CSIRT Description for NSZW CERT (English version)

==========

## 1. About this document

This document contains a description of NSZW CERT according to RFC 2350.

It provides basic information about the CERT, 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 2020/05/22.

### 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 document can be found at:

http://www.nszw.pl/soc

### 1.4 Authenticating this Document

This document includes NSZW CERT PGP signature. See section 2.8 for more details.

## 2. Contact Information

### 2.1 Name of the Team

"NSZW CERT": Cybersecurity Incident Response Team - called as NSZW SOC

### 2.2 Address

NSZW SOC

ul. Fieldorfa 2, 54-049 Wrocław, Poland

### 2.3 Time Zone

Central European Time (GMT+0100, GMT+0200 from April to October)

**2.4 Telephone Number**

+48 71 306 4002

**2.5 Facsimile Number**

+48 71 7359 300

**2.6 Other Telecommunication**

None available.

**2.7 Electronic Mail Address**

it@nszw.pl

**2.8 Public Keys and Other Encryption Information**

NSZW CERT uses the PGP key:

Fingerprint: 06DE 9DC6 573C A263 198A 798B EA32 55A5 D4B0 CB61

The public key can be found at our website:

http://www.nszw.pl/soc

**2.9 Team members**

Team SOC NSZW consists of IT security experts.

**2.10 Other Information**

More information about SOC NSZW can be found at

https://www.nszw.pl/soc

**2.11 Points of Customer Contact**

NSZW SOC prefers e-mail contact.

Regular cases:

Business hours response only: 08:00-16:00 local time on Monday-Friday save public holidays in Poland.

Emergency cases:

Use NSZW SOC phone number with back-up of e-mail for all detail.

The NSZW SOC phone number is available at all times.

## 3. Charter

### 3.1 Mission Statement

The main purpose of the SOC NSZW is taking actions to minimize the probability of occurrence of cyber security incidents, as well as minimizing the effect of their occurrence in constituency.

Contribute to the national cybersecurity efforts.

### 3.2 Constituency

SOC NSZW provides cybersecurity incident management for customers

### 3.3 Sponsorship and/or Affiliation

NSZW SOC is an internal unit of NSZW Sp. z o.o.

It is financed by NSZW Sp. z o.o.

### 3.4 Authority

SOC NSZW operates under the auspices of, and with authority delegated by, the management of NSZW Sp. z o.o. and is bound by its internal terms. SOC NSZW handles and coordinates incidents on behalf of NSZW Sp. z o.o. and its clients.

## 4. Policies

### 4.1 Types of Incidents and Level of Support

SOC NSZW is authorized to address all types of computer security incidents which occur, or threaten to occur in the scope of services provided. All types of incidents, level of support are defined in Policy of Management for Incidents for NSZW Sp. z o.o.

The level of support given by NSZW SOC varies depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and the availability of NSZW's resources at the time.

Incidents will be prioritized according to their severity and extent.

### 4.2 Co-operation, Interaction and Disclosure of Information

NSZW SOC exchanges all necessary to cooperation information with other CSIRTs, as well as with affected parties administrators. No personally identifying information is exchanged, unless explicitly authorized. All information related to incidents handled is considered Confidential. All sensitive data (such as personal data, system configurations, known vulnerabilities, etc.) are encrypted, if they must be transmitted over unsecured environment.

Information submitted to NSZW SOC may be distributed on a need-to-know basis to trusted parties (such as ISPs, other CERT teams) for the sole purpose of incident handling.

### 4.3 Communication and Authentication

NSZW SOC is bound to obey regulations and policies enforced in Poland and EU covering sensitive information handling.

Any e-mail communication should be tagged using TLP standards. Low-sensitivity data can be sent via unencrypted e-mail, however it's not considered secure. PGP encryption is recommended, especially for sensitive data.

## 5. Services

### 5.1 Incident Response

NSZW SOC will assist NSZW Sp. z o.o. in handling the technical and organizational aspects of security incidents. NSZW CERT capabilities cover the full cycle of incident response:

- handling
- managing
- resolving
- mitigating

#### 5.1.1 Incident Triage

Service involves:

- Prioritizing incident according to its apparent severity and extent,
- Investigating whether indeed an incident occurred,
- Determining the extent of the incident.

#### 5.1.2 Incident Coordination

- Determining the initial cause of the incident (vulnerability exploited).
- Facilitating contact with other sites which may be involved.
- Contact with CSIRT NASK and/or appropriate law enforcement officials, if necessary.
- Making reports to other CSIRTs.
- Composing announcements to users, if applicable.

### 5.1.3 Incident Resolution

- Advise and coordination local teams on appropriate actions,
- Follow up on the progress of the concerned involved local team,
- Ask for reports,
- Report back.

### 5.2 Proactive Activities

NSZW SOC makes an efforts to enhance constituents immunity to security incidents and to limit the impact of incidents that occur.

## 6. Incident Reporting Forms

Mentioned above Policy of Management for Cybersecurity Incidents for NSZW Sp. z o.o. defines also information set needed for reporting the incidents, but you can directly use the e-mail contact with proper information when needed.

In case of emergency or crisis, please provide to NSZW SOC at least the following information:

Contact details and organizational information: name of person and organization name and address, email address, telephone number, IP address(es), FQDN(s), and any other relevant technical element with associated observation; Scanning results (if any) and/or any extract from the log showing the problem.

## 7. Disclaimers

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

-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBF7LaGcBDACkVss+KRxSHDJuY49YNj1a03cQPWVkT6CQLkgJQLWBFx06mUcj
JK0w92CY69SbibRTUB5+CLvhipvdJElAT5h/jwTXV7Kwoqu7v1UmVTk+54aPGbfb
PIUj+q9UBCOrVEC/o3ZnOfdoYukY5e0Z82FkmDCCudzmQfKxFdaQOIrCr+epwyaQ
L4g8jkSBn1LQ6RJjfjiWmcyWSELq1cjUI1qb8jqmLyojBHw+uUktgq6baj6c4lpf
pEnjVh9b97zQ1HrCrRM+JJdq4Z7u1rFr+Q7/4VGKchYRVAKXvY9hD0Vswc+5Ht54
VIlcmoVJv2BvmerKOG+prZfvC9nliYiwpdSVI3ZKB0dxuLrZfdXXzTsVIO+qtIuj
ahnwz40Pvw4JiOXA4IVrtjzbO/ZB6M0Nq1gHuImzGQDm+wjHUIrdPevZSZ87alDW
Vewt5NHcn0PKVs0PmHtO8oW0XGl+Fu8BVY2otL5aQ7WxpoFMfDmPpBnMlrl/+QZW
MmZ10ziyIa+uUZ0AEQEAAbQcTnN6dyBTcC4geiBvLm8uIDxpdEBuc3p3LnBsPokB
1AQTAQgAPhYhBAbencZXPKJjGYp5i+oyVaXUsMthBQJey2hnAhsDBQkILw45BQsJ
CAcCBhUKCQgLAgQWAgMBAh4BAheAAAoJEOoyVaXUsMthUtML/AoRUkFPczf7hBpm
QlLTDp1zph+L4ixGPtcVWYB5dTHBIzDb58uDDwQhdhmqmjXEabxngjZKMiejd18T
+qaOegDdkt404c9zxGJidHUcSveWKO061k8etrO1C7spHh92RRwTfUCUaDGgzaGQ
b0GP2uMNXkHjYu9sUPly+OgMqypZoK4nYnpLFn5E1+FHYJjFJbTiUV4jA9NQNTid
b5/yFSLY6AgQvfnzjdHhfjh2dp0MwJmg4MbahPlz4l+D81ng12F7unaTlb9BHkQd
GOCIve0Wbj/9VozVxbM4uhew9c8XvLn3oU1jVjB8eWE3UqyWscKOvH0ju3M35smV
/ZF4CnN6buj5YTTLBNlA5jCVxu6UiARDECVZkutNTWDr71H6HOepPUEgylGu0KkW
y6aaUaI6Qym0UZddus7vGopFKt5fvw2hM50wZv7N1tNnlptt0iOZHyHNzSfDAinp
Le19Ek8To0v2N1S43tZvcZ0+P+yCcPVUMj43ZGRDh37H4ni1krkBjQRey2hnAQwA
vYWtv2GvRodrg0JFUU7c4iqKauhpb66kz07WdykVEV4Uu9jRDJjcqsVW51OsTpuE
vaP4l5q9Fy1Iw6A4p2kpxR/Yb9HFohiANWDO9s6FOWquGTBAb1nOzOF9XHVF94VX
ImDvJtpAsec7pm0s95Wlp62tpm4z/t3mCKXNoAbBE3AFXpQTUOnlRVTt9Mjq7CGh
tiE4FQDei1/rU19BSymxjlWIv+sqXiQGbhj017q/NzJINdTKPsQuwoxHPnn5R6GV
mnxFixFDvA85IlchAwKMqJqhTi+PBEisqpw+pdwIujfzlKEl6v+RLoBRAlKifZy0
wLPGRmd2AHgyawYu6t9zqBHDeuM3xoBH5LCaCZVcM5tkG0DQCIfdHZOZjJfOGXBo
+PtRwCo3ZWRAGlqNpoGB/NxNSdh4oh400IB3el9ZjqdtmZSfPWxtlM6eghsetg1y
Kya7lB0bGeXM5SnfqxNGOahDBhRMSzx6yf53myRDEvPVzTbU0wnZ+4I40CHDWo5f
ABEBAAGJAbwEGAEIACYWIQQG3p3GVzyiYxmKeYvqMlWl1LDLYQUCXstoZwIbDAUJ
CC8OOQAKCRDqMlWl1LDLYYq5C/9/sGIEfmlxU79rcAX3jj8BhjeVzLTcC0lvB0x7

idOTHR92HUZ7m4XyAA3UDHZwPuyx746GqAWinhjSKh9HG96V6+AQx07d5a2qCkNw
1QqR7mFGznYsaFzPDds3RD9nBxC1sOxFyen/LLhDFNwHeJSMN1cZ6nk50oxDlt/g
Gr49oZTD6tN+ZF5Vo0IToGxhci9r5mB0A1W23x4hAlAoKNjjJw8VWlsGtiRhGzFO
KNxtSp+ximhcb1nfotGiquhEXm3DZL1IE8Ou/OYgW19tiWnVZYRqaJvrb4qeXteS
mcbmwvt/1Qz5+FC+Ao/u4AoHcMWY6CpjUdY9FbQXhPhqKDsjhdvTsqH7Od3tBYVe
bvSs1MU+vwgwgulCKqgGokHcVBEAa8KQqNWE0oJVH4apyOfmilWHdnd06j3+6WUY
sYr/c0/iiICH4HQBy1fR0v5aD+dQAYPc2P8z3yYFzhEICHK5g0QpEZuxK+Jhnr3w
A7efYOve1NHn4j45XBpGOLhAIM4=
=7MpT
-----END PGP PUBLIC KEY BLOCK-----