ITMS 478 SYLLABUS

ITMS 478 Cyber Security Management

Hours: 3 credit hours / 45 contact hours

Instructor: Ray Trygstad

Textbook, title, author, and year: *Management of Information Security, Sixth Edition,* Michael E. Whitman & Herbert J. Mattord, 2018

Specific course information

a. **Catalog description:** In-depth examination of topics in the management of information technology security including access control systems & methodology, business continuity & disaster recovery planning, legal issues in information system security, ethics, computer operations security, physical security and security architecture & models using current standards and models.
b. **Prerequisites:** None.
c. **Required for Applied Cybersecurity and Information Technology.**

Specific goals for the course

a. **Course Outcomes:** Each successful student will demonstrate foundation knowledge and application of cybersecurity concepts as they to apply the management of information system security in a large organizational environment. Students will describe and identify policy frameworks, legal and moral implications, and best practices in information security management. Students will be able assist in the conduct of a security audit of an organization and report on the results with appropriate suggestions for amelioration of problem areas identified.
b. **Course student outcomes:**
Upon completion of this course, each student should be able to:
    - Discuss the history of computer security and how it evolved into information security
    - Identify and define key terms and critical concepts of information security
    - Describe the business need for information security
    - Differentiate between laws and ethics, describe the role of ethics in professional practice in information security, and identify major national laws that relate to the practice of information security
    - Define risk management and its role in the Security Systems Development Life Cycle
    - Assist in the preparation and conduct of a cybersecurity audit of an existing business, government agency or organization and prepare a complete audit report with appropriate suggestions for amelioration of problem areas identified
    - Describe management's role in the development, maintenance, and enforcement of information security policy, standards, practices, procedures, and guidelines
    - Assist in the design and implementation of a comprehensive enterprise security program using policy and standards to implement technical, operational, and managerial controls
    - Recall and describe recommended security management models
    - Explain what contingency planning is and how incident response planning, disaster recovery planning, and business continuity plans are related to contingency planning.
    - Describe common technical security controls, implementations in an enterprise setting, and how they are driven by policy and standards

Topics to be covered

a. Introduction to Information Security
b. Compliance, Legal, Ethical/Professional Issues Governance and Planning for Security
c. Security Policy
d. Developing Security Programs
e. Risk Management I
f. Risk Management II
g. The Information Security Audit
h. Security Management Models
i. Security Management Practices
j. Contingency Planning: Disasters/Business Continuity
k. Security Maintenance and Digital Forensics Protection Mechanisms
l. HIPAA