07 December 2022

eduGAIN Policy Framework

eduGAIN CSIRT Terms of Reference

Document Revision History

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

eduGAIN Policy Framework

eduGAIN CSIRT Terms of Reference

Contents

1 Title

The name of the group is eduGAIN Computer Security Incident Response Team (CSIRT).

2 Definitions

This document makes use of the Definitions described in the eduGAIN Constitution [eduGAIN-Constitution] and of the following additional ones:

CSIRT	Computer Security Incident Response Team
eduGAIN stakeholder	eduGAIN Steering Group members, REFEDS members, NRENs, research and education community members, Service Providers.
Entity Security Contact	An entity mail address dedicated to security issues and incident response. It is recommended that the security contact is monitored by multiple individuals.

3 Purpose and Responsibilities

eduGAIN-CSIRT provides computer security incident response coordination for eduGAIN. It serves as the primary contact point for all security related issues affecting eduGAIN and more specifically for all the security issues affecting multiple entities from different Federations.

The eduGAIN-CSIRT maintains a communication infrastructure to assure that all the relevant information is received by the relevant Federation Operators and Entities security contacts in eduGAIN. That the information is processed and needed response actions are carried out is the responsibility of the Entity and respective Federation Operator Security Contacts.

3.1 Constituency

eduGAIN-CSIRT provides incident response coordination for the Entities of members of Identity Federations participating in eduGAIN.

3.2 Service Description

Members of eduGAIN-CSIRT provide the services described in section 5 of the [eduGAIN-CSIRT RFC 2350] document.

3.3 Service Level Description

The services described above are provided at least during business hours (9x5 CET/CEST) with 4-hour response, and outside business hours on a best-effort basis.

4 Composition

4.1 Membership

eduGAIN-CSIRT consists of:

- the eduGAIN-CSIRT Security Officer, that will be nominated by the GEANT project.
- At the time of the establishment of the eduGAIN-CSIRT the eduGAIN Participants will be invited to propose members of the eduGAIN-CSIRT. The proposed members must be senior security professionals from research and education IT infrastructures and it must have previous experience in a security position in the home organization. The proposals will be reviewed for acceptance by the eduGAIN Security Officer.
- An eduGAIN Participant can always propose a new member of the eduGAIN-CSIRT, following the same criteria specified above. The proposal will be reviewed for acceptance by the eduGAIN Security Officer according to the actual needs of the eduGAIN-CSIRT.
- Each member of the eduGAIN-CSIRT will be funded by the respective organization either through the GEANT project, or direct funding.

4.2 Chair

The Chair of eduGAIN-CSIRT is the eduGAIN Security Officer.

4.3 Duties and responsibilities

The duties and responsibilities of the Chair include:

- Managing team membership.
- Reporting to the the eSG as appropriate..
- Ensuring all discussion items end with a decision, action or definite outcome.
- Acting as general point of contact for eduGAIN-CSIRT.
- Ensuring team activity and output is documented, approved when needed, and distributed to the appropriate audience.
- Ensuring that the eduGAIN-CSIRT meets the various demands placed on it to produce and maintain security policies, security procedure and best practice. This will include negotiation with eSG, members of the eduGAIN-CSIRT, and other stakeholders to agree on priorities and timelines, in a manner commensurate with the effort available to the eduGAIN-CSIRT.
- Ensuring that the eduGAIN-CSIRT provides the services and the service level described in 3.2 and 3.3.

The duties and responsibilities of the members include:

- Participating to the eduGAIN-CSIRT meetings.
- Following the eduGAIN CSIRT internal procedures.
- Actively contributing to the mission of the eduGAIN-CSIRT.
- Providing expertise and guidance to the best of their knowledge.
- Abiding to the Trusted Introducer Code of Conduct [TI CCoP].
- Respecting TLP restrictions [FIRST TLP] and appropriate confidentiality requirements.
- Providing the services and the service level described in 3.2 and 3.3.

4.4 Term of Office

The Term of Office is unlimited.

4.5 Method of Appointment

The eduGAIN-CSIRT Chair is appointed by the GÉANT project.

5 Operating Procedures

The operation of eduGAIN-CSIRT will obey the eduGAIN Declaration [eduGAIN Declaration] and the eduGAIN Constitution [eduGAIN Constitution] and follow the procedures approved by the eSG. Any eduGAIN stakeholder has the right to suggest new policies and procedures: such requests should be submitted to the eduGAIN Security Officer. The decision whether to accept this request will be discussed within the eduGAIN CSIRT and decision will be recorded in the minutes of the meeting and feedback will be provided to the original requestor.

5.1 Communications and Meetings

All the members of the eduGAIN-CSIRT must subscribe to the eduGAIN-CSIRT mailing list (edugain-support-sec-team@lists.geant.org) and should use it as the primary written communication channel. To allow for low latency communications, the team may communicate using end-to-end encrypted instant messaging channels provided all end-points have been pre-authenticated during a face-to-face validation.

The group deliberations happen at face-to-face meetings, phone/video conferences, or via the group mailing list. To enable consideration, where practicable, the draft agenda together with reports and documents that relate to the group will be forwarded to members three working days prior to scheduled meetings.

Accurate minutes will be kept of each meeting of the group. The minutes of a meeting shall be submitted to group members for ratification at the next subsequent meeting of the group.

5.2 Decision making

Decisions by the group will be made as follows:

- Wherever possible, the Group will arrive at proposed draft recommendations documents and/or advice by clear consensus, as determined by the Chair;
- A voting process will only start if consensus cannot be reached after two consecutive group meetings or if at least one third of voting members of the Group call for a vote;
- A decision is adopted if more than 50% of the voting members present cast their vote for the proposed decision;
- If the group's recommendations are adopted by majority vote, minority positions will be recorded and reported;
- The group, by majority decision, may refer matters for decision to the eduGAIN Steering Group on issues where a consensus cannot be achieved.

5.3 Peer Organisations

The eduGAIN-CSIRT shall proactively communicate with recognized peer organisations regarding suspected and confirmed security incidents that could affect such peers. It shall maintain a reference to the operating policies and practices of such peer infrastructures and participate in their processes and the evolution thereof.

5.4 External Collaborations

The eduGAIN-CSIRT members can decide to collaborate with external experts or entities for the purpose of assisting in a specific incident response or investigation. The external experts' contribution will be limited to the scope of the incident and it will last for the time of the investigation and resolution of the incident.

5.5 Communication Channels

eduGAIN-CSIRT email list	edugain-support-sec-team@lists.geant.org
Report of abuse	abuse@edugain.org
eduGAIN-CSIRT wiki & meeting minutes	https://wiki.geant.org/display/eduGAIN/eduGAIN+Security
Telephone	+44 1223 733033

Instant messaging channels	Signal group, keybase.io: edugain_sec

5.6 Related material and references

Related material is available on the eduGAIN website at the following location: https://edugain.org/edugain-security/references/.

5.7 Reporting

eduGAIN-CSIRT provides input about current operational security activities to Federation Operators group and eSG on request.

6 Authority

eduGAIN-CSIRT is authorised by the eSG to coordinate computer security incident response activities within its Terms of Reference and the applicable security policies. The eSG is the governing body of eduGAIN-CSIRT.

7 References

[eduGAIN Constitution] https://technical.edugain.org/doc/eduGAIN-Constitution-v3ter-web.pdf.
[eduGAIN-CSIRT RFC2350] https://edugain.org/edugain-security/rfc2350.
[eduGAIN Declaration] https://technical.edugain.org/doc/eduGAIN-Declaration-v2bis-web.pdf.
[FIRST TLP] https://www.first.org/tlp.
[TI CCoP]https://www.trusted-introducer.org/TI-CCoP.pdf.