CYBR – Cybersecurity Operations

Technology

Effective Term & Year: Fall 2027
Program Outline Review Date: 2032-03-01

Program Area: Information Technology

Description:

The Cybersecurity Diploma equips students with the technical, analytical, and professional skills needed for entry-level careers in cybersecurity. Students build a strong foundation in computer systems, networking, cybersecurity principles, communication, and mathematics before progressing to network security, scripting, incident response, cloud security, risk management, governance, compliance, and ethical hacking. Through hands-on learning with industry-standard tools, students develop the ability to identify, analyze, and respond to security threats while applying ethical and professional practices. The program concludes with a capstone project, certification preparation, and work-integrated learning preparation to support graduates' transition into the cybersecurity workforce.

Program Information:

This 2-year full-time program provides the knowledge, skills, and training required to prepare students for a career as a Cybersecurity Analyst.

Credentials Granted:

Cybersecurity Operations Diploma

Delivery Methods: Blended (Hybrid)

Credits: 60

Admission Requirements:

Recommended Admission Requirements:

Basic computer literacy skills are expected, including Windows operating system and file management skills, the ability to use word processing software, and the ability to communicate, research, exchange and download files using web browsing and email software.

Program Completion Requirements:

None

Program Learning Outcomes:

Upon completion of the proposed program, graduates will be able to:

- implement firewalls, intrusion detection/prevention systems, antivirus software, and other security solutions to ensure secure network operations;
- use security tools and methodologies to detect, analyze, and respond to cybersecurity threats, incidents, and system breaches, maintaining system integrity and availability;
- apply principles of risk management and threat mitigation to design and enforce protective controls that reduce vulnerabilities across networks and systems;
- apply organizational security policies and response procedures in compliance with legal, ethical, and industry standards;
- assess networking environments to support compliance with relevant frameworks, standards, and regulations across various industries, aligning practices with legal and organizational requirements;
- use written, visual, and verbal communication to explain security concepts, report incidents, and collaborate within multidisciplinary teams in professional contexts;
- analyze complex security and networking problems, identify root causes, and develop effective solutions using structured reasoning and troubleshooting approaches;
- adhere to professional codes of conduct and cybersecurity ethics, recognizing and addressing ethical dilemmas and the impact of actions on individuals and organizations; and
- reflect on personal performance and keep pace with emerging cybersecurity and networking technologies, standards, and threats through self-directed learning.

Prior Learning and Recognition: Yes

Students are able to request formal recognition of their prior learning or experience outside the classroom. Challenge examination, portfolio-assisted assessment, work-based assessment or a combination of assessments that is appropriate to identify, assess, and recognize prior skills, competencies, and knowledge to achieve course credit. Tuition fees apply, refer to Policy 2.5.5 Prior Learning Assessment and Recognition (PLAR) or contact an education advisor for more information.

Program Transfer Credit:

For information about block transfer agreements between programs in British Columbia, Alberta, and elsewhere, please visit http://www.cotr.bc.ca/transfer.

To minimize transfer issues, check with an academic advisor at the institution that will receive the transfer credits.

Academic Policies:

College of the Rockies policies related to courses can be found at https://cotr.bc.ca/about-us/college-policies/ and include the following:

- Policy 2.1.4 Course Audit
- Policy 2.4.1 Credential Framework
- Policy 2.4.3 Students with Documented Disabilities
- Policy 2.4.4 Student Rights, Responsibilities and Conduct
- Policy 2.4.8 Academic Performance
- Policy 2.4.9 Student Feedback and Concerns
- Policy 2.4.11 Storage of Academic Works
- Policy 2.5.3 Student Appeal
- Policy 2.5.5 Prior Learning Assessment and Recognition (PLAR)

Program Changes:

Information contained in this program outline is correct at the time of publication. Courses and course content may be revised from time to time based on changing educational, employment and marketing needs. The timetable may also be revised.

Course Descriptions: Refer to Course Outlines – https://outlines.cotr.bc.ca/course/