RFC 2350

Document specification:

Title	RFC 2350 WSzS in Biała Podlaska
First version issue date	14.04.2023
Document expiry date	The document is valid until its next version is issued.
Owner	Wojewódzki Szpital Specjalistyczny w Białej Podlaska (Regional Specialist Hospital in Biała Podlaska)
Current version	1.0
Date the current version was published	14.04.2023

1. Document information

The document contains a description of the Cybersecurity Team in the Regional Specialist Hospital in Biała Podlaska, in accordance with RFC 2350, and provides basic information about the Team, contact forms; describes the Team's tasks and the services offered.

1.1. Last updated

This is version 1.0, issued on 14.04.2023.

1.2. Distribution list with notifications about changes in the document

The Cybersecurity Team in the Regional Specialist Hospital in Biała Podlaska does not use any distribution list aimed at communicating changes in this document.

1.3. Document locations

The current version of the document is available at the link below:
https://www.szpitalbp.pl/pl/szpital/cyberbezpieczenstwo/

1.4. Document authentication

This document was signed using the PGP key of the Regional Specialist Hospital in Biała Podlaska. Its signature is available at the link below:
https://www.szpitalbp.pl/pl/szpital/cyberbezpieczenstwo/

2. Contact information

2.1. Team Name

Cybersecurity Team

2.2. Address

Cybersecurity Team
Wojewódzki Szpital Specjalistyczny w Białej Podlaska (Regional Specialist Hospital in Biała Podlaska)
ul. Terebelska 57-65

21-500 Biała Podlaska

Poland

2.3.Time zone

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

2.4.Phone number

83 41 47 200

2.5.Fax number

Niedostępny

2.6.E-mail address

All incidents should be reported to the following e-mail address:

cyberbezpieczenstwo@szpitalbp.pl

2.7.Other forms of communication

Not available

2.8.Public keys and other encryption information

The Cybersecurity Team uses the PGP key

Email: cyberbezpieczenstwo@szpitalbp.pl

The public key is available at this link:

https://www.szpitalbp.pl/pl/szpital/cyberbezpieczenstwo/

2.9.Team Members

The Cybersecurity Team is composed of experts on issues related to cybersecurity, environmental security and physical security.

2.10. Other information

General information about the Regional Specialist Hospital in Biała Podlaska and cybersecurity are available at this link:

https://www.szpitalbp.pl/pl/szpital/cyberbezpieczenstwo/

2.11. Customer points of contact

The Cybersecurity Team prefers e-mail contact using cryptographic keys to ensure the integrity and confidentiality of communication.

General enquiries: contact is possible from 7.30 am to 3.05 pm local time from Monday to Friday, except for public holidays in Poland.

Incident reporting, crisis situations: the Cybersecurity Team is available via phone and/or e-mail with details provided via phone.
The Cybersecurity Team phone is available during working hours from 7.30 am to 3.05 pm local time from Monday to Friday, except for public holidays in Poland.

3. Statute

3.1. Mission

The Cybersecurity Team's mission is to build competence and capacity of patients and employees to identify, prevent and take actions aimed at minimising the likelihood of cybersecurity incidents, as well as mitigating their consequences (within the scope of the services).

3.2. Scope of services

The Cybersecurity Team provides support in handling cyberspace security incidents for its patients, employees and customers.

3.3. Funding and membership

The activity of the Regional Specialist Hospital in Biała Podlaska is supervised by the Management Board of the Lubelskie Voivodeship. The Regional Specialist Hospital in Biała Podlaska operates financial management based on the terms set out in the applicable provisions of the Polish law.

3.4. Authorisation

The founding body of the Regional Specialist Hospital in Biała Podlaska is the Local Government of the Lubelskie Voivodeship.

4. Rules for handling incidents (policy)

4.1. Types of incidents and level of support

The normal priority is the default priority for all types of cybersecurity incidents that may occur in the teleinformatic environment in the scope of the services provided.

The way the Cybersecurity Team handles the incidents depends on the type and severity of an incident or an event, the elements affected by the incident, the number of affected users and the availability of the Cybersecurity Team resources at a given time. For events, priorities are defined according to their severity and extent.

Incidents served on a voluntary basis, in the public interest, therefore have a normal priority, regardless of the designation attached to the notification of the event. Each decision concerning priority is made by the Cybersecurity Team.

4.2. Cooperation, interaction and disclosure

The Cybersecurity Team represents that all information concerning incident handling is considered confidential.

The Cybersecurity Team shall exchange all information necessary for cooperation with other CSIRT teams, as well as with the administrators of interested parties. No personal data shall be exchanged, unless expressly authorised. All information related to handled incidents shall be treated as protected. Protected information (such as personal data, system configurations, known gaps, etc.) are encrypted, if they have to be transmitted in an unsecured environment.

Information sent to the Cybersecurity Team can be shared according to the needs of trusted third parties (such as Internet service providers, other CERT teams) only for the purposes of handling the incidents.

4.3. Communication and authentication

The Cybersecurity Team uses encryption to ensure confidentiality and integrity of communication. All sensitive information which is sent should be encrypted.

Low-sensitivity data can be sent via unencrypted e-mails, however, it is not considered safe. PGP encryption is recommended, especially for confidential data.

The Cybersecurity Team reserves the right to verify the authenticity of the information or its source to the extent permitted by law.

5. Services

5.1. Incident response

The Regional Specialist Hospital in Biała Podlaska established the organisational and technical incident response process. The process includes a full incident response cycle:

- handling,
- managing,
- solving,
- mitigating.

5.2. Prevention

The Cybersecurity Team performs activities aimed at increasing the resilience of the IT environment to incidents related to cybersecurity and minimising the potential impact of these incidents.

6. Incident reporting forms

There are no special forms for incident reporting to the Cybersecurity Team.

7. Reservations

All precautions shall be taken when preparing information, notifications and alerts.

The Cybersecurity Team shall not be liable for errors, omissions or damage resulting from the use of the information contained in this document.