

Oklahoma State University Institute of Technology
Face to Face Syllabus
Spring 2018

ITD 1243 Principles of Information Security

Students explore the principles of cyber security, with an emphasis on current threats and vulnerabilities. Topics include infrastructure and operational security, cryptography, legal and ethical issues, and security policies, practices and procedures.

Type of course: Theory/Lab

Credit Hours: 3;

Total hours of theory per semester: 30

Total hours of lab for the semester: 45

Class length - Full Semester

Class days and times:

Monday	Tuesday	Wednesday	Thursday	Friday
Does not meet	9:30 a.m. to 11:45 a.m.	Does not meet	9:30 a.m. to 11:45 a.m.	Does not meet

- Or -

Monday	Tuesday	Wednesday	Thursday	Friday
12:30 p.m. to 2:45 p.m.	Does not meet	12:30 p.m. to 2:45 p.m.	Does not meet	Does not meet

Prerequisites: None

Instructor Name: Howard Licht

Instructor Phone: (918) 293-4786

Office: ET/IT 15B

Instructor email: licht@okstate.edu

Contact: The preferred method of contact is email. Please allow 24-48 hours to return correspondence during the normal work week.

Instructor's Office Hours:

Monday	Tuesday	Wednesday	Thursday	Friday
9:00 a.m. to 11:30 a.m.	12:30 p.m. to 3:30 p.m.	9:00 a.m. to 11:30 a.m.	12:30 p.m. to 3:30 p.m.	By appointment Only

Other times available by appointment

School Name:
Information Technologies

School Phone:
(918) 293-5440

REQUIRED TEXT, REFERENCES, AND MATERIALS

Texts:

Principles of Information Security, Sixth Edition , Michael E. Whitman and Herbert J. Mattord, Cengage Course Technology

ISBN-13:978-1-337-68575-7

References:

Online Classroom

Materials:

Portable Drive/USB Drive, pencil(s), notebook paper

Access to a computer with broadband Internet Access (2Mbps upload preferred)

Uniform/Tools:

none

Estimated Cost for Text:	\$174
Estimated Cost for Materials:	\$20
Estimated Cost for Uniform/Tools:	\$0
Total Estimated Cost	\$194

Upon completion of the course, students should:

COURSE OBJECTIVES		ASSESSMENT OF OBJECTIVE
E.1	evaluate and document IT security risks and make recommendations for mitigation	Projects Ch 2, 4, 6, 7, 8, 9
E.2	list or describe the applicable laws or policies related to information systems and describe the major components of each pertaining to the storage or transmission of data	Projects Ch 1, 3
L.2	create or assess a comprehensive security plan, set of policies or procedures to protect the IT assets of an organization	Projects Ch 5, 12 & Final Project
N.1	determine the scope, time, or cost goals for a specific project	Projects Ch 5, 10 , 11, 12 & Final Project

*Aspects of the competency assessments may be used in the university's assessment of student learning.

COURSE ACTIVITIES

In this course students will:

- Apply problem-solving skills to problems
- Install and manage Microsoft Windows patches and updates
- Explore digital certificates and their capabilities
- Perform a backup in Microsoft Windows
- Configure Microsoft Windows firewall
- Perform security hardening techniques in Microsoft Internet Explorer
- Develop a security baseline report of a computer

- Use software to assess system vulnerabilities
- Participate in class discussions and class activities
- Take examinations and quizzes

EVALUATION - GRADES WILL BE BASED ON THE QUALITY AND COMPLETION OF THESE TASKS:

Final Grade Calculation	
Assignments, Lab, Projects, Class Activities	40%
Exams	25%
Class Project	15%
Final Exam*	10%
Professional Development**	5%
Course Portfolio	5%
Total	100%

OSUIT Grading Scale
A = 90-100
B = 80-89.99
C = 70-79.99
D = 60-69.99
F = 59.99 & below

*The student's grade for this assignment will be used in the university's assessment of student learning. A 70% competency or higher receives a Pass rating. This Pass/Fail rating is independent of the student's course grade.

** Information Technologies students are expected to participate in professional development activities as defined in the supplemental professional development activity guidelines in the online classroom.

RECOMMENDED STUDENT COMPETENCIES/SKILLS

Students enrolled for Principles of Information Security should have the following competencies/skills in order to participate successfully: (List is not all-inclusive)

- Basic typing skills
- Knowledge of basic computer functions including the ability to load/start software applications
- Ability to use a simple text editor and save text files in various formats/extensions
- Capability to screen-capture ([ALT]-[PrtScn]) and copy/paste to a Word® document
- Understanding of onscreen folder systems and the ability to create/organize/navigate among folders
- Familiarity with different browser types
- Working knowledge of how to zip/unzip files for bulk submission

INTERACTION WITH INSTRUCTOR

In addition to office hours (as indicated on the first page of this syllabus), students can also expect the instructor to provide:

- input to class discussion
- additional information and updates about the course as needed through e-mails and the News feature in the Online Classroom (D2L)
- detailed analysis, feedback and explanation of grades according to the following schedule

Daily and/or weekly quizzes, small weekly assignments and similar type projects:
Normal return time to students is about one (1) week.

Extensive assignments, large lab projects, extensive quizzes, exams and similar type projects: Normal return time to students in about one (1) to two (2) weeks.

Students may contact the instructor by email at any time with questions or concerns about their course; however, student should allow 24-48 hours to receive a reply to their correspondence on weekdays. The instructor may not be available to respond to correspondence on the weekend, so it is advisable that student not leave coursework until the last possible moment in case they need assistance.

AUTHORIZED TOOLS

Students may use any/all course materials, including books and notes, while participating in classroom activities with the exception of-class exams. All quizzes, exams, and written assignments are to be completed independently; no collaboration with classmates is permitted and any instance of such will be considered academic dishonesty.

LATE WORK POLICY

Assignments must be completed and submitted on time. Absence or personal problems will not be considered an excuse for submitting assignments late. Late assignments are accepted only at the instructor's discretion and an adjustment may be assessed to the grade. Class demonstrations, workshops and/or training sessions will not be repeated. If a student is to be absent, it is the student's responsibility to make sure the work is submitted by the due date and time. To meet course competencies, students will be required to complete all assignments and course work.

TESTING

Exams:

Regular exams may include any combination of multiple choice, matching, true/false, fill in the blank, completion, hands on projects, programming assignments, essay and/or short answer questions. Exams may be taken early at the discretion of the instructor. Exams may not be taken late unless there is an accepted, excused, and documented absence.

Exams will be given on the date and time set by the instructor. Make-up exams will not be given without proper documentation. Make-up exams will only be given at times arranged with the instructor.

UNIVERSITY & COURSE EXPECTATIONS

As a student of OSUIT, a student should understand that it is their responsibility to read, abide by and maintain a copy of the syllabi for this course. Syllabi are also available on the OSUIT website.

As a student of OSUIT, a student should understand that excerpts of portions of their work may be utilized for institutional assessment purposes. The purpose of institutional assessment is for verification of student learning and program improvement. The student should recognize that every effort will be made to keep this information confidential.

AMERICANS WITH DISABILITIES ACT (ADA)

According to the Americans with Disabilities Act, each student with a disability is responsible for notifying the University of his/her disability and requesting accommodations. If you think you have a qualified disability and need special accommodations, you should notify the instructor and request verification of eligibility for accommodations from the Office of Academic Accommodations/LASSO Center. Please advise the instructor of your disability as soon as possible, and contact The LASSO Center, to ensure timely implementation of appropriate accommodations. Faculty have an obligation to respond when they receive official notice of a disability but are under no obligation to provide retroactive accommodations. To receive services, you must submit appropriate documentation and complete an intake process during which the existence of a qualified disability is verified and reasonable accommodations are identified. The LASSO Center is located on the 3rd floor of the Noble Center. You may call [918.293.4855](tel:918.293.4855) for more information or fax documentation to [918.293.4853](tel:918.293.4853).

ACADEMIC DISHONESTY

Academic dishonesty or misconduct is neither condoned nor tolerated at OSUIT. Any student found guilty of academic dishonesty or misconduct shall be subject to disciplinary action. Academic dishonesty or academic misconduct includes, but is not limited to, the following actions:

- (1) Plagiarism: the representation of previously written, published, or creative work as one's own
- (2) Unauthorized collaboration on projects
- (3) Cheating on examinations
- (4) Unauthorized advance access to exams
- (5) Fraudulent alteration of academic materials
- (6) Knowing cooperation with another person in an academically dishonest undertaking.

Students are required to actively protect their work against misuse by others. For details, refer to The OSUIT Student Handbook (Student Rights and Responsibilities Governing Student Behavior) available online at:

http://www.osuit.edu/academics/forms/student_rights_responsibility.pdf.

ATTENDANCE POLICY FOR FACE TO FACE COURSES

A primary component of OSUIT's Mission is "to prepare and sustain a diverse student body as competitive members of a world-class workforce." Regular and consistent attendance not only aids in academic success, dependable attendance is a requirement in today's real-world employment; therefore, regular and consistent attendance is a requirement in all OSUIT courses.

Definitions: Absent: Failing to attend all or a significant portion of a class or lab session.

- A. Students may not be marked as absent if missing class for situations such as, but not limited to
1. participating in a required university activity such as a field trip;
 2. fulfilling a military obligation;
 3. a mandatory court appearance;
 4. death in the immediate family;
 5. extreme illness or accident to oneself or immediate family. Instructors, at their discretion, may require proof of such events.
- B. It is the responsibility of the student to contact and inform the instructor and/or department in advance of such excused absences whenever possible.
- Tardy: Arriving late to class as defined by the individual class instructor. Faculty, at their discretion, may equate three tardies to equal one absence.

Procedures:

Early Intervention

- A. Any student who misses 10% of an individual course (or earlier at faculty discretion) during a regular fifteen-week semester, or the equivalent portion of time in a shorter session, will have their name submitted by that course instructor to the OSUIT Early Alert System for retention intervention.
- B. At the point the Early Alert is issued, the student *must* meet with their assigned faculty advisor or designated faculty/staff member within seven (7) academic calendar days for counseling on how to improve their attendance and academic success.

Excessive Absences

- A. The University reserves the right to administratively withdraw any student from an individual course who misses 20% of that course, whether excused or unexcused, and, in the opinion of the instructor, the student does not have a reasonable opportunity to be successful in the course.
- B. Students should be aware any of the following may impact their financial aid:
1. being administratively withdrawn from a course
 2. dropping a course
 3. their last date of attendance in a course

Please see OSUIT Policy 2-021 for full details and procedures.

COURSE PORTFOLIO

Each student is required to keep a portfolio of all work in the course. The portfolio is used for reference to help a student in case questions arise and with all other classes that the student will take in this school. The portfolio will be kept electronically and an electronic folder structure template will be provided to help organize the portfolio. This compilation will be submitted at the end of semester in the portfolio area on the online classroom. There may be at least one assignment during the semester based on the portfolio. All information will be placed into the portfolio template following the instructions given by the instructor on the course companion site.

ASSIGNMENT SUBMISSION

Assignments, labs, projects and written work for the course will utilize the Drop box submission process in Online Classroom. Before submission, a student should ensure the assignment has the correct heading (assignment template) and that the assignment is being submitted on or before the due date. The instructor may request an additional hard copy of assignments throughout the term. A hard copy of the assignment does not replace the need to submit the assignment to the appropriate drop box in the Online Classroom unless specifically stated by the instructor.

It is the responsibility of the student to ensure that work submitted to the Drop box was received and is accessible. Assignments may require research. Research is considered “a search for the truth”. Until the correct information is found your search is incomplete. In order to complete the chapter study guides and course assignments, you may have to conduct searches outside of the course curriculum materials. It is important for this course to note that no one source can provide all the information needed to complete assignments. Multiple sources from those provided in class can help to build your ability to find answers and complete assignments, labs and projects. Be prepared to provide evidence of your searches to the instructor.

When work is submitted to the drop box, the file name needs to follow this naming convention.
<Student’s first name><Student’s Last name><Original Assignment File Name>

For example, if student John Smith was submitting his assignment with the original file name of HomeworkAssignment02.docx then his filename of his submitted file should be:

JohnSmithHomeworkAssignment02.docx

Homework and In-Class Activities: Students may submit work anytime up to the due date and time to the appropriate Online Classroom drop boxes. All homework submitted by 11:59PM on the day the homework is due is considered to be on time.

No homework is accepted late. The only exceptions are the same that you will encounter in the workforce. These are listed in the policy on absences in this document. Appropriate documentation may be required for all activities. If an exception is allowed per stated policy, the student will be informed and the homework must be turned into the instructor by the allowed due date.

All work should be type written with a 12 point Times New Roman font. Double spacing is not required although may be best for some sections of assignments. Any handwritten assignments accepted must be readable by the instructor. Excessively small, sloppy, or otherwise unreadable written assignments may not earn credit.

Each assignment must be written appropriately for industry standards. Industry requirements include proper spelling and grammar use in reports. The proper use of grammar and spelling assists in the communication of information as a technician to customers, clients, and supervisors. Each assignment and lab report should include the appropriate and proper use of grammar, punctuation, and spelling. The grading criterion for every assignment and lab report includes grammar, punctuation, and spelling.

Each assignment must contain a heading. Headings for assignments in this course include your name, due date, course ID, and instructor name. This heading is used for both electronic and hard copy work. Failure to use the correct heading will result in a reduction of points from the final assessment score of the assignment. Assignments submitted with no name will not be graded.

This is the heading table template.

Course Name	ITD 1243 – Principles Of Information Security
Instructor	Howard Licht
Student Name	<i>student name here</i>
Due date	<i>assignment due date here</i>
Grade	<i>grade earned here</i>
Grading Comments	<i>instructor comments here</i>

Replace the material tags (stuff in **bold** and *italics*) with the appropriate information

OTHER LAB AND CLASSROOM POLICIES

Proper Safety Procedures: Information Technologies courses may require students to enter labs where tools and equipment are being used. As a result, students must dress and use safety equipment appropriate to the setting they are in. If students do not understand proper safety procedures, they must ask an instructor for assistance. In addition, students must ask for permission to use any equipment or facilities in advance.

Children in Class Policy: Only in extreme cases--where no other arrangements can be made for childcare and with **prior instructor approval**--will children be allowed in classrooms or laboratories. In such instances, children must be supervised at all times by a parent or guardian. If this becomes frequent, if the child or equipment is at risk of harm, or if this situation causes a distraction to other students and the learning environment, the instructor or lab assistant will ask the student to leave with the child.

The *Proper Safety Procedures* and the *Children in the Class Policy* applies when a student is on campus using the campus facilities in the pursuit of the class requirements.

Drops and Withdrawals: Students are strongly advised to meet with their instructors to discuss possible alternatives before deciding to drop a course or withdraw from school. Students must meet with the Division Chair to initiate drops and withdrawals. Due to federal requirements and guidelines for Student Financial Aid, students are advised to consult a representative from Student Financial Services in addition to the School Chair prior to dropping a class or withdrawing from the University. Students have the responsibility of processing drops and withdrawals. Note: Most failing grades result when students cease attending class, but do not take the steps necessary to preserve their academic standing.

Standard Policies and Procedures: Each student is responsible for being aware of the information contained in the OSU Institute of Technology Catalog, on-line Student Handbook, and semester Class Schedule. Policies and procedures not addressed in this document will follow the on-line Student Handbook, the Students' Rights and Responsibilities, and the OSU Institute of Technology Policy and Procedures Manual. Policies not addressing the documents identified above will follow those provided by the State Regents' of Oklahoma and A&M Colleges. Policies and procedures not addressed in the standard manual will follow the policies of the federal, state and local governmental (or professional) organizations, which issued them.

Course Outline Modification: Instructors reserve the right to change or modify course content during an academic term. Any changes will be shared with students in writing or posted in the online classroom.

COMPUTER LAB USER GUIDELINES

The primary purpose of the computer labs is to support the educational process. Therefore, priority of use will be given to the completion of assignments, exercises, and projects for academic courses. Inappropriate or illegal use of University resources may result in: the termination of access privileges, legal action or disciplinary review. Violation of this policy may constitute a criminal offense. In general, misconduct involving technology use—regardless of time or location—relates to the following:

- Destruction of equipment;
- Accessing or altering any form of technology communication without consent;
- Transmitting or receiving inappropriate information or graphics;
- Disruption of technology or classroom/lab operations.

Use of IT School computer labs and equipment must conform to campus IT policies available at http://www.osuit.edu/campus_community/cis—except where specifically allowed by School or instructor policies. In addition, students will be expected to abide by the following guidelines.

1. Be respectful of other users. Keep personal belongings out of the path of traffic.
2. Recreational use of computers during class is not permitted.
3. Rendering of images, sounds, language or messages that may be considered offensive by any other individual is unacceptable.
4. Modification of software and hardware are prohibited except with an instructor's guidance and approval.

The *Computer Lab User Guidelines* applies when a student is on campus using the campus facilities in the pursuit of the class requirements.

IT CAMPUS CLOSURE POLICY

In the event of occurrences (e.g., inclement weather) which require campus closure, students should log into the Online Classroom by the beginning of their regularly scheduled class times for instructions regarding the online sessions. Students unable to participate in the sessions are responsible for their content—which will be facilitated through the instructor's choice of online tools (e.g. BlackBoard Collaborate, Online Classroom Discussions, etc.).

Faculty will notify students prior in the event a session will not be held. If the faculty member does not login within the first 15 minutes of the scheduled class time, the session will be considered cancelled and arrangements will be made for making up the missed time. Courses not affected by campus closure will continue to operate as normal.

ONLINE CLASSROOM

The OSUIT Online Classroom will serve as the primary conduit for course information and deliverables. Therefore, students are responsible for checking it regularly. Unless otherwise directed, assignments must be submitted via the Online Classroom.

Course Schedule*

Chapter Exercises, Chapter Assignments, and Chapter Programming Labs are generally scheduled to be due on the last day during a given coverage period for the material. Exams are generally given at the end of a coverage period or immediately thereafter and are announced ahead of time.

Week(s)	Topics and Competencies	Assignment(s)
1	<p>Chapter 01 – Introduction to Information Security</p> <ul style="list-style-type: none"> • Define information security • Relate the history of computer security and how it evolved into information security • Define key terms and critical concepts of information security as presented in the unit • Discuss the phases of the security systems development life cycle • Present the roles of professionals involved in information security within an organization 	<p>Read Chapter 01</p> <ul style="list-style-type: none"> • Chapter Exercises and Projects • Chapter Exam • Weekly Current Events Activity
2	<p>Chapter 02 – The Need for Security</p> <ul style="list-style-type: none"> • Recognize that organizations have a business need for information security • Understand that a successful information security program is the responsibility of both an organization’s general management and IT management • Identify the threats posed to information security and the more common attacks associated with those threats, and differentiate threats to the information within systems from attacks against the information within systems • Describe the issues facing software developers, as well as the most common errors made by developers, and explain how software development programs can create software that is more secure and reliable 	<p>Read Chapter 02</p> <ul style="list-style-type: none"> • Chapter Exercises and Projects • Chapter Exam • Weekly Current Events Activity
3	<p>Chapter 03 – Legal, Ethical and Professional Issues in Information Security</p> <ul style="list-style-type: none"> • Use this chapter as a guide for future reference on laws, regulations, and professional organizations • Differentiate between laws and ethics • Identify major national laws that relate to the practice of information security • Understand the role of culture as it applies to ethics in information security 	<p>Review Chapter 03</p> <ul style="list-style-type: none"> • Chapter Exercises and Projects • Chapter Exam • Weekly Current Events Activity

Course Schedule*

Chapter Exercises, Chapter Assignments, and Chapter Programming Labs are generally scheduled to be due on the last day during a given coverage period for the material. Exams are generally given at the end of a coverage period or immediately thereafter and are announced ahead of time.

Week(s)	Topics and Competencies	Assignment(s)
4	<p>Chapter 04 – Planning for Security</p> <ul style="list-style-type: none"> • Define management’s role in the development, maintenance, and enforcement of information security policy, standards, practices, procedures, and guidelines • Describe what an information security blueprint is, what its major components are, and how it is used to support the information security program • Discuss how an organization institutionalizes its policies, standards, and practices using education, training, and awareness programs • Explain what contingency planning is and how incident response planning, disaster recovery planning, and business continuity plans are related to contingency planning 	<p>Review Chapter 04</p> <ul style="list-style-type: none"> • Chapter Exercises and Projects • Chapter Exam • Weekly Current Events Activity
5	<p>Chapter 05 – Risk Management</p> <ul style="list-style-type: none"> • Define risk management, risk identification, and risk control • Understand how risk is identified and assessed • Assess risk based on probability of occurrence and impact on an organization • Grasp the fundamental aspects of documenting risk through the creation of a risk assessment • Describe the risk mitigation strategy options for controlling risks • Identify the categories that can be used to classify controls • Recognize the conceptual frameworks that exist for evaluating risk controls and be able to formulate a cost benefit analysis • Understand how to maintain and perpetuate risk controls 	<p>Read Chapter 05</p> <ul style="list-style-type: none"> • Chapter Exercises and Projects • Chapter Exam • Weekly Current Events Activity

Course Schedule*

Chapter Exercises, Chapter Assignments, and Chapter Programming Labs are generally scheduled to be due on the last day during a given coverage period for the material. Exams are generally given at the end of a coverage period or immediately thereafter and are announced ahead of time.

Week(s)	Topics and Competencies	Assignment(s)
6	<p>Chapter 06 – Security Technology: Firewalls and VPNs</p> <ul style="list-style-type: none"> • Explain the role of physical design in the implementation of a comprehensive security program • Describe firewall technology and the various approaches to firewall implementation • Identify the various approaches to remote and dial-up access protection—that is, how these connection methods can be controlled to assure confidentiality of information, and the authentication and authorization of users • Explain content filtering technology • Describe the technology that enables the use of virtual private networks 	<p>Read Chapter 06</p> <ul style="list-style-type: none"> • Chapter Exercises and Projects • Chapter Exam • Weekly Current Events Activity
7	<p>Chapter 07 – Security Technology: Intrusion Detection, Access Control, and Other Security Tools</p> <ul style="list-style-type: none"> • Identify and describe the categories and operating models of intrusion detection systems • Identify and describe honey pots, honey nets, and padded cell systems • List and define the major categories of scanning and analysis tools, and describe the specific tools used within each of these categories • Explain the various methods of access control, including the use of biometric access mechanisms 	<p>Read Chapter 07</p> <ul style="list-style-type: none"> • Chapter Exercises and Projects • Chapter Exam • Weekly Current Events Activity
8	<p>Chapter 08 – Cryptography</p> <ul style="list-style-type: none"> • Chronicle the most significant events and discoveries in the history of cryptology • Explain the basic principles of cryptography • Describe the operating principles of the most popular tools in the area of cryptography • List and explicate the major protocols used for secure communications • Discuss the nature and execution of the dominant methods of attack used against cryptosystems 	<p>Review Chapter 08</p> <ul style="list-style-type: none"> • Chapter Exercises and Projects • Chapter Exam • Weekly Current Events Activity

Professional Development
Due: June 23, 2017

Course Schedule*

Chapter Exercises, Chapter Assignments, and Chapter Programming Labs are generally scheduled to be due on the last day during a given coverage period for the material. Exams are generally given at the end of a coverage period or immediately thereafter and are announced ahead of time.

Week(s)	Topics and Competencies	Assignment(s)
9	<p>Chapter 09 – Physical Security</p> <ul style="list-style-type: none"> • Discuss the relationship between threats to information security and physical security • Describe the key physical security considerations including fire control and surveillance systems • Identify critical physical environment considerations for computing facilities, including uninterruptible power supplies 	<p>Read Chapter 09</p> <ul style="list-style-type: none"> • Chapter Exercises and Projects • Chapter Exam • Weekly Current Events Activity
10	<p>Chapter 10 – Implementing Information Security</p> <ul style="list-style-type: none"> • Explain how an organization’s information security blueprint becomes a project plan • Discuss the many organizational considerations that a project plan must address • Demonstrate the significance of the project manager’s role in the success of an information security project • Illustrate the need for professional project management for complex projects • Follow technical strategies and models for implementing a project plan • Identify the nontechnical problems that organizations face in times of rapid change 	<p>Review Chapter 10</p> <ul style="list-style-type: none"> • Chapter Exercises and Projects • Chapter Exam • Weekly Current Events Activity
11	<p>Chapter 11 – Security and Personnel</p> <ul style="list-style-type: none"> • Describe where and how the information security function is positioned within organizations • Explain the issues and concerns related to staffing the information security function • Identify the credentials that information security professionals can acquire to gain recognition in the field • Illustrate how an organization’s employment policies and practices can support the information security effort • Present the special security precautions that must be taken when using contract workers • Explain the need for the separation of duties • Describe the special requirements needed to ensure the privacy of personnel data 	<p>Read Chapter 11</p> <ul style="list-style-type: none"> • Chapter Exercises and Projects • Chapter Exam • Weekly Current Events Activity

Course Schedule*

Chapter Exercises, Chapter Assignments, and Chapter Programming Labs are generally scheduled to be due on the last day during a given coverage period for the material. Exams are generally given at the end of a coverage period or immediately thereafter and are announced ahead of time.

Week(s)	Topics and Competencies	Assignment(s)
12	<p>Chapter 12 – Information Security Maintenance</p> <ul style="list-style-type: none"> • Understand the need for ongoing maintenance of the information security program • List the recommended security management models • Define a model for a full maintenance program • Identify the key factors involved in monitoring the external and internal environment • Describe how planning, risk assessment, vulnerability assessment, and remediation tie into information security maintenance • Explain how to build readiness and review procedures into information security maintenance • Define digital forensics, and describe the management of the digital forensics function • Describe the process of acquiring, analyzing, and maintaining potential evidentiary material 	<p>Review Chapter 12</p> <ul style="list-style-type: none"> • Chapter Exercises and Projects • Chapter Exam • Weekly Current Events Activity
		<p>PROJECT DUE: April 6, 2018</p>
13	Final Project Presentations	<ul style="list-style-type: none"> • Weekly Current Events Activity
14	Final Project Presentations (cont.)	<ul style="list-style-type: none"> • Weekly Current Events Activity
Wk of 4/16	Final Week Activities	Final Exam
4/19	Portfolio	<p>FINAL COURSE PORTFOLIO DUE: April 19, 2018</p>

Refer to the drop boxes and chapter review question items in the online classroom for due dates on assigned class work

*Schedule subject to change at instructor discretion and extenuating circumstances.