Course Information

Course Title	Security Management Practices
Course Prefix, Num. and Title	ITSY 2341 – Security Management Practices
Division	Technology & Business
Department	Computer Science
Course Type	WECM Course
Course Catalog Description	In-depth coverage of security management practices, including asset evaluation and risk management; cyber law and ethics issues; policies and procedures; business recovery and business continuity planning; network security design; and developing and maintaining a security plan. (Capstone course)
Pre-Requisites	ITSY 2300 & ITSY 2301
Co-Requisites	None

Semester Credit Hours

Total Semester Credit Hours (SCH): Lecture Hours: Lab/Other Hours	3:2:2
Equated Pay Hours	3
Lab/Other Hours Breakdown: Lab Hours	2
Lab/Other Hours Breakdown: Clinical Hours	0
Lab/Other Hours Breakdown: Practicum Hours	0
Other Hours Breakdown	0

Approval Signatures

Title	Signature	Date
Prepared by:		
Department Head:		
Division Chair:		
Dean/VPI:		
Approved by CIR:		

Additional Course Information

Topical Outline: Each offering of this course must include the following topics (be sure to include information regarding lab, practicum, and clinical or other non-lecture instruction).

- Introduction to Management of Information Security
- Compliance: Laws and Ethics
- Governance and Planning for Security
- Security Policies
- Developing Security Programs
- Risk Management - identifying and assessing risk
- Controlling Risk
- Security Management Models
- Security Management Practices
- Planning for Contingencies
- Personnel and Security

Course Learning Outcomes:

Learning Outcomes – Upon successful completion of this course, students will:

1. Develop a security plan
2. Establish suitable level of protection
3. Determine legal issues
4. Implement network security design
5. Revise risk analysis and security plan

Methods of Assessment:

- Individual Projects
- Group Projects
- Lab Assignments
- Tests and Quizzes
- Final Exam

Required text(s), optional text(s) and/or materials to be supplied by the student:

Management of Information Security, 5th Edition, Michael E. Whitman - Herbert J. Mattord, ISBN-13: 978-1305501256 | © 2017 or current similar textbook in the field.

Suggested Course Maximum:

16

List any specific or physical requirements beyond a typical classroom required to teach the course.

Limited by equipment. This is capstone course.
Access to netlab
• Computer (64 bit CPU) equipped with 12 GB RAM or more (running virtual machines), graphics card capable of supporting virtual machines, 19" or better monitor, and removable hard drive (500 GB or better) for each student and same for instructor.
• Instructor's machine needs 2 network interface cards (one to connect to WCJC network and one to connect to student pcs). And Data projector

• Cat 5 network cable, RJ-45 jacks and crimper for each student and 2 cable tester
• Router and cables to separate class from WCJC network
• Microsoft Windows 7 (or current version) (64 bit) operating system software for each pc (student and instructors)
• Microsoft Office suite for each pc (student and instructors)
• VMWare Workstation 11 (or current version) for each student and instructor
• Antivirus software for each pc

Course Requirements/Grading System: Describe any course specific requirements such as research papers or reading assignments and the generalized grading format for the course.

Attendance and Participation 0-10%
Labs (Projects) 25-50%
Tests 25-50%
Final Exam / Project 10-50%

A = 90.0 - 100
B = 80.0 - 89.9
C = 70.0 - 79.9
D = 60.0 - 69.9
F = less than 60.0

Curriculum Checklist:

☐**Administrative General Education Course** (from ACGM, but not in WCJC Core) – No additional documents needed.

☐**Administrative WCJC Core Course**. Attach the Core Curriculum Review Forms

  ☐Critical Thinking

  ☐Communication

  ☐Empirical & Quantitative Skills

  ☐Teamwork

  ☐Social Responsibility

  ☐Personal Responsibility

☒**WECM Course** -If needed, revise the Program SCANS Matrix and Competencies Checklist