Data Classification Policy

Document ID: **SEC-02**
For: Alliance Federation
Approval Date: 2022-03-15
Approved By: CSAC

1. Introduction

The purpose of this policy is to establish the methodology for classifying data based on its level of sensitivity, value and criticality to the Alliance Federation as required by the *SEC-05 Cybersecurity Risk Management Policy*. Classification of data will aid in determining baseline security controls for the protection of data based upon the corresponding level of risk. It is important to classify data to ensure it has the appropriate level of protection.

2. Definitions

Refer to *SEC-00 Information Security Glossary* definitions used in this Policy

3. Applicability

3.1 This Policy applies to all persons as well as any other affiliates who are authorized to access one or more ***National Service*** and who are responsible for classifying and protecting data on systems within the Alliance Federation and its affiliates.

3.2 Roles and Responsibilities

3.2.1 The Steward/Owner is responsible for determining the data security classification of their datasets. In the course of its operation, the Alliance Federation may treat or handle data as if its classification is of a higher level, but never use a lower level of classification. Data may be classified at a higher level than the examples listed in table 4.1 but may not be reclassified to a lower level.

3.2.2 The Custodian is responsible for knowing the types of electronic data under their control, the risk their datasets present to the Alliance Federation or its affiliate, its data security classification, and where it is stored.

4. Classification

4.1 Data Classifications:

Data classification reflects the level of risk to the Alliance Federation or affiliates if confidentiality, integrity or availability is compromised. Classification also reflects the inherent value of data and the controls that should be in place to protect it.

Low-Risk Information (Level 1)

Examples:

- Information that requires no protection
- Information that is publicly accessible (e.g. Published annual reports, press releases, new articles)
- Names and work contact information of Alliance Federation Team Members
- Information that may be posted to public websites
- Information of a non-personal and non-proprietary nature including anonymous research data where access to that data is not restricted

Potential risk:

- Minor embarrassment but very limited in scope

Moderate-Risk Information (Level 2)

Examples:

- Proprietary information received from a third party under non-disclosure agreements (NDA) or that we would share under non-disclosure agreements if higher-risk categories are not applicable
- Restricted circulation library journals
- Aggregate financial information and reports
- Technical information about systems or facilities that is unlikely to result in any harm.
- Information of a non-personal, possibly proprietary nature including anonymous research data where access to that data should be restricted

Potential risk:

- Limited impact on reputation or finances within a national host site or affiliate
- Limited impact on operations within a national host site or affiliate
- Loss of priority of publication (e.g. first to publish)
- Loss of access to journals or other copyrighted materials

High-Risk Information (Level 3)

Examples:

- Controlled data requiring protection by law, NDA or industry regulation
- Data associated with patents or patent applications
- Personally identifiable information
- Confidential financial information and records
- Technical information that facilitates compromise of systems or facilities
- Research data that would take significant efforts or cost to collect or reproduce (e.g. additional funding may be required)

Potential risk:

- Impact on reputation or finances of a national host site or affiliate
- Impact on operations of a national host site or affiliate
- Potential for identity theft
- Potential for fraud or spear phishing

Very High-Risk Information (Level 4)

Examples:

- Customer Payment Card Information when a national host site or affiliate is acting in a merchant capacity
- Personal Health Information as defined by provincial or federal legislation (PHI)
- Personally identifiable genetic data
- Biometric data
- Copy of government identification card
- Strategic or sensitive research software or dataset
- Personally identifiable data protected by regulation/legislation (e.g. GDPR)
- Research data that may not be possible to collect or reproduce

Potential disclosure risk:

- Serious impact on reputation or finances of multiple national host sites or affiliates
- Serious impact on operations of multiple national host sites or affiliates
- Financial loss (regulatory fines or damages from litigation)
- Loss of competitiveness of key strategic research area
- Identity theft severely impacting individuals

5. Directive

5.1 Data Handling Standard:

The National Security Council must publish and maintain a data handling standard that specifies treatment and control requirements for each of the data classifications listed in this Policy.

6. Related Information

SEC-00 Information Security Glossary
SEC-03 Data Handling Standard
SEC-05 Cybersecurity Risk Management Policy