CSIRT Multidisciplinary Hospital - Independent Public Health Care Complex in Zgorzelec CERT (English version)

1. About this document

This document contains a description of Multidisciplinary Hospital - Independent Public Health Care Complex in Zgorzelec 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 2023-04-27.

1.2 Distribution list of notifications about changes to the document

Multidisciplinary Hospital - Independent Public Health Care Complex in Zgorzelec 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.spzoz.zgorzelec/index.php/rodo/cyberbezpieczenstwo

1.4 Authenticating this Document

This document includes Multidisciplinary Hospital - Independent Public Health Care Complex in Zgorzelec CERT PGP signature.
More details in chapter 2.8

2. Contact Information

2.1 Name of the Team

"Multidisciplinary Hospital - Independent Public Health Care Complex in Zgorzelec CERT": Cybersecurity Incident Response Team – Information Security Management Team

2.2 Address

Information Security Management Team
Multidisciplinary Hospital - Independent Public Health Care Complex in Zgorzelec
ul. Lubańska 11-12
59-900 Zgorzelec
Poland

2.3 Time Zone

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

2.4 Telephone Number

608359043 lub 571334972

2.5 Facsimile Number

None available.

2.6 Other Telecommunication

None available.

2.7 Electronic Mail Address

cyberbezpieczenstwo@spzoz.zgorzelec.pl

2.8 Public Keys and Other Encryption Information

Information Security Management Team uses the PGP key:
User ID: WS-SPZOZ w Zgorzelcu Zespół ds. Zarządzania Bezpieczeństwem Informacji
Email: cyberbezpieczenstwo@spzoz.zgorzelec.pl
Key ID: ECE27B76
Key size: 4096
Key type: RSA

This key can be received directly from our website:
https://www.spzoz.zgorzelec.pl/index.php/rodo/cyberbezpieczenstwo

2.9 Team members

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

2.10 Other Information

General information about Multidisciplinary Hospital - Independent Public Health Care Complex in Zgorzelec can be found at
https://www.spzoz.zgorzelec.pl/index.php

2.11 Points of Customer Contact

Information Security Management Team prefers e-mail contact.
Please use our cryptographic key above to ensure integrity and confidentiality.
Regular cases:
Contact is possible during business hours: 07:30 - 15:00 local time from Monday to Friday, except for public holidays in Poland.

Incident reports, emergency situations:
Telephone contact with the Information Security Management Team and / or an e-mail with details provided by telephone.
The phone number of the Information Security Management Team is available during business hours: 07:30 - 15:00 local time from Monday to Friday, except for public holidays in Poland.

3. Charter

3.1 Mission

Building competence and capabilities of Multidisciplinary Hospital - Independent Public Health Care Complex in Zgorzelec in avoiding,
identifying and mitigating the cyber threats.
Contribute to the national cybersecurity efforts.

3.2 Range of activity

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

3.3 Sponsorship and/or Affiliation

The District Office in Zgorzelec supervises the operation of the Hospital.
The hospital conducts financial management on the principles set out in the applicable provisions of Polish law.

3.4 Anchorage

The founding and supervising body of the Hospital is the Poviat Starost in Zgorzelec.

4. Policies

4.1 Types of Incidents and Level of Support

Information Security Management Team 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

Information Security Management Team 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 Information Security Management Team may be provided as needed to trusted parties (such as ISPs, other CERT teams) solely for the purpose of incident handling.

Information submitted to Information Security Management Team 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

Information Security Management Team 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

Chairman of the Information Security Management Team 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

Information Security Management Team makes an efforts to enhance constituents immunity to security incidents
and to limit the impact of incidents that occur.

6. Incident Reporting Forms

The information security incident management process mentioned above is defined by the e-mail (cyberbezpieczenstwo@spzoz.zgorzelec.pl) incident reporting channel.

When reporting an incident, please provide the Information Security Management Team with at least the following information:

- contact details and organizational information: name and surname, organization name and address, e-mail address, telephone number and any relevant technical elements and observations
- IP addresses or domain name (if any)
- scan results (if any)
- extract from the system log register (if any)

7. Disclaimers

All precautions will be taken when preparing information, notifications and alerts.
The Information Security Management Team is not responsible for errors, omissions or damages resulting from the use of the information contained in this document.