Course Code: BCSE317L
Course Title/Subject Title: INFORMATION SECURITY

Module 1: Information Security Concepts (4 hours)

1. Information Security
2. Computer Security
3. Threats, Harm, and Vulnerabilities
4. Program Security
5. Malicious Code and Malware:
o Viruses
o Trojan Horses
o Worms
6. Countermeasures

Module 2: Authentication and Access Control (6 hours)

1. Authentication
2. Key Management Schemes
3. Hierarchical Key Management Techniques
4. Security Standards
5. User Authentication Protocols
6. Implementing Access Controls
7. Access Control Models
8. Role-Based Access Control (RBAC)
9. Attribute-Based Access Control (ABAC)
10.Attribute-Based Encryption in Information Storage
11.Physical Access Controls

Module 3: Operating Systems Security (7 hours)

1. Security in Operating Systems
2. Security in OS Design:
o Simplified Design
o Layered Design
o Kernelized Design
o Reference Monitor
o Trusted Systems
o Trusted System Functions
3. Trusted Operating System Design
4. Rootkit Attacks and Mitigation

Module 4: Security Countermeasures (7 hours)

1. Design of Firewalls
2. Types of Firewalls
3. Personal Firewalls and Configurations
4. Network Address Translation (NAT)
5. Data Loss Prevention (DLP)
6. Intrusion Detection and Prevention Systems (IDPS):
o Types of IDS
o Intrusion Prevention Systems (IPS)
o Intrusion Response Mechanisms
o Goals, Strengths, and Limitations of IDS

Module 5: Database Security (6 hours)

1. Database Security Fundamentals
2. Database Security Requirements
3. Reliability and Integrity of Databases
4. Handling Sensitive Data
5. Types of Data Disclosures
6. Methods for Preventing Disclosures
7. Inference Attacks and Mitigation
8. Multilevel Databases and Security
9. Database Attacks:
o SQL Injection Attacks
o Other Common Database Exploits

Module 6: Web Security (6 hours)

1. Browser Attacks:
o Types of Browser-Based Attacks
o Failed Identification and Authentication
2. Misleading and Malicious Web Content
3. Protection Against Malicious Web Pages
4. Website Data Vulnerabilities:
o Code within Data
o Cross-Site Scripting (XSS) Attacks
o Prevention Techniques for Data Attacks
5. Fake Emails and Email-Based Threats
6. Spam Detection Techniques
7. Phishing Attacks:
o Phishing URL Detection

o Phishing Prevention StrategiesModule

7: Privacy Issues (7 hours)

1. Privacy Concepts:
o Aspects of Information Privacy
o Computer-Related Privacy Concerns
2. Threats to Personal Data Privacy
3. People-Based Privacy Concerns
4. Privacy Principles and Policies
5. Actions for Individual Privacy Protection
6. Government Regulations on Privacy
7. Identity Theft and Prevention
8. Privacy Issues in Web Data Management
9. Application of Cryptographic Techniques for Privacy Preservation