CERT-GRDF

RFC 2350

VERSION : RFC2350 V1.6

TLP:CLEAR

1. Document Information

This document contains a description of CERT-GRDF according to RFC 2350.
It provides information about the CERT-GRDF, how to contact the team, and describes its responsibilities and services offered by CERT-GRDF.

1.1. Date of Last Update

The current version of this document is version 1.5 and was released on October 21th, 2024.

1.2. Distribution List for Notifications

There is no distribution list for notifications.

1.3. Locations where this Document May Be Found

The current version of this document is available on GRDF public web site, at the following location: https://www.grdf.fr/cert

1.4. Authenticating this Document

This document has been signed with the PGP key of CERT-GRDF. The signature is available at: https://www.grdf.fr/cert

1.5. Document Identification

Title: CERT-GRDF RFC 2350
Version: 1.6
Document Date: 2026/01/08
Expiration: this document is valid until superseded by a later version

2. Contact Information

2.1. Name of the Team

Shortname: CERT-GRDF

Full name: CERT-GRDF is a part of the “Pôle Cyberdéfense” of GRDF.

2.2. Address

CERT-GRDF – Pôle Cybersécurité Opérationnelle
17 Rue des Bretons
93210 Saint-Denis
FRANCE

2.3. Time Zone

CET/CEST: Europe/Paris (GMT+01:00, and GMT+02:00 on DST)

2.4. Telephone Number

+33 9 69 37 05 38

2.5. Facsimile Number

CERT-GRDF does not use Facsimile, please choose another communication technology.

2.6. Other Telecommunication

None available

2.7. Electronic Mail Address

cert[at]grdf.fr

2.8. Public Keys and Encryption Information

PGP is used for functional exchanges with CERT-GRDF

- User ID: CERT GRDF <cert[at]grdf.fr>
- Key ID: 0xDB6AA1C1867C3CC4
- Fingerprint: 8F55 5C42 3A69 6F52 4C33 83B5 DB6A A1C1 867C 3CC4

The public PGP key is available at: https://www.grdf.fr/cert

2.9. Team Members

The preferred method to contact the CERT-GRDF is by sending an email using the following address : cert[at]grdf.fr

2.10. Other Information

None

2.11. Points of Customer Contact

The preferred method to contact CERT GRDF is to send an email to the following address: cert[at]grdf.frè

Please use our PGP key to ensure integrity and confidentiality.

In case of emergency, please specify the [URGENT] tag in the subject field in your e-mail.

CERT-GRDF can be joined on business hours between 09:00 to 18:00, from Monday to Friday.
Outside of business hours, an analyst can be joined at the following number:
+33 9 69 37 05 38

3. Charter

3.1. Mission Statement

The CERT-GRDF is responsible for monitoring, responding to, and mitigating computer security incidents affecting the organization's information systems and networks.
The team's primary objectives are to protect the confidentiality, integrity, and availability of the organization's critical assets, minimize the impact of security incidents, and provide relevant security intelligence to support the organization's risk management and decision-making processes.

3.2. Constituency

The CERT-GRDF serve the entire GRDF Organization, including all departments, subsidiaries, and affiliated entities.

3.3. Sponsorship and/or Affiliation

CERT-GRDF is sponsored and supported by the GRDF Organization's Executive Leadership and IT/Security Management teams.
It's a private CSIRT in the energy sector.
It is owned, operated, and financed by GRDF.

3.4. Authority

The CERT-GRDF operates with the authority delegated by CIO and the CISO of GRDF and is responsible to anticipate, detect, react and coordinate the remediation across the whole company for all perimeters (corporate and industrial IT systems).

4. Policies

4.1. Types of Incidents and Level of Support

CERT-GRDF handles all the incidents with a security or personal data component such as

- Abusive Content
- Malicious Code
- Information Gathering
- Intrusion Attempts
- Intrusion
- Information Content Security
- Vulnerable

The services provided are :

- Incident detection
- Incident analysis and forensics
- Incident response and remediation coordination
- Vulnerability and threat intelligence analysis
- Vulnerability response and coordination

CERT-GRDF will adjust the level of support depending on the incident's severity, its potential impact and the available staff resources at the time of the incident.

4.2. Co-operation, Interaction and Disclosure of Information

The CERT-GRDF value the importance of cooperation with his peers.

The CERT-GRDF proceed to exchange with others CERTs , CSIRTs about technical topics, process or services evolutions.
It maintains relationships with different CSIRTs in France

4.3. Communication and Authentication

CERT-GRDF strongly encourage you to send email signed using a PGP Key. All emails containing restricted information must be encrypted using our PGP-Key.

For general non-restricted communication, a phone-call or unencrypted email may be used.

CERT-GRDF supports the Information Sharing Traffic Light Protocol (TLP).

5. Services

5.1. Incident response

5.1.1. Incident Triage

The CERT-GRDF triage is divided in several parts to contextualize, categorize and define a severity level associated to the incoming incident.

5.1.2. Incident Coordination

The CERT-GRDF ensures Information security incident coordination and Crisis management support for its constituency and acts as point-of-contact with internal constituency and external partners when needed

5.1.3. Incident Resolution

In regards to the Incident categorization and severity level the resolution could involve

- Information security incident analysis ;
- Artefact and forensic evidence analysis ;
- Mitigation and recovery.

5.2. Proactive activities

The CERT-GRDF team offers the following proactive services:

- Threat intelligence monitoring;
- IOC Sharing
- Vulnerability exposure monitoring

6. Incident Reporting Forms

CERT-GRDF does not have public incident reporting form.

We encourage you to report any security incidents via encrypted e-mail to cert[at]grdf.fr

Incident reports must contain the following information:

- Brief description of the incident : occurrence date & time (dd/mm/yyyy hh:mm) including time zone
- Basic information of the affected system :
    - Source Ips, ports and protocols
    - Destination Ips, ports and protocols
    - Domain or url
    - IP address
    - Any relevant information

7. Disclaimers

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