CSSS - Cybersecurity | Undergrad

CSSS - Cybersecurity

Global Citizenship Program Knowledge Areas
(bolded code)

- **ARTS**: Arts Appreciation
- **GLBL**: Global Understanding
- **PNW**: Physical & Natural World
- **QL**: Quantitative Literacy
- **ROC**: Roots of Cultures
- **SSHB**: Social Systems & Human Behavior

Global Citizenship Program Skill Areas
(not bolded code)

- CRI: Critical Thinking
- ETH: Ethical Reasoning
- INTC: Intercultural Competence
- OCOM: Oral Communication
- WCOM: Written Communication
- ** Course fulfills two skill areas

Course Descriptions

CSSS 2410 Cybersecurity and Internet Architecture (3)

This course will introduce students to the field of cybersecurity and internet architecture. The application, physical, link, network and transport layers of the protocol stack are presented. Students will study technologies, processes and practices designed to protect networks, computers, programs, and data from attacks. Cybersecurity issues such as malware (worms, phishing, trojans and viruses) and other vulnerabilities will be presented. There is an additional course fee of $380. **Prerequisites**: COSC 2610 and COSC 2670.

CSSS 2510 Cyber Attacks and Defense (3)

This course provides students with insight on common cyber-attacks and the techniques for identifying, detecting and defending against cybersecurity threats. The course will cover firewalls, intrusion detection/prevention, authentication, ciphers, cryptography, etc. The course presents emerging technologies such as virtualization, cloud computing and multimedia protocols. This course also discusses critical infrastructures and how to protect them. **Prerequisite**: CSSS 2410.

CSSS 3510 Writing Secure Code (3)

This course will provide an overview of some of the key issues of secure coding. Students will learn the basics of building secure software that prevents security vulnerabilities that are often exploited by hackers. Topics covered include buffer overflows, un-validated input, race conditions, access-control problems, authentication or authorization weaknesses, and cryptographic practices. Students will also learn best practices that, if followed, will help avoid most security vulnerabilities. The course explores the good and bad security traits of many of the top programming languages such as C, C++, C#, Java, Python, PHP and Ruby. **Prerequisites:** COSC 2810 and CSSS 2510. CS students without Cybersecurity emphasis can take COSC 3410 instead of CSSS 2510.

CSSS 3520 Cybersecurity Programs, Policies and Ethics (3)

This course presents an overview of cybersecurity policies, programs and ethical standards for the cybersecurity career field. To achieve these goals, the course content includes discussions of governance, risk and asset management, physical security, human and environmental security, as well as an overview of the practices of communications and operational security, information systems acquisition, regulatory and legal aspects of the discipline. Additionally, the course presents the ethical and moral responsibilities of cybersecurity practitioners as they use the methods and tools of the discipline. **Prerequisite**: CSSS 2510.

CSSS 4510 Cybersecurity Capstone Project (3)

This course uses project-based instruction and teamwork to reinforce cybersecurity skills. Students will complete an assigned project as a comprehensive assessment of knowledge and skills in cybersecurity. The project activities include research into security problems and planning and designing and implementing security solutions for a user organization. **Prerequisites**: CSSS 3510 and CSSS 3520.