1 INFORMATION CLASSIFICATION AND HANDLING STANDARD

Title	Information Classification and Handling Standard
Reference	ISS-03
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 outlines the University's Information Security framework. This policy is to be read in conjunction with the university other policies for data and records management, including Compliance with appropriate legislation.

It describes the University's Information Handling policy, the roles and responsibilities related to Information Assets, and how to appropriately secure and handle information based on its classification to support the Information Security Policy and 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 AUDIENCE

This Standard applies to the Information Services of the University. 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.

5 INFORMATION CLASSIFICATION STANDARDS

5.1 INFORMATION ASSET REGISTRY

The University will maintain an Information Asset Register detailing its main information assets and assigning ownership to information asset owners. Each asset will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset.

5.2 INFORMATION CLASSIFICATION:

All information assets should be classified based on their sensitivity and confidentiality level. This includes but is not limited to, personal data, financial information, and intellectual property. The classification should be reviewed periodically to ensure that the classification level is still appropriate.

6 INFORMATION HANDLING STANDARDS

Procedures for handling information assets should be established and communicated to all personnel who have access to sensitive information. These procedures should include guidelines on access control, data storage, and data transmission.

6.1 ACCESS CONTROL

Members of the University will be granted access to the information they need to fulfil their roles within the University. Members who have been granted access must not pass on information to others unless the others have also been granted access through appropriate authorisation. All access should be authorized and monitored, and access privileges should be revoked when they are no longer required.

6.2 DATA STORAGE:

Sensitive information should be stored securely, either in a locked room, a secure filing cabinet or encrypted storage device. All electronic devices should be password-protected and encrypted. When sensitive information is no longer needed, it should be securely destroyed using an approved destruction method.

6.3 DATA TRANSMISSION:

When transmitting sensitive information, encryption should be used to protect the data during transmission. Transmission methods should be secure, and personnel should be trained on how to securely transmit data.

6.4 HANDLING OF PERSONAL DATA:

When handling personal data, strict guidelines should be followed. These guidelines should include informing individuals of their data privacy rights, obtaining consent for data collection, and ensuring that the data is used only for the purposes for which it was collected. Personal data should be stored and transmitted securely, and personnel should be trained on how to handle personal data securely.

6.5 DISPOSAL OF INFORMATION

Information assets must be disposed of with care in accordance with classification requirements.

Paper waste that is classified as confidential or above must be disposed of following formal University procedure.

Electronic information must be securely erased or otherwise rendered inaccessible before leaving the possession of the University unless the disposal is undertaken under contract by an approved contractor.

Destroy media containing Personal Data when it is no longer needed for business or legal reasons by following procedures including, but not limited to:

- Disposal of media containing Personal Data so that it is rendered unreadable or undecipherable, such as by burning, shredding, pulverizing, or overwriting. Media sanitization processes shall be implemented following the NIST 800-88 standard, where possible.
- Disposal logs that provide an audit trail of disposal activities shall be securely maintained. Disposal logs will be kept for a minimum of ninety (90) days.
- Certificates of destruction shall be maintained for at least one year.

In cases where a storage system (for example a USB stick, portable drive, or printer hard drive) is required to be returned to a supplier, it should be securely erased before being returned unless contractual arrangements are in place with the supplier which guarantee the secure handling of the returned equipment. If this is not possible, then the storage system should not be returned to the supplier and should remain in the possession of the University until it is disposed of securely.

6.6 REMOVAL OF INFORMATION

University data subject to PIPEDA, BC PIPA, or other data protection legislation, or that has a classification of confidential or above must be stored using University facilities or with third parties subject to a formal, written legal contract with the University. In cases where it is necessary to

otherwise remove data from the University, appropriate security measures must be taken to protect the data from unauthorised disclosure or loss.

Information classed as confidential or above in electronic form must be strongly encrypted prior to removal or transmission. Secret data must never be removed except with the explicit written permission, and in accordance with the directions of, the data owner.

6.7 BACKUPS

Information asset owners must ensure that appropriate backup and system recovery measures are in place and that those measures are compliant with any agreements with external partners from whom data has been obtained.

For all backups, appropriate security measures must be taken to protect against unauthorised disclosure or loss. Recovery procedures should be tested on a regular basis.

Information that is entrusted to the care of IT Services will meet these requirements.

6.8 EXCHANGE OF INFORMATION

Information classified as sensitive and confidential must be strongly encrypted prior to electronic exchange, both within the University and in exchanges with third parties. Information classified as confidential or higher may not be transmitted electronically except with the explicit written permission of the information owner and in accordance with their handling requirements.

When exchanging information by email, collaboration, instant messaging, or other digital information sharing methods, recipient addresses or identifiers should be checked carefully prior to transmission.

Unsolicited emails, telephone calls, instant messages or any other communication requesting information that is not classified as public should not be acted upon until and unless the authenticity and validity of the communication has been verified.

Members of the University must not disclose or copy any information classified as confidential or above unless they are authorised to do so.

Whenever significant amounts of personal data or other confidential information are exchanged with other organisations, appropriate information security measures must be established to ensure the integrity and confidentiality of the data transferred. Regular exchanges must be covered by a formal written agreement with the third party.

To protect the confidentiality of PII in transit:

- Ensure that all data in transit is either encrypted and/or the transmission channel itself is encrypted following Data Protection & Encryption Policy.
- Monitor all data exchange channels to detect unauthorized information releases.
- Use Information Security approved security controls and data exchange channels.

6.9 INFORMATION ON DESKS, SCREENS, AND PRINTERS

Members of staff who handle paper documents containing information classified as confidential or above must take appropriate measures to protect against unauthorised disclosure, particularly when they are away from their desks. Documents classified as confidential or above should not be left unattended and secured overnight.

Care must also be taken when printing confidential documents to prevent unauthorised disclosure.

Computer screens on which information classified as confidential or above is processed or viewed must be sited in such a way that they cannot be viewed by unauthorised persons.

Computer screensavers must be enabled to lock after a specified time on inactivity.

All computers must be locked while unattended.

6.10 REMOVABLE MEDIA POLICY

All removable media brought in from outside must be scanned for viruses/malware prior to use. Any identified malware/viruses shall be removed with the assistance of Information Technology Support prior to use.

University data is prohibited to be saved on any kind of removable device unless the device is approved by the Information Security team (cybersecurity@ufv.ca) and is encrypted following Data Protection & Encryption Policy. Personnel will follow company policies and procedures, including Information Security Policy, and Acceptable Use to mitigate the risk of a Data Breach.

6.11 REPORTING LOSSES

All members of the University have a duty to report the loss, suspected loss or unauthorised disclosure of any University information asset to the information security incident response team (cybersecurity@ufv.ca). This includes the loss of personal devices, such as phones or USB drives, on which University information assets might reside.