DIFFUSION RESTREINTE

Ce document ne doit être communiqué qu'aux personnes qualifiées pour le connaître.

FORMULAIRE DE DÉCLARATION D'UN INCIDENT DE SÉCURITÉ

Application de l'article 4 de l'arrêté ministériel n° 2018-1053 du 8 novembre 2018 portant application de l'article 27 de la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique.

Application du paragraphe 4.13.4 de l'annexe à l'arrêté ministériel n°2022-331 du 13 juin 2022 portant application de 23 de la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique, fixant les mesures de sécurité des systèmes d'information de l'État (PSSI-E).

Formulaire à compléter et à déposer sur votre espace de travail Cryptobox.

Déclaration

Date de la déclaration*

(jj/mm/aaaa)

Nom de l'entité*

Type de d'éclaration* : Veuillez sélectionner

n° du ticket RTIR fourni par l'AMSN*

Coordonnées de la personne effectuant la déclaration

Nom*

Prénom*

Service*

Fonction*

Téléphone mobile*

Adresse électronique*

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*

Téléphone mobile*

Adresse électronique*

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

b) Contact privilégié en heures non-ouvrées

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

Description de l'incident

Dénomination du Système d'information*	
Brève description du système d'information*	
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 constatés sur la sécurité ou présumés*	Disponibiltité ☐ Intégrité ☐ Confidentialité ☐ Traçabilité ☐
Impacts sur les activités constatés ou présumés*(1)	

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

(1)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.

DIFFUSION RESTREINTE

Qualification de l'incident

Type d'incident*(2)	
État de la qualification de l'incident*	Veuillez sélectionner
En cas d'incident d'origine malveillante, description de la méthode de l'attaquant *(3)	
En cas d'incident d'origine malveillante, identification d'indicateurs techniques de compromission du système*(4)	Veuillez sélectionner
En cas d'incident d'origine **non** malveillante, description des causes de l'incident*	
Description des mesures prises et envisagées*(5)	
Dépôt de plainte*	Veuillez sélectionner
Autres déclarations de l'incident*(6)	

Signature de la personne effectuant la déclaration*		Date à laquelle la déclaration est complétée*	*(jj/mm/aaaa)*

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

(2) 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 27 de la Loi 1.435.

(3) 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.

(4) 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.

(5) 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.

(6) Obligations réglementaires concernant la protection des données personnelles.