Information Security

Credit Hours:	3+0	**Prerequisites:**	None

Course Learning Outcomes (CLOs):		
At the end of the course the students will be able to:	**Domain**	**BT Level**[*]
1. **Explain** key concepts of information security such as design principles, cryptography, risk management, and ethics	C	2
2. **Discuss** legal, ethical, and professional issues in information security.	A	2
3. **Apply** various security and risk management tools for achieving information security and privacy.	C	3
4. **Identify** appropriate techniques to tackle and solve problems in the discipline of information security.	C	4

* BT= Bloom's Taxonomy, C=Cognitive domain, P=Psychomotor domain, A= Affective domain

Course Content:

Information security foundations, security design principles; security mechanisms, symmetric and asymmetric cryptography, encryption, hash functions, digital signatures, key management, authentication and access control; software security, vulnerabilities and protections, malware, database security; network security, firewalls, intrusion detection; security policies, policy formation and enforcement, risk assessment, cybercrime, law and ethics in information security, privacy and anonymity of data.

Teaching Methodology:

Lectures, Written Assignments, Semester Project, Presentations

Course Assessment:

Sessional Exam, Home Assignments, Quizzes, Project, Presentations, Final Exam

Reference Materials:

1. Computer Security: Principles and Practice, 3rd edition by William Stallings
2. Principles of Information Security, 6th edition by M. Whitman and H. Mattord
3. Computer Security, 3rd edition by Dieter Gollmann
4. Computer Security Fundamentals, 3rd edition by William Easttom
5. Official (ISC)2 Guide to the CISSP CBK, 3rd edition