1. Document Information

This document contains a description NCZI CSIRT according to RFC 2350. It provides basic information about the NCZI CSIRT, the ways it can be contacted, describes its responsibilities and the services offered.

1.1 Date of Last Update

This is version 1.0 published on July 30, 2024.

1.2 Distribution List for Notifications

This profile is kept up to date on the location specified in the chapter 1.3. E-mail notifications of updates are sent to all NCZI CSIRT members.
Any specific questions or remarks please address to the NCZI CSIRT mail address.

1.3 Locations where this Document May Be Found

The current version of this document can always be found at https://csirt.nczisk.sk/rfc2350.txt

2. Contact Information

2.1 Name of the Team

NCZI CSIRT: Computer Security Incident Response Team of NCZI

2.2 Address

Národné centrum zdravotníckych informácií (NCZI)
Lazaretská 26

811 09 Bratislava 1
Slovakia

2.3 Time Zone

CET, Central European Time (UTC+1, from the last Sunday in October to the last Saturday in March)
CEST, Central European Summer Time (UTC+2, from the last Sunday in March to the last Saturday in October)

2.4 Telephone Number

+421 911 869 943

2.5 Other Telecommunication

Not available at present time.

2.6 Electronic Mail Address

Official e-mail address for non-incident related messages: csirt@nczisk.sk
Address assigned for incident reporting: incident@nczisk.sk

2.7 Public Keys and Encryption Information

For the incident related communication, you may use this key:

```
pub 4096R/0xE4480B4B0284F2B2
uid CSIRT NCZI 2023 <csirt@nczisk.sk>

key fingerprint =  E005 2547 17C9 17AB 78AA 3343 E448 0B4B 0284 F2B2
```

2.8 Team Members

A full list of NCZI CSIRT team members is not publicly available. Team members will identify themselves to the reporting party with their full name in an official communication when handling an incident, providing support or similar action.

2.9 OTHER INFORMATION

General information about the NCZI CSIRT can be found at https://csirt.nczisk.sk.

2.10 Contact Information

The preferred method for contacting NCZI CSIRT is via e-mail.

Incident reports and related issues should be sent to the address incident@nczisk.sk. This action will create a ticket in our tracking system.
In case of reporting incident outside of working hours also contact the person on duty at +421 911 869 943

.
For general questions use the e-mail address csirt@nczisk.sk.

If it's not possible to use e-mail, you can reach out via telephone at +421 911 869 943.

The NCZI CSIRT hours of operation are generally restricted to regular business hours (08:00 - 16:00 Monday to Friday, except holidays).

3. Charter

3.1 Mission Statement

NCZI CSIRT's mission is to coordinate and operate activities related to IT security issues for the audience defined in chapter 3.2.

3.2 Constituency

NCZI CSIRT provides its services to its home organization and the national health information system managed by NCZI.

3.3 Sponsorship and/or Affiliation

NCZI CSIRT is part of National Health Information Centre (NCZI). National Health Information Centre (NCZI) is a state-funded organization founded by the Ministry of Health of the Slovak Republic.

NCZI performs tasks in the area of informatisation of health service, administration of the National Health Information System, standardisation of health informatics, health statistics and provision of library and information services in the field of medical sciences and health service. It administrates national health registries and national health administrative registries as well.

At international level, NCZI collaborates with WHO, OECD, EUROSTAT and EMCDDA.

3.4 Authority

NCZI CSIRT as a part of National Health Information Centre operates with authority delegated by the law č. 153/2013 Z. z. o národnom zdravotníckom informačnom systéme a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (law about NCZI) and within the bounds of the Slovak legislation.

NCZI CSIRT expects to work cooperatively with administrators and users within its consitituency.

4. Policies

4.1 Types of Incidents and Level of Support

The NCZI CSIRT is authorized to address all types of computer security incidents which occur, or threaten to occur, in its constituency.

The level of support given by NCZI CSIRT 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 NCZI CSIRT's resources at the time, though in all cases some response will be made within one working day.

Note that no direct support will be given to end users; they are expected to contact their system administrator, network administrator or their ISP for assistance.
NCZI CSIRT is committed to its proactive and reactive services provided to its constituency.

4.2 Co-operation, Interaction and Disclosure of Information

All incoming information is handled confidentially by NCZI CSIRT, regardless of its priority. Information that is evidently very sensitive in nature is only communicated and stored in a secure environment, if necessary using encryption technologies.

NCZI CSIRT will use the information you provide to help solve security incidents. Information will only be distributed further to other teams and members on a need-to-know basis, and preferably in an anonymized fashion.
The NCZI CSIRT operates within the bounds of the Slovak legislation.

4.3 Communication and Authentication

E-mails and telephones are considered sufficiently secure to be used even unencrypted for the transmission of low-sensitivity data. If it’s necessary to send highly sensitive data by e-mail, PGP will be used.

If it is necessary to authenticate a person before communicating, this can be done either through existing webs of trust (e.g. TI, FIRST) or by other methods like call-back, mail-back or even face-to-face meeting if necessary.

5. Services

5.1 Incident Response

NCZI CSIRT will assist local administrators 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

- Determining whether an incident is authentic.
- Determining the extent of the incident, and its severity.

5.1.2. INCIDENT COORDINATION

- Contact the involved parties to investigate the incident and take the appropriate steps.
- Facilitate contact to other parties which can help resolve the incident.
- Making reports to other CERT® teams or CSIRTs if needed.
- Communicate with stakeholders.

5.1.3. INCIDENT RESOLUTION

- Providing advice to the local security teams and administrators on appropriate actions.
- Follow up on the progress of the local security teams and administrators concerned.
- Provide assistance in evidence collection and data interpretation.

In addition, NCZI CSIRT may collect statistics concerning incidents which occur within or involve its constituency and will notify the community as necessary to assist it in protecting against known attacks.

5.2 Proactive Activities

NCZI CSIRT performs vulnerability management and takes advantage of cyber threat intelligence.
NCZI CSIRT is in contact with IT security personnel of their constituency to raise the security awareness.
NCZI CSIRT takes part in information security related activities on a national and European level.

6. INCIDENT REPORTING FORMS

The form is available on our website https://csirt.nczisk.sk/incident_form.txt / No specific requirements.

7. Disclaimers

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