Oklahoma State University Institute of Technology
Online Syllabus
Summer 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.

COURSE PURPOSE:
The purpose of the class is to provide the learner an overview of the field of Information Security and introduce the learner to the various tasks of a Security Professional in the dynamic environment in which the professionals operate.

Type of course: Theory/Lab
Credit Hours: 3;
> Total clock hours of theory per semester: 30
> Total clock hours of lab for the semester: 45

Class length - Full Semester
Class days and times: Fully online

Prerequisites: None

Instructor Name: Howard Licht   **Instructor Phone:** (918) 293-4786
Office: IT/ET 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. **Please include course name/number in the subject line along with the subject of the email.**

Instructor's Office Hours:

Monday	Tuesday	Wednesday	Thursday	Friday
1:00 p.m. to 3:30 p.m.	9:30 a.m. to 11:30 a.m. 3:00 p.m. to 3:45 p.m.	1:00 p.m. to 3:30 p.m.	9:30 a.m. to 11:30 a.m. 3:00 p.m. to 3:45 p.m.	By appointment Only

Additional hours by phone: Monday and Wednesday evenings, 6:30 to 8:30

School Name: **School Phone:**
Information Technologies   (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: 978-1-337-10206-3

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:

Estimated Cost for Text:	$200
Estimated Cost for Materials:	$20
Estimated Cost for Uniform/Tools:	$0
Total Estimated Cost	$220

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	Module Exercises Ch 2, 4, 5, 7, 8, 9 **Final Exam***
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	Module Exercises 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	Module Exercises Ch 6, 12 & Final Project
N.1	determine the scope, time, or cost goals for a specific project	Module Exercises Ch 6, 10 , 11, 12 & Final Project

Aspects of the course objective assessments may be used in the university's assessment of student learning. If applicable, an asterisk (*) above indicates this assignment is used in the university assessment program.

COURSE ACTIVITIES

In this course students will:

➢ Complete reading assignments.
➢ Use software to assess system vulnerabilities
➢ Explore Application Security
➢ Research security applicable regulations and laws
➢ Perform incident/disaster classification and analysis
➢ Explore digital certificates and their capabilities
➢ Configure Microsoft Windows firewall
➢ Perform encryption and exchange information securely using encryption
➢ Perform security hardening techniques in Microsoft Internet Explorer
➢ Perform a physical security threat analysis
➢ Research careers in Information Security
➢ Develop a security baseline report of a computer
➢ Apply problem-solving skills to problems
➢ Participate in class discussions and class activities
➢ Take examinations and quizzes
➢ Participate in class discussions and activities.
➢ View videos that depict the various concepts.
➢ Compile a portfolio of work produced.

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

Final Grade Calculation	
Module Exercises, 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.

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

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

RECOMMENDED STUDENT COMPETENCIES/SKILLS

The following list of competencies/skills are recommended for student success in the course:
- ➢ The ability to create and write essay level material
- ➢ The use of a web browser and web search engine
- ➢ Utilize Office products effectively, such as Word, Excel, PowerPoint
- ➢ The use of Screen Capture Software
- ➢ The use of software to create archived zip files
- ➢ The ability to install and uninstall software
- ➢ Manage time effectively

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 with appropriate documentation and 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.

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.

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.

SYLLABUS ATTACHMENT
View the Syllabus Attachment, which contains other important information, by visiting
http://osuit.edu/center/student_syllabus_information

The syllabus attachment contains several topics of interest to the student and is part of the syllabus. Topics contained on the attachment include but are not limited to:
➢ Americans with Disabilities Act (ADA)
➢ Class Attendance policies (both in class and online)
➢ Dropping and Withdrawing from classes
➢ University Expectations and Policies including Academic Dishonesty
➢ List of Campus Services to aid Students

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. In Class Assignments are generally due in the given class 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 must be provided 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 14 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	*student name here*
Due date	*assignment due date here*
Grade	*grade earned here*
Grading Comments	*instructor comments here*

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

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.

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)

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.

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.

Week(s)	Topics and Competencies	Assignment(s)
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.		
1 5-3-18 thru 5-6-18	**Chapter 01 – Introduction to Information Security** • 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 • Explain the role of security in the SDLC • Describe the IS roles of professionals within an organization	Read Chapter 01 • Chapter Exercises and Projects • Chapter Exam • Weekly Current Events Activity
2 5-7-18 thru 5-13-18	**Chapter 02 – The Need for Security** • Discuss organizational need for information security • Explain why a successful information security program is the shared responsibility of an organization's 3 communities of interest • List and Describe the threats posed to information security and common attacks associated with those threats • List the common failures and errors that result from poor software security efforts	Read Chapter 02 • Chapter Exercises and Projects • Chapter Exam • Weekly Current Events Activity
3 5-14-18 thru 5-20-18	**Chapter 03 – Legal, Ethical and Professional Issues in Information Security** • Describe the functions of and relationships among laws, regulations, and professional organizations in information security • Explain the differences between laws and ethics • Identify major national laws that affect the practice of information security • Discuss the role of privacy as it applies to law and ethics in information security	Review Chapter 03 • 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 5-21-18 thru 5-27-18	**Chapter 04 – Planning for Security** • Describe management's role in the development, maintenance, and enforcement of information security policy, standards, practices, procedures, and guidelines • Explain what an information security blueprint is, identify its major components, and explain how it supports the information security program • Discuss how an organization institutionalizes its policies, standards, and practices using education, training, and awareness programs • Describe what contingency planning is and how it relates to incident response planning, disaster recovery planning, and business continuity plans	Review Chapter 04 • Chapter Exercises and Projects • Chapter Exam • Weekly Current Events Activity
5 5-28-18 thru 6-3-18	**Chapter 05 – Risk Management** • Define risk management, risk identification, risk assessment, and risk control • Describe how risk is identified and assessed • Assess risk based on probability of occurrence and likely expected impact • Explain the fundamental aspects of documenting risk via the process of risk assessment • Describe various options for a risk mitigation strategy • Define risk appetite and explain how it relates to residual risk • Discuss conceptual frameworks for evaluating risk controls and formulate a cost-benefit analysis	Read Chapter 05 • 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 6-4-18 thru 6-10-18	**Chapter 06 – Security Technology – Access Controls, Firewalls, and VPNs** • Define risk management, risk identification, risk assessment, and risk control • Describe how risk is identified and assessed • Assess risk based on probability of occurrence and likely expected impact • Explain the fundamental aspects of documenting risk via the process of risk assessment • Describe various options for a risk mitigation strategy • Define risk appetite and explain how it relates to residual risk • Discuss conceptual frameworks for evaluating risk controls and formulate a cost-benefit analysis	Read Chapter 06 • Chapter Exercises and Projects • Chapter Exam • Weekly Current Events Activity
7 6-11-18 thru 6-17-18	**Chapter 07 – Security Technology: IDPS and Other Security Tools** • Identify and describe the categories and models of intrusion detection and prevention systems • Describe the detection approaches employed by modern intrusion detection and prevention systems • Define and describe honeypots, honeynets, and padded cell systems • List and define the major categories of scanning and analysis tools, and describe the specific tools used within each category	Read Chapter 07 • Chapter Exercises and Projects • Chapter Exam • Weekly Current Events Activity
8 6-18-18 thru 6-24-18	**Chapter 08 – Cryptography** • 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 cryptographic tools • List and explain the major protocols used for secure communications	Review Chapter 08 • Chapter Exercises and Projects • Chapter Exam • Weekly Current Events Activity Professional Development Due: June 22, 2018
Summer Break – Week 6-25-18 thru 7-18-18		

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 7-9-18 thru 7-15-18	**Chapter 09 – Physical Security** • Discuss the relationship between information security and physical security • Describe key physical security considerations, including fire control and surveillance systems • Identify critical physical environment considerations for computing facilities, including uninterruptible power supplies	Read Chapter 09 • Chapter Exercises and Projects • Chapter Exam • Weekly Current Events Activity
10 7-16-18 thru 7-22-18	**Chapter 10 – Implementing IS** • Explain how an organization's information security blueprint becomes a project plan • Discuss the many organizational considerations that a project plan must address • Explain the significance of the project manager's role in the success of an information security project • Describe the need for professional project management for complex projects • Discuss technical strategies and models for implementing a project plan • List and discuss the nontechnical problems that organizations face in times of rapid change	Review Chapter 10 • Chapter Exercises and Projects • Chapter Exam • Weekly Current Events Activity
11 7-23-18 thru 7-29-18	**Chapter 11 –Security and Personnel** • Explain how an organization's information security blueprint becomes a project plan • Discuss the many organizational considerations that a project plan must address • Explain the significance of the project manager's role in the success of an information security project • Describe the need for professional project management for complex projects • Discuss technical strategies and models for implementing a project plan • List and discuss the nontechnical problems that organizations face in times of rapid change	Read Chapter 11 • 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 7-30-18 thru 8-5-18	**Chapter 12 – Information Security Maintenance** • Explain how an organization's information security blueprint becomes a project plan • Discuss the many organizational considerations that a project plan must address • Explain the significance of the project manager's role in the success of an information security project • Describe the need for professional project management for complex projects • Discuss technical strategies and models for implementing a project plan • List and discuss the nontechnical problems that organizations face in times of rapid change	Review Chapter 12 • Chapter Exercises and Projects • Chapter Exam • Weekly Current Events Activity **PROJECT DUE:** **August 3, 2018**
13 8-6-18 thru 8-12-18	Additional Information Security Topics as Time Permits	• Weekly Current Events Activity
14 8-13-18 thru 8-19-18	Additional Information Security Topics as Time Permits	• Weekly Current Events Activity
	Finals Activities	
8-20-18 thru 8-23-18	Comprehensive Final Exam	**FINAL EXAM** **Online – May be Proctored** **August 20-23. 2-18**
8-23-18	Portfolio	**FINAL COURSE PORTFOLIO DUE:** **August 23, 2018**

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.