CIS 333 – Networking Security Fundamentals

Course Description

This is a lab-based course that provides an overview of information technology security principles, challenges, vulnerabilities and countermeasure strategies. Topics include definition of security terms, concepts, elements, and goals. Students will explore industry standards and practices that focus on the availability, integrity and confidentiality aspects of information systems security.

Instructional Materials

Kim, D., & Solomon, M. (2013). *Fundamentals of information systems security* (2nd ed.). Sudbury, MA: Jones and Bartlett.

Course Learning Outcomes

1. Explain the concepts of information systems security as applied to an IT infrastructure.
2. Describe the principles of risk management, common response techniques, and issues related to recovery of IT systems.
3. Describe how malicious attacks, threats, and vulnerabilities impact an IT infrastructure.
4. Explain the means attackers use to compromise systems and networks, and defenses used by organizations.
5. Explain the role of access controls in implementing a security policy.
6. Explain the role of operations and administration in effective implementation of a security policy.
7. Describe the ethical principles and standards in information security.
8. Explain the importance of security audits, testing, and monitoring to effective security policy implementation.
9. Explain how businesses apply cryptography in maintaining information security.
10. Analyze the importance of network principles and architecture to security operations.
11. Apply international and domestic information security standards and compliance laws to real-world implementation in both the private and public sector.
12. Use technology and information resources to research issues in information systems security.
13. Write clearly and concisely about network security topics using proper writing mechanics and technical style conventions.