DRAFT

eduGAIN Security Incident Response Handbook

Chapter 1. Understanding Your Role and Responsibilities

Introduction

This document defines the roles and responsibilities of each party taking part in the Security Incident Response process that is when a Federation Participant suspects a security incident affects its resources and has reason to believe that Federation Participants outside its origin federation may be affected.

A **Security incident** is a suspected or confirmed violation of an explicit or implied security policy.

This document is aimed at minimising the impact of security incidents in the eduGAIN federated environment, by Federation Participants, Federation Operators and the eduGAIN Security Team. The objective is to ensure that all security incidents are investigated as fully as possible and that Federation Participants promptly report any incident that poses a risk to other Federation

Participants. Security incidents are to be treated as serious matters and their investigation resourced appropriately.

This document is based on the previous work conducted in the AARC2 project[1].

Roles

Federation Operators are the entities operating the federations that are members of eduGAIN, as listed in https://technical.edugain.org/status.

Federation Participants operate the entities that belong to or are accessible via any eduGAIN member federation, including Service Providers, Identity Providers, Attribute Authorities, Research Community AAIs, identity and service provider Proxies, or e-Infrastructures. Federation Participants that are directly published in eduGAIN are listed in https://technical.edugain.org/entities/ (note that this list does not necessarily include entities behind Proxies).

The **eduGAIN Security Team[2]** manages incident response at the inter-federation level providing a unique point of security coordination.

Scope

This document focuses on security incidents that affect Federation Participants within or outside the federation where the suspected security incident occurred.

In particular, this document defines the role of the eduGAIN Security Team as a central coordinator when multiple administrative domains (within one or spanning multiple federations) are suspected to be affected by an ongoing incident.

Nothing in these procedures is meant to restrict the flow of information among Federation Participants, Federation Operators, and external parties. Likewise, nothing in these procedures is meant to supersede established Federation Participant or Federation Operator incident response policies or procedures. They are, however, intended to augment local procedures when an incident may extend beyond the local domain.

Federation Participants that support the Sirtfi framework[3] will be fully included in Incident Response. Federation Participants that do not support Sirtfi may only receive limited information and support.

[1] https://aarc-project.eu/wp-content/uploads/2017/02/DNA3.2-Security-Incident-Response-Procedure-v1.0.pdf
[2] https://edugain.org/edugain-security/
[3] https://refeds.org/sirtfi

Responsibilities

Federation Participants, Federation Operators, and the eduGAIN Security Team each ensure that the security incident resolution process does not stall within their respective domains of operation. They are mutually responsible for understanding and resolving the ongoing security incident by ensuring it is contained, coordinating the response with the various affected parties, tracking progress of the incident response process, disseminating information, and providing expertise and guidance.

Federation Operators and the eduGAIN Security Team are expected to marshal concerned Federation Participants and Federation Operators to participate in the response to a security incident.

Federation Participants

Federation Participants are expected to follow the Security Incident Response Procedures for Federation Participants (in Chapter 2 below), including:

- Report on all suspected ongoing security incidents posing a risk to any Federation Participants within or outside their own federation to their Federation Operator.
- Investigate and coordinate the resolution of suspected security incidents within their domain of operation and keep the Federation Operator and other involved parties updated appropriately.

Depending on their expertise and available effort, Federation Participants can also choose to actively take a leading role in the investigation and in the coordination of the response to the security incident on a global scale.

For Federation Participants supporting the Sirtfi framework, it is expected that the Sirtfi security contact is the means to engage their incident response team.

Federation Operators

Federation Operators are expected to follow the Security Incident Response Procedures for Federation Operators (in Chapter 2 below), including:

- Act as a contact and support point for security incidents reported by their Federation Participants.
- Report on all suspected security incidents potentially affecting multiple parties, whether inside one federation or spanning multiple federations, to the eduGAIN Security Team.
- Coordinate the resolution and investigate suspected security incidents within their domain of operation and keep the eduGAIN Security Team, Federation Participants and other involved parties updated appropriately.

This role is expected to be fulfilled by the security contact point as expressed in their federation profile published in the eduGAIN Member Database. If security contact information is not available then the federation general contacts are used.

In order to fulfil this role adequately, Federation Operators may be supported by Federation Participants, external parties, Research Communities, or e-Infrastructure security teams, as appropriate.

eduGAIN Security Team

The eduGAIN Security Team is expected to follow the Security Incident Response Procedures for the eduGAIN Security Team (in Chapter 2 below), including:

- Act as a central contact and support point for security incidents reported by Federation Operators
- Notify potentially affected parties outside a given federation to their respective Federation Operators
- Coordinate the resolution of and investigate suspected security incidents with affected Federation Operators and Federation Participants

Chapter 2. Security Incident Response Procedures

The procedures below use the Traffic Light Protocol[4] (TLP) to mark information being shared according to its sensitivity and the audience with whom it may be shared.

If a suspected security incident is discovered to be a false positive, the procedure may be stopped after appropriate notification of the involved parties.

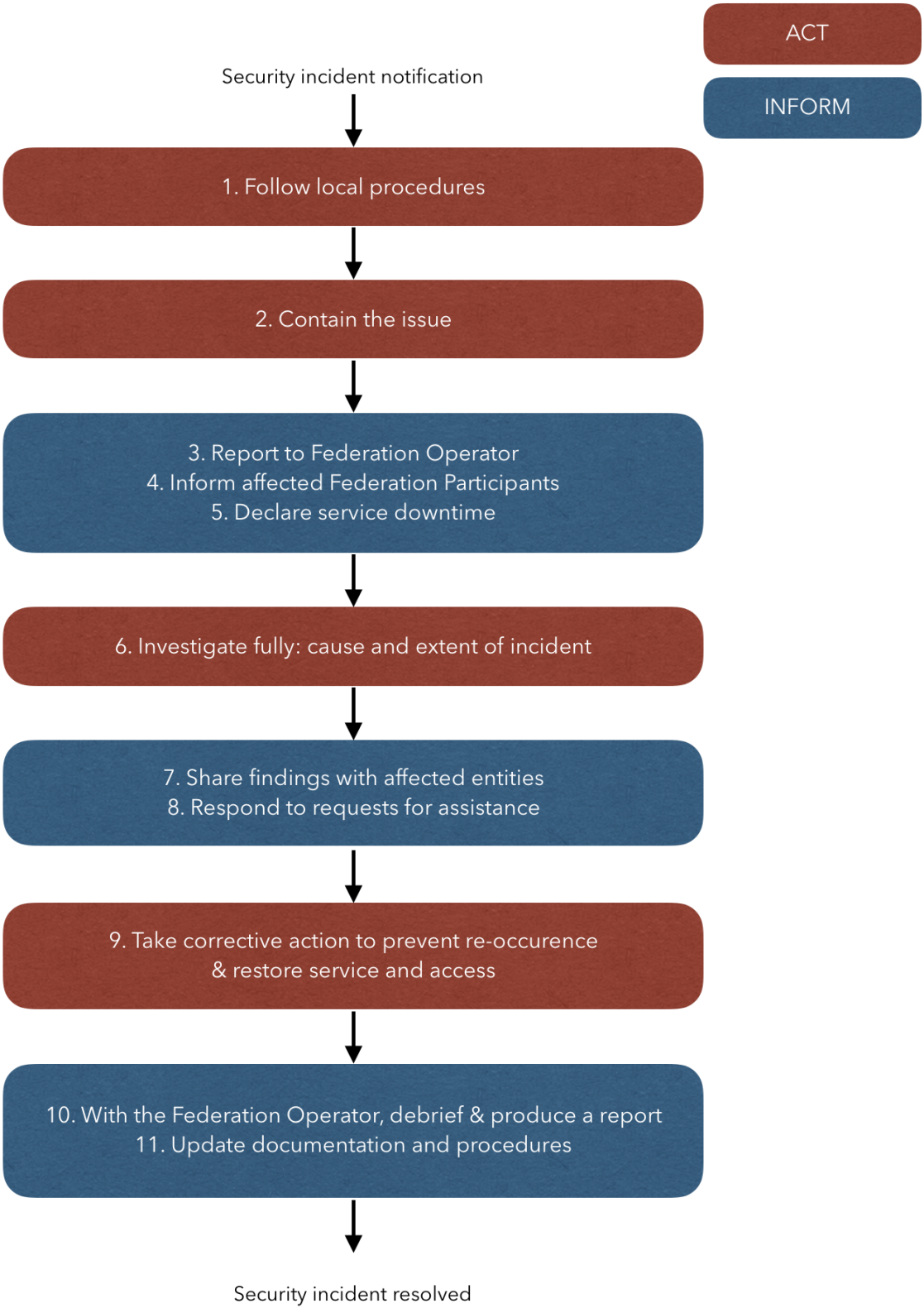
All actions detailed below are understood to be on a best-effort basis and that some parties at some times may not be able to do all that is specified by the procedure.

In the event of conflict between this procedure and other applicable policies or procedures for your organisation, local policies and procedures take precedence. If for any reason this procedure cannot be followed, the security contact of the Federation Operator immediately superior to your organisation must be notified, or the eduGAIN Security Team, if you are a Federation Operator.

Federation Participants

[4] https://www.first.org/tlp/

1. Follow all security incident response procedures established for your organisation and your federation.
2. Initial incident response:
    a. Contain the security incident to avoid further propagation, including to other entities, while aiming at carefully preserving evidence and logs. Record all actions taken, along with an accurate timestamp.
    b. Report on all suspected ongoing security incidents posing a risk to any Federation Participants within or outside your own federation to your Federation Operator as soon as possible, but within one local working day of becoming aware of the suspected incident.
3. In collaboration with your Federation Operator, ensure that all affected Federation Participants are notified, including those belonging to other federations. Include relevant information, when possible, to allow them to take action.
4. Investigate and coordinate the resolution of suspected security incidents within your domain of operation and keep the Federation Operator and other involved parties updated appropriately.
5. Announce suspension of service (if applicable) to your Federation Operator, in accordance with federation practices.
6. Perform appropriate investigation, system analysis and forensics, and strive to understand the cause of the security incident, as well as its full extent. Identifying the cause of security incidents is essential to prevent them from reoccurring. The time and effort needs to be commensurate with the scale of the problem and with the potential damage and risks faced by affected Federation Participants.
7. Share additional information as often as necessary to keep all affected parties up-to-date with the status of the security incident and enable them to investigate and take action should new information appear.
8. Respond to requests for assistance from others involved in the security incident within one working day (in case of limited trust or doubt regarding the party behind a given request, please involve your Federation Operator and eduGAIN Security Team).
9. Take corrective action, restore access to service (if applicable) and legitimate user access.
10. In collaboration with your Federation Operator, produce and share a report of the incident with all Sirtfi-compliant organisations in all affected federations within one month. This report should be labelled TLP AMBER or higher.
11. Update your own organisation’s documentation and procedures as necessary.


ACT
INFORM
Security incident notification
1. Follow local procedures
2. Contain the issue
3. Report to Federation Operator
4. Inform affected Federation Participants
5. Declare service downtime
6. Investigate fully: cause and extent of incident
7. Share findings with affected entities
8. Respond to requests for assistance
9. Take corrective action to prevent re-occurence
& restore service and access
10. With the Federation Operator, debrief & produce a report
11. Update documentation and procedures
Security incident resolved

Federation Operators

1. Follow all security incident response procedures established for your federation and for eduGAIN.
2. Report all suspected security incidents potentially affecting multiple parties, whether inside one federation or spanning multiple federations to the eduGAIN Security Team, as soon as possible, but within one local working day of becoming aware of the suspected incident.
3. Assist Federation Participants in performing appropriate investigation, system analysis and forensics, and strive to understand the cause of the security incident, as well as its full extent. The time and effort needs to be commensurate with the scale of the problem and with the potential damage and risks faced by affected Federation Participants.
4. In collaboration with the eduGAIN Security Team, ensure that all affected Federation Operators and Federation Participants are notified. In addition, if any other federations are affected, ensure the eduGAIN Security Team is notified, even if the affected Federation Operators have been contacted directly.
5. Investigate and coordinate the resolution of suspected security incidents within your domain of operation and keep the eduGAIN Security Team, Federation Participants and other involved parties updated appropriately.
6. Share additional information as often as necessary to keep all affected parties up-to-date with the status of the security incident and enable them to investigate and take action should new information appear.
7. Assist and advise Federation Participants in taking corrective action, or restoring access to services (if applicable) and legitimate user access.
8. In collaboration with Federation Participants and the eduGAIN Security Team, produce and share a report of the incident with all Sirtfi-compliant organisations in all affected federations within one month. This report should be labelled TLP AMBER or higher.
9. Update your own federation documentation and procedures as necessary.

The eduGAIN Security Team may be contacted and involved at any time for security advice, recommendations, technical support, and expertise, regardless of the severity of the suspected incident, at the discretion of and based on the needs of the Federation Operator.

eduGAIN Security Team

- Act as a central contact and support point for security incidents reported by Federation Operators or Federation Participants.
- Assist Federation Operators and Federation Participants to identify the cause of security incidents, which may include performing appropriate investigation, system analysis and forensics, and strive to understand the cause of the security incident, as well as its full extent. Identifying the cause of security incidents is essential to prevent them from reoccurring.

- In collaboration with their respective Federation Operators, ensure all affected Federation Participants are notified via their security contact within one local working day.
- Coordinate the resolution of and investigate suspected security incidents with affected Federation Operators and Federation Participants.
- Coordinate the communication with third-parties outside of eduGAIN, if relevant.
- Share additional information as often as necessary to keep all affected parties up-to-date with the status of the security incident and enable them to investigate and take action should new information appear.
- Assist and advise Federation Participants and Federation Operators in taking corrective action, or restoring access to service (if applicable) and legitimate user access.
- Produce and share a report of the incident with all Sirtfi-compliant organisations in all affected federations within one month. This report should be labelled TLP AMBER or higher. Also produce and publish a TLP WHITE version of the report.
- Update documentation and procedures as necessary.