Déclaration des événements

**1. Objet**

**1.1 Finalité**

**1.2 Domaine d'application**

**1.3 Glossaire**

**2. Responsabilité**

**3. Documents**

**4. Exigences de la norme ISO 27001 : 2022**

**5. Déroulement**

Historique

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| Toutes | Création | 01/01/2022 |
| **Page** | **Changement** | **Date** |

**1. Objet**

**1.1 Finalité**

La présente procédure a pour finalité de soutenir le signalement opportun, cohérent et efficace des événements de sécurité de l'information qui peuvent être identifiés par le personnel.

**1.2 Domaine d'application**

Le domaine d’application de la procédure « Déclaration des événements » s’applique à l’ensemble du personnel ayant accès à l’information et aux autres actifs de l’organisation.

**1.3 Glossaire**

SMSI – système de management de la sécurité de l’information

RSI – responsable de la sécurité de l’information

**2. Responsabilité**

Le responsable de la sécurité de l’information (RSI) a l’autorité de l’écriture et de la mise à jour de cette procédure. Il est garant de son application. Il a l’appui de la direction et des pilotes de processus.

**3. Documents**

Incidents

Registre des incidents

Événement de sécurité de l’information

Sécurité de l’information

Vulnérabilités techniques

**4. Exigences de la norme ISO 27001 : 2022**

A.6.8 Déclaration des événements liés à la sécurité de l’information

L'organisation doit fournir un mécanisme au personnel pour déclarer rapidement les événements liés à la sécurité de l'information observés ou suspectés, à travers des canaux appropriés.

**5. Déroulement**

Toute personne ayant accès à l’information et aux autres actifs est informée de sa responsabilité pour signaler les événements de sécurité de l'information aussi rapidement que possible afin de prévenir ou de minimiser l'effet des incidents de sécurité de l'information selon la procédure Incidents.

La notification des événements de sécurité de l'information est envoyée au RSI avec un moyen simple, comme courriel ou appel téléphonique et enregistrée dans le Registre des incidents et la fiche Événement de sécurité de l’information.

Les événements de sécurité de l'information incluent les incidents, les violations des politiques Sécurité de l’information et Vulnérabilités techniques.

Les différents événements de sécurité de l'information à prendre en compte sont :

* des mesures de sécurité de l'information inefficaces
* la violation des attentes en matière de confidentialité, d'intégrité ou de disponibilité de l’information
* des erreurs humaines
* le non-respect :
  + de la politique de sécurité de l'information
  + des autres politiques
  + des normes applicables
* le manquement aux mesures de sécurité physique
* des changements qui n'ont pas été soumis au processus de gestion des changements
* des dysfonctionnements ou autres comportements anormaux d’un logiciel ou d’un matériel
* des violations d'accès
* des vulnérabilités techniques
* une infection suspectée par un programme malveillant

L’ensemble du personnel est averti de ne pas chercher à prouver les vulnérabilités suspectées en matière de sécurité de l'information. C’est la responsabilité du RSI.

Les vulnérabilités de test peuvent être interprétées comme une mauvaise utilisation potentielle du système, peuvent endommager le système et peuvent corrompre ou masquer les preuves numériques. Restez prudent et concentré, cela peut entraîner une responsabilité légale pour la personne effectuant le test.