GENERAL EDUCATION, KMITL

COURSE SYLLABUS

รหัสวิชา	90642205	**ชื่อวิชา**	ภัยไซเบอร์และการรักษาความปลอดภัย (Cyber Threats and Security)				
หน่วยกิต	3 (3-0-6)	**ภาคการศึกษา**	2569	**กลุ่มเรียน**	xxx	**วัน-เวลาเรียน**	จันทร์ เวลา 16.30-19.30 น. อังคาร เวลา 13.00-16.00 น.
คำอธิบายรายวิชา ภาษาไทย	ศึกษาและวิเคราะห์ภาพรวมของภัยคุกคามทางไซเบอร์ในยุคดิจิทัล ประเภทของอาชญากรรมคอมพิวเตอร์ วิศวกรรมสังคม (Social Engineering) ภัยคุกคามจากมัลแวร์ และรูปแบบการโจมตีระบบ ศึกษากลไกการป้องกัน การจัดการอัตลักษณ์ดิจิทัล การรักษาความปลอดภัยของข้อมูล (CIA Triad) ตลอดจนกฎหมายที่เกี่ยวข้อง เช่น พ.ร.บ.คอมพิวเตอร์ และ PDPA เพื่อสร้างความตระหนักรู้และทักษะในการรักษาความปลอดภัยไซเบอร์ระดับบุคคลและองค์กร						
คำอธิบายรายวิชา ภาษาอังกฤษ	Study and analyze the overview of cyber threats in the digital age, types of computer crimes, social engineering, malware threats, and various system attack vectors. Explore defense mechanisms, digital identity management, and the principles of information security (CIA Triad). The course also covers relevant regulations and ethics, including the computer-Related Crime Act and the Personal Data Protection Act (PDPA), to cultivate cybersecurity awareness and essential skills for individuals and organizations.						
อาจารย์ผู้รับผิดชอบรายวิชา	รศ.ดร.สมเกียรติ ตันติวงศ์วาณิช และ ผศ.ดร.กฤษฎา บุศรา						
อาจารย์ผู้สอน	รศ.ดร.สมเกียรติ ตันติวงศ์วาณิช และ ผศ.ดร.กฤษฎา บุศรา						
ผู้ช่วยสอน (ถ้ามี)							
ช่องทางและวันเวลาให้คำปรึกษา	Facebook และ/หรือ Line	**สอนโดยใช้ภาษา**	☒ ภาษาไทย ☐ ภาษาอังกฤษ ☐ อื่นๆ โปรดระบุ				
เว็บไซต์หรือช่องทางการเรียนออนไลน์ (ถ้ามี)	MS Team ของกลุ่มเรียน						

ผลการเรียนรู้ของรายวิชา (Course Learning Outcome)

หลังจากที่นักศึกษาได้ศึกษารายวิชานี้แล้ว คาดหวังว่า

CLO 1: วิเคราะห์และแยกแยะ รูปแบบภัยคุกคามทางไซเบอร์ มัลแวร์ และกลโกงวิศวกรรมสังคม (Social Engineering) ในชีวิตประจำวันได้อย่างถูกต้อง

CLO 2: วางแผนและกำหนดขั้นตอน การตอบสนอง ประเมินความเสี่ยง และแก้ไขสถานการณ์เมื่อเผชิญเหตุภัยคุกคามทางไซเบอร์ (Incident Response) ทั้งในระดับบุคคลและองค์กร

CLO 3: ปฏิบัติตาม กฎหมายที่เกี่ยวข้อง (เช่น พ.ร.บ.คอมพิวเตอร์ และ PDPA) พร้อมทั้งแสดงออกถึงความซื่อสัตย์สุจริต มีวินัย และความรับผิดชอบต่อตนเองและผู้อื่นในการใช้งานโลกดิจิทัล

CLO 4: สื่อสารและถ่ายทอด วิธีการป้องกันภัยไซเบอร์ แนวคิดความปลอดภัย และแนวทางการปฏิบัติตนให้ผู้อื่นเข้าใจง่ายและตระหนักรู้ได้อย่างมีประสิทธิภาพ

CLO 5: ประยุกต์ใช้และตั้งค่า เครื่องมือดิจิทัลและเทคโนโลยีความปลอดภัย (เช่น MFA, Encryption, Privacy Settings) เพื่อสร้างแผนปฏิบัติการความปลอดภัยส่วนบุคคล (Personal Roadmap) ได้อย่างถูกต้องตามเกณฑ์มาตรฐาน

ผลการเรียนรู้ของหมวดวิชาศึกษาทั่วไป (GE-LO)

GE-LO	ค่าน้ำหนัก
☒ **GE-LO**-1 การคิดวิเคราะห์และการคิดอย่างมีวิจารณญาณ (Analytical and Critical Thinking)	2
☒ **GE-LO**-2 การแก้ปัญหาเชิงซับซ้อน (Complex Problem Solving)	4
☐ **GE-LO**-3 การคิดสร้างสรรค์ (Creativity)	-
☐ **GE-LO**-4 ความสัมพันธ์กับผู้อื่น (Interpersonal Skills)	-
☒ **GE-LO**-5 ความซื่อสัตย์และความพากเพียรพยายาม (Integrity and Perseverance)	1
☐ **GE-LO**-6 การเรียนรู้เชิงรุกและการใฝ่รู้ (Active Learning and Learning Strategies)	-
☐ **GE-LO**-7 ความอดทน ยืดหยุ่น และฟื้นตัวจากสภาวะความเครียด (Resilience, Stress Tolerance and Flexibility)	-
☐ **GE-LO**-8 การเป็นผู้นำและผู้เปลี่ยนแปลงสังคม (Leadership and Social Influence)	-
☒ **GE-LO**-9 การสื่อสารอย่างมีประสิทธิภาพ (Communication)	2
☐ **GE-LO**-10 การเป็นผู้ประกอบการและการลงทุน (Entrepreneurship and Startup)	-
☒ **GE-LO**-11 การรู้เท่าทันดิจิทัลและการผลิตสื่อดิจิทัล (Digital Quotient Literacy and Digital Media Production)	6
ค่าน้ำหนักรวม	**15**

แผนการเรียน

สัปดาห์ที่	หัวข้อ/หัวข้อย่อย	วิธีการเรียน/กิจกรรมในชั้นเรียน	หมายเหตุ
1	ชีวิตในโลกดิจิทัลกับภัยใกล้ตัว - ทำไมเราทุกคนถึงตกเป็นเป้าหมายของมิจฉาชีพ? - ข่าวเด่นและกรณีศึกษาการถูกหลอกลวงในปัจจุบัน	บรรยายร่วมกับการชวนคุย แลกเปลี่ยนประสบการณ์ภัยใกล้ตัวของนักศึกษาในชีวิตประจำวัน - [เริ่มเช็คชื่อและประเมินพฤติกรรมในชั้นเรียน: เก็บคะแนนต่อเนื่องสัปดาห์ที่ 1-15 รวมเต็ม 4 คะแนน]	
2	รู้จักมิจฉาชีพและแฮกเกอร์ - แฮกเกอร์คือใคร? เขาหาข้อมูลเราจากไหน? - ส่องพฤติกรรมการหลอกลวงที่ระบาดในหมู่วัยรุ่น	บรรยายประกอบการดูคลิปสั้นกรณีศึกษาจริงเรื่องการแกะรอยและพฤติกรรมของมิจฉาชีพ - [เช็คชื่อและประเมินพฤติกรรมในชั้นเรียนต่อเนื่อง]	
3	วิศวกรรมสังคม: กลโกงและการหลอกลวงออนไลน์ - แก๊งคอลเซ็นเตอร์, ลิงก์ปลอม (Phishing), SMS ล่อลวง - จิตวิทยาที่มิจฉาชีพใช้ทำให้อีกฝ่ายกลัวหรือโลภ	บรรยาย พร้อมทำกิจกรรม Workshop ในห้อง: "เกมจับผิดข้อความลวง และอีเมลปลอม" - [เช็คชื่อและประเมินพฤติกรรมในชั้นเรียนต่อเนื่อง]	
4	ภัยร้ายจากมัลแวร์และไวรัส - ไวรัส, มัลแวร์เรียกค่าไถ่ (Ransomware), แอปฯ ดูดเงิน - สัญญาณเตือนเมื่อมือถือหรือคอมพิวเตอร์ติดมัลแวร์	บรรยาย และสาธิตวิธีตรวจสอบลิงก์หรือไฟล์น่าสงสัยด้วยเว็บไซต์ง่าย ๆ (เช่น VirusTotal) - [เช็คชื่อและประเมินพฤติกรรม in-class participation ต่อเนื่อง]	
5	ความปลอดภัยเมื่อเชื่อมต่ออินเทอร์เน็ต - อันตรายจาก Wi-Fi สาธารณะฟรี และการหลอกให้โหลดแอปฯ - สังเกตความปลอดภัยของเว็บไซต์ (https:// กับ http://)	บรรยายสรุปแนวทางการป้องกันตัวเมื่อใช้งานอินเทอร์เน็ตนอกสถานที่และสรุปบทเรียนพาร์ทภัยไซเบอร์ - [ส่งงานและประเมินผล: ใบงานวิเคราะห์ภัยไซเบอร์รายบุคคล ชิ้นที่ 1 — คะแนนเต็ม 4 คะแนน	

สัปดาห์ที่	หัวข้อ/หัวข้อย่อย	วิธีการเรียน/กิจกรรมในชั้นเรียน	หมายเหตุ
6	หลักการรักษาความปลอดภัยข้อมูลแบบเข้าใจง่าย - ความลับ (Confidentiality), ความถูกต้อง (Integrity), ความพร้อมใช้ (Availability) ของข้อมูลส่วนตัว	- บรรยาย, ยกตัวอย่างเรื่องใกล้ตัว เช่น การตั้งรหัสผ่าน, การแชร์โลเคชั่น - [เช็คชื่อและประเมินพฤติกรรมในชั้นเรียนต่อเนื่อง]	
7	การตั้งค่าความปลอดภัยและบัญชีส่วนบุคคล - การตั้งรหัสผ่านให้ปลอดภัยแต่จำง่าย (Strong Password) - ระบบยืนยันตัวตนสองชั้น (MFA/2FA) ที่ทุกคนต้องเปิดใช้	- บรรยาย, Workshop ทุกคนเปิดระบบ 2FA ใน Facebook/IG/Gmail พร้อมกัน - [เช็คชื่อและประเมินพฤติกรรมในชั้นเรียนต่อเนื่อง]	
8	การปกป้องข้อมูลและการสำรองข้อมูล - การเข้ารหัสไฟล์งานเบื้องต้น และการแชร์ไฟล์บน Cloud - วิธีป้องกันข้อมูลหายเมื่อโทรศัพท์มือถือสูญหาย	- บรรยายสรุปทบทวนเนื้อหาครึ่งแรกของภาคการศึกษา - [ทดสอบย่อย: ทำแบบทดสอบวัดความรู้พื้นฐาน (Quiz) ในห้องเรียน — คะแนนเต็ม 8 คะแนน]	
9	กฎหมายไซเบอร์ที่ควรรู้สำหรับวัยรุ่น - แชร์ข้อมูลแบบไหนเสี่ยงติดคุก? (พ.ร.บ.คอมพิวเตอร์) - ถ่ายรูป/โพสต์รูปอย่างไรไม่ให้ละเมิดสิทธิ์ผู้อื่น (PDPA)	- บรรยาย, ชวนวิเคราะห์เคสการโพสต์ดราม่าและการละเมิดสิทธิ์ในโซเชียล - [เช็คชื่อและประเมินพฤติกรรมในชั้นเรียนต่อเนื่อง]	
10	จริยธรรมดิจิทัลและการอยู่ร่วมกันบนออนไลน์ - มารยาทในโลกออนไลน์, ปัญหา Cyberbullying - หน้าที่และความรับผิดชอบเมื่อเราพบเห็นการหลอกลวง	- บรรยาย และทำกิจกรรมระดมสมองกลุ่มย่อยหัวข้อ "แนวทางการรับมือเมื่อโดนบูลลี่ออนไลน์" - [ส่งงานและประเมินผล: ใบงานวิเคราะห์ภัยไซเบอร์รายบุคคล ชิ้นที่ 2 — คะแนนเต็ม 4 คะแนน]	

สัปดาห์ที่	หัวข้อ/หัวข้อย่อย	วิธีการเรียน/กิจกรรมในชั้นเรียน	หมายเหตุ
11	การประเมินและการลดความเสี่ยงส่วนบุคคล - การสำรวจจุดเสี่ยงของตัวเองในการใช้เทคโนโลยี - การวางแผนเพื่อไม่ให้ตัวเองตกเป็นเหยื่อ (Risk Assessment)	- บรรยาย และฝึกปฏิบัติการประเมินจุดเสี่ยงรายกลุ่มจากแบบทดสอบกรณีศึกษา - [เช็คชื่อและประเมินพฤติกรรมในชั้นเรียนต่อเนื่อง]	
12	วิธีเอาตัวรอดและแก้ปัญหาเมื่อถูกแฮก - ขั้นตอนแรกที่ต้องทำเมื่อรู้ว่าโดนโกงเงิน โดนแฮกเฟซบุ๊ก - ช่องทางการแจ้งความออนไลน์ (ศูนย์ AOC 1441) และการเก็บหลักฐาน	- บรรยาย และทำกิจกรรม Workshop: ซ้อมรวบรวมแคปหลักฐานและจำลองการแจ้งความออนไลน์ - [เช็คชื่อและประเมินพฤติกรรมในชั้นเรียนต่อเนื่อง]	
13	การจัดทำแผนปฏิบัติการความปลอดภัยส่วนบุคคล - แนะนำกรอบการสร้างคู่มือเอาตัวรอด (Personal Roadmap) - มอบหมายและให้คำปรึกษาโครงงานกลุ่มปลายภาค	"ชี้แจงโจทย์สถานการณ์จำลอง (Scenario-based) เกี่ยวกับภัยคุกคามไซเบอร์ พร้อมทั้งอธิบายเกณฑ์รูบริค (Rubric) การให้คะแนน โครงงานกลุ่มปลายภาค: ชิ้นงานสื่อดิจิทัล (คะแนนเต็ม 16 คะแนน) กิจกรรมกลุ่ม (Group Work): นักศึกษาร่วมกันระดมสมอง ออกแบบสตอรี่บอร์ด (Storyboard) หรือร่างเนื้อหาเพื่อเตรียมจัดทำชิ้นงานสื่อดิจิทัลเตือนภัยไซเบอร์ (เช่น คลิปสั้นรณรงค์ หรือ แผนภาพอินโฟกราฟิก) โดยมีอาจารย์ให้คำปรึกษาแนะนำในชั้นเรียน" โดยกำหนดให้นักศึกษาไปพัฒนาชิ้นงานกลุ่มให้สมบูรณ์นอกเวลาเรียน และส่งมอบไฟล์ชิ้นงานผ่านระบบออนไลน์ก่อนเข้าสู่การเรียนในสัปดาห์ที่ 14	

สัปดาห์ที่	หัวข้อ/หัวข้อย่อย	วิธีการเรียน/กิจกรรมในชั้นเรียน	หมายเหตุ
14	การสื่อสารเพื่อสร้างความตระหนักรู้ (Awareness) - เทคนิคการเล่าเรื่องภัยไซเบอร์ให้ครอบครัวและเพื่อนฟังได้ง่าย ๆ	กิจกรรมการเรียนรู้และกระบวนการในชั้นเรียน: "1. อาจารย์ให้ข้อเสนอแนะสะท้อนกลับ (Feedback) จากชิ้นงานสื่อดิจิทัลที่นักศึกษาส่งผ่านระบบออนไลน์ "หมายเหตุ:ครบกำหนดส่งงานและบันทึกการประเมิน: โครงงานกลุ่มปลายภาค: ชิ้นงานสื่อดิจิทัล (คะแนนเต็ม 16 คะแนน) (จากสัปดาห์ที่ 13) 2. กิจกรรมกลุ่ม (Workshop): นักศึกษานำโจทย์ภัยคุกคามที่ปรากฏในสื่อนั้น มาขยายผลร่วมกันคิด วิเคราะห์ วางลำดับขั้นตอนการตอบสนองต่อเหตุการณ์ (Incident Response Plan) เพื่อแก้ไขปัญหาเชิงซับซ้อนตามสถานการณ์จำลอง" การวัดและประเมินผล : กำหนดให้นักศึกษาไปพัฒนาชิ้นงานกลุ่ม “การแก้ปัญหา” ให้สมบูรณ์นอกเวลาเรียน และส่งมอบไฟล์ชิ้นงานผ่านระบบออนไลน์ก่อนเข้าสู่การเรียนในสัปดาห์ที่ 15 (คะแนนเต็ม 16 คะแนน)	

สัปดาห์ที่	หัวข้อ/หัวข้อย่อย	วิธีการเรียน/กิจกรรมในชั้นเรียน	หมายเหตุ
15	การนำเสนอโครงงานปลายภาค (Final Presentation) - นำเสนอผลงานกลุ่ม (คลิปสั้นเตือนภัย หรือแผนภาพอินโฟกราฟิก) และตอบข้อซักถาม	"หมายเหตุ:ครบกำหนดส่งงานและบันทึกการประเมิน: โครงงานกลุ่มปลายภาค: ชิ้นงานการแก้ปัญหา (คะแนนเต็ม 16 คะแนน) (จากสัปดาห์ที่ 14) กิจกรรมการเรียนรู้และการประเมินผล: นักศึกษานำเสนอผลงานกลุ่ม (Cybersecurity Pitching) อธิบายสรุปขั้นตอนการแก้ปัญหาและสื่อสารความเสี่ยง • ส่งงานและบันทึกการประเมิน: โครงงานกลุ่มปลายภาค: การนำเสนอผลงาน (คะแนนเต็ม 8 คะแนน)	

แผนการวัดผล

กิจกรรมการวัดผล	ค่าน้ำหนัก	คะแนนเต็ม	ช่วงเวลา	หมายเหตุ
1. การมีส่วนร่วมและการเข้าเรียน	1	4	สัปดาห์ที่ 1 - 15	เช็คชื่อต้นคาบด้วยระบบ QR-Code / ประเมินความรับผิดชอบและการรักษากฎกติกาจริยธรรมในห้องเรียน
2. ใบงานวิเคราะห์ภัยไซเบอร์รายบุคคล	2	8	สัปดาห์ที่ 5 และสัปดาห์ที่ 10	ชิ้นที่ 1 (สัปดาห์ 5): แคปหน้าจอข้อความมิจฉาชีพ/Phishing แล้วเขียนจุดสังเกต ชิ้นที่ 2 (สัปดาห์ 10): วิเคราะห์เคสการแชร์ข้อมูลบนโซเชียลที่เสี่ยงละเมิดกฎหมาย/PDPA
3. แบบทดสอบวัดความรู้ (Quiz)	2	8	สัปดาห์ที่ 8	ทำข้อสอบปรนัย (กากบาท/เลือกตอบ) เน้นความรู้ทั่วไปเรื่องรูปแบบมัลแวร์ การระบุขั้นตอนการกู้คืนบัญชี (Incident Response) และวิธีตั้งค่าระบบความปลอดภัยพื้นฐาน
4. โครงงานกลุ่มปลายภาค: ชิ้นงานสื่อดิจิทัล	4	16	สัปดาห์ที่ 13	พัฒนาสื่อความรู้ในรูปแบบที่ถนัดและเข้าใจง่าย เช่น คลิปสั้นรณรงค์เตือนภัย (TikTok/Reels) หรือแผนภาพอินโฟกราฟิกเตือนภัยไซเบอร์ในชีวิตประจำวัน
5. โครงงานกลุ่มปลายภาค: การแก้ปัญหา	4	16	สัปดาห์ที่ 13 - 15	ประเมินกระบวนการคิดเชิงระบบในการแก้ไขปัญหาเมื่อเผชิญเหตุภัยคุกคามไซเบอร์ (Incident Response) โดยพิจารณาจากการจัดลำดับขั้นตอนการแก้ปัญหา การวิเคราะห์ประเมินเพื่อลดความเสี่ยงอย่างเป็นขั้นตอน และการเลือกใช้มาตรการทางเทคนิคหรือแนวปฏิบัติที่ถูกต้องตามหลักจริยธรรมและกฎหมาย เพื่อจำกัดความเสียหายของระบบหรือข้อมูลในสถานการณ์จำลองที่ได้รับมอบหมาย
6. โครงงานกลุ่มปลายภาค: การนำเสนอผลงาน	2	8	สัปดาห์ที่ 15	การนำเสนอผลงานกลุ่มแบบปากเปล่า (Oral Presentation) เน้นเทคนิคการสื่อสารที่ย่อยเรื่องยากให้เข้าใจง่าย และการตอบข้อซักถามในการวิเคราะห์ประเมินความเสี่ยงใกล้ตัว
รวม	**15**	**60**		

เกณฑ์การประเมิน

☐ **อิงกลุ่ม**								
☒ **อิงเกณฑ์**								
เกรด (แสดงเฉพาะอิงเกณฑ์)	A	B+	B	C+	C	D+	D	F
ช่วงคะแนน (เต็ม 60 คะแนน)	57-60	49-56.9	41-48.9	34-40.9	27-33.9	21-26.9	15-20.9	0-14.9
☐ **ผ่าน / ไม่ผ่าน (S/U)**								
เกรด	S				U			
ช่วงคะแนน (เต็ม 60 คะแนน)	30-60				0-29.9			

เกณฑ์การให้คะแนนตามผลการเรียนรู้

กิจกรรมการวัดผล	ทักษะ	ค่าน้ำหนัก	ระดับคะแนน			
			4 (ดีมาก)	3 (ดี)	2 (พอใช้)	1 (ควรปรับปรุง)
1. การมีส่วนร่วมและการเข้าเรียน	GE-LO-5	1	เข้าเรียนตรงเวลาทุกครั้ง ไม่ขาดเรียนเลย หรือขาดไม่เกิน 1 ครั้ง (โดยมีเหตุจำเป็นและแจ้งล่วงหน้า)	เข้าเรียนสม่ำเสมอ ตรงเวลาเป็นส่วนใหญ่ และขาดเรียนไม่เกิน 2 ครั้ง	เข้าเรียนสายบางครั้ง หรือขาดเรียนไม่เกิน 3 ครั้ง (ตามเกณฑ์ขั้นต่ำของรายวิชา)	ขาดเรียนเกิน 3 ครั้ง หรือละเมิดข้อตกลงและวินัยในชั้นเรียน
2. ใบงานวิเคราะห์ภัยไซเบอร์รายบุคคล	GE-LO-1	2	วิเคราะห์กลโกง แยกแยะประเภทมัลแวร์ และระบุจุดสังเกตภัยใกล้ตัวในใบงานได้ถูกต้อง แม่นยำ และมีเหตุผลประกอบ	แยกแยะประเภทภัยคุกคามและพฤติกรรมการหลอกลวงทั่วไปในใบงานได้ถูกต้อง และมีเหตุผลสนับสนุน	แยกแยะภัยไซเบอร์ใกล้ตัวได้เฉพาะกรณีที่ชัดเจน แต่การเขียนวิเคราะห์ยังขาดรายละเอียด	ไม่ส่งงาน หรือไม่สามารถแยกแยะความเสี่ยง/กลโกงออนไลน์ในใบงานได้
3. แบบทดสอบความรู้ (Quiz)	GE-LO-11	2	ทำคะแนนสอบพาร์ทการใช้เครื่องมือความปลอดภัยดิจิทัลพื้นฐานได้ 85% - 100% (หรือได้ 9-10 คะแนนเต็ม 10)	ทำคะแนนสอบพาร์ทการใช้เครื่องมือความปลอดภัยดิจิทัลพื้นฐานได้ 70% - 84% (หรือได้ 7-8 คะแนน)	ทำคะแนนสอบพาร์ทการใช้เครื่องมือความปลอดภัยดิจิทัลพื้นฐานได้ 50% - 69% (หรือได้ 5-6 คะแนน)	ทำคะแนนสอบพาร์ทการใช้เครื่องมือความปลอดภัยดิจิทัลพื้นฐานได้ ต่ำกว่า 50% (หรือได้ต่ำกว่า 5 คะแนน)
4. โครงงานกลุ่มปลายภาค: ชิ้นงานสื่อดิจิทัล	GE-LO-11	4	พูดถ่ายทอดเนื้อหาภัยไซเบอร์ให้เข้าใจง่าย ชัดเจน ลำดับเรื่องราวได้น่าสนใจ และตอบข้อซักถามได้ตรงประเด็น	สื่อสารเนื้อหาและขั้นตอนการรับมือภัยไซเบอร์ได้ถูกต้องชัดเจน ไม่ทำให้ผู้ฟังเกิดความสับสน	นำเสนอเนื้อหาได้ตามเกณฑ์ แต่วิธีการพูดสื่อสารยังไม่ดึงดูดหรือใช้คำอธิบายที่เข้าใจยากเกินไป	เนื้อหาที่นำเสนอมีความผิดพลาดหรือไม่สามารถอธิบายข้อมูลให้ผู้ฟังและกรรมการเข้าใจได้
5. โครงงานกลุ่มปลายภาค: การแก้ปัญหา	GE-LO-2	4	วางลำดับขั้นตอนการแก้ปัญหาเมื่อโดนโจมตี (Incident Response) และประเมินความเสี่ยงในโครงงานได้อย่างเป็นระบบและครบถ้วน	ระบุวิธีเอาตัวรอดและขั้นตอนการแก้ไขปัญหาเมื่อบัญชี/ระบบถูกแฮกในโครงงานได้ถูกต้องตามหลักการ	ระบุวิธีการแก้ปัญหาและการแจ้งความออนไลน์ได้เป็นจุด ๆ แต่ขั้นตอนยังไม่ต่อเนื่องหรือขาดความชัดเจน	แผนงานในโครงงานไม่ระบุแนวทางหรือขั้นตอนในการแก้ปัญหาเมื่อเผชิญเหตุคุกคามไซเบอร์
6. โครงงานกลุ่มปลายภาค: การนำเสนอผลงาน	**GE-LO-9**	2	วิเคราะห์กลโกงและจุดสังเกตได้แม่นยำ ลึกซึ้ง และมีเหตุผลประกอบ	แยกแยะภัยคุกคามทั่วไปได้ถูกต้อง พร้อมระบุเหตุผลได้ดี	แยกแยะภัยได้เฉพาะที่เห็นชัดเจน แต่ยังขาดความละเอียด	ไม่สามารถแยกแยะความเสี่ยงหรือวิเคราะห์ความน่าเชื่อถือได้