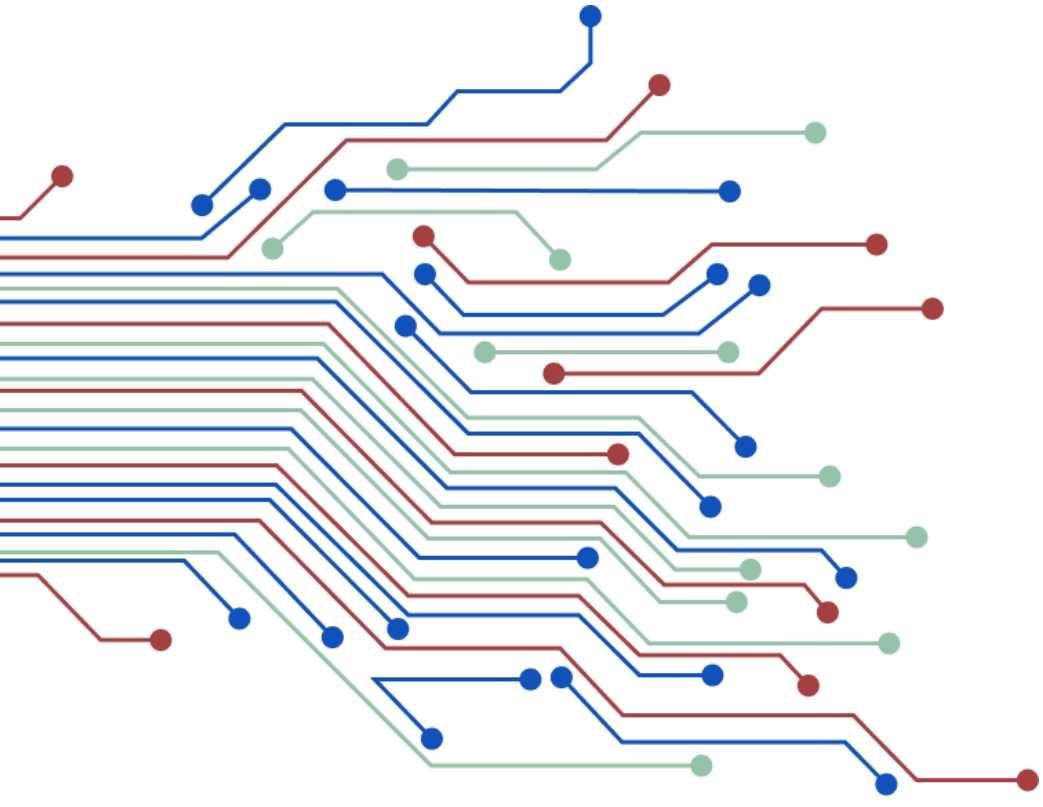
فريق الاستجابة للحوادث
السيبرانية للقطاع المالي
والمصرفي
Jo-FinCERT

# RFC 2350

## Jo-FinCERT

Version 1.0



# 1. Document Information

This document outlines the Jo-FinCERT in alignment with RFC 2350, offering essential details regarding its communication channels, roles and responsibilities.

## 1.1. Date of Last Update

The initial version was published in January 2024.

## 1.2. Distribution List for Notifications

No distribution list is maintained for notifications.

## 1.3. Locations where this Document May Be Found

The most recent version of this document is accessible on the Central Bank of Jordan's website under the Jo-FinCERT section. The URL is:

Https://www.cbj.gov.jo/Pages/viewpage.aspx?Pageid=1480

## 1.4. Authenticating this Document

This document has been signed with the PGP key of Jo-FinCERT. The signature can be verified on the Jo-FinCERT Tab within the Central Bank of Jordan website. The URL is:

Https://www.cbj.gov.jo/Pages/viewpage.aspx?Pageid=1480

## 1.5. Document Identification Title of Document

**Title of the Document**: "Jo-FinCERT-RFC2350-EN_v1-0"

**Version**: 1.0 Document

**Date**: Jan - 2024

**Expiration**: This document remains valid until a newer version supersedes it.

# 2. Contact Information

## 2.1 Name of the Team

Full name: Financial Cyber Emergency Response Team

Short name: Jo-FinCERT

## 2.2. Address

Jo-FinCERT Amman, Jordan, King Al Hussein Street 37 - 11118

## 2.3. Time Zone

The Hashemite Kingdom of Jordan Time Zone: (GMT +3)

## 2.4. Telephone Number

+962 6 4630301 ext.4978

## 2.5. Facsimile Number

+962 6 4613307

## 2.6. Other Telecommunication

Not available.

## 2.7. Electronic Mail Address

For information about security incident or cyber threats targeting financial institutions, please notify us at Fincert@cbj.gov.jo.

Public Keys and Encryption Information.

The key is accessible at:

Https://www.cbj.gov.jo/Pages/viewpage.aspx?Pageid=1480

## 2.8. Team Members

The Jo-FinCERT team comprises of cybersecurity specialists and threat Intelligence Analysts. Eng. Ibrahim M. Shafei serves as The Executive Manager.

## 2.9. Points of Customer Contact

To report incidents, please use the preferred method: Fincert@cbj.gov.jo.

Jo-FinCERT team members are accessible for assistance during regular response hours via this email. These hours typically align with regular Jordanian business hours (Sunday to Thursday, 08:00 to 16:00), excluding local Jordanian holidays.

For emergency or urgent cases, incident should be reported with [EMERGENCY] (within brackets) in the email subject line. Outside of business hours, a designated duty-officer will assess the need for Jo-FinCERT involvement after communication evaluation.

# 3. Charter

## 3.1. Mission Statement

Jo-FinCERT is the Financial Sector Cyber Security Incident Response Team.

This unit is in charge of all Digital Forensics and Incident Response (DFIR) activities. Jo-FinCERT' s mission is to support and protect financial institutions and its business, interests, and reputation from any kind of cyber-attacks that would hamper or harm it.

Jo-FinCERTs activities encompass Cyber-vigilance, anticipation, prevention, detection, response, and recovery. Its primary objectives in supporting financial institutions include:

- Enhancing the resilience of the Jordanian financial and banking sector against cyber risks.

- Strengthening the capabilities of the financial and banking sector to identify and address cyber incidents promptly.

- Improving access to digital forensic intelligence on potential cyber threats faced by the sector.

- Enhancing the competencies of financial sector personnel, fostering a deeper understanding of cyber risks.

## 3.2. Constituency

Jo-FinCERT operates a sector-focused CERT, catering specifically to the financial and banking sectors in Jordan. Its consistency includes banks, exchange companies, payment institutions, insurance, and microfinance institutions regulated by the Central Bank of Jordan.

### 3.3. Affiliation

Jo-FinCERT is affiliated with Central Bank of Jordan and maintains partnership with various local and international CSIRTs and CERTs, as per the requirements, information exchange protocol, and cooperative principles aligned with its mission and values.

### 3.4. Authority

Jo-FinCERT operates under the directive of the Governor of the Central Bank of Jordan.

## 4. Policies

### 4.1 Types of Incidents and Level of Support

Jo-FinCERT is empowered to coordinate, manage, address, and respond to all forms of cyber threats, attacks, and security incidents that either occur or pose a threat to the business, interests, and reputation of any financial entity under the oversight and regulation of the Central Bank of Jordan.

Services provisions by Jo-FinCERT follows a phased approach, tailored to the nature, criticality, and potential impact of security incidents. Jo-FinCERT level of support is also determined by the severity of the security event or incident, its potential or actual impact, and the available resources at the time.

### 4.2. Co-operation, Interaction and Disclosure of Information

Jo-FinCERT categories data and information of all kinds. It aims to assign appropriate classification levels to implement corresponding security measures and mitigate the risk of unauthorized information disclosure.

All incoming information is treated with confidentiality by Jo-FinCERT, irrespective of its priority or classification level. Information that is clearly sensitive in nature is only communicated and stored in a secure environment, employing encryption technologies when required.

Jo-FinCERT exchanges information with the global CSIRT community to enhance security measures, and promote extensive information sharing by using Traffic Light Protocol (TLP).

### 4.3. Communication and Authentication

All communication should be preferably conducted via e-mail. In case where the content is sensitive or requires authentication, Jo-FinCERT employs its PGP key for signing purposes. Any sensitive communication directed to Jo-FinCERT must be encrypted using the team's PGP key.

## 5. Services

### 5.1. Alerts and Warnings

### 5.2. Incident Response

### 5.3. Penetration Testing & Vulnerability Assessments

### 5.4. Threat Intelligence Reports

### 5.5. Security Audits and Assessment

### 5.6. Awareness Programs

### 5.7. Education & Training

## 6. Incident Reporting Forms

To report an incident or vulnerability to Jo-FinCERT CERT, please utilize the email address provided (Fincert@cbj.gov.jo.)

## 7. Disclaimers

While utmost care is taken in the preparation of information, notifications, and alerts, Jo-FinCERT assumes no responsibility for errors, omissions, or for damages resulting from the use of the information provided.