Veuillez sélectionner

FORMULAIRE DE DÉCLARATION D'UN INCIDENT DE SÉCURITÉ

(Article R. 1332-41-10 du code de la défense)
Formulaire à compléter et à adresser à l'Agence nationale de la sécurité des systèmes d'informations (ANSSI), 51, boulevard de La Tour-Maubourg, 75700 Paris 07 SP

1. Type de déclaration

Date de la déclaration*

(jj/mm/aaaa)

Nom de l'opérateur d'importance vitale effectuant la déclaration *

Déclaration* : Veuillez sélectionner

Référence de la déclaration initiale fournie par l'ANSSI (si connue de l'opérateur)

2. Coordonnées de la personne effectuant la déclaration

Nom*

Prénom*

Service*

Fonction*

Adresse postale*

Téléphone*

Adresse électronique*

* Les champs marqués d'un astérisque sont obligatoires dans le cas d'une déclaration initiale.

Veuillez sélectionner

Veuillez sélectionner

3. Coordonnées de la personne à contacter pour obtenir des informations complémentaires relatives à l'incident

a) Contact privilégié en heures ouvrées

Nom*	
Prénom*	
Service*	
Fonction*	
Adresse postale*	
Téléphone*	
Adresse électronique*	
Adresse ISIS*[1]	

b) Contact privilégié en heures non-ouvrées

Nom*	
Prénom*	
Service*	
Fonction*	
Téléphone*	
Adresse électronique*	

* Les champs marqués d'un astérisque sont obligatoires dans le cas d'une déclaration initiale.

[1] Champ à compléter si l'opérateur dispose d'une adresse ISIS (Intranet Sécurisé Interministériel pour la Synergie gouvernementale).

Veuillez sélectionner

Veuillez sélectionner

4. Description de l'incident

a) Système d'information d'importance vitale affecté

Dénomination du système d'information d'importance vitale*

Identifiant du système d'information fourni par l'ANSSI (si connu de l'opérateur)* *(XXX-XXXXXX)*

Brève description du système d'information*

b) Incident constaté

Date à laquelle l'incident a été constaté* *(jj/mm/aaaa)*

Date et heure estimées du début de l'incident *(jj/mm/aaaa)* Heure locale :

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

En cas d'attaque, état constaté ou présumé de l'attaque* Veuillez sélectionner

Impacts sur la sécurité constatés ou présumés* Veuillez sélectionner

* Les champs marqués d'un astérisque sont obligatoires dans le cas d'une déclaration initiale.

Veuillez sélectionner

Veuillez sélectionner

Impacts sur les activités constatés ou présumés*[2]

c) Qualification de l'incident

Type d'incident[3]

État de la qualification de l'incident*

Veuillez sélectionner

En cas d'incident d'origine malveillante, description de la méthode de l'attaquant[4]

En cas d'incident d'origine malveillante, identification d'indicateurs techniques de compromission du système[5]

Veuillez sélectionner

En cas d'incident d'origine **non** malveillante, description des causes de l'incident

* Les champs marqués d'un astérisque sont obligatoires dans le cas d'une déclaration initiale.

[2] Précisez les impacts sur les activités (exfiltration de données, destruction d'équipements, indisponibilité du système, etc.) et notamment la nature des données exfiltrées, les équipements affectés ou détruits par l'incident et les équipements visés en cas d'attaque.

[3] Précisez le type de l'incident dont relève l'incident parmi les types d'incident prévus par l'arrêté pris en application de l'article R. 1332-41-10 du code de la défense et relatif au secteur d'activités d'importance vitale de l'opérateur.

[4] Décrivez les caractéristiques générales de l'attaque (motivation présumée de l'attaquant, type d'attaque, niveau de complexité de l'attaque, etc.) ainsi que les caractéristiques techniques de l'attaque (chronologie et nature des différentes étapes de l'attaque, périmètre de la compromission du système, vulnérabilités exploitées par l'attaquant, moyens techniques utilisés par l'attaquant, etc.).
Le cas échéant, joignez au formulaire les résultats d'analyse de l'attaque dont vous disposez.

[5] Il s'agit d'indicateurs caractérisant l'attaque tels que des adresses IP, des noms de domaine, des adresses URL, des empreintes cryptographiques, des noms de fichiers ou de codes malveillants, des données contenues dans des codes malveillants ou dans les bases de registre du système, etc.
Le cas échéant, joignez au formulaire les indicateurs que vous avez identifiés.

Veuillez sélectionner

Veuillez sélectionner

d) Mesures prises et envisagées

Description des mesures prises et envisagées[6]	
Autres déclarations de l'incident[7]	
Dépôt de plainte	Veuillez sélectionner

5. Observations complémentaires

[6] Décrivez les mesures techniques et organisationnelles prises et envisagées relatives au traitement de l'incident et notamment au renforcement de la détection d'incidents. Le cas échéant, précisez les mesures prises en relation avec le prestataire de détection.

[7] Précisez le cas échéant les autres déclarations relatives à cet incident que vous auriez effectuées auprès d'autres organismes.

Veuillez sélectionner