Colorado State University GLOBAL CAMPUS

ITS455: DIGITAL FORENSICS AND INVESTIGATIONS

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 an insight to cyber security professional intrusion detection methods, information security tools, and preventative measures to information security risks. Students will learn how to respond to cyber breaches which includes the recovery, preservation, analysis of digital crime scene evidence, and proper incident response to cyber criminals.

Course Overview:

This course provides students with an insight into cybersecurity, professional intrusion, detection methods, information security tools, and preventative measures to information security risks. Students will learn how to respond to cyberbreaches, which includes the recovery, preservation, analysis of digital crime scene evidence, and proper incident response to cybercriminals.

In addition to the tools of the digital forensics trade, students will become familiar with relevant federal statutes. They will be presented with various scenarios that a digital forensics investigator might face and will be asked how they would react.

Course Learning Outcomes:

1. Demonstrate the ability to secure digital assets using best practices, appropriate laws, and relevant regulations related to digital investigations.
2. Evaluate situations associated with major computer and network forensics cases and provide insights on possible mitigations to future matters.
3. Demonstrate the ability to apply knowledge of the management of digital investigations, which may include but is not limited to collection, storage, cataloging evidence for use in prosecution of a digital crime scene.
4. Evaluate situations and propose innovative solutions to managing digital investigations related to cyber based crime.
5. Demonstrate the ability to identity and respond to cyber security attacks with preservation of the crime scene, and discuss various tools and file systems.

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:

Nelson, B., Phillips, E., & Steuart, C. (2016). *Guide to computer forensics and investigations: Processing digital evidence* (5th ed.). Boston, MA: Cengage Learning. ISBN: 9781285060033

Suggested:

N/A

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 at 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 *Guide to Computer Forensics and Investigations*
- Jain, N., Kalbande, D. R., & Sharma, P. (2016). Empirical relationship between victim's occupation and their knowledge of digital forensic. In D. Kumar Mishra, R. Sheikh, & S. Jain (Eds.), *Proceedings of the ACM Symposium on Women in Research 2016* (pp. 61-65). New York, NY: ACM.

- Patil, R. Y., & Devane, S. R. (2017). Unmasking of source identity, a step beyond in cyber forensic. *Proceedings of the 10th International Conference on Security of Information and Networks*, 157-164.

Opening Exercise (0 points)

Discussion (25 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: Knoppix

Knoppix is a Linux distribution that can run entirely from a CD or DVD. Write a short paper discussing the possibility of using Knoppix (or other similar distributions) as a forensic boot disk. Give a real-life scenario demonstrating Knoppix's (or other similar distribution's) impact and application.

Your paper must meet the following requirements:

- 4-5 pages in length, not including the cover page and reference page.
- Formatted according to the *CSU-Global Guide to Writing and APA*. Include an introduction, a body with fully developed paragraphs, and a conclusion.
- Be clearly and well written using excellent grammar and style techniques. Be concise. Be logical. You are being graded in part on the quality of your writing. If you need assistance with your writing style, visit the Writing Center, which is also accessible from the Library's homepage.
- Support your paper with at least two peer-reviewed, scholarly references. The CSU-Global Library is a great place to find these resources.

Refer to the Critical Thinking Rubric in Module 1 for more information on expectations for this assignment.

Option #2: Workstation Brands

Investigate several low-emanation workstation brands, and write a short paper about the brands' advantages and disadvantages. Give a real-life scenario portraying the impact and the current application of the workstation brands.

Your paper must meet the following requirements:

- 4-5 pages in length, not including the cover page and reference page.
- Formatted according to the *CSU-Global Guide to Writing and APA*. Include an introduction, a body with fully developed paragraphs, and a conclusion.
- Be clearly and well-written using excellent grammar and style techniques. Be concise. Be logical. You are being graded in part on the quality of your writing. If you need assistance with your writing style, visit the Writing Center, which is also accessible from the Library's homepage.
- Support your paper with at least two peer-reviewed, scholarly references. The CSU-Global Library is a great place to find these resources.

Refer to the Critical Thinking Rubric in Module 1 for more information on expectations for this assignment.

Mastery Exercise (10 points)

Module 2

Readings

- Chapter 4 (135-154) in *Guide to Computer Forensics and Investigations*
- Deutchman, L. (2015). The case for making cell phone data available at trial. *Criminal Justice, 29*(4), 21-26.
- Ramanathan, T., Schmit, C., Menon, A., & Fox, C. (2015). The role of law in supporting secondary uses of electronic health information. *Journal of Law, Medicine & Ethics, 43*(s1), 48-*51.*

Opening Exercise (0 points)

Discussion (25 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: Consolidated Electronics Group Incident Response Plan

Scenario

Consolidated Electronics Group, Inc. is a manufacturer and supplier of avionics equipment to various airlines across the continental United States. Recently, the company laid off several employees, resulting in many disgruntled workers.

Now, the information technology (IT) staff has reported a spike in network attacks numbering in the thousands. Reports from the intrusion detection system (IDS) indicate that two of these potential attacks may have compromised highly classified plans for a new prototype avionics switchboard, which is expected to revolutionize the market. The IT staff suspects that the attacks and potential security breach may have something to do with the recently laid-off staff.

Assignment Instructions

The U.S. National Institute of Standards and Technology (NIST) is a recognized authority for providing security standards, guidelines and procedures. NIST provides a large array of other security-related documents, which are of great value to information security professionals.

To complete this assignment, use NIST's *Computer Security Incident Handling Guide*, Section 3 starting on page 21. Once on the site, click the link on the right side of the screen to download the PDF.

Using the guidance from guide, craft an incident response plan that includes:

1. A description of the specific measures that will be taken to investigate a security breach
2. An explanation of steps taken to prevent future attacks and to secure the company's information systems
3. A communication plan to disseminate the results and findings of this event to the organization

Your plan must meet the following requirements:

- 4-5 pages in length, not including the cover page and reference page.
- Formatted according to the *CSU-Global Guide to Writing and APA*. Include an introduction, a body with fully developed paragraphs, and a conclusion.
- Be clearly and well written using excellent grammar and style techniques. Be concise. Be logical. You are being graded in part on the quality of your writing. If you need assistance with your writing style, visit the Writing Center, which is also accessible from the Library's homepage.

Refer to the Critical Thinking Rubric in Module 2 for more information on expectations for this assignment.

Option 2: Public School District

Scenario
A public school district has been facing a district-wide situation. Someone accesses LMS systems and the registrar's portal, changing grades for many students. They have not been able to identify the suspect yet and the case is under investigation but in the meantime, the superintendent has ordered all users of those resources (teachers and employees) to undergo training on data protection and security. You have been called to run the training sessions.

Assignment Instructions
Create a PowerPoint presentation identifying possible breaches or negligent steps that will lead to intruders having access to school data. List recommendations to improve security and data protection. Address physical security as well.

Your presentation must meet the following requirements:

- Include an introduction slide with the title of the presentation, your name, the submission date, and a reference slide.
- 10 or more slides of easy-to-understand content (text and visuals). Remember, your audience is teachers and employees of the school district who know nothing about data protection and security.
- Speaker's notes containing 50-100 words per slide to elaborate on the slide. In your notes, support slide content with at least two peer-reviewed, scholarly references. The CSU-Global Library is a great place to find these resources.
- Avoid distracting transition elements and animations.
- Formatted according to the *CSU-Global Guide to Writing and APA*.

Refer to the Critical Thinking Rubric in Module 2 for more information on expectations for this assignment.

Mastery Exercise (10 points)

Portfolio Milestone (25 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: Job Candidate Case

The first deliverable of your Portfolio Project is a screenshot of the installation, download, and new case describing the work performed to complete this milestone.

1. Download and install FTK Forensic Toolkit version 1.81 [EXE File Size 60.3 Mb]
2. Download and unzip the precious disk image [ZIP File Size 38.4 Mb]. Use password **On31mag3t0rul3th3ma11** to unzip the file, if necessary. (The password is case sensitive so use it as it is.)
3. Start FTK and create two new cases.
4. Add the Precious.E01 evidence file.
5. Explore the evidence in the Precious evidence file. Look at images, email messages, deleted files, and word documents, among other items.

6. Take screenshots of your work (installation, download and new case).

Refer to the Portfolio Project Milestone Rubric in Module 2 for more information on expectations for this assignment.

Option 2: Economic Espionage Case – Preparation

The first deliverable of your Portfolio Project is to identify an economic espionage criminal case to be the focus of your report.

1. Search fbi.gov for a case.
2. Research the case to find out more details.
3. Identify the legal and regulatory sources for your report.
4. Submit the case to your instructor for approval.

Refer to the Portfolio Project Milestone Rubric in Module 2 for more information on expectations for this assignment.

Module 3

Readings

- Chapter 2 in *Guide to computer Forensics and Investigations*
- Jhaveri, M. H., Cetin, O., Gañán, C., Moore, T., & Van Eeten, M. (2017). Abuse reporting and the fight against cybercrime. *ACM Computing Surveys, 49*(4), 1-27.
- Mba, G., Onaolapo, J., Stringhini, G., & Cavallaro, L. (2017). Flipping 419 cybercrime scams: Targeting the weak and vulnerable. *Proceedings of the 26th International Conference on World Wide Web Companion*, 1301-1310.

Opening Exercise (0 points)

Discussion (25 points)

Mastery Exercise (10 points)

Module 4

Readings

- Chapters 5 & 6 in *Guide to Computer Forensics and Investigations*
- Alrajeh, D., Pasquale, L., & Nuseibeh, B. (2017). On evidence preservation requirements for forensic-ready systems. *Proceedings of the 2017 11th Joint Meeting on Foundations of Software Engineers*, 559-569.
- Potapchuk, J. L. (2016). A second bite at the Apple: Federal courts' authority to compel technical assistance to government agents in accessing encrypted smartphone data under the All Writs Act. *Boston College Law Review, 57*(4), 1403-1446.

Opening Exercise (0 points)

Discussion (25 points)

Mastery Exercise (10 points)

Portfolio Milestone (50 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: Job Candidate Case – Evidence

The second deliverable of your Portfolio Project is an analysis of the evidence you examined in the Precious.EO1 evidence file. Describe what you learned about the images, emails, encrypted files, and website histories.

Your paper must meet the following requirements

- 1-2 pages in length, not including the cover page and reference page.
- Formatted according to the *CSU-Global Guide to Writing and APA*. Include an introduction, a body with fully developed paragraphs, and a conclusion.
- Be clearly and well written, using excellent grammar and style techniques. Be concise. Be logical. You are being graded in part on the quality of your writing. If you need assistance with your writing style, visit the Writing Center, which is also accessible from the Library's homepage.

Refer to the Portfolio Project Milestone Rubric in Module 4 Folder for more information on expectations for this assignment.

Option 2: Economic Espionage

The second deliverable of your Portfolio Project is an analysis of the evidence presented in the economic espionage case. Describe what you learned about the evidence collected about the case.

Your paper must meet the following requirements

- 1-2 pages in length, not including the cover page and reference page.
- Formatted according to the *CSU-Global Guide to Writing and APA*. Include an introduction, a body with fully developed paragraphs, and a conclusion.
- Be clearly and well written using excellent grammar and style techniques. Be concise. Be logical. You are being graded in part on the quality of your writing. If you need assistance with your writing style, visit the Writing Center, which is also accessible from the Library's homepage.

Refer to the Portfolio Project Milestone Rubric in Module 4 for more information on expectations for this assignment.

Module 5

Readings

- Chapters 3 & 4 (pages 154-175) in *Guide to Computer Forensics and Investigations*
- Sultan, S., & Salman, A. (2017). Towards digital forensics pedagogical framework. *Proceedings of the of the 2017 International Conference on Education and E-Learning*, 13-21.
- van den Bos, J. (2017) Sustainable automated data recovery: A research roadmap. *Proceedings of the 1st ACM SIGSOFT International Workshop on Software Engineering and Digital Forensics*, 6-9.

Opening Exercise (0 points)

Discussion (25 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: Tool Testing Report

To respond to various computer security breaches and perform a proper forensics investigation, it is important to ensure that tried and true tools and software are utilized. Tool testing provides a confirmation that the tool or software that you are using to perform a forensic investigation is performing the actions that you intend and nothing more.

The U.S. National Institute of Standards and Technology (NIST) has a rigorous testing program for computer forensic tools and equipment.

Assignment Instructions
Write a paper that addresses these three sections:

1. Provide an overview of the NIST Computer Forensic Tool Testing (CFTT) program and its usefulness to computer forensic investigators.
2. Describe in detail the work that NIST has done in testing "disk imaging" and "deleted file recovery" tools.
3. Describe the significance and importance of the various computer forensic offerings from NIST.
4. Visit https://www.nist.gov/itl/ssd/digital-forensics for additional information.

Your paper must meet the following requirements:

- 4-5 pages in length, not including the cover page and reference page.
- Formatted according to the *CSU-Global Guide to Writing and APA*. Include an introduction, a body with fully developed paragraphs, and a conclusion.
- Be clearly and well written, using excellent grammar and style techniques. Be concise. Be logical. You are being graded in part on the quality of your writing. If you need assistance with your writing style, visit the Writing Center, which is also accessible from the Library's homepage.
- Support your paper with at least two peer-reviewed, scholarly references. The CSU-Global Library is a great place to find these resources.

Refer to the Critical Thinking Rubric in Module 5 for more information on expectations for this assignment.

Option 2: Tool Testing Report

Scenario
A marketing company has implemented a BYOD (Bring Your Own Device) program and would like to introduce its IT department to mobile device forensics standards, practices, and tools endorsed by NLST called Computer Forensics Tool Testing (CFTT). You have been brought in to conduct a training session for the IT Department.

Assignment Instructions
Create a PowerPoint presentation describing CFTT concepts and its components pertaining to mobile devices. Visit https://www.nist.gov/itl/ssd/digital-forensics for additional information.

Your presentation must meet the following requirements:

- Include an introduction slide with the title of the presentation, your name, the submission date, and a reference slide.

- 10 or more slides of easy-to-understand content (text and visuals). Remember, your audience is teachers and employees of the school district who know nothing about data protection and security.
- Speaker's notes containing 50-100 words per slide to elaborate on the slide. In your notes, support slide content with at least two peer-reviewed, scholarly references. The CSU-Global Library is a great place to find these resources.
- Avoid distracting transition elements and animations.
- Formatted according to the *CSU-Global Guide to Writing and APA*.

Refer to the Critical Thinking Rubric in Module 5 for more information on expectations for this assignment.

Mastery Exercise (10 points)

Module 6

Readings

- Chapters 9 & 10 (pages 389-407) in *Guide to Computer Forensics and Investigations*
- Choo, K. R. (2017). Research challenges and opportunities in big forensic data. *Proceedings of the 2017 International Workshop on Managing Insider Security Threats*, 79-80.
- Mayer, O., & Stamm, M. C. (2017). Countering anti-forensics of lateral chromatic aberration. *Proceedings of the 5th ACM Workshop on Information Hiding and Multimedia Security*, 15-20.

Opening Exercise (0 points)

Discussion (25 points)

Critical Thinking (100 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: Cybercrime at a Financial Institution

Cybercrime and information security breaches are a hot topic in the news today. When interacting with organizations, consumers are concerned with the privacy and security of the information they provide. Recent news reports show serious security breaches, sabotage, and even theft has occurred in both private and government institutions.

Assignment Instructions

Create a PowerPoint presentation analyzing a recent cybercrime or security breach at a financial institution as reported by a reputable news source.

- Describe the organization's background.
- Explain the nature of the cybercrime that occurred.
- Describe methods and tools potentially used to investigate the cybercrime, particularly analysis, validation, and acquisition.
- Analyze and describe details about the impact of the cybercrime including financial losses, number of individuals affected, and the effect on the reputation of the organization.
- Analyze the organization's incident response and if the incident was handled in an appropriate manner

Your presentation must meet the following requirements:

- Include an introduction slide with the title of the presentation, your name, the submission date, and a reference slide.
- 12 or more slides of easy to understand content (text and visuals). Remember, your audience is an IT department within a marketing company.
- Speaker's notes containing 50-100 words per slide to elaborate on the slide. In your notes, support slide content with at least two peer-reviewed, scholarly references as well as the news source. The CSU-Global Library is a great place to find these resources.
- Avoid distracting transition elements and animations.
- Formatted according to the *CSU-Global Guide to Writing and APA*.

Refer to the Critical Thinking Rubric in Module 6 for more information on expectations for this assignment.

Option 2: Cybercrime at a Health Insurance Organization

Cybercrime and information security breaches are a hot topic in the news today. When interacting with organizations, consumers are concerned with the privacy and security of the information they provide. Recent news reports show serious security breaches, sabotage, and even theft has occurred in both private and government institutions.

Assignment Instructions
Write a paper analyzing a recent cybercrime or security breach at a health insurance organization as reported by a reputable news source.

- Describe the organization's background.
- Explain the nature of the cybercrime that occurred.
- Describe methods and tools potentially used to investigate the cybercrime, particularly analysis, validation, and acquisition.
- Analyze and describe details about the impact of the cybercrime including financial losses, number of individuals affected, and the effect on the reputation of the organization.
- Analyze the organization's incident response and if the incident was handled in an appropriate manner.

Your paper must meet the following requirements:

- 6-7 pages in length, not including the cover page and reference page.
- Formatted according to the *CSU-Global Guide to Writing and APA*. Include an introduction, a body with fully developed paragraphs, and a conclusion.
- Be clearly and well written using excellent grammar and style techniques. Be concise. Be logical. You are being graded in part on the quality of your writing. If you need assistance with your writing style, visit the Writing Center, which is also accessible from the Library's homepage.
- Support your paper with at least two peer-reviewed, scholarly references. The CSU-Global Library is a great place to find these resources.

Refer to the Critical Thinking Rubric in Module 6 for more information on expectations for this assignment.

Mastery Exercise (10 points)

Module 7

Readings

- Chapters 10 (pp. 408 – 415) & 11 in *Guide to Computer Forensics and Investigations*
- Alrashe, T., Awadalla, A. H., & Dumais, S. (2018). The lifetime of email messages: A large scale analysis of email revisitation. *Proceedings of the 2018 Conference on Human Information Interaction &* Retrieval, 120-129.
- Cai, K., Xie, H., & Lui, J. C. S. (2018). Information spreading forensics via sequential dependent snapshots*. IEEE/ACM Transactions on Networking, 26*(1), 478-491.

Opening Exercise (0 points)

Discussion (25 points)

Mastery Exercise (10 points)

Module 8

Readings

- Chapter 12 in *Guide to Computer Forensics and Investigations*
- Saleem, S., Popov, O., & Baggili, I. (2016). A method and a case study for the selection of the best available tool for mobile device forensics using decision analysis. *Digital Investigation, 16*, S55-S64.
- Wilson, R., & Chi, H. (2018). A framework for validating aimed mobile digital forensics evidences. *Proceedings of the ACMSE 2018 Conference,* 1-8.

Opening Exercise (0 points)

Discussion (25 points)

Mastery Exercise (10 points)

Portfolio Project (275 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: Job Candidate Final Report

For this Portfolio Project, you will work with forensic software to analyze a disk image for electronic evidence to make the hiring decision. You will analyze the forensic data and write a detailed report, following this format:

- Abstract
- Table of Contents
- Body of Report
- Conclusion
- References
- Glossary
- Acknowledgements
- Appendixes

Refer to Chapter 14 in *Guide to Computer Forensics and Investigations: Processing Digital Evidence* for descriptions of each section of the report.

Be sure to include in your report:

- A detailed analysis of the evidence within the body.
- A recommendation about the hiring of the job candidate in the conclusion.
- Raw data in the appendixes.
- Proof of your discovery i.e. screenshots or other exported information from the disk image.
- Lessons learned about computer forensics in the acknowledgement.

In addition to the report requirements above, your report must meet these requirements as well:

- 8-10 pages in length, not including the cover page and reference page.
- Formatted according to the *CSU-Global Guide to Writing and APA*. Include an introduction, a body with fully developed paragraphs, and a conclusion.
- Be clearly and well written using excellent grammar and style techniques. Be concise. Be logical. You are being graded in part on the quality of your writing. If you need assistance with your writing style, visit the Writing Center, which is also accessible from the Library's homepage.
- Support your report with at least four peer-reviewed, scholarly references. The CSU-Global Library is a great place to find these resources.

Refer to the Portfolio Project Rubric in Module 8 for more information on expectations for this assignment.

Option 2: Economic Espionage Forensic Report

Economic espionage is a serious threat to U.S. companies that rely on innovation, according to the National Counterintelligence and Security Center's 2018 report, *Foreign Economic Espionage in Cyberspace*.

Based on the case you researched and analyzed in Modules 2 and 4, write revised policies in response to the economic espionage attack.

Be sure to include in your assignment:

1. Background information about case
    a. A profile of the organization
    b. When the incident occurred
    c. What happened as a result of the attack
2. What the organization must protect
3. Potential threats to security
4. User responsibilities
5. Monitoring of the computer systems
6. Access controls
7. Penalties for violation

Your paper must meet the following requirements:

- 8-10 pages in length, not including the cover page and reference page.
- Formatted according to the *CSU-Global Guide to Writing and APA*. Include an introduction, a body with fully developed paragraphs, and a conclusion.
- Be clearly and well-written using excellent grammar and style techniques. Be concise. Be logical. You are being graded in part on the quality of your writing. If you need assistance with your writing style, visit the Writing Center, which is also accessible from the Library's homepage.

- Support your paper with at least four peer-reviewed, scholarly references. The CSU-Global Library is a great place to find these resources.

Refer to the Portfolio Project Rubric in Module 8 for more information on expectations for this assignment.

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
0% Live Classroom
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.