



EU-LISA CSIRT
RFC 2350

Contents

Contents	2
1. Document Information	3
1.1. Date of Last Update	3
1.2. Distribution List for Notifications	3
1.3. Locations where this Document May Be Found	3
1.4. Authenticating this Document	3
1.5. Document Identification	3
2. Contact Information	3
2.1. Name of the Team	3
2.2. Address	4
2.3. Time Zone	4
2.4. Telephone Number	4
2.5. Facsimile Number	4
2.6. Other Telecommunication	4
2.7. Electronic Mail Address	4
2.8. Public Keys and Encryption Information	4
2.9. Team Members	5
2.10. Other Information	5
2.11. Points of Customer Contact	5
3. Charter	5
3.1. Mission Statement	5
3.2. Constituency	5
3.3. Sponsorship and/or Affiliation	5
3.4. Authority	5
4. Policies	6
4.1. Types of Incidents and Level of Support	6
4.2. Co-operation, Interaction and Disclosure of Information	6
4.3. Communication and Authentication	6
5. Services	6
5.1. Prevention	6
5.2. Security monitoring	7
5.3. Incident Response	7
6. Incident Reporting	7
7. Disclaimer	7

1. Document Information

This document contains a description of eu-LISA CSIRT in accordance with RFC 23501. It provides basic information about eu-LISA CSIRT, the channels of communication, its roles and responsibilities.

1.1. Date of Last Update

Version 3.0 – 11/01/2023

1.2. Distribution List for Notifications

There is no distribution list for notifications.

1.3. Locations where this Document May Be Found

The current version of this CSIRT description document is available on request by sending an e-mail to [Csirt\[at\]eulisa.europa.eu](mailto:Csirt[at]eulisa.europa.eu).

1.4. Authenticating this Document

This document has been signed with the eu-LISA CSIRT PGP key.

1.5. Document Identification

Title: "eu-LISA CSIRT RFC 2350"

Version: 2.0

Document date: 10 January 2023

Expiration: This document is valid until superseded by a later version

2. Contact Information

2.1. Name of the Team

eu-LISA Computer Security Incident Response Team (CSIRT)

Short name: eu-LISA CSIRT

2.2. Address

Headquarters	Operational Site
eu-LISA - European Union Agency for the Operational Management of Large-Scale IT Systems Security and Continuity Unit Vesilennuki 5, 10415 Tallinn, Estonia	eu-LISA - European Union Agency for the Operational Management of Large-Scale IT Systems Security and Continuity Unit 18 Rue de la Faisanderie, 67100 Strasbourg, France

2.3. Time Zone

EET/EEST

CET/CEST

2.4. Telephone Number

No phone number publicly available.

2.5. Facsimile Number

N/A

2.6. Other Telecommunication

Video conferencing available on request.

2.7. Electronic Mail Address

For notifications, security incident reporting and operational matters, please contact us at: Csirt[at]eulisa.europa.eu.

This e-mail address is monitored by a duty officer during hours of operation.

2.8. Public Keys and Encryption Information

PGP is used for functional exchanges between eu-LISA CSIRT and its partners (incident reports, alerts, etc.).

eu-LISA CSIRT has a PGP key, whose KeyID is 0xF1FD5203.

Fingerprint is 7816 2541 634E F409 0626 62CC F7DB EA91 F1FD 5203.

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

2.9. Team Members

The list of eu-LISA CSIRT team members is not publicly available. The identity of the Head of the eu-LISA CSIRT and team members may be divulged on a case-by-case basis according to the need-to-know restrictions.

2.10. Other Information

No other information is publicly available.

2.11. Points of Customer Contact

The eu-LISA CSIRT prefers to receive incident reports via e-mail at [csirt\[at\]eulisa.europa.eu](mailto:csirt[at]eulisa.europa.eu), which is monitored by a duty officer during hours of operation. Please use our cryptographic key to ensure integrity and confidentiality. In case of emergency, please specify the [URGENT] tag in the subject field in your e-mail.

Days/Hours of Operation: 09:00 to 17:30 Monday to Friday.

3. Charter

3.1. Mission Statement

The mission of eu-LISA CSIRT is to ensure the coordinated response across the Agency to IT security incidents, minimizing their negative effects through providing effective guidance for response and recovery activities, and to work to prevent incidents in the future.

3.2. Constituency

eu-LISA CSIRT's constituency is composed of all the elements of the Information Systems managed and operated by eu-LISA, including its users, its systems, its applications and its networks.

3.3. Sponsorship and/or Affiliation

The eu-LISA CSIRT is part of the Security Unit within eu-LISA.

3.4. Authority

The eu-LISA CSIRT operates under the auspices of, and with the authority delegated by, the eu-LISA Management Authority, in accordance with the Decision of the Management Board of eu-LISA No 2019-148 of 9 April 2020 on the Security Rules on the Protection of Communication and Information Systems ('CIS') in eu-LISA¹.

¹ https://eulisa.europa.eu/AboutUs/Documents/MB_Decissions/2019-148_Decision on Security Rules on the protection of CIS in eu-LISA.pdf

In this context, the eu-LISA CSIRT may have access to systems and data corporate wide to detect, analyse and handle computer security incidents. Such activities are performed according to the rules defined in Regulation (EC) 2018/1725 of 23 October 2018² governing the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.

4. Policies

4.1. Types of Incidents and Level of Support

The eu-LISA CSIRT is authorized to address all types of computer security incidents which occur, or threaten to occur, in eu-LISA.

4.2. Co-operation, Interaction and Disclosure of Information

eu-LISA CSIRT operates within the confines imposed by EU legislation. We collaborate and share information with CERT-EU.

eu-LISA CSIRT highly regards the importance of operational cooperation and information sharing between CSIRTs and other organisations which may contribute towards the efficiency and effectiveness of provided services.

All requests to the eu-LISA CSIRT are treated with due care. eu-LISA CSIRT adheres to the traffic light protocol (TLP version 2.0). See <https://www.first.org/tlp/> for a description. Sensitive messages should be tag in the subject as [TLP:Color]. A similar stamp should be clearly visible in other documents, such as PDF files etc, sent to the eu-LISA CSIRT. If contact is through phone or video conference, the TLP classifications should be stated prior to the delivery of the information.

Please encrypt all sensitive information with the PGP key mentioned above. Other encryption methods are available upon request.

4.3. Communication and Authentication

eu-LISA CSIRT protects sensitive information in accordance with relevant regulations and policies within the agency and EU.

5. Services

5.1. Prevention

² [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1725#:~:text=Regulation%20\(EU\)%202018%2F1725,EC\)%20No%2045%2F2001%20and](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1725#:~:text=Regulation%20(EU)%202018%2F1725,EC)%20No%2045%2F2001%20and)

This service aims at raising awareness and preventing security events, by providing technical security alerts and warnings, technical guidance on specific targeted cyber-attacks (ie. APT attacks) and technical security assessments.

5.2. Security monitoring

This service aims to provide a security monitoring to detect intrusion events and response capability including a set of operational processes build around detection monitoring and security logs analysis tools.

5.3. Incident Response

This service aims to provide specialised technical security incident analysis and handling actions, which include activities to evaluate available information, to validate and verify it, to gather additional evidence if required, to communicate with relevant parties, and finally to propose solutions in order to resolve the incident.

6. Incident Reporting

Whenever possible the incidents should be reported to eu-LISA CSIRT by e-mail using the address: **csirt[at]eulisa.europa.eu**.

If the incident is reported by an external entity, it is preferably that the e-mail is encrypted with eu-LISA CSIRT PGP public key.

Please provide at least the following information:

- Contact details and organizational information – name of person and organisation name and address, -email address, telephone number;
- Short summary of the incident; type of event;
- Source of indication; (i.e. the system produced an alert etc.);
- System affected; (i.e. network asset etc.);
- Estimated impact; (i.e. loss of communications etc.);
- Other particularities:
 - Details of the observations that led to the discovery of the incident - scanning results (if any); an extract from the log showing the problem, etc.;
 - In case there is a need to forward any e-mails to eu-LISA CSIRT, please make sure that all e-mail headers, body and any attachments are included.

7. Disclaimer

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

