COMPUTER SECURITY FUNDAMENTALS
GBIS 742
COURSE OUTLINE

Course Dates: **Tuesdays January 19 – May 4, 2010**
Course Time: **6:30 P.M. – 9:30 P.M.**
Instructor: **Joe Szewculak**
E-mail: **jszewculak@dom.edu**

Course Description:
This course provides the student with an introduction to information security and management. Topics include a basic understanding of digital crimes and criminals, computer security threats, vulnerabilities including worms and viruses, database security, control and protection methods, hardware and software concerns, policies, cryptographic techniques, authentication techniques and protocols, authorization and confidentiality, and legal, ethical and privacy issues associated with information security.

January 19: **Course Introduction (Who - What - Where - When - How)**
a) Course Structure/Grading /Required Materials
b) Inspirational Speech
c) Security Knowledge Survey

January 26: **Computer Security Concepts**

February 2: **Cryptography**

February 9: **Authentication**

February 16: **Security Attacks**

February 23: **Firewalls & Intrusion Prevention**

March 2: Midterm Exam

March 9: **SPRING BREAK (NO CLASS)**

March 16: **System Access Control & Intrusion Detection**

March 23: **Software Security**

March30: **Physical & Infrastructure Security**

April 6: **Security Management & Auditing**

April 13: **Security Planning & Control**

April 20: **Internet Security**

April 27: **Operating System Security**

May 4: Final Exam

GBIS 742 Objectives:

- Upon completion of this course, students should be able to:
    - Define computer security and protection of digital information.
    - Define the three characteristics of information.
    - Explain the two types of security (Physical & Logical).
    - Describe the two implementation strategies of security
    - Perform a Risk Analysis.
    - Define authentication and ID management.
    - Perform an Encryption and Decryption of information.
    - Identify password vulnerabilities
    - Explain Role based and Discretionary based access control.
    - Describe security attacks and their countermeasures.
    - Explain how a Firewall works.
    - Design a Firewall protection strategy.
    - Describe Access Control and physical security methods.
    - List and describe methods for securing software.
    - Describe methods of securing infrastructure.
    - Explain security management and the responsibilities involved.
    - Analyze and interpret system log files.
    - Define and describe Change Management.
    - Explain information security planning and security practices.
    - Describe the types of security policies.
    - Create a security policy for an organization.
    - Explain the purpose of an Acceptable Use Policy.
    - Explain the importance and methods of web browser security.
    - Identify and explain Internet security appliances.
    - Define Operating System Security.