ERIE COMMUNITY COLLEGE
STATE UNIVERSITY of NEW YORK

A. Course Number and Title: DA102
Introduction to Computer Security Investigations and Hardware Fundamentals (Intro to CSI/DF)

B. Curriculum: Information Technology (1492)

C. Course Description: Overview of computer security investigations including, but not limited to: guidelines and procedures; policies and regulations and proper incident response. Various digital media, operating/file systems, and forensic software will be introduced. Overview of hardware fundamentals including safe handling of, installation and configuration of microcomputer hardware components. Hands-on laboratory exercises will be included.
(N)

D. Duration of Instructional Period: 150 Minutes Lecture per week for 15 weeks
100 Minutes Laboratory per week for 15 weeks

E. Academic Credit Hours: Four (4.0)
Contact hours: Five (5.0)
Lecture, Lab, Credit Hours: (3,2,4)

F. Suggested Text(s):

G. Course Outcomes: Upon completion, the student will be able to:

1. Explain the guidelines and procedures of computer security investigations.
2. Understand regulatory issues related to computer security investigations.
3. Demonstrate knowledge of digital forensics hardware and software.
4. Demonstrate knowledge of various operating systems and their file systems, digital media and forensics software.
5. Understand how to discharge static electricity before working with computer hardware and other safety issues.
6. Understand what the main components of a PC are and how they are installed and configured.
7. Demonstrate knowledge of disassembly of computer and other electronic device hardware.
8. Demonstrate a general understanding of other hardware devices such as PDAs, cell phones, and iPods.

H. Program Competencies:

Upon graduation with an Associate in Applied Science degree in Information Technology, the graduate will be able to:

1. Demonstrate knowledge of a broad business and real world perspective of information technology.
2. Demonstrate analytical and critical thinking skills.
3. Demonstrate the ability to apply analytical and logical thinking to gathering and analyzing information, designing and testing solutions to problems, and formulating plans.
4. Demonstrate the ability to visualize and articulate complex problems and concepts.
5. Demonstrate the ability to gather, analyze and organize data using a logical and systematic process.
6. Demonstrate the ability to select, implement and evaluate appropriate problem solving techniques and tools.
7. Demonstrate the ability to effectively adapt problem solving techniques to specific situations.
8. Use and apply current technical concepts and practices in the core information technologies.
9. Identify and evaluate current and emerging technologies and assess their applicability to address the users' needs.
10. Analyze the impact of technology on individuals, organizations and society, including ethical, legal and policy issues.
11. Demonstrate an understanding of best practices, standards and their application.
12. Demonstrate independent critical thinking and problem solving skills.
13. Communicate effectively and efficiently with clients, users and peers both verbally and in writing, using appropriate terminology.
14. Demonstrate the ability to present and discuss how computer systems impact the operation and management of business and society.
15. Demonstrate the ability to discuss the impact of information technology on society and the workplace.

Certificate competencies:

Upon graduation with a Certificate in CSI/DF (Computer Security Investigation and Digital Forensics), the graduate will be able to:

1. Be conversant with multiple digital devices including, but not limited to; computers, personal digital assistants, cameras, cell phones, iPods, and removable flash media.

2. Comprehend the process for digital evidence to be admissible in a court of law.
3. Comprehend the "Chain of Custody" process.
4. Understand the rules of evidence, and basic NY State law with regard to the search and seizure of digital evidence.
5. Explain the physical handling of digital devices.
6. Create understandable and accurate reports.
7. Acquire, validate, extract, analyze and report upon digital evidence.

I. SUNY General Education Knowledge and Skills Areas: N/A

J. ECC Graduate Learning Outcomes:

1. Read and think critically.
   Related Course Objectives 1-5
2. Apply appropriate mathematical procedures and quantitative methods.
   Related Course Objective 5
3. Demonstrate competence with computers and technology.
   Related Course Objectives 1-5

K. Assessment of Student Learning:

Projects/Assignments 60%
Exams 40%
Students will be required to exhibit knowledge and application of the topics listed in the topical outline.

L. Learning Resource Center: Students are strongly encouraged to use the library and Internet, where appropriate, when completing assignments.

NIST.gov (Special Publications SP 800-72, 86, 101)

PC Hardware Essentials
Groth | Glister (Wiley)
978-0-470-07400-8

Computer Forensics and CyberCrime – 2nd edition
Britz (Prentice Hall)
978-0-13-244749-2

M. Topical Outline

Topics	Instructional Period
A) Introduction to Computer Security Investigations 1) Guidelines 2) Procedures 3) Private vs. public investigations 4) Policies 5) Regulations	2 weeks
B) Incident Response 1) Forensic Process (data acquisition, validation, extraction, analysis, and reporting) 2) Chain of custody 3) Evidence handling and storage	2 weeks
C) Software, Operating Systems and File Systems 1) Current forensic software products will be introduced 2) Volatile and non-volatile data 3) Windows (FAT, NTFS) 4) MAC (HFS, HFS+)	3 weeks
D) Hardware Fundamentals for Digital Forensics 1) Safety i) Electrostatic Discharge - Grounding ii) Power Supplies iii) Safe handling and transport of equipment 2) Microcomputer Device and Component Recognition i) Desktop computers ii) Laptop Computers 3) Hardware Installation, Configuration and Removal i) Disassembly and Reassembly of a PC ii) Installation of Hardware Components iii) Hard Drive types and configuration 4) New Technologies i) Cell phones ii) PDAs iii) iPods, iTouch	7 weeks
E) Current Topics in Digital Forensics	1 week

Prepared by: Louise M. Kowalski / Lisa A. Palombo 1/27/09