# RFC-2350 STATEMENT

DATE Monday, May 27, 2024
CLASSIFICATION TLP: WHITE

# Contents

  

# Document Information

## History of Changes

| VERSION | TYPES OF CHANGES | DATE |
|---|---|---|
| **1.0** | Final | 16/04/2021 |
| **1.1** | Changes to par. 2.8 | 26/05/2024 |
| | | |
| | | |

## Document Properties

| Owner | Department | Comments |
|---|---|---|
| **OBRELA** | MSS | |
| | | |

# 1. Document Location

The current version of this CSIRT description document is available at https://www.obrela.com/rfc-2350

  

# 2. Document Information

The document describes the operation of OBRELA-CSIRT, formally known as Obrela Security Industries CSIRT, according to RFC2350. It provides basic information about the team, its channels of communication, its' roles and responsibilities.

## 2.1 Date of Last Update

This is version 1.1, published in May 2024. This version is in effect until it is overwritten by a recent version.

## 2.2 Distribution List for Notifications

Email notification of updates is sent to OBRELA management and responders and to business partners.

Please send any questions or comments about updates to the OBRELA CSIRT to ir[at]obrela.com

## 2.3 Locations where this Document May Be Found

The current version of this document is always available on the Obrela Security Industries website, at https://www.obrela.com/advisory/csirt-rfc-2350-declaration/ . Please check that you hold the latest version.

# 3. Contact Information

## 3.1 Name of the Team

Full name: OBRELA Computer Security Incident Response Team

Short name: OBRELA-CSIRT

## 3.2 Address

Obrela Security Industries

117 Argous str. & 33-35 Timeou Street

10441 Athens, Greece

## 3.3 Time Zone

UTC+3 (EEST) summertime between the last Sunday of March and the last Sunday of October

UTC+2 (EET) otherwise

## 3.4 Telephone Number

+30 211 800 3865

## 3.5 Facsimile Number

Not applicable

## 3.6 Other Telecommunication

Depending on the emergency and the confidentiality of the information disclosed to the CSIRT, secure communication is provided via out-of-bounds channels such as Wire. Instructions on establishing a secure channel can be requested upon communication with the CSIRT. Please make sure you have downloaded the official application on your platforms (https://wire.com/en/download/)

## 3.7 Electronic Mail Address

Report an Incident directly , by sending an email to mailto:ir[at]obrela.com

## 3.8 Public Keys and Encryption Information

Please encrypt sensitive email with the PGP key of the Incident Response team, signing the message with a key that can be verified by public key servers.

| | |
|---|---|
| **ID** | 0xDA41C8B5 |
| **PGP Fingerprint** | A1656A9B59F99C370A87B92228C48D57DA41C8B5 |

## 3.9 Team Members

OBRELA-CSIRT is operated by Obrela Security Industries, a privately-held cyber-security firm. The team is made up of Incident Responders, Threat Hunters and Cyber Security Analysts.

## 3.10 Other Information

General information about the Obrela Security Industries services can be found on the website: https://www.obrela.com/solutions/mdr/

## 3.11 Points of Customer Contact

OBRELA-CSIRT hours of operation are 10:00 to 18:00 UTC+2, Monday to Friday, excluding public holidays.

The preferred, unstructured, method to contact OBRELA-CSIRT is email to ir[at]obrela.com or customersecurity@obrela.com which are monitored by a duty officer during hours of operation to notify for an active incident. In case of emergency, please specify the [URGENT INCIDENT] tag in the subject field of the email.

# 4. Charter

## 4.1 Mission Statement

Obrela Security Industries' Computer Security Incident Response Team (OBRELA-CSIRT) mission is to defend its constituency and provide guidance in mitigation against cyber incidents that would harm the integrity of assets and information. The scope of OBRELA-CSIRT activities covers detection, response and recovery of security incidents that may occur. This may include technical assistance in any of the following fields:

- Interpretation of the data collected by the MDR technology stack of OBRELA (SIEM and XDR platforms)
- Guidance on the actions needed to contain incident and eradicate the threat
- Guidance for recovery actions if that is necessary
- Documentation on the investigation of the root-cause

OBRELA-CSIRT can provide immediate, remote or on-site support in order to assist the recovery from an incident. Apart from the information briefing, OSI's response team will physically examine and analyze implicated and potentially compromised systems, will assist in mitigation and recovery and will provide consulting services for the successful and on-time containment of the threat.

## 4.2 Constituency

The constituency of OBRELA-CSIRT is composed of all the organizations having a defined relationship, partnerships or business contracts with Obrela Security Industries.

## 4.3 Affiliation

OBRELA-CSIRT is a team of responders, analysts, and engineers within Obrela Security Industries.

## 4.4 Authority

OBRELA-CSIRT is not authoritative, by achieving its functions through services delivered to its constituents. OBRELA-CSIRT coordinates, investigates, and remediates security incidents within the framework defined by Obrela Security Industries HR and Legal policies, collaborating with vendors, peers and information security community and acting when asked to do so by affected organizations or persons.

## 4.5 Types of Incidents and Level of Support

The level of support given by OBRELA-CSIRT will vary depending on the type and severity of the incident or issue, the type of constituent, the affected resources (human or infrastructure) affected, and the team resources at the time, though in all cases some response will be made within one working day.

Incidents will be prioritized according to their apparent severity and extent.

All incidents reported by retained clients are considered HIGH priority.

All incidents are considered normal priority unless they are labeled EMERGENCY.

## 4.6 Co-operation, Interaction and Disclosure of Information

All incoming information is handled confidentially by OBRELA-CSIRT, regardless of its priority.

OBRELA-CSIRT will never disclose information to third parties unless required by law.

OBRELA-CSIRT supports the Information Sharing Traffic Light Protocol. Communication that is marked with the tags WHITE, GREEN, AMBER, or RED will be handled appropriately.

## 4.7 Communication and Authentication

The preferred method for contacting OBRELA CSIRT is email: ir@obrela.com

Communication via telephone is considered sufficiently secure to be used even unencrypted. Depending on the emergency and the confidentiality of the information disclosed to the CSIRT, secure communication via out-of-bounds channels should be considered.

# 5. Services

## 5.1 Incident Response

OBRELA-CSIRT provides assistance to constituents, business partners and organizations in handling the technical and operational aspects of security incidents.

### 5.1.1 Incident Triage

- Investigating whether an incident is authentic, assessing and prioritizing the incident
- Determining the gravity of the incident

### 5.1.2 Incident Coordination

- Determining the initial cause of the incident (e.g. phishing emails, weaponized documents, vulnerability exploit, etc.)
- Sharing threat intelligence to enhance perimeter and ensure readiness
- Collecting evidence where criminal prosecution or fraud is suspected

### 5.1.3 Incident Resolution

- Containing the incident to avoid greater impact
- Assisting in recovery efforts by providing advisory on mitigation actions
- Collecting evidence about incidents that could be used for protecting against future attacks
- Evaluating whether mitigation actions are likely to reap results in proportion to their cost and risk

### 5.2 Proactive Activities

OBRELA-CSIRT provides information (e.g. on threat landscape, published vulnerabilities, new attack tools or artefacts, security/protection measures, etc.) needed to protect systems and networks available on https://www.obrela.com/resources/insight/

## 6. Incident Reporting Forms

No specific form is provided to report security incidents. Make sure you have described the following information:

- Point of Contact First and Last name
- Organization name
- Email address
- Phone Number
- Description of events that lead to incident identification
- Attachment of evidence, if possible
- Request for remote or on-site CSIRT investigation

## 7. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, OBRELA-CSIRT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within this document.