# **ISY Information Security Degree Program**

## **CIS/CNE Program Graduate Competencies**

## **(Students enrolled in the ISY degree program are required to take some CIS/CNE foundation courses)**

1. Utilize the latest integrated application software package.
2. Install, configure and secure operating systems and application software.
3. Design, write, and debug structured business computer programs.
4. Analyze and design complex computer applications to solve business problems.
5. Integrate the principles of the Internet into web development.

**CIS 120 – Introduction to Programming**

**Course Description**

This course provides students with an introduction to the design and implementation of basic computer programming. Topics include logic development, control structures, variables, input/output, and debugging techniques of modern programming.

**Core Course Performance Objectives**

1. Translate logic into computer executable instructions.
2. Evaluate and construct control structures of computer programs.
3. Construct an effective computer program using proper variables
4. Justify the use of modularization in computer programming.
5. Construct user-friendly input and output for effective user communication.

## **CIS 141 – Operating Systems I**

**Course Description**

This course provides a basic overview of Windows and Linux. Students will install, configure, maintain, and troubleshoot the operating systems. Students will be introduced to basic operating system security.

**Course Performance Objectives**

1. Demonstrate an understanding of management of computer operating system’s architecture and command utilities.
2. Manage system resources.
3. Apply basic computer skills to maintain operating system security.

## **CIS 192 – Network Technician and Administration**

**Course Description**

This course provides students with the knowledge and skills necessary to install, maintain, and troubleshoot computer network infrastructure. Students will learn to describe computer networking technologies, apply basic design principles, adhere to computer wiring standards, and use test equipment.

**Course Performance Objectives**

1. Demonstrate an understanding of the basic functions and interconnectivity of computer networks.
2. Develop a plan to design and implement a basic computer network.
3. Maintain, troubleshoot, and repair a basic computer network.

## **CNE 180 – Computer Assembly and Maintenance**

**Course Description**

This course provides an overview of the personal computer and its components. Students explore and assemble personal computers. An introduction to non-component troubleshooting is included.

**Course Performance Objectives**

1. Install standard personal computer components.
2. Maintain, troubleshoot, and repair personal computers.
3. Install, configure, and maintain select operating systems and software.
4. Configure and troubleshoot basic personal computer client networks.
5. Identify the most effective security practices to select operating system desktop clients.

## **ISY Program Graduate Competencies**

1. Identify and remediate vulnerabilities.
2. Design, plan, and install network systems.
3. Install and configure operating systems.
4. Demonstrate the ability to write and debug scripts.
5. Demonstrate professionalism and ethical responsibility.
6. Communicate effectively to diverse groups of stakeholders.
7. Perform change management analysis and documentation.
8. Perform evidence collection and forensics analysis.
9. Create, modify, and/or implement security policies.

**ISY 111 – Ethics and the Information Age**

**Course Description**

This course provides students with knowledge of ethics and moral philosophy appropriate to the field of computer information and technology. A framework for ethically-grounded decision making in the information age is also provided.

**Core Course Performance Objectives**

1. Explain the history of computing.
2. Evaluate and discuss the social context of computing.
3. Give examples of and explain ethical theory and tools of analysis.
4. Examine and explain professional and ethical responsibilities.
5. Differentiate risks and liabilities of computer-based systems.
6. Examine the ethical dimensions of intellectual property, privacy and civil liberties.
7. Describe crime related to information technology.
8. Examine information technology issues within the framework of ethical theory.

## **ISY 143 – Introduction to Information Security**

**Course Description**

This course introduces students to information security vocabulary and terminology, the legal environment, risk management, security technologies, and security planning and implementation. Students will be prepared for further study in computer forensics and cyber network protection.

**Course Performance Objectives**

1. Discuss computer security terminology.
2. Identify security threats, vulnerabilities, and countermeasures.
3. Describe technical methods to implement and monitor defense strategies.
4. Analyze basic network security issues and Web vulnerabilities.
5. Explain the role of government in information security and information secrecy.

## **ISY 150 – Introductory Scripting**

**Course Description**

This course examines various types of scripting languages and their appropriate use for integration of applications and systems. It also addresses the use of scripting languages to facilitate the management, integration, and security of the systems that support an organization. Students will experience hands-on application and problem-solving orientated introduction to script programming.

**Course Performance Objectives**

1. Write, run, and debug programs in scripting languages.
2. Design and implement simple programs from user requirements.
3. Construct logical conditions with appropriate control statements.
4. Create and manipulate objects that store a collection of data.
5. Modify and utilize existing industry scripts.

## **ISY 201 – Advanced Operating Systems**

**Course Description**

This course covers advanced topics in computer operating systems and their design implementation. Essential topics include portable operation systems, mobile operation systems, virtual memory management, file systems, parallel computing, and virtualization.

**Course Performance Objectives**

1. Compare mobile operating systems including the features, security issues, and management of those operating systems.
2. Create and customize portable operating systems to resolve system issues.
3. Describe how desktop and server PCs use virtual memory management, parallel computing, and other features.
4. Apply industry standards for desktop and server virtualization.
5. Configure server file systems and implement file system security.

## **ISY 243 – Information and Network Security**

**Course Description**

This course introduces the student to beginning computer information and networking security principles and how the field relates to other areas of Information Technology. It covers topics on how to harden a network, protect communications and use cryptography and Public Key Infrastructure (PKI) to thwart attackers. This course also provides the board-based knowledge necessary to take an optional network security certification examination.

**Course Performance Objectives**

1. Define information security and its components.
2. Define network security basics, baseline and network infrastructure.
3. Assess attackers and their attacks over the Internet.
4. Protect wired and wireless communications.
5. Secure with cryptography and digital certificates.
6. Manage operational security with policies and procedures.

## **ISY 250 – Network Defenses and Countermeasures**

**Course Description**

This course examines the critical defensive technologies needed to secure network perimeters. Coverage of network security threats and goals, advanced TCP/IP concepts, router security, intrusion detection, firewall design and configuration, IPSec and virtual private network (VPN) design, and wireless network design and security.

**Course Performance Objectives**

1. Identify and distinguish the importance of ethical practices of penetration testing.
2. Plan and execute a penetration test.
3. Produce and present an incident report.

## **ISY 251 – Hardening the Infrastructure**

**Course Description**

This course examines tools, techniques, and technologies used in the securing of information assets. This course is designed to provide in-depth information on the software and hardware components of Information Security and Assurance. Topics covered include firewall configurations, network security, virtual private networks (VPNs) and security monitoring tools.

**Course Performance Objectives**

1. Evaluate and discuss firewall planning and design.
2. Create firewall configurations and perform administration.
3. Explain and evaluate proxy servers.
4. Demonstrate an understanding of encryption, and implement encryption schemes.
5. Evaluate and select an identity management structure.
6. Analyze and evaluate the setup of a Virtual Private Network (VPN).
7. Explain and configure intrusion detection and prevention systems.

## **ISY 270 – Computer Forensics**

**Course Description**

This course provides a solid introduction to digital investigations, preparing students to acquire and analyze digital evidence. It covers file structures in different computer operating systems, data recovery techniques, data hiding, data preservation techniques, chain –of-evidence procedures and expert witness testimony.

### **Course Performance Objectives**

1. Define computer forensics and investigations.
2. Work with different computer operating systems, their boot processes and file systems.
3. Prepare and use current computer forensics tools.
4. Process crime and incident scenes.
5. Perform forensic analysis.
6. Write investigation reports and become an expert witness.

## **ISY 280 – Advanced Security Topics**

**Course Description**

This course covers advanced topics in information and network security. Students will utilize all the previously learned knowledge, skills, and abilities to perform “real world” tasks related to the field of information security. The course is based on a sequence of hands-on laboratory exercises for teams of students. It emphasizes defensive tools and techniques at the expense of attacks.

### **Course Performance Objectives**

1. Compare and install server and desktop OS.
2. Diagram and implement network design.
3. Configure firewall settings and maintain network security.
4. Configure and implement intrusion detection/prevention systems.
5. Identify and exploit vulnerabilities in a network.
6. Prepare and present an incident report.