CULLETTIVITÀ DI CORSICA
COLLECTIVITÉ DE CORSE

Soutenu par
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

RFC2350 : VERSION 1.2 – 24 JUIN 2026

CULLETTIVITÀ DI CORSICA
COLLECTIVITÉ DE CORSE

INDEX OF CONTENT

1. ABOUT THIS DOCUMENT

This document provides a description of the CSIRT CyberCorsica cyber incident response team, as recommended by RFC 2350: http://www.ietf.org/rfc/rfc2350.txt

It presents information about the team, the services offered and the means of contacting CSIRT CyberCorsica.

1.1 DATE DE DERNIERE MISE A JOUR

This is version V1.2 of this document, published on 24/06/2026.

1.2 DISTRIBUTION LIST FOR NOTIFICATIONS

All changes made to this document will be shared through the following channels:

- InterCERT-FR / french CSIRT Network -www.cert.ssi.gouv.fr/csirt/intercert-fr

1.3 WHERE TO FIND THIS DOCUMENT

This document can be found in the footer of the CSIRT CyberCorsica website: www.cyber.corsica

1.4 DOCUMENT AUTHENTICITY

This document has been signed using the CSIRT CyberCorsica PGP key.

The public PGP key, its identifier and fingerprint are available on the CSIRT CyberCorsica website at: https://cyber.corsica/index.php/pgp/

1.5 DOCUMENT IDENTIFICATION

Title: RFC 2350 of CSIRT CyberCorsica

Version: V1.2

Last updated: 24/06/2026

Validity: This document is valid as long as no later version exists.

2. CONTACT INFORMATION

2.1 TEAM NAME

Short name: Cybercorsica

Full name: CSIRT CyberCorsica

2.2 Address

10 rue Général Fiorella

20000 AJACCIO France

2.3 Time Zone

CET/CEST: Paris (GMT+01:00, and GMT+02:00 during summer time)

2.4 Phone Number

04 20 97 00 97

2.5 Fax Number

N/A

2.6 Other Communication Channels

https://www.linkedin.com/company/csirt-cybercorsica/

2.7 Email Address

contact@cyber.corsica

2.8 Public Key and Encryption Information

PGP is used to guarantee the confidentiality and integrity of communications with CSIRT CyberCorsica.

Public Key :

mDMEZd3mjBYJKwYBBAHaRw8BAQdAHB1q8lYUfkCwVW5pULnBssvBk5KaVPOAJYrc
JlayrcO0KkNTSVJUIEN5YmVyQ29yc2ljYSA8Y29udGFjdEBjeWJlci5jb3JzaWNh
PoiTBBMWCgA7FiEEKJ63P8qKn0TwjD7O4TicEv7LRg8FAmXd5owCGyMFCwkIBwIC
IgIGFQoJCAsCBBYCAwECHgcCF4AACgkQ4TicEv7LRg9DHAD/cPj9DHiQQ78jB2Mi
nwbMNsS18XL1ouetqCS0oSO06b8A/2BtGwSYkmrKHX/5Zo/7Q2UIev+yljk44GFR
a/PuaI8EuDgEZd3mjBIKKwYBBAGXVQEFAQEHQDaxzoXfOQ2JopupXah3viZaJzsE
1uHSIXWHpfKHnMsnAwEIB4h4BBgWCgAgFiEEKJ63P8qKn0TwjD7O4TicEv7LRg8F
AmXd5owCGwwACgkQ4TicEv7LRg8TXwD8D7dZB4w8EkgvXAmgVJ7hmlSNO1yl97Py
LGXTJGXnYiABAJyDlSS/7p9OWbq/VG2eUoLZXGeLYhH7VbRP5Wat/kAD
=hSb0
-----END PGP PUBLIC KEY BLOCK-----

Key ID: E138 9C12 FECB 460F

Fingerprint: 289EB73FCA8A9F44F08C3ECEE1389C12FECB460F

The public PGP key is available at: https://cyber.corsica/index.php/pgp/ as well as on the main PGP key servers (MIT, CIRCL).

2.9 Team Members

The team consists of 3 members:

- One CSIRT Manager
- Deux Analystes en cyber sécurité ;

2.10 Other Information

None at this time.

2.11 Contact

CSIRT CyberCorsica is available during business hours, from 8:30 AM to 12:30 PM and from 2:00 PM to 5:30 PM, Monday to Friday (excluding public holidays).

The preferred method of contact is by email at: contact@cyber.corsica

We encourage the use of encryption with the information provided in section 2.8 Public Key and Encryption Information to ensure the integrity and confidentiality of communications.

In case of urgency, please include the tag [URGENT] in the subject line of your email.

CSIRT CyberCorsica can also be reached by phone at 04 20 97 00 97.

3. CHARTER

3.1 Mission Statement

CSIRT CyberCorsica is the computer security incident response team for Corsica. Its objective is to provide assistance to organisations within its territory (described in section 3.2 Constituency) in responding to the cyber incidents they face.

The missions of CSIRT CyberCorsica are as follows:

- Support beneficiaries (described in section 3.2 Constituency) who are victims of a computer incident and direct them towards referenced cybersecurity service providers,
- Monitor threats and vulnerabilities,
- Alert beneficiaries (described in section 3.2 Constituency) about these threats and vulnerabilities,
- Contribute to raising awareness among stakeholders in the territory by relaying information available from government bodies and specialised cybersecurity companies.

3.2 Constituency

The entities that may benefit from CSIRT CyberCorsica's support are organisations located in the territory of the Collectivité de Corse, including in particular:

- Businesses,
- Local authorities and associated public bodies,
- Associations.

3.3 Affiliation

This CSIRT is a mission of the Cullettività di Corsica – Collectivité de Corse and therefore carries out a public service mission.

3.4 Authority

CSIRT CyberCorsica carries out its activities under the responsibility of its manager, who is himself under the authority of the President of the Executive Council of Corsica.

4. POLICIES

4.1 Types of Incidents and Level of Intervention

The scope of CSIRT CyberCorsica covers all computer security incidents affecting organisations in its territory as described in section 3.2 Constituency.

The main missions of CSIRT CyberCorsica are:

- Provide a first-level response to cyber incidents occurring at its beneficiaries;
- Redirect its beneficiaries to referenced service providers for incident remediation;
- Act as a liaison between CERT-FR, regional service providers, Police and Gendarmerie services and beneficiaries;
- Consolidate incident statistics across the territory of the Collectivité de Corse.

4.2 Cooperation, Interaction and Information Sharing

Information relating to an incident, such as the name of the organisation and technical details, is not published without the consent of the named party.

CSIRT CyberCorsica may communicate information to other regional CSIRTs or to CERT-FR when an organisation requests their support. Similarly, information may be shared with a sectoral CSIRT (health, maritime, etc.) for the purpose of capitalising on incidents specific to the sector concerned.

Information dissemination will be handled in accordance with the TLP protocol defined by FIRST (https://www.first.org/tlp).

4.3 Communication and Authentication

CSIRT CyberCorsica strongly recommends the use of secure communication channels and PGP encryption, in particular for communicating confidential or sensitive information.

Non-confidential or non-sensitive information may be transmitted via unencrypted emails.

5. SERVICES

5.1 Incident Response

The main activity of CSIRT CyberCorsica is to assist its beneficiaries by providing a first-level cyber incident response service and helping them refine their choice of service provider to support them in the subsequent resolution of incidents.

In particular, it offers the services detailed in the following sections.

5.2 Reception and Qualification

- Receipt of the report and contact with the declarant;
- Collection of information about the incident and confirmation or assessment of the nature of the incident;
- Determination of the severity of the incident (its impact) and its scope (number of machines affected);
- Recording and categorisation of the incident.

5.3 Coordination and Communication

- Identification of the best partner within the national incident response framework to support the applicant;
- Support in the dissemination, where applicable, of notifications to the competent State authorities according to the nature of the incident. In particular, but not exhaustively:
- To ANSSI in the event of a major cybersecurity incident that may impact other sectors;
- To the Commission Nationale de l'Informatique et des Libertés (CNIL) in the event of a personal data breach.

5.4 Resolution Support

- Proposal of reflex actions, including emergency measures to limit the impact of the incident or measures designed to facilitate investigations and incident handling;
- Sharing of a shortlist of local service providers capable of ensuring incident resolution and remediation;
- Monitoring of resolution and remediation phases.

5.5 Proactive Monitoring and Information Activities

CSIRT CyberCorsica may also offer proactive services to its beneficiaries, including:

- Monitoring services;
- Threat analyses;
- A monitoring bulletin for subscribers.

6. INCIDENT NOTIFICATION FORMS

An incident declaration form is available online at: www.cyber.corsica

In the event of a declaration by email, to facilitate the processing of reports, it is requested where possible to provide the following elements in the email:

- Information about the affected organisation (name, contact details of management and technical teams, size, etc.);
- Contact information of the applicant including: name, position and mobile phone number;
- Contact information of the Information System Manager including: name, mobile phone number;
- Incident timeline: date and time of the start of the incident and its detection;
- Description of the incident including in particular the impact on the organisation and the number and type of machines affected;
- Actions taken since the detection of the incident;
- Any other results of investigations already conducted;
- Information system architecture;
- Defence tools and policies against incidents in place;
- Whether the applicant is already in contact with an IT security incident response service provider;
- Services expected from an incident response team.

7. DISCLAIMER

Although all precautions are taken in the preparation of information, notifications and alerts, CSIRT CyberCorsica assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained herein.

RFC2350 : VERSION 1.2 – 24 JUIN 2026

INFOS :

	www.cyber.corsica
	04 20 97 00 97
@	contact @ cyber . corsica
	https://www.linkedin.com/company/csirt-cybercorsica/