J. Sargeant Reynolds Community College
Course Content Summary

Course Prefix and Number: ITN 275 **Credits:** 4

Course Title: Incident Response and Computer Forensics

Course Description: Prepares the student for a role on an organizational IT support staff where the need for resolving computer incidents is becoming increasingly common. Includes legal and ethical issues of search and seizure of computer and peripheral storage media leading to laboratory exercises examining computers configured with mix of both simulated criminal and other activities which are not criminal in nature, but do violate scenario-driven organizational policy. Requires the student to make choices/recommendations for further pursuit of forensics evidence gathering and analysis. Students will select and gather the utilities and procedures necessary for a court-acceptable forensics toolkit which will then be used to gather and examine specially configured desktop computers. Students will then participate in a mock court proceeding using the collected evidence. Credit will be given to either ITN 275 or ITN 276 and ITN 277, but not all three courses. Prerequisite: ITN 260 or equivalent. Lecture 3 hours. Laboratory 2 hours. Total 5 hours per week.

General Course Purpose: This course is required for the Cyber Security Career Studies Certificate and may be used as an elective in the Information Systems Technology AAS degree.

Course Prerequisites and Co-requisites:
Prerequisite: ITN 260 or equivalent

Course Objectives:
Upon completing the course, the student will be able to
a. Demonstrate sound incident response methodology;
b. Gather computer resident evidence using current best practices;
c. Document and analyze computer-resident evidence;
d. Formulate root cause hypotheses regarding computer intrusion events;
e. Test root cause hypotheses of computer intrusion events;
f. Report on causal factors; and
g. Recommend mitigating controls.

Major Topics to Be Included:
a. Introduction to Computer Forensics
b. History of Computer Crime
c. Incident Response
d. Forensic Methodology
e. Preservation of Best Evidence
f. Forensic Image Creation
g. File System Indexing
h. Data Analysis
i. Forensic Analysis Tools
j. Reporting

Effective Date of Course Content Summary: November 16, 2015