Information is an asset that must be protected. Without adequate protection or network security, many individuals, businesses, and governments are at risk of losing that asset. It is imperative that all networks be protected from threats and vulnerabilities so that a business can achieve its fullest potential. Security risks cannot be eliminated or prevented completely; however, effective risk management and assessment can significantly minimize the existing security risks. In order to provide effective protection to the organization's critical infrastructure and services, continuous monitoring as well as various processes, procedures, and technology is required to detect and prevent cyber-attacks, breaches, and security violations. In addition, existence of a comprehensive incident response plan is vitally connected to the survivability of an organization after a severe security breach or compromise of critical business operations. This course focuses on the operational aspect of managing challenges inherent in protecting a corporate network infrastructure and business information systems. The student will develop situational awareness of an organization's network and learn to manage, and maintain a defensive infrastructure that comprises of log servers, network firewalls, web application firewalls, and intrusion detection systems. Additional topics include information security operations, access control, risk management, business continuity planning, disaster recovery, and ethics.

B. Course Effective Dates: 08/20/2016 - Present

C. Outline of Major Content Areas:

See Course Description for major content areas.

D. Learning Outcomes (General)

1. Articulate why information security is essential in today's computing environments;
2. Discuss measures to secure remote access users, Email, web services, wireless networks, and operating systems; and
3. Work in virtualized environments
4. Identify and evaluate different vulnerabilities and understand how these vulnerabilities are exploited by hackers to gain entry into networks as well as to perform privilege escalation
5. Recognize the best practices and guidelines for developing and verifying effective security policies and procedures, security goals, threats and vulnerabilities, standards and security policy development, forensics, privacy implications, and ethics.
6. Evaluate severity levels and possible fixes to remediate the uncovered issues and be able to provide comprehensive solutions
7. Identify the goals of information security;
8. Describe common security threats and attacks, their ramifications and how to safeguard against them;
9. Identify and explain how various security-related technologies work;
10. Differentiate between the various cryptographic concepts;
11. Differentiate between physical security, disaster recovery, and business continuity;
12. Demonstrate ethical behavior appropriate to security-related technologies
13. Describe computer forensics and its role in information security;
14. Demonstrate a practical understanding of Incident Detection and Response procedures

E. Learning Outcomes (MN Transfer Curriculum)
This contains no goal areas.

**G. Special Information**

Note: Students are responsible to both be aware of and abide by prerequisites for ICS courses for which they enroll, and will be administratively dropped from a course if they have not met prerequisites.