# รายละเอียดของรายวิชา

**หลักสูตรบริหารธุรกิจบัณฑิต เทคโนโลยีทางธุรกิจดิจิทัล (หลักสูตรปรับปรุง พ.ศ. 2566)**

**คณะบริหารธุรกิจ สาขาวิชาเทคโนโลยีสารสนเทศทางธุรกิจ พื้นที่วิทยาเขตวังไกลกังวล**

## หมวดที่ 1 ข้อมูลทั่วไป

**1. รหัสและชื่อรายวิชา**

DBT 2222 ชื่อวิชาภาษาไทย ความปลอดภัยไซเบอร์

ชื่อวิชาภาษาอังกฤษ Cyber Security

**2. จำนวนหน่วยกิต**

3 (2-2-5)

**3. ประเภทของรายวิชา**

หมวด วิชาชีพเฉพาะ กลุ่มวิชา วิชาชีพบังคับ

**4. รายวิชาที่ต้องเรียนมาก่อน (Pre – requisite) (ถ้ามี)**

ไม่มี

**5. รายวิชาที่ต้องเรียนพร้อมกัน (Co – requisites) (ถ้ามี)**

ไม่มี

**6. ภาคการศึกษา /ชั้นปี**

ภาคการศึกษาที่ 1 ชั้นปีที่ 2

**7. อาจารย์ผู้รับผิดชอบรายวิชาและอาจารย์ผู้สอน**

อาจารย์ผู้รับผิดชอบรายวิชา อาจารย์ นพดล สายคติกรณ์

อาจารย์ผู้สอน อาจารย์ นพดล สายคติกรณ์

**8. วันที่จัดทำหรือปรับปรุงรายละเอียดของรายวิชาครั้งล่าสุด**

มิถุนายน 2568

**9. วัตถุประสงค์และรายละเอียดในการพัฒนา /ปรับปรุงรายวิชา**

ปรับปรุงให้มีความทันสมัย/ตามการปรับปรุงรอบระยะเวลาของหลักสูตร 5 ปี/ปรับปรุงตาม RMUTR-5

| แผนการปรับปรุงการจัดการเรียนรู้ให้สอดคล้องกับ CLO และภาคการทำงาน | ผลการดำเนินการปรับปรุงในครั้งนี้ |
|---|---|
| - ปรับกิจกรรมการเรียนรู้ให้สอดคล้องกับสถานการณ์จริง<br>- เพิ่ม Cyber Lab, การใช้เครื่องมือเช่น Wireshark, Snort, Metasploit<br>- จัด Capture The Flag (CTF) Simulation<br>- บูรณาการทักษะ Soft Skills ในการเรียนรู้<br>- ทำงานกลุ่ม, วิเคราะห์เหตุการณ์โจมตีจริง, Critical Thinking, Team Role Assignment<br>- เพิ่มเนื้อหา Cyber Ethics และ Cyber Law<br>- ศึกษาคดีตัวอย่าง เช่น Facebook breach, PDPA Thailand<br>- เชิญวิทยากรที่มีประสบการณ์มาบรรยายให้ความรู้ | - นักศึกษาสามารถแสดงทักษะวิเคราะห์ Packet และตรวจจับภัยคุกคามได้<br>- นักศึกษานำเสนอแผน Cyber Security Framework สำหรับองค์กรจำลอง<br>- นักศึกษาเข้าใจหลัก PDPA และจริยธรรมการเข้าถึงข้อมูล |

**10. คำอธิบายรายวิชา**

หลักการเบื้องต้นของความมั่นคงปลอดภัยในระบบสารสนเทศ ประเภทของภัยคุกคาม กลไกการโจมตีและการป้องกัน นโยบายและการปฏิบัติเพื่อความมั่นคงของระบบ การพิสูจน์ทราบในระบบคอมพิวเตอร์ การวิเคราะห์ การรุกราน การจัดการและบริการด้านความมั่นคง และการควบคุมการเข้าถึงตัวระบบ เทคโนโลยีและเครื่องมือที่ใช้ การควบคุมระบบเครือข่ายคอมพิวเตอร์ การป้องกันการบุกรุก การควบคุมทางชีวภาพ การใช้ซอฟต์แวร์ป้องกัน ประเด็นกฎหมายและจริยธรรมที่เกี่ยวข้อง แนวโน้มและ การประยุกต์งานด้านความมั่นคงปลอดภัย ปฏิบัติการใช้ซอฟต์แวร์ป้องกันภัยคุกคามทางคอมพิวเตอร์

## หมวดที่ 2 รายละเอียดผลลัพธ์การเรียนรู้และการประเมินผล

**1. ผลลัพธ์การเรียนรู้ระดับหลักสูตร** (ใส่เฉพาะ PLO ที่เกี่ยวข้อง หากเป็นหลักสูตรปรับปรุงเกณฑ์เดิมใช้ TQF 5 ด้านแทน)

**PLO1 อธิบายหลักการพื้นฐานและแนวคิดด้านบริหารธุรกิจและเทคโนโลยีสารสนเทศได้อย่างถูกต้องและชัดเจน**

PLO2 สื่อสารภาษาไทยและภาษาอังกฤษในการนำเสนอและอภิปรายได้อย่างมีประสิทธิภาพ และทำงานร่วมกับผู้อื่นได้ตามหน้าที่ความรับผิดชอบ

**PLO3 ประยุกต์ใช้เครื่องมือปัญญาประดิษฐ์และเทคโนโลยีดิจิทัลอย่างเหมาะสมเพื่อสนับสนุนการตัดสินใจในการแก้ไขปัญหาทางธุรกิจ**

PLO4 วิเคราะห์และนำเสนอข้อมูลเชิงธุรกิจที่สอดคล้องกับความต้องการของผู้ใช้โดยใช้เทคโนโลยีดิจิทัลและเทคโนโลยีปัญญาประดิษฐ์อย่างเหมาะสม

**PLO5 ประเมินและเลือกใช้เทคโนโลยีสืบค้นข้อมูลเพื่อพัฒนาตนเองอย่างต่อเนื่องสำหรับการเรียนรู้ตลอดชีวิตและการเป็นผู้ประกอบการ**

PLO6 สร้างสรรค์นวัตกรรมทางธุรกิจโดยประยุกต์ใช้เทคโนโลยีดิจิทัลและเทคโนโลยีปัญญาประดิษฐ์เพื่อพัฒนาและสนับสนุนการแก้ไขปัญหาทางธุรกิจ

PLO7 พัฒนาโครงงาน สิ่งประดิษฐ์ และนวัตกรรมโดยใช้ความรู้ในสาขาวิชาเทคโนโลยีธุรกิจอัจฉริยะเพื่อแก้ปัญหาในการทำงานและสร้างมูลค่าเพิ่มทางธุรกิจ

**2. ผลลัพธ์การเรียนรู้ระดับรายวิชา เมื่อนักศึกษาเรียนรายวิชานี้แล้ว นักศึกษาจะสามารถ**

CLO1: อธิบายและจำแนกหลักการพื้นฐาน ประเภทของภัยคุกคาม และกลไกการโจมตีไซเบอร์ได้.

CLO2: วิเคราะห์และประยุกต์ใช้นโยบาย, กลไกการป้องกัน, และการควบคุมการเข้าถึงเพื่อบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศได้.

CLO3: ใช้เครื่องมือและซอฟต์แวร์ด้านความมั่นคงปลอดภัยเพื่อพิสูจน์ยืนยันตัวตน, ป้องกันการบุกรุกเครือข่าย, และจัดการกับภัยคุกคามทางคอมพิวเตอร์ได้.

CLO4: วิเคราะห์และนำเสนอแนวทางการตอบสนองต่อการบุกรุก และประเด็นทางกฎหมายและจริยธรรมที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ได้.

CLO5: ประเมินแนวโน้มและประยุกต์ใช้ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์เพื่อพัฒนาตนเองอย่างต่อเนื่องและสร้างมูลค่าเพิ่มทางธุรกิจ.

## 3. ความรับผิดชอบผลลัพธ์การเรียนรู้ระดับรายวิชาต่อผลลัพธ์การเรียนรู้ระดับหลักสูตร

| ความรับผิดชอบผลลัพธ์การเรียนรู้ | PLO 1 | PLO 2 | PLO 3 | PLO 4 | PLO 5 | PLO 6 | PLO 7 |
|---|---|---|---|---|---|---|---|
| CLO1: อธิบายและจำแนกหลักการพื้นฐาน ประเภทของภัยคุกคาม และกลไกการโจมตีไซเบอร์ได้. | ✓ | | | | | | |
| CLO2: วิเคราะห์และประยุกต์ใช้นโยบาย, กลไกการป้องกัน, และการควบคุมการเข้าถึงเพื่อบริหารจัดการความมั่นคงปลอดภัยของระบบสารสนเทศได้. | | | ✓ | ✓ | | | |
| CLO3: ใช้เครื่องมือและซอฟต์แวร์ด้านความมั่นคงปลอดภัยเพื่อพิสูจน์ยืนยันตัวตน, ป้องกันการบุกรุกเครือข่าย, และจัดการกับภัยคุกคามทางคอมพิวเตอร์ได้. | | | ✓ | | | ✓ | |
| CLO4: วิเคราะห์และนำเสนอแนวทางการตอบสนองต่อการบุกรุกและประเด็นทางกฎหมายและจริยธรรมที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ได้. | | ✓ | | | ✓ | | |
| CLO5: ประเมินแนวโน้มและประยุกต์ใช้ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์เพื่อพัฒนาตนเองอย่างต่อเนื่องและสร้างมูลค่าเพิ่มทางธุรกิจ. | | | | | | ✓ | ✓ |

## 4. กลยุทธ์การสอนและการประเมินผลลัพธ์การเรียนรู้รายวิชา (CLO)

| CLO | วิธีการสอน/กิจกรรมการเรียนรู้ | วิธีการวัดผล | เครื่องมือ/เกณฑ์การประเมิน |
|---|---|---|---|
| **CLO1** อธิบายและจำแนกหลักการพื้นฐาน ประเภทของภัยคุกคาม และกลไกการโจมตีไซเบอร์ | - บรรยาย (Lecture)<br>- กรณีศึกษา (Case Study)<br>- การอภิปรายในชั้นเรียน | - แบบทดสอบก่อน–หลังเรียน (Quiz/Test)<br>- การตอบคำถามในชั้นเรียน | - คะแนนสอบ 20%<br>- Rubric การตอบคำถาม (ความถูกต้อง/ความเข้าใจ) |
| **CLO2** วิเคราะห์และประยุกต์ใช้นโยบาย กลไกการป้องกัน และการควบคุมการเข้าถึง | - วิเคราะห์กรณีศึกษาองค์กร (Case-based Learning)<br>- การเรียนรู้แบบใช้ปัญหา (Problem-based Learning: PBL) | - รายงานวิเคราะห์นโยบายและมาตรการ (Assignment)<br>- การนำเสนอผลการวิเคราะห์ | - Rubric การวิเคราะห์ (ความครบถ้วน, ความถูกต้อง, เหตุผล)<br>- คะแนนรายงาน/การนำเสนอ 20% |
| **CLO3** ใช้เครื่องมือและซอฟต์แวร์ด้านความมั่นคงปลอดภัย | - ปฏิบัติการในห้อง Lab (Hands-on Lab)<br>- การทดลองใช้เครื่องมือจริง (Firewall, IDS/IPS, Authentication Tools)<br>- Mini Project | - การปฏิบัติใน Lab<br>- รายงานผลการปฏิบัติ | - Checklist/Performance Rubric<br>- คะแนนปฏิบัติและรายงาน 25% |

| CLO | วิธีการสอน/กิจกรรมการเรียนรู้ | วิธีการวัดผล | เครื่องมือ/เกณฑ์การประเมิน |
|---|---|---|---|
| **CLO4** วิเคราะห์และนำเสนอแนวทางการตอบสนองต่อการบุกรุก และประเด็นทางกฎหมาย/จริยธรรม | - อภิปรายเชิงกลุ่ม (Group Discussion)<br>- วิเคราะห์ข่าว Cybersecurity (Current Issue Analysis)<br>- การโต้วาที (Debate) | - รายงาน/บทความวิเคราะห์<br>- การนำเสนอในชั้นเรียน | - Rubric การนำเสนอ (ความชัดเจน, การใช้เหตุผล, การอ้างอิงกฎหมาย/จริยธรรม)<br>- คะแนนกิจกรรม 15% |
| **CLO5** ประเมินแนวโน้มและประยุกต์ใช้ความรู้ด้าน Cybersecurity เพื่อพัฒนาตนเองและสร้างมูลค่าเพิ่มทางธุรกิจ | - โครงงานกลุ่ม (Project-based Learning)<br>- การใช้ Design Thinking พัฒนา Solution<br>- การสะท้อนคิด (Reflective Learning) | - Project Report & Presentation<br>- การประเมินตนเองและเพื่อนร่วมทีม | - Rubric การทำโครงงาน (นวัตกรรม, ความเป็นไปได้เชิงธุรกิจ, การนำเสนอ)<br>- คะแนนโครงงาน 20% |

## 5. การนำปรัชญาการศึกษาของมหาวิทยาลัยในการจัดการเรียนการสอน (ตามที่มหาวิทยาลัยกำหนด)

| ปรัชญาการศึกษา | กิจกรรมการเรียนการสอน |
|---|---|
| "สร้างคนสู่งาน เชี่ยวชาญเทคโนโลยี มุ่งสู่สังคมการประกอบการ" | 1. สร้างคนสู่งาน (Work-oriented Learning)<br>• ออกแบบกิจกรรมการเรียนรู้ให้เชื่อมโยงกับงานจริง เช่น การวิเคราะห์ภัยคุกคามที่เกิดขึ้นจริง (Case Study) หรือสถานการณ์จำลอง (Simulation/CTF: Capture the Flag)<br>• จัดทำโครงงานที่ให้นักศึกษาออกแบบระบบความปลอดภัยขององค์กรจำลอง ⟶ ทำให้นักศึกษามีประสบการณ์ใกล้เคียงกับงานจริง<br>• ส่งเสริมการเรียนรู้ผ่านการทำงานกลุ่ม (Teamwork) เพื่อฝึกทักษะการทำงานร่วมกัน<br>2. เชี่ยวชาญเทคโนโลยี (Technology Mastery)<br>• จัดให้มี **Lab ปฏิบัติการ** ใช้เครื่องมือด้าน Cybersecurity จริง เช่น Firewall, Wireshark, IDS/IPS, Authentication Tools<br>• ให้นักศึกษาเรียนรู้การใช้ซอฟต์แวร์ป้องกันภัยคุกคามและฝึกแก้ปัญหาที่เกิดขึ้นในระบบเครือข่ายจำลอง<br>• เชื่อมโยงกับมาตรฐานสากล เช่น NIST Cybersecurity Framework, ISO/IEC 27001 เพื่อให้นักศึกษารู้จักแนวทางปฏิบัติระดับโลก<br>3. มุ่งสู่สังคมการประกอบการ (Entrepreneurship-oriented Learning)<br>• บูรณาการ Cybersecurity กับ **บริบทธุรกิจดิจิทัล** เช่น SMEs, E-Commerce, Digital Startup |

| ปรัชญาการศึกษา | กิจกรรมการเรียนการสอน |
|---|---|
| | • ให้นักศึกษาออกแบบ **แผนบริหารจัดการความปลอดภัยไซเบอร์** สำหรับธุรกิจดิจิทัล (Cybersecurity Business Plan)<br>• ส่งเสริมให้นักศึกษาใช้ความรู้ที่เรียนไปสร้าง **Solution/Innovation** ที่สามารถนำไปต่อยอดเชิงพาณิชย์ได้ เช่น Security-as-a-Service |

## 6. การพัฒนาทักษะการเรียนรู้ตลอดชีวิต Life-long Learning (LLL) ของหลักสูตร (ถ้ามี)

| ทักษะ LLL | กิจกรรมการเรียนการสอน | วิธีการประเมินผล |
|---|---|---|
| 1. การแสวงหาความรู้ด้วยตนเอง (Self-directed Learning) | - มอบหมายการค้นคว้าข้อมูลด้าน Cybersecurity จากฐานข้อมูลออนไลน์/งานวิจัยใหม่<br>- การเรียนรู้ผ่าน e-Learning / MOOC<br>- การอ่านบทความวิชาการและสรุปผล | - การบ้าน/รายงานสรุป (Assignment)<br>- แบบทดสอบออนไลน์ (Quiz)<br>- การสะท้อนคิด (Reflective Journal) |
| 2. การคิดวิเคราะห์และการแก้ปัญหา (Critical Thinking & Problem-solving) | - วิเคราะห์กรณีศึกษา (Case Study) ด้านภัยคุกคามไซเบอร์<br>- การเรียนรู้แบบใช้ปัญหา (Problem-based Learning: PBL)<br>- การแก้ปัญหาโจทย์ Hackathon/CTF | - การนำเสนอแนวทางแก้ปัญหา (Presentation)<br>- Rubric การวิเคราะห์กรณีศึกษา<br>- ผลงานการแก้โจทย์แข่งขัน |
| 3. การเรียนรู้จากการปฏิบัติจริง (Experiential Learning) | - Lab ปฏิบัติการใช้เครื่องมือ Cybersecurity<br>- โครงงานกลุ่มด้านการรักษาความปลอดภัยไซเบอร์<br>- การฝึกงาน/โครงการบริการวิชาการกับชุมชน/ธุรกิจ | - การสอบปฏิบัติ (Lab Test)<br>- Rubric โครงงานกลุ่ม<br>- การประเมินจากแหล่งฝึกงาน |
| 4. การสื่อสารและการทำงานร่วมกัน (Communication & Collaboration) | - การทำงานกลุ่ม (Team Project)<br>- การอภิปราย/โต้วาทีประเด็นกฎหมายและจริยธรรมไซเบอร์<br>- การนำเสนอรายงานทั้งภาษาไทยและอังกฤษ | - Rubric การนำเสนอ (Presentation Rubric)<br>- Peer Evaluation (การประเมินเพื่อนร่วมทีม)<br>- คะแนนการมีส่วนร่วมในชั้นเรียน |
| 5. การปรับตัวต่อการเปลี่ยนแปลงและนวัตกรรม (Adaptability & Innovation) | - การติดตามข่าวสาร Cybersecurity Trends และ Threat Intelligence<br>- การออกแบบนวัตกรรมความปลอดภัยเชิงธุรกิจ (Cybersecurity Solution)<br>- การใช้ Design Thinking | - รายงาน/บทความวิเคราะห์แนวโน้ม<br>- Rubric การสร้างนวัตกรรม/โครงงาน<br>- การประเมินการสะท้อนคิด (Reflection Report) |

**7. การพัฒนาทักษะการเป็นผู้ประกอบการของหลักสูตร (ถ้ามี)**

ไม่มี

**8. เกณฑ์การประเมินผลแบบอื่น ๆ (เฉพาะ CLOs ที่จำเป็น แบบ Rubric Score หรืออื่นๆ)**

ไม่มี

**9. แผนการประเมินผลการเรียนรู้**

| CLO | กิจกรรมที่ | วิธีการประเมินผล | สัปดาห์ที่ประเมิน | สัดส่วน (%) |
|---|---|---|---|---|
| **CLO1** อธิบายและจำแนกหลักการพื้นฐาน ประเภทของภัยคุกคามและกลไกการโจมตีไซเบอร์ | - แบบทดสอบย่อย (Quiz)<br>- การตอบคำถาม/อภิปรายในชั้นเรียน | - Quiz (ออนไลน์/ในชั้นเรียน)<br>- Participation Rubric | 1–4 | 15% |
| **CLO2** วิเคราะห์และประยุกต์ใช้นโยบาย กลไกการป้องกัน และการควบคุมการเข้าถึง | - กรณีศึกษา (Case Study)<br>- รายงานกลุ่มวิเคราะห์นโยบาย | - Assignment/Report Rubric<br>- การนำเสนอในชั้นเรียน | 5–7 | 20% |
| **CLO3** ใช้เครื่องมือและซอฟต์แวร์ด้านความมั่นคงปลอดภัย | - Lab ปฏิบัติการ Firewall, IDS/IPS, Authentication Tools<br>- Lab Test | - Checklist/Performance Rubric<br>- Lab Report | 6–10 | 20% |
| **CLO4** วิเคราะห์และนำเสนอแนวทางการตอบสนองต่อการบุกรุกและประเด็นทางกฎหมาย/จริยธรรม | - การอภิปราย/โต้วาที<br>- วิเคราะห์ข่าว Cybersecurity<br>- นำเสนอรายงาน | - Rubric การนำเสนอ (ชัดเจน, เหตุผล, อ้างอิงกฎหมาย)<br>- Peer Evaluation | 11–13 | 15% |
| **CLO5** ประเมินแนวโน้มและประยุกต์ใช้ความรู้ด้าน Cybersecurity เพื่อพัฒนาตนเองและสร้างมูลค่าเพิ่มทางธุรกิจ | - โครงงานกลุ่ม (Cybersecurity Project)<br>- Project Presentation | - Project Report Rubric<br>- Presentation Rubric<br>- Self & Peer Assessment | 14–16 | 20% |
| – | **สอบกลางภาค** (ทฤษฎี + ปฏิบัติ) | - Written Exam + Lab Exam | 8 | 10% |

**10. การประเมินผลรายวิชา**

| ระดับคะแนน (GRADE) | ค่าระดับคะแนนต่อหน่วยกิต | ผลการศึกษา | ช่วงคะแนน |
|---|---|---|---|
| ก หรือ A | 4.0 | ดีเยี่ยม (Excellent) | 80 ขึ้นไป |
| ข+ หรือ B+ | 3.5 | ดีมาก (Very Good) | 75-79 |
| ข หรือ B | 3.0 | ดี (Good) | 70-74 |
| ค+ หรือ C+ | 2.5 | ดีพอใช้ (Fair Good) | 65-69 |
| ค หรือ C | 2.0 | พอใช้ (Fair) | 60-64 |
| ง+ หรือ D+ | 1.5 | อ่อน (Poor) | 55-59 |
| ง หรือ D | 1.0 | อ่อนมาก (Very Poor) | 50-54 |
| จ หรือ F | 0.0 | ตก (Fall) | 0-49 |

# หมวดที่ 3 แผนการจัดการเรียนรู้

## 1. แผนการจัดการเรียนรู้รายสัปดาห์

| สัปดาห์ที่ | หัวข้อ/รายละเอียด | จำนวนชั่วโมง | | ผลลัพธ์การเรียนรู้รายบทเรียน (LLO) | กิจกรรมการเรียนรู้/สื่อการสอน | ความสอดคล้องกับ CLO |
|---|---|---|---|---|---|---|
| | | ทฤษฎี | ปฏิบัติ | | | |
| 1 | **บทนำสู่ความมั่นคงปลอดภัยไซเบอร์**<br>- ความหมายและความสำคัญของ Cyber Security<br>- ภาพรวมภัยคุกคามและผลกระทบ | 2 | 2 | LLO1: อธิบายความหมายและความสำคัญของ Cyber Security ได้<br>LLO2: จำแนกประเภทภัยคุกคามพื้นฐานได้ | - การบรรยาย + การอภิปราย<br>- Video Case: Global Cyber Attack<br>- Pre-test | CLO 1 |
| 2 | **แนวคิดพื้นฐานด้านความมั่นคงสารสนเทศ** (CIA Triad)<br>- Confidentiality, Integrity, Availability<br>- แนวคิด Risk, Threat, Vulnerability | 2 | 2 | LLO3: อธิบายองค์ประกอบ CIA Triad และการจัดการความเสี่ยงได้ | - Lecture + Mindmap<br>- แบบฝึกการระบุ Threat & Vulnerability | CLO 1 |
| 3 | **ประเภทของภัยคุกคามไซเบอร์และรูปแบบการโจมตี**<br>- Malware, Phishing, DoS/DDoS, Ransomware, Social Engineering | 2 | 2 | LLO4: จำแนกประเภทและวิเคราะห์วิธีการโจมตีไซเบอร์ได้ | - Case Study: Malware Evolution<br>- Quiz-1 | CLO 1 |
| 4 | **นโยบายและมาตรการความมั่นคง**<br>- Security Policy & Governance<br>- Risk Management Framework | 2 | 2 | LLO5: อธิบายโครงสร้างนโยบายและมาตรการด้านความมั่นคงสารสนเทศได้ | - Lecture + ตัวอย่าง Policy<br>- Workshop วิเคราะห์ Policy ขององค์กร | CLO 2 |
| 5 | **การควบคุมการเข้าถึง (Access Control)**<br>- Authentication, Authorization | 2 | 2 | LLO6: อธิบายและประยุกต์ใช้วิธีการควบคุมการเข้าถึงได้ | - Lecture + Lab: Basic Access Control | CLO 2, CLO 3 |

| สัปดาห์ที่ | หัวข้อ/รายละเอียด | จำนวนชั่วโมง | | ผลลัพธ์การเรียนรู้รายบทเรียน (LLO) | กิจกรรมการเรียนรู้/สื่อการสอน | ความสอดคล้องกับ CLO |
|---|---|---|---|---|---|---|
| | | ทฤษฎี | ปฏิบัติ | | | |
| | - Role-based & Rule-based Access Control | | | | | |
| 6 | **การยืนยันตัวตนและการควบคุมทางชีวภาพ (Biometric Control)**<br>- MFA, OTP, Biometric | 2 | 2 | LLO7: ใช้เครื่องมือสำหรับการพิสูจน์และยืนยันตัวตนได้ | - Lab Practice: MFA & Biometric<br>- Quiz-2 | CLO 3 |
| 7 | **การควบคุมระบบเครือข่ายและอุปกรณ์**<br>- Network Security Devices: Firewall, IDS/IPS<br>- Endpoint Protection | 2 | 2 | LLO8: ใช้เครื่องมือ Network Security ป้องกันภัยคุกคามได้ | - Lab Practice: Firewall Rules<br>- Case Study | CLO 3 |
| 8 | สอบกลางภาคเรียน | | | | | |
| 9 | การตรวจจับและป้องกันการบุกรุก (Intrusion Detection & Prevention) | 2 | 2 | LLO9: วิเคราะห์และตั้งค่าระบบ IDS/IPS ได้ | - Lab Practice: IDS/IPS Demo<br>- Workshop: Threat Scenario | CLO 4 |
| 10 | การบริหารจัดการเหตุการณ์ (Incident Management) | 2 | 2 | LLO10: อธิบายขั้นตอนการตอบสนองต่อเหตุการณ์ (IR Process) ได้ | - Role-play: Incident Response Team<br>- Reflection Discussion | CLO 4 |
| 11 | Digital Forensics & Log Analysis | 2 | 2 | LLO11: วิเคราะห์หลักฐานทางดิจิทัลและรายงานผลได้ | - Lab: Log Analysis<br>- Mini Project Task | CLO 3, CLO 4 |
| 12 | **ประเด็นกฎหมายด้านความมั่นคงและคุ้มครองข้อมูล**<br>- PDPA, Computer Crime Act | 2 | 2 | LLO12: อธิบายข้อกำหนดทางกฎหมายและจริยธรรมที่เกี่ยวข้องได้ | - Debate: Security vs Privacy<br>- Case Study: Legal Issues | CLO 4 |
| 13 | จริยธรรมด้านความมั่นคงและความเป็นส่วนตัว | 2 | 2 | LLO13: นำเสนอแนวทางการประยุกต์ใช้จริยธรรมในวิชาชีพได้ | - Flipped Learning: Reading & Discussion | CLO 4 |

| สัปดาห์ที่ | หัวข้อ/รายละเอียด | จำนวนชั่วโมง | | ผลลัพธ์การเรียนรู้รายบทเรียน (LLO) | กิจกรรมการเรียนรู้/สื่อการสอน | ความสอดคล้องกับ CLO |
|---|---|---|---|---|---|---|
| | | ทฤษฎี | ปฏิบัติ | | | |
| | | | | | - Group Presentation | |
| 14 | **แนวโน้มเทคโนโลยีความมั่นคง (Trends & Future)**<br>- Cloud Security, Zero Trust, AI in Cyber Security | 2 | 2 | LLO14: วิเคราะห์และอธิบายแนวโน้มเทคโนโลยีในอนาคตได้ | - Research Activity<br>- Peer Sharing | CLO 5 |
| 15 - 16 | Workshop สรุปองค์ความรู้แบบบูรณาการ | 2 | 6 | LLO15: ประยุกต์ใช้ความรู้และทักษะจากบทเรียนแก้ไขสถานการณ์จริงได้ | - Simulation Game: Cyber Attack & Response<br>- Presentation | CLO 2, CLO 3, CLO 4 |
| 17 | สอบปลายภาคเรียน | | | | | |

## 2. หนังสือ ตำรา สื่อ ทรัพยากรประกอบการเรียนการสอน

จตุชัย แพงจันทร์. (2559). Master's in security (พิมพ์ครั้งที่ 3). นนทบุรี: ไอทีซีฯ.

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (n.d.). กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ = Cyber Security Law [หนังสืออิเล็กทรอนิกส์]. https://dg.th/byzgvo-t9sq

พงษ์พิสิฐ วุฒิพิษณุโชติ, เกียรติศักดิ์ จันทร์ลอย, & สมชิต กิจทองพูล. (n.d.). Cyber Security: อย่าปล่อยให้ใครมาใช้ข้อมูลคุณ. หมวดหมู่: จิตวิทยาและการพัฒนาตนเอง.

## 3. แหล่งเรียนรู้เพิ่มเติม

1. NCSA Mooc (https://ncsec.ncsa.or.th/ncsa-mooc/)
2. TPQI E-Training (https://e-training.tpqi.go.th/)
3. TDGA (Thailand Digital Government Academy) (https://e-learning.dga.or.th/xlms_ega/portal/ )
4. https://www.netacad.com/

## หมวดที่ 4 การประเมินและปรับปรุงการดำเนินการของรายวิชา

**1. การประเมินประสิทธิผลของรายวิชาโดยผู้เรียน**

1. การประเมินการสอนของอาจารย์โดยนักศึกษา
2. การสนทนากลุ่มระหว่างผู้สอนและผู้เรียน
3. แบบสอบถามความพึงพอใจต่อการเรียนการสอน
4. การสะท้อนคิดของนักศึกษาต่อวิธีการเรียนรู้

**2. การประเมินกระบวนการจัดการเรียนการสอนโดยอาจารย์ผู้สอน**

1. การสังเกตการณ์สอนโดยผู้ร่วมสอน
2. ผลการเรียนของนักศึกษา
3. การทวนสอบผลการประเมินการเรียนรู้
4. วิเคราะห์ข้อสอบและคุณภาพของเครื่องมือวัดผล

**3. การทวนสอบผลลัพธ์การเรียนรู้ของนักศึกษาในรายวิชา**

1. การทวนสอบการให้คะแนนจากการสุ่มตรวจผลงานของนักศึกษาโดยอาจารย์อื่น
2. การตั้งคณะกรรมการในสาขาวิชา ตรวจสอบผลการประเมินการเรียนรู้ของนักศึกษา
3. การทวนสอบโดยใช้ข้อสอบหรือการสอบปากเปล่า
4. การสอบถามนักศึกษาเกี่ยวกับความสอดคล้องของข้อสอบกับเนื้อหาที่เรียน

**4. การดำเนินการทบทวนและการวางแผนปรับปรุงประสิทธิผลของรายวิชา**

1. ปรับปรุงรายวิชาทุก 3-5 ปี หรือตามข้อเสนอแนะและผลการทวนสอบ
2. ปรับปรุงเนื้อหาให้ทันสมัยและสอดคล้องกับความต้องการของตลาดแรงงาน
3. นำผลการประเมินจาก RMUTR 5 มาประกอบการพิจารณาปรับปรุงการเรียนการสอน

**อาจารย์ผู้รับผิดชอบรายวิชา** **อาจารย์ นพดล สายคติกรณ์**

ลงชื่อ.....

วันที่รายงาน.....

**อาจารย์ผู้รับผิดชอบหลักสูตร** **อาจารย์ นพดล สายคติกรณ์**

ลงชื่อ.....

วันที่รายงาน.....

**หัวหน้าสาขาวิชา** **ผู้ช่วยศาสตราจารย์ พัชราภรณ์ ชัยพัฒนเมธี**

ลงชื่อ.....

วันที่รายงาน.....