



BUREAU
VERITAS

TLP:CLEAR 

CERT-BV - RFC2350

Bureau Veritas

ISS Technology
Version n°1.3 - 06/2025



Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

TLP:CLEAR information may be distributed without restriction, subject to copyright controls

1. Introduction

1.1 Date of Last Update

Version 1.0, published on 2025/03/07 – Initial Version

Version 1.1, published on 2025/03/21 - Minor corrections

Version 1.2, published on 2025/04/03 - Minor corrections

Version 1.3, published on 2025/06/02 – Minor corrections

1.2 - Distribution List of Notifications

Changes to that document are notified to:

_ InterCERT France / Network of French CSIRTs - <https://intercert-france.fr>

1.3 - Locations where this document may be found

The current and latest version of this document is available at CERT-BV's website at:

https://group.bureauveritas.com/about-us/cert/CERT-BV_RFC2350_EN.pdf

1.4 - Authenticating this document

This document has been signed with the PGP key of CERT-BV.

The signature and our public PGP key (ID and fingerprint) are available on our website:

<https://group.bureauveritas.com/about-us/cert/>

1.5 - Document Identification

Title : 'CERT-BV_RFC2350_EN'

Expiration: this document is valid until superseded by a later version

2. Contact Information

This document contains a description of CERT BUREAU VERITAS as implemented by RFC 2350.

It provides basic information about CERT BUREAU VERITAS, its channels of communication, its roles and responsibilities.



2.1 - Name of the team

Official Name:

Computer Emergency Response Team Bureau Veritas

Short Name:

CERT-BV

2.2 - Address

CERT Bureau Veritas
4, pl Saisons – Tour Alto
92400 Courbevoie
France

2.3 - Time Zone

CET – Central Europe Time (UTC/GMT + 1 hour)

CEST – Central Europe Summertime (UTC/GMT + 2 hours)

2.4 - Telephone Number

To be defined

2.5 - Facsimile Number

Not Applicable

2.6 - Other Telecommunication

Not Applicable

2.7 - Electronic Mail Address

If you need to notify us about an information security incident or a cyber-threat targeting or involving CERT-BV, please contact us at:

cert[at]bureauveritas[dot]com

2.8 - Public Keys and Encryption Information

PGP is used for functional exchanges with CERT-BV.

User ID: CERT-BV - Key ID: 0x3DC13EC5

Fingerprint: 8CD7 8051 686C 2D9E 44DA FD29 7932 5352 3DC1 3EC5

The public PGP key is available at the following location: <https://group.bureauveritas.com/about-us/cert/>



2.9 - Team Members

CERT-BV team is composed of IT security experts. The list of CERT-BV team members is not publicly available. The identity of CERT-BV team members might be shared on a case-by-case basis according to the need-to-know restrictions.

2.10 - Point of Contacts

The primary and preferred method to send incident reports is via e-mail at **cert[at]bureauveritas[dot]com**. Please use our cryptographic key to ensure integrity and confidentiality. In case of emergency, please use the [URGENT] tag in the subject field in your e-mail.

A telephone call, a postal service or an unencrypted email can be used for non-sensitive information sharing. CERT-BV's hours of operation are 9am/6PM CET from Monday to Friday on business days for France.

3. Charter

3.1 - Mission Statement

The CERT of Bureau Veritas's mission is to coordinate and investigate IT security incident response for the Group Bureau Veritas.

The CERT of Bureau Veritas will investigate any security incident that may involve a Bureau Veritas Group subsidiaries or Bureau Veritas as a source or target of an attack or any cyber-threat.

3.2 - Constituency

Our constituency is composed of Bureau Veritas Group and all subsidiaries. This only concerns the countries where Bureau Veritas Group is operating.

3.3 - Sponsorship and/or affiliation

CERT-BV is the Computer Emergency Response Team (CERT) for the Group Bureau Veritas. Its funding is provided by Bureau Veritas Group.

3.4 - Authority

CERT-BV of Bureau Veritas coordinate security incidents concerning our constituency.

4. Policies

4.1 - Types of incidents and level of support

The CERT of Bureau Veritas addresses all kinds of security incidents which occur, or threaten to occur, within its constituency.

The level of support depends on the type and severity of the given security incident.



4.2 - Co-operation, interaction and disclosure of information

Bureau Veritas CERT's will exchange all necessary information with other CERT / CSIRT as well as with other affected parties if they are involved in the incident or incident response process.

Legal requests will be evaluated by our legal department and an appropriate response will be given if the request is acceptable, within the limits of the court order, the related investigation and the information requested

4.3 - Communication and authentication

The preferred method of communication is email.

For the exchange of sensitive information and authenticated communication CERT-BV uses PGP for encrypting and/or signing

5. Services

5.1 - Incident Response Services

CERT-BV provides the following Incident Response Services:

Information Security Incident Management:

- Incident analysis and investigation
- Incident response support
- Incident response coordination

Information Security Event Management:

- Monitoring and Detection
- Event Analysis
- Threat Intelligence coordination

Vulnerability Management:

- Vulnerability Report Intake
- Vulnerability Coordination

5.2 - Proactive Services

In order to adapt its diagnostic capacity, CERT-BV provides the following Proactive Services:

- Monitoring of threats and vulnerabilities
- Analysis of attack scenarios and the cybersecurity measures to protect Information systems.
- Threat Hunting

CERT-BV is also providing Cybersecurity awareness and communication to its constituency in order to warn and prevent risks and limit their consequences.



6. Incidents Reporting Forms

CERT-BV does not have an incident reporting form. Please report security incidents via encrypted e-mail to [cert\[at\]bureauveritas\[dot\]com](mailto:cert[at]bureauveritas[dot]com)

Incident reports should contain the following information when possible:

- Incident date and time (including time zone)
- Description of the Incident
- Source/ Destination IPs, ports, and protocols
- Any other relevant information

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, CERT-BV assumes no responsibility for errors or omissions, or for prejudice resulting from the use of the information contained within. If you notice any error in this document, please notify us by email. We will try to rectify the information as soon as possible.