Introduction to Cyber Security/Information Assurance

2023-2024 Catalog

[ARCHIVED CATALOG]

CSIA 105 - Introduction to Cyber Security/Information Assurance

---

PREREQUISITES: ITSP 135 - Hardware / Software Support or (ITSP 132 - IT Support Essentials I and ITSP 134 - IT Support Essentials II) or NETI 104 - Introduction to Networking or NETI 109 - Networking I or CSCI 101 - Computer Science I
PROGRAM: Cyber Security/Information Assurance
CREDIT HOURS MIN: 3
LECTURE HOURS MIN: 3
DATE OF LAST REVISION: Fall, 2020

The students will explore the field of Cyber Security/Information Assurance focusing on the technical and managerial aspects of the discipline. Students will be introduced to the basic terminology, concepts, and best practices of computer/network security and the roles and responsibilities of management/security personnel. The students will learn the technologies used and techniques involved in creating a secure computer networking environment including authentication and the types of attacks against an organization.

MAJOR COURSE LEARNING OBJECTIVES: Upon successful completion of this course the student will be expected to:

1. Use virtual machine technology to test security tools in a sandbox environment.
2. Identify security threats to network services, devices, traffic and data.
3. Use tools to secure network communications.
4. Monitor the security infrastructure with current industry standard utilities.
5. Discuss roles and responsibilities of information security personnel.
6. Use cryptography and public key infrastructures to secure remote access, wireless, and virtual private networks.
7. Implement "defense in depth" to shield against network attacks.
8. Discuss computer forensics and incident response.
9. Discuss basic characteristics of information.
10. Discuss information security as it applies to application guidance, and policies.
11. Describe the legal elements of investigative authorities in criminal prosecution, evidence collection, and evidence preservation.
12. Understand the concepts of trust through assurance, mechanism, and policy.
13. Understand the practical performance measures employed in designing security measures and programs.
14. Describe and discuss administrative security procedural controls.
15. Discuss the auditing and monitoring of security systems.

COURSE CONTENT: Topical areas of study include -

- Security reviews
- Effectiveness of security programs
- Investigation of security breaches
- Monitoring systems for accuracy and abnormalities

- Privacy
- Accountability controls
- Audit trails and logs
- Software design standards
- Denial of service, spoofing, and hijacking
- Networking
- Defense in depth
- Cryptography
- Security Technologies
- Legal, ethical and professional issues in Information Security
- Attribution
- Destruction of media

Course Addendum - Syllabus (Click to expand)
