NRD Cyber Security

RFC2350 NRD CIRT v3.0

TLP:WHITE

Document information

Project Title:	NRD CIRT		
Report Title:	RFC2350 NRD CIRT		
Version:	V3.0	**Version date:**	2021 09 28
Prepared by:	Vilius Benetis		
Reviewed by:	Marius Urkis		
Contact person:	Marius Urkis		

Information flow

Whom	Action*	Date
Vilius Benetis, Director NRD Cyber Security	Approved	2021 09 28

*Actions: approve, review, inform, other (specify)

Chronology of versions:

Version No.	Date	Comment
3.0	2021-09-30	Updated version
2.0	2017-02-17	Marius Urkis, Updated version
1.1	2014-06-09	Martynas Buožis, Initial version

1 Document information

1.1 Date of Last Update	28 September 2021
1.2 Document location	https://www.nrdcs.lt/cirt
1.3 Document Authentication	PGP signature of the PDF can be found in the page https://www.nrdcs.lt/cirt

2 Contact Information

2.1 Name of the Team	NRD CIRT NRD Computer Incident Response Team
2.2 Address	NRD CS, Gynėjų g. 14, LT-01109, Vilnius, Lithuania
2.3 Time Zone	GMT+2 (Europe/Vilnius)
2.4 Telephone Number	+370 5 2191919, GMT+2
2.5 Facsimile Number	N/A
2.6 Other Telecommunication	N/A
2.7 Electronic Mail Address	cirt@nrdcs.lt
2.8 Public Keys and Other Encryption Information	2048R/0BE6C08E 2014-04-11 NRD CIRT <cirt@nrdcs.lt> Fingerprint=367D 9ABB 301A E05C C106 F49C 1154 3E9E 0BE6 C08E
2.9 Team Members	Team members of NRD CIRT are employees of NRD Cyber Security company (UAB NRD CS). All contact information can be found in the web page of the company https://www.nrdcs.lt.
2.10 Other Information	All contact information about NRD CIRT can be found in the webpage: https://nrdcs.lt/cirt
2.11 Points of Customer Contact	Preferred method for contacting NRD CIRT is via email at cirt@nrdcs.lt, or by using web form for incident reporting https://nrdcs.lt/cirt

3 Charter

3.1 Mission Statement

Mission of NRD CIRT is:

1. To provide cybersecurity incident management-related services to the NRD CIRT constituency.
2. To assist in prompt and proactive cybersecurity risk management, monitoring and compliance with standards and regulations.
3. To assist in identifying, analyzing and mitigation of the impact of security threats.
4. To coordinate exchange of information between law enforcement agencies, corporations and individuals.
5. To ensure monitoring and exchange of information, collaboration with national and international incident response and cybersecurity teams and organizations.

3.2 Constituency

NRD CIRT's constituents are customers of NRD Cyber Security receiving managed security services according to the contracts and agreements.

3.3 Sponsorship and/or Affiliation

All activities of NRD CIRT is funded by NRD Cyber Security.

3.4 Authority

NRD CIRT operates under supervision of director of NRD Cyber Security.

4 Policies

4.1 Types of Incidents and Level of Support

NRD CIRT is authorized to deal with all types of cyber security incidents as specified in the contracts with the customers. Level of support is specified in the contracts as well.

4.2 Co-operation, Interaction and Disclosure of Information

All incoming information is tagged as either a Confidential or Public. To support TLP scheme all incoming information marked as TLP:RED, TLP:AMBER or TLP:GREEN is considered as a Confidential internally. TLP:WHITE marking is tagged as a Public accordingly.

Confidential information can be distributed internally on need-to-know basis according to the business needs and cannot be disclosed to third party persons who are not explicitly authorized to receive the information. It is the responsibility of the employee to take necessary measures in order to avoid unauthorized disclosure of Confidential information. Confidential information can be disclosed to the third parties on NDA basis only and with authorization of the head of the company.

Public information can be released freely without any restrictions.

Incident information can be disclosed according to the stipulations in the service agreements with constituents. All incoming incident related data is considered as Confidential and is handled accordingly.

4.3 Communication and Authentication

PGP is considered as a preferable and secure method to protect information. NRD CIRT has a team key as described in 2.8. Every team member possess personal PGP key in order exchange personal messages in secure manner.

5 Services

5.1 Reactive, proactive and quality management services

Services are organised according FIRST.org CSIRT Services Framework 2.1:

1. Information Security Event Management service
2. Information Security Incident Management service
3. Vulnerability Management service
4. Situational Awareness service
5. Knowledge Transfer service

6 Incident Reporting Forms

6.1 Web form

Incident reporting form is available at the following webpage:

https://nrdcs.lt/cirt

7 Disclaimers

The purpose of this document is to provide a generalized overview of NRD CIRT services.

NRD CIRT services description provided in client contracts might differ from services description provided in this document. Client contracts always take precedence over this document.