WISDOM *for* Sustainable Development

สภาสถาบันบัณฑิตพัฒนบริหารศาสตร์
ให้ความเห็นชอบหลักสูตรนี้แล้ว
ในการประชุมครั้งที่ 5/2569 เมื่อวันที่ 20 พฤษภาคม 2569
กองบริการการศึกษา สถาบันบัณฑิตพัฒนบริหารศาสตร์

หลักสูตรวิทยาศาสตรมหาบัณฑิต
สาขาวิชาการจัดการความเสี่ยงความมั่นคงทางไซเบอร์
(หลักสูตรปรับปรุง พ.ศ. 2569)

คณะสถิติประยุกต์
สถาบันบัณฑิตพัฒนบริหารศาสตร์

หลักสูตรวิทยาศาสตรมหาบัณฑิต
สาขาวิชาการจัดการความเสี่ยงความมั่นคงทางไซเบอร์
(หลักสูตรปรับปรุง พ.ศ. 2569)

ชื่อสถาบันอุดมศึกษา สถาบันบัณฑิตพัฒนบริหารศาสตร์

คณะ คณะสถิติประยุกต์

หมวดที่ 1 ชื่อหลักสูตร และระบบการจัดการศึกษา

1. ชื่อหลักสูตร

ภาษาไทย	หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการจัดการความเสี่ยงความมั่นคงทางไซเบอร์
ภาษาอังกฤษ	Master of Science Program in Cybersecurity Risk Management

2. ชื่อปริญญาและสาขาวิชา

ภาษาไทย(เต็ม)	วิทยาศาสตรมหาบัณฑิต (การจัดการความเสี่ยงความมั่นคงทางไซเบอร์)
ภาษาไทย(ย่อ)	วท.ม. (การจัดการความเสี่ยงความมั่นคงทางไซเบอร์)
ภาษาอังกฤษ(เต็ม)	Master of Science (Cybersecurity Risk Management)
ภาษาอังกฤษ(ย่อ)	M.S. (Cybersecurity Risk Management)

3. วิชาเอกหรือความเชี่ยวชาญเฉพาะหลักสูตร (ถ้ามี)

- ไม่มี -

4. รูปแบบของหลักสูตร

4.1 รูปแบบ

หลักสูตรระดับปริญญาโท ตามเกณฑ์มาตรฐานหลักสูตรระดับบัณฑิตศึกษา พ.ศ. 2565

4.2 ภาษาที่ใช้

ภาษาไทย หรือภาษาอังกฤษ หรือทั้งสองภาษารวมกัน (สำหรับการบรรยาย เอกสาร ตำรา หรือสื่อการเรียนการสอน)

4.3 การรับเข้าศึกษา

รับผู้สำเร็จการศึกษาระดับปริญญาตรีหรือเทียบเท่าจากทุกสาขาวิชา จากสถาบันอุดมศึกษาทั้งในและต่างประเทศที่สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม (สป.อว.) รับรองมาตรฐานการศึกษา ทั้งนี้ เนื่องจากปรัชญาของหลักสูตรและแนวโน้มการประยุกต์ใช้เทคโนโลยีดิจิทัลในทุกภาคส่วน ทำให้การพัฒนาบุคลากรด้านการจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ไม่จำเป็นต้องจำกัดเฉพาะผู้จบการศึกษาสาขาการจัดการความเสี่ยงความมั่นคงทางไซเบอร์ หรือสาขาที่เกี่ยวข้องเท่านั้น หลักสูตรจึงเปิดโอกาสให้ผู้สำเร็จการศึกษาจากสาขาอื่นสมัครเข้าศึกษาได้ด้วย

อย่างไรก็ตาม เพื่อให้การจัดการเรียนการสอนเป็นไปอย่างมีประสิทธิภาพและบรรลุผลลัพธ์การเรียนรู้ของหลักสูตร ผู้เข้าศึกษาต้องมีพื้นฐานความรู้ที่จำเป็นทั้งด้านการจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ รวมถึงพื้นฐานความรู้ภาษาอังกฤษ โดยกำหนดให้นักศึกษาที่ไม่มีพื้นฐานเพียงพอในด้านดังกล่าวต้องลงทะเบียนเรียนรายวิชาเสริมพื้นฐานที่หลักสูตรกำหนด และต้องมีผลการเรียนไม่ต่ำกว่า B

ในกรณีที่นักศึกษาสำเร็จการศึกษาระดับปริญญาตรีจากสาขาที่เกี่ยวข้อง หรือมีผลการสอบมาตรฐานภาษาอังกฤษตามเกณฑ์ที่หลักสูตรกำหนด นักศึกษาสามารถยื่นคำร้องขอพิจารณาเทียบโอน/ยกเว้นรายวิชาเสริมพื้นฐานได้ ภายในสองสัปดาห์แรกของภาคการศึกษาที่นักศึกษาลงทะเบียนเรียนในหลักสูตรเป็นครั้งแรก โดยคณะกรรมการที่ได้รับการแต่งตั้งจะพิจารณาจากผลการสอบวัดความรู้ในประเด็นพื้นฐานที่กำหนด หรือจากคำอธิบายรายวิชาในระดับปริญญาตรีของรายวิชาที่เกี่ยวข้อง หากผลการพิจารณาไม่ผ่านนักศึกษาต้องลงทะเบียนเรียนในรายวิชาเสริมพื้นฐานนั้น ๆ และต้องได้ผลการเรียนไม่ต่ำกว่า B เช่นเดียวกัน

เนื่องจากหลักสูตรนี้ได้รับอนุมัติให้จัดการเรียนการสอนเป็นภาษาไทยเป็นหลัก หลักสูตรจึงพิจารณารับนักศึกษาสัญชาติไทยเป็นกลุ่มเป้าหมายหลัก อย่างไรก็ตาม จากนโยบายของรัฐบาลไทยในการให้ทุนแก่นักศึกษาจากสาธารณรัฐประชาธิปไตยประชาชนลาวผ่านกระทรวงการต่างประเทศ หลักสูตรเคยรับนักศึกษาสัญชาติลาวที่ได้รับทุนดังกล่าวเข้าศึกษา โดยนักศึกษาต้องมีความสามารถในการอ่าน พูด และเขียนภาษาไทยได้ในระดับที่สามารถเรียนรู้ในหลักสูตรภาษาไทยได้อย่างมีประสิทธิภาพ ดังนั้น หลักสูตรนี้สามารถรับทั้งนักศึกษาไทยและนักศึกษาต่างชาติที่มีความสามารถในการสื่อสารภาษาไทยได้ตามเกณฑ์ที่หลักสูตรกำหนด

4.4 ความร่วมมือกับสถาบันอื่น

เป็นหลักสูตรเฉพาะของสถาบันที่จัดการเรียนการสอนโดยตรง แต่มีความร่วมมือทางด้านวิชาการกับสถาบันอุดมศึกษาต่าง ๆ ทั้งภายในประเทศและต่างประเทศ

4.5 การให้ปริญญาแก่ผู้สำเร็จการศึกษา

ให้ปริญญาเพียงสาขาวิชาเดียว

5. สถานภาพของหลักสูตรและการพิจารณาอนุมัติ/เห็นชอบหลักสูตร

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการจัดการความเสี่ยงความมั่นคงทางไซเบอร์ (หลักสูตรปรับปรุง พ.ศ. 2569) ปรับปรุงจากหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการจัดการความเสี่ยงความมั่นคงทางไซเบอร์ (หลักสูตรปรับปรุง พ.ศ. 2564) จะเริ่มเปิดสอนในภาคการศึกษาที่ 1 ปีการศึกษา 2569

คณะกรรมการสภาวิชาการ อนุมัติ/เห็นชอบหลักสูตรในการประชุม ครั้งที่ 4/2569 เมื่อวันที่ 28 เมษายน 2569

สภาสถาบันบัณฑิตพัฒนบริหารศาสตร์ อนุมัติ/เห็นชอบหลักสูตรในการประชุม ครั้งที่ 5/2569 เมื่อวันที่ 20 พฤษภาคม 2569

6. สถานที่จัดการเรียนการสอน

ห้องเรียนและสถานที่ของสถาบันบัณฑิตพัฒนบริหารศาสตร์

เลขที่ 148 ถนนเสรีไทย คลองจั่น บางกะปิ กรุงเทพฯ 10240 (โทร. 02-727-3038–3040)

7. ความสัมพันธ์ (ถ้ามี) กับหลักสูตรอื่นที่เปิดสอนในคณะ/วิทยาลัย อื่น ๆ ของสถาบัน

7.1 กลุ่มวิชา/รายวิชาในหลักสูตรนี้ที่เปิดสอนโดยสำนักงานอธิการบดี ได้แก่ รายวิชาในหมวดวิชาเสริมพื้นฐาน

สพ 4000 วิชาพื้นฐานสำหรับบัณฑิตศึกษา 3 หน่วยกิต

กลุ่มวิชา/รายวิชาในหลักสูตรนี้ที่เปิดสอนโดยคณะภาษา ได้แก่ รายวิชาในหมวดวิชาเสริมพื้นฐาน

ภส 4001 การพัฒนาทักษะการอ่านภาษาอังกฤษสำหรับบัณฑิตศึกษา 3 หน่วยกิต

ภส 4002 การพัฒนาทักษะภาษาอังกฤษแบบบูรณาการ 3 หน่วยกิต

ภส 4011 การซ่อมเสริมการพัฒนาทักษะการอ่านภาษาอังกฤษสำหรับบัณฑิตศึกษา 3 หน่วยกิต

ภส 4012 การซ่อมเสริมการพัฒนาทักษะภาษาอังกฤษแบบบูรณาการ 3 หน่วยกิต

7.2 กลุ่มวิชา/รายวิชาในหลักสูตรที่เปิดสอนให้ภาควิชา/หลักสูตรอื่น

นักศึกษาหลักสูตรอื่นของสถาบัน สามารถเลือกเรียนทุกรายวิชาของหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการจัดการความเสี่ยงความมั่นคงทางไซเบอร์ได้ ยกเว้นวิชาการค้นคว้าอิสระ ทั้งนี้ ต้องเป็นไปตามข้อกำหนดของแต่ละหลักสูตร และได้รับอนุมัติจากอาจารย์ผู้แนะนำและอาจารย์ผู้สอน

7.3 การบริหารจัดการ

หลักสูตรได้ดำเนินการภายใต้ความรับผิดชอบของคณะกรรมการบริหารหลักสูตร และคณะกรรมการจัดการเรียนการสอน อาจารย์ผู้รับผิดชอบหลักสูตรและอาจารย์ประจำหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการจัดการความเสี่ยงความมั่นคงทางไซเบอร์ โดยคณะกรรมการมีหน้าที่กำหนดนโยบายกรอบการดำเนินงานและวางระเบียบหลักเกณฑ์เพื่อให้หลักสูตรมีคุณภาพ ในกลุ่มวิชาเลือกของหลักสูตรนักศึกษาสามารถเลือกวิชาเลือกในคณะ/ภาควิชาอื่นของสถาบันที่มีเนื้อหาสอดคล้องและเหมาะสมกับหลักสูตรของคณะ โดยนักศึกษาสามารถลงทะเบียนและนับเป็นหน่วยกิตในหลักสูตรได้ และผู้อำนวยการหลักสูตรให้คำปรึกษาแก่นักศึกษาที่ประสงค์จะลงทะเบียนรายวิชาของหลักสูตรอื่นเป็นวิชาเลือก อาจารย์ผู้สอนรายวิชานั้น ๆ เป็นผู้อนุญาตหรือให้ความเห็นชอบ โดยมีนักวิชาการศึกษาของแต่ละคณะเป็นผู้ประสานงานและตรวจสอบให้เป็นไปตามข้อบังคับว่าด้วยการศึกษาของสถาบันบัณฑิตพัฒนบริหารศาสตร์

8. ระบบการจัดการศึกษา

8.1 ระบบ

เป็นการศึกษาแบบหน่วยกิตตามระบบทวิภาค โดยปีการศึกษาหนึ่ง ๆ แบ่งเป็น 2 ภาคการศึกษาปกติ คือ ภาคการศึกษาที่ 1 และภาคการศึกษาที่ 2 และอาจมีภาคการศึกษาที่ 3 (ภาคฤดูร้อน) ก็ได้ การศึกษาในภาคการศึกษาปกติมีระยะเวลาไม่น้อยกว่า 15 สัปดาห์ ส่วนการศึกษาภาคฤดูร้อนมีระยะเวลาไม่น้อยกว่า 8 สัปดาห์ แต่มีชั่วโมงการเรียนของแต่ละวิชาเท่ากับชั่วโมงของภาคการศึกษาปกติ

8.2 การจัดการศึกษาภาคฤดูร้อน

การจัดการเรียนการสอนภาคฤดูร้อน ขึ้นอยู่กับการพิจารณาของคณะกรรมการบริหารหลักสูตรประจำคณะสถิติประยุกต์ และผู้อำนวยการหลักสูตร

8.3 การเทียบเคียงหน่วยกิตในระบบทวิภาค

การเทียบเคียงหน่วยกิตจากหลักสูตรอื่น การฝึกอบรมและพัฒนาที่มีการประเมินผลลัพธ์การเรียนรู้ ให้เป็นไปตามข้อบังคับสถาบันบัณฑิตพัฒนบริหารศาสตร์ว่าด้วยการศึกษา พ.ศ. 2563 และฉบับที่แก้ไขเพิ่มเติม และตามประกาศสถาบันบัณฑิตพัฒนบริหารศาสตร์ เรื่อง หลักเกณฑ์และวิธีการเทียบหน่วยกิตและผลการศึกษาจากการศึกษานอกระบบ และการศึกษาตามอัธยาศัยเข้าสู่การศึกษาในระบบตามหลักสูตรของสถาบัน และฉบับที่แก้ไขเพิ่มเติม โดยผลการเรียนรู้ต้องสอดคล้องกับผลการเรียนรู้ของรายวิชาที่ต้องการเทียบเคียง และ ประกาศคณะกรรมการมาตรฐานการอุดมศึกษา เรื่อง หลักเกณฑ์และวิธีการเทียบโอนหน่วยกิต และผลการศึกษาในระดับอุดมศึกษา พ.ศ. 2565

8.4 วัน–เวลาในการดำเนินการเรียนการสอน

ภาคการศึกษาที่ 1 เดือนสิงหาคม–เดือนธันวาคม

ภาคการศึกษาที่ 2 เดือนมกราคม–เดือนพฤษภาคม

ภาคฤดูร้อน เดือนมิถุนายน–เดือนกรกฎาคม

8.5 รูปแบบการจัดการเรียนการสอน

แบบชั้นเรียน ภาคปกติเรียนในเวลาทำการวันจันทร์–วันศุกร์ และภาคพิเศษเรียนนอกเวลาทำการ วันเสาร์–วันอาทิตย์

9. แผนการรับนักศึกษาและผู้สำเร็จการศึกษาในระยะ 5 ปี

จำนวนผู้ที่คาดว่าจะรับเข้าศึกษาในหลักสูตรและจำนวนที่คาดว่าจะมีผู้สำเร็จการศึกษาในแต่ละปีการศึกษาในระยะเวลา 5 ปี

แผน 1

ชั้นปี	ปี 2569	ปี 2570	ปี 2571	ปี 2572	ปี 2573
1	5	5	5	5	5
2	-	5	5	5	5
3	-	-	5	5	5
รวม	5	10	15	15	15
จำนวนนักศึกษาที่คาดว่าจะจบ	-	-	4	5	5

แผน 2

ชั้นปี	ปี 2569	ปี 2570	ปี 2571	ปี 2572	ปี 2573
1	55	55	55	55	55
2	-	55	55	55	55
3	-	-	55	55	55
รวม	55	110	165	165	165
จำนวนนักศึกษาที่คาดว่าจะจบ	-	-	53	53	53

10. งบประมาณตามแผน

ค่าใช้จ่ายต่อหัวในการผลิตบัณฑิตของหลักสูตร

ภาค	แผนการศึกษา	ปีที่ 1 (บาท/คน)	ปีที่ 2 (บาท/คน)	ปีที่ 3 (บาท/คน)
ปกติ	แผน 1	40,000	40,000	16,000
	แผน 2	40,000	40,000	16,000
พิเศษ	แผน 1	84,000	76,000	31,000
	แผน 2	84,000	76,000	31,000

หมายเหตุ – ค่าใช้จ่ายคำนวณทุกวิชาตามแผนการศึกษาและวิชารหัส 4XXX ครบทุกวิชา

11. คุณสมบัติของผู้เข้าศึกษา

11.1 เป็นผู้สำเร็จการศึกษาระดับปริญญาตรีหรือเทียบเท่าทุกสาขาจากสถาบันการศึกษาของรัฐหรือเอกชน ทั้งในและต่างประเทศที่สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม (สป.อว.) รับรองมาตรฐานการศึกษา หรือมีวิทยฐานะที่สภาสถาบันบัณฑิตพัฒนบริหารศาสตร์อนุมัติให้เข้าเป็นนักศึกษา สำหรับประสบการณ์การทำงาน ให้เป็นไปตามประกาศของสถาบัน

11.2 ต้องมีความสามารถในการฟัง พูด อ่าน และเขียนภาษาไทยในระดับที่สามารถศึกษาในหลักสูตรได้อย่างมีประสิทธิภาพ

11.3 ผ่านการคัดเลือกตามเกณฑ์ของสถาบัน โดยการสอบข้อเขียนและ/หรือสัมภาษณ์

11.4 คุณสมบัติของผู้มีสิทธิ์สมัครเข้าศึกษาอาจเปลี่ยนแปลงหรือมีเกณฑ์เพิ่มเติมได้ ทั้งนี้ให้เป็นไปตามประกาศของสถาบันบัณฑิตพัฒนบริหารศาสตร์ และประกาศของคณะสถิติประยุกต์

12. อาชีพที่สามารถประกอบได้หลังสำเร็จการศึกษา

ผู้สำเร็จการศึกษาจากหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาการจัดการความเสี่ยงความมั่นคงทางไซเบอร์ มีศักยภาพในการทำงานในตำแหน่งด้านการจัดการความเสี่ยงไซเบอร์ ความมั่นคงปลอดภัยสารสนเทศ และการบริหารเทคโนโลยีดิจิทัล ในหน่วยงานภาครัฐ รัฐวิสาหกิจ ภาคเอกชน สถาบันการเงิน สถาบันการศึกษา สาธารณสุข โทรคมนาคม และองค์กรระหว่างประเทศ โดยตำแหน่งงานที่สามารถประกอบได้ เช่น

1) ผู้จัดการความเสี่ยงด้านไซเบอร์ / ผู้จัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Cyber / IT Risk Manager)
2) นักวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ (IT & Cyber Risk Analyst)
3) ผู้เชี่ยวชาญหรือนักวิชาการด้านความมั่นคงปลอดภัยสารสนเทศ และการกำกับดูแล ความเสี่ยง และการปฏิบัติตามข้อกำหนด (Information Security & GRC Specialist)
4) ผู้บริหารเทคโนโลยีสารสนเทศ หรือผู้บริหารด้านความมั่นคงปลอดภัยสารสนเทศ เช่น CIO, CISO (ขึ้นอยู่กับประสบการณ์ทำงานและคุณสมบัติอื่นประกอบ)
5) ผู้เชี่ยวชาญหรือนักวิเคราะห์ด้านความมั่นคงปลอดภัยไซเบอร์ เช่น Security Analyst, SOC Analyst, Incident Responder, Threat Hunter
6) สถาปนิกด้านความมั่นคงปลอดภัยของระบบเครือข่าย ระบบคลาวด์ และสถาปัตยกรรมองค์กร (Security Architect / Cloud Security Architect / Enterprise Security Architect)
7) ผู้จัดการโครงการสารสนเทศและโครงการด้านความมั่นคงปลอดภัยไซเบอร์ (IT / Cybersecurity Project Manager)

8) นักวิเคราะห์และออกแบบระบบงานคอมพิวเตอร์และระบบสารสนเทศที่บูรณาการการบริหารความเสี่ยงและความมั่นคงปลอดภัยไซเบอร์เข้าไปในสถาปัตยกรรมระบบ (Secure Systems Analyst & Designer)
9) ผู้ตรวจสอบระบบสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ (IT Auditor / Cybersecurity Auditor)
10) ผู้ทดสอบการเจาะระบบและผู้ประเมินช่องโหว่ระบบสารสนเทศ (Penetration Tester / Vulnerability Assessor)
11) ผู้ดูแลและบริหารโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและระบบความมั่นคงปลอดภัย (IT Infrastructure & Security Administrator / Engineer)
12) ผู้ดูแลและบริหารฐานข้อมูลและข้อมูลสำคัญขององค์กร รวมถึงด้านการคุ้มครองข้อมูลส่วนบุคคล (Database Administrator / Data Protection Officer Assistant)
13) ที่ปรึกษาด้านการจัดการความเสี่ยงไซเบอร์ มาตรฐานความมั่นคงปลอดภัยสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคล (Cyber Risk, InfoSec & Privacy Consultant)
14) นักวิชาการคอมพิวเตอร์และเทคโนโลยีสารสนเทศ หรือนักวิชาการด้านความมั่นคงปลอดภัยไซเบอร์ในหน่วยงานราชการ สถาบันการศึกษา และองค์การระหว่างประเทศ
15) นักวิจัยด้านความมั่นคงปลอดภัยไซเบอร์ การจัดการความเสี่ยงดิจิทัล และการกำกับดูแลเทคโนโลยีสารสนเทศ (Cybersecurity & Digital Risk Researcher)

หมวดที่ 2 ปรัชญา วัตถุประสงค์ และผลลัพธ์การเรียนรู้

1. ปรัชญาของหลักสูตร

มุ่งพัฒนาบัณฑิตให้เป็นผู้นำด้านการบริหารความเสี่ยงและความมั่นคงปลอดภัยไซเบอร์ มีความรู้ด้านเทคโนโลยี การจัดการ กฎหมาย และมาตรฐานสากล ควบคู่คุณธรรม จริยธรรม ธรรมาภิบาล และความรับผิดชอบต่อสังคม สามารถสร้างองค์ความรู้และนวัตกรรมเพื่อคาดการณ์ ป้องกัน รับมือ และฟื้นฟูจากภัยคุกคามไซเบอร์ สนับสนุนเศรษฐกิจและสังคมดิจิทัลที่มั่นคง ปลอดภัย และยั่งยืน

2. วัตถุประสงค์ของหลักสูตร

1) ผลิตบุคลากรด้านการจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ที่มีความรู้เชิงลึกทั้งด้านเทคโนโลยีและการบริหารจัดการ สามารถวิเคราะห์ วางแผน ออกแบบ และบริหารจัดการความเสี่ยงของระบบสารสนเทศ บริการดิจิทัล และโครงสร้างพื้นฐานดิจิทัลขององค์กรได้อย่างเป็นระบบ มีจิตสำนึกในจริยธรรมวิชาชีพและความรับผิดชอบต่อสังคม และสามารถมีส่วนสนับสนุนการยกระดับความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานและประเทศในภาพรวม

2) ผลิตนักวิชาการและนักวิจัยด้านการจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ที่มีศักยภาพในการสร้างองค์ความรู้ งานวิจัย และนวัตกรรม เพื่อยกระดับมาตรการ แนวปฏิบัติ และการกำกับดูแลด้านความมั่นคงปลอดภัยของระบบสารสนเทศและบริการดิจิทัลในระดับองค์กรให้มีประสิทธิภาพ สอดคล้องกับกฎหมายและมาตรฐานสากล และสามารถรองรับภัยคุกคามไซเบอร์รูปแบบใหม่ได้อย่างต่อเนื่อง

3. ตารางเชื่อมโยงผลลัพธ์การเรียนรู้ ปรัชญา วัตถุประสงค์ และมาตรฐานคุณวุฒิของหลักสูตร

เมื่อสำเร็จการศึกษาแล้ว ผู้สำเร็จการศึกษาจากหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการจัดการความเสี่ยงความมั่นคงทางไซเบอร์ จะมีผลลัพธ์การเรียนรู้ (Program Learning Outcomes: PLOs) ดังนี้

PLO1 ความรู้ด้านวิทยาการไซเบอร์และโครงสร้างพื้นฐานดิจิทัล

สามารถอธิบายและบูรณาการหลักการ แนวคิด และสถาปัตยกรรมด้านความมั่นคงปลอดภัยไซเบอร์ ครอบคลุมเครือข่าย ระบบปฏิบัติการ ระบบคลาวด์ IoT OT ระบบสารสนเทศสมัยใหม่ รวมถึงระบบที่ขับเคลื่อนด้วยข้อมูลและปัญญาประดิษฐ์ ตลอดจนกลไกการเข้ารหัส การพิสูจน์ตัวตน และการควบคุมสิทธิ์การเข้าถึงข้อมูล

PLO2 ทักษะเชิงเทคนิคด้านความมั่นคงปลอดภัยไซเบอร์

สามารถออกแบบ เลือกใช้ ดำเนินการ และประเมินกลไกหรือเทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกัน ตรวจจับ ตอบสนอง และฟื้นฟูระบบสารสนเทศและบริการดิจิทัลขององค์กร รวมถึงการใช้เครื่องมือทดสอบช่องโหว่ การตรวจสอบความมั่นคงปลอดภัย การวิเคราะห์เหตุการณ์ และการปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ (เช่น SOC / Incident Response) ได้อย่างเป็นระบบและมีประสิทธิภาพ

PLO3 การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และดิจิทัล

สามารถระบุ วิเคราะห์ ประเมิน และจัดลำดับความสำคัญของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และความเสี่ยงดิจิทัล (รวมถึงความเสี่ยงจากระบบคลาวด์ IoT และระบบที่ใช้ปัญญาประดิษฐ์) กำหนดกลยุทธ์และมาตรการควบคุม/บรรเทาความเสี่ยงที่เหมาะสม และบูรณาการการบริหารความเสี่ยงไซเบอร์เข้ากับการบริหารความเสี่ยงองค์รวมและทิศทางเชิงกลยุทธ์ขององค์กรได้

PLO4 กฎหมาย มาตรฐาน และธรรมาภิบาลด้านไซเบอร์และปัญญาประดิษฐ์

สามารถทำความเข้าใจและประยุกต์ใช้กฎหมาย ระเบียบ ข้อบังคับ และมาตรฐานที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ การคุ้มครองข้อมูลส่วนบุคคล และการใช้ปัญญาประดิษฐ์อย่างรับผิดชอบ (เช่น PDPA กฎหมายไซเบอร์ที่เกี่ยวข้อง มาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001 และมาตรฐานระบบบริหารจัดการปัญญาประดิษฐ์ ISO/IEC 42001 เป็นต้น) ในการออกแบบนโยบาย ระเบียบปฏิบัติ และกรอบธรรมาภิบาลเทคโนโลยีขององค์กรให้สอดคล้องกับข้อกำหนดและมาตรฐานสากล

PLO5.1 การวิจัยและการสร้างองค์ความรู้/นวัตกรรมด้านการจัดการความเสี่ยงไซเบอร์ สำหรับแผน 1

สามารถออกแบบและดำเนินการวิจัยเชิงวิชาการระดับบัณฑิตศึกษาอย่างเป็นระบบ เพื่อสร้างองค์ความรู้ใหม่ กรอบแนวคิด แบบจำลอง หรือหลักฐานเชิงประจักษ์ด้านการจัดการความเสี่ยงไซเบอร์และดิจิทัล (รวมถึงการกำกับดูแลเทคโนโลยีและปัญญาประดิษฐ์) โดยมีความถูกต้องด้านระเบียบวิธี คุณภาพทางวิชาการ การวิเคราะห์เชิงลึก และยึดหลักจริยธรรมการวิจัย

PLO5.2 การวิจัยและการสร้างองค์ความรู้/นวัตกรรมด้านการจัดการความเสี่ยงไซเบอร์ สำหรับแผน 2

สามารถออกแบบและดำเนินการศึกษาค้นคว้าเชิงประยุกต์ เพื่อสร้างแนวทางปฏิบัติ ต้นแบบระบบ เครื่องมือ หรือแนวทางนวัตกรรมที่นำไปใช้ได้จริงในการยกระดับความมั่นคงปลอดภัยไซเบอร์และการบริหารความเสี่ยงดิจิทัลขององค์กร (รวมถึงเทคโนโลยีและปัญญาประดิษฐ์) โดยมีการประเมินผลที่เหมาะสม ความน่าเชื่อถือในการสรุปผล และยึดหลักจริยธรรมที่เกี่ยวข้อง

PLO6 การสื่อสาร ประสานงาน และภาวะผู้นำด้านความมั่นคงปลอดภัยไซเบอร์และความเสี่ยง

สามารถสื่อสาร วิเคราะห์ และนำเสนอข้อมูลเชิงเทคนิคและเชิงบริหารด้านความเสี่ยง และความมั่นคงปลอดภัยไซเบอร์/ดิจิทัลแก่ผู้บริหารและผู้มีส่วนได้ส่วนเสียในรูปแบบที่เข้าใจง่ายและนำไปใช้ตัดสินใจได้ สามารถทำงานเป็นทีมข้ามสายงาน บริหารผู้มีส่วนได้ส่วนเสียและแสดงภาวะผู้นำในการขับเคลื่อนมาตรการ นโยบาย และวัฒนธรรมด้านความมั่นคงปลอดภัยไซเบอร์ในองค์กร

PLO7 คุณธรรม จริยธรรม และความรับผิดชอบต่อวิชาชีพและสังคม

มีจิตสำนึกด้านคุณธรรม จริยธรรมวิชาชีพ ความโปร่งใส และความรับผิดชอบต่อสังคม ตระหนักถึงสิทธิในความเป็นส่วนตัว ศักดิ์ศรีความเป็นมนุษย์ และผลกระทบจากการใช้เทคโนโลยีดิจิทัลและปัญญาประดิษฐ์ สามารถส่งเสริมวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กร และมุ่งมั่นพัฒนาตนเองอย่างต่อเนื่องในฐานะผู้เชี่ยวชาญด้านการจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์และดิจิทัล

มาตรฐานคุณวุฒิของหลักสูตร

รหัส	มาตรฐานคุณวุฒิ	ความหมาย
QS1	ความรู้ (Knowledge)	ความรู้เชิงลึกด้านความมั่นคงปลอดภัยไซเบอร์ การบริหารความเสี่ยง กฎหมาย มาตรฐาน ธรรมาภิบาล เทคโนโลยีดิจิทัล และปัญญาประดิษฐ์
QS2	ทักษะ (Skills)	ทักษะการคิดวิเคราะห์ การแก้ปัญหา การใช้เครื่องมือ การประเมินและบริหารความเสี่ยง การวิจัย การสื่อสาร และการปฏิบัติงานเชิงวิชาชีพ
QS3	จริยธรรม (Ethics)	จริยธรรมวิชาชีพ ความซื่อสัตย์ ความโปร่งใส ความรับผิดชอบต่อสังคม การเคารพกฎหมาย มาตรฐาน สิทธิส่วนบุคคล และการใช้เทคโนโลยีอย่างรับผิดชอบ
QS4	ลักษณะบุคคล (Character)	ภาวะผู้นำ ความรับผิดชอบ ความเป็นมืออาชีพ การทำงานร่วมกับผู้อื่น การเรียนรู้ตลอดชีวิต และความสามารถในการปรับตัวต่อการเปลี่ยนแปลง

ตารางที่ 1 ความเชื่อมโยงระหว่างผลลัพธ์การเรียนรู้ ปรัชญา วัตถุประสงค์ และมาตรฐานคุณวุฒิของหลักสูตร

ผลลัพธ์การเรียนรู้ (PLO)	ปรัชญาหลักสูตร (PH)	วัตถุประสงค์หลักสูตร (O)	มาตรฐานคุณวุฒิ
PLO1 ความรู้ด้านวิทยาการไซเบอร์และโครงสร้างพื้นฐานดิจิทัล - สามารถอธิบายและบูรณาการหลักการ แนวคิด และสถาปัตยกรรมด้านความมั่นคงปลอดภัยไซเบอร์ ครอบคลุมเครือข่าย ระบบปฏิบัติการ ระบบคลาวด์ IoT และระบบสารสนเทศสมัยใหม่ รวมถึงระบบที่ขับเคลื่อนด้วยข้อมูลและปัญญาประดิษฐ์ ตลอดจนกลไกการเข้ารหัส การพิสูจน์ตัวตน และการควบคุมสิทธิ์การเข้าถึงข้อมูล	PH2: บูรณาการ ความรู้ด้านเทคโนโลยี กับการจัดการ PH4: มุ่งสร้าง องค์ความรู้และนวัตกรรม เพื่อคาดการณ์ ป้องกัน รับมือ และฟื้นฟูจากภัยคุกคามไซเบอร์อย่างเป็นระบบ PH5: สนับสนุน การเปลี่ยนผ่านสู่เศรษฐกิจและสังคมดิจิทัลที่มั่นคง ปลอดภัย และยั่งยืนภายใต้กฎหมายและมาตรฐานสากล	O1: ผลิตบุคลากรด้านการจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ เพื่อเป็นกำลังสำคัญในการพัฒนาและดูแลระบบสารสนเทศของประเทศ	QS1: ความรู้เชิงลึกเฉพาะสาขาวิชาความมั่นคงปลอดภัยไซเบอร์และการจัดการความเสี่ยง QS2: ทักษะทางปัญญา การคิดวิเคราะห์ สังเคราะห์ และแก้ปัญหาที่ซับซ้อนด้านไซเบอร์และความเสี่ยง
PLO2 ทักษะเชิงเทคนิคด้านความมั่นคงปลอดภัยไซเบอร์ - สามารถออกแบบ เลือกใช้ ดำเนินการ และประเมินกลไกหรือเทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์เพื่อป้องกัน ตรวจจับ ตอบสนอง และฟื้นฟูระบบสารสนเทศและบริการดิจิทัลขององค์กร รวมถึงการใช้เครื่องมือทดสอบช่องโหว่ การตรวจสอบความมั่นคงปลอดภัย การวิเคราะห์เหตุการณ์ และการปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ (เช่น SOC / Incident Response) ได้อย่างเป็นระบบและมีประสิทธิภาพ	PH1: พัฒนาบัณฑิตให้เป็น ผู้นำด้านการบริหารความเสี่ยงและความมั่นคงปลอดภัยไซเบอร์ PH2: บูรณาการ ความรู้ด้านเทคโนโลยี กับการจัดการ PH4: มุ่งสร้าง องค์ความรู้และนวัตกรรม เพื่อคาดการณ์ ป้องกัน รับมือ และฟื้นฟูจากภัยคุกคามไซเบอร์อย่างเป็นระบบ PH5: สนับสนุน การเปลี่ยนผ่านสู่เศรษฐกิจและสังคมดิจิทัลที่มั่นคง ปลอดภัย และยั่งยืนภายใต้กฎหมายและมาตรฐานสากล	O1: ผลิตบุคลากรด้านการจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ เพื่อเป็นกำลังสำคัญในการพัฒนาและดูแลระบบสารสนเทศของประเทศ	QS2: ทักษะทางปัญญา การคิดวิเคราะห์ สังเคราะห์ และแก้ปัญหาที่ซับซ้อนด้านไซเบอร์และความเสี่ยง QS2: ทักษะวิชาชีพและการปฏิบัติด้านเทคนิค/การจัดการความมั่นคงปลอดภัยไซเบอร์

ผลลัพธ์การเรียนรู้ (PLO)	ปรัชญาหลักสูตร (PH)	วัตถุประสงค์หลักสูตร (O)	มาตรฐานคุณวุฒิ
PLO3 การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และดิจิทัล - สามารถระบุ วิเคราะห์ ประเมิน และจัดลำดับความสำคัญของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และความเสี่ยงดิจิทัล (รวมถึงความเสี่ยงจากระบบคลาวด์ IoT และระบบที่ใช้ปัญญาประดิษฐ์) กำหนดกลยุทธ์และมาตรการควบคุม/บรรเทาความเสี่ยงที่เหมาะสม และบูรณาการการบริหารความเสี่ยงไซเบอร์เข้ากับการบริหารความเสี่ยงองค์รวมและทิศทางเชิงกลยุทธ์ขององค์กรได้	PH1: พัฒนาบัณฑิตให้เป็น ผู้นำด้านการบริหารความเสี่ยงและความมั่นคงปลอดภัยไซเบอร์ PH2: บูรณาการ ความรู้ด้านเทคโนโลยี กับการจัดการ PH5: สนับสนุน การเปลี่ยนผ่านสู่เศรษฐกิจและสังคมดิจิทัลที่มั่นคง ปลอดภัย และยั่งยืนภายใต้กฎหมายและมาตรฐานสากล	O1: ผลิตบุคลากรด้านการจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ เพื่อเป็นกำลังสำคัญในการพัฒนาและดูแลระบบสารสนเทศของประเทศ	QS1: ความรู้เชิงลึกเฉพาะสาขาวิชาความมั่นคงปลอดภัยไซเบอร์และการจัดการความเสี่ยง QS2: ทักษะทางปัญญา การคิดวิเคราะห์ สังเคราะห์ และแก้ปัญหาที่ซับซ้อนด้านไซเบอร์และความเสี่ยง QS2: ทักษะวิชาชีพและการปฏิบัติด้านเทคนิค/การจัดการความมั่นคงปลอดภัยไซเบอร์
PLO4 กฎหมาย มาตรฐาน และธรรมาภิบาลด้านไซเบอร์และปัญญาประดิษฐ์ - สามารถทำความเข้าใจและประยุกต์ใช้กฎหมาย ระเบียบ ข้อบังคับ และมาตรฐานที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ การคุ้มครองข้อมูลส่วนบุคคล และการใช้ปัญญาประดิษฐ์อย่างรับผิดชอบ (เช่น PDPA กฎหมายไซเบอร์ที่เกี่ยวข้อง มาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001 และ มาตรฐานระบบบริหารจัดการปัญญาประดิษฐ์ ISO/IEC 42001 เป็นต้น) ในการ	PH2: บูรณาการ ความรู้ด้านเทคโนโลยี กับการจัดการ PH3: ยึดมั่น คุณธรรม จริยธรรม และความรับผิดชอบต่อสังคมและประเทศชาติ PH5: สนับสนุน การเปลี่ยนผ่านสู่เศรษฐกิจและสังคมดิจิทัลที่มั่นคง ปลอดภัย และยั่งยืนภายใต้กฎหมายและมาตรฐานสากล	O1: ผลิตบุคลากรด้านการจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ เพื่อเป็นกำลังสำคัญในการพัฒนาและดูแลระบบสารสนเทศของประเทศ O2: ผลิตนักวิชาการ/นักวิจัยด้านการจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ เพื่อสร้างองค์ความรู้และงานวิจัยรองรับการ	QS1: ความรู้เชิงลึกเฉพาะสาขาวิชาความมั่นคงปลอดภัยไซเบอร์และการจัดการความเสี่ยง QS3: คุณธรรม จริยธรรมวิชาชีพ ความรับผิดชอบต่อสังคม และการเคารพกฎหมาย/มาตรฐาน

ผลลัพธ์การเรียนรู้ (PLO)	ปรัชญาหลักสูตร (PH)	วัตถุประสงค์หลักสูตร (O)	มาตรฐานคุณวุฒิ
ออกแบบนโยบาย ระเบียบปฏิบัติ และกรอบธรรมาภิบาลเทคโนโลยีขององค์กรให้สอดคล้องกับข้อกำหนดและมาตรฐานสากล		รักษาความมั่นคงปลอดภัยของระบบสารสนเทศ	
PLO5.1 การวิจัยและการสร้างองค์ความรู้/นวัตกรรมด้านการจัดการความเสี่ยงไซเบอร์ สำหรับแผน 1 สามารถออกแบบและดำเนินการวิจัยเชิงวิชาการระดับบัณฑิตศึกษาอย่างเป็นระบบ เพื่อสร้างองค์ความรู้ใหม่ กรอบแนวคิด แบบจำลอง หรือหลักฐานเชิงประจักษ์ด้านการจัดการความเสี่ยงไซเบอร์และดิจิทัล (รวมถึงการกำกับดูแลเทคโนโลยีและปัญญาประดิษฐ์) โดยมีความถูกต้องด้านระเบียบวิธีคุณภาพทางวิชาการ การวิเคราะห์เชิงลึก และยึดหลักจริยธรรมการวิจัย **PLO5.2 การวิจัยและการสร้างองค์ความรู้/นวัตกรรมด้านการจัดการความเสี่ยงไซเบอร์ สำหรับแผน 2** สามารถออกแบบและดำเนินการศึกษาค้นคว้าเชิงประยุกต์เพื่อสร้างแนวทางปฏิบัติ ต้นแบบระบบ เครื่องมือ หรือแนวทางนวัตกรรมที่นำไปใช้ได้จริงในการยกระดับความมั่นคงปลอดภัยไซเบอร์และการบริหารความเสี่ยงดิจิทัลขององค์กร (รวมถึงเทคโนโลยีและปัญญาประดิษฐ์) โดยมีการประเมินผลที่	PH4: มุ่งสร้าง องค์ความรู้และนวัตกรรม เพื่อคาดการณ์ ป้องกัน รับมือ และฟื้นฟูจากภัยคุกคามไซเบอร์อย่างเป็นระบบ PH5: สนับสนุน การเปลี่ยนผ่านสู่เศรษฐกิจและสังคมดิจิทัลที่มั่นคง ปลอดภัย และยั่งยืนภายใต้กฎหมายและมาตรฐานสากล	O2: ผลิตนักวิชาการ/นักวิจัยด้านการจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ เพื่อสร้างองค์ความรู้และงานวิจัยรองรับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ	QS1: ความรู้เชิงลึกเฉพาะสาขาวิชาความมั่นคงปลอดภัยไซเบอร์และการจัดการความเสี่ยง QS2: ทักษะทางปัญญา การคิดวิเคราะห์ สังเคราะห์ และแก้ปัญหาที่ซับซ้อนด้านไซเบอร์และความเสี่ยง QS2: ทักษะการวิจัยและการสร้างนวัตกรรมด้านความมั่นคงปลอดภัยไซเบอร์และการจัดการความเสี่ยงดิจิทัล

ผลลัพธ์การเรียนรู้ (PLO)	ปรัชญาหลักสูตร (PH)	วัตถุประสงค์หลักสูตร (O)	มาตรฐานคุณวุฒิ
เหมาะสม ความน่าเชื่อถือในการสรุปผล และยึดหลักจริยธรรมที่เกี่ยวข้อง			
PLO6 การสื่อสาร ประสานงาน และภาวะผู้นำด้านความมั่นคงปลอดภัยไซเบอร์และความเสี่ยง - สามารถสื่อสาร วิเคราะห์ และนำเสนอข้อมูลเชิงเทคนิคและเชิงบริหารด้านความเสี่ยงและความมั่นคงปลอดภัยไซเบอร์/ดิจิทัลแก่ผู้บริหารและผู้มีส่วนได้ส่วนเสีย ในรูปแบบที่เข้าใจง่ายและนำไปใช้ตัดสินใจได้ - สามารถทำงานเป็นทีมข้ามสายงาน บริหารผู้มีส่วนได้ส่วนเสียและแสดงภาวะผู้นำในการขับเคลื่อนมาตรการ นโยบาย และวัฒนธรรมด้านความมั่นคงปลอดภัยไซเบอร์ในองค์กร	PH1: พัฒนาบัณฑิตให้เป็น ผู้นำด้านการบริหารความเสี่ยงและความมั่นคงปลอดภัยไซเบอร์ PH5: สนับสนุน การเปลี่ยนผ่านสู่เศรษฐกิจและสังคมดิจิทัลที่มั่นคง ปลอดภัย และยั่งยืนภายใต้กฎหมายและมาตรฐานสากล	O1: ผลิตบุคลากรด้านการจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ เพื่อเป็นกำลังสำคัญในการพัฒนาและดูแลระบบสารสนเทศของประเทศ O2: ผลิตนักวิชาการ/นักวิจัยด้านการจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ เพื่อสร้างองค์ความรู้และงานวิจัยรองรับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ	QS4: ทักษะการสื่อสาร การทำงานเป็นทีม ภาวะผู้นำ และการบูรณาการข้ามสาขา

ผลลัพธ์การเรียนรู้ (PLO)	ปรัชญาหลักสูตร (PH)	วัตถุประสงค์หลักสูตร (O)	มาตรฐานคุณวุฒิ
PLO7 คุณธรรม จริยธรรม และความรับผิดชอบต่อวิชาชีพและสังคม - มีจิตสำนึกด้านคุณธรรม จริยธรรมวิชาชีพ ความโปร่งใส และความรับผิดชอบต่อสังคม ตระหนักถึงสิทธิในความเป็นส่วนตัว ศักดิ์ศรีความเป็นมนุษย์ - และผลกระทบจากการใช้เทคโนโลยีดิจิทัลและปัญญาประดิษฐ์ - สามารถส่งเสริมวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กร และมุ่งมั่นพัฒนาตนเองอย่างต่อเนื่องในฐานะผู้เชี่ยวชาญด้านการจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์และดิจิทัล	PH3: ยึดมั่น คุณธรรม จริยธรรม และความรับผิดชอบต่อสังคมและประเทศชาติ PH5: สนับสนุน การเปลี่ยนผ่านสู่เศรษฐกิจและสังคมดิจิทัลที่มั่นคง ปลอดภัย และยั่งยืนภายใต้กฎหมายและมาตรฐานสากล	O1: ผลิตบุคลากรด้านการจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ เพื่อเป็นกำลังสำคัญในการพัฒนาและดูแลระบบสารสนเทศของประเทศ O2: ผลิตนักวิชาการ/นักวิจัยด้านการจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ เพื่อสร้างองค์ความรู้และงานวิจัยรองรับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ	QS3: คุณธรรม จริยธรรมวิชาชีพ ความรับผิดชอบต่อสังคม และการเคารพกฎหมาย/มาตรฐาน

หมวดที่ 3 โครงสร้างหลักสูตร รายวิชาและหน่วยกิต

1. จำนวนหน่วยกิต

36 หน่วยกิต แผน 1 รายวิชา 24 หน่วยกิต วิทยานิพนธ์ 12 หน่วยกิต รวม 36 หน่วยกิต
แผน 2 รายวิชา 33 หน่วยกิต การค้นคว้าอิสระ 3 หน่วยกิต รวม 36 หน่วยกิต

2. โครงสร้างหลักสูตร

หมวดวิชา	แผน 1 แบบวิชาการ	แผน 2 แบบวิชาชีพ
หมวดวิชาเสริมพื้นฐาน	3–18 หน่วยกิต (ไม่นับหน่วยกิต)	3–18 หน่วยกิต (ไม่นับหน่วยกิต)
หมวดวิชาหลัก	9 หน่วยกิต	9 หน่วยกิต
หมวดวิชาเลือก (อย่างน้อย)	15 หน่วยกิต	24 หน่วยกิต
การค้นคว้าอิสระ	—	3 หน่วยกิต
สอบประมวลความรู้	สอบ	สอบ
สอบปากเปล่า	—	สอบ
วิทยานิพนธ์ (ผ่านการสอบป้องกันวิทยานิพนธ์)	12 หน่วยกิต	—
รวมไม่น้อยกว่า	**36 หน่วยกิต**	**36 หน่วยกิต**

3. รายวิชา

(1) หมวดวิชาเสริมพื้นฐาน หมายถึงวิชาที่มุ่งปรับความรู้ในระดับต่ำกว่าขั้นบัณฑิตศึกษาของนักศึกษาเพื่อให้พร้อมที่จะศึกษาในชั้นปริญญาโท ประกอบด้วย

สพ 4000	พื้นฐานสำหรับบัณฑิตศึกษา	3(2–2–5)
ND 4000	Foundation for Graduate Studies	
ภส 4001	การพัฒนาทักษะการอ่านภาษาอังกฤษสำหรับบัณฑิตศึกษา	3(3–0–6)
LC 4001	Reading Skills Development in English for Graduate Studies	
ภส 4002	การพัฒนาทักษะภาษาอังกฤษแบบบูรณาการ	3(3–0–6)
LC 4002	Integrated English Language Skills Development	
ภส 4011	การซ่อมเสริมการพัฒนาทักษะการอ่านภาษาอังกฤษสำหรับบัณฑิตศึกษา	3(3–0–6)
LC 4011	Remedial Reading Skills Development in English for Graduate Studies	
ภส 4012	การซ่อมเสริมการพัฒนาทักษะภาษาอังกฤษแบบบูรณาการ	3(3–0–6)
LC 4012	Remedial Integrated English Language Skills Development	

สมซ 4001	ระบบกฎหมายและนิติวิธีสำหรับดิจิทัลและไซเบอร์	3(3–0–6)
CRM 4001	Legal Systems and Methods for Digital and Cyber Contexts	
สมซ 4002	การปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์และศูนย์ปฏิบัติการ	3(2–2–5)
CRM 4002	Cybersecurity Operations and SOC	
สมซ 4003	ภาษาอังกฤษสำหรับการจัดการความเสี่ยงความมั่นคงทางไซเบอร์	3(3–0–6)
CRM 4003	English for Cybersecurity Risk Management	

หมายเหตุ 1. ข้อกำหนดและการยกเว้นการเรียนวิชาในหมวดวิชาเสริมพื้นฐาน ให้เป็นไปตามประกาศของคณะ/สถาบัน ยกเว้นข้อกำหนดและการยกเว้นการเรียนวิชาเสริมพื้นฐานภาษาอังกฤษของคณะภาษาและการสื่อสาร ให้เป็นไปตามเงื่อนไขของวิชาภาษาอังกฤษสำหรับบัณฑิตศึกษา

2. ในกรณีที่มีการปรับปรุงวิชาภาษาอังกฤษสำหรับบัณฑิตศึกษา การเรียนวิชาเสริมพื้นฐานภาษาอังกฤษที่กำหนดไว้ในหลักสูตรนี้ จะต้องเปลี่ยนแปลงให้เป็นไปตามวิชาภาษาอังกฤษสำหรับบัณฑิตศึกษาที่ปรับปรุงใหม่ด้วย

3. การกำหนดการเรียนวิชาเสริมพื้นฐานของคณะขึ้นอยู่กับประกาศคณะสถิติประยุกต์ สถาบันบัณฑิตพัฒนบริหารศาสตร์ เรื่อง ข้อกำหนดเกี่ยวกับวิชาเสริมพื้นฐาน

(2) หมวดวิชาหลัก หมายถึง กลุ่มวิชาที่มุ่งให้นักศึกษามีความรู้ความชำนาญเฉพาะด้านกำหนดให้แผน 1 และ แผน 2 เรียนวิชาในหมวดวิชาหลัก 3 วิชา (9 หน่วยกิต) ประกอบด้วยวิชาต่อไปนี้

สมซ 6001	การบริหารความมั่นคงปลอดภัยสารสนเทศ	3(3–0–6)
CRM 6001	Information Security Management	
สมซ 6002	การวิเคราะห์ความเสี่ยงสำหรับความมั่นคงปลอดภัยสารสนเทศ	3(3–0–6)
CRM 6002	Information Security Risk Analysis	
สมซ 6003	กฎหมายเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	3(3–0–6)
CRM 6003	Cybersecurity Law	

(3) หมวดวิชาเลือก ประกอบด้วยกลุ่มวิชารหัส สมซ 7XXX/สมซ 8XXX สำหรับผู้ที่เลือกเรียนแผน 1 กำหนดให้เรียนวิชาเลือกอย่างน้อย 15 หน่วยกิต และสำหรับผู้ที่เลือกเรียนแผน 2 กำหนดให้เรียนวิชาเลือกอย่างน้อย 24 หน่วยกิต โดยสามารถเลือกเรียนได้ตามความสนใจ ทั้งนี้ ต้องผ่านความเห็นชอบของอาจารย์ที่ปรึกษา รายวิชาดังต่อไปนี้

สมซ 7001	ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และเครือข่าย	3(3–0–6)
CRM 7001	Computer and Network Security	
สมซ 7002	ความมั่นคงปลอดภัยของคลาวด์และระบบคลาวด์เนทีฟ	3(2–2–5)
CRM 7002	Cloud and Cloud-Native Security	
สมซ 7003	ปัญญาประดิษฐ์ขั้นสูงสำหรับการปฏิบัติการความมั่นคงปลอดภัยไซเบอร์	3(2–2–5)
CRM 7003	Advanced AI for Cybersecurity Operations	

สมซ 7004	การทดสอบการเจาะระบบและการจัดการช่องโหว่	3(2–2–5)
CRM 7004	Penetration Testing and Vulnerability Management	
สมซ 7005	นิติดิจิทัลและการสืบสวน	3(3–0–6)
CRM 7005	Digital Forensics and Investigations	
สมซ 7006	นโยบายความมั่นคงปลอดภัยสารสนเทศ	3(3–0–6)
CRM 7006	Information Security Policy	
สมซ 7007	การกำกับดูแลระบบสารสนเทศ	3(3–0–6)
CRM 7007	Information Systems Governance	
สมซ 7008	กฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์	3(3–0–6)
CRM 7008	Cybercrime Law	
สมซ 7009	กฎหมายพาณิชย์อิเล็กทรอนิกส์และธุรกิจดิจิทัล	3(3–0–6)
CRM 7009	Electronic Commerce and Digital Business Law	
สมซ 7010	กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและความเป็นส่วนตัว	3(3–0–6)
CRM 7010	Data Protection and Privacy Law	
สมซ 7011	การจัดการความเสี่ยงสำหรับเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัย	3(3–0–6)
CRM 7011	สารสนเทศ	
	Information Security and IT Risk Management	
สมซ 7012	การตรวจสอบความมั่นคงปลอดภัยสารสนเทศ	3(3–0–6)
CRM 7012		
	Information Security Auditing	

วิชาเลือกอื่น ๆ

สมซ 8701	การศึกษาเฉพาะเรื่องทางการจัดการความเสี่ยงความมั่นคงทางไซเบอร์ 1	1(1–0–2)
CRM 8701	Selected Topics in Cybersecurity Risk Management 1	
สมซ 8702	การศึกษาเฉพาะเรื่องทางการจัดการความเสี่ยงความมั่นคงทางไซเบอร์ 2	2(2–0–4)
CRM 8702	Selected Topics in Cybersecurity Risk Management 2	
สมซ 8703	การศึกษาเฉพาะเรื่องทางการจัดการความเสี่ยงความมั่นคงทางไซเบอร์ 3	3(3–0–6)
CRM 8703	Selected Topics in Cybersecurity Risk Management 3	

หมายเหตุ 1. นอกจากวิชาเลือกดังกล่าวแล้ว นักศึกษายังสามารถเลือกวิชาเลือกอื่น ๆ ซึ่งอาจเป็นวิชาหลักหรือวิชาเลือกอื่นในระดับบัณฑิตศึกษาของหลักสูตรอื่นทั้งในและนอกคณะสถิติประยุกต์ ทั้งนี้ ให้เป็นไปตามคำแนะนำและได้รับการอนุญาตจากอาจารย์ที่ปรึกษาและอาจารย์ผู้สอนในรายวิชานั้น

2. การจัดการเรียนการสอนในหมวดวิชาเลือกให้เป็นไปตามที่คณะและสถาบันกำหนด

(4) หมวดวิชาการค้นคว้าอิสระ

		นับหน่วยกิต
สมซ 9000	การค้นคว้าอิสระ	3(0–0–12)
CRM 9000	Independent Study	

(5) หมวดวิชาวิทยานิพนธ์

		นับหน่วยกิต
สมซ 9004	วิทยานิพนธ์	12 หน่วยกิต
CRM 9004	Thesis	

4. แผนการศึกษา

แผน 1 วิชาการ (ทำวิทยานิพนธ์)

ปีที่ 1 ภาคการศึกษาที่ 1		
สพ 4000	พื้นฐานสำหรับบัณฑิตศึกษา	3 หน่วยกิต */**/***
ภส 4001	การพัฒนาทักษะการอ่านภาษาอังกฤษสำหรับบัณฑิตศึกษา	3 หน่วยกิต */**
สมช 4XXX	วิชาเสริมพื้นฐานของคณะ	3–6 หน่วยกิต *
สมช 6XXX	วิชาหลัก 2 วิชา	6 หน่วยกิต
รวม		**6 หน่วยกิต**
ปีที่ 1 ภาคการศึกษาที่ 2		
ภส 4002	การพัฒนาทักษะภาษาอังกฤษแบบบูรณาการ	3 หน่วยกิต */**
สมช 4XXX	วิชาเสริมพื้นฐานของคณะ	3 หน่วยกิต *
สมช 6XXX	วิชาหลัก 1 วิชา	3 หน่วยกิต
สมช 7XXX หรือ	วิชาเลือก 1 วิชา	3 หน่วยกิต
สมช 8XXX		
รวม		**6 หน่วยกิต**
ปีที่ 2 ภาคการศึกษาที่ 1		
สมช 7XXX หรือ	วิชาเลือก 3 วิชา	9 หน่วยกิต
สมช 8XXX		
รวม		**9 หน่วยกิต**
	สอบประมวลความรู้	
ปีที่ 2 ภาคการศึกษาที่ 2		
สมช 7XXX หรือ	วิชาเลือก 1 วิชา	3 หน่วยกิต
สมช 8XXX		
สมช 9004	วิทยานิพนธ์	3 หน่วยกิต
รวม		**6 หน่วยกิต**
ปีที่ 3 ภาคการศึกษาที่ 1		
สมช 9004	วิทยานิพนธ์	9 หน่วยกิต
รวม		**9 หน่วยกิต**
ปีที่ 3 ภาคการศึกษาที่ 2		
	สอบวิทยานิพนธ์	

* ไม่นับหน่วยกิต

** วิชาเสริมพื้นฐานสำหรับนักศึกษาภาคปกติ

*** กำหนดให้เรียนก่อนเปิดภาคการศึกษา

หมายเหตุ จะต้องเสนอหัวข้อวิทยานิพนธ์ให้ผ่านภายในสองภาคการศึกษาหลังจากลงทะเบียนรายวิชาครบถ้วนตามหลักสูตรแผน 1 (ทำวิทยานิพนธ์)

แผน 2 วิชาชีพ (ไม่ทำวิทยานิพนธ์)

ปีที่ 1 ภาคการศึกษาที่ 1		
สพ 4000	พื้นฐานสำหรับบัณฑิตศึกษา	3 หน่วยกิต */**/***
ภส 4001	การพัฒนาทักษะการอ่านภาษาอังกฤษสำหรับบัณฑิตศึกษา	3 หน่วยกิต */**
สมช 4XXX	วิชาเสริมพื้นฐาน	3–6 หน่วยกิต *
สมช 6XXX	วิชาหลัก 2 วิชา	6 หน่วยกิต
รวม		**6 หน่วยกิต**
ปีที่ 1 ภาคการศึกษาที่ 2		
ภส 4002	การพัฒนาทักษะภาษาอังกฤษแบบบูรณาการ	3 หน่วยกิต */**
สมช 4XXX	วิชาเสริมพื้นฐานของคณะ	3 หน่วยกิต *
สมช 6XXX	วิชาหลัก 1 วิชา	3 หน่วยกิต
สมช 7XXX หรือ	วิชาเลือก 1 วิชา	3 หน่วยกิต
สมช 8XXX		
รวม		**6 หน่วยกิต**
ปีที่ 2 ภาคการศึกษาที่ 1		
สมช 7XXX หรือ	วิชาเลือก 3 วิชา	9 หน่วยกิต
สมช 8XXX		
รวม		**9 หน่วยกิต**
	สอบประมวลความรู้	
ปีที่ 2 ภาคการศึกษาที่ 2		
สมช 7XXX หรือ	วิชาเลือก 3 วิชา	9 หน่วยกิต
สมช 8XXX		
รวม		**9 หน่วยกิต**
ปีที่ 3 ภาคการศึกษาที่ 1		
สมช 7XXX หรือ	วิชาเลือก 1 วิชา	3 หน่วยกิต
สมช 8XXX		
สมช 9000	การค้นคว้าอิสระ	3 หน่วยกิต
รวม		**6 หน่วยกิต**
ปีที่ 3 ภาคการศึกษาที่ 2		
	สอบปากเปล่า	

* ไม่นับหน่วยกิต

** วิชาเสริมพื้นฐานสำหรับนักศึกษาภาคปกติ

*** กำหนดให้เรียนก่อนเปิดภาคการศึกษา

5. คำอธิบายรายวิชา

สพ 4000 พื้นฐานสำหรับบัณฑิตศึกษา 3(2–2–5)

ND 4000 Foundations for Graduate Studies

วิชานี้เพื่อพัฒนาทักษะด้านต่าง ๆ ให้มีประสิทธิภาพตามแนวทางการพัฒนาที่ยั่งยืน (SDGs) และให้สอดคล้องกับทักษะและองค์ความรู้ที่สถาบันให้ความสำคัญ ซึ่งเป็นทักษะเฉพาะ จำนวน 4 ด้าน คือ 1) ด้านดิจิทัล 2) ด้านการเป็นพลเมืองโลก 3) ด้านการพัฒนาภาวะความเป็นผู้นำ และ 4) ด้านการพัฒนาที่ยั่งยืน

This course is designed to enhance a range of skills in accordance with the principles of sustainable development (SDGs) and the core competencies emphasized by the institution. The course focuses on four key skill sets: 1. Digital Literacy, 2. Glocal Citizenship, 3. Leadership Development, and 4. Sustainable Development.

ภส 4001 การพัฒนาทักษะการอ่านภาษาอังกฤษสำหรับบัณฑิตศึกษา 3(3–0–6)

LC 4001 Reading Skills Development in English for Graduate Studies

วิชานี้สร้างเสริมทักษะการอ่านบทความจากหลากหลายสาขาวิชา ซึ่งประกอบด้วยทักษะการอ่านเพื่อจับใจความสำคัญและสนับสนุน การตีความประโยค การเข้าใจจุดประสงค์และน้ำเสียงของผู้เขียน การอ่านแบบข้ามเพื่อหาข้อมูลเฉพาะ การตีความคำพูดอ้างอิงและข้อมูลจากรูปภาพ การหาความสัมพันธ์ของประโยค การเดาความหมายของคำศัพท์และสำนวนจากบริบท โดยในการพัฒนาทักษะเหล่านี้ นักศึกษาจะมีโอกาสในการทำกิจกรรมเพื่อเพิ่มพูนคำศัพท์ การคิดเชิงวิพากษ์และการทำงานร่วมกันควบคู่ไปทุกครั้ง

This course is aimed at enhancing English reading skills necessary for reading texts from a variety of academic disciplines. Emphasis is placed on identifying an argument (main idea) and supporting details, making inferences, identifying purpose and tone, scanning, interpreting quotes and graphic information, recognizing discourse organization, and using context clues to understand terminology and fixed expressions. Through reading practice, students will engage in a sequence of vocabulary-expanding, critical thinking and collaboration activities.

ภส 4002 การพัฒนาทักษะภาษาอังกฤษแบบบูรณาการ 3(3–0–6)

LC 4002 Integrated English Language Skills Development

วิชานี้มีเนื้อหาและกิจกรรมที่มุ่งเน้นการเรียนการสอนแบบบูรณาการทักษะทั้ง 4 ทักษะ คือ การฟัง การพูด การอ่านและการเขียนเชิงวิชาการเบื้องต้น

This course is aimed at providing contents and teaching activities that focus on the integrated skills of listening, speaking, reading and writing with a particular emphasis on academic writing at the introductory level.

ภส 4011 การซ่อมเสริมการพัฒนาทักษะการอ่านภาษาอังกฤษสำหรับบัณฑิตศึกษา 3(3–0–6)

LC 4011 Remedial Reading Skills Development in English for Graduate Studies

วิชานี้เน้นการฝึกทักษะและกลยุทธ์การอ่านภาษาอังกฤษเชิงวิชาการเพิ่มเติมและซ่อมเสริมทักษะดังกล่าวสำหรับนักศึกษาที่ยังบกพร่องในการเรียนวิชา ภส 4001 การพัฒนาทักษะการอ่านภาษาอังกฤษสำหรับบัณฑิตศึกษา ทั้งนี้ นักศึกษาจะได้รับการฝึกฝนในลักษณะเฉพาะบุคคลมากขึ้น

The course is intended to provide additional practices in the reading skills and strategies covered in LC 4001 Reading Skills Development in English for Graduate Studies. Students receive individualized attention to enhance their reading skills for academic purposes.

ภส 4012 การซ่อมเสริมการพัฒนาทักษะภาษาอังกฤษแบบบูรณาการ 3(3–0–6)

LC 4012 Remedial Integrated English Language Skills Development

วิชานี้เน้นการฝึกทักษะการฟัง การพูด การอ่าน และการเขียนเพิ่มเติมและซ่อมเสริมทักษะดังกล่าวสำหรับนักศึกษาที่ยังบกพร่องในการเรียนวิชา ภส 4002 การพัฒนาทักษะภาษาอังกฤษแบบบูรณาการ เพื่อปรับปรุงความสามารถในการใช้ภาษาอังกฤษเพื่อการสื่อสารด้วยการสอนและฝึกในลักษณะเฉพาะบุคคล

This course is intended to provide additional practice in the four skills—listening, speaking, reading and writing strategies covered in LC 4002 Integrated English Language Skills Development. Students receive individualized attention to enhance their communication skills in English.

สมซ 4001 ระบบกฎหมายและนิติวิธีสำหรับดิจิทัลและไซเบอร์ 3(3–0–6)

CRM 4001 Legal Systems and Methods for Digital and Cyber Contexts

ระบบกฎหมายและแหล่งที่มาของกฎหมาย นิติวิธีและการตีความกฎหมาย โครงสร้างศาลและกระบวนการยุติธรรม หลักกฎหมายแพ่ง–พาณิชย์ที่เกี่ยวกับธุรกรรมดิจิทัล หลักกฎหมายอาญาที่เกี่ยวกับเทคโนโลยีสารสนเทศ หลักฐานดิจิทัลและสายโซ่การรับรอง บทนำกฎหมายคอมพิวเตอร์ กฎหมายความมั่นคงปลอดภัยไซเบอร์ และกฎหมายคุ้มครองข้อมูลส่วนบุคคล จริยธรรมวิชาชีพด้านกฎหมายและความมั่นคงปลอดภัยไซเบอร์

Legal systems and sources of law, legal methodology and statutory interpretation, court structures and justice processes, basic civil and commercial law for digital transactions, criminal law related to information technology, digital evidence and chain of custody, introduction to computer law, cybersecurity law, and data protection law, professional ethics in law and cybersecurity

สมซ 4002 การปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์และศูนย์ปฏิบัติการ 3(2–2–5)

CRM 4002 Cybersecurity Operations and SOC

ภูมิทัศน์ภัยคุกคามไซเบอร์ แนวคิดการปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ บทบาทและสถาปัตยกรรมศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ (SOC) ระบบบันทึกเหตุการณ์และการจัดการบันทึก การใช้งานพื้นฐานของระบบ SIEM แนวคิดและบทบาทของ EDR และ XDR วงจรการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ การวิเคราะห์เหตุการณ์จากบันทึกและหลักฐานดิจิทัลเบื้องต้น ข่าวกรองภัยคุกคามไซเบอร์ กรอบ MITRE ATT&CK แนวคิดพื้นฐานการล่าภัยคุกคาม สคริปต์และการทำงานอัตโนมัติพื้นฐานเพื่อสนับสนุนการปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์

Cyber threat landscape, cybersecurity operations concepts, security operations center roles and architecture, logging and log management, basic use of SIEM platforms, EDR and XDR concepts, cybersecurity incident response lifecycle, basic incident analysis using logs and digital artifacts, cyber threat intelligence fundamentals, MITRE ATT&CK framework, basic threat hunting concepts, basic scripting and security automation for security operations

สมซ 4003 ภาษาอังกฤษสำหรับการจัดการความเสี่ยงความมั่นคงทางไซเบอร์ 3(3–0–6)

CRM 4003 English for Cybersecurity Risk Management

คำศัพท์ โครงสร้างของประโยค การอ่านบทความงานวิจัยและตำราในสาขาที่เกี่ยวข้อง การเขียนประโยค การลดรูปประโยค การเขียนข้อความในรูปแบบย่อหน้า การพูดและการฟังภาษาอังกฤษในหัวข้อที่เกี่ยวข้อง

Vocabularies, sentence structures, reading research articles and textbooks in related areas, writing sentences, reducing sentences, writing paragraphs, speaking and listening in English on related topics

สมซ 6001 การบริหารความมั่นคงปลอดภัยสารสนเทศ 3(3–0–6)

CRM 6001 Information Security Management

แนวคิดและหลักการบริหารความมั่นคงปลอดภัยสารสนเทศ มาตรฐานและกรอบการบริหารความมั่นคงปลอดภัยสารสนเทศ เช่น ISO/IEC 27001:2022, NIST Cybersecurity Framework, CIS Controls, มาตรฐานระบบบริหารจัดการปัญญาประดิษฐ์ ISO/IEC 42001 การออกแบบและบริหารโครงการด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร, โครงสร้างการกำกับดูแลและบทบาทหน้าที่ด้านความมั่นคงปลอดภัยไซเบอร์ การจัดทำนโยบายและมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ การบริหารบุคลากรและวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์, การบริหารความมั่นคงปลอดภัยของผู้ให้บริการและคู่ค้า, ตัวชี้วัดประสิทธิภาพและตัวชี้วัดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์, การเชื่อมโยงการบริหารความมั่นคงปลอดภัยสารสนเทศกับการกำกับดูแลระบบดิจิทัลและระบบที่ใช้ปัญญาประดิษฐ์

Concepts and principles of information security management, information security management standards and frameworks such as ISO/IEC 27001:2022, NIST Cybersecurity Framework and CIS Controls, AI management system standard ISO/IEC 42001, organizational cybersecurity strategy and program management, security governance structures and roles, development of security policies and controls, human factors and security culture, third-party and supplier security management, security performance and risk metrics, linkage between information security management, digital governance and AI-enabled systems

สมซ 6002 การวิเคราะห์ความเสี่ยงสำหรับความมั่นคงปลอดภัยสารสนเทศ 3(3–0–6)

CRM 6002 Information Security Risk Analysis

แนวคิดและหลักการบริหารความเสี่ยง กรอบการบริหารความเสี่ยงตามมาตรฐาน ISO 31000 และ ISO/IEC 27005 การระบุสินทรัพย์ดิจิทัล ภัยคุกคาม ช่องโหว่ และผลกระทบ การวิเคราะห์และประเมินระดับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ การใช้ตัวชี้วัดและเกณฑ์การยอมรับความเสี่ยง การวิเคราะห์ฉากทัศน์ความเสี่ยง เช่น การโจมตีเรียกค่าไถ่และการรั่วไหลของข้อมูล การใช้กรอบเชิงปริมาณและกึ่งปริมาณในการประเมินความเสี่ยง การจัดทำทะเบียนความเสี่ยงและการเชื่อมโยงกับผลกระทบทางธุรกิจ การใช้กรอบการจัดอันดับความรุนแรงช่องโหว่ เช่น CVSS และ EPSS ประกอบการวิเคราะห์ความเสี่ยง

Risk management concepts and principles, risk management frameworks based on ISO 31000 and ISO/IEC 27005, identification of digital assets threats vulnerabilities and impacts, analysis and evaluation of information security risks, use of risk criteria and risk appetite, risk scenario analysis such as ransomware and data breach, quantitative and semi-quantitative approaches to risk assessment, development of risk registers and linkage to business impacts, use of vulnerability scoring frameworks such as CVSS and EPSS in risk analysis

สมซ 6003 กฎหมายเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ 3(3–0–6)

CRM 6003 Cybersecurity Law

กรอบกฎหมายเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย ความสัมพันธ์ระหว่างกฎหมายความมั่นคงปลอดภัยไซเบอร์ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายโทรคมนาคม และกฎหมายอื่นที่เกี่ยวข้อง บทบาทและอำนาจหน้าที่ของหน่วยงานกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ หลักเกณฑ์เกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภาระหน้าที่ของผู้ให้บริการและผู้ควบคุมระบบสารสนเทศ ระบบการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ตามกฎหมาย การรายงานเหตุการณ์และการแจ้งเตือน กรอบกฎหมายและแนวทางระหว่างประเทศที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ประเด็นด้านสิทธิและเสรีภาพในการดูแลความมั่นคงปลอดภัยไซเบอร์

National cybersecurity legal framework, relationship between cybersecurity law computer crime law telecommunications law and other related legislation, roles and powers of cybersecurity regulators, legal requirements for critical information infrastructure, duties of service providers and system controllers, legal aspects of cybersecurity incident management, incident reporting and notification, international legal and policy frameworks related to cybersecurity, rights and freedoms considerations in cybersecurity enforcement

สมซ 7001 ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และเครือข่าย 3(3–0–6)

CRM 7001 Computer and Network Security

หลักการความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และเครือข่าย สถาปัตยกรรมเครือข่ายและการแบ่งส่วนเครือข่าย ไฟร์วอลล์และระบบป้องกันการบุกรุก ระบบตรวจจับและป้องกันการบุกรุก ความมั่นคงปลอดภัยของโพรโตคอลเครือข่ายและการสื่อสารที่ปลอดภัย เทคโนโลยี VPN และการเข้าถึงจากระยะไกลอย่างปลอดภัย แนวคิดสถาปัตยกรรม Zero Trust และ SASE การรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย การรักษาความมั่นคงปลอดภัยของอุปกรณ์ปลายทางและเซิร์ฟเวอร์ โซลูชัน EDR/XDR และการวิเคราะห์พฤติกรรม การตรวจสอบและการประกันความมั่นคงปลอดภัยของเครือข่าย การจัดการช่องโหว่ด้านเครือข่าย

Principles of computer and network security, network architecture and segmentation, firewalls and intrusion prevention systems, intrusion detection and prevention, secure network protocols and secure communications, VPN technologies and secure remote access, Zero Trust architecture and SASE concepts, wireless network security, endpoint and server hardening, EDR/XDR solutions and behavioral analytics, network monitoring and assurance, network vulnerability management

สมซ 7002 ความมั่นคงปลอดภัยของคลาวด์และระบบคลาวด์เนทีฟ 3(2–2–5)

CRM 7002 Cloud and Cloud-Native Security

สถาปัตยกรรมคลาวด์และรูปแบบการให้บริการ โมเดลความรับผิดชอบร่วมด้านความมั่นคงปลอดภัยของคลาวด์ การบริหารอัตลักษณ์และการเข้าถึงบนคลาวด์ การออกแบบสถาปัตยกรรมความมั่นคงปลอดภัยคลาวด์สำหรับองค์กร การรักษาความมั่นคงปลอดภัยของข้อมูลและการเข้ารหัสบนคลาวด์ การคุ้มครองข้อมูลส่วนบุคคลบนคลาวด์และการโอนข้อมูลข้ามพรมแดน การรักษาความมั่นคงปลอดภัยของคอนเทนเนอร์และ Kubernetes การรักษาความมั่นคงปลอดภัยของโครงสร้างพื้นฐานแบบโค้ด เครื่องมือด้านความมั่นคงปลอดภัยของคลาวด์ เช่น CSPM CWPP และ CIEM การบูรณาการ DevSecOps และความมั่นคงปลอดภัยในกระบวนการ CI/CD การตรวจสอบและตอบสนองเหตุการณ์บนคลาวด์ การใช้ AI/ML ด้านความมั่นคงปลอดภัยบนแพลตฟอร์มคลาวด์

Cloud service models and architectures, shared responsibility model for cloud security, cloud identity and access management, secure cloud architecture design for enterprises, cloud data protection and encryption, privacy and cross-border data transfer in cloud environments, container and Kubernetes security, infrastructure as code security, cloud security tools such as CSPM CWPP and CIEM, DevSecOps and security in CI/CD pipelines, cloud monitoring and incident response, AI/ML-based security capabilities in cloud platforms

สมซ 7003 ปัญญาประดิษฐ์ขั้นสูงสำหรับการปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ 3(2–2–5)

CRM 7003 Advanced AI for Cybersecurity Operations

แนวคิดขั้นสูงด้านปัญญาประดิษฐ์และการประยุกต์ใช้ในความมั่นคงปลอดภัยไซเบอร์ รวมทั้งพื้นฐานปัญญาประดิษฐ์และการเรียนรู้ของเครื่อง สำหรับการวิเคราะห์บันทึกเหตุการณ์และการตรวจจับความผิดปกติ กรอบธรรมาภิบาลและมาตรฐานด้านปัญญาประดิษฐ์ เช่น กรอบการจัดการความเสี่ยงด้านปัญญาประดิษฐ์ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (NIST AI RMF) และมาตรฐานสากล ISO/IEC 42001 การใช้โมเดลภาษาขนาดใหญ่ (LLMs) เพื่อสนับสนุนการวิเคราะห์ log การจัดการแจ้งเตือน การวิเคราะห์เหตุการณ์ และข่าวกรองภัยคุกคามไซเบอร์ ภูมิทัศน์ข่าวกรองภัยคุกคามไซเบอร์และวงจรข่าวกรอง ครอบคลุมแหล่งข่าวกรองแบบเปิด เชิงพาณิชย์ และแบบความร่วมมือ การใช้ปัญญาประดิษฐ์สนับสนุนการรวบรวม เพิ่มคุณค่า และวิเคราะห์ข่าวกรองภัยคุกคาม กรอบ MITRE ATT&CK และการเชื่อมโยงบันทึกเหตุการณ์กับเทคนิคการโจมตี การออกแบบกฎตรวจจับและการล่าภัยคุกคามเชิงสมมติฐานที่เสริมด้วยปัญญาประดิษฐ์ การออกแบบกรณีใช้งานการล่าภัยคุกคาม ตัวชี้วัด และคู่มือการปฏิบัติงาน แนวคิดและสถาปัตยกรรมของแพลตฟอร์มการสั่งการและตอบสนองด้านความมั่นคงปลอดภัยอัตโนมัติ (SOAR) การออกแบบขั้นตอนการทำงาน และคู่มือการปฏิบัติงาน สำหรับการตอบสนองเหตุการณ์แบบกึ่งอัตโนมัติและอัตโนมัติเต็มรูปแบบ การใช้สคริปต์และการเชื่อมต่อผ่านส่วนต่อประสานโปรแกรมประยุกต์ ระหว่าง SIEM EDR/XDR แหล่งข่าวกรองภัยคุกคาม และ SOAR เพื่อสนับสนุนระบบอัตโนมัติด้านความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยงและการโจมตีต่อระบบปัญญาประดิษฐ์ ในบริบทความมั่นคงปลอดภัยไซเบอร์ เช่น การหลอกลวงโมเดล การวางยาข้อมูล การขโมยโมเดลและการโจมตีผ่านคำสั่ง แนวปฏิบัติและกรอบธรรมาภิบาลสำหรับการใช้ปัญญาประดิษฐ์ ในการปฏิบัติการของ SOC และการจัดการความเสี่ยงจากปัญญาประดิษฐ์ กรณีศึกษาและโครงงานเชิงปฏิบัติด้านการล่าภัยคุกคามและระบบอัตโนมัติด้านความมั่นคงปลอดภัยไซเบอร์ที่ขับเคลื่อนด้วยปัญญาประดิษฐ์

Advanced concepts of artificial intelligence and its applications in cybersecurity, including AI/ML foundations for log analytics and anomaly detection, AI governance frameworks and standards such as NIST AI RMF and ISO/IEC 42001, leveraging large language models (LLMs) to support log analysis, alert triage, incident analysis and cyber threat intelligence, cyber threat intelligence landscape and intelligence lifecycle with open-source, commercial and collaborative threat intelligence sources, AI-assisted threat intelligence collection, enrichment and analysis, MITRE ATT&CK framework and mapping logs and incidents to attack techniques, AI-enhanced detection engineering and hypothesis-driven threat hunting methodologies, design of threat hunting use cases, indicators and playbooks, concepts and architectures of security automation and SOAR platforms, design of semi-automated and fully automated incident response workflows and playbooks, scripting and API integration across SIEM, EDR/XDR, threat intelligence feeds and SOAR for security automation, risks and attacks against AI systems in cybersecurity such as adversarial machine learning, data poisoning, model theft and prompt injection, secure practices and governance frameworks for using AI in SOC operations and managing AI-related cyber risks, case studies and hands-on projects on AI-enabled threat hunting and security automation workflows

สมซ 7004 การทดสอบการเจาะระบบและการจัดการช่องโหว่ 3(2–2–5)

CRM 7004 Penetration Testing and Vulnerability Management

หลักการและขั้นตอนการทดสอบการเจาะระบบ การกำหนดขอบเขตและข้อตกลงการทดสอบ เทคนิคการสแกนและทำแผนที่เครือข่าย การทดสอบความมั่นคงปลอดภัยของบริการเครือข่ายและเว็บแอปพลิเคชัน OWASP Top Ten และความมั่นคงปลอดภัยของ API การใช้เครื่องมือสำหรับการทดสอบการเจาะระบบ การวิเคราะห์และจัดลำดับความสำคัญของช่องโหว่ วงจรการบริหารจัดการช่องโหว่ (สแกน ประเมิน แก้ไข และยืนยันผล) การเชื่อมโยงผลการทดสอบกับกระบวนการ DevSecOps และ CI/CD แนวคิด Red Team Blue Team และ Purple Team จริยธรรมและกรอบกฎหมายในการทดสอบการเจาะระบบ

Penetration testing principles and methodologies, scope definition and rules of engagement, network scanning and reconnaissance techniques, network service and web application security testing, OWASP Top Ten and API security, tools for penetration testing, vulnerability analysis and prioritization, vulnerability management lifecycle (scan assess remediate verify), integration of penetration testing and vulnerability findings into DevSecOps and CI/CD pipelines, Red Team Blue Team and Purple Team concepts, ethics and legal frameworks of penetration testing

สมซ 7005 นิติดิจิทัลและการสืบสวน 3(3–0–6)

CRM 7005 Digital Forensics and Investigations

หลักการและกระบวนการนิติดิจิทัล การเก็บรักษาและวิเคราะห์พยานหลักฐานดิจิทัล การสืบสวนระบบปฏิบัติการและไฟล์ระบบ การสืบสวนเครือข่ายและบันทึกเหตุการณ์ การสืบสวนอุปกรณ์พกพาและแอปพลิเคชัน การสืบสวนบนคลาวด์และสภาพแวดล้อมเสมือน การวิเคราะห์หน่วยความจำและมัลแวร์เบื้องต้น กรอบการตอบสนองเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ การใช้ข่าวกรองภัยคุกคามไซเบอร์สนับสนุนการสืบสวน การล่าภัยคุกคามเชิงลึกจากบันทึกและอุปกรณ์ปลายทาง การประยุกต์ใช้เครื่องมืออัตโนมัติและสคริปต์ในการสืบสวน การจัดทำรายงานนิติดิจิทัลเพื่อใช้ในกระบวนการยุติธรรม จริยธรรมและกฎหมายที่เกี่ยวข้องกับงานนิติดิจิทัล

Principles and processes of digital forensics, preservation and analysis of digital evidence, operating system and file system forensics, network and log forensics, mobile device and application forensics, cloud and virtual environment forensics, basic memory and malware analysis, cybersecurity incident response frameworks, use of cyber threat intelligence in investigations, advanced threat hunting using logs and endpoints, automation and scripting in digital forensics, digital forensic reporting for legal proceedings, ethics and legal issues in digital forensics

สมซ 7006 นโยบายความมั่นคงปลอดภัยสารสนเทศ 3(3–0–6)

CRM 7006 Information Security Policy

บทบาทและความสำคัญของนโยบายความมั่นคงปลอดภัยสารสนเทศ โครงสร้างและลำดับชั้นของเอกสารด้านความมั่นคงปลอดภัยสารสนเทศ การออกแบบนโยบาย มาตรฐาน แนวปฏิบัติ และระเบียบการปฏิบัติ การกำหนดขอบเขตและเป้าหมายของนโยบาย นโยบายสำหรับระบบคลาวด์และการทำงานจากระยะไกล นโยบายอุปกรณ์ส่วนบุคคลและการนำอุปกรณ์มาใช้ในงาน (BYOD) นโยบายการบริหารบัญชีผู้ใช้และรหัสผ่าน นโยบายการจัดการเหตุการณ์และการแจ้งเหตุ นโยบายการคุ้มครองข้อมูลและความเป็นส่วนตัว นโยบายการพัฒนาและจัดการซอฟต์แวร์และ DevSecOps การบริหารการเผยแพร่ การฝึกอบรม และการสร้างวัฒนธรรมด้านนโยบาย การทบทวนและปรับปรุงนโยบายตามกฎหมายและมาตรฐานที่เปลี่ยนแปลง

Roles and importance of information security policy, structure and hierarchy of security documentation, design of policies standards guidelines and procedures, defining policy scope and objectives, policies for cloud systems and remote work, BYOD and personal device policies, account and password management policies, incident management and notification policies, data protection and privacy policies, secure software development and DevSecOps policies, policy communication training and security culture, policy review and updates according to changing laws and standards

สมซ 7007 การกำกับดูแลระบบสารสนเทศ 3(3–0–6)

CRM 7007 Information Systems Governance

แนวคิดและหลักการกำกับดูแลเทคโนโลยีสารสนเทศ กรอบการกำกับดูแลเช่น COBIT และ ITIL บทบาทของคณะกรรมการและผู้บริหารระดับสูงในการกำกับดูแลด้านเทคโนโลยีและความมั่นคงปลอดภัยไซเบอร์ การเชื่อมโยงกลยุทธ์ด้านดิจิทัลกับเป้าหมายองค์กร โครงสร้างและกระบวนการกำกับดูแลด้านข้อมูลและระบบสารสนเทศ การกำกับดูแลโครงการด้านดิจิทัลและระบบสารสนเทศ การจัดการผู้รับจ้างและผู้ให้บริการภายนอก การบูรณาการการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์กับการบริหารความเสี่ยงองค์รวม การประเมินความคุ้มค่าการลงทุนด้านเทคโนโลยีและความมั่นคงปลอดภัยไซเบอร์ ความเชื่อมโยงกับกรอบ ESG และความยั่งยืน ตัวชี้วัดด้านการกำกับดูแลระบบสารสนเทศและความมั่นคงปลอดภัยไซเบอร์

Concepts and principles of IT governance, governance frameworks such as COBIT and ITIL, roles of boards and senior executives in technology and cybersecurity oversight, alignment of digital strategy with organizational objectives, data and information systems governance structures and processes, governance of digital and IT projects, management of vendors and outsourced services, integration of cybersecurity governance with enterprise risk management, evaluation of investments in technology and security, linkage with ESG and sustainability frameworks, governance metrics for information systems and cybersecurity

สมซ 7008 กฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ 3(3–0–6)

CRM 7008 Cybercrime Law

กรอบกฎหมายเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ ประเภทของอาชญากรรมทางคอมพิวเตอร์และอาชญากรรมที่ใช้เทคโนโลยีสนับสนุน การโจมตีระบบและข้อมูล การเข้าถึงโดยมิชอบ และการแทรกแซงข้อมูล อาชญากรรมออนไลน์ เช่น การหลอกลวง ฟิชชิง การโจมตีแบบเรียกค่าไถ่ การฟอกเงินและการใช้สกุลเงินดิจิทัลในอาชญากรรมไซเบอร์ กระบวนการสืบสวนและรวบรวมหลักฐานทางคอมพิวเตอร์ตามกฎหมาย บทบาทของหน่วยงานบังคับใช้กฎหมายและหน่วยงานกำกับดูแล แนวคิดเกี่ยวกับอนุสัญญาระหว่างประเทศด้านอาชญากรรมไซเบอร์ ประเด็นด้านสิทธิส่วนบุคคลและเสรีภาพในการดำเนินคดีอาชญากรรมไซเบอร์

Legal framework for computer-related offenses, types of cyber-dependent and cyber-enabled crimes, system and data attacks unauthorized access and data interference, online crimes such as fraud phishing and ransomware, money laundering and use of cryptocurrencies in cybercrime, legal procedures for investigation and digital evidence collection, roles of law enforcement and regulatory agencies, international conventions and cooperation on cybercrime, privacy and civil liberties issues in cybercrime enforcement

สมซ 7009 กฎหมายพาณิชย์อิเล็กทรอนิกส์และธุรกิจดิจิทัล 3(3–0–6)

CRM 7009 Electronic Commerce and Digital Business Law

กรอบกฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ สัญญาอิเล็กทรอนิกส์และการทำธุรกรรมออนไลน์ ลายมือชื่ออิเล็กทรอนิกส์และการรับรองความน่าเชื่อถือ ความรับผิดของผู้ให้บริการตัวกลางและเจ้าของแพลตฟอร์มดิจิทัล การคุ้มครองผู้บริโภคออนไลน์ การโฆษณาทางดิจิทัลและการส่งเสริมการขาย การชำระเงินอิเล็กทรอนิกส์และบริการทางการเงินดิจิทัล การยืนยันตัวตนลูกค้าและมาตรการป้องกันการฟอกเงิน การค้าขายข้ามพรมแดนและกฎหมายที่เกี่ยวข้อง ข้อพิพาททางพาณิชย์อิเล็กทรอนิกส์และกระบวนการระงับข้อพิพาท ความเชื่อมโยงกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลและความเป็นส่วนตัว

Legal framework for electronic transactions, electronic contracts and online transactions, electronic signatures and trust services, liability of intermediaries and digital platform operators, online consumer protection, digital advertising and marketing practices, electronic payments and digital financial services, customer due diligence and anti-money laundering measures, cross-border e-commerce and relevant regulations, e-commerce disputes and dispute resolution mechanisms, interaction with data protection and privacy laws

สมซ 7010 กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและความเป็นส่วนตัว 3(3–0–6)

CRM 7010 Data Protection and Privacy Law

หลักการพื้นฐานของการคุ้มครองข้อมูลส่วนบุคคล กรอบกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย ฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล สิทธิของเจ้าของข้อมูลและหน้าที่ของผู้ควบคุมและผู้ประมวลผลข้อมูล การจัดทำบันทึกรายการประมวลผลและการประเมินผลกระทบด้านการคุ้มครองข้อมูล (DPIA) การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล การโอนข้อมูลส่วนบุคคลข้ามพรมแดน ข้อกำหนดเฉพาะในภาคส่วนต่าง ๆ การเปรียบเทียบกับกรอบกฎหมายต่างประเทศ เช่น GDPR แนวคิดความเป็นส่วนตัวโดยออกแบบและโดยค่าเริ่มต้น บทบาทของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) การบูรณาการกฎหมายคุ้มครองข้อมูลในกระบวนการบริหารความเสี่ยงและธรรมาภิบาลข้อมูล

Fundamental principles of personal data protection, national personal data protection legal framework, legal bases for processing personal data, data subject rights and duties of controllers and processors, records of processing activities and data protection impact assessment, personal data breach notification, cross-border data transfers, sector-specific data protection requirements, comparison with international frameworks such as GDPR, privacy by design and by default, role of data protection officers, integration of data protection law into risk management and data governance

สมซ 7011 การจัดการความเสี่ยงสำหรับเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยสารสนเทศ 3(3–0–6)

CRM 7011 Information Security and IT Risk Management

กรอบการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยสารสนเทศ การบูรณาการการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศกับการบริหารความเสี่ยงองค์รวมขององค์กร การวิเคราะห์ความเสี่ยงเชิงสถานการณ์และการวิเคราะห์สถานการณ์เลวร้าย การจัดการความเสี่ยงด้านไซเบอร์ในห่วงโซ่อุปทานและผู้ให้บริการภายนอก การใช้ตัวชี้วัดความเสี่ยงด้านไซเบอร์และตัวชี้วัดประสิทธิภาพการจัดการความเสี่ยง การจัดทำแดชบอร์ดรายงานความเสี่ยงสำหรับผู้บริหารและคณะกรรมการ การออกแบบและติดตามแผนการจัดการความเสี่ยง การพิจารณาการทำประกันความเสี่ยงไซเบอร์ การเชื่อมโยงการจัดการความเสี่ยงกับความยืดหยุ่นขององค์กรด้านไซเบอร์

IT and information security risk management frameworks, integration of IT and cybersecurity risk management with enterprise risk management, scenario-based and stress-testing approaches to cyber risk, cyber risk in supply chains and third-party relationships, cyber risk indicators and performance metrics, risk dashboards and reporting to executives and boards, design and tracking of risk treatment plans, consideration of cyber insurance, linkage between cyber risk management and organizational cyber resilience

สมซ 7012 การตรวจสอบความมั่นคงปลอดภัยสารสนเทศ 3(3–0–6)

CRM 7012 Information Security Auditing

หลักการและแนวคิดการตรวจสอบความมั่นคงปลอดภัยสารสนเทศ บทบาทของการตรวจสอบในระบบการบริหารความมั่นคงปลอดภัยสารสนเทศ การวางแผนและดำเนินการตรวจสอบตามมาตรฐาน ISO/IEC 27001:2022 และมาตรฐานที่เกี่ยวข้อง การสำรวจและประเมินการออกแบบและประสิทธิผลของมาตรการควบคุมด้านความมั่นคงไซเบอร์ การใช้กรอบการประเมินระดับความพร้อมและขีดความสามารถด้านความมั่นคงปลอดภัย การใช้เทคนิคและเครื่องมือวิเคราะห์ข้อมูลสนับสนุนการตรวจสอบ แนวคิดการเฝ้าระวังควบคุมอย่างต่อเนื่อง การจัดทำรายงานการตรวจสอบและติดตามการแก้ไขข้อบกพร่อง การประสานงานระหว่างสายงานตรวจสอบ บริหารความเสี่ยงและความมั่นคงปลอดภัยไซเบอร์ จริยธรรมและมาตรฐานวิชาชีพการตรวจสอบระบบสารสนเทศ

Principles and concepts of information security auditing, role of auditing in information security management systems, planning and conducting audits in accordance with ISO/IEC 27001:2022 and related standards, assessment of design and effectiveness of cybersecurity controls, security maturity and readiness assessments, use of data analytics tools in security auditing, continuous control monitoring concepts, audit reporting and follow-up of corrective actions, coordination among audit risk management and cybersecurity functions, ethics and professional standards in IT and security auditing

สมซ 8701 การศึกษาเฉพาะเรื่องทางการจัดการความเสี่ยงความมั่นคงทางไซเบอร์ 1 1(1–0–2)

CRM 8701 Selected Topics in Cybersecurity Risk Management 1

หัวข้อวิจัยเฉพาะทางการจัดการความเสี่ยงความมั่นคงทางไซเบอร์

Selected research topics in Cybersecurity Risk Management

สมซ 8702 การศึกษาเฉพาะเรื่องทางการจัดการความเสี่ยงความมั่นคงทางไซเบอร์ 2 2(2–0–4)

CRM 8702 Selected Topics in Cybersecurity Risk Management 2

หัวข้อวิจัยเฉพาะทางการจัดการความเสี่ยงความมั่นคงทางไซเบอร์

Selected research topics in Cybersecurity Risk Management

สมซ 8703 การศึกษาเฉพาะเรื่องทางการจัดการความเสี่ยงความมั่นคงทางไซเบอร์ 3 3(3–0–6)

CRM 8703 Selected Topics in Cybersecurity Risk Management 3

หัวข้อวิจัยเฉพาะทางการจัดการความเสี่ยงความมั่นคงทางไซเบอร์

Selected research topics in Cybersecurity Risk Management

สมซ 9000 การค้นคว้าอิสระ 3(0–0–12)

CRM 9000 Independent Study

การกำหนดประเด็นปัญหาและหัวข้อการวิจัยด้านการจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ การทบทวนวรรณกรรมด้านความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยงไซเบอร์ และกฎหมายที่เกี่ยวข้อง การเลือกแนวทางและระเบียบวิธีวิจัยที่เหมาะสม การออกแบบและเก็บรวบรวมข้อมูลเชิงปริมาณหรือเชิงคุณภาพ การประยุกต์ใช้เครื่องมือและเทคนิคการวิเคราะห์ข้อมูล การตีความผลการศึกษาและเชื่อมโยงกับทฤษฎีและการปฏิบัติ การจัดทำรายงานการค้นคว้าอิสระเชิงวิชาการ การนำเสนอผลงานวิชาการด้านการจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ จริยธรรมการวิจัยและการคุ้มครองข้อมูลในการวิจัย

Identification of research problems and topics in cybersecurity risk management, literature review in cybersecurity cyber risk and related laws, selection of appropriate research approaches and methodologies, design and collection of quantitative or qualitative data, application of data analysis tools and techniques, interpretation of findings and linkage to theory and practice, preparation of academic independent study reports, presentation of research results in cybersecurity risk management, research ethics and data protection in research

สมซ 9004 วิทยานิพนธ์ 12 หน่วยกิต

CRM 9004 Thesis

การกำหนดปัญหาวิจัยและคำถามวิจัยด้านการจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ การสำรวจและสังเคราะห์วรรณกรรมอย่างเป็นระบบ การออกแบบกรอบแนวคิดและสมมติฐานการวิจัย การเลือกและใช้ระเบียบวิธีวิจัยขั้นสูง การเก็บรวบรวมและวิเคราะห์ข้อมูลเชิงลึก การสร้างหรือพัฒนาแบบจำลอง เครื่องมือ หรือนวัตกรรมด้านความมั่นคงปลอดภัยไซเบอร์และการจัดการความเสี่ยง การอภิปรายผลและข้อเสนอเชิงนโยบายหรือเชิงปฏิบัติ การเขียนและจัดทำวิทยานิพนธ์ตามมาตรฐานวิชาการ การเผยแพร่ผลงานวิชาการและงานวิจัย จริยธรรมการวิจัย การคุ้มครองข้อมูล และการอ้างอิงงานวิจัยอย่างถูกต้อง

Formulation of research problems and questions in cybersecurity risk management, systematic literature review and synthesis, development of conceptual frameworks and research hypotheses, selection and application of advanced research methodologies, collection and analysis of in-depth data, development of models tools or innovations in cybersecurity and risk management, discussion of results and policy or practical implications, thesis writing in accordance with academic standards, dissemination of research outputs, research ethics data protection and proper citation practices

หมวดที่ 4 การบริหารจัดการหลักสูตร

1. อาจารย์ผู้รับผิดชอบหลักสูตร

ตำแหน่งทางวิชาการ/ ชื่อ – สกุล	คุณวุฒิสูงสุด/สาขาวิชา	สถาบันที่สำเร็จการศึกษา/ ปี พ.ศ. ที่สำเร็จการศึกษา
ผศ.ดร.ปราโมทย์ ลือนาม	Ph.D. (Information Systems) M.S. (Information Systems) บธ.ม. (การจัดการ) วท.ม. (วิทยาการคอมพิวเตอร์) วศ.บ. (ชลประทาน)	University of Maryland (UMBC), U.S.A. (ค.ศ. 2008) University of Maryland (UMBC), U.S.A. (ค.ศ. 2002) มหาวิทยาลัยเกษตรศาสตร์ (พ.ศ. 2541) จุฬาลงกรณ์มหาวิทยาลัย (พ.ศ. 2536) มหาวิทยาลัยเกษตรศาสตร์ (พ.ศ. 2530)
รศ.ดร.โอม ศรนิล	Ph.D. (Computer Science and Applications) M.S. (Computer Science) วศ.บ. (วิศวกรรมไฟฟ้า) (เกียรตินิยมอันดับสอง)	Virginia Polytechnic Institute and State University, U.S.A. (ค.ศ. 2001) Syracuse University, U.S.A. (ค.ศ. 1997) มหาวิทยาลัยเกษตรศาสตร์ (พ.ศ. 2536)
ผศ.ดร.รัฐกร พูลทรัพย์	Sc.D. (Computer Science) M.B.A (Computer Information System) พบ.ม. (สถิติประยุกต์) วท.บ. (คอมพิวเตอร์)	University of Massachusetts Lowell, U.S.A. (ค.ศ. 2003) New Hampshire College, U.S.A. (ค.ศ. 1996) สถาบันบัณฑิตพัฒนบริหารศาสตร์ (พ.ศ. 2534) มหาวิทยาลัยรามคำแหง (พ.ศ. 2532)

2. อาจารย์ประจำหลักสูตร

ตำแหน่งทางวิชาการ/ ชื่อ – สกุล	คุณวุฒิสูงสุด/สาขาวิชา	สถาบันที่สำเร็จการศึกษา/ ปี พ.ศ. ที่สำเร็จการศึกษา
ผศ.ดร.ปราโมทย์ ลือนาม	Ph.D. (Information Systems) M.S. (Information Systems) บธ.ม. (การจัดการ) วท.ม. (วิทยาการคอมพิวเตอร์) วศ.บ. (ชลประทาน)	University of Maryland (UMBC), U.S.A. (ค.ศ. 2008) University of Maryland (UMBC), U.S.A. (ค.ศ. 2002) มหาวิทยาลัยเกษตรศาสตร์ (พ.ศ. 2541) จุฬาลงกรณ์มหาวิทยาลัย (พ.ศ. 2536) มหาวิทยาลัยเกษตรศาสตร์ (พ.ศ. 2530)

ตำแหน่งทางวิชาการ/ ชื่อ – สกุล	คุณวุฒิสูงสุด/สาขาวิชา	สถาบันที่สำเร็จการศึกษา/ ปี พ.ศ. ที่สำเร็จการศึกษา
รศ.ดร.โอม ศรนิล	Ph.D. (Computer Science and Applications) M.S. (Computer Science) วศ.บ. (วิศวกรรมไฟฟ้า) (เกียรตินิยมอันดับสอง)	Virginia Polytechnic Institute and State University, U.S.A. (ค.ศ. 2001) Syracuse University, U.S.A. (ค.ศ. 1997) มหาวิทยาลัยเกษตรศาสตร์ (พ.ศ. 2536)
ผศ.ดร.รัฐกร พูลทรัพย์	Sc.D. (Computer Science) M.B.A (Computer Information System) พบ.ม. (สถิติประยุกต์) วท.บ. (คอมพิวเตอร์)	University of Massachusetts Lowell, U.S.A. (ค.ศ. 2003) New Hampshire College, U.S.A. (ค.ศ. 1996) สถาบันบัณฑิตพัฒนบริหารศาสตร์ (พ.ศ. 2534) มหาวิทยาลัยรามคำแหง (พ.ศ. 2532)
รศ.ดร.ฐิติรัตน์ ศิริบวรรัตนกุล	Ph.D. (Electrical Engineering and Information Systems) M.E. (Electronic Engineering) วศ.บ. (วิศวกรรมคอมพิวเตอร์)	The University of Tokyo, Japan. (ค.ศ. 2011) The University of Tokyo, Japan. (ค.ศ. 2008) จุฬาลงกรณ์มหาวิทยาลัย (พ.ศ. 2548)
ผศ.ดร.ธนาสัย สุคนธ์พันธุ์	Ph.D. (Computer Science) M.S. (Computer Science) วท.ม.(วิทยาการคอมพิวเตอร์) วศ.บ. (วิศวกรรมอุตสาหการ)	University of Southern California, U.S.A. (ค.ศ. 2012) University of Southern California, U.S.A. (ค.ศ. 2003) มหาวิทยาลัยมหิดล (พ.ศ. 2543) จุฬาลงกรณ์มหาวิทยาลัย (พ.ศ. 2540)
รศ.ดร.สุรพงค์ เอื้อวัฒนามงคล	Ph.D. (Computer Science) M.S. (Information and Computer Science) วิศวกรรมศาสตรบัณฑิต (วิศวกรรมไฟฟ้า)	Southern Methodist University, U.S.A. (ค.ศ. 1991) Georgia Institute of Technology, U.S.A. (ค.ศ. 1982) จุฬาลงกรณ์มหาวิทยาลัย (พ.ศ. 2521)

ตำแหน่งทางวิชาการ/ ชื่อ – สกุล	คุณวุฒิสูงสุด/สาขาวิชา	สถาบันที่สำเร็จการศึกษา/ ปี พ.ศ. ที่สำเร็จการศึกษา
รศ.ดร.ปราโมทย์ กั่วเจริญ	Ph.D. (Electrical and Computer Engineering) M.S. (Electrical and Computer Engineering) B.S. (Computer and Systems Engineering)	Georgia Institute of Technology, U.S.A. (ค.ศ. 2004) Georgia Institute of Technology, U.S.A. (ค.ศ. 2001) Rensselaer Polytechnic Institute, U.S.A. (ค.ศ. 1995)
ผศ.ดร.สุเทพ ทองงาม	Ph.D. (Computer Science) M.S. (Computer Science) บธ.ม. วศ.บ. (วิศวกรรมคอมพิวเตอร์)	Illinois Institute of Technology, U.S.A. (ค.ศ. 2008) Towson University, U.S.A. (ค.ศ. 2002) จุฬาลงกรณ์มหาวิทยาลัย (พ.ศ. 2536) จุฬาลงกรณ์มหาวิทยาลัย (พ.ศ. 2531)
ผศ.ดร.เอกรัฐ รัฐกาญจน์	Ph.D. (Electrical Engineering and Computer Science) วท.ม. (เทคโนโลยีสารสนเทศ) สถาปัตยกรรมศาสตรบัณฑิต	National Chiao Tung University (NCTU), Taiwan. (ค.ศ. 2016) มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี (พ.ศ. 2546) จุฬาลงกรณ์มหาวิทยาลัย (พ.ศ. 2542)
อ.ดร.ธนชาตย์ ฤทธิ์บำรุง	วท.ด. (เทคโนโลยีสารสนเทศทางธุรกิจ) วท.ม. (เทคโนโลยีสารสนเทศทางการจัดการ) วศ.บ. (วิศวกรรมโยธา)	จุฬาลงกรณ์มหาวิทยาลัย (พ.ศ.2553) จุฬาลงกรณ์มหาวิทยาลัย (พ.ศ.2546) จุฬาลงกรณ์มหาวิทยาลัย (พ.ศ. 2542)
ผศ.ดร. อัครนันท์ พงศธรวิวัฒน์	ปร.ด. (วิศวกรรมศาสตร์และเทคโนโลยี) (หลักสูตรนานาชาติ) Ph.D. (Knowledge Science) วศ.ม. (วิศวกรรมอุตสาหการ) วศ.บ. (ปิโตรเคมีและวัสดุพอลิเมอร์)	สถาบันเทคโนโลยีนานาชาติสิรินธร, มหาวิทยาลัยธรรมศาสตร์ (พ.ศ. 2561) Japan Advanced Institute of Science and Technology, Japan (ค.ศ.2016) จุฬาลงกรณ์มหาวิทยาลัย (พ.ศ.2553) มหาวิทยาลัยศิลปากร (พ.ศ.2551)
รศ.ดร.อมรรัตน์ กุลสุจริต	Docteur en Droit (Droit Public) นิติศาสตรมหาบัณฑิต (กฎหมายมหาชน) นิติศาสตรบัณฑิต	Université Aix-Marseille III, France (ค.ศ.2011) มหาวิทยาลัยธรรมศาสตร์ (พ.ศ.2541) มหาวิทยาลัยธรรมศาสตร์ (พ.ศ.2532)

ตำแหน่งทางวิชาการ/ ชื่อ – สกุล	คุณวุฒิสูงสุด/สาขาวิชา	สถาบันที่สำเร็จการศึกษา/ ปี พ.ศ. ที่สำเร็จการศึกษา
อ.ดร.อัญธิกา ณ พิบูลย์	Ph.D. in Law Master of Law (Innovation, Technology, and the Law) นิติศาสตรมหาบัณฑิต (กฎหมายอาญา) นิติศาสตรบัณฑิต	The University of Strathclyde, UK (ค.ศ.2018) The University of Edinburgh, UK (ค.ศ.2013) จุฬาลงกรณ์มหาวิทยาลัย (พ.ศ.2552) จุฬาลงกรณ์มหาวิทยาลัย (พ.ศ.2548)
ผศ.ดร.ธนัทเทพ เธียรประสิทธิ์	Ph.D. in Law (Criminal Law and Criminal Justice) Master of Laws (Intellectual Property Law) นิติศาสตรมหาบัณฑิต (กฎหมายอาญาและกระบวนการยุติธรรมทางอาญา) นิติศาสตรบัณฑิต	University of Aberdeen, United Kingdom (ค.ศ. 2018) Queen Mary University, United Kingdom (ค.ศ. 2008) จุฬาลงกรณ์มหาวิทยาลัย (พ.ศ. 2549) มหาวิทยาลัยธรรมศาสตร์ (พ.ศ. 2543)
ผศ.ดร.ธีทัต ชวิศจินดา	Ph.D. in Law (Law) Master of Law (European Master in Law and Economics (EMLE)) นิติศาสตรมหาบัณฑิต (กฎหมายระหว่างประเทศ) นิติศาสตรบัณฑิต	University of Washington, U.S.A. (ค.ศ. 2016) University of Hamburg, Germany (ค.ศ. 2010) มหาวิทยาลัยธรรมศาสตร์ (พ.ศ. 2551) มหาวิทยาลัยธรรมศาสตร์ (พ.ศ. 2545)
รศ.ดร.นิธินันท์ ธรรมากรนนท์	Ph.D. (Industrial Management) M.S. (Business) สถ.บ. (สถิติ)	Clemson University, U.S.A. (ค.ศ. 2001) Virginia Commonwealth University, U.S.A. (ค.ศ. 1997) จุฬาลงกรณ์มหาวิทยาลัย (พ.ศ. 2535)

3. วิทยากรภายนอก (ถ้ามี)

กำหนดภายหลังตามที่อาจารย์ผู้สอนรายวิชาเห็นควร

4. คณะกรรมการพัฒนาหลักสูตร

คำสั่งคณะสถิติประยุกต์ สถาบันบัณฑิตพัฒนบริหารศาสตร์ ที่ 14/2568 เรื่อง การแต่งตั้งคณะกรรมการพัฒนาหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการจัดการความเสี่ยงความมั่นคงทางไซเบอร์ หลักสูตรปรับปรุง พ.ศ. 2569 (คำสั่งตามเอกสารแนบ)

5. คณะกรรมการบริหารหลักสูตร

1) คณบดีคณะสถิติประยุกต์ (อาจารย์ ดร.ศิวิกา ดุษฎีโหนด) ประธานคณะกรรมการ
2) รองคณบดีฝ่ายวิชาการ (ผู้ช่วยศาสตราจารย์ ภัทราวดี ธนวงศ์สุวรรณ) กรรมการ
3) รองคณบดีฝ่ายวางแผนและพัฒนา (ผู้ช่วยศาสตราจารย์ ดร.ธิฏิรัตน์ พิมลศรี) กรรมการ
4) รองคณบดีฝ่ายบริหาร (ผู้ช่วยศาสตราจารย์ ดร.เอกรัฐ รัฐกาญจน์) กรรมการ
5) ผู้อำนวยการหลักสูตรปริญญาโท สาขาวิชาสถิติประยุกต์ กรรมการ
(รองศาสตราจารย์ ดร.อานนท์ ศักดิ์วรวิชญ์)
6) ผู้อำนวยการหลักสูตรปริญญาโท สาขาวิชาการวิเคราะห์ข้อมูลฯ กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.เอกรัฐ รัฐกาญจน์)
7) ผู้อำนวยการหลักสูตรปริญญาโท สาขาวิชาการจัดการความเสี่ยงความมั่นคงฯ กรรมการ
(รองศาสตราจารย์ ดร.ปราโมทย์ กั่วเจริญ)
8) ผู้อำนวยการหลักสูตรปริญญาโท สาขาวิชาบริหารเทคโนโลยีสารสนเทศ กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.ปราโมทย์ ลือนาม)
9) ผู้อำนวยการหลักสูตรปริญญาโท สาขาวิชาโลจิสติกส์อัจฉริยะฯ กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.อัครนันท์ พงศธรวิวัฒน์)
10) ผู้อำนวยการหลักสูตรปริญญาโท สาขาวิชาการจัดการวิเคราะห์ฯ กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.ธนชาตย์ ฤทธิ์บำรุง)
11) ผู้อำนวยการหลักสูตรปริญญาโท สาขาวิชาวิทยาการคอมพิวเตอร์ฯ กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.ธนาสัย สุคนธ์พันธุ์)
12) ผู้อำนวยการหลักสูตรปริญญาเอก สาขาวิชาวิทยาการคอมพิวเตอร์ฯ กรรมการ
(รองศาสตราจารย์ ดร.นิธินันท์ ธรรมากรนนท์)
13) ผู้อำนวยการหลักสูตรปริญญาเอก สาขาวิชาสถิติประยุกต์ กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.ปรีชา วิจิตรธรรมรส)
14) ผู้อำนวยการหลักสูตรปริญญาเอก สาขาวิชาการวิเคราะห์ข้อมูลฯ กรรมการ
(รองศาสตราจารย์ ดร.วรพล พงษ์เพ็ชร)
15) ผู้อำนวยการหลักสูตรปริญญาเอก สาขาวิชาโลจิสติกส์อัจฉริยะฯ กรรมการ
(รองศาสตราจารย์ ดร.กาญจ์นภา อมรัชกุล)
16) รักษาการผู้อำนวยการหลักสูตรชั้นปริญญาโท ภาคพิเศษ กรรมการและเลขานุการ
(ผู้ช่วยศาสตราจารย์ ภัทราวดี ธนวงศ์สุวรรณ)

6. สิ่งสนับสนุนการเรียนรู้ที่สำคัญของหลักสูตร

หลักสูตรมีสิ่งสนับสนุนการเรียนรู้ที่ครอบคลุมทั้งด้านทรัพยากรสารสนเทศ ฐานข้อมูลวิชาการ มาตรฐานสากล หนังสือ ตำรา ซอฟต์แวร์ ห้องปฏิบัติการ อุปกรณ์เฉพาะทาง และสภาพแวดล้อมดิจิทัล เพื่อสนับสนุนการเรียนการสอน การวิจัย การฝึกปฏิบัติ และการพัฒนาทักษะวิชาชีพด้านการจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์

6.1 ฐานข้อมูลงานวิจัยและฐานข้อมูลอิเล็กทรอนิกส์

นักศึกษาสามารถใช้บริการฐานข้อมูลงานวิจัยและฐานข้อมูลอิเล็กทรอนิกส์ เช่น e-Books, e-Journals, e-Theses และ e-Newspapers ที่ให้บริการโดยสำนักบรรณสารการพัฒนาของสถาบัน โดยสามารถสืบค้นออนไลน์ผ่านเว็บไซต์ได้อย่างสะดวก รวดเร็ว และเข้าถึงได้ทั้งภายในและภายนอกเครือข่ายของสถาบันผ่าน WiFi, VPN หรือการตั้งค่า Proxy

ฐานข้อมูลอิเล็กทรอนิกส์ที่สนับสนุนการเรียนการสอนและการวิจัยของหลักสูตร ได้แก่

- ACM Digital Library
- IEEE Xplore
- Wiley e-Journals
- ScienceDirect
- SpringerLink
- Engineering Source (EBSCO)
- Cambridge Core
- Open Access Theses and Dissertations (OATD)
- E-Theses Online Service (EThOS)
- Thai Digital Collection (TDC)
- Thai Journals Online (ThaiJo)

นอกจากนี้ ยังมีฐานข้อมูลสำหรับตรวจสอบการอ้างอิงผลงานทางวิชาการ ได้แก่

1. **Web of Science** สำหรับตรวจสอบการอ้างอิงผลงานวิชาการระดับนานาชาติ
2. **Thai-Journal Citation Index Centre (TCI)** สำหรับสืบค้น ตรวจสอบ และประเมินคุณภาพผลงานวิชาการและวารสารไทย รวมถึงข้อมูลการอ้างอิง ค่า TCI Impact Factors และข้อมูลที่เกี่ยวข้องกับคุณภาพผลงานวิจัยไทย

6.2 หนังสือ ตำรา มาตรฐาน และแหล่งเรียนรู้ทางวิชาชีพ

สำนักบรรณสารการพัฒนาให้บริการทรัพยากรสารสนเทศทั้งในรูปแบบสิ่งพิมพ์และอิเล็กทรอนิกส์ ได้แก่ หนังสือ ตำรา วารสาร หนังสือพิมพ์ และสื่อโสตทัศนวัสดุ โดยจัดเก็บตามระบบหอสมุดรัฐสภาอเมริกัน (Library of Congress Classification: LC) รวมถึงฐานข้อมูล e-Books เช่น

- ProQuest eBook
- Gale eBook

- University Press Collection (EBSCO)
- EBSCO eBooks
- Directory of Open Access Books (DOAB)

นอกจากหนังสือและตำราอิเล็กทรอนิกส์แล้ว สำนักบรรณสารการพัฒนายังจัดหาหนังสือและตำราฉบับพิมพ์อย่างต่อเนื่องทุกปีงบประมาณ รวมถึงคณะฯ มีห้องสมุดจิรกิติเป็นแหล่งรวบรวมหนังสือ ตำรา วิทยานิพนธ์ และสารนิพนธ์ที่เกี่ยวข้องกับหลักสูตร เพื่อสนับสนุนการค้นคว้าเพิ่มเติมของนักศึกษา สำหรับหลักสูตรด้านการจัดการความเสี่ยงความมั่นคงทางไซเบอร์ หลักสูตรจัดให้มีทรัพยากรเฉพาะทางด้านมาตรฐาน กรอบการทำงาน และหนังสือวิชาชีพ ดังนี้

1) มาตรฐานและกรอบการทำงานด้านความมั่นคงปลอดภัยสารสนเทศและความเสี่ยงไซเบอร์

- ISO/IEC 27000 — ภาพรวมและคำศัพท์ของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ
- ISO/IEC 27001 — ข้อกำหนดสำหรับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ หรือ ISMS
- ISO/IEC 27002 — แนวปฏิบัติและมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ
- ISO/IEC 27005 — แนวทางการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
- ISO/IEC 27017 — แนวปฏิบัติด้านความมั่นคงปลอดภัยสำหรับบริการคลาวด์
- ISO/IEC 27018 — แนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลบนคลาวด์สาธารณะ
- ISO/IEC 27701 — ระบบบริหารจัดการข้อมูลส่วนบุคคลและความเป็นส่วนตัว
- ISO/IEC 42001:2023 — ระบบบริหารจัดการปัญญาประดิษฐ์ หรือ Artificial Intelligence Management System: AIMS
- NIST Cybersecurity Framework (CSF) 2.0
- NIST SP 800-53 Security and Privacy Controls
- NIST SP 800-61 Computer Security Incident Handling Guide
- NIST SP 800-218 Secure Software Development Framework (SSDF)
- CIS Controls
- COBIT
- ITIL
- MITRE ATT&CK Framework
- OWASP Top 10 และ OWASP Application Security Verification Standard (ASVS)

ISO ระบุว่า ISO/IEC 27001 เป็นมาตรฐานหลักที่รู้จักแพร่หลายสำหรับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ และมาตรฐานในตระกูล ISO/IEC 27000 สนับสนุนแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ การคุ้มครองข้อมูล และ cyber resilience (ISO) ส่วน ISO/IEC 42001:2023 เป็นมาตรฐานสำหรับการจัดตั้ง ดำเนินการ รักษา และปรับปรุงระบบบริหารจัดการปัญญาประดิษฐ์ภายในองค์กรอย่างต่อเนื่อง (ISO) นอกจากนี้ NIST CSF 2.0 เป็นกรอบแนวทางสำหรับองค์กรในการบริหารความเสี่ยงด้านไซ

เบอร์ (csrc.nist.gov) และ NIST SP 800-218 หรือ SSDF ให้แนวปฏิบัติด้านการพัฒนาซอฟต์แวร์อย่างมั่นคงปลอดภัยตลอดวงจร SDLC (csrc.nist.gov)

2) หนังสือและคู่มือด้าน Certification ที่เกี่ยวข้อง

- CISSP: Certified Information Systems Security Professional
- CISM: Certified Information Security Manager
- CISA: Certified Information Systems Auditor
- CRISC: Certified in Risk and Information Systems Control
- CCSP: Certified Cloud Security Professional
- Security+
- CySA+
- PenTest+
- CEH: Certified Ethical Hacker
- ISO/IEC 27001 Lead Implementer
- ISO/IEC 27001 Lead Auditor
- AWS Certified Security – Specialty
- Microsoft Security, Compliance, and Identity Certifications
- Cisco CCNA / CyberOps Associate

หนังสือและคู่มือดังกล่าวช่วยสนับสนุนให้นักศึกษาเชื่อมโยงความรู้เชิงวิชาการกับมาตรฐานวิชาชีพสากล และเตรียมความพร้อมสำหรับการทำงานจริงในสายงานความมั่นคงปลอดภัยไซเบอร์ การบริหารความเสี่ยง การตรวจสอบระบบสารสนเทศ และธรรมาภิบาลเทคโนโลยี

6.3 โปรแกรมคอมพิวเตอร์และซอฟต์แวร์สนับสนุนการเรียนรู้

สำนักเทคโนโลยีดิจิทัลและสารสนเทศ และโครงการศูนย์คอมพิวเตอร์คณะสถิติประยุกต์ จัดหาและติดตั้งซอฟต์แวร์ในห้องเรียนและห้องปฏิบัติการคอมพิวเตอร์ เพื่อสนับสนุนการเรียนการสอน การวิจัย การวิเคราะห์ข้อมูล การตรวจสอบความซ้ำทางวิชาการ และการฝึกปฏิบัติด้านเทคโนโลยีสาร สนเทศ โดยมีซอฟต์แวร์พื้นฐานและซอฟต์แวร์สนับสนุน ดังนี้

- Turnitin สำหรับตรวจสอบความซ้ำของบทความ วิทยานิพนธ์ และผลงานวิชาการระดับนานาชาติ
- อักขราวิสุทธิ์ สำหรับตรวจสอบความเหมือนของวิทยานิพนธ์และผลงานวิชาการภาษาไทย
- Microsoft Windows
- Microsoft 365
- Amazon Web Services (AWS) Cloud
- IBM SPSS
- R, Python และซอฟต์แวร์เสรีที่เกี่ยวข้อง

- NIDA UApp
- EndNote
- G*Power
- MS SQL Server
- MATLAB
- Tableau Desktop
- Unity Pro Subscription
- SolidWorks ED
- ZBrush
- ซอฟต์แวร์ออกแบบสามมิติ

เพื่อให้สอดคล้องกับหลักสูตรด้านการจัดการความเสี่ยงความมั่นคงทางไซเบอร์ มีการจัดหาซอฟต์แวร์ เครื่องมือ และแพลตฟอร์มเฉพาะทางด้าน Cybersecurity เช่น

1) ระบบปฏิบัติการและสภาพแวดล้อมสำหรับการฝึกปฏิบัติ

- Kali Linux
- Ubuntu Linux
- Windows Server
- Docker
- VirtualBox
- VMware Workstation / VMware Player
- Cloud-based Cyber Range หรือ Virtual Lab Environment

2) เครื่องมือด้าน Network Security และ Vulnerability Assessment

- Nmap
- Wireshark
- OpenVAS / Greenbone Community Edition
- Nessus Essentials
- Netcat
- Masscan
- Nikto

3) เครื่องมือด้าน Penetration Testing และ Web Application Security

- Metasploit Framework
- Burp Suite Community / Professional
- OWASP ZAP
- SQLmap

- Hydra
- John the Ripper
- Hashcat

4) เครื่องมือด้าน Digital Forensics และ Incident Response

- Autopsy
- FTK Imager
- Volatility Framework
- Sleuth Kit
- Plaso / Log2Timeline
- YARA
- CyberChef

5) เครื่องมือด้าน Security Monitoring, SIEM และ Threat Detection

- Wazuh
- Security Onion
- Elastic Stack
- Splunk Free / Academic License
- Zeek
- Suricata
- Snort

6) เครื่องมือด้าน Secure Software Development และ DevSecOps

- Git / GitHub / GitLab
- SonarQube
- OWASP Dependency-Check
- Semgrep
- Bandit
- Trivy
- Snyk
- Docker Bench for Security
- GitHub Actions หรือ GitLab CI/CD สำหรับฝึกแนวคิด DevSecOps

ซอฟต์แวร์เหล่านี้ช่วยให้นักศึกษาได้ฝึกปฏิบัติจริงในด้านการประเมินช่องโหว่ การทดสอบการเจาะระบบ การวิเคราะห์เหตุการณ์ความมั่นคงปลอดภัย การตรวจพิสูจน์พยานหลักฐานดิจิทัล การเฝ้าระวังภัยคุกคาม และการพัฒนาซอฟต์แวร์อย่างมั่นคงปลอดภัย

6.4 อุปกรณ์และห้องปฏิบัติการที่สำคัญ

สถาบันและคณะจัดให้มีห้องปฏิบัติการคอมพิวเตอร์พร้อมเครื่องคอมพิวเตอร์สมรรถนะสูงและสิ่งอำนวยความสะดวกด้านเทคโนโลยีสารสนเทศ เพื่อสนับสนุนการเรียนการสอน การค้นคว้า และการวิจัย โดยมีห้องปฏิบัติการคอมพิวเตอร์ที่ให้บริการ ดังนี้

- ห้องปฏิบัติการคอมพิวเตอร์ของสถาบัน โดยสำนักเทคโนโลยีดิจิทัลและสารสนเทศ ณ ชั้น 9 และ 10 อาคารสยามบรมราชกุมารี จำนวนกว่า 130 เครื่อง
- ห้องปฏิบัติการคอมพิวเตอร์ของคณะ โดยโครงการศูนย์คอมพิวเตอร์คณะสถิติประยุกต์ ณ ชั้น 4 อาคารสยามบรมราชกุมารี และชั้น 12 อาคารนวมินทราธิราช รวมเครื่องคอมพิวเตอร์สมรรถนะสูงประมาณ 130 เครื่อง

นอกจากนี้ ยังมีอุปกรณ์เฉพาะทางที่ช่วยสนับสนุนการเรียนการสอนและการวิจัย ได้แก่

- โดรนบังคับวิทยุ
- เครื่องเสมือนจริง
- เครื่องพิมพ์สามมิติ
- Raspberry Pi 4
- กล้องจับภาพสามมิติ
- อุปกรณ์แว่นตาสวมศีรษะ
- แว่นตาอัจฉริยะ
- ชุดอุปกรณ์ห้องปฏิบัติการ Internet of Things แบบ Android

เพื่อสนับสนุนการเรียนรู้ด้าน Cybersecurity และ IoT Security ควรเพิ่มเติมอุปกรณ์และสภาพแวดล้อมเฉพาะทาง เช่น

- ชุดอุปกรณ์ IoT Security Lab
- อุปกรณ์เครือข่าย เช่น Router, Switch, Firewall และ Access Point
- อุปกรณ์สำหรับฝึก Network Segmentation และ Firewall Policy
- อุปกรณ์สำหรับฝึกระบบปฏิบัติการ Linux และ Windows Server
- ระบบ Virtual Lab สำหรับฝึก Penetration Testing และ Incident Response
- ระบบ Cyber Range หรือ Capture the Flag (CTF) Platform
- เครื่องแม่ข่ายสำหรับจำลองระบบ SOC, SIEM และ Digital Forensics Lab

6.5 สิ่งสนับสนุนอื่น ๆ ที่ช่วยส่งเสริมการเรียนรู้ของหลักสูตร

หลักสูตรมีสิ่งสนับสนุนอื่น ๆ เพื่อเสริมสร้างประสบการณ์การเรียนรู้เชิงปฏิบัติและการพัฒนาทักษะวิชาชีพของนักศึกษา ได้แก่

- ห้องปฏิบัติการเฉพาะทางด้านความมั่นคงปลอดภัยไซเบอร์
- ห้องปฏิบัติการเฉพาะทาง Cisco Certified Network Associate
- ห้องปฏิบัติการเฉพาะทางระบบปฏิบัติการ iOS

- Campus-wide Internet Access via WiFi
- Virtual Private Networks (VPN)
- ระบบ Cloud Lab สำหรับฝึกใช้งาน AWS, Azure หรือ Google Cloud
- ระบบฝึกปฏิบัติ Capture the Flag (CTF)
- ระบบจำลองเหตุการณ์ Cyber Incident Response
- ระบบฝึกปฏิบัติด้าน Secure Software Development และ DevSecOps
- แหล่งเรียนรู้ออนไลน์ด้าน Cybersecurity เช่น OWASP, NIST, MITRE ATT&CK, CIS Benchmarks และ Cybersecurity & Infrastructure Security Agency (CISA)
- กิจกรรมอบรมเชิงปฏิบัติการ สัมมนา และการบรรยายพิเศษโดยผู้เชี่ยวชาญจากภาครัฐ ภาคเอกชน และหน่วยงานวิชาชีพ
- การสนับสนุนให้นักศึกษาเข้าร่วมการแข่งขัน CTF, Cybersecurity Hackathon, Security Workshop และกิจกรรมวิชาชีพที่เกี่ยวข้อง

สิ่งสนับสนุนดังกล่าวช่วยให้นักศึกษาสามารถพัฒนาความรู้ ทักษะ และสมรรถนะที่จำเป็นต่อการทำงานจริง ทั้งในด้านการบริหารความเสี่ยงไซเบอร์ การกำกับดูแลความมั่นคงปลอดภัยสารสนเทศ การปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ การตรวจสอบระบบสารสนเทศ การทดสอบการเจาะระบบ การวิเคราะห์เหตุการณ์ และการพัฒนาซอฟต์แวร์อย่างมั่นคงปลอดภัย.

หมวดที่ 5 การจัดการกระบวนการเรียนรู้

1. การจัดการการเรียนรู้เพื่อให้เกิดผลลัพธ์การเรียนรู้

ผลลัพธ์การเรียนรู้ของหลักสูตร (Program Learning Outcomes: PLOs) มีดังนี้

PLO1 ความรู้ด้านวิทยาการไซเบอร์และโครงสร้างพื้นฐานดิจิทัล

สามารถอธิบายและบูรณาการหลักการ แนวคิด และสถาปัตยกรรมด้านความมั่นคงปลอดภัยไซเบอร์ ครอบคลุมเครือข่าย ระบบปฏิบัติการ ระบบคลาวด์ IoT OT ระบบสารสนเทศสมัยใหม่ รวมถึงระบบที่ขับเคลื่อนด้วยข้อมูลและปัญญาประดิษฐ์ ตลอดจนกลไกการเข้ารหัส การพิสูจน์ตัวตน และการควบคุมสิทธิ์การเข้าถึงข้อมูล

PLO2 ทักษะเชิงเทคนิคด้านความมั่นคงปลอดภัยไซเบอร์

สามารถออกแบบ เลือกใช้ ดำเนินการ และประเมินกลไกหรือเทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์เพื่อป้องกัน ตรวจจับ ตอบสนอง และฟื้นฟูระบบสารสนเทศและบริการดิจิทัลขององค์กร รวมถึงการใช้เครื่องมือทดสอบช่องโหว่ การตรวจสอบความมั่นคงปลอดภัย การวิเคราะห์เหตุการณ์ และการปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ (เช่น SOC / Incident Response) ได้อย่างเป็นระบบและมีประสิทธิภาพ

PLO3 การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และดิจิทัล

สามารถระบุ วิเคราะห์ ประเมิน และจัดลำดับความสำคัญของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และความเสี่ยงดิจิทัล (รวมถึงความเสี่ยงจากระบบคลาวด์ IoT และระบบที่ใช้ปัญญาประดิษฐ์) กำหนดกลยุทธ์และมาตรการควบคุม/บรรเทาความเสี่ยงที่เหมาะสม และบูรณาการการบริหารความเสี่ยงไซเบอร์เข้ากับการบริหารความเสี่ยงองค์รวมและทิศทางเชิงกลยุทธ์ขององค์กรได้

PLO4 กฎหมาย มาตรฐาน และธรรมาภิบาลด้านไซเบอร์และปัญญาประดิษฐ์

สามารถทำความเข้าใจและประยุกต์ใช้กฎหมาย ระเบียบ ข้อบังคับ และมาตรฐานที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ การคุ้มครองข้อมูลส่วนบุคคล และการใช้ปัญญาประดิษฐ์อย่างรับผิดชอบ (เช่น PDPA, กฎหมายไซเบอร์ที่เกี่ยวข้อง, มาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001 และมาตรฐานระบบบริหารจัดการปัญญาประดิษฐ์ ISO/IEC 42001 เป็นต้น) ในการออกแบบนโยบาย ระเบียบปฏิบัติ และกรอบธรรมาภิบาลเทคโนโลยีขององค์กรให้สอดคล้องกับข้อกำหนดและมาตรฐานสากล

PLO5.1 การวิจัยและการสร้างองค์ความรู้/นวัตกรรมด้านการจัดการความเสี่ยงไซเบอร์ สำหรับแผน 1

สามารถออกแบบและดำเนินการวิจัยเชิงวิชาการระดับบัณฑิตศึกษาอย่างเป็นระบบ เพื่อสร้างองค์ความรู้ใหม่ กรอบแนวคิด แบบจำลอง หรือหลักฐานเชิงประจักษ์ด้านการจัดการความเสี่ยงไซเบอร์และดิจิทัล (รวมถึงการกำกับดูแลเทคโนโลยีและปัญญาประดิษฐ์) โดยมีความถูกต้องด้านระเบียบวิธี คุณภาพทางวิชาการ การวิเคราะห์เชิงลึก และยึดหลักจริยธรรมการวิจัย

PLO5.2 การวิจัยและการสร้างองค์ความรู้/นวัตกรรมด้านการจัดการความเสี่ยงไซเบอร์ สำหรับแผน 2

สามารถออกแบบและดำเนินการศึกษาค้นคว้าเชิงประยุกต์ เพื่อสร้างแนวทางปฏิบัติ ต้นแบบระบบ เครื่องมือ หรือแนวทางนวัตกรรมที่นำไปใช้ได้จริงในการยกระดับความมั่นคงปลอดภัยไซเบอร์และการบริหารความเสี่ยง

ดิจิทัลขององค์กร (รวมถึงเทคโนโลยีและปัญญาประดิษฐ์) โดยมีการประเมินผลที่เหมาะสม ความน่าเชื่อถือในการสรุปผล และยึดหลักจริยธรรมที่เกี่ยวข้อง

PLO6 การสื่อสาร ประสานงาน และภาวะผู้นำด้านความมั่นคงปลอดภัยไซเบอร์และความเสี่ยง

สามารถสื่อสาร วิเคราะห์ และนำเสนอข้อมูลเชิงเทคนิคและเชิงบริหารด้านความเสี่ยง และความมั่นคงปลอดภัยไซเบอร์/ดิจิทัลแก่ผู้บริหารและผู้มีส่วนได้ส่วนเสียในรูปแบบที่เข้าใจง่ายและนำไปใช้ตัดสินใจได้ สามารถทำงานเป็นทีมข้ามสายงาน บริหารผู้มีส่วนได้ส่วนเสียและแสดงภาวะผู้นำในการขับเคลื่อนมาตรการ นโยบาย และวัฒนธรรมด้านความมั่นคงปลอดภัยไซเบอร์ในองค์กร

PLO7 คุณธรรม จริยธรรม และความรับผิดชอบต่อวิชาชีพและสังคม

มีจิตสำนึกด้านคุณธรรม จริยธรรมวิชาชีพ ความโปร่งใส และความรับผิดชอบต่อสังคม ตระหนักถึงสิทธิในความเป็นส่วนตัว ศักดิ์ศรีความเป็นมนุษย์และผลกระทบจากการใช้เทคโนโลยีดิจิทัลและปัญญาประดิษฐ์ สามารถส่งเสริมวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กร และมุ่งมั่นพัฒนาตนเองอย่างต่อเนื่องในฐานะผู้เชี่ยวชาญด้านการจัดการความเสี่ยงความมั่นคงทางไซเบอร์และดิจิทัล

ตารางที่ 2 ความสอดคล้องของรายวิชากับผลลัพธ์การเรียนรู้ของหลักสูตร (PLO) ผลลัพธ์การเรียนรู้ของรายวิชา (CLO) วิธีการจัดการเรียนรู้ และวิธีวัดผลการเรียนรู้

รายวิชา	PLO 1	PLO 2	PLO 3	PLO 4	PLO 5.1	PLO 5.2	PLO 6	PLO 7	CLO	วิธีการจัดการเรียนการสอน	วิธีวัดผลการเรียนรู้
สมช 4001 ระบบกฎหมายและนิติวิธีสำหรับดิจิทัลและไซเบอร์	X			X					1. อธิบายโครงสร้างระบบกฎหมาย แหล่งที่มาของกฎหมาย และกระบวนการยุติธรรมที่เกี่ยวข้องกับบริบทดิจิทัลและไซเบอร์ได้อย่างถูกต้อง	บรรยายเชิงโต้ตอบ อภิปรายตัวอย่างกฎหมาย และสรุปโครงสร้างกระบวนการยุติธรรมด้วยแผนภาพหรือกรณีศึกษา	สอบข้อเขียน แบบทดสอบสั้น และการประเมินการอภิปราย/ตอบคำถามในชั้นเรียน
			X	X					2. วิเคราะห์ประเด็นปัญหาทางกฎหมายเบื้องต้นที่เกี่ยวกับธุรกรรมดิจิทัล เทคโนโลยีสารสนเทศ และการใช้ข้อมูลได้อย่างมีเหตุผลเชิงนิติวิธี	Workshop ตีความกฎหมาย การวิเคราะห์กรณีศึกษา และการทำ case brief/legal memo เป็นรายบุคคลหรือกลุ่ม	งาน case brief/legal memo แบบประเมินการวิเคราะห์กรณีศึกษา และสอบข้อเขียนเชิงวิเคราะห์
				X					3. ระบุและประเมินบทบาทของหลักฐานดิจิทัล รวมทั้งการรักษาสายโซ่การรับรอง (chain of custody) ในกระบวนการยุติธรรมได้อย่างเหมาะสม	สาธิตกระบวนการจัดการหลักฐานดิจิทัล ฝึกจัดทำเอกสาร chain of custody และจำลองสถานการณ์การรับ–ส่งมอบหลักฐาน	ชุดเอกสารหลักฐานดิจิทัล แบบประเมิน simulation และแบบฝึกหัดการจัดทำ chain of custody
				X				X	4. ประยุกต์ใช้หลักกฎหมายคอมพิวเตอร์ กฎหมายความมั่นคงปลอดภัยไซเบอร์ และกฎหมายคุ้มครองข้อมูลส่วนบุคคลเบื้องต้นกับกรณีศึกษาได้	วิเคราะห์กรณีศึกษา การอภิปรายประเด็นกฎหมายหลายฉบับ และการฝึกจัดทำข้อเสนอแนวทางปฏิบัติตามกฎหมาย	รายงานวิเคราะห์กรณีศึกษา การนำเสนอ และแบบประเมินความถูกต้องของการประยุกต์ใช้กฎหมาย
								X	5. แสดงจิตสำนึกด้านคุณธรรม จริยธรรมวิชาชีพ และความรับผิดชอบต่อสังคมในการนำกฎหมายไปใช้ในบริบทความมั่นคงปลอดภัยไซเบอร์	อภิปรายประเด็นจริยธรรม บทบาทสมมติ และสะท้อนคิดจากกรณีศึกษาการใช้กฎหมายในงานไซเบอร์	Reflection paper คะแนนการมีส่วนร่วม และแบบประเมินพฤติกรรมด้านจริยธรรมจากกิจกรรมกลุ่ม

รายวิชา	PLO 1	PLO 2	PLO 3	PLO 4	PLO 5.1	PLO 5.2	PLO 6	PLO 7	CLO	วิธีการจัดการเรียนการสอน	วิธีวัดผลการเรียนรู้
สมซ 4002 การปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์และศูนย์ปฏิบัติการ	X	X							1. อธิบายโครงสร้าง บทบาท และหน้าที่ของศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ (SOC) และองค์ประกอบสำคัญของการปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ได้	บรรยายเชิงโต้ตอบ สาธิตโครงสร้าง SOC/SIEM/EDR/XDR และอภิปรายกรณีศึกษาการปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์	แบบทดสอบ สอบข้อเขียน และการประเมินการอภิปรายในชั้นเรียน
		X							2. ใช้เครื่องมือพื้นฐานด้านการจัดการบันทึกเหตุการณ์ (log management) และระบบ SIEM เพื่อรวบรวมและวิเคราะห์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ระดับเบื้องต้นได้	ฝึกปฏิบัติในห้องปฏิบัติการ SIEM การวิเคราะห์ log และการสาธิตการรวบรวมเหตุการณ์จากแหล่งข้อมูลต่าง ๆ	ผลงานปฏิบัติการ รายงานวิเคราะห์ log และแบบประเมิน lab rubric
		X	X						3. อธิบายวงจรการตอบสนองเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ และมีส่วนร่วมในการวิเคราะห์เหตุการณ์จากบันทึกและหลักฐานดิจิทัลอย่างเป็นระบบได้	กรณีศึกษา incident response การจำลองเหตุการณ์ และกิจกรรมกลุ่มวิเคราะห์เหตุการณ์จาก log และหลักฐานดิจิทัล	รายงานวิเคราะห์เหตุการณ์ การนำเสนอผลการวิเคราะห์ และแบบประเมินการทำงานกลุ่ม
	X	X							4. ประยุกต์ใช้แนวคิดข่าวกรองภัยคุกคามไซเบอร์ กรอบ MITRE ATT&CK และการล่าภัยคุกคามเบื้องต้นในการตรวจจับความผิดปกติในระบบได้	ฝึก mapping เหตุการณ์กับ MITRE ATT&CK, mini threat hunting workshop และการวิเคราะห์กรณีศึกษาภัยคุกคาม	งาน threat hunting use case แบบฝึกหัด mapping และการนำเสนอผลการวิเคราะห์
		X							5. พัฒนาและใช้สคริปต์อย่างง่ายเพื่อสนับสนุนการทำงานอัตโนมัติในงานปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างปลอดภัยและเหมาะสม	ฝึกเขียนสคริปต์พื้นฐาน สาธิต automation workflow และกิจกรรมปฏิบัติรายบุคคล/กลุ่ม	ชิ้นงานสคริปต์ รายงานผลการทดลองและแบบประเมินความถูกต้อง/ความปลอดภัยของการใช้งาน

รายวิชา	PLO 1	PLO 2	PLO 3	PLO 4	PLO 5.1	PLO 5.2	PLO 6	PLO 7	CLO	วิธีการจัดการเรียนการสอน	วิธีวัดผลการเรียนรู้
สมซ 4003 ภาษาอังกฤษสำหรับการจัดการความเสี่ยงความมั่นคงทางไซเบอร์							X		1. มีความรู้เกี่ยวกับคำศัพท์และไวยากรณ์ภาษาอังกฤษในระดับที่เพียงพอต่อการสื่อสารในระดับงานวิจัย	บรรยายและฝึกใช้คำศัพท์เฉพาะทางจากบทความวิชาการ รายงานด้านไซเบอร์ และตัวอย่างประโยคในบริบทวิชาชีพ	แบบฝึกหัดคำศัพท์/ไวยากรณ์ แบบทดสอบ และการประเมินการใช้คำศัพท์ในงานเขียนสั้น
							X		2. มีความเข้าใจในโครงสร้างการเขียนภาษาอังกฤษในระดับย่อหน้า	วิเคราะห์ตัวอย่างย่อหน้าจากบทความ/ตำรา ฝึกเขียน topic sentence, supporting details และ concluding sentence	ชิ้นงานเขียนย่อหน้า rubric การเขียน และการปรับปรุงงานตาม feedback
							X		3. อ่านและสรุปสาระสำคัญจากบทความ ตำรา หรือเอกสารภาษาอังกฤษที่เกี่ยวข้องกับการจัดการความเสี่ยงความมั่นคงทางไซเบอร์ได้	ฝึกอ่านเชิงวิเคราะห์ กิจกรรมสรุปบทความ และการอภิปรายคำศัพท์/แนวคิดสำคัญจากเอกสารจริง	รายงานสรุปบทความ แบบทดสอบ reading comprehension และการนำเสนอสาระสำคัญ
							X		4. เขียนประโยคและย่อหน้าภาษาอังกฤษในหัวข้อที่เกี่ยวข้องกับการจัดการความเสี่ยงความมั่นคงทางไซเบอร์ได้อย่างเหมาะสม	ฝึกเขียนจากแบบฝึกหัด peer review และการแก้ไขงานเขียนตามข้อเสนอแนะ	ชิ้นงานเขียนรายบุคคล portfolio งานเขียน และ rubric ด้านความถูกต้อง/ความชัดเจน
							X		5. พูดและฟังภาษาอังกฤษในหัวข้อที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์และการบริหารความเสี่ยงในสถานการณ์ทางวิชาการหรือวิชาชีพได้	ฝึกฟังวิดีโอ/บทสนทนา กิจกรรม role play และการนำเสนอปากเปล่าสั้น	การนำเสนอในชั้นเรียน แบบประเมิน speaking/listening rubric และคะแนนกิจกรรมเดี่ยว/กลุ่ม
สมซ 6001 การบริหารความมั่นคงปลอดภัยสารสนเทศ	X			X					1. อธิบายหลักการ แนวคิด และกรอบมาตรฐานด้านการบริหารความมั่นคงปลอดภัยสารสนเทศ เช่น ISO/IEC 27001, NIST CSF, CIS Controls ได้อย่างถูกต้อง	บรรยายกรอบ ISO/NIST/CIS วิเคราะห์ตัวอย่างมาตรฐาน และอภิปรายกรณีการนำมาตรฐานไปใช้ในองค์กร	สอบ แบบทดสอบ และงานสรุปเปรียบเทียบกรอบมาตรฐาน

รายวิชา	PLO 1	PLO 2	PLO 3	PLO 4	PLO 5.1	PLO 5.2	PLO 6	PLO 7	CLO	วิธีการจัดการเรียนการสอน	วิธีวัดผลการเรียนรู้
			X	X					2. วิเคราะห์บริบทองค์กรและออกแบบโครงสร้างการบริหารและกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับกลยุทธ์และเป้าหมายขององค์กรได้	Workshop วิเคราะห์บริบทองค์กร การออกแบบ governance structure และกรณีศึกษาองค์กรจริง	รายงานวิเคราะห์องค์กร แผนผัง governance structure และการนำเสนอ
		X	X	X					3. ออกแบบและจัดทำนโยบาย มาตรการควบคุม และกระบวนการบริหารความมั่นคงปลอดภัยสารสนเทศในระดับองค์กรได้อย่างเป็นระบบ	ฝึกจัดทำนโยบาย/มาตรการควบคุม กลุ่มออกแบบ ISMS และ peer review เอกสารควบคุม	ชิ้นงานนโยบาย/มาตรการควบคุม โครงงานแผน ISMS และ rubric ความครบถ้วนของเอกสาร
			X	X					4. ประเมินและบริหารความมั่นคงปลอดภัยของผู้ให้บริการและคู่ค้า รวมทั้งปัจจัยด้านบุคลากรและวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ขององค์กรได้อย่างเหมาะสม	กรณีศึกษาการบริหาร third-party risk และกิจกรรมออกแบบแนวทางสร้าง security culture	รายงานประเมินผู้ให้บริการ แผนพัฒนาวัฒนธรรมความมั่นคงและการอภิปราย
			X				X		5. กำหนดและใช้ตัวชี้วัดด้านประสิทธิภาพ (KPIs) และตัวชี้วัดด้านความเสี่ยง (KRIs) เพื่อสนับสนุนการตัดสินใจด้านการบริหารความมั่นคงปลอดภัยสารสนเทศด้	Workshop ออกแบบ KPI/KRI และ dashboard สำหรับผู้บริหาร พร้อมการนำเสนอผลการออกแบบ	ชิ้นงาน KPI/KRI dashboard การนำเสนอ และแบบประเมินความสอดคล้องกับเป้าหมายองค์กร
สมซ 6002 การวิเคราะห์ความเสี่ยงสำหรับความมั่นคงปลอดภัยสารสนเทศ	X		X						1. อธิบายหลักการและกรอบการบริหารความเสี่ยงตามมาตรฐานที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศได้อย่างชัดเจน	บรรยาย ISO 31000/ISO/IEC 27005 และอภิปรายตัวอย่างการบริหารความเสี่ยงสารสนเทศ	สอบ แบบทดสอบ และแบบฝึกหัดอธิบายกรอบการบริหารความเสี่ยง
	X		X						2. ระบุสินทรัพย์ดิจิทัล ภัยคุกคาม ช่องโหว่ และผลกระทบต่อธุรกิจ พร้อมทั้งวิเคราะห์ระดับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศได้อย่างเป็นระบบ	Workshop ระบุ asset-threat-vulnerability-impact และฝึกประเมินระดับความเสี่ยงจากกรณีศึกษา	งาน risk assessment worksheet รายงานวิเคราะห์ความเสี่ยง และแบบประเมินความครบถ้วน

รายวิชา	PLO 1	PLO 2	PLO 3	PLO 4	PLO 5.1	PLO 5.2	PLO 6	PLO 7	CLO	วิธีการจัดการเรียนการสอน	วิธีวัดผลการเรียนรู้
			X						3. ประยุกต์ใช้แนวทางการประเมินความเสี่ยงเชิงคุณภาพ กึ่งปริมาณ และเชิงปริมาณ รวมทั้งกรอบ เช่น CVSS และ EPSS ในการประเมินความเสี่ยงได้อย่างเหมาะสม	ฝึกคำนวณ/จัดลำดับความเสี่ยงด้วย CVSS/EPSS และกิจกรรมเปรียบเทียบแนวทางประเมินความเสี่ยง	แบบฝึกหัดคำนวณ risk scoring รายงานจัดลำดับช่องโหว่ และ quiz
	X		X						4. พัฒนาและวิเคราะห์ฉากทัศน์ความเสี่ยง (risk scenarios) ของเหตุการณ์ไซเบอร์สำคัญ เช่น ransomware และการรั่วไหลของข้อมูล เพื่อประเมินผลกระทบต่อธุรกิจได้	Workshop risk scenario และ stress-testing โดยใช้กรณี ransomware/data breach	รายงาน scenario analysis แบบประเมินผลกระทบธุรกิจ และการนำเสนอ
			X				X		5. จัดทำทะเบียนความเสี่ยงและเสนอแนวทางการจัดการความเสี่ยงที่สอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ขององค์กรได้อย่างมีเหตุผล	ฝึกจัดทำ risk register, heatmap และ risk treatment plan จากกรณีศึกษาองค์กร	ชิ้นงาน risk register + heatmap รายงาน risk treatment plan และ rubric ด้านเหตุผลของข้อเสนอ
สมซ 6003 กฎหมายเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	X			X					1. อธิบายกรอบกฎหมายและนโยบายระดับชาติที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์และโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้อย่างถูกต้อง	บรรยายกรอบกฎหมายไทยและนโยบายระดับชาติ อภิปรายกรณี CII และเหตุการณ์ไซเบอร์	สอบข้อเขียน แบบทดสอบ และงานสรุปกรอบกฎหมาย
				X					2. วิเคราะห์ความสัมพันธ์ระหว่างกฎหมายความมั่นคงปลอดภัยไซเบอร์ กฎหมายคอมพิวเตอร์ กฎหมายโทรคมนาคม และกฎหมายอื่นที่เกี่ยวข้องในบริบทการคุ้มครองความมั่นคงปลอดภัยของระบบสารสนเทศได้	Workshop mapping กฎหมายที่เกี่ยวข้องกับกรณีศึกษา และการอภิปรายประเด็นกฎหมายหลายฉบับ	งานวิเคราะห์ความสัมพันธ์ของกฎหมาย compliance matrix และการนำเสนอ

รายวิชา	PLO 1	PLO 2	PLO 3	PLO 4	PLO 5.1	PLO 5.2	PLO 6	PLO 7	CLO	วิธีการจัดการเรียนการสอน	วิธีวัดผลการเรียนรู้
			X	X					3. ระบุหน้าที่และความรับผิดชอบตามกฎหมายของหน่วยงานรัฐ ผู้ให้บริการและผู้ควบคุมระบบสารสนเทศในการป้องกัน ตรวจจับ และตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ได้	กรณีศึกษาหน้าที่ของผู้มีส่วนเกี่ยวข้องและ workshop จัดทำ checklist การปฏิบัติตามกฎหมาย	งาน compliance checklist รายงานวิเคราะห์หน้าที่ตามกฎหมายและสอบข้อเขียน
				X				X	4. วิเคราะห์ประเด็นทางกฎหมายและสิทธิขั้นพื้นฐานที่เกี่ยวข้องกับมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ และเสนอแนวทางปฏิบัติที่สมดุลระหว่างความมั่นคงกับสิทธิเสรีภาพได้	อภิปรายสิทธิและเสรีภาพในมาตรการไซเบอร์ บทบาทสมมติ และกรณีศึกษาที่มีความขัดแย้งทางจริยธรรม	reflection paper รายงานวิเคราะห์สิทธิและเสรีภาพ และคะแนนการอภิปราย
			X	X					5. ประยุกต์ใช้หลักเกณฑ์ทางกฎหมายและแนวทางระหว่างประเทศที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์กับกรณีศึกษาในบริบทองค์กรได้อย่างเหมาะสม	กรณีศึกษาเชิงเปรียบเทียบแนวทางระหว่างประเทศและการฝึกออกแบบแนวทางปฏิบัติสำหรับองค์กร	รายงานกรณีศึกษา งานจัดทำแนวทางปฏิบัติ และการนำเสนอ
สมซ 7001 ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และเครือข่าย	X								1. อธิบายหลักการความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และเครือข่าย รวมถึงภัยคุกคามและช่องโหว่สำคัญได้อย่างถูกต้อง	บรรยายหลักการและสถาปัตยกรรมความมั่นคงเครือข่าย พร้อมวิเคราะห์ตัวอย่างภัยคุกคามและช่องโหว่	สอบ แบบทดสอบ และแบบฝึกหัดวิเคราะห์ภัยคุกคาม
		X	X						2. ออกแบบสถาปัตยกรรมเครือข่ายและการแบ่งส่วนเครือข่าย โดยประยุกต์ใช้แนวคิด Zero Trust และ SASE เพื่อเพิ่มความมั่นคงปลอดภัยของระบบได้	Workshop ออกแบบ secure network architecture และ network segmentation โดยใช้กรณีองค์กร	งานออกแบบ secure network diagram รายงานอธิบายเหตุผล และการนำเสนอ

รายวิชา	PLO 1	PLO 2	PLO 3	PLO 4	PLO 5.1	PLO 5.2	PLO 6	PLO 7	CLO	วิธีการจัดการเรียนการสอน	วิธีวัดผลการเรียนรู้
		X							3. เลือกใช้และกำหนดค่ากลไกป้องกันเครือข่ายและอุปกรณ์ปลายทาง เช่น ไฟร์วอลล์ IDS/IPS VPN และ EDR/XDR ได้อย่างเหมาะสมกับบริบทการใช้งาน	Lab การกำหนดค่า firewall/IDS/IPS/VPN และสาธิต endpoint/server hardening	ผลการปฏิบัติ lab รายงานการตั้งค่า และแบบประเมิน practical rubric
		X	X						4. ประเมินความมั่นคงปลอดภัยของเครือข่ายและอุปกรณ์ปลายทางจากบันทึกเหตุการณ์และการสแกนช่องโหว่ พร้อมเสนอแนวทางปรับปรุงเชิงเทคนิคได้อย่างมีเหตุผล	ฝึกวิเคราะห์ทราฟฟิก บันทึกเหตุการณ์และผลสแกนช่องโหว่ พร้อมกิจกรรมจัดลำดับการแก้ไข	รายงานการประเมินความมั่นคง รายงานช่องโหว่ และข้อเสนอการปรับปรุง
		X					X		5. สร้างและนำเสนอข้อเสนอเชิงเทคนิคด้านความมั่นคงปลอดภัยของระบบและเครือข่ายให้แก่ผู้มีส่วนได้ส่วนเสียทางเทคนิคและไม่ใช่เทคนิคได้อย่างชัดเจน	กิจกรรมจัดทำข้อเสนอเชิงเทคนิคและฝึกนำเสนอสำหรับผู้บริหาร/ผู้ใช้งานทั่วไป	เอกสารข้อเสนอเชิงเทคนิค การนำเสนอ และ rubric ด้านความชัดเจนของการสื่อสาร
สมซ 7002 ความมั่นคงปลอดภัยของคลาวด์และระบบคลาวด์เนทีฟ	X								1. อธิบายสถาปัตยกรรมคลาวด์ รูปแบบการให้บริการ และโมเดลความรับผิดชอบร่วมด้านความมั่นคงปลอดภัยคลาวด์ได้อย่างชัดเจน	บรรยาย cloud service models และ shared responsibility model พร้อมกรณีศึกษา cloud incident	สอบ แบบทดสอบ และแบบฝึกหัดวิเคราะห์ความรับผิดชอบร่วม
		X	X	X					2. ออกแบบสถาปัตยกรรมคลาวด์ขององค์กรที่คำนึงถึงการบริหารอัตลักษณ์และการเข้าถึง การปกป้องข้อมูล และข้อกำหนดด้านความเป็นส่วนตัวได้อย่างเหมาะสม	Workshop cloud security architecture, IAM design และ privacy-aware design จากกรณีองค์กร	งานออกแบบ cloud security architecture รายงานเหตุผลด้าน IAM/data protection และการนำเสนอ
		X							3. ประยุกต์ใช้แนวทางด้านความมั่นคงปลอดภัยของคอนเทนเนอร์ Kubernetes และโครงสร้างพื้นฐานแบบโค้ด (IaC) เพื่อ	Lab container/Kubernetes/IaC security และสาธิตการตรวจสอบ configuration	ผลการปฏิบัติ lab รายงาน configuration review และ practical rubric

รายวิชา	PLO 1	PLO 2	PLO 3	PLO 4	PLO 5.1	PLO 5.2	PLO 6	PLO 7	CLO	วิธีการจัดการเรียนการสอน	วิธีวัดผลการเรียนรู้
									ป้องกันความเสี่ยงในสภาพแวดล้อมคลาวด์เนทีฟได้		
		X	X						4. เลือกใช้และประเมินเครื่องมือด้านความมั่นคงคลาวด์ เช่น CSPM CWPP และ CIEM เพื่อเฝ้าระวังและจัดการความเสี่ยงบนคลาวด์ได้อย่างมีประสิทธิภาพ	สาธิตเครื่องมือ cloud security และกิจกรรมประเมินความเหมาะสมของ CSPM/CWPP/CIEM ตามสถานการณ์	รายงานประเมินเครื่องมือ แบบฝึกหัด risk monitoring และการนำเสนอผลการเลือกใช้
		X	X						5. ผสานแนวคิด DevSecOps และความมั่นคงในกระบวนการ CI/CD รวมถึงการตรวจสอบและตอบสนองเหตุการณ์บนคลาวด์ในเชิงรุกได้	งานออกแบบ CI/CD security control รายงาน incident response บนคลาวด์ และ rubric โครงงาน	งานออกแบบ CI/CD security control รายงาน incident response บนคลาวด์ และ rubric โครงงาน
สมซ 7003 ปัญญาประดิษฐ์ขั้นสูงสำหรับการปฏิบัติการความมั่นคงปลอดภัยไซเบอร์	X	X							1. ประยุกต์ AI/ML และ LLMs เพื่อสนับสนุนงาน SOC ได้แก่ log analytics, anomaly detection, alert triage และ incident analysis ได้อย่างเหมาะสม	บรรยาย AI/ML และ LLMs สำหรับ SOC พร้อม lab วิเคราะห์ log/anomaly และสาธิต alert triage	โครงงานย่อยหรือ lab report แบบทดสอบ และ rubric การประยุกต์ใช้ AI/ML
					X	X			2. ออกแบบและดำเนินวงจรข่าวกรองภัยคุกคาม โดยคัดเลือกแหล่งข่าวกรอง (OSINT/เชิงพาณิชย์/ความร่วมมือ) และใช้ AI เพื่อรวบรวม–เพิ่มคุณค่า–วิเคราะห์ Threat Intelligence ได้	Workshop threat intelligence lifecycle การคัดเลือกแหล่งข่าวกรอง และการใช้ AI ช่วย enrichment/analysis	รายงาน threat intelligence workflow ชิ้นงาน enrichment และการนำเสนอผลวิเคราะห์
	X	X							3. แม็ปเหตุการณ์กับ MITRE ATT&CK และออกแบบ detection rules + hypothesis-driven threat hunting พร้อม use case, ตัวชี้วัด และ playbook ที่วัดผลได้	ฝึก ATT&CK mapping, detection engineering และ hypothesis-driven threat hunting workshop	งาน detection rule/hunting use case, playbook และ rubric ด้านความถูกต้อง/วัดผลได้

รายวิชา	PLO 1	PLO 2	PLO 3	PLO 4	PLO 5.1	PLO 5.2	PLO 6	PLO 7	CLO	วิธีการจัดการเรียนการสอน	วิธีวัดผลการเรียนรู้
			X				X		4. ออกแบบสถาปัตยกรรมและ workflow ระบบอัตโนมัติ (SOAR) รวมถึงการเชื่อมต่อ SIEM, EDR/XDR และ Threat Intel ผ่านสคริปต์/API เพื่อการตอบสนองเหตุการณ์แบบกึ่งอัตโนมัติ/อัตโนมัติได้	Workshop SOAR workflow และ playbook design พร้อมสาธิตการเชื่อมต่อ API/automation	ชิ้นงาน SOAR workflow/playbook รายงานการออกแบบ และการนำเสนอ
								X	5. ประเมินและจัดการความเสี่ยง/ธรรมาภิบาล AI สำหรับงานไซเบอร์ รวมถึงภัยคุกคามต่อ AI (เช่น prompt injection, data poisoning, model theft, adversarial ML) และการอ้างอิงกรอบมาตรฐาน (เช่น NIST AI RMF, ISO/IEC 42001)	อภิปราย AI governance และ AI security risk กรณีศึกษา prompt injection/data poisoning และการประเมินตามกรอบมาตรฐาน	รายงานประเมินความเสี่ยง AI แบบฝึกหัด mapping มาตรฐาน และ reflection ด้านจริยธรรม/ธรรมาภิบาล
สมซ 7004 การทดสอบการเจาะระบบและการจัดการช่องโหว่	X	X		X					1. อธิบายหลักการ ขั้นตอน และข้อจำกัดของการทดสอบการเจาะระบบในบริบททางเทคนิคและทางกฎหมายได้อย่างถูกต้อง	บรรยาย methodology, scope และ rules of engagement พร้อมอภิปรายข้อจำกัดทางกฎหมายและจริยธรรม	สอบ แบบทดสอบ และแบบประเมินความเข้าใจ ROE/ข้อจำกัดทางกฎหมาย
		X							2. วางแผนและดำเนินการทดสอบการเจาะระบบเครือข่ายและเว็บแอปพลิเคชันระดับพื้นฐาน โดยใช้เครื่องมือและเทคนิคที่เหมาะสมได้	Lab recon, scanning, web/API testing และการใช้เครื่องมือทดสอบการเจาะระบบในสภาพแวดล้อมควบคุม	ผลการปฏิบัติ lab รายงาน pentest และ practical rubric
		X	X						3. วิเคราะห์ จัดลำดับความสำคัญ และสรุปผลช่องโหว่ที่ค้นพบ พร้อมทั้งเสนอแนวทางแก้ไขที่สอดคล้องกับบริบทขององค์กรได้	Workshop vulnerability triage และ remediation planning จากผลการทดสอบตัวอย่าง	รายงาน vulnerability triage แผน remediation และแบบประเมินการจัดลำดับความสำคัญ

รายวิชา	PLO 1	PLO 2	PLO 3	PLO 4	PLO 5.1	PLO 5.2	PLO 6	PLO 7	CLO	วิธีการจัดการเรียนการสอน	วิธีวัดผลการเรียนรู้
		X	X						4. ออกแบบและบริหารวงจรการจัดการช่องโหว่ ตั้งแต่การสแกน ประเมิน แก้ไข จนถึงการยืนยันผลในลักษณะเชิงระบบได้	กิจกรรมออกแบบ vulnerability management lifecycle และจำลองกระบวนการ verify/remediate	งานออกแบบวงจรจัดการช่องโหว่ รายงานขั้นตอน และ rubric ความครบถ้วนของกระบวนการ
		X	X					X	5. เชื่อมโยงผลการทดสอบการเจาะระบบและการจัดการช่องโหว่เข้ากับกระบวนการ DevSecOps และการปรับปรุงมาตรการควบคุมด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กรได้	Workshop เชื่อมโยงผลทดสอบกับ DevSecOps/CI-CD และอภิปรายจริยธรรมการรายงานช่องโหว่	รายงานเชื่อมโยง pentest กับ DevSecOps แผนปรับปรุง controls และ reflection ด้านจริยธรรม
สมซ 7005 นิติดิจิทัลและการสืบสวน	X			X					1. อธิบายหลักการ กระบวนการ และมาตรฐานที่เกี่ยวข้องกับนิติดิจิทัล และการจัดการพยานหลักฐานดิจิทัลได้อย่างถูกต้อง	บรรยายกระบวนการ forensic และมาตรฐานการจัดการหลักฐาน พร้อมกรณีศึกษา	สอบ แบบทดสอบ และแบบฝึกหัด chain of custody
		X							2. ปฏิบัติการเก็บรักษาและวิเคราะห์หลักฐานดิจิทัลจากระบบปฏิบัติการ เครือข่าย อุปกรณ์พกพา และสภาพแวดล้อมคลาวด์ในระดับพื้นฐานได้	Lab เก็บและวิเคราะห์หลักฐานดิจิทัลระดับพื้นฐานจากแหล่งข้อมูลหลายประเภท	ผลการปฏิบัติ lab รายงาน forensic analysis และ practical rubric
	X	X	X						3. ประยุกต์ใช้กรอบการตอบสนองเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ร่วมกับข่าวกรองภัยคุกคามไซเบอร์ในการสืบสวนเหตุการณ์ไซเบอร์ได้อย่างเป็นระบบ	กรณีศึกษา incident response + threat intelligence และฝึก timeline/log forensics	รายงานสืบสวนเหตุการณ์ timeline analysis และการนำเสนอผลการสืบสวน
		X							4. ใช้เทคนิคการวิเคราะห์หน่วยความจำและมัลแวร์เบื้องต้น รวมถึงเครื่องมืออัตโนมัติและสคริปต์ เพื่อสนับสนุนการสืบสวนเชิงลึกได้	Lab memory/malware analysis เบื้องต้นและสาธิตการใช้เครื่องมืออัตโนมัติ/สคริปต์	ผลการปฏิบัติ lab รายงานวิเคราะห์เบื้องต้น และแบบประเมินการใช้เครื่องมือ

รายวิชา	PLO 1	PLO 2	PLO 3	PLO 4	PLO 5.1	PLO 5.2	PLO 6	PLO 7	CLO	วิธีการจัดการเรียนการสอน	วิธีวัดผลการเรียนรู้
				X			X	X	5. จัดทำรายงานนิติดิจิทัลที่มีความถูกต้อง น่าเชื่อถือ และเหมาะสมต่อการใช้ในกระบวนการยุติธรรม โดยคำนึงถึงจริยธรรมและประเด็นทางกฎหมายที่เกี่ยวข้องได้	ฝึกจัดทำ forensic report การนำเสนอผลสืบสวน และอภิปรายข้อควรระวังทางกฎหมาย/จริยธรรม	รายงาน forensic report การนำเสนอ และ rubric ด้านความถูกต้อง น่าเชื่อถือ และจริยธรรม
สมซ 7006 นโยบายความมั่นคงปลอดภัยสารสนเทศ	X			X					1. อธิบายบทบาท ความสำคัญ และโครงสร้างของเอกสารด้านนโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กรได้	บรรยายโครงสร้างนโยบาย มาตรฐาน แนวปฏิบัติ และขั้นตอนปฏิบัติ พร้อมตัวอย่างเอกสารจริง	สอบสั้น แบบทดสอบ และงานสรุปโครงสร้างเอกสารนโยบาย
		X	X	X					2. ออกแบบและจัดทำนโยบาย มาตรฐาน แนวปฏิบัติ และระเบียบการปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศให้สอดคล้องกับบริบทขององค์กรและมาตรฐานที่เกี่ยวข้องได้	Workshop เขียน policy/standard/procedure และ peer review ตามบริบทองค์กร	ชิ้นงาน policy set, rubric ความครบถ้วน/สอดคล้องมาตรฐาน และการนำเสนอ
		X	X	X					3. กำหนดนโยบายเฉพาะด้าน เช่น นโยบายคลาวด์ นโยบายการทำงานจากระยะไกล นโยบาย BYOD นโยบายการจัดการเหตุการณ์ และนโยบายการคุ้มครองข้อมูลได้อย่างเหมาะสม	กิจกรรมกลุ่มออกแบบนโยบายเฉพาะด้านจากกรณีองค์กร และอภิปรายการบังคับใช้	ชิ้นงานนโยบายเฉพาะด้าน แบบประเมินความเหมาะสม และการนำเสนอ
							X	X	4. ออกแบบแนวทางการสื่อสาร การฝึกอบรม และการส่งเสริมวัฒนธรรมด้านนโยบายความมั่นคงปลอดภัยสารสนเทศในองค์กรได้	จำลองการสื่อสารนโยบาย กิจกรรมออกแบบ training/awareness campaign และ role play	แผนการสื่อสาร/อบรม การนำเสนอ และ rubric ด้านความชัดเจนและการสร้างวัฒนธรรม

รายวิชา	PLO 1	PLO 2	PLO 3	PLO 4	PLO 5.1	PLO 5.2	PLO 6	PLO 7	CLO	วิธีการจัดการเรียนการสอน	วิธีวัดผลการเรียนรู้
			X	X					5. ประเมินและปรับปรุงนโยบายความมั่นคงปลอดภัยสารสนเทศให้สอดคล้องกับการเปลี่ยนแปลงของเทคโนโลยี กฎหมาย และมาตรฐานได้อย่างต่อเนื่อง	Workshop policy review และ gap analysis กับกฎหมาย/มาตรฐานที่เปลี่ยนแปลง	รายงาน policy gap analysis แผนปรับปรุงนโยบาย และแบบประเมินเหตุผลของข้อเสนอ
สมซ 7007 การกำกับดูแลระบบสารสนเทศ	X			X					1. อธิบายแนวคิดและหลักการกำกับดูแลระบบสารสนเทศ และกรอบการกำกับดูแล เช่น COBIT และ ITIL ได้อย่างถูกต้อง	บรรยาย COBIT/ITIL และหลักการ IT/digital governance พร้อมอภิปรายกรณีศึกษา	สอบ แบบทดสอบ และงานสรุปเปรียบเทียบกรอบ governance
				X			X		2. วิเคราะห์บทบาทของคณะกรรมการและผู้บริหารระดับสูงในการกำกับดูแลเทคโนโลยีและความมั่นคงปลอดภัยไซเบอร์ และเชื่อมโยงกับกลยุทธ์ดิจิทัลขององค์กรได้	กรณีศึกษา board oversight และกิจกรรม mapping กลยุทธ์ดิจิทัลกับบทบาทผู้บริหาร	รายงานวิเคราะห์บทบาทผู้บริหาร การนำเสนอ และแบบประเมินการเชื่อมโยงเชิงกลยุทธ์
			X	X					3. ออกแบบโครงสร้างและกระบวนการกำกับดูแลด้านข้อมูล ระบบสารสนเทศ และโครงการดิจิทัลที่เหมาะสมกับบริบทขององค์กรได้	Workshop ออกแบบ governance structure/process และวิเคราะห์กรณีโครงการดิจิทัล	ชิ้นงาน governance model รายงานการออกแบบกระบวนการ และ rubric ความเหมาะสม
			X						4. ประเมินความคุ้มค่าและความเสี่ยงของการลงทุนด้านเทคโนโลยีและความมั่นคงปลอดภัยไซเบอร์ โดยบูรณาการกับการบริหารความเสี่ยงองค์รวมได้	กิจกรรมวิเคราะห์ investment/risk trade-off และเชื่อมโยงกับ enterprise risk management	รายงานประเมินความคุ้มค่าและความเสี่ยง แบบฝึกหัด และการนำเสนอ
			X				X		5. กำหนดและใช้ตัวชี้วัดด้านการกำกับดูแลระบบสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ เพื่อสนับสนุนการตัดสินใจเชิงกลยุทธ์และการรายงานต่อผู้บริหารได้	Workshop ออกแบบ governance metrics/dashboard และฝึกนำเสนอรายงานต่อผู้บริหาร	ชิ้นงาน dashboard/metrics การนำเสนอ และ rubric ด้านการสนับสนุนการตัดสินใจ

รายวิชา	PLO 1	PLO 2	PLO 3	PLO 4	PLO 5.1	PLO 5.2	PLO 6	PLO 7	CLO	วิธีการจัดการเรียนการสอน	วิธีวัดผลการเรียนรู้
สมซ 7008 กฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์	X			X					1. อธิบายกรอบกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์และประเภทของอาชญากรรมไซเบอร์ที่สำคัญได้อย่างชัดเจน	บรรยายกรอบความผิดและประเภท cyber-dependent/cyber-enabled crimes พร้อมตัวอย่างคดี	สอบข้อเขียน แบบทดสอบ และงานสรุปประเภทความผิด
			X	X					2. วิเคราะห์รูปแบบการกระทำความผิดทางคอมพิวเตอร์ เช่น การเข้าถึงโดยมิชอบ การแทรกแซงข้อมูล การหลอกลวงออนไลน์ และ ransomware ได้อย่างมีเหตุผลทางกฎหมาย	กรณีศึกษา phishing/ransomware/unauthorized access และ workshop วิเคราะห์องค์ประกอบความผิด	งานวิเคราะห์คดี/องค์ประกอบความผิด การนำเสนอ และสอบข้อเขียนเชิงวิเคราะห์
	X			X					3. อธิบายขั้นตอนและข้อกำหนดทางกฎหมายในการสืบสวนและรวบรวมหลักฐานทางคอมพิวเตอร์ได้อย่างถูกต้อง	บรรยายกระบวนการสืบสวนและ workshop ขั้นตอนรวบรวมพยานหลักฐาน	งานขั้นตอนรวบรวมพยานหลักฐาน แบบทดสอบ และการอภิปราย
				X			X		4. ประเมินบทบาทและข้อจำกัดของหน่วยงานบังคับใช้กฎหมายและความร่วมมือระหว่างประเทศในการรับมืออาชญากรรมไซเบอร์ได้	อภิปรายบทบาทหน่วยงานบังคับใช้กฎหมายและความร่วมมือระหว่างประเทศ พร้อมกรณีศึกษา	รายงานวิเคราะห์บทบาท/ข้อจำกัด การนำเสนอ และ participation
				X				X	5. พิจารณาประเด็นด้านสิทธิส่วนบุคคลและเสรีภาพในการบังคับใช้กฎหมายอาชญากรรมทางคอมพิวเตอร์ และเสนอแนวทางที่สมดุลระหว่างการบังคับใช้กฎหมายกับการคุ้มครองสิทธิได้	อภิปรายสิทธิส่วนบุคคล บทบาทสมมติ และกรณีศึกษา balancing test	reflection paper รายงานข้อเสนอเชิงสมดุล และคะแนนการอภิปราย
สมซ 7009 กฎหมายพาณิชย์อิเล็กทรอนิกส์และธุรกิจดิจิทัล	X			X					1. อธิบายกรอบกฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ สัญญาอิเล็กทรอนิกส์ และลายมือชื่ออิเล็กทรอนิกส์ได้อย่างถูกต้อง	บรรยายกฎหมายธุรกรรม/สัญญาอิเล็กทรอนิกส์ และวิเคราะห์ตัวอย่างเอกสาร/ธุรกรรมออนไลน์	สอบ แบบทดสอบ และแบบฝึกหัดวิเคราะห์ธุรกรรม

รายวิชา	PLO 1	PLO 2	PLO 3	PLO 4	PLO 5.1	PLO 5.2	PLO 6	PLO 7	CLO	วิธีการจัดการเรียนการสอน	วิธีวัดผลการเรียนรู้
			X	X					2. วิเคราะห์ความรับผิดของผู้ให้บริการตัวกลางและเจ้าของแพลตฟอร์มดิจิทัล รวมทั้งประเด็นการคุ้มครองผู้บริโภคออนไลน์ได้อย่างมีเหตุผล	กรณีศึกษาแพลตฟอร์มดิจิทัลและ workshop วิเคราะห์ข้อกำหนด/ความรับผิด	case memo รายงานวิเคราะห์ความรับผิด และการนำเสนอ
			X	X					3. อธิบายกรอบกฎหมายที่เกี่ยวข้องกับการชำระเงินอิเล็กทรอนิกส์ บริการทางการเงินดิจิทัล และมาตรการป้องกันการฟอกเงินในบริบทดิจิทัลได้	บรรยาย digital payment/AML และอภิปรายกรณีบริการทางการเงินดิจิทัล	สอบสั้น แบบฝึกหัด compliance checklist และรายงานกรณีศึกษา
			X	X					4. วิเคราะห์ประเด็นกฎหมายในบริบทการค้าข้ามพรมแดน การระงับข้อพิพาททางพาณิชย์อิเล็กทรอนิกส์ และความเชื่อมโยงกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลได้	Workshop cross-border e-commerce dispute และการวิเคราะห์ข้อพิพาทจำลอง	case memo ข้อพิพาท รายงานวิเคราะห์กฎหมายที่เกี่ยวข้อง และการนำเสนอ
			X	X					5. ประยุกต์ใช้หลักเกณฑ์ทางกฎหมายด้านพาณิชย์อิเล็กทรอนิกส์และธุรกิจดิจิทัลในการประเมินความเสี่ยงและออกแบบมาตรการควบคุมในกรณีศึกษาได้	กิจกรรมประเมิน legal risk ของธุรกิจดิจิทัลและออกแบบมาตรการควบคุม	รายงาน legal risk/control design และ rubric ความเหมาะสมของมาตรการ
สมซ 7010 กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและความเป็นส่วนตัว	X			X					1. อธิบายหลักการพื้นฐานและกรอบกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย รวมถึงฐานทางกฎหมายในการประมวลผลข้อมูลได้อย่างถูกต้อง	บรรยาย PDPA/GDPR และฐานทางกฎหมาย พร้อมตัวอย่างกิจกรรมประมวลผลข้อมูล	สอบ แบบทดสอบ และแบบฝึกหัดระบุฐานทางกฎหมาย
			X	X					2. ระบุสิทธิของเจ้าของข้อมูลส่วนบุคคลและหน้าที่ของผู้ควบคุมและผู้ประมวลผลข้อมูล พร้อมทั้งอธิบายวิธีการปฏิบัติตามข้อกำหนดได้	กรณีศึกษา data subject rights และ workshop ออกแบบกระบวนการตอบสนองคำขอ	งาน process design รายงานวิเคราะห์หน้าที่ และ quiz

รายวิชา	PLO 1	PLO 2	PLO 3	PLO 4	PLO 5.1	PLO 5.2	PLO 6	PLO 7	CLO	วิธีการจัดการเรียนการสอน	วิธีวัดผลการเรียนรู้
			X	X					3. ออกแบบกระบวนการบันทึกรายการประมวลผล (ROPA) และการประเมินผลกระทบด้านการคุ้มครองข้อมูล (DPIA) สำหรับกิจกรรมประมวลผลที่มีความเสี่ยงได้	Workshop ROPA/DPIA โดยใช้กรณีประมวลผลข้อมูลที่มีความเสี่ยงสูง	ชิ้นงาน ROPA/DPIA rubric ความครบถ้วน และการนำเสนอ
			X	X					4. วิเคราะห์ข้อกำหนดเกี่ยวกับการแจ้งเหตุละเมิดข้อมูล การโอนข้อมูลข้ามพรมแดน และข้อกำหนดเฉพาะในภาคส่วนต่าง ๆ โดยเปรียบเทียบกับกรอบกฎหมายต่างประเทศ เช่น GDPR ได้	จำลอง data breach notification และกรณีศึกษา cross-border transfer/sector-specific requirements	งานแผนรับมือเหตุละเมิดข้อมูล รายงานเปรียบเทียบกฎหมาย และการนำเสนอ
			X	X				X	5. ประยุกต์ใช้แนวคิดความเป็นส่วนตัวโดยออกแบบและโดยค่าเริ่มต้น รวมถึงบทบาทของ DPO ในการบูรณาการกฎหมายคุ้มครองข้อมูลเข้ากับการบริหารความเสี่ยงและธรรมาภิบาลข้อมูลขององค์กรได้	Workshop privacy by design/default และกิจกรรมออกแบบบทบาท DPO/การบูรณาการกับ risk governance	รายงาน privacy-by-design plan แบบประเมินการบูรณาการกับความเสี่ยง และ reflection ด้านจริยธรรม
สมซ 7011 การจัดการความเสี่ยงสำหรับเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยสารสนเทศ	X		X						1. อธิบายกรอบการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยสารสนเทศ และความสัมพันธ์กับการบริหารความเสี่ยงองค์รวมขององค์กรได้	บรรยาย IT/cyber risk management และ ERM integration พร้อมกรณีศึกษาองค์กร	สอบ แบบทดสอบ และงานสรุปการเชื่อมโยง IT/cyber risk กับ ERM
			X						2. วิเคราะห์ความเสี่ยงด้านไซเบอร์ในระดับองค์กรโดยใช้วิธีการวิเคราะห์เชิงสถานการณ์ การทดสอบความทนทานและการพิจารณาผลกระทบเชิงระบบได้	Workshop scenario-based risk analysis และ stress testing สำหรับเหตุการณ์ไซเบอร์ระดับองค์กร	แบบฝึกหัด scenario/stress test รายงานวิเคราะห์ผลกระทบ และการนำเสนอ

รายวิชา	PLO 1	PLO 2	PLO 3	PLO 4	PLO 5.1	PLO 5.2	PLO 6	PLO 7	CLO	วิธีการจัดการเรียนการสอน	วิธีวัดผลการเรียนรู้
		X	X						3. ประเมินความเสี่ยงด้านไซเบอร์ในห่วงโซ่อุปทานและผู้ให้บริการภายนอก และเสนอแนวทางการควบคุมที่เหมาะสมได้	กรณีศึกษา third-party/supply chain cyber risk และกิจกรรมออกแบบ control requirements	รายงาน third-party risk assessment แผนควบคุม และ rubric ความเหมาะสม
			X				X		4. ออกแบบตัวชี้วัดความเสี่ยง ตัวชี้วัดประสิทธิภาพ และแดชบอร์ดรายงานความเสี่ยงที่ตอบโจทย์การตัดสินใจของผู้บริหารและคณะกรรมการได้	Workshop KRI/KPI และ risk dashboard สำหรับผู้บริหาร/คณะกรรมการ	ชิ้นงาน dashboard/risk report การนำเสนอ และ rubric ด้านการใช้ตัดสินใจ
			X				X		5. เสนอแผนการจัดการความเสี่ยง รวมถึงทางเลือกการโอนความเสี่ยง เช่น การประกันความเสี่ยงไซเบอร์ และเชื่อมโยงกับการเสริมสร้างความยืดหยุ่นขององค์กรด้านไซเบอร์ได้	กิจกรรมออกแบบ risk treatment plan และอภิปราย cyber insurance/cyber resilience	รายงาน risk treatment plan การประเมินทางเลือก cyber insurance และการนำเสนอ
สมซ 7012 การตรวจสอบความมั่นคงปลอดภัยสารสนเทศ	X			X					1. อธิบายหลักการและบทบาทของการตรวจสอบความมั่นคงปลอดภัยสารสนเทศในระบบการบริหารความมั่นคงปลอดภัยสารสนเทศได้อย่างถูกต้อง	บรรยายหลักการ auditing และบทบาท audit ใน ISMS พร้อมกรณีศึกษา	สอบ แบบทดสอบ และงานสรุปบทบาท audit
		X		X					2. วางแผนและดำเนินการตรวจสอบความมั่นคงปลอดภัยสารสนเทศตามมาตรฐานที่เกี่ยวข้อง เช่น ISO/IEC 27001:2022 ได้ในระดับที่เหมาะสม	Workshop audit plan/checklist และ role play การประชุมเปิด/ปิดการตรวจสอบ	ชิ้นงาน audit plan/checklist แบบประเมิน role play และสอบข้อเขียน
		X	X						3. ประเมินการออกแบบและประสิทธิผลของมาตรการควบคุมด้านความมั่นคงปลอดภัยไซเบอร์ และวิเคราะห์ระดับความพร้อมและขีดความสามารถด้านความมั่นคงปลอดภัยขององค์กรได้	ฝึก control testing และ security maturity/readiness assessment จากกรณีศึกษา	working papers รายงาน control testing และ rubric การประเมิน maturity

รายวิชา	PLO 1	PLO 2	PLO 3	PLO 4	PLO 5.1	PLO 5.2	PLO 6	PLO 7	CLO	วิธีการจัดการเรียนการสอน	วิธีวัดผลการเรียนรู้
		X	X						4. ใช้เทคนิคและเครื่องมือวิเคราะห์ข้อมูลเพื่อสนับสนุนการตรวจสอบ รวมถึงแนวคิดการเฝ้าระวังควบคุมอย่างต่อเนื่อง (continuous monitoring) ได้	Lab data analytics for audit และ สาธิต continuous monitoring concept	ผลการปฏิบัติ lab รายงาน data analytics และแบบประเมินการตีความผล
				X			X	X	5. จัดทำรายงานการตรวจสอบที่ชัดเจนเป็นระบบ และเสนอข้อเสนอแนะเชิงปฏิบัติ พร้อมทั้งติดตามผลการแก้ไขข้อบกพร่อง โดยยึดถือจริยธรรมและมาตรฐานวิชาชีพการตรวจสอบได้	ฝึกจัดทำ audit report และ CAPA follow-up พร้อมอภิปรายจริยธรรมและมาตรฐานวิชาชีพ	รายงานผลตรวจ+CAPA follow-up การนำเสนอ และ rubric ด้านความชัดเจน/จริยธรรม
สมซ 9000 การค้นคว้าอิสระ						X			1. ระบุและกำหนดประเด็นปัญหาและคำถามวิจัยที่เกี่ยวข้องกับการจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ได้อย่างชัดเจนและมีนัยสำคัญทางวิชาการหรือเชิงปฏิบัติ	สัมมนาและให้คำปรึกษารายบุคคล workshop การกำหนดปัญหา/คำถามวิจัย และ peer feedback	ข้อเสนอโครงการค้นคว้าอิสระ rubric ความชัดเจนของปัญหา และรายงานความก้าวหน้า
		X				X	X		2. สืบค้น ทบทวน และสังเคราะห์วรรณกรรมที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยงไซเบอร์ และกฎหมายที่เกี่ยวข้อง เพื่อสร้างกรอบแนวคิดของการศึกษาค้นคว้าได้	clinic literature review การสาธิตการค้นฐานข้อมูล และ workshop การสังเคราะห์วรรณกรรม	literature review matrix รายงานทบทวนวรรณกรรม และการนำเสนอกรอบแนวคิด
						X			3. เลือกใช้ระเบียบวิธีวิจัยและเทคนิคการเก็บรวบรวมและวิเคราะห์ข้อมูลที่เหมาะสมกับปัญหาวิจัยด้านการจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ได้	Workshop methodology และ data collection/analysis design พร้อมคำปรึกษาจากอาจารย์ที่ปรึกษา	แผนระเบียบวิธีวิจัย แบบประเมินความเหมาะสม และรายงานความก้าวหน้า

รายวิชา	PLO 1	PLO 2	PLO 3	PLO 4	PLO 5.1	PLO 5.2	PLO 6	PLO 7	CLO	วิธีการจัดการเรียนการสอน	วิธีวัดผลการเรียนรู้
		X				X	X		4. วิเคราะห์และตีความผลการศึกษาค้นคว้า พร้อมเชื่อมโยงกับทฤษฎีและการปฏิบัติ และเสนอข้อเสนอแนะเชิงนโยบายหรือเชิงปฏิบัติได้อย่างมีเหตุผล	ติดตามความก้าวหน้าเป็นระยะ clinic การวิเคราะห์ข้อมูล และกิจกรรมอภิปรายผลการศึกษา	รายงานผลการวิเคราะห์ การนำเสนอความก้าวหน้า และ rubric ด้านเหตุผลของข้อเสนอ
						X	X	X	5. จัดทำรายงานค้นคว้าอิสระและนำเสนอผลการศึกษาในรูปแบบทางวิชาการ โดยยึดหลักจริยธรรมการวิจัยและการคุ้มครองข้อมูลได้อย่างเคร่งครัด	ให้คำปรึกษาการเขียนรายงาน rehearsal นำเสนอ และตรวจสอบจริยธรรม/การอ้างอิง/การคุ้มครองข้อมูล	รายงานค้นคว้าอิสระฉบับสมบูรณ์ การสอบปากเปล่า/การนำเสนอ และ rubric จริยธรรม/การอ้างอิง
สมซ 9004 วิทยานิพนธ์			X		X				1. กำหนดปัญหาวิจัยและคำถามวิจัยด้านการจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ที่มีความซับซ้อนและมีคุณค่าทางวิชาการหรือเชิงนโยบายได้อย่างชัดเจน	ให้คำปรึกษาเข้มข้น สัมมนาวิจัย และ workshop การกำหนดปัญหา/คำถามวิจัยระดับบัณฑิตศึกษา	proposal defense ข้อเสนอโครงการวิทยานิพนธ์ และ rubric ด้านคุณค่าทางวิชาการ/นโยบาย
		X			X	X			2. ดำเนินการทบทวนและสังเคราะห์วรรณกรรมอย่างเป็นระบบ เพื่อพัฒนากรอบแนวคิดและสมมติฐานการวิจัยในประเด็นความมั่นคงปลอดภัยไซเบอร์และความเสี่ยงดิจิทัลได้	systematic review workshop, peer feedback และการให้คำปรึกษาการสร้างกรอบแนวคิด	รายงานทบทวนวรรณกรรม กรอบแนวคิด/สมมติฐาน และการประเมินจากอาจารย์ที่ปรึกษา
		X	X		X				3. เลือกและประยุกต์ใช้ระเบียบวิธีวิจัยขั้นสูงและเทคนิคการวิเคราะห์ข้อมูลที่เหมาะสม เพื่อสร้างองค์ความรู้ แบบจำลอง เครื่องมือ หรือนวัตกรรมใหม่ด้านการจัดการความเสี่ยงความมั่นคงปลอดภัยไซเบอร์ได้	methodology clinic, data analysis workshop และการติดตามความก้าวหน้าการพัฒนาแบบจำลอง/เครื่องมือ/นวัตกรรม	รายงานระเบียบวิธีวิจัย ผลการวิเคราะห์ข้อมูล ชิ้นงานแบบจำลอง/เครื่องมือ และ progress defense

รายวิชา	PLO 1	PLO 2	PLO 3	PLO 4	PLO 5.1	PLO 5.2	PLO 6	PLO 7	CLO	วิธีการจัดการเรียนการสอน	วิธีวัดผลการเรียนรู้
			X		X		X		4. วิเคราะห์ผลการวิจัยอย่างลุ่มลึก เชื่อมโยงกับทฤษฎีและการปฏิบัติ และเสนอข้อเสนอเชิงนโยบายหรือเชิงกลยุทธ์ที่มีความสมเหตุสมผลและมีศักยภาพในการนำไปใช้ได้จริง	สัมมนาอภิปรายผลการวิจัย peer review และคำปรึกษาเชิงลึกด้านการตีความผล/ข้อเสนอเชิงนโยบาย	บทผลการวิจัยและอภิปรายผล การนำเสนอความก้าวหน้า และ rubric ด้านความลุ่มลึก/ความสมเหตุสมผล
					X		X	X	5. เขียน จัดทำ และนำเสนอวิทยานิพนธ์ตามมาตรฐานวิชาการ รวมทั้งเผยแพร่ผลงานวิจัยในช่องทางที่เหมาะสม โดยยึดถือจริยธรรมการวิจัยและการคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด	ให้คำปรึกษาการเขียนวิทยานิพนธ์ rehearsal การสอบปากเปล่า และการเตรียมเผยแพร่ผลงานวิชาการ	วิทยานิพนธ์ฉบับสมบูรณ์ การสอบปากเปล่า ผลงานเผยแพร่/บทความ (ถ้ามี) และ rubric ระเบียบวิธี/จริยธรรม

หมายเหตุ – รายวิชาเสริมพื้นฐานของสถาบัน ขอให้เป็นไปตามที่สถาบันกำหนด

2. ผลลัพธ์การเรียนรู้คาดหวังรายชั้นปี (Yearly Learning Outcome: YLO)

หลักสูตรไม่มีการกำหนดผลลัพธ์การเรียนรู้คาดหวังรายชั้นปี (YLO) แยกเป็นการเฉพาะ เนื่องจากเป็นหลักสูตรระดับบัณฑิตศึกษาที่มีโครงสร้างการเรียนรู้และแผนการศึกษาแตกต่างกันตามความเหมาะสมของผู้เรียน อย่างไรก็ตาม หลักสูตรใช้ระบบติดตามและประเมินความก้าวหน้าของผู้เรียนเป็นรายภาคการศึกษา โดยอาศัยผลการบรรลุผลลัพธ์การเรียนรู้ระดับรายวิชา (Course Learning Outcomes: CLOs) ของแต่ละรายวิชา ซึ่งมีการกำหนดความเชื่อมโยงกับผลลัพธ์การเรียนรู้ระดับหลักสูตร (Program Learning Outcomes: PLOs) อย่างชัดเจน

การประเมินการบรรลุ CLO ของผู้เรียนดำเนินการผ่านเครื่องมือประเมินที่หลากหลายตามลักษณะของรายวิชา เช่น การสอบ การทำรายงาน การนำเสนอ โครงงาน กรณีศึกษา การปฏิบัติการ และการประเมินผลงาน โดยใช้เกณฑ์การให้คะแนน (rubric) ที่กำหนดไว้ในรายละเอียดรายวิชา ทั้งนี้ ผู้เรียนจะถือว่าบรรลุ CLO เมื่อมีผลการประเมินตามเกณฑ์ขั้นต่ำที่รายวิชากำหนดไว้อย่างชัดเจน เช่น การได้คะแนนไม่ต่ำกว่าร้อยละที่กำหนด หรือมีระดับผลการประเมินตาม rubric อยู่ในระดับที่ยอมรับได้

หลักสูตรใช้ผลการประเมิน CLO ของผู้เรียนในแต่ละภาคการศึกษาเป็นข้อมูลสำคัญในการติดตามพัฒนาการด้านความรู้ ทักษะ และสมรรถนะอย่างต่อเนื่อง และใช้ประกอบการวิเคราะห์ความเชื่อมโยงไปสู่การบรรลุ PLO ของหลักสูตร หากพบว่าผู้เรียนยังไม่บรรลุ CLO ในรายวิชาใด อาจารย์ผู้สอนและหลักสูตรจะดำเนินมาตรการสนับสนุนหรือพัฒนาการเรียนรู้เพิ่มเติมตามความเหมาะสม เช่น การมอบหมายงานเพิ่มเติม การให้ปรับปรุงรายงานหรือชิ้นงาน การให้คำปรึกษาทางวิชาการ หรือการจัดกิจกรรมเสริมเฉพาะด้าน เพื่อช่วยให้ผู้เรียนสามารถพัฒนาสมรรถนะตามผลลัพธ์การเรียนรู้ที่กำหนดไว้

นอกจากนี้ หลักสูตรจะนำผลการบรรลุ CLO ของรายวิชาต่าง ๆ มาวิเคราะห์ในภาพรวมตามความเชื่อมโยงกับ PLO เพื่อใช้ในการทบทวนคุณภาพการจัดการเรียนการสอน และเพื่อให้มั่นใจว่าผู้เรียนที่สำเร็จการศึกษามีสมรรถนะทางวิชาการและทักษะวิชาชีพสอดคล้องกับมาตรฐานคุณวุฒิและเป้าหมายของหลักสูตร

หมวดที่ 6 การประเมินผลการเรียนและเกณฑ์สำเร็จการศึกษา

1. หลักเกณฑ์ในการให้ระดับคะแนน (เกรด)

ผลการศึกษา หมายถึง ผลรวมของการทดสอบ การทำแบบฝึกหัด การเขียนรายงาน การสอบ การฝึกภาคสนาม และการประเมินผลในรูปแบบอื่น ๆ ตามที่อาจารย์ผู้สอนกำหนด ผลการสอบวิทยานิพนธ์และวิชาการค้นคว้าอิสระ การประเมินผลรายวิชาเป็นไปตามข้อบังคับของสถาบันบัณฑิตพัฒนบริหารศาสตร์ว่าด้วยการศึกษา ดังนี้

1.1 ผลการศึกษารายวิชาที่มีค่าระดับและนำมาคำนวณระดับคะแนนเฉลี่ยแสดงออกเป็นขั้นต่าง ๆ และมีค่าเฉลี่ยต่อหนึ่งหน่วยกิตดังต่อไปนี้

A	=	4.0	หมายถึง Excellent (ดีเลิศ)
A-	=	3.7	หมายถึง Almost Excellent (เกือบดีเลิศ)
B+	=	3.3	หมายถึง Very good (ดีมาก)
B	=	3.0	หมายถึง Good (ดี)
B-	=	2.7	หมายถึง Almost Good (เกือบดี)
C+	=	2.3	หมายถึง Fair (พอใช้)
C	=	2.0	หมายถึง Almost Fair (เกือบพอใช้)
C-	=	1.7	หมายถึง Poor (อ่อน)
D	=	1.0	หมายถึง Very Poor (อ่อนมาก)
F	=	0	หมายถึง Failure (ตก)

1.2 ผลการศึกษาที่ไม่มีค่าระดับ และไม่นำมาคำนวณระดับคะแนนเฉลี่ย ให้แสดงดังต่อไปนี้

W	หมายถึง Withdrawal (เพิกถอน)
I	หมายถึง Incomplete (ผลการศึกษาไม่สมบูรณ์)
S	หมายถึง Satisfactory (เป็นที่พอใจ)
U	หมายถึง Unsatisfactory (ไม่เป็นที่พอใจ)
AU	หมายถึง Audit (ร่วมฟัง)
P	หมายถึง Pass (ผ่าน)
N	หมายถึง Not Pass (ไม่ผ่าน)
IP	หมายถึง In Progress (อยู่ระหว่างดำเนินการ)
T	หมายถึง Terminate (ให้ยุติ)
TR	หมายถึง Transferring from formal education, outside the institute (การโอนจากการศึกษาในระบบภายนอกสถาบัน)
TR1	หมายถึง Transferring from non-formal education (การโอนจากการศึกษานอกระบบ)
TR2	หมายถึง Transferring from informal education (การโอนจากการศึกษาตามอัธยาศัย)

2. กระบวนการตรวจสอบผลสัมฤทธิ์ของนักศึกษา

2.1 การตรวจสอบผลลัพธ์การเรียนรู้แต่ละรายวิชา

แต่ละรายวิชามีการจัดการเรียนรู้ให้มีความสอดคล้องของรายวิชากับผลลัพธ์การเรียนรู้ของหลักสูตร (PLO) วัดผลลัพธ์การเรียนรู้ของรายวิชา (CLO) มีวิธีการจัดการเรียนรู้ และวิธีวัดผลการเรียนรู้ตามที่ระบุในตารางที่ 1

2.2 การตรวจสอบผลลัพธ์การเรียนรู้เมื่อสำเร็จการศึกษา

นักศึกษาได้ผ่านการตรวจสอบผลลัพธ์การเรียนรู้รายวิชา (CLO) แสดงว่า นักศึกษาบรรลุผลลัพธ์การเรียนรู้ของหลักสูตร (PLO) ครบถ้วน อย่างไรก็ตาม หลักสูตรกำหนดให้นักศึกษาต้องสอบประมวลความรู้ซึ่งจะประกอบไปด้วยวิชาหลักตามที่คณะประกาศกำหนด โดยมีเกณฑ์การประเมินเพื่อเพิ่มความมั่นใจว่า นักศึกษาบรรลุผลลัพธ์การเรียนรู้ที่สำคัญ เมื่อผ่านการสอบประมวลความรู้แล้ว นักศึกษายังต้องสอบปากเปล่าซึ่งจะเป็นการตรวจสอบการบรรลุผลลัพธ์การเรียนรู้อีกครั้งหนึ่ง

3. เกณฑ์การสำเร็จการศึกษาตามหลักสูตร

ใช้เกณฑ์สำเร็จการศึกษาตามข้อบังคับของสถาบันบัณฑิตพัฒนบริหารศาสตร์ว่าด้วยการศึกษา พ.ศ. 2563 และที่แก้ไขเพิ่มเติมฉบับที่ 2 พ.ศ. 2566 ฉบับที่ 3 พ.ศ. 2568 และประกาศคณะกรรมการมาตรฐานการอุดมศึกษา เรื่อง เกณฑ์มาตรฐานหลักสูตรระดับบัณฑิตศึกษา พ.ศ. 2565 โดยการสำเร็จการศึกษาของนักศึกษาระดับปริญญาโท จะต้องปฏิบัติได้ครบถ้วนตามข้อกำหนด ดังนี้

3.1 สำหรับนักศึกษาที่ศึกษาแผน 1 (แบบวิชาการ)

1) มีความรู้ภาษาอังกฤษหรือภาษาต่างประเทศ และ/หรือความรู้พิเศษอย่างอื่น ตามมาตรฐานที่สถาบันกำหนด

2) ศึกษาครบถ้วนตามข้อกำหนดของหลักสูตร และมีผลการศึกษาของทุกวิชาที่ลงทะเบียนเข้าเรียนเพื่อหน่วยกิตตามหลักสูตรเฉลี่ยสะสมไม่ต่ำกว่า 3.00

3) ได้ผลการศึกษาของวิชาหลัก และ/หรือวิชารหัส 6000 มีผลการศึกษาเฉลี่ยสะสมไม่ต่ำกว่า 3.00

4) สอบประมวลความรู้ ได้ผล “P” (ผ่าน)

5) ต้องมีผลการศึกษาวิชาวิทยานิพนธ์เป็น “S”และส่งวิทยานิพนธ์แล้ว

6) เสนอวิทยานิพนธ์และสอบผ่านการสอบป้องกันวิทยานิพนธ์ขั้นสุดท้าย จนบรรลุผลลัพธ์การเรียนรู้ของหลักสูตร (PLO) โดยให้ดำเนินการโดยคณะกรรมการสอบป้องกันวิทยานิพนธ์ที่คณะสถิติประยุกต์แต่งตั้ง และเป็นระบบเปิดให้ผู้สนใจเข้ารับฟังได้

7) ผลงานวิทยานิพนธ์หรือส่วนหนึ่งของวิทยานิพนธ์ต้องได้รับการตีพิมพ์ หรืออย่างน้อยได้รับการเผยแพร่ในรูปแบบบทความหรือนวัตกรรมหรือสิ่งประดิษฐ์หรือผลงานทางวิชาการอื่น ซึ่งสามารถสืบค้นได้ตามที่สภาสถาบันกำหนด

8) มีผลลัพธ์การเรียนรู้ที่กำหนดไว้ในหลักสูตร

3.2 สำหรับนักศึกษาที่ศึกษาแผน 2 (แบบวิชาชีพ)

1) มีความรู้ภาษาอังกฤษหรือภาษาต่างประเทศ และ/หรือความรู้พิเศษอย่างอื่น ตามมาตรฐานที่สถาบันกำหนด

2) ศึกษาครบถ้วนตามข้อกำหนดของหลักสูตร และมีผลการศึกษาของทุกวิชาที่ลงทะเบียนเข้าเรียนเพื่อหน่วยกิตตามหลักสูตรเฉลี่ยสะสมไม่ต่ำกว่า 3.00

3) ได้ผลการศึกษาของวิชาหลัก และ/หรือวิชารหัส 6000 มีผลการศึกษาเฉลี่ยสะสมไม่ต่ำกว่า 3.00

4) สอบประมวลความรู้ ได้ผล “P” (ผ่าน)

5) สอบปากเปล่า (Oral Examination) ได้ผล “P” (ผ่าน)

6) เสนอและเผยแพร่รายงานการค้นคว้าอิสระและสอบผ่านการสอบปากเปล่าขั้นสุดท้าย จนบรรลุผลลัพธ์การเรียนรู้ของหลักสูตร (PLO) โดยให้ดำเนินการโดยคณะกรรมการสอบการค้นคว้าอิสระที่คณะสถิติประยุกต์แต่งตั้ง และเป็นระบบเปิดให้ผู้สนใจเข้ารับฟังได้ โดยจัดทำเป็นประกาศเชิญชวนให้ผู้สนใจเข้ารับฟังได้ตามกำหนดเวลาการสอบ

7) มีผลลัพธ์การเรียนรู้ที่กำหนดไว้ในหลักสูตร

หมวดที่ 7 การประกันคุณภาพหลักสูตร

1. ระบบการประกันคุณภาพที่ใช้

การบริหารจัดการหลักสูตรตามประกาศคณะกรรมการมาตรฐานการอุดมศึกษา เรื่อง เกณฑ์มาตรฐานหลักสูตรระดับบัณฑิตศึกษา พ.ศ. 2565 และมีการนำเกณฑ์ในระดับสากลมาใช้ คือ เกณฑ์ AUN-QA (ASEAN University Network Quality Assurance) โดยหลักสูตรมีการประเมินคุณภาพภายในทุกปี

2. ระบบประกันและการบริหารคุณภาพหลักสูตร

2.1 การวางแผนคุณภาพ เพื่อให้นักศึกษาเกิดการเรียนรู้ตามผลลัพธ์การเรียนรู้ที่กำหนด หลักสูตรมีกระบวนการดำเนินงานดังนี้

- กระบวนการปรับปรุงหลักสูตร โดยอธิบายขั้นตอนอยู่ในหมวดที่ 8 ระบบและกลไกในการพัฒนาหลักสูตร
- กระบวนการคัดเลือก
    - มีการกำหนดคุณสมบัติของผู้ที่มีสิทธิสมัครเป็นนักศึกษา
    - กำหนดเกณฑ์การพิจารณา
    - มีการสอบสัมภาษณ์
- กระบวนการก่อนเปิดภาคการศึกษา
    - จัดปฐมนิเทศเพื่อชี้แจง และทำความเข้าใจในเรื่องต่าง ๆ เช่น การลงทะเบียน แผนการศึกษา ผลลัพธ์การเรียนรู้ บริการต่าง ๆ เป็นต้น
    - อาจารย์ผู้สอนนำผลการประเมินจากภาคการศึกษาที่ผ่านมาใช้ในการปรับปรุงรายวิชา
    - อาจารย์ผู้สอนจัดทำ course syllabus และแจ้งให้นักศึกษาทราบ
    - มีการประชุมคณะกรรมการบริหารหลักสูตรเพื่อพิจารณาภาระงานสอน
- กระบวนการปรับพื้นฐาน
    - ในกรณีที่นักศึกษามีความรู้พื้นฐานไม่เพียงพอ หลักสูตรมีวิชาเสริมพื้นฐานให้นักศึกษาได้เตรียมความพร้อม
    - การปรับพื้นฐานทางภาษาอังกฤษ
    - การเรียนวิชาพื้นฐานเพื่อการสื่อสารและนำเสนอ
- กระบวนการทดสอบ
    - มีการจัดสอบย่อย กลางภาค ปลายภาค ตามที่กำหนดใน course syllabus
    - มีการให้การบ้าน โครงงาน รายงาน ตามที่กำหนดใน course syllabus
- กระบวนการหลังปิดภาคการศึกษา
    - การให้เกรดผ่านการพิจารณาเห็นชอบจากคณบดี
    - มีการติดตามการส่งเกรดให้เป็นไปตามกำหนด
    - ผู้สอนมีการบันทึกผลและแนวทางการปรับปรุงสำหรับภาคการศึกษาถัดไป

- นักศึกษาประเมินผู้สอนและการเรียนการสอนในแต่ละรายวิชา
- มีการประชุมคณะกรรมการพัฒนาหลักสูตรเพื่อพิจารณาทบทวนผลสัมฤทธิ์ของหลักสูตร

- กระบวนการในระหว่างการศึกษา
  - นักศึกษาสามารถพบอาจารย์ที่ปรึกษาหรืออาจารย์ประจำวิชาเพื่อขอคำแนะนำหรือคำปรึกษาได้ตลอดระยะเวลาที่ศึกษา โดยอาจใช้ช่องทางที่หลากหลายหรือการนัดหมายหรือในชั่วโมงที่กำหนด
  - จัดให้มีการสัมมนา เพื่อให้นักศึกษาได้พบกับอาจารย์และนักศึกษาด้วยกันในหลักสูตรต่าง ๆ ของคณะหลังจากที่ได้ศึกษามาประมาณหนึ่งปีการศึกษา เพื่อรับฟังปัญหาและทำความเข้าใจเพิ่มเติม
  - นักศึกษาสามารถเข้าร่วมประชุมวิชาการหรือศึกษาดูงานได้
  - ส่งเสริมให้นักศึกษาสอบใบรับรองความสามารถทางวิชาชีพ (certificate)
- การปรับปรุงแก้ไขกรณีผลลัพธ์การเรียนรู้ของหลักสูตร (PLO) ไม่เป็นไปตามที่กำหนด
  - ผลลัพธ์การเรียนรู้ไม่เป็นไปตามที่กำหนดโดยตรวจสอบจาก CLO ของแต่ละรายวิชาและเชื่อมโยงไปสู่ PLO แบ่งเป็นกรณีต่าง ๆ ดังนี้
    - กรณีที่อาจต้องปรับปรุงรายวิชา คำอธิบายรายวิชา ผลลัพธ์การเรียนรู้หลักสูตร
      - เมื่อพบความผิดปกติของผลการเรียนการสอน การประเมินอาจารย์ผู้สอน หรือข้อมูลอื่นใด คณะกรรมการพัฒนาหลักสูตรจะจัดให้มีการประชุมเพื่อหารือแนวทางในการปรับปรุง
      - ขอความเห็นชอบในการปรับปรุงต่อ คณะกรรมการบริหารหลักสูตร คณะกรรมการประจำคณะ ที่ประชุมคณะกรรมการบริหารสถาบัน สภาวิชาการ สภาสถาบัน ตามลำดับ
    - กรณีที่เครื่องมือสนับสนุนการเรียนรู้ไม่เหมาะสมหรือไม่เพียงพอ
      - อาจารย์ในแต่ละรายวิชาส่งคำขอให้คณะฯ หรือสถาบัน จัดหาเครื่องมือดังกล่าว
    - กรณีอาจารย์ที่มีอยู่ไม่เพียงพอ
      - หลักสูตรโดยความเห็นชอบของคณะกรรมการประจำคณะ เสนอรายชื่ออาจารย์ภายนอกที่มีคุณสมบัติในการสอนในรายวิชาที่ขาดแคลนอาจารย์ผู้สอน
      - ดำเนินการเปิดรับสมัครอาจารย์ผู้สอนตามกรอบอัตรากำลังที่ได้รับอนุมัติจากสถาบัน

- กระบวนการก่อนสำเร็จการศึกษา
    - สำหรับนักศึกษาที่เรียนแผน 1 แบบวิชาการ จะต้องสอบประมวลความรู้ โดยได้ผลเป็น “ผ่าน” ซึ่งข้อสอบจะประกอบไปด้วยวิชาหลัก และผลงานวิทยานิพนธ์หรือส่วนหนึ่งของวิทยานิพนธ์ต้องได้รับการตีพิมพ์ หรืออย่างน้อยได้รับการเผยแพร่ในรูปแบบบทความหรือนวัตกรรมหรือสิ่งประดิษฐ์หรือผลงานทางวิชาการอื่น ซึ่งสามารถสืบค้นได้ตามที่สภาสถาบันกำหนด
    - สำหรับนักศึกษาที่เรียนแผน 2 แบบวิชาชีพ จะต้องสอบประมวลความรู้และสอบปากเปล่า โดยได้ผลเป็น “ผ่าน” ซึ่งข้อสอบจะประกอบไปด้วยวิชาหลัก มีการประเมินผลวิชาค้นคว้าอิสระ โดยนักศึกษาต้องผ่านการนำเสนอผลการศึกษาต่อคณะกรรมการประเมินผลวิชาค้นคว้าอิสระซึ่งประกอบไปด้วยอาจารย์ในหลักสูตรอย่างน้อยสองคน จากนั้นนำผลงานการค้นคว้าอิสระไปเผยแพร่สู่สาธารณะ
- กระบวนการหลังสำเร็จการศึกษา
    - มีการสำรวจข้อมูลการได้งาน
    - มีการประชุมคณะกรรมการพัฒนาหลักสูตรเพื่อพิจารณาผลสัมฤทธิ์ของหลักสูตร

2.2 การรักษาคุณภาพ

ในการดำเนินงานหลักสูตร จะต้องปฏิบัติตามแผนคุณภาพในข้อ 2.1 โดยผู้รับผิดชอบหลักคือ ผู้อำนวยการหลักสูตรและอาจารย์ผู้รับผิดชอบหลักสูตร ซึ่งผลการดำเนินการต้องมีการขออนุมัติต่อคณบดี คณะกรรมการบริหารหลักสูตร คณะกรรมการประจำคณะ หรือ คณะกรรมการบริหารสถาบันแล้วแต่กรณี

2.3 การควบคุมคุณภาพ

2.3.1 การตรวจประเมินหลักสูตร

หลักสูตรจะมีการดำเนินการตามเกณฑ์มาตรฐานหลักสูตรระดับบัณฑิตศึกษา พ.ศ. 2565 และเกณฑ์ AUN-QA (ASEAN University Network Quality Assurance) และมีการประเมินโดยคณะกรรมการทั้งภายในและภายนอก ซึ่งจะดำเนินการตรวจประเมินปีละหนึ่งครั้งหลังสิ้นสุดปีการศึกษา นอกจากนี้ ยังมีคณะกรรมการพัฒนาหลักสูตร คณะกรรมการบริหารหลักสูตร คณะกรรมการประจำคณะ คณะอนุกรรมการบริหารสถาบัน คณะกรรมการบริหารสถาบัน สภาวิชาการและสภาสถาบัน ที่จะเป็นผู้พิจารณาผลการประเมินคุณภาพของหลักสูตร และติดตามการปรับปรุงหลักสูตรให้มีคุณภาพ โดยผ่านการประชุมของคณะกรรมการต่าง ๆ ดังกล่าว รวมไปถึงการติดตามคุณสมบัติของอาจารย์ผู้สอน อาจารย์ประจำหลักสูตร อาจารย์ผู้รับผิดชอบหลักสูตร ให้เป็นไปตามเกณฑ์มาตรฐานหลักสูตรระดับบัณฑิตศึกษา พ.ศ. 2565 โดยผ่านการรายงานผลการปฏิบัติตามภาระงานประจำอีกด้วย

2.3.2 การศึกษาวิชาเสริมพื้นฐาน

นักศึกษาที่เข้าศึกษาโดยมิได้สำเร็จการศึกษาในสาขาที่เกี่ยวข้องหรือไม่ผ่านการประเมินความรู้พื้นฐานที่กำหนด จะต้องลงทะเบียนเรียนวิชาเสริมพื้นฐาน ซึ่งจะทำให้นักศึกษามีความพร้อมในการศึกษาในรายวิชาตามที่กำหนดในหลักสูตรต่อไปได้

2.3.3 การประเมินในระหว่างการศึกษาแต่ละรายวิชา

อาจารย์ผู้สอนจะติดตามและประเมินผลการเรียนรู้ของนักศึกษาตามวิธีการที่ระบุไว้ในหมวดที่ 6 ข้อ 2.1 พร้อมทั้งให้คำแนะนำแก่นักศึกษาอย่างเหมาะสม ในกรณีที่ผลการตรวจสอบผลลัพธ์การเรียนรู้ของนักศึกษาไม่เป็นไปตามเกณฑ์ที่กำหนด หรือมีผลการศึกษาต่ำกว่า B อาจารย์ผู้สอนสามารถพิจารณาให้ผู้เรียนจัดทำรายงานเพิ่มเติม ดำเนินกิจกรรมเสริมเพื่อพัฒนาผลลัพธ์การเรียนรู้ หรือเข้ารับการวัดและประเมินผลการเรียนรู้ใหม่

2.3.4 การขอตรวจสอบผลการศึกษา

ในกรณีที่นักศึกษามีข้อสงสัยในผลการศึกษา หรือ ผลลัพธ์การเรียนรู้ต่ำกว่าเกณฑ์ที่กำหนด นักศึกษาสามารถขอตรวจสอบการประเมินการบรรลุผลลัพธ์การเรียนรู้ต่ออาจารย์ผู้สอนได้ ซึ่งนักศึกษาจะได้รับคำอธิบายถึงเหตุผลที่ไม่บรรลุผลลัพธ์การเรียนรู้ผ่านวิธีการตรวจสอบผลลัพธ์การเรียนรู้ในคราวนั้น ๆ

2.3.5 การติดตามและประเมินในแต่ละภาคการศึกษา

หลักสูตรมีระบบการติดตามและประเมินผลความก้าวหน้าของนักศึกษาอย่างต่อเนื่องในทุกสิ้นภาคการศึกษา โดยจำแนกสถานะผู้เรียนออกเป็นกลุ่มต่างๆ อย่างชัดเจน ได้แก่ กลุ่มคงอยู่ กลุ่มที่สำเร็จการศึกษา กลุ่มลาออก กลุ่มพ้นสภาพเนื่องจากครบระยะเวลาการศึกษา และโดยเฉพาะกลุ่มเสี่ยงที่มีผลการเรียนต่ำกว่าเกณฑ์ ซึ่งข้อมูลเหล่านี้จะถูกนำมาวิเคราะห์เพื่อดำเนินมาตรการเชิงรุกในการช่วยเหลือนักศึกษาเป็นรายบุคคล เช่น การตรวจสอบผังการศึกษาและการให้คำปรึกษาทางวิชาการ เพื่อให้มั่นใจว่านักศึกษาจะสามารถบรรลุผลลัพธ์การเรียนรู้ได้ตามเป้าหมาย พร้อมกันนี้ สถิติและข้อมูลสารสนเทศที่ได้จากการติดตามจะถูกนำไปใช้วางแผนบริหารจัดการและปรับปรุงคุณภาพหลักสูตรให้มีประสิทธิภาพยิ่งขึ้นต่อไป

2.4 การปรับปรุงและพัฒนาคุณภาพ

เมื่อสิ้นสุดการประเมินเกณฑ์มาตรฐานหลักสูตรระดับบัณฑิตศึกษา พ.ศ. 2565และเกณฑ์ AUN-QA (ASEAN University Network Quality Assurance) ในแต่ละปี ทางหลักสูตรจะนำการวิเคราะห์จุดแข็ง/แนวทางเสริมจุดแข็ง จุดที่ต้องการพัฒนา/ข้อเสนอแนะในการปรับปรุง ที่ได้รับจากคณะกรรมการประเมินไปปรับปรุงและพัฒนาคุณภาพของหลักสูตรต่อไป ร่วมกับข้อมูลที่วัดได้ในกรณีอื่น เช่น การประเมินการเรียนการสอน การสำรวจความคิดเห็นในโอกาสและกิจกรรมต่าง ๆ โดยในส่วนของหลักสูตร จะมีการประชุมคณะกรรมการพัฒนาหลักสูตรเพื่อหารือถึงแนวทางในการปรับปรุงและพัฒนาคุณภาพ ในส่วนของคุณสมบัติของอาจารย์นั้น สถาบันและคณะมีหลักเกณฑ์และงบประมาณในการสนับสนุนให้อาจารย์ทำผลงานและขอกำหนดตำแหน่งทางวิชาการสูงขึ้น ซึ่งจะเป็นการทำให้อาจารย์มีคุณสมบัติเป็นไปตามเกณฑ์มาตรฐานหลักสูตรระดับบัณฑิตศึกษาพ.ศ. 2565

3. การสื่อสารและเผยแพร่ข้อมูลของหลักสูตรให้ผู้มีส่วนได้ส่วนเสียได้รับทราบ

หลักสูตรมีการเผยแพร่ข้อมูลของหลักสูตรผ่านช่องทางเว็บไซต์ของคณะฯ และสถาบัน (กองบริการการศึกษา) ซึ่งสามารถเข้าถึงได้โดยบุคคลทั่วไป และมีการประชาสัมพันธ์เผยแพร่ข้อมูลต่าง ๆ ผ่านหลายช่องทางดังแสดงในตารางที่ 3 นอกจากนี้ คณะฯ และสถาบัน ยังได้จัดโครงการเปิดบ้านเพื่อเป็นช่องทางเผยแพร่ข้อมูลอีกทางหนึ่ง อีกทั้งในวันปฐมนิเทศนักศึกษาทั้งภาคปกติและภาคพิเศษ จะมีการพบปะพูดคุยกับผู้อำนวยการหลักสูตรเพื่อชี้แจงรายละเอียดเกี่ยวกับข้อมูลของหลักสูตรทั้งหมด มีการแจกคู่มือนักศึกษาของหลักสูตร โดยในคู่มือดังกล่าวได้ระบุข้อมูลรายละเอียดของหลักสูตรไว้อย่างครบถ้วน

ตารางที่ 3 ข้อมูลข่าวสาร สื่อ/ช่องทางการสื่อสารจำแนกตามผู้มีส่วนได้ส่วนเสีย

ผู้มีส่วนได้ส่วนเสีย	ข้อมูลข่าวสาร	สื่อ/ช่องทาง
นักศึกษา	-รายละเอียดสาระวิชา/การประเมิน เอกสารประกอบการสอน	-ไฟล์เอกสารบน Microsoft Teams
	-ตารางเรียน	-เว็บไซต์ของคณะ (https://as.nida.ac.th)
	-ระเบียบ ข้อบังคับ	-เว็บไซต์กองบริการการศึกษา (https://edserv.nida.ac.th)
	-กิจกรรม	-เว็บไซต์ของคณะ (https://as.nida.ac.th) Line application เพจเฟซบุ๊กของคณะ (Graduate School of Applied Statistics, NIDA)
ศิษย์เก่า	-กิจกรรม	-เว็บไซต์ของคณะ (https://as.nida.ac.th), Line application, เพจเฟซบุ๊กของคณะ (Graduate School of Applied Statistics, NIDA), e-mail
บุคคลทั่วไป และองค์กรต่าง ๆ	-ข้อมูลหลักสูตร	-เว็บไซต์ของคณะ (https://as.nida.ac.th), ติดต่อด้วยตนเอง, สอบถามทางโทรศัพท์ หรือ e-mails หรือ inbox, เพจเฟซบุ๊กของคณะ (Graduate School of Applied Statistics, NIDA)
	-การรับสมัครเรียน	-เว็บไซต์สถาบัน (https://nida.ac.th), เว็บไซต์กองบริการการศึกษา (https://edserv.nida.ac.th), เว็บไซต์ของคณะ (https://as.nida.ac.th), เพจเฟซบุ๊กของคณะ (Graduate School of Applied Statistics, NIDA)
	-กิจกรรม	-เว็บไซต์ของคณะ (https://as.nida.ac.th), เพจเฟซบุ๊กของคณะ (Graduate School of Applied Statistics, NIDA)

หมวดที่ 8 ระบบและกลไกในการพัฒนาหลักสูตร

1. คณะกรรมการพัฒนาหลักสูตร (คณะกรรมการร่างหลักสูตร คณะกรรมการวิพากษ์หลักสูตร)

มีการแต่งตั้งคณะกรรมการพัฒนาหลักสูตรตามคำสั่งคณะสถิติประยุกต์ สถาบันบัณฑิตพัฒนบริหารศาสตร์ที่ 14/2568 ลงวันที่ 19 มีนาคม 2568 เรื่อง การแต่งตั้งคณะกรรมการพัฒนาหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการจัดการความเสี่ยงความมั่นคงทางไซเบอร์ หลักสูตรปรับปรุง พ.ศ. 2569 ดังนี้

1. รองศาสตราจารย์ ดร.ปราโมทย์ กั่วเจริญ ประธานกรรมการ
2. ผู้ช่วยศาสตราจารย์ ดร.สุเทพ ทองงาม กรรมการ
3. รองศาสตราจารย์ ดร.โอม ศรนิล กรรมการ
4. รองศาสตราจารย์ ดร.นิธินันท์ ธรรมากรนนท์ กรรมการ
5. ผู้ช่วยศาสตราจารย์ ดร.ธนาสัย สุคนธ์พันธุ์ กรรมการ
6. อาจารย์ ดร.อัญธิกา ณ พิบูลย์ กรรมการ
7. อาจารย์ ดร.บุญฤทธิ์ อดิพัฒน์ ผู้ทรงคุณวุฒิภายนอก
8. นายสัจจะ โชคบุญส่งสวัสดิ์ ผู้ทรงคุณวุฒิภายนอก
9. อาจารย์ ดร.นันทพงศ์ เขียนดวงจันทร์ ผู้ทรงคุณวุฒิภายนอก
10. นางสาวศศินันท์ บัญลือสิงห์ เลขานุการ

โดยให้คณะกรรมการพัฒนาหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการจัดการความเสี่ยงความมั่นคงทางไซเบอร์ หลักสูตรปรับปรุง พ.ศ. 2569 มีหน้าที่ดังนี้

1. จัดการพัฒนาหลักสูตรให้เป็นไปตามเกณฑ์มาตรฐานหลักสูตร
2. วางแผนการพัฒนาและบริหารหลักสูตรเกี่ยวกับโครงสร้าง เนื้อหารายวิชาของหลักสูตร
3. จัดเตรียมแผนการเปิดสอนและการประชาสัมพันธ์หลักสูตร
4. คณะกรรมการภายนอกเข้าร่วมประชุมหารือ ให้คำปรึกษา ข้อเสนอแนะและความคิดเห็นในการพัฒนาหรือปรับปรุงหลักสูตร และ/หรือเข้าร่วมในการวิพากษ์หลักสูตร

2. ขั้นตอนการพัฒนาหลักสูตร การตรวจสอบหลักสูตร จนถึงการอนุมัติของสภาสถาบัน

- แต่งตั้งคณะกรรมการพัฒนาหลักสูตร
- จัดประชุมคณะกรรมการพัฒนาหลักสูตรเพื่อกำหนดกรอบและแนวทางการดำเนินงาน
- รวบรวมข้อมูลที่เกี่ยวข้องกับการพัฒนาหลักสูตร และนำเสนอในที่ประชุมคณะกรรมการพัฒนาหลักสูตร
- กำหนดแนวทางการปรับปรุงหลักสูตร
- ดำเนินการจัดทำร่างหลักสูตรปรับปรุง
- จัดประชุมคณะกรรมการพัฒนาหลักสูตรเพื่อพิจารณาและให้ความเห็นชอบต่อร่างหลักสูตร
- ดำเนินการวิพากษ์หลักสูตรโดยผู้ทรงคุณวุฒิ
- ปรับปรุงหลักสูตรตามข้อเสนอแนะจากการวิพากษ์

- เวียนร่างหลักสูตรปรับปรุงให้คณะกรรมการพัฒนาหลักสูตรพิจารณาให้ความเห็นชอบเพิ่มเติมผ่านกลุ่ม Line หรือช่องทางออนไลน์
- นำเสนอร่างหลักสูตรปรับปรุงต่อที่ประชุมคณะกรรมการบริหารหลักสูตรเพื่อพิจารณา
- นำเสนอร่างหลักสูตรต่อที่ประชุมคณะกรรมการบริหารคณะ เพื่อพิจารณาให้ความเห็นชอบ
- ส่งร่างหลักสูตรให้กองบริการการศึกษาตรวจสอบความถูกต้องของข้อมูลและเอกสาร
- นำเสนอร่างหลักสูตรต่อที่ประชุมอนุกรรมการบริหารสถาบันด้านการศึกษา เพื่อพิจารณาให้ความเห็นชอบ
- นำเสนอร่างหลักสูตรต่อที่ประชุมสภาวิชาการ เพื่อพิจารณาให้ความเห็นชอบ
- นำเสนอร่างหลักสูตรต่อที่ประชุมคณะกรรมการบริหารสถาบัน เพื่อพิจารณาให้ความเห็นชอบ
- นำเสนอร่างหลักสูตรเข้าสู่ที่ประชุมสภาสถาบัน เพื่ออนุมัติหลักสูตรอย่างเป็นทางการ

3. ผลการดำเนินงานของหลักสูตรที่ผ่านมา ปรากฏตามตารางด้านล่างนี้

ภาคปกติ

ปีการศึกษา-ภาคการศึกษา	ขึ้นทะเบียน	รักษาสถานภาพ	ลาพักการศึกษา	ลาออก	พ้นสภาพ	สำเร็จการศึกษา
67-2	1	-	-	-	-	-
68-1	5	-	-	-	-	-
68-2	3	-	-	-	-	-

ภาคพิเศษ

ปีการศึกษา-ภาคการศึกษา	ขึ้นทะเบียน	รักษาสถานภาพ	ลาพักการศึกษา	ลาออก	พ้นสภาพ	สำเร็จการศึกษา
64-2	8	-	-	-	-	8
65-1	7	-	-	-	1	6
65-2	7	2	-	-	1	4
66-1	9	-	-	1	1	-
66-2	14	-	-	-	2	-
67-1	12	-	-	-	-	-
67-2	12	-	-	1	-	-
68-1	24	-	2	1	-	-
68-2	15	-	-	-	-	-

จากข้อมูลจำนวนนักศึกษาที่ขึ้นทะเบียนในช่วงปีการศึกษา 64-2 ถึง 68-2 พบว่าหลักสูตรมีแนวโน้มการเติบโตของจำนวนนักศึกษาโดยรวมเพิ่มขึ้นอย่างต่อเนื่อง แม้จะมีความผันผวนในบางภาคการศึกษา โดยในช่วงแรกจำนวนผู้ขึ้นทะเบียนอยู่ในระดับ 7–8 คน ก่อนจะเพิ่มขึ้นเป็น 9 และ 14 คนในปีการศึกษา 66 ทรงตัวที่ 12 คนในปีการศึกษา 67 และขยายตัวอย่างชัดเจนในปีการศึกษา 68 โดยเฉพาะภาค

การศึกษา 68-1 ที่มีจำนวนผู้ขึ้นทะเบียนสูงสุด 24 คน ทั้งนี้ แม้ภาคการศึกษา 68-2 จะลดลงเหลือ 15 คน แต่ยังถือว่าสูงกว่าหลายภาคการศึกษาในอดีต สะท้อนให้เห็นว่าหลักสูตรได้รับความสนใจเพิ่มขึ้นและมีแนวโน้มเติบโตในระยะยาว

4. สิ่งที่นำมาพิจารณาในการกำหนดผลลัพธ์การเรียนรู้ของหลักสูตร

หลักสูตรได้กำหนดผลลัพธ์การเรียนรู้ของหลักสูตร (PLO1–PLO7) โดยพิจารณาให้สอดคล้องกับความต้องการและความคาดหวังของผู้มีส่วนได้เสีย แนวโน้มทักษะและเทคโนโลยี ตลอดจนกรอบนโยบายทั้งในระดับประเทศและระดับสถาบัน ทั้งนี้ หลักสูตรใช้ข้อมูลเชิงประจักษ์จากหลายแหล่ง ได้แก่ การสำรวจ การสัมภาษณ์ การสนทนากลุ่ม การประเมินความพึงพอใจของนายจ้าง การวิเคราะห์ตลาดแรงงาน และการเทียบเคียงหลักสูตร (benchmarking) เพื่อใช้ประกอบการทบทวนและปรับปรุงโครงสร้างหลักสูตร รายวิชา เนื้อหา กิจกรรมการเรียนรู้ และวิธีการประเมินผล ให้สามารถสนับสนุนการบรรลุผลลัพธ์การเรียนรู้ของหลักสูตรได้อย่างเหมาะสม

4.1 ความคิดเห็นและความคาดหวังของผู้มีส่วนได้เสีย

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการจัดการความเสี่ยงความมั่นคงทางไซเบอร์ ให้ความสำคัญกับการพัฒนาหลักสูตรบนฐานของข้อมูลจากผู้มีส่วนได้เสียและแหล่งข้อมูลเชิงประจักษ์ที่สะท้อนความต้องการจริงของตลาดแรงงาน วิชาชีพ กฎหมาย มาตรฐาน และบริบทการเปลี่ยนแปลงของเทคโนโลยี เพื่อให้ผลลัพธ์การเรียนรู้ของหลักสูตร โครงสร้างรายวิชา เนื้อหาการเรียนการสอน และแนวทางการประเมินผล มีความสอดคล้องกับความต้องการของประเทศ ภาคอุตสาหกรรม หน่วยงานกำกับดูแล และมาตรฐานสากลด้านความมั่นคงปลอดภัยไซเบอร์

4.1.1 ระบบและวิธีการได้มาซึ่งข้อมูลจากผู้มีส่วนได้เสียและแหล่งข้อมูลที่เกี่ยวข้อง

หลักสูตรกำหนดกระบวนการรับฟังความคิดเห็นและวิเคราะห์ข้อมูลจากผู้มีส่วนได้เสียอย่างเป็นระบบ โดยใช้ทั้งข้อมูลเชิงปริมาณและเชิงคุณภาพ ได้แก่ การสำรวจความคิดเห็นด้วยแบบสอบถาม การสัมภาษณ์ การสนทนากลุ่ม การประชุมคณะกรรมการพัฒนาหลักสูตร การประชุมคณะกรรมการบริหารหลักสูตร และการรับฟังข้อเสนอแนะจากผู้ทรงคุณวุฒิ ผู้ใช้บัณฑิต ศิษย์เก่า นักศึกษาปัจจุบัน อาจารย์ผู้สอน และผู้เชี่ยวชาญจากภาครัฐ ภาคเอกชน และองค์กรวิชาชีพที่เกี่ยวข้อง

นอกจากข้อมูลจากผู้มีส่วนได้เสียโดยตรงแล้ว หลักสูตรยังใช้แหล่งข้อมูลเชิงประจักษ์จากภายนอกประกอบการวิเคราะห์ความต้องการของหลักสูตร ได้แก่

- ตลาดแรงงาน แหล่งงาน และแพลตฟอร์มจัดหางาน

หลักสูตรวิเคราะห์ข้อมูลตลาดแรงงานจาก ประกาศรับสมัครงานจำนวน 176 ประกาศ จาก 139 บริษัทในประเทศไทย ซึ่งรวบรวมจากแพลตฟอร์มจัดหางานและแหล่งประกาศรับสมัครงานออนไลน์ที่เกี่ยวข้อง โดยครอบคลุมตำแหน่งงานในสายงานความมั่นคงปลอดภัยไซเบอร์ การบริหารความเสี่ยงเทคโนโลยีสารสนเทศ การตรวจสอบระบบสารสนเทศ การคุ้มครองข้อมูลส่วนบุคคล ธรรมาภิบาลดิจิทัล และการกำกับดูแลเทคโนโลยี

ในการวิเคราะห์ หลักสูตรพิจารณารายละเอียดตำแหน่งงาน หน้าที่ความรับผิดชอบ คุณสมบัติที่ต้องการ ประสบการณ์ที่เกี่ยวข้อง เครื่องมือหรือเทคโนโลยีที่ระบุในประกาศ และทักษะที่นายจ้างต้องการ เพื่อสะท้อนความต้องการกำลังคนและสมรรถนะที่ใช้จริงในตลาดแรงงานภายในประเทศ ข้อมูลดังกล่าวช่วยให้หลักสูตรสามารถระบุแนวโน้มของตำแหน่งงานเป้าหมายและทักษะสำคัญที่บัณฑิตควรมี เช่น technical cybersecurity, SOC/incident response, cloud security, penetration testing, vulnerability management, IT/cyber risk, GRC, compliance, information security audit, data protection, privacy governance และการสื่อสารกับผู้บริหารหรือผู้มีส่วนได้ส่วนเสียในองค์กร

นอกจากนี้ หลักสูตรยังใช้ข้อมูลแนวโน้มอาชีพจาก U.S. Bureau of Labor Statistics (BLS) เป็นข้อมูลประกอบในระดับสากล โดยเฉพาะกลุ่มอาชีพ Information Security Analysts ซึ่ง BLS คาดการณ์ว่าอัตราการจ้างงานจะเพิ่มขึ้น ร้อยละ 29 ในช่วงปี 2024–2034 สูงกว่าค่าเฉลี่ยของทุกอาชีพซึ่งอยู่ที่ ร้อยละ 3 อย่างมีนัยสำคัญ และคาดว่าจะมีตำแหน่งงานเปิดใหม่เฉลี่ยประมาณ 16,000 ตำแหน่งต่อปี ตลอดช่วงเวลาดังกล่าว ข้อมูลนี้สะท้อนแนวโน้มความต้องการบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ในระดับนานาชาติ และสนับสนุนความจำเป็นในการพัฒนาหลักสูตรให้ผลิตบัณฑิตที่มีสมรรถนะตรงกับความต้องการของตลาดแรงงานทั้งในประเทศและต่างประเทศ

ตำแหน่งงานที่นำมาวิเคราะห์ เช่น Cybersecurity Analyst, SOC Analyst, Incident Responder, IT Risk Officer, GRC Specialist, Information Security Officer, Cloud Security Engineer, Penetration Tester, Vulnerability Assessor, IT Auditor, Data Protection Officer และ Privacy/Compliance Specialist ทั้งนี้ ผลการวิเคราะห์ประกาศรับสมัครงานจากแพลตฟอร์มจัดหางานถูกนำมาใช้เป็นข้อมูลเชิงประจักษ์ประกอบการกำหนดผลลัพธ์การเรียนรู้ของหลักสูตร โครงสร้างรายวิชา เนื้อหารายวิชา และวิธีการจัดการเรียนการสอน เพื่อให้หลักสูตรสอดคล้องกับความต้องการจริงของตลาดแรงงานและวิชาชีพ.

- มาตรฐานสากลและกรอบการทำงานด้านวิชาชีพ

หลักสูตรพิจารณามาตรฐานและกรอบการทำงานที่เกี่ยวข้อง เช่น ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 27701, ISO/IEC 42001, NIST Cybersecurity Framework, NIST AI Risk Management Framework, CIS Controls, COBIT, ITIL, MITRE ATT&CK, OWASP Top 10 และกรอบ DevSecOps เพื่อใช้เป็นข้อมูลในการกำหนดองค์ความรู้ ทักษะ และสมรรถนะที่ผู้สำเร็จการศึกษาควรมี

- กฎหมาย ระเบียบ และข้อกำหนดด้าน Compliance

หลักสูตรวิเคราะห์กฎหมายและข้อกำหนดที่เกี่ยวข้องกับการทำงานด้านไซเบอร์และดิจิทัล เช่น กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายคุ้มครองข้อมูลส่วนบุคคล กฎหมายธุรกรรมอิเล็กทรอนิกส์ กฎหมายที่เกี่ยวข้องกับบริการดิจิทัลและการกำกับดูแลเทคโนโลยี รวมถึงข้อกำหนดด้าน compliance ของหน่วยงานกำกับดูแลในภาคส่วนต่าง ๆ เพื่อให้หลักสูตรสามารถผลิตบัณฑิตที่เข้าใจทั้งมิติเทคนิค มิติความเสี่ยง และมิติกฎหมาย/การกำกับดูแล

- คุณวุฒิวิชาชีพและ Certifications

หลักสูตรพิจารณาองค์ความรู้และสมรรถนะที่สะท้อนอยู่ในคุณวุฒิวิชาชีพและการรับรองระดับสากล เช่น CISSP, CISM, CISA, CRISC, CCSP, Security+, CySA+, PenTest+, CEH, ISO/IEC 27001 Lead Implementer, ISO/IEC 27001 Lead Auditor, AWS Certified Security - Specialty, Microsoft Security/Compliance Certifications และ Cisco CyberOps เพื่อใช้เป็นแนวทางเทียบเคียงสมรรถนะของหลักสูตรกับมาตรฐานวิชาชีพ

ข้อมูลจากแหล่งดังกล่าวถูกนำมาวิเคราะห์ร่วมกับข้อมูลจากผู้มีส่วนได้เสียโดยตรง เพื่อให้หลักสูตรสามารถกำหนดผลลัพธ์การเรียนรู้ที่มีความทันสมัย สอดคล้องกับความต้องการจริงของตลาดแรงงาน และเชื่อมโยงกับมาตรฐานวิชาชีพ กฎหมาย และข้อกำหนดที่เกี่ยวข้อง

- หลักสูตรของสถาบันอื่นและการเทียบเคียงหลักสูตร

หลักสูตรใช้การเทียบเคียงหลักสูตรกับสถาบันอุดมศึกษาทั้งในประเทศและต่างประเทศ เพื่อใช้เป็นข้อมูลประกอบการพัฒนาหลักสูตรให้มีมาตรฐานทางวิชาการ เทียบเคียงได้ในระดับสากล และสอดคล้องกับพัฒนาการของสาขาวิชาความมั่นคงปลอดภัยไซเบอร์ การบริหารความเสี่ยงดิจิทัล กฎหมายและธรรมาภิบาลเทคโนโลยี โดยหลักสูตรได้พิจารณาแนวทางจากหลักสูตรที่เกี่ยวข้องของสถาบันอุดมศึกษา เช่น มหาวิทยาลัยธรรมศาสตร์ มหาวิทยาลัยมหิดล Lehigh University, Rutgers University และ Carnegie Mellon University

การเทียบเคียงหลักสูตรพิจารณาจากองค์ประกอบสำคัญ ได้แก่ ชื่อและเป้าหมายของหลักสูตร โครงสร้างหลักสูตร กลุ่มรายวิชาหลักและรายวิชาเลือก สาระการเรียนรู้ ผลลัพธ์การเรียนรู้ที่คาดหวัง แนวทางการจัดการเรียนการสอน การฝึกปฏิบัติ การวิจัย การบูรณาการกับมาตรฐานวิชาชีพ และความเชื่อมโยงกับความต้องการของตลาดแรงงาน ทั้งนี้ เพื่อให้หลักสูตรสามารถปรับปรุงโครงสร้างรายวิชาและสาระการเรียนรู้ให้ครอบคลุมทั้งมิติด้านเทคนิค ด้านการบริหารความเสี่ยง ด้านกฎหมายและ compliance ด้านธรรมาภิบาลข้อมูลและปัญญาประดิษฐ์ ด้านการวิจัย และด้านทักษะการสื่อสารเชิงวิชาชีพ

ข้อมูลจากการเทียบเคียงหลักสูตรช่วยให้หลักสูตรสามารถระบุจุดแข็ง จุดที่ควรพัฒนา และช่องว่างของสมรรถนะที่ควรเสริมสร้างให้แก่ผู้เรียน เช่น ความมั่นคงปลอดภัยของระบบคลาวด์และคลาวด์เนทีฟ การปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์และ SOC การทดสอบการเจาะระบบและการจัดการช่องโหว่ การบริหารความเสี่ยงไซเบอร์และ GRC การตรวจสอบความมั่นคงปลอดภัยสารสนเทศ การคุ้มครองข้อมูลส่วนบุคคล การกำกับดูแลระบบที่ใช้ปัญญาประดิษฐ์ และการสร้างองค์ความรู้หรือนวัตกรรมจากงานวิจัยระดับบัณฑิตศึกษา

ผลจากการเทียบเคียงดังกล่าวถูกนำมาใช้ประกอบการกำหนดและทบทวนผลลัพธ์การเรียนรู้ของหลักสูตร เพื่อให้ PLO มีความสมบูรณ์ ครอบคลุม และสอดคล้องกับมาตรฐานทางวิชาการและวิชาชีพมากยิ่งขึ้น รวมทั้งสนับสนุนให้หลักสูตรมีความร่วมสมัย สามารถตอบสนองต่อความเปลี่ยนแปลงของเทคโนโลยี ภัยคุกคามไซเบอร์ กฎหมาย มาตรฐานสากล และความต้องการของตลาดแรงงานทั้งในประเทศและระดับนานาชาติ.

4.1.2 กลุ่มผู้มีส่วนได้เสียและแหล่งข้อมูลที่ใช้ในการพัฒนาหลักสูตร

กลุ่ม/แหล่งข้อมูล	วิธีการได้มาซึ่งข้อมูล	เหตุผลที่ใช้เป็นแหล่งข้อมูล
ผู้ใช้บัณฑิตและตัวแทนภาคอุตสาหกรรม	แบบสอบถาม สัมภาษณ์ ประชุมรับฟังความคิดเห็น	สะท้อนสมรรถนะที่องค์กรต้องการจากผู้สำเร็จการศึกษา
ผู้ทรงคุณวุฒิและผู้เชี่ยวชาญภายนอก	ประชุมคณะกรรมการพัฒนาหลักสูตร ให้ข้อเสนอแนะ	ให้มุมมองเชิงวิชาการ วิชาชีพ และทิศทางการเปลี่ยนแปลงของสาขา
ศิษย์เก่าและนักศึกษาปัจจุบัน	แบบสอบถาม สัมภาษณ์ หรือประชุมรับฟังความคิดเห็น	สะท้อนประสบการณ์การเรียน การนำความรู้ไปใช้ และช่องว่างของหลักสูตร
อาจารย์ผู้รับผิดชอบหลักสูตร อาจารย์ประจำหลักสูตร และอาจารย์ผู้สอน	ประชุมหลักสูตร วิเคราะห์รายวิชาและทบทวนผลการเรียนรู้	ใช้กำกับความเหมาะสมของโครงสร้างหลักสูตร รายวิชา และผลลัพธ์การเรียนรู้
ตลาดแรงงาน แหล่งงาน และแพลตฟอร์มจัดหางาน และ Job Outlook	วิเคราะห์ประกาศรับสมัครงาน จำนวน 176 ประกาศ จาก 139 บริษัทในประเทศไทย จากแพลตฟอร์มจัดหางาน ร่วมกับข้อมูล Job Outlook จาก U.S. Bureau of Labor Statistics ช่วงปี 2024–2034	สะท้อนทักษะที่ตลาดแรงงานต้องการจริงทั้งในประเทศและแนวโน้มสากล โดย BLS คาดว่า Information Security Analysts จะเติบโต 29% ระหว่างปี 2024–2034 สูงกว่าค่าเฉลี่ยทุกอาชีพที่ 3%
มาตรฐานและกรอบการทำงาน	วิเคราะห์ข้อกำหนด แนวปฏิบัติ และ competency ที่เกี่ยวข้อง	ใช้เทียบเคียงองค์ความรู้และทักษะกับมาตรฐานสากล
กฎหมายและข้อกำหนด compliance	วิเคราะห์ข้อบังคับ หน้าที่ตามกฎหมาย และแนวปฏิบัติขององค์กร	ทำให้หลักสูตรครอบคลุมมิติการกำกับดูแลและความรับผิดทางกฎหมาย
Certifications และคุณวุฒิวิชาชีพ	วิเคราะห์ body of knowledge และ exam domains	ใช้เทียบเคียงหลักสูตรกับมาตรฐานวิชาชีพสากล
หลักสูตรของสถาบันอื่นและการเทียบเคียงหลักสูตร	เทียบเคียงหลักสูตรที่เกี่ยวข้องทั้งในประเทศและต่างประเทศ เช่น มหาวิทยาลัยธรรมศาสตร์ มหาวิทยาลัยมหิดล Lehigh University, Rutgers University และ Carnegie Mellon University	ใช้ระบุจุดแข็ง ช่องว่างของหลักสูตร และแนวทางปรับปรุง PLO รายวิชา และสาระการเรียนรู้

4.1.3 การวิเคราะห์ข้อมูลเพื่อนำไปกำหนด PLO

หลักสูตรนำข้อมูลจากผู้มีส่วนได้เสียและแหล่งข้อมูลภายนอกมาวิเคราะห์ร่วมกัน โดยใช้แนวทางการจัดกลุ่มสาระสำคัญจากข้อมูลหลายแหล่ง เพื่อให้มั่นใจว่าผลลัพธ์การเรียนรู้ของหลักสูตรไม่ได้ตั้งอยู่บนความเห็นเฉพาะกลุ่มใดกลุ่มหนึ่ง แต่สะท้อนความต้องการร่วมกันของภาควิชาการ ภาควิชาชีพ ตลาดแรงงาน มาตรฐาน กฎหมาย และข้อกำหนดด้าน compliance

- รวบรวมข้อมูลจากหลายแหล่ง: ได้แก่ ผู้ใช้บัณฑิต ผู้เชี่ยวชาญ ศิษย์เก่า นักศึกษาปัจจุบัน อาจารย์ผู้สอน ตลาดแรงงาน แพลตฟอร์มจัดหางาน มาตรฐานสากล กฎหมาย ข้อกำหนด compliance และ certifications

- จัดกลุ่มทักษะและสมรรถนะที่พบซ้ำ: หลักสูตรจัดกลุ่มข้อมูลเป็นประเด็นสำคัญ เช่น ความรู้ด้านระบบไซเบอร์ ทักษะ technical cybersecurity การบริหารความเสี่ยง GRC กฎหมายและ compliance ความปลอดภัยคลาวด์ SOC/Incident Response การตรวจสอบและ audit การคุ้มครองข้อมูลส่วนบุคคล AI governance การวิจัย การสื่อสาร และจริยธรรมวิชาชีพ

- วิเคราะห์ความสำคัญและความสอดคล้อง: ประเด็นที่พบถูกพิจารณาตามความสำคัญต่อการทำงานจริง ความสอดคล้องกับมาตรฐานวิชาชีพ ความจำเป็นตามกฎหมายและ compliance และความเหมาะสมกับระดับบัณฑิตศึกษา

- แปลงเป็นสมรรถนะของผู้สำเร็จการศึกษา: ข้อมูลที่ผ่านการวิเคราะห์ถูกสังเคราะห์เป็นสมรรถนะหลักของบัณฑิต ทั้งด้านความรู้ ทักษะ จริยธรรม และลักษณะบุคคล

- กำหนดเป็น PLO และตรวจสอบความครอบคลุม: สมรรถนะดังกล่าวถูกนำไปกำหนดเป็น PLO ของหลักสูตร และตรวจสอบว่า PLO ครอบคลุมความต้องการจากผู้มีส่วนได้เสีย ตลาดแรงงาน มาตรฐาน กฎหมาย compliance และ certifications อย่างเหมาะสม

4.1.4 ความเชื่อมโยงระหว่างแหล่งข้อมูลกับการกำหนด PLO

แหล่งข้อมูล/ความคาดหวัง	ประเด็นที่วิเคราะห์ได้	การนำไปกำหนด PLO
ตลาดแรงงานและแพลตฟอร์มจัดหางาน	ต้องการความรู้ด้านเครือข่าย ระบบ คลาวด์ SOC ความปลอดภัยของข้อมูล และ AI	PLO1, PLO2
ตำแหน่งงานด้าน SOC, Security Analyst, Incident Responder	ต้องการทักษะตรวจจับ วิเคราะห์ ตอบสนอง และฟื้นฟูเหตุการณ์ไซเบอร์	PLO2
ตำแหน่งงานด้าน IT Risk, Cyber Risk, GRC, Compliance	ต้องการทักษะบริหารความเสี่ยง ควบคุมภายใน รายงานความเสี่ยง และ governance	PLO3, PLO4, PLO6
มาตรฐาน ISO/IEC 27001, ISO/IEC 27005, NIST CSF, CIS Controls	ต้องการความรู้ด้าน ISMS, risk management, controls และ cybersecurity framework	PLO1, PLO3, PLO4
มาตรฐาน ISO/IEC 42001 และ NIST AI RMF	ต้องการความเข้าใจการกำกับดูแล AI และความเสี่ยงของระบบที่ใช้ปัญญาประดิษฐ์	PLO1, PLO3, PLO4
กฎหมายไซเบอร์ กฎหมายคอมพิวเตอร์ PDPA และ compliance	ต้องการบัณฑิตที่เข้าใจกฎหมาย หน้าที่ ความรับผิด และการปฏิบัติตามข้อกำหนด	PLO4, PLO7

แหล่งข้อมูล/ความคาดหวัง	ประเด็นที่วิเคราะห์ได้	การนำไปกำหนด PLO
Certifications เช่น CISSP, CISM, CISA, CRISC, CCSP, Security+, CySA+, PenTest+	ต้องการสมรรถนะเชิงวิชาชีพด้าน security management, audit, risk, cloud security, SOC และ penetration testing	PLO1, PLO2, PLO3, PLO4
ผู้ใช้บัณฑิตและผู้เชี่ยวชาญ	ต้องการบัณฑิตที่สื่อสารกับผู้บริหาร ทำงานข้ามสายงาน และเชื่อมโยงเทคนิคกับธุรกิจได้	PLO6
ศิษย์เก่าและนักศึกษาปัจจุบัน	ต้องการรายวิชาที่ทันสมัย มีการฝึกปฏิบัติ และเชื่อมโยงกับการทำงานจริง	PLO2, PLO3, PLO5.2, PLO6
อาจารย์และผู้รับผิดชอบหลักสูตร	ต้องการให้หลักสูตรมีความสอดคล้องเชิงวิชาการ มีการวิจัย และมีระบบประเมินผลลัพธ์การเรียนรู้	PLO5.1, PLO5.2

4.1.5 การนำผลการวิเคราะห์ไปใช้ในการปรับปรุงหลักสูตร

- กำหนด PLO ให้ครอบคลุมทั้งความรู้ด้านเทคโนโลยี ความมั่นคงปลอดภัยไซเบอร์ การบริหารความเสี่ยง กฎหมาย ธรรมาภิบาล การวิจัย การสื่อสาร และจริยธรรม

- ปรับปรุงรายวิชาให้สอดคล้องกับทักษะที่ตลาดแรงงานต้องการ เช่น SOC, Incident Response, Cloud Security, Penetration Testing, Vulnerability Management, Digital Forensics, DevSecOps, Cyber Risk, GRC, Data Protection และ AI Governance

- เชื่อมโยงเนื้อหารายวิชากับมาตรฐานและกรอบสากล เช่น ISO/IEC 27001, ISO/IEC 27005, ISO/IEC 42001, NIST CSF, NIST AI RMF, CIS Controls, COBIT, ITIL, MITRE ATT&CK และ OWASP

- เพิ่มความชัดเจนด้านกฎหมายและ compliance เพื่อให้ผู้เรียนเข้าใจหน้าที่ ความรับผิด และข้อกำหนดที่เกี่ยวข้องกับงานไซเบอร์และดิจิทัล

- ใช้ certifications และคุณวุฒิวิชาชีพเป็นข้อมูลเทียบเคียง เพื่อให้เนื้อหาหลักสูตรสอดคล้องกับ body of knowledge ที่เป็นที่ยอมรับในระดับสากล

- ออกแบบ CLO วิธีการเรียนการสอน และการวัดผลให้สะท้อนทักษะเชิงปฏิบัติและสมรรถนะที่ใช้จริงในการทำงาน

- กำหนดระบบทบทวนข้อมูลจากตลาดแรงงาน มาตรฐาน กฎหมาย และ certifications อย่างต่อเนื่อง เพื่อให้หลักสูตรสามารถปรับตัวได้ทันต่อการเปลี่ยนแปลง

ด้วยกระบวนการดังกล่าว หลักสูตรจึงใช้ทั้งข้อมูลจากผู้มีส่วนได้เสียโดยตรงและข้อมูลเชิงประจักษ์จากตลาดแรงงาน มาตรฐาน กฎหมาย compliance และ certifications เพื่อกำหนดผลลัพธ์การเรียนรู้ของหลักสูตรอย่างเป็นระบบ ทำให้ผู้รับผิดชอบหลักสูตรสามารถอธิบายได้ชัดเจนว่า PLO แต่ละข้อมีที่มาจากความต้องการจริงของภาควิชาการ ภาควิชาชีพ และตลาดแรงงาน

4.2 ทิศทาง นโยบายและยุทธศาสตร์การพัฒนากำลังคนของประเทศ

หลักสูตรพิจารณาทิศทางและยุทธศาสตร์การพัฒนากำลังคนของประเทศที่มุ่ง **ยกระดับศักยภาพกำลังคนด้านดิจิทัลและความมั่นคงปลอดภัยไซเบอร์** ควบคู่กับการส่งเสริม **การใช้ข้อมูลและปัญญาประดิษฐ์อย่างรับผิดชอบ** (Responsible/Trustworthy AI) เพื่อนำไปใช้จริงในการขับเคลื่อนองค์กรและเศรษฐกิจดิจิทัล

จากแนวทางดังกล่าว หลักสูตรได้นำมาใช้ในการกำหนดและปรับปรุงผลลัพธ์การเรียนรู้ของหลักสูตร (PLO) และการจัดรายวิชาให้สอดคล้องอย่างเป็นรูปธรรม โดยเน้น 4 มิติหลัก ได้แก่

1. **ความรู้ด้านโครงสร้างพื้นฐานดิจิทัลและความมั่นคงปลอดภัยไซเบอร์** เพื่อให้เข้าใจสถาปัตยกรรม เทคโนโลยี และกลไกความปลอดภัยที่รองรับระบบดิจิทัลของประเทศและองค์กร (เชื่อมโยง **PLO1**)

2. **ทักษะเชิงปฏิบัติการด้านไซเบอร์** สำหรับการป้องกัน ตรวจจับ ตอบสนอง และฟื้นฟูบริการดิจิทัลอย่างเป็นระบบ (เชื่อมโยง **PLO2**)

3. **การบริหารความเสี่ยงไซเบอร์และความเสี่ยงดิจิทัล** ให้บูรณาการได้กับการบริหารความเสี่ยงองค์รวมขององค์กรและรองรับการตัดสินใจเชิงกลยุทธ์ (เชื่อมโยง **PLO3**)

4. **กฎหมาย มาตรฐาน และธรรมาภิบาล รวมถึงจริยธรรม** เพื่อให้การดำเนินงานด้านไซเบอร์และการใช้ AI เป็นไปตามข้อกำหนด โปร่งใส ตรวจสอบได้ และคำนึงถึงผลกระทบต่อสังคม (เชื่อมโยง **PLO4 และ PLO7**)

ดังนั้น แนวนโยบายระดับประเทศจึงถูกแปลงเป็น “สมรรถนะเป้าหมายของบัณฑิต” และสะท้อนในทั้งโครงสร้างรายวิชา กิจกรรมเชิงปฏิบัติ และการประเมินผล เพื่อให้บัณฑิตสามารถทำงานได้จริงและตอบโจทย์ทิศทางการพัฒนากำลังคนของประเทศอย่างยั่งยืน.

4.3 ยุทธศาสตร์ของสถาบัน

หลักสูตรนำยุทธศาสตร์การพัฒนาสถาบัน มาใช้เป็นกรอบในการกำหนดและปรับปรุงผลลัพธ์การเรียนรู้ของหลักสูตร (PLO) รวมถึงการออกแบบรายวิชา กิจกรรมการเรียนรู้ และการประเมินผล เพื่อให้บัณฑิตมีสมรรถนะสอดคล้องกับทิศทางของสถาบันอย่างเป็นรูปธรรม ดังนี้

- **ยุทธศาสตร์ที่ 1: สนับสนุนการทำวิจัย การต่อยอดสู่นวัตกรรม และการบริการวิชาการเพื่อความยั่งยืน**

  หลักสูตรออกแบบให้ผู้เรียนสามารถทำงานวิจัย/พัฒนาเชิงประยุกต์ สร้างองค์ความรู้ เครื่องมือ หรือแนวทางปฏิบัติที่นำไปใช้จริง และคำนึงถึงจริยธรรม/ผลกระทบต่อสังคม จึงเชื่อมโยงกับ **PLO5 (และ PLO5.1/5.2 ตามแผน), PLO7**

- **ยุทธศาสตร์ที่ 2: พัฒนาหลักสูตรที่เน้น Project-based Learning และ Data Analytics เพื่อการตัดสินใจและการบริหาร**

  หลักสูตรกำหนดให้รายวิชามีการเรียนรู้จากการลงมือทำ โครงงาน/กรณีศึกษา และการวิเคราะห์ข้อมูลอย่างเป็นระบบ (เช่น log analytics, threat intelligence analytics, risk

analytics) เพื่อสนับสนุนการตัดสินใจเชิงบริหารและการจัดการความเสี่ยง เชื่อมโยงกับ **PLO2, PLO3, PLO6** (และเสริม **PLO1**)

- **ยุทธศาสตร์ที่ 3: สร้างประสบการณ์การเรียนรู้ตลอดชีวิตและเข้าถึงได้หลากหลายช่องทาง**

  หลักสูตรส่งเสริมการเรียนรู้อย่างต่อเนื่องผ่านการอัปเดตองค์ความรู้ตามเทคโนโลยี/มาตรฐานใหม่ การฝึกทักษะที่ต่อยอดได้ และการเรียนรู้แบบยืดหยุ่น ซึ่งสะท้อนในสมรรถนะการพัฒนาตนเองและความรับผิดชอบต่อวิชาชีพ เชื่อมโยงกับ **PLO7** (และสนับสนุน **PLO6**)
- **ยุทธศาสตร์ที่ 4: ขับเคลื่อนการพลิกโฉมด้วยดิจิทัลเทคโนโลยี และการบริหารจัดการแบบเปิด (Open Governance)**

  หลักสูตรเน้นการบูรณาการเทคโนโลยีดิจิทัล/ไซเบอร์/AI เข้ากับการกำกับดูแล ความโปร่งใส ตรวจสอบได้ และการบริหารความเสี่ยงขององค์กร จึงเชื่อมโยงกับ **PLO3, PLO4, PLO6, PLO7**
- **ยุทธศาสตร์ที่ 5: ส่งเสริมความร่วมมือทางวิชาการระดับนานาชาติ (Internationalization)**

  หลักสูตรใช้กรอบมาตรฐาน/แนวปฏิบัติสากล (เช่น ISO/IEC, NIST, MITRE) และกรณีศึกษานานาชาติ รวมถึงการพัฒนาทักษะการสื่อสารเชิงวิชาชีพให้พร้อมทำงานในบริบทสากล เชื่อมโยงกับ **PLO4, PLO6** (และเสริม **PLO1–PLO2**)
- **ยุทธศาสตร์ที่ 6: สร้างความผูกพันและการมีส่วนร่วมของผู้มีส่วนได้ส่วนเสีย และการระดมทรัพยากร**

  หลักสูตรออกแบบให้เกิดการมีส่วนร่วมของนายจ้าง ศิษย์เก่า ผู้ทรงคุณวุฒิ และหน่วยงานที่เกี่ยวข้องผ่านเวทีให้ข้อเสนอแนะ โครงงานจากโจทย์จริง และกิจกรรมร่วมพัฒนา เพื่อให้ผลลัพธ์การเรียนรู้ตอบโจทย์ผู้ใช้บัณฑิต และให้ผู้เรียนสื่อสาร/ทำงานข้ามสายงานได้อย่างมีประสิทธิภาพ เชื่อมโยงกับ **PLO6, PLO3** (และเสริม **PLO2**)

4.4 การจัดกลุ่มสถาบันอุดมศึกษา

หลักสูตรมุ่งดำเนินการให้สอดคล้องกับการจัดกลุ่มสถาบันอุดมศึกษา โดยเน้นบทบาทของสถาบันในฐานะสถาบันอุดมศึกษาที่ผลิตบัณฑิตระดับบัณฑิตศึกษา สร้างองค์ความรู้ และพัฒนางานวิจัยที่ตอบสนองต่อการเปลี่ยนแปลงของเศรษฐกิจและสังคมดิจิทัล ทั้งในระดับประเทศ ภูมิภาค และระดับสากล โดยเฉพาะด้านการจัดการความเสี่ยงความมั่นคงทางไซเบอร์ ความมั่นคงปลอดภัยสารสนเทศ ธรรมาภิบาลดิจิทัล การคุ้มครองข้อมูลส่วนบุคคล และการกำกับดูแลเทคโนโลยีปัญญาประดิษฐ์

หลักสูตรให้ความสำคัญกับการพัฒนาศักยภาพด้านการวิจัยของคณาจารย์และนักศึกษาให้สามารถสร้างผลงานวิจัยระดับแนวหน้าของโลก ผ่านการกำหนดโจทย์วิจัยที่สอดคล้องกับปัญหาสำคัญและความท้าทายใหม่ของโลกไซเบอร์ เช่น การบริหารความเสี่ยงจากภัยคุกคามไซเบอร์ขั้นสูง ความยืดหยุ่นทางไซเบอร์ขององค์กร ความมั่นคงปลอดภัยของระบบคลาวด์และโครงสร้างพื้นฐานดิจิทัล ความเสี่ยงของระบบที่ใช้

ปัญญาประดิษฐ์ การกำกับดูแลข้อมูลและ AI อย่างรับผิดชอบ ตลอดจนประเด็นกฎหมายและจริยธรรมที่เกี่ยวข้องกับเทคโนโลยีดิจิทัล

ในการขับเคลื่อนงานวิจัย หลักสูตรสนับสนุนการทำวิจัยเชิงบูรณาการระหว่างศาสตร์ด้านเทคโนโลยี การจัดการ ความเสี่ยง กฎหมาย นโยบายสาธารณะ และธรรมาภิบาล เพื่อสร้างองค์ความรู้ใหม่ แบบจำลอง เครื่องมือ แนวปฏิบัติ และนวัตกรรมที่สามารถนำไปใช้ประโยชน์ได้จริงทั้งในภาครัฐ ภาคเอกชน และสังคมโดยรวม รวมทั้งส่งเสริมการตีพิมพ์เผยแพร่ผลงานในวารสารวิชาการระดับนานาชาติ การนำเสนอผลงานในการประชุมวิชาการชั้นนำ การพัฒนาความร่วมมือกับเครือข่ายวิจัยระดับนานาชาติ และการเชื่อมโยงงานวิจัยกับมาตรฐานสากลและแนวปฏิบัติระดับโลก

นอกจากนี้ หลักสูตรส่งเสริมการสร้างระบบนิเวศการเรียนรู้และการวิจัยที่เอื้อต่อความเป็นเลิศทางวิชาการ โดยสนับสนุนการใช้ฐานข้อมูลวิชาการ ห้องปฏิบัติการดิจิทัล ห้องปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ ระบบจำลองสถานการณ์ Cyber Range เครื่องมือวิเคราะห์ข้อมูลและภัยคุกคาม ตลอดจนความร่วมมือกับผู้เชี่ยวชาญจากภาคอุตสาหกรรม หน่วยงานกำกับดูแล และองค์กรวิชาชีพระดับนานาชาติ เพื่อให้นักศึกษาและคณาจารย์สามารถพัฒนางานวิจัยที่มีคุณภาพสูง มีผลกระทบทางวิชาการ และมีคุณค่าต่อการยกระดับขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศให้แข่งขันได้ในระดับสากล.

4.5 การเปลี่ยนแปลงของสภาพแวดล้อมที่เกี่ยวข้องกับหลักสูตร

หลักสูตรติดตามการเปลี่ยนแปลงของสภาพแวดล้อมที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์และดิจิทัลอย่างต่อเนื่อง ทั้งในมิติ **ภัยคุกคาม เทคโนโลยี และข้อกำกับดูแล** เพื่อให้เนื้อหารายวิชา กิจกรรมการเรียนรู้ และผลลัพธ์การเรียนรู้ของหลักสูตร (PLO) มีความร่วมสมัยและตอบโจทย์การใช้งานจริง โดยมีแนวทางดำเนินการสำคัญดังนี้

1. **ติดตามภัยคุกคามและรูปแบบการโจมตีที่เปลี่ยนแปลงรวดเร็ว**
   เช่น ภัยคุกคามที่ใช้ AI สนับสนุน (social engineering/automation), ransomware-as-a-service, supply-chain attacks, cloud abuse และการโจมตีต่อระบบ AI (เช่น prompt injection, data poisoning) เพื่อนำมาใช้ปรับกรณีศึกษา สถานการณ์จำลอง และ use case เชิงปฏิบัติให้สอดคล้องกับสถานการณ์จริง (เชื่อมโยง **PLO2, PLO3, PLO7**)
2. **ปรับเนื้อหาให้สอดคล้องกับเทคโนโลยีใหม่และสถาปัตยกรรมสมัยใหม่**
   ครอบคลุม cloud/cloud-native, data-driven systems และ AI/LLMs รวมถึงแนวทางการออกแบบความมั่นคงปลอดภัยให้เหมาะกับสภาพแวดล้อมดังกล่าว เพื่อให้ผู้เรียนมีความรู้เชิงสถาปัตยกรรมและสามารถประยุกต์ใช้เทคโนโลยีได้อย่างปลอดภัย (เชื่อมโยง **PLO1, PLO2**)

3. **อัปเดตกฎหมาย มาตรฐาน และกรอบธรรมาภิบาลที่เกี่ยวข้องอย่างสม่ำเสมอ**
   โดยเฉพาะด้านการคุ้มครองข้อมูลส่วนบุคคล ความมั่นคงปลอดภัยไซเบอร์ และการกำกับดูแล AI เพื่อนำไปสู่การออกแบบนโยบาย แนวปฏิบัติ และมาตรการควบคุมที่สอดคล้องกับข้อกำหนดและตรวจสอบได้ (เชื่อมโยง **PLO4, PLO3**)
4. **เชื่อมโยงกับความต้องการตลาดแรงงานและสมรรถนะที่องค์กรต้องการ**
   นำข้อมูลจากตลาดแรงงาน/วิชาชีพมาปรับเป้าหมายทักษะ (เช่น incident response, log analytics, risk & compliance, communication) และกำหนดการประเมินผลจากชิ้นงานจริง เพื่อให้บัณฑิตพร้อมทำงาน (เชื่อมโยง **PLO2, PLO6, PLO7**)

ด้วยแนวทางดังกล่าว หลักสูตรจึงสามารถปรับตัวให้ทันต่อการเปลี่ยนแปลงของบริบทเทคโนโลยีและความเสี่ยงดิจิทัลอย่างต่อเนื่อง และทำให้ผลลัพธ์การเรียนรู้สอดคล้องกับ **PLO1–PLO4 และ PLO7** อย่างเป็นรูปธรรม (พร้อมสนับสนุนมิติการสื่อสาร/การทำงานร่วมกันตามบริบทการใช้งานจริงด้วย).