



# IT & Data Assurance I

Course Syllabus

3 – 0 - 3

Revised 12/12/11

**COURSE NUMBER:** IST 293

**PREREQUISITE(S):** CPT 114 and IST 220 with a minimum grade of C.

**CO-REQUISITE(S):** None

**COURSE DESCRIPTIONS**

This course introduces the basics of network security. Topics covered will include network vulnerabilities and threats, security planning, security technology, network security organization, as well as legal and ethical issues related to network security.

**TEXTBOOK(S):** Security + Guide to Network Security, Fourth Edition, Course Technology, ISBN: 9-7811-3330-1400 Lab Connection access code bundled with textbook if purchased in SCC Book Inn. To purchase the access code separately, visit [www.cengagebrain.com](http://www.cengagebrain.com)

**REFERENCE(S):**

**OTHER REQUIRED MATERIALS, TOOLS, AND EQUIPMENT:** Computer with Internet access, Internet Explorer 6.0 or higher or other current browser, Java, word processing software (must be able to save Word format), and anti-virus software.

**METHOD OF INSTRUCTION:** Online

**GRADING SYSTEM:**

90	-	100	=	A
80	-	89	=	B
70	-	79	=	C
60	-	69	=	D
Below	-	60	=	F

**GRADE CALCULATION METHOD:**

Course work participation	=	23.0%
Exam 1	=	23.5%
Exam 2	=	23.5%
Final Exam	=	30.0%
	=	<u>100%</u>

### **CONFIDENTIALITY:**

All students' e-mail addresses may be available to other students in the class. Although some assignments in an online course may encourage or require peer communication, the instructor will make every effort to protect the confidentiality of any personal communication (for example, grades). However, you should recognize that e-mail and other electronic media are not secure; there is no guarantee of the privacy of your e-mail or other personal information.

### **APPROPRIATE ONLINE BEHAVIOR:**

The use of Spartanburg Community College's website, e-mail service or course management software for creation and/or distribution of material not pertaining to course participation is prohibited and is grounds for dismissal according to College policy under "disruptive behavior." Such actions, include, but are not limited to:

- Inappropriate use of email and discussion boards for:
  - ✓ Harassment
  - ✓ Unlawful solicitation
  - ✓ "Spamming"
  - ✓ "Flaming"
- Use of online editing tools within the course management software to:
  - ✓ Create offensive material
  - ✓ Link to inappropriate materials

### **ATTENDANCE POLICY:**

An electronic e-mail is required from each student to the instructor by the end of the drop/add period. At this time the Instructor will drop the student from the course if it is not received.

Instructors maintain attendance records. However, it is the student's responsibility to withdraw from a course. A student who stops attending the online class and fails to initiate a withdrawal will remain on the class roster. *With this in mind, for every assignment, test or exam not completed while still enrolled in the course the student will receive a grade of zero and the final course grade will be calculated accordingly.*

Withdrawal Policy: During the first 75% of the course, a student may initiate withdrawal and receive a grade of W. A student cannot initiate a withdrawal during the last 25% of the course. Extenuating circumstances require documentation and approval by the appropriate department head and academic dean.

**ACADEMIC  
CONDUCT:**

**ACADEMIC DISHONESTY:** Students are expected to uphold the integrity of the College's standard of conduct, specifically in regards to academic honesty. All forms of academic dishonesty including, but not limited to, cheating on assignments/tests, plagiarism, collusion, and falsification of information will call for disciplinary action. Disciplinary action imposed may include one or more of the following: written reprimand, loss of credit for assignment/test, termination from course, and probation, suspension, or expulsion from the College. For further explanation of this and other conduct codes, please refer to the Student Handbook.

**CLASS/LAB  
PROCEDURES:**

See Course Instructions.

**ACCOMMODATIONS:**

Students who need special accommodations in this class because of a documented disability should notify Student Disability Services by calling (864) 592-4818, toll-free 1-800-922-3679; via email through the SCC web site at [www.sccsc.edu/resources/disabilities](http://www.sccsc.edu/resources/disabilities); or by visiting the office located in the East Building Room 30-B on the SCC Central campus. Contacting Student Disability Services early in the semester gives the College an opportunity to provide necessary support services and appropriate accommodations.

**The Learning Center**, located in the rooms E-2 & E-5 of the East Building, provides computers for your use. Check the website <http://www.sccsc.edu/resources/tutoring/tlc> or call 592-4968 for current semester operating hours.

**Program Department Chair**

Marcia Schenck

592-4839

[schenckm@sccsc.edu](mailto:schenckm@sccsc.edu)

**COURSE**  
**COMPETENCIES &**  
**OBJECTIVES:**

Upon satisfactory completion of this course, the student will be able to:

- I. Define information security.
  1. Describe the challenges of securing information.
  2. List 3 different information security careers.
  
- II. Describe security threats.
  1. Identify the types of attackers that are common today.
  2. List the basic steps of an attack.
  3. List the 5 steps in a defense.
  4. Describe 3 different types of software-based attacks.
  5. List 3 types of hardware attacks.
  6. Define virtualization and explain how attackers are targeting virtual systems.
  
- III. List ways to protect information.
  1. Describe how to harden operating systems...
  2. List ways to prevent attacks through Web browsers.
  3. Describe various software security applications.
  
- IV. Explain types of network vulnerabilities.
  1. List categories of network attacks.
  
- V. List network defenses.
  1. Define network address translation and network access control.
  2. List 3 different types of network security devices and explain how they can be used.
  
- VI. Describe the basic IEEE 802.11 wireless security protections.
  1. Define vulnerabilities of open system authentication and WEP.
  2. Describe WPS and WPA2 personal security models.
  
- VII. Define access control.
  1. List the four access control models.
  2. Explain different types of physical access control.
  
- VIII. Define authentication.
  1. Describe authentication credentials.
  2. List authentication models.
  3. Explain how a Virtual Private Network works.

- IX. Define basic cryptography.
  - 1. Define hashing.
  - 2. Differentiate between symmetric and asymmetric cryptography.
  - 3. Explain how whole disk encryption works.
  
- X. List types of organizational security policies.
  - 1. Describe how education and training can limit the impact of social engineering.