Administrative Master Syllabus

Course Information

Course Title	Fundamentals of Information Security
Course Prefix, Num. and Title	ITSY 1300 - Fundamentals of Information Security
Division	Technology and Business
Department	Information Technology and Networking
Course Type	WECM Course
Course Catalog Description	An introduction to information security including vocabulary and terminology, ethics, the legal environment, and risk management. Identification of exposures and vulnerabilities and countermeasures are addressed. The importance of appropriate planning, policies and controls is also discussed.
Pre-Requisites	None
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
Department Head:	Muna Saqer, Comp Sci and IT&N Program Director	11-16-2023
Division Chair:	David Kucera, Technology & Business Division	11-16-2023
VPI:		

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).

- Information security, including vocabulary and terminology
- Threats and Vulnerabilities
- Network Security and Defense
- Backup and Disaster Recovery
- Security Products and Encryption
- Security and Ethics
- legal environment
- Security and Risk management
- Identification of exposures and vulnerabilities and countermeasures
- The importance of appropriate planning, policies, and controls

Course Learning Outcomes:

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

- Outline best practices for the information security goals of confidentiality, integrity, and availability
- Explain ethical practices related to information security
- Define vocabulary/terminology related to information security

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:

- Ciampa, Mark. CompTIA Security+ Guide to Network Security Fundamentals,Latest Edition, Cengage or other suitable Security textbook.
- USB Flash Drive
- Online classes: webcam and internet access

Suggested Course Maximum:

20

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

- Computer (64-bit CPU) equipped with 16 GB RAM, and removable hard drive (I TB or better) for each student and same for instructor.
- The instructor's machine needs two network interface cards (one to connect to the WCJC network and one to connect to student PCs).
- Data projector

Rev. June 2023

- Cat 5 network cable, RJ-45 jacks and crimper for each student, and two cable testers
- Router and cables to separate class from WCJC network
- Microsoft Windows current version (64-bit) operating system software for each PC (student and instructors)
- Microsoft Office suite for each PC (student and instructors)
- 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.

Assignments 20-30%
Labs 20-30%
Tests and Final Exam 30-50%

Grade System:
90-100% .... =A
80-89% .... =B
70-79% .... =C
60-69% .... =D
Below 60%.... =F

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