Cybersecurity Team for the District Hospital in Zawiercie (English version)

1. Document Information

This document contains information about the Cybersecurity Team for the District Hospital in Zawiercie. It has been prepared according to RFC 2350.

1.1 Date of Last Update

This is version 1.2, published on 11.08.2024.

1.2 Distribution of Notifications About Changes to the Document

The Cybersecurity Team does not use a distribution list.

1.3 Location Where the Document Can Be Found

The current versions of the documents are available on the Hospital's website under the links: Polish version and English version. Please always ensure that you are using the latest version of the document.

1.4 Document Authentication

Both the Polish and English versions of the document have been signed with the PGP key of the Cybersecurity Team. The document files, signature files, and checksums generated using the sha256 algorithm are available on the Hospital's website under the RFC documents link.

2. Contact Information

2.1 Team Name

Full name: Cybersecurity Monitoring Team for the District Hospital in Zawiercie.
Short name: Cybersecurity Team.

2.2 Address

Cybersecurity Monitoring Team
District Hospital in Zawiercie
14 Miodowa Street
42-400 Zawiercie
Poland

2.3 Time Zone

Central European Time UTC+1.
Central European Summer Time UTC+2 (from the last Sunday in March to the last Sunday in October).

2.4 Phone Number

+48 32 67-40-371
+48 885-999-138

2.5 Fax Number

Not available

2.6 Other Telecommunications

Not available

2.7 Email Address

incydent@szpitalzawiercie.pl

2.8 Public Key and Other Encryption Information

PGP key used by the Cybersecurity Team:
Key fingerprint: 5152 3F73 0B49 F813 32DD 372E 3FB9 CAF9 904E 5A35
The public key can be downloaded from the Hospital's website under the PGP key link.

2.9 Team Members

The Cybersecurity Team consists of individuals with practical knowledge and experience in ensuring physical and IT security.

2.10 Other Information

Information on Cybersecurity is included in the current document and published on the Hospital's website under the Cybersecurity link.

2.11 Additional Contact Information

The preferred method of contacting the Cybersecurity Team is via email. To ensure the security (confidentiality) of correspondence, it is recommended to encrypt it using the PGP key mentioned in section 2.8. If it is necessary to establish another secure communication channel, please contact the Cybersecurity Team directly.
Phone contact with the Cybersecurity Team is available from Monday to Friday, excluding public holidays in Poland, from 08:00 to 15:30 local time.
In urgent situations (e.g. reporting a Cyber threat), information can be communicated by phone to the mobile number provided in section 2.4. The report should then also be sent by email with all details previously provided by phone.

3. Charter

3.1 Mission

The mission of the Cybersecurity Team is to continuously improve the resilience of the IT resources of the District Hospital in Zawiercie by identifying, avoiding, and counteracting potential physical and IT threats.

3.2 Scope of Operation

The Cybersecurity Team covers IT systems and services operating within the District Hospital in Zawiercie.

3.3 Funding and Affiliation

The Cybersecurity Team is financially maintained by the District Hospital in Zawiercie. The Hospital conducts financial operations according to the principles specified in the applicable Polish law.

3.4 Authority

The Cybersecurity Team's activities are supervised by the Hospital Director.

4. Incident Handling Policies

4.1 Types of Incidents and Support Levels

The Cybersecurity Team actively participates in handling all types of IT security incidents that occur or may occur in the Hospital. The classification of incidents and the manner of handling them will vary depending on the severity of the incident, its type, the elements it affects, the number of users involved, and other factors.

4.2 Cooperation, Interaction, and Information Disclosure

The Cybersecurity Team exchanges all necessary information with CERT teams, CSIRT, and other entities that are part of the National Cybersecurity System as well as with the administrators of affected sites. All information regarding incident handling is confidential; therefore, we recommend encrypting the information provided to us using the Cybersecurity Team's PGP key or using another mutually agreed communication channel.

No personal data is shared with entities cooperating with the Hospital unless explicitly authorized.

4.3 Communication and Authentication

The Cybersecurity Team uses PGP key encryption to ensure the confidentiality, integrity, and authentication of communication.

5. Services

5.1 Incident Response

The Hospital has established an organizational and technical process for incident response.

5.1.1 Incident Categorization

Incident assessment includes:

- Analysis and classification of the event as a security incident or a false alarm,
- If classified as an incident, determining its scope and impact on the security of information processed in the Hospital,
- Assigning priority according to the type and severity of the incident.

5.1.2 Incident Coordination

The Data Protection Officer, in collaboration with the IT Systems Administrator, is responsible for coordinating actions. The main tasks of the coordinator include:

- Analyzing artifacts and evidence of the incident to determine the root cause (security vulnerabilities),
- Notifying CSIRT NASK, CSIRT CeZ, and if necessary, appropriate services and law enforcement agencies,
- Ensuring effective communication with other parties that may be involved in the incident,
- If applicable, informing users.

5.1.3 Incident Resolution

Includes:

- Eliminating the cause of the incident,
- Restoring normal operation of the systems affected by the incident,
- Collecting evidence from the incident,
- Providing conclusions and recommendations following the analysis of the incident.

5.2 Proactive Activities

The Cybersecurity Team conducts activities aimed at increasing the resilience of the IT environment and minimizing the potential impact of such events on the security of the Hospital's IT resources.

6. Incident Reporting Forms

No ready-made incident reporting forms have been developed yet. The aforementioned information security incident management process defines the email channel for reporting incidents (incydent@szpitalzawiercie.pl). When reporting an incident, please provide the Cybersecurity Team with as much information as possible, including:

- Contact details and information about the reporter: name, email address, phone number, and the name and address of the organization,
- Observations and analysis results,
- All relevant technical elements (IP addresses, domain name, etc.),
- Scan results (if available),
- System log extracts (if available),
- Any other available information that may be related to the report and that will expedite its resolution and help in its thorough analysis.

7. Disclaimers

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