รายละเอียดของรายวิชา

คณะวิทยาศาสตร์และเทคโนโลยี **สาขาวิชา** วิทยาการคำนวณและเทคโนโลยีดิจิทัล

ภาคการศึกษาที่ 1 **ปีการศึกษา** 2565

มหาวิทยาลัยหัวเฉียวเฉลิมพระเกียรติ

หมวดที่ 1 ข้อมูลทั่วไป

1. **รหัสและชื่อรายวิชา** AI3443 ความมั่นคงทางไซเบอร์ (Cyber Security)
2. **จำนวนหน่วยกิต** 3
3. **หลักสูตร และประเภทรายวิชา** หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาปัญญาประดิษฐ์ หลักสูตรปรับปรุง พ.ศ.2563 วิชาเอกบังคับ
4. **ภาคการศึกษา / ชั้นปีที่เรียน** ภาคการศึกษาที่ 1 / ชั้นปีที่ 3
5. **รายวิชาที่ต้องเรียนมาก่อน (Pre-requisite)** AI 2443
6. **รายวิชาที่ต้องเรียนพร้อมกัน (Co-requisites)** ไม่มี
7. **ชื่ออาจารย์ผู้รับผิดชอบรายวิชา** อาจารย์ณัฐพร นันทจิระพงศ์
   ชื่ออาจารย์ผู้รับผิดชอบรายวิชาร่วม ไม่มี
8. **สถานที่เรียน**

   Onsite กลุ่ม 01 วันพฤหัสบดี ภาคบรรยาย เวลา 10.30-12.30 น. ห้อง 2-422 (เรียนร่วมกับรายวิชา CS3443)

   วันพฤหัสบดี ภาคปฏิบัติ เวลา 13.30-15.30 น. ห้อง 2-427

   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 มีความสามารถในการหลักการพื้นฐานและความสำคัญของการรักษาความมั่นคงทางกายภาพและทางขีวมาตร วิทยาการรหัสลับและนิติวิทยาศาสตร์ดิจิทัลเบื้องต้น

1.3 มีทักษะปฏิบัติในการใช้งานคำสั่ง ซอฟต์แวร์และเครื่องมือที่ใช้ในการรักษาความมั่นคงทางไซเบอร์ คอมพิวเตอร์และเทคโนโลยีสารสนเทศ

1.4 มีความสามารถในการศึกษาค้นคว้าด้วยตนเองเกี่ยวกับเทคโนโลยีด้านความมั่นคงทางไซเบอร์ใหม่ ๆ รวมถึงการประยุกต์ใช้ทฤษฎีและทักษะปฏิบัติที่ได้เรียนรู้ในรายวิชาในการนำเสนอแนวคิดและแนวปฏิบัติสำหรับการออกแบบนโยบายรวมถึงการเลือกใช้เครื่องมือให้เหมาะสมกับโครงงานด้านความมั่นคงทางไซเบอร์

ผลลัพธ์การเรียนรู้ระดับรายวิชา (Course-level Learning Outcomes: CLOs)

เมื่อสิ้นสุดการเรียนการสอนแล้ว นักศึกษาที่สำเร็จการศึกษาในรายวิชานี้ สามารถ

1. อธิบายความสำคัญของความมั่นคงทางไซเบอร์
2. จำแนกแยกแยะประเภท และชนิดของอาชญากรรมทางคอมพิวเตอร์และทางไซเบอร์
3. เปรียบเทียบความแตกต่างของผู้กระทำความผิดทางคอมพิวเตอร์และทางไซเบอร์
4. วิเคราะห์ผลกระทบของภัยคุกคามและการโจมตีทางไซเบอร์
5. นำเสนอแนวทางการสร้างความมั่นคงทางไซเบอร์ ทั้งการกำหนดนโยบาย การบังคับใช้กฎหมาย รวมถึงการประยุกต์ใช้ฮาร์ดแวร์และซอฟต์แวร์ที่เกี่ยวข้อง
6. อธิบายหลักการและประโยชน์ของวิทยาการรหัสลับและนิติวิทยาศาสตร์ดิจิทัล

2 วัตถุประสงค์ในการพัฒนา/ปรับปรุงรายวิชา

2.1 การปรับปรุงรายวิชาโดยอาจารย์ผู้สอน

- เพื่อให้การเรียนการสอนของรายวิชานี้เป็นไปตามกรอบมาตรฐานคุณวุฒิแห่งชาติ พ.ศ.2552 ที่อยู่ภายใต้ข้อกำหนดของ สำนักงานการอุดมศึกษาแห่งชาติ (สกอ.)
- จัดกิจกรรมการเรียนการสอนและการมอบหมายงานให้เหมาะสมกับสภาพผู้เรียน เน้นการเรียนรู้จากการปฏิบัติจริง **(Active learning) ทักษะของบัณฑิตไทยในศตวรรษที่ 21** แนวโน้มการเปลี่ยนแปลงของเทคโนโลยี พร้อมทั้งส่งเสริมการพัฒนา**ทักษะด้านการร่วมมือร่วมใจ (Collaboration) การคิดสร้างสรรค์ (Creativity) การติดต่อสื่อสาร (Communication) และการคิดวิเคราะห์ (Critical Thinking) ตามหลักการของ 4C** ให้กับผู้เรียน
- ปรับรูปแบบการเรียนการสอนให้เป็น**<u>การผสมผสานระหว่างการเรียนในชั้นเรียนและการเรียนออนไลน์ (Hybrid learning) ร่วมกับการจัดการเรียนการสอนภาคทฤษฎีแบบห้องเรียนกลับด้าน (Flipped classroom) ในบางหัวข้อ</u> และการเรียนรู้ภาคปฏิบัติโดยใช้ทักษะเป็นฐาน (Skill based learning)** เพื่อให้สอดคล้องกับสถานการณ์หลังเกิดการแพร่ระบาดของโรค Covid-19 และการพัฒนาทักษะปฏิบัติของนักศึกษาในยุคของ**การแปลี่ยนแปลงเทคโนโลยีดิจิทัล (Digital Transformation)**

- จัดหาสื่อที่มีความหลากหลายและทันสมัย ได้แก่ **E-books, Video clip, Infographics Course online และสื่ออื่น ๆ** ที่น่าสนใจทั้งที่**เป็นภาษาไทยและภาษาอังกฤษ**จากเว็บไซต์และสื่อสังคมออนไลน์ต่าง ๆ มาประกอบการเรียนการสอนในหัวข้อที่เกี่ยวข้องกับเนื้อหารายวิชา **เพื่อให้นักศึกษาได้ความรู้ที่ทันสมัยและได้ฝึกทักษะการอ่านและการฟังภาษาอังกฤษ รวมถึงการนำไปทบทวนด้วยตนเองนอกเวลาเรียน**
- จัดหา **Software** หรือเครื่องมือที่ไม่ละเมิดลิขสิทธิ์มาประกอบการจัดการเรียนการสอนภาคปฏิบัติการ เพื่อให้นักศึกษาได้เรียนรู้และฝึกทักษะการรักษาความมั่นคงปลอดภัยในการใช้งานคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต ที่สอดคล้องกับเนื้อหารายวิชา

2.2 การปรับปรุงตามข้อวิพากษ์ของนักศึกษา

ไม่มี เนื่องจากเป็นการสอนครั้งแรกของหลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาปัญญาประดิษฐ์ (หลักสูตรปรับปรุง พ.ศ.2563)

หมวดที่ 3 ส่วนประกอบของรายวิชา

1. คำอธิบายรายวิชา

ประวัติความเป็นมาของความมั่นคงทางไซเบอร์ อาชญากรรมทางคอมพิวเตอร์และทางไซเบอร์ ภัยคุกคามต่อความมั่นคงทางไซเบอร์ ประเภทของผู้กระทำความผิดทางคอมพิวเตอร์และทางไซเบอร์ ช่องโหว่และความเสี่ยงทางไซเบอร์ การโจมตีและความมั่นคงของเว็บ นโยบายความมั่นคงทางไซเบอร์ หลักการขั้นพื้นฐานของวิทยาการรหัสลับและนิติวิทยาศาสตร์ดิจิทัล กฎหมายที่เกี่ยวข้อง การฝึกปฏิบัติการด้วยซอฟต์แวร์สำเร็จรูปและเครื่องมือที่เกี่ยวข้อง

History of Cyber security, Computer crime and Cybercrime, Cyber security threat, Computer and Cyber criminals, Cyber risk and vulnerability, Web attack and security, Basic concept of cryptography and digital forensic, Cyber security policy and related laws, and practices with software package and related 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 อิสสริยะกุล	**วันพฤหัสบดี เวลา 9.30-10.30 น. ในวันที่มาสอน** อาจารย์พิเศษจากบริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
อาจารย์ ดร. กรินทร์ สุมังคะโยธิน	**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 และประกาศไว้ในตารางสอนที่หน้าบูธห้องพักอาจารย์

- 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.ทักษะการวิเคราะห์เชิงตัวเลขการสื่อสารและการใช้เทคโนโลยีสารสนเทศ					
			1	2	3	4	5	6	1	2	3	4	5	6	7	8	1	2	3	4	1	2	3	4	5	1	2	3	4	5	6
AI3443	ความมั่นคงทางไซเบอร์	3(2/2-1/2-0)				●			●		○	●		●					●	○		●				●			●		

1. คุณธรรม จริยธรรม

(1) คุณธรรม จริยธรรมที่ต้องพัฒนา

1.3 เคารพกฎระเบียบและข้อบังคับต่าง ๆ ขององค์กรและสังคม

(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 รวมทั้งได้เน้นย้ำให้นักศึกษาตระหนักถึงความสำคัญของการเข้าสู่ประชาคมอาเซียน และการยึดหลักปรัชญาของเศรษฐกิจพอเพียงในการเรียนและการใช้ชีวิตประจำวัน
- ในการมอบหมายงานทุกครั้ง ผู้สอนได้ย้ำให้นักศึกษาพิจารณาวางแผนจัดลำดับความสำคัญของงานทั้งงานเดี่ยว งานคู่ และงานกลุ่ม ความรับผิดชอบในการทำงานของตนเองและการทำงานกลุ่ม การมีภาวะผู้นำผู้ตามในการเรียนและทำงานร่วมกับเพื่อน ๆ ทั้งในและนอกเวลาเรียน

(3) วิธีการประเมินผล

- การเข้าชั้นเรียนและการมีส่วนร่วมในชั้นเรียน
- การปฏิบัติตามระเบียบการเข้าใช้ห้องปฏิบัติการคอมพิวเตอร์
- การปฏิบัติตามระเบียบการเข้าห้องสอบทั้งกลางภาคและปลายภาค

2. ความรู้

(1) ความรู้ที่ต้องได้รับ

2.1 มีความรู้ความเข้าใจเกี่ยวกับหลักการและทฤษฎีที่สำคัญในเนื้อหาสาขาวิชาที่ศึกษา

2.3 วิเคราะห์ ออกแบบ ติดตั้ง ปรับปรุงและ/หรือประเมินระบบองค์ประกอบต่าง ๆ ของระบบปัญญาประดิษฐ์ให้ตรงตามข้อกำหนด

2.4 สามารถติดตามความก้าวหน้าทางวิชาการและวิวัฒนาการคอมพิวเตอร์ รวมทั้งการนำไปประยุกต์

2.6 มีความรู้ในแนวกว้างของหลักสูตรเพื่อให้เล็งเห็นการเปลี่ยนแปลง และเข้าใจผลกระทบของเทคโนโลยีใหม่ ๆ

(2) วิธีการสอน

- ในคาบบรรยาย ผู้สอนเลือกใช้วิธีการบรรยายประกอบไฟล์นำเสนองาน (Microsoft PowerPoint) ร่วมกับสื่อการเรียนการสอนที่มีความหลากหลายและทันสมัย เช่น หนังสืออิเล็กทรอนิกส์ (E-book) วีดิทัศน์ (Video clip)) หลักสูตรออนไลน์ (Online course) และเว็บไซต์ (Web site) ที่เกี่ยวข้อง เป็นต้น เพื่อให้นักศึกษาเห็นภาพและเข้าใจเนื้อหา รวมถึงเปิดโอกาสให้นักศึกษาได้แลกเปลี่ยนความคิดเห็นระหว่างกันในหัวข้อเนื้อหาที่น่าสนใจและมีความสำคัญ
- ในคาบปฏิบัติการ ให้นักศึกษาได้เรียนรู้และฝึกปฏิบัติด้วเครื่องมือและซอฟต์แวร์ที่สอดคล้องกับเนื้อหารายวิชา **ในรูปแบบของกระบวนการจัดการเรียนรู้ที่ผู้เรียนได้ลงมือกระทำ (Active learning)** แล้วมอบหมายให้นักศึกษา**ทำแบบฝึกปฏิบัติการด้วยตนเอง (Learning by doing) ทั้งงานเดี่ยวและงานกลุ่ม** ภายใต้การดูแลและให้คำแนะนำจากอาจารย์ผู้สอน ซึ่งเป็นการพัฒนาทักษะการแก้ไขปัญหาทางคอมพิวเตอร์ และการเรียนรู้ด้วยตนเอง ซึ่งเป็นส่วนหนึ่งของ**คุณสมบัติของบัณฑิตไทยในศตวรรษที่ 21** และเพื่อนำไปต่อยอดกับการเรียนในรายวิชาอื่น ๆ หรือการพัฒนาผลงานทางวิชาการต่อไป
- การแนะนำให้นักศึกษาทำการศึกษาค้นคว้าด้วยตนเองจากแหล่งอ้างอิงอื่น ๆ ที่อาจารย์ผู้สอนรวบรวมและแนะนำไว้ในระบบ E-Learning
- การมอบหมายให้นักศึกษาทำการบ้านในหัวข้อเนื้อหาที่สำคัญเพื่อเป็นการทบทวนความรู้ที่ได้เรียนในชั้นเรียน พร้อมส่งในระบบ E-learning ในวันและเวลาที่ผู้สอนกำหนด
- การมอบหมายให้นักศึกษาทำการศึกษางานวิจัยที่เกี่ยวข้องกับเทคโนโลยี Cyber security และ AI จากบทความวิจัยที่เผยแพร่ในวารสารวิชาการระดับนานาชาติในหัวข้อที่นักศึกษามีความสนใจ แล้วนำเสนอหน้าชั้นเรียนใน **กิจกรรมนี้ถือเป็นการส่งเสริมทักษะมีความสามารถในการหาความรู้เพิ่มเติม มีนิสัยใฝ่รู้ มีความเท่าทันกับความเคลื่อนไหว และความก้าวหน้าในศาสตร์ที่ศึกษา ซึ่งเป็นคุณลักษณะของบัณฑิตไทยในศตวรรษที่ 21**
- การมอบหมายให้นักศึกษาจับคู่กันเพื่อ**ทำการศึกษาค้นคว้าด้วยตนเองเกี่ยวกับภัยคุกคามช่องโหว่ และการโจมตีทางไซเบอร์** ที่มีผลกระทบหรือความเสียหายรุนแรงต่อ ระบบข้อมูล/สารสนเทศและระบบเครือข่ายคอมพิวเตอร์ โดยศึกษาถึงความหมาย วิวัฒนาการ รูปแบบ/ลักษณะ ตัวอย่างความเสียหายที่เกิดขึ้นจากข่าวหรือภาพยนตร์ **(ภาษาไทยและอังกฤษอย่างละ 1 เรื่อง)** สถิติที่เกี่ยวข้อง การวิเคราะห์ผลกระทบที่เกิดขึ้นต่อบุคคล องค์กร และสังคม แนวทางการป้องกัน และวิธีการแก้ไข (ด้วยวิธีการใช้ฮาร์ดแวร์ ซอฟต์แวร์ หรือการใช้กฎระเบียบ ข้อบังคับต่าง ๆ ขององค์กรและสังคม) ที่เป็นผลจากการศึกษาค้นคว้าจากสื่อและแหล่งข้อมูลอ้างอิงที่หลากหลายที่มีความน่าเชื่อถือ**ทั้งภาษาไทยและภาษาอังกฤษ** เช่น ตำรา หนังสือ สื่อสิ่งพิมพ์ งานวิจัย วารสารวิชาการ เว็บไซต์ เป็นต้น และยึดหลักการไม่ละเมิดลิขสิทธิ์และทรัพย์สินทางปัญญาของผู้อื่น **พร้อมนำเสนอหน้าชั้นเรียน 2 รอบคือรอบ**

นำเสนอหัวข้อและขอบเขต เพื่อแลกเปลี่ยนความคิดเห็นระหว่างเพื่อนร่วมชั้นเรียนและรับข้อมูลป้อนกลับจากผู้สอน เพื่อนำไปใช้ประกอบการนำเสนอผลการศึกษาตามเวลาที่กำหนด กิจกรรมนี้ถือเป็นการส่งเสริมทักษะการรู้สารสนเทศ ทักษะการเรียนรู้ด้วยตนเอง การหาความรู้และมีนิสัยใฝ่รู้ มีความเท่าทันกับความเคลื่อนไหว และความก้าวหน้าในศาสตร์ที่ศึกษา และการยึดมั่นในจรรยาบรรณวิชาชีพซึ่งเป็นคุณลักษณะของบัณฑิตไทยในศตวรรษที่ 21 และ**ยังเป็นกิจกรรมที่พัฒนาทักษะการร่วมมือร่วมใจ (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 และเทคโนโลยีทางด้านปัญญาประดิษฐ์ที่เหมาะสมกับลักษณะธุรกิจหรืออุตสาหกรรมที่เลือกแล้วนำเสนอหน้าชั้นเรียนตามระยะเวลาที่ผู้สอนกำหนด โดยทำการศึกษาค้นคว้าจากสื่อและแหล่งข้อมูลอ้างอิงที่หลากหลายที่มีความน่าเชื่อถือ**ทั้งภาษาไทยและภาษาอังกฤษ** เช่น ตำรา หนังสือ สื่อสิ่งพิมพ์ งานวิจัย วารสารวิชาการ เว็บไซต์ เป็นต้น และยึดหลักการไม่ละเมิดลิขสิทธิ์และทรัพย์สินทางปัญญาของผู้อื่น กิจกรรมนี้ถือเป็นการส่งเสริมทักษะการรู้สารสนเทศ ทักษะการเรียนรู้ด้วยตนเอง การหาความรู้และมีนิสัยใฝ่รู้ ความสามารถในการประยุกต์ใช้ความรู้ให้เหมาะกับบริบททางสังคม และการยึดมั่นในจรรยาบรรณวิชาชีพซึ่งเป็นคุณลักษณะของบัณฑิตไทยในศตวรรษที่ 21 และยังเป็น**กิจกรรมที่พัฒนาทักษะการร่วมมือร่วมใจ (Collaboration) การคิดสร้างสรรค์ (Creativity) การติดต่อสื่อสาร (Communication) และการคิดวิเคราะห์ (Critical Thinking) ตามหลักการ 4C**

(3) วิธีการประเมินผล

- การเข้าชั้นเรียน และการมีส่วนร่วมในชั้นเรียน
- การส่งงานมอบหมายในชั้นเรียนภาคปฏิบัติ
- การนำเสนอผลการศึกษาบทความวิจัยด้านความมั่นคงทางไซเบอร์และปัญญาประดิษฐ์
- การนำเสนอผลการศึกษาค้นคว้าด้วยตนเองเกี่ยวกับภัยคุกคาม ช่องโหว่และการโจมตีทางไซเบอร์
- การนำเสนอโครงงานด้านความมั่นคงทางไซเบอร์
- การสอบกลางภาคเรียน
- การสอบปลายภาคเรียน

3. ทักษะทางปัญญา

(1) ทักษะทางปัญญาที่ต้องพัฒนา

3.3 รวบรวม ศึกษา วิเคราะห์ และสรุปประเด็นปัญหาและความต้องการ

3.4 สามารถประยุกต์ความรู้และทักษะกับการแก้ไขปัญหาทางคอมพิวเตอร์ได้อย่างเหมาะสม

(2) วิธีการสอน

- ในคาบปฏิบัติการ ให้นักศึกษาได้เรียนรู้และฝึกปฏิบัติด้วเครื่องมือและซอฟต์แวร์ที่สอดคล้องกับเนื้อหารายวิชา **ในรูปแบบของกระบวนการจัดการเรียนรู้ที่ผู้เรียนได้ลงมือกระทำ (Active learning)** แล้วมอบหมายให้นักศึกษา**ทำแบบฝึกปฏิบัติการด้วยตนเอง (Learning by doing) ทั้งงานเดี่ยวและงานกลุ่ม** ภายใต้การดูแลและให้คำแนะนำจากอาจารย์ผู้สอน ซึ่งเป็นการพัฒนาทักษะการแก้ไขปัญหาทางคอมพิวเตอร์ และการเรียนรู้ด้วยตนเอง ซึ่งเป็นส่วนหนึ่งของ**คุณสมบัติของบัณฑิตไทยในศตวรรษที่ 21** และเพื่อนำไปต่อยอดกับการเรียนในรายวิชาอื่น ๆ หรือการพัฒนาผลงานทางวิชาการต่อไป
- การมอบหมายให้นักศึกษาจับคู่กันเพื่อ**ทำการศึกษาค้นคว้าด้วยตนเองเกี่ยวกับภัยคุกคามช่องโหว่ และการโจมตีทางไซเบอร์** ที่มีผลกระทบหรือความเสียหายรุนแรงต่อ ระบบข้อมูล/สารสนเทศและระบบเครือข่ายคอมพิวเตอร์ โดยศึกษาถึงความหมาย วิวัฒนาการ รูปแบบ/ลักษณะ ตัวอย่างความเสียหายที่เกิดขึ้นจากข่าวหรือภาพยนตร์ **(ภาษาไทยและอังกฤษอย่างละ 1 เรื่อง)** สถิติที่เกี่ยวข้อง การวิเคราะห์ผลกระทบที่เกิดขึ้นต่อบุคคล องค์กร และสังคม แนวทางการป้องกัน และวิธีการแก้ไข (ด้วยวิธีการใช้ฮาร์ดแวร์ ซอฟต์แวร์ หรือการใช้กฎระเบียบ ข้อบังคับต่าง ๆ ขององค์กรและสังคม) ที่เป็นผลจากการศึกษาค้นคว้าจากสื่อและแหล่งข้อมูลอ้างอิงที่หลากหลายที่มีความน่าเชื่อถือ**ทั้งภาษาไทยและภาษาอังกฤษ** เช่น ตำรา หนังสือ สื่อสิ่งพิมพ์ งานวิจัย วารสารวิชาการ เว็บไซต์ เป็นต้น และยึดหลักการไม่ละเมิดลิขสิทธิ์และทรัพย์สินทางปัญญาของผู้อื่น **พร้อมนำเสนอหน้าชั้นเรียน 2 รอบคือรอบนำเสนอหัวข้อและขอบเขต เพื่อแลกเปลี่ยนความคิดเห็นระหว่างเพื่อนร่วมชั้นเรียนและรับข้อมูลป้อนกลับจากผู้สอน เพื่อนำไปใช้ประกอบการนำเสนอผลการศึกษาตามเวลาที่กำหนด**กิจกรรมนี้ถือเป็นการส่งเสริมทักษะการรู้สารสนเทศ ทักษะการเรียนรู้ด้วยตนเอง การหาความรู้และมีนิสัยใฝ่รู้ มีความเท่าทันกับความเคลื่อนไหว และความก้าวหน้าในศาสตร์ที่ศึกษา และการยึดมั่นในจรรยาบรรณวิชาชีพซึ่งเป็นคุณลักษณะของบัณฑิตไทยในศตวรรษที่ 21 และ**ยังเป็นกิจกรรมที่พัฒนาทักษะการร่วมมือร่วมใจ (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 แล้วนำเสนอหน้าชั้นเรียนตามระยะเวลาที่ผู้สอนกำหนด โดยทำการศึกษาค้นคว้าจากสื่อและแหล่งข้อมูลอ้างอิงที่หลากหลายที่มีความน่าเชื่อถือ**ทั้งภาษาไทยและภาษาอังกฤษ** เช่น ตำรา หนังสือ สื่อสิ่งพิมพ์ งานวิจัย วารสารวิชาการ เว็บไซต์ เป็นต้น และยึดหลักการไม่ละเมิดลิขสิทธิ์และทรัพย์สินทางปัญญาของผู้อื่น กิจกรรมนี้ถือเป็นการส่งเสริมทักษะการรู้สารสนเทศ ทักษะการเรียนรู้ด้วยตนเอง การหาความรู้และมีนิสัยใฝ่รู้ ความสามารถในการประยุกต์ใช้ความรู้ให้เหมาะกับบริบททางสังคม และการยึดมั่นในจรรยาบรรณวิชาชีพซึ่งเป็นคุณลักษณะของบัณฑิตไทยในศตวรรษที่ 21 และยังเป็น**กิจกรรมที่พัฒนาทักษะการร่วมมือร่วมใจ (Collaboration) การคิดสร้างสรรค์ (Creativity) การติดต่อสื่อสาร (Communication) และการคิดวิเคราะห์ (Critical Thinking) ตามหลักการ 4C**

(3)วิธีการประเมินผล

- การส่งงานมอบหมายในชั้นเรียนภาคปฏิบัติ
- การนำเสนอผลการศึกษาค้นคว้าด้วยตนเองเกี่ยวกับภัยคุกคาม ช่องโหว่และการโจมตีทางไซเบอร์
- การนำเสนอโครงงานด้านความมั่นคงทางไซเบอร์
- การสอบกลางภาคเรียน
- การสอบปลายภาคเรียน

4. ทักษะความสัมพันธ์ระหว่างบุคคลและความรับผิดชอบ

(1) ทักษะความสัมพันธ์ระหว่างบุคคลและความรับผิดชอบที่ต้องพัฒนา

4.2 ให้ความช่วยเหลือและอำนวยความสะดวกแก่การแก้ปัญหาสถานการณ์ต่าง ๆ ในกลุ่มทั้งบทบาทของผู้นำหรือ บทบาทของผู้ร่วมทีมทำงาน

(2) วิธีการสอน

- ในคาบปฏิบัติการ ให้นักศึกษาได้เรียนรู้และฝึกปฏิบัติด้วเครื่องมือและซอฟต์แวร์ที่สอดคล้องกับเนื้อหารายวิชา **ในรูปแบบของกระบวนการจัดการเรียนรู้ที่ผู้เรียนได้ลงมือกระทำ (Active learning)** แล้วมอบหมายให้นักศึกษา**ทำแบบฝึกปฏิบัติการด้วยตนเอง (Learning by doing) ทั้งงานเดี่ยวและงานกลุ่ม** ภายใต้การดูแลและให้คำแนะนำจากอาจารย์ผู้สอน ซึ่งเป็นการพัฒนา

ทักษะการแก้ไขปัญหาทางคอมพิวเตอร์ และการเรียนรู้ด้วยตนเอง ซึ่งเป็นส่วนหนึ่งของ**คุณสมบัติของบัณฑิตไทยในศตวรรษที่ 21** และเพื่อนำไปต่อยอดกับการเรียนในรายวิชาอื่น ๆ หรือการพัฒนาผลงานทางวิชาการต่อไป

- การมอบหมายให้นักศึกษาจับคู่กันเพื่อ**ทำการศึกษาค้นคว้าด้วยตนเองเกี่ยวกับภัยคุกคามช่องโหว่ และการโจมตีทางไซเบอร์** ที่มีผลกระทบหรือความเสียหายรุนแรงต่อ ระบบข้อมูล/สารสนเทศและระบบเครือข่ายคอมพิวเตอร์ โดยศึกษาถึงความหมาย วิวัฒนาการ รูปแบบ/ลักษณะ ตัวอย่างความเสียหายที่เกิดขึ้นจากข่าวหรือภาพยนตร์ **(ภาษาไทยและอังกฤษอย่างละ 1 เรื่อง)** สถิติที่เกี่ยวข้อง การวิเคราะห์ผลกระทบที่เกิดขึ้นต่อบุคคล องค์กร และสังคม แนวทางการป้องกัน และวิธีการแก้ไข (ด้วยวิธีการใช้ฮาร์ดแวร์ ซอฟต์แวร์ หรือการใช้กฎระเบียบ ข้อบังคับต่าง ๆ ขององค์กรและสังคม) ที่เป็นผลจากการศึกษาค้นคว้าจากสื่อและแหล่งข้อมูลอ้างอิงที่หลากหลายที่มีความน่าเชื่อถือ**ทั้งภาษาไทยและภาษาอังกฤษ** เช่น ตำรา หนังสือ สื่อสิ่งพิมพ์ งานวิจัย วารสารวิชาการ เว็บไซต์ เป็นต้น และยึดหลักการไม่ละเมิดลิขสิทธิ์และทรัพย์สินทางปัญญาของผู้อื่น **พร้อมนำเสนอหน้าชั้นเรียน 2 รอบคือรอบนำเสนอหัวข้อและขอบเขต เพื่อแลกเปลี่ยนความคิดเห็นระหว่างเพื่อนร่วมชั้นเรียนและรับข้อมูลป้อนกลับจากผู้สอน เพื่อนำไปใช้ประกอบการนำเสนอผลการศึกษาตามเวลาที่กำหนด** กิจกรรมนี้ถือเป็นการส่งเสริมทักษะการรู้สารสนเทศ ทักษะการเรียนรู้ด้วยตนเอง การหาความรู้และมีนิสัยใฝ่รู้ มีความเท่าทันกับความเคลื่อนไหว และความก้าวหน้าในศาสตร์ที่ศึกษา และการยึดมั่นในจรรยาบรรณวิชาชีพซึ่งเป็นคุณลักษณะของบัณฑิตไทยในศตวรรษที่ 21 และ**ยังเป็นกิจกรรมที่พัฒนาทักษะการร่วมมือร่วมใจ (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 และเทคโนโลยีทางด้านปัญญาประดิษฐ์ที่เหมาะสมกับลักษณะธุรกิจหรืออุตสาหกรรมที่เลือกแล้วนำเสนอหน้าชั้นเรียนตามระยะเวลาที่ผู้สอนกำหนด โดยทำการศึกษาค้นคว้าจากสื่อและแหล่งข้อมูลอ้างอิงที่หลากหลายที่มีความน่าเชื่อถือ**ทั้งภาษาไทยและภาษาอังกฤษ** เช่น ตำรา หนังสือ สื่อสิ่งพิมพ์ งานวิจัย วารสารวิชาการ เว็บไซต์ เป็นต้น และยึดหลักการไม่ละเมิดลิขสิทธิ์และทรัพย์สินทางปัญญาของผู้อื่น กิจกรรมนี้ถือเป็นการส่งเสริมทักษะการรู้สารสนเทศ ทักษะการเรียนรู้ด้วยตนเอง การหาความรู้และมีนิสัยใฝ่รู้ ความสามารถในการ

ประยุกต์ใช้ความรู้ให้เหมาะกับบริบททางสังคม และการยึดมั่นในจรรยาบรรณวิชาชีพซึ่งเป็นคุณลักษณะของบัณฑิตไทยในศตวรรษที่ 21 และยังเป็น**กิจกรรมที่พัฒนาทักษะการร่วมมือร่วมใจ (Collaboration) การคิดสร้างสรรค์ (Creativity) การติดต่อสื่อสาร (Communication) และการคิดวิเคราะห์ (Critical Thinking) ตามหลักการ 4C**

(3)วิธีการประเมิน

- การส่งงานมอบหมายในชั้นเรียนภาคปฏิบัติ
- การนำเสนอผลการศึกษาค้นคว้าด้วยตนเองเกี่ยวกับภัยคุกคาม ช่องโหว่และการโจมตีทางไซเบอร์
- การนำเสนอโครงงานด้านความมั่นคงทางไซเบอร์

5. ทักษะการวิเคราะห์เชิงตัวเลข การสื่อสารและการใช้เทคโนโลยีสารสนเทศ

(1) ทักษะการวิเคราะห์เชิงตัวเลข การสื่อสารและการใช้เทคโนโลยีสารสนเทศที่ต้องพัฒนา

5.1 มีทักษะในการใช้เครื่องมือที่จำเป็นที่มีอยู่ในปัจจุบันต่อการทำงานที่เกี่ยวกับคอมพิวเตอร์

5.3 สื่อสารอย่างมีประสิทธิภาพทั้งปากเปล่าและการเขียน เลือกใช้รูปแบบของสื่อการนำเสนออย่างเหมาะสม

(2)วิธีการสอน

- ในคาบปฏิบัติการ ให้นักศึกษาได้เรียนรู้และฝึกปฏิบัติด้วเครื่องมือและซอฟต์แวร์ที่สอดคล้องกับเนื้อหารายวิชา **ในรูปแบบของกระบวนการจัดการเรียนรู้ที่ผู้เรียนได้ลงมือกระทำ (Active learning)** แล้วมอบหมายให้นักศึกษา**ทำแบบฝึกปฏิบัติการด้วยตนเอง (Learning by doing) ทั้งงานเดี่ยวและงานกลุ่ม** ภายใต้การดูแลและให้คำแนะนำจากอาจารย์ผู้สอน ซึ่งเป็นการพัฒนาทักษะการแก้ไขปัญหาทางคอมพิวเตอร์ และการเรียนรู้ด้วยตนเอง ซึ่งเป็นส่วนหนึ่งของ**คุณสมบัติของบัณฑิตไทยในศตวรรษที่ 21** และเพื่อนำไปต่อยอดกับการเรียนในรายวิชาอื่น ๆ หรือการพัฒนาผลงานทางวิชาการต่อไป
- การมอบหมายให้นักศึกษาทำการศึกษางานวิจัยที่เกี่ยวข้องกับเทคโนโลยี Cyber security และ AI จากบทความวิจัยที่เผยแพร่ในวารสารวิชาการระดับนานาชาติในหัวข้อที่นักศึกษามีความสนใจ แล้วนำเสนอหน้าชั้นเรียนใน **กิจกรรมนี้ถือเป็นการส่งเสริมทักษะมีความสามารถในการหาความรู้เพิ่มเติม มีนิสัยใฝ่รู้ มีความเท่าทันกับความเคลื่อนไหว และความก้าวหน้าในศาสตร์ที่ศึกษา ซึ่งเป็นคุณลักษณะของบัณฑิตไทยในศตวรรษที่ 21**

(3) วิธีการประเมินผล

- การส่งงานมอบหมายในชั้นเรียนภาคปฏิบัติ
- การนำเสนอผลการศึกษาบทความวิจัยด้านความมั่นคงทางไซเบอร์และปัญญาประดิษฐ์
- การนำเสนอผลการศึกษาค้นคว้าด้วยตนเองเกี่ยวกับภัยคุกคาม ช่องโหว่และการโจมตีทางไซเบอร์
- การนำเสนอโครงงานด้านความมั่นคงทางไซเบอร์
- การสอบปลายภาคเรียน

หมวดที่ 5 แผนการสอนและการประเมินผล

1. แผนการสอน (เขียนให้สอดคล้องกับ Curriculum Mapping และสอดคล้องกับหมวดที่ 4 การพัฒนาผลการเรียนรู้ของนักศึกษา)

สัปดาห์ที่	หัวข้อ/รายละเอียด	กิจกรรมการเรียนการสอน และสื่อที่ใช้	จำนวนชั่วโมง	ชื่อผู้สอน
1 (11/8/65)	**บรรยาย** ● **แนะนำรายละเอียดวิชา (Course Introduction)** ทำความตกลงเรื่อง กติกาในการเรียนการสอน การมอบหมายงานต่าง ๆ การวัดและประเมินผล **รวมถึงการมอบหมายงานตลอดภาคการศึกษา** ● **Introduction to Information security and Cyber security** ● **History of Information security** ● **มอบหมายงานการศึกษาค้นคว้างานวิจัยที่เกี่ยวข้องกับเทคโนโลยีด้านความมั่นคงทางไซเบอร์และปัญญาประดิษฐ์**	**ภาคบรรยาย** ● ชี้แจงรายละเอียดวิชา รูปแบบวิธีการเรียนการสอนและเกณฑ์การวัดและประเมินผล **ที่ให้นักศึกษามีส่วนร่วมและการมอบหมายงานตลอดภาคการศึกษา <u>รวมถึงการทำข้อตกลงกับนักศึกษา</u>** ● ชี้แจงและมอบหมายให้นักศึกษาทำการศึกษาบทเรียนจากเอกสารประกอบการสอน และ Video clips หรือสื่ออื่น ๆ ที่ปรากฏในเอกสาร มคอ.3 และ e-Learning ล่วงหน้าก่อนเรียนคาบถัดไปทุกครั้ง **รวมถึงการจัดการเรียนการสอนแบบห้องเรียนกลับด้าน (Flipped classroom) ในบางหัวข้อ** ● การสอดแทรกจริยธรรมและคุณธรรมอัตลักษณ์ของมหาวิทยาลัย (ยึดมั่นในคุณธรรม 6 ประการ ขยัน อดทน ประหยัด เมตตา ซื่อสัตย์ กตัญญู) และได้ย้ำเตือนให้นักศึกษาดำเนินชีวิตตามหลักปรัชญาเศรษฐกิจพอเพียง และเรียนรู้เพื่อรับใช้สังคม รวมถึงการปฏิบัติตามกฎระเบียบของมหาวิทยาลัย การไม่ทุจริตในการสอบ การไม่ละเมิดลิขสิทธิ์ และการยึดมั่นในจรรยาบรรณวิชาชีพ ● บรรยายประกอบการยกตัวอย่างด้วย MS-PowerPoint, E-books, Video clips, Course online และ Website ที่เกี่ยวข้อง	(2/2/0)	**บรรยาย** อาจารย์ณัฐพร

		• รับชมวีดิทัศน์ที่เกี่ยวข้อง • ถาม-ตอบคำถามสั้น ๆ เพื่อประเมินศักยภาพผู้เรียน • แนะนำแหล่งข้อมูลอ้างอิงและสื่อการสอนต่าง ๆ ที่เกี่ยวข้อง **สื่อที่ใช้** • MS-PowerPoint • HCU e-learning • e-book (Thai and English) • Video clips • Other medias/References website [Publish on HCU E-learning] • Online conference system: MS-Teams and etc.		
	ปฏิบัติ • **Create TryHackMe.com account https://tryhackme.com/** • **Learning how to use tryhackme.com from tutorial https://tryhackme.com/room/tutorial** • **Search for Cyber security and AI research paper**	**ปฏิบัติ** • สมัครใช้งาน TryHackMe.com website • ฝึกปฏิบัติการเรียนรู้การใช้งาน TryHackme.com website จาก Tutorial • นักศึกษาสืบค้นข้อมูลงานวิจัยด้าน Cyber security และ AI ภายใต้คำแนะนำของอาจารย์ผู้สอน **สื่อที่ใช้** • MS-PowerPoint • HCU e-Learning • Google Search Engine • Cyber security website • Online conference system: MS-Teams, and etc.		**ปฏิบัติ** อาจารย์ณัฐพร
2 **(18/8/65)**	**บรรยาย** • **Telecommunication security**	**บรรยาย** • บรรยายประกอบการยกตัวอย่างด้วย MS-PowerPoint, E-books, Video clips, Course online และ Website ที่เกี่ยวข้อง	(2/2/0)	**บรรยาย** อาจารย์ ดร. ธีรวัฒน์

		• ตอบคำถามสั้น ๆ เพื่อประเมินความรู้ความเข้าใจของนักศึกษา • รับชมวีดิทัศน์ที่เกี่ยวข้อง **สื่อที่ใช้** • MS-PowerPoint • HCU e-learning • e-book (Thai and English) • Video clips • Other medias/References website [Publish on HCU e-Learning] • Online conference system: MS-Teams and etc.		
	ปฏิบัติ • **Vulnerability Assessment (VA) lab**	**ปฏิบัติ** • ฝึกปฏิบัติการที่เกี่ยวกับช่องโหว่ของระบบและ Website ตัวอย่าง จาก TryHackme.com website **สื่อที่ใช้** • MS-PowerPoint • HCU e-Learning • Cyber security software/tools • Cyber security website • Online conference system: MS-Teams, and etc.		**ปฏิบัติ** อาจารย์ ดร. ธีรวัฒน์
3 **(25/8/65)**	**บรรยาย** • **Cybercrime, threat, attack, and vulnerability**	**บรรยาย** • บรรยายประกอบการยกตัวอย่างด้วย MS-PowerPoint, E-books, Video clips, Course online และ Website ที่เกี่ยวข้อง • ตอบคำถามสั้น ๆ เพื่อประเมินความรู้ความเข้าใจของนักศึกษา • รับชมวีดิทัศน์ที่เกี่ยวข้อง **สื่อที่ใช้** • MS-PowerPoint • HCU e-Learning • e-book (Thai and English)	(2/3/0)	**บรรยาย** อาจารย์ณัฐพร

		• Video clips • Other medias/References website [Publish on HCU e-Learning] • Online conference system: MS-Teams and etc.		
	ปฏิบัติ • Network security command on OS • Network security lab from TryHackme.com • **มอบหมายงานการศึกษาค้นคว้าด้วยตนเองเกี่ยวกับภัยคุกคาม ช่องโหว่และการโจมตีทางไซเบอร์**	**ปฏิบัติ** • ฝึกปฏิบัติการ Network security command [Windows/Ubuntu]: whois, ping, traceroute/tracert, arp, nslookup, netstat] • ฝึกปฏิบัติการ Network security จาก TryHackme.com website • นักศึกษาจับคู่และหาหัวข้อการศึกษาค้นคว้าด้วยตนเองภายใต้คำแนะนำของอาจารย์ผู้สอน **สื่อที่ใช้** • MS-PowerPoint • HCU e-Learning • Network security command • Cyber security website • Online conference system: MS-Teams, and etc.		**ปฏิบัติ** อาจารย์ณัฐพร
4 (1/9/65)	**บรรยาย** • **Security Policies, Standards, Procedures, and Guidelines**	**บรรยาย** • บรรยายประกอบการยกตัวอย่างด้วย MS-PowerPoint, E-books, Video clips, Course online และ Website ที่เกี่ยวข้อง • ตอบคำถามสั้น ๆ เพื่อประเมินความรู้ความเข้าใจของนักศึกษา • รับชมวีดิทัศน์ที่เกี่ยวข้อง **สื่อที่ใช้** • MS-PowerPoint • HCU e-learning • e-book (Thai and English) • Video clips	(2/2/0)	**บรรยาย** อาจารย์ณัฐพร

		• Other medias/References website [Publish on HCU E-learning] • Online conference system: MS-Teams and etc.		
	ปฏิบัติ • **การนำเสนอหัวข้อการศึกษาค้นคว้าด้วยตนเองเกี่ยวกับภัยคุกคาม ช่องโหว่และการโจมตีทางไซเบอร์ [Proposal presentation]**	**ปฏิบัติ** • นักศึกษานำเสนอหัวข้อและขอบเขตการศึกษาค้นคว้าด้วยตนเองเกี่ยวกับภัยคุกคาม ช่องโหว่และการโจมตีทางไซเบอร์ • ถามตอบ ให้ข้อมูลป้อนกลับ และแลกเปลี่ยนความคิดเห็นระหว่างกัน **สื่อที่ใช้** • HCU e-Learning • Cyber security website • Online conference system: MS-Teams and etc. • Other media upon students		**ปฏิบัติ** อาจารย์ณัฐพร
5 (9/9/64)	**บรรยาย** • **Critical Infrastructure attack** • **Cyber security framework**	**บรรยาย** • บรรยายประกอบการยกตัวอย่างด้วย MS-PowerPoint, E-books, Video clips, Course online และ Website ที่เกี่ยวข้อง • ตอบคำถามสั้น ๆ เพื่อประเมินความรู้ความเข้าใจของนักศึกษา • รับชมวีดิทัศน์ที่เกี่ยวข้อง **สื่อที่ใช้** • MS-PowerPoint • HCU e-Learning • e-book (Thai and English) • Video clips • Other medias/References website [Publish on HCU e-Learning] • Online conference system: MS-Teams and etc.	(2/2/0)	**บรรยาย** อาจารย์ ดร. ธีรวัฒน์

	ปฏิบัติ ● **View source lab from TryHackme.com**	**ปฏิบัติ** ● ฝึกปฏิบัติการหัวข้อ View source จาก TryHackme.com website **สื่อที่ใช้** ● HCU e-Learning ● Cyber security software/tools ● https://tryhackme.com/room/walkinganapplication ● Online conference system: MS-Teams and etc. ● Other media upon students		**ปฏิบัติ** อาจารย์ ดร. ธีรวัฒน์
6 **(15/9/65)**	**บรรยาย** ● Ethics, Laws, and professional issues in Cyber security	**บรรยาย** ● บรรยายประกอบการยกตัวอย่างด้วย MS-PowerPoint, E-books, Video clips, Course online และ Website ที่เกี่ยวข้อง ● ตอบคำถามสั้น ๆ เพื่อประเมินความรู้ความเข้าใจของนักศึกษา ● รับชมวีดิทัศน์ที่เกี่ยวข้อง **สื่อที่ใช้** ● MS-PowerPoint ● HCU e-Learning ● e-book (Thai and English) ● Video clips ● Other medias/References website [Publish on HCU e-Learning] ● Online conference system: MS-Teams and etc.	(2/2/0)	**บรรยาย** อาจารย์ ดร. ธีรวัฒน์
	ปฏิบัติ ● **Group workshop about Cyber security law and Personal Data Privacy Act [PDPA}**	**ปฏิบัติ** ● ฝึกปฏิบัติการจาก Case study ที่กำหนดให้ โดยแบ่งเป็นกลุ่ม **สื่อที่ใช้** ● HCU e-Learning ● Cyber security case study ● Online conference system: MS-		**ปฏิบัติ** อาจารย์ ดร. ธีรวัฒน์

		Teams and etc. ● Other media upon students		
7 (22/9/65)	**บรรยาย** ● Physical security	**บรรยาย** ● บรรยายประกอบการยกตัวอย่างด้วย MS-PowerPoint, E-books, Video clips, Course online และ Website ที่เกี่ยวข้อง ● ตอบคำถามสั้น ๆ เพื่อประเมินความรู้ความเข้าใจของนักศึกษา ● รับชมวีดิทัศน์ที่เกี่ยวข้อง **สื่อที่ใช้** ● MS-PowerPoint ● HCU e-Learning ● e-book (Thai and English) ● Video clips ● Other medias/References website [Publish on HCU e-Learning] ● Online conference system: MS-Teams and etc.	(2/2/0)	**บรรยาย** อาจารย์ณัฐพร
	ปฏิบัติ ● **การนำเสนอผลการศึกษาค้นคว้างานวิจัยที่เกี่ยวข้องกับเทคโนโลยีด้านความมั่นคงทางไซเบอร์และปัญญาประดิษฐ์**	**ปฏิบัติ** ● นักศึกษานำเสนอผลการศึกษาค้นคว้างานวิจัยที่เกี่ยวข้องกับเทคโนโลยีด้านความมั่นคงทางไซเบอร์และปัญญาประดิษฐ์ ● ถามตอบ ให้ข้อมูลป้อนกลับ และแลกเปลี่ยนความคิดเห็นระหว่างกัน ● **นักศึกษาประเมินผลงานของตนเองและเพื่อนร่วมชั้นเรียน** **สื่อที่ใช้** ● HCU e-Learning ● Online conference system: MS-Teams and etc. ● Other media upon students		**ปฏิบัติ** อาจารย์ณัฐพร
8 (29/9/6)	**การสอบกลางภาค (Midterm examination) ใช้เวลา 3 ชั่วโมง (24/9/65-2/10/65)**			

9 **(6/10/65)**	บรรยาย ● Identification, Authentication, and Authorization ● Biometrics security	**บรรยาย** ● บรรยายประกอบการยกตัวอย่างด้วย MS-PowerPoint, E-books, Video clips, Course online และ Website ที่เกี่ยวข้อง ● ตอบคำถามสั้น ๆ เพื่อประเมินความรู้ความเข้าใจของนักศึกษา ● รับชมวีดิทัศน์ที่เกี่ยวข้อง **สื่อที่ใช้** ● MS-PowerPoint ● HCU e-Learning ● e-book (Thai and English) ● Video clips ● Other medias/References website [Publish on HCU e-Learning] ● Online conference system: MS-Teams and etc.	(2/2/0)	**บรรยาย** อาจารย์ณัฐพร
	ปฏิบัติ ● **การนำเสนอผลการศึกษาค้นคว้าด้วยตนเองเกี่ยวกับภัยคุกคาม ช่องโหว่และการโจมตีทางไซเบอร์** [Complete presentation] ● **มอบหมายโครงงานด้าน Cyber security**	**ปฏิบัติ** ● นักศึกษานำเสนอผลการศึกษาค้นคว้าด้วยตนเองเกี่ยวกับภัยคุกคาม ช่องโหว่และการโจมตีทางไซเบอร์ ● ถามตอบ ให้ข้อมูลป้อนกลับ และแลกเปลี่ยนความคิดเห็นระหว่างกัน ● **นักศึกษาประเมินผลงานของตนเองและเพื่อนร่วมชั้นเรียน** **สื่อที่ใช้** ● HCU e-Learning ● Cyber security software/tools ● Online conference system: MS-Teams and etc. ● Other media upon students		**ปฏิบัติ** อาจารย์ณัฐพร
10 **(13/10/65)**	**บรรยาย** ● **Basic concept of cryptography**	**บรรยาย** ● บรรยายประกอบการยกตัวอย่างด้วย MS-PowerPoint, E-books, Video clips, Course online และ	(2/2/0)	**บรรยาย** อาจารย์ ดร. กรินทร์

		Website ที่เกี่ยวข้อง • ตอบคำถามสั้น ๆ เพื่อประเมินความรู้ความเข้าใจของนักศึกษา • รับชมวีดิทัศน์ที่เกี่ยวข้อง **สื่อที่ใช้** • MS-PowerPoint • HCU e-Learning • e-book (Thai and English) • Video clips • Other medias/References website [Publish on HCU e-Learning] • Online conference system: MS-Teams and etc.		
	ปฏิบัติ • **Classic cryptography** • **Modern cryptography**	**ปฏิบัติ** • ฝึกปฏิบัติการจากสื่อการทดลองที่กำหนด **สื่อที่ใช้** • HCU E-learning • Cryptool2 application • Online conference system: MS-Teams and etc. • Other media upon students		**ปฏิบัติ** อาจารย์ ดร. กรินทร์
11 **(20/10/65)**	**บรรยาย** • **Basic concept of cryptography (cont.)**	**บรรยาย** • บรรยายประกอบการยกตัวอย่างด้วย MS-PowerPoint, E-books, Video clips, Course online และ Website ที่เกี่ยวข้อง • ตอบคำถามสั้น ๆ เพื่อประเมินความรู้ความเข้าใจของนักศึกษา • รับชมวีดิทัศน์ที่เกี่ยวข้อง **สื่อที่ใช้** • MS-PowerPoint • HCU e-Learning • e-book (Thai and English) • Video clips	(2/2/0)	**บรรยาย** อาจารย์ ดร. กรินทร์

		• Other medias/References website [Publish on HCU e-Learning] • Online conference system: MS-Teams and etc.		
	ปฏิบัติ • **Public-key cryptography** • **Message Digest and Certificates**	**ปฏิบัติ** • ฝึกปฏิบัติการจากสื่อการทดลองที่กำหนด **สื่อที่ใช้** • HCU E-learning • Cryptool2 application • Online conference system: MS-Teams and etc. • Other media upon students		**ปฏิบัติ** อาจารย์ ดร. กรินทร์
12 **(27/10/65)**	**บรรยาย** • **Web attack and security**	**บรรยาย** • บรรยายประกอบการยกตัวอย่างด้วย MS-PowerPoint, E-books, Video clips, Course online และ Website ที่เกี่ยวข้อง • ตอบคำถามสั้น ๆ เพื่อประเมินความรู้ความเข้าใจของนักศึกษา • รับชมวีดิทัศน์ที่เกี่ยวข้อง **สื่อที่ใช้** • MS-PowerPoint • HCU e-Learning • e-book (Thai and English) • Video clips • Other medias/References website [Publish on HCU e-Learning] • Online conference system: MS-Teams and etc.	(2/2/0)	**บรรยาย** อาจารย์ ดร. กรินทร์
	ปฏิบัติ • **Cross site scrip (XSS)** • **Cookie Hijacking**	**ปฏิบัติ** • ฝึกปฏิบัติการจากสื่อการทดลองที่กำหนด **สื่อที่ใช้**		**ปฏิบัติ** อาจารย์ ดร. กรินทร์

		• HCU E-learning • Virtual Box • Docker • Online conference system: MS-Teams and etc. • Other media upon students		
13 **(3/11/65)**	**บรรยาย** • **Web attack and security (cont.)**	**บรรยาย** • บรรยายประกอบการยกตัวอย่างด้วย MS-PowerPoint, E-books, Video clips, Course online และ Website ที่เกี่ยวข้อง • ตอบคำถามสั้น ๆ เพื่อประเมินความรู้ความเข้าใจของนักศึกษา • รับชมวีดิทัศน์ที่เกี่ยวข้อง **สื่อที่ใช้** • MS-PowerPoint • HCU e-Learning • e-book (Thai and English) • Video clips • Other medias/References website [Publish on HCU e-Learning] • Online conference system: MS-Teams and etc.	(2/2/0)	**บรรยาย** อาจารย์ ดร. กรินทร์
	ปฏิบัติ • **SQL injection** • **Command injection**	**ปฏิบัติ** • ฝึกปฏิบัติการจากสื่อการทดลองที่กำหนด **สื่อที่ใช้** • HCU E-learning • Virtual Box • Docker • Online conference system: MS-Teams and etc. • Other media upon students		**ปฏิบัติ** อาจารย์ ดร. กรินทร์
14 **(10/11/65)**	**บรรยาย** • **Digital forensic**	**บรรยาย** • บรรยายประกอบการยกตัวอย่างด้วย	(2/2/0)	**บรรยาย** รอง

	introduction	MS-PowerPoint, E-books, Video clips, Course online และ Website ที่เกี่ยวข้อง • ตอบคำถามสั้น ๆ เพื่อประเมินความรู้ความเข้าใจของนักศึกษา • รับชมวีดิทัศน์ที่เกี่ยวข้อง **สื่อที่ใช้** • MS-PowerPoint • HCU e-Learning • e-book (Thai and English) • Video clips • Other medias/References website [Publish on HCU e-Learning] • Online conference system: MS-Teams and etc.		ศาสตราจารย์ ดร. สุรทศ
	ปฏิบัติ • **Digital Forensics Lab**	**ปฏิบัติ** • ฝึกปฏิบัติการจากสื่อการทดลองที่กำหนด **สื่อที่ใช้** • HCU E-learning • VirtualBox หรือ VMWare • Online conference system: MS-Teams and etc. • Other media upon students		**ปฏิบัติ** รอง ศาสตราจารย์ ดร. สุรทศ
15 (17/11/65)	**บรรยาย** • **Basic of ethical hacking**	**บรรยาย** • บรรยายประกอบการยกตัวอย่างด้วย MS-PowerPoint, E-books, Video clips, Course online และ Website ที่เกี่ยวข้อง • ตอบคำถามสั้น ๆ เพื่อประเมินความรู้ความเข้าใจของนักศึกษา • รับชมวีดิทัศน์ที่เกี่ยวข้อง **สื่อที่ใช้** • MS-PowerPoint • HCU e-Learning	(2/2/0)	**บรรยาย** อาจารย์ ดร. กรินทร์

		• e-book (Thai and English) • Video clips • Other medias/References website [Publish on HCU e-Learning] • Online conference system: MS-Teams and etc.		
	ปฏิบัติ • **Ethical hacking and Vulnerability Assessment Applications**	**ปฏิบัติ** • ฝึกปฏิบัติการจากสื่อการทดลองที่กำหนด **สื่อที่ใช้** • HCU E-learning • Virtual Box • Online conference system: MS-Teams and etc. • Other media upon students		**ปฏิบัติ** อาจารย์ ดร. กรินทร์
16 **(24/11/65)**	**บรรยาย** • **Enterprise security** • **Security organization**	**บรรยาย** • บรรยายประกอบการยกตัวอย่างด้วย MS-PowerPoint, E-books, Video clips, Course online และ Website ที่เกี่ยวข้อง • ตอบคำถามสั้น ๆ เพื่อประเมินความรู้ความเข้าใจของนักศึกษา • รับชมวีดิทัศน์ที่เกี่ยวข้อง **สื่อที่ใช้** • MS-PowerPoint • HCU e-Learning • e-book (Thai and English) • Video clips • Other medias/References website [Publish on HCU e-Learning] • Online conference system: MS-Teams and etc.	(2/3/0)	**บรรยาย** ดร.ธีรวัฒน์
	ปฏิบัติ • **การนำเสนอโครงงานด้าน**	**ปฏิบัติ** • นักศึกษานำเสนอโครงงานด้าน Cyber		**ปฏิบัติ** ดร.ธีรวัฒน์

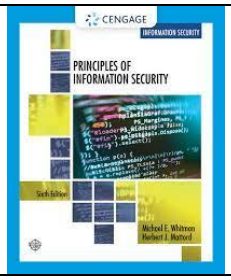
	Cyber security	security • ถามตอบ ให้ข้อมูลป้อนกลับ และแลกเปลี่ยนความคิดเห็นระหว่างกัน • **นักศึกษาประเมินผลงานของตนเองและเพื่อนร่วมชั้นเรียน** **สื่อที่ใช้** • HCU e-Learning • Web browser • Online conference system: MS-Teams, and etc. • Other media upon students		
16 **(6/12/65)**	**สอบปลายภาค 3 ชั่วโมง (28/11/65-13/12/65)**			
	รวม		**(30/30/0)**	

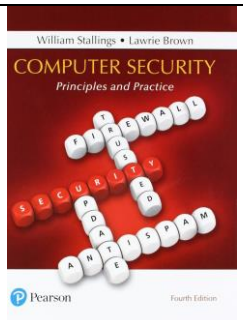
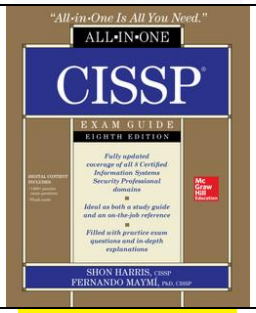
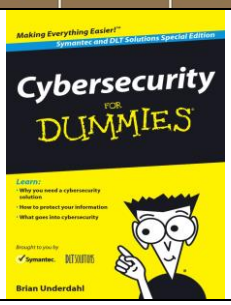
2. แผนการประเมินผลการเรียนรู้

ผลการเรียนรู้ที่เกี่ยวข้อง	กิจกรรมการประเมิน (เช่น การเขียนรายงาน โครงงาน การสอบย่อย การสอบกลางภาค การสอบปลายภาค)	สัปดาห์ที่ประเมิน	สัดส่วนของการประเมินผล
1.3, 2.1, 4.4	การเข้าชั้นเรียน และการมีส่วนร่วมในชั้นเรียน	ตลอดภาคการศึกษา	4%
2.3, 3.3, 3.4, 4.2, 5.1	การส่งงานมอบหมายในชั้นเรียนภาคปฏิบัติ	ตลอดภาคการศึกษา	16%
2.1, 2.4, 2.6, 5.3	การนำเสนอผลการศึกษางานวิจัยที่เกี่ยวกับเทคโนโลยีความมั่นคงทางไซเบอร์และปัญญาประดิษฐ์ (งานเดี่ยว)	สัปดาห์ที่ 4	10%
2.1, 2.3, 2.4, 2.6, 3.3, 3.4, 4.2, 5.1, 5.3	การนำเสนอผลการศึกษาค้นคว้าด้วยตนเองเกี่ยวกับการภัยคุกคาม ช่องโหว่และการโจมตีทางไซเบอร์ (งานคู่)	สัปดาห์ที่ 9	10%
2.1, 2.3, 2.4, 3.3, 3.4, 4.2, 5.1, 5.3	การนำเสนอโครงงานด้านความมั่นคงทางไซเบอร์ (งานกลุ่ม)	สัปดาห์ที่ 16	15%
1.3, 2.1, 2.6, 3,3, 3.4	การสอบกลางภาคเรียน	สัปดาห์ที่ 8	20%
1.3, 2.1, 2.3, 2.6, 5.1	การสอบปลายภาคเรียน	สัปดาห์ที่ 17	25%

หมวดที่ 6 ทรัพยากรประกอบการเรียนการสอน

1. ตำรา หนังสืออิเล็กทรอนิกส์ และเอกสารหลักที่ใช้ในการเรียนการสอน

รายการ	ภาพประกอบ
• Michael E. Whitman and Herbert J. Mattord, **Principle of Information Technology,** 6th Edition, Cengage learning, 2018.	

รายการ	ภาพประกอบ
• William Stallings and Lawrie Brown, **Computer Security: Principles and Practice,** 4th Edition, Pearson, 2017.	
• Shon Harris and Fernando Maymi, **CISSP All-in-One Exam Guide**, 8th Edition, McGraw-Hill, 2018	
• Joseph Steinberg, **Cyber security for Dummies**, 2nd Edition, John Wiley & Sons, 2016.	

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 รับพิมพ์ 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)
- Cyber Security Tutorials for Beginners | Learn eTutorials
- 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 ภายหลังได้รับทราบผลประเมินการสอนออนไลน์ของมหาวิทยาลัย
- การประชุมปรึกษาหารือเกี่ยวกับการเรียนการสอนในการประชุมคณะกรรมการบริหารหลักสูตรฯ ภายหลังได้รับทราบข้อเสนอแนะจากการตรวจประเมินการประกันคุณภาพการศึกษา

4. การทวนสอบมาตรฐานผลสัมฤทธิ์ของนักศึกษาในรายวิชา

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

5. การดำเนินการทบทวนและการวางแผนปรับปรุงประสิทธิผลของรายวิชา

- หลังจากสิ้นภาคการศึกษา ผู้สอนจะทำเข้าสู่ระบบประเมินผลการสอนออนไลน์ที่ได้จากการประมวลผลการตอบแบบประเมินออนไลน์ของนักศึกษาที่ลงทะเบียนเรียนในภาคการศึกษานั้น เพื่อดูผลและอ่านข้อแนะนำของนักศึกษาทุก ๆ คน และนำไปใช้ประกอบการปรับปรุงในภาค/ปีการศึกษาถัดที่เปิดสอน
- ปรับปรุงรายวิชาและหลักสูตรตามข้อกำหนดของเกณฑ์มาตรฐานหลักสูตรปริญญาตรี พ.ศ. 2558 กรอบมาตรฐานคุณวุฒิระดับปริญญาตรี สาขาคอมพิวเตอร์ พ.ศ.2552