Course Name: SOFTWARE SECURITY **Course Code: ITEC434**

General Information						
Course Code	**ITEC 434**	**Level/Year**	**7th / 4th**	**Required (R) / Selected Elective (SE)**		**SE**
Credit Hours	**Theory**	**2**	**Lab**	**1**	**Total**	**3**
Prerequisites	**ITEC331**	**Course Coordinator**		**Dr. Nithinsha Shajahan**		
Corequisites	**-**	**Track Leader**		**Dr. Rahama Salman**		

Course Description

This course offers a comprehensive understanding of software security principles and practices. Students will delve into secure software requirements, identifying various security threats, vulnerabilities, and attack vectors impacting software systems. The curriculum includes learning about security policies, risk management strategies, and compliance with security standards. It covers the secure software development life cycle, along with security assessment and audit techniques. Through real-world case studies, students will acquire the skills to identify and mitigate security risks in software development and deployment. By the end of the course, students will be well-equipped with the knowledge and tools to create robust and secure software solutions.

Course Objectives : On completion of the course, the student will be able to:

- Understand the key concepts, principles, and importance of software security in the development and deployment of software systems.
- Identify and analyze secure software requirements, various types of security threats, vulnerabilities, and attack vectors that can compromise software applications.
- Contrast security policies, risk management strategies, and compliance requirements to ensure adherence to industry standards and best practices.
- Evaluate secure software development life cycle, and security assessments and audit techniques to identify potential security risks and recommend mitigation strategies.
- Communicate effectively with stakeholders regarding software security issues, solutions, and best practices.

Course Contents

List of Topics	Weeks
UNIT 1: Fundamental Principles of Software Security	1,2
UNIT 2: Secure Software Requirements, Security Threats, and Vulnerabilities	3, 4, 5
UNIT 3: Secure Software Architectures	5, 6, 7
UNIT 4: Security Policies, Risk Management Strategies, and Compliance Requirements	8, 9, 10
UNIT 5: Secure Software Development Life Cycle	10, 11, 12
UNIT 6: Security Assessments and Audits Techniques	13, 14, 15

Textbook

- Suhel Ahmad Khan, Rajeev Kumar, Raees Ahmad Khan,"Software Security: Concepts & Practices", CRC Press, 1st Edition, ISBN-10: 1032356316 | ISBN-13: 9781032356310, 2023.
- Erik Fretheim, Marie Deschene,"Secure Software Systems: Design and Development", Jones & Bartlett Learning, 1st Edition, ISBN-10: 1284261158 | ISBN-13: 9781284261158, 2023.

Reference Materials

- Loren Kohnfelder,"Designing Secure Software: A Guide for Developers", No Starch Press, 1st Edition, ISBN-10: 1718501927 | ISBN-13: 9781718501928, 2021.
- James F. Ransome & Anmol Misra & Mark S. Merkow,"Practical Core Software Security: A Reference Framework", CRC Press, 1st Edition, ISBN-10: 1032333144 | ISBN-13: 9781003319078, 2023.

Course Learning Outcomes

CLO	Description	Mapped PI
CLO#01	**Understand** the fundamental principles of software security and their importance in software development and deployment.	Understanding
CLO#02	**Identify** and analyze secure software requirements, security threats, vulnerabilities, and attack vectors affecting software systems.	Remembering
CLO#03	**Design** secure software architectures by developing plans that integrate security principles into the overall structure to mitigate potential threats.	Creating
CLO#04	**Compare** and analyze security policies, risk management strategies, and compliance requirements to ensure adherence to industry standards and best practices.	Analyzing
CLO#05	**Evaluate** secure software development life cycle, and security assessments and audit techniques to identify potential security risks and recommend mitigation strategies.	Evaluating
CLO#06	**Communicate** effectively with stakeholders about software security issues, solutions, and best practices through documentation and presentations.	Applying

CLO-PI-SO Mapping

	SO-1	SO-2	SO-3	SO-4	SO-5	SO-6
CLO#01	PI 1.2	-	-	-	-	-
CLO#02	PI 1.3	-	-	-	-	PI 6.1
CLO#03	-	PI 2.1	-	-	-	PI 6.2
CLO#04	-	PI 2.2	-	-	-	-
CLO#05	-	-	-	-	-	PI 6.4
CLO#06	-	-	PI 3.1 PI 3.2 PI 3.3 PI 3.4	-	-	-