โครงสร้างหลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาความมั่นคงปลอดภัยไซเบอร์ หลักสูตรใหม่ พ.ศ. 2568

จำนวนหน่วยกิตที่ศึกษาตลอดหลักสูตร	**120**	**หน่วยกิต**
โครงสร้างหลักสูตร		
1) หมวดวิชาศึกษาทั่วไป ไม่น้อยกว่า	**24**	**หน่วยกิต**
2) หมวดวิชาเฉพาะ	**90**	**หน่วยกิต**
2.1) วิชาแกน	27	หน่วยกิต
2.2) วิชาเฉพาะด้าน	45	หน่วยกิต
2.3) วิชาเลือก	12	หน่วยกิต
2.4) วิชาฝึกประสบการณ์วิชาชีพ	6	หน่วยกิต
3) หมวดวิชาเลือกเสรี ไม่น้อยกว่า	**6**	**หน่วยกิต**

รายละเอียดโครงสร้างหลักสูตร

1) หมวดวิชาศึกษาทั่วไป ไม่น้อยกว่า 24 หน่วยกิต

รหัสวิชา	ชื่อวิชา	หน่วยกิต
1500125	ภาษาอังกฤษเพื่อการเรียนรู้ตลอดชีวิต English for Lifelong Learning	3(3-0-6)
1500126	ภาษาอังกฤษในสังคมนานาชาติ English in International Society	3(3-0-6)
1500127	ทักษะการสื่อสารภาษาไทย Thai Communication Skills	3(3-0-6)
1500203	ความเป็นสวนดุสิต Suan Dusit Spirit	3(3-0-6)
4000116	วิทยาศาสตร์ในชีวิตประจำวัน Science in Everyday Life	3(3-0-6)
4000117	คณิตศาสตร์ในชีวิตประจำวัน Mathematics in Everyday Life	3(3-0-6)
4000118	เทคโนโลยีดิจิทัลในชีวิตประจำวัน Digital Technology in Everyday Life	3(3-0-6)
2500122	พลเมืองไทยในศตวรรษที่ 21 Thai Citizens in the 21st Century	3(3-0-6)

2) หมวดวิชาเฉพาะ 90 หน่วยกิต

2.1) วิชาแกน 27 หน่วยกิต

รหัสวิชา	ชื่อวิชา	หน่วยกิต
4231101	หลักการเขียนโปรแกรมคอมพิวเตอร์ Principles of Computer Programming	3(2-2-5)
4231301	หลักการวิทยาการข้อมูล Principles of Data Science	3(2-2-5)
4231401	จริยธรรมและกฎหมายไซเบอร์ Ethics and Cyber Laws	3(3-0-6)
4231402	ความมั่นคงปลอดภัยไซเบอร์ Cyber Security	3(2-2-5)
4231102	การเขียนโปรแกรมเพื่อความมั่นคงปลอดภัย Secure Programming	3(2-2-5)
4231103	สถาปัตยกรรมระบบปฏิบัติการ Operating System Architecture	3(2-2-5)
4231201	ระบบเครือข่ายคอมพิวเตอร์ Computer Network System	3(2-2-5)
4232301	การจัดการฐานข้อมูลอย่างมั่นคงปลอดภัย Secure Database Management	3(2-2-5)
4232501	สถาปัตยกรรมการประมวลผลแบบคลาวด์ Cloud Computing Architecture	3(2-2-5)

2.2) วิชาเฉพาะด้าน 45 หน่วยกิต

รหัสวิชา	ชื่อวิชา	หน่วยกิต
4232502	การพัฒนาเว็บแอปพลิเคชันให้มีความมั่นคงปลอดภัย Secure Web Application Development	3(2-2-5)
4232201	โพรโทคอลและบริการเครือข่าย Protocols and Network Services	3(2-2-5)
4232202	เครือข่ายไร้สายและความมั่นคงปลอดภัย Wireless Networking and Security	3(2-2-5)
4232203	การตรวจจับและการวินิจฉัยการบุกรุก Intrusion Detection and Diagnosis	3(2-2-5)
4232205	เครือข่ายไคลเอนต์และเซิร์ฟเวอร์ Client and Server Networks	3(2-2-5)
4232503	การตอบสนองต่อเหตุการณ์และการฟื้นฟู Incident Responses and Disaster Recovery	3(2-2-5)

รหัสวิชา	ชื่อวิชา	หน่วยกิต
4232204	การเขียนสคริปต์เพื่อความมั่นคงปลอดภัยไซเบอร์ Cyber Security Scripting	3(2-2-5)
4232302	วิทยาการข้อมูลเพื่อความมั่นคงปลอดภัยไซเบอร์ Data Science for Cyber Security	3(2-2-5)
4233301	การทดสอบเจาะระบบ Penetration Testing	3(2-2-5)
4233101	การจัดการศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัย Security Operation Center	3(2-2-5)
4233401	การบริหารความเสี่ยงและการรับรองความมั่นคงปลอดภัยไซเบอร์ Cyber Security Risk Management and Assurance	3(2-2-5)
4233102	ปัญญาประดิษฐ์และการเรียนรู้ของเครื่อง Artificial Intelligence and Machine Learning	3(2-2-5)
4233501	ความมั่นคงปลอดภัยของระบบคลาวด์ Cloud System Security	3(2-2-5)
4233502	นิติวิทยาศาสตร์ไซเบอร์ Cyber Forensics	3(2-2-5)
4234901	โครงงานวิจัยความมั่นคงปลอดภัยไซเบอร์ Cyber Security Research Project	3(0-6-6)

2.3) วิชาเลือก ไม่น้อยกว่า 12 หน่วยกิต

รหัสวิชา	ชื่อวิชา	หน่วยกิต
4233302	การบริหารจัดการระบบปฏิบัติการ Operating System Management	3(2-2-5)
4233303	การบริการไดเรกทอรีสำหรับระบบปฏิบัติการ Directory Service for Operating Systems	3(2-2-5)
4233304	การป้องกันและมาตรการตอบโต้ Prevention and Countermeasures	3(2-2-5)
4233103	ส่วนต่อประสานโปรแกรมประยุกต์ Application Programming Interface	3(2-2-5)
4233106	การทำงานอัตโนมัติด้วยหุ่นยนต์ Robotic Process Automation	3(2-2-5)
4233402	การวิเคราะห์และการตรวจจับการฉ้อโกง Fraud Analysis and Detection	3(2-2-5)

รหัสวิชา	ชื่อวิชา	หน่วยกิต
4233305	ความมั่นคงปลอดภัยบนมือถือ Mobile Security	3(2-2-5)
4233104	ความมั่นคงปลอดภัยสำหรับอินเทอร์เน็ตของสรรพสิ่ง Internet of Things Security	3(2-2-5)
4233105	การเข้ารหัสและการรักษาความมั่นคงปลอดภัยของข้อมูล Cryptography and Data Security	3(2-2-5)
4233503	เทคโนโลยีบล็อกเชน Blockchain Technology	3(2-2-5)
4233306	หลักการปกปิดข้อมูลและการซ่อนรหัสโปรแกรม Principles of Steganography and Program Obfuscation	3(2-2-5)

2.4) วิชาฝึกประสบการณ์วิชาชีพ 6 หน่วยกิต โดยเลือกเรียนจากกลุ่มต่อไปนี้

2.4.1 กลุ่มสหกิจศึกษา 6 หน่วยกิต

รหัสวิชา	ชื่อวิชา	หน่วยกิต
4234801	สหกิจศึกษาและการศึกษาเชิงบูรณาการกับการทำงาน Cooperative and Work Integrated Education	6(600)

2.4.2 กลุ่มการฝึกประสบการณ์วิชาชีพ 6 หน่วยกิต

รหัสวิชา	ชื่อวิชา	หน่วยกิต
4234802	การฝึกประสบการณ์วิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ Professional Training in Cyber Security	3(450)
4234401	หัวข้อพิเศษทางความมั่นคงปลอดภัยไซเบอร์ Special Topics in Cyber Security	3(2-2-5)

3) หมวดวิชาเลือกเสรี ไม่น้อยกว่า 6 หน่วยกิต

ให้เลือกเรียนรายวิชาอื่น ๆ อีกไม่น้อยกว่า 6 หน่วยกิต ในหลักสูตรระดับปริญญาตรีของมหาวิทยาลัยสวนดุสิต โดยไม่ซ้ำกับรายวิชาที่เคยเรียนมาแล้ว และไม่เป็นรายวิชาที่กำหนดให้เรียนโดยไม่นับหน่วยกิตรวมในเกณฑ์การสำเร็จหลักสูตร

หมวดวิชาเฉพาะ

วิชาแกน 27 หน่วยกิต

4231101 หลักการเขียนโปรแกรมคอมพิวเตอร์ 3(2-2-5)
Principles of Computer Programming

โครงสร้างพื้นฐานของโปรแกรมและขั้นตอนการพัฒนาโปรแกรม คำสั่งในการประมวลผล คำสั่งในการคำนวณ คำสั่งควบคุมโปรแกรม คำสั่งรับข้อมูลและแสดงผล ตัวแปรและชนิดของข้อมูล ตัวดำเนินการและนิพจน์ ฟังก์ชัน การวนซ้ำ การจัดการความผิดปกติของโปรแกรม ส่วนต่อประสานกับผู้ใช้ การใช้ไลบรารีและเฟรมเวิร์ค และการฝึกปฏิบัติการเขียนโปรแกรม

Program fundamentals and program development process; processing commands; calculation commands; program control commands; input and output commands; variables and data types; operators and expressions; functions; loops; exception handling; user interfaces; utilizing libraries and frameworks; and practical programming exercises

4231301 หลักการวิทยาการข้อมูล 3(2-2-5)
Principles of Data Science

แนวคิดของวิทยาการข้อมูล กระบวนการวิเคราะห์ข้อมูลเชิงสำรวจ ประเภทของข้อมูล การแปลงข้อมูล การแบ่งประเภทข้อมูล การจัดเตรียมข้อมูล กระบวนการแก้ปัญหาโดยใช้วิทยาการข้อมูล หลักสถิติเบื้องต้น การวิเคราะห์ข้อมูลตัวแปรเดียว การวิเคราะห์ข้อมูลตั้งแต่ 2 ตัวแปรขึ้นไป เทศนิคและเครื่องมือสำหรับวิทยาการข้อมูลการประยุกต์ใช้เครื่องมือและเทคนิคของวิทยาการข้อมูลเพื่อวิเคราะห์และประเมินความมั่นคงปลอดภัยไซเบอร์

Data science concepts; exploratory data analysis process; types of data; data transformation; data classification; data preparation; problem-solving process using data science; basic statistical principles; univariate data analysis; multivariate data analysis; techniques and tools for data science; application of data science tools and techniques for cybersecurity analysis and assessment

4231401 จริยธรรมและกฎหมายไซเบอร์ 3(3-0-6)
Ethics and Cyber Laws

กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ทรัพย์สินทางปัญญา การจดสิทธิบัตรและลิขสิทธิ์ซอฟต์แวร์ กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ จริยธรรมในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และกรณีศึกษา

Personal data protection law; computer crime law; cybersecurity law; intellectual property; software patent and copyright registration; electronic transactions law; cybersecurity frameworks; ethics in cybersecurity and case studies

4231402 ความมั่นคงปลอดภัยไซเบอร์ 3(2-2-5)

Cyber Security

แนวคิดของของการรักษาความมั่นคงปลอดภัย อาชญากรรมทางไซเบอร์ ภัยคุกคามทางไซเบอร์ นโยบายและมาตรฐานความมั่นคงปลอดภัย การบริหารจัดการความเสี่ยง การรักษาความมั่นคงปลอดภัยเครือข่าย การเข้ารหัสข้อมูล กลไกการพิสูจน์ตัวตน การอนุญาต รูปแบบการควบคุมการเข้าถึง ความมั่นคงปลอดภัยของเว็บ ความมั่นคงปลอดภัยมือถือ การตรวจจับและตอบสนองเหตุการณ์ด้านความมั่นคงปลอดภัย มาตรฐานและข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

Security concepts; cyber crime; cyber threats; security policies and standards; risk management; network security; data encryption; authentication mechanisms; authorization; access control models; web security; mobile security; security incident detection and response; cybersecurity standards and regulations

4231102 การเขียนโปรแกรมเพื่อความมั่นคงปลอดภัย 3(2-2-5)

Secure Programming

แนวคิดและหลักปฏิบัติที่ดีในการเขียนโปรแกรมอย่างมั่นคงปลอดภัย การตรวจสอบรหัสโปรแกรม หลักการเขียนคำสั่งเพื่อป้องกันการโจมตี เอสคิวแอลอินเจ็กชัน ครอสไซต์สคริปติ้ง (เอ็กซ์เอสเอส) ครอสไซต์รีเครสฟอร์เจอรี่ (ซีเอสอาร์เอฟ) การเขียนคำสั่งควบคุมการเข้าถึง การเขียนคำสั่งเข้ารหัส การเขียนคำสั่งรักษาความมั่นคงปลอดภัยของข้อมูล

Concepts and best practices in secure programming; code review; secure coding principles to prevent attacks; SQL injection; Cross-Site Scripting (XSS); Cross-Site Request Forgery (CSRF); access control coding; encryption coding; data security coding

4231103 สถาปัตยกรรมระบบปฏิบัติการ 3(2-2-5)

Operating System Architecture

หลักการทำงานของเครื่องคอมพิวเตอร์ องค์ประกอบและโครงสร้างของระบบคอมพิวเตอร์ สถาปัตยกรรมระบบปฏิบัติการ ส่วนประกอบของฮาร์ดแวร์ หน่วยประมวลผล ระบบบัส การเชื่อมต่ออุปกรณ์ภายนอก การจัดการหน่วยความจำ การจัดการหน่วยความจำเสมือน การจัดการกระบวนการ ภาวะพร้อมกัน หน่วยเก็บบันทึกข้อมูล การจัดการและการกำหนดลำดับกระบวนการ การจัดการรับเข้าและส่งออก การจัดการไฟล์และไดเรกทอรี การแชร์ข้อมูล การจัดการการเข้าถึงระบบ ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ การฝึกปฏิบัติการติดตั้งและจัดการระบบปฏิบัติการ

Computer operating principles; components and structure of computer systems; operating system architecture; hardware components; processing unit; bus system; external device connections; memory management; virtual memory management; process management; concurrency; storage devices; process scheduling and management; input/output management; file and directory management; data sharing; system access management; computer system security; practical installation and management of operating systems.

4231201 ระบบเครือข่ายคอมพิวเตอร์ 3(2-2-5)

Computer Network System

องค์ประกอบของระบบเครือข่าย อุปกรณ์ระบบเครือข่าย ประเภทของระบบเครือข่าย ตัวกลางการเชื่อมต่อเครือข่าย โพรโทคอล มาตรฐานการสื่อสารข้อมูล รูปแบบการเชื่อมต่อเครือข่าย ส่วนประกอบของไคลเอนต์เซิร์ฟเวอร์สถาปัตยกรรมระบบไคลเอ็นต์เซิร์ฟเวอร์ โพรโทคอลไคลเอ็นต์เซิร์ฟเวอร์ หลักการสื่อสารเครือข่ายไคลเอนต์และเซิร์ฟเวอร์ การออกแบบและการติดตั้ง การกำหนดค่าพื้นฐาน การจัดการผู้ใช้ สิทธิการเข้าถึง การสร้างและการจัดการไฟล์และโฟลเดอร์ การส่งข้อมูลระหว่างอุปกรณ์ที่เชื่อมต่อกัน การส่งข้อมูลผ่านเครือข่าย การจัดการแบนด์วิดท์ การฝึกปฏิบัติการติดตั้ง การตรวจสอบและใช้งานระบบเครือข่าย

Network system components; network devices; types of networks; network connection media; protocols; data communication standards; network connection types; components of client-server architecture; client-server architecture; client-server protocols; principles of client and server network communication; design and installation; basic configuration; user management; access rights; file and folder creation and management; data transfer between connected devices; data transmission over networks; bandwidth management; practice in installation; testing and using network systems

4232301 การจัดการฐานข้อมูลอย่างมั่นคงปลอดภัย 3(2-2-5)

Secure Database Management

ทฤษฎีและหลักการเกี่ยวกับฐานข้อมูล ประเภทของโครงสร้างฐานข้อมูล ชนิดของข้อมูล โมเดลความสัมพันธ์ โมเดลข้อมูลแบบ NoSQL ภาษาสำหรับการจัดการข้อมูล การทำความสะอาดข้อมูล การเรียงลำดับข้อมูล การเรียกใช้ข้อมูลจากฐานข้อมูล การรักษาความมั่นคงปลอดภัยของฐานข้อมูล การป้องกันข้อมูลจากการสูญหายและเสียหาย การควบคุมการเข้าถึงข้อมูล การกำหนดสิทธิ์ในการเข้าถึงข้อมูล การสำรองข้อมูล การฝึกปฏิบัติการวิเคราะห์และออกแบบฐานข้อมูล

Theory and principles of databases; type of database structure; data type; relationship model; NoSQL data models; data management language; data cleaning; sorting data; retrieving data from the database; database security; protecting data from loss and damage; data access control; determination of rights to access information; data backup; database analysis and design practice

4232501 สถาปัตยกรรมการประมวลผลแบบคลาวด์ 3(2-2-5)

Cloud Computing Architecture

หลักการของสถาปัตยกรรมการประมวลผลแบบคลาวด์ รูปแบบการให้บริการบนคลาวด์ การให้บริการด้านโครงสร้างพื้นฐาน การให้บริการเกี่ยวกับแพลตฟอร์ม การให้บริการด้านซอฟต์แวร์ ประเภทของคลาวด์ การติดตั้งการประมวลผลแบบคลาวด์ ความมั่นคงปลอดภัยของระบบคลาวด์ การบริหารจัดการความมั่นคงปลอดภัย และความเสี่ยงของคลาวด์

Principles of cloud computing architecture; cloud services model; infrastructure as a service; platform as a service; software as a service; using the cloud both in public cloud; private cloud; hybrid cloud; guidelines for installing cloud computing; cloud security; cloud security and risk management

วิชาเฉพาะด้าน 45 หน่วยกิต

4232502 การพัฒนาเว็บแอปพลิเคชันให้มีความมั่นคงปลอดภัย 3(2-2-5)
Secure Web Application Development

แนวคิดการออกแบบและสร้างเว็บแอปพลิเคชันให้มีความมั่นคงปลอดภัย เทคนิคการสื่อสารข้อมูลระหว่างไคลเอนต์และเซิร์ฟเวอร์ การออกแบบและการเชื่อมต่อกับฐานข้อมูลสำหรับเว็บแอปพลิเคชันอย่างมั่นคงปลอดภัย การประเมินความเสี่ยงและการวิเคราะห์จุดอ่อนของเว็บแอปพลิเคชัน การใช้งานเทคโนโลยีและเครื่องมือต่าง ๆ ในการตรวจจับและป้องกันการโจมตี ขั้นตอนการพัฒนา การปรับปรุง การดำเนินการและการบำรุงรักษาเว็บแอปพลิเคชันอย่างมีประสิทธิภาพ

Designing and building web applications for security and stability; techniques for data communication between clients and servers; designing and securely connecting to databases for web applications; assessing risks and analyzing vulnerabilities of web applications; using various technologies and tools to detect and prevent attacks; and steps in developing; improving; operating; and maintaining web applications efficiently

4232201 โพรโทคอลและบริการเครือข่าย 3(2-2-5)
Protocols and Network Services

ประเภทของโพรโทคอล โครงสร้างและการทำงานของโพรโทคอล บริการที่มีในระบบเครือข่าย การถ่ายโอนข้อมูลผ่านเครือข่าย การทำงานและปฏิสัมพันธ์ของโพรโทคอล การประยุกต์ใช้โพรโทคอลและบริการ โพรโทคอลเครือข่ายไร้สาย การออกแบบ การดำเนินการ และแก้ไขปัญหาระบบเครือข่าย

Types of protocols; the structure and function of protocols; services available in a network; data transfer across networks; the operation and interaction of protocols; the application of protocols and services; wireless network protocols; design; operation; and troubleshooting of network systems

4232202 เครือข่ายไร้สายและความมั่นคงปลอดภัย 3(2-2-5)
Wireless Networking and Security

หลักการและเทคโนโลยีเครือข่ายไร้สาย มาตรฐานเครือข่ายไร้สาย การออกแบบเครือข่ายไร้สาย การติดตั้งเครือข่ายไร้สาย ความมั่นคงปลอดภัยเครือข่ายไร้สาย การเข้ารหัสและการรักษาความลับของข้อมูลผ่านเครือข่ายไร้สาย เครื่องมือและเทคนิคในการป้องกันความมั่นคงปลอดภัยของเครือข่ายไร้สาย เทคโนโลยีในการรักษาความมั่นคงปลอดภัย การตรวจจับการบุกรุกและการโจมตีเครือข่ายไร้สาย และฝึกปฏิบัติการจัดการเครือข่ายไร้สายให้มีความมั่นคงปลอดภัย

Principles and technologies of wireless networks; wireless network standards; wireless network design; wireless network installation; wireless network security; encryption and data confidentiality over wireless networks; tools and techniques for securing wireless networks; technologies for maintaining network security; detection of intrusions and attacks on wireless networks; and training for managing secure wireless networks

4232203 การตรวจจับและการวินิจฉัยการบุกรุก 3(2-2-5)

Intrusion Detection and Diagnosis

หลักการตรวจจับการบุกรุก ประเภทของการบุกรุก เทคนิคที่ใช้ในการตรวจจับการบุกรุก เครื่องมือที่ใช้ในการตรวจจับการบุกรุก การจัดการข้อมูลจราจรทางคอมพิวเตอร์ การวิเคราะห์พฤติกรรมที่น่าสงสัย การตรวจจับการบุกรุกระบบเครือข่ายและระบบคอมพิวเตอร์ การวินิจฉัยการบุกรุกระบบเครือข่าย และฝึกปฏิบัติเพื่อตรวจจับการบุกรุก

Principles of intrusion detection; types of intrusions; techniques used in detecting intrusions; tools used for intrusion detection; management of computer network traffic; analysis of suspicious behaviors; detection of intrusions in network and computer systems; diagnosis of network intrusions; and training for intrusion detection

4232205 เครือข่ายไคลเอนต์และเซิร์ฟเวอร์

Client and Server Networks

แนวคิดระบบไคลเอ็นต์เซิร์ฟเวอร์ ส่วนประกอบของไคลเอนต์เซิร์ฟเวอร์ สถาปัตยกรรมระบบไคลเอ็นต์เซิร์ฟเวอร์ โพรโทคอลไคลเอ็นต์เซิร์ฟเวอร์ หลักการสื่อสารเครือข่ายไคลเอนต์และเซิร์ฟเวอร์ การออกแบบและการติดตั้ง การกำหนดค่าพื้นฐาน การจัดการผู้ใช้ สิทธิการเข้าถึง การสร้างและการจัดการไฟล์และโฟลเดอร์ การทำงานกับโปรแกรมและแอปพลิเคชัน การติดตั้งและการจัดการกับบริการเครือข่าย การดูแลรักษาเครือข่ายไคลเอนต์และเซิร์ฟเวอร์

Client-server system concept; components of a client-server computer; client-server system architecture; client server protocol; principles of client and server network communication; design and installation; basic configuration; user management access rights; creating and managing files and folders; working with programs and applications; installing and managing network services; maintaining networks using client and server systems and case studies

4232503 การตอบสนองต่อเหตุการณ์และการฟื้นฟู 3(2-2-5)

Incident Responses and Disaster Recovery

แนวทางการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อระบบสารสนเทศขององค์กร การตอบสนองต่อเหตุการณ์บุกรุก การบริหารจัดการภัยพิบัติและการวางแผนฟื้นฟู การประยุกต์ใช้เครื่องมือในการรับมือกับสถานการณ์วิกฤตที่อาจเกิดขึ้นในองค์กร

Approaches to managing incidents that may impact an organization's information systems; responding to intrusion incidents; disaster management and recovery planning; and applying tools to handle potential crises in an organization

4232204 การเขียนสคริปต์เพื่อความมั่นคงปลอดภัยไซเบอร์ 3(2-2-5)
Cyber Security Scripting

หลักการสร้างสคริปต์สำหรับการตั้งค่าเครือข่าย การติดตั้ง การกำหนดค่า การจัดการพอร์ตและโพรโทคอล การปรับแต่งเครือข่าย การเรียกใช้บริการเครือข่าย การจัดการไฟล์และไดเรกทอรี การโต้ตอบกับฐานข้อมูล การใช้สคริปต์เพื่อการเข้าถึงข้อมูล การตรวจจับปัญหาและการดำเนินงานระดับเครือข่าย การเขียนโปรแกรมเครือข่ายด้วยซอกเก็ตและเอพีไอ การบริหารจัดการระบบ การสำรวจและจัดการเครือข่ายแบบมีสายและไร้สาย

Principles of creating scripts for network setup; installation; configuration; managing ports and protocols; network customization; invoking network services; file and directory management; interacting with databases; using scripts for data access; detecting issues; and network level operations; programming networks with sockets and APIs; system administration; and surveying and managing both wired and wireless networks

4232302 วิทยาการข้อมูลเพื่อความมั่นคงปลอดภัยไซเบอร์ 3(2-2-5)
Data Science for Cyber Security

ความสำคัญของวิทยาการข้อมูลกับภัยคุกคามไซเบอร์ วิทยาการข้อมูลและเครื่องมือ ปัญญาประดิษฐ์ การใช้เทคนิคการเรียนรู้ของเครื่องเพื่อสร้างแบบจำลองทำนายสำหรับตรวจจับและวิเคราะห์การโจมตีทางไซเบอร์ การสร้างและปรับปรุงกฎระเบียบในการเข้าถึงข้อมูล ความมั่นคงปลอดภัยของข้อมูลและการวิเคราะห์ข้อมูล การวิเคราะห์ข้อมูลเพื่อค้นหาและตรวจจับพฤติกรรมที่ไม่ปกติ การใช้เครื่องมือและเทคนิคด้านวิทยาการข้อมูลเพื่อวิเคราะห์และตรวจสอบระบบไซเบอร์ อนาคตของวิทยาการข้อมูลในโลกความมั่นคงปลอดภัยไซเบอร์

Importance of data science in cyber threats; data science and tools; artificial intelligence; using machine learning techniques to create predictive models for detecting and analyzing cyber attacks; creating and improving regulations for data access; data security and analysis; analyzing data to find and detect abnormal behavior; using data science tools and techniques for analyzing and monitoring cyber systems; and the future of data science in the world of cyber security

4233301 การทดสอบเจาะระบบ 3(2-2-5)
Penetration Testing

เทคนิคการเจาะระบบ กระบวนการทดสอบการเจาะระบบ การสแกนช่องโหว่ การจัดการช่องโหว่ เครื่องมือที่ใช้ในการทดสอบเจาะระบบ การวางแผนและกระบวนการเสริมระบบเพื่อป้องกันการบุกรุก การสร้างระบบที่มีความมั่นคงปลอดภัยด้านเทคนิคและนโยบาย และฝึกปฏิบัติการทดสอบเจาะระบบ

Penetration testing techniques; penetration testing process; vulnerability scanning; vulnerability management; tools used in penetration testing; planning and processes to enhance systems against intrusion; creating systems that are secure both technically and in terms of policy; and conducting penetration testing exercises

4233101 การจัดการศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัย 3(2-2-5)
Security Operation Center

บทบาทหน้าที่และความรู้เกี่ยวกับศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัย การดำเนินงานและการจัดการศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัย โครงสร้างและการดำเนินงานของศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัย เทคโนโลยีและเครื่องมือที่ใช้ในการดำเนินงานในศูนย์ การจัดการและการวิเคราะห์ข้อมูลความมั่นคงปลอดภัย การตรวจจับ การรายงาน และการตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยที่เกิดขึ้นRoles, responsibilities and knowledge regarding security operations centers; operation and management of security operations center; structure and function of security operations centers; technologies and tools used in the operations of the center; management and analysis of security data; and detection; reporting; and response to security Incidents

4233401 การบริหารความเสี่ยงและการรับรองความมั่นคงปลอดภัยไซเบอร์ 3(2-2-5)
Cyber Security Risk Management and Assurance

ความรู้เบื้องต้นเกี่ยวกับการบริหารความเสี่ยง คำศัพท์เฉพาะทางด้านความมั่นคงปลอดภัยไซเบอร์และความเสี่ยง กรอบความมั่นคงปลอดภัยไซเบอร์ เศรษฐศาสตร์ความมั่นคงปลอดภัยไซเบอร์ การประเมินความคุ้มค่าของการลงทุนในมาตรการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ระเบียบวิธีการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูล วิธีการประเมินความเสี่ยง มาตรฐานไอเอสโอ 27001 การประกันภัยทางไซเบอร์ เทคโนโลยีและเครื่องมือการประกันความมั่นคงปลอดภัยไซเบอร์ และแนวโน้มของการประกันความมั่นคงปลอดภัยไซเบอร์

Basic knowledge of risk management; specialized vocabulary in cybersecurity and risk; cybersecurity frameworks; cybersecurity economics; evaluating the cost-effectiveness of investments in information technology security measures; methodologies for managing information security risks; risk assessment methods; ISO 27001 standard; cyber insurance; technologies and tools for ensuring cybersecurity; and trends in cybersecurity insurance

4233102 ปัญญาประดิษฐ์และการเรียนรู้ของเครื่อง 3(2-2-5)
Artificial Intelligence and Machine Learning

หลักการและแนวคิดเกี่ยวกับปัญญาประดิษฐ์และการเรียนรู้ของเครื่อง การสร้างและพัฒนาโมเดล วิธีการของปัญญาประดิษฐ์และการเรียนรู้ของเครื่อง หลักการและเทคนิคในการใช้ข้อมูลเพื่อสร้างและฝึกโมเดล การเรียนรู้จากข้อมูล การทำนาย การจำแนกประเภท การเรียนรู้เชิงลึก เทคนิคเพื่อการตรวจจับและแก้ไขปัญหา และการฝึกเรียนรู้ด้วยปัญญาประดิษฐ์ด้านความมั่นคงปลอดภัยไซเบอร์

Principles and concepts related to artificial intelligence and machine learning; creating and developing models; methods of artificial intelligence and machine learning; principles and techniques for using data to create and train models; learning from data; prediction; classification; deep learning; techniques for detecting and solving problems; and training in artificial intelligence for cyber security

4233501 ความมั่นคงปลอดภัยของระบบคลาวด์ 3(2-2-5)

Cloud System Security

การออกแบบและสถาปัตยกรรมของระบบคลาวด์ที่มีความมั่นคงปลอดภัย การแยกโครงสร้างพื้นฐานทางกายภาพและตรรกะอย่างมั่นคงปลอดภัย การปกป้องข้อมูลสำหรับระบบคลาวด์ การควบคุมการเข้าถึงระบบคลาวด์ การติดตาม ตรวจสอบและจัดการระบบคลาวด์ การจัดการข้อมูลประจำตัวในการประมวลผลแบบคลาวด์ การออกแบบความมั่นคงปลอดภัยในการประมวลผลแบบคลาวด์ นโยบาย กฎระเบียบ และการจัดการความเสี่ยงในการประมวลผลแบบคลาวด์ การประเมินและการรายงานการปฏิบัติตามข้อกำหนดของระบบคลาวด์และผู้ให้บริการคลาวด์

Design and architecture of secure cloud systems; securely separating physical and logical infrastructures; data protection for cloud systems; controlling access to cloud systems; monitoring; auditing; and managing cloud systems; managing identity data in cloud computing; designing security in cloud processing; policies, regulations and risk management in cloud computing; assessing and reporting compliance of cloud systems and providers

4233502 นิติวิทยาศาสตร์ไซเบอร์ 3(2-2-5)

Cyber Forensics

แนวคิดของนิติวิทยาศาสตร์ไซเบอร์ ความสำคัญของนิติวิทยาศาสตร์ไซเบอร์ กระบวนการนิติวิทยาศาสตร์ไซเบอร์ ประเภทของนิติวิทยาศาสตร์ไซเบอร์ ทักษะที่จำเป็นสำหรับผู้เชี่ยวชาญด้านนิติวิทยาศาสตร์ไซเบอร์ เครื่องมือนิติวิทยาศาสตร์ไซเบอร์ ความท้าทายสำหรับนิติวิทยาศาสตร์ไซเบอร์

Concept of cyber forensics; importance of cyber forensics; cyber forensics process; types of cyber forensics; skills required for cyber forensic specialists; cyber forensic tools; challenges for cyber forensics

4234901 โครงงานวิจัยความมั่นคงปลอดภัยไซเบอร์ 3(0-6-6)

Cyber Security Research Project

การประยุกต์ใช้ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ระเบียบวิธีวิจัย การออกแบบโครงงาน การพัฒนาโครงงานที่เกี่ยวข้องกับงานด้านความมั่นคงปลอดภัยไซเบอร์ การจัดทำรูปเล่มโครงงาน และการนำเสนอโครงงาน

Application of cyber security knowledge; research methodologies; project design; development of projects related to cyber security work; project documentation and presentation of project

วิชาเลือก ไม่น้อยกว่า 12 หน่วยกิต

4233302 การบริหารจัดการระบบปฏิบัติการ 3(2-2-5)

Operating System Management

แนวคิดของการบริหารจัดการระบบปฏิบัติการ การติดตั้งระบบปฏิบัติการ การกำหนดค่าระบบ การจัดการสิทธิ์ของผู้ใช้และการควบคุมการเข้าถึง การบริหารจัดการกระบวนการ การจัดการหน่วยความจำและไฟล์ระบบ การติดตั้งและบริหารจัดการบริการ การสำรองข้อมูลและการกู้คืนข้อมูล การเพิ่มประสิทธิภาพและความมั่นคงปลอดภัย การตรวจสอบและแก้ไขปัญหา และการใช้งานเครื่องมือสคริปต์เพื่อการบริหารจัดการระบบ

Concepts of operating system management; installing operating systems; configuring systems; managing user rights and access control; process management; managing system memory and files; installing and managing services; data backup and recovery; optimizing performance and security; monitoring and troubleshooting; and using scripting tools for system management

4233303 การบริการไดเรกทอรีสำหรับระบบปฏิบัติการ 3(2-2-5)

Directory Service for Operating Systems

หลักการทำงานของระบบไดเรกทอรี การออกแบบ การสร้าง และการดูแลรักษาไดเรกทอรี เทคนิคในการกำหนดโครงสร้างของโดเมน โครงสร้างของระบบไดเรกทอรี การสร้างและการจัดการกับองค์ประกอบของไดเรกทอรี การสร้างและการจัดการกับอ็อบเจกต์ที่เกี่ยวข้อง การใช้เครื่องมือจัดการไดเรกทอรี เทคนิคในการจัดการไดเรกทอรี การจัดการระบบไดเรกทอรีในระบบปฏิบัติการ การตั้งค่าระบบและการควบคุมสิทธิ์การเข้าถึงข้อมูล และการใช้งานในระบบปฏิบัติการ

Principles of directory system operation; designing, creating, and maintaining directories; techniques for structuring domains; directory system structures; creating and managing directory components; creating and managing related objects; using directory management tools; directory management techniques; managing directory systems in operating systems; configuring systems and controlling data access rights; and usage in operating systems

4233304 การป้องกันและมาตรการตอบโต้ 3(2-2-5)

Prevention and Countermeasures

หลักการและเครื่องมือที่ใช้ในการป้องกันการโจมตี การวางระบบตอบโต้เพื่อเสริมความมั่นคงปลอดภัย วิธีการวิเคราะห์การโจมตีทางเครือข่าย การสแกนและการรับรู้การบุกรุก การใช้เครื่องมือและเทคนิคในการตอบโต้ต่อการบุกรุก การป้องกันโดยใช้ระบบไฟร์วอลล์ การใช้ระบบตรวจจับการบุกรุก การป้องกันการโจมตีทางเว็บ และการป้องกันและตอบโต้การโจมตีในระบบสารสนเทศ

Principles and tools used in attack prevention; implementing response systems to enhance security; methods for analyzing network attacks; scanning and intrusion detection; using tools and techniques to respond to intrusions; protection using firewall systems; employing intrusion detection systems; preventing web-based attacks; and defending and responding to attacks in information systems

4233103 ส่วนต่อประสานโปรแกรมประยุกต์ 3(2-2-5)

Application Programming Interface

ความสำคัญและหลักการออกแบบส่วนต่อประสานโปรแกรม เทคโนโลยีส่วนต่อประสานโปรแกรม การสร้างและการใช้งานส่วนต่อประสานโปรแกรม การสื่อสารระหว่างโปรแกรมประยุกต์และส่วนต่อประสานโปรแกรม และฝึกปฏิบัติการพัฒนาส่วนต่อประสานโปรแกรมสำหรับโปรแกรมประยุกต์

Importance and principles of designing program interfaces; program interface technologies; creating and using program interfaces; communication between applications and program interfaces; and practical training in developing program interfaces for applications

4233106 การทำงานอัตโนมัติด้วยหุ่นยนต์ 3(2-2-5)

Robotic Process Automation

แนวคิดพื้นฐาน และหลักการทำงานอัตโนมัติด้วยหุ่นยนต์ การใช้เครื่องมือและแพลตฟอร์มในการพัฒนาการทำงานอัตโนมัติด้วยหุ่นยนต์ การวิเคราะห์กระบวนการทางธุรกิจเพื่อระบุโอกาสในการทำงานอัตโนมัติด้วยหุ่นยนต์ การออกแบบและพัฒนาโปรแกรมอัตโนมัติ (บอท) การบูรณาการการทำงานอัตโนมัติด้วยหุ่นยนต์กับระบบที่มีอยู่เดิมในองค์กร การบริหารจัดการและกำกับดูแลโครงการการทำงานอัตโนมัติด้วยหุ่นยนต์ กรณีศึกษาการทำงานอัตโนมัติด้วยหุ่นยนต์ในอุตสาหกรรม

Basic concepts and principles of robotic process automation; use of tools and platforms for robotic process automation development; analysis of business processes to identify opportunities for robotic process automation; design and development of automated programs (bots); integration of robotic process automation with existing systems in organizations; management and governance of robotic process automation projects; case studies of robotic process automation applications in industry

4233402 การวิเคราะห์และการตรวจจับการฉ้อโกง 3(2-2-5)

Fraud Analysis and Detection

วิธีการวิเคราะห์และตรวจจับการฉ้อโกง เครื่องมือและเทคนิคในการตรวจจับการฉ้อโกง รูปแบบของการฉ้อโกง การวิเคราะห์และตรวจจับการฉ้อโกง กฎหมายและนโยบายที่เกี่ยวข้องกับการป้องกันและการจัดการฉ้อโกง การเตรียมพร้อมในการป้องกันและจัดการภัยคุกคามกับการฉ้อโกงในองค์กร

Methods for analyzing and detecting fraud; tools and techniques for fraud detection; forms of fraud; analysis and detection of fraud; laws and policies related to fraud prevention and management; preparedness for preventing and managing the threat of fraud in organizations

4233305 ความมั่นคงปลอดภัยบนมือถือ 3(2-2-5)

Mobile Security

หลักการและเทคโนโลยีเกี่ยวกับการป้องกันความมั่นคงปลอดภัยของโทรศัพท์มือถือ กลไกและเทคโนโลยีที่ใช้ในการควบคุมการเข้าถึงข้อมูล การจัดการสิทธิ์และการควบคุมความมั่นคงปลอดภัยของโทรศัพท์มือถือ การใช้งานและการกำหนดค่าการเข้าถึง การควบคุมและการตรวจสอบการเข้าถึงข้อมูล การตรวจหาช่องโหว่ เทคนิคการโจมตี การปกป้องความมั่นคงปลอดภัยของโทรศัพท์มือถือ

Principles and technologies related to mobile security protection; mechanisms and technologies used in data access control; management of rights and security control of mobile phones; usage and access configuration; control and auditing access; vulnerability detection; attack techniques; and protection of mobile phone security

4233104 ความมั่นคงปลอดภัยของอินเทอร์เน็ตของสรรพสิ่ง 3(2-2-5)

Internet of Things Security

หลักการความมั่นคงปลอดภัยของอินเทอร์เน็ตของสรรพสิ่ง ข้อกำหนดด้านความมั่นคงปลอดภัยของอินเทอร์เน็ตของสรรพสิ่ง โพรโทคอลการสื่อสารของอินเทอร์เน็ตของสรรพสิ่ง ช่องโหว่ของอินเทอร์เน็ตของสรรพสิ่ง การรักษาความมั่นคงปลอดภัยอินเทอร์เน็ตของสรรพสิ่ง องค์ประกอบสำคัญของการรักษาความมั่นคงปลอดภัยของอินเทอร์เน็ตของสรรพสิ่ง การพัฒนาอุปกรณ์อินเทอร์เน็ตของสรรพสิ่ง การออกแบบแอปพลิเคชันอินเทอร์เน็ตของสรรพสิ่ง และการเตรียมพร้อมในการป้องกันและจัดการกับภัยคุกคามอุปกรณ์อินเทอร์เน็ตของสรรพสิ่ง

Principles of Internet of Things security; security requirements for the Internet of Things; communication protocols of the Internet of Things; vulnerabilities of the Internet of Things; maintaining the security of the Internet of Things; key components of Internet of Things security; development of Internet of Things devices; designing Internet of Things applications; and preparedness for preventing and managing threats to Internet of Things devices

4233105 การเข้ารหัสและการรักษาความมั่นคงปลอดภัยของข้อมูล 3(2-2-5)

Cryptography and Data Security

หลักการและเทคนิคการเข้ารหัสข้อมูล การเข้ารหัสแบบสมมาตรและแบบอสมมาตร การใช้การเข้ารหัสเพื่อรักษาความลับ ความถูกต้องและความน่าเชื่อถือของข้อมูล การบริหารจัดการกุญแจเข้ารหัส การประเมินความแข็งแรงของระบบการเข้ารหัส กฎระเบียบและมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของข้อมูล และการประยุกต์ใช้หลักการเข้ารหัสด้านความมั่นคงปลอดภัยไซเบอร์

Principles and techniques of data encryption; symmetric and asymmetric encryption; utilizing encryption for preserving confidentiality; integrity and reliability of information; cryptographic key management; evaluating the strength of encryption systems; regulations and standards related to data security; and applying encryption principles in the context of cyber security

4233503 เทคโนโลยีบล็อกเชน 3(2-2-5)

Blockchain Technology

หลักการและการใช้งานของเทคโนโลยีบล็อกเชน โครงสร้างและการทำงานของบล็อก การสร้างบล็อกใหม่ การยืนยันและการเชื่อมต่อบล็อกในเครือข่าย การประยุกต์ใช้เทคโนโลยีบล็อกเชนในธุรกิจและอุตสาหกรรม และการจัดการข้อมูล

Principles and operation of blockchain technology; structure and function of blocks; creation of new blocks; verification and connection of blocks in the network; application of blockchain technology in business and industry; and data management

4233306 หลักการปกปิดข้อมูลและการซ่อนรหัสโปรแกรม 3(2-2-5)

Principles of Steganography and Program Obfuscation

เทคนิคและหลักการในการปกปิดข้อมูล การใช้เทคโนโลยีเชิงลึกซ่อนรหัสโปรแกรม เทคนิคในการสร้างภาพเพื่อปกปิดข้อมูลและซ่อนรหัสโปรแกรม การเขียนโปรแกรมเพื่อให้รหัสของโปรแกรมยากต่อการวิเคราะห์และทำความเข้าใจ และการเตรียมการป้องกันข้อมูลและรหัสโปรแกรม

Techniques and principles in data obfuscation; using deep technology to hide program code; techniques in creating images to conceal data and obscure program code; programming to make the code difficult to analyze and understand; and preparing to protect data and program code

วิชาฝึกประสบการณ์วิชาชีพ 6 หน่วยกิต

4234801 สหกิจศึกษาและการศึกษาเชิงบูรณาการกับการทำงาน 6(600)

Cooperative and Work Integrated Education

วิชาบังคับก่อน : ตามเงื่อนไขของสาขาวิชา และผ่านการอบรมเตรียมความพร้อมก่อนไปปฏิบัติงานสหกิจศึกษาและการศึกษาเชิงบูรณาการกับการทำงาน ไม่น้อยกว่า 30 ชั่วโมง

การปฏิบัติงานจริงเสมือนหนึ่งเป็นพนักงานในสถานประกอบการที่มีการดำเนินงานเกี่ยวข้องกับสาขาวิชาที่ศึกษาอยู่เป็นระยะเวลาไม่น้อยกว่า 600 ชั่วโมง ต่อเนื่อง นักศึกษาจะต้องผ่านการอบรมเตรียมความพร้อมก่อนไปปฏิบัติงาน ต้องจัดทำรายงานผลการปฏิบัติงาน นำเสนอผลงานในการสัมมนาระหว่างนักศึกษา อาจารย์ที่ปรึกษา หรืออาจารย์นิเทศก์ หลังจากเสร็จสิ้นการปฏิบัติงานแล้ว การฝึกงานภาคสนามของนักศึกษาสาขาวิชาความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย การฝึกปฏิบัติงานในหน่วยงานของรัฐบาล รัฐวิสาหกิจ หรือธุรกิจเอกชน เพื่อเพิ่มประสบการณ์การปฏิบัติงานในสาขาวิชาความมั่นคงปลอดภัยไซเบอร์ ตลอดจนจัดทำรายงานผลการปฏิบัติงานพร้อมนำเสนอผลการปฏิบัติงาน

Practical training in a cyber security -related workplace for at least 600 hours consecutively; student is regarded to pass pre-training preparation, write performance, and present work results in a seminar between students and advisors after finishing training; practical training covers works in a government department, public enterprise or private company to enhance work experiences in cyber security, prepare for performance report and presentation

4234802 ประสบการณ์วิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ 3(450)

Professional Training in Cyber Security

วิชาบังคับก่อน : ตามเงื่อนไขของสาขาวิชาและผ่านการอบรมเตรียมความพร้อมก่อนไปฝึกประสบการณ์วิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ ไม่น้อยกว่า 30 ชั่วโมง

การฝึกงานภาคสนามของนักศึกษาสาขาวิชาความมั่นคงปลอดภัยไซเบอร์ ในหน่วยงานของรัฐบาล รัฐวิสาหกิจ หรือธุรกิจเอกชน เป็นระยะเวลาไม่น้อยกว่า 450 ชั่วโมง ต่อเนื่อง เพื่อเพิ่มประสบการณ์การปฏิบัติงานในสาขาวิชาความมั่นคงปลอดภัยไซเบอร์ โดยมีการจัดทำรายงานการฝึกปฏิบัติงานและนำเสนอ และมีการประเมินผลจากหน่วยงานที่ให้การฝึกแก่นักศึกษา

Fieldwork training of a cyber security student covers work in a government department; public enterprise; or private company for at least 450 hours consecutively; to enhance work experiences in cyber security by preparing a cyber security training report and presentation and evaluation from the agency that provides training to students

4234401 หัวข้อพิเศษทางความมั่นคงปลอดภัยไซเบอร์ 3(2-2-5)

Special Topics in Cyber Security

หัวข้อที่เกิดขึ้นใหม่ด้านความมั่นคงปลอดภัยไซเบอร์ แนวโน้มของความมั่นคงปลอดภัยไซเบอร์ และวิธีการใหม่ด้านความมั่นคงปลอดภัยไซเบอร์

Emerging topics in cyber security; cyber security trends; and new methods in cyber security

หมวดวิชาเลือกเสรี ไม่น้อยกว่า 6 หน่วยกิต

ให้เลือกเรียนรายวิชาอื่น ๆ อีกไม่น้อยกว่า 6 หน่วยกิต ในหลักสูตรระดับปริญญาตรีของมหาวิทยาลัยสวนดุสิต โดยไม่ซ้ำกับรายวิชาที่เคยเรียนมาแล้ว และไม่เป็นรายวิชาที่กำหนดให้เรียนโดยไม่นับหน่วยกิตรวม ในเกณฑ์การสำเร็จหลักสูตร

แผนการศึกษาหลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาความมั่นคงปลอดภัยไซเบอร์

ปีที่ 1 / ภาคการศึกษาที่ 1	
หมวดวิชาศึกษาทั่วไป	
xxxxxxx	วิชาศึกษาทั่วไป 1
xxxxxxx	วิชาศึกษาทั่วไป 2
xxxxxxx	วิชาศึกษาทั่วไป 3
หมวดวิชาเฉพาะ : วิชาแกน	
4231101	หลักการเขียนโปรแกรมคอมพิวเตอร์
4231301	หลักการวิทยาการข้อมูล
4231401	จริยธรรมและกฎหมายไซเบอร์

ปีที่ 1 / ภาคการศึกษาที่ 2	
หมวดวิชาศึกษาทั่วไป	
xxxxxxx	วิชาศึกษาทั่วไป 4
xxxxxxx	วิชาศึกษาทั่วไป 5
หมวดวิชาเฉพาะ : วิชาแกน	
4231402	ความมั่นคงปลอดภัยไซเบอร์
4231102	การเขียนโปรแกรมเพื่อความมั่นคงปลอดภัย
4231103	สถาปัตยกรรมระบบปฏิบัติการ
4231201	ระบบเครือข่ายคอมพิวเตอร์

ปีที่ 2 / ภาคการศึกษาที่ 1	
หมวดวิชาศึกษาทั่วไป	
xxxxxxx	วิชาศึกษาทั่วไป 6
หมวดวิชาเฉพาะ : วิชาแกน	
4232301	การจัดการฐานข้อมูลอย่างมั่นคงปลอดภัย
4232501	สถาปัตยกรรมการประมวลผลแบบคลาวด์
หมวดวิชาเฉพาะ : วิชาเฉพาะด้าน	
4232502	การพัฒนาเว็บแอปพลิเคชันให้มีความมั่นคงปลอดภัย
4232201	โพรโทคอลและบริการเครือข่าย
4232202	เครือข่ายไร้สายและความมั่นคงปลอดภัย

ปีที่ 2 / ภาคการศึกษาที่ 2	
หมวดวิชาศึกษาทั่วไป	
xxxxxxx	วิชาศึกษาทั่วไป 7
หมวดวิชาเฉพาะ : วิชาเฉพาะด้าน	
4232203	การตรวจจับและการวินิจฉัยการบุกรุก
4232205	เครือข่ายไคลเอนต์และเซิร์ฟเวอร์
4232503	การตอบสนองต่อเหตุการณ์และการฟื้นฟู
4232204	การเขียนสคริปต์เพื่อความมั่นคงปลอดภัยไซเบอร์
4232302	วิทยาการข้อมูลเพื่อความมั่นคงปลอดภัยไซเบอร์

ปีที่ 3 / ภาคการศึกษาที่ 1	
หมวดวิชาศึกษาทั่วไป	
xxxxxxx	วิชาศึกษาทั่วไป 8
หมวดวิชาเฉพาะ : วิชาเฉพาะด้าน	
4233301	การทดสอบเจาะระบบ
4233101	การจัดการศูนย์ปฏิบัติการ ด้านความมั่นคงปลอดภัย
4233401	การบริหารความเสี่ยงและการรับรองความมั่นคงปลอดภัยไซเบอร์
4233102	ปัญญาประดิษฐ์และการเรียนรู้ของเครื่อง
หมวดวิชาเฉพาะ : วิชาเลือก	
xxxxxxx	วิชาเลือก

ปีที่ 3 / ภาคการศึกษาที่ 2	
หมวดวิชาเฉพาะ : วิชาเฉพาะด้าน	
4233501	ความมั่นคงปลอดภัยของระบบคลาวด์
4233502	นิติวิทยาศาสตร์ไซเบอร์
หมวดวิชาเฉพาะ : วิชาเลือก	
xxxxxxx	วิชาเลือก
xxxxxxx	วิชาเลือก
xxxxxxx	วิชาเลือก

ปีที่ 4 / ภาคการศึกษาที่ 1	
หมวดวิชาเฉพาะ : วิชาเฉพาะด้าน	
4234901	โครงงานวิจัยความมั่นคงปลอดภัยไซเบอร์
หมวดวิชาเฉพาะ : วิชาเลือก	
*4234401	หัวข้อพิเศษทางความมั่นคงปลอดภัยไซเบอร์ Special Topics in Cyber Security
หมวดวิชาเลือกเสรี	
xxxxxxx	เลือกเสรี 1
xxxxxxx	เลือกเสรี 2

* สำหรับนักศึกษาที่เลือกลงทะเบียนรายวิชาการฝึกประสบการณ์วิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์

ในกรณีเลือกเรียนสหกิจศึกษาให้เลือกเรียนในกลุ่มสหกิจศึกษา 6 หน่วยกิต ดังนี้

ปีที่ 4 / ภาคการศึกษาที่ 2	
หมวดวิชาเฉพาะ : วิชาฝึกประสบการณ์วิชาชีพ	
4234801	สหกิจศึกษาและการศึกษาเชิงบูรณาการกับการทำงาน

หมายเหตุ: ฝึกปฏิบัติงานเต็มเวลาในหน่วยงานที่เกี่ยวข้องกับด้านความมั่นคงปลอดภัยไซเบอร์ เป็นเวลาต่อเนื่อง โดยไม่ลงทะเบียนเรียนรายวิชาอื่นในช่วงปฏิบัติสหกิจศึกษา ตามข้อกำหนดของมาตรฐานสหกิจศึกษา รวมระยะเวลาฝึกปฏิบัติงานไม่น้อยกว่า 600 ชั่วโมง และระยะเวลาปฏิบัติงานเป็นไปตามข้อกำหนดของหน่วยงาน ทั้งนี้นักศึกษาต้องจัดทำรายงานผลการปฏิบัติงานพร้อมนำเสนอผลการปฏิบัติงาน

ในกรณีไม่เลือกเรียนสหกิจศึกษา ให้เลือกเรียนในกลุ่มฝึกประสบการณ์วิชาชีพ 3 หน่วยกิต ดังนี้

ปีที่ 4 / ภาคการศึกษาที่ 2	
หมวดวิชาเฉพาะ : วิชาฝึกประสบการณ์วิชาชีพ	
4234802	การฝึกประสบการณ์วิชาชีพ ด้านความมั่นคงปลอดภัยไซเบอร์

หมายเหตุ: ฝึกปฏิบัติงานในหน่วยงานที่เกี่ยวข้องกับด้านความมั่นคงปลอดภัยไซเบอร์ เป็นเวลาต่อเนื่อง รวมระยะเวลาฝึกปฏิบัติงานไม่น้อยกว่า 450 ชั่วโมง โดยระยะเวลาปฏิบัติงานเป็นไปตามข้อกำหนดของหน่วยงาน ทั้งนี้นักศึกษาต้องจัดทำรายงานผลการปฏิบัติงานพร้อมนำเสนอผลการปฏิบัติงาน