

# **CS5601 Security Operations & Program Management**

**Credit Hours:** Three (3)

Instructor, Karl F. Lutzen, [kfl@mst.edu](mailto:kfl@mst.edu), 203D Centennial Hall (email first), (573) 341-6398

## **Course Objectives:**

Security Operations and Program Management looks at the broad range of topics that make up information security management concepts. This course examines many of the information security management concepts and techniques that are necessary in today's complex information technology environment.

## ***Course Description:***

An overview of information security operations, access control, risk management, systems and application life cycle management, physical security, business continuity planning, telecommunications security, disaster recovery, software piracy, investigations, ethics and more. There will be extensive reporting, planning and policy writing.

## ***Pre-requisites:***

A writing emphasized course and operating systems course and computer networking course

Note: Times given are estimates and are subject to change based upon discussion and other needs of the class

## **Information Security Management (2 weeks)**

Overview of information security management, confidentiality-integrity-availability (CIA) triad, non-repudiation, information classification, risk analysis and assessment, how policies, procedures, standards, baselines, guidelines define the security architecture, security planning, awareness programs

## **Security Architecture and Models (1 1/2 Weeks)**

Information protection environment, confidentiality and integrity models, protection mechanisms, security evaluation criteria, systems certification and accreditation.

## **Access Control and Methodology (1 1/2 Weeks)**

Information protection requirements and environment, security technology and tools, access control methodologies, information intrusion detection, analysis methods, authentication considerations.

### **Application and Systems Development (1 week)**

Software environment, software and system life cycle, system and software development methods, security in development methods, configuration management, information integrity, information accuracy and auditing.

### **Operation Security (2 weeks)**

Identify security events, alerting of proper authorities, understanding using types of controls, taking appropriate corrective or recovery actions, backups, data retention, redundancy, data handling, residual data, change management, policies and procedures.

### **Cryptography and PKI (1 or 2 days)**

Basics of cryptography, ciphers, pki, etc. Where they are used and issues associated with using encryption.

### **Telecommunications/Network Security Management (1 week)**

Operation overview, telecommunications/network environment, protection, network intrusion detection and remediation, vulnerabilities, access controls, securing the traffic, communication specific policies

### **Physical Security (1 week)**

Electrical power and threats, environmental designs, inside and outside building security designs, vulnerability and penetration testing, fire suppression, physical controls.

### **Business Continuity/Disaster Recovery (1 week)**

Business impact analysis, recovery strategies, policies/requirements, plan testing, plan maintenance, plan awareness and training, disaster recovery processes.

### **Security Incident Handling (1 week)**

Security incidents, Incident response, detection, remediation

### **Law, Investigations and Ethics (2 weeks)**

Licensing, intellectual laws, privacy laws, investigations, ethics

## ***Grading***

4 Regular Exams @ 100 points each

There is NO comprehensive final exam in this course. All exams are short answer/essay type questions.

Homework (10 to 14 weekly security scenarios) 25 points each.

Submitting a corrected copy can recover deducted points.

### **Group Case Study**

Students will be assigned randomly to small groups and required to collaborate on a security incident case study. Each group will provide a report on the security incident, how it occurred, what was the target, and what the victim could have done to prevent the security incident. Students will evaluate input and participation of each other.

## ***Reference Material***

1. There is no assigned text book for this course. Instead, various NIST Documents, handouts and other Internet documents will be used as reference material.

## ***Campus Policies***

**Academic Alert System:** <http://academicalert.mst.edu>

I will utilize the online Academic Alert System. The purpose of the Academic Alert System is to improve the overall academic success of students by improving communication among students, instructors and advisors; reducing the time required for students to be informed of their academic status; and informing students of actions necessary by them in order to meet the academic requirements in their courses.

**Disability Support Services:** <http://dss.mst.edu>

Any student inquiring about academic accommodations because of a disability should be contact Disability Support Services so that appropriate and reasonable accommodative services can be determined and recommended. Disability Support Services is located in 204 Norwood Hall. Their phone number is 341-4211 and their email is [dss@mst.edu](mailto:dss@mst.edu).

If you have a documented disability and anticipate needing accommodations in this course, you are strongly encouraged to meet with me early in the semester. You will need to request that the Disability Services staff send a letter to me verifying your disability and specifying the accommodation you will need before I can arrange your accommodation.

**Academic Dishonesty:** <http://registrar.mst.edu/academicregs/index.html>

Page 30 of the Student Academic Regulations handbook describes the student standard of conduct relative to the System's Collected Rules and Regulations section 200.010, and offers descriptions of academic dishonesty including cheating, plagiarism or sabotage. A description of the process for dealing with issues related to academic dishonesty, is available on-line at <http://ugs.mst.edu> .

**Classroom Egress Maps:**

Please familiarize yourself with the classroom egress maps posted on-line at: <http://registrar.mst.edu/links/egress.html> .