Wharton County Junior College

Administrative Master Syllabus

Course Information

Course Title	Incident Response & Handling
Course Prefix, Num. and Title	ITSY2342 - Incident Response and Handling
Division	Technology and Business Division
Department	Computer Science
Course Type	WECM Course
Course Catalog Description	In-depth coverage of incident response and incident handling, including identifying sources of attacks and security breaches; analyzing security logs; recovering the system to normal; performing postmortem analysis; and implementing and modifying security measures.
Pre-Requisites	ITSY 2300 and 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:	Stephen Lyford Digitally signed by Stephen Lyford Date: 2020.06.04 19:56:19 -05'00'	06/04/2020
Department Head:	Stephen Lyford Digitally signed by Stephen Lyford Date: 2020.06.04 19:56:39 -05'00'	06/04/2020
Division Chair:	David Kucera Digitally signed by David Kucera DN: cn=David Kucera, o=Wharton County Junior College, ou=Division of Technology and Business, email=davidk@wcjc.edu, c=US Date: 2020.06.08 10:36:56 -05'00'	06/08/2020
Dean/VPI:	Paul J. Quinn Digitally signed by Paul J. Quinn Date: 2020.06.10 08:33:24 -05'00'	06/10/2020
Approved by CIR:	Paul J. Quinn Digitally signed by Paul J. Quinn Date: 2020.06.10 08:33:42 -05'00'	06/10/2020

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).

Planning for Organizational Readiness
Incident Response Team Structure
Incident Response Planning
Incident Response: Detection and Decision Making (DoS, Malicious Code, Unauthorized Access,
  Detection and Analysis
  Response Strategies: Containment, Eradication and Recovery
  Post-incident Activity
  Disaster Recovery
Online Tools and Resources
Crisis Handling Steps
Federal Agency Incident Reporting

Course Learning Outcomes:

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

1. Identify sources of attacks;
2. Restore the system to normal operation;
3. Identify and prevent security threats;
4. Perform a postmortem analysis;
5. Identify computer investigation issues;
6. Identify the roles and responsibility of the incident response team.

Methods of Assessment:

All outcomes will be accessed by one or more of the following:

* 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:

NIST Special Publication 800-61 Revision 1: Computer Security Incident Handling Guide, 2012, Computer Security Division, NIST, Gaithersburg, MD, Emmanuel Aroms and
Principles of Incident Response and Disaster Recovery, 2nd Edition, Michael E. Whitman, Mattford, Herbert and Green, Andrew, Cengage, 2014, ISBN 978-1111138059
or current textbook on the topic.

Suggested Course Maximum:

20

List any specific or physical requirements beyond a typical classroom required to teach the 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) Linux Operating system*
• 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

The course maximum is set by current equipment contained in the lab.

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%
Chapter Review Questions 0-10%
Labs (Projects) 25-50%
Tests 25-50%
Final Exam / Project 10-25%

100 -90 = A
89 - 80 = B
79 - 70 = C
69 - 60 = D
60 and below = 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