CSIRT/SOC Description for Bank Polskiej Spółdzielczości SA

1. About this document

1.1. Data of last update

This is version 1.0, published on 20 November 2020.

1.2. Distribution List for Notifications

Currently CSIRT/SOC does not use any distribution lists to notify about changes in this document.

1.3. Locations where this Document May Be Found

The current version of this CSIRT/SOC description document is available from the bank Polskiej Spółdzielczości WWW site; its URL is https://www.bankbps.pl/

Please make sure you are using the latest version.

2. Contact Information

2.1. Short Name of the Team

SOC BPS

2.2. Name of the Team

Security Operations Center Bank BPS

2.3. Address

Bank Polskiej Spółdzielczości S.A.

ul. Grzybowska 81

00-844 - Warszawa

Poland

2.4. Time Zone

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

2.5. Telefhone Number

- 801 321 456

- (+48) 86 215 50 00 (from mobile phone)

2.6. Facsimile Number

- (+48) 86 215 50 01

2.7. Email address incydent@bankbps.pl

2.8. Public keys and Other Encryption Information

Not available at this time

2.9. Other Information

Not available at this time

2.10. Points of Customer Contact

The preferred method for contacting SOC BPS is via e-mail at incydent@bankbps.pl;

e-mail sent to this address will be handled by the responsible human.

If it is not possible (or not advisable for security reasons) to use e-mail SOC can be reached by telephone 24/7.

SOC BPS hours of operation are generally restricted to regular business hours (07:00 - 19:00 CET/CEST Monday to Friday except holidays) with 24/7.

3. Charter

3.1. Mission Statement

The main role of SOC BPS is the operational service of global ICT security incidents with early warning, threat detection, malware analysis, issuing security messages, security assessments and audits as well as consultations in the field of IT security.

3.2. Constituency

SOC BPS constituency is:

- ASN: AS21280
- IP: 193.30.160/24;
- Domains: bankbps.pl

3.3. Sponsorship and/or Affiliation

SOC BPS is financially maintained by the Bank Polskiej Spółdzielczości which it is formally a part

of.

3.4. Authority

Authority SOC BPS operates under the auspices of, and with authority delegated by Bank Polskiej Spółdzielczości S.A.

The SOC BPS expects to work cooperatively with system administrators and users (customers) at Bank Polskiej Spółdzielczości S.A. Jednakże, However, should circumstances warrant it, the SOC BPS has the authority to take the measures it deems appropriate to properly handle a computer security related incident.

4. Policies

4.1. Types of Incidents and Level of Support

SOC BPS is authorized to address all types of computer security incidents which occur, or threaten to occur, in sieciach Bank Polskiej Spółdzielczości S.A.

The level of support given by SOC BPS will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and the SOC BPS resources at the time.

Incidents will be prioritized according to their apparent severity and extent.

4.2. Co-operation, Interaction and Disclosure of Information

SOC BPS exchanges all necessary information with other CSIRTs as well as with affected parties' administrators. No personal nor overhead data are exchanged unless explicitly authorized.
All sensitive data (such as personal data, system configurations, known vulnerabilities with their locations) are encrypted if they must be transmitted over unsecured environment as stated below.

4.3. Communication and Authentication

Unencrypted e-mail will not be considered particularly secure, but will be sufficient for the transmission of low-sensitivity data. If it is necessary to send highly sensitive data by e-mail, GPG will be used. Network file transfers will be considered to be similar to e-mail for these purposes:sensitive data should be encrypted for transmission

5. Services

5.1. Incident Response

SOC BPS will assist system administrators in handling the technical and organizational aspects of the incidents. In particular, it will provide assistance or advice with respect to the following aspects of incidents management:

5.1.1. Incident Response

- Investigating whether indeed an incident occurred.
- Determining the extent of the incident.

5.1.2. Incident Coldination

- Determining the initial cause of the incident (vulnerability exploited)
- Facilitating contact with other sites which may be involved.
- Facilitating contact with appropriate law enforcement officials, if necessary.
- Making reports to other CSIRTs - Composing announcements to users, if applicable

5.1.3. Incident Resolition

SOC BPS will give advice but no physical support whatsoever to customers from the Bank Polskiej Spółdzielczosci internal network with respect to the incident resolution.

- Removing the vulnerability.
- Securing the system from the effects of the incident.
- Collecting the evidence of the incident.

In addition, SOC BPS will collect statistics concerning incidents processed, and will notify the community as necessary to assist it in protecting against known attacks.

SOC BPS will give advice but no physical support whatsoever to customers from the Bank Polskiej Spółdzielczości S.A. internal network with respect to the incident resolution.

5.2. Proactive Services

SOC BPS coordinates and maintains the following services to the extent possible depending on its resources:

- Information services through the following channels:
- website: https://bankbps.pl
- Training and educational services

6. Incident Reporting Formsin

   SOC BPS only handles incidents reported by e-mail or phone. Contact data is available at: https://www.bankbps.pl/kontakt

7. Discalaimers

   While every precaution will be taken in the preparation of information, notifications and alerts SOC BPS assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.