1 EMAIL AND COMMUNICATIONS SECURITY STANDARD

Title	Email and Communications Security Standard
Reference	ISS-05
Status	PUBLISHED
Version	1
Date	December 2024
Review	TBD
Classification	Public
Guidance	NIST SP 800-171, Section 3.5.1-3.5.11

The Chief Information Officer has issued this standard under the authority of UFV's Information Security Policy. Questions about this standard may be referred to cybersecurity@ufv.ca

2 SUMMARY

This e-mail Communications Policy is a sub-policy of the Information Security Policy (ISP-01) and outlines the University's requirement to comply with certain legal and regulatory frameworks. This policy is to be read in conjunction with other university directions to legislation and provides details of the legislation relevant to information security e.g., the BC Privacy Act.

This standard describes requirements for securing infrastructure against cyber threats in order to support the Information Security Policy and to ensure that the Company meets its business requirements for Information Security.

3 SCOPE

This Standard applies to

a) those applications and infrastructure which the University has designated as being subject to the Standard,
b) all new applications and infrastructure as they are acquired or developed, and
c) all other applications and infrastructure as substantive changes may be made to them.

Whenever circumstances or technologies make immediate compliance with this Standard impractical, the exception process outlined in the Information Security Policy will be used.

This Standard applies to the Information Services Organization of the company. It shall guide the development of, and become part of, the methodologies, procedures, processes and other activities of the Information Services Organization.

This Standard also applies to all staff who perform Information Services functions, who shall be familiar with this Standard and, to the extent that it applies to their work and functions, shall comply with it.

4 E-MAIL POLICY

4.1 EMAIL TERMS OF USE:

Use of email must be consistent with the university of the Fraser Valley's policies and procedures of ethical conduct, safety, compliance with applicable laws and professional practices.

UFV supplied email account should be used primarily for university related purposes; personal communication is permitted on a limited basis, but non-university related commercial uses are prohibited.

Data contained within an email message, or an attachment must be secured according to the Data Protection Standard.

Email will be retained if it qualifies as a UFV record. Email that is identified as a UFV record shall be retained according to the universities Record Retention Schedule.

UFV email systems shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.

Users are prohibited from automatically forwarding University of the Fraser Valley email to a third-party email system. Individual messages which are forwarded by the user must not contain University of the Fraser Valley confidential or above information.

A reasonable amount of University of the Fraser Valley resources for personal emails is acceptable, but personal or non-work-related email should be saved in a separate folder from work related email.

UFV constituents shall have no expectation of privacy in anything they store, send or receive on the University's email system.

Use of UFV email signals acceptance of incoming email shall be scanned for viruses, phishing attempts, and spam.

Outgoing email may have data loss prevention (DLP) monitoring in place.

Any third party messaging service shall be approved by Information Security prior to usage and shall include appropriate audit trails and encryption of data at rest and in transit. Data loss prevention (DLP) tools and processes shall be implemented, where possible.

4.2 EMAIL AUTHENTICATION:

Email authentication protocols, such as SPF, DKIM, and DMARC, should be implemented to prevent email spoofing and phishing attacks. Email gateways should be configured to reject or quarantine messages that fail authentication checks.

4.3 ENCRYPTION:

Emails containing sensitive information should be encrypted using an approved encryption method. Encryption helps to ensure that the information remains confidential and cannot be intercepted by unauthorized parties.

4.4 ACCESS CONTROL:

Access to email accounts should be granted only to authorized individuals who require access to perform their duties.

4.5 MOBILE DEVICE SECURITY:

Mobile devices used to access email should be secured with a password or other form of authentication. Mobile devices should have remote wiping enabled in case of loss or theft. Users should be encouraged to keep their devices up to date with security patches and software updates.

4.6 ARCHIVING AND RETENTION:

Emails should be archived and retained according to the organization's information retention policy. Archiving and retention policies should comply with relevant laws and regulations.

4.7 MONITORING AND REVIEW:

Email and communication systems should be monitored regularly for suspicious activity, such as phishing attempts or unauthorized access attempts. Regular reviews should be conducted to ensure that email security policies and procedures are being followed.

4.8 RELATED STANDARDS, POLICIES AND PROCESSES

- Data Protection Standard