Colorado State University GLOBAL CAMPUS

ISM530: ENTERPRISE CYBERSECURITY

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:

This course provides students with insight into the cybersecurity issues surrounding an enterprise. These include securing organizational data, responding to cyber-based security breaches, emerging technologies, and ensuring a secured computing environment for safeguarding company information. The course reviews the network security and cryptographic techniques that are currently being used. The nuances involved in defining cybersecurity strategies and complying with security standards to ensure governance are also discussed.

Course Overview:

This course allows students the opportunity to research and apply solutions for securing information assets using different methodologies. The course also examines the need for security and explores the legal, ethical, and professional issues facing organizations today. Risk management strategies and technologies are analyzed. Security technology tools, cryptography, and physical security, are also explored. The course concludes with a look at information security management.

Course Learning Outcomes:

1. Develop an organizational strategy to mitigate cybercrime attacks based on possible threats to organizational data.
2. Provide solutions to secure information assets based on different authentication methodologies.
3. Discuss the use of authentication with cryptography to secure information access.
4. Describe threats that can impact an organization's information assets.
5. Summarize the commitment of foreign governments for the expansion of nationally owned telecommunications services for the support of business and government technologies.

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. (2015). *Principles of information security* (6th ed.). Boston, MA: Cengage Learning. ISBN-13: 978-1337102063

Virtual Labs – Access Control, Authentication, and Public Key Infrastructure

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.
- **Critical Thinking & Labs:** Assignments are due Sunday at 11:59 p.m. MT.

Weekly Reading and Assignment Details

Module 1

Readings

· Chapter 1 in *Principles of Information Security*

Discussion (25 points)

Lab (40 points)

Part 1 – (Lab #1): Configure an Active Directory Domain Controller

The first part of this lab assignment (Lab #1) provides a hands-on opportunity to configure an Active Directory domain controller. Active Directory is at the heart of Windows Server security and provides a mechanism to establish a variety of other security measures within a Windows-based network.

Follow the steps below to complete this portion of the assignment:

1. Read through the **Student Lab Guide** carefully. It provides detailed instructions for accessing and completing the labs in this course.
2. Open the **Lab 1 Assessment Worksheet**. Save a copy of the worksheet to your computer; this will allow you to fill it out electronically and save your answers. You will complete this worksheet and submit it to your instructor after you have completed the hands-on portion of the lab. However, it is strongly recommended that you read through the worksheet before you begin.
3. Click the **Lab Access** link below to enter the virtual lab environment.
4. Read through all of the material under the Intro and Steps tabs before you start working.
5. Follow the step-by-step instructions under the Steps tab to perform the lab. **Note:** You will not be completing a lab report, so you can disregard instructions on how to make screen captures.
6. After completing the hands-on lab, complete and submit the Lab 1 Assessment Worksheet. (Use the worksheet that you saved to your computer.) Be sure to save it again before submitting it.

For additional information on accessing and completing the lab, refer to the **Student Lab Guide.**

Part 2 – (Lab #2): Manage Windows Accounts and Organizational Units

In Part 2 of this lab (Lab #2), you will use the Microsoft Active Directory Users and Computers utility to create and manage Windows accounts.

Follow the steps below to complete this portion of the assignment:

1. Open the **Lab 2 Assessment Worksheet**. Save a copy of the worksheet to your computer; this will allow you to fill it out electronically and save your answers. You will complete this worksheet and submit it to your instructor after you have completed the hands-on portion of the lab. However, it is strongly recommended that you read through the worksheet before you begin.
2. Click the **Lab Access** link below to enter the virtual lab environment.
3. Read through all of the material under the Intro and Steps tabs before you start working.
4. Follow the step-by-step instructions under the Steps tab to perform the lab. **Note:** You will not be completing a lab report, so you can disregard instructions to make screen captures.
5. After completing the hands-on lab, complete and submit the Lab 2 Assessment Worksheet. Use the worksheet that you saved to your computer. Be sure to save it again before submitting it.

For additional information on accessing and completing the lab, refer to the **Student Lab Guide**.

Module 2

Readings

- Chapters 2 & 3 in *Principles of Information Security*

Discussion (25 points)

Critical Thinking (55 points)

Choose one of the following two assignments to complete this week. Do *not* complete both assignments. Identify your assignment choice in the title of your submission. Note that, while there are two options for this Critical Thinking Assignment, there is only one rubric. Review the rubric to confirm that you are meeting the assignment requirements.

Option #1: Cybercrime Laws
Many cybercrime laws have been enacted over the past few decades. Which one of these laws do you believe is the most effective cybercrime law available to law enforcement? Support your arguments by discussing two cases in which the law was used to prosecute the perpetrators. You may select a federal/state law or a provision targeting a specific cybercrime.

***Directions*:**
Your paper should be four to five pages in length (excluding cover page and references) and formatted according to the CSU-Global Guide to Writing and APA Requirements. Be sure to discuss and reference concepts taken from the assigned textbook reading and relevant research. You must include a minimum of three credible, academic, or professional references beyond the text or other course materials. Review the grading rubric to see how you will be graded for this assignment.

Option #2: Corporate Cybercrimes
Cyber criminals use different methods to harm corporations. Which corporate cybercrime do you believe is the most damaging? Support your arguments by discussing two recent cases.

***Directions*:**
Your paper should be four to five pages in length (excluding cover page and references) and formatted according to the CSU-Global Guide to Writing and APA Requirements. Be sure to discuss and reference concepts taken from the assigned textbook reading and relevant research. You must include a minimum of three credible, academic, or professional references beyond the text or other course materials. Review the grading rubric to see how you will be graded for this assignment.

Portfolio Project Milestone (25 points)

Portfolio Topic – Option #1: Major Information Security Incident

Submit your Portfolio Project topic to your instructor for preliminary approval. Provide reasons for your choice. Your submission should contain no more than one page of content, framed by a cover page and references page. This assignment is required and is worth 25 points toward your final project grade.

Portfolio Topic – Option #2: 2016 Security Trends

Submit your Portfolio Project topic to your instructor for preliminary approval. Provide reasons for your choice. Your submission should contain no more than one page of content, framed by a cover page and references page. This assignment is required and is worth 25 points toward your final project grade.

Lab (20 points)

Lab 3 – Configure Windows File System Permissions

When considering security, many professionals often start with configuring file permissions. This lab provides an opportunity to configure file permissions on a Windows-based system.

Follow the steps below to complete this assignment:

1. Open the **Lab 3 Assessment Worksheet**. Save a copy of the worksheet to your computer; this will allow you to fill it out electronically and save your answers. You will complete this worksheet and submit it to your instructor after you have completed the hands-on portion of the lab. However, it is strongly recommended that you read through the worksheet before you begin.
2. Click the **Lab Access** link below to enter the virtual lab environment.
3. Read through all of the material under the Intro and Steps tabs before you start working.
4. Follow the step-by-step instructions under the Steps tab to perform the lab. **Note:** You will not be completing a lab report, so you can disregard instructions to make screen captures.
5. After completing the hands-on lab, complete and submit the Lab 3 Assessment Worksheet. (Use the worksheet that you saved to your computer.) Be sure to save it again before submitting it.

For additional information on accessing and completing the lab, refer to the **Student Lab Guide**.

Module 3

Readings

- Chapter 4 in *Principles of Information Security*

Discussion (25 points)

Critical Thinking (55 points)

Choose one of the following two assignments to complete this week. Do *not* complete both assignments. Identify your assignment choice in the title of your submission. Note that, while there are two options for this Critical Thinking Assignment, there is only one rubric. Review the rubric to confirm that you are meeting the assignment requirements.

Option #1: ABC Corporation

The policies that organizations put in place are similar to laws in that they are directives for how to act properly. Like laws, policies should be impartial and fair and are often founded on ethical and moral belief systems of the people who create them. In some cases, especially when organizations expand into foreign countries, they experience a form of culture shock when the laws of their new host country conflict with their internal policies.

Suppose that the ABC Corporation has expanded its operations into your country. Setting aside any legal requirements that ABC makes to its policies to conform to your local laws, does ABC have an ethical imperative to modify its policies to better meet the needs of its stakeholders and their geographical region/country?

Directions:

Your paper should be four to five pages in length (excluding cover page and references) and formatted according to the CSU-Global Guide to Writing and APA Requirements. Be sure to discuss and reference concepts taken from the assigned textbook reading and relevant research. You must include a minimum of three credible, academic or professional references beyond the text or other course materials. Review the grading rubric to see how you will be graded for this assignment.

Option #2: Electronic Frontier Foundation

The Electronic Frontier Foundation is one of the leading nonprofit organization defending civil liberties in the digital world. In a written paper, address the following:

- Using a Web browser, go to www.eff.org.
- What are the current top concerns of this organization?

Directions:
Your paper should be four to five pages in length (excluding cover page and references) and formatted according to the CSU-Global Guide to Writing and APA Requirements. Be sure to discuss and reference concepts taken from the assigned textbook reading and relevant research. You must include a minimum of three credible, academic or professional references beyond the text or other course materials. Review the grading rubric to see how you will be graded for this assignment.

Lab (20 points)

Lab 4 – Manage Group Policy Objects in Active Directory

In Windows-based networks, Group Policy provides a mechanism to control various aspects of network operation, performance, and security. This lab will introduce you to the management of group policy objects in a Windows server.

Follow the steps below to complete this assignment:

1. Open the **Lab 4 Assessment Worksheet**. Save a copy of the worksheet to your computer; this will allow you to fill it out electronically and save your answers. You will complete this worksheet and submit it to your instructor after you have completed the hands-on portion of the lab. However, it is strongly recommended that you read through the worksheet before you begin.
2. Click the **Lab Access** link below to enter the virtual lab environment.
3. Read through all of the material under the Intro and Steps tabs before you start working.
4. Follow the step-by-step instructions under the Steps tab to perform the lab. **Note:** You will not be completing a lab report, so you can disregard instructions to make screen captures.
5. After completing the hands-on lab, complete and submit the Lab 4 Assessment Worksheet. (Use the worksheet that you saved to your computer.) Be sure to save it again before submitting it.

For additional information on accessing and completing the lab, refer to the **Student Lab Guide**.

Module 4

Readings

- Chapter 5 in *Principles of Information Security*

Discussion (25 points)

Critical Thinking (60 points)

Choose one of the following two assignments to complete this week. Do *not* complete both assignments. Identify your assignment choice in the title of your submission. Note that while there are two options for this Critical Thinking Assignment, there is only one rubric. Review the rubric to confirm that you are meeting the assignment requirements.

Option #1:
Conduct research on the Internet to identify a recent cyber-attack on an organization. Describe the occurrence and what could have been done to prevent the situation or lessen its impact. How might risk management have been used to lessen the impact?

Directions:
Your paper should be four to five pages in length (excluding cover page and references) and formatted according to the CSU-Global Guide to Writing and APA Requirements. Be sure to discuss and reference concepts taken from the assigned textbook reading and relevant research. You must include a minimum of three credible, academic or professional references beyond the text or other course materials. Review the grading rubric to see how you will be graded for this assignment.

Option #2:
Risk management has become more of a concern to senior leaders in organizations over the years. In a written paper, answer the following questions:

- What is risk management?
- Why is the identification of risks and vulnerabilities to assets so important in risk management?

Directions:
Your paper should be four to five pages in length (excluding cover page and references) and formatted according to the CSU-Global Guide to Writing and APA Requirements. Be sure to discuss and reference concepts taken from the assigned textbook reading and relevant research. You must include a minimum of three credible, academic or professional references beyond the text or other course materials. Review the grading rubric to see how you will be graded for this assignment.

Portfolio Project Milestone (25 points)

Options #1/#2
Submit an outline of your Portfolio Project

- State your paper topic.
- Provide an outline of your paper.
    - Your outline should include headers (the major topics), major resources, and the intended flow of the information in the project.
    - Under each header, write a few sentences on what you think you might cover in that section.
- Provide three articles that you might consider using for your final Portfolio Project. These sources cannot include the textbook or other course materials.
  Give a short reason why you feel each source would be pertinent to your project. This is not expected to be a final list. The goal here is to motivate you to begin examining research that might help you in your final Portfolio Project.

Lab (20 points)

Lab 5 – Configure Windows Firewall

One important aspect of any cybersecurity plan is a firewall. While various types of firewalls exist, their key purpose is to provide a barrier of protection between an internal and external network. In this lab, you will have the opportunity to configure a Windows firewall.

Follow the steps below to complete this assignment:

1. Open the **Lab 5 Assessment Worksheet**. Save a copy of the worksheet to your computer; this will allow you to fill it out electronically and save your answers. You will complete this worksheet and submit it to your instructor after you have completed the hands-on portion of the lab. However, it is strongly recommended that you read through the worksheet before you begin.
2. Click the **Lab Access** link below to enter the virtual lab environment.
3. Read through all of the material under the Intro and Steps tabs before you start working.
4. Follow the step-by-step instructions under the Steps tab to perform the lab. **Note:** You will not be completing a lab report, so you can disregard instructions to make screen captures.
5. After completing the hands-on lab, complete and submit the Lab 5 Assessment Worksheet. (Use the worksheet that you saved to your computer.) Be sure to save it again before submitting it.

For additional information on accessing and completing the lab, refer to the **Student Lab Guide**.

Module 5

Readings

· Chapters 6 and 7 in *Principles of Information Security.*

Discussion (25 points)

Critical Thinking (60 points)

Security Technology

Choose one of the following two assignments to complete this week. Do *not* complete both assignments. Identify your assignment choice in the title of your submission. Note that while there are two options for this Critical Thinking Assignment, there is only one rubric. Review the rubric to confirm that you are meeting the assignment requirements.

Option #1: IDPS

An IDPS can be an invaluable tool if used correctly in the organization to minimize hacks. Using the Internet, search for commercial IDPS systems. In a written paper, answer the following questions:

- What classification systems and descriptions are used?
- How can they be used to compare the features and components of each IDPS?

Your paper should be four to five pages in length (excluding cover page and references) and formatted according to the CSU-Global Guide to Writing and APA Requirements. Be sure to discuss and reference concepts taken from the assigned textbook reading and relevant research. You must include a minimum of three credible, academic or professional references beyond the text or other course materials. Review the grading rubric to see how you will be graded for this assignment.

Option #2: Secure Passwords

Insecure passwords are among the main security risks facing organizations. Locate at least three passphrase generators on the Internet. In a written paper, answer the following questions:

- What did you observe?
- What would be your criteria for establishing secure passwords?

Your paper should be four to five in length (excluding cover page and references) and formatted according to the CSU-Global Guide to Writing and APA Requirements. Be sure to discuss and reference concepts taken from the assigned textbook reading and relevant research. You must include a minimum of three credible, academic or professional references beyond the text or other course materials. Review the grading rubric to see how you will be graded for this assignment.

Lab (40 points)

Part 1 – (Lab #6): Manage Linux Accounts

Earlier in this course, you had the opportunity to experiment with the management and configuration of a Windows-based account. Linux is another popular operating system that is frequently used by organizations. This lab introduces you to the tools and techniques needed to manage Linux accounts.

Follow the steps below to complete this assignment:

1. Open the **Lab 6 Assessment Worksheet**. Save a copy of the worksheet to your computer; this will allow you to fill it out electronically and save your answers. You will complete this worksheet and submit it to your instructor after you have completed the hands-on portion of the lab. However, it is strongly recommended that you read through the worksheet before you begin.
2. Click the **Lab Access** link below to enter the virtual lab environment.
3. Read through all of the material under the Intro and Steps tabs before you start working.
4. Follow the step-by-step instructions under the Steps tab to perform the lab. **Note:** You will not be completing a lab report, so you can disregard instructions to make screen captures.
5. After completing the hands-on lab, complete and submit the Lab 6 Assessment Worksheet. (Use the worksheet that you saved to your computer.) Be sure to save it again before submitting it.

For additional information on accessing and completing the lab, refer to the **Student Lab Guide**.

Part 2 – (Lab #7): Configure Linux File System Permissions

Now that you've had the chance to work with Linux and Linux accounts, we will move on to another important aspect of Linux administration—file system permissions. As in Windows systems, Linux has some particularities when assigning file permissions. This hands-on lab provides the opportunity to configure a Linux file system.

Follow the steps below to complete this assignment:

1. Open the **Lab 7 Assessment Worksheet**. Save a copy of the worksheet to your computer; this will allow you to fill it out electronically and save your answers. You will complete this worksheet and submit it to your instructor after you have completed the hands-on portion of the lab. However, it is strongly recommended that you read through the worksheet before you begin.
2. Click the **Lab Access** link below to enter the virtual lab environment.
3. Read through all of the material under the Intro and Steps tabs before you start working.
4. Follow the step-by-step instructions under the Steps tab to perform the lab. **Note:** You will not be completing a lab report, so you can disregard instructions to make screen captures.

5. After completing the hands-on lab, complete and submit the Lab 7 Assessment Worksheet. (Use the worksheet that you saved to your computer.) Be sure to save it again before submitting it.

For additional information on accessing and completing the lab, refer to the **Student Lab Guide**.

Module 6

Readings

· Chapters 8 and 9 in *Principles of Information Security*

Discussion (25 points)

Critical Thinking (60 points)

Choose one of the following two assignments to complete this week. Do *not* complete both assignments. Identify your assignment choice in the title of your submission. Note that while there are two options for this Critical Thinking Assignment, there is only one rubric. Review the rubric to confirm that you are meeting the assignment requirements.

Option #1: Physical Security

Based on this week's readings and additional research, in a written paper answer the following questions:

- What is physical security?
- What are the primary threats to physical security?
- How are these threats manifested in attacks against the organization?

Directions

Your paper should be four to five pages in length (excluding cover page and references) and formatted according to the CSU-Global Guide to Writing and APA Requirements. Be sure to discuss and reference concepts taken from the assigned textbook reading and relevant research. You must include a minimum of three credible, academic or professional references beyond the text or other course materials. Review the grading rubric to see how you will be graded for this assignment.

Option #2: Secure Facility

Based on this week's readings and additional research, in a written paper answer the following questions:

- Define a secure facility.
- What is the primary objective of designing such a facility?
- What are some secondary objectives of designing a secure facility?

Your paper should be four to five in length (excluding cover page and references) and formatted according to the CSU-Global Guide to Writing and APA Requirements. Be sure to discuss and reference concepts taken from the assigned textbook reading and relevant research. You must include a minimum of three credible, academic or professional references beyond the text or other course materials. Review the grading rubric to see how you will be graded for this assignment.

Lab (20 points)

Lab 8 – Encrypt and Decrypt Files with PKI

Another important means of maintaining security is through the use of public key infrastructure, or PKI. PKI is commonly used on the web (for such things as certificates) to ensure that traffic is securely encrypted prior to transmission. In this lab, you will experiment with PKI encryption techniques.

Follow the steps below to complete this assignment:

1. Open the **Lab 8 Assessment Worksheet**. Save a copy of the worksheet to your computer; this will allow you to fill it out electronically and save your answers. You will complete this worksheet and submit it to your instructor after you have completed the hands-on portion of the lab. However, it is strongly recommended that you read through the worksheet before you begin.
2. Click the **Lab Access** link below to enter the virtual lab environment.
3. Read through all of the material under the Intro and Steps tabs before you start working.
4. Follow the step-by-step instructions under the Steps tab to perform the lab. **Note:** You will not be completing a lab report, so you can disregard instructions to make screen captures.
5. After completing the hands-on lab, complete and submit the Lab 9 Assessment Worksheet. (Use the worksheet that you saved to your computer.) Be sure to save it again before submitting it.

For additional information on accessing and completing the lab, refer to the **Student Lab Guide**.

Module 7

Readings

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

Discussion (25 points)

Module 8

Readings

- Chapter 12 in *Principles of Information Security*

Discussion (25 points)

Portfolio Project (300 points)

Choose one of the following two Portfolio Projects. Do *not* complete both assignments. Identify your assignment choice in the title of your submission. Review the Portfolio Project grading rubric to understand how you'll be graded on your final project.

Option #1: Major Information Security Incident

Identify a major information security incident that has occurred in the recent past (within the last five years). *If possible, identify a breach that occurred in, or otherwise impacted, a Fortune 500 company.* Review and analyze your chosen incident along the following dimensions:

- What went wrong?
- Why did it occur?
- Who was responsible?
- How could it have been prevented?
- What advice would you offer to prevent such an incident from occurring in the future?

Portfolio Milestones
You will submit your topic in Week 2 and your project outline in Week 4. You will be expected to account for the instructor's feedback in the final version of the Portfolio Project assignment.

Directions:

- The content of the paper must be 8-10 pages in length and formatted according to the CSU-Global Guide to Writing and APA Requirements. The length is not inclusive of the title and references pages.
- A minimum of six references (in addition to course materials, like the textbook or articles). At least two of these being peer-reviewed articles. The CSU-Global Library is a good place to search for credible, scholarly sources. You may want to view the "Does your paper look like this?" sample paper found in the Library under the "APA Guide & Resources" link.

Option #2: 2018 Security Trends
Identify one of the biggest data breaches of 2018. *If possible, identify a major breach that occurred in, or otherwise impacted, a company in 2018.* Review and analyze your chosen incident along the following dimensions:

- What went wrong?
- Why did it occur?
- Who was responsible?
- How could it have been prevented?
- What advice would you offer to prevent such an incident from occurring in the future?

Portfolio Milestones
You will submit your topic in Week 2 and your project outline in Week 4. You will be expected to account for the instructor's feedback in the final version of the Portfolio Project assignment.

Directions:

- The content of the paper must be 8-10 pages in length and formatted according to the *CSU-Global Guide to Writing and APA Requirements*. The length is not inclusive of the title and references pages.
- A minimum of six references (in addition to course materials, like the textbook or articles). At least two of these being peer-reviewed articles. The CSU-Global Library is a good place to search for credible, scholarly sources. You may want to view the "Does your paper look like this?" sample paper found in the Library under the "APA Guide & Resources" link.

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 Questions
29% Critical Thinking Assignments
16% Labs
35% Portfolio Project and Milestones

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.