DEREE COLLEGE SYLLABUS FOR: CS 4250 INFORMATION SYSTEMS SECURITY AND CONTROL

(Updated Fall 2021)

UK LEVEL: 6
UK CREDITS: 15
US CREDITS: 3/0/3

PREREQUISITES:	CS 1070 Introduction to Information Systems **or** ITC1070 Information Technology Fundamentals CS 2179 Business Information Systems
CATALOG DESCRIPTION:	An overview of information systems security function. Threats, attacks and security technology measures. Legal, ethical and professional issues. Risk assessment and management. Planning for security.
RATIONALE:	In this course, students are introduced into information systems security principles and standards as well as in control objectives for information technology. It also covers concepts, methods, and best practices in securing information systems. Moreover, this course equips students with sufficient knowledge to view information systems as organizational assets to be valued and protected.
LEARNING OUTCOMES:	As a result of taking this course the student, should be able to: 1. Examine the multiple layers of information systems security and controls in organizations. 2. Analyze the risk management approach to information assets' security with respect to operational and organizational goals. 3. Evaluate contingency strategies in respect to the information security framework in a business context.
METHOD OF TEACHING AND LEARNING:	In congruence with the learning and teaching strategy of the College, the following tools/activities are used: ➢ Lectures, class discussions of recent information systems' security best practices ➢ Office hours held by the instructor to provide further assistance to students. ➢ Use of the Blackboard Learning platform to further support communication, by posting lecture notes, assignment instruction, timely announcements, and online submission of assignments.
ASSESSMENT:	**Summative**:

First Assessment - Midterm Examination	**30%**	Answers to essay questions
Final Assessment – Research Project	**70%**	Literature review, data collection, methodology, interpretation (2,500-2,700 words)

Formative:

Case problems risk, assessment assignments	**0%**

The formative assessment(s) aim to prepare students for the summative ones.

	The First Assessment tests Learning Outcomes 1 and 2. The Final Assessment tests Learning Outcomes 1, 2 and 3. The final grade for this module will be determined by averaging all summative assessment grades, based on the predetermined weights for each assessment. If students pass the comprehensive assessment that tests all Learning Outcomes for this module and the average grade for the module is 40 or higher, students are not required to resit any failed assessments. (Guidelines and assessment rubrics are distributed on the first day of classes along with the course outline).
INDICATIVE READING:	**REQUIRED READING:** Whitman, M. E. and Mattord, H. J. (2003). Principles of Information Security. Thomson Course Technology, ISBN: 0619063181. **RECOMMENDED READING:** Ray Rothrock, R. (2018). Digital Resilience: Is Your Company Ready for the Next Cyber Threat? AMACOM; First edition, ISBN-10: 0814439241. Brotherston, L. and Berlin, A. (2017). Defensive Security Handbook: Best Practices for Securing Infrastructure. O'Reilly Media; 1st edition, ISBN-10: 9781491960387. Hubbard, D. W. and Seiersen, R. (2016). How to Measure Anything in Cybersecurity Risk. Wiley; 1st edition, ISBN-10: 9781119085294. Schou, C. and Hernandez, S. (2014). Information Assurance Handbook: Effective Computer Security and Risk Management Strategies. McGraw Hill Professional, ISBN0071826319. Menezes, A. J., van Oorschot, P. and Vanstone, S. A. (1997). Handbook of Applied Cryptography. CRC Press, Taylor & Francis Group, ISBN 9780849385230. Porter, M. E. (1985). Competitive Advantage: Creating and Sustaining Superior Performance. New York, N.Y.: Collier Macmillan.
INDICATIVE MATERIAL: (e.g. audiovisual, digital material, etc.)	**REQUIRED MATERIAL:** N/A **RECOMMENDED MATERIAL:** N/A
COMMUNICATION REQUIREMENTS:	Use of appropriate academic conventions as applicable in oral and written communications.
SOFTWARE REQUIREMENTS:	MS-Office 365 applications
WWW RESOURCES:	https://www.nist.gov/ https://www.sans.org/information-security https://www.csoonline.com

	https://sei.cmu.edu/about/divisions/cert/index.cfm https://www.enisa.europa.eu/ https://ec.europa.eu/info/law/law-topic/data-protection_en https://owasp.org/www-project-top-ten/ https://resources.infosecinstitute.com/ http://www.iso27001security.com/html/27033.html https://www.isaca.org/ https://isc2-chapter.gr/ https://www.giac.org/
INDICATIVE CONTENT:	1. Information Systems Integrity, Confidentiality and Availability a. Logical Access Controls b. Physical Access Controls c. Environmental Controls d. Data validation, processing and balancing controls 2. Information Systems Security Standards 3. Laws and Regulations 4. Policies and Procedures 5. Risk assessment and management 6. Security Technologies (IDS, VPN, PKI) 7. Contingency Strategies, Business Continuity and Disaster Recovery 8. Information Security strategies to achieve business management objectives