CENTRAL BANK
OF THE REPUBLIC OF AZERBAIJAN

İnformation and Cybersecurity Departament

Sectoral Computer Incident Response Center for the Financial Sector in the Republic of Azerbaijan

RFC-2350

03.02.2026

FinCERT.AZ

Table of Contents

1. Document Information 3
1.1. Last Update 3
1.2. Distribution of Changes 3
1.3. Document Locations 3
2. Contact Information 3
2.1. Team Name 3
2.2. Address 3
2.3. Time Zone 3
2.4. Contact Number 3
2.5. Fax Number 3
2.6. Other Contact Methods 3
2.7. Email Address 3
2.8. Public Keys and Encryption Information 3
2.9. Team Members 4
2.10. Operating Hours 4
2.11. Other Information 4
3. Charter 4
3.1. Mission Statement 4
3.2. Scope 5
3.3. Sponsorship and/or Affiliation 5
3.4. Authority 5
4. Policies 6
4.1. Types of Incidents and Level of Support 6
4.2. Cooperation, Interaction, and Information Disclosure 6
4.3. Communication and Authentication 6
5. Services 6
5.1. Incident Coordination 6
5.2. Incident Analysis and Initial Response Support 7
5.3. Threat Intelligence and Cyber Threat Analysis 7
5.4. Awareness and Capacity Building 7
5.5. Stakeholder Cooperation and Liaison 7
6. Incident Reporting Channels 8
7. Additional Notes 8

1. Document Information

This document has been prepared in accordance with the RFC-2350 standard and provides information about FinCERT.AZ. This document outlines the core functions, contact methods, roles, and responsibilities of FinCERT.AZ.

1.1. Last Update

Version 1.0 (Published on 03.02.2026).

1.2. Distribution of Changes

Information regarding changes to this document is distributed via email.

1.3. Document Locations

The current version of this document can be accessed via the following link: https://uploads.cbar.az/assets/02c3d655e376515419c623ce2.pdf

2. Contact Information

2.1. Team Name

Short name: FinCERT.AZ
Full name: Sectoral Computer Incident Response Center for the Financial Sector in the Republic of Azerbaijan

2.2. Address

Central Bank of the Republic of Azerbaijan
167 Heydar Aliyev Ave., AZ1029
Baku, Azerbaijan

2.3. Time Zone

Asia/Baku (GMT+4)

2.4. Contact Number

+994 12 437 00 97

2.5. Fax Number

+994 12 493 55 41

2.6. Other Contact Methods

Not specified.

2.7. Email Address

fincert@cbar.az

2.8. Public Keys and Encryption Information

FinCERT.AZ uses the PGP encryption system for digital signatures and to receive encrypted information. The key is available on PGP/GPG key servers (https://keys.openpgp.org/).

PGP/GPG Key:

- **ID:** FinCERT.AZ fincert@cbar.az

- **Fingerprint:** C07D58873331F02C82BF3AE733D6197718C425A6

2.9. Team Members
Information regarding the members of the FinCERT.AZ team is not disclosed to the public.

2.10. Operating Hours
The preferred method of contacting FinCERT.AZ is via the email address: **fincert@cbar.az**.

FinCERT.AZ's operating hours are **09:00–18:00 (GMT+4)** on business days.

The 24/7 contact phone number is provided in Section 2.4.

For incident reporting procedures, please refer to Section 6 of this document.

2.11. Other Information
General information about FinCERT.AZ in English is available at the following link:
https://www.cbar.az/page-893/fincert?language=en

General information in Azerbaijani is located at:
https://www.cbar.az/page-893/fincert?language=az

3. Charter

3.1. Mission Statement
The mission of FinCERT is to strengthen the level of cybersecurity and resilience in the country's financial sector. To this end, FinCERT's primary areas of activity are as follows:

3.1.1. Collection and Sharing of Incident Information
FinCERT centrally collects and shares information regarding cybersecurity incidents affecting financial organizations, institutions, and other entities. In this capacity, FinCERT:

- maintains close contact and cooperation with national CERTs in accordance with legislation.
- establishes an effective communication environment to ensure the enhancement of cybersecurity levels in financial markets.
- applies global best practices by cooperating with international financial CERTs.

3.1.2. Incident Analysis and Provision of Initial Response Measures
FinCERT analyzes incoming data to identify the root causes of incidents, evaluates their impact on the financial sector, and ensures rapid information exchange and the provision of guidance to enable relevant parties to take appropriate action. These activities help minimize the potential impacts of incidents and foster a deeper understanding of cyber threats in the financial ecosystem.

3.1.3. Coordination of Incident-Related Activities and Strengthening Resilience in the Financial Ecosystem

FinCERT organizes incident response processes in a unified manner by ensuring coordination between financial institutions, national CERTs, and other stakeholders. As a result of this coordination, faster and more effective responses are achieved across the sector, enhancing the resilience of the financial system. Additionally, FinCERT:

- Creates conditions for the enhancement of cybersecurity knowledge and skills within the financial sector.
- Raises the level of cyber hygiene through awareness initiatives.
- Cooperates closely with national CERTs to ensure the dissemination of cybersecurity information through digital channels.

3.1.4. Proactive Threat Detection and Timely Notification of Financial Institutions

One of FinCERT's areas of activity is the early detection of cyber threats targeting the financial sector and the prevention of their potential consequences. Within this framework, FinCERT identifies new and emerging threats using various data collection and analysis mechanisms, assesses their potential impact on financial institutions, and informs participants in a timely manner to ensure appropriate preventive measures are taken.

With these efforts, the financial sector identifies risks proactively, enhances the preparedness among market participants and strengthens overall cyber resilience.

3.2. Scope

FinCERT.AZ serves the financial ecosystem of the Republic of Azerbaijan. Its primary scope includes all financial market participants supervised by the Central Bank of the Republic of Azerbaijan. Furthermore, FinCERT.AZ cooperates with the following institutions:

- Government agencies and critical infrastructure operators related to the financial sector.
- National and international CERTs – for the purposes of information exchange, cooperation, and alignment with international best practices.

The scope of FinCERT.AZ may be expanded in the future in accordance with the national strategic priorities and evolving cybersecurity requirements in the financial sector.

3.3. Sponsorship and/or Affiliation

FinCERT.AZ operates under the Central Bank of the Republic of Azerbaijan.

3.4. Authority

FinCERT.AZ operates under the Central Bank of the Republic of Azerbaijan. By cooperating with national and international cybersecurity communities, government

agencies, and private sector partners, FinCERT.AZ ensures effective coordination, threat intelligence sharing, the implementation of best practices, and capacity building within the financial sector.

4. Policies
FinCERT.AZ operates in accordance with national legislation, internal regulations, and international best practices to ensure the confidentiality, integrity, and responsible management of cybersecurity information. The core principles are as follows:

4.1. Types of Incidents and Level of Support
FinCERT.AZ handles cybersecurity incidents affecting financial institutions within its scope, including:

- Malware infections.
- Phishing campaigns and theft of credentials.
- Distributed Denial of Service (DDoS) attacks.
- Data breaches.
- Exploitation of software or hardware vulnerabilities.
- Insider threats and suspicious behavior.

FinCERT.AZ provides coordination, advisory, and analytical support for these incidents. Operational involvement depends on the severity of the incident and available resources.

4.2. Cooperation, Interaction, and Information Disclosure
4.2.1. FinCERT.AZ highly values operational cooperation and information exchange between CERTs and other institutions that can benefit from or contribute to its services.

4.2.2. FinCERT.AZ protects sensitive information in accordance with the relevant legislation of the Republic of Azerbaijan.

4.3. Communication and Authentication
Telephone calls and unencrypted emails are considered secure for transmitting information with a low sensitivity level.

All high-sensitivity information sent to

FinCERT.AZ must be encrypted using the team's PGP key. FinCERT.AZ recognizes and supports the TLP (Traffic Light Protocol) principles for information sharing.

5. Services
FinCERT.AZ provides coordinated cybersecurity services to support the resilience and incident response capabilities of financial institutions. These services include:

5.1. Incident Coordination
FinCERT.AZ acts as a central point of contact for coordinating responses to cybersecurity incidents affecting financial institutions. Services in this category include:

- Receiving and processing incident reports from partners.
- Facilitating communication and cooperation between affected institutions and external partners.
- Escalating critical incidents to relevant authorities or national CERTs when necessary.
- Supporting incident communication protocols during crisis situations.

5.2. Incident Analysis and Initial Response Support

FinCERT.AZ provides support in the analysis of cybersecurity incidents and the provision of effective initial reactions. This encompasses:

- Analyzing the root causes of incidents and assessing potential impact based on available data.
- Providing recommendations for containment, eradication, and recovery
- Contributing to the enhancement of situational awareness within the financial sector.

5.3. Threat Intelligence and Cyber Threat Analysis

FinCERT.AZ collects, analyzes, and shares cyber threat intelligence to strengthen cybersecurity in the financial sector. This service includes:

- Collection and contextual analysis of Indicators of Compromise (IoCs), attack techniques (TTPs), and emerging threats.
- Identification of patterns, anomalies, and potential risks based on collected incident data and external information sources.
- Distribution of informational updates, technical bulletins, and risk advisories to financial institutions.
- Organizing secure information exchange with national and international CERTs and trusted partners to support early warning and coordinated defense.
- Providing technical analyses to support proactive risk mitigation and increase sector-wide situational awareness.

5.4. Awareness and Capacity Building

To strengthen overall cybersecurity resilience in the financial sector, FinCERT.AZ offers the following services:

- Development and distribution of awareness materials to promote secure behaviors in institutions.
- Cooperation with national and international partners to support long-term capacity building.

5.5. Stakeholder Cooperation and Liaison

FinCERT.AZ ensures that all relevant stakeholders are informed about its mission, services, and mutual cooperation procedures. These activities include:

- Conducting awareness and coordination efforts with financial institutions, regulatory authorities, and strategic partners.
- Maintaining up-to-date communication rules and contact points for incident escalation.

- Serving as a liaison between the financial sector and national/international cybersecurity communities.

6. Incident Reporting Channels

Incidents must be reported via the Central Bank's 'Unified Electronic Reporting Portal': https://portal.e-cbar.az/
If the portal is unavailable, reports may be submitted via email:
fincert@cbar.az

7. Additional Notes

7.1. While all precautions are taken during the preparation of information and notifications shared by FinCERT, FinCERT.AZ assumes no responsibility for any errors, omissions, or damages resulting from the use of the information provided.