

# CIS - 2772 - Security Operations Center

## XXX 3.0 New Course Proposal

### Section I: Submission Information

Submission and Meeting Dates\* 9/6/2021 for meeting ~~10/1/2021~~ 11/5/2021

Faculty Proposer(s)\* Dr. Melinda Lyles and Dr. Mary Myers

Faculty Presenter\* Dr. Melinda Lyles and Dr. Mary Myers

Hierarchy Owner (Department)\*

Activity Log

Melinda Lyles

+ 2. Department of Computer Science

2. Computer Science

List of department/program faculty who support this proposal\*

Dr. Mary Myers

Dr. Roger Webster

Prof. David Piro

Does this course already exist in SCNS (already being offered at other state colleges and universities)?\*

Activity Log

Melinda Lyles

+ Yes

Yes

Is this an "experimental course" that you intend to offer 3 or fewer times?\*

Activity Log

Melinda Lyles

+ No

No

Course Prefix\*

Activity Log

Melinda Lyles

+ CIS

CIS

Course Number\* 2772

New Course Prefix N/A

Course Title\* Security Operations Center

Course Description\* Introduction to trending and in-demand technical skills that focus on the fundamentals of Security Operations Center (SOC) operations. Practice in relaying the knowledge of log management and correlation, Security Information and Event Management (SIEM) deployment, advanced incident detection, and incident response.

Justification for new course\* This course is being added as a requirement for the new AS Cybersecurity Operations Degree degree. The state frameworks require a course in the fundamentals of management within a Security operations center Operations Center.

Is this course replacing an existing FSW course?\*

Activity Log

Melinda Lyles

+ No

No

Was a change of course prefix/number requested by SCNS?\*

Activity Log

Melinda Lyles

+ No

Yes  No  N/A

Indicate the course prefix and number of the course to be replaced.\*

N/A

Will the new course be equivalent to the course it is replacing?\*

Activity Log

Melinda Lyles

+ N/A

Yes  No  N/A

Are you submitting a Course Discontinuation proposal for the course that is being replaced?\*

Activity Log

Melinda Lyles

+ N/A

Yes  No, not at this time  N/A

## Section II: Effective Dates

Published Effective Date for approved action\*

Melinda Lyles  
+ Fall 2022

Activity Log

Fall 2022

Requested Effective Date for Exception\*

Melinda Lyles  
+ N/A

Activity Log

N/A

Reason for requesting exception to effective date\*

N/A

## Section III: Proposed Course Requirements

Are you proposing any of the designations under K, L, or M be assigned to this course?\*

Melinda Lyles  
+ No

Activity Log

No

A. Course Prerequisites\*

CTS 1120 Security Fundamentals 2420 with (with 1314 with a grade of "C" or above better better) better

B. Course Corequisites\*

None

B. Is this course listed as a corequisite on a paired course?\*

Melinda Lyles  
+ No

Activity Log

Yes  No

B. If Yes, please enter the prefix, number, and title of the paired course.

N/A

**C. Topic Outline\***

- **Security Operations operations Center Operations Center (SOC) management**
- **SOC roles and Management management responsibilities**
- **Characteristics of a modern SOC**
- **Develop SOC assessment standards**
- **Cyber Threats threats, Indicator Indicators of Compromise (IoC) (IoCs); and Attack Incidents attack incidents (IOC)**
- **Incidents, Events events, and Logging logging Using threat intelligence to focus detection efforts**
- **Incident Detection detection with Security Information and Event Management (SIEM)**
- **Enhanced Incident Detection incident detection with Threat Intelligence threat intelligence Incident Response response Building, training and empowering an Incident Response Team (IRT)**

**D. Minimum grade required to pass the course\*** **C**

**E. Course Credits or Clock Hours\*** **3 Credits**

**F. Contact Hours (Faculty Load)\*** **3**

**F. Do the contact hours differ from the course/lecture/lab credits?\***

**Activity Log**

Melinda Lyles

+ **No**

Yes

No

**F. If Yes, please explain.**

**G. Grade Mode\***

**Activity Log**

Melinda Lyles

+ **Standard Grading (A-F)**

Standard Grading (A-F)

**H. Credit Type\***

**Activity Log**

Melinda Lyles

+ **College Credit**

College Credit

**I. Should any Program Restrictions be listed on this course?\***

**Activity Log**

Melinda Lyles

+ No

Yes

No

**I. List all program restrictions**

**J. Is this course repeatable for credit?\***

**Activity Log**

Melinda Lyles

+ No, course is not repeatable for credit

Yes, course is repeatable for credit

No, course is not repeatable for credit

**J. If course is repeatable, list the maximum number of credits the student may earn (including the first passing attempt).**

**K. Will this course be designated General Education (GE)?\***

**Activity Log**

Melinda Lyles

+ No

Yes  No

**L. Will this course be designated Writing Intensive (WI)?\***

**Activity Log**

Melinda Lyles

+ No

Yes  No

**M. Will this course be designated International or Diversity (I) focus?\***

**Activity Log**

Melinda Lyles

+ No

Yes  No

**If you checked Yes to any question K, L, M, please provide justifications for including the designation(s) on this new course.**

N/A

**Section IV: Syllabus Course Competencies and Learning Outcomes**

**Integral GE Course Competencies and supporting Course Learning Outcomes\***

**General Education Competency: Evaluate Think**

**Course Outcomes outcomes or Objectives Supporting objectives supporting the General Education Competency Selected competency:**

- **Describe SOC Security Operations Center (SOC) processes; procedures Compare and contrast attacker Implement ethical hacking tools, technologies tactics, and workflows procedures to identify Indicators of Compromise (IOCs) (IOC) that can be utilized during active and future investigations.**
- **Coordinate a prevention strategy using demonstrated knowledge of security threats, attacks, and vulnerabilities.**

**Supplemental GE Competencies and supporting Course Learning Outcomes\***

**N/A**

**Is this course identified by the State in FAC Rule 6A 14.0303 as a General Education Core course?\***

**Activity Log**

Melinda Lyles

+ No

No

**If YES, in which of the five General Education areas is this a Core course? (Drop down: Communication, Humanities, Social Sciences, Natural Sciences, Mathematics)\***

**Activity Log**

Melinda Lyles

+ Communication

Communication

**Additional Course Learning Outcomes\***

- Describe SOC processes, procedures, technologies, and workflows.
- Explain the importance of SOC and IRT collaboration for better improved incident response.
- Articulate the basic understanding and in-depth Develop a Cybersecurity Playbook using knowledge of security: threats SOC processes, attacks procedures, vulnerabilities; attacker's behaviors; cyber kill chain technologies, etc and workflows.
- Compare and contrast attacker tools; tactics; and procedures to identify indicators of compromise (IOCs) that can be utilized during active and future investigations: Demonstrate the ability to monitor and analyze logs and alerts from a variety of different technologies across multiple platforms (IDS/IPS; end-point protection; servers and workstations): Analyze Security security events and log collection; monitoring; and analysis: Administer SIEM solutions (such as: Splunk/AlienVault/OSSIM/ELK): Explain Explore the architecture, implementation, and fine tuning methods of improvement for SIEM solutions (such as: Splunk/ AlienVault/OSSIM/ELK) Splunk/AlienVault/OSSIM/ELK).
- Formulate threat cases (correlation rules) and create reports: Plan; organize; and perform threat monitoring and analysis in the enterprise Administer SIEM solutions (such as: Splunk/AlienVault/OSSIM/ELK).
- Identify emerging threat patterns and perform Perform a security threat analysis to apply through the application of a triaging process. Construct briefings Demonstrate the ability to monitor and reports analyze logs and alerts from a variety of analysis methodology different technologies across multiple platforms (IDS/IPS; end-point protection; servers; and workstations):
- Analyze security and assess cybersecurity events and by using log collection, monitoring, and results analysis software tools.
- Discover integrating Integrate threat intelligence into SIEM for enhanced incident detection and response.
- Compile Create an Incidence Response Plan using the Incident Response Process: Explain the importance of SOG and IRT collaboration for better incident response phases.
- Examine Indicators of Compromise (IOC) and assign ranks to risk level indicators.

**Section V: Impacts**

Will this new course be included in any programs or certificates?\*

Melinda Lyles  
+ Yes

**Activity Log**

Yes  No

List programs/certificates that will include this new course.\*

AS Cybersecurity Operations

Have you discussed the impact(s) with leaders of affected programs/department:\*

Activity Log

Melinda Lyles

+ Yes

Yes  No  N/A

## Section VI: State Information

Copy and paste the SCNS course profile description below (<http://scns.fldoe.org>)

THIS COURSE IS THE FIRST OF TWO ADVANCED CYBER-SECURITY COURSES WHERE STUDENTS LEARN CORE NETWORK SECURITY CONCEPTS AND TECHNIQUES THAT ARE NEEDED IN TODAY'S SECURITY OPERATIONS CENTER (SOC) TO MONITOR, ANALYZE, AND RESPOND TO THREATS ON A NETWORK USING A VARIETY OF SECURITY TOOLS. STUDENTS WILL ACQUIRE HANDS-ON EXPERIENCE ON HOW TO DETECT AND RESPOND TO SECURITY INCIDENTS WHILE PREPARING STUDENTS FOR THE CCNA CYBER-SECURITY OPERATIONS CERTIFICATION.

ICS code for this course\*

Activity Log

Melinda Lyles

+ Advanced and Professional - 1.16.07 - Computer & Info Science

Advanced and Professional - 1.16.07 - Computer & Info Science

Institutional Reporting Code\*

Activity Log

Melinda Lyles

+ 11607 Computer And Infor Science

11607 Computer And Infor Science

Course Attributes\*

Activity Log

Melinda Lyles

+ AA - AA Course

AA - AA Course



## Section VII: Attachments



List any related proposals that are being submitted for the same meeting that include this new course, or are directly linked to this proposal\*

The course ~~GTS1120-Network Security Fundamentals~~; is a prerequisite A New Program proposal for this course and is being presented to AS Cybersecurity Operations will be submitted for the committee this month as well 11/5/2021 meeting. This course will be included in that degree program.

## Steps for CIS - 2772 - Security Operations Center

<b>Originator</b>	<i>Status: Approved</i>
<b>Participants</b>  Melinda Lyles 10/8/2021 12:27 PM	
▼	
<b>Department Chair/Program Coordinator/Director</b>	<i>Status: Approved</i>
<b>Participants</b>  Mary Myers 10/8/2021 12:30 PM	
▼	
<b>Academic Dean</b>	<i>Status: Force Approved</i>
<b>Participants</b> ▲ <b>Academic Dean Committee - School of Business and Technology</b> Thomas Norman * ▲ <b>Additional Participants</b>	
▼	
<b>Curriculum Coordinator and Advising</b>	<i>Status: Restarted</i>
<b>Participants</b> ▲ <b>Office of the Registrar and Advising Committee</b> Jeffrey Peterman * ▲ <b>Additional Participants</b>	
▼	
<b>Curriculum Coordinator and Advising</b>	<i>Status: Restarted</i>
<b>Participants</b> ▲ <b>Office of the Registrar and Advising Committee</b> April Falso * Jeffrey Peterman * ▲ <b>Additional Participants</b>	
▼	
<b>Curriculum Coordinator and Advising</b>	<i>Status: Restarted</i>

**Participants**

▲ **Office of the Registrar and Advising Committee**

April Falso \*

Jeffrey Peterman \*

▲ **Additional Participants**

**Curriculum Coordinator and Advising**

Status: *Approved*

**Participants**

▲ **Office of the Registrar and Advising Committee**

✔ April Falso \* 10/22/2021 10:57 AM

**Office of Accountability (AASPIRE)**

Status: *Approved*

**Participants**

▲ **Office of Accountability (AASPIRE) Committee**

✔ D'ariel Barnard \* 10/25/2021 3:49 PM

**Curriculum Committee**

Status: *Approved*

**Participants**

▲ **Curriculum Committee**

[Curriculum Committee Nov. 5, 2021 meeting agenda](#)

■ ✔ Sheila Seelau \* 11/11/2021 11:16 AM

**Provost (Final Signature)**

Status: *Approved*

**Participants**

▲ **Provost Committee**

✔ Eileen DeLuca \* 11/15/2021 9:08 AM

**Office of Accountability (AASPIRE)**

Status: *Approved*

**Participants**

▲ **Office of Accountability (AASPIRE) Committee**

✔ D'ariel Barnard \* 11/15/2021 6:54 PM

**Office of the registrar-Curriculum Coordinator**

Status: *Working*

## Participants

## **Attachments for CIS - 2772 - Security Operations Center**

**CIS 2772 Integration Manager.pdf** (uploaded by Melinda Lyles, 10/8/2021 12:20 pm)  
**New Course CIS 2772 Security Operation Center.docx** (uploaded by Melinda Lyles, 10/8/2021 12:20 pm)      **SCNS Email 9-16-2021 multiple courses approved.pdf**  
(uploaded by Melinda Lyles, 10/8/2021 12:20 pm)      **CIS 2772 Reviewer comments - completed 10-10-2021.docx** (uploaded by Sheila Seelau, 10/10/2021 6:51 pm)      **CIS 2772 Security Operation Center syllabus 10-14-21.docx** (uploaded by Sheila Seelau, 10/14/2021 5:57 pm)      **CIS 2772 - Curriculum Committee Reviews\_10-25-2021.docx** (uploaded by Kelsea Cid, 10/25/2021 5:59 pm)      **CIS 2772 Security Operation Center syllabus 10-27-2021.docx** (uploaded by Sheila Seelau, 11/1/2021 10:27 pm)      **CIS 2772 Reviews - edits finalized 11-1-2021.docx** (uploaded by Sheila Seelau, 11/1/2021 10:28 pm)      **CIS 2772 Security Operation Center syllabus 11-11-21 for Fall 2022.docx** (uploaded by Sheila Seelau, 11/11/2021 11:14 am)

## Comments for CIS - 2772 - Security Operations Center

**Sheila Seelau**

11/11/2021 11:16 am

CIS 2772 Security Operations Center New Course proposal with prerequisite = CTS 1314 was accepted by unanimous vote of CC membership, 11/5/2021. This course will be added to the 2022-2023 catalog and may be offered beginning in Fall 2022.

Prerequisite has been changed from CTS 2120 to CTS 1314 on both proposal and syllabus by approval of Drs. Myers & Lyles.

Syllabus dated 11-11-21 and labeled "for Fall 2022" is finalized and ready to lock but should be held by the department chair or administrative assistant until the Document Manager files open for AY 2022-2023.

**Sheila Seelau**

11/11/2021 11:04 am [1 Reply](#)

During the 11/5/2021 Curriculum Committee meeting, it was determined that the prerequisite for this course should be CTS 2314 rather than CTS 2120 ("with a "C" or better" remains). This change has been made in the proposal and syllabus by the CC Chair on behalf of Drs. Myers and Lyles.

This prerequisite change will also affect course sequencing in the AS Cybersecurity degree program. Dr. Myers is revising AS documents accordingly.

**Sheila Seelau**

11/11/2021 11:05 am

**CORRECTION: CTS 1314 is the correct course number, not 2314.**

**Kelsea Cid**

10/25/2021 5:59 pm [1 Reply](#)

The Curriculum Committee has completed their pre-meeting review of this course. Please see the Word document added on 10/25/2021 to review and/or answer reviewer comments/edits.

**Sheila Seelau**

11/1/2021 10:29 pm

All review comments addressed on syllabus by Melinda Lyles 10/27/2021. Final formatting copied to proposal by SSeelau 11-1-2021.

Uploaded docs:  
Review - edits finalized 11-1-2021  
Syllabus 10-27-2021

Please refer to this syllabus for 11/5 meeting.

**Sheila Seelau**

10/14/2021 6:01 pm [1 Reply](#)

Per Mary Myers, syllabus and proposal updated 10/14/2021, and syllabus labeled 10-14-21 uploaded to Curriculog. Reviewers should use this version of the syllabus when making comparisons to proposal for Nov. 5 CC meeting.

**Sheila Seelau**

11/1/2021 10:30 pm

Syllabus updated on 10/27/2021 is final version

**Sheila Seelau**

10/10/2021 6:55 pm [2 Replies](#)

Curriculum Committee review comments file added 10-10-2021. Comments have been addressed by Originator on updated syllabus and copied to proposal by SSeelau.

Additional issues are under discussion with originator and department chair.

**Sheila Seelau**

10/10/2021 7:04 pm

"Additional issues are under discussion with originator and department chair."

Issues include:

\* Course prefix/number confusion (CNT 2401 vs. CIS 2772). Will need to fix SCNS Profile Description on proposal.

\* Course learning objectives (CLOs) redundant with Network Defense & Countermeasures course sequence CTS 1314 & CTS 2317. Originator/Department asked to review CLOs of these courses and possibly modify to show uniqueness of each course and progression of skills across sequenced courses.

**Sheila Seelau**

10/12/2021 2:11 pm

Discussed with Mary Myers via email:

Removed this paragraph from proposal field, SCNS Profile Description, as it is not relevant to CIS 2772:

**THIS COURSE WILL PROVIDE A FUNDAMENTAL UNDERSTANDING OF NETWORK SECURITY PRINCIPLES AND IMPLEMENTATION. THE STUDENT WILL LEARN THE TECHNOLOGIES USED AND THE PRINCIPLES INVOLVED IN CREATING A SECURE COMPUTER NETWORKING ENVIRONMENT. THE STUDENT WILL LEARN ABOUT THE AUTHENTICATION, THE TYPES OF ATTACKS AND MALICIOUS CODE THAT MAY BE USED AGAINST NETWORKS, THE THREATS AND COUNTERMEASURES FOR EMAIL, WEB APPLICATIONS, REMOTE ACCESS, AND FILE AND PRINT SERVICES. A VARIETY OF SECURITY TOPOLOGIES ARE DISCUSSED AS WELL AS TECHNOLOGIES AND CONCEPTS USED FOR PROVIDING SECURE COMMUNICATIONS CHANNELS, SECURE INTERNETWORKING DEVICES, AND NETWORK MEDIUM.**

**Sheila Seelau**

10/10/2021 6:40 pm

New Course proposal (NCP) form has an error in the State Information section. When "No" is chosen, the next question containing the drop-down list should not be required, or the drop-down list should contain an "N/A" option.

Due to this problem, "Communication" was chosen - but reviewers should ignore this field altogether, since the answer to the preceding question was "No."

JP will fix this drop-down question in the next iteration of the NCP.

**Jeffrey Peterman**

10/8/2021 1:24 pm

Force approval for proposal- as the original was inadvertently deleted. It will be moved to CC for review.

**Melinda Lyles**

10/8/2021 12:27 pm

This Proposal was resubmitted for Dr. Lyles due to accidental deletion. JP

## **Signatures for CIS - 2772 - Security Operations Center**

**There are no signatures required on this proposal.**



## **Crosslistings for CIS - 2772 - Security Operations Center**

**CIS - 2772 - Security Operations Center (parent proposal)**

**This proposal does not have any active crosslisted proposals.**

## Decision Summary for CIS - 2772 - Security Operations Center

Office of the registrar-Curriculum Coordinator

Status: *Working*

### Step Summary

This step requires 100% approval from all participants to move forward.

Participants

Totals

Users Approved: *0*

Users Rejected: *0*

