UNIVERSITY OF THE FRASER VALLEY

Number	249
Effective Date	2024-10-08
Next Review Date	2031-10

INFORMATION SECURITY

Approval Authority	President
Responsible Executive	Vice-President Administration
Related Policies / Legislation	Freedom of Information and Protection of Privacy Act Information Act Appropriate Use of Computing and Network Resources (14 – replacement policy under development)

PURPOSE

The Information Security policy addresses the University of the Fraser Valley's (UFV) management and security of its information and information systems, and the use of these assets by its constituents and others who may use university information. As part of UFV's Enterprise Risk Management program, this policy speaks to the reduction of information technology security risks and the management of information.

PHILOSOPHY

Information and information systems are vital assets of UFV, essential for the delivery of education and services and the management of resources. UFV prioritizes the protection of the information in its custody from unauthorized access, modification, disclosure, or destruction. This involves identifying and assessing information security threats and developing and implementing mitigation controls. It also includes having an overall information security framework that aligns with UFV's risk framework and regulatory and contractual requirements.

SCOPE

This policy applies to:

- Faculty, staff, volunteers, students, alumni, and authorized users of UFV's information assets including computing resources, data, networks, or information.
- Technology or services used to process or transmit information assets.
- Information assets which are processed for, by or on behalf of UFV, including with external parties.
- Information assets that are stored by UFV, or on behalf of UFV on an external service provider.
- Information created or transmitted to or from UFV by authorized agreement.
- Third-party cloud computing systems owned by vendors and managed by the university.
- Information which the university processes, stores, transmits irrespective of ownership or form.

POLICY

UFV adheres to the recommendations set out in the *UCISA Information Security Toolkit* which is based on the control guidelines set out in the industry standard ISO 27001.

The University's information security is managed through the framework which comprises this policy and standards alongside supporting governance processes. This approach provides a flexible and effective platform to achieve the University's information security objectives.

The University adopts guiding principles and standards which underpin this policy and are available on the UFV Cybersecurity website.

ROLES AND RESPONSIBILITIES

The CIO or designate is responsible to maintain and publish standards, procedures, information security programs, mitigation strategies, communications, training, and other related requirements of this policy.

General Counsel

The General Counsel, who also serves as the Privacy Officer at UFV*,* in consultation with the CIO or designate, receives suspected violations of this policy that involve personal information. This may involve Campus Security, other units, or individuals to assist in specific situations. The General Counsel, when necessary, initiates a review and may recommend appropriate action.

Records Management

The General Counsel or designate takes reasonable effort to ensure the UFV's records management protocols are integrated into information and information security standards, procedures, and protocols.