CS5294: INFORMATION SECURITY TECHNOLOGY MANAGEMENT

Effective Term
Semester A 2026/27

Part I Course Overview

Course Title
Information Security Technology Management

Subject Code
CS - Computer Science
Course Number
5294

Academic Unit
Computer Science (CS)

College/School
College of Computing (CC)

Course Duration
One Semester

Credit Units
3

Level
P5, P6 - Postgraduate Degree

Medium of Instruction
English

Medium of Assessment
English

Prerequisites
Nil

Precursors
Nil

Equivalent Courses
Nil

Exclusive Courses
Nil

Part II Course Details

Abstract

The course provides an overview of the concepts and elements in information security technology management. It is important that information security requirements be understood at the organizational level; appropriate information security policy be derived; cost-effective information security solution be planned and deployed; and evidence to auditors be provided on how well an organization has performed when required.

Course Intended Learning Outcomes (CILOs)

	CILOs	Weighting (if app.)	DEC-A1	DEC-A2	DEC-A3
1	Describe major information security technologies; understand their limitations and applications as countermeasures to IT threats.			x	
2	Describe threats and vulnerabilities in an IT environment; and recognize the relationship of threat, vulnerability, and countermeasure; and its impact on organizational information security.			x	
3	Describe the information security management framework; formulate a basic information security policy for an organization and design appropriate guidelines in implementing the policy with reference to appropriate Information Security Management Standards.		x	x	
4	Recognize and critique legal issues in information security.		x		

A1: Attitude
Develop an attitude of discovery/innovation/creativity, as demonstrated by students possessing a strong sense of curiosity, asking questions actively, challenging assumptions or engaging in inquiry together with teachers.

A2: Ability
Develop the ability/skill needed to discover/innovate/create, as demonstrated by students possessing critical thinking skills to assess ideas, acquiring research skills, synthesizing knowledge across disciplines or applying academic knowledge to real-life problems.

A3: Accomplishments
Demonstrate accomplishment of discovery/innovation/creativity through producing /constructing creative works/new artefacts, effective solutions to real-life problems or new processes.

Learning and Teaching Activities (LTAs)

	LTAs	Brief Description	CILO No.	Hours/week (if applicable)
1	Lectures	Students will learn the basic concepts, the relationship of these concepts and their practical use in information security technology management.	1, 2, 3, 4	2 hours/ week

2	Tutorials	Students will take tutorial sessions for understanding the concepts related to the lectures and discussing some real-life examples in applying the concepts.	1, 2, 3, 4	1 hour/ week
3	Group assignment 1 - simple risk analysis	Students will be required to identify threats, vulnerabilities, and countermeasures in a given security scenario, and inquire on their effectiveness.	1, 2	2 hours/ week for 4 weeks
4	Group assignment 2 - simple policy statement with solutions	Students will be required to design simple information security policy, to recommend controls according to standards, to suggest associated guidelines for recommended controls and to suggest some audit questions.	2, 3	2 hours/ week for 4 weeks

Assessment Tasks / Activities (ATs)

	ATs	CILO No.	Weighting (%)	Remarks ("-" for nil entry)	Allow Use of GenAI?
1	Group assignment 1	1, 2	12	-	No
2	Group assignment 2	2, 3	12	-	No
3	Short test	1	6	-	No

Continuous Assessment (%)

30

Examination (%)

70

Examination Duration (Hours)

2

Minimum Examination Passing Requirement (%)

30

Additional Information for ATs

For a student to pass the course, at least 30% of the maximum mark for the examination must be obtained.

Assessment Rubrics (AR)

Assessment Task

Assignment 1 (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

Criterion
Ability to identify threats and vulnerabilities in scenarios and understand relationship among threats, vulnerabilities, and countermeasure.

Excellent
(A+, A, A-) High

Good
(B+, B, B-) Significant

Fair
(C+, C, C-) Moderate

Marginal
(D) Basic

Failure
(F) Below marginal level

Assessment Task
Assignment 2 (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

Criterion
Ability to write high-level information security objectives in an environment propose reasonable procedures or guidelines, and suggest checklist or questions for security auditing.

Excellent
(A+, A, A-) High

Good
(B+, B, B-) Significant

Fair
(C+, C, C-) Moderate

Marginal
(D) Basic

Failure
(F) Below marginal level

Assessment Task
Short Test (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

Criterion
Ability to explain and apply information security technology and countermeasures

Excellent
(A+, A, A-) High

Good
(B+, B, B-) Significant

Fair
(C+, C, C-) Moderate

Marginal
(D) Basic

Failure
(F) Below marginal level

Assessment Task
Assignment 1 (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion
Ability to identify threats and vulnerabilities in scenarios and understand relationship among threats, vulnerabilities, and countermeasure.

Excellent
(A+, A, A-) High

Good
(B+, B) Moderate

Marginal
(B-, C+, C) Basic

Failure
(F) Below marginal level

Assessment Task
Assignment 2 (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion
Ability to write high-level information security objectives in an environment propose reasonable procedures or guidelines, and suggest checklist or questions for security auditing.

Excellent
(A+, A, A-) High

Good
(B+, B) Moderate

Marginal
(B-, C+, C) Basic

Failure
(F) Below marginal level

Assessment Task
Short Test (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion
Ability to explain and apply information security technology and countermeasures

Excellent
(A+, A, A-) High

Good
(B+, B) Moderate

Marginal
(B-, C+, C) Basic

Failure
(F) Below marginal level

Part III Other Information

Keyword Syllabus
Syllabus:

1. Overview of Information Security
   - Risks and Attacks in an Information System Environment.
   - Requirements on Confidentiality, Integrity, Availability, Authentication, and Non-repudiation
2. Information Security Technologies
   - Access Control
   - Encryption Techniques
   - Authentication and Public Key Infrastructure
3. Information Security Management
   - Security Policies, Relationship to Business Process
   - Security Organizations
   - Risk Analysis Processes
   - Information Security Management Standards
4. Legal Issues
   - Cyber Crimes
   - E-commerce Law
   - Data Protection Issues
   - Compliance and Information Security Audits
   - Digital Forensic
   - Incident Response

Reading List

Compulsory Readings

	Title
1	Whitman and Mattord (2010). Management of Information Security, Cengage Learning, 4th edition.

Additional Readings

	Title
1	Merkow & Breithaupt (2005), Information Security: Principles and Practices, Pearson
2	Greene (2006), Security Polices and Procedures: Principles and Practices, Pearson