**Course Name :** **Advanced Digital Security**

**Course Code: MIS 9303**

**Course Level: Year 2, Semester 1**

**Course Credit Units:**  **3 CUs; 45CH**

**Course Description**

The course aims to teach students information security awareness, standards, design, control, monitoring and response given both computer software environment and the physical environment in which human beings operate; so that the learners are capable of designing and implementing information security policies, internalizing cyber laws and, analyzing and handling information security risks and effectively respond to incidences of information security breaches for business and organizational continuity.

**Expected Learning Outcomes**

By the end of the course students should be able to:

* Assess level of information security in an organizational setting.
* Analyze information security risks.
* Explain apply information security standards at hardware, software and human levels.
* Design information security polices and systems at hardware, software and human levels.
* Discuss implement information security polices and systems at hardware, software and human levels.
* Describe the monitor information security in an organization.
* Explain the respond to incidences of information security breaches for business and organizational continuity.

**Course Content**

*Overview of Information Security/Assurance*

* Confidentiality, integrity and availability (CIA) of data
* And issues relating to authenticity, non-repudiation
* Risk management, administrative control
* Logical and physical security

*Security Classification*

* Value of information and defining appropriate procedures
* Protection requirements for information

*Information Security Process*

* Method of achieving information security objectives
* Threats, vulnerabilities, attack prevention techniques
* The expected frequency of attacks
* Institution operations and technology, and the institution’s defensive posture)

*Governance Issues*

* Information security governance
* Responsibility
* Accountability
* Audit-ability, access control
* And consequence of security breach)

*Information Security Standards*

* The ISO; establishment and maintenance a documented Information Security

*Management System (ISMS)*

* Information security policy
* Information security management of identifiable risks)

*Information Security Risk and Assessment*

* Information security risk
* Vulnerability, threat; risk assessment
* Risk management process: analysis, description, estimation and treatment; risk management policy
* Risk management standards; risk mitigation; risk management tools)

*Information Security Monitoring*

* Collection and analysis of data to guard against policy violations and anomalous behavior
* Architecture issues; activity monitoring
* Network intrusion detection systems
* Condition monitoring; independent tests

*Information Security Incidents*

* Analysis of incidents
* Intrusion response
* Incident management

*Access Control*

* Authorization; access rights administration
* Authentication: shared secret systems, token systems, public key infrastructure, biometrics; firewalls; operating system access
* Application access; remote access; encryption
* Malicious code prevention; physical security

*Human Resource Security*

* Risks posed by internal users
* Background checks and screening at recruitment
* Agreements: confidentiality, non-disclosure and authorized use
* Job descriptions; training

*Data Security*

* Data and information security theories and tools
* Data creation, handling, storage
* Transmission and destruction)

*Asset Management*

* Inventories; responsibilities and operational procedures
* Media handling
* Systems documentation

*Information Security Laws and Regulations*

* Cyber laws; compliance
* Corporate relationships and exchange of information
* Information crime; scene of crime; evidence of crime
* Law enforcement; business continuity during crime investigation
* Video surveillance and paper records

*Advances in Information Security*

* Emerging issues on information security

**Mode Of Delivery**

 Lectures

 Reading assignments

 Presentations

 Group discussions

**Instructional Materials And / Or Equipment**

 Whiteboard and Markers

 Flip Charts

 LCD Projectors

 CDs, DVDs and Tapes

**Course Assessment**

 Continuous assessments tests 20%

 Group and individual project (course work) 20%

 End of Semester Examination 60%

Total 100%

**Reading Materials**

1. International conference on privacy , security and trust

2. International journal of Information Security

3. International journal of applied cryptography

4. Journal of Computer Security

5. Security Journal