Title (Units): **COMP7850 Information Security Management (3,2,1)**

Course Aims: To learn: (1) the principles and practices of information security management at different levels: bit level, message level, protocol level, system and network level, and managerial level, and (2) the current topics, including blockchain.

Prerequisite: Nil

Course Intended Learning Outcomes (CILOs):
Upon successful completion of this course, students should be able to:

No.	Course Intended Learning Outcomes (CILOs)
	Knowledge
1	Describe the information security management problems at bit level, message level, protocol level, system and network level, and managerial level .
2	Describe the solutions to the information management security problems at different levels.
	Professional Skill
3	Analyze and identify potential security problems and provide solutions to these problems.

Calendar Description: Students will learn the principles and practices of information security management at different levels: bit level, message level, protocol level, system and network level, and managerial level. They will also learn the current topics, including blockchain.

Teaching and Learning Activities (TLAs):

CILOs	Type of TLA
1-2	Students will attend lectures and tutorials to learn the principles of information security management. They will learn how the security problems at different levels are solved in practice.
3	Students will be given hands-on works by which they could discover information security problems and provide solutions in real-world settings.

Assessment:

No.	Assessment Methods	Weighting	CILOs to be addressed	Description of Assessment Tasks
1	Continuous Assessment	30%	1-3	Written assignments and a written quiz are designed to measure how well the students have learned the basic concepts of information security management, and their understanding of different types of information security mechanisms.
2	Hands-on Assessments	20%	3	Hands-on assessments are designed to measure how well the student could discover information security problems and provide solutions in real-world settings.
3	Examination	50%	1-3	Final examination questions are designed to evaluate students' understanding of the principles and practices of information security management, and how far students have achieved the intended learning outcomes.

Assessment Rubrics:

Excellent (A)	• Achieve the three CILOs, demonstrating a good mastery of both the conceptual and practical aspects of information security • Have a solid understanding of computer security fundamental concepts, and be able to explain and highlight the key points of these concepts

	• Able to produce high quality security analysis reports on information systems and information security management policies or procedures • Able to highlight security vulnerabilities in information systems with detailed explanations, and be able to make reasonable suggestions and recommendations • Able to identify key assets in information systems and the security needs of different situations and computing environments, and be able to recommend appropriate information security policies and computer security mechanisms to protect those assets
Good (B)	• Achieve the three CILOs, demonstrating a good understanding of both the conceptual and practical aspects of information security • Have a good understanding of computer security fundamental concepts • Able to produce security analysis reports on information systems and information security management policies or procedures • Able to identify most security vulnerabilities in information systems with detailed explanations, and be able to make suggestions and recommendations • Able to identify key assets in most information systems and the security needs of familiar situations and computing environments, and be able to recommend appropriate information security policies and computer security mechanisms to protect those assets
Satisfactory (C)	• Achieve most of the three CILOs, with a minimal level of understanding of the conceptual and practical aspects of information security • Have a minimal level of understanding of computer security fundamental concepts • Able to conduct basic security analysis on information systems and information security management policies or procedures under a limited number of typical situations • Demonstrate an acceptable level of ability of identifying familiar security vulnerabilities in information systems • Demonstrate an acceptable level of ability of identifying most key assets in familiar information systems and the security needs of familiar situations and computing environments
Fail (F)	• Achieve less than three of the three CILOs, and have little understanding of the conceptual and practical aspects of information security • Unable to provide solutions to simple problems which require basic understanding of computer security fundamental concepts • Unable to conduct basic security analysis on information systems, information security management policies or procedures • Unable to identify security vulnerabilities in information systems • Unable to identify key assets in familiar information systems or the security needs of computing environments

Course Content and CILOs Mapping:

Content		CILO No.
I	Cryptography	1, 2, 3
II	Security Protocols	1, 2, 3
III	System and Network Security	1, 2, 3
IV	Security Management	1, 2, 3
V	Blockchain	1, 2, 3

References:

- Michael E. Whitman and Herbert J. Mattord. Management of Information Security, 6th Edition, Cengage Learning, 2018.
- Michael E. Whitman and Herbert J. Mattord. Principles of Information Security, 7th Edition, Cengage Learning, 2022.
- William Stallings, Computer Security: Principles and Practice, 5th Edition, Pearson, 2023.
- Andrew Hoffman, Web Application Security, O′ Reilly Media, 2020.

- Daniel Cawrey and Loren Lantz, Mastering Blockchain, O′ Reilly Media, Inc, 2020.
- F. Tschorsch and B. Scheuermann, ″Bitcoin and beyond: a technical survey on decentralized digital currencies,″ IEEE Communications Surveys and Tutorials, vol. 18, no. 3, pp. 2084-2123, 3rd Quarter, 2016.

Course Content:

<u>Topic</u>

I. Cryptography
- A. Symmetric cryptography and public key cryptography
- B. Hash functions, digital signatures, message authentication

II. Security Protocols
- A. Internet Protocol Security (IPsec)
- B. Transport Layer Security (TLS) and HyperText Transfer Protocol Secure (HTTPS)
- C. Authentication Protocols: digital certificate, mutual authentication protocol, two-factor authentication

III. System and Network Security
- A. Intruders, viruses, worms, phishing, malware, denial-of-service, distributed denial-of-service
- B. Access control list, virtual private networks, firewalls, intrusion detection systems
- C. Web security
- D. Wi-Fi security

IV. Security Management
- A. Policies, procedures, guidelines
- B. Access control, operations security, physical security
- C. Risk management, disaster recovery and business continuity
- D. IT security audit
- E. Software development security
- F. Laws, ethics, and privacy

V. Blockchain
- A. Blockchain: principles, features, applications
- B. Cryptocurrency: principles, transactions, mining
- C. Consensus protocols
- D. Smart contracts and Non-Fungible Tokens (NFT)