VIRGINIA COMMONWEALTH UNIVERSITY

MSIS Program
INFO 535: Ethical, Social, and Legal Issues in Computer and Information Systems Security[1]
Snead Hall B2177
Monday 1900-2140

PROFESSOR

Elizabeth White Baker, Ph.D.
Office: Snead Building 4209 ☎ 804.828.7118 🖱 bakerew@vcu.edu
Office Hours by appointment via Zoom or Skype
View my profile on Linked in

COURSE CATALOG LISTING

Semester course: 3 lecture hours (delivered online, face-to-face, or hybrid). 3 credits. Analyzing socio-political and ethical issues surrounding computer and information systems security. Topics include privacy laws, identity theft, information collection and retention policies, and enforcement. Formerly INFO 635.

COURSE OBJECTIVES

In an era where information technology changes constantly, a thoughtful response to these rapid changes requires a basic understanding of IT history, an awareness of current issues, and a familiarity with ethics. This course tries to introduce a balanced coverage of ethical problems and issues computer professionals encounter in today's environment. This course will cover provocative issues such as social networking, government surveillance, privacy laws, computer security and reliability, and intellectual property from all points of view. Students are asked to think critically and draw their own conclusions as they face these challenges, which ultimately prepare them to become responsible, ethical users of future technologies.

By completing this course, you will be able to:

- Define ethics, morality, and moral system and recognize the distinction between ethical theory and professional ethics
- Summarize the basic concepts of relativism, utilitarianism, and deontological theories.
- Apply theories of ethics to case situations in the context of organizational use of information technology.
- Identify the strengths and weaknesses of relevant professional codes as expressions of professionalism and guides to decision-making.
- Summarize the legal bases for the right to privacy and freedom of expression in one's own nation, how those concepts vary from country to country, and how these would apply to security policies.
- Identify the professional's role in security in an organization and the tradeoffs involved.
- Outline the technical basis of viruses and denial-of-service attacks and enumerate techniques to combat the same.
- Distinguish among patent, copyright, and trade secret protection and explain how patent and copyright laws may vary internationally.
- Explain the various U.S. legislation and regulations that impact technology and the disadvantages and advantages of free expression in cyberspace.
- Explain why computing/network access is restricted in some countries.
- Define a computer use policy with enforcement measures.
- Understand the ethical issues associated with gathering, storing, and accessing genetic information in databases.

COURSE

[1] Revised August 12, 2024

FORMAT

This course consists of interactive seminars (lectures and participatory discussions). You are required to complete the assigned readings and discussions before each class session. Participation in the 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 necessary.

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. **Required:** Deborah Johnson, Computer Ethics (4th Edition). Prentice Hall, 2009. ISBN-13: 978-0131112414

2. Readings, presentations, cases, and other materials are published as PDF or PPT files on the course's Canvas site. The material on the Canvas course site will be updated frequently.

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

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 and your preparedness for the course.

2. **Reading Discussion Threads (in Blackboard)**
   You are expected to participate regularly and in a valuable manner during seminar and case discussions. Based on the quality of your contributions to the online discussion forums given for each case, case discussion points will be allocated to you. Several posted questions will be presented in the discussions reflecting your required readings, the course modules, and current events relevant to the assigned case. You are required to make a minimum of 4 discussion postings for each case: You are to post two answers to any of the discussion topics ("initial postings") and post two responses to other student postings ("response postings"), which includes a substantive commentary on their answer (e.g., supplement with additional information and examples, provide a critique and counterexamples, ask probing questions, etc.).

   The following grading criteria will be used to grade your posts:
   A. Each posting must be at least 100 words long, or it receives no credit. Only the first two initial postings and the first two response postings meeting the 100-word requirement will be graded.
   B. The two initial postings must be submitted by Friday at 11:59 p.m. EST, and the two response postings are due Sunday at 11:59 p.m. EST. Any late postings receive a 20% deduction per day.
   C. Each of the two initial postings must include two references – one internal (course readings, course modules, primers, webliography, etc.) and one external (other authoritative sources beyond our course material, including ***specific*** personal and professional scenarios). ***Note: No wiki or blog references.***

   The discussion posting grading rubric will be posted on Canvas for your reference.

3. **Individual Project**

You are expected to complete an information security ethics project on one of the course topics. A separate handout available from the course Canvas site will provide additional instructions.

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

GRADING & OTHER POLICIES

Your course grade will be based on the following components:

Activity	Responsibility	Weight (%)
Discussion (in Canvas)	Individual	35
Course participation, including attendance	Individual	20
Individual Project	Individual	25
Case-Based Final Exam	Individual	20

Your course deliverables will be graded using the following standards:

Grade	*Numeric*	*Performance*
A	4	Outstanding without flaw
A-	4	Excellent, but some minor issues
B+	3	Very good, yet some room for improvement
B	3	Good, but significant room for improvement
B-	3	Okay, but needs major improvement
C+	2	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 courteous conduct to the instructor and to the other students in all of the interactions necessary for the course's completion. *All exams and assignments are completed outside of class; thus, no make-up assignments or exams are required.*

Grades will be posted on Blackboard for all work within seven 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 one 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 seven 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 when cheating occurs. 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.
- Computer and Network Use
- Important dates for the semester – Academic Calendar; Reading Days

- 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
- Withdrawal from classes
- Faculty communication with students

COURSE SCHEDULE

#	Date	Topic
Week 1 8/26/24		**Course Introduction; Why are Ethics in CISS important?**
Week 2 9/9/24		**Socio-technical Computer Ethics**
Week 3 9/16/24		**Introduction to Ethical Thinking**
Week 4 9/23/24		**Cybersecurity and Society:** The evolution of cyber attacks: actors, motives, techniques, surfaces; economics of cyber crime and cybersecurity
Week 5 9/30/24		**Codes of Ethics; Professional Responsibility in Cybersecurity**
Week 6 10/7/24		**Cybersecurity Standards; Incident Response; Hacking Back** organizational security policy**,** surveillance
Week 7 10/14/24		**Responsible Disclosure: Whistleblower, Leaker, Insider Threat**
Week 8 10/21/24		**Law and Ethics; Enforcement** security breach notice laws
Week 9 10/28/24		**Privacy** identity theft
Week 10 11/4/24		**Intellectual Property**
Week 11 11/11/24		**Computer Reliability** critical infrastructure designation
Week 12 11/18/24		**Information, Propaganda, Misinformation, and Disinformation (information collection and retention policies)** surveillance; nation-state internet restriction/freedom of speech
Week 13 12/2/24		**Cyberwarfare** Stuxnet

Week 14 **12/9/24**	**The Future of Cyber** Internet governance; Internet technical redesign for security; database storage of genetic information
	Final Exam – Take home exam due Dec 16th, 2024 at 9:40pm US Eastern Time

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