CURRICULUM

Week 1: Introduction to Cyber Security: Core Principles, Threat Landscape, and Key Terminologies

- Understanding cybersecurity, defining cybersecurity, and its importance in today's digital world. Discuss the CIA triad (Confidentiality, Integrity, Availability) as a foundation of security goals.
- Exploring the threat landscape by providing an overview of common cybersecurity threats, including malware, phishing, ransomware, and social engineering.
- Key Terminologies and concepts by introducing essential terms such as vulnerability, risk, threat, attack vectors, firewall, encryption, and authentication

Case Study Discussion: Through discussions and the presentation of short case studies or scenario-based discussions, students will be asked to identify potential risks and consider preventive measures.

Week 2: Cybersecurity risks and risk management fundamentals

The theme introduces students to the concept of risk in cybersecurity, teaching them how to identify, assess, and prioritize risks - crucial skills for building effective security strategies. Learning objectives:

- Introduction to cybersecurity risks.
- Risk assessment process, including assessing risk appetite.
- Risk management strategies, such as avoidance, mitigation, transfer, or acceptance. Students will be introduced to NIST and ISO 27001 as guides for structured risk management.

Assignment: Have students apply risk assessment concepts to hypothetical organizations (alternatively, their own organizations), identifying potential risks and suggesting initial steps to mitigate high-priority threats

Week 3: Network Security Basics: Protecting and Monitoring Digital Infrastructure

This module introduces fundamental network security concepts, helping students understand how to secure networks against unauthorized access and attacks. Learning objectives:

- Introduction to network security, explain the purpose of network security.
- Network security tools and technologies.
- Common network threats and vulnerabilities.
- Hands-on/Interactive activity, engaging students in scenarios where they must identify network security controls. Discover (e.g., reading materials, topic notes).

Assignment: Identify network security controls for a small business or hypothetical organization

Week 4: Introduction to Cryptography: securing data through encryption and authentication

This module covers the basics of cryptography, giving students an understanding of how encryption, hashing, and digital signatures protect data and communications Learning objectives:

- Fundamentals of cryptography.
- Encryption methods and techniques.
- Hashing and digital signatures.

Assignment: Students will analyze a scenario and must recommend cryptographic methods to secure sensitive data in an organization. They can choose appropriate encryption, hashing, and authentication methods for different types of communication channels.

Week 5: Endpoint and application security: Safeguarding devices and software

Students are introduced to the importance of securing individual devices (endpoints) and applications, covering vulnerabilities and best practices for protection. Learning Objectives:

- Introduction to endpoint security, including inventory identification of endpoints.
- Application security basics.
- Tools and techniques for endpoint and application security.

Assignment: Students will be presented with a scenario in which they need to secure endpoints and applications for a small business. This will include identifying key security measures to implement.

Week 6: Incident response and cybersecurity forensics: detecting, responding to, and investigating

The module introduces students to the basics of handling and investigating cybersecurity incidents, emphasizing the steps needed to minimize damage and prevent future breaches. Learning Objectives:

- Introduction to Incident Response.
- Roles and responsibilities in incident responses.
- Cybersecurity forensics basics.
- We will simulate an incident scenario, such as a data breach or malware attack (see assignment below).

Assignment: Based on the simulation discussed in class, please outline a response plan and identify each stage of incident response, focusing on containment and investigation steps

Week 7: Cybersecurity policies and compliance: Building a culture of security. threats

This module covers the importance of cybersecurity policies, regulatory compliance, and how organizations establish security as a part of their culture and operations. It prepares students to think about the organizational side of cybersecurity. Learning Objectives:

- Introduction to cybersecurity policies.
- Overview of regulatory compliance (introduce participants ' country-specific regulations).
- Developing a security-aware culture.

Assignment: Draft a basic cybersecurity policy and compliance checklist for a hypothetical organization, considering its industry and data protection needs. Outline essential policy components.

Week 8: Establishing a cybersecurity strategy for “Fintrust Bank” - A regional financial institution

Capstone Project: Fintrust Bank is a regional bank with several branches and a growing number of online customers. As a financial institution, Fintrust faces heightened cybersecurity risks, including data breaches, fraud, and regulatory pressures. Recent cyber incidents, including a malware attack on their online platform, have highlighted gaps in the security posture. Students are tasked with designing a cybersecurity strategy to protect customer data, secure online banking services, and ensure compliance with industry regulations. During the class, we will discuss specifics from the previous courses and the case, and direct students to work on the final assignment.

The final assignment is to build a comprehensive cybersecurity strategy that addresses FinTrust Bank’s unique security and regulatory challenges. The plan should include measures for protecting customer data, securing financial transactions, and complying with regulations, such as the Gramm-Leach-Bliley Act, PCI-DSS