Veuillez sélectionner

FORMULAIRE DE DÉCLARATION D'UN INCIDENT DE SÉCURITÉ RELATIF À UN SERVICE CERTIFIÉ

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.76.85.80 - Télécopie 01.84.82.40.60.

Veuillez sélectionner

Consignes

Le présent formulaire permet aux fournisseurs de services de déclarer un incident de sécurité affectant ou susceptible d'affecter leurs services.

Les champs du formulaire marqués d'un astérisque (*) doivent impérativement être renseignés.

Une délcaration d'incident dans le cadre du suivi de la sécurité d'un service ne se substitue pas aux éventuelles autres obligations légales et réglementaires auxquelles le fournisseur de service pourrait être soumis, notamment la déclaration d'incident en application de la loi relative à l'informatique, aux fichiers et aux libertés ou de l'article L1332-6-2 du code de la défense.

Marquage

Le choix du niveau de confidentialité du formulaire renseigné relève de la personne effecturant la déclaration d'incident. Un marquage « Confidentiel industrie » ou « Diffusion restreinte » peut être ajouté sur chacune des pages du formulaire renseigné.

Protection

Lorsqu'il est transmis par voie électronique et qu'il porte la mention « Confidentiel Industrie » ou équivalente, le formulaire renseigné est protégé en confidentialité au moyen d'un outil défini conjointement entre l'ANSSI et la personne effectuant la déclaration d'incident.

Lorsqu'il est transmis par voie électronique et qu'il porte la mention « Diffusion Restreinte », le formulaire renseigné est protégé en confidentialité au moyen d'un outil défini conjointement entre l'ANSSI et la personne effectuant la déclaration d'incident, agréé par l'ANSSI au niveau adéquat et utilisé conformément aux conditions d'utilisation figurant dans la décision d'agrément de l'outil.

Modalités d'envoi

Le présent formulaire doit être renseigné puis transmis au format électronique :

Par voie postale :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre opérationnel de la sécurité des systèmes d'information
51, boulevard de la Tour-Maubourg
75700 Paris 07 SP

ou

Par voie électronique :

cert-fr.cossi[at]ssi.gouv.fr

Précisez l'objet du message : **[Incident service]** pour toute déclaration d'un incident relatif à un service

Veuillez sélectionner

INFORMATIONS GÉNÉRALES RELATIVES AU SERVICE

1 Informations générales

Date de la déclaration* *(jj/mm/aaaa)* : ☐☐ / ☐☐ / ☐☐☐☐

Nom de l'entité* :

2 Fournisseur de services

☐ Cocher si sans objet

Service(s) concerné(s)* *(Plusieurs choix possibles)* :

☐ Service de vérification d'identité à distance ☐ Moyen d'identification électronique ☐ Autre

Si « autre », précisez :

Identifiant du ou des services concerné(s)* :

(pour les services certifiés, précisez les références des décisions de certification)

3 Cadre règlementaire de la certification du service

Cadre réglementaire de la certification du service faisant l'objet de la déclaration* *(plusieurs choix possibles)* :

☐ Décret n° 2020-118 du 12 février 2020 renforçant le dispositif national de lutte contre le blanchiment de capitaux et le financement du terrorisme

☐ Article L102 du Code des postes et des communications électroniques Non certifié

Veuillez sélectionner

CONTACTS

5 Personne effectuant la déclaration

Nom-Prénom* :

Fonction*:

Adresse postale

N°, rue* :

Code postal* :

Commune* :

Pays* :

Téléphone bureau* : .

Fax : .

Adresse électronique* :

6 Personne à contacter pour tout renseignement complémentaire concernant l'incident de sécurité

Nom-Prénom* :

Fonction*:

Adresse postale

N°, rue* :

Code postal* :

Commune* :

Pays* :

Téléphone bureau* : .

Fax : .

Adresse électronique* :

Veuillez sélectionner

DESCRIPTION DE L'INCIDENT

7 Système d'information affecté

Dénomination du système d'information* :

Brève description du système d'information* :

8 Incident constaté

Date à laquelle l'incident a été constaté :

Date* *(jj/mm/aaaa)* : / / Heure locale*:

Date estimée du début de l'incident :

Date* *(jj/mm/aaaa)* : / / Heure locale* :

Localisation des équipements du système d'information affectés par l'incident* :

Description de l'incident* *(l'annexe du présent formulaire identifie certains types d'incidents)* :

En cas d'attaque, état constaté ou présumé de l'attaque* : Choisissez un élément

Veuillez sélectionner

9 Qualification de l'incident

État de la qualification[1] de l'incident* *(cocher la case correspondante)* : ☐ Non envisagé ☐ En cours de traitement ☐ Résolu

Origine de l'incident* *(cocher la case correspondante)* : ☐ Malveillance ☐ Accident ☐ Inconnue

En cas d'incident d'origine malveillante, précisez l'origine de la malveillance* *(cocher la case correspondante)* : ☐ Interne ☐ Externe ☐ Inconnue

En cas d'incident d'origine accidentelle, description des causes de l'incident* :

10 Impacts de l'incident

Impact(s) présumé(s) ou constaté(s) sur la sécurité* : Choisissez un élément

Entités auxquelles le produit ou le service a été fourni et auxquelles l'incident est susceptible de porter préjudice*
(Si des entités sont situées à l'étranger, le préciser) :

[1] *Détermination de la nature et de la gravité d'un incident de sécurité.*

Veuillez sélectionner

11 Mesures prises et envisagées

Description des mesures prises* : ☐ Cocher si sans objet

Description des mesures envisagées* : ☐ Cocher si sans objet

Dépôt de plainte* *(cocher la case correspondante)* : ☐ Non envisagé ☐ Envisagé ☐ Effectué

Autorités autres que l'ANSSI auxquelles l'incident a ou va être notifié* :

12 Observations complémentaires ☐ Cocher si sans objet

Veuillez sélectionner

ANNEXE 1

Liste non exhaustive de types d'incidents de sécurité

La liste suivante présente, de manière non exhaustive, des exemples d'incidents de sécurité devant être notifiés à l'ANSSI, s'ils ont un impact sur la sécurité du service, ou sur les données relatives aux utilisateurs du service, que ces données soient à caractère personnel ou non.

De manière générale, tout incident de sécurité lié à un évènement redouté de gravité importante ou critique dans l'analyse de risques doit être notifié.

Perte et vol de supports

- Perte ou vol d'un support papier ou de stockage d'informations confidentielles relatives au produit ou au service
- Perte ou vol d'un support papier ou de stockage d'informations confidentielles relatives aux utilisateurs du produit ou du service
- Perte ou vol d'un support de stockage de la clé privée d'une autorité de certification

Perte et vol de postes

- Perte ou vol du poste d'un administrateur
- Perte ou vol du poste d'un opérateur

Intrusion physique

- Intrusion physique dans les locaux hébergeant tout ou partie du système d'information impliqué dans la spécification, la conception, le développement, la fabrication, l'exploitation, la maintenance, l'avant-vente, le support technique ou la livraison du produit
- Intrusion physique dans les locaux hébergeant tout ou partie du système d'information impliqué dans l'exploitation, la maintenance, ou le support technique du service

Intrusion logique

- Intrusion logique dans tout ou partie du système d'information impliqué dans la spécification, la conception, le développement, la fabrication, l'exploitation, la maintenance, l'avant-vente, le support technique ou la livraison du produit
- Intrusion logique dans tout ou partie du système d'information impliqué dans l'exploitation, la maintenance, ou le support technique du service

Code malveillant

- Détection de la présence d'un code malveillant

Disponibilité du service

- Indisponibilité de tout ou partie du service
- Indisponibilité de la fonction de prise en compte des révocations de certificats électroniques
- Indisponibilité de la fonction d'information du statut de révocation des certificats électroniques

Atteinte à la confidentialité

- Atteinte à la confidentialité de la clé privée d'une autorité de certification
- Atteinte à la confidentialité des données relatives aux utilisateurs du service
- Atteinte à la confidentialité des données à caractère personnel relatives aux utilisateurs du service

Atteinte à l'intégrité

- Atteinte à l'intégrité de tout ou partie du service
- Atteinte à l'intégrité d'un service de conservation de signatures ou cachets électronique
- Atteinte à l'intégrité de la fonction d'information du statut de révocation des certificats
- Atteinte à l'intégrité de la source de temps d'un service d'horodatage électronique
- Atteinte à l'intégrité de la clé privée d'une autorité de certification
- Atteinte à l'intégrité des données relatives aux utilisateurs du service
- Atteinte à l'intégrité des données à caractère personnel relatives aux utilisateurs du service
- Atteinte à l'intégrité de la configuration du système d'information
- Atteinte à l'intégrité physique d'un équipement (étiquettes de sécurité déchirées ou retirées, capots arrachés, etc.)

Abus de privilège

- Usurpation d'identité d'un administrateur
- Usurpation d'identité d'un opérateur
- Délivrance frauduleuse de certificats électroniques
- Émission frauduleuse de jetons d'horodatage électronique dans le système d'information du service