

# Signalement d'un incident lié à la technologie ou à la cybersécurité

## 1. Renseignements sur l'incident et coordonnées

Nom ou identifiant de l'incident:

Date et heure de découverte/détection de l'incident:

Date et heure de survenance de l'incident:

Nom de votre institution:

Nom de la principale personne-ressource

Poste de la principale personne-ressource

Adresse courriel de la principale personne-ressource:

Numéro de téléphone de la principale personne-ressource

Nom du responsable de la gestion de l'incident

Poste du responsable de la gestion de l'incident

## 2. Site/emplacement et secteurs d'activité touchés

Nom du secteur d'activité ou de la fonction concerné(e)

Actif(s) technologique(s) concerné(s)

Site ou emplacement touché

## 3. Description du risque et de l'incident

Catégorie d'incident

Où l'incident s'est-il produit?

- Technologie  
 Cyber  
 Autre (préciser ci-dessous)

- IFF  
 Partie tierce  
 Chaînes d'approvisionnement  
 Autre (préciser ci-dessous)

Si autre, veuillez préciser

Si autre, veuillez préciser

Indiquez le(s) type(s) d'incident:

- |   |  |  |
|---|--|--|
| <input type="checkbox"/> Interruption/panne d'un actif technologique* | <input type="checkbox"/> DDoS                                    | <input type="checkbox"/> Raçongiciel                 |
| <input type="checkbox"/> Dégradation/retard d'un actif technologique* | <input type="checkbox"/> Menace interne                          | <input type="checkbox"/> Accès non autorisé          |
| <input type="checkbox"/> GAB Jackpotting                              | <input type="checkbox"/> Logiciels malveillants/Maliciel - Autre | <input type="checkbox"/> Perte/vol d'équipement      |
| <input type="checkbox"/> Prise de contrôle de compte                  | <input type="checkbox"/> Lancement massif de maliciels           | <input type="checkbox"/> Autre (précisez ci-dessous) |
| <input type="checkbox"/> Cybercriminalité                             | <input type="checkbox"/> Extorsion en ligne                      |  |
| <input type="checkbox"/> Violation/fuite de données                   | <input type="checkbox"/> Hameçonnage                             |  |

\* Un "actif technologique" est quelque chose de tangible (par exemple, le matériel, l'infrastructure) ou d'intangible (par exemple, les logiciels/applications, les données, les informations) qui doit être protégé et qui soutient la livraison de services technologiques.

Si autre, veuillez préciser

Sélectionnez un niveau ou une priorité d'incident dans la liste déroulante.

Si autre, veuillez préciser

Ajoutez des détails supplémentaires ci-dessous, notamment: l'état actuel, leurs impacts directs et indirects connus, les actions réalisées et en cours, ainsi que les délais estimés pour remédier à l'incident.

--

Ajoutez une description de la cause principale ou de la cause de l'incident, si elle est connue:

--

Ajoutez une description des informations sensibles compromises ou à risque. Si aucune information sensible n'est à risque, veuillez indiquer N/A.	
---	--

Ajoutez des détails sur le tactiques, techniques et procédures impliquées dans l'incident	Fournir les indicateurs de compromission.
---	---

**Notifications internes et externes**

Les cadres supérieurs ont-ils été prévenus?	Date et heure où les cadres supérieurs ont été prévenus (le cas échéant)
---	--

D'autres organismes de réglementation ou de surveillance ont-ils été prévenus?	Date et heure où les organismes de réglementation ou de surveillance ont été prévenus (le cas échéant)

--	--

Nom des autres organismes de réglementation ou de surveillance ayant été prévenus.

--

Les forces de l'ordre ont-elles été prévenues?	Nom des forces de l'ordre ayant été prévenues
--	---

--	--

Des fournisseurs de services d'assurance contre le cyberrisque ont-ils été prévenus?	Nom des fournisseurs de services d'assurance contre le cyberrisque ayant été prévenus
--	---

--	--

Une réclamation d'assurance (contre le cyberrisque ou autre) a-t-elle été présentée?	A-t-on retenu les services d'une firme d'enquête externe?
--	---

--	--

L'expert en compromission a-t-il été prévenu?	A-t-on fait appel à un conseiller juridique interne ou externe?
---	---

--	--