



BUREAU  
VERITAS

TLP:CLEAR 

# CERT-BV - RFC2350

## Bureau Veritas

ISS Technology  
Version n°1.3 - 06/2025



Les sources peuvent utiliser TLP:CLEAR lorsque l'information comporte un risque minimal ou nul d'utilisation abusive, conformément aux règles et procédures applicables pour la diffusion publique.

Les documents TLP:CLEAR peuvent être distribués sans restriction, sous réserve des contrôles de droits d'auteur.

## 1. Introduction

### 1.1 Date de dernière mise à jour

Version 1.0, publiée le 07/03/2025 – Version initiale

Version 1.1, publiée le 21/03/2025 – Corrections mineures

Version 1.2, publiée le 03/04/2025 – Corrections mineures

Version 1.3, publiée le 02/06/2025 – Corrections mineures

### 1.2 – Liste de Distribution des Notifications

Les changements de ce document sont notifiés à :

\_ InterCERT France / Réseau de CSIRTs Français - <https://intercert-france.fr>

### 1.3 – Endroit où ce document peut être trouvé

La dernière version courante de ce document est disponible sur le site web du CERT-BV à l'adresse suivante :

[https://group.bureauveritas.com/fr/groupe/cert/CERT-BV\\_RFC2350\\_FR.pdf](https://group.bureauveritas.com/fr/groupe/cert/CERT-BV_RFC2350_FR.pdf)

### 1.4 – Authentification de ce document

Ce document a été signé numériquement via la clé PGP de CERT-BV.

La signature et la clé publique PGP (ID et empreinte) sont disponible sur notre site web :

<https://group.bureauveritas.com/fr/groupe/cert/>

### 1.5 – Identification de ce Document

Titre : 'CERT-BV\_RFC2350\_FR'

Date d'expiration : Ce document est valide jusqu'à ce qu'une version plus récente soit validée.

## 2. Information de Contact

Ce document contient la description de CERT BUREAU VERITAS tel qu'implémenté dans la RFC 2350.

Il fournit des informations basiques à propos de CERT BUREAU VERITAS, ses moyens de communications, ses rôles et responsabilités.



## 2.1 – Nom de l'équipe

Nom Officiel :

Computer Emergency Response Team Bureau Veritas

Nom Court :

CERT-BV

## 2.2 - Adresse

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

## 2.3 – Fuseaux Horaires

CET – Central Europe Time (UTC/GMT + 1 heure)  
CEST – Central Europe Summertime (UTC/GMT + 2 heures)

## 2.4 – Numéro de Téléphone

*A définir*

## 2.5 – Numéro de Facsimile

Non Applicable

## 2.6 – Autres moyens de Télécommunication

Non Applicable

## 2.7 – Adresse e-mail

Si vous devez nous notifier un incident de sécurité de l'information ou une menace cybernétique ciblant ou impliquant CERT-BV, veuillez nous contacter à l'adresse suivante :

cert[at]bureauveritas[dot]com

## 2.8 – Informations lié au Chiffrement et Clé Publique

PGP est utilisé pour les échanges fonctionnels avec CERT-BV.

ID utilisateur : CERT-BV - ID de clé : 0x3DC13EC5

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

La clé publique PGP est disponible à l'emplacement suivant : <https://group.bureauveritas.com/fr/groupe/cert>



## 2.9 – Membres de l'Équipe

L'équipe CERT-BV est composée d'experts en sécurité informatique. La liste des membres de l'équipe CERT-BV n'est pas publiquement disponible.

L'identité des membres de l'équipe CERT-BV peut être partagée au cas par cas selon les restrictions du "besoin d'en connaître".

## 2.10 - Point de Contact

La méthode principale et préférée pour envoyer des rapports d'incident est par e-mail à l'adresse [cert\[at\]bureauveritas\[dot\]com](mailto:cert[at]bureauveritas[dot]com).

Veuillez utiliser notre clé cryptographique pour assurer l'intégrité et la confidentialité. En cas d'urgence, veuillez utiliser le tag "[URGENT]" dans le champ "Objet" de votre e-mail.

Un appel téléphonique, un service postal ou un e-mail non chiffré peuvent être utilisés pour le partage d'informations non sensibles.

Les heures d'ouverture de CERT-BV sont de 9h à 18h CET du lundi au vendredi, les jours ouvrables en France.

# 3. Charte

## 3.1 - Déclaration de mission

La mission du CERT de Bureau Veritas est de coordonner et d'enquêter sur la réponse aux incidents de sécurité informatique pour le Groupe Bureau Veritas.

Le CERT de Bureau Veritas enquêtera sur tout incident de sécurité susceptible d'impliquer une filiale du Groupe Bureau Veritas ou Bureau Veritas en tant que source ou cible d'une attaque ou de toute menace cyber.

## 3.2 - Juridiction

Notre juridiction se compose du Groupe Bureau Veritas et de toutes ses filiales. Cela concerne uniquement les pays où le Groupe Bureau Veritas est présent.

## 3.3 - Sponsorship et/ou affiliation

CERT-BV est l'Équipe d'intervention en cas d'urgence informatique (CERT) pour le Groupe Bureau Veritas. Son financement est assuré par le Groupe Bureau Veritas.

## 3.4 - Autorité

CERT-BV de Bureau Veritas coordonne les incidents de sécurité concernant notre juridiction.



## 4. Politiques

### 4.1 - Types d'incidents et niveau de soutien

Le CERT de Bureau Veritas traite tous les types d'incidents de sécurité qui se produisent, ou qui menacent de se produire, au sein de sa juridiction.

Le niveau de soutien dépend du type et de la gravité de l'incident de sécurité donné.

### 4.2 - Coopération, interaction et Divulgence d'Informations

Le CERT de Bureau Veritas échangera toutes les informations nécessaires avec d'autres CERT/CSIRT ainsi qu'avec d'autres parties concernées si elles sont impliquées dans l'incident ou le processus de réponse à l'incident.

Les demandes légales seront évaluées par notre service juridique et une réponse appropriée sera donnée si la demande est acceptable, dans les limites de l'ordonnance du tribunal, de l'enquête connexe et des informations demandées.

### 4.3 - Communication et authentification

La méthode de communication préférée est le courrier électronique.

Pour l'échange d'informations sensibles et la communication authentifiée, CERT-BV utilise PGP pour le chiffrement et/ou la signature.

## 5. Services

### 5.1 - Services de Réponse à Incidents

CERT-BV fournit les Services de Réponse à Incident suivants :

Gestion des Informations relatives aux Incidents de Sécurité :

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

Gestion des Informations relatives aux Evénements de Sécurité :

- Monitoring and Detection
- Event Analysis
- Threat Intelligence coordination

Gestion des Vulnérabilités :

- Vulnerability Report Intake
- Vulnerability Coordination

### 5.2 – Services Proactifs

Afin d'adapter sa capacité de diagnostic, CERT-BV fournit les services proactifs suivants :

- Surveillance des menaces et des vulnérabilités



- Analyse des scénarios d'attaque et des mesures de cybersécurité pour protéger les systèmes d'information.
- Recherche de menaces (Threat Hunting)

CERT-BV fournit également une sensibilisation et une communication à la cybersécurité à sa juridiction afin d'avertir et de prévenir les risques et d'en limiter les conséquences.

## 6. Formulaire de signalement d'incidents

CERT-BV n'a pas de formulaire de signalement d'incidents. Veuillez signaler les incidents de sécurité par e-mail chiffré à [cert\[at\]bureauveritas\[dot\]com](mailto:cert[at]bureauveritas[dot]com).

Les rapports d'incident doivent contenir les informations suivantes dans la mesure du possible :

- Date et heure de l'incident (y compris le fuseau horaire)
- Description de l'incident
- Adresses IP source/destination, ports et protocoles
- Toute autre information pertinente

## 7. Avertissements

Bien que toutes les précautions soient prises dans la préparation des informations, des notifications et des alertes, CERT-BV n'assume aucune responsabilité pour les erreurs ou omissions, ou pour les préjudices résultant de l'utilisation des informations contenues dans le présent document.

Si vous remarquez une erreur dans ce document, veuillez-nous en informer par e-mail. Nous nous efforcerons de rectifier l'information dans les meilleurs délais.