1 DATA LOSS AND ENCRYPTION STANDARD

Title	Data Loss and Encryption Standard
Reference	ISS-04
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 standard is part of the University's Information Security Policy and sets out the requirements in conjunction with the university other policies for data and records management, including Compliance with appropriate legislation. This standard describes how data loss prevention processes and technologies must be deployed and configured to ensure that the University meets its requirements for Information Security.

3 SCOPE

This Policy applies to Information Assets owned by and/or entrusted to the University (including whether held by the University or by others for the University) and to all computer systems, hardware and software, and networks which the company has designated as being subject to this policy.

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

4 DATA LOSS PREVENTION STANDARD

4.1 DEPLOY DATA LOSS PREVENTION TECHNOLOGIES AND PROCESSES.

Information leakage protection mechanisms must be:

a) centrally managed,

b) configured to include a register of keywords, electronic document characteristics and the specific types of information that need to be protected from unauthorized disclosure.
c) capable of considering the context of information before identifying information as being at risk of disclosure or detected as being disclosed to unauthorized parties,
d) updated on a regular basis and continuously refined to ensure their configurations reflect the sensitive information that needs to be protected,
e) reviewed to help minimize false positives and false negatives.

4.2 MONITOR FOR DATA AT RISK.

Information leakage protection mechanisms must:

a) Scan databases, collaboration spaces, network folders, local hard disk drives
b) Monitor electronic documents, to identify pre-defined sensitive information that is stored in locations that may increase the risk of unauthorized disclosure.
c) Detect when pre-registered sensitive information is disclosed.

4.3 MONITOR FOR UNAUTHORIZED DATA EXFILTRATION.

Information leakage protection mechanisms must monitor network traffic leaving the company to identify:

a) the use of unauthorized encryption, which might be used to conceal unauthorized disclosure,
b) unauthorized external network connections,
c) network traffic destined for known malicious servers or network domains on the Internet.

4.4 MONITOR EGRESS POINTS.

Information leakage protection mechanisms must monitor all egress points including:

a) email (including attachments),
b) web, including encrypted traffic to web mail and cloud storage services,
c) file transfers, including from internal workstations,
d) storage media,
e) mobile devices,
f) instant messaging,
g) Voice over IP traffic,
h) all encrypted traffic.

4.5 PREVENT POTENTIAL DATA LOSS.

Information leakage protection mechanisms must be configured to protect preregistered sensitive information that is at risk of disclosure or is being disclosed to unauthorized parties, by:

a) removing pre-registered sensitive information from locations that violate the information handling requirements of the Information Assets,

b) warning users of potential unauthorized disclosure of pre-registered sensitive information,

c) monitoring information copied to portable storage devices,

d) detecting and recording details about the connection of unauthorized portable storage devices,

e) restricting the copying of pre-registered sensitive information only to authorized portable storage devices,

f) blocking unauthorized user actions that violate the information handling requirements of the Information Assets (e.g. Unauthorized exporting of data from applications, unauthorized printing),

g) preventing the unauthorized transmission of pre-registered sensitive information,

h) quarantining information for further analysis, for example to determine if the disclosure is a legitimate business action.

4.6 ALERT ON POTENTIAL DATA LOSS.

Information leakage protection mechanisms must be configured to:

a) provide an alert when unauthorized disclosure activity is detected,

b) report relevant events to the centralize Security Information Event Management (SIEM) service for analysis and actioning.