Introduction to Information Security
Course Outline

DIVISION: Information Technology

CURRICULUM: Elective course for the following programs:
- Database Administration and Development
- Network Design and Administration
- Programming
- Web Design
- Web Development
- Wireless Communications

COURSE TITLE: Introduction to Information Security

COURSE NUMBER: ITC 150

QUARTER-HOUR CREDITS: 5

APPROXIMATE CLOCK HOURS PER QUARTER FOR:
- LECTURE: 55 (Integrated lecture and hands-on)
- LABS:

TYPE OF COURSE: Professional/Technical

COURSE DESCRIPTION:
Students will learn the foundations of information security and how to protect their personal information. This class will cover laws, ethics, physical security, security policies, and social engineering. Students will receive hands-on experience with firewalls, virus scanners, encryption and diagnostic tools. The instructor will present encryption, digital certificates, authentication, and network vulnerabilities. Students will work with local, Internet, and wireless networks.

COURSE OBJECTIVES:
This course will prepare students to be good corporate citizens and responsible users of the Internet. Students will learn:
1. The fundamentals of information security, data communications and cryptography
2. The basics of data transfer across local, wireless and Internet networks
3. The various international laws that regulate data security
4. The laws and ethics of personal privacy
5. The role of psychology in information security
6. How hackers have influenced corporate and personal behavior
7. The foundations of encryption and how encryption is employed over various Internet protocols
8. The physical risks to information security

STUDENT OUTCOMES:
After completing this course the students will be able to:
1. Identify and recommend good corporate security policies
2. Install and administer personal security tools such as firewalls and virus scans
3. Minimize risks presented by the physical realm such as machines, offices, and paper
4. Encrypt files with personal encryption software
5. Use diagnostic tools to test for PC and network vulnerabilities
6. Generate solid passwords resistant to password cracking
7. Discriminate between secure and insecure data transfer from browsers to Web sites
8. Prevent personal computer attacks
9. Understand the influence of laws on industry security requirements
10. Protect personal data on their personal computers and over networks
11. Understand emerging technologies such as wireless devices and the inherent security vulnerabilities
12. Make informed decisions about security technologies and tools
13. Secure their home computers and home computer networks

LENGTH OF COURSE: 1 quarter

CLASS SIZE (maximum): 20

PREREQUISITES:
WEB 110, or NET 120. or NET 142, or ITC 140 with 2.0 or better, or with instructor permission.

TOPICAL OUTLINE AND MAJOR DIVISIONS:
1. Physical security
   • Data storage and disaster recovery
   • Physical storage of passwords
   • Loss of physical devices
2. Basics of Internet structure
   • TCP/IP overview
   • Concept of ports
   • ISO data communications model
3. Human resource policies
   • New employee orientation
   • Exit interviews and employee departure procedures
4. Computer vulnerabilities
   • Viruses
   • Trojan horses
   • Worms
   • Logic bombs
5. Browser vulnerabilities
   • Cookies
   • JavaScript
   • ActiveX Controls
   • Signed applets
6. Preventive tools
   • Firewalls
   • Virus Scanners
   • Human detection of vulnerabilities
7. Access control methods
   • Kerberos
   • Challenge Handshake Authentication Protocol
   • User name/password
   • Biometrics
8. Passwords
   • Password Cracking
     i) Birthday
     ii) Brute Force
     iii) Dictionary
   • Password Generators
9. Encryption
   • Basics of cryptography
   • Personal encryption tools
   • Secure Sockets Layer
   • Encrypted Web pages and detecting the https protocol
   • Encrypted email
10. Wireless security
    • Authentication over wireless networks
    • Wireless snooping and intrusions
    • Choosing a secure wireless network
    • Using handheld devices over a wireless network
• Sending information over handheld devices

11. Laws and ethics
  • US security laws
  • US privacy laws
  • International security laws, survey of countries/regions such as:
    i) France
    ii) European Union
    iii) Korea
    iv) Japan
    v) Germany
  • Ethics of security practices

12. Human vulnerabilities
  • Email hoaxes
  • Spam

13. Social Engineering

14. Auditing tools and basic risk analysis
  • Port scans
  • Vulnerability assessments
  • White hat hacking

15. Budgetary concerns
  • Open source and commercial tools
  • Assessing needs and budgets for various industries and budgets

OUTLINE DEVELOPED BY: Kimberlee Jensen

DATE: October 25, 2004

REVISED: December 9, 2004