Sharing allow:
TLP - GREEN

Approved

Cybersecurity Policy

Document ID: **SEC-01**
For: Alliance Federation
Approval Date: 2024-10-01
Approved By: CSAC

1. Introduction

Cybersecurity is one of the fundamental elements of the effective delivery of services by the Alliance Federation. This policy and its associated standards, procedures, specifications and other supporting documents outline the Alliance Federation cybersecurity framework.

2. Definitions

Refer to *SEC-00 Information Security Glossary* for definitions used in this Standard.

3. Applicability

This Policy applies to all Alliance Federation Systems and Services, associated data and all persons authorized to access these. Some services incorporate a shared responsibility model, as defined in their associated terms of service which may assign additional responsibilities to Users.

4.0 Cybersecurity Requirements

4.1. Protection of Information Systems

4.1.1. All ***Alliance Federation Systems and Services*** and associated data must be protected in a manner that is considered reasonable and appropriate to the data classification and criticality and throughout their life cycle.

4.1.2. The Alliance Federation must implement appropriate controls to preserve the confidentiality, integrity, and availability of data stored and processed within **Alliance Federation Systems and Services** in accordance with the AFCF.

4.1.3. Access to **Alliance Federation Systems and Services** and associated data must be authorized and restricted based on the principle of Least Privilege.

4.1.4. Any suspected or confirmed security incident affecting ***Alliance Federation Systems and Services*** must immediately be reported to security@tech.alliancecan.ca.

4.2. Training and Awareness

All ***Alliance DRI Professionals*** (ADP) must complete the Privacy and Security training and awareness program(s) applicable to their role as defined in the AFCF.

4.3. Monitoring

All use of ***Alliance Federation Systems and Services*** must be monitored in an auditable way in accordance with the AFCF.

4.4. Service Agreement

The Alliance Federation must document the cybersecurity requirements of the AFCF within a service agreement for all services and infrastructure it offers (examples include Terms of Use, SLA, MoU, Contribution Agreement, etc.). At a minimum, the service agreement must include details and roles (RACI) for:

- Incident response
- Access to information
- Backup
- Maintenance
- Data ownership
- Data lifecycling
- Logging and monitoring

4.5. Request for Variance

In the event it is impossible to comply with any aspect of the AFCF, a request for variance can be made in writing to security@tech.alliancecan.ca. Any variance must be approved by the VP Operations and Security, at their discretion and in consultation with the Cybersecurity Advisory Council (CSAC) as required.

4.6. Roles and Responsibilities

Cybersecurity is a responsibility that falls on everyone: Users, ADPs, and management alike. Everyone must take the necessary steps to protect **Alliance Federation Systems and Services** from potential cyber threats. This includes complying with all Alliance Federation policies, standards, procedures, and specifications, being aware of risks, implementing strong security measures, and staying vigilant against possible attacks. By working together, we can create a safer and more secure digital research environment for everyone.

4.7. Governance and Documentation

The Alliance VP Operations and Security is accountable for ensuring that an appropriate cybersecurity program including a policy and governance framework is established, maintained, and published for the Alliance Federation. The Alliance VP Operations and Security must direct the National Security Council (NSC) to establish a working group that is responsible for reviewing and maintaining this policy and governance framework. This includes but is not limited to:

- The cybersecurity program and strategy;
- Creation, maintenance, and periodic review of the AFCF including:
  - policies, standards, procedures, and specifications;
- Creation and maintenance of supporting documents, e.g., guidelines, checklists.

4.8. Implementation

Effective implementation of the cybersecurity program involves many different parties. The Alliance VP Operations and Security is accountable for the overall implementation. Different parts of the program's implementation are the responsibility of different groups (see RACI chart section 4.12).

Implementation elements include:

- Investment and resources
- AFCF project management
- Training and awareness for the AFCF
- Risk management
- Incident management
- Security operations (threat intelligence, vulnerability management, etc.)
- Variance and escalation

- Continuous improvement

4.9. Compliance and Audit

The Operations Management Committee (OMC) is accountable to ensure compliance audits of the AFCF and audits of the Alliance Federation are conducted or commissioned. The OMC must work together with the Operations Steering and Advisory Council (OSAC), Security Operations, and the NSC to collect the necessary information, document findings, and communicate resulting priorities for improvement. These tasks include but are not limited to:

- Operational audit(s) and monitoring (internal)
- External audit(s)

4.10. Reporting and Metrics

Appropriate reporting of cybersecurity metrics is required to gauge the effectiveness of the cybersecurity program by oversight agencies. The Alliance VP Operations and Security is accountable for ensuring accurate data is collected and reported. The NSC and Security Operations are the primary groups responsible for the collection of this information, which include:

- Collection and identification of metrics
- Operational Reporting for continuous improvement of AFCF
- Reports to Innovation, Science and Economic Development Canada (ISED)
- Reports to Partner Organizations

4.11. RACI Matrix for Cybersecurity Activities

	Governance and Documentation	Implementation	Compliance and Audit	Reporting and Metrics
Alliance VP Operations and Security	A	A	C	A
OMC	C	C	A	I

CSAC	C	C	I	I
OSAC	C	C	R	I
NSC	R	R	R	R
SecOps	C	R	R	R
TLC	C	R	I	I
ADPs	C	R	-	-
Users	I	R	-	-

5. Related Information

SEC-00 Cybersecurity Glossary
SECSD-00 Governance Document Registry