CSIRT Szpital Powiatowy in Zawiercie
(English version)

1. Document information

This document contains a description of the CERT Team in Szpital Powiatowy in Zawiercie in accordance with RFC 2350, provides basic information about means of contact and describes the responsibilities of the team and offered services.

1.1 Date of last update
Version 1.00, published on 2024-05-17.

1.2 Notification list for document changes
The CERT Team in Szpital Powiatowy in Zawiercie does not have any distributon list for notifying about changes in this document.

1.3 Locations where this document can be found
The current version of this document can be found at:
www.szpitalzawiercie.pl/RFC-2350-PL – Polish version
www.szpitalzawiercie.pl/RFC-2350-ENG – English version

1.4 Document authenticity
This document has been signed using the Cybersecurity Monitoring Team's PGP key of Szpital Powiatowy in Zawiercie. More details in section 2.8.

2. Contact information

2.1 Team name
Szpital Powiatowy in Zawiercie „Cybersecurity Monitoring Team" – further referred to as „ZMPC Team".

2.2 Address
ZMPC Team
Szpital Powiatowy in Zawiercie
ul. Miodowa 14
42-400 Zawiercie
Poland

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

2.4 Phone number
+48 32 67 40 350

2.5 Fax number
+48 32 67 40 350

2.6 Other communication methods
Unavailable

2.7 E-mail address
incydent@szpitalzawiercie.pl

2.8 Public keys and encryption information
ZMPC Team uses PGP key:
Email: incydent@szpitalzawiercie.pl
Key ID: 51523F730B49F81332DD372E3FB9CAF9904E5A35
Key size: 3072
Algorithm: RSA
Key print: 5152 3F73 0B49 F813 32DD 372E 3FB9 CAF9 904E 5A35
This key can be obtained directly from our website: www.szpitalzawiercie.pl/rfc

2.9 Team members
ZMPC Team consists of experts in cybersecurity issues.

2.10 Other information
General information about Szpital Powiatowy in Zawiercie is available on the website: www.szpitalzawiercie.pl

2.11 Customer contact points
Preferred contact method is e-mail. We recommend using PGP to ensure integrity and confidentiality.

General inquiries:
Contact is possible during working hours: 07:00-14:35 local time from Monday to Friday except for public holidays in Poland.

Incident reports, emergencies:
Contact the ZMPC Team by phone and/or e-mail containing details provided earlier by phone. The ZMPC Team's phone is available during working hours: 07:00-14:35 local time from Monday to Friday except for public holidays in Poland.

3. Policy statement

3.1 Mission
The mission is to build the competencies and capabilities of Szpital Powiatowy in Zawiercie in avoiding, identyfing and mitigating cyber threats. Support for national cybersecurity activities.

3.2 Scope of activity
The ZMPC Team provides support for handling cybersecurity incidents for its patients and clients.

3.3 Funding and affiliation
The activities of the Hospital are handled by Zawiercie County. The Hospital conducts financial management according to the provisions of applicable law in Poland.

3.4. Establishment
The entity creating and supervising the Hospital is Zawiercie county.

4. Incident handling policies

4.1 Types of incidents and support levels

The ZMPC Team is dedicated to handling all types of computer security incidents that occur or may occur in the Hospital's ICT environment. Incident classification and handling methods are defined in the information security incident management process. Handling depends on the type and severity of the incident or event, the number of users affected, and resource availability. Priorities are set for events according to their severity and scale.

4.2 Cooperation, interaction and information disclosure

The ZMPC Team exchanges all necessary cooperation information with other CSIRT teams an administrators of interested parties. No personal data is exchanged unless explicitly authorized. All information related to 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 unsecured environment. Information sent to the ZMPC Team may be shared as needed with trusted parties (such as ISPs, other CERT teams) solely for incident handling purposes.

4.3 Communication and authentication

The ZMPC Team uses encryption to ensure the confidentiality and integrity of communication. All protected data sent should be encrypted.

5. Services

5.1 Incident response

The Hospital has established an organizational and technical incident response process. The process includes the full incident response cycle:

- analysis,
- handling,
- management,
- resolution,
- mitigation.

5.1.1 Incident assessment

Incident assessment includes

- analyzing the impact of the incident on the security of information processed in the Hospital,
- prioritizing according to the type and severity of the incident,
- defining the scope of the incident,
- investigating the causes of the incident.

5.1.2 Incident coordination

Coordination is the responsibility of the ZMPC Team Liaison, including:

- facilitating contact with other involved parties,
- contact with CSIRT NASK and/or appropriate law enforcement if necessary,
- creating reports for other CSIRT Teams.

5.1.3 Incident resolution

Includes:

- notyfing the team and coordinating appropriate actions,
- tracking progress of the involved team,
- handling reporting requests,
- presenting reports.

5.2 Proactive activities

The ZMPC Team conducts actvities aimed at increasing the resilience of the ICT environment to security events and minimizing the potential impact of such events.

6. Incident reporting forms

The aforementioned information security incident management process defines an e-mail (incydent@szpitalzawiercie.pl) for reporting events.

When reporting an incident, please provide at least the following information to the ZMPC Team:

- contact details and information of the organization: name, organization name and address, e-mail address, domain name, and any relevant technical elements and observations,
- scan results (if any),
- system log extracts (if any).

7. Disclaimers

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