THE CYPRUS INTERNATIONAL INSTITUTE OF MANAGEMENT

COURSE UNIT DESCRIPTION

Course Unit Title	**Information Security Management for Business**	
Course Unit Code	BI425	
Type of Unit	Elective	
Level of Course Unit	Second cycle	
Year of Study	First/second year	
Number of ECTS Credits	6.0 ECTS	
Class Contact Hours	28	
Minimum Learning Effort (In Hours)	150	
Course Unit Objectives	The aims of this course is to teach to the students the fundamentals behind security engineering and principles that underpin today's cyber world. The course introduces the concepts and issues related to security of systems, data and infrastructures and present the state-of-art techniques and policies used to protect these assets. The course covers both technical, like cryptographic primitives and security designs, and managerial material that needed to be understood by a leader in an IT organization. Topics include the historical overview of security, security issues and trends, the threat landscape, cryptographic primitives as used to ensure confidentiality and integrity and the role of policy, people and processes in information security. Upon completion, students will acquire the necessary understanding and critical thinking for assessing threats involved to the cyber world and suggest appropriate countermeasures for both detection and prevention.	
Learning Outcomes	The students completing the course should be able to	
	CILO 1	Understanding of the fundamental security requirements such as confidentiality, integrity and availability.
	CILO 2	Demonstrate fundamental understanding of the notions of threat, vulnerability and risk.
	CILO 3	Demonstrate understanding regarding how to perform a risk analysis assessment on a given scenario.
	CILO 4	Demonstrate understanding of both quantitative and qualitative assessment of the risks involved in a given scenario.
	CILO 5	Develop communication skills regarding communicating the results of a technical risk analysis to the executive business team (CEO, CIO, CFO, COO).
	CILO 6	Develop critical assessment capabilities regarding known notions of security design.
	CILO 7	Demonstrate understanding of the basic threat landscape in today's cyber world.

	CILO 8	Develop critical assessment of the appropriateness of the selection of countermeasures to a given set of IT and WEB related threats.
	CILO 9	Understanding of data security notions and current authentication techniques.
	CILO 10	Understanding of the basic cryptographic mechanisms as used to protect an organization.
	CILO 11	Understanding the human-computer interaction and its implications to today's security.
	CILO 12	Develop the appropriate knowledge regarding the latest industrial and governmental standards.

Name of Lecturer(s)		
Mode of delivery	Face to Face	
Prerequisites or corequisites	None	
Course Content	1. Introduction to the fundamental security principles; confidentiality, integrity and availability.	CILO 1
	2. Risk Analysis: Identification of threats, vulnerabilities and suggestions of countermeasures for mitigation.	CILO 2,3,4,5,8
	3. The threat landscape: social engineering, phishing attack, malware, Trojan horses and DDos attacks.	CILO 7
	4. Security Design: Open Standards or Security through Obscurity?	CILO 6,8,9
	5. Cryptographic Primitives as used for data protection: encryption (block ciphers, stream ciphers, modes of operation), hashing (hash functions), digital signatures.	CILO 9,10
	6. Means of Authentication and their security/privacy implications: passwords, biometrics, OTP, hardware tokens and memorable information.	CILO 9
	7. Human-Computer Interaction: Theory behind passwords, the art of social engineering and the notion of the weakest link.	CILO 9,11
	8. Card-data Industrial standards: PCI-DSS	CILO 12
	9. Industrial standards for security: ISO/IEC 28001, ISO/IEC	CILO 12
Recommended or required reading	Required Reading: 1. Ross J. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley (2nd Edition) 2008 2. Charles P. Pfleeger and Shari Lawrence Pfleeger. Security in Computing. Prentice Hall (4th Edition). 2007 Further Reading: 3. Bruce Schneier. Applied Cryptography: Protocols, Algorithms and Source Code in C. Wiley (2015 Special Edition). 2015	
Planned learning activities and teaching methods	Face to Face	

Assessment methods and criteria	Class participation: 20% In-class examination: 80%
Language of Instruction	English
Work Placement(s)	Not applicable