Backup Standard

Document ID: **SEC-12**
For: Alliance Federation
Approval Date: 2024-05-01
Approved By: NSC

1. Introduction

This standard describes the backup requirements for the Alliance Federation Systems and Services. Implementation of these requirements will promote a consistent level of backup across the Alliance Federation to support and promote a resilient environment. They also make it clear to all Users when a backup is in place and when it is not.

2. Definitions

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

3. Applicability

This standard applies to the data centres hosting Alliance Federation Systems and Services.

4.0 Systems and Services Requiring Backup

4.1. The following Alliance Federation Systems and Services must have a backup:

4.1.1. CCDB Portal;

4.1.2. TECC wiki;

4.1.3. Data elements required to rebuild infrastructure where restoration without a backup would take excessive time or may be impossible to accurately reproduce. Including configurations and source code (e.g., firewall rules, network routes and subnets, IP assignments, DNS, LDAP, source code repositories, etc.).

4.2. The following should have a backup:

4.2.1. Logs contained in central logging systems.

4.3. In all cases, service owners are responsible for taking a risk-based approach to assess if a backup is required and appropriate for the system or service they own. Include the nature of the backup (e.g., on-site vs. off-site, backup media, restore time, backup type, and frequency) when conducting this assessment.

4.4. All user-facing Alliance Federation Systems and Services must clearly publish if there is a backup in place or not and the nature of the backup. All other services should also document if a backup is in place or not and the nature of the backup.

4.5. In all cases where a backup is documented as being in place, it must conform to the requirements of this standard.

5.0 Requirements for Backups

5.1. Backups must be validated to include:

5.1.1. Documented procedures for validating backup data integrity;

5.1.2. Regular data integrity checks, data reconciliation, and monitoring;

5.1.3. Regular restoration testing, sufficient to provide confidence that a restoration of the backup would succeed. This should be conducted at a minimum of 2 times per year;

5.1.4. Backup processes should include alerts that are monitored, in the event of failure.

5.2. At all stages of the data lifecycle, during backup and restoration, data must be classified according to *SEC-02 Data Classification Policy*, and handled in accordance with *SEC-03 Data Handling Standard* based on the highest- risk data included in the backup.

5.3. Logging must be sufficient to document the integrity of the backup, times and nature of backup and restore operations.

5.4. The data included in the backup must be documented, including when data will automatically expire from the backup. A process must be documented to address requests for this information.

5.5. A retention schedule must be established that defines if and when backup data will be deleted.

5.6. An access and restoration process must be documented that defines the following:

5.6.1. Who may approve of access to and/or restoration of a backup;

5.6.2. Conditions for restoration of backup data (including granularity as well as who may request restoration).

6. Related Information

SEC-00 Cybersecurity Glossary
SEC-02 Data Classification Policy
SEC-03 Data Handling Standard