COURSE OUTLINE: NASA205 - CISSP PREP

Prepared: Dr. Michael Biocchi
Approved: Martha Irwin, Dean, Business and Information Technology

Course Code: Title	NASA205: CISSP PREPARATION
Program Number: Name	2196: NETWRK ARCH & SEC AN
Department:	COMPUTER STUDIES
Academic Year:	2024-2025
Course Description:	This course provides a comprehensive review of information security concepts and industry best practices. Students will learn concepts and best practices from the eight domains of the CISSP Common Body of Knowledge: Security and Risk Management, Asset Security, Security Engineering, Communications and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security.
Total Credits:	4
Hours/Week:	4
Total Hours:	56
Prerequisites:	There are no pre-requisites for this course.
Corequisites:	There are no co-requisites for this course.
Essential Employability Skills (EES) addressed in this course:	EES 2 Respond to written, spoken, or visual messages in a manner that ensures effective communication. EES 3 Execute mathematical operations accurately. EES 4 Apply a systematic approach to solve problems. EES 5 Use a variety of thinking skills to anticipate and solve problems. EES 7 Analyze, evaluate, and apply relevant information from a variety of sources. EES 10 Manage the use of time and other resources to complete projects. EES 11 Take responsibility for ones own actions, decisions, and consequences.
Course Evaluation:	Passing Grade: 50%, A minimum program GPA of 2.0 or higher where program specific standards exist is required for graduation.
Other Course Evaluation & Assessment Requirements:	A+ = 90-100% A = 80-89% B = 70-79% C = 60-69% D = 50-59% F < 50% Students are expected to be present to write all tests in class, unless otherwise specified. If a student is unable to write a test due to illness or a legitimate emergency, that student must contact the professor prior to class and provide reasoning. Should the student fail to contact the

professor, the student shall receive a grade of zero on the test.

If a student is not present 10 minutes after the test begins, the student will be considered absent and will not be given the privilege of writing the test.
Students exhibiting academic dishonesty during a test will receive an automatic zero. Please refer to the College Academic Dishonesty Policy for further information.

In order to qualify to write a missed test, the student shall have:
a.) attended at least 75% of the classes to-date.
b.) provide the professor an acceptable explanation for his/her absence.
c.) be granted permission by the professor.

NOTE: The missed test that has met the above criteria will be an end-of-semester test.

Labs / assignments are due on the due date indicated by the professor. Notice by the professor will be written on the labs / assignments and verbally announced in advance, during class.

Labs and assignments that are deemed late will have a 10% reduction per academic day to a maximum of 5 academic days at 50% (excluding weekends and holidays). Example: 1 day late - 10% reduction, 2 days late, 20%, up to 50%. After 5 academic days, no late assignments and labs will be accepted. If you are going to miss a lab / assignment deadline due to circumstances beyond your control and seek an extension of time beyond the due date, you must contact your professor in advance of the deadline with a legitimate reason that is acceptable.

It is the responsibility of the student who has missed a class to contact the professor immediately to obtain the lab / assignment. Students are responsible for doing their own work. Labs / assignments that are handed in and are deemed identical or near identical in content may constitute academic dishonesty and result in a zero grade.

Students are expected to be present to write in-classroom quizzes. There are no make-up options for missed in-class quizzes.

Students have the right to learn in an environment that is distraction-free, therefore, everyone is expected to arrive on-time in class. Should lectures become distracted due to students walking in late, the professor may deny entry until the 1st break period, which can be up to 50 minutes after class starts or until that component of the lecture is complete.

The total overall average of test scores combined must be 50% or higher in order to qualify to pass this course. In addition, combined tests, Labs / Assignments total grade must be 50% or higher.

Books and Required Resources:

CISSP: Certified Information Systems Security Professional Official Study Guide by Mike Chapple, James M. Stewart, Darril Gibson
Publisher: Sybex Edition: 9th
ISBN: 978-1-119-78623-8

Course Outcomes and Learning Objectives:

Course Outcome 1	Learning Objectives for Course Outcome 1
1. Security and Risk Management	1.1 Understand and apply concepts of confidentiality, integrity, and availability 1.2 Evaluate and apply security governance principles 1.3 Determine compliance requirements 1.4 Understand legal and regulatory issues that pertain to information security in a global context

	1.5 Understand, adhere to, and promote professional ethics 1.6 Develop, document, and implement security policy, standards, procedures, and guidelines 1.7 Identify, analyse, and prioritise Business Continuity Requirements 1.8 Contribute to and enforce personnel security policies and procedures 1.9 Understand and apply risk management concepts 1.10 Understand and apply threat modeling concepts and methodologies 1.11 Apply risk-based management concepts to the supply chain 1.12 Establish and maintain a security awareness, education, and training program
Course Outcome 2	**Learning Objectives for Course Outcome 2**
2. Asset Security	2.1 Identify and classify information and assets 2.2 Determine and maintain information and asset ownership 2.3 Protect privacy 2.4 Ensure appropriate asset retention 2.5 Determine data security controls 2.6 Establish information and asset handling requirements
Course Outcome 3	**Learning Objectives for Course Outcome 3**
3. Security Architecture and Engineering	3.1 Implement and manage engineering processes using secure design principles 3.2 Understand the fundamental concepts of security models 3.3 Select controls based upon systems security requirements 3.4 Understand security capabilities of information systems 3.5 Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements 3.6 Assess and mitigate vulnerabilities in web-based systems 3.7 Assess and mitigate vulnerabilities in mobile systems 3.8 Assess and mitigate vulnerabilities in embedded devices 3.9 Apply cryptography 3.10 Apply security principles to site and facility design 3.11 Implement site and facility security controls
Course Outcome 4	**Learning Objectives for Course Outcome 4**
4. Communication and Network Security	4.1 Implement secure design principles in network architectures 4.2 Secure network components 4.3 Implement secure communication channels according to design
Course Outcome 5	**Learning Objectives for Course Outcome 5**
5. Identity and Access Management	5.1 Control physical and logical access to assets 5.2 Manage identification and authentication of people, devices, and services 5.3 Integrate identity as a third-party service 5.4 Implement and manage authorization mechanisms 5.5 Manage the identity and access provisioning life cycle

Course Outcome 6	Learning Objectives for Course Outcome 6
6. Security Assessment and Testing	6.1 Design and validate assessment, test, and audit strategies 6.2 Conduct security control testing 6.3 Collect security process data 6.4 Analyse test output and generate report 6.5 Conduct or facilitate security audits
Course Outcome 7	**Learning Objectives for Course Outcome 7**
7. Security Operations	7.1 Understand and support investigations 7.2 Understand requirements for investigation types 7.3 Conduct logging and monitoring activities 7.4 Securely provisioning resources 7.5 Understand and apply foundational security operations concepts 7.6 Apply resource protection techniques 7.7 Conduct incident management 7.8 Operate and maintain detective and preventive measures 7.9 Implement and support patch and vulnerability management 7.10 Understand and participate in change management processes 7.11 Implement recovery strategies 7.12 Implement Disaster Recovery processes 7.13 Test Disaster Recovery Plans 7.14 Participate in Business Continuity planning and exercises 7.15 Implement and manage physical security 7.16 Address personnel safety and security concerns
Course Outcome 8	**Learning Objectives for Course Outcome 8**
8. Software Development Security	8.1 Understand and integrate security in the Software Development Life Cycle 8.2 Identify and apply security controls in development environments 8.3 Assess the effectiveness of software security 8.4 Assess security impact of acquired software 8.5 Define and apply secure coding guidelines and standards

Evaluation Process and Grading System:

Evaluation Type	Evaluation Weight
Quizzes	25%
Test: Domain 1-2	15%
Test: Domain 3	15%
Test: Domain 4-6	20%
Test: Domain 7-8	25%

Date: June 16, 2024

Addendum: Please refer to the course outline addendum on the Learning Management System for further information.