Enel CERT - RFC 2350 profile

1 Document Information

This document contains a description of Enel CERT (Cyber Emergency Readiness Team) as implemented by RFC 2350. It provides basic information about Enel CERT, its channels of communication, its roles and responsibilities.

1.1 Date of Last Update

Version 1.0, updated on 29/05/2017.

1.2 Distribution List for Notifications

There is no distribution list for notifications.

1.3 Locations where this Document may be found

The current and latest version of this document is available on Enel CERT website. Its URL is: https://cert.enel.com

1.4 Authenticating this Document

This document has been signed with the PGP key of Enel CERT. The signature is available from Enel CERT's website. Its URL is: https://cert.enel.com

1.5 Document Identification

Title:	Enel CERT - RFC 2350 profile
Version:	1.0
Document Date:	29/05/2017

Expiration: this document is valid until superseded by a later version

2 Contact Information

2.1 Name of the Team

Enel CERT (Cyber Emergency Readiness Team)

2.2 Address

Corso Regina Margherita 267, 10143 Torino, Italy

2.3 Time Zone

CET/CEST

2.4 Electronic Mail Address

If you need to notify us about an information security incident or a cyber-threat targeting or involving Enel, please contact us at: cert@enel.com

2.5 Facsimile Number

None.

2.6 Other Telecommunication

None.

2.7 Public Keys and Encryption Information

PGP/GnuPG is supported for secure communication.
The PGP public key for the email address cert@enel.com is available on the public PGP keyservers and on Enel CERT website. Public Key of Enel CERT:

User-ID:	Enel CERT <cert@enel.com>
Key-ID:	9120ADA6
Fingerprint:	F0F2E177D09AF248860EDCF4B04A67F89120ADA6

2.8 Team Members

Enel CERT’s team leader is the Head of CERT. The team consists of Cyber Security analysts.

2.9 Other Information

General information about Enel CERT can be found at the following URL: https://cert.enel.com

2.10 Points of Customer Contact

The preferred method to contact Enel CERT is to send an email to the following address: cert@enel.com
A duty security analyst can be contacted at this email address during hours of operation.
Enel CERT’s hours of operation follow regular business hours (09:00 to 16:00, Monday to Friday).

3 Charter

3.1 Mission Statement

Enel CERT mission is to support and protect Enel, from intentional and malicious attacks that would hamper its Constituency. Enel CERT's activities cover prevention, detection, response and recovery.
The actions taken by Enel CERT are driven by several key values available in the following Enel’s Code of Ethics: https://www.enel.com/en/investors/a201608-code-of-ethics.html

3.2 Constituency

The Constituency of Enel CERT includes all the employees and assets of Enel Group, worldwide.

3.3 Affiliation

Enel CERT is affiliated to Enel S.p.A.

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

3.4 Authority

Enel CERT operates under the authority of Enel’s Organization and Procedures.

4 Policies

4.1 Types of Incidents and Level of Support

Enel CERT is authorized to handle all types of cyber attacks that would hamper confidentiality, integrity and availability of Enel Constituency.

The level of support given by Enel CERT will vary, depending on the severity of the security incident, its potential or assessed impact and the available Enel CERT’s resources at the time.

4.2 Co-operation, Interaction and Disclosure of Information

Enel CERT 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 Enel CERT.

Enel CERT also recognizes and supports the ISTLP (Information Sharing Traffic Light Protocol).

4.3 Communication and Authentication

Enel CERT protects sensitive information in accordance with relevant Local regulations and policies.

Communication security (which includes both encryption and authentication) is achieved using primarily PGP or any other agreed means, depending on the sensitivity level and context.

5 Services

5.1 Incident Response coordination

Enel CERT performs incident response for its constituency. The incident response service as developed by Enel CERT covers all “5 steps”: preparedness and prevention, detection, analysis, response, recovery.

6 Incident Reporting Forms

No local form has been developed to report incidents to Enel CERT.

In case of incident, please provide Enel CERT at least the following information:

- email address;
- any relevant technical element with associated observation (e.g. IP address, FQDN);
- in case you wish to forward any emails to Enel CERT, please include all email headers, body and any attachments if possible and as permitted by the regulations, policies and legislation under which you operate.

7 Disclaimers

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