CSIRT Szpital Wojewódzki im. M. Kopernika w Koszalinie CERT (English version)

1. About this document

This document contains a description of Hospital M. Copernicus in Koszalin CERT according to RFC 2350 and 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 1.00, published 2021-10-01.

1.2 Distribution list of notifications about changes to the document
Hospital M. Copernicus in Koszalin CERT does not use any distribution list to notify about changes to this document.

1.3 Locations where this Document May Be Found
The current version of this document is available on:
https://www.swk.med.pl/o-szpitalu/cyberbezpieczenstwo

1.4 Authenticating this Document
This document includes Hospital M. Copernicus in Koszalin CERT PGP signature.
More details in chapter 2.8

2. Contact Information

2.1 Name of the Team
"Hospital M. Copernicus in Koszalin CERT": Cybersecurity Incident Response Team – Team SZBI

2.2 Address
Team SZBI
Hospital M. Copernicus in Koszalin
St. Chałubińskiego 7
75-581 Koszalin
Poland

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

2.4 Telephone Number
+48 517 191 373

2.5 Facsimile Number
None available.

2.6 Other Telecommunication
None available.

2.7 Electronic Mail Address
incydent@swk.med.pl

2.8 Public Keys and Other Encryption Information
Team SZBI uses the PGP key:
User ID: SWK Zespół SZBI
Email: pelnomocnik.szbi@swk.med.pl
Key ID: 0BAD8B5C
Key size: 4096
Key type: RSA
Fingerprint: 0D13 2045 1E79 4251 87C4 BFA2 86BE A4F3 0BAD 8B5C

This key can be received directly from our website:
https://www.swk.med.pl/o-szpitalu/cyberbezpieczenstwo

2.9 Team members

The ISMS team consists of experts in the field of Cybersecurity issues.

2.10 Other Information

General information about Hospital M. Copernicus in Koszalin can be found at https://www.swk.med.pl

2.11 Points of Customer Contact

Team SZBI prefers e-mail contact.
Please use our cryptographic key above to ensure integrityand confidentiality.
Regular cases:
Contact is possible during business hours: 08:00 – 16:00 local time from Monday to Friday, except for public holidays in Poland.

Incident reports, emergency situations:
Telephone contact with the Team SZBI and / or an e-mail with details provided by telephone.
The phone number of the Team SZBI is available during business hours: 08:00 – 16:00 local time from Monday to Friday, except for public holidays in Poland.

3. Charter

3.1 Mission

Building competence and capabilities of Hospital M. Copernicus in Koszalin in avoiding, Identifying and mitigating the cyber threats.
Contribute to the national cybersecurity efforts.

3.2 Range of activity

Team SZBI provides support in the field of handling cybersecurity events for its patients and clients.

3.3 Sponsorship and/or Affiliation

The operation of the hospital is supervised by Zarząd Województwa Zachodniopomorskiego Region.
The hospital manages its finances in accordance with the principles set out in the applicable provisions of Polish law.

3.4 Authority

The founding body of the hospital is the Samorząd Województwa Zachodniopomorskiego Self-Government, and the Zarząd Województwa Zachodniopomorskiego Management Board supervises its activities.

4. Policies

4.1 Types of Incidents and Level of Support

Team SZBI is authorized to address all types of computer security incidents which occur or threaten to occur in Hospital.
All types of incidents, level of support are defined in Policy of Management for Incidents.
The method of handling incidents depends on the type and severity of the incident or event, the elements affected by the incident, the number of users affected by the incident and the availability of resources. Events are prioritized according to their severity and size.
Incidents will be prioritized according to their severity and extent.

4.2 Co-operation, Interaction and Disclosure of Information

Team SZBI exchanges all necessary information for collaboration with other CSIRTs as well as with stakeholder administrators. No personal data is exchanged except with explicit authorization. All information related to handled incidents is treated as protected. Protected information (such as personal data, system configurations, known vulnerabilities, etc.) is encrypted if it must be transmitted in an insecure environment.
Information sent to Team SZBI may be provided as needed to trusted parties (such as ISPs, other CERT teams) solely for the purpose of incident handling.

Information submitted to Team SZBI 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

Team SZBI uses encryption to ensure the confidentiality and integrity of communication. All sensitive information sent in should be encrypted.

5. Services

5.1 Incident Response

The hospital has established an organizational and technical incident response process. The process includes a complete incident response cycle:
- handling
- - managing
- resolving
- mitigating

5.1.1 Incident Assessment

Incident Assessment includes
- analysis of the impact of the incident on the security of information processed at the Hospital
- prioritization according to the type and severity of the incident
- definition of the scope of the incident
- investigating the causes of the incident

5.1.2 Incident Coordination

Pełnomocnik SZBI is responsible for coordinating the activities, including:
- facilitating contact with other parties that may be involved
- contact with CSIRT NASK and / or, if necessary, with the relevant law enforcement authorities
- creating reports for other CSIRTs

5.1.3 Incident Resolution

Includes:
- alerting the team and coordinating relevant activities
- tracking the progress of work of the team involved
- handling of reporting requests
- presenting reports

5.2 Proactive Activities

Team SZBI 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 information security incident management process is defined by the e-mail (incydent@swk.med.pl) incident reporting channel.
In the incident report, please provide at least the following information to Team SZBI:
- - contact details and organizational information: name and surname, organization name and address, e-mail address, telephone number, IP addresses, domain name and any relevant technical elements and observations
- scan results (if any)
- log extract from the system log (if any)

7. Disclaimers

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