Security Management	Code & No:	CS 441
	Credits:	3 (3,0,1)
	Pre-requisite:	IT 341
	Co-requisite:	None
	Level:	10

Course Description:

This course will cover a variety of topics that will prepare students who wish to develop skills in information security management. It is a survey course that will cover a full range of information security topics, ranging from technical areas like cryptology and network security to a policy area like risk management. Technical subjects will be explored as well as other less technical topic areas where managers are required to lead an information security group and make sound business decisions surrounding information systems and security. Topics include:

- Fundamentals of cryptology (key mathematical concepts behind cryptography)
- Identification of information assets
- Identification of threats to information assets
- Information security strategy and architecture
- Intruders in an information system
- Legal and public relations implications of security and privacy issues
- Disaster recovery plan for recovery of information assets after an incident

Course Aims:

- Describe the fundamentals of cryptology.
- Discuss network threats and countermeasures.
- Describe several models of access control, both at a theoretical and practical level.
- Understand the problems and potential solutions associated with designing and implementing operating system and application security.
- Explain common practices and be able to cite some common approaches to risk management and analysis
- Understand what is required to formulate and implement a plan for incident response.

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. Describe threats to information security
2. Identify methods, tools and techniques for combating these threats
3. Identify types of attacks and problems that occur when systems are not properly protected
4. Explain integral parts of overall good information security practices
5. Identify and discuss issues related to access control
6. Describe the need for and development of information security policies, and identify guidelines and models for writing policies
7. Define risk management and explain why it is an important component of an information security strategy and practice
8. Describe the types of contingency plan and the steps involved in developing each

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									√					
CLO6									√					
CLO7											√			
CLO8											√			

No.	Topics	Weeks	Teaching hours
1	Fundamentals of cryptography	2	6
2	Identification of information assets	1	3
3	Information security strategy and architecture	2	6
4	Identification of threats to information assets	1	3
5	Threats and vulnerabilities, Intruders in an information system	2	6
6	Hardware and software control, incident handling and analysis	2	6
7	Disaster recovery plan for recovery of information assets after an incident	2	6
8	Legal and public relations implications of security and privacy issues	2	6

Total	**14**	**42**

Textbook:

- Information Security and IT Risk Management, ISBN : 978-1-118-33589-5 ,Wiley, Manish Agrawal, Alex Campoe, Eric Pierce,March 2014, ©2014

Essential references:

- Principles of Information Security, ISBN-13: 97811111382194th Edition,Michael E. Whitman ,Herbert J. Mattord, cengage learning,2009
- Practical Cryptography, Niels Ferguson and Bruce Schneier, ISBN 0-471-22357-3, John Wiley& Sons, 2003.
- Applied Cryptography, Bruce Schneier, 2nd edition, ISBN 0-471-11709-9, John Wiley& Sons, 2nd edition, 1996.