ContinuingEducation GPRC

CONTINUING EDUCATION

COURSE OUTLINE – Introduction to Cybersecurity

INSTRUCTOR:	N/A	**PHONE:**	780-539-2975
OFFICE:	M105	**E-MAIL:**	ce@gprc.ab.ca

PREREQUISITE(S): This course requires some basic understanding of IT concepts.

REQUIRED TEXT/RESOURCE MATERIALS:

Course materials are included.

CALENDAR DESCRIPTION:

Globally, incidents of data breaches, identity thefts, and cybercrimes are on the rise, along with the explosive growth of online personal data and the expansion of computer networks. This course teaches the fundamental concepts of information security one will encounter in the cybersecurity field. This course will set the groundwork with basic vocabulary and then introduces concepts such as access controls, risk management, cyber attacks, and digital forensics.

CONTACT HOURS: 5 hours

CEUs: 0.5

PDUs: 5

DELIVERY MODE: Online self-paced

TRANSFERABILITY: N/A

GRADING CRITERIA:

Upon successful completion of the course, you will receive a Certificate of Completion.

EVALUATIONS: Learners must achieve an average test score of at least 70% to meet the minimum successful completion requirement and qualify to receive IACET CEUs.

The following list outlines the PDUs you will earn for completing this course, based on the certification you have.

Designation	Technical	Leadership	Strategic/Business	TOTAL
PMP®/PgMP®	2	1.5	1.5	5
PMI-RMP®	2	1.5	1.5	5
PMI-SP®	0	1.5	1.5	3
PMI-ACP®	2	1.5	1.5	5
PfMP®	0	1.5	1.5	3
PMI-PBA®	0	1.5	1.5	3

STUDENT RESPONSIBILITIES: Completion of any practice lessons, quizzes, assignments, or tests.

COURSE SCHEDULE/TENTATIVE TIMELINE:
Dates vary (refer to website for current availability).

LEARNING OUTCOMES:
Upon successful completion of this course, learners will be able to:

- Describe fundamental information security concepts
- Discuss data breaches and hacker motivations
- Identify different types of information access controls
- Describe the importance of accountability and audits
- Explain the technologies used to provide identification and authentication
- Relate the role of risk and risk management in information technology
- Describe different methods of cryptography
- Define the elements of a business continuity and disaster recovery plan
- Identify common access control attacks and countermeasures
- Describe the steps involved in a digital forensics investigation