CULLETTIVITÀ DI CORSICA
COLLECTIVITÉ DE CORSE

Soutenu par
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité



RFC2350 : VERSION 1.3 – OCTOBER, 22TH 2026

CULLETTIVITÀ DI CORSICA
COLLECTIVITÉ DE CORSE

INDEX OF CONTENT

1. ABOUT THIS DOCUMENT 3

1.1 Distribution List for Notifications 3
1.2 Where to Find This Document 3
1.3 Document Authenticity 3
1.4 Document Identification 3

2. CONTACT INFORMATION 3

2.1 Team Name 3
2.2 Address 3
2.3 Time Zone 3
2.4 Phone Number 3
2.5 Other Communication Channels 3
2.6 Email Address 4
2.7 Public Key and Encryption Information 4
2.8 Team Members 4
2.9 Other Information 4
2.10 Contact 4

3. CHARTER 5

3.1 Mission Statement 5
3.2 Constituency 5
3.3 Affiliation 5
3.4 Authority 5

4. POLICIES 5

4.1 Types of Incidents and Level of Intervention 5
4.2 Cooperation, Interaction and Information Sharing 6
4.3 Communication and Authentication 6

5. SERVICES 6

5.1 **VICTIM ASSISTANCE AND INCIDENT HANDLING** 6
5.1.1 Incident triage 6
5.1.2 Incident coordination 6
5.1.3 Incident resolution support 6
5.2 EXPOSURE SURFACE ANALYSIS AND “MON PARCOURS CYBER” DIAGNOSTICS 7
5.3 CYBER THREAT MONITORING AND TARGETED ALERTS 7
5.4 REGIONAL CYBER SITUATION AND THREAT LANDSCAPE 7
5.5 AWARENESS RAISING, WORKSHOPS AND QUICK-REFERENCE SHEETS 7
5.6 CYBER NETWORK FACILITATION AND COOPERATION WITH PARTNERS 7
5.7 ANALYSIS OF SUSPICIOUS URLS AND E-MAILS 8
5.8 INFORMATION, PUBLICATIONS AND COMMUNICATION 8

6. INCIDENT NOTIFICATION FORMS 8

7. DISCLAIMER 9

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 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

1.2 Where to Find This Document

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

1.3 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/

1.4 Document Identification

Title: RFC 2350 of CSIRT CyberCorsica

Version: V1.3

Last updated: 22/10/2026

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 Other Communication Channels

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

2.6 Email Address

contact@cyber.corsica

2.7 Public Key and Encryption Information

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

Public Key :

——BEGIN PGP PUBLIC KEY BLOCK——

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).

2.8 Team Members

The team consists of 3 members:

- One CSIRT Manager
- Deux Analystes en cyber sécurité ;

2.9 Other Information

None at this time.

2.10 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

CyberCorsica CSIRT provides its constituents (described in section 3.2 Constituency) with eight services, structured on the FIRST CSIRT Services Framework (v2.1) and detailed in the CyberCorsica CSIRT service catalogue. These services are delivered as part of a public service mission, with an advisory and support role: the CSIRT advises, guides and refers, without any power of injunction or control.

5.1 VICTIM ASSISTANCE AND INCIDENT HANDLING

The core activity of CyberCorsica CSIRT is to assist its constituents by providing a first-level response to cyber incidents, supporting them through to resolution or, where appropriate, referring them to suitable expertise for the rest of the resolution. In particular, it provides the services detailed below.

5.1.1 Incident triage

- Receiving the report, acknowledging it and contacting the reporter;
- Collecting information on the incident and confirming or assessing its nature;
- Determining the severity (impact) and scope (number of affected machines) of the incident;
- Recording and categorising the incident.

5.1.2 Incident coordination

- If resolution is not possible in-house, identifying the most suitable island-based incident response partner to support the requester;
- Informing the requester of their obligations, in particular filing a complaint and, in case of a personal data breach, notifying the CNIL (the French data protection authority);
- Helping, where appropriate, to forward reports to the competent State authorities depending on the nature of the incident, including but not limited to:
    - ANSSI (the French national cybersecurity agency) in case of a major cybersecurity incident that may affect other sectors;
    - the CNIL in case of a personal data breach.

5.1.3 Incident resolution support

- Proposing immediate actions, in particular emergency measures to limit the impact of the incident or to facilitate investigation and handling;
- Sharing, if needed, a short list of local providers able to resolve and remediate the incident;

- Following up on the resolution and remediation phases;
- Closure and lessons learned, where possible.

5.2 EXPOSURE SURFACE ANALYSIS AND "MON PARCOURS CYBER" DIAGNOSTICS

At the request of a constituent and with its authorisation, CyberCorsica CSIRT provides:

- An analysis of the organisation's Internet-facing exposure surface, without any intrusion into its information systems;
- A digital hygiene diagnostic, based on ANSSI's MesServicesCyber tools;
- A debriefing of findings, prioritised recommendations and, where more in-depth work is needed, referral to suitable resources or providers.

5.3 CYBER THREAT MONITORING AND TARGETED ALERTS

CyberCorsica CSIRT monitors threats, exploited vulnerabilities, attack campaigns and fraud that may concern its constituents. Information is verified, qualified and put into context before being relayed. The CSIRT provides:

- General alerts, published on www.cyber.corsica;
- Targeted alerts, sent directly to the constituents concerned when a threat targets a particular sector or type of organisation.

This service is being structured. Monitoring does not guarantee the detection of all threats.

5.4 REGIONAL CYBER SITUATION AND THREAT LANDSCAPE

Based on the incidents it is aware of and its monitoring, CyberCorsica CSIRT gradually builds an aggregated and anonymised view of the cyber threat in Corsica. It may produce:

- An annual report and incident trend summaries;
- A threat landscape specific to the territory;
- Its contribution to the joint annual report of the French territorial CSIRTs.

Publications protect the confidentiality of the information handled and do not allow a victim to be identified, even indirectly (see section 4.2).

5.5 AWARENESS RAISING, WORKSHOPS AND QUICK-REFERENCE SHEETS

CyberCorsica CSIRT carries out awareness activities across the territory, close to its constituents:

- Round tables and thematic workshops;
- Sessions tailored to the type of organisation and its maturity level, to business sectors or to local areas;
- Practical advice and quick-reference (reflex) sheets, distributed to constituents.

Topics may include phishing, passwords, backups, updates, CEO fraud and what to do in case of an incident. Formats, durations and availability are agreed case by case.

5.6 CYBER NETWORK FACILITATION AND COOPERATION WITH PARTNERS

CyberCorsica CSIRT facilitates and co-facilitates the network of cybersecurity stakeholders in Corsica. It provides:

- Introductions between organisations and the appropriate contacts;
- Sharing of useful information, according to the TLP protocol and the rules applying to each partner;

- Cooperation with sector-specific CSIRTs/CERTs, with its network and with local and national partners, in particular under cooperation agreements.

Coordination does not automatically transfer responsibility for an incident to the CSIRT.

5.7 ANALYSIS OF SUSPICIOUS URLS AND E-MAILS

Constituents may submit a suspicious URL, e-mail or file to CyberCorsica CSIRT. The CSIRT:

- Examines the item and, for an e-mail, its headers, in a suitable analysis environment that may include a sandbox, without executing anything on the user's workstation;
- Reports its observations and precautionary recommendations (blocking, reporting, preserving the item).

Constituents are asked not to send sensitive data without a secure channel (online form or PGP encryption, see section 2.8). This first-level analysis is neither a full forensic examination nor judicial evidence, and requires prior contact.

5.8 INFORMATION, PUBLICATIONS AND COMMUNICATION

CyberCorsica CSIRT provides clear and useful cyber information to its constituents and partners:

- Publications on its website www.cyber.corsica and its LinkedIn page: prevention information, alerts, news and good practices;
- Press relations, within the framework defined with the Communication Department of the Collectivité de Corse.

Published information is verified and contains no sensitive information.

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.

CULLETTIVITÀ DI CORSICA
COLLECTIVITÉ DE CORSE

CSIRT CYBER CORSICA

RFC2350 : VERSION 1.3 – OCTOBER, 22TH 2026

INFOS :

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