MINISTÈRE
DE LA JUSTICE
Liberté
Égalité
Fraternité

Description du CSIRT du ministère de la justice

RFC 2350

Date	N° version	Statut	Classification	Auteur
22/04/2026	1	Validé	Public	Bureau FSSI

SOMMAIRE :

1. A propos du document

Ce document contient une description du CSIRT du ministère de la Justice conformément à la RFC2350. Il présente des informations de base sur le CSIRT et décrit ses responsabilités, les services qu'il propose et les moyens de communication.

1.1. Version et date de mise à jour

Version 1.0, publiée le 22/04/2026.

1.2. Liste de diffusion pour les modifications

Les modifications apportées à ce document sont notifiées par courriel à :

- InterCERT France / réseau de CSIRTs français – https://www.intercertfrance.fr/
- CERT-FR

Veuillez envoyer vos questions à l'adresse e-mail de l'équipe : csirt-ext@justice.gouv.fr

1.3. Positionnement du document

Ce document (version courante) et sa dernière version peuvent être trouvés sur

https:// justice.gouv.fr/csirt

1.4. Authenticité du document

Ce document a été signé à l'aide de la clé PGP du CSIRT. La clé publique PGP, son identifiant et son empreinte digitale sont disponibles sur le site Internet du CSIRT à l'adresse suivante :

https:// justice.gouv.fr/csirt

1.5 Identification du document

Identification du document	
Titre	**'CSIRT Justice RFC2350'**
Version	**1.0**
Date du document	**22/04/2026**
Expiration	**Ce document est valide jusqu'à ce qu'il soit remplacé par une version ultérieure**

2. Informations de contact

Cette partie décrit les moyens de communication du CSIRT.

2.1. Nom de l'équipe

Le nom complet de l'équipe est « CSIRT du ministère de la Justice ».

Le nom court de l'équipe est « CSIRT Justice ».

2.2. Adresse

Positionnement de l'équipe CSIRT du ministère de la Justice :

35 Rue de la Gare

75019 Paris

Adresse postale du ministère de la Justice :

13 Place Vendôme

75001 Paris

2.3. Zone horaire

CET/CEST : Paris (GMT+01, et GMT+02 heure d'été)

2.4. Numéro de téléphone

Le CSIRT est joignable au +33 6 23 06 63 55

2.5. Adresse e-mail

L'adresse e-mail du CSIRT est : csirt-ext@justice.gouv.fr

2.6. Clé publique et informations liées au chiffrement

La clé PGP est utilisée pour garantir la confidentialité et l'intégrité des échanges avec le CSIRT.

Chiffrement / Clé PGP	
Identifiant utilisateur	**CSIRT <csirt-ext@justice.gouv.fr>**
Identifiant de clé	**BB802747B2ED67AF**
Empreinte digitale	**EFBDA086E235357F6A85053EBB802747B2ED67AF**

La clé publique du CSIRT peut être obtenue par l'envoi d'un e-mail à csirt-ext@justice.gouv.fr.

Elle peut également être récupérée depuis le lien suivant https://justice.gouv.fr/csirt

2.7. Membres de l'équipe

L'équipe CSIRT est composée d'experts en sécurité informatique. La liste des membres de l'équipe du CSIRT n'est pas accessible au public.

Les informations nominatives relatives aux membres du CSIRT ne sont pas diffusées publiquement.

2.8. Horaires de fonctionnement

Le CSIRT est disponible durant les heures ouvrées, soit du lundi au vendredi de 09h00 à 18h00 hors jours fériés. En dehors des heures ouvrées, une permanence est assurée et joignable au numéro indiqué ci-dessus.

2.9. Contacts

Pour contacter le CSIRT, le moyen de communication privilégié est l'adresse e-mail csirt-ext@justice.gouv.fr.

Nous recommandons de chiffrer les mails avec les informations présentées dans le paragraphe 2.6 (Clé publique et informations liées au chiffrement) pour garantir l'intégrité et la confidentialité des échanges.

En cas d'urgence, veuillez utiliser la balise [URGENT] dans le champ objet de votre e-mail.

En dehors des heures ouvrées, il est également possible de signaler un incident auprès de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) sur : www.cybermalveillance.gouv.fr/diagnostic.

Les coordonnées du CERT-FR figurent à l'adresse suivante : http://www.cert.ssi.gouv.fr/contact/.

3. Charte

3.1. Missions

Le CSIRT du ministère de la Justice soutient ses bénéficiaires dans l'atteinte de leurs objectifs tout en les protégeant des cyberattaques intentionnelles et opportunistes qui pourraient porter atteinte à l'intégrité, la confidentialité, la disponibilité, et la traçabilité de leurs données et nuire à leurs intérêts ou à leur réputation.

Le CSIRT met un catalogue de service à la disposition de ses bénéficiaires, comprenant des zones de service, à savoir :

Zone 1 : La gestion des événements de sécurité

- Supervision et détection
- Analyse des évènements de sécurité

Zone 2 : La gestion des incidents de sécurité

- Qualification des incidents
- Analyse des incidents
- Corrélation des incidents
- Appui à la gestion de crise

Zone 3 : La gestion des vulnérabilités

- Gestion des rapports de vulnérabilités
- Diffusion des vulnérabilités
- Coordination et suivi des vulnérabilités résiduelles du SI
- Analyse des vulnérabilités

Zone 4 : La connaissance de la menace

- Gestion des sources d'information
- Analyse et synthèse
- Gestion de la communication

Zone 5 : Le partage de la connaissance

- Sensibilisation sur la menace
- Formation

3.2. Bénéficiaires

Les entités pouvant bénéficier de l'accompagnement du CSIRT sont les entités rattachées au ministère de la Justice.

La liste des bénéficiaires (repartis sur plusieurs périmètres) et les services fournis par le CSIRT sont confidentiels. Ils sont indiqués dans le mandat.

3.3. Affiliation

Le CSIRT est rattaché au département de la Haute Fonctionnaire de Défense et de Sécurité (DHFDS), plus précisément au bureau du pilotage de la sécurité numérique (BPSN). Il maintient des relations avec le CERT-FR, les CSIRT ministériels et le SOC du ministère de la Justice.

3.4. Autorité

Le CSIRT est placé sous l'autorité du secrétariat général du ministère de la Justice représenté par Madame la secrétaire générale, Haute fonctionnaire de défense et de sécurité, qui donne délégation au Fonctionnaire de sécurité des systèmes d'information (FSSI).

4. Politiques

4.1. Types d'incidents et niveau d'intervention

Le CSIRT traite tous les types d'incidents de sécurité pouvant affecter ou menacer son périmètre.

Le niveau d'intervention ou d'assistance apporté par le CSIRT dépend de la gravité de l'incident de sécurité et de son impact.

4.2. Coopération, interaction et partage d'information

Selon les principes du besoin d'en connaitre et en fonction de la classification des données, le CSIRT échangera de manière chiffrée toutes les informations nécessaires (par exemple, les détails techniques) avec les autres CERT/CSIRT susceptibles d'être concernés. Tout partage d'information respectera les différentes règlementations de protection et les bonnes pratiques existantes.

Par conséquent, ces informations pourront être transmises à des entités telles que :

- Les experts techniques du CERT FR (ANSSI) ;
- Les parties concernées au sein du ministère (et ses bénéficiaires) ;
- Les fournisseurs d'accès à internet (ISP - *Internet Service Provider*) / hébergeurs affectés sur le territoire français ;
- Les organismes français chargés de l'application des lois (si cela est exigé par la loi ou sur demande) ;
- Les groupes de coopération CERT/CSIRT.

Seuls les extraits d'information spécifiquement pertinents et anonymisés seront partagés.

La diffusion d'information est réalisée en accord avec le protocole TLP (*Traffic Light Protocol*) défini par FIRST (https://www.first.org/tlp). Nous recommandons de lire la politique de partage et d'utilisation (pour les informations opérationnelles) sur le site du CERT FR (Politique de partage et d'utilisation des informations à caractère opérationnel – CERT-FR (ssi.gouv.fr)).

4.3. Communication et authentification

La méthode de communication recommandée par le CSIRT du ministère de la Justice est le courrier électronique. Pour l'échange d'informations sensibles et la communication authentifiée, le CSIRT utilise la clé PGP pour chiffrer et / ou signer les messages (voir la section 2.6 (Clé publique et informations liées au chiffrement)).

Les informations considérées non confidentielles ou peu sensibles peuvent être transmises via des courriels non chiffrés.

5. Services

5.1. Réponse aux incidents

L'activité principale du CSIRT est l'évaluation ainsi que la gestion des aspects techniques et organisationnels des incidents de sécurité liés à l'information et aux technologies de communication. Il propose à ses bénéficiaires un service de réponse de premier niveau aux incidents cyber et choisit le prestataire pour l'accompagnement dans la suite de la résolution des incidents.

Le CSIRT propose les services suivants dans le cadre de la réponse aux incidents de sécurité.

5.1.1. Triage / gestion d'incident

- Évaluation de la gravité de l'incident ;
- Détermination du périmètre de l'incident et son impact ;
- Catégorisation de l'incident.

5.1.2. Coordination

- Catégorisation des informations liées à l'incident (fichiers journaux, informations de contacts, etc.) en respectant la politique de divulgation des informations ;
- Notification des autres parties impliquées sur le principe du besoin d'en connaitre, conformément à la politique de divulgation d'informations, notamment :
    - l'ANSSI en cas d'incident majeur (ou avec un niveau de gravité plus élevé) de cybersécurité pouvant affecter d'autres secteurs ;
    - le DPD (Délégué à la protection des données) qui se charge de notifier la CNIL.

5.1.3. Résolution d'incident

- Analyse des systèmes compromis ;
- Proposition de mesures d'urgence pour limiter l'impact de l'incident ;
- Résolution et remédiation de l'incident i.e. élimination de la cause de l'incident et de ses effets, durcissement des SI, etc.
- Suivi des phases de résolution et de remédiation.

5.2. Activités proactives

- Supervision du réseau et des systèmes pour une détection des attaques en temps opportun
- Formation et sensibilisation des agents au domaine de la cybersécurité.

Des services d'avertissements et d'informations sont également disponibles sur le site du CERT FR : https://cert.ssi.gouv.fr/

6. Formulaire de notification d'incident

Le signalement des incidents de sécurité se fait par courrier électronique chiffré à l'adresse suivante csirt@justice.gouv.fr avec au moins les informations suivantes :

- Le TLP (clear, green, amber, red) de partage d'informations ;

- Les coordonnées et les informations sur l'organisation ;
- La date, l'heure et le fuseau horaire de l'incident (indiquer si les informations fournies sont des suppositions) ;
- L'adresse IP, le nom complet (FQDN), et toute autre information technique pertinente, avec les observations associées ;
- L'impact de l'incident (en termes de confidentialité, d'intégrité, de disponibilité et de traçabilité) ;
- Toute information pertinente sur une menace ou un incident concernant le ministère de la justice ;

7. Décharge de responsabilité

La directive NIS2 exige d'un CSIRT qu'il prenne des mesures de sécurité appropriées pour prévenir les incidents de sécurité, qu'il notifie les autorités compétentes en cas d'incident, et qu'il établisse des procédures de gestion des incidents de sécurité sur l'ensemble du périmètre supervisé (3.2 - Bénéficiaires).

Le CSIRT ne peut être tenu responsable (conformément à la directive NIS 2) des erreurs ou omissions, ou des dommages qui résultent de l'utilisation des informations communiquées sur l'ensemble du périmètre supervisé et listé au point 3.2 (Bénéficiaires) de ce document.