Module Title:	**Information Security**
Module ID:	**CAP 430**
Prerequisite:	**CAP 240**
Level:	**7**
Credit Hours:	**3 (3+0+1)**

Module Description:

This course defines information security. Topics include security services and its mechanisms, such as confidentiality, integrity, availability and non-repudiation, security policies, access control models, authentication methods, types of attacks (including social engineering, man in the middle, DoS…etc), malware, security principles (such as separation of duties, need to know…etc), basic principles of hashing, symmetric & asymmetric cryptography, digital certificates &PKI , Email security through S/MIME & PGP, Web Security, overview of firewalls and Intrusion detection system, Operating System security, physical security, risk assessment, incidence response, disaster recovery, business continuity and a general look into computer forensics.

Module Aims:

- Understand the need for information security.
- Describe the legal and ethical issues that are related to the information security.
- Understand the important role of the risk management to achieve the security within an organization
- Learn different strategies to implement and integrate security within an organization.
- Understand the difference between business continuity and disaster recovery plan and how to design them.

Learning Outcomes:

- State the basic concepts in information security, including security policies, security models, and security mechanisms.
- Explain the requirements for trusted operating systems, and describe the independent evaluation, including evaluation criteria and evaluation process and concepts related to applied cryptography.
- Understanding the defenses methods and how to avoid the attacks
- The ability to work independently to accomplish assigned tasks.
- Describe threats to networks, and explain techniques for ensuring network security and the type of attackers.
- The ability to communicate and to discuss related topics of the course with instructor inside and outside class.

List of Topics	No. of Weeks	Contact Hours
Introduction to Information Security	3	9
Malware and Social Engineering Attacks	2	6
Application and Network Attacks	2	6
Introduction To Cryptography	2	6
Network Defenses	3	9
Access Control Fundamentals	2	6
Review	1	3

Textbook:

Security in computing, Charles P. Pfleeger , 3/E, Prentic Hall, 2002

Computer security, Dieter Gollmann , John Wiley & Sons

Network Security Essentials , (2nd Edition) by William Stallings, Prentice Hall; 2002