CSEC - 3755 - Defensive Cyber Operations

04. UG Course Modification (No Special Designation)

Due Dates and Resources

If you have questions or need assistance in filling out this proposal form, you may contact the Office of Curriculum.

Deadlines for curriculum can be found:

- Curriculum SharePoint
- Curriculum Website
- Procedural Calendar
- On your Curriculog dashboard under 'My Upcoming Events'

In order to meet the deadline, this proposal must be on the *Nonsubstantive, Substantive Colleg/School, OR Substantive University Level Review* step on or before the listed due date. Which step will depend on the changes being made.

Resources for curriculum can be found:

- Originator How-To Guide
- Curriculum SharePoint

This form **SHOULD** be used for the following:

- Modification of a course **without** a special designation (General Studies, Service Learning, Ethnic Studies & Social Justice, or Senior Experience).

This form **SHOULD NOT** be used for the following:

- Modifying a course with a special designation (General Studies, Service Learning, Ethnic Studies & Social Justice, or Senior Experience).
- Creating a new course with or without a special designation (General Studies, Service Learning, Ethnic Studies & Social Justice, or Senior Experience).
- Creating or

modifying a
graduate course.

Directions for Form

General Instructions and Information

You may collapse individual sections of this form by clicking the arrow or "V" icon to the right of the section title.
All fields that are marked with an asterisk (*) are required.
Each section may have additional directions attached. Please follow instructions.

Note: Proposals that are incomplete or filled out incorrectly will be returned to the originator.

INSTRUCTIONS FOR MODIFYING AN EXISTING COURSE

Import the course you wish to modify.
Fill out Part I of the form.

Carefully follow the instructions on selecting the level of review your proposal requires. Incorrect review selection will require a resubmission of the proposal.

LAUNCH the proposal.
Fill out Part II to indicate all the modifications you make to the course.
Modify any course fields in Part III as needed.

Modification Note: DO NOT MAKE CHANGES TO YOUR COURSE INFORMATION (PART III) UNTIL AFTER YOU LAUNCH THE PROPOSAL in order to track changes. Failure to use the track changes feature may cause a delay or denial of your proposal.
If you modify additional fields not already indicated in Part II, please make sure you add them to the modification list.

Approve the proposal.

Use the checkmark icon on the right of the screen to approve the proposal.

Part I: Department and Originator Information (Fill out BEFORE launching the proposal)

If you are changing course ownership, please list both departments and if applicable, both college/schools.

College/School:* College of Aerospace, Computing, Engineering, and Design

Department:* Department of Computer Sciences

Name of Proposal Originator* Klaus Streicher

Email of Proposal Originator* Nstreich@msudenver.edu

Justification and Resource Implication for Curriculum Proposal:*

CSEC 3755 Defensive Cyber Operations:

Cyber operations encompass both offensive and defensive operations. Defensive operations are needed to protect computer systems and networks from attack. Also, it is essential that cyber operators understand how defense compliments offense.

This course will now serve as a core course and supports NSA CAE-CO & ABET learning outcomes for the proposed Computer Security degree.

Related Curriculum Proposals:* https://msudenver.curriculog.com/proposal:11729/form

Impact Report Results:*

Impact Report for CS 3755

There are no results for this report.

Course Modification Level Review

The modification level review question will determine the workflow of this proposal, so it is essential you select the correct one. Please consult this tool which will help you determine the review level you need. If you select a level of review that does not include the changes you make to the course, this proposal will be denied and you will have to resubmit a new proposal. If you are unsure which level of review you need to select, please contact the Curriculum Staff here.

Note: Changing the level of review after launching the proposal will not change the workflow. If you discover that you have selected an incorrect review level post-launch, you must submit a new proposal. You can contact the Curriculum Office to delete the incorrect proposal.

Course Modification Level Review Selection:* ○ Nonsubstantive ○ Substantive College/School Level ◉ Substantive University Level

According to the Undergraduate Curriculum Manual, it is the responsibility of both the originator as well as each level of review to consider potential overlap and curriculum conflict. Any potential overlap or conflict with existing curriculum should be reviewed, and the impacted department(s) should be requested to provide a letter of notification or support, depending on the circumstances. Attach documentation that supports affected Departments were notified and/or provided support of the proposed changes in the Proposal Toolbox by clicking on the paperclip icon on the right side of the form.

Please Confirm That:* ☑ I, the originator of this proposal, have completed the necessary due diligence to review this proposal for any potential overlap and/or conflict with existing curriculum. Any departments identified as having potential overlap and/or conflicts have been contacted and a letter of notification and/or a letter of support has been obtained.

Part II: Course Modification Information

Reminder: This form CANNOT be used to change courses with special designations (Ethnic Studies & Social Justice, Service Learning, Senior Experience, General Studies). If you submit a course with special designation(s) with this form, it will be denied and you will need to resubmit.

Please indicate on the below list all of the course modifications you are making. **Please do not make changes to sections you do not specify are being modified and make sure to select ALL sections that you modify.**

Specify which sections have been modified (check all that apply):
- ☑ Part IIIa (prefix, course number, course title, transcript/banner course title, course type, CIP code)
- ☑ Part IIIb (credits, distribution of credits, schedule type, grade mode, contact hours, repeats, equivalencies, crosslistings, registration restrictions)
- ☑ Part IIIc (prerequisites, corequisites, or prerequisite(s)/corequisite(s), banner enforced prerequisites, corequisites, or prerequisite(s)/corequisite(s), catalog course description, catalog note, lab fees, field trips)
- ☑ Part IIId (required reading, SBLOs, outline, evaluation of student performance)

If the course modification includes changing prefixes, is it a new prefix?
- ☑ Yes
- ☐ No
- ☐ N/A

Reminder: DO NOT MAKE CHANGES TO YOUR COURSE INFORMATION (PART IIIa-IIId) UNTIL AFTER YOU LAUNCH THE PROPOSAL in order to track changes. Failure to use the track changes feature may cause a delay or denial of your proposal.

If you modify additional sections not already indicated, please make sure you add them to the modification checklist.

Part IIIa: Course Information

Prefix:* CSEC

Course Number:* 3755

Course Title:* Defensive Cyber Operations

Transcript/Banner Defensive Cyber Operations

Transcript/Banner Course Title:* Defensive Cyber Operations

Course Type:* Computer Security

CIP Code: 11.1003

Part IIIb: Course Information, continued

Please check all that apply from the selections below. You may select more than one option if applicable.

Check All that Apply:*
- [x] Required for Major
- [ ] Required for Minor
- [ ] Required for Concentration
- [ ] Required for Certificate
- [x] Elective
- [ ] Specified Elective

To receive Title IV financial aid funds, all institutions of higher education must comply with the federal definition of a credit hour. The Higher Learning Commission requires institutions to maintain policies and procedures for verifying compliance with this definition.

Federal Credit Hour Definition: *A credit hour is an amount of work represented in intended learning outcomes and verified by evidence of student achievement that is an institutionally-established equivalency that reasonably approximates not less than:*
(1) one hour of classroom or direct faculty instruction and a minimum of two hours of out-of- class student work each week for approximately fifteen weeks for one semester or trimester hour of credit, or ten to twelve weeks for one quarter hour of credit, or the equivalent amount of work over a different amount of time; or (2) at least an equivalent amount of work as required in paragraph (1) of this definition for other activities as established by an institution, including laboratory work, internships, practica, studio work, and other academic work leading toward to the award of credit hours. 34CFR 600.2 (11/1/2010)

Credits:* 4

Distribution of Credits:* 4+0

Schedule Type(s):* Lecture

Grade Mode(s):* Letter

Face-to-Face or Equivalent Hours per course

Consult Appendix B and C of the Curriculum Manual to determine the hours for the course

Lecture: 50

Lab:

Internship:

Practicum:

Other Hours:

Additional Student Work Hours: 120

Please answer yes or no to the below questions. If you answer yes to any of the questions, please fill out the related field on the right.

A specified repeatable course is a course that allows a student to repeat the course either in its entirety or for a certain identified total number of credit hours. If you decide to make your course repeatable, please specify either how many times a student can repeat the course for credit, or for the total number of credits they can receive.

Is this course a specified repeatable course?* (•) No ( ) Yes

If yes, indicate specified repeatable number of credits and/or repeats allowed:

Is this course a variable topics umbrella course?* (•) No ( ) Yes

If yes, indicate variable topic number of credits and/or repeats available:

A crosslisting is when a course is made available under additional prefixes for students in other programs.

An equivalency is when two courses are coded in Banner to be equal to each other.

Generally equivalencies are used when an old, archived course is needed to be equal to a new course. Crosslistings are used for all active courses. Supporting documentation should be included to demonstrate approval for crosslistings.

Are there course equivalencies?* (•) No ( ) Yes

If yes, list all equivalent courses in alphabetical order:

Are there course crosslistings?* (•) No ( ) Yes

If yes, list all crosslistings in alphabetical order:

Registration Restrictions

Program:

Major:

Level: Undergraduate

Class:

Student Attribute:

Part IIIc: Course Information, continued

The following fields will allow you to attach prerequisites, corequisites, or prerequisites or corequisites to your course. Please specify if you want and of these prerequisites, corequisites, or prerequisites or corequisites Banner enforced.

Banner enforcement means that the requirement will be enforced when the student attempts to register for a course. If you do not Banner enforce the requirement, the system will not check the student's record for the requirement to be met.

Please also indicate the minimum passing grade.

Prerequisite(s):	CS 3700 AND CS 3750
Banner Enforced Prerequisite(s):	CS 3700 AND CS 3750
Minimum Passing Grade for Banner Enforced Prerequisite(s):	C- or T
Corequisite(s):	
Banner Enforced Corequisite(s):	
Prerequisite(s) or Corequisite(s):	
Banner Enforced Prerequisite(s) or Corequisite(s):	
Minimum Passing Grade for Banner Enforced Prerequisite(s) or Corequisite(s):	
Catalog Course Description:*	Students develop the skills and knowledge necessary to defend against sophisticated cyber threats by engaging in adversarial thinking. They learn to anticipate and counteract potential adversaries' actions, identify and mitigate software vulnerabilities, and implement robust security measures through a combination of theoretical instruction and hands-on practice. The course includes essential system administration tasks, network security, and the detection and removal of malicious activity. By applying these skills, students practice securing systems and data, responding to cyber incidents, and maintaining infrastructure integrity.

The note field DOES show up in the course listing in the university catalog. A note should be made in specific instances where additional information about a course needs to be conveyed to students. The most common reasons for adding a note are:

The course is crosslisted Example: *(Note: Credit will be granted for only one prefix.)*
Variable credit courses Example: *(Note: Variable Credit)*
A course is repeatable Example: *(Note: This course may be repeated up to 3 times under different topics)* OR *(Note: This course is repeatable for a maximum of six semester hours)*
If a student cannot take two courses and earn credit for both Example: *(Note: Students cannot earn credit for XXX1234 and XXX2345)*

Note:

Lab Fees: **Field Trips:**

Part IIId: Course Information, continued

The following section is the course content.

Required reading: Please list materials in preferred citation style (eg. MLA, APA, etc.).

List each material in this format. If there are multiple material please format them in a bullet or list style

Specific Measurable Student Behavioral Learning Objectives: Please list the SBLOs in your preferred numbering or bulleting style. Start section with: Upon completion of this course, the student should be able to:.
Detailed Outline of Course Content or Outline of Field Experience/Internship: Please list the course outline in your preferred numbering or bulleting style. It is recommended that you use a numbering format for this field.
Evaluation of Student Performance: Please list the evaluation of student performance in your preferred numbering or bulleting style.

You must use the numbering list feature within the toolbar above each field. Right click on a number in the list and select "Numbered List Properties" to change the numbering style. Please maintain consistency in the selected numbering or bulleting styles.

Reminder: DO NOT MAKE CHANGES TO YOUR COURSE INFORMATION (PART IIIa-IIId) UNTIL AFTER YOU LAUNCH THE PROPOSAL in order to track changes. Failure to use the track changes feature may cause a delay or denial of your proposal.

If you modify additional sections not already indicated, please make sure you add them to the modification checklist.

Required reading and other materials will be equivalent to:*

Bertram, A. (2020). *PowerShell for Sysadmins: Workflow Automation Made Easy*. No Starch Press.

Farhi, D., & Aleks, N. (2024). *Black Hat Bash: Creative Scripting for Hackers and Pentesters*. No Starch Press.

Forshaw, J. (2024). *Windows Security Internals: A Deep Dive into Windows Authentication, Authorization, and Auditing*. No Starch Press.

Specific, Measurable Student Behavioral Learning Objectives:*

Upon completion of this course, students should be able to

1. Apply adversarial thinking to anticipate the strategic actions of adversaries
2. Identify common programming errors that lead to vulnerabilities.
3. Develop secure software following best practices.
4. Create and implement firewall rules given high-level objectives.
5. Perform system administration tasks on the command-line and using scripts in Windows and Unix-based environments.
6. Scan networks and computer systems to discover vulnerabilities.
7. Secure computer systems and data from tampering and unauthorized access.
8. Patch vulnerabilities in operating systems and software.
9. Detect and remove malware from computer systems.
10. Detect malicious activity in computer systems and networks.

Detailed Outline of Course Content (Major Topics and Subtopics) or Outline of Field Experience/Internship *

1. **Software Security Vulnerabilities**
    1. **Common Vulnerabilities (e.g., Buffer Overflows, SQL Injection, Cross-Site Scripting)**
    2. **Understanding the OWASP Top Ten**
    3. **Vulnerability Discovery Techniques (e.g., Code Review, Static Analysis)**
    4. **Vulnerability Mitigation Strategies**
2. **Secure Software Development Practices**
    1. **Principles of Secure Coding**
    2. Incorporating Security into the Software Development Life Cycle (SDLC)
    3. Secure Design Patterns and Principles
    4. Threat Modeling and Risk Assessment
    5. Code Reviews and Static/Dynamic Analysis Tools
    6. **Continuous Integration and Deployment (CI/CD) Security**
3. **Software Security Testing**
    1. **Types of Security Testing (e.g., Unit, Integration, Penetration Testing)**
    2. Automated vs. Manual Testing Techniques
    3. Use of Fuzz Testing for Vulnerability Discovery
    4. Security Test Planning and Execution
    5. Reporting and Remediation of Security Findings
4. Firewalls
    1. Types of Firewalls (e.g., Packet Filtering, Stateful Inspection, Next-Gen Firewalls)
    2. Firewall Configuration and Rule Management
    3. Implementing Access Controls and Policies
    4. Intrusion Prevention Systems (IPS) Integration
    5. Monitoring and Responding to Firewall Alerts
5. Operating System Hardening
    1. Applying Security Patches and Updates
    2. Configuration of Security Settings (e.g., Disable Unnecessary Services)
    3. Implementing Least Privilege and Access Control
    4. Securing User Accounts and Authentication
    5. Kernel Hardening Techniques and Tools
6. Scripting

1. Writing Scripts for Automated Defense (e.g., Python, Bash, PowerShell)
2. Automating Security Monitoring and Response Tasks
3. Developing Custom Security Tools and Utilities
4. Scripting for Incident Response and Forensics
5. Maintaining Secure Script Repositories

7. Vulnerability Scanners
    1. Overview of Popular Vulnerability Scanners (e.g., Nessus, OpenVAS, Qualys)
    2. Configuring and Running Vulnerability Scans
    3. Analyzing and Prioritizing Scan Results
    4. Integrating Vulnerability Scanning into Routine Security Operations
    5. Managing False Positives and Negatives
8. Patching
    1. Patch Management Process and Best Practices
    2. Identifying and Prioritizing Critical Patches
    3. Automating Patch Deployment
    4. Verifying Patch Effectiveness and Compliance
    5. Rollback Procedures and Patch Testing
9. Malware Detection
    1. Types of Malware (e.g., Viruses, Trojans, Ransomware, Rootkits)
    2. Detection Techniques (e.g., Signature-Based, Behavior-Based, Heuristic Analysis)
    3. Analyzing Malware Behavior and Patterns
    4. Using Anti-Malware Tools and Platforms
    5. Implementing Advanced Detection Methods (e.g., Machine Learning)
10. Indicators of Compromise (IOCs)
    1. Defining and Identifying IOCs
    2. IOC Collection and Analysis Techniques
    3. Utilizing IOCs in Threat Intelligence
    4. Sharing and Consuming IOCs (e.g., STIX, TAXII)
    5. Case Studies of IOC Usage in Cyber Defense
11. Log Analysis
    1. Understanding Log Types (e.g., System, Application, Security Logs)
    2. Log Management Best Practices
    3. Analyzing Logs for Anomalous Activity
    4. Using SIEM (Security Information and Event Management) Tools for Correlation
    5. Automating Log Analysis and Alerting
12. Process and File Activity Monitors

1. Monitoring Tools and Techniques (e.g., Sysmon, OSSEC)

2. Identifying Suspicious Process and File Activities
3. Correlating Process and File Activities with Threat Indicators
4. Developing Baselines and Detecting Deviations
5. Mitigating and Responding to Detected Threats

13. Network Activity Monitors

1. Network Traffic Analysis Fundamentals
2. Tools for Network Monitoring (e.g., Wireshark, Zeek, Suricata)
3. Detecting Anomalous and Malicious Network Behavior
4. Implementing Network Segmentation and Micro-Segmentation
5. Responding to Network-Based Threats

Evaluation of Student Performance:* Student evaluations can include asessments of the following types:

1. Homework assignments
2. Projects
3. Quizzes and/or exams
4. Active participation

CAEPD and Registrar's Office Use Only

Notes An exception is being made for this course to be included in the catalog addendum. The reason it would not have been without the exception is because a proposal that adds a course prerequisite on a course is not allowed for the addendum. However, due to the circumstances of the proposals, this will be allowed for this proposal during this addendum cycle.

This course modification will be effective for the University 2025-2026 Undergraduate Catalog via the Summer 2025 Catalog Addendum and will be available in Banner beginning in Spring 2026.

Form updated May 2024