07 December 2022

eduGAIN Policy Framework

eduGAIN CSIRT RFC2350

Document Revision History

Version	Date	Description of Change	Person
1.0	07-12-2022	Proposal for approval by eduGAIN Steering Group	S Gabriel

eduGAIN Policy Framework

eduGAIN-CSIRT RFC2350

Contents

1 DESCRIPTION FOR EDUGAIN CSIRT 4

1.1 About this document 4

1.2 Distribution List for Notifications 4

1.3 Locations where this Document May Be Found 4

1.4 Authenticating this Document 4

2 CONTACT INFORMATION 4

2.1 Name of the Team 4

2.2 Address 4

2.3 Time Zone 5

2.4 Telephone Number 5

2.5 Facsimile Number 5

2.6 Other Telecommunication/Instant messaging 5

2.7 Electronic Mail Address 5

2.8 Public Keys and Other Encryption Information 5

2.9 Team Members 5

2.10 Other Information 6

3 CHARTER 6

3.1 Mission Statement 6

3.2 Constituency 6

3.3 Sponsorship and/or Affiliation 6

3.4 Authority 6

4 POLICIES 7

4.1 Types of Incidents and Level of Support 7

4.2 Co-operation, Interaction and Disclosure of Information 7

4.3 Communication and Authentication 7

5 SERVICES 7

5.1 Incident Response 7

5.2 Incident Triage 8

5.3 Incident Response Coordination 8

5.4 Incident Resolution 8

5.5 Proactive Activities 8

6 INCIDENT REPORTING FORMS 8

7 DISCLAIMERS 9

8 REFERENCES 9

1 Description for eduGAIN-CSIRT

1.1 About this document

This is version 1.0, 7th December 2022.

1.2 Distribution List for Notifications

Notifications of updates are submitted to the eduGAIN Steering Group mailing list edugain-sg@lists.geant.org. The eduGAIN Steering Group mailing list is composed of all the delegates and deputies of the eduGAIN participants, the subscription is managed by the eduGAIN Service. The mailing list is not moderated.

1.3 Locations where this Document May Be Found

The current version of this CSIRT description document is available from the eduGAIN-CSIRT website, https://edugain.org/edugain-security/.

Please make sure you are using the latest version.

1.4 Authenticating this Document

This document has been signed with the eduGAIN-CSIRTs PGP key. The signatures are also on our Web site, under: https://edugain.org/edugain-security/.

2 Contact Information

2.1 Name of the Team

eduGAIN-CSIRT: The eduGAIN Computer Security Incident Response Team.

2.2 Address

GEANT C/O eduGAIN-CSIRT
Hoekenrode 3
6th floor
1102 BR Amsterdam
The Netherlands

2.3 Time Zone

Europe/Amsterdam (GMT+0100, and GMT+0200 from April to October).

2.4 Telephone Number

+44 1223 733033.

2.5 Facsimile Number

Not available.

2.6 Other Telecommunication/Instant messaging

Not available.

2.7 Electronic Mail Address

abuse@edugain.org This address can be used to report all security incidents which relate to the eduGAIN participants. This is a mail alias that relays mail to the human(s) on duty for the eduGAIN-CSIRT.

2.8 Public Keys and Other Encryption Information

The eduGAIN CSIRT has a PGP key, whose fingerprint is:

0497 8576 D7A6 3151 5401 DB98 697A 900B 7C8E 095E

The key and its signatures can be found at the usual large public keyservers.

2.9 Team Members

The eduGAIN-CSIRT team is coordinated by the eduGAIN-CSIRT security officer and it is composed by security experts from the constituent participants and the Research and Education community. The current team composition is available on the eduGAIN website: https://edugain.org/edugain-security/.

eduGAIN-CSIRT will use the information you provide to help solve security incidents affecting eduGAIN. This means that by default the information will be distributed further to the appropriate parties – but only on a need-to-know base, and preferably anonymized.

2.10 Other Information

General information about eduGAIN security is in https://edugain.org/edugain-security/.

The eduGAIN-CSIRTs hours of operation are Monday - Friday 09:00-17:00 (CET/CEST), except public holidays. Outside business hours, eduGAIN CSIRT provides support on a best effort basis.

3 Charter

3.1 Mission Statement

The eduGAIN-CSIRT provides a central contact and support point for security incidents at the inter-federation level. It will work in close collaboration with Federation Security Contacts and Federation Operators to coordinate the investigation and resolution of suspected security incidents at the inter-federation level.

3.2 Constituency

eduGAIN consists of Federations whose primarily goal is to provide authentication and authorisation services to the research and education community. The eduGAIN Service provides an infrastructure for establishing trusted communications between Entities, such as Identity and Service Providers, belonging to different Federations.

Please refer to the [eduGAIN Constitution] for further details.

For an up-to-date list of the current eduGAIN Participants you can refer to: https://technical.edugain.org/status.

3.3 Sponsorship and/or Affiliation

eduGAIN-CSIRT team members affiliated to a GÉANT members will be funded by the GÉANT project. Other members will be funded by their respective organisations.

3.4 Authority

eduGAIN-CSIRT operates with authority delegated by the eduGAIN Steering Group to coordinate incident response at the inter-federation level and provide the services described in section 5 of this document.

4 Policies

The eduGAIN policy framework is available on the eduGAIN Technical site at the following URL: https://technical.edugain.org/documents.

4.1 Types of Incidents and Level of Support

All security incidents that may have an impact at the inter-federation level are managed by eduGAIN-CSIRT.

eduGAIN-CSIRT aims to respond to requests within 4 office hours.

4.2 Co-operation, Interaction and Disclosure of Information

The eduGAIN-CSIRT closely collaborates with the Federation Security Contacts, Federation Operators, entities Security Contacts and the National Research and Education Network CSIRTs and CERTs to ensure that all the parties affected by a security incident at the inter-federation level are timely alerted and supported in the investigation, limitation and remediation process.

The roles and interactions of the different entities relevant to incident response within eduGAIN are described in the eduGAIN Security Incident Response Handbook [eduGAIN-SIRH].

eduGAIN-CSIRT reports to the eduGAIN Steering Group (eSG).

4.3 Communication and Authentication

ALL incoming information is handled confidentially by eduGAIN-CSIRT, regardless of its priority.

eduGAIN-CSIRT supports the Traffic Light Protocol [FIRST TLP] - information that comes in with the tags CLEAR, GREEN, AMBER, AMBER+STRICT or RED will be handled appropriately.

Untagged information will be treated as TLP-GREEN (see above). eduGAIN-CSIRT will use the information you provide to help solve security incidents affecting eduGAIN. This means that by default the information will be distributed further to the appropriate parties – within the limits of the set TLP Tag, but only on a need-to-know base, and preferably anonymised.

5 Services

5.1 Incident Response

eduGAIN-CSIRT's major IT security incident management function is incident coordination across eduGAIN Federations.

5.2 Incident Triage

eduGAIN-CSIRT will support the eduGAIN participants investigating whether indeed an incident occurred and in case, determining the extent of the incident. This ranges from a single entity registered in one or more federations, to multiple entities from different federations affected.

5.3 Incident Response Coordination

eduGAIN-CSIRT will organise the security incident communications across affected participants and coordinate the response activities to allow for an efficient containment and subsequently resolution of security incidents.

5.4 Incident Resolution

The incident resolution is ultimately the task of the organizations responsible for the affected entities. If possible and on request, eduGAIN CSIRT will support the entities in coordination with the federations.

5.5 Proactive Activities

The eduGAIN-CSIRT will maintain the security communication channels with all the eduGAIN participants. In order to do that, from time to time, the eduGAIN CSIRT will organize communication challenges to assess the reliability and responsiveness of the communication infrastructure.

The eduGAIN-CSIRT will occasionally share information about prominent security threats and vulnerabilities that may affect the eduGAIN community.

6 Incident Reporting Forms

The following form will be used to notify a suspected or verified security incident to any affected party. All the incident reports will be signed by the eduGAIN-CSIRT with its PGP key.

```
Subject: [TLP:COLOR] subject

TLP:COLOR

## SUMMARY ##
Summary of the report.

## INTRUSION TIMELINE ##
YYYY-MM-DD HH:MM:SS event 1
..
YYYY-MM-DD HH:MM:SS event N
```

```
## INDICATORS OF COMPROMISE
Available IoCs.

## REPORTING & SHARING
Where to report back about new findings on the incident.
```

The above form is based on the AARC Deliverable DNA3.2 - Security Incident Response Procedure [AARC-DNA3.2].

7 Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, eduGAIN-CSIRT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.

8 References

[eduGAIN Constitution] https://technical.edugain.org/doc/eduGAIN-Constitution-v3ter-web.pdf
[FIRST TLP] https://www.first.org/tlp.

[eduGAIN-SIRH] https://wiki.geant.org/download/attachments/218464365/eduGAIN%20Security%20Incident%20Response%20Handbook-v1-eSG-feedback.pdf.

[AARC-DNA3.2] https://aarc-project.eu/wp-content/uploads/2017/02/DNA3.2-Security-Incident-Response-Procedure-v1.0.pdf.