CS 200-4

California State University, San Marcos General Education Program
GENERAL EDUCATION NEW COURSE CERTIFICATION REQUEST
• AREA A3: Critical Thinking
See GE Handbook for information on each section of this form

ABSTRACT

Course Abbreviation and Number: CS 200-4 **Number of Units: 3**_____	**Course Title:** Critical Thinking about Cyber Security for You and Our Critical Infrastructure	
College or Program: ☐CHABSS ☒CSM ☐CEHHS ☐COBA ☐Other	**Desired term of implementation:** ☐ Fall ☐Spring ☒Summer Year:2016	**Mode of Delivery:** ☒ face to face ☐ hybrid ☐ fully on-line
Course Proposer (please print): **Youwen Ouyang**	**Email:** **ouyang@csusm.edu**	**Submission Date:** **03/11/2016**

1. Course Catalog Description: This course is designed to introduce students to Critical Thinking Skills. The course is also designed to introduce students to Cyber Security with an emphasis on how Cyber Security will affect them personally. Students will be introduced to the key concepts of Cyber Security. Cyber Security-related news reports will be examined using Critical Thinking skills. Examples will include the debate over personal privacy vs. the FBI's need to decrypt smartphones. Students will be asked to reason about the impact a cyber-attack on any of our 16 critical infrastructure sectors. What can students do to defend themselves and their families from cyber security attacks? What should we, as a nation, do "before the lights go out"?
See http://hp.ipviking.com/ to see the attacks that are occurring right now.

2. GE Syllabus Checklist: The syllabi for all courses certified for GE credit must contain the following:

☒	Course description, course title and course number
☒	Student learning outcomes for General Education Area and student learning objectives specific to your course, linked to how students will meet these objectives through course activities/experiences
☒	Topics or subjects covered in the course
☒	Registration conditions
☒	Specifics relating to how assignments meet the writing requirement
☒	Tentative course schedule including readings
☒	Grading components including relative weight of assignments

SIGNATURES

Course Proposer — Date: 3/13/16

Department Chair — date: 3/13/16

Please note that the department will be required to report assessment data to the GEC annually. _____ *DC Initial*

GEC attached email — Library Faculty — Date: 4/1/2016 — Support ☒ — Do not support* ☐

Impacted Discipline Chair — Date — Support ☐ — Do not support* ☐

Impacted Discipline Chair — Date — Support ☐ — Do not Support* ☐

GEC Chair — Date — Approve ☐ — Do not Approve ☐

Lib. Support

From: Talitha Matlin
Sent: Friday, April 01, 2016 6:39 AM
To: Youwen Ouyang <ouyang@csusm.edu>
Cc: Laurie Schmelzer <lschmelz@csusm.edu>
Subject: Re: CS course w/GE info

Hi Youwen,

Yes, this looks good and I believe GEC will approve the information literacy portion of this course. This form has my signature.

The course looks interesting, and I do hope that it passes. I will keep my eye on the GEC minutes and so that I can purchase relevant supplementary texts related to the course content.

Best,
Talitha

--
Talitha Matlin
STEM Librarian
California State University San Marcos
tmatlin@csusm.edu KEL 3423 760-750-4342
http://biblio.csusm.edu

On Apr 1, 2016, at 12:27 AM, Youwen Ouyang <ouyang@csusm.edu> wrote:

Hi Talitha,

Attached please find an updated syllabus addressing your concerns on assignments. I hope you can sign and forward the form to GEC. I appreciate your tips about what GEC is looking for regarding a course proposal.

Your support in moving the process forward would be greatly appreciated.

Best,
Youwen

California State University, San Marcos General Education Program
GENERAL EDUCATION NEW COURSE CERTIFICATION REQUEST
• AREA A3: Critical Thinking
See GE Handbook for information on each section of this form

Part A: Critical Thinking General Education Learning Outcomes (GELOs) related to course content. [Please type responses into the tables.]

Critical Thinking GELOs this course will address:	**Course content that addresses each GELO.**	**How will these GELOs be assessed?**
A3.1: Distinguish matters of fact from issues of judgment or opinion and derive factual or judgmental inferences from unambiguous statements of knowledge or belief.	Reasoning Skills Book: Lesson 1 Critical Thinking and Reasoning Skills Lesson 2 Problem Solving Strategies Lesson 3 Thinking vs Knowing Cyber Security Book: Ch 1 Stuxnet – The First Cyber Guided Missile Ch 8 Nations at Cyber War Ch 14 Listening In and Going Dark	Students will be asked to participate in both in-class and online discussions on critical cyber security related issues such as privacy rights versus government need to protect citizens. Students will be asked to distinguish facts from opinions and explain how both sides of the debate derive judgment from facts and opinions.
A3.2: Judge the reliability and credibility of sources.	Reasoning Skills Book: Lesson 4 Who Makes the Claim Lesson 5 Partial Claims and Half Truths Cyber Security Book: Ch 12 Big Data – "They" Know Everything about You	Students will be asked to research topics related to cyber security, cyber-attacks and our Critical Infrastructure. Students will write essays based on their research and include discussions of the reliability and credibility of the sources selected for use in their essays.
A3.3: Effectively argue a point of view by clarifying the issues, focusing on the pertinent issues, and staying relevant to the topic.	Reasoning Skills Book: Lessons 7 Working with Arguments Lesson 8 Evaluating Evidence Lesson 9 Recognizing a Good Argument Cyber Security Book: Ch 18: Looking Forward – What Does the Future Hold?	When stating their point of view regarding cyber security policies and practices, students will be asked to focus on selected problems and keep their argument relevant to the topic.
A3.4: Understand the nature of inductive and deductive reasoning, identify formal and informal fallacies of reasoning, and employ various methods for testing the strength, soundness, and validity of different argument forms.	Reasoning Skills Book: Lesson 11Logical Fallacies: Appeals to Emotion Lesson 12 Logical Fallacies: Distracters and Distorters Lesson 14 Why Did It Happen Lesson 15 Inductive Reasoning Part I Lesson 17 Inductive Reasoning Part II Cyber Security Book: Ch 12 Big Data – "They" Know Everything about You Ch 14 Listening In and Going Dark Logic Book: An Illustrated Book of Bad Arguments	Students will be asked to evaluate examples of cyber events to determine whether such events post any threat to cyber security using inductive and deductive reasoning. Students will also be asked to assess potential errors in inductive and deductive reasoning presented by news reports on cyber-attacks. Students will be asked to apply sound reasoning (avoid "Bad Arguments") when writing their essays, and when stating their views.
A3.5: Understand the basic concepts	Reasoning Skills Book: Lesson 5 Partial Claims and Half Truths	The Cybersecurity Awareness Training includes a printable certificate which can serve as

of meaning (sense, reference, connotation, etc.) and identify different methods of word definition.	Lesson 6 What's in a Word Lesson 7 Working with Arguments Lesson 8 Evaluating Evidence Lesson 9 Recognizing a Good Argument Lesson 10 Putting It All Together Additional Resources: Cybersecurity Awareness Training Version 2.0 This is Cybersecurity training to explain the Cyber Security concepts in an interactive, audio, video, and kinetic (AVK) way. http://cdsetrain.dtic.mil/cybersecurity/	evidence that a student completed the course. Students will be asked to submit the printed certificate to the instructor as evidence of completion.
A3.6: Understand logic and its relationship to language by identifying the basic components of reasoning, including the propositional content of statements, the functions of premises and conclusions in the makeup of arguments, the linkage between evidence and inference, and the rules of inference and logical equivalence.	Reasoning Skills Book: Lesson 5 Partial Claims and Half Truths Lesson 6 What's in a Word Lesson 7 Working with Arguments Lesson 8 Evaluating Evidence Lesson 9 Recognizing a Good Argument Lesson 10 Putting It All Together Lesson 14 Why Did It Happen Lesson 16 Jumping to Conclusions Lesson 18 Numbers Neve Lie Cyber Security Book: Ch 7 Hacktivists and Insurgency	Students will be asked to present analyses of news reports based on logic and draw conclusions about the relative importance of a cyber-attack on different Critical Infrastructure sectors. Students will also be asked to reason about the cyber-attacks that are occurring daily, and to determine the potential for serious cyber-attacks in the future. Students will be asked to discuss, as an example, whether corporations that are being cyber-attacked can (and should) counter attack? Should the US Government protect them? How? Students will be asked to reason about, as an example, the activities of Hacktivists like the group "Anonymous". Are their actions justified? Do they help the situation or make it worse?

Part B: General Education Learning Outcomes required of all GE courses related to course content:

GE Outcomes required of <u>all</u> Courses	**Course content that addresses each GE outcome?**	**How will these GELOs be assessed?**
Students will communicate effectively in writing to various audiences. (writing)	Cyber Security Book: Ch 1 – 17	Students will be asked to write several essays, and to present several topics to the class. Students will select topics of interest to them from the options provided during the course. Students will be asked to debate (in writing) Course Topics in the Discussion Board after each Session.
Students will think critically and	Do not complete. This information is provided in	Do not complete. This information is provided in Part A.

analytically about an issue, idea or problem. (critical thinking)	Part A.	
Students will find, evaluate and use information appropriate to the course and discipline. (Faculty are strongly encouraged to collaborate with their library faculty.)	Additional Resources: Critical Infrastructure Sectors This resource identifies the Critical Infrastructure Sectors that we will be discussing in class and writing about in essays. http://www.dhs.gov/critical-infrastructure-sectors Additional Resources: Cybersecurity Awareness Training Version 2.0 This is Cybersecurity training to explain the Cyber Security concepts in an interactive, audio, video, and kinetic (AVK) way. http://cdsetrain.dtic.mil/cybersecurity/ Students will be encouraged to use the Library resources to find additional authoritative sources to round out their perspective.	Students will be asked to research topics related to cyber security, cyber-attacks and our Critical Infrastructure. Authoritative sources such as the Department of Homeland Security and cyber security-related firms will be accessed. The Cybersecurity Awareness Training includes a printable certificate which can serve as evidence that a student completed the course. Students will be asked to submit the printed certificate to the instructor.

Part C: GE Programmatic Goals: The GE program aligns with CSUSM specific and LEAP Goals. All A3 courses must meet at least one of the LEAP Goals.

GE Programmatic Goals	***Course addresses this LEAP Goal:***
LEAP 1: Knowledge of Human Cultures and the Physical and Natural World.	☐ *No* ☒ *Yes*
LEAP 2: Intellectual and Practical Skills	☐ *No* ☒ *Yes*
LEAP 3: Personal and Social Responsibility	☐ *No* ☒ *Yes*
LEAP 4: Integrative Learning	☐ *No* ☒ *Yes*
CSUSM Specific Programmatic Goals	**Course content that addresses the following CSUSM goals. Please explain, *if applicable.***
CSUSM 1: Exposure to and critical thinking about issues of diversity.	☐ *No* ☒ *Yes (please describe):Students will be asked to evaluate the actions of several diverse groups in terms of their disaster preparedness.*
CSUSM 2: Exposure to and critical thinking about the interrelatedness of peoples in local, national, and global contexts.	☐ *No* ☒ *Yes (please describe):Students will be asked to look at the impact of our Critical Infrastructure (e.g., the power grid) and see how it would impact the whole US. Also the global nature of cyber security and cyber-attacks will be addressed.*

Part D: Course requirements to be met by the instructor.

California State University, San Marcos General Education Program
GENERAL EDUCATION NEW COURSE CERTIFICATION REQUEST
• AREA A3: Critical Thinking

See GE Handbook for information on each section of this form

Course Requirements:	**How will this requirement be met by the instructor?**
Course meets the All-University Writing requirement: A minimum of 2500 words of writing shall be required for 3+ unit courses.	The instructor will assign the following: Students will be asked to write two (2) 1,250 word essays / student presentations on topics related to cyber security and our critical infrastructure.
Critical thinking may be taught in the context of a subject area, by including specific attention to general principles of critical thinking and applying them to examples and exercises in the subject area.	The instructor will guide the students through the areas of concern for Cyber Security and our Critical Infrastructure segments.
The course proposals will demonstrate the application of information literacy to the course materials.	The instructor will show the relationship between computers, Cyber Security and the various Critical Infrastructure Sectors.
All critical thinking courses will be open to all students regardless of their majors; therefore, the basic reasoning skills listed in the above objectives must be explicitly covered.	*The instructor will address the fundamentals of Cyber Security and relate it to common areas of knowledge and practical experience (e.g., the electrical power grid)*

California State University San Marcos
Dept. of Computer Science and Information Systems Infrastructure
(Summer 2016)

Course Description:

This course is designed to introduce students to Critical Thinking Skills. The course is also designed to introduce students to Cyber Security with an emphasis on how Cyber Security will affect them personally. Students will be introduced to the key concepts of Cyber Security. Cyber Security-related news reports will be examined using Critical Thinking skills. Examples will include the debate over personal privacy vs. the FBI's need to decrypt smartphones. Students will be asked to reason about the impact a cyber-attack on any of our 16 critical infrastructure sectors. What can students do to defend themselves and their families from cyber security attacks? What should we, as a nation, do "before the lights go out"?

See http://hp.ipviking.com/ to see the cyber-attacks that are occurring right now.

Course Learning Outcomes:

Upon successful completion of this course, students will (be able to):

- apply Critical Thinking skills
- identify the key concepts of Cyber Security
- identify the Critical Infrastructure Sectors
- think critically about daily Cyber Security news reports
- prepare a personal plan to defend themselves and their families against cyber security attacks
- contribute to the ongoing social debate on Cyber Security-related issues

Required / Recommended Materials / Services:

Reasoning Skills Success in 20 Minutes a Day 3rd Edition

LearningExpress LLC Editors (Author)

Series: 20 Minutes a Day

Paperback: 192 pages

Publisher: LearningExpress, LLC; 3rd edition (February 16, 2010)

Language: English

ISBN-10: 1576857204

ISBN-13: 978-1576857205

http://www.amazon.com/gp/product/1576857204

$15.49

Thinking about Cybersecurity: From Cyber Crime to Cyber Warfare

Professor Paul Rosenzweig

http://www.audible.com/pd/Nonfiction/Thinking-about-Cybersecurity-From-Cyber-Crime-to-Cyber-Warfare-Audiobook/B00DL152XU/ref=a_search_c4_1_1_srTtl?qid=1456895991&sr=1-1

An Illustrated Book of Bad Arguments

Hardcover – September 23, 2014

by Ali Almossawi (Author), Alejandro Giraldo (Illustrator)

#1 Best Seller in Philosophy of Logic & Language

Hardcover: 64 pages

Publisher: The Experiment; ILL edition (September 23, 2014)

Language: English

ISBN-10: 1615192255

ISBN-13: 978-1615192250

http://www.amazon.com/gp/product/1615192255

$9.11

Additional Resources

Suggested Reading: Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath

This resource illustrates the current state of preparedness of the United States to defend against a cyber-attack against one of the critical infrastructure sectors – and how long it might take to recover from an attack. This is a valuable resource for student essays or presentations.

Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath

Ted Koppel

Available in paperback, hardcover and as an audiobook.

ISBN-10: 055341996X (Hardcover) ISBN-13: 9780553419962 (Hardcover)

$15.60

http://www.audible.com/pd/Science-Technology/Lights-Out-Audiobook/B0143R30SY

Critical Infrastructure Sectors

This resource identifies the Critical Infrastructure Sectors that we will be discussing in class. Additional information is provided at the URL below.

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure.

PPD-21 identifies 16 critical infrastructure sectors are:

1. Chemical Sector
2. Commercial Facilities Sector
3. Communications Sector
4. Critical Manufacturing Sector
5. Dams Sector
6. Defense Industrial Base Sector
7. Emergency Services Sector
8. Energy Sector
9. Financial Services Sector
10. Food and Agriculture Sector
11. Government Facilities Sector
12. Healthcare and Public Health Sector
13. Information Technology Sector
14. Nuclear Reactors, Materials, and Waste Sector
15. Transportation Systems Sector
16. Water and Wastewater Systems Sector

http://www.dhs.gov/critical-infrastructure-sectors

United States Computer Emergency Readiness Team (US-CERT)

This resource identifies the United States Computer Emergency Readiness Team (US-CERT). Specifically, it provides some resources to help students prepare a plan to secure their home or small business. Additional information is provided at the URL below.

Home and Business: Explore the resources here to learn more about cybersecurity and to better secure your home and small-business networks.

https://www.us-cert.gov/home-and-business

Cybersecurity Awareness Training Version 2.0

This resource identifies some of the Cybersecurity training that is available to help students prepare for the future. Specifically, it provides some resources to help students prepare a plan to secure their home. Additional information is provided at the URL below.

The training course introduces the automated information systems (AIS) environment and the threats and vulnerabilities faced when working within the government or defense industrial systems. It provides a working knowledge of cyber intrusion methods and cybersecurity countermeasures to assist employees in preventing cyber-attacks and protecting their systems and information. The user experience centers on a single, large-scale, disastrous event. Several contributing scenarios are presented to show different vantage points related to the large event. Through the large event and associated contributing scenarios, students learn about different cyber threats and methods of operation, targeted information, countermeasures, and reporting requirements. This approach demonstrates for users that even small events can contribute and lead to immeasurable consequences.

NOTE: The course includes a printable certificate which can serve as evidence that a student completed the course. When a student takes the course using this link, CDSE will not maintain any record of that student by name or any personally identifiable information. If the student needs documentation that he or she has completed the course, he or she will have to print the certificate at the end of the course.

http://cdsetrain.dtic.mil/cybersecurity/

Course Schedule and Assignments:

Date	Session	Thinking about Cybersecurity: From Cyber Crime to Cyber Warfare	Chapter Reviews (Quiz)	Debate Questions on Discussion Board	Write Essays	Student Presentations	Exams
6/11/16 9:30 AM	1	Critical Thinking: Pretest		Introductions			
	1	Critical Thinking: Recognizing a Problem					
	1	Critical Thinking: Defining a Problem					
	1	Cyber Security: 1 Stuxnet—The First Cyber Guided Missile	1	Course Topics			
6/18/16 9:30 AM	2	Critical Thinking: Focused Observation					
	2	Critical Thinking: Brainstorming with Graphic Organizers					
	2	Cyber Security: 2 The Incredible Scope of Cyberspace					
	2	Cyber Security: The Five Gateways of Internet Vulnerability	2, 3	Course Topics			
6/25/16 9:30 AM	3	Critical Thinking: Setting Goals					
	3	Critical Thinking: Troubleshooting					
	3	Cyber Security: 4 Of Viruses, Botnets, and Logic Bombs					
	3	Cyber Security: 5 The Problem of Identity on the Network	4,5	Course Topics			
7/2/16 9:30 AM	4	Critical Thinking: Finding Resources			1250 Word Essay	Essay Topic 1	
	4	Critical Thinking: Evaluating Facts					
	4	Cyber Security: 6 Cyber Fraud, Theft, and Organized Crime					
	4	Cyber Security: 7 Hacktivists and Insurgency	6, 7	Course Topics			
7/9/16 9:30 AM	5	Critical Thinking: Persuasion Techniques					
	5	Critical Thinking: The Numbers Game					
	5	Cyber Security: 8 Nations at Cyber War					
	5	Cyber Security: 9 Government Regulation of Cyberspace	8,9	Course Topics			Exam 1
7/16/16 9:30 AM	6	Critical Thinking: Checking Your Emotions					
	6	Critical Thinking: Deductive Reasoning					
	6	Cyber Security: 10 International Governance and the Internet					
	6	Cyber Security: 11 The Constitution and Cyberspace	10, 11	Course Topics			
7/23/16 9:30 AM	7	Critical Thinking: Errors in Deductive Reasoning					
	7	Critical Thinking: Inductive Reasoning					
	7	Cyber Security: 12 Big Data—"They" Know Everything about You					
	7	Cyber Security: 13 Privacy for the Cyber Age	12, 13	Course Topics			
7/30/16 9:30 AM	8	Critical Thinking: Errors in Inductive Reasoning			1250 Word Essay	Essay Topic 2	
	8	Critical Thinking: Distracting Techniques					
	8	Cyber Security: 14 Listening In and Going Dark					
	8	Cyber Security: 15 The Devil in the Chips—Hardware Failures	14, 15	Course Topics			
8/6/16 9:30 AM	9	Critical Thinking: Making Judgement Calls					
	9	Critical Thinking: Explanation or Argument					
	9	Cyber Security: 16 Protecting Yourself in Cyberspace					
	9	Cyber Security: 17 Critical Infrastructure and Resiliency	16, 17	Course Topics			
8/13/16 9:30 AM	10	Critical Thinking: Critical Thinking for Exams					
	10	Critical Thinking: Putting It All Together					
	10	Critical Thinking: Posttest					
	10	Cyber Security: 18 Looking Forward—What Does the Future Hol	18	Course Topics			Exam 2

Course Requirements and Graded Course Components:

	Attendance / Class Discussion Participation	Chapter Reviews (Quiz)	Debate Questions on Discussion Board	Write Essays	Student Presentations	Exams	Totals
Percentage of Grade	10%	15%	15%	20%	15%	25%	100%
Points	100	150	150	200	150	250	1000

Course Assignments Overview:

In addition to classroom activities, during which students will be introduced to all of the Course Materials, including the Additional Resources, there will be a wide variety of Course Assignments and Activities. (For example, students will be asked to take Cybersecurity Awareness Training and present a certificate of completion.) These are summarized below for your convenience.

Chapter Reviews (Quiz)

Critical Thinking Pretest: This quiz measures how well students are prepared before taking the course to effectively apply Critical Thinking. It is a 30 question quiz which can be taken in class and easily graded. It can be used as an icebreaker event.

Cyber Security: These chapter reviews will review the primary points presented in the Cyber Security reading assignments as well as from the Critical Thinking book, and the Illustrated Book of Bad Arguments book. The Chapter Reviews will each consist of 10 to 20 Multiple Choice, True / False, and Short Essay questions.

Critical Thinking Posttest: This quiz measures how well students are prepared after taking the course to effectively apply Critical Thinking. It is a 30 question quiz which can be taken in class and easily graded. The class may want to compare results with the Pretest.

Debate Questions on Discussion Board

The Discussion Board will be used to allow students to exercise their Critical Thinking skills by discussing as a class some of the examples from the Critical Thinking book, the Illustrated Book of Bad Arguments book and the topics presented in the Cyber Security resources. The Discussion Board Topics may also be "freshened up" periodically with new examples from the many books on Critical Thinking. The Discussion Boards will each consist of between 3 and 7 questions, depending upon the complexity of the questions and their tendency to support lively debate.

Write Essays

Students will be asked to research, prepare and present cyber-security related topics in written and verbal forms. Students will be asked to write two (2) - 1,500 word essays on topics related to cyber security and our critical infrastructure. They will be asked to use their Critical Thinking skills to identify any logical fallacies (e.g., Slippery Slope) related to the topics and information sources they select. Students will be expected to identify 4-5 authoritative and relevant sources for their Essays. Of these, 2-3 may be from authoritative and relevant web sites (e.g., DHS.gov), given the speed of cyber-security's evolution and the highly-relevant cases that are occurring each day. Students will also be asked to properly construct arguments to support their case.

These are example Essay prompts:

> *Review recent Cyber Security-related world events where the needs for individual privacy came into conflict with the government's need to protect the US from threats (e.g., terrorist or criminal attacks). Where do you think we should draw the line between individual privacy and government surveillance?*

Research the laws that constrain an individual and / or a Corporation's ability to counter Cyber-attacks (for example, to counter-attack or to prosecute the attackers). Should the laws be changed?

Research the prevalence and frequency of Cyber-attacks. Consider the estimated cost (and techniques) to recover from and defend against Cyber-attacks for a Corporation or an individual. How significant are these costs?

How effective are the recent Cyber-attacks? Provide some examples.

How does the cost of defending against Cyber-attacks compare with the cost of potential damages from an attack?

What are the 16 Critical Infrastructure elements as identified by the Department of Homeland Defense? What is the impact of a successful attack against one of these sectors?

What can be done to protect yourself as an individual or as a small business from Cyber-attacks?

Student Presentations

Students will be asked to research, prepare and present cyber-security related topics in written and verbal forms. The student presentations will be 10-15 minutes in length, be presented in front of the class, and will be supported by appropriate visual aids (a PowerPoint presentation with 7-12 content slides). Students actively watching the presentations will be required to ask several insightful questions about the content, and to identify any possible errors in Critical Thinking - in order to earn Class Participation points.

Exams

There will be two (2) Exams. They will cover the Critical Thinking and Cyber Security topics presented in any of the Resources or Course Activities. The exams will each consist of 50 to 100 Multiple Choice, True / False, and Short Essay questions.

Course Final Grade:

The Final Course Grade		
Grade	Lower	Upper
A	93%	100%
A-	90%	93%
B+	87%	90%
B	83%	87%
B-	80%	83%
C+	77%	80%

C	73%	77%
C-	70%	73%
D	60%	70%
F	60%	0%

Credit Hour Policy Statement:

Students are expected to spend a minimum of two hours outside of the classroom each week for each unit of credit engaged in learning.

Final Exam Statement:

Students are expected to take the final exam on the last day of class as shown on the course schedule. The final will be presented online via a Cougar Course.

ADA Statement:

Students with disabilities who require reasonable accommodations must be approved for services by providing appropriate and recent documentation to the Office of Disabled Student Services (DSS). This office is located in Craven Hall 4300, and can be contacted by phone at (760) 750-4905, or TTY (760) 750-4909, and by email sent to dss@csusm.edu. Students authorized by DSS to receive reasonable accommodations should meet with me during my office hours in order to ensure confidentiality.

All-University Writing Requirement:

Students will be asked to write two (2) - 1,500 word essays on topics related to cyber security and our critical infrastructure.

Students will be asked to engage in a lively debate on questions related to course topics on a Discussion Board.

Students will be asked to answer Exam questions with Short Essays.

Course Format:

The Online Instruction Policy lists the following alternatives to face-to-face, traditional (FT) instruction: face-to-face, online (FO); local, online (LO); remote, online (RO); or hybrid (HY).

This course format will be:

Face-to-Face

Necessary Technical Competency Required of Students:

N/A – for online and hybrid courses.

Contact Information for Technical Support Assistance:

N/A – for online and hybrid courses.

Program Student Learning Outcomes (PSLOs):

See the General Education Program Student Learning Outcomes (GEPSLOs)

General Education Program Student Learning Outcomes (GEPSLOs)

	Upon completion of General Education coursework, students will be able to:	How GEPSLOs are addressed in the course and how students will be expected to achieve them.
1	Describe and/or apply principles and methods that are necessary to understand the physical and natural world.	Evaluate the various Critical Infrastructure Sectors (e.g., the Dams Sector) to understand the how the Dams and Cyber Security are inter-related.
2	Compare and contrast relationships within and between human cultures.	Evaluate the motives and motivations of potential cyber adversaries.
3	Communicate effectively in writing, using conventions appropriate to various contexts and diverse audiences.	Research, prepare and present cyber-security related topics in written and verbal forms.
4	Use oral communication to effectively convey meaning to various audiences.	Research, prepare and present cyber-security related topics in written and verbal forms. Participate in classroom discussions. Apply Critical Thinking tools and techniques from the book "Critical Thinking Skills."
5	Find, evaluate, and use authoritative and/or scholarly information to comprehend a line of inquiry.	Research, prepare and present cyber-security related topics in written and verbal forms.
6	Think critically and analytically about an issue, idea or problem, considering alternative perspectives and re-evaluation of one's own position.	Apply Critical Thinking tools and techniques from the book "Critical Thinking Skills." Research, prepare and present cyber-security related topics in written and verbal forms. Participate in classroom discussions.
7	Apply numerical/mathematical concepts in order to illustrate fundamental concepts within fields of study.	Research the magnitude of the cyber security issues and the impact of a cyber-attack on our Critical Infrastructure.
8	Describe the importance of diverse experiences, thoughts, and identities needed to be effective in working and living in diverse communities and environments.	Evaluate the various Critical Infrastructure Sectors (e.g., the Food and Agriculture Sector, Energy and Water Sectors) to understand how they and Cyber Security are inter-related.

9	Apply knowledge gained from courses in different disciplines to new settings and complex problems.	Evaluate the various Critical Infrastructure Sectors (e.g., the Healthcare Sector) to understand the how they and Cyber Security are inter-related.

How Course Materials Will Be Made Available:

Via Cougar Courses

Course Attendance Policy:

Course attendance policy is integrated with the course grading standards.

Full attendance and active (constructive) participation in classroom discussions is expected.

See Course Requirements and Graded Course Components.

Policy on Late / Missed Work:

All Assignments are Due on Saturday at Midnight unless noted otherwise:

If assignment is Late but is turned in ...	Penalty (Maximum)
Within 24 hours of the deadline	10% of the assignment's possible points
Within 24 to 48 hours of the deadline	20% of the assignment's possible points
Within 48 to 72 hours of the deadline	30% of the assignment's possible points
More than 72 hours after the deadline	50% of the assignment's possible points

Note: Once the solution of the assignment is discussed in the class or emailed no assignment will be accepted.

Note: This policy does not apply to exams.

Exams should be taken as scheduled and according to the relevant policies.

Student Collaboration Policy:

1. Students may only collaborate on assignments when explicitly authorized by the instructor. Unauthorized collaboration will be considered cheating. See the Academic Honesty Statement.
2. Students are expected to collaborate on assignments when explicitly authorized by the instructor. Failure to collaborate when it has been assigned will result in a reduction in the score assigned to each assignment.

Class Meeting Time and Location:

See Course Schedule and Assignments for class meeting times.

Course Location is specified in the Course Registration Information.

Academic Honesty Statement:

Students will be expected to adhere to standards of academic honesty and integrity, as outlined in the Student Academic Honesty Policy. All assignments must be original work, clear and error-free. All ideas/material that are borrowed from other sources must have appropriate references to the original sources. Any quoted material should give credit to the source and be punctuated accordingly.

Academic Honesty and Integrity: Students are responsible for honest completion and representation of their work. Your course catalog details the ethical standards and penalties for infractions. There will be zero tolerance for infractions. If you believe there has been an infraction by someone in the class, please bring it to the instructor's attention. The instructor reserves the right to discipline any student for academic dishonesty, in accordance with the general rules and regulations of the university. Disciplinary action may include the lowering of grades and/or the assignment of a failing grade for an exam, assignment, or the class as a whole.

Students are referred to the full Academic Honesty Policy at

https://www.csusm.edu/policies/active/documents/Academic_Honesty_Policy.html

Class Behavior Expectations:

Students in this class are expected to follow these basic principles:

- Demonstrate respect for oneself and for others.
- Treat other with dignity and behave in a way which promotes a physically and psychologically safe, secure, and supportive climate.
- Allow all community members to engage as full and active participants where the free flow of ideas is encouraged and affirmed.
- Students are expected to uphold the highest expectations for 'netiquette'.

Ethics:

Ethical behavior in the classroom is required of every student. The course will identify ethical policies and practices relevant to course topics.

Technology:

Students are expected to be competent in using current technology appropriate for this discipline. Such technology may include word processing, spreadsheet, and presentation software. Use of the internet and e-mail may also be required.

Diversity:

Learning to work with and value diversity is essential in every class. Students are expected to exhibit an appreciation for multinational and gender diversity in the classroom.

Civility:

As a diverse community of learners, students must strive to work together in a setting of civility, tolerance, and respect for each other and for the instructor. Rules of classroom behavior (which apply to online as well as onsite courses) include but are not limited to the following:

1. Conflicting opinions among members of a class are to be respected and responded to in a professional manner.
2. Side conversations or other distracting behaviors are not to be engaged in during lectures, class discussions or presentations
3. There are to be no offensive comments, language, or gestures

Change Statement:

This syllabus is "subject to change."

Area-Specific General Education Requirements:

The General Education area-specific requirements (formerly called General Education Learning Outcomes, or GELOs) the course satisfies, and how these requirements are addressed in the course are discussed above.

Student Responsibility for Add/Drop Deadlines:

Students are responsible for understanding all processes and timelines associated with adding or withdrawing from a course. Published detailed information can be found with the Class Schedule on the CSUSM website.

Student Responsibility for Assignment Deadlines and Failed Technology:

Assume that technology will fail at some point. Do not assume that everything will go smoothly when it comes to computers. Plan ahead. Do not leave completion/submission of assignments/projects for the last possible moment.

Tips and Suggestions for Student Success in the Course:

Read to the book chapters several times. Take notes.

Research the Critical Infrastructure Sectors and other topics using the Additional Resources noted.