RFC-2350
SOC SGB-Bank S.A.

1. Information about the document

1.1. Document location

The current version hereof is available on www.sgb.pl/kontakt

1.2. Document authentication

The document has been signed using the PGP key of SGB-Bank S.A. referenced on www.sgb.pl/kontakt

2. Contact details

2.1. Team name

SOC SGB-Bank S.A.

2.2. Team address

SOC SGB-Bank S.A.

SGB-Bank S.A.

ul. Szarych Szeregów 23a

60-462 Poznań

2.3. Time zone

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

2.4. E-mail

All incidents must be reported by e-mail (to: soc[at]sgb.pl)

2.5. Public keys and encryption

PGP Key of SOC SGB-Bank S.A.

Fingerprint: 95BE4234FF79E9591D2DE01029BF0115CE729A1D

The public key is referenced on: https://www.sgb.pl/wp-content/uploads/sgb-bank_cert_pgp_key.txt

2.6. Team members

The SOC SGB-Bank S.A. team members are experienced cybersecurity experts who are responsible for the security of the services rendered by SGB-Bank S.A.

3. Articles of Association

3.1. Mission

The mission of SOC SGB-Bank S.A. is to make sure that the cybersecurity of the services rendered by SGB-Bank S.A. is at the highest level and to support Banki Spółdzielcze that form part of SGB Group in managing cybersecurity-related threats and incidents.

3.2. User group (scope of activities)

SOC SGB-Bank S.A. provides SGB-Bank S.A. and entities that use its ITC infrastructure with support in handling network security incidents. It also offers assistance to users of the services rendered by the Bank.

3.3. Financing and ownership

SOC SGB-Bank S.A. is supported financially by SGB-Bank S.A. and acts within its structure.

3.4. Authorisation

SOC SGB-Bank S.A. acts under the auspices and authorisation of the management of SGB-Bank S.A. and is bound by internal regulations of SGB-Bank S.A.

4. Policy

4.1. Types of incidents and support level

SOC SGB-Bank S.A. handles cybersecurity-related incidents that may occur at SGB-Bank S.A.

SOC SGB-Bank S.A. prioritises incidents based on their severity, extent and subject matter. Incidents are handled according to the priority given. The support offered by SOC SGB-Bank S.A. depends on the severity and type of the incident reported, as well as on other circumstances that are of crucial importance in relation thereto.

4.2. Cooperation, interaction and disclosure of information

To the extent permitted by law, SOC SGB-Bank S.A. exchanges data with entities that perform cybersecurity-related tasks, within the cybersecurity system that complies with the Polish National Cybersecurity System Act. Personal data is processed in accordance with the applicable provisions of law. Sensitive data (personal data, system configurations, known vulnerabilities, etc.) is encrypted when transmitted over unsecured environment. All data relating to the incidents handled is confidential. Any information collected during the handling of any incident by SOC SGB-Bank S.A. may

be transferred to any of the entities defined in other acts and regulations applicable on the territory of Poland.

SOC SGB-Bank S.A. has adopted and follows the Information Sharing Traffic Light Protocol (v1.1). Any TLP-coded communication is handled in keeping with the provisions thereof.

TLP colour codes and their meanings

TLP:RED	Recipients may not share any information with any other person, except for other recipients thereof.
TLP:AMBER	Recipients may share information only within their organisation (and that of their clients) and only with persons who must become familiar with it and in such a scope as is necessary for the appropriate operations to be performed.
TLP:GREEN	Recipients may share information with their collaborators, both within their own and within their partners' organisations, as well as in their environment. Such information may not be made available through any public information channel.
TLP:WHITE	Information may be distributed freely, without restriction (except for the copyright).

4.3. Communication and authentication

SOC SGB-Bank S.A. is obliged to comply with the provisions of law and regulations applicable both in Poland and in the European Union.

All e-mails must be TLP-coded. Any low-sensitivity data may be e-mailed unencrypted; however, this is not considered secure. It is recommended that the PGP encryption is applied, in particular, to confidential data.

5. Services

5.1. Response to incidents

For incidents in the user group, SOC SGB-Bank S.A. provides a wide range of services, including in particular:

5.1.1. Detection and analysis of incidents

- Determining authenticity of events

- Determining initial causes for events
- Defining adequate responses
- Assessing severity
  - Evaluating potential risks of adverse effects
  - Evaluating a potential scale of incidents and resources affected by them
  - Prioritising incidents
- Collecting evidence and indicators of compromise
- Analysing malicious software

5.1.2. Threat mitigation and recovery plans

- Developing post-incident recovery strategies
- Recommending improvements in the security to system administrators
- Developing procedures for handling various types of security incidents

5.1.3. Incident assessment and evaluation

- Correlating incidents, based on the data collected
- Continuously exploring ways to improve the team performance
- Preparing reports and storing them for further use

5.2. Prevention

- Coordinating responses in order to identify vulnerabilities
- Collecting data on security threats and indicators of compromise from various sources
- Monitoring current threats to technology and security
- Developing and improving security tools and mechanisms in order to continue increasing the levels of security

5.3. Proactive activities

- Co-issuing security alerts to clients
- Provide training and carrying out other activities (including actual incident simulations) in order to improve the team performance

6. Reporting security incidents

Security incidents must be reported by encrypted e-mail (to: soc[at]sgb.pl). For incidents to be resolved more efficiently, when reporting any incident, please provide the following information:

- Identification and contact data of the person reporting the incident;
- Incident occurrence and detection date and time;
- Description of the incident reported and of the circumstances of its detection, as well as the source of information on the incident.

7. Disclaimer

When preparing any security-related information, notices or alerts, SOC SGB-Bank S.A. takes all available precautionary measures.

SOC SGB-Bank S.A. disclaims any liability for errors or omissions resulting from or any damage caused by information included herein.

Document history

Title:	RFC-2350 SOC SGB-Bank S.A.
Expiry date:	The document continues in force until the next issue hereof.
The owner:	SGB-Bank S.A.
Current issue:	1.1
Current issue publication date:	13/04/2021