

[PDK08]

# Security Incident Response Procedure

## Context

A common incident response procedure ensures all Service Providers act consistently in the resolution and reporting of security incidents.

Incident responses should be informed first by internal (local) governance frameworks, policies and procedures. Where those incidents affect the Collaboration, Collaboration Policies should take precedence to secure its assets.

Some Service Providers may be part of 'interfederations'. In such circumstances, the Service Provider (usually an IdP) may have security incident response obligations to the inter federation.

## Questions to consider when establishing the Collaboration or onboarding a new Service Provider:

- Where will you store the security contact details of the Collaboration and its Service Providers? How will this information be maintained (currency and accuracy)?
- Will the Collaboration require a dedicated Security Incident Response (CSIRT) team? If not, how will you source investigative and forensics skills appropriately at short notice during incidents?
- Can your Collaboration establish (secure) communication between its Service Providers, Collaboration Management and the Community?
- Does your Collaboration need to set up a secure data store for evidence gathered during Incident Response?
- Do you have established practices to announce suspension of services? Will the Collaboration require a Communications Plan?

*\*delete this box after completing the policy.*

## 1 Introduction and Purpose

### 1.1 Objectives

This Procedure establishes a consistent, scalable security incident response to ensure effective cooperation and action across the Collaboration to manage a security event. These procedures are informed by and aim to facilitate a response compliant with the Sirtfi Framework.<sup>1</sup>

<sup>1</sup> The *Security Incident Response Trust Framework for Federated Identity* (v2.0). Refer to [refeds.org/sirtfi](https://refeds.org/sirtfi). Sirtfi v2.0 compliance includes but is not limited to compliance with v1.0.

## 1.2 Scope

This Procedure applies for any suspected or confirmed security breach with a potential impact on the Collaboration, or its Service Providers, Communities and Users.

## 1.3 Definitions

**Interfederations:** Services that connect national and international Collaborations where Users authenticated by one Service in the Collaboration may access Services in a different Collaboration, such as eduGAIN (EU) or InCommon (USA).

**Security Contact:** A nominated individual or group responsible for the operational security within the Collaboration. This includes the Collaboration Security Contact and nominated Security Contacts within, or operating on behalf of, a Service Provider.

**Security Incident Response Coordinator:** The Security Incident Response Coordinator is a group or individual nominated by the Collaboration Security Contact to coordinate the resolution of security incidents, usually within Service Providers.

**Traffic Light Protocol (TLP):** A Traffic Light Protocol is a non-legally binding classification scheme that defines protocols for the sharing of potentially sensitive information, including restrictions on access and use.

# 2 Security Incident Response Procedure for Service Providers

Service Providers:

1. Must contain the security incident in accordance with local processes, legislation and Collaboration Policies to avoid further propagation whilst aiming to carefully preserve evidence and logs. Record all actions taken, including accurate timestamps.
2. Report the security incident to the Collaboration Security Contact within one local working day of the initial discovery or notification of the security incident.
3. In collaboration with the Security Incident Response Coordinator (identified by the Collaboration Security Contact):
  - a. Collect and strive to identify indicators of compromise (IoCs)
  - b. Share incident status reports and IoCs with all affected participants (a “heads-up” and subsequent updates as needed), in the Collaboration via the Security Contact (and, if needed, in other federations and with any external trusted entity involved)
4. Announce suspension of Service(s) (if applicable) in accordance with Collaboration practices (and interfederation practices, as required). Public announcements should not contain details other than “Security operations in progress,” unless agreed otherwise with the Collaboration Security Contact.

5. Perform appropriate investigation, system and network analysis and adequate forensics, and strive to understand the exact cause of the security incident, as well as its full extent. Identifying the cause of security incidents is essential to prevent them from reoccurring. Time and effort must be commensurate with the scale of the problem and the potential damage and risks faced by the Collaboration.
6. Share additional status updates and IoCs as often as necessary to keep all affected Service Providers up to date with the security incident and enable them to investigate and act should new information appear.
7. Respond to requests for assistance from other Service Providers involved in the security incident within one working day and investigate new IoCs being shared.
8. Take corrective action or restore access to Services for legitimate Collaboration Users.
9. The Security Incident Response Coordinator and the Security Contact will produce and share a report of the incident with all Collaboration Service Providers and all other affected Sirtfi-compliant Collaborations and interfederations within one month. This report should be labelled Traffic Light Protocol (TLP) AMBER or higher.
10. Update documentation and procedures as necessary.

### 3 Security Incident Response Procedure for the Collaboration Security Contact

The Collaboration Security Contact will:

1. Assist Collaboration Service Providers in performing appropriate investigation, system and network analysis and forensics, and strive to understand the cause of the security incident, as well as its full extent. Time and effort must be commensurate with the scale of the problem and with the potential damage and risks faced by the Collaboration, and affected Service Providers, Communities and Users.
2. Report the security incident to the Collaboration's nominated Security Contacts within one local working day of the initial discovery or notification of the security incident.
3. Coordinate the security incident resolution process and communication as it relates to the Collaboration with affected Service Providers until the security incident is resolved:
  - a. Collect and strive to identify indicators of compromise (IoCs) from all involved entities
  - b. Share incident status reports and IoCs with all affected Service Providers (a "heads-up" and subsequent updates as needed), in the Collaboration via nominated Security Contacts (and, if needed, in other Collaborations and with any external trusted entity involved). If other Collaborations or interfederations are affected the appropriate Security Contacts must be notified, even if affected participants in all other Collaborations have been contacted directly.
4. Ensure suspension of service (if applicable) is announced in accordance with Collaboration and interfederation practices (where applicable).

AAF NRI Policy Development Kit – Security Incident Response Procedure [PDK08]

© Owned by the authors and made available under license: <https://creativecommons.org/licenses/by-nc-sa/4.0/>

Other Sources / Attribution / Acknowledgements: The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2). Adapted by the Trust and Identity Pathfinder Policy Working Group coordinated by the AAF, comprised of members from Australian national research infrastructure, and enabled by funding through the Australian Government's National Collaborative Research Infrastructure Strategy (NCRIS).

*This document is provided as guidance only. Each organisation or Collaboration must consider its own unique context, legislative obligations, and trust and identity requirements to complete and implement the Trust and Identity Policy Development Kit. AAF and other national research infrastructure members of the Policy Working Group, are not liable for any loss or damage, from any implementation or action taken to implement this Policy.*

5. Share additional status updates and IoCs as often as necessary to keep all affected Service Providers up to date with the security incident and enable them to investigate and act should new information appear.
6. Assist and advise Service Providers in taking corrective action or restoring access to Services for legitimate Collaboration Users.
7. Produce and share a report of the incident with all Sirtfi-compliant organisations in all affected Collaborations and interfederations within one month, in accordance with clause 2.9 of this Procedure. This report should be labelled TLP AMBER or higher.
8. Update documentation and procedures as necessary.

## 4 Associated Documents

### 4.1 Collaboration Policies

- Top-Level Collaboration Policy [PDK01]
- Membership Management Policy [PDK06]
- Service Operations Security Agreement [PDK07]

## Version Control

Document Control			
Document Approved:		Date Effective:	
Last Review Date:		Next Review Date:	
Version Control			
Version	Author	Summary of Changes	Date
1.5	AAF	Review and alignment of language. Refinement of document context. Refinement of context statements. Corrected attributions. Updated disclaimer.	March 2025