

# RFC 2350 CIRT.ME

## 1. Document information

This document contains information and describe responsibilities, services, and other information about CIRT.ME. The document complies with the requirements of RFC 2350 (<https://www.ietf.org/rfc/rfc2350.txt> )

### 1.1.Date of last update:

This is version 3.00, published in April 2026.

### 1.2.Distribution list for notifications

There is currently no distribution list for notifications about the document change.

### 1.3.Locations where this document may be found

The current version is available on CIRT.ME website on the following link: [www.gov.me/cirt/RFC2350](http://www.gov.me/cirt/RFC2350)

### 1.4.Authenticating

- Title: "RFC2350 CIRT.ME"
- Version: 3.00
- Document date: April 2026
- Expiration: This document is valid until further notice

This document has been signed with the CIRT.ME's PGP key.

## 2. Contact Information

### 2.1.Name of the team

Full name: CIRT.ME – Montenegro National Computer Incident Response Team

### 2.2.Team HQ address:

CIRT.ME  
Cetinjska 11, The Capital Plaza, The Business Tower  
81000 Podgorica  
Montenegro

### 2.3.Team time zone:

CET Central European Time (UTC+01:00)

### 2.4.Team contact telephone number:

+382 20 247 863

## **2.5. Team facsimile number:**

There's none available.

## **2.6. Other telecommunication:**

There's none available.

## **2.7. Electronic mail address**

[kontakt@asb.me](mailto:kontakt@asb.me) - for incident reporting

[info@asb.me](mailto:info@asb.me) - for other communication

## **2.8. Public keys and other encryption information:**

For encrypted communication CIRT.ME uses PGP with key signature: AADD 7E04 C26D DD80 F22B  
9CA5 F383 482E BB31 CDF7

## **2.9. Team members:**

Full list of CIRT members is not publicly available.

## **2.10. Other information:**

General information about the CIRT.ME, as well as links to various recommended security resources can be found at: [www.gov.me/cirt](http://www.gov.me/cirt)

Facebook: (<https://www.facebook.com/asb.mne/>)

Instagram: (<https://www.instagram.com/asb.mne/>)

Twitter: ([https://x.com/asb\\_mne/](https://x.com/asb_mne/))

## **2.11. Point of contact:**

Primary communication method for is via e-mail [kontakt@asb.me](mailto:kontakt@asb.me)

Secondary method is by telephone and CIRT.ME can be reached at +382 20 247 863

Working hours from Monday to Friday (07:00h-15:00h)

# **3. Team charter**

## **3.1. Mission:**

The mission of National CIRT.ME is to ensure a high and consistent level of cybersecurity across Montenegro, through close cooperation with key national and international stakeholders.

CIRT.ME is responsible for the prevention, detection, analysis, and coordinated response to cybersecurity incidents at the national level, with a particular focus on the protection of critical information infrastructure important and essential services.

In addition, CIRT.ME plays a main role in strengthening the resilience of information systems by implementing proactive security measures, issuing early warnings, providing guidance and support to stakeholders, and facilitating information sharing on emerging threats and vulnerabilities.

### **3.2.Constituents:**

CIRT.ME is the Montenegrin National CIRT and is responsible for coordinating the prevention and protection against security risks in ICT systems of critical information infrastructure at the national level. It is in charge for raising cybersecurity awareness among operators of essential and important services and entities responsible for critical infrastructure.

### **3.3.Sponsorship and/or affiliation:**

CIRT.ME is established in 2012 as part of a joint project of the Government of Montenegro and the International Telecommunication Union (ITU). CIRT.ME operates within the Cyber Security Agency.

CIRT is a member of the following organizations:

- FIRST (Forum of Incident Response Teams) - <https://www.first.org/members/teams/cirt-me>
- TF-CSIRT (Task Force on Cyber Security Incident Response Teams) - <https://www.trusted-introducer.org/trusted-introducer/directory/teams/cirtme-me/>

### **3.4.Authority:**

CIRT.ME is established in accordance with the Law on Information Security, operates within the Cyber Security Agency and is designated as the national CIRT of Montenegro, responsible for the protection of network and information systems and for responding to cybersecurity incidents at the national level.

Within its organizational structure, CIRT.ME includes dedicated units for monitoring, detection, and analysis of security events, as well as for incident coordination.

## **4. Policies**

### **4.1.Types of Incidents:**

CIRT.ME will respond to all reported incidents. Level of support provided will be factored by severity of incident, type of constituency, scope of incident and available CIRT.ME resources.

### **4.2.Cooperation, Interaction and Disclosure of Information:**

Identifiable data will be adequately protected and will not be publicly published.

All information shared by CIRT.ME will be shared by using TLP 2 protocol. More information about TLP 2 protocol and its usage can be found at [www.gov.me/cirt/tlp2](http://www.gov.me/cirt/tlp2)

CIRT.ME may share statistical information about cybersecurity incidents.

#### **4.3.Communication and Authentication:**

Email with PGP should be used for encrypted communication of sensitive information. Email without PGP should be used only for non-sensitive information sharing.

Phone communication is considered safe enough for communication.

## **5. Services**

### **5.1.Incident Response:**

This service is aimed at providing relevant and timely information such as insights into the threat landscape, known vulnerabilities, emerging attack tools and techniques, and recommended security measures necessary for the effective protection of systems and networks.

In accordance with the Law on Information Security and within its competence, CIRT.ME provides support in addressing both technical and organizational aspects of cybersecurity incidents.

### **5.2.Proactive services:**

CIRT.ME coordinates and delivers the following proactive services, to the extent possible based on available resources:

- Dissemination of key security recommendations through the website, social media channels, or direct email notifications.
- Organization of training sessions, workshops, and seminars on cybersecurity topics.
- Advisory services and guidance aimed at enhancing the cybersecurity resilience of organizations and critical systems.

## **6. Incident reporting forms**

Reports are normally sent to the e-mail address [kontakt@asb.me](mailto:kontakt@asb.me), but can also be reported via on-line form located at: <https://www.gov.me/cirt/prijavi-incident>

## **7. Disclaimer**

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