UNIVERSITY OF THE FRASER VALLEY

ORIGINAL COURSE IMPLEMENTATION DATE: January 2005
REVISED COURSE IMPLEMENTATION DATE: September 2026
COURSE TO BE REVIEWED (six years after UEC approval)**:** March 2032
Course outline form version: 29/08/2024

OFFICIAL UNDERGRADUATE COURSE OUTLINE FORM

Note: The University reserves the right to amend course outlines as needed without notice.

Course Code and Number: CIS 497	**Number of Credits:** 3 Course credit policy (105)
Course Full Title: Advanced Topics in Information Security **Course Short Title:** Adv Topics in Info Security	
Faculty: Faculty of Business and Computing	**Department/School:** School of Computing

Calendar Description:

This advanced topics course is designed to provide study of the current and emerging trends, technologies, and challenges in information security not covered in other courses. Topics may be drawn from areas such as physical and network security, secure programming, policies and ethics, intrusion detection, OS hardening, cryptography, blockchain and web3 security, privacy and data protection, digital forensics, cloud security and AI for threat detection and response. Topics will vary depending on semester and instructor. Students should consult the department for current offerings.

Prerequisites (or NONE):	COMP 325.
Corequisites (if applicable, or NONE):	
Pre/corequisites (if applicable, or NONE):	

Antirequisite Courses *(Cannot be taken for additional credit.)*

Former course code/number:

Cross-listed with:

Equivalent course(s):

(If offered in the previous five years, antirequisite course(s) will be included in the calendar description as a note that students with credit for the antirequisite course(s) cannot take this course for further credit.)

Typical Structure of Instructional Hours

Lecture/seminar	45
Total hours	**45**

Scheduled Laboratory Hours

Labs to be scheduled independent of lecture hours: **No**

Course Details

Special Topics course: **Yes**

(If yes, the course will be offered under different letter designations representing different topics.)

Directed Study course: **No**

(See policy 207 for more information.)

Grading System: **Letter grades**

Delivery Mode: **May be offered in multiple delivery modes**

Expected frequency: **Annually**

Maximum enrolment (for information only)**: 35**

Prior Learning Assessment and Recognition (PLAR)

PLAR is available for this course.

Transfer Credit *(See bctransferguide.ca.)*

Transfer credit already exists: **No**

Submit outline for (re)articulation: **No**

(If yes, fill in transfer credit form.)

Department approval	**Date of meeting:**	January 2026
Faculty Council approval	**Date of meeting:**	February 13, 2026
Undergraduate Education Committee (UEC) approval	**Date of meeting:**	March 27, 2026

Learning Outcomes *(These should contribute to students' ability to meet program outcomes and thus Institutional Learning Outcomes.)*

Upon successful completion of this course, students will be able to:

1. Analyze emerging trends and technologies in information security.
2. Evaluate advanced security models and frameworks in diverse contexts.
3. Design secure solutions to address evolving cybersecurity threats
4. Integrate ethical and societal considerations particularly those relevant to Indigenous perspectives into the development and implementation of security practices.

Recommended Evaluation Methods and Weighting

Assignments:	10%	Quizzes/tests/midterm:	30%	Final exam:	30%
Holistic assessment:	10%	Project:	20%		%

Details:

NOTE: The following sections may vary by instructor. Please see course syllabus available from the instructor.

Typical Instructional Methods *(Guest lecturers, presentations, online instruction, field trips, etc.)*

Lecture, hands-on experience where applicable.

Texts and Resource Materials *(Include online resources and Indigenous knowledge sources. Open Educational Resources (OER) should be included whenever possible. If more space is required, use the Supplemental Texts and Resource Materials form.)*

For sample topic **Privacy and Data Protection**:

	Type	Author or description	Title and publication/access details	Year
1.	Book	William Stallings	Information Privacy Engineering and Privacy by Design	2021
2.	Article	Carlisle Adams	Introduction to Privacy Enhancing Technologies	2021
3.	Online resource	Government of Canada	Personal Information Protection and Electronic Documents Act	2000
4.	Indigenous knowledge	First Nations Information Governance Centre (FNIGC)	OCAP® Principles: Ownership, Control, Access, and Possession	2023
5.				

Required Additional Supplies and Materials *(Software, hardware, tools, specialized clothing, etc.)*

Determined by instructor and topic.

Course Content and Topics

For sample topic **Privacy and Data Protection**:

1. Foundations of privacy and data protection
2. Legal and regulatory frameworks
3. Privacy risks, threats, and violations
4. Data classification and risk assessment
5. Technical privacy and security measures
6. Privacy-preserving technologies
7. Privacy architecture and system design
8. Ethical, societal, and Indigenous perspectives