RE: New Cybersecurity Programs (AAS C255) (CER C255) (STC C255) and Supporting Courses

Effective spring 2021, the Department of Computer Information Systems Technology has been approved to offer the following Cybersecurity programs:

Associate in Applied Science in Cybersecurity (AAS C255)

General Courses **(24 hours)**

Course	*Title*	*Sem Hrs*
ENG 101	English Composition I	3
SPH 107	Fundamentals of Public Speaking or	3
SPH 106	Fundamentals of Oral Communication	
MTH 100	Intermediate College Algebra	3
Lab Science Elective: (ASCI)	(astronomy, biology, chemistry, physical science, physics)	4
Social and Behavioral Science Elective: (ASOC)	(anthropology, geography, history, economics, political science, sociology psychology)	3
Humanities and Fine Arts Elective: (AHUM)	(art, humanities, religion, theatre, music philosophy, foreign language, literature)	3
One elective from:	ART 220*, ART 221*, BUS 241, BUS 275	3
	HED or PED Elective	2

Major Courses: **(12 hours)**

Course	*Title*	*Sem Hrs*
CIS 146	Microcomputer Applications	3
CIS 150	Introduction to Computer Logic and Programming	3
CIS 263	Computer Maintenance	3
CIS 270	Cisco CCNA I	3

Cybersecurity Option **(27 hours)**

Course	*Title*	*Sem Hrs*
CIS 202	Python Programming	3
CIS 211S	Principles of Information Assurance	3
CIS 214	Security Analysis (Pen Testing)	3
CIS 222	Database Management Systems	3
CIS 244	Introduction to Cybersecurity	3
CIS 245	Cyber Defense	3
CIS 246	Ethical Hacking	3
CIS 260	Network Security and Risk	3
CIS 282	Computer Forensics	3
TOTAL CREDIT HOURS		**63**

Computer Information Systems Technology Certificate In Cybersecurity (CER C255)

Cybersecurity Option

Course	Title	Sem Hrs
ENG 101	English Composition	3
MTH 100	Intermediate College Algebra	3
CIS 146	Microcomputer Applications	3
Humanities and	Fine Arts Elective: (AHUM) (art, humanities, religion, theatre, music, philosophy, foreign language, literature)	3
CIS 150	Introduction to Computer Logic and Programming	3
CIS 263	Computer Maintenance	3
CIS 270	Cisco CCNA I	3
CIS 214	Security Analysis (Pen Testing)	3
CIS 244	Introduction to Cybersecurity	3
CIS 246	Ethical Hacking	3
CIS 260	Network Security and Risk Management	3
Total Credit Hours		**33**

Computer Information Systems Technology Short Term Certificate in Cybersecurity (STC C255)

Cybersecurity Option

Course	Title	Sem Hrs
CIS 202	Python Programming	3
CIS 263	Computer Maintenance	3
CIS 270	Cisco CCNA I	3
CIS 214	Security Analysis (Pen Testing)	3
CIS 244	Introduction to Cybersecurity	3
CIS 246	Ethical Hacking	3
CIS 260	Network Security and Risk Management	3
Total Credit Hours		**21**

In support of these new programs, effective spring 2021 the following Computer Information Systems (CIS) courses have been added to Jefferson State's Course Inventory:

CIS 202: Python Programming. 3 hrs.
PREREQUISITE: CIS 150
This course is an introduction to the Python programming language. Topics include input and output, decision structures, repetition structures, functions, working with files, strings, object-oriented programming and inheritance. Upon completion, students will be able to demonstrate knowledge of the topics through the completion of programming projects and appropriate tests.

CIS 211: Principles of Information Assurance. 3 hrs.
PREREQUISITE: CIS 146 or database experience
This course is designed to introduce students to information security principles. Topics covered in this course will include the need for security, risk management, security technology, cryptography, and physical security. Security policies and legal/ethical issues will also be covered.

CIS 214: Security Analysis (PEN Testing). 3 hrs.
PREREQUISITE: None.
This course introduces students to the concept of security analysis, or penetration testing, of information systems. Students will evaluate the security of a computer system or network, assessing security risks from the position of a potential attacker. Emphasis is on identifying security flaws and providing technical solutions.

CIS 244: Introduction to Cybersecurity. 3 hrs.
PREREQUISITE: None
This course will introduce students to cybersecurity, while they gain additional insight into the challenges companies face today. Students will develop an understanding of cybercrime, security principles, technologies, and procedures and techniques used to defend networks.

CIS 245: Cyber Defense. 3 hrs.
PREREQUISITE: None
The course provides students with information on the concept of cyber defense. Topics include information relative to legal aspects of cyber-attacks, threats to various levels of national and local social infrastructure, financial systems, personal data, and other direct and indirect threats. As part of this course, students explore current and historical cyber threats and U.S. policy regarding infrastructure protection.

CIS 246: Ethical Hacking. 3 hrs.
PREREQUISITE: None
This course emphasizes scanning, testing, and securing computer systems. The lab-intensive environment provides opportunities to understand how perimeter defenses work and how hackers are able to compromise information systems. With awareness of hacking strategies, students learn to counteract those attempts in an ethical manner.

CIS 260 : Network Security and Risk Management. 3 hrs.
PREREQUISITE: None
This course exposes students to essential concepts of networking security and IT risk management. Topics include design, protocols and administrative principles of secure networks, identification and elimination of threats and vulnerabilities, compliance and operational security, access control and identity management, application, data, and host security, cryptography and current and evolving issues in network security.
Upon successful completion of this course, students will be able to demonstrate the knowledge and skills necessary to identify security issues, to mitigate and deter threats, to apply security controls and to implement and maintain an organization's security policies. **This course prepares students to sit for the CompTIA Security+ certification exam.**