

# NRD CIRT description, according to RFC 2350

Document date: 2017-02-17  
Document version: 2.1

## Table of contents

<b>TABLE OF CONTENTS.....</b>	<b>2</b>
<b>1 DOCUMENT INFORMATION .....</b>	<b>3</b>
<b>2 CONTACT INFORMATION.....</b>	<b>4</b>
2.1 Name of the Team.....	4
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 Other Encryption Information.....	4
2.9 Team Members .....	4
2.10 Other Information .....	4
2.11 Points of Customer Contact .....	4
<b>3 CHARTER.....</b>	<b>4</b>
3.1 Mission Statement .....	5
3.2 Constituency.....	5
3.3 Sponsorship and/or Affiliation .....	5
3.4 Authority .....	5
<b>4 POLICIES .....</b>	<b>5</b>
4.1 Types of Incidents and Level of Support .....	5
4.2 Co-operation, Interaction and Disclosure of Information.....	6
4.3 Communication and Authentication.....	6
<b>5 SERVICES.....</b>	<b>6</b>
5.1 Reactive services .....	6
5.2 Proactive Services.....	7
5.3 Quality Management Services .....	7
<b>6 INCIDENT REPORTING FORMS .....</b>	<b>7</b>
6.1 Web form .....	7
<b>7 DISCLAIMERS .....</b>	<b>7</b>

## 1 Document information

<b>Document date</b>	2017-02-17
<b>Version date</b>	2017-02-24
<b>Version</b>	2.1
<b>Document status</b>	Final
<b>Author</b>	Marius Urkis
<b>Reviewer</b>	Gabrielė Tilvikaitė
<b>Review date</b>	2017-02-20
<b>Document location</b>	<a href="https://nrdcs.lt/RFC-2350-NRD-CIRT-979.html">https://nrdcs.lt/RFC-2350-NRD-CIRT-979.html</a>
<b>Document authentication</b>	PGP signature of the PDF can be found in the page <a href="https://nrdcs.lt/RFC-2350-NRD-CIRT-979.html">https://nrdcs.lt/RFC-2350-NRD-CIRT-979.html</a>

Chronology of versions:

Version No.	Date	Reviewed	Description
<b>V.1.1</b>	2014-06-09	Martynas Buožis	Initial version
<b>V.2.0</b>	2017-02-17	Marius Urkis	Major review
<b>V.2.1</b>	2017-02-20	Gabrielė Tilvikaitė	Document review

---

## 2 Contact Information

---

<b>2.1 Name of the Team</b>	NRD CIRT NRD Computer Incident Response Team
<b>2.2 Address</b>	Gynėjų g. 16, LT-01109, Vilnius, Lithuania
<b>2.3 Time Zone</b>	GMT+2
<b>2.4 Telephone Number</b>	+370 5 2191919, GMT+2
<b>2.5 Facsimile Number</b>	+370 5 2196533, GMT+2
<b>2.6 Other Telecommunication</b>	N/A
<b>2.7 Electronic Mail Address</b>	cirt@nrdfs.lt
<b>2.8 Public Keys and Other Encryption Information</b>	2048R/ <a href="#">0BE6C08E</a> 2014-04-11 NRD CIRT <cirt@nrdfs.lt>  Fingerprint=367D 9ABB 301A E05C C106 F49C 1154 3E9E 0BE6 C08E
<b>2.9 Team Members</b>	Team members of NRD CIRT are employees of NRD CS company. All contact information can be found in the web page of the company <a href="https://www.nrdfs.lt">https://www.nrdfs.lt</a> .
<b>2.10 Other Information</b>	All contact information about NRD CIRT can be found in the webpage:  <a href="https://nrdfs.lt/NRD-CIRT-contact-information-947.html">https://nrdfs.lt/NRD-CIRT-contact-information-947.html</a>
<b>2.11 Points of Customer Contact</b>	Preferred method for contacting NRD CIRT is via email at <a href="mailto:cirt@nrdfs.lt">cirt@nrdfs.lt</a> , or by using web form for incident reporting <a href="https://nrdfs.lt/Report-incident-948.html">https://nrdfs.lt/Report-incident-948.html</a> .

---

## 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://nrdfs.lt/Report-incident-948.html>

---

# 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.

---