CSIRT 5th Military Clinical Hospital with Polyclinic Individual Public Health Center (IPHC) in Krakow (English version)

1. Information about the document
   This document contains a description of the CERT team in the 5th Military Clinical Hospital with Polyclinic IPHC in Krakow, in compliance with RFC 2350 and it provides basic information about CERT team, methods of contact, describes the responsibilities of the team and the services offered.

   1.1 Date of the last update

   Document version 1.00, published on 11/18/2022.

   1.2 Distribution list of notifications about changes to the document

   CERT in the 5th Military Clinical Hospital with Polyclinic IPHC in Krakow does not use any distribution list to notify about changes in this document.

   1.3 The place where you can find the document

   The current version of this document is available at:
   https://5wszk.com.pl/strona/1170-cyberbezpieczenstwo

   1.4 Credibility of the document

   This document has been signed by the CERT team in 5th Military Clinical Hospital with Polyclinic IPHC in Krakow using the PGP key.

2. Contact information

   2.1 Name of the team

   The Team for Monitoring Threats and Maintaining Information Security Policy was established in the 5th Military Clinical Hospital with Polyclinic IPHC in Krakow. The work of this team is managed by the hospital Commandant's Plenipotentiary for the Information Security Management System.
   The CERT Local Cybersecurity Team of the 5th Military Clinical Hospital with Polyclinic IPHC in Krakow was established on the basis of the IT Department.

   2.2 Address

   Local Cybersecurity Team of the 5th Military Clinical Hospital
   with Polyclinic IPHC in Krakow
   ul. Wrocławska 1-3
   30-901 Krakow
   Poland

   2.3 Time zone

   Central European UTC + 01: 00 Sarajevo, Skopje, Warsaw, Zagreb

   2.4 Telephone number

   +48 126 308 022 from 7:00 to 15:00
   emergency phone + 48 729 316 899

   2.5 Telefax Number

   Unavailable

   2.6 Other communication options

   Unavailable

   2.7 E-mail address

   incydent@5wszk.com.pl

2.8 Public keys and other information about encryption

Local Cybersecurity Team uses the PGP key:

Name: Zespół LZC 5WSzKzP
Email: pelnomocnik.szbi@5wszk.com.pl
Key ID: CDAD EA8B 3EF0 6B2E
Key size: ed25519 + cv25519
Algorithm: ECDSA/EdDSA + ECDH
Fingerprint: 3B53 B3CB FC04 4AE0 EC77 9BB0 CDAD EA8B 3EF0 6B2E
This key can be obtained directly from our website:
https://5wszk.com.pl/strona/1170-cyberbezpieczenstwo

2.9 Team members

The Local Cybersecurity Team consists of the administrators of IT Systems and Security Systems responsible for monitoring cybersecurity threats and responding to incidents in the hospital's ICT systems.

2.10 Other information

General information on the 5th Military Clinical Hospital with Polyclinic IPHC in Krakow is available on the website: https://5wszk.com.pl/ .

2.11 Customer contact points

The Local Cybersecurity Team prefers contact by email.

Use the cryptographic key above to ensure the integrity and confidentiality of communication.

In general issues:
Contact is possible during working hours: 07:00 - 15:00 local time from Monday to Friday, except for public holidays in Poland by phone at +48 126 308 022.

Incident reports, emergency situations:

Incidents (events) or vulnerabilities should be reported via e-mail using *the Event and Incident Reporting Form* to the e-mail address: incydent@5wszk.com.pl

or by phone at +48 126 308 022 in the hours from 7:00 a.m. to 3:00 p.m. local time from Monday to Friday, except for public holidays in Poland and the emergency phone number + 48 729 316 899.

3. Statute

3.1 Mission

Building competencies and capabilities in the 5th Military Clinical Hospital with Polyclinic IPHC in Krakow area of avoiding, identifying and reducing cyber threats.
Support for national activities in the field of cybersecurity.

3.2 Scope of activities

The Local Cybersecurity Team provides support in handling cybersecurity events for hospital’s patients and clients.

3.3 Financing and affiliation

The Hospital is supervised by the Minister of National Defense or persons authorized by them.
The Hospital manages its finances in accordance with the rules provided for by an independent public health care facility, as specified in the Act.

3.4. Authorization

The founding body of the Hospital is the Minister of National Defense. The operation of the hospital is supervised by the Minister of National Defense or by persons authorized by them.

4. Rules for handling incidents (policies)

4.1 Types of incidents and level of support

The Local Cybersecurity Team is dedicated to handling all types of computer security incidents that occur or may occur in the IT environment of the Hospital.

The classification of incidents and the way they are handled are defined in the information security incident management process.

The method of handling incidents depends on the type and severity of the incident or event, the system 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.

4.2 Collaboration, Interaction and Disclosure of Information.

The Local Cybersecurity Team exchanges all necessary information for cooperation 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 unsecured environment.

Information sent to the Local Cybersecurity Team may be transferred, as needed, to trusted parties (such as Internet service providers, other CERT teams) solely for the purpose of handling incidents.

4.3 Communication and authentication

The Local Cybersecurity Team uses encryption to ensure confidentiality and integrity of communication. All transmitted protected information should be encrypted.

5. Services

5.1 The Incident Response

Hospital has established an organizational and technical incident response process.
The process covers the complete incident response cycle:

- service,
- management,
- resolution,
- mitigation.

5.1.1 Incident assessment

Incident assessment includes:

an analysis of the impact of the incident on the security of information processed in the hospital:

- prioritization according to the type and severity of the incident,
- determination of the scope of the incident,
- investigation of the causes.

5.1.2 Incident resolution coordination

The Plenipotentiary of the Local Cybersecurity Team is responsible for the coordination of the activities that include:

- facilitating contact with other parties that may be involved
- contacting the CSIRT MON, NASK and / or, if necessary, the relevant law enforcement authorities
- creating reports for other CSIRTs

5.1.3 Incident resolution includes:

- notifying the team and coordinating appropriate activities,
- tracking the progress of the team involved,
- handling reporting requests,

- presenting reports.

5.2 Proactive activities

The Local Cybersecurity Team conducts activities aimed at increasing the resilience of the IT environment to security events and minimizing the potential impact of these events.

6. Incident reporting forms

The above-mentioned information security incident management process is defined by the e-mail (incydent@5wszk.com.pl).

In the incident report, in accordance with the form, please provide the Local Cybersecurity Team with at least the following information:

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

7. Disclaimers

Every precaution will be taken in the preparation of information, notifications and alerts. The Local Cybersecurity Team is not responsible for any errors, omissions or damages resulting from the use of the information contained in this document.