RFC 2350: CERT.LV Description

Version 7.0
Document OID: 1.3.6.1.4.1.28446.2.1.7.0

1. About this document

1.1 Date of Last Update

This is version 7.0, published on 21.07.2025.

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 CERT.LV description document is available from the CERT.LV WWW site: https://www.cert.lv/lv/par-mums and https://www.cert.lv/en/about-us

1.4 Identification

1. Document title: "CERT.LV Description"
2. Version: 7.0.
3. Document Date: 21.07.2025.
4. OID: 1.3.6.1.4.1.28446.2.1.7.0

IANA	1.3.6.1.4.1
IMCS UL	28446
CERT.LV	.2
Description	.1
Major Version	.7
Minor Version	.0

5. Expiration: This document is valid until new version is adopted.

2. Contact Information

2.1 Name of the Team

CERT.LV: Cyber Incident Response Institution of the Republic of Latvia.
CERT.LV formerly known as CERT NIC.LV and LATNET CERT was established on 01 August 2006.
DDIRV (National Computer Security Incident Response Team) was merged with CERT NIC.LV on 1 February 2011 to form CERT.LV.

2.2 Address

CERT.LV
Institute of Mathematics and Computer Science, University of Latvia
Raiņa bulvāris 29
Rīga, LV-1459
Latvia

2.3 Time Zone

Eastern European Time [EET]: GMT+0200
Daylight Savings Time: GMT+0300 (from last Sunday in March till last Sunday in October).

2.4 Telephone Number

+371 67085888

2.5 Facsimile Number

Not available.

2.6 Other Telecommunication

Not available.

2.7 Electronic Mail Address

cert@cert.lv is the main address for incident reporting.

All emails are processed using the incident tracking system and ticket numbers will be assigned. It is recommended to use the assigned ticket numbers for all communication concerning the same incident. New incidents shall never re-use an already assigned ticket number.

2.8 Public Keys and Other Encryption Information

The CERT.LV has a PGP key, the details:
User ID: CERT.LV
Key ID: 0x87BCCEEDC0DE2EC3
Key type: RSA
Key size: 4096 bit
Expiration: Never
Fingerprint: B5E8 82A1 338E 7749 09D0 A8F0 87BC CEED C0DE 2EC3

The key and its signatures can be found here: https://www.cert.lv/en/contacts and at the usual large public key servers.

2.9 *Team Members*

Baiba Kaškina is the Head of CERT.LV.
Varis Teivāns is the Deputy Head of CERT.LV.
Information about other team members is not publicly available.

2.10 *Other Information*

General information about the CERT.LV, as well as details on CERT.LV activity areas and links to various recommended security resources, can be found at https://www.cert.lv.
Most information is available in Latvian only.

2.11 *Points of Customer Contact*

The preferred method for contacting CERT.LV is via email to cert@cert.lv. We encourage our constituents to use PGP encryption when sending any sensitive information to CERT.LV.

Our regular response hours are workdays 09:00 – 18.00 (local time, save public holidays in Latvia). Reporting of incidents is possible by telephone 24x7. The person on duty will involve CERT.LV specialists as needed.

3. *Charter*

3.1 *Mission Statement*

The mission of CERT.LV is to improve and promote the overall cybersecurity in Latvia and European Union by focussing on the following objectives:

- conduct analysis at the State level of significant cyber threats, vulnerabilities, and cyber incidents;
- respond to cyber incidents, upon request of the subject to provide support in cyber incident handling or to coordinate the prevention of a cyber incident;
- warn and provide the National Cybersecurity Centre, the Constitution Protection Bureau, the subjects, and, if necessary, other institutions with the information on current significant cyber incidents, cyber incidents, near misses, cyber threats, and vulnerabilities;
- organise educational measures, perform analytical and research work, and organise thematic trainings in the field of cybersecurity;
- provide support to State authorities in the protection of State security and also detection (investigation) of criminal offences and other violations of the law in the field of information and communication technologies;
- cooperate with the competent authorities and computer security incident response teams of the European Union, foreign and international organisations, to participate in the network of computer security incident response teams of the European Union Member States (hereinafter - the CSIRT network);
- inform without delay the National Cybersecurity Centre and State security institutions of the significant cyber incident and also to inform the competent authority of another European Union Member State of the significant cyber incident which disrupts the

continuity of operation of an essential service or important service in the particular Member State;

- inform the National Cybersecurity Centre and the Constitution Protection Bureau of the detected non-conformity of information and communication technologies of the subject with the laws and regulations laying down the cybersecurity requirements and also of the detected cases when the subject has not reported on a cyber incident;
- within the limits of competence, to cooperate with the State and private sector authorities in order to facilitate cybersecurity and cyber resilience, and also to cooperate and exchange the relevant information on current cyber threats with the communities of the subjects;
- upon request of the subject, to perform proactive scanning of the networks and information systems of the subject to detect vulnerabilities with potentially essential impact;
- carry out other obligations under laws and regulations.

As part of its assigned functions within the National Cybersecurity Centre, CERT.LV has the following objectives:

- maintain a unified depiction of the activities occurring in the cyberspace of Latvia, except for the content of the information transmitted therein;
- inform the public of current cyber threats;
- ensure the operation of security operations centres in the data centres conforming to the requirements stipulated by the Cabinet of Ministers;
- participate in coordinated vulnerability discovery and prevention within the limits of the competence;
- where necessary, to inform the European Union Agency for Cybersecurity of the information to be included in the database of vulnerabilities;
- in cases when vulnerability also affects another European Union Member State, to cooperate with the competent authorities of that Member State;
- where necessary, to participate in assessments of the cybersecurity capacity and action policy of the European Union Member States in the status of an independent expert.

3.2 Constituency

CERT.LV primary constituency stems from the National Cyber Security law which implements NIS2 directive and are:

- state institutions and local authorities of Latvia;
- Providers of Essential Services and Important Services as defined by Latvian National Cybersecurity Law[1] which implements NIS2 Directive[2];
- IT Critical infrastructure of Latvia.

CERT.LV secondary constituency are:

- private sector using IP addresses of Latvia and resources with TLD .lv;
- citizens using IP addresses of Latvia and resources with TLD .lv.

[1] https://likumi.lv/ta/en/en/id/353390-national-cybersecurity-law

[2] https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

The list of IP addresses of Latvia can be found at: http://www.nic.lv/lix.

3.3 Sponsorship and/or Affiliation

The CERT.LV is financed and supervised by the Ministry of Defence of the Republic of Latvia.
CERT.LV is mandated by the National Cybersecurity Law to represent Latvia in the NIS CSIRTs Network[3].
CERT.LV is actively taking part in TF-CSIRT[4].
CERT.LV is certified by the Trusted Introducer[5] since September 2016 (and accredited since May 2008).
CERT.LV is full member of FIRST[6] since April 2009.

3.4 Authority

CERT.LV operates under the auspices of Institute of Mathematics and Computer Science[7], University of Latvia, with authority delegated by and under supervision of the Ministry of Defence[8] of the Republic of Latvia.

National Cybersecurity Law empowers CERT.LV:

- request and obtain information from state, municipal, and private legal entities concerning implemented ICT security measures, identified vulnerabilities, and cyber threats, as well as detailed technical data on past or ongoing cyber incidents.
- subject to mutual agreement with the subject, access online data flows to detect and prevent cyber threats.
- conduct inspections of ICT infrastructure used by essential and important service providers, and, upon request of the Constitution Protection Bureau, inspect critical ICT infrastructure.
- request that the National Cybersecurity Centre sends information to the competent authority of a European Union Member State, the NIS Cooperation Group, the CSIRT network, or the European Union Agency for Cybersecurity on a cyber incident which has an impact on the provision of essential services or important services in the particular Member State.
- proactively scan publicly accessible networks and information systems of the subjects for vulnerabilities or insecure configurations, and inform the respective entities accordingly.
- to process personal data in the exercise of its legal tasks and rights for the purposes of confirming or eliminating suspicions of a cyber threat, preventing such threats, and maintaining communication with involved parties. Following the resolution of a vulnerability or cyber incident, CERT.LV may retain and analyze the collected personal data if it is relevant for the detection or prevention of related threats. CERT.LV may also share such data with other institutions as provided by law.

[3] https://csirtsnetwork.eu/

[4] https://tf-csirt.org/

[5] https://www.trusted-introducer.org/

[6] https://www.first.org/

[7] https://lumii.lv/

[8] https://www.mod.gov.lv/

- to maintain a list of restricted internet resources (DNS Firewall) which must be used by the providers of electronic communications services and maintainer of the top-level domain name registry to restrict the access of end-users to the internet resourses included in the list. The DNS Firewall service is also available as optional service to every citizen and company, including as a mobile app service, protecting end-users from accessing internet resources containing cyber threats, such as fake bank pages, fraudulent trading platforms, malware-spreading websites, etc.

Carrying out the decisions of the National Cybersecurity Centre, CERT.LV is empowered to:

- where a cyber threat or a cyber incident causes or might cause a significant threat to the security of information systems and electronic communications networks or national security and the cyber incident or cyber threat cannot be prevented in any other way:
    - to disconnect or limit access to the domain name involved in the cyber incident or cyber threat;
    - to limit access to the Internet Protocol (IP) address involved in the cyber incident or cyber threat;
    - to limit access to the mobile platform application involved in the cyber incident or cyber threat.
- request that subject of the National Cybersecurity Law closes access for the user to the electronic communications network for not longer than five days if the user significantly endangers the rights of other users or security of the electronic communications network, information system, or service.
- request that National Cybersecurity Centre adopts compulsory decisions, to ensure that public insitutions and private entities are compliant with duties imposed by the law.

4. Policies

4.1 Types of Incidents and Level of Support

The CERT.LV is authorized to address all types of cybersecurity incidents which occur, or threaten to occur, at all networks in Latvia. A cybersecurity incident (hereinafter - Incident) is an event compromising the availability, authenticity, integrity, or confidentiality of processed data or of the services offered by, or accessible via, network and information systems. Issues and events related to content i.e. copyright, are not considered incident from CERT.LV point of view.

Incidents are prioritized according to type and the severity of the incident. Incidents directly affecting primary constituency are treated with higher priority.

The level of support given by CERT.LV will vary depending on the type of constituent, type and severity of the incident or issue, the size of the user community affected, and CERT.LV resources at the time; though in all cases some meaningful response will be made within one working day. Upon receiving an initial report of a significant incident, CERT.LV will provide an initial assessment and propose preventive measures within 24 hours.

CERT.LV will provide support also for the end users, however it is preferred that they contact their system administrator, network administrator, or department head for assistance before contacting CERT.LV.

CERT.LV services are provided on a best effort basis.

In case of significant Incidents or crisis affecting the primary constituency (see point 3.2.), the response times will be longer for incidents affecting the secondary constituency.
CERT.LV uses international version of incident classification/incident taxonomy which is published: https://www.trusted-introducer.org/processes/standards.html

4.2 Co-operation, Interaction and Disclosure of Information

CERT.LV maintains and moderates cooperation with people responsible for cybersecurity in their institutions, mostly from the primary constituency (see point 3.2.) as well as Latvian ISPs security and abuse teams and with law enforcement representatives. CERT.LV is one of the founders of the DEG initiative (Information Technology and Information Systems Security Experts Group).
CERT.LV is sharing information on a need-to-know basis, and where required by regulations in an anonymized fashion when this will assist appropriate entities in resolving or preventing cybersecurity incidents.

Information being considered for release will be classified as follows:

- Private user information will not be released in identifiable form outside the CERT.LV, except as provided below. If the identity of the user is disguised, then the information can be released freely.
- Intruder information, and in particular identifying information will not be released to the public (unless it becomes a matter of public record, for example because criminal charges have been laid), it will be exchanged freely with system administrators and CSIRTs tracking the incident.
- Private site information will not be released without the permission of the site in question, except as provided below.
- Vulnerability information will be exchanged with affected parties. CERT.LV will follow-up if the vulnerability is patched. Public annnouncements will be considered according to the National Cybersecurity Law.
- Information on significant cybersecurity incident or cyber threat may be disclosed to the public by CERT.LV (upon previous discussion with the subject), or, upon its request, by the subject, if such disclosure may help prevent or manage a major cybersecurity incident, mitigate the threat, or otherwise serve the public interest, unless such disclosure would conflict with national security interests.
- Statistical information will be released at the discretion of the CERT.LV. CERT.LV publishes monthly and quarterly statistics on the website. https://cert.lv/lv/incidenti/statistika
- Contact information on the institutions and organizations is shared only with trusted partners on need to know basis. Contact information of private users will not be shared with any third parties.

Potential recipients of information from the CERT.LV will be classified as follows:

- Constituency: entitled to receive information that is not protected by confidentiality or secrecy obligations and is necessary to facilitate the handling of cybersecurity incidents which occur in their jurisdictions.
- Cybersecurity managers / system administrators / responsible persons for the cybersecurity within the constituency, by virtue of their responsibilities, trusted with confidential information.
- Users within the constituency are entitled to information which pertains to the security of their own digital identities. Users within the constituency are entitled to be notified if their account is believed to have been compromised.
- The CERT.LV constituencies will not receive restricted information, except where the affected parties (legitimate owners, operators, and users of the relevant asstes) have given permission for the information to be disseminated.
- The cybersecurity community, Trusted Introducer community of accredited and certified CSIRTs, NIS CSIRT Network as well as FIRST members are treated as trusted circles and information is released using TLP protocol to mark information dissemination expectations. When members of CERT.LV participate in discussions within the cybersecurity community, such as mailing lists and conferences, they will treat such forums as though they were the public at large. While technical issues (including vulnerabilities) may be discussed to any level of detail, any examples taken from CERT.LV experience will be disguised to avoid identifying the affected parties.
- The press will also be considered as part of the general public. CERT.LV will provide comments and give interviews regarding situation in the cyber space, vulnerabilities, cybersecurity incidents, and general security topics without disclosing sensitive information that might help to identify involved organizations or individuals.
- Other sites and CSIRTs, when they are partners in the investigation of a cybersecurity incident, will in some cases be trusted with confidential information. This will happen only if the foreign sites bona fide can be verified, and the information transmitted will be limited to that which is likely to be helpful in resolving the incident.
- Law enforcement officers will receive full cooperation from the CERT.LV, according to legislation requirements including any information they require to pursue an investigation, notwithstanding the earlier statements made about confidentiality.

CERT.LV understands and supports the traffic light protocol (TLP https://www.first.org/tlp).

4.3 Communication and Authentication

In view of the types of information that the CERT.LV will likely be dealing with, telephones will be considered sufficiently secure to be used even unencrypted. Unencrypted e-mail will not be considered particularly secure, but will be sufficient for the transmission of low-sensitive data. If it is necessary to send highly sensitive data by e-mail, PGP will be used. Network file transfers will be considered to be similar to e-mail for these purposes: sensitive data should be encrypted for transmission.

Where it is necessary to establish trust, for example before relying on information given to the CERT.LV, or before disclosing confidential information, the identity and bona fide of the other party will be ascertained to a reasonable degree of trust. Within constituency, and with known neighbour sites,

referrals from known trusted people will suffice to identify someone. Otherwise, appropriate methods will be used, such as a search of FIRST members or Trusted Introducer data base, the use of WHOIS and other Internet registration information, etc. along with telephone call-back or e-mail mail-back to ensure that the party is not an impostor. Incoming e-mail whose data must be trusted will be checked with the originator personally or by means of digital signatures (PGP in particular).
Signal groups and Mattermost channels are also used to exchange information and are considered more secure than plain text email. Members of such groups are authorised by their institutions prior to adding them to the groups.

4.4 Information handling

Information is stored according to the following procedure:

- in paper form – it is stored in dedicated folders/safe (depending on classification) in the CERT.LV premises which are protected with electronic door cards;
- in electronic form – it is stored on CERT.LV servers and workstations, protected with all normal security measures.

Information is archived according to the following procedure:

- in paper form – it is archived in dedicated folders/safe (depending on classification) in the CERT.LV premises which are protected with electronic door cards;
- in electronic form – it is archived on CERT.LV servers, protected with all normal security measures.

Information is destructed according to the following procedure:

- in paper form – it is destructed in the shredder;
- in electronic form – it is destructed by deleting and overwriting using special software.

5. Services

CERT.LV offers wide range of services to its constituency. The services can be grouped into the following categories:

- Daily protection of constituency;
- Testing, i.e., services aimed to provide necessary help in identifying of the vulnerabilities, protecting and securing constituency networks and ICT environment to mitigate risk of possible attacks;
- educational services, i.e., awareness raising, training, seminars and coferences.

All above mentioned services are provided free of charge.
Below services are listed based on the FIRST Services framework (https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2-1).

5.1 Daily protection services

5.1.1 Incident Response

CERT.LV offers all services from service area Information Security Incident Management, including:

- Information security incident report acceptance
- Information security incidents analysis
- Artifact and forensic evidence analysis
- Mitigation and recovery
- Information security incident coordination
- Crisis management support

5.1.2 Information Security Event Management

- Monitoring and detection :
  - - Early Warning Sensor (ABS) service (sensor networks) for network monitoring;
  - Security Operation Center (SOC) Service based on EDR/XDR technology and deployed on constiutents end point devices;
- Event analysis and DNS firewall services. DNS Firewall using DNS RPZ technology, available to all internet users in Latvia. More information https://dnsmuris.lv/.

5.1.3 Situational Awareness

CERT.LV offers all services from service area Situational Awareness, including:

- Data acquisition,
- Analysis and synthesis,
- Communication,
- Incident statistics. Records of security incidents handled will be kept. While the records will remain confidential, periodic statistical reports are made available on-line.

5.2 Testing (Prevention)

5.2.1 ICT security testing (penetration testing)

Security testing of ICT resources and systems to identify potential vulnerabilities, security threats, and system weaknesses to prevent possible cyberattacks and data leaks.

5.2.2 Cybersecurity threat hunt

CERT.LV, individually and together with a joint team of cooperation partners, operates in a pre-selected information system network (the selection of the target institution is evaluated in cooperation with state security institutions) to identify the presence of the attacker, detect, monitor and analyze malicious actions, as well as to analyze attack tactics, techniques and procedures.

5.2.3 Cyberthreat simulation

With the help of the CERT.LV service, organizations can simulate customized and realistic phishing attacks to train employees and enhance personnel's abilities to identify potentially risky behavior patterns and recognize and prevent cyber threats and information leaks.

5.2.4 Phishing simulation management

CERT.LV offers simulation of cyberattack tools, methods and actions to test and improve an institution's threat identification capabilities. Vulnerability management

CERT.LV offers all services from service area Vulnerability Management, including:

- Vulnerability discovery / research
- Vulnerability report intake
- Vulnerability analysis
- Vulnerability coordination
- Vulnerability disclosure
- Vulnerability response

Maintaining a vulnerability reporting platform https://cvd.cert.lv/.

5.3 Knowledge Transfer

CERT.LV offers Knowledge Transfer services for its constituency.

5.3.1 Awareness building

- Lectures/presentations on cybersecurity topics for different constituencies;
- organisation of seminars on various security related issues;
- active information sharing in social media (on Facebook, X, LinkedIn);
- dissemination of security related materials in mass media;
- preparing brochures and posters for the constituency on cybersecurity related topics.

5.3.2 Training and education

- Presentations on cybersecurity related topics for state and governmental institutions, as well as for other primary constituents.
- Participation in various events that are promoting cybersecurity, e.g., Safer Internet Day, E-skills Week, European Cyber Security Month;
- Organisation of the annual security conference “Kiberšahs”/”Cybershock”
- organisation of bi-annual seminars for IT security professionals “Be safe”.

5.3.3 Exercises

CERT. LV Participation in EU, NATO and LV cybersecurity exercises.

5.3.4 Technical and policy advisor

- Maintenance of websites www.cert.lv (official website) and www.esidross.lv (for general public);
- Participation in public discussions on cybersecurity related subjects
- organisation of security specialists’ meetings and discussions;
- joining organizations that promote cybersecurity;
- Reccomendations for vulnerability avoidance;
- Advice to constituency regarding implementation of ISMS (Information security management systems) measures;

5.4 Other services

The CERT.LV coordinates and maintains the following other services :

- NTP Stratum - 1 level time clock service;
- OT (operational technologies) security testing lab.

6. Incident Reporting Forms

Significant cybersecurity incidents must be reported using the forms adopted by the Cabinet of Ministers Rules 02.07.2025, No 397 on the “Minimum Cybersecurity Requirements”. The notification forms must be electronically filled and signed by secured electronic signature, and must be sent to CERT.LV e-mail (cert@cert.lv).

There are no special forms required to report a cybersecurity incident which does not qualify as significant cybersecurity incident. The notification must be provided in free form and must be sent to CERT.LV e-mail (cert@cert.lv).

7. Disclaimers

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