Business Continuity in an Information World

2023-2024 Catalog

[ARCHIVED CATALOG]

CSIA 260 - Business Continuity in an Information World

PREREQUISITES: CSIA 105 - Introduction to Cyber Security/Information Assurance or IT Chair Approval.
PROGRAM: Cyber Security/Information Assurance
CREDIT HOURS MIN: 3
LECTURE HOURS MIN: 3
DATE OF LAST REVISION: Spring, 2020

Students will learn principles of incident response and disaster recovery. Identification of vulnerabilities and appropriate countermeasures to prevent and mitigate risks to an organization will be discussed. Students will learn risk assessment, incident response, contingency planning, and prioritizing systems for disaster recovery. The importance of management's roles and interaction with other organizational members will be discussed. Students will learn how to create a hardened network by developing system specific plans for the protection of intellectual property, the implementation of access controls, and patch/change management. Students will gain an understanding of information assurance including the governing rules and guidelines.

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

1. Explain network threats, mitigation techniques, and the basics of securing a network.
2. Describe methods for protecting data confidentiality, integrity, and availability.
3. Develop and demonstrate an understanding of incident response (human and non-human) specific to an organization.
4. Describe legal and ethical issues concerning disaster recovery and business continuity planning.
5. Describe assets to be included in planning.
6. Describe the handling process of disaster recovery, business continuity and security policy planning documentation, and schedule maintenance of documents.
7. Describe the process of building redundancy into systems for disaster recovery ensuring business continuity.
8. Develop maintenance schedule for equipment and assessment of equipment needs for disaster preparedness.
9. Create a disaster recovery plan to include a comprehensive security policy; the steps and conditions that would initiate the plan becoming active; and the life of the plan and the cross over for business continuity.
10. Demonstrate how to implement, test and assess a disaster recovery plan and to secure equipment and information.

COURSE CONTENT: Topical areas of study include -

- Information security
- Security policies and procedures
- Business continuity
- Risk management
- Information assurance
- Confidentiality, Integrity, and Availability
- Authorization, Authentification, and Accounting
- Incident response

- Disaster recovery
- Maintenance
- Documentation
- Legal and ethical issues
- Redundancy

Course Addendum - Syllabus (Click to expand)