CSIRT Powiatowe Centrum Zdrowia Sp. z o.o. CERT (English version)

1. About this document

This document contains a description of District Health Centre Sp. z o.o. 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 2022-11-23.

1.2 Distribution list of notifications about changes to the document

District Health Centre Sp. z o.o. 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.pczkartuzy.pl/cyberbezpieczenstwo.html

1.4 Authenticating this Document

This document includes District Health Centre Sp. z o.o. CERT PGP signature.
More details in chapter 2.8

2. Contact Information

2.1 Name of the Team

" District Health Centre Sp. z o.o. CERT": Cybersecurity Incident Response Team – Cybersecurity Team

2.2 Address

Cybersecurity Team
District Health Centre Ltd.
Floriana Ceynowy 7 St.
83-300 Kartuzy
Poland

2.3 Time Zone

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

2.4 Telephone Number

+48 58 685 49 05

2.5 Facsimile Number

None available.

2.6 Other Telecommunication

None available.

2.7 Electronic Mail Address

incydent@pczkartuzy.pl

2.8 Public Keys and Other Encryption Information

Cybersecurity Team uses the PGP key:
User ID: District Health Centre Sp. z o.o. Cybersecurity Team
Email: incydent@pczkartuzy.pl
Key ID: 699C F941 C9D5 4B04
Key size: 4096
Key type: RSA
Fingerprint: B0066DFF85D6992119EE060A969CF941C9D54B04

This key can be received directly from our website:
https://www.pczkartuzy.pl/cyberbezpieczenstwo.html

2.9 Team members

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

2.10 Other Information

General information about District Health Centre Sp. z o.o. can be found at https://www.pczkartuzy.pl/cyberbezpieczenstwo.html

2.11 Points of Customer Contact

Cybersecurity Team prefers e-mail contact.
Please use our cryptographic key above to ensure integrityand confidentiality.
Regular cases:
Contact is possible during business hours: 07:00 – 14:35 local time from Monday to Friday, except for public holidays in Poland.

Incident reports, emergency situations:
Telephone contact with the Cybersecurity Team and / or an e-mail with details provided by telephone.
The phone number of the Cybersecurity Team is available during business hours: 07:00 – 14:35 local time from Monday to Friday, except for public holidays in Poland.

3. Charter

3.1 Mission

Building competence and capabilities of District Health Centre Sp. z o.o. in avoiding, identifying and mitigating the cyber threats.
Contribute to the national cybersecurity efforts.

3.2 Range of activity

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

3.3 Sponsorship and/or Affiliation

The operation of the Company is supervised by Supervisory Board and Shareholders' Meeting.
The Company manages its finances in accordance with the principles set out in the applicable provisions of Polish law.

3.4 Authority

The Kartuski District owns the Company's shares in its entirety.

4. Policies

4.1 Types of Incidents and Level of Support

Cybersecurity 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

Cybersecurity 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 Cybersecurity 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 Cybersecurity 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

Cybersecurity 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 Company 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 Company
- 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

Cybersecurity Commissioner 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

Cybersecurity Team 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@pczkartuzy.pl) incident reporting channel.

In the incident report, please provide at least the following information to Cybersecurity Team:

- 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, Cybersecurity Team assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.