THE CYPRUS INTERNATIONAL INSTITUTE OF MANAGEMENT

COURSE UNIT DESCRIPTION

Course Unit Title	**Information Security Management for Business**	
Course Unit Code	BI425	
Type of Unit	Core	
Level of Course Unit	First cycle	
Year of Study	First	
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 the students the fundamentals behind security engineering principles that underpin today's cyber world. The course introduces the concepts and issues related to security of systems, data and infrastructures and presents the state-of-art techniques for mitigating cyber threats and ensuring compliance with regulations and policies. 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. Upon completion of this course, students will acquire the necessary understanding and critical thinking for assessing threats based on widely-used risk-assessment methodologies and being in position to lead the implementation of an Information Security Management System (ISMS) in their enterprise or organization.	
Learning Outcomes	The students completing the course should be able to	
	CILO 1	Understand fundamental security notions such as confidentiality, integrity, availability, threat, vulnerability and risk.
	CILO 2	Acquire skills regarding applications of information security risk assessment on a given scenario for mitigating a threat and the implementation of security policies.
	CILO 3	Develop communication skills regarding communicating the results of a technical risk assessment analysis to the executive business team (CEO, CIO, CFO, COO).
	CILO 4	Understand notions underpinning digital infrastructures from a security point of view; authentication, fingerprinting, backup, passwords, security policies
	CILO 5	Understand technical cryptographic primitives and how they are combined to secure an IT infrastructure; hash functions, encryption algorithms, digital signatures, message authentication codes, PKI
	CILO 6	Understanding the human-computer interaction and its implications to today's security.
	CILO 7	Develop the appropriate knowledge and build sufficient skills to provide leadership in the the implementation of an Information Security Management System (ISMS) in an enterprise organization.
Name of Lecturer(s)	Dr Theodosis Mourouzis	
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 assets, threats, vulnerabilities and suggestions of countermeasures for mitigation.	CILO 1,2,3
	3. The threat landscape: social engineering, phishing attack, malware, Trojan horses and DDos attacks.	CILO 2
	4. Security Design: Open Standards or Security through Obscurity?	CILO 4,5
	5. Cryptographic Primitives as used for data protection: encryption (block ciphers, stream ciphers, modes of operation), hashing (hash functions), digital signatures, PKI, Message Authentication Codes.	CILO 5
	6. Means of Authentication and their security/privacy implications: passwords, biometrics, OTP, hardware tokens and memorable information.	CILO 4,5
	7. Human-Computer Interaction: Theory behind passwords, the art of social engineering and the notion of the weakest link.	CILO 6
	8. Information Security Management System (ISMS) Implementation: Introduction to ISO/IEC 27001 standard	CILO 7
Recommended or required reading	**Required Reading:** 1. Charles P. Pfleeger, Shari Lawrence Pfleeger and Jonathan Marguilies. *Security in Computing*. Prentice Hall (5th Edition), 2015. **Recommended Reading:** Textbooks 2. Bruce Schneier. *Applied Cryptography: Protocols, Algorithms and Source Code in C.* Wiley (2015 Special Edition), 2015. 3. Ross J. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley (2nd Edition), 2008. Research Articles 4. Stefan Bauer, Edward Bernroider and Katharina Chudzikowski. *Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks*. Computers & Security, Jul2017, Vol. 68, p145-159, 2017. 5. Yan Chen, K. Ramamurth and Kuang-Wei Wen.	

	Organizations' Information Security Policy Compliance. Stick or Carrot Approach. Journal of Management Information Systems, Vol 29(3), 2012. 6. Adel Yazdanmehr and Jingguo Wang. *Employees' Information Security Policy Compliance: A norm activation Perspective.* Decision Support Systems Vol 92, 2016.	
Planned learning activities and teaching methods	lectures, group work, lab work, role playing, project-based learning, homework	
Assessment methods and criteria	Class participation: 10% Group assignment and presentation: 30% In-class examination: 60%	
Language of Instruction	English	
Work Placement(s)	Not applicable	