SYLLABUS
PART I
EDISON STATE COMMUNITY COLLEGE
CYB 121S INTRO TO CYBERSECURITY
3 CREDIT HOURS

COURSE DESCRIPTION
Introduction to core cybersecurity and network defense concepts, including computer-enabled abuse, encryption, network attacks, malware, security protocols, incident response, and compliance frameworks. Through hands-on activities, students develop skills to analyze threats, apply defense strategies, and respond to cyber incidents. The course aligns with the Cisco Certified Support Technician certification and prepares students for entry-level IT and cybersecurity roles. Recommended: CIS 214S and CIS 215S.

COURSE GOALS
The student will:

Bloom's Level		Program Outcomes
2	1. Discuss the social theories of computer-enabled abuse and the importance of compliance frameworks in mitigating abuse.	1, 2
2	2. Explain various motivations of malicious users, including social engineering tactics and cyber warfare methods.	1
4	3. Analyze the characteristics and behavior of different types of malicious software, including worms, trojans, viruses, spyware, and ransomware.	2, 5
2	4. Demonstrate an understanding of encryption, its uses, and potential abuses in cybersecurity, covering aspects such as symmetric and asymmetric encryption, cryptographic algorithms, and key management.	4, 5
2	5. Describe key cybersecurity standards and communication protocols, including how they are used to enhance network security.	6
5	6. Evaluate various network and computer attack types, identifying potential attackers and their methods.	2, 3, 7
4	7. Compare and contrast different network defense mechanisms, including firewalls, access control lists (ACL), intrusion detection systems (IDS), and intrusion prevention systems (IPS).	4, 5, 7, 8
4	8. Examine how information security measures and tools can be applied to mitigate cyber-crimes and protect data integrity in various operating system (OS) and network operating system (NOS) environments.	1, 3
5	9. Create a comprehensive defense strategy to protect against various cyber threats, emphasizing the importance of layered security.	2, 3, 8
5	10. Create an incident response plan that outlines the steps to take during and after a cyber-attack to minimize damage and recover effectively.	2, 7
5	11. Create security policies for an organization, including password management, data encryption, and user access controls, to protect information systems.	1, 3, 5, 6

CORE VALUES

The Core Values are a set of principles that guide Edison State Community College in creating its educational programs and environment. They will be reflected in every aspect of the College. Students' educational experiences will incorporate the Core Values at all levels, so that a student who completes a degree program at Edison State Community College will not only have been introduced to each value, but will have had them reinforced and refined at every opportunity.

TOPIC OUTLINE

1. Introduction to Cybersecurity
2. Cybersecurity Ethics, Legal Considerations, and Compliance Frameworks
3. Cyber Threats and Malicious Actors
4. Malicious Software: Worms, Viruses, Spyware, and Ransomware
5. Network Security Fundamentals and Communication Protocols
6. Network Security
7. Cryptography and Encryption Fundamentals
8. Endpoint Security and Device Protection
9. Information Security and Risk Management Strategies
10. Cybersecurity Policies and Creating Defense Plans
11. Incident Response Planning and Execution
12. Virtual Machines and Secure Computing Environments
13. Cybersecurity Tools and Implementing Protective Measures
14. Current Trends in Cybersecurity and Threat Mitigation
15. CCST (100-110) Certification Exam