NRD CIRT description, according to RFC 2350

Document date:	2017-02-17
Document version:	2.2

Table of contents

1 Document information

Document date	2017-02-17
Version date	2018-01-12
Version	2.2
Document status	Final
Author	Marius Urkis
Reviewer	Gabrielė Tilvikaitė
Review date	2017-02-20
Document location	https://www.nrdcs.lt/en/emergency-assistance/
Document authentication	PGP signature of the PDF can be found in the page https://www.nrdcs.lt/en/emergency-assistance/

Chronology of versions:

Version No.	Date	Reviewed	Description
V.1.1	2014-06-09	Martynas Buožis	Initial version
V.2.0	2017-02-17	Marius Urkis	Major review
V.2.1	2017-02-20	Gabrielė Tilvikaitė	Document review
V.2.2	2018-01-12	Marius Urkis	Reference update

2 Contact Information

2.1 Name of the Team	NRD CIRT NRD Computer Incident Response Team
2.2 Address	Gynėjų g. 14, LT-01109, Vilnius, Lithuania
2.3 Time Zone	GMT+2
2.4 Telephone Number	+370 5 2191919, GMT+2
2.5 Facsimile Number	+370 5 2196533, GMT+2
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 CS company. 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://www.nrdcs.lt/en/contacts/
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://www.nrdcs.lt/en/report-an-incident/ .

3 Charter

3.1 Mission Statement	Mission of NRD CIRT is: • To assist in prompt and proactive cybersecurity risk management, monitoring and compliance with standards and regulations. • To assist in identifying, analyzing and mitigation of the impact of security threats. • To coordinate exchange of information between law enforcement agencies, corporations and individuals. • 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 CS receiving managed security services according to the contract.
3.3 Sponsorship and/or Affiliation	All activities of NRD CIRT is funded by NRD CS.
3.4 Authority	NRD CIRT operates under supervision of director of NRD CS.

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 customer. Level of support is specified in the contract 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 services	• artifact analysis • artifact response • forensic analysis • incident analysis • incident response • incident response support • incident response on-site • incident response coordination

5.2 Proactive Services	• configuration and maintenance of security tools, applications and infrastructures • intrusion detection services • security audits or assessments • security-related information dissemination • technology watch • trend and neighborhood watch
5.3 Quality Management Services	• awareness building • business continuity and disaster recovery planning • education/training • product evaluation or certification • risk analysis • security consulting

6 Incident Reporting Forms

6.1 Web form	Incident reporting form is available at the following webpage: https://www.nrdcs.lt/en/report-an-incident/

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.