



UNIVERSITY OF  
SOUTH FLORIDA  

---

SARASOTA-MANATEE

# **Program in Information Technology**

## **CIS 3360**

# **Principles of Information Security**

**Fall 2011  
3 Credit Hours**

*University of South Florida – Sarasota/Manatee*  
8350 N. Tamiami Trail, SMC-C263; Sarasota, FL 34243-2025  
Telephone: 941-359-4200 Fax: 941-359-4367

**University of South Florida - Sarasota/Manatee  
Course Syllabus - Fall 2011**

|                                |  |
|--------------------------------|--|
| <b>Course Number:</b>          | CIS3360  |
| <b>Classroom:</b>              | Every Tuesday 6:00 pm - 8:50 pm<br>The class is completely online via Elluminate. If we have students with compelling needs for a physical classroom and face-to-face interactions, a room will be identified for them. The rest of the students can continue to be online.  |
| <b>Course Name:</b>            | <b>Principle of Information Security</b>   |
| <b>Learning Outcome:</b>       | This course provides a broad review of the entire field of Information Security, background on many related elements, at quite a bit of detail, and hands-on exercises to facilitate an understanding of the topic as a whole. The course covers the terminology of the field, the history of the discipline, and an overview of how to manage an information security program.  |
| <b>Instructor:</b>             | Dr. Sunita Lodwig  |
| <b>Office:</b>                 | C266 at the SM campus<br><b>e-mail:</b> <a href="mailto:slodwig@sar.usf.edu">slodwig@sar.usf.edu</a> Phone: 941-966-1260   |
| <b>Office Hours:</b>           | By appointment! We can meet face-to-face at school in my office, or we can meet in my virtual office via Elluminate.<br><b>Best way to contact me is via email. Please send course-related email from BlackBoard only. I receive close to a 100 messages a day, and it is very easy for important emails to get buried. Email from BlackBoard is flagged by Course Number and is easier to spot and respond to. In case you need to reach me very quickly, my home phone number is 941-966-1260.</b> |
| <b>Required Materials:</b>     | Michael E. Whitman and Herbert J. Mattord, <i>Principles of Information Security, 4<sup>th</sup> edition</i> . Thomson Course Technology, ISBN-13:978-1-4239-0177-8, ISBN-10: 1-4239-0177-0  |
| <b>Supplemental Materials:</b> | <a href="http://www.informationsecurity.techtarget.com">www.informationsecurity.techtarget.com</a><br><a href="http://www.sans.org/rr">www.sans.org/rr</a><br><a href="http://www.ftc.gov/infosecurity">www.ftc.gov/infosecurity</a><br><a href="http://www.issa.org">www.issa.org</a><br>The course requires students to use the internet extensively for investigative purposes as well as some lab exercises - <b>several other web-sites will be shared in class.</b>                            |
| <b>Prerequisites:</b>          | Admission to Program   |
| <b>Attendance Policy:</b>      | Class attendance is optional. However, the course moves through the material at a rapid pace, and each topic builds  |

|  |  |                           |     |                            |     |                                   |            |              |             |
|--|--|---------------------------|-----|----------------------------|-----|-----------------------------------|------------|--------------|-------------|
|  | <p>on the ones that preceded it. Catching up is difficult, and attempting to “cram” the material will surely lead to failure to adequately grasp it.</p> <p>Therefore, students are responsible for their class attendance, online or offline, and are <b>strongly advised that falling behind will affect their grades</b> (see Performance Evaluation and Grading).</p>  |                           |     |                            |     |                                   |            |              |             |
| <b>Religious Observances:</b>              | Students who anticipate being absent from class due to the observation of major religious holidays can do so after providing written notice of the date(s) to the instructor by the second class meeting.  |                           |     |                            |     |                                   |            |              |             |
| <b>Disabilities Accommodation:</b>         | Students are responsible for registering with the Office of Students with Disabilities Services (SDS) in order to receive academic accommodations. Reasonable notice must be given to the SDS office (typically 5 working days) for accommodations to be arranged. It is the responsibility of the student to provide each instructor with a copy of the official Memo of Accommodation. Contact Information: Pat Lakey, Coordinator, 941-359-4714, <a href="mailto:plakey@sar.usf.edu">plakey@sar.usf.edu</a> , <a href="http://www.sarasota.usf.edu/Students/Disability/">www.sarasota.usf.edu/Students/Disability/</a>  |                           |     |                            |     |                                   |            |              |             |
| <b>Performance Evaluation and Grading:</b> | <p>Student performance will be evaluated based on class participation (either in-class or via the Discussion Board), two exams, lab exercises (virtual), and assignments.</p> <p>Late assignments will be accepted but only upto a point. Once an assignment has been discussed in class, it will no longer be accepted. Also, please note, late assignments will be penalized by a loss of 5 points (could be as much as 25% of the grade).</p> <p>The relative weights for each of these components in determining the final grade are as follows:</p> <table style="margin-left: 40px;"> <tr> <td>Exercises and Assignments</td> <td style="text-align: right;">60%</td> </tr> <tr> <td>2 Tests (mid-term &amp; Final)</td> <td style="text-align: right;">30%</td> </tr> <tr> <td>In-class and online participation</td> <td style="text-align: right;"><u>10%</u></td> </tr> <tr> <td><b>Total</b></td> <td style="text-align: right;"><u>100%</u></td> </tr> </table> <p>A grade will be determined based on the total of possible points earned, as follows: A 90-100; B 80-89; C 70-79; D 60-69; F 0-59.</p> | Exercises and Assignments | 60% | 2 Tests (mid-term & Final) | 30% | In-class and online participation | <u>10%</u> | <b>Total</b> | <u>100%</u> |
| Exercises and Assignments                  | 60%  |                           |     |                            |     |                                   |            |              |             |
| 2 Tests (mid-term & Final)                 | 30%  |                           |     |                            |     |                                   |            |              |             |
| In-class and online participation          | <u>10%</u>   |                           |     |                            |     |                                   |            |              |             |
| <b>Total</b>                               | <u>100%</u>  |                           |     |                            |     |                                   |            |              |             |
| <b>Important Date</b>                      | <b>Last day to Withdraw from Course: October 29.</b>   |                           |     |                            |     |                                   |            |              |             |

## COURSE OBJECTIVES

The goals for this course are:

- This course is structured to follow a model called the Security Systems Development Life cycle (or SecSDLC), a methodology that can be used to implement information security in an organization that has little or no formal information security in place.

This structure provides a theme that will guide students through an examination of the various components of the vast number of information domains of information security.

On completion of this course students will be able to:

- Describe the broader field of information security by defining key terms and essential concepts.
- Explain the business drivers that are propelling the increased interest in information security.
- Discuss the various threats facing organization and the process of prioritizing them for the security planning process.
- Outline the current legislation, regulation, and common ethical expectations that constrain an organization's options.
- Explain how to conduct an initial risk assessment with regard to security mechanisms in place and policies and procedures.
- State best business practices and standards of due care and diligence as inputs to the development of security policy including the major components, scope and target audience for each of the levels of the policy.
- Describe the planning process that supports business continuity, disaster recovery, and incident response, including when to involve outside law enforcement agencies.
- Explain the perspective on the configuration and use of technologies designed to segregate the organization from the insecure Internet.
- State the various definitions and categorizations of firewall technologies and the architectures under which firewalls may be deployed.
- Explain the concept of intrusions and the technologies needed to prevent, detect, react, and recover from such intrusions.
- Discuss the role of asymmetric systems as the foundation of Public Key Encryption systems.
- Describe the cryptography-based protocols used in secure communications (SHTTP, SMIME, SET, SSH)
- State the elements critical to successful implementation of an information security program.

### **White Hat Oath and Agreement**

Along with this syllabus is an Ethics Statement known as the White Hat Oath (available on Blackboard). Please study this document and be prepared to sign the Agreement. The Agreement states that you will not use the information learned to perform unauthorized examinations of systems and information both inside and outside the University. You must sign this agreement in order to participate in the laboratory portion of this course.

## COURSE DESCRIPTION AND SCHEDULE

| <u>Week #/Start Date</u>  | <u>Topic</u>                                       | <u>Lab Work/Due Date</u>  |
|---|--|---|
| Wk 1 - Aug 21   | Chapter 1 - Introduction to Information Security   |   |
| <b>Security Investigation Phase</b>   |  |   |
| Wk 2 - Aug 28   | Chapter 2 - The need for security                  | Chap 1 homework   |
| Wk 3 - Sep 4  | Chapter 3 - Legal, Ethical and Professional Issues | Chap 2 homework   |
| <b>Security Analysis and Planning - Risk Management</b>                     |  |   |
| Wk 4 - Sep 11   | Chapter 4 - Risk Management                        | Chap 3 homework<br>Lab Ex. - Footprinting                           |
| Wk 5 - Sep 18   | Chapter 5 - Planning for Security                  | Chap 4 homework   |
| Wk 6 - Sep 25   | <b>TEST (based on Ch 1 - 5)</b>                    |   |
| <b>Security Technology</b>  |  |   |
| Wk 7 - Oct 2  | Chapter 6 - Firewalls and VPNs                     | Chap 5 homework<br>Lab Ex. - Scanning & Enumeration                 |
| Wk 8 - Oct 9  | Chapter 7 - Security Tools                         | Chap 6 homework   |
| Wk 9 - Oct 16   | Chapter 8 - Cryptography                           | Chap 7 homework<br>Lab Ex. - OS Vulnerabilities & Resolutions       |
| Wk 10 - Oct 23  | Chapter 9 - Physical Security                      | Chap 8 homework   |
| <b>October 29</b>   | <b>Last day to Withdraw from Course</b>            |   |
| Wk 11 - Oct 30  | Chapter 10 - Implementing Security                 | Chap 9 homework<br>Lab Ex. - Network Security Tools & Technologies  |
| Wk 12 - Nov 6   | <b>Veteran's Day - November 11th</b>               |   |
| Wk 13 - Nov 13  | Chapter 11 - Security and Personnel                | Chap 10 homework  |
| <b>Week 14 - Thanksgiving (we will use the class this week to catch up)</b> |  |   |
| Wk 15 - Nov 27  | Chapter 12 - Maintenance                           | Chap 11 homework<br>Lab Ex. - File System Security and Cryptography |
| Wk 16 - Dec 4   | <b>FINAL</b>                                       | Chap12 homework   |

**Note: The above schedule is a tentative one - there could be some shifting depending on how fast or slow things progress during the semester. Also note the lab exercises could change over the semester.**

## INSTRUCTIONAL METHODOLOGY AND GRADING POLICY

**Instructional Methodology:** The Blackboard on-line course tools package, which may be accessed from campus computer labs and via the Internet at <https://my.usf.edu>, will be used to enhance the course. All that is required is Internet access and a reasonably up-to-date web browser. Except for response speed, there should be no difference in functionality between accessing from a lab and from home. Any exceptions to this will be announced as they become apparent. If you are new to Blackboard, please review the Blackboard tutorials at:

[www.sarasota.usf.edu/CampusComputing/Documents/CC\\_Student\\_Resources.php](http://www.sarasota.usf.edu/CampusComputing/Documents/CC_Student_Resources.php)

If you need technical assistance with Blackboard, the following two modes of help are available:

- o Toll-free Helpline: 866-974-1222
- o Live online help: <http://usfsupport.custhelp.com/cgi-bin/usfsupport.cfg/php/enduser/chat.php>

**Grading Policy:** Your grade in this course will depend on the following:

Student and instructor presentations, demonstrations, discussions, and hands-on use of computers to complete exercises and assignments based on the Laboratory Manual which accompanies the required text book. Students will also be expected to access web sites focused on security issues (e.g., U.S Government, NASA, DOD, Homeland Security,....) to research current issues, then report back to the class on their findings.

**Two exams.** Both exams are worth ~30% of your grade. The exams are not cumulative - each covers only the topics indicated, although an understanding of earlier material may be a practical necessity for understanding and solving problems on new material. There will be no makeup exams!

**Quizzes & assignments** will be required regularly. You should submit all work on time. Tardiness in submission will be penalized (and, as announced for some assignments, not permitted). These will be worth a total of 60% of your grade. As assignments and quizzes will occur as we complete corresponding topics in the course, and how quickly we cover those topics can vary, dates for these assessments cannot be given in advance.

**Assignments' Presentations:** Researching information and developing presentation skills are important for everyone, and it's a good way to share information. **Each student will research, prepare, and present at least two individual presentations (extra points for these).** The individual presentations must include at least two outside references that are documented in footnotes and a reference page. Students should turn in a copy of their presentation notes, including a bibliography, or include the information in their visuals.

Presentations will be evaluated on content, delivery, and audience response.

**Participation in class/on-line discussions** constitutes 10% of your grade. You are expected to frequently review the Blackboard discussion function and take part in discussions of assigned topics. It is anticipated that there will be several discussion topics during the course, with announced (and possibly overlapping) participation timeframes. Participation that occurs after the closing participation date for a topic will not be counted for credit!

**Class Attendance:** As mentioned earlier, class attendance is optional. However, it is my observation that final course grades tend to be positively correlated with regular class attendance, even in the absence of any credit for attendance, because understanding of the material is best gained through a combination of exposures to the material, of which course lecture is an important one. In any event, you are responsible for the material covered in class, any announcements, schedule changes, etc. Absenteeism is not an excuse for late work or missed exams unless approval from your instructor is

obtained in advance.

**Incomplete Grade:** An Incomplete grade in the course is reserved for those with **good reason** for having missed a **little bit** of the work, and a completion plan agreed to by the student and instructor during the course, as circumstances require. Otherwise, exams not taken or assignments not turned in will receive a zero for that grade, and the course grade assigned accordingly.

### STATEMENT ON ACADEMIC HONESTY

The instructor of this course trusts that all students behave in strict compliance with accepted standards of academic honesty. A conscious effort is made to ensure that grading standards are fair, and that anyone who makes an honest and consistent attempt to do well in the course will succeed, as, by this time in your degree program, it is expected that you are capable of doing the work. There will be no tolerance for anyone who attempts to "succeed" by dishonest routes.

Academic honesty includes, but is not limited to:

- Honesty in taking examinations - all exams are to be taken on an individual basis.
- Honesty in completing your assignments yourself or with your team member, as the case may be. There is no objection to some degree of helpful collaboration in completion of assignments; often a rough spot can be overcome with a helpful word. But assignments passed in for grading must be substantially one person's - the submitter's - work. Please note that in many of the assignments for this course, it will be fairly obvious to the instructor when students have collaborated beyond a reasonable degree (having exactly the same wrong answer, for example, is usually a dead giveaway).
- Honesty in attributing others' work. In all submitted work, including papers and presentations, ideas, concepts and quotations obtained from other persons' works must be properly attributed. Not doing so constitutes theft of intellectual property.
- Consequences for violating this trust will be severe. Credit will not be given for any work that does not meet the above criteria. In an extreme violation or repeated violations, a failing grade in the course for reasons of academic dishonesty is an appropriate and reasonable penalty.

**Academic Dishonesty:** In accordance with university guidelines as found in the Student Handbook, anyone found cheating during exams, submitting work that is not theirs, plagiarizing or falsifying work that is submitted to represent work they have done shall receive an "F" with numerical value of zero on the item submitted, and the "F" shall be used to determine the final course grade. It is the option of the instructor to assign the student a grade of "F" or "FF" (the latter indicating dishonest) in the course.

- The instructor may use the "Turnitin.com" software to access potential plagiarism and precise obligation to reference all materials taken from electronic sources.
- **Academic Disruption:**  
The University does not tolerate behavior that disrupts the learning process. The policy for addressing academic disruption is included with Academic Dishonesty in the catalog: [www.ugs.usf.edu/catalogs/0607/adadap.htm](http://www.ugs.usf.edu/catalogs/0607/adadap.htm). The consequences to the student can range from an administrative reprimand to suspension from USF.

# EMERGENCY PROCEDURES

In the event of an emergency, it may be necessary for USF to suspend normal operations. During this time, USF may opt to continue delivery of instruction through methods that include but are not limited to: Blackboard, Elluminate, Skype, and email messaging and/or an alternate schedule. It's the responsibility of the student to monitor Blackboard site for each class for course specific communication, and the main USF, College, and department websites, emails, and MoBull messages for important general information. More details are given below.

## Emergency Preparedness

It is strongly recommended that you become familiar with the USF Sarasota-Manatee Emergency Action Plan <http://www.sarasota.usf.edu/Alpha/ready/EAP.pdf> and of the Safety Preparedness site <http://www.sarasota.usf.edu/Alpha/ready/index.html>

- **1 (800) Hotline:** The USF hotline at 1 (800) 992-4231 is updated with pre-recorded information during an emergency. The hotline can also be operated by staff during an emergency if the situation necessitates that additional information, direction or resources need to be communicated and the personnel can be put in place in advance, such as in the event of a hurricane or ongoing emergency
- **Fire Alarm Instructions:**  
At the beginning of each semester please note the emergency exit maps posted in each classroom. These signs are marked with the primary evacuation route (red) and secondary evacuation route (orange) in case the building needs to be evacuated.  
Emergency Evacuation Procedures: [http://www.sarasota.usf.edu/Alpha/ready/EAP\\_FAQ.pdf](http://www.sarasota.usf.edu/Alpha/ready/EAP_FAQ.pdf)
- **Contingency Plans**  
The University requires professors to have a contingency plan for continuing course instruction, if possible, in the event of continued natural disruption (e.g., significant hurricane damage to the area or a pandemic affecting the area). Since all courses at USFSM are supported by Blackboard, the most feasible plan would be to move instruction more completely online. Also, advisable would be a plan to extend deadlines as appropriate.  
[http://sarasota.usf.edu/Academics/AcadAffairs/Handbook/USFSM\\_FH\\_EmergencyGuidelinesAcademicContinuity.pdf](http://sarasota.usf.edu/Academics/AcadAffairs/Handbook/USFSM_FH_EmergencyGuidelinesAcademicContinuity.pdf)