

**Columbus State Community College**

**Workforce Innovation Information Technology**

**Course Syllabus**

**Fall Semester 2018 - Cohort 1**

**COURSE: WIIT- 7410 — CyberSecurity Fundamentals I**

# Faculty Information

**Instructor Name:** Mr. Kent King, Mr. Tim Oroszi **Email**: [kking83@cscc.edu](mailto:kking83@cscc.edu)

**Office:** **Phone:**

**Office Hours:**

**CLASS MEETS: Tuesday at**

**PREREQUISITES:** (need list)

**DESCRIPTION OF COURSE:**

WIIT-7410 is designed for students to learn foundational cyber security concepts, terminology and implementation. Students will learn the practical knowledge and skills necessary to become comfortable with basic concepts, technologies, risks and controls. This course prepares the student for the Systems Security Certified Practitioner (SSCP) certification from ISC2. The course of study will focus on a Common Body of Knowledge including:

* Access Controls
* Security Operations and Administration
* Risk Identification, Monitoring, and Analysis
* Incident Response, and Recovery
* Networks and Communications Security

Students will take an active part in the course by applying hands-on knowledge completing various quizzes and assignments.

**STUDENT LEARNING OUTCOMES**

*Upon successful completion of this course, the student should be able to:*

* Use risk management frameworks and risk profiles
* Explain the difference between qualitative and quantitative risks
* Demonstrate the security foundations of confidentiality, integrity and availability
* Explain the difference between due diligence and due care
* Predict types of attackers and motivations for attack
* Explain the risks of outsourcing and use of 3rd party services
* Explain discretionary and mandatory risk control processes
* Outline the access control lifecycle
* Discuss incident response, continuity plans and recovery strategies
* Identify recovery objectives (RTO, RPO, MTD)
* Compare forensic processes and chain of custody
* Conduct assessments and establish controls
* Utilize asset management and data classification
* Explain patch management, change controls and risks of unauthorized changes
* Discuss security awareness programs, social engineering techniques and user risks
* Evaluate network security risks and mitigation
* Enumerate commonly used ports and protocols
* Assess risks presented by wireless networking
* Identify mobile devices and associated risks
* Outline risks with VoIP, DNS, DHCP and other sensitive network protocols
* Explain basic cloud implementation platforms (SaaS, PaaS) and associated risks

**COURSE MATERIALS REQUIRED**

**Access to CSCC online materials**

**TEXTBOOK**

**Required Digital Text:** **TDB**

**GENERAL INSTRUCTIONAL METHODS**

**ASSESSMENT**

Columbus State Community College is committed to assessment (measurement) of student achievement of academic outcomes. This process addresses the issues of what you need to learn in your program of study and if you are learning what you need to learn. The assessment program at Columbus State has four specific and interrelated purposes: (1) to improve student academic achievements; (2) to improve teaching strategies; (3) to document successes and identify opportunities for program improvement; (4) to provide evidence for institutional effectiveness. In class you are assessed and graded on your achievement of the outcomes for this course. Students will receive a letter grade of either P - Pass, or, F - Fail in the course. Students must obtain 70% or higher to pass the course with a letter grade of “P”.

**STANDARDS AND METHODS FOR EVALUATION**

**Tests and lab exercises will have the following weights:**

|  |  |
| --- | --- |
| **Item** | **Points** |
| Online Quizzes | 100 |
| Assignments 4@25 pts ea | 100 |
| **Total Points** | **200** |

**GRADING SCALE**

|  |  |  |
| --- | --- | --- |
| **Points** | **Percentage** | **Grade** |
| 140 – 200 points | 70 - 100% | P |
| 000 – 139 points | 0 – 69% | F |

**SPECIAL COURSE REQUIREMENTS**

**Attendance Policy**

Frequent attendance is a must for a successful student. Students are expected to attend and prepare for each class by reading and studying the course assignments in advance of scheduled classes.

**Assignment Policy**

Assignments are expected to be completed in a timely manner and students are expected to work on these assignments outside of the regularly scheduled class hours.

**Due dates for online quizzes and assignments are listed on the course syllabus.**

**Capstone**

The Capstone project will gauge the students understanding of cybersecurity fundamentals within a Nationwide-specific experience.

**Course Email Statement:** <https://mail.cscc.edu/student/index.html>

Check your CSCC email regularly. Your instructor will send course information, give updates, or answer questions through your CSCC email. Students are expected to use their CSCC student email account when communicating with your instructor, not your personal email account.

**INCLEMENT WEATHER OR OTHER EMERGENCIES**

In the event of severe weather or other emergencies that could force the college to close or to cancel classes, such information will be broadcast on radio stations and television stations. Students who reside in areas that fall under a Level III emergency should not attempt to drive to the college even if the college remains open.

Assignments due on a day the college is closed will be due the next scheduled class period. If an examination is scheduled for a day the campus is closed, the examination will be given on the next class day. If a laboratory is scheduled on the day the campus is closed, it will be made up at the next scheduled laboratory class. If necessary, laboratory make-up may be held on a Saturday.

Students who miss a class because of weather-related problems with the class is held as scheduled are responsible for reading and other assignments as indicated in the syllabus. Remember! It is the student’s responsibility to keep up with reading and other assignments when a scheduled class does not meet, whatever the reason.

In the event the college is forced to close during Final Examination Week, exams scheduled for the first missed date will be rescheduled for the next day, in the same location at the same time scheduled. Exams scheduled for a second missed date will be rescheduled.

**Campus Closings/Holidays**

* Tuesday, August 14, 2018 – Fall Semester Cohort 1 2018 Begins
* Monday, Sep 3, 2018 – ***Labor Day (Campuses Closed)***
* Monday, November 12 – ***Veteran’s Day (Campuses Closed)***
* November 21-25, 2018 – ***Thanksgiving Holiday (Campuses Closed)***
* Tuesday, December 4, 2018 – Fall Semester Cohort 1 2018 Ends

**UNITS OF INSTRUCTION**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **WEEK #** | **UNIT OF INSTRUCTION** | **LEARNING OBJECTIVES/GOALS** | **ASSESSMENT METHODS** | **ASSIGNMENTS** | **DUE DATE** |
| **1** | Introduction to Cybersecurity | Establish course objectives, responsibilities and online access to materials. Learn cybersecurity terminology. Understand basic cybersecurity concepts (due diligence, least privilege, assets and the CIA pillars).  Learn the primary security categories (prevention, detection and recovery). | Online quiz | **Lesson 1: Introduction to Cybersecurity** | **Quiz responses due 8/20/18** |
| **2** | Risk Management | Describe risk frameworks and assessment methods. Learn qualitative vs. quantitative risk assessments. Understand likelihood, impact and residual risks. Understand controls and control frameworks. Explain risk monitoring processes and control feedback. Explain the difference between a threat and a vulnerability. | Online quiz | **Lesson 2: SSCP Risk Management Domain**  Assignment 1 – Develop a risk register | **Quiz responses due 8/27/18**  **Assignment due 8/28/18** |
| **3** | Access Controls | Learn the distinction between authentication and authorization. Describe multi-factor and federated authentication systems. Explain control frameworks: mandatory, discretionary and access levels. Understand the identity lifecycle. Learn biometric controls and measurements. | Online quiz | **Lesson 3: SSCP Access Control Domain**  Assignment 2 – short essay on the primary vulnerability of the sign-in process | **Quiz responses due 9/3/18**  **Assignment due 9/4/18** |
| **4** | Incident Response & Recovery | Explain the business impact assessment process and the difference from a business continuity plan. Define and describe MTD, RPO and RTO. Learn data backup methodologies. Describe the incident response process and preservation of forensic data. | Online quiz | **Lesson 4: SSCP Incident Response & Recovery Domain**  Assignment 3 – locate an incident response plan on the web. Highlight items you believe are important or missing from your chosen plan. | **Quiz responses due 9/10/18**  **Assignment due 9/11/18** |
| **5** | Incident Response & Recovery | Conduct an incident response “table top” exercise. During the exercise, follow the plan you identified in Assignment 3. Note deficiencies and highlights of the chosen plan. Be prepared to review and discuss the outcome of the exercise. |  | **Lesson 5: SSCP Security Controls Overview & Mobile Device Management**  Assignment 3 (continued) – Summarize (1 page) results of table top and how your selected plan fared. | **Assignment due 9/18/18** |
| **6** | Security Operations & Administration | Learn terminology and fundamental structures for mobile devices, virtualization and stand-alone systems.  Learn change management, testing and accreditation. Discuss security awareness training and social engineering. | Online quiz | **Lesson 6: SSCP Configuration Management** | **Quiz responses due 9/24/18** |
| **7** | Network Security | Describe basic network topologies and security considerations for routers, switches and firewalls. Learn common ports and protocols and associated risks. Explain methods used to monitor network activity. Learn intrusion detection and prevention processes. Describe secure remote access methods. Explain the security related similarities and differences between wireless and wired connectivity. | Online quiz | **Lesson 7: SSCP Network Security**  Assignment 4 – Install nmap and scan your home network. Be prepared to discuss your findings, questions and concerns. | **Quiz responses due 10/1/18**  **Assignment due 10/2/18** |
| **8** | Part I Review and Capstone Introduction | Discuss the ISC2 Code of Ethics and ethical considerations for cybersecurity practitioners. Discuss and launch the Nationwide Capstone. | Capstone |  |  |