Curriculum Committee

FLORIDA SOUTHWESTERN STATE COLLEGE

New Course Proposal

School or Division	School of Business and Technology
Program or Certificate	Information Systems Technology
Proposed by (faculty only)	Melinda Lyles & Mary Myers
Presenter (faculty only)	Melinda Lyles
Note that the presenter (faculty) listed above must be present at the Curriculum Committee meeting or the proposal will be returned to the School or Division and must be submitted for a later date.	
Submission date	3/6/2020
Course prefix, number, and title	CIS 3360 Principles of Security

All Curriculum proposals require approval of the Curriculum Committee and the Provost. Final approval or denial of a proposal is reflected on the completed and signed proposal.

☒ Approve ☐ Do Not Approve

Mary R. Myers 4/8/2020

Curriculum Committee Chair Signature *Date*

☑ Approve ☐ Do Not Approve

5-21-2020

Provost Signature *Date*

All Curriculum proposals require review by the Office of Accountability & Effectiveness.

☑ Reviewed

5/21/2020

Office of Accountability & Effectiveness Signature *Date*

Section I, Important Dates and Endorsements Required

NOTE: Course and Program changes must be submitted by the dates listed on the published Curriculum Committee Calendar. Exceptions to the published submission deadlines must receive prior approval from the Provost' Office.

Term in which approved action will take place	Fall 2021
Provide an explanation below for the requested exception to the effective **date.**	
Type in the explanation for exception.	

Any exceptions to the term start date requires the signatures of the Academic Dean and Provost prior to submission to the Dropbox.		
Dean	**Signature**	**Date**
Dr. Debbie Psihountas		
Provost	**Signature**	**Date**
Dr. Eileen DeLuca		

Required Endorsements	Type in Name	Select Date
Department Chair or Program Coordinator/Director	Dr. Mary Myers	3/18/2020
Academic Dean or Provost	Dr. Debbie Psihountas	3/18/2020

List all faculty endorsements below. (Note that proposals will be returned to the School or Division if faculty endorsements are not provided).
Prof Melinda Lyles, Dr. Mary Myers, Dr. George Kodsey, Dr. Roger Webster

Has the Libraries' Collection Manager been contacted about the new course and discussed potential impacts to the libraries' collections?
No Impact.

Section II, New Course Information (must complete all items)

List course prerequisite(s) and minimum grade(s) (must include minimum grade if higher than a "D").	CTS2120 with a grade of C" or better.
Provide justification for the proposed prerequisite(s).	Students need a fundamental understanding of network security before taking this course.
Will students be taking any of the prerequisites listed for this course in different parts of the same term (ex. Term A and Term B)?	No
List course co-requisites.	List course co-requisites
Provide justification for the proposed co-requisite(s).	
Is any co-requisite for this course listed as a co-requisite on its paired course? (Ex. CHM 2032 is a co-requisite for CHM 2032L, and CHM 2032L is a co-requisite for CHM 2032)	Choose an item. List the co-requisite
Course credits or clock hours	3 course credits Must pass with a "C" or better.
Contact hours (faculty load)	3
Are the Contact hours different from the credit/lecture/lab hours?	No
Select grade mode	Standard Grading (A, B, C, D, F)
Credit type	College Credit
Possible Delivery Types (Online, Blended, On Campus)	Online, Blended, On Campus

Course description (provide below)
This course provides an overview of information systems security principles, practices, methods, and tools for organizational and institutional computing. Students will explore the relationship between policy and security, the mechanisms used to implement countermeasures to align and apply to policies, methodologies and technologies necessary for information assurance, cybersecurity threat analysis, and intrusion detection.

General topic outline (type in outline below)
Part I: GATHERING – Threat Management: What technology are we currently using? 1. Applying Environmental Reconnaissance.

2. Analyzing Network Reconnaissance.
3. Strengthening the Network.
4. Securing a Corporate Environment.

Part II: UNCOVERING – Vulnerability Management: What are our weaknesses?

1. Scanning for Vulnerabilities.
2. Analyzing Vulnerability Scans.
3. Contrasting Scans with Commonly Known Vulnerabilities.

Part III: RESPONDING: Incident Response: How do we react in an attack?

1. Determining the Impact of An Attack.
2. Using Forensics Tools.
3. Communicating During the Incident.
4. Deciding on a Course of Action.
5. Gathering Lessons Learned.

Part IV: IMPROVING: Architecture & Tool Sets: How do we make our security better?

1. Using Structures for Security.
2. Using Data for Remediation of Identity and Access Management.
3. Using Security Architecture for Controls.
4. Using Software Development Life Cycle for Applications.

Revised: 11/11, 6/12, 6/13, 7/14, 8/15, 8/16, 8/17, 5/18, 6/18;10/18;7/19

Learning Outcomes: For information purposes only.

IV. Course Competencies, Learning Outcomes and Objectives

A. General Education Competencies and Course Outcomes

1. Integral *General Education Competency or competencies*:

General Education Competency: **Think**

Course Outcomes or Objectives Supporting the General Education Competency Selected:
RESPONDING: Incident Response: How do we react in an attack?

- Analyze and apply tools and techniques to apply appropriate countermeasures to manage various threats
- Perform scans using tools and analyzing outputs using techniques to control, resolve, and report on vulnerability management
- Distinguish behavior and data threats to determining the course of action to report or responds to cyber incidence
- Apply best practice during Software Development Life Cycle (SDLC)
- Identify security issues within identity and access management.
- Explain various frameworks, policies, security controls, and procedures within a security Architecture to include tool and technologies.

2. Supplemental *General Education Competency or competencies*:

General Education Competency: **Research**

Course Outcomes or Objectives Supporting the General Education Competency Selected:
Vulnerability Management: What are our weaknesses ?

B. In accordance with Florida Statute 1007.25 concerning the state's general education core course requirements, this course meets the general education competencies for ....
Part B would only be included in the course outlines of those courses are included in the FSW Catalog as a General Education Core Course. If this is not a core course, then outline letter C would become B.

C. Other Course Objectives/Standards

Copy and Paste the SCNS Course Profile Description below (http://scns.fldoe.org/scns/public/pb_index.jsp).

COMPUTER SECURITY THREATS AND ATTACKS, COVERT CHANNELS, TRUSTED OPERATING SYSTEMS, ACCESS CONTROL, ENTITY AUTHENTICATION, SECURITY POLICIES, MODELS OF SECURITY, DATABASE SECURITY AND BRIEF INTRODUCTIONS TO NETWORK SECURITY AND LEGAL AND ETHICAL ASPECTS OF SECURITY.

Revised: 11/11, 6/12, 6/13, 7/14, 8/15, 8/16, 8/17, 5/18, 6/18;10/18;7/19

ICS code for this course	ADVANCED AND PROFESSIONAL - 1.16.07 - COMPUTER & INFO SCIENCE
Institutional Reporting Code	11607 COMPUTER AND INFOR SCIENCE
Degree Attributes	BAS - BAS COURSE
Degree Attributes (if needed)	Choose an item.
Degree Attributes (if needed)	Choose an item.
Degree Attributes (if needed)	Choose an item.
Should any major restriction(s) be listed on this course? If so, select "yes" and list the appropriate major restriction code(s) or select "no".	BAS - IST
Is the course an "International or Diversity Focus" course?	No, not International or Diversity Focus
Is the course a General Education course?	No
Is the course a Writing Intensive course?	No
If Replacing a course, combining a Lecture/Lab or splitting a C course – Is there a course equivalency?	
Is the course repeatable*? (A repeatable course may be taken more than one time for additional credits. For example, MUT 2641, a 3 credit hour course can be repeated 1 time and a student can earn a maximum of 6 credits). *Not the same as Multiple Attempts or Grade Forgiveness	No
Do you expect to offer this course three times or less (experimental)?	No

Impact of Course Proposal	
Will this new course proposal impact other courses, programs, departments, or budgets?	Choose an item.
If the answer to the question above is "yes", list the impact on other courses, programs, or budgets?	List impacts here
Have you discussed this proposal with anyone (from other departments, programs, or institutions) regarding the impact? Were any agreements made? Provide detail information below.	

Revised: 11/11, 6/12, 6/13, 7/14, 8/15, 8/16, 8/17, 5/18, 6/18;10/18;7/19

Section III, Justification for proposal

Provide justification (below) for this proposed curriculum action.
This course is being proposed as an update to the curriculum in the BAS- Information Technology Systems degree. Principles of Security is a foundational course in the Networking Track.