Colorado State University GLOBAL CAMPUS

ITS350: INFORMATION SYSTEMS AND SECURITY

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:

ITS350 provides students with the skills and knowledge required to support IT security, planning, and cryptology in organizational settings. The course also prepares the student for the Testout Security Pro and CompTIA Security + certifications.

COURSE OVERVIEW:

This course enhances students' skills in the area of security, planning, cryptology, and security technologies. Prepares students for CompTIA Security+ certification exam. Recommended Prior Course: ITS310 or ITS315.

COURSE LEARNING OUTCOMES:

1. Analyze an organization's network security needs and potential vulnerabilities.
2. Employ viable solutions to meet the security needs of an organization.
3. Demonstrate working knowledge of network security concepts, issues, vulnerabilities, and required planning for industry network security concerns.
4. Use assessments and lab simulations to prepare for the Security + exam.
5. Apply tools, conceptual knowledge, and concrete skills to align organizational needs with Information Technology initiatives for a secure network environment.

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:
LabSim Online Labs. (2013). *Labsim for CompTIA's Security Pro: Exam SY0-401.* Pleasant Grove, UT (Do not purchase, access is provided with the course materials).

***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:** Assignments are due Sunday at 11:59 p.m. MT.

Weekly Reading and Assignment Details

Module 1

Readings

- LabSim Security Pro - Chapter 3: Policies, Procedures, and Awareness (Read and view **ALL** content).
- Adnan, M., Just, M., Baillie, L., & Kayacik, H.G. (2015). Investigating the work practices of network security professionals. *Information and Computer Security, 23*(3), 347-368.
- Chapple, M. (2016). Network security. [Video]. *CompTIA Security+ Cert Prep (SY0-401): The Basics.* Retrieved from https://www.lynda.com/Security-tutorials/Network-security/440661/506727-4.html

Discussion (25 points)

Critical Thinking (75 points)
Complete the Week 1 Critical Thinking Assignment in LabSim, which can be accessed from your TestOut LabSim home page per the following instructions:

> To the right of the ITS350 course name under My Classes, click **New Exam** to access the Assessment Exam dialog box. Then click **Begin** to start the **Week 1 Critical Thinking Assignment**.

You will have *one opportunity and a limit of three* hours to complete this assignment so it is strongly recommended that you prepare by completing all videos, simulations, and exam questions provided in this week's LabSim module.

When you have finished the Critical Thinking Assignment, take a screen shot of the final screen showing the score to certify that you have completed all tasks. Then paste the screen images into a Word document with your name, date, school name, section, course name, and instructor name and submit as the deliverable for this assignment.

Note: Internet Explorer or Mozilla Firefox required for Labsim assignments. For more information and steps on how to access Labsim with Google Chrome, click here.

MODULE 2

Readings

- LabSim Security Pro - Chapter 4: Physical (Read and view **ALL** content).
- Fisher, P. (2016). *Cryptography overview.* [Video]. Programming Foundations: Discrete Mathematics. Retrieved from https://www.lynda.com/Programming-Foundations-tutorials/Cryptography/411376/475444-4.html
- Mizroch, A. (2015, Dec 10). In Belgium, an encryption powerhouse rises; University of Leuven has become a battleground in the fight between privacy and surveillance. *Wall Street Journal (Online)*.

Discussion (25 points)

Critical Thinking (75 points)

Complete the Week 2 Critical Thinking Assignment in LabSim, which can be accessed from your TestOut LabSim home page per the following instructions:

> To the right of the ITS350 course name under My Classes, click **New Exam** to access the Assessment Exam dialog box. Then click **Begin** to start the **Week 2 Critical Thinking Assignment**.

You will have *one opportunity and a limit of three* hours to complete this assignment so it is strongly recommended that you prepare by completing all videos, simulations, and exam questions provided in this week's LabSim module.

When you have finished the Critical Thinking Assignment, take a screen shot of the final screen showing the score to certify that you have completed all tasks. Then paste the screen images into a Word document with your name, date, school name, section, course name, and instructor name and submit as the deliverable for this assignment.

Note: Internet Explorer or Mozilla Firefox required for Labsim assignments. For more information and steps on how to access Labsim with Google Chrome, click here.

MODULE 3

Readings

- LabSim Security Pro - Chapter 5: Perimeter - Chapter 6: Network (Read and view **ALL** content).
- Bowles, B. (2017). Business continuity. [Video]. *Cybersecurity Awareness: Backing Up Your Data.* Retrieved from https://www.lynda.com/IT-Infrastructure-tutorials/Business-continuity-plan-BCP/648921/651546-4.html
- Sahebjamnia, N., Torabi, S.A., & Mansouri, S.A. (2015). Integrated business continuity and disaster recovery planning: Towards organizational resilience. *European Journal of Operational Research, 242*(1), 261-273. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0377221714007942

Discussion (25 points)

Critical Thinking (75 points)

Complete the Week 3 Critical Thinking Assignment in LabSim, which can be accessed from your TestOut

LabSim home page per the following instructions:

> To the right of the ITS350 course name under My Classes, click **New Exam** to access the Assessment Exam dialog box. Then click **Begin** to start the **Week 3 Critical Thinking Assignment**.

You will have *one opportunity and a limit of three* hours to complete this assignment so it is strongly recommended that you prepare by completing all videos, simulations, and exam questions provided in this week's LabSim module.

When you have finished the Critical Thinking Assignment, take a screen shot of the final screen showing the score to certify that you have completed all tasks. Then paste the screen images into a Word document with your name, date, school name, section, course name, and instructor name and submit as the deliverable for this assignment.

Note: Internet Explorer or Mozilla Firefox required for Labsim assignments. For more information and steps on how to access Labsim with Google Chrome, click here.

Portfolio Milestone (0 points)

Submit your Portfolio 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.

MODULE 4

Readings

- LabSim Security Pro - Chapter 6: Network (Read and view **ALL** content).
- Dimase, D., Collier, Z. A., Heffner, K., & Linkov, I. (2015, June). Systems engineering framework for cyber physical security and resilience. *Environment Systems & Decisions, 35*(2), 291-300. http://dx.doi.org.csuglobal.idm.oclc.org/10.1007/s10669-015-9540-y
- Jernigan, S. (2017). Physical security. [Video]. *Help Desk Handbook for End Users: Mobile, Networking, Security, and Troubleshooting.* https://www.lynda.com/IT-Infrastructure-tutorials/Physical-security/645047/654136-4.html

Discussion (25 points)

Critical Thinking (75 points)

Complete the Week 4 Critical Thinking Assignment in LabSim, which can be accessed from your TestOut LabSim home page per the following instructions:

> To the right of the ITS350 course name under My Classes, click **New Exam** to access the Assessment Exam dialog box. Then click **Begin** to start the **Week 4 Critical Thinking Assignment**.

You will have *one opportunity and a limit of three* hours to complete this assignment so it is strongly recommended that you prepare by completing all videos, simulations, and exam questions provided in this week's LabSim module.

When you have finished the Critical Thinking Assignment, take a screen shot of the final screen showing

the score to certify that you have completed all tasks. Then paste the screen images into a Word document with your name, date, school name, section, course name, and instructor name and submit as the deliverable for this assignment.

Note: Internet Explorer or Mozilla Firefox required for Labsim assignments. For more information and steps on how to access Labsim with Google Chrome, click here.

MODULE 5

Readings

- LabSim Security Pro - Chapter 7: Host - Chapter 8: Applications (Read and view **ALL** content).
- Collin, S. (2017). Firewalls explained. [Video]. *macOS Server Essential Training.* Retrieved from https://www.lynda.com/Network-Administration-tutorials/Firewalls-explained/427975/456962-4.html
- Firstenberg, M. (2017, June). Industrial cybersecurity: How much is enough? *Chemical Engineering Progress, 113*(6), 26-29.

Discussion (25 points)

Critical Thinking (75 points)

Complete the Week 5 Critical Thinking Assignment in LabSim, which can be accessed from your TestOut LabSim home page per the following instructions:

> To the right of the ITS350 course name under My Classes, click **New Exam** to access the Assessment Exam dialog box. Then click **Begin** to start the **Week 5 Critical Thinking Assignment**.

You will have *one opportunity and a limit of three* hours to complete this assignment so it is strongly recommended that you prepare by completing all videos, simulations, and exam questions provided in this week's LabSim module.

When you have finished the Critical Thinking Assignment, take a screen shot of the final screen showing the score to certify that you have completed all tasks. Then paste the screen images into a Word document with your name, date, school name, section, course name, and instructor name and submit as the deliverable for this assignment.

Note: Internet Explorer or Mozilla Firefox required for Labsim assignments. For more information and steps on how to access Labsim with Google Chrome, click here.

MODULE 6

Readings

- LabSim Security Pro - Chapter 8: Application (Read and view **ALL** content).
- Jacob, M. (2014). [Video]. Learning IPv6. Retrieved from https://www.lynda.com/iP-tutorials/Getting-Know-IPv6/184149-2.html
- Li, S., Tryfonas, T., & Li, H. (2016). The internet of things: A security point of view. *Internet Research, 26*(2), 337-359.

Discussion (25 points)

Critical Thinking (75 points)

Complete the Week 6 Critical Thinking Assignment in LabSim, which can be accessed from your TestOut LabSim home page per the following instructions:

> To the right of the ITS350 course name under My Classes, click **New Exam** to access the Assessment Exam dialog box. Then click **Begin** to start the **Week 6 Critical Thinking Assignment**.

You will have *one opportunity and a limit of three* hours to complete this assignment so it is strongly recommended that you prepare by completing all videos, simulations, and exam questions provided in this week's LabSim module.

When you have finished the Critical Thinking Assignment, take a screen shot of the final screen showing the score to certify that you have completed all tasks. Then paste the screen images into a Word document with your name, date, school name, section, course name, and instructor name and submit as the deliverable for this assignment.

Note: Internet Explorer or Mozilla Firefox required for Labsim assignments. For more information and steps on how to access Labsim with Google Chrome, click here.

MODULE 7

Readings

- LabSim Security Pro - Chapter 9: Data (Read and view **ALL** content).
- Fu, Y., Xiao, N., Liao, X., & Liu, F. (2013, Nov). Application-aware client-side data reduction and encryption of personal data in cloud backup services. *Journal of Computer Science and Technology, 28*(6), 1012-1024. http://dx.doi.org.csuglobal.idm.oclc.org/10.1007/s11390-013-1394-5
- Linthicum, D. (2017). Security. [Video]. *Cloud Computing: Private Cloud Platforms.* Retrieved from https://www.lynda.com/CISSP-tutorials/Understanding-data-security/476939/543568-4.html

Discussion (25 points)

MODULE 8

Readings

- LabSim Security Pro - Chapter 9: Data (Read and view **ALL** content).
- Ancog, R. C., Rebancos, C. M., & Sumalde, Z. M. (2016). Levels and determinants of vulnerability of two indigenous communities in the Philippines: Implications from using mixed-methods approach. *International Journal of Climate Change Strategies and Management, 8*(2), 154-174.
- Chapple, M. (2015). Penetration testing. [Video]. *CompTIA Security+ (SYO-401) Cert Prep: Threats and Vulnerabilities.* Retrieved from https://www.lynda.com/Security-tutorials/Penetration-testing/415404/440360-4.html

Discussion (25 points)

Final Exam (100 points)

Complete the **Security Pro Exam**, which can be accessed from your Home page in LabSim, before midnight of week 8. The exam will be in a separate location from the Critical Thinking assignments. You can only take this exam once.

Note: You may also complete the Security Pro **Practice** Exam in Labsim. You may take this exam as many times as you would like.

Portfolio Project (250 points)

Choose one of the following two Portfolio Project options to complete by the end of Week 8. Do not do both assignments. Identify your assignment choice in the title of your submission. When you are ready to submit, click the Week 8 Portfolio Project header on the Assignments page to upload the document.

OPTION #1: XYZ Corporation

XYZ Corporation is a small organization of roughly 20 to 30 employees working in a simple office space using basic peer-to-peer type networking in which all employees keep their data on their own PCs and each has his or her own devices (i.e., printers, scanners, and other peripherals).

In the last few months, XYZ developed a revolutionary widget that will change technology as we know it. The company received a substantial investment and will quickly ramp up to 100 employees. They moved into a new building that was wired and set up for a local area network (LAN). They have implemented a client server-based network in which all printers, folders, and other resources are shared but everyone has access to everything and there is no security outside of the defaults in place when the system was set up.

You have been hired to secure XYZ Inc's network and ensure that the company has the highest levels of security to prevent internal or external attacks. In an 8-10 page proposal, address the following items to provide a comprehensive secure environment:

1. A plan to provide secure Access Control Methods for all user access
2. A viable Password policy, which includes complexity, duration, and history requirements
3. A cryptography method to ensure vital data is encrypted
4. A remote access plan to ensure that users that access the network remotely do so in a secure and efficient manner
5. A thorough plan to protect the network from Malware and other Malicious attacks

Your proposal should address all of the elements noted above with support, detail, and elaboration for each section explicitly grounded in knowledge from the assigned readings and media, along with any outside sources you may choose to bring into your writing. Your paper should be 8-10 pages in length, conform to *CSU-Global Guide to Writing and APA*, and include 3-5 scholarly references in addition to the course textbook to support your views. The CSU-Global Library is a good place to find these references.

OPTION #2: ABC Corporation

ABC Corporation is a small but global organization of roughly 200 to 250 employees working in a work-at-home type of office space around the world using Wide Area Network connectivity via VPNs. The company deals with lot of financial information to be shared between the offices that requires encrypted traffic as well as data-at-rest encryption.

You have been hired to secure ABC Inc's network and ensure that the company has the highest levels of security to prevent internal or external attacks. In an 8-10 page proposal, address the following items to provide a comprehensive secure environment:

1. A plan to provide secure Access Control Methods for all user access
2. A viable Password policy, which includes complexity, duration, and history requirements
3. A cryptography method to ensure vital data is encrypted, including recommendation on algorithms
4. A VPN recommendation to access the network remotely do so in a secure and efficient manner

Your proposal should address all of the elements noted above with support, detail, and elaboration for each section explicitly grounded in knowledge from the assigned readings and media along with any outside sources you may choose to bring into your writing. Your paper should be 8-10 pages in length, conform to *CSU-Global Guide to Writing and APA*, and include 3-5 scholarly references in addition to the course textbook to support your views. The CSU-Global Library is a good place to find these references.

COURSE POLICIES

Course Grading

20% Discussion Participation
37% Critical Thinking Assignments
43% Final Portfolio Project

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

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 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.