1. DOCUMENT INFORMATION

1.1. ABOUT THIS DOCUMENT

This document contains a description of Computer Emergency Readiness Team - Terna (hereinafter referred as to TERNA-CERT) in according to RFC 2350. It defines the basic information related to TERNA-CERT, 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 19/04/2019.

1.3. LOCATIONS WHERE THIS DOCUMENT MAY BE FOUND

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

Its URL is https://www.terna.it/en-gb/chi-siamo/trasparenzaeintegrita/securityoperationscenter.aspx

1.4. AUTHENTICATING THIS DOCUMENT

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

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

1.5. DOCUMENT IDENTIFICATION

Title: TERNA-CERT - RFC 2350

Version: 1.0.

Document Date: 19/04/2019

Expiration: this document is valid until a later version is issued.

2. CONTACT INFORMATION

2.1. NAME OF THE TEAM

Full Name: Computer Emergency Readiness Team - Terna

Short Name: TERNA-CERT

2.2. ADDRESS

Postal Address: TERNA-CERT Via della Marcigliana 911, Roma 00138, 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 83157835.

2.5. ELECTRONIC MAIL ADDRESS

The email cert@terna.it is available to contact TERNA-CERT. All members of TERNA-CERT team can read the 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 employed. TERNA-CERT's public GPG key for cert@terna.it is available on TERNA-CERT website.

TERNA-CERT's Public Key:

- USER-ID: TERNA-CERT cert@terna.it
- KEY-ID: 0x6AC6F72B
- Fingerprint: 62E7F92DD38D1B36322B5F88383458716AC6F72B

Third parties shall use GPG public key to establish a secure communication with TERNA-CERT.

2.7. TEAM MEMBERS

TERNA-CERT's team leader is Matteo Macina. The team is composed of CERT Analysts.

3. OTHER INFORMATION

General information about TERNA-CERT are available on Terna website: https://www.terna.it/en-gb/chi-siamo/trasparenzaeintegrita/securityoperationscenter.aspx

3.1. POINTS OF COSTUMER CONTACT

The email address cert@terna.it is the preferred method to contact TERNA-CERT.

The mailbox is monitored 24/7.

The use of GPG is mandatory when confidential or sensitive information are involved.

If for security reasons it is not possible to get in touch with TERNA-CERT via e-mail, the contact may take place via telephone.

3.2. CHARTER

3.2.1. MISSION STATEMENT

The TERNA-CERT mission is:

- Guarantee real-time centralized monitoring of the security status of the Group's ICT platforms in the IT and OT environment;
- Manage communication ("Cyber Security Situational Awareness") both internal and external and escalation processes/procedures during Cyber Security Incidents and coordinate the response actions.
- Ensure the development and management of "Threat Intelligence" tools, of the ones used to monitor the Cyber Security status, to respond to the incidents and of external/internal digital tools, like Digital Signature, Certified email (PEC), Encryption and Authentication for the Group.

3.2.2. CONSTITUENCY

The Constituency consists of the entire Gruppo Terna. All companies receive support from Terna-CERT--within the established service contract--in the execution of the operational activities of Incident Management Process related to Security Information and in the management and notification of any Data Breach.

3.2.3. SPONSORSHIP AND/OR AFFILIATION

TERNA-CERT is affiliated to Terna S.p.A.

It maintains contacts with various national and international CERT and CSIRT teams, with FIRST, TFCSIRT, ENISA and Carnegie Mellon University according to its needs and to its culture of information exchange.

3.2.4. AUTHORITY

The establishment of the TERNA-CERT was mandated via corporate directive on 01/01/2018.

3.3. POLICIES

3.3.1. TYPE OF INCIDENT AND LEVEL OF SUPPORT

TERNA-CERT manages and addresses information security incidents, which occur or threaten to occur within its constituency. The level of support given by TERNA-CERT will vary depending on the severity of the information security incident, the assets impacted and the CERT's currently available resources.

3.3.2. CO-OPERATION, INTERACTION AND DISCLOSURE OF INFORMATION

TERNA-CERT highly values the importance of operational coordination and information sharing among CERTs, CSIRTs, SOCs and similar parties, as well as other organizations, which may aid them in delivering their services or provide other benefits.
TERNA-CERT recognizes and supports ISTLP (Information Sharing Traffic Light Protocol).

3.3.3. COMMUNICATION AND AUTHENTICATION

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

4. SERVICE

4.1. INCIDENT MANAGEMENT

TERNA-CERT performs incident handling and provides its constituency with support, on-site response and coordination through its internal structure. The incident management services as developed by TERNA-CERT cover all the “5 steps”:

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

4.2. THREAT INTELLIGENCE

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

5. INCIDENT REPORTING FORM

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

6. DISCLAIMERS

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