1. Document information

This document describes the Security Operations Center (SOC) capabilities of Československá obchodná banka, a.s. (ČSOB Slovenská republika).
Last updated: [2026-07-28]
Version: 1.0
Distribution: Public

2. Contact information

Team name: ČSOB SK SOC
Organization: Československá obchodná banka, a.s.

E-mail: security@csob.sk

Availability: 24/7 monitoring and incident response capabilities

Public encryption key: Available upon request

3. Charter

The ČSOB SK SOC is responsible for monitoring, detecting, analyzing, and responding to information security incidents affecting the organization.

The team operates within the organizational structure of ČSOB Slovenská republika and supports the protection of information assets, systems, and services.

4. Constituency

The SOC provides services to systems, networks, and endpoints owned or operated by Československá obchodná banka, a.s.
This includes internal infrastructure, user endpoints, and services supporting banking operations.

The SOC provides the following high-level services:

- security monitoring and event detection,
- incident triage and response coordination,
- threat analysis and investigation,
- support for vulnerability handling processes,
- collaboration with internal and external stakeholders.

6. Incident Reporting

Security incidents can be reported via the contact e-mail addresses listed above.

Reports should include relevant technical and contextual information where available. The SOC will handle reported incidents in accordance with internal processes and policies.

7. Policies

Classification

All information handled by the team is classified according to internal information classification policies and shared on a strict need-to-know basis. Sensitive information is protected against unauthorized disclosure.

Exclusivity

The team provides its services exclusively to internal entities and systems of the organization.

Disclosure

The team follows a coordinated disclosure approach. Information related to incidents and vulnerabilities may be shared with relevant stakeholders, national authorities, and trusted security communities when appropriate and in line with internal policies.

Legal considerations
All activities are performed in compliance with applicable laws and regulations, including data protection and confidentiality requirements.

Cryptography
Secure communication channels are used where appropriate. The team supports encrypted communication mechanisms (e.g. TLS, PGP) to ensure confidentiality and integrity of sensitive information.

8. Cooperation

The SOC cooperates with relevant stakeholders, including internal teams, external partners, and recognized security communities.
Collaboration may include information sharing and coordinated incident handling where appropriate.

9. Publication

This document is publicly available and serves as a general description of the SOC capabilities. It does not contain sensitive or confidential operational details.