SEC 402 – Cyber Security

Course Description

This course explores the practices and framework designed to ensure cyberspace security. Students will explore the areas of common practice in the Department of Homeland Security (DHS) Essential Body of Knowledge. Topics include the various roles, functions, and competencies within the cybersecurity domain to mitigate risks and secure organizational assets.

Instructional Materials


Course Learning Outcomes

1. Describe and apply the 14 areas of common practice in the Department of Homeland Security (DHS) Essential Body of Knowledge.
2. Describe best practices in cybersecurity.
3. Identify and analyze the role of the Chief Information Officer, Information Security Officer, and IT Security Compliance Officer in the context of cybersecurity.
4. Compare and contrast the functional roles of an organization in the context of cybersecurity.
5. Describe the corollary roles of security in an enterprise.
6. Explain data security competencies to include turning policy into practice.
7. Describe digital forensics and process management.
8. Create an enterprise continuity plan.
9. Describe and create an incident management and response plan.
10. Describe system, application, network, and telecommunications security policies and response.
11. Describe physical security plans and processes.
12. Explain legal and regulatory compliance practices.
13. Explain risk management plans and policies.
14. Identify the strategic management issues in cybersecurity planning and response.
15. Develop a cybersecurity plan that incorporates the Department of Homeland Security (DHS) Essential Body of Knowledge.
16. Evaluate the ethical concerns inherent in cybersecurity and how these concerns affect organizational policies.
17. Use technology and information resources to research issues in cybersecurity.
18. Write clearly and concisely about topics associated with cybersecurity using proper writing mechanics and technical style conventions.