นคงของระบบ มาตรฐานด้านความปลอดภัยของระบบคอมพิวเตอร์ การพิสูจน์ทราบผู้ใช้ในระบบคอมพิวเตอร์ การวิเคราะห์ความเสี่ยงด้านความมั่นคง ซอฟต์แวร์ต่อต้านไวรัส การเข้ารหัสข้อมูล การจัดการและการบริการด้านความมั่นคง จรรยาบรรณการใช้งานระบบคอมพิวเตอร์ กฎหมายอาชญากรรมคอมพิวเตอร์ กฎหมายธุรกรรมทางอิเล็กทรอนิกส์และกฎหมายที่เกี่ยวข้องกับความปลอดภัย

The fundamentals of information system security, types of security threat, system attack and protection, security policy and model, computer security standard, user authentication system, security risk analysis, anti-virus software, data encryption, security management and services, code of ethic for using computer, computer criminal law, electronics transaction law and related security law

8. Course Learning Outcome

จาก มคอ 2. การกำหนด ผลการเรียนรู้ของหลักสูตร (Program Learning outcome: PLO) และมาตรฐานการเรียนรู้ 5 ด้าน (TQF) ของรายวิชานี้ เป็นดังรูป

รายวิชา		1 คุณธรรม จริยธรรม			2 ความรู้			3 ทักษะทางปัญญา				4 ทักษะความสัมพันธ์ระหว่างบุคคลและความรับผิดชอบ			5 ทักษะการวิเคราะห์เชิงตัวเลข การสื่อสาร และการใช้เทคโนโลยีสารสนเทศ		
		1	2	3	1	2	3	1	2	3	4	1	2	3	1	2	3
		PLO4	PLO1	PLO7	PLO1	PLO7	PLO1	PLO8	PLO6	PLO9	PLO4	PLO3	PLO2	PLO9	PLO1	PLO9	PLO5
05-510-409	ความมั่นคงของระบบสารสนเทศ	●			●						●	●				●	

เพื่อตอบผลการเรียนรู้ของทั้ง PLO รายวิชานี้จึงมีการกำหนด ผลการเรียนรู้ของรายวิชา (Course learning outcome: CLO) ดังนี้

PLO ของหลักสูตร	CLO ของรายวิชา
PLO1 ประยุกต์ใช้ความรู้ด้านศาสตร์คอมพิวเตอร์ในการแก้ปัญหาได้	CLO 2 ประเมินความเสี่ยงของภัยคุกคามที่มีต่อระบบสารสนเทศขององค์กร CLO 3 ประเมินวิธีการและเทคนิคในการสร้างความมั่นคงให้กับระบบ
PLO3 จัดทำแผนงาน/แผนผังในการบริหารจัดการระบบคอมพิวเตอร์และเครือข่ายที่คำนึงถึงสภาพแวดล้อมที่เหมาะสม เป็นมิตรต่อบุคคล องค์การ และสังคม	CLO 4 วิเคราะห์ภัยคุกคามความเสี่ยงและหามาตรการในการปกป้องระบบ
PLO4 เข้าใจจริยธรรม กฎหมาย ความมั่นคง ประเด็นด้านสังคม พัฒนาตนไปสู่ความเป็นมืออาชีพ ตลอดจนสามารถประยุกต์ใช้และประเมินความมั่นคงของระบบข่ายงาน เลือกใช้เครื่องมือและระบบที่ท าให้เกิดการลดลงของภัยคุกคามได้อย่างเหมาะสม	CLO 5 เข้าใจเรื่องกฎหมายและจริยธรรมที่เกี่ยวข้องกับความมั่นคงและใช้งานอย่างเหมาะสม
PLO9 สื่อสารกับผู้อื่นได้อย่างมีประสิทธิภาพ ออกแบบและประยุกต์ใช้สถาปัตยกรรมระดับองค์การได้อย่างเหมาะสม สอดคล้องกับความต้องการ	CLO 1 เข้าใจหลักการสำคัญและแนวคิดพื้นฐานด้านความมั่นคงของระบบสารสนเทศและสื่อสารให้ทุกฝ่ายที่เกี่ยวข้องได้ทราบ

9. แผนการสอน (จัดทำการสอน 17 สัปดาห์)

CLO	สัปดาห์ที่ (Week)	หัวเรื่องทีสอน Topic	กลยุทธ์/วิธีการสอน Teaching and Learning	กลยุทธ์/วิธีการประเมินผล Assessment	สัดส่วนการประเมิน
CLO 1 เข้าใจหลักการสำคัญและแนวคิดพื้นฐานด้านความมั่นคงของระบบสารสนเทศและสื่อสารให้ทุกฝ่ายที่เกี่ยวข้องได้ทราบ	**1**	• แนะนำรายวิชาและการเรียนการสอนรายวิชาความมั่นคงของระบบสารสนเทศ • ปัญหาความมั่นคงของระบบประมวลผล	1. การบรรยาย 2. การใช้กรณีศึกษา	1. การประเมินการบ้าน	2
CLO 1 เข้าใจหลักการสำคัญและแนวคิดพื้นฐานด้านความมั่นคงของระบบสารสนเทศและสื่อสารให้ทุกฝ่ายที่เกี่ยวข้องได้ทราบ	**2**	การรักษาความมั่นคงของทรัพยากรอื่นที่มีความเสี่ยง	1. การบรรยาย 2. การใช้กรณีศึกษา 3. กิจกรรม	1. การประเมินการบ้าน	2
CLO 1 เข้าใจหลักการสำคัญและแนวคิดพื้นฐานด้านความมั่นคงของระบบสารสนเทศและสื่อสารให้ทุกฝ่ายที่เกี่ยวข้องได้ทราบ	**3**	การออกแบบระบบรักษาความมั่นคง	1. การบรรยาย 2. การใช้กรณีศึกษา (Case) 3. การสอนแบบโปรแกรม (Programmed Instruction)/ การเรียนด้วยบทเรียนคอมพิวเตอร์ช่วยสอน/การเรียนแบบผสมผสาน/การเรียนแบบออนไลน์	1. การประเมินการบ้าน	2

CLO	สัปดาห์ที่ (Week)	หัวเรื่องทีสอน Topic	กลยุทธ์/วิธีการสอน Teaching and Learning	กลยุทธ์/วิธีการประเมินผล Assessment	สัดส่วนการประเมิน
			4. การศึกษาค้นคว้าโดยอิสระ (Independent study)		
CLO2 ประเมินความเสี่ยงของภัยคุกคามที่มีต่อระบบสารสนเทศขององค์กร	**4**	การวางแผนในการจัดตั้งศูนย์คอมพิวเตอร์	1. การบรรยาย 2. การใช้กรณีศึกษา (Case) 3. การฝึกปฏิบัติ (Practice) 4. การเรียนรู้ด้วยตนเอง	1. การประเมินการบ้าน	2
CLO3 ประเมินวิธีการและเทคนิคในการสร้างความมั่นคงให้กับระบบ	**5**	ความรู้พื้นฐานเกี่ยวกับการเข้ารหัสข้อมูล	1. การบรรยาย 2. การใช้ปัญหาเป็นฐาน 3. การใช้กรณีศึกษาจริง 4. การฝึกปฏิบัติ (Practice) 5. การเรียนรู้ด้วยตนเอง	1. การประเมินการบ้าน	4
CLO1 เข้าใจหลักการสำคัญและแนวคิดพื้นฐานด้านความมั่นคงของระบบสารสนเทศและสื่อสารให้ทุกฝ่ายที่เกี่ยวข้องได้ทราบ	**6**	การเข้ารหัสโดยการแทนที่ตัวอักษร	1. การบรรยาย 2. การใช้ปัญหาเป็นฐาน 3. การใช้กรณีศึกษาจริง 4. การฝึกปฏิบัติ (Practice) 5. การเรียนรู้ด้วยตนเอง	1. การประเมินการบ้าน	4

CLO	สัปดาห์ที่ (Week)	หัวเรื่องที่สอน Topic	กลยุทธ์/วิธีการสอน Teaching and Learning	กลยุทธ์/วิธีการประเมินผล Assessment	สัดส่วนการประเมิน
CLO2 ประเมินความเสี่ยงของภัยคุกคามที่มีต่อระบบสารสนเทศขององค์กร	**7**	โปรแกรมที่สร้างความเสียหายต่อระบบคอมพิวเตอร์	1. การบรรยาย 2. การใช้กรณีศึกษา 3. กิจกรรม 4. การเรียนรู้ด้วยตนเอง	1. การประเมินการบ้าน	4
CLO1 เข้าใจหลักการสำคัญและแนวคิดพื้นฐานด้านความมั่นคงของระบบสารสนเทศและสื่อสารให้ทุกฝ่ายที่เกี่ยวข้องได้ทราบ CLO2 ประเมินความเสี่ยงของภัยคุกคามที่มีต่อระบบสารสนเทศขององค์กร CLO3 ประเมินวิธีการและเทคนิคในการสร้างความมั่นคงให้กับระบบ	**8**	ทบทวนและนำเสนองาน	1. การสอนโดยใช้ปัญหาเป็นฐาน	1.การประเมินรายงาน/โครงงาน 2. การประเมินการนำเสนอ	3 2
	9	**สอบกลางภาค**		การสอบทักษะ	25
CLO3 ประเมินวิธีการและเทคนิคในการสร้างความมั่นคงให้กับระบบ	10	การรักษาความมั่นคงของโปรแกรมประมวลผล	1. การบรรยาย 2. การใช้ปัญหาเป็นฐาน 3. การใช้กรณีศึกษาจริง 4. การฝึกปฏิบัติ (Practice) 5. การเรียนรู้ด้วยตนเอง	1. การประเมินการบ้าน	2

CLO	สัปดาห์ที่ (Week)	หัวเรื่องทีสอน Topic	กลยุทธ์/วิธีการสอน Teaching and Learning	กลยุทธ์/วิธีการประเมินผล Assessment	สัดส่วนการประเมิน
CLO1 เข้าใจหลักการสำคัญและแนวคิดพื้นฐานด้านความมั่นคงของระบบสารสนเทศและสื่อสารให้ทุกฝ่ายที่เกี่ยวข้องได้ทราบ	**11**	แบบจำลองการรักษาความมั่นคง	1. การบรรยาย 2. การใช้ปัญหาเป็นฐาน 3. การใช้กรณีศึกษาจริง 4. การฝึกปฏิบัติ (Practice) 5. การเรียนรู้ด้วยตนเอง	1. การประเมินการบ้าน	2
CLO2 ประเมินความเสี่ยงของภัยคุกคามที่มีต่อระบบสารสนเทศขององค์กร	**12**	ความมั่นคงของระบบเครือข่าย	1. การบรรยาย 2. การระดมสมอง 3. การใช้กรณีศึกษาจริง 4. การฝึกปฏิบัติ (Practice) 5. การเรียนรู้ด้วยตนเอง	1.การประเมินการบ้าน	4
CLO4 วิเคราะห์ภัยคุกคามความเสี่ยงและหามาตรการในการปกป้องระบบ	**13**	การบริหารเรื่องความมั่นคง	1. การบรรยาย 2. การระดมสมอง 3. การใช้กรณีศึกษาจริง 4. การฝึกปฏิบัติ (Practice) 5. การเรียนรู้ด้วยตนเอง	1.การประเมินการบ้าน	4
CLO5 เข้าใจเรื่องกฎหมายและจริยธรรมที่เกี่ยวข้องกับความมั่นคงและใช้งานอย่างเหมาะสม	**14**	จรรยาบรรณของผู้ปฏิบัติงานในระบบคอมพิวเตอร์	1. การบรรยาย 2. การสอนโดยโครงงาน (Project-based instruction) 3. การฝึกปฏิบัติ (Practice) 4. การเรียนรู้ด้วยตนเอง	1.การประเมินการบ้าน	4

CLO	สัปดาห์ที่ (Week)	หัวเรื่องทีสอน Topic	กลยุทธ์/วิธีการสอน Teaching and Learning	กลยุทธ์/วิธีการประเมินผล Assessment	สัดส่วนการประเมิน
CLO5 เข้าใจเรื่องกฎหมายและจริยธรรมที่เกี่ยวข้องกับความมั่นคงและใช้งานอย่างเหมาะสม	**15**	นโยบายเกี่ยวกับจรรยาบรรณวิชาชีพในภาคธุรกิจ	1. การบรรยาย 2. การสอนโดยโครงงาน (Project-based instruction) 3. การฝึกปฏิบัติ (Practice) 4. การเรียนรู้ด้วยตนเอง	1. การประเมินการบ้าน/ชิ้นงาน	4
CLO4 วิเคราะห์ภัยคุกคามความเสี่ยงและหามาตรการในการปกป้องระบบ CLO5 เข้าใจเรื่องกฎหมายและจริยธรรมที่เกี่ยวข้องกับความมั่นคงและใช้งานอย่างเหมาะสม	**16**	ทบทวนเนื้อหาและนำเสนองาน	1.การสอนโดยใช้ปัญหาเป็นฐาน	1. การประเมินรายงาน/โครงงาน 2. การประเมินการนำเสนอหน้าชั้นเรียน	**3** **2**
	17	**สอบปลายภาค**		สอบทักษะ	25

10. การประเมินผลการเรียน (สอบ 50 แนน เก็บ 50 คะแนน)

รายการประเมิน	PLO1	PLO3	PLO4	PLO9		รวม
คะแนนสอบ 50 คะแนน						
1. สอบกลางภาค (AP)	5			10		15
2. สอบกลางภาค (MANI)	10					10
3. สอบปลายภาค (AP)				10		10
4. สอบปลายภาค (MANI)	15					15
คะแนนจากงานมอบหมายและกิจกรรมในชั้นเรียน 50 คะแนน						
5. การบ้าน	10	10	10	10		40
6. การเข้าเรียนและการมีส่วนร่วมในชั้นเรียน	3	2	3	2		10
รวม	**43**	**12**	**13**	**32**		**100**

***** U=Understanding วัดความเข้าใจ (ข้อสอบง่าย)

***** AP = Applying วัดการนำไปใช้ ประมาณค่าได้ ตัดสินใจเบื้องต้นได้ (ข้อสอบปานกลาง และข้อสอบยาก)

* Mani = Manipulation วัดทักษะ

แผนการสอบ สอบกลางภาค 25 คะแนน และสอบปลายภาค 25 คะแนน รวม 50 คะแนน

รายการสอบ	คะแนน
สอบครั้งที่ 1 สอบกลางภาค	**25**
บทที่ 1 ความมั่นคงของระบบสารสนเทศ	5
บทที่ 2 การออกแบบระบบความมั่นคง	5
บทที่ 3 การวางแผนจัดตั้งศูนย์คอมพิวเตอร์	5
บทที่ 4 ความรู้พื้นฐานเกี่ยวกับการเข้ารหัสข้อมูล	5
บทที่ 5 โปรแกรมที่สร้างความเสียหายต่อระบบคอมพิวเตอร์	5
สอบครั้งที่ 2 สอบปลายภาค	**25**
บทที่ 6 การรักษาความมั่นคงของโปรแกรมประมวลผล	5
บทที่ 7 แบบจำลองการรักษาความมั่นคงปลอดภัย	5
บทที่ 8 ความมั่นคงของระบบเครือข่าย	5
บทที่ 9 การบริหารเรื่องความมั่นคง	5
บทที่ 10 จริยธรรมผู้ปฏิบัติงาน และกฎหมายที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ	5
รวม	**100**

11. เกณฑ์ค่าระดับคะแนน

☑ เกณฑ์ผ่าน (Minimum Score) 50 (%)

☑ ใช้เกณฑ์ค่าระดับคะแนน (Score Criteria)

ตั้งแต่ 80 % ขึ้นไป	A	=	4	ดีเยี่ยม(Excellent)
75 – 79 %	B^+	=	3.5	ดีมาก(Very Good)
70 – 74 %	B	=	3	ดี(Good)
65 – 69 %	C^+	=	2.5	ดีพอใช้(Fairly Good)
60 – 64 %	C	=	2	พอใช้(Fair)
55 – 59 %	D^+	=	1.5	อ่อน(Poor)
50 – 54 %	D	=	1	อ่อนมาก(Very Poor)
ต่ำกว่า 50 %	F	=	0	ตก(Failure)

12. **เอกสารและตำราหลักประกอบการเรียนการสอน**

เอกสารและตำราหลัก :

สุรีรัตน์ อินทร์หม้อ, ตำราวิชาความมั่นคงของระบบสารสนเทศ, ปรับปรุงครั้งที่ 4, 2566

เอกสารอ่านเพิ่มเติม

1. Charles P. P., Shari L., and Jonathan M., (2015). Security in Computing 5th Edition, Prentice Hall.

2. Misty E. Vermaat., Susan L. Sebok., Steven M. Freund., Jennifer T. Campbell., and Mark Frydenberg., (2016), Discovering Computers 2016, CENGAGE Learning.