

Document Information:

Title	RFC2350 CSIRT BOŚ
Version	1.1
Author	Daniel Bancer
Review	Krzysztof Trela
Approved by	Krzysztof Trela
Document format (electronic/paper)	Electronic



Changes History:

Status	Date	Version	Changes History	Author
Creation	2022-12-16	1.0	Document creation	D.Bancer
Modification	2024-07-05	1.1	Document modification	D.Bancer

Signatures:

	Name and Surname	KOC	Date	Signature	Comments
Creation	Daniel Bancer	DCB	2024-07-05		
Review	Krzysztof Trela	DCB	2024-07-05		
Approval	Krzysztof Trela	DCB	2024-07-05		

Bank Ochrony Środowiska S.A.

 ul. Żelazna 32, 00-832 Warszawa  infolinia 801 355 455 | +48 22 543 34 34  www.bosbank.pl

Sąd Rejonowy dla m.st. Warszawy XIII Wydział Gospodarczy Krajowego Rejestru Sądowego 0000015525 | NIP 527 020 33 13 | Kapitał zakładowy: 929 476 710 zł

1. Document Information

This document contains a description of CSIRT BOŚ based on the standard RFC2350. The information were collected about the CSIRT BOŚ Team, methods of communication, and provided services.

1.1. Date of last update

Version 1.1 published on 05.07.2024

1.2. Distribution list for notifications

N/A

Updates delivered to Trusted Introducer on email address <ti@trusted-introducer.org>

1.3. Locations where this document may be found

Current version of the document is available in Polish at:

https://www.bosbank.pl/_data/assets/pdf_file/0011/52202/RFC2350_BOS_PL.pdf

Current version of the document is available in English at:

https://www.bosbank.pl/_data/assets/pdf_file/0012/52203/RFC2350_BOS_EN.pdf

1.4. Credibility of the document

Document was signed using PGP key of CSIRT BOŚ. Signature details below (2.8).

2. Contact information

2.1. Name of the Team

CSIRT BOŚ

2.2. Address

ul. Żelazna 32, 00-832 Warszawa, Poland

2.3. Date of document creation

16.12.2022

2.4. Time zone




UTC/GMT +1 hour – Central European time from October to March

UTC/GMT +2 hours – Central European time from March to October

2.5. Telephone number

+48 22 543 34 34; +48 801 355 455

Bank Ochrony Środowiska S.A.

 ul. Żelazna 32, 00-832 Warszawa  infolinia 801 355 455 | +48 22 543 34 34  www.bosbank.pl

Sąd Rejonowy dla m.st. Warszawy XIII Wydział Gospodarczy Krajowego Rejestru Sądowego 0000015525 | NIP 527 020 33 13 | Kapitał zakładowy: 929 476 710 zł

2.6. Fax Number

Not available in communication with CSIRT BOŚ

2.7. Other telecommunication

We kindly ask for contact via form available at

https://wnioski.bosbank.pl/ords/f?p=FORMULARZE_WWW:INCYDENT_BEZPIECZENSTWA

2.8. Electronic mail address

csirt@bosbank.pl

2.9. Public keys and encryption information

PGP Key of CSIRT BOŚ

Fingerprint: 9573 5EAA 847E 6D5D 2449 AE56 A175 9778 2207 2976

Public key is available for download at:

<https://www.bosbank.pl/wazne-informacje/bezpieczenstwo/csirt-bos-klucz-pgp>

2.10. Team members

CSIRT BOŚ Team consists of experienced cybersecurity analysts employed in Department of Cybersecurity.

2.11. Contact information for clients

CSIRT BOŚ monitors threats occurring in the area of operations (3.2) 24/7/365. Contact with analyst on duty is possible by presented methods of communication (2.5, 2.7, 2.8, 2.9).

2.12. Other information

Information about newest threats can be found at:

<https://www.bosbank.pl/wazne-informacje/bezpieczenstwo>

3. Charter

3.1. Mission statement

Mission of CSIRT BOŚ is to: coordinate and provide adequate response to ICT security incidents, carry out active operations to minimize risk and effects of events and incidents occur within its constituency (3.2).

3.2. Constituency

Constituency of CSIRT BOŚ includes clients, employees and resources necessary for proper functioning of Bank Ochrony Środowiska S.A.

Bank Ochrony Środowiska S.A.

 ul. Żelazna 32, 00-832 Warszawa  infolinia 801 355 455 | +48 22 543 34 34  www.bosbank.pl

Sąd Rejonowy dla m.st. Warszawy XIII Wydział Gospodarczy Krajowego Rejestru Sądowego 0000015525 | NIP 527 020 33 13 | Kapitał zakładowy: 929 476 710 zł

3.3. Sponsorship and affiliation

CSIRT BOŚ is sponsored by Bank Ochrony Środowiska S.A.

3.4. Authority

CSIRT BOŚ reports directly to the Management Board of the BOŚ S.A. and operates within the Bank's structures.

4. Policies

4.1. Types of incidents and level of support

CSIRT BOŚ handles all types of cybersecurity incidents within constituency (3.2). Firstly, all incidents are given a priority depending on severity, scope and subject, which determines engagement of appropriate resources. Secondly, the incident is classified in accordance with internal procedures. CSIRT BOŚ analyst can increase or decrease the priority of an incident based on obtained information. The activities undertaken by CSIRT BOŚ, which determine the appropriate level of ICT security, are based on individual policies and internal documents.

4.2. Co-operation, interaction and disclosure of information

CSIRT BOŚ co-operates with parties constituting system functioning on the basis of Bill of National Cybersecurity System(UKSC). Only essential data about handled incidents is shared. Artifacts, evidence and other data related to specific incidents are treated as confidential. Communication and data disclosure to law enforcement can take place if stated in distinct legislation. CSIRT BOŚ fully supports Sharing Traffic Light Protocol, information about which can be found on: <https://www.trusted-introducer.org/ISTLP.pdf>. Personal data is processed in accordance with applicable law. Databases containing sensitive data are encrypted.

4.3. Communication and authentication

E-mail communication is labeled with the use of Traffic Light Protocol. Based on the type of information it can be shared in different ways. Confidential information should be delivered to CSIRT BOŚ encrypted by PGP/GPG protocol (2.9). Other information should be delivered by other means available. In case of doubts about choosing the right communication channel, prior contact with CSIRT BOŚ is encouraged (2.5, 2.6, 2.7, 2.8, 2.9). Authentication before making contact can be made on the basis of publicly available information i.a. social media, Trusted Introducer network or others.

5. Services

5.1. Incident response

In response to ICT threats, CSIRT BOŚ within its constituency (3.2) takes actions securing confidentiality, integrity, availability and authenticity of information according to national and international documents and standards. The following Incident response phases are distinguished:

Bank Ochrony Środowiska S.A.

 ul. Żelazna 32, 00-832 Warszawa  infolinia 801 355 455 | +48 22 543 34 34  www.bosbank.pl

Sąd Rejonowy dla m.st. Warszawy XIII Wydział Gospodarczy Krajowego Rejestru Sądowego 0000015525 | NIP 527 020 33 13 | Kapitał zakładowy: 929 476 710 zł

5.1.1. Incident triage

- to observe and analyse of events occurring in ICT systems,
- determine authenticity of the incident,
- record, analyse, classify and assign priority of the incident,
- identify and manage the risk within constituency.

5.1.2. Incident coordination

- define the initial cause of the event,
- prepare an answer to the incident and remedial strategy,
- disclose relevant information to the parties involved through the established methods of communication.

5.1.3. Incident resolution

- post factum analyse of compromised elements of ICT infrastructure,
- eliminate of both cause and effects of the incident,
- evidence gather,
- compile of conclusions,
- prepare recommendations,
- create incident response procedures and documents based on the gained knowledge,
- constant refine processes and update the documentation.

5.2. Incident prevention

- upgrade cybersecurity tools with new threats in mind,
- periodical verify and adjust of procedures to the ever changing attack vectors,
- external and internal scans of infrastructure under the process of identification of vulnerabilities

5.3. Proactive activities


- active monitoring of events,
- disclosed vulnerability management,
- periodical tests and audits of resources and processes,
- periodical staff training,
- inform participants and subjects of the constituency on a regular basis (pkt 3.2)
- exchange of information with actors of the cybersecurity system functioning under UKSC.

6. Incident reporting forms

We kindly ask for contact with Bank's Infoline: +48 22 543 34 34; +48 801 355 455 or contact through dedicated form:

https://wnioski.bosbank.pl/ords/f?p=FORMULARZE_WWW:INCYDENT_BEZPIECZENSTWA

Bank Ochrony Środowiska S.A.

 ul. Żelazna 32, 00-832 Warszawa  infolinia 801 355 455 | +48 22 543 34 34  www.bosbank.pl

Sąd Rejonowy dla m.st. Warszawy XIII Wydział Gospodarczy Krajowego Rejestru Sądowego 0000015525 | NIP 527 020 33 13 | Kapitał zakładowy: 929 476 710 zł

7. Disclaimers

CSIRT BOŚ Bank exercises due diligence in compiling information, warnings and notifications. Simultaneously reserves the right to take no responsibility for errors, omissions or damages resulting from utilising information included in the present document.

RFC2350 CSIRT BOŚ was prepared in Polish language. English translation may ambiguously reflect some wording. In all cases of disparity, polish version takes precedence.