ContinuingEducation GPRC

CONTINUING EDUCATION

COURSE OUTLINE – Security Engineering

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

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

REQUIRED TEXT/RESOURCE MATERIALS:

Course materials are included.

CALENDAR DESCRIPTION:

This course contains an introduction to the key concepts of cryptography and security engineering. It examines the role of encryption in information security and considers common encryption methods. In addition, the course discusses ciphers, their substitutes, and how they work. Public key infrastructure and management is also covered.

The content in this course aligns with Domain Three in the CISSP exam, offered by (ISC)2. However, the course can be taken as a stand-alone without the intention of sitting for the exam.

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®	3	0	2	5
PMI-RMP®	3	0	2	5
PMI-SP®	0	0	2	2
PMI-ACP®	3	0	2	5
PfMP®	0	0	2	2
PMI-PBA®	0	0	2	2

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:

- Understand how cryptography works and its role in information security
- Compare and contrast different ciphers and explain how they work
- Create substitution ciphers and encode and decode cleartext and ciphertext
- Discuss how encryption enables secure transmission of sensitive data
- Explain and compare symmetric and asymmetric cryptography
- Describe the role of public key infrastructure and key management