ITS460: Information Security Legal and Ethical Issues

Credit Hours: 3

Contact Hours: This is a 3-credit course, offered in accelerated format. This means that 16 weeks of material is covered in 8 weeks. The exact number of hours per week that you can expect to spend on each course will vary based upon the weekly coursework, as well as your study style and preferences. You should plan to spend 14-20 hours per week in each course reading material, interacting on the discussion boards, writing papers, completing projects, and doing research.

Faculty Information

Faculty contact information and office hours can be found on the faculty profile page.

Course Description and Outcomes

Course Description:

In this course students will examine how law, ethics, and technology intersect in organizations that rely on information technology. Students will gain an understanding and insight into issues arising from privacy, secrecy, access control, and policy enforcement, as well as other legal and ethical dilemmas prevalent in today's organizations.

Course Overview:

ITS460 examines the intersection among law, ethics, and technology in organizations that rely on information technology (IT) or offer IT services. Course readings include a combination of foundational texts and current news articles, which introduce foundational concepts and practical applications concerning security, privacy, law and ethics. Students will gain insight and skills for dealing with issues arising from privacy, secrecy, access control, hacking attacks, network vulnerabilities and policy enforcement as well as other legal and ethical dilemmas prevalent or emerging in today's organizations. Students apply the course concepts to real-world developments and events through a variety of exercises including discussion forums, critical thinking essays and a Portfolio Project.

Course Learning Outcomes:

1. Explain the importance of information security to an organization.
2. Describe the risks, threats, and vulnerabilities of security and privacy in IT systems and networks.
3. Explain what is meant by cyber ethics and how this concept may relate to issues of law, policy, and innovation.
4. Analyze how technical and architectural choices may reflect ethical and moral values.

5. Identify the common attacks on IT networks and explain how the motivations behind them have evolved over time.
6. Explain the relationship between security and privacy.
7. Identify and explain some basic approaches to IT security and privacy and how they can be applied in a multinational or international context.

Participation & Attendance

Prompt and consistent attendance in your online courses is essential for your success at CSU-Global Campus. Failure to verify your attendance within the first 7 days of this course may result in your withdrawal. If for some reason you would like to drop a course, please contact your advisor.

Online classes have deadlines, assignments, and participation requirements just like on-campus classes. Budget your time carefully and keep an open line of communication with your instructor. If you are having technical problems, problems with your assignments, or other problems that are impeding your progress, let your instructor know as soon as possible.

Course Materials

Required:

Whitman, M. E., & Mattord, H. J. (2017). *Management of information security* (5th ed.). Boston, MA: Cengage. ISBN: 9781305501256

NOTE: All non-textbook required readings and materials necessary to complete assignments, discussions, and/or supplemental or required exercises are provided within the course itself. Please read through each course module carefully.

Course Schedule

Due Dates
The Academic Week at CSU-Global begins on Monday and ends the following Sunday.

- Discussion Boards: The original post must be completed by Thursday at 11:59 p.m. MT and Peer Responses posted by Sunday 11:59 p.m. MT. Late posts may not be awarded points.
- Opening Exercises: Take the opening exercise before reading each week's content to see which areas you will need to focus on. You may take these exercises as many times as you need. The opening exercises will not affect your final grade.
- Mastery Exercises: Students may access and retake mastery exercises through the last day of class until they achieve the scores they desire.
- Critical Thinking: Assignments are due Sunday at 11:59 p.m. MT.

Week #	Readings	Assignments
1	• Chapter 1 in *Management of Information Security*	• Discussion (25 points) • Opening Exercise (0 points) • Mastery Exercise (10 points) • Critical Thinking (90 points)
2	• Chapter 2 in *Management of Information Security*	• Discussion (25 points) • Opening Exercise (0 points) • Mastery Exercise (10 points) • Critical Thinking (95 points) • Portfolio Milestone (20 points)
3	• Chapters 3 & 4 in *Management of Information Security* • Chapter 2 in *Code and Other Laws of Cyberspace* through http://www.codev2.cc	• Discussion (25 points) • Opening Exercise (0 points) • Mastery Exercise (10 points) • Critical Thinking (95 points)
4	• Chapter 5 in *Management of Information Security*	• Discussion (25 points) • Opening Exercise (0 points) • Mastery Exercise (10 points)
5	• Chapters 6 & 7 in *Management of Information Security*	• Discussion (25 points) • Opening Exercise (0 points) • Mastery Exercise (10 points) • Critical Thinking (90 points)
6	• Chapters 8 & 9 in *Management of Information Security* • Cavoukian, A. (2009). *Privacy by design*. Retrieved from http://www.privacybydesign.ca/index.php/paper/privacy-by-design/	• Discussion (25 points) • Opening Exercise (0 points) • Mastery Exercise (10 points)
7	• Chapters 10 & 11 in *Management of Information Security*	• Discussion (25 points) • Opening Exercise (0 points) • Mastery Exercise (10 points)
8	• Chapter 12 in *Management of Information Security*	• Discussion (25 points) • Opening Exercise (0 points) • Mastery Exercise (10 points) • Portfolio (330 points)

Assignment Details

This course includes the following assignments/projects:

Module 1

CRITICAL THINKING ASSIGNMENT (90 points)

The McCumber Cube

The McCumber Cube shows three proportions. If theorized, the three dimensions of each axis become a 3 × 3 × 3 cube with 27 cells representing areas that must be addressed to secure today's information systems. To ensure system security, each of the 27 areas must be properly addressed during the security process (McCumber, 1991).

The three-dimensional model's factors are Confidentiality, Integrity, Availability, Policy, Education, Technology Storage, Processing, and Transmission.

Search the internet or the CSU-Global Library for examples of the CNSS security model and its three dimensions. Note: you can use the same example or examples for this assignment that you cited for this week's discussion forum.

Then briefly elaborate on each of these dimensions and their importance to a solid InfoSec program. Be sure to expand on the importance of each dimension and how they work together to ensure a secure infrastructure.

Support your analysis by citing specific statements from the text or two outside sources.

Discuss and cite the course textbook and at least one additional credible or scholarly source to support your analysis and positions. The CSU-Global Library is a good place to find credible and scholarly sources. Your paper should be 2-3 pages in length with document and citation formatting per the *CSU-Global Guide to Writing & APA.*

Watch the video below for insight on the CNSS security model and how the dimensions coincide.

CNSS security model: https://www.youtube.com/watch?v=_HK3XB4sCMw

Your paper should be 2-3 pages in length and conform to the *CSU-Global Guide to Writing and APA*. Include at least two scholarly references in addition to the course textbook. The CSU-Global Library is a good place to find these references.

PORTFOLIO PROJECT REMINDER

A final Portfolio Project is due at the end of the course. Please read the full Portfolio Project description in the Module 8 folder to preview your Portfolio Project assignment. Also be sure to review the final Portfolio Project grading rubric, which you can find in the Module 8 folder as well.

Project: Propose a security policy for your organization

Preparation: Choose a real or hypothetical organization, corporation (profit or nonprofit), or institution that uses IT in its product, activities, or operations. If you work in an organization or field that could benefit from an information network security policy, you might wish to apply the project to it.

Module 2

CRITICAL THINKING ASSIGNMENT (95 points)

Morals, Ethics, and Law in a Code of Ethics

In readings and class discussions, we have talked about the relationship and distinctions between morality and ethics. Morality deals with basic principles of right and wrong or good and bad. Ethics deals with behavior and actions. Provide a cut-and-paste copy of the codes in your assignment or summarize them briefly.

Search the internet or the CSU-Global Library to find two examples of a code of ethics and/or code of conduct for an organization or group.

Apply what you have learned from the module to identify, describe, and analyze the moral principles, ethical and legal requirements, and implications with respect to criminal behavior (if relevant) that are reflected in each element of the code of ethics case examples that you have found. In the concluding page, evaluate the effectiveness of morals, ethics and law in contributing to the effectiveness of the code overall.

Discuss and cite the course textbook and at least one additional credible or scholarly source to support your analysis and positions. The CSU-Global Library is a good place to find credible and scholarly sources. Your paper should be 2-3 pages in length, not counting cut-and-pasted codes, with document and citation formatting per the *CSU-Global Guide to Writing and APA*.

PORTFOLIO PROJECT MILESTONE (20 Points)

Scenario Selection

Submit a brief description of the "real or hypothetical organization, corporation (profit or nonprofit), or institution that uses IT in its product, activities, or operations" that will serve as the scenario for your Portfolio Project. If you work or have worked for an organization could benefit from an information network security policy, consider using your place of employment as the scenario for your project.

Your description should be at least a paragraph and no more than a page in length.

Though you will not receive immediate points for this deliverable, it is a part of your Portfolio Project requirements and points will be applied to or deducted from your final project grade if the deliverable is not completed and submitted as assigned. You will receive valuable instructor feedback on your description that should be processed when you complete the Portfolio assignment.

See the Portfolio Project Description and the Portfolio Project grading rubric in the Module 8 folder for details.

Module 3

CRITICAL THINKING ASSIGNMENT (95 points)

Case Study Analysis

Networks and personal computers are under continuous assault from hackers. The types of attacks vary widely in complexity and severity, but hackers generally have one of three motives for compromising a network (Judge, 2014):
- Financial fraud
- Political reasons
- Personal reasons

Search the internet or the CSU-Global Library to find an example of a hacking activity or situation that represents a morally, ethically, or criminally ambiguous situation, but is different from any examples you used in other assignments for this course.

Write a critical essay that meets the following requirements:

1. Cite and briefly describe your example.
2. Apply what you have learned from the course to this point to identify arguments both in support of and critical of the behavior of the attackers.
3. Describe and explain the relationships among morality, ethics, law, and crime as they intersect in the case example that you have identified.

The CSU-Global Library is a good place to find credible and scholarly sources. Your paper should be 2-3 pages in length with document and citation formatting per the *CSU-Global Guide to Writing & APA*.

Module 5

CRITICAL THINKING ASSIGNMENT (90 points)

Security on the Internet

Write a 2-3 page critical essay dealing with the following questions.

1. What are the security and privacy risks and vulnerabilities in using the internet?
2. List some specific common attack strategies, and describe how they work. What are their effects/consequences on the security and privacy of both individual users and organizations? Cite some specific examples, and show how the damage can be mitigated or avoided (if possible).
3. How can security awareness and program evaluation mitigate risk?

Discuss and cite the course and at least one additional credible or scholarly source to support your analysis and positions. The CSU-Global Library is a good place to find credible and scholarly sources. Your paper should be 2-3 pages in length with document and citation formatting per the *CSU-Global Guide to Writing & APA*.

Module 8

PORTFOLIO PROJECT (330 Points)

Propose a Security Policy for an Organization

Preparation: Choose a real or hypothetical organization, corporation (profit or nonprofit), or institution that uses IT in its product, services, activities, and/or operations. If you work in an organization or field that could benefit from an information network security policy, you might wish to apply the project to it.

Assignment: Prepare a well-written security policy proposal for your organization that utilizes the concepts learned in the course as a basis for your analysis and policy.

Make sure that your proposal includes the basic elements of a good security policy including:

1. Introduction describing your organization and describing its mission, products/services, technical resources, and technical strategy
2. Analysis of the organization's relationships to its clients/customers, staff, management, and owners or other stakeholders

3. A vulnerability assessment
4. Your recommendation, including:
   a. Proposed remedial measures (as appropriate to the situation; these might include firewall/gateway provisions, authentication and authorization, encryption systems, intrusion detection, virus detection, incident reporting, education/training, etc.)
   b. Proposed code of ethics or code of practice to be applied within the organization
   c. Legal/compliance requirements and description of how they will be met
   d. Proposed security policy statement/summary

Important: Your proposal must justify every element of your proposal in ethical and legal terms. In other words, you need to state why each policy/code element (including technical elements) is good for business and why it is good/sound ethical policy (how it is good for the organization and why it is good for customers, users, or employees, or the public). Also identify any ethical/legal tensions, conflicts, and/or contradictions and justify any trade-offs being made in the recommendation.

Discuss and cite at least three credible or scholarly sources other than the course textbooks (which can be cited as well) to support your analysis and policy choices. The CSU-Global Library is a good place to find credible and scholarly sources. Your paper should be 8-10 pages in length with document and citation formatting per the *CSU-Global Guide to Writing & APA.*

Recommendation: It is recommended that students review Chapter 8 in the course textbook, which is required reading for Module 6, early in the term and apply the knowledge therein to planning and drafting the Portfolio Project. In Chapter 8 (and also in the early part of Chapter 10), the textbook author discusses the role of a security policy in the compliance of an organization. He observes that in response to public outcry in the 1990s, governments went on a binge passing laws to regulate the new Internet. But privacy advocates pushed back and by the early 2000s, the result of much politicking was a mixed system of sectoral laws (dealing with specific situations) and largely voluntary norms. These norms were adopted by organizations and enshrined in security and privacy policies regarding data and networking. Kizza (2011) made the point that, "A good, balanced and unified approach to information security compliance consists of a good security policy that effectively balances and enforces core information security and compliance elements" (p. 184).

Incremental Deliverable due 11:59 P.M. on Sunday of Week 2

Submit a brief description of the "real or hypothetical organization, corporation (profit or non-profit), or institution that uses IT in its product, activities, or operations" that will serve as the scenario for your Portfolio Project. If you work or have worked for an organization could benefit from an information network security policy, consider using your place of employment as the scenario for your project.

Your description should be at least a paragraph and no more than a page in length.

Course Policies

Course Grading

20% Discussion Participation
0% Opening Exercises
8% Mastery Exercises
37% Critical Thinking Assignments
35% Final Portfolio Project

Grading Scale and Policies

A	95.0 – 100
A-	90.0 – 94.9
B+	86.7 – 89.9
B	83.3 – 86.6
B-	80.0 – 83.2
C+	75.0 – 79.9

C	70.0 – 74.9
D	60.0 – 69.9
F	59.9 or below

In-Classroom Policies
For information on late work and incomplete grade policies, please refer to our **In-Classroom Student Policies and Guidelines** or the Academic Catalog for comprehensive documentation of CSU-Global institutional policies.

Academic Integrity
Students must assume responsibility for maintaining honesty in all work submitted for credit and in any other work designated by the instructor of the course. Academic dishonesty includes cheating, fabrication, facilitating academic dishonesty, plagiarism, reusing /re-purposing your own work (see *CSU-Global Guide to Writing and APA Requirements* for percentage of repurposed work that can be used in an assignment), unauthorized possession of academic materials, and unauthorized collaboration. The CSU-Global Library provides information on how students can avoid plagiarism by understanding what it is and how to use the Library and Internet resources.

Citing Sources with APA Style
All students are expected to follow the *CSU-Global Guide to Writing and APA Requirements* when citing in APA (based on the APA Style Manual, 6th edition) for all assignments. For details on CSU-Global APA style, please review the APA resources within the CSU-Global Library under the "APA Guide & Resources" link. A link to this document should also be provided within most assignment descriptions in your course.

Disability Services Statement
CSU–Global is committed to providing reasonable accommodations for all persons with disabilities. Any student with a documented disability requesting academic accommodations should contact the Disability Resource Coordinator at 720-279-0650 and/or email ada@CSUGlobal.edu for additional information to coordinate reasonable accommodations for students with documented disabilities.

Netiquette
Respect the diversity of opinions among the instructor and classmates and engage with them in a courteous, respectful, and professional manner. All posts and classroom communication must be conducted in accordance with the student code of conduct. Think before you push the Send button. Did you say just what you meant? How will the person on the other end read the words?

Maintain an environment free of harassment, stalking, threats, abuse, insults or humiliation toward the instructor and classmates. This includes, but is not limited to, demeaning written or oral comments of an ethnic, religious, age, disability, sexist (or sexual orientation), or racist nature; and the unwanted sexual advances or intimidations by email, or on discussion boards and other postings within or connected to the online classroom.

If you have concerns about something that has been said, please let your instructor know.