

**Course Name:CS-412, Information Security**

Credit Hours: 2-1

Contact Hours: 2-3

Pre-requisites: None

**Course Introduction:**

The Information Security course is designed to provide students with a comprehensive understanding of the principles and practices of information security. Students will learn how to assess risks, develop security policies and procedures, implement security controls, and respond to security incidents. The course will cover various topics, including access control, cryptography, network security, web security, operating system security, and cloud security.

CLO No	Course Learning Outcomes	Bloom Taxonomy
CLO-1	Understand the principles of information security, including the concepts of confidentiality, integrity, and availability.	C2 (Understand)
CLO-2	Understand and identify and assess risks to information security.	C2 (Understand)
CLO-3	Develop and apply security policies, standards, and guidelines.	C3 (Apply)
CLO-4	Implement and analyze security controls, including access control, authentication, cryptography, and network security.	C4 (Analyze)

**Course Plan:**

#	Weekly Distribution of Course Contents
Week-1	Introduction to Information Security, Types of threats and attacks
Week-2	Security policies, standards, and guidelines
Week-3	Incident response and disaster recovery
Week-4	Access Control and Authentication
Week-5	Cryptography, Symmetric and asymmetric encryption

Week-6	Hash functions and digital signatures, Cryptographic protocols (e.g., SSL/TLS, IPSec)
Week-7	Network architecture and protocols
Week-8	Network perimeter security , Web architecture and protocols
Week-9	Web application security
Week-10	Operating system architecture and security mechanisms
Week-11	Malware defense and detection
Week-12	Cloud security threats and vulnerabilities
Week-13	Cloud security controls and techniques
Week-14	Mobile security and device management
Week-15	Internet of Things (IoT) security
Week-16	Blockchain security

#### **Reference Materials:**

1. "Principles of Information Security" by Michael E. Whitman and Herbert J. Mattord (2021)
2. "Introduction to Computer Security" by Michael T. Goodrich and Roberto Tamassia (2021)
3. "Cryptography and Network Security: Principles and Practice" by William Stallings (2019)
4. "Security Engineering: A Guide to Building Dependable Distributed Systems" by Ross J. Anderson (2021)