### INSTRUCTION COUNCIL

### **MINUTES**

# Thursday, May 16, 2024 126 ITLE or Zoom

https://okstate-edu.zoom.us/i/96284911705?pwd=bklTQk5Kc08ydC9GVXJnU2FLaTq0Zz09

PASSCODE: 596082 9:00 a.m. – 10:30 a.m.

In attendance: Shannon Baker, Laurie Beets, Larry Burns, Kyndal Campbell, Aaron Christensen, Cynda Clary, Andrew Doust, Craig Freeman, Richard Frohock, Jami Fullerton, Jeff Hartman, Sarah Johnson, Diane Jones, Janes Knecht, Rita Peaster, Jerry Ritchey, Adrienne Sanogo, Candace Thrasher, Jean Van Delinder, John Veenstra and Chris Francisco, Chair.

#### 1. General Education Discussion - Chris Francisco

Trails:

All Instruction Council (IC) members were sent eight (8) General Education (GenEd) trails to review and provide feedback, with our faculty's top five (5) included. This process will be repeated again in August. In the next call, C. Francisco would like a list of sample courses to get a better idea of what IC members think of the intro courses, along with the capstone courses. He will be meeting with Tammy Mix, Chair of the General Education Working Group, to discuss details regarding the trails focused on the strategic priority areas. Our goal is to offer three pilot trails in the Fall 2024 semester.

As students begin enrollment for Fall 2024 semester, they will learn about the GenEd Trails in their UNIV course. We have identified the two pilot populations that will be introduced to the concept of Trails in their section of UNIV. Those students will have a follow up conversation at their enrollment meeting with their academic advisor.

C. Francisco specified he would like to have 20 to 25 trails finished by the middle of Fall 2024 so they are fully ready for implementation and enrollment Fall 2025. A request will be made to the Oklahoma State Regents for Higer Education (OSRHE) for each trail to lead to a formal certificate. The current OSRHE vice chancellor has been very supportive of these trails, however there is a transition occurring with the Vice Chancellor's resignation, and with any transition could come change.

Currently we have four (4) strategic priority area trails in preparation, with plans for five (5) trails ready by August, 2024, and 10-15 trails ready by October/November, 2024. R. Peaster and T. Mix will discuss the details of tracking these trails. As we talk about improving trails, we are open to various structures for change. We will need to develop a structure for proposing new trails, as other trails may fall off. Documents will be needed that detail these processes. Possibly General Education Advisory Council could monitor the courses to make sure they are fulfilling the learning outcomes and competencies expected. We need a critical mass of enrollment in the trails to ensure they can run efficiently.

#### Written/Oral/Visual Competencies:

The GenEd working group introduced changes to the requirements for the designations that are not the STEM designations. The main idea was to expand beyond the existing writing requirements to allow for oral or visual communication, along with written. GenEd working group felt that the minimum competencies they outlined are truly the minimum a student would need in order to verify those students are expressing themselves appropriately through that means of communication. They did not want to see mixing and matching of the different types of communication to make up the 20%. Possibly each GenEd course could carry a separate attribute so that it would be more visible to students which communication competencies that course carries. If the course specifies visual competencies, it should meet the minimum competency requirement. IC members discussed the importance of offering multiple ways of assessment. R. Peaster stated the latest draft of this proposed change indicates that courses with multiple competencies must meet the minimum for each competency. With the new way of looking at general education we are attempting to focus on how our students meet these outcomes, what are the learning outcomes of this course, what should students be taking away from this course. General education is meant to be a breadth requirement, what a broadly educated student gets out of college. We want our students to be able to write, speak, make presentations and illustrate ideas visually. The written component has a minimum quantity but the other two, visual and oral, do not. Discussion

was held by IC members regarding how to quantify the minimum requirement for visual and oral assessment. As weight of grade from presentation is the only quantity at this point, additional feedback will need to be incorporated into this next assignment. We are looking to provide more flexibility for faculty as possible in these new communication competencies.

C. Francisco will take this feedback to the GenEd working group for further discussion. If there is additional feedback from department heads, IC members were encouraged to communicate that information to C. Francisco.

#### 2. Curriculum

**Information Items Only:** 

N/A

**Course Action Summaries:** 

# OKLAHOMA STATE UNIVERSITY CURRICULAR REQUESTS FROM THE COLLEGE OF ARTS & SCIENCES

Date: SPRING 2024 Pt2

PRESENT	PROPOSED	PRESENT	PROPOSED	PRESENT	PROPOSED	ACTION SUMMAR
PREFIX/NUMB		TITLE		ACTION		
New Course					New Course Descriptions:	
	CS 4383		Network Security and Defense		Network Security and Defense exposes students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using appropriate tools in	New Course  Mutually Exclusive: CS 5583

Recurity    Security   Recursion   Recursi	CC 1102	T	Motural Attack	I	This source will	Now Course
knowledge of cyber attacks and their defense technologies as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit with CS 5483.  Total Crodit Hours: 3 LECTH Total Contact Hours: 3 LECTH Total Contact Hours: 3 LECTH Prequisite(s): CS 3443, cs 34243, and CS 4283  CS 5483  Network Attack Security  Network Security  This course will expand the practical knowledge of cyber attacks and their defense technologies as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit  Network Security and Defense exposes students to intrusion detection, network auditing, (forensic) elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit  Network Security and Defense exposes students to intrusion detection, network auditing, (forensic) elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and incidence response. Students exposes the feather of the viewpoint of both the attacker and the defender (network administratory) using	CS 4483		Network Attack		This course will	New Course
Exclusive:  defense technologies as applied to an industrial setting. The ocurse covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from oyber threats and attacks. May not to be used for degree redit with CS \$433.  Total Credit Hours: 3 LECTH Total Contact Hours: 3 LECTH Perequisite(s): CS 3443, CS 4243, and CS 4243.  CS 5483  Network Attack Security  Network Attack Security  Network and their defense technologies as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from oyber threats and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from oyber threats and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from oyber threats and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from oyber threats and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from oyber threats and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from oyber threats and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from oyber threats and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from oyber threats and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from oyber threats and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from oyber threats and purposes of the key elements used to analyze, create, secure, and protect an industrial secure of contact the contact the contact the contact the contac			Security			Mutually
defense technologies as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, creatle, secure, and protect an industrial cyber intrastructure from cyber threats and attacks. May not be used for degree credit with CS 5433.  Total Credit Hours: 3, 1EC/TH Prerequisite(s): CS 344, CS 2425, and CS 4283  CS 5483  Network Attack Security  Network Attack Security  Requirements used to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, creatle, secure, and purposes of the key elements used to analyze, creatle, secure, and purposes of the key elements used to analyze, creatle, secure, and purposes of the key elements used to analyze, creatle, secure, and purposes of the key elements used to analyze, creatle, secure, and purposes of the key elements used to analyze, creatle, secure, and purposes of the key elements used to analyze, creatle, secure, and protect an industrial cyber intrastructure from cyber threats and attacks. May not be used for degree credit intrastructure from cyber threats and attacks. May not be used for degree credit intrastructure from cyber threats and incidence response. Students explore the veryonit of both the attacker and the defender (network administratory) using						
as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit with CS 5483.  Total Credit Hours: 3.LEC/TH Total Contact Hours: 3.LEC/TH Total Contact Hours: 3.LEC/TH Total Contact Hours: 3.LEC/TH Prerequisite(s): CS 4443, cs 4243, and CS 4283  This course will expand the practical knowledge of cyber attacks and their deflense technologies as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit with Cyber infrastructure from cyber threats and attacks. May not be used for degree credit with Cyber infrastructure from cyber threats and attacks. May not be used for degree credit with Cyber infrastructure from cyber threats and attacks. May not be used for degree credit cyber infrastructure from cyber threats and attacks. May not be used for degree credit cyber infrastructure from cyber threats and attacks. May not be used for degree credit cyber infrastructure from cyber threats and attacks. May not be used for degree credit cyber infrastructure from cyber threats and attacks. May not be used for degree credit cyber infrastructure from cyber threats and attacks. May not be used for degree credit with Cyber infrastructure from cyber threats and attacks. May not be used for degree credit with Cyber infrastructure from cyber threats and attacks. May not be used for degree credit with Cyber infrastructure from cyber threats and attacks. May not be used for degree credit with Cyber infrastructure from cyber threats and attacks. May not be used for degree credit with Cyber infrastructure from cyber threats and the defender (network and incidence response. Students to general cyber and cyber a						
industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit with CS 5483.  Total Contact Hours: 3.LECTH Total Contact Hours: 3.LECTH Perequisite(s): CS 3443, CS 4243, and CS 4283  CS 5483  Network Attack Security  New Course will expand the practical knowledge of cyber attacks and their defense technologies as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit will be used for						US 3403
course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit with CS 5493.  Total Credit Hours: 3 LEC/TH Total Contact Hours: 3 LEC/TH Prerequisite(s): CS 3443, CS 4243, and CS 4238  CS 5483  Network Attack Security  Network Attack Security  This course will expand the practical knowledge of cyber attacks and their defense technologies as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit very elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit very elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit very elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit very elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit very elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks may not be used for degree credit very elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit very elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and the defense exposes. Subdents explore the very elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and the defense exposes students to intrusion the protect and the defense exposes.						
functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit with CS 5483.  CS 5483  CS 5483  Network Attack Security  Network Attack Security  Total Contact Hours: 3 LECTH CS 5483  Network Attack Security  This course will expand the practical knowledge of cyber attacks and their defense technologies as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit Security and Defense exposes students to intrusion detection, network auditing, (retorsic) evidence collection, security policy design/implementation for networks, and incidence response. Students expiore the viewpoint of both the attacker and the defender (network administrator) using						
purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit with CS 5483.  Total Credit Hours: 3. I.EC/TH Total Contact Hours: 3. I.EC/TH Prerequisite(s): CS 3443, CS 4243, and CS 4283  CS 4283  Network Attack Security  New Course will expand the practical knowledge of cyber attacks and their defense technologies as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit  CS 5583  Network Security and Defense exposes students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit with CS 5483.  Total Credit Hours: 3 LECTH Total Contact Hours: 3 LECTH Prerequisite(s): CS 3443, CS 4243, and CS 4283  Network Attack Security  Network Attack Security  This course will expand the practical knowledge of cyber attacks and their defense technologies as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit  CS 5583  Network  Network Security and Defense exposes students to intrusion detection, network auditing, derivative policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit with CS 5483.  Total Credit Hours: 3 LEC/TH Total Contact Hours: 3 LEC/TH Prerequisire(s): CS 3443, CS 4243, and CS 4283  CS 4283  Network Attack Security  Network attack Security  Network attack Security  This course will expand the practical knowledge of cyber attacks and their defense technologies as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit  CS 5583  Network Security and Defense exposes students to intrusion detection, network auditing, (forerisc) evidence collection, security policy design/implementation for networks, and indidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
Secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit with to S 5483.  Total Credit Hours: 3 LEC/TH Total Contact Hours: 3 LEC/TH Prerequisite(s): CS 3443, CS 4243, and CS 4283  Network Attack Security  This course will expand the practical knowledge of cyber attacks and their defense technologies as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit Network Security and Defense exposes students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit with CS 5483.  Total Credit Hours: 3 LEC/TH Trotal Contact Hours: 3 LEC/TH Prerequisite(s): CS 3443, CS 4243, and CS 4283.  This course will expand the practical knowledge of cyber attacks and their defense technologies as applied to an industrial setting. The course overest the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit with the functions and purpose of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit with the function of the cyber defense exposes students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
infrastructure from cyber threats and attacks. May not be used for degree credit with CS 5483.  Total Credit Hours: 3 LEC/TH Total Contact Hours: 3 LEC/TH Prerequisite(s): CS 3443, CS 4243, and CS 4283  CS 5483  Network Attack Security  Network Attack Security  Network Attack Security  This course will expand the practical knowledge of cyber attacks and their defense technologies as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit  CS 5583  Network Security and Defense exposes students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
cyber threats and attacks. May not be used for degree credit with CS 5483.  Total Credit Hours: 3 LEC/TH Total Contact Hours: 3 LEC/TH Prerequisite(s): CS 3443, CS 4243, and CS 4283  CS 5483  Network Attack Security  This course will expand the practical knowledge of cyber attacks and their defense technologies as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, an analyze, create, an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit view of defense exposes students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administration using limitation and the defender (network administration using limitation using limitation and the defender (network administration using limitation using limitation and the defender (network administration using limitation using limitation and the defender (network administration using limitation using limitation and the defender (network administration using limitation using limitation and limitation using limitation limitation using limitation limita						
atlacks. May not be used for degree credit with CS 5483.  Total Credit Hours: 3 LEC/TH Total Contact Hours: 3 LEC/TH Prerequisite(s): CS 3443, CS 4243, and CS 4283  Network Atlack Security  New Course expand the practical knowledge of cyber attacks and their defense technologies as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit view of the cyber threats and attacks. May not be used for degree credit view of the cyber threats and befanse exposes students to intrusion detection, network audifing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
used for degree credit with CS 5483  Total Credit Hours: 3 LEC/TH Total Contact Hours: 3 LEC/TH Prerequisite(s): CS 3443, CS 4243, and CS 4283  This course will expand the practical knowledge of cyber attacks and their defense technologies as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit view of degree cre						
with CS 5483. Total Credit Hours: 3 LEC/TH Total Contact Hours: 3 LEC/TH Prerequisite(s): CS 3443, CS 4243, and CS 4283  CS 5483  Network Attack Security  Network Attack Security  This course will expand the practical knowledge of cyber attacks and their defense technologies as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit.  Network Security and Defense exposes students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using					attacks. May not be	
Total Credit Hours: 3 LEC/TH Total Contact Hours: 3 LEC/TH Prerequisite(s): CS 3443, CS 4243, and CS 4283  Network Attack Security  Network expand the practical knowledge of cyber attacks and their defense technologies as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit  CS 5583  Network Security and Defense exposes students to intrusion detection, network auditing, forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
CS 5483  Network Attack Security  Network Security  New Course will expand the practical knowledge of cyber attacks and their defense technologies as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber firreats and attacks. May not be used for degree credit Security and Defense exposes students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
Total Contact Hours: 3 LEC/TH Prerequisite(s): CS 3443, CS 4243, and CS 4283  Network Attack Security  New Course will expand the practical knowledge of cyber attacks and their defense technologies as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit  CS 5583  Network Security and Defense  New Course Mutually Exclusive: CS 4483  New Course be used for degree credit Network Security and Defense students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
CS 5483  Network Attack Security  Network Attack Security  This course will expand the practical knowledge of cyber attacks and their defense technologies as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit  CS 5583  Network Security and Defense exposes students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
CS 5483  Network Attack Security  Network Attack Security  This course will expand the practical knowledge of cyber attacks and their defense technologies as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit  CS 5583  Network Security and Defense exposes students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
CS 5483  Network Attack Security  Network Attack Security  Network Attack Security  This course will expand the practical knowledge of cyber attacks and their defense technologies as applied to an industrial esting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit Network Security and Defense exposes students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
CS 5483  Network Attack Security  Network Attack Security  Network Attack Security  This course will expand the practical knowledge of cyber attacks and their defense technologies as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an infastracture from cyber threats and attacks. May not be used for degree credit  CS 5583  Network Security and Defense Students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
CS 5483  Network Attack Security  Network Attack Security  This course will expand the practical knowledge of cyber attacks and their defense technologies as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit  CS 5583  Network Security and Defense exposes students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
Security  expand the practical knowledge of cyber attacks and their defense technologies as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit  CS 5583  Network Security and Defense exposes Defense  Network Security and Defense exposes students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using					CS 4283	
Security  expand the practical knowledge of cyber attacks and their defense technologies as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit  CS 5583  Network Security and Defense exposes Defense  Network Security and Defense exposes students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using	CS 5483		Network Attack		This course will	New Course
knowledge of cyber attacks and their defense technologies as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit values for federace collection, security and Defense exposes students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using	00 0 100					11011 000100
attacks and their defense technologies as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit  CS 5583  Network Security and Defense exposes students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using			Cooding			Mutually
defense technologies as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit  CS 5583  Network Security and Defense  Network Security and Defense exposes students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
as applied to an industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit  CS 5583  Network Security and Defense exposes students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
industrial setting. The course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit  Network Security and Defense exposes students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						00 4400
course covers the functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit  CS 5583  Network Security and Defense Poses Students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
functions and purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit  CS 5583  Network Security and Defense  Network Security and Defense exposes students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
purposes of the key elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit  CS 5583  Network Security and Defense exposes students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
elements used to analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit  CS 5583  Network Security and Defense  Network Security and Defense exposes students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
analyze, create, secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit  CS 5583  Network Security and Defense exposes students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
secure, and protect an industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit  CS 5583  Network Security and Defense exposes students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
industrial cyber infrastructure from cyber threats and attacks. May not be used for degree credit  CS 5583  Network Security and Defense exposes students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
infrastructure from cyber threats and attacks. May not be used for degree credit  CS 5583  Network Security and Defense Defense Defense Defense  Network Security and Defense exposes students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
CS 5583  Network Security and Defense Defense  Network Security and Defense Students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
CS 5583  Network Security and Defense Defense  New Course New Cour						
CS 5583  Network Security and Defense exposes students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
CS 5583  Network Security and Defense exposes students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
Security and Defense exposes students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using	00.5500		Materials		_	NO-
Defense  students to intrusion detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using	CS 5583					New Course
detection, network auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using					Detense exposes	Moderall
auditing, (forensic) evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using			Detense			
evidence collection, security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
security policy design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						CS 4383
design/implementation for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
for networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
networks, and incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
incidence response. Students explore the viewpoint of both the attacker and the defender (network administrator) using						
Students explore the viewpoint of both the attacker and the defender (network administrator) using						
viewpoint of both the attacker and the defender (network administrator) using						
attacker and the defender (network administrator) using						
defender (network administrator) using						
administrator) using						
appropriate tools in						
					appropriate tools in	
laboratory exercises.						

### **Program Modifications:**

## College of Education and Human Sciences

K-12 STEM Educator, GCRT (266)

Course requirement change

- Remove SMED 5323 as a required course
- Add 3 hours of guided electives
- Reason for requested action: To create flexibility for students and address course scheduling issues.
- Total credit hours will not change

Motion was made by A. Doust and seconded by J. Van Delinder to accept the above-mentioned College of Education and Human Sciences K-12 STEM Educator Graduate Certificate program modifications, and Instruction Council members approved.

# College of Engineering, Architecture and Technology

Civil Engineering, PHD (049)

Course requirement change

- Clarifying that students with a Bachelor's degree must complete 72 credit hours
- Reason for requested action: To update requirements to clarify that students complete 72 hours beyond a Bachelor's degree
- Total credit hours will increase from 60 to 72 hours for students with a bachelor's degree

Motion was made by A. Doust and seconded by A. Sanogo to accept the above-mentioned College of Engineering, Architecture and Technology, Civil Engineering PHD program modifications, and Instruction Council members approved.

## Spears School of Business

Accounting: Corporate Finance, MS (002)

Degree requirement change

- Remove the GMAT requirement
- Reason for requested action: To allow a more holistic admissions process.

Course requirement change

- Remove ACCT 5103
- Change ACCT 5994 to ACCT 5980
- Increase guided electives from 3 to 6 credit hours
- Reason for requested action: To provide students with additional flexibility
- Total credit hours will not change

Motion was made by J. Fullerton and seconded by A. Sanogo to accept the above-mentioned Spears School of Business, Accounting program modifications, and Instruction Council members approved.

### **Center for Health Sciences**

Forensic Psychology, GCRT (282)

Degree requirement change

- Remove requirement for three letters of recommendation
- Reason for requested action: To streamline the application process, especially for students adding the certificate as a secondary matriculation.

Course requirement change

- Remove FRNS 5613
- Add 3 hours of guided electives
- Reason for requested action: To create flexibility for students
- Total credit hours will not change

Motion was made by A. Sanogo and seconded by A. Doust to accept the above-mentioned Center for Health Sciences, Forensic Psychology program modifications, and Instruction Council members approved.

### 3. Other

- Explanation of corequisite section of Math 1493 math for general public the Math Department would like to add a corequisite offering of MATH 1493, proposing a five-day format with an ALEKS prerequisite of 15. Math affects so many people on campus, and every time we had a request like this, IC was required to review for approval. The request would then move forward for further approval. Jeanette Mendez, the vice provost at the time, changed protocol to be less restrictive with no need to be approved by IC. However, with Mathematics being C. Francisco's home department, he wanted to approach IC with complete transparency:
  - Proposal will add a section of Math 1493 with a corequisite format that meets 5 days per week. ALEKS cut off would be 15 for this course.
    - McGraw Hill's recommendation for ALEKS score for college algebra is 46. OSU set at 40 with the corequisite course set at 30 (intermediate algebra).
    - McGraw Hill's recommendation for ALEKS score for lower level developmental math course is 15-20. OSU set corequisite course Math 1483 at 25. MATH 1493 does not require even the facility with algebra at MATH 1483, and so Math has set the ALEKS score at 15 (below the threshold for any sort of developmental math course that McGraw Hill sets, so this should encompass the vast majority of our students and allow them to be able to get into a college level math class).
    - This does not mean this course will assist the student with their degree plan, especially if they are a STEM student, but it is something that will get them in a college level math course.
  - o IC members acknowledged their endorsement of MATH 1493 corequisite section.
  - C. Francisco thanked all those who attended commencement, with special thanks to R. Peaster and the Registrar's Office for their work during the undergraduate ceremonies remarkable undertaking.
  - C. Francisco commended all colleges and departments for submitted grades all grades, with the exception of 15, were submitted.
  - Next year there will be additional department head workshops and training focused on the use of eprints and cowboy data roundup.
  - C. Francisco will be submitting reminders about grade submission for Niblack Research Scholars and similar programs classified under Academic Affairs. For other announcements, associate deans will need to assist.
  - Faculty Council requests:
    - i. FC presented several recommendations regarding Academic Standards Policy (ASP) committee and committee membership. Currently, the policies say that there should be a representative from ASP on Late Drop, Reprieve, and Grade Appeals. FC would like to remove the restriction regarding a representative from the ASP committee and allow anyone from Faculty Council to serve as representative on the abovementioned academic committees.
    - ii. Representation from Faculty Council's ASP committee on General Education Advisory Council Faculty Council to decide.
    - iii. Representation from Faculty Council's ASP committee on Instruction Council (nonvoting seat) IC members agreed.

Meeting was adjourned at 9:58am

Minutes were recorded by K. Campbell