CCRI CURRICULUM REVIEW COMMITTEE MEETING
February 3, 2023 9:00-11:00 AM
Knight Campus, Board Room 4090

AGENDA

1. CALL TO ORDER

2. ROLL CALL

3. APPROVAL OF MINUTES

4. NON-ACTION/ANNOUNCEMENTS

5. ACTION/VOTING ITEMS

NON-ACTION/ANNOUNCEMENTS

COMMITTEE ANNOUNCEMENTS:

1. Rescheduling of March 17, 2023 Curriculum Review Committee Meeting
2. Rescheduling of April 21, 2023 Curriculum Review Committee Meeting

DEPARTMENT ANNOUNCEMENTS:

The Business & Professional Studies Department is announcing the closing of the following program:

1. Travel, Tourism and Hospitality Certificate

The Computer Studies & Information Processing Department is announcing the closing of the following programs:

1. Computer Programming Certificate
2. General Information Processing A.S. Degree
3. General Information Processing Certificate

The Physics & Engineering Department is announcing the suspension of the following program:

1. Engineering, Chem-Biology A.S. in Engineering

ACTION/VOTING ITEMS

New Course Proposal: Ethical Hacking
COMI 2038, 3 credits
Originator: Kevin Crawford

RATIONALE:
Ethical Hacking detects vulnerabilities in applications and network infrastructure that a hacker can exploit and cause a breach. The rise in security vulnerabilities has increased the need for certified ethical hackers to assist in the securing of data and systems against illicit cyber attacks. Our CAE certification is aligned to the NIST categories of Operate & Maintain and Protect & Defend. The addition of the ethical hacking course strengthens our CAE alignment to the Protect & Defend category and provides our students with the opportunity to develop skills in a high-demand area of cybersecurity. The course aligns with E-C Council's Certified Ethical Hacker (CEH) certification which is highly desirable.

CATALOG DESCRIPTION:
This course is an introduction to hacking tools, techniques, and incident handling. Topics of instruction include: the evolution of hacking and penetration testing; the basics of cryptology for information security; footprinting; vulnerability scanning and exploit; wireless, web, and database attacks; malware and system exploit; traffic analysis; incident response; and defensive technologies and controls. In this course, the students will learn how to discover vulnerabilities, how to attack and defend systems, how to respond to attacks, and how to identify and design controls to prevent future attacks. This course prepares students to pass the EC-Council Certified Ethical Hacker certification exam.

Revised Course Proposal**: Defending External Threats Using the Cyber Range**
CYBR 1100, 3 credits
Originator: Kevin Crawford

RATIONALE:
To fix hours only.

CATALOG DESCRIPTION:
This course focuses on techniques, considered preventative in nature, which are used to manage and protect networking devices from external attacks. This course utilizes hands-on virtual labs which allow students to examine sophisticated devices such as Adaptive Security Appliance (ASA) firewalls and to explore how these devices may be used to control access to resources. We will also explore methods to test, audit, and analyze the outcomes of a cyber-attack.

Revised Course Proposal**: Defending Internal Threats Using the Cyber Range**
CYBR 1200, 3 credits
Originator: Kevin Crawford

RATIONALE:
To fix hours only.

CATALOG DESCRIPTION:
This course focuses on techniques, considered preventative in nature, which are used to manage and protect networking devices from internal attacks. This course utilizes hands-on virtual labs which allow students to examine sophisticated devices such as Adaptive Security Appliance (ASA) firewalls and to explore how these devices may be used to control access to resources. We will also explore methods to test, audit, and analyze the outcomes of a cyber-attack.

Revised Program Proposal**: Cloud Computing**
CCNT, 65 credits
Originator: Kevin Crawford

RATIONALE:
To fix a course that is no longer valid.

CATALOG DESCRIPTION:
Cloud computing allows users to access and implement business and technology tools over the internet. Users can access that information at any time or from anywhere. Cloud services run over a vast variety of networks, and services can range from different types of hardware or software architecture. Students will learn how to

create networks, work with a variety of computers, and create cloud services that are scalable. Students also learn how to secure cloud networks and systems.

Revised Program Proposal: Computer Studies and Information Processing, Networking Technology, Network Hardware Emphasis
CNTH, 60-62 credits
Originator: Kevin Crawford

RATIONALE:
Remove an option as course is no longer going to be offered.

CATALOG DESCRIPTION:
Networks continue to expand in all aspects of our personal activities in business, manufacturing, education, and health care. This program provides balanced coverage of technology fundamentals, emphasis on this concentration prepares students for careers in modern office environments, focused on both client/server technologies and networking technology. Importance is placed on operating principles of programming, hardware, software, networking models, network operating systems, internetworking components, and industry standards along with hands-on laboratory activities for developing practical problem-solving skills. Students develop the ability to design, configure, secure, and troubleshoot basic local area networks (LANs) and internetworks using servers, routers, and switches. Integrated into the program are courses that prepare students to sit for both the server and networking certifications. Depending on the path taken, students can choose between networking or programming emphasis.

Revised Program Proposal: Cyber Defense Certificate
CYBC, 22 credits
Originator: Kevin Crawford

RATIONALE:
Due to the results of the five-year CAE Program Re-Designation Review we needed to make changes based on new Knowledge Units (KU's) that provide the basis of the Cybersecurity Degree. The Cyber Defense Certificate is based upon the Cyber Defense Path which certifies that we meet the required KU's for CAE certification. The changes in our KU alignment caused a change in our Cyber Defense Path which necessitates the change to the Cyber Defense Certificate. Simply, COMP-1200 is out and is being replaced by COMI-1800. It doesn't change the degree, both courses are still there.

CATALOG DESCRIPTION:
The Cyber Defense program is part of the Cybersecurity degree designed to provide students with a strong foundation in the principles and methods of cybersecurity, as well as the fundamental knowledge and tools for applying security measures across a variety of network architectures and settings. This certificate program will provide the educational background and hands-on training necessary to prepare students in the cybersecurity defense sector. The curriculum meets the National Security Agency (NSA) and Centers of Academic Excellence (CAE) core foundational content and standards.

Revised Program Proposal: Cybersecurity A.S. Degree
CYBR, 61 credits
Originator: Kevin Crawford

RATIONALE:
Ethical Hacking detects vulnerabilities in applications and network infrastructure that a hacker can exploit and cause a breach. The rise in security vulnerabilities has increased the need for certified ethical hackers to assist in

the securing of data and systems against illicit cyber attacks. Our CAE certification is aligned to the NIST categories of Operate & Maintain and Protect & Defend. The addition of the ethical hacking course strengthens our CAE alignment to the Protect & Defend category and provides our students with the opportunity to develop skills in a high-demand area of cybersecurity. The course aligns to E-C Council's Certified Ethical Hacker (CEH) certification which is highly desirable.

CATALOG DESCRIPTION:
The Cybersecurity program is designed to provide students with a strong foundation in the principles and methods of cybersecurity, as well as the fundamental knowledge and tools for applying security measures across a variety of network architectures and settings. In addition to serving as a strong foundation for pursuing a bachelor's degree in cybersecurity, this associate degree program will provide the educational background and hands-on training necessary to prepare students for entry into the cybersecurity sector. The curriculum includes a combination of general education, computer science, and network technology courses to provide students with the knowledge, skills, and training necessary for a successful transition into a career in security, and to meet National Security Agency (NSA) and Centers of Academic Excellence (CAE) core foundational content and standards.