REGIONE CAMPANIA

CSIRT Regione Campania
RFC 2350

Finanziato dall'Unione europea
NextGenerationEU

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

REGIONE CAMPANIA

SOMMARIO

1. DOCUMENT INFORMATION

This document contains a description of Computer Security Incident Response Team of Regione Campania, which will be referred as **CSIRT Regione Campania**, in according to RFC 2350. It provides basic information about the **CSIRT Regione Campania**, its channels of communication, its roles, and responsibilities.

1.1. DATE OF LAST UPDATE

Title	CSIRT Regione Campania - RFC 2350
Version	Version: 1.1
Document Date	2025/12/11
Expiration	This document is valid until it is replaced by a later version

1.2. DISTRIBUTION LIST FOR NOTIFICATIONS

Notifications of updates of this document will be shared internally by means of **CSIRT Regione Campania** internal document management and published on the web site as described in the next section.

1.3. LOCATION WHERE THIS DOCUMENT MAY BE FOUND

The current and latest version of this document is available on the **CSIRT Regione Campania** website.

Its URL is **https://csirt.regione.campania.it/chi-siamo**.

2. CONTACT INFORMATION

2.1. NAME OF THE TEAM

Full Name	Computer Security Incident Response Team – Regione Campania
Short Name	CSIRT Regione Campania

2.2. ADDRESS

Main site: Via Don Bosco 9/E, 80141 Napoli (NA), Italy.

2.3. TIME ZONE

Rome - Central European Time (GMT+0100 and GMT+0200 from the last Sunday of March to the last Sunday of October).

2.4. TELEPHONE NUMBER

Tel: +39 0817968329

2.5. OTHER TELECOMMUNICATION

Not available.

2.6. ELECTRONIC MAIL ADDRESS

CSIRT Regione Campania can be reached via csirt@pec.regione.campania.it or csirt@regione.campania.it. All members of the **CSIRT Regione Campania Team** can read messages sent to the address csirt@regione.campania.it. Additionally, the **CSIRT Manager of CSIRT Regione Campania** can read all messages received at the address csirt@pec.regione.campania.it.

This email address is monitored by a duty officer during hours of operation. Operating days/hours are from 09:00 to 17:00 CET/CEST on business days. **CSIRT Regione Campania** may operate out of these hours and days in case of an emergency only.

If it is not possible to contact **CSIRT Regione Campania** via e-mail for security reasons, the contact may take place via telephone.

2.7. PUBLIC KEYS AND OTHER ENCRYPTION INFORMATION

To guarantee the security of communications (notifications, incident reporting, etc.) with peers, partners and constituents the PGP technology is supported.

Fingerprint	8D9B 68A6 143E C09F 768D 13E0 0434 858A EF3A 4D3A
Location	https://csirt.regione.campania.it/contatti

The key shall be used whenever information must be sent to **CSIRT Regione Campania** in a secure manner.

2.8. TEAM MEMBERS

Massimo Bisogno is the CSIRT Manager of **CSIRT Regione Campania**.

The organization of **CSIRT Regione Campania** personnel follows international best practices, with gradually increasing skills in the field of cyber security.

For each service provided by **CSIRT Regione Campania** a Service Manager and specialized figures will be identified.

2.9. OTHER INFORMATION

General information about the **CSIRT Regione Campania**, as well as links to various recommended security resources, can be found at **CSIRT Regione Campania** website: https://csirt.regione.campania.it.

2.10. POINTS OF CUSTOMER CONTACT

The best method to contact **CSIRT Regione Campania** is via e-mail at csirt@pec.regione.campania.it or csirt@regione.campania.it: the e-mails sent to this address will be handled by the responsible staff, or they will be automatically forward to the appropriate backup staff. If you require urgent assistance, put "urgent" in your subject line.

If it is not possible to use e-mail (or it is not advisable for security reasons), **CSIRT Regione Campania** can be reached by telephone.

3. CHARTER

3.1. MISSION STATEMENT

The purpose of **CSIRT Regione Campania** is, first of all, to assist members of all the facilities of Regione Campania in implementing proactive measures to reduce the risks of security incidents in their infrastructures, assisting those organizations in responding to such incidents when they occur.

Moreover, the **CSIRT Regione Campania** assists the main entities of Regione Campania in implementing proactive measures to reduce the risks of security incidents in the internal infrastructure and assist them in responding to such incidents when they occur.

3.2. CONSTITUENCY

The Constituency of **CSIRT Regione Campania** are:

- **Internal**: all Departments and Units of Regione Campania;
- **External**: upon request for affiliation, to the main entities in the regional territory who benefit from Managed Security Services provided by **CSIRT Regione Campania**.

3.3. SPONSORSHIP AND/OR AFFILIATION

CSIRT Regione Campania is affiliated with Regione Campania, and it maintains contact with various national and international CERT and CSIRT teams according to its needs and to its culture of information exchange.

3.4. AUTHORITY

The establishment of the **CSIRT Regione Campania** was mandated on 24 October 2024.

The **CSIRT Regione Campania** expects to work cooperatively with all the stakeholders involved in the service provisioning, insofar as possible, to avoid authoritarian relationships.

For the internal Constituency **CSIRT Regione Campania** has full authority, it can direct the engaged teams to perform the actions or response steps necessary to improve the security position of the organization or to recover from an incident.

For external Constituency **CSIRT Regione Campania** has no authority, it can act only as a consultant to the entity in the regional territory who benefits from Managed Security Services provided by **CSIRT Regione Campania**.

4. POLICIES

4.1. TYPE OF INCIDENT AND LEVEL OF SUPPORT

The level of support given by **CSIRT Regione Campania** will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, the criticality of the incident, and related resources available at the time, though in all cases response will be made within the agreed SLAs.

4.2. CO-OPERATION, INTERACTION AND DISCLOSURE OF INFORMATION

CSIRT Regione Campania highly considers the importance of operational coordination and information sharing among CERTs, CSIRTs, SOCs and similar bodies, and with other organizations, which may help to deliver its services, or which provide benefits to **CSIRT Regione Campania**.

Therefore, every information, report and request received from its constituencies and from third parties, will be treated with the utmost professionalism.

In the same way, the sharing of information externally will be managed with great care. In fact, **CSIRT Regione Campania** will share information about the constituencies solely for the purpose of resolving and preventing cybersecurity incidents, while implementing appropriate measures to protect the identity of the constituents.

CSIRT Regione Campania operates within the current Italian and European regulations, and follows and supports the CSIRT *Code of Conduct*, which is approved by the management of the team.

4.3. COMMUNICATION AND AUTHENTICATION

For communications between **CSIRT Regione Campania** and its constituents, the PGP key indicated in point 2.7 of the document (Public Keys and Encryption Information) will be used. For the protection of correspondence **CSIRT Regione Campania** will also use additional tools, and it is expected that those

communicating with **CSIRT Regione Campania** will use matching certification tools, such as the PGP keys themselves.

For urgent communications, the telephone/fixed line will be used, at the numbers indicated in point 2.4 of the document (Telephone Number). This method will be deemed to be sufficiently safe, subject to a short identification process.

CSIRT Regione Campania recognizes and observes the FIRST TLP – Version 2.0, as it was created to facilitate greater sharing of potentially sensitive information and more effective collaboration.

5. SERVICES

5.1. INFORMATION SECURITY EVENT MANAGEMENT

Information Security Event Management aims to identify security incidents based on the correlation and analysis of security events from a wide variety of events and contextual data sources. The information security incident management service is based on qualified and accurate data on information security events.

5.2. INFORMATION SECURITY INCIDENT MANAGEMENT

The service aims to collect and evaluate reports on information security incidents, but also to analyze relevant data and perform detailed technical analysis of the incident itself and any artifacts used. From this analysis, mitigation and steps to recover from the incident can be recommended, and constituents will be supported in applying the recommendations.

5.3. VULNERABILITY MANAGEMENT

The Vulnerability Management service includes all activities designed to assist the Constituency through detection, assessment, and management of vulnerabilities, both new and previously identified. The goal is to synchronize the activities of the Constituency to remediate or mitigate security vulnerabilities within a given perimeter.

5.4. SITUATIONAL AWARENESS

Situational Awareness encompasses all services aimed at identifying, processing, interpreting, and communicating critical elements that may impact the Constituency. Given the nature of its services, **CSIRT Regione Campania** is uniquely positioned to collect relevant data, perform analysis of threats, trends and security risks.

5.5. KNOWLEDGE TRANSFER

Knowledge Transfer service includes all the activities that enable **CSIRT Regione Campania** to share its expertise and experience with the aim of planning targeted and ongoing activities over time regarding the training and awareness of CSIRT operators at all levels, in order to keep their knowledge and skills up to date.

6. INCIDENT REPORTING

CSIRT Regione Campania does not provide any Incident Response Form on its public Web site. Incident must be reported through the dedicated ticketing platform for all the member of the Constituency or can be reported via encrypted e-mail to csirt@regione.campania.it for all the other subjects.

When reporting incidents please provide as much information as possible, such as:

- contact details and organizational information (name of person, organization name and address, email address, telephone number);
- short summary of the incident / emergency / crisis and type of event:
- the event / incident source (e.g. which system produced an alert);
- affected system(s);
- estimated impact (e.g. loss of communications);
- additional information such as details of the observations that led to the discovery of the incident - scanning results (if any), an extract from the log showing the problem, etc.

Please specify the level of confidentiality of information sent (whether public domain or not). TLP protocol is accepted and enforced. In case of absence of this information, **CSIRT Regione Campania** will assume that the information received is in the public domain and may act accordingly.

7. DISCLAIMER

Under no circumstances, including negligence, shall **CSIRT Regione Campania,** its suppliers or its collaborators, be liable for any direct, indirect, incidental, consequential damage related to the use of the information disseminated and its contents. It also includes, without limitation, damage such as loss of profits or turnover, interruption of business or professional activity, the loss of programs or other data located on your computer system or other system.

This disclaimer is not intended to circumvent compliance with the requirements prescribed by current legislation, nor to exclude liability for cases in which it cannot be excluded under the applicable legislation.