TLP:CLEAR

National Cybersecurity Authority
General Directorate of Operational Planning
EL-CSIRT
Chandri 1, Moschato 18346, Greece

EL-CSIRT RFC 2350

Version. 1.0 - 2025-04-14

1 Document information

This document describes the functions of the Computer Security Incident Response Team (CSIRT) of the Hellenic National Cybersecurity Authority (EL-CSIRT) according to RFC 2350 specifications. It provides basic information about the EL-CSIRT and describes the responsibilities and services offered.

1.1 Date of last update

- **Title**: EL-CSIRT RFC 2350
- **Version**: 1.0
- **Release Date**: 2025-04-14
- **Expiration**:This document is valid until superseded by a later version.

1.2 Distribution list for notifications

Changes to this document are notified at the following address of the website of the Hellenic National Cybersecurity Authority: https://cyber.gov.gr/el-csirt/

Questions regarding updates can be sent via email, as stated in paragraph 2.7.

1.3 Locations where this document may be found

The current version of this EL-CSIRT description document is available from the website of the Hellenic National Cybersecurity Authority, at the following email address: https://cyber.gov.gr/el-csirt/

Make sure you are using the latest version.

2 Contact details

2.1 Name of the team

- **Full Name**: Computer Security Incident Response Team (CSIRT) of the Hellenic National Cybersecurity Authority
- **Short Name**: EL-CSIRT

2.2 Address

National Cybersecurity Authority

Chandri 1, Moschato 18346, Greece

2.3 Time Zone

UTC+2 (EET – Eastern European Time) during the winter period (from the last Sunday of October to the last Sunday of March).

UTC+3 (EEST – Eastern European Summer Time) during the summer period (from the last Sunday of March to the last Sunday of October).

2.4 Telephone number

+30 210 4802166

2.5 Fax Number

Not available.

2.6 Other Telecommunications

Not available.

2.7 Electronic mail address

Contact us at the email address: : csirt@cyber.gov.gr .If you need to report an information security incident or a cyber threat within our jurisdiction, please use the email address: incident@cyber.gov.gr

2.8 Public keys and encryption information

EL-CSIRT uses PGP to exchange information (alerts, incident reports, etc.) with peers, partners, and stakeholders.

- User: el-csirt <csirt@cyber.gov.gr>
- Footprint PGP: CD5B138D39005BB715714003C639A0184948BBAA
- Location: https://cyber.gov.gr/el-csirt/

2.9 Team Members

The EL-CSIRT team consists of information security experts. The list of EL-CSIRT team members is not publicly available. The identities of EL-CSIRT team members may be disclosed on a case-by-case basis, in accordance with need-to-know restrictions.

2.10 Other Information

General information about the EL-CSIRT of the Hellenic National Cybersecurity Authority, as well as links to various recommended information security websites, are available at https://cyber.gov.gr/ .

EL-CSIRT is a member of the EU CSIRT Network (EU CNW), which was created in accordance with the NIS (Network and Information Systems Directive) of the European Union.

2.11 Points of customer contact

The preferred method of communication with the EL-CSIRT of the Hellenic National Cybersecurity Authority is by email at the address provided in paragraph 2.7. Please use the EL-CSIRT PGP cryptographic key provided in paragraph 2.8 to ensure integrity and confidentiality. In case of emergency, please use the tag [URGENT] in the subject field of your email.

3 Charter

3.1 Mission statement

By law 5086/2024, article 10, paragraph 1.c, the General Directorate of Operational Planning of the National Cybersecurity Authority is assigned the management of cyber incidents and the operation of the Cybersecurity Incident Response Team (CSIRT).

By law 5160/2024, the National Cybersecurity Authority is designated as the competent authority, the single point of contact and the response team for computer security incidents (CSIRT) of key and important entities. The CSIRT of the National Cybersecurity Authority performs a coordinating role of CSIRTs in Greece to achieve a high common level of cybersecurity.

3.2 Constituency

The constituency of EL-CSIRT of the Greek National Cybersecurity Authority includes:

- Critical, essential and important entities as defined by Greek legislation
- In particular, for Public Sector entities, these fall under the National CERT (NCERT-GR) of the National Intelligence Service.

Furthermore EL-CSIRT of the National Cybersecurity Authority is the coordinating CSIRT of Greece.

3.3 Affiliation

The EL-CSIRT operates within the General Directorate of Operational Planning of the National Cybersecurity Authority and is financially supported by the National Cybersecurity Authority.

3.4 Authority

The responsibilities and authorization of the EL-CSIRT of the National Cybersecurity Authority are determined by the following national laws:

- Law 5086/2024, Government Gazette 23, issue A/ 14-02-2024
- Law 5160/2024, Government Gazette 195, issue A / 27-11-2024.

4 Policies

4.1 Types of Incidents and Level of Support

The level of support provided by the EL-CSIRT varies depending on the type and severity of the incident or cyber threat, the type of key or significant entity affected, the significance of its impact on critical infrastructure or service, and the resources available to the EL-CSIRT at the time. The EL-CSIRT provides proactive cybersecurity services, as well as cybersecurity incident response services, such as the following:

- Receive incident reports
- Monitoring and analysis of cyber threats, vulnerabilities and incidents at a national level, exclusively for the sectors and organizations under its responsibility

- Providing timely warnings, alerts, announcements and information to key and important entities involved, as well as to competent authorities and other relevant stakeholders, regarding cyber threats, vulnerabilities and incidents, if possible, in near real time
- Providing, upon request of a key or significant entity, a proactive scan of the network and information systems of the entity concerned to identify vulnerabilities with a potential significant impact
- Preventive non-intrusive scanning of publicly accessible network systems and information systems of key and important entities, as long as it does not have negative consequences for the operation of the entities' services
- Responding to incidents and providing assistance to affected essential and important entities, upon their request
- Collection and analysis of forensic data and dynamic analysis of risks and incidents and situational awareness in cybersecurity matters

4.2 Co-operation, interaction and disclosure of information

Incident-related information, such as names and technical details, is not published without the consent of the entities involved. Unless otherwise agreed, information disclosed to the EL-CSIRT is kept confidential. The EL-CSIRT will never pass on information to third parties unless required by law.

EL-CSIRT handles the information transmitted to it according to its classification and based on the need-to-know principle. Therefore, each transmission of information includes only specific relevant and anonymized excerpts.

Incident-related information may be shared with entities such as:

- Technical experts of the Greek National Cybersecurity Authority
- Affected entities under the jurisdiction of EL-CSIRT
- Greek law enforcement agencies (if required by law or upon request)
- CERT/CSIRT collaboration teams and networks

EL-CSIRT works closely with groups at national, European and international levels and strongly supports voluntary cooperation between CSIRTs at all levels. To this end, EL-CSIRT ensures presence and networking with its partners through active participation in working groups and international meetings and conferences.

When providing information to EL-CSIRT using the Traffic Light Protocol (TLP), EL-CSIRT respects the information exchange policy as defined by the FIRST organization in: https://www.first.org/tlp/.

4.3 Communication and authentication

The preferred method of communication with EL-CSIRT is electronic mail, as stated in paragraph 2.7. EL-CSIRT uses PGP for encryption and/or signing of messages. All sensitive communications with EL-CSIRT should be encrypted. It is recommended that e-mails sent to EL-CSIRT be encrypted, utilizing EL-CSIRT's PGP public key, as described in paragraph 2.8.

5 Services

5.1 Incident Response

EL-CSIRT provides incident response coordination services available 24/7 at the national level based on its scope of competence (par. 3.2) in order to facilitate other CSIRTs, and exchanges information with key and important entities and other relevant stakeholders to keep their information systems and networks secure.

5.1.1 Incident triage

- Monitoring and detection of potential threats and vulnerabilities
- Investigating whether a security incident actually occurred
- Determination of the extent of the event
- Information on decisions and containment measures

5.1.2 Incident Coordination

EL-CSIRT supports key stakeholders in responding to security incidents by providing coordination services such as:

- Determining the root cause of the incident
- Facilitating communication between the involved parties
- Facilitate communication with relevant law enforcement authorities, if necessary
- Analysis and reporting to other CSIRTs
- Writing announcements

5.1.3 Incident resolution

The responsibility for designing, developing and operating systems and services in a secure manner and resolving security incidents always remains with the owners of such systems and services. In certain cases, and upon request, assistance is provided to the affected key and important entities, as follows:

- Guidance or operational advice on the implementation of potential mitigation actions
- Collection and analysis of forensic data
- Dynamic risk and incident analysis
- Receive relevant reports
- Sending relevant reports

The extent of this support will depend on the type and severity of the incident and the type of entity affected.

5.2 Proactive activities

The EL-CSIRT coordinates and maintains the following services to the extent possible according to its resources:

- Providing timely warnings, alerts, announcements and information to key and important entities involved, as well as to competent authorities and other relevant stakeholders regarding cyber threats, vulnerabilities and incidents

- Providing, upon request, proactive scanning of network and information systems to identify vulnerabilities with a potential significant impact
- Proactive non-intrusive scanning of publicly accessible network and information systems to identify vulnerable or poorly configured systems
- Information services via the website https://www.cyber.gov.gr
- Monitoring technology trends
- Coordination of vulnerability disclosure (CVD) at national level
- Contribute to cybersecurity awareness and education

6 Incident Reporting Forms

The receipt of security incident reports from key and important entities under the responsibility of the EL-CSIRT is based on a specific reporting procedure available at the electronic address: https://cyber.gov.gr/kyvernoepitheseis/anafora-symvanton/ .

7 Disclaimers

EL-CSIRT takes all necessary organizational and technical measures to protect the information provided to it. For any error, omission or damage that may arise from the use of or in relation to the information provided to it, it bears no responsibility for any claim for compensation.