



## **I. Basic Course Information**

- A. Date of Proposal: April 2002
- B. Course Developers: Michael Sukkarieh & Pratap Reddy
- C. Course Number and Title:  
*CISY 229, Information Security Fundamentals*
- D. Sponsoring Department: Computer Information Systems (CIS)
- E. Semester Credit Hours: 3
- F. Weekly Contact Hours: 4 (2 lecture, 2 lab)
- G. Prerequisite: Networking Essentials & Operating Systems or permission of instructor
- H. Laboratory Fees: Yes

## **II. Catalog Description**

In this introductory Information Security Fundamentals course, students will be introduced to Information Security Principles, Components and Architectures. The course will introduce students to the application of Information Security Principles to support Information Technology (IT) Architectures, Management and Data Protection. The use of case studies, simulated exercises, and data analysis, will reinforce what is learned in the classroom. Students will learn how to find a practical equilibrium in the implementation of the learned controls in a business environment that balances technologies, processes and policies.

### **III. Statement of Course Need**

With the popularity and the global nature of the Internet, the past few years saw a dramatic transformation of the way computers and networks were traditionally used. Computers are no longer standalone tools. Networks are no longer private. The need to be connected was obvious, since with such a fluid, open, and young global infrastructure, came good strategic business opportunities. However, along with these opportunities came challenges of protecting and improving current controls over information assets and data privacy. This course prepares students for entry-level positions as an Information Security Officer or an IT Auditor. It will introduce students to Principles; Components and IT Support Architecture of Information Security and Data Privacy. In addition, the curriculum may be used as a study guide for the Certified Information System and Security Professional (CISSP) exam.

### **IV. Place of Course in College Curriculum**

CIS Programming Elective  
Students from industry requiring further education

### **V. General Education Goals and Objectives**

1. The student will develop the ability to think critically
2. The student will develop the ability to reason quantitatively

### **VI. Student Learning Outcomes**

*At the conclusion of the course, students will be able to:*

- Design a corporate information security strategy
- Develop a secure IT architecture
- Write an information security policy
- Monitor and analyze information security events and controls
- Sort and respond to information security threats
- Research and connect to the best resources relating to Information Security

### **VII. Outline of Course Content**

At the end of the semester, a final project and a final exam are given. The three major content providers are (1) The textbook(s), (2) Instructor's lectures, and (3) experiences gained in lab work and assignments. The Outline for the Course is below. This outline can be adapted by individual instructors according to the steps in which they cover content

# **CISY \*\*\* – INFORMATION SECURITY FUNDEMENTATLS**

## **COURSE OUTLINE**

### **Phase I:**

- Network Security
- Principles of IT security
  - OSI model
  - Information Security Components
  - Security threats and the need for information security
  - Information Security Principles: Authentication and Authorization, Access Controls, Confidentiality, Data Integrity, Non-repudiation, Accountability and Availability
  - Research Methods
- Security Management Practices
- Application and System Development Security
- Operations Security
- Data Network Protocols (TCP/IP, IPSec, UDP etc.)
- Firewalls and Firewall Architecture
- Hacker Tools and Techniques
  - War dialers, scanners, sniffers, session hijacking, password cracking

### **Phase II:**

- Basic OS Security Architecture for UNIX and MS OS (i.e. NT and Win 2k)
  - Unix File system security
  - NFS
  - Access Controls and Configuring Network Services
  - Case Studies on Unix Vulnerability
  - MS OS Security Principles
  - Windows NT Security Architecture (Registry, Domain, Authentication etc.)

### Ns and Remote Access

- Auditing and Logging
- Security Architecture and Models
  - Kerberos
  - Public Key Infrastructure
  - Directory Structures
  - Entitlement
- Basic Database security
- Intrusion Detection and Monitoring
  - Purpose and Rationale
  - Design and Architecture
  - Technology, Process and Procedures
- Business Continuity Planning
- Physical Security
- Basic Cyberlaw and Forensics
  - Privacy regulation that affect information security

### **LAB WORK and ASSIGNMENTS:**

The lab work will be detailed as needed. However, students will be expected to

- 1- Run and analyze firewall statistics, (bi-weekly)
- 2- Analyze sample configuration files for routers and firewalls (in group)
- 3- Run at least one simulated ethical hacking exercises and to analyze data (in group)
- 4- Design a Demilitarized (DMZ) Architecture (Group Project)
- 5- Write an Information Security Policy to a fictitious company (in group)
- 6- Summarize major concepts learned in class (weekly)
- 7- Create an IT Audit Program (Group)

### **VIII. Suggested Materials**

#### **Bibliography:**

##### **Textbook:**

- Hacking Exposed by Joel Scambray, Stuart McClure and George Kurtz, McGraw-Hill Professional Publishing; ISBN: 0072127481
- Internet Security Secrets by John Vacca, Hungry Minds, Inc; ISBN: 1568844573; Bk& Cd edition (January 1996)

##### **Other:**

- BS7799 (Free download)
- CISSP Examination Textbooks (Volume 1 Theory) by S. Rao Vallabhaneni
- Data Privacy Act (DPA)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulation

Lab Tools:

- ❑ COMMERCIAL SOFTWARE: BlackIce Personal Firewall, PGP
- ❑ FREEWARE SOFTWARE: WAR DIALER, NMAP, and Linux

Further Recommended Readings: TBD

- ❑ The CISSP Prep Guide: Mastering the Ten Domains of Computer Security by Ronald L. Krutz, Russell Dean Vines, Edward M. Stroz (Foreword), John Wiley & Sons; ISBN: 0471413569
- ❑ Secured Computing: A Cissp Study Guide by Carl F. Endorf
- ❑ Writing Information Security Policies by Scott Barman, New Riders Publishing; ISBN: 157870264X
- ❑ The CERT(R) Guide to System and Network Security Practices by Julia H. Allen, Addison-Wesley Pub Co; ISBN: 020173723X

<http://www.cissp.com/default.html>, the web portal for the certified information systems security professionals