Information Security	Code & No:	CS 450
	Credits:	3 (3,0,0)
	Pre-requisite:	IT 341
	Co-requisite:	None
	Level:	9

Course Description:

This course helps the students to learn Principles of Information Security, Need for Information security, Place of security and contributed parties, Legal and ethical issues, Information security and risk management, Information security implementation, Security Auditing, Incident response, Business continuity and disaster recovery planning.

This course includes the following topics:

1. Introduction to Information Security
2. Need for Information security
3. Place of security and contributed parties
4. Legal and ethical issues
5. Information security and risk management
6. Information security implementation
7. Security Auditing
8. Incident response
9. Business continuity
10. Disaster recovery planning

Course Aims:

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

Student Outcomes (SOs):

☐(a) An ability to apply knowledge of computing and mathematics appropriate to the program's student outcomes and to the discipline

☐(b) An ability to analyze a problem, and identify and define the computing requirements appropriate to its solution

☐(c) An ability to design, implement, and evaluate a computer-based system, process, component, or program to meet desired needs

☐(d) An ability to function effectively on teams to accomplish a common goal

☒(e) An understanding of professional, ethical, legal, security and social issues and responsibilities

☐(f) An ability to communicate effectively with a range of audiences

☒(g) An ability to analyze the local and global impact of computing on individuals, organizations, and society

☒(h) Recognition of the need for and an ability to engage in continuing professional development

☒(i) An ability to use current techniques, skills, and tools necessary for computing practice.

☐(j) An ability to apply mathematical foundations, algorithmic principles, and computer science theory in the modeling and design of computer-based systems in a way that demonstrates comprehension of the tradeoffs involved in design choices. [CS]

☐(k) An ability to apply design and development principles in the construction of software systems of varying complexity. [CS]

☐(j) An ability to use and apply current technical concepts and practices in the core information technologies of human computer interaction, information management, programming, networking, and web systems and technologies. [IT]

☐(k) An ability to identify and analyze user needs and take them into account in the selection, creation, evaluation, and administration of computer-based systems. [IT]

☐(l) An ability to effectively integrate IT-based solutions into the user environment. [IT]

☐(m) An understanding of best practices and standards and their application. [IT]

☐(n) An ability to assist in the creation of an effective project plan. [IT]

Course Learning Outcomes (CLOs):

1. Understand the need for Information security.
2. Identify different management processes that play the important roles in applying information security.
3. Understand the major challenges and issues that affect information security.
4. Identify and analysis risks in any organization and how to choose from risk handling options.
5. Plan, design and implement security in the system development life cycle.

SOs and CLOs Mapping:

CLO/SO	a	b	c	d	e	f	g	h	i	j	k	l	m	n
CLO1					√									
CLO2					√									
CLO3									√					
CLO4					√				√					
CLO5					√				√					

No.	Topics	Weeks	Teaching hours
1	Introduction to Information Security (Reviewing security basics discussed in previous course that are needed in this course)	1	3
2	Need for Information security (Motivations, challenges and examples from real world)	1	3
3	Place of security and contributed parties	1	3
4	Legal and ethical issues	1	3
5	Information security and risk management	1	3
6	Information security implementation	2	6
7	Standards and compliance	1	3
8	Security Auditing	2	6
9	Incident response	1	3
10	Business continuity	1	3
11	Disaster recovery planning	1	3
12	Information security education and training	1	3
	Total	**14**	**42**

Textbook:

- Principles of Information Security, 4th Edition, Course Technology, By Micheal E. Whitman and Herbert J. Mattord.). (2012). ISBN-10: 1111138214, ISBN-13: 9781111138219.

Essential references

- Management of Information Security, 3rd Edition, Cengage Learning, By Michael E. Whitman and Herbert J. Mattoro.
- CISSP Certification All-in-One Exam Guide, 6th Edition, McGraw-Hill Osborne Media, By Shon Harris.