SYLLABUS
PART I
EDISON STATE COMMUNITY COLLEGE
CYB 236S COMPUTER SECURITY ESSENTIALS
3 CREDIT HOURS

COURSE DESCRIPTION
Covers essential cybersecurity skills for protecting information systems and mitigating threats. Topics include access control, cryptography, network defense strategies, monitoring, vulnerability assessment, and incident response. Hands-on labs develop practical skills in identifying risks and applying security controls. Prepares students for the CompTIA Security+ certification. Discounted CompTIA Security+ Certification Exam voucher available upon successful completion of this course. Prerequisite: CIS 214S and CIS 215S. Lab fee.

COURSE GOALS
The student will:

Bloom's Level		Program Outcomes
2	1. Classify various types of cyber threats including malware, phishing, social engineering, and network attacks.	1, 2, 7
3	2. Implement security measures such as firewalls, encryption, and multi-factor authentication to secure systems and data.	1, 2, 8
3	3. Configure network monitoring tools to detect anomalies and identify potential security breaches.	1, 2, 3, 4
5	4. Develop an incident response plan to contain, eradicate, and recover from cyber-attacks, supporting disaster recovery and business continuity objectives.	1, 2, 4, 7
5	5. Perform vulnerability assessments and risk analysis to inform security strategies.	1, 2, 5
3	6. Apply access control mechanisms to protect data and manage user permissions effectively.	1, 2, 6, 8
5	7. Analyze network security protocols and evaluate their effectiveness in maintaining secure communications.	1, 2, 8
3	8. Apply cryptographic techniques, including encryption and hashing, for data security.	1, 2
4	9. Perform forensic investigations and analyze system, network, and security logs, including reviewing and auditing log data, to detect and respond to cyber incidents.	1, 2, 4, 8
3	10. Apply secure application development, deployment, and ongoing hardening strategies, including software updates, patch management, and configuration baselines.	1, 2, 8
5	11. Discuss compliance frameworks and their impact on security planning and risk management.	1, 2, 7
5	12. Create detailed documentation for security policies, procedures, and incident response plans.	1, 2, 8

CORE VALUES

The Core Values are a set of principles that guide in creating educational programs and environments at Edison State. They include communication, ethics, critical thinking, human diversity, inquiry/respect for learning, and interpersonal skills/teamwork. The goals, objectives, and activities in this course will introduce/reinforce these Core Values whenever appropriate.

TOPIC OUTLINE

1. Introduction to Cybersecurity and Threat Landscape
2. Types of Cyber Attacks: Malware, Phishing, and Social Engineering
3. Security Controls and Frameworks
4. Cryptographic Solutions: Encryption, Hashing, and Digital Signatures
5. Network Security Protocols: Firewalls, VPNs, secure communication protocols (e.g., TLS/SSL, IPsec), and IDS/IPS
6. Vulnerability Assessment, Risk Analysis, and Risk-Based Security Controls
7. Network Monitoring and Incident Detection
8. Access Control and Authentication Mechanisms
9. Incident Response and Forensic Analysis
10. Compliance Frameworks: GDPR, HIPAA, and NIST-based security controls and risk management
11. Operating Systems and Applications Security
12. Multi-Factor Authentication and Secure Protocols
13. Mobile and Wireless Security
14. Cloud Security and Virtualization Threats
15. Security Documentation, Audit assessment and Governance
16. CompTIA Security+ Certification Preparation