Cybersecurity Requirements for RPs v1

Integration Roadmap Task

### Task Type(s): Technology Start by phase: Integration Complete by phase: Operations RP role(s): Cybersecurity and incident response contact(s)

# Summary

The cybersecurity requirements for RPs ensures that the ACCESS community’s cybersecurity needs are satisfied when a new service is added to the system. For instance: membership and participation in incident response, vulnerability patching and mitigation, retention of system logs, etc. Requirements are driven by ACCESS community policies.

The purpose of this document is to define the expectations and responsibilities of the ACCESS Resource Providers with respect to security and incident response. These requirements ensure the ability to (i) protect ACCESS assets, (ii) respond to threats to those assets, and (iii) maintain the lines of communication necessary for the former two goals.

## Effort

It is difficult to estimate the time and effort required because each RPs cybersecurity program and implementations are different. However, many of these are considered best practices or baseline controls and RPs are likely to be implementing most of these already. Nonetheless, resources must be devoted to ensure that the standards are properly implemented and processes developed to ensure they are maintained.

# Prerequisite tasks

None

# Support Information

For assistance with this task see the *Support Information* section in the *Integration Roadmap Description*.

# Detailed Instructions

## Description

Requirements for this review are driven by ACCESS community policies, listed below.

1. [**ACCESS Core Information Security Policy and Procedures**](https://docs.google.com/document/d/1h8w1E9Z2yrXAoBGtCVGH6MxF3rRBKz0uQOBUJ58Jt6M/edit)
2. [ACCESS Vulnerability Management Policy](https://docs.google.com/document/d/1ehpsijz97ag_WGwT8fb0E3KC3tDNXruWAytuvB3TFMY/edit)
3. ACCESS Training and Awareness Policy
4. ACCESS Identity and Access Management Policy
5. ACCESS Information Classification Policy
6. ACCESS Disaster Recovery Policy
7. [ACCESS Privacy Policy](https://docs.google.com/document/d/1jo-Sl5P9m0Xwyd6d1Ntqf4Wtefw5nlYBBgrst9SfAXM/edit)
8. [ACCESS Incident Response Policy](https://docs.google.com/document/d/1PMlZx40W0XF5NHlBkuPv1JAW7Fc2Fm__1JvIBZUaEQw)
9. [ACCESS Acceptable Use Policy](https://docs.google.com/document/d/1LiWUmN3YRTPOd1u3CODRdeK87VLV_md4nEj-Ehqinls)
10. [ACCESS Security Standards](https://docs.google.com/document/d/1NX95bkuvsdXo1fvGvyTzwGJ7Lx3BeC51luue-ddtkPE/edit)

## Responsibilities

1. Beyond just reporting security incidents, the RPs incident response point of contact is expected to actively participate in investigations as appropriate. This requires the RP to keep appropriate logs for ACCESS relevant systems.
2. Be able to determine if resources are affected by a particular vulnerability, and work with their staff to patch or mitigate.
3. Protect sensitive information (phone contacts, PGP keys, wiki accounts, etc) as it relates to ACCESS and the AIRTG
4. Make any local security and privacy policies available and easy to find for ACCESS users who may be running jobs on their systems. For example Acceptable Use, Incident Response, etc.

# Document Management

| Status | Draft |
| --- | --- |
| Official date | <mm/dd/yyyy> |
| Retired date |  |
| Coordinators | Alex Withers, CONECT Cybersecurity Program  Shane Filus, CONECT Cybersecurity Program |
| Last revised date | 02/16/2023 |