1. DOCUMENT INFORMATION

1.1. ABOUT THIS DOCUMENT

This document contains a description of Computer Emergency Response Team ENAV (hereinafter referred as to CERT-ENAV) in according to RFC 2350. It defines the basic information related to CERT-ENAV, including a brief explanation of the tasks and services offered and contacts to get in touch with us.

1.2. DATE OF LAST UPDATE

Version 1.0, updated on 15/12/2017.

1.3. LOCATIONS WHERE THIS DOCUMENT MAY BE FOUND

The current and latest version of this document is available on ENAV website.

Its URL is https://www.enav.it/sites/public/en/Corporate/Security-Operation-Center.html

1.4. AUTHENTICATING THIS DOCUMENT

This document has been signed with the GPG key of CERT-ENAV.

The public GPG key is available in CERT-ENAV website.

1.5. DOCUMENT IDENTIFICATION

Title: CERT-ENAV - RFC 2350

Version: 1.0.

Document Date: 15/12/2017

Expiration: this document is valid until it is replaced by a later version

2. CONTACT INFORMATION

2.1. NAME OF THE TEAM

Full Name: CERT ENAV

Short Name: CERT-ENAV

2.2. ADDRESS

Postal Address: CERT-ENAV Via Appia Nuova, 1491, 00178 Rome, Italy.

2.3. TIME ZONE

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

2.4. TELEPHONE NUMBER

Tel: (H24/7 365 day) +39 06 79086556.

2.5. ELECTRONIC MAIL ADDRESS

To communicate with CERT-ENAV is possible to send an email to cert@enav.it. All members of CERT-ENAV team can read messages sent to this address.

2.6. PUBLIC KEYS AND OTHER ENCRYPTION INFORMATION

In order to guarantee the security of communications the GPG technology is supported. CERT-ENAV public GPG key for cert@enav.it is available on the public GPG key servers and on CERT-ENAV website.

Public Key of CERT-ENAV:

- USER-ID: CERT-ENAV cert@enav.it
- KEY-ID: 0x97ACC23E
- Fingerprint: 66C34586BFAE7FD4B5827CC17D6910A397ACC23E

Third parties to establish a security communication with CERT-ENAV shall use GPG public key.

2.7. TEAM MEMBERS

The CERT-ENAV team leader is Giovanni Mellini. The team is made up of Cyber Security specialist and SOC Analyst.

3. OTHER INFORMATION

General information about CERT-ENAV can be found on CERT-ENAV website: https://www.enav.it/sites/public/en/Corporate/Security-Operation-Center.html

3.1. POINTS OF COSTUMER CONTACT

The preferred method to contact CERT-ENAV is by email: cert@enav.it.

The mailbox is checked 24h/7days.

The use of GPG is required to send confidential or sensitive information.

If is not possible to contact CERT-ENAV via e-mail for security reasons, the contact may take place via telephone.

3.2. CHARTER

3.2.1. MISSION STATEMENT

The CERT-ENAV mission is to support and protect its constituency from potentially critical cyber threats having concrete possibility to compromise company operational capability or to pose a serious threat to information security.

CERT-ENAV will operate according to the following key values:

- Highest standards of ethical integrity;
- Improve cyber-security awareness and culture;
- High degree of service orientation and operational readiness;
- Effective responsiveness in case of incidents and emergencies and maximum commitment to resolve the issues;
- Facilitating the exchange of good practices between constituents and with peers;

3.2.2. CONSTITUENCY

The constituency of CERT-ENAV is composed by ENAV Spa and its subsidiary Techno Sky Srl which are part of the ENAV Group.

3.2.3. SPONSORSHIP AND/OR AFFILIATION

CERT-ENAV maintains contacts with various national and international CERT/CSIRT teams, with FIRST, TF-CSIRT and Carnegie Mellon University according to its needs and the information exchange culture that it values.

3.2.4. AUTHORITY

The establishment of the CERT-ENAV was mandated via corporate directive on 01/09/2017.

3.3. POLICIES

3.3.1. TYPE OF INCIDENT AND LEVEL OF SUPPORT

CERT-ENAV manage and address information security incidents, which occur or threaten to occur in its constituency. The level of support given by CERT-ENAV will vary depending on the severity of the information security incident, the related assets impacted and the CERT's resources at the time.

3.3.2. CO-OPERATION, INTERACTION AND DISCLOSURE OF INFORMATION

CERT-ENAV highly considers the importance of operational coordination and information sharing among CERTs, CSIRTs, SOCs and similar bodies, and also with other organizations, which may aid to deliver its services or which provide benefits to CERT-ENAV.
CERT-ENAV recognizes and supports the ISTLP (Information Sharing Traffic Light Protocol).

3.3.3. COMMUNICATION AND AUTHENTICATION

CERT-ENAV protects sensitive information in accordance with relevant local regulations and policies. Communication security (which includes both encryption and authentication) is achieved using primarily GPG or any other agreed means, depending on the sensitivity level and context.

4. SERVICE

4.1. INCIDENT MANAGEMENT

CERT-ENAV performs incident handling, response on-site, support and coordination for its constituency through its internal structure. The incident management services as developed by CERT-ENAV covers all “5 steps”:

- Preparedness and prevention;
- Detection;
- Analysis;
- Response;
- Recovery;

4.2. THREAT INTELLIGENCE

The CERT-ENAV performs the threat intelligence services in order to improve prevention, detection, identification and information security incidents response capabilities and strength the ENAV Group cyber security posture.

5. INCIDENT REPORTING FORM

CERT-ENAV does not provide any incident reporting form in a public web page.
For CERT-ENAV’s constituency, the incident reporting must follow the internal procedures.

6. DISCLAIMERS

While every precaution will be taken in the preparation of information, notification and alerts, ENAV assumes no responsibility for errors or omissions, or for damages resulting fron the use of the information contained within.