# Alliance Federation Data Handling Standard

Document ID: SEC-03
Approval Date: 2022-08-24
Approved By: NSC

## 1. Introduction

This standard details appropriate handling of data based on the data classification defined in *SEC-02 Data Classification Policy*.

## 2. Definitions

Refer to *SEC-00 Cybersecurity Glossary*.

## 3. Applicability

This standard applies to data stored, processed, and transmitted by the Alliance Federation.

## 4. Data Handling Requirements

### 4.1 Data Labeling/Disclaimer

Where possible, Moderate, High, or Very High Risk data must be labeled to specify its classification and owner according to *SEC-02 Data Classification Policy*. The method for labeling data will depend on its format. These may include:

- Document header/footer
- Linked or embedded metadata
- Disclaimer or readme file to describe a collection or data-set
- Banner message in application/database
- Printed cover for hard-copy or other physical media

Preferably, labels should be visible when accessing the data directly (e.g. within a document rather than a readme file).

### 4.2 Data Inventory

The Data Owner or their assigned Data Steward must maintain an inventory of all High or Very High Risk data for which they are responsible. At a minimum the inventory should contain the following:

- Data Owner
- Data Steward (if applicable)
- Data Classification
- Location/System
- Medium/Format (Digital document, Database, Hardcopy)
- A General Description

## 4.3 Data Held by Third Parties

Alliance Federation data managed by 3rd parties including vendors and partners must be handled in accordance with this standard. In addition the *Vendor Security Checklist* should be completed prior to providing access to Alliance Federation data.

## 4.4 System and Service Hardening

Systems, Services and their underlying infrastructure must be hardened according to industry best practices including but not limited to:

- Use of a Configuration Management system
- Disabling unnecessary services
- Limit network exposure and access accounts
- Resource Isolation

## 4.5 Transmission of Data

Data transmission involves a copy of data being moved from one place to another. When data is transferred from one security realm/domain to another it must be secured in accordance with its data classification.
All data should be transferred in accordance with industry best practices for encryption in transit (see https://cyber.gc.ca/en/guidance/guidance-securely-configuring-network-protocols-itsp40062)
It is recommended that all data be transferred through an encrypted channel whenever possible.

The following table outlines examples of data sharing/transmission modalities based on classification:

| Example | Low Risk | Moderate Risk | High Risk | Very High Risk |
|---|---|---|---|---|
| Email[1] | Acceptable | Acceptable | Not Recommended - Use encrypted attachment if necessary. | |
| Email (Personal/Other) | Acceptable | Not Recommended | Prohibited | |
| Globus | Recommended (when encrypted transfers are used) | | | |
| Collab Tools[2] (OTRS, Gitlab) | Recommended | Not Recommended | Prohibited | |
| Text Chat - Slack[2] | Recommended | | Acceptable | Prohibited |
| Videoconferencing Tools (Slack[2], Meet[2], Zoom[1], Teams[1]) | Recommended | | | |
| File Sharing ( G-Suite[2], NextCloud[2]) | Recommended | | | |
| Third-party Tools (Dropbox, personal accounts, other institutional tools, etc.) | Not Recommended | Prohibited | | |

## 4.6 Protection at Rest

Data must be stored, accessed, and maintained in accordance with industry best practices including encryption at rest. The selected encryption technology must ensure appropriate levels of confidentiality against unauthorized third-party access. Examples of acceptable encryption methods include full-disk, volume, and file-level encryption. The following table outlines example cases and whether use of encryption is optional, recommended, or required:

[1] Digital Research Alliance of Canada tennant(s)
[2] Alliance Federation tennant(s)

| Storage location | Low Risk | Moderate Risk | High Risk | Very High Risk |
|---|---|---|---|---|
| Alliance Federation Data Centers | Optional | Recommended | Required | Required |
| Commercial clouds | Optional | Recommended | Required | Required |
| Partner institutions | Optional | Recommended | Required | Required |
| Laptops and other portable devices (e.g. USB hard drives, USB keys, smartphones) | Optional | Required | Required | Required |
| All other data | Optional | Required | Required | Required |

## 4.7 Auditing and Logging

Access to all data must be logged in accordance with *SEC-05-System Logging and Security Monitoring Standard*.

## 4.8 Backup and Recovery

The classification of data must be taken into account as part of the backup and restoration process. The same controls and principles must be applied to data at all stages of the lifecycle and to all copies of data (e.g. portable storage, temporary storage locations, scratch space).

## 4.9 Patch Management

All Alliance Federation assets must be patched on a regular basis, and prior to patching production environments, changes should be tested in a non-production environment to ensure there are no adverse impacts.

## 4.10 Vulnerability Management

Systems, services and their underlying infrastructure must have regular vulnerability scanning in accordance with *SEC-04-Vulnerability Management Standard*.

## 4.11 Endpoints and Physical Security

The handling of data, including personnel involved in handling data must be protected in accordance with industry norms including but not limited to:

- Enforced Screen Timeouts
- Use of Non-shared devices
- Unlock is required to access systems and services
- Utilizing automatic software updates / Up to date patches
- Use of Anti-virus or EDR
- Reasonable network security (See https://www.getcybersafe.gc.ca/en)
- Awareness of surroundings and the potential for shoulder surfing
- Awareness of social engineering and phishing attacks

## 4.12 Data Disposal/Destruction

All data must be retained as long as required by applicable regulation and/or policy. Once data is no longer required it must be destroyed, including cases involving the reuse of storage devices.
Refer to https://cyber.gc.ca/en/guidance/sanitization-and-disposal-electronic-devices-itsap40006 for more information (note that “Erase and factory reset” is insufficient for data destruction).

The following table summarizes appropriate methods to employ:

| Method | Encrypted Magnetic Media | Unencrypted Magnetic Media | Encrypted Solid State | Unencrypted Solid State |
|---|---|---|---|---|
| **Overwrite and secure erase (SE)** | ✓ | ✓ | | |
| **Crypto erase (CE)** | ✓ | | ✓ | |
| **Degaussing** | ✓ | ✓ | | |
| **Physical destruction** | ✓ | ✓ | ✓ | ✓ |

- When deleting data from an active storage system, any backup copies of the data must also be deleted and purged as soon as possible and never longer than 12 months.
- Data held by vendors must be certified to be destroyed through one of the means specified in the *Vendor Security Checklist*.

## 5. Related Information

SEC-00 Information Security Glossary
SEC-02-Data Classification Policy
SEC-04-Vulnerability Management Standard
SEC-05-System Logging and Security Monitoring Standard
Vendor Security Checklist