

TotalEnergies CERT RFC 2350

1. Document Information	2
1.1 Date of the Last Update	2
1.2 Distribution List for Notifications.....	2
1.3 Location where this Document May be Found.....	2
1.4 Document authenticity	2
1.5. Document Identification	2
2. Contact information.....	2
2.1 Name of the team	2
2.2 Postal Address.....	2
2.3 Time Zone.....	3
2.4 Telephone Number	3
2.5 Facsimile Number	3
2.6 Electronic Mail Address.....	3
2.7 Public Keys and Encryption Information.....	3
2.8 Team Members	3
2.9 Other information	3
2.10 Points of Contact.....	3
3. Charter	4
3.1 Mission Statement	4
3.2 Constituency	4
3.3 Sponsoring Organization / Affiliation.....	4
3.4 Authority	4
4 Policies	4
4.1 Types of Incidents and Level of Support.....	4
4.2 Co-operation, Interaction and Disclosure of Information	4
4.3 Communication and Authentication.....	5
5 Services	5
5.1 Incident Response	5
5.2 Proactive Activities.....	5
6. Incident Reporting Forms	5
7. Disclaimers	5

1. Document Information

This document contains a description of TotalEnergies CERT according to RFC 2350¹. It provides basic information about the TotalEnergies CERT, its responsibilities and services offered by TotalEnergies CERT.

1.1 Date of the Last Update

This is the version 1.2 published on June 10st, 2021.

1.2 Distribution List for Notifications

Notification of document changes is not distributed by a mailing list or any other mechanisms.

1.3 Location where this Document May be Found

The current and latest version of this document is available on TotalEnergies's website at: <https://www.totalenergies.com/cert>

1.4 Document authenticity

This document has been signed with the PGP Key of TotalEnergies CERT.

The PGP public key, ID and fingerprint are available on the TotalEnergies website at: <https://www.totalenergies.com/cert>

1.5. Document Identification

Title: 'CERT_TotalEnergies_RFC2350_EN_v1.2'

Version: 1.2

Document Date: June 10th, 2021

SHA-256

Expiration: this document is valid until superseded by a later version.

2. Contact information

2.1 Name of the team

Official name: TotalEnergies CERT

Short name: TotalEnergies CERT

2.2 Postal Address

TotalEnergies CERT

Direction des Systèmes d'Information Groupe (DG/STI/SI)

2 place Jean Millier

¹ <https://www.ietf.org/rfc/rfc2350.txt>

Arche Nord Coupole/Regnault
92078 PARIS LA DEFENSE CEDEX
FRANCE

2.3 Time Zone

CET/CEST

2.4 Telephone Number

Main number (duty office): +33 141352203

2.5 Facsimile Number

N/A

2.6 Electronic Mail Address

If you need to notify us about an information security incident or a cyber-threat targeting or involving TotalEnergies CERT, please contact us at: [contact\[at\]cert.total](mailto:contact[at]cert.total).

2.7 Public Keys and Encryption Information

TotalEnergies CERT uses the following PGP Key:

User ID: [contact\[at\]cert.total](mailto:contact[at]cert.total)

Key ID: 0xB2F5B2F5D0E4AE28

Fingerprint: 2C2D 5AEB 78C7 3E1C 95EB 428F B2F5 B2F5 D0E4 AE28

The PGP key can be retrieved from applicable public key servers such as <https://pgp.mit.edu>.

2.8 Team Members

The list of the team members is not publicly available. The identity of TotalEnergies CERT's team members might be disclosed on a case by case basis according to the need to know restrictions.

2.9 Other information

See our web site at <https://www.totalenergies.com/cert> for additional information about TotalEnergies CERT.

2.10 Points of Contact

The preferred method for contacting TotalEnergies CERT is via e-mail at [contact\[at\]cert.total](mailto:contact[at]cert.total).

Please use our cryptographic key to ensure integrity and confidentiality. In case of emergency, please specify the [URGENT] tag in the subject field in your e-mail.

If it is not possible (or not advisable for security reasons) to use e-mail, the TotalEnergies CERT can be reached by telephone during regular office hours (local time). Telephone messages are checked on a regular basis.

TotalEnergies CERT operates during regular business hours (9:00 AM-6:00 PM CET/CEST,

from Monday to Friday).

3. Charter

3.1 Mission Statement

TotalEnergies CERT assists TotalEnergies Group entities and TotalEnergies Group affiliates (as defined hereafter) in managing all types and scales of cybersecurity incident.

TotalEnergies CERT is responsible for coordinating the incident response and cybersecurity assessment across TotalEnergies Group entities and TotalEnergies Group affiliates.

3.2 Constituency

The constituency of TotalEnergies CERT is composed of TotalEnergies Group entities² and TotalEnergies Group affiliates³.

3.3 Sponsoring Organization / Affiliation

TotalEnergies CERT is a private CERT in the energy sector (oil & gas and electricity). It is set up and operated by TotalEnergies S.E.

It maintains relationships with different national and international CSIRTs and CERTs.

3.4 Authority

TotalEnergies CERT operates under the authority of the TotalEnergies Group CISO.

4 Policies

4.1 Types of Incidents and Level of Support

TotalEnergies CERT's assistance may be requested in all types of cybersecurity incidents that may occur within its constituencies.

The level of support depends on the type and severity of the given security incident, the amount of affected entities, and our resources at the time.

4.2 Co-operation, Interaction and Disclosure of Information

TotalEnergies CERT can collaborate with other CSIRTs and CERTs as well as with other affected third parties to the extent they are involved in the incident or incident response process.

Information received by TotalEnergies CERT may be shared with TotalEnergies Group entities and TotalEnergies Group affiliates, as well as to cybersecurity service providers, on a need to know basis.

² Group "entity" refers to a Group branch, division, department, or other business segment

³ Group "affiliate" refers to a company in which TotalEnergies S.E. holds, directly or indirectly, the majority of the voting rights

4.3 Communication and Authentication

The preferred method of communication is email. For the exchange of sensitive information and authenticated communication TotalEnergies CERT uses several encryption solutions. By default, all sensitive communication should be encrypted with our public PGP key detailed in Section 2.7.

General non-restricted information can be transmitted by telephone, regular mail or unencrypted email.

TotalEnergies CERT respects the Information Sharing Traffic Light Protocol (TLP) that comes with the tags WHITE, GREEN, AMBER or RED.

5 Services

5.1 Incident Response

TotalEnergies CERT will assist TotalEnergies Group entities and TotalEnergies Group affiliates in handling the technical and organizational aspects of security incidents:

- Incident handling
- Incident analysis
- Incident response on site
- Incident response support
- Incident response coordination
- Artifact analysis
- Artifact response
- Artifact response coordination

5.2 Proactive Activities

TotalEnergies CERT coordinates and maintains the following services to the extent possible depending on its resources:

- Cybersecurity assessments

6. Incident Reporting Forms

There is no specific security incident reporting form. Incidents should be reported via encrypted e-mail.

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, TotalEnergies CERT shall not be responsible for any errors or omissions, or for any damages resulting from or arising out of the use of the information contained herein and therein.