VIRGINIA COMMONWEALTH UNIVERSITY

MSIS Program Fall 2024
INFO 544: Principles of Computer and Information Systems Security[1]
Snead B2177 (-901); Snead B2175 (-902)
W 1900-2140 (-901); MW 1600-1715 (-902)

PROFESSOR

Elizabeth White Baker, Ph.D.
Office: Snead Building 4209 ☎ 804.828.7118 bakerew@vcu.edu
Office Hours by appointment via Zoom or Skype

COURSE CATALOG LISTING

Semester course: 3 lecture hours (delivered online, face-to-face or hybrid). 3 credits. Explores issues related to protecting information resources of a firm. Various tools and techniques useful for assessing CISS concerns in organizations are introduced. Principles and models for CISS and security management are presented and selected computer and CISS topics are introduced. Material is presented and discussed from a management frame of reference. Formerly INFO 644.

COURSE OBJECTIVES

This course is designed to introduce you to managerial aspects of information security and assurance and important issues that *business and IS* managers face when using, developing and managing the security of information systems (IS). Strategic and tactical issues of information systems security are addressed. The topics mastered in the course will prepare you to develop and drive implementation of information security plans for your organization through knowledge of compliance, governance and strategic planning, policy, and risk management.

By completing this course, you will be able to:

- describe the importance of a manager's role in securing an organization's information assets;
- identify legal, ethical, and professional issues that relate to the practice of InfoSec;
- explain strategic organizational planning for InfoSec and its relationship to organization-wide and IT strategic planning;
- discuss the importance, benefits, and desired outcomes of information security governance and how such a program would be implemented;
- explain what is necessary to implement effective InfoSec policy and what consequences the organization may face if it does not;
- discuss the components of a security education, training, and awareness program and explain how organizations create and manage these programs;
- describe risk management techniques and risk assessment based on the identification and likelihood of adverse events;
- evaluate InfoSec control alternatives under the defense risk treatment strategy and explain how to maintain and perpetuate controls;
- describe and recommend an InfoSec management model for a specific organization;
- describe the security practices used to regulate employee behavior and prevent information misuse;
- discuss how an organization would prepare and execute a test of contingency plans;
- describe how planning, risk assessment, vulnerability assessment, and remediation ties into InfoSec maintenance; and
- discuss key InfoSec security protection mechanisms (access controls, firewalls, IDPs, physical security, and encryption).

[1] Revised August 12, 2024

At the end of the course, students will have knowledge, skills, and insights to more effectively secure IT resources to assist in meeting the needs of the business. As this is an *integrative* course, concepts from your other business and IS classes will be utilized in it.

COURSE FORMAT

This course consists of a series of interactive seminars (lectures and participatory discussions). You are required to complete the assigned readings and online content quizzes before each class session. Participation in interactive course seminars during class time is essential to maximize the course learning outcomes. Thus, participation in the material for the seminar's discussion ahead of time is essential.

You are responsible for doing all assigned readings and grasping all the material presented in the course modules, which may or may not originate from the textbook. All course material, including discussion content, online modules, and assigned reading content, are all "fair game" for graded course deliverables and assessments.

COURSE MATERIAL

For this course, we will use the following materials:

1. Readings, presentations, cases, and other materials that are published as PDF or PPT files on the course's Blackboard site. The material on the Blackboard course site will be updated on a frequent basis.

2. **Required Book:** Whitman, M.E., and Mattord, H.J. (2021) *Principles of Information Security, 7th edition*. Cengage. [Electronic version acceptable.]

If a specific topic that we cover in class is of interest to you, the instructor can usually provide additional references that will enable you to explore it in more depth. Please feel free to share with your classmates (by email or other means) timely articles on topics that are discussed in the course.

COURSE REQUIREMENTS

1. **Course participation, including attendance**
   Attendance is taken for all course meetings. Excused absences are given in advance by the professor. This participation grade also reflects your conversational involvement in the interactive seminars, reflecting on your preparedness for the course.

2. **Quizzes (in Blackboard)**
   You are expected to complete each reading and its quiz prior to the assigned due date in the syllabus/on Blackboard. You must complete all the online course material quizzes prior to sitting the final exam for the course.

3. **Hands-on Exercises in Security**
   There are three exercises where students will be completing assignments providing hands-on experience in cybersecurity, with one planning exercise and two lab exercises.

4. **InfoSec Architecture Project**
   You are expected to complete an information security architecture project, designing an appropriate security architecture for a fictitious organization detailed to the student. Additional instructions will be provided in a separate handout that is available from the course Blackboard site.

5. **Case Report – Final Exam**
   The final exam is a take-home essay exam where the students will read and analyze an information security organizational breach and prepare a report for future security recommendations for the organization.

GRADING & OTHER POLICIES

Your course grade will be based on the following components:

Activity	Responsibility	Weight (%)
Quizzes (in Blackboard)	Individual	20
Course participation, including attendance	Individual	5
Hands-on Exercises	Individual	30
InfoSec Architecture Project	Individual	25
Case-Based Final Exam	Individual	20

Your course deliverables will be graded using the following standard:

Grade	*Numeric*	*Performance*
A	4	Outstanding without flaw
A-	3.67	Excellent, but some minor issues
B+	3.33	Very good, yet some room for improvement
B	3	Good, but significant room for improvement
B-	2.67	Okay, but needs major improvement
C+	2.33	Just below acceptable (unsatisfactory)
C	2	Serious deficiencies (unsatisfactory)
F	0	Not worthy of graduate school credit (Fail)

The student is responsible for submitting the assignments when scheduled by the instructor. Late work will be penalized by 20% each 24-hour period after which the assignment is submitted. Students are expected to exhibit conduct that is courteous to the instructor and to the other students in all of the interactions that are necessary for completion of the course. *All exams and assignments are completed outside of class, and thus, there are no make-up assignments or exams necessary.*

Grades will be posted on Blackboard for all work within 7 days after the assignment is due. It is the student's responsibility to check the posted grade frequently. Questions pertaining to grades MUST be made within 1 week of when the grade is returned. No adjustments will be made after the one-week period. Grades for online module quizzes are posted with feedback once all attempts for grade have been submitted to the instructor, no later than 7 days after the due date, to accommodate late submissions.

Additional Course Policy Information
Students should visit http://go.vcu.edu/syllabus and review all syllabus statement information. The full university syllabus statement includes information on topics such as:

- Campus emergency information
- Registration requirements for class attendance
- The VCU Honor System Policy
    - ***Specific to this course:*** Cheating of any kind shall result in a grade of zero (0) on the test, assignment or quiz in question, with a minimum deduction of one letter grade should the assignment be worth less than 10%. The instructor shall be the sole judge as to when cheating has occurred. Collaboration, copying of other's electronic work, or handing in the work of others is considered cheating. Violations will follow the guidelines in the VCU Bulletin.
- Important dates for the semester – Academic Calendar
- Student success
- Institutional attendance requirements and consequences of poor attendance (withdrawals from classes)

- Career Services
- Managing stress
- Mandatory responsibility of faculty members to report incidents of sexual misconduct
- Military short-term training or deployment
- Student email standard
- Student financial responsibility
- Students representing the university – excused absences
- Students with disabilities
- Faculty communication about students

COURSE SCHEDULE

#	Date	Topic	Readings/Cases	Assignments for the Week (Due Dates for Assignments)
Week 1 8/20/24		Course Introduction; Introduction to Information Security	**Book:** Chapter 1	
Week 2 8/26/24		Further Discussion on Introduction to Information Security	**Book:** Chapter 1	
Week 3 9/3/24		The Need for Information Security	**Book:** Chapter 2	**Quiz:** Chapter 2 due
Week 4 9/9/24		Information Security Management	**Book:** Chapter 3	**Quiz:** Chapter 3 due
Week 5 9/16/24		Intro to Risk Management; Incident Response and Contingency Planning	**Book:** Chapter 4 partial, Chapter 5	**Quiz:** Chapter 5 due
Week 6 9/23/24		Incident Response and Contingency Planning (cont) with exercise	**Book:** Chapter 5	**Business Continuity/Disaster Recovery Planning Exercise Due**
Week 7 9/30/24		Legal, Ethical, and Professional Issues in Cybersecurity	**Book:** Chapter 6	**Quiz:** Chapter 6 due
Week 8 10/7/24		Security Technology: Access Controls, Firewalls, and VPNs	**Book:** Chapter 8	**Quiz:** Chapter 8 due
Week 9 10/14/24		Security Technology: Intrusion Detection and Prevention Systems and Other Security Tools	**Book:** Chapter 9	**Quiz:** Chapter 9 due
Week 10 10/21/24		Security Technology: Intrusion Detection and Prevention Systems and Other Security Tools (cont) with lab	**Book:** Chapter 9	**IDP and IDS Systems Lab Due**
Week 11 10/28/24		Cryptography	**Book:** Chapter 10	**Quiz:** Chapter 10 due

Week 12 11/4/24	**Cryptography (cont) with lab**	**Book:** Chapter 10	**Cryptography Lab Due**
Week 13 11/11/24	**Implementing Information Security**	**Book:** Chapter 11	**Quiz:** Chapter 11 due
Week 14 11/25/24	**Information Security Maintenance**	**Book:** Chapter 12	**Quiz:** Chapter 12 due
Week 15 12/2/24	**Information Security Maintenance (cont)**	**Book:** Chapter 12	**InfoSec Architecture Design Project Due**
	Final Exam	Case study will be presented for individual completion for the final exam deliverable.	**Final Exam Due – Dec 11, 2024 at 11:59pm**

The above schedule is subject to change.
You can find any updated schedule on the course Blackboard site.