

## รายละเอียดของรายวิชา

คณะวิทยาศาสตร์และเทคโนโลยี สาขาวิชา วิทยาการคำนวณและเทคโนโลยีดิจิทัล

ภาคการศึกษาที่ 1 ปีการศึกษา.....2565

มหาวิทยาลัยหัวเฉียวเฉลิมพระเกียรติ

### หมวดที่ 1 ข้อมูลทั่วไป

1. รหัสและชื่อรายวิชา CS3443 ความมั่นคงทางไซเบอร์ (Cyber Security)
2. จำนวนหน่วยกิต 3
3. หลักสูตร และประเภทรายวิชา หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์  
หลักสูตรปรับปรุง พ.ศ.2563 วิชาเอกบังคับ
4. ภาคการศึกษา / ชั้นปีที่เรียน ภาคการศึกษาที่ 1 / ชั้นปีที่ 3
5. รายวิชาที่ต้องเรียนมาก่อน (Pre-requisite) CS3723
6. รายวิชาที่ต้องเรียนพร้อมกัน (Co-requisites) ไม่มี
7. ชื่ออาจารย์ผู้รับผิดชอบรายวิชา อาจารย์ณัฐพร นันทจิระพงศ์  
ชื่ออาจารย์ผู้รับผิดชอบรายวิชาาร่วม ไม่มี
8. สถานที่เรียน
 

Onsite	กลุ่ม 01	วันพฤหัสบดี	ภาคบรรยาย เวลา 10.30-12.30 น. ห้อง 2-422 (เรียนร่วมกับรายวิชา AI3443)
		วันจันทร์	ภาคปฏิบัติ เวลา 8.30-11.30 น. ห้อง 2-430

อาคารเรียน มหาวิทยาลัยหัวเฉียวเฉลิมพระเกียรติ

Online ระบบการประชุมออนไลน์ MS-Teams, and etc.
9. วันที่จัดทำหรือปรับปรุงรายละเอียดของรายวิชาครั้งล่าสุด 25 กรกฎาคม 2565

### หมวดที่ 2 จุดมุ่งหมายและวัตถุประสงค์

- 1 จุดมุ่งหมายของรายวิชา เพื่อให้นักศึกษา
  - 1.1 มีความรู้เกี่ยวกับทฤษฎีเกี่ยวกับความมั่นคงทางไซเบอร์เบื้องต้นได้แก่ ประวัติความเป็นมา หลักการพื้นฐาน ชนิดของอาชญากรรมและภัยคุกคามทางไซเบอร์ อาชญากรและช่องโหว่ที่เกี่ยวข้อง การบริหารจัดการความเสี่ยง มาตรฐาน นโยบาย รวมถึงกฎหมายด้านความมั่นคงทางไซเบอร์
  - 1.2 มีความสามารถในการหลักการพื้นฐานและความสำคัญของการรักษาความมั่นคงทางกายภาพและทางชีวมาตร วิทยาการรหัสลับและนิติวิทยาศาสตร์ดิจิทัลเบื้องต้น
  - 1.3 มีทักษะปฏิบัติในการใช้งานคำสั่ง ซอฟต์แวร์และเครื่องมือที่ใช้ในการรักษาความมั่นคงทางไซเบอร์คอมพิวเตอร์และเทคโนโลยีสารสนเทศ

- 1.4 มีความสามารถในการศึกษาค้นคว้าด้วยตนเองเกี่ยวกับเทคโนโลยีด้านความมั่นคงทางไซเบอร์ใหม่ ๆ รวมถึงการประยุกต์ใช้ทฤษฎีและทักษะปฏิบัติที่ได้เรียนรู้ในรายวิชาในการนำเสนอแนวคิดและแนวปฏิบัติสำหรับการออกแบบนโยบายรวมถึงการเลือกใช้เครื่องมือให้เหมาะสมกับโครงการด้านความมั่นคงทางไซเบอร์

### ผลลัพธ์การเรียนรู้ระดับรายวิชา (Course-level Learning Outcomes: CLOs)

เมื่อสิ้นสุดการเรียนการสอนแล้ว นักศึกษาที่สำเร็จการศึกษาในรายวิชานี้ สามารถ

1. อธิบายความสำคัญของความมั่นคงทางไซเบอร์
2. จำแนกชนิดของอาชญากรรมและอาชญากรทางไซเบอร์
3. วิเคราะห์ผลกระทบของภัยคุกคามและการโจมตีทางไซเบอร์
4. นำเสนอแนวทางการสร้างความมั่นคงทางไซเบอร์ ทั้งการกำหนดนโยบาย การบังคับใช้กฎหมาย รวมถึงการประยุกต์ใช้ฮาร์ดแวร์และซอฟต์แวร์ที่เกี่ยวข้อง
5. อธิบายหลักการและประโยชน์ของวิทยาการรหัสลับและนิติวิทยาศาสตร์ดิจิทัล

## 2 วัตถุประสงค์ในการพัฒนา/ปรับปรุงรายวิชา

### 2.1 การปรับปรุงรายวิชาโดยอาจารย์ผู้สอน

- เพื่อให้การเรียนการสอนของรายวิชานี้มีคุณภาพและมาตรฐานที่เป็นไปตามกรอบมาตรฐานคุณวุฒิแห่งชาติ พ.ศ.2552 กรอบมาตรฐานคุณวุฒิระดับปริญญาตรี สาขาคอมพิวเตอร์ พ.ศ.2552 และเกณฑ์มาตรฐานหลักสูตรระดับปริญญาตรี พ.ศ. 2558
- จัดกิจกรรมการเรียนการสอนและการมอบหมายงานให้เหมาะสมกับสภาพผู้เรียน เน้นการเรียนรู้จากการปฏิบัติจริง (Active learning) ทักษะของบัณฑิตไทยในศตวรรษที่ 21 แนวโน้มการเปลี่ยนแปลงของเทคโนโลยี พร้อมทั้งส่งเสริมการพัฒนาทักษะด้านการร่วมมือร่วมใจ (Collaboration) การคิดสร้างสรรค์ (Creativity) การติดต่อสื่อสาร (Communication) และการคิดวิเคราะห์ (Critical Thinking) ตามหลักการของ 4C ให้กับผู้เรียน รวมถึงการพัฒนาทักษะการนำเสนอและการศึกษาค้นคว้าด้วยตนเอง ซึ่งเป็น ทักษะการเรียนรู้ตลอดชีวิต (Lifelong learning)
- ปรับรูปแบบการเรียนการสอนให้เป็น การผสมผสานระหว่างการเรียนในชั้นเรียนและการเรียนออนไลน์ (Blended learning) ร่วมกับการจัดการเรียนการสอนภาคทฤษฎีแบบ ห้องเรียนกลับด้าน (Flipped classroom) ในบางหัวข้อ และการเรียนรู้ภาคปฏิบัติโดยใช้ ทักษะเป็นฐาน (Skill based learning) เพื่อให้สอดคล้องกับสถานการณ์หลังเกิดการแพร่ระบาดของโรค Covid-19 และการพัฒนาทักษะปฏิบัติของนักศึกษาในยุคของการเปลี่ยนแปลงเทคโนโลยีดิจิทัล (Digital Transformation)
- จัดหาสื่อที่มีความหลากหลายและทันสมัย ได้แก่ E-books, Video clip, Infographics Course online และสื่ออื่น ๆ ที่น่าสนใจทั้งที่เป็นภาษาไทยและภาษาอังกฤษจากเว็บไซต์

และสื่อสังคมออนไลน์ต่าง ๆ มาประกอบการเรียนการสอนในหัวข้อที่เกี่ยวข้องกับเนื้อหา รายวิชา เพื่อให้นักศึกษาได้ความรู้ที่ทันสมัยและได้ฝึกทักษะการอ่านและการฟัง ภาษาอังกฤษ รวมถึงการนำไปทบทวนด้วยตนเองนอกเวลาเรียน

- จัดหา **Software** หรือเครื่องมือที่ไม่ละเมิดลิขสิทธิ์มาประกอบการจัดการเรียนการสอน ภาควิชาปฏิบัติการ เพื่อให้นักศึกษาได้เรียนรู้และฝึกทักษะการรักษาความมั่นคงปลอดภัยในการใช้ งานคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต ที่สอดคล้องกับเนื้อหาวิชา ซึ่งเป็นทักษะที่ สำคัญของผู้เรียนหลักสูตรวิทยาศาสตร์บัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์
- ปรับเกณฑ์และรูปแบบการวัดและประเมินโครงการประจำรายวิชา โดยมีการให้ข้อมูล **ป้อนกลับ (Feedback)** ในการนำเสนอผลงานรอบหัวข้อโครงการและรอบความก้าวหน้า เพื่อให้ให้นักศึกษาใช้ประกอบการพัฒนาผลงานและนำเสนอโครงการรอบสุดท้าย รวมถึงให้ **นักศึกษามีส่วนร่วมในการเสนอความคิดเห็นและประเมินผลงานของเพื่อนร่วมชั้นเรียน**

## 2.2 การปรับปรุงตามข้อวิพากษ์ของนักศึกษา

ไม่มี เนื่องจากเป็นการสอนครั้งแรกของหลักสูตรวิทยาศาสตร์บัณฑิต สาขาวิชาวิทยาการ คอมพิวเตอร์ (หลักสูตรปรับปรุง พ.ศ.2563)

## หมวดที่ 3 ส่วนประกอบของรายวิชา

### 1. คำอธิบายรายวิชา

ประวัติความเป็นมาของความมั่นคงทางไซเบอร์ ชนิดของอาชญากรรมทางไซเบอร์ ภัยคุกคามต่อ ความมั่นคงทางไซเบอร์ อาชญากรรมทางไซเบอร์ ช่องโหว่และความเสี่ยงทางไซเบอร์ มาตรฐานและการบริหารจัดการ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ การโจมตีและความมั่นคงของเว็บ นโยบายความมั่นคงทางไซเบอร์ กฎหมายด้านความมั่นคงทางไซเบอร์ การรักษาความมั่นคงทางชีวมาตร หลักการขั้นพื้นฐานของวิทยาการรหัสลับ นิติวิทยาศาสตร์ดิจิทัลเบื้องต้น และการฝึกปฏิบัติด้วยซอฟต์แวร์สำเร็จรูปและเครื่องมือที่เกี่ยวข้อง

History of Cyber security, Types of Cybercrime, Cyber security threat, Cyber criminals, Cyber risk and vulnerability, IT security and Risk management, Web attack and security, Cyber security policy, Cyber security laws, Biometric security, Basic concept of cryptography, Introduction to digital forensic, and Practicing with related software packages and tools.

### 2. จำนวนชั่วโมงที่ใช้ในการเรียนการสอน/ภาคการศึกษา

บรรยาย	ปฏิบัติ
บรรยาย 30 ชั่วโมง ต่อภาคการศึกษา	ฝึกปฏิบัติ 30 ชั่วโมง ต่อภาคการศึกษา

### 3. จำนวนชั่วโมงต่อสัปดาห์ที่อาจารย์ให้คำปรึกษาและแนะนำทางวิชาการเป็นรายบุคคล

- เข้าพบเป็นรายบุคคลหรือรายกลุ่ม เพื่อปรึกษาหารือกับอาจารย์ผู้รับผิดชอบและอาจารย์ผู้รับผิดชอบร่วมได้ตามความต้องการครั้งละ 1-2 ชั่วโมงต่อสัปดาห์ (เป็นช่วงเวลาที่อาจารย์ผู้สอนไม่ติดภาระงานสอนรายวิชาอื่น)

อาจารย์	วันเวลาที่พบได้
อาจารย์ณัฐพร นันทจิระพงศ์	วันพฤหัสบดี เวลา 15.30-17.00 น.
อาจารย์ ดร.ธีรวัฒน์ อีสริยะกุล	วันพฤหัสบดี เวลา 9.30-10.30 น. ในวันที่มาสอน อาจารย์พิเศษจากบริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
อาจารย์ ดร. กรินทร์ สุ่มังคะโยธิน	วันพฤหัสบดี เวลา 9.30-10.30 น. ในวันที่มาสอน อาจารย์พิเศษจากภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล
รองศาสตราจารย์ ดร. สุรทศ ไตรติลานันท์	วันพฤหัสบดี เวลา 9.30-10.30 น. ในวันที่มาสอน อาจารย์พิเศษจากภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล

ทั้งนี้ อาจารย์ผู้รับผิดชอบรายวิชาได้แจ้งให้นักศึกษาทราบในคาบเรียนแรก และประกาศไว้ในตารางสอนที่หน้าบุรุษห้องพักอาจารย์

- ส่งข้อความออนไลน์ที่ HCU E-Learning <http://online.hcu.ac.th>
- การสื่อสารออนไลน์ (Microsoft Teams/Line Openchat group)

ส่วนช่องทางการติดต่ออาจารย์พิเศษ จะแจ้งให้ทราบในวันที่อาจารย์พิเศษมาสอนครั้งแรก

#### หมวดที่ 4 การพัฒนาผลการเรียนรู้ของนักศึกษา

การพัฒนาผลการเรียนรู้ในมาตรฐานผลการเรียนรู้แต่ละด้าน ให้ข้อมูลในแต่ละด้าน ดังนี้

- 1) เขียนผลการเรียนรู้ในแต่ละด้าน ซึ่งต้องสอดคล้องกับที่ระบุในแผนที่แสดงการกระจายความรับผิดชอบต่อมาตรฐานผลการเรียนรู้จากหลักสูตรสู่รายวิชา (Curriculum Mapping)

- 2) ระบุวิธีการสอนที่ใช้ในการพัฒนาความรู้/หรือทักษะใน ข้อ 1
- 3) ระบุวิธีวัดและประเมินผลรายวิชาที่สอดคล้องกับประเมินผลการเรียนรู้ในมาตรฐานการเรียนรู้แต่ละด้าน

รหัส	ชื่อวิชา	หน่วยกิต	1.คุณธรรม จริยธรรม								2.ความรู้								3.ทักษะทางปัญญา				4.ทักษะความสัมพันธ์ระหว่างบุคคลและความรับผิดชอบ						5.ทักษะในการวิเคราะห์เชิงตัวเลข การสื่อสาร และการใช้เทคโนโลยีสารสนเทศ							
			1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	1	2	3	4	5	6	1	2	3	4				
CS 4773	เรขภาพคอมพิวเตอร์	3(2/2-1/2-0)			o								•	o	•			o							•							•				o

## 1. คุณธรรม จริยธรรม

### (1) คุณธรรม จริยธรรมที่ต้องพัฒนา

1.3 มีภาวะความเป็นผู้นำและผู้ตาม สามารถทำงานเป็นทีมและสามารถแก้ไขข้อขัดแย้งและลำดับความสำคัญ

### (2) วิธีการสอน

- ในคาบแรกของการสอน ผู้สอนได้ทำความตกลงกับนักศึกษาเกี่ยวกับการปฏิบัติตนตามกฎระเบียบของมหาวิทยาลัย เช่น การตรงต่อเวลาในการเข้าชั้นเรียน/การสอบ/การส่งงาน การแต่งกาย การใช้ห้องปฏิบัติการคอมพิวเตอร์ การไม่นำอาหารและน้ำเข้ามาทานและดื่มในชั้นเรียน การไม่ทิ้งขยะในห้องเรียน การไม่ทุจริตในการสอบ ไม่คัดลอกผลงานของผู้อื่น ความสำคัญของ 7 ส เป็นต้น เพื่อส่งเสริมให้นักศึกษาเคารพกฎระเบียบของมหาวิทยาลัย และมีความซื่อสัตย์ต่อคำสัญญาที่ได้ตกลงไว้
- ในทุกชั่วโมงของการสอน ผู้สอนได้สอดแทรกคุณธรรม 6 ประการ จริยธรรม อัตลักษณ์ของมหาวิทยาลัย รวมทั้งได้เน้นย้ำให้นักศึกษาระหนักถึงความสำคัญของการเข้าสู่ประชาคมอาเซียน และการยึดหลักปรัชญาของเศรษฐกิจพอเพียงในการเรียนและการใช้ชีวิตประจำวัน
- ในการมอบหมายงานทุกครั้ง ผู้สอนได้ย้าให้นักศึกษาพิจารณาวางแผนจัดลำดับความสำคัญของงาน ทั้งงานเดี่ยว งานคู่ และงานกลุ่ม ความรับผิดชอบในการทำงานของตนเองและการทำงานกลุ่ม การมีภาวะผู้นำผู้ตามในการเรียนและทำงานร่วมกับเพื่อน ๆ ทั้งในและนอกเวลาเรียน
- การมอบหมายให้นักศึกษาจับกลุ่มกัน (กลุ่มละ 2-3 คน) เพื่อนำเสนอโครงการด้านความมั่นคงทางไซเบอร์ของหน่วยงาน/สถานประกอบการของภาคธุรกิจหรือภาคอุตสาหกรรมตามความสนใจ (แต่ต้องไม่ซ้ำกัน) โดยทำการการออกแบบและพัฒนาระบบรักษาความมั่นคงทางไซเบอร์ ให้กับระบบฐานข้อมูล เครือข่ายคอมพิวเตอร์ทั้งแบบ Wired และ Wireless network รวมถึงเว็บไซต์ของหน่วยงาน/สถานประกอบการที่เลือก ซึ่งระบบรักษาความมั่นคงทางไซเบอร์ที่นำเสนอจะต้องประกอบด้วยฮาร์ดแวร์ ซอฟต์แวร์ นโยบาย มาตรฐาน และเทคโนโลยีทางด้านปัญญาประดิษฐ์ที่เหมาะสมกับลักษณะธุรกิจหรืออุตสาหกรรมที่เลือก แล้วนำเสนอหน้าชั้นเรียน 3 ครั้งคือ **ครั้งที่ 1** นำเสนอหัวข้อและขอบเขตของโครงการงาน **ครั้งที่**

2 นำเสนอความคืบหน้าในการดำเนินงาน และครั้งที่ 3 นำเสนอโครงการรอบสุดท้าย ซึ่งต้องแสดงให้เห็นถึงพัฒนาการของการทำงานร่วมกัน และมีการแสดงถึงการปรับปรุงพัฒนาผลงานตามข้อมูลป้อนกลับ (Feedback) ของผู้สอนและเพื่อนร่วมชั้นเรียน โดยทำการศึกษาค้นคว้าจากสื่อและแหล่งข้อมูลอ้างอิงที่หลากหลายที่มีความน่าเชื่อถือทั้งภาษาไทยและภาษาอังกฤษ เช่น ตำรา หนังสือ สื่อสิ่งพิมพ์ งานวิจัย วารสารวิชาการ เว็บไซต์ เป็นต้น และยึดหลักการไม่ละเมิดลิขสิทธิ์และทรัพย์สินทางปัญญาของผู้อื่น กิจกรรมนี้ถือเป็นการส่งเสริมทักษะการรู้สารสนเทศ ทักษะการเรียนรู้ด้วยตนเอง การหาความรู้และมีนิสัยใฝ่รู้ความสามารถในการประยุกต์ใช้ความรู้ให้เหมาะกับบริบททางสังคม และการยึดมั่นในจรรยาบรรณวิชาชีพซึ่งเป็นคุณลักษณะของบัณฑิตไทยในศตวรรษที่ 21 และยังเป็นกิจกรรมที่พัฒนาทักษะการร่วมมือร่วมใจ (Collaboration) การคิดสร้างสรรค์ (Creativity) การติดต่อสื่อสาร (Communication) และการคิดวิเคราะห์ (Critical Thinking) ตามหลักการ 4C

### (3) วิธีการประเมินผล

- การเข้าชั้นเรียน และการมีส่วนร่วมในชั้นเรียน
- การนำเสนอผลการศึกษาค้นคว้าด้วยตนเองเกี่ยวกับสถานการณ์จำลองด้านความมั่นคงทางไซเบอร์
- การนำเสนอโครงการด้านความมั่นคงทางไซเบอร์

## 2. ความรู้

### (1) ความรู้ที่ต้องได้รับ

2.1 มีความรู้ความเข้าใจเกี่ยวกับหลักการและทฤษฎีที่สำคัญในเนื้อหาสาขาวิชาที่ศึกษา

2.2 สามารถวิเคราะห์ปัญหา เข้าใจและอธิบายความต้องการทางคอมพิวเตอร์ รวมทั้งประยุกต์ความรู้ ทักษะ และการใช้เครื่องมือที่เหมาะสมกับการแก้ไขปัญหา

2.4 สามารถติดตามความก้าวหน้าทางวิชาการและวิวัฒนาการคอมพิวเตอร์ รวมทั้งการนำไปประยุกต์

2.7 มีประสบการณ์ในการพัฒนาและ/หรือการประยุกต์ซอฟต์แวร์ที่ใช้งานได้จริง

### (2) วิธีการสอน

- ในคาบบรรยาย จัดการเรียนการสอนแบบผสมผสานระหว่างการเรียนในห้องเรียนและการเรียนออนไลน์ (Blended learning) ผู้สอนเลือกใช้วิธีการบรรยายประกอบไฟล์นำเสนองาน (Microsoft PowerPoint) ร่วมกับสื่อการเรียนการสอนที่มีความหลากหลายและทันสมัย เช่น หนังสืออิเล็กทรอนิกส์ (E-book) วิดีทัศน์ (Video clip) ภาพยนตร์ (Movie) หลักสูตรออนไลน์ (Online course) ซอฟต์แวร์จำลองการฝึกปฏิบัติ (Simulation software or Virtual lab) และเว็บไซต์ (Web site) ที่เกี่ยวข้อง เป็นต้น เพื่อให้นักศึกษาเห็นภาพและเข้าใจเนื้อหา รวมถึงเปิดโอกาสให้นักศึกษาได้แลกเปลี่ยนความคิดเห็นระหว่างกันในหัวข้อเนื้อหาที่น่าสนใจและมีความสำคัญ และในบางหัวข้อจะมีการมอบหมายให้นักศึกษาสื่อวีดิทัศน์ และเอกสาร

ประกอบการสอนมาล่วงหน้าก่อนเข้าชั้นเรียน รวมถึงการศึกษาค้นคว้าด้วยตนเองในเรื่องที่สอดคล้องกับหัวข้อเนื้อหา แล้วมาทำกิจกรรมถามตอบ อภิปราย รวมถึงนำเสนอในห้องเรียนเพื่อแลกเปลี่ยนความรู้และความคิดเห็นร่วมกันในรูปแบบของห้องเรียนกลับด้าน (Flipped classroom)

- ในคาบปฏิบัติการ ให้นักศึกษาได้เรียนรู้และฝึกปฏิบัติด้วยซอฟต์แวร์สำเร็จรูปและภาษาโปรแกรมที่สอดคล้องกับเนื้อหารายวิชา ในรูปแบบของการเรียนรู้ที่เน้นทักษะเป็นฐาน (Skill based learning) แล้วมอบหมายให้นักศึกษาทำแบบฝึกปฏิบัติด้วยตนเอง (Learning by doing) ส่งเสริมทักษะพื้นฐานด้านวิทยาการคอมพิวเตอร์และเทคโนโลยีที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์ ได้แก่ ทักษะการเขียนโปรแกรมและการใช้ซอฟต์แวร์สำเร็จรูปที่เกี่ยวข้อง ภายใต้การดูแลและให้คำแนะนำจากอาจารย์ผู้สอน รวมถึงทักษะการคิดริเริ่มสร้างสรรค์ และการเรียนรู้ด้วยตนเอง ซึ่งเป็นส่วนหนึ่งของคุณสมบัติของบัณฑิตไทยในศตวรรษที่ 21 และเพื่อนำไปต่อยอดกับการเรียนในรายวิชาอื่น ๆ หรือการพัฒนาผลงานทางวิชาการต่อไป
- การแนะนำให้นักศึกษาทำการศึกษาค้นคว้าด้วยตนเองจากแหล่งอ้างอิงอื่น ๆ ที่อาจารย์ผู้สอนรวบรวมและแนะนำไว้ในระบบ E-Learning
- การมอบหมายให้นักศึกษาทำการบ้านในหัวข้อเนื้อหาที่สำคัญเพื่อเป็นการทบทวนความรู้ที่ได้เรียนในชั้นเรียน พร้อมส่งในระบบ E-learning ในวันและเวลาที่ผู้สอนกำหนด
- การมอบหมายให้นักศึกษาทำการศึกษางานวิจัยที่เกี่ยวข้องกับเทคโนโลยี Cyber security จากบทความวิจัยที่เผยแพร่ในวารสารวิชาการระดับนานาชาติในหัวข้อที่นักศึกษาให้ความสนใจ แล้วนำเสนอหน้าชั้นเรียน กิจกรรมนี้ถือเป็นการส่งเสริมทักษะมีความสามารถในการหาความรู้เพิ่มเติม มีนิสัยใฝ่รู้ มีความเท่าทันกับความเคลื่อนไหว และความก้าวหน้าในศาสตร์ที่ศึกษา ซึ่งเป็นคุณลักษณะของบัณฑิตไทยในศตวรรษที่ 21
- การมอบหมายให้นักศึกษาจับคู่กันเพื่อทำการศึกษาค้นคว้าด้วยตนเองเกี่ยวกับสถานการณ์จำลองด้านความมั่นคงทางไซเบอร์ จากโปรแกรม CyberCIEGE ที่มีลักษณะเป็นจำลองสามมิติ (3D Simulation game) ซึ่งประกอบด้วยสถานการณ์จำลอง (Scenario) หลายสถานการณ์ที่สอดคล้องกับเนื้อหาวิชา เช่น Stop worm, Identity theft, Password identify, Network filter เป็นต้น และจากเว็บ Tryhackme.com อย่างละ 1 หัวข้อตามความสนใจ แต่ต้องไม่ซ้ำกันและไม่ซ้ำกับที่ผู้สอนนำมาสอนในชั้นเรียนภาคปฏิบัติการ พร้อมทั้งนำเสนอผลการศึกษาค้นคว้าด้วยตนเองหน้าชั้นเรียนตามที่กำหนดไว้ในแผนการศึกษา อย่างน้อย 2 ครั้งคือ ครั้งที่ 1 นำเสนอหัวข้อที่เลือกศึกษา เพื่อแลกเปลี่ยนความคิดเห็นระหว่างเพื่อนร่วมชั้นเรียนและรับข้อมูลป้อนกลับจากผู้สอน เพื่อนำไปใช้ประกอบการนำเสนอผลการศึกษาในครั้งที่ 2 ตามเวลาที่กำหนดไว้ในแผนการสอน โดยเนื้อหาที่ต้องนำเสนอประกอบด้วย ลักษณะเหตุการณ์ที่เกิดขึ้น ความสอดคล้องของเหตุการณ์กับทฤษฎีหรือหลักการที่เกี่ยวข้อง สถิติของภัยอันตรายที่พบในเหตุการณ์ (อ้างอิงจากหน่วยงานที่มีความน่าเชื่อถือ) ผลกระทบที่มีต่อบุคคล องค์กร และสังคม แนวทางแก้ไขปัญหาที่

เกิดขึ้น รวมไปถึงวิธีป้องกัน (ที่มีเนื้อหาเกี่ยวข้องกับฮาร์ดแวร์ ซอฟต์แวร์ เทคโนโลยี มาตรฐาน และ กฎระเบียบ) ซึ่งมีการอ้างอิงจากแหล่งข้อมูลที่หลากหลายและมีความน่าเชื่อถือ กิจกรรมนี้ถือเป็นการส่งเสริมทักษะการรู้สารสนเทศ ทักษะการเรียนรู้ด้วยตนเอง การหาความรู้และมีนิสัยใฝ่รู้ มีความเท่าทันกับความเคลื่อนไหว และความก้าวหน้าในศาสตร์ที่ศึกษา และการยึดมั่นใน จรรยาบรรณวิชาชีพซึ่งเป็นคุณลักษณะของบัณฑิตไทยในศตวรรษที่ 21 และยังเป็นกิจกรรมที่ พัฒนาทักษะการร่วมมือร่วมใจ (Collaboration) การคิดสร้างสรรค์ (Creativity) การ ติดต่อสื่อสาร (Communication) และการคิดวิเคราะห์ (Critical Thinking) ตามหลักการ 4C

- การมอบหมายให้นักศึกษาจับกลุ่มกัน (กลุ่มละ 2-3 คน) เพื่อนำเสนอโครงงานด้านความ มั่นคงทางไซเบอร์ของหน่วยงาน/สถานประกอบการของภาคธุรกิจหรือภาคอุตสาหกรรมตาม ความสนใจ (แต่ต้องไม่ซ้ำกัน) โดยทำการการออกแบบและพัฒนาระบบรักษาความมั่นคงทาง ไซเบอร์ ให้กับระบบฐานข้อมูล เครือข่ายคอมพิวเตอร์ทั้งแบบ Wired และ Wireless network รวมถึงเว็บไซต์ของหน่วยงาน/สถานประกอบการที่เลือก ซึ่งระบบรักษาความมั่นคง ทางไซเบอร์ที่นำเสนอจะต้องประกอบด้วยฮาร์ดแวร์ ซอฟต์แวร์ นโยบาย มาตรฐาน และ เทคโนโลยีทางด้านปัญญาประดิษฐ์ที่เหมาะสมกับลักษณะธุรกิจหรืออุตสาหกรรมที่เลือก แล้วนำเสนอหน้าชั้นเรียน 3 ครั้งคือ **ครั้งที่ 1** นำเสนอหัวข้อและขอบเขตของโครงงาน **ครั้งที่ 2** นำเสนอความคืบหน้าในการดำเนินงาน และ**ครั้งที่ 3** นำเสนอโครงงานรอบสุดท้าย ซึ่งต้อง แสดงให้เห็นถึงพัฒนาการของการทำงานร่วมกัน และมีการแสดงถึงการปรับปรุงพัฒนาผลงาน ตามข้อมูลป้อนกลับ (Feedback) ของผู้สอนและเพื่อนร่วมชั้นเรียน โดยทำการศึกษาค้นคว้า จากสื่อและแหล่งข้อมูลอ้างอิงที่หลากหลายที่มีความน่าเชื่อถือทั้งภาษาไทยและ ภาษาอังกฤษ เช่น ตำรา หนังสือ สื่อสิ่งพิมพ์ งานวิจัย วารสารวิชาการ เว็บไซต์ เป็นต้น และ ยึดหลักการไม่ละเมิดลิขสิทธิ์และทรัพย์สินทางปัญญาของผู้อื่น กิจกรรมนี้ถือเป็นการส่งเสริม ทักษะการรู้สารสนเทศ ทักษะการเรียนรู้ด้วยตนเอง การหาความรู้และมีนิสัยใฝ่รู้ ความสามารถในการประยุกต์ใช้ความรู้ให้เหมาะสมกับบริบททางสังคม และการยึดมั่นใน จรรยาบรรณวิชาชีพซึ่งเป็นคุณลักษณะของบัณฑิตไทยในศตวรรษที่ 21 และยังเป็นกิจกรรมที่ พัฒนาทักษะการร่วมมือร่วมใจ (Collaboration) การคิดสร้างสรรค์ (Creativity) การ ติดต่อสื่อสาร (Communication) และการคิดวิเคราะห์ (Critical Thinking) ตามหลักการ 4C

### (3)วิธีการประเมินผล

- การเข้าชั้นเรียน และการมีส่วนร่วมในชั้นเรียน
- การส่งงานมอบหมายในชั้นเรียนภาคปฏิบัติ
- การนำเสนอผลการศึกษาค้นคว้าเกี่ยวกับความมั่นคงทางไซเบอร์
- การนำเสนอผลการศึกษาค้นคว้าด้วยตนเองเกี่ยวกับสถานการณ์จำลองด้านความมั่นคงทางไซเบอร์



- การนำเสนอโครงการด้านความมั่นคงทางไซเบอร์
- การสอบกลางภาคเรียน
- การสอบปลายภาคเรียน

### 3. ทักษะทางปัญญา

#### (1) ทักษะทางปัญญาที่ต้องพัฒนา

3.4 สามารถประยุกต์ความรู้และทักษะกับการแก้ไขปัญหาทางคอมพิวเตอร์ได้อย่างเหมาะสม

#### (2) วิธีการสอน

- ในคาบปฏิบัติการ ให้นักศึกษาได้เรียนรู้และฝึกปฏิบัติด้วยซอฟต์แวร์สำเร็จรูปและภาษาโปรแกรมที่สอดคล้องกับเนื้อหารายวิชา ในรูปแบบของการเรียนรู้ที่เน้นทักษะเป็นฐาน (Skill based learning) แล้วมอบหมายให้นักศึกษาทำแบบฝึกปฏิบัติการด้วยตนเอง (Learning by doing) ส่งเสริมทักษะพื้นฐานด้านวิทยาการคอมพิวเตอร์และเทคโนโลยีที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์ ได้แก่ ทักษะการเขียนโปรแกรมและการใช้ซอฟต์แวร์สำเร็จรูปที่เกี่ยวข้อง ภายใต้การดูแลและให้คำแนะนำจากอาจารย์ผู้สอน รวมถึงทักษะการคิดริเริ่มสร้างสรรค์ และการเรียนรู้ด้วยตนเอง ซึ่งเป็นส่วนหนึ่งของคุณสมบัติของบัณฑิตไทยในศตวรรษที่ 21 และเพื่อนำไปต่อยอดกับการเรียนในรายวิชาอื่น ๆ หรือการพัฒนาผลงานทางวิชาการต่อไป
- การมอบหมายให้นักศึกษาจับคู่กันเพื่อทำการศึกษาค้นคว้าด้วยตนเองเกี่ยวกับสถานการณ์จำลองด้านความมั่นคงทางไซเบอร์ จากโปรแกรม CyberCIEGE ที่มีลักษณะเป็นจำลองสามมิติ (3D Simulation game) ซึ่งประกอบด้วยสถานการณ์จำลอง (Scenario) หลายสถานการณ์ที่สอดคล้องกับเนื้อหาวิชา เช่น Stop worm, Identity theft, Password identify, Network filter เป็นต้น และจากเว็บ Tryhackme.com อย่างละ 1 หัวข้อตามความสนใจ แต่ต้องไม่ซ้ำกันและไม่ซ้ำกับที่ผู้สอนนำมาสอนในชั้นเรียนภาคปฏิบัติการ พร้อมทั้งนำเสนอผลการศึกษาค้นคว้าด้วยตนเองหน้าชั้นเรียนตามที่กำหนดไว้ในแผนการศึกษา อย่างน้อย 2 ครั้งคือ ครั้งที่ 1 นำเสนอหัวข้อที่เลือกศึกษา เพื่อแลกเปลี่ยนความคิดเห็นระหว่างเพื่อนร่วมชั้นเรียนและรับข้อมูลป้อนกลับจากผู้สอน เพื่อนำไปใช้ประกอบการนำเสนอผลการศึกษาในครั้งที่ 2 ตามเวลาที่กำหนดไว้ในแผนการสอน โดยเนื้อหาที่ต้องนำเสนอประกอบด้วย ลักษณะเหตุการณ์ที่เกิดขึ้น ความสอดคล้องของเหตุการณ์กับทฤษฎีหรือหลักการที่เกี่ยวข้อง สถิติของภัยอันตรายที่พบในเหตุการณ์ (อ้างอิงจากหน่วยงานที่มีความน่าเชื่อถือ) ผลกระทบที่มีต่อบุคคล องค์กร และสังคม แนวทางแก้ไขปัญหาที่เกิดขึ้น รวมไปถึงวิธีป้องกัน (ที่มีเนื้อหาเกี่ยวข้องกับฮาร์ดแวร์ ซอฟต์แวร์ เทคโนโลยี มาตรฐาน และกฎระเบียบ) ซึ่งมีการอ้างอิงจากแหล่งข้อมูลที่หลากหลายและมีความน่าเชื่อถือ กิจกรรมนี้ถือเป็นการส่งเสริมทักษะการรู้สารสนเทศ ทักษะการเรียนรู้ด้วยตนเอง การหาความรู้และมินิสัยไฟรู้

มีความเท่าทันกับความเคลื่อนไหว และความก้าวหน้าในศาสตร์ที่ศึกษา และการยึดมั่นในจรรยาบรรณวิชาชีพซึ่งเป็นคุณลักษณะของบัณฑิตไทยในศตวรรษที่ 21 และยังเป็นกิจกรรมที่พัฒนาทักษะการร่วมมือร่วมใจ (Collaboration) การคิดสร้างสรรค์ (Creativity) การติดต่อสื่อสาร (Communication) และการคิดวิเคราะห์ (Critical Thinking) ตามหลักการ 4C

- การมอบหมายให้นักศึกษาจับกลุ่มกัน (กลุ่มละ 2-3 คน) เพื่อนำเสนอโครงงานด้านความมั่นคงทางไซเบอร์ของหน่วยงาน/สถานประกอบการของภาคธุรกิจหรือภาคอุตสาหกรรมตามความสนใจ (แต่ต้องไม่ซ้ำกัน) โดยทำการการออกแบบและพัฒนาระบบรักษาความมั่นคงทางไซเบอร์ ให้กับระบบฐานข้อมูล เครือข่ายคอมพิวเตอร์ทั้งแบบ Wired และ Wireless network รวมถึงเว็บไซต์ของหน่วยงาน/สถานประกอบการที่เลือก ซึ่งระบบรักษาความมั่นคงทางไซเบอร์ที่นำเสนอจะต้องประกอบด้วยฮาร์ดแวร์ ซอฟต์แวร์ นโยบาย มาตรฐาน และเทคโนโลยีทางด้านปัญญาประดิษฐ์ที่เหมาะสมกับลักษณะธุรกิจหรืออุตสาหกรรมที่เลือก แล้วนำเสนอหน้าชั้นเรียน 3 ครั้งคือ **ครั้งที่ 1** นำเสนอหัวข้อและขอบเขตของโครงงาน **ครั้งที่ 2** นำเสนอความคืบหน้าในการดำเนินงาน และ**ครั้งที่ 3** นำเสนอโครงงานรอบสุดท้าย **ซึ่งต้องแสดงให้เห็นถึงพัฒนาการของการทำงานร่วมกัน และมีการแสดงถึงการปรับปรุงพัฒนาผลงานตามข้อมูลป้อนกลับ (Feedback) ของผู้สอนและเพื่อนร่วมชั้นเรียน** โดยทำการศึกษาค้นคว้าจากสื่อและแหล่งข้อมูลอ้างอิงที่หลากหลายที่มีความน่าเชื่อถือทั้งภาษาไทยและภาษาอังกฤษ เช่น ตำรา หนังสือ สื่อสิ่งพิมพ์ งานวิจัย วารสารวิชาการ เว็บไซต์ เป็นต้น และยึดหลักการไม่ละเมิดลิขสิทธิ์และทรัพย์สินทางปัญญาของผู้อื่น กิจกรรมนี้ถือเป็นการส่งเสริมทักษะการรู้สารสนเทศ ทักษะการเรียนรู้ด้วยตนเอง การหาความรู้และมีนิสัยใฝ่รู้ความสามารถในการประยุกต์ใช้ความรู้ให้เหมาะกับบริบททางสังคม และการยึดมั่นในจรรยาบรรณวิชาชีพซึ่งเป็นคุณลักษณะของบัณฑิตไทยในศตวรรษที่ 21 และยังเป็นกิจกรรมที่พัฒนาทักษะการร่วมมือร่วมใจ (Collaboration) การคิดสร้างสรรค์ (Creativity) การติดต่อสื่อสาร (Communication) และการคิดวิเคราะห์ (Critical Thinking) ตามหลักการ 4C

### (3)วิธีการประเมินผล

- การส่งงานมอบหมายในชั้นเรียนภาคปฏิบัติ
- การนำเสนอผลการศึกษาค้นคว้าด้วยตนเองเกี่ยวกับสถานการณ์จำลองด้านความมั่นคงทางไซเบอร์
- การนำเสนอโครงงานด้านความมั่นคงทางไซเบอร์
- การสอบกลางภาคเรียน
- การสอบปลายภาคเรียน

#### 4. ทักษะความสัมพันธ์ระหว่างบุคคลและความรับผิดชอบ

##### (1) ทักษะความสัมพันธ์ระหว่างบุคคลและความรับผิดชอบที่ต้องพัฒนา

##### 4.4 มีความรับผิดชอบในการกระทำของตนเองและรับผิดชอบงานในกลุ่ม

##### (2) วิธีการสอน

- ในคาบปฏิบัติการ ให้นักศึกษาได้เรียนรู้และฝึกปฏิบัติด้วยซอฟต์แวร์สำเร็จรูปและภาษาโปรแกรมที่สอดคล้องกับเนื้อหารายวิชา ในรูปแบบของการเรียนรู้ที่เน้นทักษะเป็นฐาน (Skill based learning) แล้วมอบหมายให้นักศึกษาทำแบบฝึกปฏิบัติการด้วยตนเอง (Learning by doing) ส่งเสริมทักษะพื้นฐานด้านวิทยาการคอมพิวเตอร์และเทคโนโลยีที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์ ได้แก่ ทักษะการเขียนโปรแกรมและการใช้ซอฟต์แวร์สำเร็จรูปที่เกี่ยวข้อง ภายใต้การดูแลและให้คำแนะนำจากอาจารย์ผู้สอน รวมถึงทักษะการคิดริเริ่มสร้างสรรค์ และการเรียนรู้ด้วยตนเอง ซึ่งเป็นส่วนหนึ่งของ คุณสมบัติของบัณฑิตไทยในศตวรรษที่ 21 และเพื่อนำไปต่อยอดกับการเรียนในรายวิชาอื่น ๆ หรือการพัฒนาผลงานทางวิชาการต่อไป
- การมอบหมายให้นักศึกษารวบรวมไฟล์การบ้าน แบบฝึกภาคปฏิบัติการ และงานมอบหมายต่าง ๆ ไว้ในระบบ HCU E-learning เพื่อใช้สำหรับประเมินช่วงก่อนสอบปลายภาค
- การมอบหมายให้นักศึกษาทำการศึกษางานวิจัยที่เกี่ยวข้องกับเทคโนโลยี Cyber security จากบทความวิจัยที่เผยแพร่ในวารสารวิชาการระดับนานาชาติในหัวข้อที่นักศึกษาให้ความสนใจ แล้วนำเสนอหน้าชั้นเรียนใน กิจกรรมนี้ถือเป็นการส่งเสริมทักษะมีความสามารถในการหาความรู้เพิ่มเติม มีนิสัยใฝ่รู้ มีความเท่าทันกับความเคลื่อนไหว และความก้าวหน้าในศาสตร์ที่ศึกษา ซึ่งเป็นคุณลักษณะของบัณฑิตไทยในศตวรรษที่ 21
- การมอบหมายให้นักศึกษาจับคู่กันเพื่อทำการศึกษาค้นคว้าด้วยตนเองเกี่ยวกับสถานการณ์จำลองด้านความมั่นคงทางไซเบอร์ จากโปรแกรม CyberCIEGE ที่มีลักษณะเป็นจำลองสามมิติ (3D Simulation game) ซึ่งประกอบด้วยสถานการณ์จำลอง (Scenario) หลายสถานการณ์ที่สอดคล้องกับเนื้อหารายวิชา เช่น Stop worm, Identity theft, Password identify, Network filter เป็นต้น และจากเว็บ Tryhackme.com อย่างละ 1 หัวข้อตามความสนใจ แต่ต้องไม่ซ้ำกันและไม่ซ้ำกับที่ผู้สอนนำมาสอนในชั้นเรียนภาคปฏิบัติการ พร้อมทั้งนำเสนอผลการศึกษาค้นคว้าด้วยตนเองหน้าชั้นเรียนตามที่กำหนดไว้ในแผนการศึกษา อย่างน้อย 2 ครั้งคือ ครั้งที่ 1 นำเสนอหัวข้อที่เลือกศึกษา เพื่อแลกเปลี่ยนความคิดเห็นระหว่างเพื่อนร่วมชั้นเรียนและรับข้อมูลป้อนกลับจากผู้สอน เพื่อนำไปใช้ประกอบการนำเสนอผลการศึกษาในครั้งที่ 2 ตามเวลาที่กำหนดไว้ในแผนการสอน โดยเนื้อหาที่ต้องนำเสนอประกอบด้วย ลักษณะเหตุการณ์ที่เกิดขึ้น ความสอดคล้องของเหตุการณ์กับทฤษฎีหรือหลักการที่เกี่ยวข้อง สถิติของภัยอันตรายที่พบในเหตุการณ์ (อ้างอิงจากหน่วยงานที่มีความน่าเชื่อถือ) ผลกระทบที่มีต่อบุคคล องค์กร และสังคม แนวทางแก้ไขปัญหาที่เกิดขึ้น รวมไปถึงวิธีป้องกัน (ที่มีเนื้อหาเกี่ยวข้องกับฮาร์ดแวร์ ซอฟต์แวร์ เทคโนโลยี มาตรฐาน และกฎระเบียบ) ซึ่งมีการอ้างอิงจากแหล่งข้อมูลที่หลากหลายและมีความน่าเชื่อถือ กิจกรรมนี้ถือเป็น

การส่งเสริมทักษะการรู้สารสนเทศ ทักษะการเรียนรู้ด้วยตนเอง การหาความรู้และมีนิสัยใฝ่รู้ มีความเท่าทันกับความเคลื่อนไหว และความก้าวหน้าในศาสตร์ที่ศึกษา และการยึดมั่นใน จรรยาบรรณวิชาชีพซึ่งเป็นคุณลักษณะของบัณฑิตไทยในศตวรรษที่ 21 และยังเป็นกิจกรรมที่ พัฒนาทักษะการร่วมมือร่วมใจ (Collaboration) การคิดสร้างสรรค์ (Creativity) การ ติดต่อสื่อสาร (Communication) และการคิดวิเคราะห์ (Critical Thinking) ตามหลักการ 4C

- การมอบหมายให้นักศึกษาจับกลุ่มกัน (กลุ่มละ 2-3 คน) เพื่อนำเสนอโครงงานด้านความ มั่นคงทางไซเบอร์ของหน่วยงาน/สถานประกอบการของภาคธุรกิจหรือภาคอุตสาหกรรมตาม ความสนใจ (แต่ต้องไม่ซ้ำกัน) โดยทำการการออกแบบและพัฒนาระบบรักษาความมั่นคงทาง ไซเบอร์ ให้กับระบบฐานข้อมูล เครือข่ายคอมพิวเตอร์ทั้งแบบ Wired และ Wireless network รวมถึงเว็บไซต์ของหน่วยงาน/สถานประกอบการที่เลือก ซึ่งระบบรักษาความมั่นคง ทางไซเบอร์ที่นำเสนอจะต้องประกอบด้วยฮาร์ดแวร์ ซอฟต์แวร์ นโยบาย มาตรฐาน และ เทคโนโลยีทางด้านปัญญาประดิษฐ์ที่เหมาะสมกับลักษณะธุรกิจหรืออุตสาหกรรมที่เลือก แล้วนำเสนอหน้าชั้นเรียน 3 ครั้งคือ **ครั้งที่ 1** นำเสนอหัวข้อและขอบเขตของโครงงาน **ครั้งที่ 2** นำเสนอความคืบหน้าในการดำเนินงาน และ**ครั้งที่ 3** นำเสนอโครงงานรอบสุดท้าย **ซึ่งต้อง แสดงให้เห็นถึงพัฒนาการของการทำงานร่วมกัน และมีการแสดงถึงการปรับปรุงพัฒนาผลงาน ตามข้อมูลป้อนกลับ (Feedback) ของผู้สอนและเพื่อนร่วมชั้นเรียน** โดยทำการศึกษาค้นคว้า จากสื่อและแหล่งข้อมูลอ้างอิงที่หลากหลายที่มีความน่าเชื่อถือ**ทั้งภาษาไทยและ ภาษาอังกฤษ** เช่น ตำรา หนังสือ สื่อสิ่งพิมพ์ งานวิจัย วารสารวิชาการ เว็บไซต์ เป็นต้น และ ยึดหลักการไม่ละเมิดลิขสิทธิ์และทรัพย์สินทางปัญญาของผู้อื่น **กิจกรรมนี้ถือเป็นการส่งเสริม ทักษะการรู้สารสนเทศ ทักษะการเรียนรู้ด้วยตนเอง การหาความรู้และมีนิสัยใฝ่รู้ ความสามารถในการประยุกต์ใช้ความรู้ให้เหมาะกับบริบททางสังคม และการยึดมั่นใน จรรยาบรรณวิชาชีพซึ่งเป็นคุณลักษณะของบัณฑิตไทยในศตวรรษที่ 21 และยังเป็นกิจกรรมที่ พัฒนาทักษะการร่วมมือร่วมใจ (Collaboration) การคิดสร้างสรรค์ (Creativity) การ ติดต่อสื่อสาร (Communication) และการคิดวิเคราะห์ (Critical Thinking) ตามหลักการ 4C**

### (3)วิธีการประเมิน

- การเข้าชั้นเรียน และการมีส่วนร่วมในชั้นเรียน
- การส่งงานมอบหมายในชั้นเรียนภาคปฏิบัติ
- การนำเสนอผลการศึกษาค้นคว้าเกี่ยวกับความมั่นคงทางไซเบอร์
- การนำเสนอผลการศึกษาค้นคว้าด้วยตนเองเกี่ยวกับสถานการณ์จำลองด้านความมั่นคงทางไซเบอร์
- การนำเสนอโครงงานด้านความมั่นคงทางไซเบอร์

## 5. ทักษะการวิเคราะห์เชิงตัวเลข การสื่อสารและการใช้เทคโนโลยีสารสนเทศ

### (1) ทักษะการวิเคราะห์เชิงตัวเลข การสื่อสารและการใช้เทคโนโลยีสารสนเทศที่ต้องพัฒนา

#### 5.1 มีทักษะในการใช้เครื่องมือที่จำเป็นที่มีอยู่ในปัจจุบันต่อการทำงานที่เกี่ยวกับคอมพิวเตอร์

5.3 สามารถสื่อสารอย่างมีประสิทธิภาพทั้งปากเปล่าและการเขียน เลือกใช้รูปแบบของสื่อการนำเสนออย่างเหมาะสม

### (2)วิธีการสอน

- ในคาบปฏิบัติการ ให้นักศึกษาได้เรียนรู้และฝึกปฏิบัติด้วยซอฟต์แวร์สำเร็จรูปและภาษาโปรแกรมที่สอดคล้องกับเนื้อหารายวิชา ในรูปแบบของการเรียนรู้ที่เน้นทักษะเป็นฐาน (Skill based learning) แล้วมอบหมายให้นักศึกษาทำแบบฝึกปฏิบัติด้วยตนเอง (Learning by doing) ส่งเสริมทักษะพื้นฐานด้านวิทยาการคอมพิวเตอร์และเทคโนโลยีที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์ ได้แก่ ทักษะการเขียนโปรแกรมและการใช้ซอฟต์แวร์สำเร็จรูปที่เกี่ยวข้อง ภายใต้การดูแลและให้คำแนะนำจากอาจารย์ผู้สอน รวมถึงทักษะการคิดริเริ่มสร้างสรรค์ และการเรียนรู้ด้วยตนเอง ซึ่งเป็นส่วนหนึ่งของคุณสมบัติของบัณฑิตไทยในศตวรรษที่ 21 และเพื่อนำไปต่อยอดกับการเรียนในรายวิชาอื่น ๆ หรือการพัฒนาผลงานทางวิชาการต่อไป
- การมอบหมายให้นักศึกษาจับคู่กันเพื่อทำการศึกษาค้นคว้าด้วยตนเองเกี่ยวกับสถานการณ์จำลองด้านความมั่นคงทางไซเบอร์ จากโปรแกรม CyberCIEGE ที่มีลักษณะเป็นจำลองสามมิติ (3D Simulation game) ซึ่งประกอบด้วยสถานการณ์จำลอง (Scenario) หลายสถานการณ์ที่สอดคล้องกับเนื้อหารายวิชา เช่น Stop worm, Identity theft, Password identify, Network filter เป็นต้น และจากเว็บ Tryhackme.com อย่างละ 1 หัวข้อตามความสนใจ แต่ต้องไม่ซ้ำกันและไม่ซ้ำกับที่ผู้สอนนำมาสอนในชั้นเรียนภาคปฏิบัติการ พร้อมทั้งนำเสนอผลการศึกษาค้นคว้าด้วยตนเองหน้าชั้นเรียนตามที่กำหนดไว้ในแผนการศึกษา อย่างน้อย 2 ครั้งคือ ครั้งที่ 1 นำเสนอหัวข้อที่เลือกศึกษา เพื่อแลกเปลี่ยนความคิดเห็นระหว่างเพื่อนร่วมชั้นเรียนและรับข้อมูลป้อนกลับจากผู้สอน เพื่อนำไปใช้ประกอบการนำเสนอผลการศึกษาในครั้งที่ 2 ตามเวลาที่กำหนดไว้ในแผนการสอน โดยเนื้อหาที่ต้องนำเสนอประกอบด้วย ลักษณะเหตุการณ์ที่เกิดขึ้น ความสอดคล้องของเหตุการณ์กับทฤษฎีหรือหลักการที่เกี่ยวข้อง สถิติของภัยอันตรายที่พบในเหตุการณ์ (อ้างอิงจากหน่วยงานที่มีความน่าเชื่อถือ) ผลกระทบที่มีต่อบุคคล องค์กร และสังคม แนวทางแก้ไขปัญหาที่เกิดขึ้น รวมไปถึงวิธีป้องกัน (ที่มีเนื้อหาเกี่ยวข้องกับฮาร์ดแวร์ ซอฟต์แวร์ เทคโนโลยี มาตรฐาน และกฎระเบียบ) ซึ่งมีการอ้างอิงจากแหล่งข้อมูลที่หลากหลายและมีความน่าเชื่อถือ กิจกรรมนี้ถือเป็น การส่งเสริมทักษะการรู้สารสนเทศ ทักษะการเรียนรู้ด้วยตนเอง การหาความรู้และมีนิสัยใฝ่รู้ มีความเท่าทันกับความเคลื่อนไหว และความก้าวหน้าในศาสตร์ที่ศึกษา และการยึดมั่นในจรรยาบรรณวิชาชีพซึ่งเป็นคุณลักษณะของบัณฑิตไทยในศตวรรษที่ 21 และยังเป็นกิจกรรมที่พัฒนาทักษะการร่วมมือร่วมใจ (Collaboration) การคิดสร้างสรรค์ (Creativity) การ

## ติดต่อสื่อสาร (Communication) และการคิดวิเคราะห์ (Critical Thinking) ตามหลักการ 4C

- การมอบหมายให้นักศึกษาจับกลุ่มกัน (กลุ่มละ 2-3 คน) เพื่อนำเสนอโครงการด้านความมั่นคงทางไซเบอร์ของหน่วยงาน/สถานประกอบการของภาคธุรกิจหรือภาคอุตสาหกรรมตามความสนใจ (แต่ต้องไม่ซ้ำกัน) โดยทำการการออกแบบและพัฒนาระบบรักษาความมั่นคงทางไซเบอร์ ให้กับระบบฐานข้อมูล เครือข่ายคอมพิวเตอร์ทั้งแบบ Wired และ Wireless network รวมถึงเว็บไซต์ของหน่วยงาน/สถานประกอบการที่เลือก ซึ่งระบบรักษาความมั่นคงทางไซเบอร์ที่นำเสนอจะต้องประกอบด้วยฮาร์ดแวร์ ซอฟต์แวร์ นโยบาย มาตรฐาน และเทคโนโลยีทางด้านปัญหาประดิษฐ์ที่เหมาะสมกับลักษณะธุรกิจหรืออุตสาหกรรมที่เลือก แล้วนำเสนอหน้าชั้นเรียน 3 ครั้งคือ **ครั้งที่ 1** นำเสนอหัวข้อและขอบเขตของโครงการ **ครั้งที่ 2** นำเสนอความคืบหน้าในการดำเนินงาน และ**ครั้งที่ 3** นำเสนอโครงการรอบสุดท้าย **ซึ่งต้องแสดงให้เห็นถึงพัฒนาการของการทำงานร่วมกัน และมีการแสดงถึงการปรับปรุงพัฒนาผลงานตามข้อมูลป้อนกลับ (Feedback) ของผู้สอนและเพื่อนร่วมชั้นเรียน** โดยทำการศึกษาค้นคว้าจากสื่อและแหล่งข้อมูลอ้างอิงที่หลากหลายที่มีความน่าเชื่อถือ**ทั้งภาษาไทยและภาษาอังกฤษ** เช่น ตำรา หนังสือ สื่อสิ่งพิมพ์ งานวิจัย วารสารวิชาการ เว็บไซต์ เป็นต้น และยึดหลักการไม่ละเมิดลิขสิทธิ์และทรัพย์สินทางปัญญาของผู้อื่น กิจกรรมนี้ถือเป็นการส่งเสริมทักษะการรู้สารสนเทศ ทักษะการเรียนรู้ด้วยตนเอง การหาความรู้และมีนิสัยใฝ่รู้ความสามารถในการประยุกต์ใช้ความรู้ให้เหมาะสมกับบริบททางสังคม และการยึดมั่นในจรรยาบรรณวิชาชีพซึ่งเป็นคุณลักษณะของบัณฑิตไทยในศตวรรษที่ 21 และยังเป็น**กิจกรรมที่พัฒนาทักษะการร่วมมือร่วมใจ (Collaboration) การคิดสร้างสรรค์ (Creativity) การติดต่อสื่อสาร (Communication) และการคิดวิเคราะห์ (Critical Thinking) ตามหลักการ 4C**

### (3)วิธีการประเมินผล

- การส่งงานมอบหมายในชั้นเรียนภาคปฏิบัติ
- การนำเสนอผลการศึกษาค้นคว้าวิจัยเกี่ยวกับความมั่นคงทางไซเบอร์
- การนำเสนอผลการศึกษาค้นคว้าด้วยตนเองเกี่ยวกับสถานการณ์จำลองด้านความมั่นคงทางไซเบอร์
- การนำเสนอโครงการด้านความมั่นคงทางไซเบอร์

### หมวดที่ 5 แผนการสอนและการประเมินผล

#### 1. แผนการสอน (เขียนให้สอดคล้องกับ Curriculum Mapping และสอดคล้องกับหมวดที่ 4 การพัฒนาผลการเรียนรู้ของนักศึกษา)

สัปดาห์ที่	หัวข้อ/รายละเอียด	กิจกรรมการเรียนการสอน และสื่อที่ใช้	จำนวน ชั่วโมง	ชื่อผู้สอน
1 (11/8/65)	<p><b>บรรยาย</b></p> <ul style="list-style-type: none"> <li>แนะนำรายละเอียดวิชา (Course Introduction) ทำความตกลงเรื่อง กติกาในการเรียนการสอน การมอบหมายงานต่าง ๆ การวัดและประเมินผล</li> <li>Introduction to Information security and Cyber security</li> <li>History of Information security</li> <li>มอบหมายงานการศึกษา ค้นคว้างานวิจัยที่เกี่ยวข้องกับเทคโนโลยีด้านความมั่นคงทางไซเบอร์</li> </ul>	<p><b>ภาคบรรยาย</b></p> <ul style="list-style-type: none"> <li>ชี้แจงรายละเอียดวิชา รูปแบบวิธีการเรียนการสอนและเกณฑ์การวัดและประเมินผล <b>ที่ให้นักศึกษามีส่วนร่วมและการมอบหมายงานตลอดภาคการศึกษา</b></li> <li>ชี้แจงและมอบหมายให้นักศึกษา ทำการศึกษาบทเรียนจากเอกสาร ประกอบการสอน Video บันทึกการสอนออนไลน์ และ Video clips หรือสื่ออื่น ๆ ที่ปรากฏในเอกสารมคอ.3 และ e-Learning ล่วงหน้าก่อนเรียนคาบถัดไปทุกครั้ง <b>รวมถึงการจัดการเรียนการสอนแบบห้องเรียนกลับด้าน (Flipped classroom)</b></li> <li>การสอดแทรกจริยธรรมและคุณธรรม อัตลักษณ์ของมหาวิทยาลัย (ยึดมั่นในคุณธรรม 6 ประการ ชยัน อดทน ประหยัด เมตตา ซื่อสัตย์ กตัญญู) และได้ย้ำเตือนให้นักศึกษาดำเนินชีวิตตามหลักปรัชญาเศรษฐกิจพอเพียง และเรียนรู้เพื่อรับใช้สังคม รวมถึงการปฏิบัติตามกฎระเบียบของมหาวิทยาลัย การไม่ทุจริตในการสอบ การไม่ละเมิดลิขสิทธิ์ และการยึดมั่นในจรรยาบรรณวิชาชีพ</li> <li>บรรยายประกอบการยกตัวอย่างด้วย MS-PowerPoint, E-books, Video clips, Movies, Course online และเว็บไซต์ที่เกี่ยวข้อง</li> <li>รับชมวีดิทัศน์ที่เกี่ยวข้อง</li> </ul>	(2/3/0)	<p><b>บรรยาย</b></p> <p>อาจารย์ณัฐพร</p>

		<ul style="list-style-type: none"> <li>● ถาม-ตอบคำถามสั้น ๆ เพื่อประเมิน ศักยภาพผู้เรียน</li> <li>● แนะนำแหล่งข้อมูลอ้างอิงและสื่อการสอนต่าง ๆ ที่เกี่ยวข้อง</li> </ul> <b>สื่อที่ใช้</b> <ul style="list-style-type: none"> <li>● MS-PowerPoint</li> <li>● HCU E-learning</li> <li>● E-book (Thai and English)</li> <li>● Video clips</li> <li>● Other medias/References website [Publish on HCU E-learning]</li> <li>● Online conference system: MS-Teams and etc.</li> </ul>		
1 (8/8/65)	<b>ปฏิบัติ</b> <ul style="list-style-type: none"> <li>● ทบทวนทักษะปฏิบัติการพื้นฐานด้านเครือข่ายคอมพิวเตอร์ <ul style="list-style-type: none"> <li>○ Command</li> <li>○ Software tools</li> </ul> </li> <li>● Search for Cyber security and AI research paper</li> </ul>	<b>ปฏิบัติ</b> <ul style="list-style-type: none"> <li>● ฝึกปฏิบัติการทบทวนด้าน Network ด้วยคำสั่งบนระบบปฏิบัติการ Windows และ Linux</li> <li>● ฝึกปฏิบัติการด้านการตรวจสอบเครือข่ายคอมพิวเตอร์ด้วยซอฟต์แวร์สำเร็จรูปที่เกี่ยวข้อง</li> <li>● นักศึกษาสืบค้นข้อมูลงานวิจัยด้าน Cyber security ภายใต้อำนาจแนะนำของอาจารย์ผู้สอน</li> </ul> <b>สื่อที่ใช้</b> <ul style="list-style-type: none"> <li>● MS-PowerPoint</li> <li>● HCU e-Learning</li> <li>● Cyber security software/tools</li> <li>● Cyber security website</li> <li>● Network software: Wireshark, Samspace, whois, etc.</li> <li>● Online conference system: MS-Teams, and etc.</li> </ul>		<b>ปฏิบัติ</b> อาจารย์ณัฐพร
2 (18/8/65)	<b>บรรยาย</b> <ul style="list-style-type: none"> <li>● Telecommunication security</li> </ul>	<b>บรรยาย</b> <ul style="list-style-type: none"> <li>● บรรยายประกอบการยกตัวอย่างด้วย MS-PowerPoint, E-books, Video</li> </ul>	(2/3/0)	<b>บรรยาย</b> อาจารย์ ดร. ธีรวัฒน์



		<p>clips, Movies/Game/Cartoon, Course online และเว็บไซต์ที่เกี่ยวข้อง</p> <ul style="list-style-type: none"> <li>• ตอบคำถามสั้น ๆ เพื่อประเมินความรู้ความเข้าใจของนักศึกษา</li> <li>• รับชมวีดิทัศน์ที่เกี่ยวข้อง</li> </ul> <p><b>สื่อที่ใช้</b></p> <ul style="list-style-type: none"> <li>• MS-PowerPoint</li> <li>• HCU E-learning</li> <li>• E-book (Thai and English)</li> <li>• Video clips</li> <li>• Other medias/References website [Publish on HCU E-learning]</li> <li>• Online conference system: MS-Teams and etc.</li> </ul>		
2 (15/8/65)	<p><b>ปฏิบัติ</b></p> <ul style="list-style-type: none"> <li>• Create TryHackMe.com account <a href="https://tryhackme.com/">https://tryhackme.com/</a></li> <li>• Learning how to use tryhackme.com from tutorial <a href="https://tryhackme.com/room/tutorial">https://tryhackme.com/room/tutorial</a></li> <li>• Introduction to CyberCIEGE website</li> </ul>	<p><b>ปฏิบัติ</b></p> <ul style="list-style-type: none"> <li>• สมัครใช้งาน TryHackMe.com website</li> <li>• ฝึกปฏิบัติการเรียนรู้การใช้งาน TryHackme.com website จาก Tutorial</li> <li>• แนะนำเว็บไซต์เพื่อดาวน์โหลด CyberCIEGE</li> </ul> <p><b>สื่อที่ใช้</b></p> <ul style="list-style-type: none"> <li>• MS-PowerPoint</li> <li>• HCU e-Learning</li> <li>• Google Search Engine</li> <li>• Cyber security website</li> <li>• CyberCIEGE website</li> <li>• Online conference system: MS-Teams, and etc.</li> </ul>		<p><b>ปฏิบัติ</b></p> <p>อาจารย์ณัฐพร</p>
3 (25/8/65)	<p><b>บรรยาย</b></p> <ul style="list-style-type: none"> <li>• Cybercrime, threat, attack, and vulnerability</li> </ul>	<p><b>บรรยาย</b></p> <ul style="list-style-type: none"> <li>• บรรยายประกอบการยกตัวอย่างด้วย MS-PowerPoint, E-books, Video clips, Movies/Game/Cartoon,</li> </ul>	(2/3/0)	<p><b>บรรยาย</b></p> <p>อาจารย์ณัฐพร</p>

		<p>Course online และเว็บไซต์ที่เกี่ยวข้อง</p> <ul style="list-style-type: none"> <li>• ตอบคำถามสั้น ๆ เพื่อประเมินความรู้ความเข้าใจของนักศึกษา</li> <li>• รับชมวีดิทัศน์ที่เกี่ยวข้อง</li> <li>• นักศึกษานำเสนอหัวข้อการศึกษา ค้นคว้าด้วยตนเอง</li> </ul> <p><b>สื่อที่ใช้</b></p> <ul style="list-style-type: none"> <li>• MS-PowerPoint</li> <li>• HCU E-learning</li> <li>• E-book (Thai and English)</li> <li>• Video clips</li> <li>• Other medias/References website [Publish on HCU E-learning]</li> <li>• Online conference system: MS-Teams and etc.</li> </ul>		
3 (22/8/65)	<p><b>ปฏิบัติ</b></p> <ul style="list-style-type: none"> <li>• Vulnerability Assessment</li> <li>• MS Windows Operating Security</li> <li>• การนำเสนอหัวข้อการศึกษาค้นคว้าวิจัยเกี่ยวกับความมั่นคงทางไซเบอร์</li> </ul>	<p><b>ปฏิบัติ</b></p> <ul style="list-style-type: none"> <li>• ฝึกปฏิบัติการที่เกี่ยวกับช่องโหว่ของระบบและ Website ตัวอย่างจาก TryHackme.com website</li> <li>• ฝึกปฏิบัติการด้วยซอฟต์แวร์สำเร็จรูป เช่น MS Baseline Security analyzer เป็นต้น</li> <li>• นักศึกษานำเสนอหัวข้อการศึกษาค้นคว้าวิจัยเกี่ยวกับความมั่นคงทางไซเบอร์</li> <li>• ถามตอบ ให้ข้อมูลป้อนกลับ และแลกเปลี่ยนความคิดเห็นระหว่างกัน</li> </ul> <p><b>สื่อที่ใช้</b></p> <ul style="list-style-type: none"> <li>• MS-PowerPoint</li> <li>• HCU e-Learning</li> <li>• Cyber security software/tools</li> <li>• Cyber security website</li> <li>• Online conference system: MS-Teams, and etc.</li> </ul>		<p><b>ปฏิบัติ</b></p> <p>อาจารย์ณัฐพร</p>

		<ul style="list-style-type: none"> <li>Other media upon students</li> </ul>		
4 (1/9/65)	<b>บรรยาย</b> <ul style="list-style-type: none"> <li>Security Policies, Standards, Procedures, and Guidelines</li> </ul>	<b>บรรยาย</b> <ul style="list-style-type: none"> <li>บรรยายประกอบการยกตัวอย่างด้วย MS-PowerPoint, E-books, Video clips, Movies/Game/Cartoon, Course online และเว็บไซต์ที่เกี่ยวข้อง</li> <li>ตอบคำถามสั้น ๆ เพื่อประเมินความรู้ความเข้าใจของนักศึกษา</li> <li>รับชมวีดิทัศน์ที่เกี่ยวข้อง</li> <li>นักศึกษานำเสนอหัวข้อการศึกษา ค้นคว้าด้วยตนเอง</li> </ul> <b>สื่อที่ใช้</b> <ul style="list-style-type: none"> <li>MS-PowerPoint</li> <li>HCU E-learning</li> <li>E-book (Thai and English)</li> <li>Video clips</li> <li>Other medias/References website [Publish on HCU E-learning]</li> <li>Online conference system: MS-Teams and etc.</li> </ul>	(2/2/0)	<b>บรรยาย</b> อาจารย์ณัฐพร
4 (29/9/65)	<b>ปฏิบัติ</b> <ul style="list-style-type: none"> <li>Network security lab from TryHackme.com</li> <li>Begin CyberCIEGE</li> <li>มอบหมายงานการศึกษา ค้นคว้าด้วยตนเองเกี่ยวกับสถานการณ์จำลองด้านความมั่นคงทางไซเบอร์จากโปรแกรม CyberCIEGE และ Tryhackme.com</li> </ul>	<b>ปฏิบัติ</b> <ul style="list-style-type: none"> <li>ฝึกปฏิบัติการด้าน Network security จาก TryHackme.com</li> <li>ฝึกปฏิบัติการเริ่มต้นเรียนรู้การใช้งาน CyberCIEGE</li> <li>นักศึกษาจับกลุ่มและหาหัวข้อการศึกษา ค้นคว้าด้วยตนเองภายใต้คำแนะนำของอาจารย์ผู้สอน</li> </ul> <b>สื่อที่ใช้</b> <ul style="list-style-type: none"> <li>MS-PowerPoint</li> <li>HCU e-Learning</li> <li>Cyber security software/tools</li> <li>Cyber security website</li> <li>Online conference system: MS-</li> </ul>		<b>ปฏิบัติ</b> อาจารย์ณัฐพร นันทจิระพงศ์

		Teams, and etc.		
5 (9/9/65)	<b>บรรยาย</b> <ul style="list-style-type: none"> <li>● Critical Infrastructure attack</li> <li>● Cyber security framework</li> </ul>	<b>บรรยาย</b> <ul style="list-style-type: none"> <li>● บรรยายประกอบการยกตัวอย่างด้วย MS-PowerPoint, E-books, Video clips, Movies/Game/Cartoon, Course online และเว็บไซต์ที่เกี่ยวข้อง</li> <li>● ตอบคำถามสั้น ๆ เพื่อประเมินความรู้ความเข้าใจของนักศึกษา</li> <li>● รับชมวีดิทัศน์ที่เกี่ยวข้อง</li> <li>● นักศึกษานำเสนอหัวข้อการศึกษา ค้นคว้าด้วยตนเอง</li> </ul> <b>สื่อที่ใช้</b> <ul style="list-style-type: none"> <li>● MS-PowerPoint</li> <li>● HCU E-learning</li> <li>● E-book (Thai and English)</li> <li>● Video clips</li> <li>● Other medias/References website [Publish on HCU E-learning]</li> <li>● Online conference system: MS-Teams and etc.</li> </ul>	(2/2/0)	<b>บรรยาย</b> อาจารย์ ดร. ธีรวัฒน์
5 (5/9/65)	<b>ปฏิบัติ</b> <ul style="list-style-type: none"> <li>● Network Intrusion and package detection</li> <li>● CyberCIEGE (Stop worm and Password scenario)</li> </ul>	<b>ปฏิบัติ</b> <ul style="list-style-type: none"> <li>● ฝึกปฏิบัติการด้านการป้องกันการบุกรุกทางคอมพิวเตอร์และระบบเครือข่ายด้วยซอฟต์แวร์สำเร็จรูป</li> <li>● ฝึกปฏิบัติการเรียนรู้การใช้งานโปรแกรม CyberCIEGE (Stop worm and Password scenario)</li> </ul> <b>สื่อที่ใช้</b> <ul style="list-style-type: none"> <li>● MS-PowerPoint</li> <li>● HCU e-Learning</li> <li>● Cyber security software/tools</li> <li>● Cyber security website</li> <li>● Online conference system: MS-Teams, and etc.</li> </ul>		<b>ปฏิบัติ</b> อาจารย์ณัฐพร

6 (15/9/65)	<b>บรรยาย</b> <ul style="list-style-type: none"> <li>Ethics, Laws, and professional issues in Cyber security</li> </ul>	<b>บรรยาย</b> <ul style="list-style-type: none"> <li>บรรยายประกอบการยกตัวอย่างด้วย MS-PowerPoint, E-books, Video clips, Movies/Game/Cartoon, Course online และเว็บไซต์ที่เกี่ยวข้อง</li> <li>ตอบคำถามสั้น ๆ เพื่อประเมินความรู้ความเข้าใจของนักศึกษา</li> <li>รับชมวีดิทัศน์ที่เกี่ยวข้อง</li> </ul> <b>สื่อที่ใช้</b> <ul style="list-style-type: none"> <li>MS-PowerPoint</li> <li>HCU E-learning</li> <li>E-book (Thai and English)</li> <li>Video clips</li> <li>Other medias/References website [Publish on HCU E-learning]</li> <li>Online conference system: MS-Teams and etc.</li> </ul>	(2/2/0)	<b>บรรยาย</b> อาจารย์ ดร. ธีรวัฒน์
6 (12/9/65)	<b>ปฏิบัติ</b> <ul style="list-style-type: none"> <li>View source lab from TryHackme.com</li> <li>นักศึกษานำเสนอหัวข้อ การศึกษาค้นคว้าด้วยตนเอง เกี่ยวกับสถานการณ์จำลอง ด้านความมั่นคงทางไซเบอร์ จากโปรแกรม CyberCIEGE และ Tryhackme.com [Proposal presentation]</li> </ul>	<b>ปฏิบัติ</b> <ul style="list-style-type: none"> <li>ฝึกปฏิบัติการหัวข้อ View source จาก TryHackme.com website</li> <li>นักศึกษานำเสนอหัวข้อและขอบเขตของการศึกษาค้นคว้าด้วยตนเอง</li> <li>ถามตอบ ให้ข้อมูลป้อนกลับ และ แลกเปลี่ยนความคิดเห็นระหว่างกัน</li> </ul> <b>สื่อที่ใช้</b> <ul style="list-style-type: none"> <li>HCU e-Learning</li> <li>Cyber security software/tools</li> <li><a href="https://tryhackme.com/room/walkinganapplication">https://tryhackme.com/room/walkinganapplication</a></li> <li>Online conference system: MS-Teams and etc.</li> <li>Other media upon students</li> </ul>		<b>ปฏิบัติ</b> อาจารย์ณัฐพร
7 (22/9/65)	<b>บรรยาย</b> <ul style="list-style-type: none"> <li>Physical security</li> </ul>	<b>บรรยาย</b> <ul style="list-style-type: none"> <li>บรรยายประกอบการยกตัวอย่างด้วย</li> </ul>	(2/3/0)	<b>บรรยาย</b> อาจารย์ณัฐพร

		<p>MS-PowerPoint, E-books, Video clips, Movies/Game/Cartoon, Course online และเว็บไซต์ที่เกี่ยวข้อง</p> <ul style="list-style-type: none"> <li>• ตอบคำถามสั้น ๆ เพื่อประเมินความรู้ความเข้าใจของนักศึกษา</li> <li>• รับชมวีดิทัศน์ที่เกี่ยวข้อง</li> <li>• นักศึกษานำเสนอหัวข้อการศึกษา ค้นคว้าด้วยตนเอง</li> </ul> <p>สื่อที่ใช้</p> <ul style="list-style-type: none"> <li>• MS-PowerPoint</li> <li>• HCU E-learning</li> <li>• E-book (Thai and English)</li> <li>• Video clips</li> <li>• Other medias/References website [Publish on HCU E-learning]</li> <li>• Online conference system: MS-Teams and etc.</li> </ul>		
7 (19/9/65)	<p><b>ปฏิบัติ</b></p> <ul style="list-style-type: none"> <li>• การนำเสนอผลการศึกษาค้นคว้างานวิจัยที่เกี่ยวข้องกับเทคโนโลยีด้านความมั่นคงทางไซเบอร์</li> </ul>	<p><b>ปฏิบัติ</b></p> <ul style="list-style-type: none"> <li>• นักศึกษานำเสนอผลการศึกษาค้นคว้างานวิจัยที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์</li> <li>• ถามตอบ ให้ข้อมูลป้อนกลับ และแลกเปลี่ยนความคิดเห็นระหว่างกัน</li> <li>• นักศึกษาประเมินผลงานของตนเอง และเพื่อนร่วมชั้นเรียน</li> </ul> <p>สื่อที่ใช้</p> <ul style="list-style-type: none"> <li>• HCU e-Learning</li> <li>• Online conference system: MS-Teams and etc.</li> <li>• Other media upon students</li> </ul>		<p><b>ปฏิบัติ</b></p> <p>อาจารย์ณัฐพร</p>
8 (29/9/65)	<p>การสอบกลางภาค (Midterm examination) ใช้เวลา 3 ชั่วโมง (24/9/65-2/10/65)</p>			
9 (6/10/65)	<p><b>บรรยาย</b></p> <ul style="list-style-type: none"> <li>• Identification, Authentication, and</li> </ul>	<p><b>บรรยาย</b></p> <ul style="list-style-type: none"> <li>• บรรยายประกอบการยกตัวอย่างด้วย MS-PowerPoint, E-books, Video</li> </ul>	(2/3/0)	<p><b>บรรยาย</b></p> <p>อาจารย์ณัฐพร</p>

	<p>Authorization</p> <ul style="list-style-type: none"> <li>● Biometrics security</li> </ul>	<p>clips, Movies/Game/Cartoon, Course online และเว็บไซต์ที่เกี่ยวข้อง</p> <ul style="list-style-type: none"> <li>● ตอบคำถามสั้น ๆ เพื่อประเมินความรู้ความเข้าใจของนักศึกษา</li> <li>● รับชมวีดิทัศน์ที่เกี่ยวข้อง</li> <li>● นักศึกษานำเสนอหัวข้อการศึกษา ค้นคว้าด้วยตนเอง</li> </ul> <p>สื่อที่ใช้</p> <ul style="list-style-type: none"> <li>● MS-PowerPoint</li> <li>● HCU E-learning</li> <li>● E-book (Thai and English)</li> <li>● Video clips</li> <li>● Other medias/References website [Publish on HCU E-learning]</li> <li>● Online conference system: MS-Teams and etc.</li> </ul>		
9 (3/10/65)	<p>ปฏิบัติ</p> <ul style="list-style-type: none"> <li>● Group workshop about Cyber security law and Personal Data Privacy Act [PDPA]</li> <li>● Password guessing lab</li> <li>● มอบหมายโครงการด้าน Cyber security</li> </ul>	<p>ปฏิบัติ</p> <ul style="list-style-type: none"> <li>● ฝึกปฏิบัติการจาก Case study ที่กำหนดให้ โดยแบ่งเป็นกลุ่ม</li> <li>● ฝึกปฏิบัติการด้านการเดารหัสผ่านด้วยซอฟต์แวร์สำเร็จรูป</li> <li>● นักศึกษาจับกลุ่มและหาหัวข้อในการทำโครงการด้าน Cyber security ภายใต้คำแนะนำของอาจารย์ผู้สอน</li> </ul> <p>สื่อที่ใช้</p> <ul style="list-style-type: none"> <li>● HCU e-Learning</li> <li>● Cyber security software/tools</li> <li>● Online conference system: MS-Teams and etc.</li> <li>● Other media upon students</li> </ul>		<p>ปฏิบัติ</p> <p>อาจารย์ณัฐพร</p>
10 (13/10/65) วันคล้ายวัน สวรรคต พระบาทสมเด็จพระ	<p>บรรยาย</p> <ul style="list-style-type: none"> <li>● Basic concept of cryptography</li> </ul>	<p>บรรยาย</p> <ul style="list-style-type: none"> <li>● บรรยายประกอบการยกตัวอย่างด้วย MS-PowerPoint, E-books, Video clips, Course online และ</li> </ul>	(2/3/0)	<p>บรรยาย</p> <p>อาจารย์ ดร. กรินทร์</p>

พระบรมชนกาทิเบศรา (Online)		Website ที่เกี่ยวข้อง <ul style="list-style-type: none"> <li>• ตอบคำถามสั้น ๆ เพื่อประเมินความรู้ความเข้าใจของนักศึกษา</li> <li>• รับชมวีดิทัศน์ที่เกี่ยวข้อง</li> </ul> <b>สื่อที่ใช้</b> <ul style="list-style-type: none"> <li>• MS-PowerPoint</li> <li>• HCU e-Learning</li> <li>• e-book (Thai and English)</li> <li>• Video clips</li> <li>• Other medias/References website [Publish on HCU e-Learning]</li> <li>• Online conference system: MS-Teams and etc.</li> </ul>		
10 (10/10/65)	<b>ปฏิบัติ</b> <ul style="list-style-type: none"> <li>• การนำเสนอผลการศึกษาค้นคว้าด้วยตนเองเกี่ยวกับสถานการณ์จำลองด้านความมั่นคงทางไซเบอร์ [Complete presentation]</li> </ul>	<b>ปฏิบัติ</b> <ul style="list-style-type: none"> <li>• นักศึกษานำเสนอผลการศึกษาค้นคว้าด้วยตนเองเกี่ยวกับสถานการณ์จำลองด้านความมั่นคงทางไซเบอร์</li> <li>• ถามตอบ ให้ข้อมูลป้อนกลับ และแลกเปลี่ยนความคิดเห็นระหว่างกัน</li> <li>• นักศึกษาประเมินผลงานของตนเองและเพื่อนร่วมชั้นเรียน</li> </ul> <b>สื่อที่ใช้</b> <ul style="list-style-type: none"> <li>• MS-PowerPoint</li> <li>• HCU e-Learning</li> <li>• Cyber security software/tools</li> <li>• Cyber security website</li> <li>• Online conference system: MS-Teams, and etc.</li> </ul>		<b>ปฏิบัติ</b> อาจารย์ณัฐพร
11 (20/10/65)	<b>บรรยาย</b> <ul style="list-style-type: none"> <li>• Basic concept of cryptography (cont.)</li> </ul>	<b>บรรยาย</b> <ul style="list-style-type: none"> <li>• บรรยายประกอบการยกตัวอย่างด้วย MS-PowerPoint, E-books, Video clips, Course online และ Website ที่เกี่ยวข้อง</li> <li>• ตอบคำถามสั้น ๆ เพื่อประเมินความรู้</li> </ul>	(2/3/0)	<b>บรรยาย</b> อาจารย์ ดร. กรินทร์



		<p>ความเข้าใจของนักศึกษา</p> <ul style="list-style-type: none"> <li>● รับชมวีดิทัศน์ที่เกี่ยวข้อง</li> </ul> <p><b>สื่อที่ใช้</b></p> <ul style="list-style-type: none"> <li>● MS-PowerPoint</li> <li>● HCU e-Learning</li> <li>● e-book (Thai and English)</li> <li>● Video clips</li> <li>● Other medias/References website [Publish on HCU e-Learning]</li> <li>● Online conference system: MS-Teams and etc.</li> </ul>		
11 (17/10/65)	<p><b>ปฏิบัติ</b></p> <ul style="list-style-type: none"> <li>● Digital Certificates using Windows</li> <li>● Message/Email Encryption and Decryption</li> <li>● Cryptography tool introduction</li> <li>● การนำเสนอโครงร่างหัวข้อโครงการด้าน Cyber security</li> </ul>	<p><b>ปฏิบัติ</b></p> <ul style="list-style-type: none"> <li>● ฝึกปฏิบัติการเพื่อตรวจสอบใบรับรองอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต</li> <li>● ฝึกปฏิบัติการด้านวิทยาการเข้ารหัสลับ ทั้งการเข้าและถอดรหัสข้อความ/อีเมลด้วยซอฟต์แวร์สำเร็จรูป</li> <li>● <b>นักศึกษานำเสนอหัวข้อและขอบเขตของโครงการด้าน Cyber security</b></li> <li>● ถามตอบ ให้ข้อมูลป้อนกลับ และแลกเปลี่ยนความคิดเห็นระหว่างกัน</li> </ul> <p><b>สื่อที่ใช้</b></p> <ul style="list-style-type: none"> <li>● MS-PowerPoint</li> <li>● HCU e-Learning</li> <li>● Cyber security software/tools</li> <li>● Cyber security website</li> <li>● Cryptool2 application</li> <li>● PGP Key generator</li> <li>● Online conference system: MS-Teams, and etc.</li> </ul>		<p><b>ปฏิบัติ</b></p> <p>อาจารย์ณัฐพร</p>
12 (27/10/65)	<p><b>บรรยาย</b></p> <ul style="list-style-type: none"> <li>● Web attack and security</li> </ul>	<p><b>บรรยาย</b></p> <ul style="list-style-type: none"> <li>● บรรยายประกอบการยกตัวอย่างด้วย MS-PowerPoint, E-books, Video clips, Course online และ</li> </ul>	(2/2/0)	<p><b>บรรยาย</b></p> <p>อาจารย์ ดร. กรินทร์</p>

		Website ที่เกี่ยวข้อง <ul style="list-style-type: none"> <li>• ตอบคำถามสั้น ๆ เพื่อประเมินความรู้ความเข้าใจของนักศึกษา</li> <li>• รับชมวีดิทัศน์ที่เกี่ยวข้อง</li> </ul> <b>สื่อที่ใช้</b> <ul style="list-style-type: none"> <li>• MS-PowerPoint</li> <li>• HCU e-Learning</li> <li>• e-book (Thai and English)</li> <li>• Video clips</li> <li>• Other medias/References website [Publish on HCU e-Learning]</li> <li>• Online conference system: MS-Teams and etc.</li> </ul>		
12 (24/10/65)	<b>ปฏิบัติ</b> <ul style="list-style-type: none"> <li>• Cryptography lab</li> <li>• Encryption and Blockchain technology</li> </ul>	<b>ปฏิบัติ</b> <ul style="list-style-type: none"> <li>• ฝึกปฏิบัติการด้านวิทยาการเข้ารหัสลับจากซอฟต์แวร์สำเร็จรูป (ต่อ)</li> <li>• ฝึกปฏิบัติการทดลองและศึกษาการเข้ารหัสข้อมูลของเทคโนโลยี Blockchain</li> </ul> <b>สื่อที่ใช้</b> <ul style="list-style-type: none"> <li>• MS-PowerPoint</li> <li>• HCU e-Learning</li> <li>• Cyber security software/tools</li> <li>• Cyber security website</li> <li>• Cryptool2 application</li> <li>• Online conference system: MS-Teams, and etc.</li> </ul>		<b>ปฏิบัติ</b> อาจารย์ณัฐพร
13 (3/11/65)	<b>บรรยาย</b> <ul style="list-style-type: none"> <li>• Web attack and security (cont.)</li> </ul>	<b>บรรยาย</b> <ul style="list-style-type: none"> <li>• บรรยายประกอบการยกตัวอย่างด้วย MS-PowerPoint, E-books, Video clips, Course online และ Website ที่เกี่ยวข้อง</li> <li>• ตอบคำถามสั้น ๆ เพื่อประเมินความรู้ความเข้าใจของนักศึกษา</li> <li>• รับชมวีดิทัศน์ที่เกี่ยวข้อง</li> </ul>	(2/2/0)	<b>บรรยาย</b> อาจารย์ ดร.กรินทร์

		<b>สื่อที่ใช้</b> <ul style="list-style-type: none"> <li>● MS-PowerPoint</li> <li>● HCU e-Learning</li> <li>● e-book (Thai and English)</li> <li>● Video clips</li> <li>● Other medias/References website [Publish on HCU e-Learning]</li> <li>● Online conference system: MS-Teams and etc.</li> </ul>		
13 (31/10/65)	<b>ปฏิบัติ</b> <ul style="list-style-type: none"> <li>● Web authentication and password encryption</li> <li>● Burb Suite lab</li> <li>● Cross-site scripting (XSS) lab</li> </ul>	<b>ปฏิบัติ</b> <ul style="list-style-type: none"> <li>● ฝึกปฏิบัติการสร้างหน้าเว็บเพจ Login ที่มีการเข้ารหัส password ด้วยภาษาโปรแกรม</li> <li>● ฝึกปฏิบัติการหัวข้อ Cross-site scripting (XSS)</li> <li>● ฝึกปฏิบัติการหัวข้อ Burb Suite</li> </ul> <b>สื่อที่ใช้</b> <ul style="list-style-type: none"> <li>● MS-PowerPoint</li> <li>● HCU e-Learning</li> <li>● Cyber security software/tools</li> <li>● Cyber security website</li> <li>● Programming language (HTML, PHP)</li> <li>● Text editor (Visual studio code)</li> <li>● Online conference system: MS-Teams, and etc.</li> <li>● <a href="https://tryhackme.com">https://tryhackme.com</a></li> </ul>		<b>ปฏิบัติ</b> อาจารย์ณัฐพร
14 (10/11/65)	<b>บรรยาย</b> <ul style="list-style-type: none"> <li>● Digital forensic introduction</li> </ul>	<b>บรรยาย</b> <ul style="list-style-type: none"> <li>● บรรยายประกอบการยกตัวอย่างด้วย MS-PowerPoint, E-books, Video clips, Course online และ Website ที่เกี่ยวข้อง</li> <li>● ตอบคำถามสั้น ๆ เพื่อประเมินความรู้ความเข้าใจของนักศึกษา</li> <li>● รับชมวีดิทัศน์ที่เกี่ยวข้อง</li> </ul>	(2/2/0)	<b>บรรยาย</b> รองศาสตราจารย์ ดร. สุรทศ

		<b>สื่อที่ใช้</b> <ul style="list-style-type: none"> <li>● MS-PowerPoint</li> <li>● HCU e-Learning</li> <li>● e-book (Thai and English)</li> <li>● Video clips</li> <li>● Other medias/References website [Publish on HCU e-Learning]</li> <li>● Online conference system: MS-Teams and etc.</li> </ul>		
14 (7/11/65)	<b>ปฏิบัติ</b> <ul style="list-style-type: none"> <li>● Digital forensic: basic workshop</li> <li>● การนำเสนอความคืบหน้าของโครงการ Cyber security</li> </ul>	<b>ปฏิบัติ</b> <ul style="list-style-type: none"> <li>● ฝึกปฏิบัติการด้วยซอฟต์แวร์สำเร็จรูปที่เกี่ยวข้องกับ Digital forensic เบื้องต้น</li> <li>● นักศึกษานำเสนอความก้าวหน้าของโครงการ Cyber security</li> <li>● ถามตอบ ให้ข้อมูลป้อนกลับ และ แลกเปลี่ยนความคิดเห็นระหว่างกัน</li> </ul> <b>สื่อที่ใช้</b> <ul style="list-style-type: none"> <li>● MS-PowerPoint</li> <li>● HCU e-Learning</li> <li>● Cyber security software/tools</li> <li>● Cyber security website</li> <li>● HashMyFile tools</li> <li>● Online conference system: MS-Teams, and etc.</li> </ul>		<b>ปฏิบัติ</b> อาจารย์ณัฐพร
15 (17/11/65)	<b>บรรยาย</b> <ul style="list-style-type: none"> <li>● Basic of ethical hacking</li> </ul>	<b>บรรยาย</b> <ul style="list-style-type: none"> <li>● บรรยายประกอบการยกตัวอย่างด้วย MS-PowerPoint, E-books, Video clips, Course online และ Website ที่เกี่ยวข้อง</li> <li>● ตอบคำถามสั้น ๆ เพื่อประเมินความรู้ความเข้าใจของนักศึกษา</li> <li>● รับชมวีดิทัศน์ที่เกี่ยวข้อง</li> </ul> <b>สื่อที่ใช้</b> <ul style="list-style-type: none"> <li>● MS-PowerPoint</li> </ul>	(2/2/0)	<b>บรรยาย</b> อาจารย์ ดร. กรินทร์

		<ul style="list-style-type: none"> <li>● HCU e-Learning</li> <li>● e-book (Thai and English)</li> <li>● Video clips</li> <li>● Other medias/References website [Publish on HCU e-Learning]</li> <li>● Online conference system: MS-Teams and etc.</li> </ul>		
15 (14/11/65)	<b>ปฏิบัติ</b> <ul style="list-style-type: none"> <li>● SQL injection</li> <li>● Command injection</li> </ul>	<b>ปฏิบัติ</b> <ul style="list-style-type: none"> <li>● ฝึกปฏิบัติการด้านการรักษาความปลอดภัยข้อมูลและสารสนเทศขององค์กร (ตัวอย่างเช่น โปรแกรมประยุกต์บนเว็บจำลองของธนาคารจำลองของบริษัท IBM เป็นต้น)</li> <li>● ฝึกปฏิบัติการหัวข้อ SQLInjection</li> <li>● ฝึกปฏิบัติการหัวข้อ Command injection</li> </ul> <b>สื่อที่ใช้</b> <ul style="list-style-type: none"> <li>● MS-PowerPoint</li> <li>● HCU e-Learning</li> <li>● Cyber security software/tools</li> <li>● Cyber security website</li> <li>● Online conference system: MS-Teams, and etc.</li> <li>● <a href="http://demo.testfire.net">http://demo.testfire.net</a></li> <li>● <a href="https://tryhackme.com">https://tryhackme.com</a></li> </ul>		<b>ปฏิบัติ</b> อาจารย์ณัฐพร
16 (24/11/65)	<b>บรรยาย</b> <ul style="list-style-type: none"> <li>● Enterprise security</li> <li>● Security organization</li> </ul>	<b>บรรยาย</b> <ul style="list-style-type: none"> <li>● บรรยายประกอบการยกตัวอย่างด้วย MS-PowerPoint, E-books, Video clips, Course online และ Website ที่เกี่ยวข้อง</li> <li>● ตอบคำถามสั้น ๆ เพื่อประเมินความรู้ความเข้าใจของนักศึกษา</li> <li>● รับชมวีดิทัศน์ที่เกี่ยวข้อง</li> </ul> <b>สื่อที่ใช้</b> <ul style="list-style-type: none"> <li>● MS-PowerPoint</li> </ul>	(2/3/0)	<b>บรรยาย</b> ดร.ธีรวัฒน์

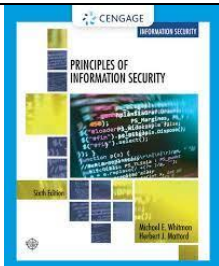
		<ul style="list-style-type: none"> <li>● HCU e-Learning</li> <li>● e-book (Thai and English)</li> <li>● Video clips</li> <li>● Other medias/References website [Publish on HCU e-Learning]</li> <li>● Online conference system: MS-Teams and etc.</li> </ul>		
16 (21/11/65)	<b>ปฏิบัติ</b> <ul style="list-style-type: none"> <li>● การนำเสนอโครงงานด้าน Cyber security</li> </ul>	<b>ปฏิบัติ</b> <ul style="list-style-type: none"> <li>● นักศึกษานำเสนอโครงงานด้าน Cyber security</li> <li>● ถามตอบ ให้ข้อมูลป้อนกลับ และ แลกเปลี่ยนความคิดเห็นระหว่างกัน</li> <li>● นักศึกษาประเมินผลงานของตนเอง และเพื่อนร่วมชั้นเรียน</li> </ul> <b>สื่อที่ใช้</b> <ul style="list-style-type: none"> <li>● MS-PowerPoint</li> <li>● HCU e-Learning</li> <li>● Cyber security software/tools</li> <li>● Cyber security website</li> <li>● Online conference system: MS-Teams, and etc.</li> <li>● Other media/tools upon students</li> </ul>		<b>ปฏิบัติ</b> อาจารย์ณัฐพร
17 (6/12/65)	การสอบปลายภาค (Final examination) ใช้เวลา3 ชั่วโมง(28/11/65-13/12/65)			
	รวม		(30/45/0)	

## 2. แผนการประเมินผลการเรียนรู้

ผลการเรียนรู้ที่เกี่ยวข้อง	กิจกรรมการประเมิน (เช่น การเขียนรายงาน โครงการงาน การสอบย่อย การสอบกลางภาค การสอบปลายภาค)	สัปดาห์ที่ประเมิน	สัดส่วนของการประเมินผล
1.3, 2.1, 4.4	การเข้าชั้นเรียน และการมีส่วนร่วมในชั้นเรียน	ตลอดภาคการศึกษา	4%
2.2, 2.7, 3.4, 4.4, 5.1	การส่งงานมอบหมายในชั้นเรียนภาคปฏิบัติ	ตลอดภาคการศึกษา	12%
2.1, 2.3, 2.4, 4.4, 5.3	การนำเสนอผลการศึกษาค้นคว้าด้วยตนเองเกี่ยวกับบทความวิจัยเกี่ยวกับความมั่นคงทางไซเบอร์	สัปดาห์ที่ 3 และ 7	10%
1.3, 2.1, 2.2, 2.3, 2.4, 3.4, 4.4, 5.3	การนำเสนอผลการศึกษาศานาการณ์จำลองด้านความมั่นคงทางไซเบอร์ (งานคู่)	สัปดาห์ที่ 6 และ 10	14%
1.3, 2.1, 2.2, 2.3, 2.4, 2.7, 3.4, 4.4, 5.1, 5.3	การนำเสนอโครงการด้านความมั่นคงทางไซเบอร์ (งานกลุ่ม)	สัปดาห์ที่ 11, 14 และ 16	15%
2.1, 2.2, 3.4	การทดสอบกลางภาคเรียน	สัปดาห์ที่ 8	20%
2.1, 2.2, 3.4	การสอบปลายภาคเรียน	สัปดาห์ที่ 17	25%

## หมวดที่ 6 ทรัพยากรประกอบการเรียนการสอน

## 1. ตำรา หนังสืออิเล็กทรอนิกส์ และเอกสารหลักที่ใช้ในการเรียนการสอน

รายการ	ภาพประกอบ
<ul style="list-style-type: none"> <li>Michael E. Whitman and Herbert J. Mattord, <b>Principle of Information Technology</b>, 6<sup>th</sup> Edition, Cengage learning, 2018.</li> </ul>	

รายการ	ภาพประกอบ
<ul style="list-style-type: none"> <li>William Stallings and Lawrie Brown, <b>Computer Security: Principles and Practice</b>, 4<sup>th</sup> Edition, Pearson, 2017.</li> </ul>	
<ul style="list-style-type: none"> <li>Shon Harris and Fernando Maymi, <b>CISSP All-in-One Exam Guide</b>, 8<sup>th</sup> Edition, McGraw-Hill, 2018</li> </ul>	
<ul style="list-style-type: none"> <li>Joseph Steinberg, <b>Cyber security for Dummies</b>, 2<sup>nd</sup> Edition, John Wiley &amp; Sons, 2016.</li> </ul>	

## 2. เอกสารอ่านประกอบ/สื่ออิเล็กทรอนิกส์/แหล่งอ้างอิงอื่นๆ ที่นักศึกษาควรอ่านเพิ่มเติม

### 2.1 หนังสือ เอกสาร และสื่ออิเล็กทรอนิกส์

- Michael E. Whitman and Herbert J. Mattord, "Hands-on Information Security lab manual", Third edition (International edition), Printed in the United States of America, Course Technology, Cengage Learning, 2011.
- สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ, "วิทยาการรหัสลับในระบบเทคโนโลยีสารสนเทศและโทรคมนาคม (Cryptography in Information Technology and Communication Systems)", บริษัท รัฟพิมพ์ จำกัด, พิมพ์ครั้งที่ 1 พฤษภาคม 2558.

### 2.2 เว็บไซต์

- [TryHackMe | Cyber Security Training](#)
- [Cyber Security Tutorial \(w3schools.com\)](#)
- [Cyber Security Tutorial - javatpoint](#)
- [Cyber Security Tutorial: A Step-by-Step Tutorial \[Updated 2021\] \(simplilearn.com\)](#)



- [Computer Security Tutorial \(tutorialspoint.com\)](http://www.tutorialspoint.com)
- [Cyber Security Tutorials for Beginners | Learn eTutorials](http://www.eTutorials.com)
- <http://www.thaicert.org/>
- <http://www.sans.org/security-resources/glossary-of-terms/>

[คำศัพท์ที่เกี่ยวข้องกับการรักษาความปลอดภัยทางเทคโนโลยีคอมพิวเตอร์ และสารสนเทศ]

### 3. เอกสารและข้อมูลแนะนำ

3.1 หนังสือ เอกสาร สื่อสิ่งพิมพ์ และเว็บไซต์นอกเหนือจากชั้นเรียน ที่มีเนื้อหาเกี่ยวข้องกับรายวิชา ที่อยู่ในศูนย์บรรณสารสนเทศ

3.2 เอกสารประกอบการสอนที่อาจารย์ผู้สอนจัดทำและเผยแพร่ไว้ใน HCU E-learning

## หมวดที่ 7 การประเมินรายวิชาและกระบวนการปรับปรุง

### 1. กลยุทธ์การประเมินประสิทธิผลของรายวิชาโดยนักศึกษา

- การประเมินผู้สอนและรายวิชาออนไลน์ของสำนักพัฒนาวิชาการเมื่อสิ้นภาคการศึกษา
- การสอบถามและพูดคุยกับนักศึกษา
- การแสดงความคิดเห็นของนักศึกษาผ่านแบบทวนสอบผลสัมฤทธิ์ทางการเรียนรู้ของนักศึกษาผ่าน Google Form

### 2. กลยุทธ์การประเมินการสอน

- การสังเกตการณ์จากผู้สอน
- การวัดผลสัมฤทธิ์ทางการศึกษา
- การสำรวจความคิดเห็นและทัศนคติของนักศึกษา
- การทวนสอบผลประเมินการเรียนรู้

### 3. วิธีการปรับปรุงการสอน

ระหว่างกระบวนการสอนรายวิชา มีการทวนสอบผลสัมฤทธิ์ในรายหัวข้อ ตามที่คาดหวังจากการเรียนรู้ในรายวิชา ได้จากการสอบถามนักศึกษา หรือการสุ่มตรวจผลงานของนักศึกษา รวมถึงพิจารณาจากผลการทดสอบ และหลังการออกผลการเรียนรายวิชา มีการทวนสอบผลสัมฤทธิ์โดยรวมในรายวิชาดังต่อไปนี้

- การประชุมคณะกรรมการบริหารหลักสูตรฯ เพื่อพัฒนาการจัดการเรียนการสอน ภายหลังจากได้รับทราบผลประเมินการสอนออนไลน์ของมหาวิทยาลัย
- การประชุมปรึกษาหารือเกี่ยวกับการเรียนการสอนในการประชุมคณะกรรมการบริหารหลักสูตรฯ ภายหลังจากได้รับทราบข้อเสนอแนะจากการตรวจประเมินการประกันคุณภาพการศึกษา

**4. การทวนสอบมาตรฐานผลสัมฤทธิ์ของนักศึกษาในรายวิชา**

- การประชุมพิจารณาข้อสอบ และผลสอบโดยคณะกรรมการบริหารหลักสูตรฯ
- การประชุมพิจารณาข้อสอบ และผลสอบโดยคณะกรรมการวิชาการคณะฯ
- การจัดทำแบบทวนสอบ 01 และ 02 ตามข้อกำหนดของสำนักพัฒนาวิชาการ

**5. การดำเนินการทบทวนและการวางแผนปรับปรุงประสิทธิผลของรายวิชา**

- หลังจากสิ้นภาคการศึกษา ผู้สอนจะทำเข้าสู่ระบบประเมินผลการสอนออนไลน์ที่ได้จากการประมวลผลการตอบแบบประเมินออนไลน์ของนักศึกษาที่ลงทะเบียนเรียนในภาคการศึกษานั้น เพื่อดูผลและอ่านข้อแนะนำของนักศึกษาทุก ๆ คน และนำไปใช้ประกอบการปรับปรุงในภาค/ปี การศึกษาถัดที่เปิดสอน
- ปรับปรุงรายวิชาและหลักสูตรตามข้อกำหนดของกรอบมาตรฐานคุณวุฒิระดับปริญญาตรี สาขา คอมพิวเตอร์ พ.ศ.2552 และเกณฑ์มาตรฐานหลักสูตรระดับปริญญาตรี พ.ศ.2558