1. About this document

This document describes the computer security incident response (CSIRT) functions of the National Cyber Security Centre of Lithuania (NKSC/CERT-LT) in accordance with RFC 2350.

1.1 Date of Last Update

This is version 1.0, published on March 13 2018.

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 NKSC/CERT-LT description document is available https://www.nksc.lt/en/contacts.html.

1.4 Authenticating this Document

Both English and Lithuanian versions of this document have been signed with NKSC/CERT-LT's GPG key, which is available at https://www.nksc.lt/NCSC-LT.asc.

2. Contact Information

2.1 Name of the Team

Since 1 January 2018, the team name has been **The National Cyber Security Centre of Lithuania,** abbreviated **NKSC/CERT-LT**

CERT-LT (National CERT) and NKSC (National Cyber Security Center) were reorganized into a new body - **The National Cyber Security Centre under Ministry of National Defence of Lithuania**

2.2 Address

Visiting and postal address is:
National Cyber Security Centre under the Ministry of National Defence.
Gedimino str. 40, Vilnius, Lithuania. Postal code is LT-01110.

2.3 Time Zone

-EET, Eastern European Time (UTC+2, between last Sunday in October and last Sunday in March)
-EEST, Eastern European Summer Time (UTC+3, between last Sunday in March and last Sunday in October)

2.4 Telephone Number

+370 706 82 250

2.5 Facsimile Number

+370 5 212 5100 (this is not a secure fax).

2.6 Other Telecommunication

Not available.

2.7 Electronic Mail Address

<cert (at) cert.lt> This e-mail forwards information to the specialists on duty at NKSC/CERT-LT.

Information on other e-mail addresses can be found at NKSC/CERT-LT web site https://www.nksc.lt/en/contacts.html.

2.8 Public Keys and Other Encryption Information

NKSC/CERT-LT has a GPG key, whose KeyID is 0xA3BACE47 and whose fingerprint is

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.10 (GNU/Linux)

mQGiBEjYp60RBACOsRsfqkDpDq3jrAlTBz+oAf05ohNXokqnYTRvIHDeRGiEMGZS
ss7G4zA88RT7OtI3uZtWfhH8vlul5FqNUx5xNIKwVseVrwZuRZ347sbeKvFUtmVG
2jqUIN0Cj0jXKf0gO58MZaxs4hdgyjGU1/f6ZfQk/W+nFouXSOlAu8EqfwCgt3Bv
IH3wkmymt7F0vwps6iTTN1MD/jWlBKY9OgXgVatA/dTu1tkfMtMmxdqRXs1ZZqJG
6PbLlkCVwTSpxuX0Ysig6ZcZlFLL8NJR+kA3DdbCzfgN2xS0ED9LgTJmBUJwTgJ1
NjtdutFtg/8JlE1kp1fiiqCjlmWaxH+szwvT5Zc0QzuYAclpYMJxxAdp+dtsrZbv
ZDpkA/9TEvJJj3dyXzxE4uu1bvR2fOu0z242j+7zBKawu/mx9bmRRJTwyg71HpH2
ZnuA70vxV9bCk+ApT2r4r8RmfaYTZvQAkYNFhViZlp1DoFRMJ3tpbVsi9zD9nbDU
JGs/ds0I3t3OFYXw9WjvJPn1bMbZ1E9zNn1chboOq5SHmRhVY7Q6Q0VSVC1MVCAo
Q0VSVCBvZiB0aGUgUmVwdWJsaWMgb2YgTGl0aHVhbmlhKSA8Y2VydEBjZXJ0Lmx0
PohgBBMRAgAgBQJI2KetAhsjBgsJCAcDAgQVAggDBBYCAwECHgECF4AACgkQwROr
cKO6zkertACfS7TT4g3VQ2vEmneDj/0u3W4S7R8AoJSyq+1IXBqbjuw8goMNzZaN
eqAEiEYEEBECAAYFAkjYqAoACgkQLf0IUkC0ubqcBQCfQIveU6ozEI+pZ4ONe5gt
d9hzGA4AoIvfbqhBgs54Wygw8mQmZFweuipJiEYEEBECAAYFAkjYqEIACgkQDDQ9
8HFvaduRHwCgo1Yb2oOxDqXwvuVBbt1p6UqwAI8An2Ey6Z9tYYUM0ZQfPCOF/IwR
w4/giEYEEBECAAYFAkjYqNoACgkQs+9+bc/XFvObwACghc9p8LQdVaNMwWrfJb3m
bHtPfXwAnR+bMXIJd66zK/vMqDgc+XAa5rfsuQINBEjYp60QCAC91zROnCuEkJ4J
gNLg/ekdo3dEv4R5cSl4RV1peWK/tixvjFGgTLe8gDVT959MzvBio6lu76gfuhWP
mmWdGF4AgIFCPGfAKQRnGIR9QUrNTmRPWMKWWvJZ7W4m+ZebVIC3DDEc0BBkw/0g
AHRfBACn2+DcYTIJqKca/FVUpSXOZWA8gnhc+zj9ZrT1ex+txiJQSPh2Edi/yCYN
ozCWj7MsMlrai1+TSgeUhxBf79BD1Yy+wVlQK7yhlyv9b0gaF52MJN3YMskz1f6z
ESGbQLYRMGZu6w2g7XTQVWbDaSOLu6TAhnCYg377pBJrGufFgR+G1jGDyJJZvIm3
N/Zd5/zHAAMFCAC1dQLFduh3lNfKzH7Sb9FfFDbm/6tCdSxOrcil0UPUA32gCXpf
i24FCe4FfvVk8bd373OYxCDxDAgaB56RWLwACfdmEqhLr8g6tmEyfxFWZG51mM4D
vP3TtIDtB/OEPFufoHajDkMd438mryyTJF4DCEuXI10fGPhkO15UGs/o6ZXVrKG1
Ay5wt3vGndaiH4xvrhm8tdVefuD2mwGTZxCzNZXakmwMyGxbqs86tsA4VUjIVu/B
Ft83fF92Vqfyhmj/qfNQPYiOE2nbcd6HCUfr3BhfXls8TjRXm0tGcTjb5DOG/4Xc
oL4IreRGKigGVlYtBiAN2KBGLXyfKTnmk5FTiEkEGBECAAkFAkjYp60CGwwACgkQ
wROrcKO6zkfcmACgrPNOZahNFgkegx1HgjiHa9YzL5EAoIf+nuC1OEReCG38uJNK
WFbEhVIK
=eyrO
-----END PGP PUBLIC KEY BLOCK-----

2.9 Team Members

Information on NKSC/CERT-LT members is available upon request.

2.10 Other Information

General information about NKSC/CERT-LT can be found at https://www.nksc.lt/en/

NKSC/CERT-LT Facebook page (mostly in Lithuanian): https://www.facebook.com/NKSC.LT
NKSC/CERT-LT Twitter profile (mostly in Lithuanian): https://twitter.com/cert_lt

2.11 Points of Customer Contact

The preferred method for contacting NKSC/CERT-LT is via e-mail cert (at) cert. If it is not possible (or not advisable for security reasons) to use e-mail, NKSC/CERT-LT can be reached by telephone during regular office hours. NKSC/CERT-LT 's hours of operation are generally restricted to regular business hours (08:00-17:00 on Monday to Thursday, 08:00-15:45 on Friday except Lithuanian holidays).

If the case is important duty officer is available 24/7 by telephone and e-mail.

3. Charter

3.1 Mission Statement

NKSC/CERT-LT mission: to be the centre of cyber security expertise for the effective management of cyber security incidents and the creation of strong cyber security prevention system in the country.

3.2 Constituency

The NKSC/CERT-LT's constituency are IP addresses of Lithuania and all resources with TLD .lt.

NKSC/CERT-LT is a single point of contact for foreign CERTs/CSIRTs, as the national CERT.

NKSC/CERT-LT welcomes all incident reports or vulnerabilities of significance to Lithuanian interests ,

3.3 Sponsorship and/or Affiliation

National Cyber Security Centre under the Ministry of National Defence (NKSC/CERT-LT) is Lithuanian institution, responsible for unified management of cyber security incidents, monitoring and control of the implementation of cyber security requirements, accreditation of information resources.

NKSC/CERT-LT is affiliated with FIRST, the global Forum of Incident Response and Security Team, as well as GÉANT and TI (Trusted Introducer for European CERTs)

3.4 Authority

The main purpose of NKSC/CERT-LT in incident handling is the coordination of incident response.

The applicable laws with duties of NKSC/CERT-LT are as follows:
- Law on Cybersecurity (12/11/2015, No. XII-1428, not available in English)
- Government Resolution on National cyber incidents handling plan (01/25/2016, No. 87, not available in English).

4. Policies

4.1 Types of Incidents and Level of Support

The NKSC/CERT-LT is authorized to address all types of computer security incidents, which occur, or threaten to occur in our constituency. The level of support that is given by NKSC/CERT-LT will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and the NKSC/CERT-LT 's resources at the time, though in all cases some response will be made within one working day.

4.2 Co-operation, Interaction and Disclosure of Information

- NKSC/CERT-LT highly regards the importance of operational cooperation and information sharing between CSIRTs and NCSCs, and also with other organizations which may contribute towards or make use of their services;

- We ensure the protection of confidential information received at the time of the investigation of security incidents and/or prevention of breaches of integrity and unauthorized disclosure of such information, also, that this information is not disclosed, copied or used for any other purposes, which could result in adverse consequences to a person having provided the confidential information, except for cases where obligation is enforced by law.

NKSC/CERT-LT understands the Traffic Light Protocol (TLP) for sharing sensitive information.

4.3 Communication and Authentication

Unencrypted e-mail will not be considered particularly secure, but will be sufficient for the transmission of low-sensitivity data. If it is necessary to send highly sensitive data via e-mail, GPG should be used. Network file transfers will be considered to be similar to e-mail for these purposes: sensitive data should be encrypted before or during the transmission.

5. Services

5.1 Incident Response

NKSC/CERT-LT will assist its constituency in handling the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management.

5.1.1 Incident Triage

- Investigating whether an incident occurred.
- Determining the extent of the incident.

5.1.2 Incident Coordination

- Determining and contacting the involved organizations.
- Asking for reports, depending on incident type and severity.
- Determining the initial cause of the incident (vulnerability exploited).
- Facilitating contact with other parties which may be involved, including law enforcement, if needed.
- Composing announcements to users/ stakeholders, if applicable.
- Communicating with media, if necessary.

5.1.3 Incident Resolution

Advise local security teams on appropriate actions
- Ask for reports
- Report back
- Collection of evidence after the fact
- Evaluating whether the results will be aimed at an eventual prosecution or disciplinary action. In addition, NKSC/CERT-LT will collect statistics concerning incidents, which occur within constituency, and will notify the community as necessary to assist it in protecting against known attacks.

Owners of the said systems hold the responsibility to operate the systems in a secure manner and resolve incidents remains at all times. L I QA-ACPR+J R also checks whether the incident was really resolved and keep corresponding records.

5.2 Activities

Available reactive services: - Alerts, warnings, sharing of information - Incident handling - Incident analysis	Available proactive services: - Announcements - Adoption of security tools - Security awareness raising.

- Incident response on site - Incident coordination.	- Education and training
6. Incident Reporting Forms	
Incident Reporting Form is available at https://www.nksc.lt/en/report.html.	
7. Disclaimers	
While every precaution will be taken in the preparation of information, notifications and alerts, NKSC/CERT-LT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.	