TLP:CLEAR

RFC 2350

# CSIRT
# BOUYGUES TELECOM
# RFC 2350

On est fait pour
être ensemble

## Table of Content

# 1. About this document

This document contains a description of CSIRT Bouygues Telecom according to RFC 2350 and provides essential information about CSIRT Bouygues Telecom, its role, responsibilities and means of communication.

## 1.1 Date of the last update

This is the version 1.1 published on February 15, 2024.

## 1.2 Distribution list for notifications

Notification of document changes is not distributed by a mailing list or any other mechanisms.

## 1.3 Location where the document may be found

The current and latest version of this document is available on Bouygues Telecom's website at: https://www.corporate.bouyguestelecom.fr/wp-content/uploads/2024/03/CSIRT-Bouygues-Telecom-RFC2350-Mars24.pdf

## 1.4 Document authenticity

This document has been signed with the PGP key of CSIRT Bouygues Telecom. The public PGP key is available from Bouygues Telecom website at : https://www.corporate.bouyguestelecom.fr/wp-content/uploads/2024/03/csirt-bouygues-telecom-pub-pgp-key.zip

## 1.5 Document identification

| | |
|---|---|
| Title | RFC 2350 – CSIRT-Bouygues Telecom.pdf |
| Version | 1.1 |
| Date | 2024-02-15 |
| Expiration | This document is valid until it is replaced by a later version |

# 2. Contact information

## 2.1 Name of the team

CSIRT Bouygues Telecom

## 2.2 Postal address

CSIRT Bouygues Telecom
Service DORSI/DCR/DRI
13 Avenue du Maréchal Juin
13 – 15 Le Technopole
92360 MEUDON
FRANCE

## 2.3 France creation date

The CSIRT team was created on September 01, 2021.

## 2.4 Time zone

The CSIRT is located in the following time zone:
CET/CEST: Europe/Paris (GMT+01:00, and GMT+02:00 on DST).

## 2.5 Telephone number

Please consider using email first, this number is only used for important subjects.
If necessary, you can contact the CSIRT team at the following number: **(+33) 1 46 01 87 00**

## 2.6 Facsimile number

N/A

## 2.7 Electronic mail address

If you need to notify us about an information security incident or a cyber-threat targeting or involving Bouygues Telecom CSIRT, please contact us at: **mbx_CSIRT@bouyguestelecom.fr**

## 2.8 Public keys and other encryption information

Bouygues Telecom CSIRT uses the following PGP Key:
**Key ID: 0x7CDA4FD5**
**Fingerprint: 2A3B 7EF5 2745 1F27 F1CA 4B4F 7AF3 A491 49B2 684E**
The PGP key can be retrieved from applicable public key servers such as https://keys.openpgp.org

## 2.9 Team members

The team is made up of cyber security analysts.

No personal information relating to members of CSIRT Bouygues Telecom is published in this document.

## 2.10 Points of contact

The preferred method to contact CSIRT Bouygues Telecom is via e-mail at: **mbx_CSIRT@bouyguestelecom.fr**

An incident response analyst on duty can be contacted at this mail address during hours of operation.

Please use our cryptographic key to ensure integrity and confidentiality.
In case of emergency, please specify the **[URGENT]** tag in the subject field in your e-mail.

# 3. Charter

## 3.1 Mission statement

Within Bouygues Telecom, the Cyber & Resilience department (DCR) translates the security strategy in actionable plans, oversees the level of implemented security controls and establishes operational security baselines.

CSIRT Bouygues Telecom is the unit in charge of incident response, digital forensics, malware analysis, and threat intelligence activities.

CSIRT Bouygues Telecom's main mission is to support Bouygues Telecom's ability to deliver on business goals while protecting it from cyberattacks that would hamper the integrity of its informational and infrastructural assets or damage its reputation. Its activities cover prevention, detection, response, containment, eradication, recovery and post-incident activities as depicted in the incident response cycle.

While delivering on objectives, CERT Bouygues Telecom is driven by the following values:

- it strives to act in accordance with the highest standards in terms of ethics, integrity, honesty and professionalism,
- it is committed to deliver high quality services to the clients within its constituency and while responding to external parties,
- it does its best to respond to security incidents as efficiently as possible within the best possible delays,
- it facilitates information exchange between Bouygues Telecom and its peers on a need-to-know basis.

## 3.2 Constituency

The constituency of CSIRT Bouygues Telecom is composed of all entities belonging to Bouygues Telecom. Please refer to the following resource for mor details: www.bouyguestelecom.fr

## 3.3 Sponsoring organization / affiliation

CSIRT Bouygues Telecom is a private CSIRT in the telecom sector. It is operated, financed and owned by **Bouygues Telecom SA**. CSIRT Bouygues Telecom strives to maintain regular contact with various national and international CSIRT, CERT, incident response and security teams whenever such communication follows Bouygues Telecom's needs and communication culture.

## 3.4 Authority

CSIRT Bouygues Telecom operates under the authority of the Bouygues Telecom Chief Information Security Officer.

# 4. Policies

## 4.1 Types of incidents and level of support

CSIRT Bouygues Telecom handles all types of incidents impacting the confidentiality, integrity or availability that may occur within its constituency.

Depending on the incident, CSIRT Bouygues Telecom’s expertise may cover, but is not limited to the areas of incident response, digital forensics, malware analysis, strategical, tactical and operational threat intelligence.

CSIRT Bouygues Telecom will adjust the extent of provided support depending on the incident’s severity, its potential impact and the available staff resources at the time of incident.

## 4.2 Co-operation, interaction, and disclosure of information

CSIRT Bouygues Telecom knows the importance for sharing information with third parties. The "need to know" principle is applied in order to share the necessary amount of information to the restricted people/organizations involved. In addition, CSIRT Bouygues Telecom respects the Information Sharing Traffic Light Protocol Version 2 (TLP 2.0) that comes with the tags CLEAR, GREEN, AMBER, AMBER+STRICT or RED as described by the FIRST definitions at: www.first.org/tlp/

CSIRT Bouygues Telecom can exchange with other entities such as external SOC, CERT and other Cybersecurity teams in order to facilitate information sharing.

CSIRT Bouygues Telecom dialogs and cooperates with a privilege way with Cybersecurity entities close to their activities.

## 4.3 Communication and authentication

CSIRT Bouygues Telecom strongly encourages the use of a PGP key for email encryption. All emails containing confidential information must be encrypted using a PGP key.

CSIRT Bouygues Telecom respects the Information Sharing Traffic Light Protocol (TLP) that comes with the tags WHITE, GREEN, AMBER or RED.

A telephone call, a postal service or an unencrypted email can be used for non-sensitive information sharing.

# 5. Services

## 5.1Proactive activities

CSIRT Bouygues Telecom is in charge of:

- Monitoring of threats and vulnerabilities;
- Pre-emptive Security Controls
- Artifact processing and analysis;

## 5.2 Reactive activities

The team offers the following reactive services:

- Alerts and warnings ;
- Intrusion detection ;
- Digital Forensics and Incident Response (including Incident Coordination, Crisis Management)
- Vulnerability Response Coordination.

This information may be exchanged with other CSIRTs if it proves useful, on a need-to-know basis.

## 5.3 Alerts and Warning

CSIRT Bouygues Telecom disseminates information and intelligence on cyberattacks, technical disruptions, security vulnerabilities, malware, and provides recommendations on how to tackle the resulting risk within its constituency. Alerts and warnings may be passed on to other CERTs, CSIRTs, SOCs and security teams if deemed necessary or useful to them on a need-to-know basis.

## 5.4 Pre-emptive Security Controls

CSIRT Bouygues Telecom performs pre-emptive security controls and follow offensive security missions (read teaming) to detect potential breaches, vulnerabilities and misconfigurations that may be leveraged by threat actors. These security controls tend to align the compliance level of various systems and applications with the existing security policies.

## 5.5 Intrusion detection

CSIRT Bouygues Telecom leverages tools, services and processes to detect potential intrusions.

## 5.6 Digital Forensics and Incident Response

CSIRT Bouygues Telecom performs incident response for its constituency. Its incident response service covers the 6 phases of the Incident Response process: Preparation, Identification, Containment, Eradication, Recovery and Lessons Learned.

# 6. Incident reporting

CSIRT Bouygues Telecom doesn’t provide any incident reporting form.
To report an external incident from the outside, please provide the following details to CSIRT Bouygues Telecom :

- Contact details and organizational information such as person or organization’s name, address and contact information ;
- Email address, phone number, PGP key if available ;
- Description of the incident (context, date and time with timezone, perimeter, ..) ;
- Any relevant technical information to illustrate the issue (FQDN, IP, port, protocols, logs, screenshots, emails, etc)

NB : In case of email transfer, please include all technical elements of the email such as headers, bodies and attachments is possible and as allowed by the regulations, policies and legislation under which you operate.

# 7. Disclaimers

CSIRT Bouygues Telecom declines all responsibility in the event *of any* error *or omission* or for any prejudice resulting from information contained in this document. If you notice any error in this document, please notify us by e-mail. We will try to rectify the information as soon as possible.