Module 1. Security Fundamentals

Module Learning Objectives

This module introduces students to fundamental concepts and principles in cybersecurity. The content provides a comprehensive coverage on what threaten the security of our cyberspace and how we could reinforce our systems in order to mitigate those. The module also covers the non-technical factors that govern cybersecurity at enterprise level. Students will also learn about cybersecurity as a promising career to get into.

Module Student Learning Outcomes

Upon completion of this module, students will be able to:

- Accurately explain basic cybersecurity related concepts.
- Clearly define principles of cybersecurity.
- Explain security models with precision.
- Demonstrate knowledge and understanding of security related frameworks.
- Describe security related legal, ethical, and social issues.
- Discuss risk management in the context of cybersecurity.
- Explain what cybersecurity entails as a profession.
- Enumerate required skill sets for different working roles in cybersecurity.

Module design:

Submodule 1: Security Concepts and Principles

- Unit CAD_01: Security Concepts
  Threats and Adversaries (threat actors, malware, natural phenomena)
  Vulnerabilities and risk management (include backups and recovery)
  Security life cycle, Data security, CIA, Access, Authentication, Authorization, Non-Repudiation, Privacy

- Unit CAD_02: Security Design Principles
  Separation, isolation, encapsulation, modularity, simplicity of design (Economy of Mechanism), Minimization of implementation (Least common mechanism), open design, complete mediation, layering (defense in depth), least privilege, fail safe defaults/fail secure, least astonishment (Psychological acceptability), minimize trust surface (reluctance to trust), usability, trust relationships

- Unit CAD_03: Security Models
  Bell-La Padula, Biba, Clark Wilson, Brewer Nash, Multi-level security

Submodule 2: Security Management

- Unit CAD_04: Security Management Frameworks, Guidelines, Policies
  NIST, ISO etc.

- Unit CAD_05: Security Controls/Practice
  Preventative, Detective, and Responsive
  Session Management
  Exception Management

- Unit CAD_06: Risk Management
  Basic risk assessment
  Security risk assessment and analysis

- Unit CAD_07: Non-technical Security-Related Issues
  Legal issues
  Ethics
    - *Ethics(Ethics associated with cybersecurity profession)*
    - *Ethical codes and frameworks*
    - *Ethics and cyberspace*
    - *Ethical issues*
    - *Property availability rights of others*
    - *Respect and principles of community resource use, allocation, and abuse censorship*
    - *Ethic-based decision tools*
    - *Cybersecurity and social responsibility*

  Privacy
    - *Personally identifiable information*
    - *Fair Information Practice Principles (FIPPS): Transparency, Individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security, accountability and auditing*
    - *Privacy impact assessments*
    - *Anonymity and pseudonymity*
    - *Privacy policies, laws and regulations*
    - *Risks to privacy*
    - *Tracking and surveillance*

Privacy tools: encryption, VPNs, scramblers *Privacy laws and legal basis*
Submodule 3: The Cybersecurity Profession and Careers
• Unit CAD_08: Cybersecurity as a profession
• Unit CAD_09: Building up your skills