CSIRT Description for CERT Kredobank (Version 1.00)
================================

1. About this document

This document contains a description of CERT Kredobank according to RFC 2350. It provides basic information about the CERT, ways it can be contacted, and describes its responsibilities and the services offered.

1.1 Date of Last Update

This is version 1.00, published on 2025-09-01.

1.2 Distribution List for Notifications

There is no public distribution list for notifications of updates.

1.3 Locations where this Document May Be Found

The current version of this CSIRT description document is available from the website at: https://www.kredobank.com.ua/cert (see the CERT Kredobank section of the Kredobank website). Please make sure you are using the latest version.

2. Contact Information

2.1 Name of the Team

CERT Kredobank

2.2 Address

Kredobank S.A.
Departament Cyberbezpieczeństwa
ul. Sakharova 78a
79026 Lviv
UKRAINE

2.3 Time Zone

Central European Time (EET) - UTC+2
Central European Summer Time (EEST) - UTC+3 according to EU regulations (from the last Sunday of March to the last Sunday of October)

2.4 Telephone Number

+380 50 413 81 29 (24/7 emergency contact)

2.5 Facsimile Number

Not available (the team does not use fax).

2.6 Other Telecommunication

None available

2.7 Electronic Mail Address

cert@kredobank.com.ua

2.8 Public Keys and Other Encryption Information

CERT Kredobank uses the following PGP public key for secure communications:

User ID:	CERT Kredobank <cert@kredobank.com.ua>
Key ID:	9B34F39B27B3834E Key type: RSA
Key size:	4096
Fingerprint:	971E 7FF8 31C6 AACE 1C5A 0CF9 9B34 F39B 27B3 834E

This key can be obtained from public PGP keyservers or directly from our website (see https://www.kredobank.com.ua/cert).

2.9 Team Members

A detailed list of CERT Kredobank team members is not publicly available.
Team members will identify themselves to the reporting party with their full name in an official communication regarding an incident.

2.10 Other Information

General information about Kredobank S.A. can be found on the www.kredobank.com.ua
In addition, the team's affiliations and memberships include:

National/Industry Initiatives: CERT Kredobank is an active member of the Cyber Security Center of the National Bank of Ukraine (CSIRT-NBU).

Trusted Introducer: CERT Kredobank is a Trusted Introducer Listed team (Listed status since 01 Dec 2017).

MISP: CERT Kredobank is registered in the MISP threat intelligence platform; its organization UUID is 59bfabb0-234c-40cf-87ad-76051c4ddf5d.

2.11 Points of Customer Contact

The preferred method for contacting CERT Kredobank is via e-mail (using the address above). Please use our PGP key to ensure integrity and confidentiality of any sensitive information in email reports.

IMPORTANT: As a Bank-internal team, CERT Kredobank does not handle individual customer complaints or service requests, such as banking account issues or fraud reports from customers; those matters should be directed to the bank's customer service channels.

For cybersecurity incidents related to KREDOBANK's infrastructure or services, please contact us via email (and phone in emergencies). We will use PGP signing on outgoing emails and request PGP encryption on sensitive incoming communications for authentication and confidentiality purposes.

3. Charter

3.1 Mission Statement

CERT Kredobank provides incident handling for Kredobank S.A., the Ukrainian commercial bank with foreign capital and a member of the PKO Bank Polski Group.
We also cooperate with other financial institutions in order to contribute to the national and financial sector cybersecurity efforts.

3.2 Constituency

The CERT Kredobank constituency are all users of IT systems, network infrastructure and service platforms of the Kredobank S.A.

In summary, CERT Kredobank's constituency encompasses the corporate network and systems of Kredobank S.A. and its affiliated entities; it does not extend to the bank's individual retail customers.

3.3 Sponsorship and/or Affiliation

CERT Kredobank is a unit within, and is fully sponsored by, Kredobank S.A. (the parent bank). The team operates as part of the Bank's Department of Cybersecurity.

3.4 Authority

CERT Kredobank operates under the authority delegated by the executive management of Kredobank S.A. The team is given the mandate to investigate and coordinate response to IT security incidents within the Bank's scope of operations, and to take appropriate action or recommend actions in line with the Bank's cybersecurity policies. In handling incidents, CERT Kredobank has the authority to make necessary decisions and engage with external parties on behalf of the Bank, as authorized by the Bank's management.

4. Policies

4.1 Types of Incidents and Level of Support

CERT Kredobank handles all types of cybersecurity and computer security incidents that may occur within its constituency. This includes, but is not limited to: malware infections, unauthorized access attempts, denial-of-service attacks, data breaches, phishing incidents, etc.

Level of Support: The level of support provided by CERT Kredobank will vary depending on the severity and scope of the incident, as determined by the CERT staff. All reported incidents are evaluated and prioritized. Severe incidents (e.g., active attacks significantly affecting critical systems or customer data) will receive immediate and full attention. Lower-impact incidents or general inquiries will be handled as resources permit. In all cases, CERT Kredobank will make best efforts to assist the users and system owners within its constituency in analyzing and resolving the security issues.

4.2 Co-operation, Interaction and Disclosure of Information

All incoming information related to incidents is handled confidentially by CERT Kredobank. Highly sensitive data is transmitted and stored in secure environments, with encryption used when necessary. Incident-related information submitted to CERT Kredobank may be shared strictly on a need-to-know basis with trusted parties and relevant authorities, solely for the purpose of incident handling.

CERT Kredobank operates under Ukrainian national cybersecurity legislation and the regulatory framework of the National Bank of Ukraine (NBU). As a financial institution supervised by the NBU, Kredobank is obliged to ensure timely detection, response, and reporting of significant ICT and cybersecurity incidents. In accordance with applicable law, CERT Kredobank promptly notifies the CSIRT-NBU of any major incidents affecting the confidentiality, integrity, or availability of critical systems.

4.3 Communication and Authentication

The preferred method of communication with CERT Kredobank is via e-mail.

For normal incident reports and queries, unencrypted email is acceptable. However, if the content of communication is sensitive or requires authentication of the source, we strongly encourage the use of our PGP public key (see section 2.8) to encrypt email messages. CERT Kredobank will sign outgoing email with the team's PGP key where possible, to allow recipients to verify authenticity. When needed (e.g., during telephone or video call coordination), we may use additional authentication methods to validate the identity of communicating parties. For urgent matters, initial contact by phone is possible (see section 2.4 for the emergency number), but we will still likely request a follow-up via email (with encryption if sensitive) for tracking and documentation purposes.

5. Services

5.1 Incident Response

CERT Kredobank offers a full-spectrum incident response service to its constituency. Our team is available 24/7 to coordinate and support the handling of cybersecurity incidents that involve Kredobank's systems or networks. This service includes the following phases of the incident response lifecycle:

Preparation: Advise and assist in preparatory measures (security awareness, best practices, preventive tools) to reduce incident occurrence and impact.

Detection and Analysis: Monitor security alerts and notifications, receive incident reports, and analyze potential incidents to confirm and assess their nature and impact.

Containment, Eradication and Recovery: Provide guidance or direct assistance in containing an incident (stopping further damage), removing the threat (eradication of malware or intruder), and recovering systems to normal operation (including system restore and patching).

Post-Incident Activity: After resolving an incident, CERT Kredobank conducts a lessons-learned process, including analysis of collected evidence and root causes, and provides recommendations to prevent similar incidents in the future.

During an incident, CERT Kredobank will act as a central point of coordination among different departments of the Bank and external entities if required (such as other banks' CERTs or law enforcement). We ensure communication flow and support decision-making to efficiently mitigate the incident.

5.2 Proactive Activities

CERT Kredobank is heavily engaged in proactive measures to strengthen the Bank's defense against cyber threats. We continuously work to enhance the organization's immunity to security incidents and to limit the damage of any incidents that might occur.

Proactive services and activities include:

Threat Intelligence and Monitoring: Gathering information on new threats, vulnerability alerts, and attack trends. We monitor various intelligence sources and share relevant indicators and warnings with the appropriate teams within the bank.

Security Advisories and Awareness: Providing constituents (IT teams, developers, employees) with up-to-date information and advice on new vulnerabilities, malware, phishing campaigns, or other threats that could impact their operations. We issue internal security advisories and guidelines, and contribute to training programs to build cybersecurity awareness and skills among employees.

Security Assessments: Assisting in periodic security audits, vulnerabilityvassessments, and architectural reviews for critical systems. While a dedicated audit team may exist, CERT Kredobank collaborates to ensure identified issues are addressed and lessons from incidents inform future architecture and controls.

Policy and Standards Development: Contributing to the development and maintenance of the Bank's cybersecurity policies, standards, and incident response plans. We leverage best practices from the industry to continually improve our policies and preparedness.

By engaging in these proactive efforts, CERT Kredobank helps reduce the likelihood of incidents and ensures that the organization is better prepared to handle those that do occur.

6. Incident Reporting Forms

We do not require any special form for reporting incidents. There are no specific incident report templates needed – a descriptive email to cert@kredobank.com.ua is sufficient. However, we encourage including all relevant details (such as date/time, source/destination IPs, error messages, screenshots, log excerpts, etc.) when reporting an issue, to facilitate effective analysis. If necessary, CERT Kredobank staff may follow up to request additional information.

7. Disclaimers

While every precaution is taken in the preparation of information, notifications, and alerts, CERT Kredobank assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within this document or any security advisories issued by the team. All information is provided on a best-effort basis and is intended solely for the purpose of assisting our constituency in improving security.