Colorado State University
GLOBAL CAMPUS

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.

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:

In ITS460, you will examine 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 fundamental concepts and practical applications concerning security, privacy, law, and ethics. You 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. You will apply the course concepts to real-world developments and events through a variety of exercises including discussion forums, Critical Thinking assignments 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. Discuss 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

Textbook Information is located in the CSU-Global Booklist on the Student Portal.

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.

Weekly Reading and Assignment Details

Module 1

Readings

- Chapter 1 in *Management of Information Security*

Opening Exercise (0 points)

Discussion (25 points)

Mastery Exercise (10 points)

Critical Thinking (90 points)
Choose one of the following two assignments to complete this week. Do not do both assignments. Identify your assignment choice in the title of your submission.

Option #1: The McCumber Cube
The McCumber Cube, embedded within the CNSS Security Model, contains three dimensions. 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.

The three dimensions of the model are:

1. Confidentiality, Integrity, Availability;
2. Policy, Education, Technology; and
3. Storage, Processing, and Transmission.

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

In the paper you submit, briefly elaborate on each of these dimensions and their importance to a solid InfoSec program. Include any impacts management has in sustaining secure information systems. Be sure to expand on the importance of each dimension and how they work together to ensure a secure infrastructure.

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 3-4 pages in length with document and citation formatting per the CSU-Global Guide to Writing and APA.

Option #2: Management Practices

Select an organization you have worked for or are familiar with. Using the management roles, leadership types, and management characteristics discussed in the textbook, evaluate the organization's approach to Information Security Management. Prepare a report that addresses the following prompts:

1. Briefly describe your organization's Information Security Program.
2. What are the management roles practiced by your organization, particularly in relation with the organization's Information Security Program?
3. What leadership types are the most effective for managing the Information Security Program?
4. What management characteristics or functions are used in running the Information Security Program?

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 3-4 pages in length with document and citation formatting per the CSU-Global Guide to Writing and APA.

Module 2

Readings

- Chapter 2 in *Management of Information Security*

Opening Exercise (0 points)

Discussion (25 points)

Mastery Exercise (10 points)

Critical Thinking (95 points)

Choose one of the following two assignments to complete this week. Do not do both assignments. Identify your assignment choice in the title of your submission.

Option #1: Developing 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.

Search the Internet or the CSU-Global Library to find an example of a code of ethics for an organization or group. Websites for professional organizations usually contain a code of ethics. In your paper, provide a cut-and-paste copy of the code or summarize it briefly.

Using that code of ethics as a starting point, develop a code of ethics for your organization or an organization you are familiar with. Justify how adherence to this code enables the organization to create greater business value.

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 and well written according to CSU-Global Guide to Writing and APA.

Option #2: 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.

Search the Internet or the CSU-Global Library to find two examples of ethics codes for an organization or group. In your paper, provide a cut-and-paste copy of the codes in your assignment or summarize them briefly.

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. On the concluding page, evaluate how morals, ethics, and law contribute to the overall effectiveness of the code.

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 and well written according to CSU-Global Guide to Writing and APA.

Portfolio Milestone (20 points)

Choose one of the following two assignments to complete this week. Do not do both assignments. Identify your assignment choice in the title of your submission.

Option #1: Scenario Selection – Information Security Policy

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 that could benefit from an information security policy, consider using it as the scenario for your project.

Your description should be at least a paragraph and no more than a page in length. 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 **Module 8**.

Option #2: Scenario Selection – Information Security Program
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 security program, consider using it as the scenario for your project.

Your description should be at least a paragraph and no more than a page in length. 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 **Module 8**.

Module 3

Readings

- Chapters 3 & 4 in *Management of Information Security*

Opening Exercise (0 points)

Discussion (25 points)

Mastery Exercise (10 points)

Critical Thinking (95 points)

Choose one of the following two assignments to complete this week. Do not do both assignments. Identify your assignment choice in the title of your submission.

Option #1: Case Study Analysis
Networks and personal computers are under continuous assault from hackers. The types of attacks vary widely in complexity and severity, but according to the text, hackers generally have one of three motives for compromising network:

- Financial fraud,
- Political reasons, or
- Personal reasons.

Search the Internet or the CSU-Global Library to find an example of a hacking activity or situation that represent a cyber-crime, but is different from any examples you used in other assignments for this course.

Write a critical essay that meets the following requirements:

- Cite and briefly describe your example.
- 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.
- Discuss which of the three motives best describes the hacker's intentions and why that motive is the correct one.
- Discuss how an information security policy or planning could have impacted the outcome of this event.

The CSU-Global Library is a good place to find credible and scholarly sources. Your paper should be 3-4 pages in length (not counting the title and reference pages) with document and citation formatting per CSU-Global Guide to Writing and APA.

Option #2: Analysis of an Information Security Strategic Plan
Your organization does not have an Information Security Strategic Plan. The CIO asked you to propose an approach for developing the strategic plan. Your report should cover the following topics:

- Strategic planning process,
- Organizational resources needed to create the plan, and
- Role of governance after the plan is created.

The CSU-Global Library is a good place to find credible and scholarly sources. Your paper should be 3-4 pages in length (not counting the title and reference pages) with document and citation formatting per CSU-Global Guide to Writing and APA.

Module 4

Readings

- Chapter 5 in *Management of Information Security*

Opening Exercise (0 points)

Discussion (25 points)

Mastery Exercise (10 points)

Module 5

Readings

- Chapters 6 & 7 in *Management of Information Security*

Opening Exercise (0 points)

Discussion (25 points)

Mastery Exercise (10 points)

Critical Thinking (90 points)
Choose one of the following two assignments to complete this week. Do not do both assignments. Identify your assignment choice in the title of your submission.

Option #1: Security on the Internet
Write a 3-4 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 3-4 pages in length with document and citation formatting per the CSU-Global Guide to Writing & APA.

Option #2: Formalized Risk Management Program
Your CIO is interested in implementing a formalized risk management program and requests that you submit a report describing the following risk management approaches:

- Microsoft Risk Management Approach,
- FAIR, and
- ISO 27005 Standard for InfoSec Risk Management.

In the report you must include some factors that your organization should consider when selecting a risk management model.

Discuss and cite the course text and other materials 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 3-4 pages in length with document and citation formatting per the CSU-Global Guide to Writing and APA.

Module 6

Readings

- Chapters 8 and 9 in *Management of Information Security*

Opening Exercise (0 points)

Discussion (25 points)

Mastery Exercise (10 points)

Module 7

Readings

- Chapters 10 & 11 in *Management of Information Security*

Opening Exercise (0 points)

Discussion (25 points)

Mastery Exercise (10 points)

Module 8

Readings

- Chapter 12 in *Management of Information Security*

Opening Exercise (0 points)

Discussion (25 points)

Mastery Exercise (10 points)

Portfolio Project (330 points)

Choose one of the following two assignments to complete this week. Do not do both assignments. Identify your assignment choice in the title of your submission.

Option #1: Propose a Security Policy for an Organization

Module 2 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. This organization, corporation, or institution will be the subject of your final Portfolio Project.

Module 8 Portfolio Project: 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: You 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). You should 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 CSU-Global Guide to Writing and APA.

Recommendation: You should review Chapter 4 in the course textbook and apply the knowledge therein to planning and drafting the Portfolio Project.

Option #2: Propose a Security Program for an Organization

Module 2 Preparation: Choose a real or hypothetical organization, corporation (profit or non-profit), 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 security program, you might wish to apply the project to it. This organization, corporation, or institution will be the subject of your final Portfolio

Project.

Module 8 Portfolio Project: Prepare a well written security program proposal for your organization that utilizes the concepts learned in the course as a basis for your analysis and proposed solution.

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

1. An introduction that describes your organization, its mission, products/services, technical resources, and technical strategy.
2. An assessment of the impact on organizational culture from implementing information security.
3. An assessment of likely challenges in implementing and sustaining the proposed information security program.
4. Your recommendation for a security program should:
    a. Propose a set of information security positions and titles and define the roles information security personnel will have in the new organization.
    b. Include an organizational chart that reflects the proposed security personnel.
    c. Describe security education and training—who is trained on what subjects and how often.
    d. Consider security awareness—how to incorporate information security awareness throughout the organization.
    e. Summarize your security program recommendations.

Important: You 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). You should 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 CSU-Global Guide to Writing and APA.

Recommendation: You should review Chapter 5 in the course textbook and apply the knowledge therein to planning and drafting the Portfolio Project.

Course Policies

Grading Scale	
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

Course Grading

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

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 /repurposing your own work (see CSU-Global Guide to Writing & APA 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 & APA when citing in APA (based on the most recent APA style manual) for all assignments. A link to this guide 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.