Title (Units): **COMP7170 Data Security and Privacy (3,2,1)**

Course Aims: To provide students with a solid understanding of data security and privacy concepts and their use cases. To explain basic data encryption, integrity protection, privacy protection techniques and advanced data security and privacy techniques. To discuss data security and privacy practice issues.Upon completion, students will be able to tackle cybercrime and foster innovation in the areas of data security and privacy.

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 data security and privacy concepts
2	Explain basic data encryption, integrity protection, and privacy protection techniques
3	Explain advanced data security and privacy techniques such as access control and cloud data security
4	Describe data security and privacy policies and regulations
	Professional Skill
5	Identify security threats and suitable data protection techniques for different use cases
6	Apply cryptographic tools for data security and privacy protection

Calendar Description: This course provides an in-depth understanding of data security and privacy protection techniques from both theoretical and practical aspects. Students will learn basic data encryption, integrity protection, and privacy protection techniques. Students will also learn advanced data security and privacy techniques such as access control and cloud data security. In addition, data security and privacy policies and regulations will be introduced. This course offers opportunities to explore cryptographic tools for data security and privacy protection and apply them to different use cases.

Teaching and Learning Activities (TLAs):

CILOs	Type of TLA
1-4	Students will acquire the knowledge on data security and privacy concepts and techniques through lectures and continuous assessment activities.
5-6	Students will acquire hands-on experience in applying security and privacy tools in different use cases via laboratories.

Assessment:

No.	Assessment Methods	Weighting	CILOs to be addressed	Description of Assessment Tasks
1	Continuous Assessment	40%	1-6	Machine problems and assignment(s) are designed to evaluate students' mastery of data security and privacy concepts and techniques.
2	Examination	60%	1-6	Final examination questions are designed to assess how well students understand and utilize the knowledge acquired.

Assessment Rubrics:

	Excellent (A)	Good (B)	Satisfactory (C)	Fail (F)
Describe data security and privacy concepts	Thorough description of almost all concepts	Description of most of the concepts	Description of some of the concepts	Description of a limited number of concepts
Explain basic data encryption, integrity protection, and privacy protection techniques	Thorough explanation of almost all techniques	Explanation of most of the techniques	Explanation of some of the techniques	Explanation of a limited number of techniques
Explain advanced data security and privacy techniques such as access control and cloud data security	Thorough explanation of almost all techniques	Explanation of most of the techniques	Explanation of some of the techniques	Explanation of a limited number of techniques
Describe data security and privacy policies and regulations	Thorough description of almost all policies and regulations	Description of most of the policies and regulations	Description of some of the policies and regulations	Description of a limited number of policies and regulations
Identify security threats and suitable data protection techniques for different use cases	Identifying almost all threats and suitable techniques	Identifying most of the threats and suitable techniques	Identifying some of the threats and suitable techniques	Identifying a very limited number of threats and suitable techniques
Apply cryptographic tools for data security and privacy protection	Application of almost all relevant tools	Application of most of the tools	Application of some of the tools	Application of only a very small number of tools

Course Content and CILOs Mapping:

Content		**CILO No.**
I	Overview of Data Security and Privacy	1,5
II	Data Encryption Techniques	2, 5, 6
III	Integrity Protection Techniques	2, 5, 6
IV	Privacy Protection Techniques	2, 5, 6
V	Advanced Topics in Data Security and Privacy	3, 5, 6
VI	Data Security and Privacy Practice	4

References:

- William Stallings and Lawrie Brown. Computer Security: Principles and Practice, 5th Edition, Pearson, 2024.
- Torra, Vicenç. Guide to Data Privacy: Models, Technologies, Solutions / by Vicenç Torra. Springer International Publishing, 2022.
- Stallings, William. Information Privacy Engineering and Privacy by Design: Understanding Privacy Threats, Technology, and Regulations Based on Standards and Best Practices. 1st Edition. Addison-Wesley Professional, 2019.
- Qiang Yang, Yang Liu, Tianjian Chen, and Yongxin Tong, Federated Machine Learning: Concept and Applications, ACM Transactions on Intelligent Systems and Technology (TIST), Volume 10, Issue 2, No. 12, January 2019.

- Dawn Xiaoding Song, D. Wagner and A. Perrig, "Practical techniques for searches on encrypted data," Proceeding 2000 IEEE Symposium on Security and Privacy. S&P 2000, Berkeley, CA, USA, 2000, pp. 44-55.

Course Content:

Topic

I. Overview of Data Security and Privacy
   A. Data Security Concepts
   B. Data Privacy Concepts
   C. Adversary Models

II. Data Encryption Techniques
   A. Symmetric Encryption
   B. Asymmetric Encryption
   C. Key Distribution and Management

III. Integrity Protection Techniques
   A. Cryptographic Hash Functions and Message Authentication Codes
   B. Authentication
   C. Digital Signatures

IV. Privacy Protection Techniques
   A. Privacy Attacks and Disclosure Risks
   B. K-anonymity Model
   C. Privacy Models beyond K-anonymity
   D. Differential Privacy

V. Advanced Topics in Data Security and Privacy
   A. Federated Machine Learning
   B. Searchable Encryption
   C. Privacy-Preserving Data Mining

VI. Data Security and Privacy Practice
   A. Cryptographic Tools for Data Security and Privacy Protection
   B. Policies and Regulations