Sensibilisation et formation

**1. Objet**

**2. Finalité**

**3. Domaine d’application**

**4. Responsabilité**

**5. Documents**

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

**7. Politique sensibilisation et formation**

Historique

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

**1. Objet**

La politique sensibilisation et formation a pour objet de décrire les méthodes utilisées pour sensibiliser le personnel sur l’importance de la sécurité de l’information dans notre organisation.

**2. Finalité**

La politique sensibilisation et formation a pour finalité d'assurer que le personnel et les parties intéressées concernées connaissent et remplissent leurs responsabilités en matière de sécurité de l'information.

**3. Domaine d’application**

La politique sensibilisation et formation s’applique à l’ensemble du personnel de notre organisation.

**4. Responsabilité**

Le responsable sécurité de l’information (RSI) a l’autorité de l’écriture et de la mise à jour de la politique sensibilisation et formation. Il est garant de son application. Il a l’appui du directeur et de tous les responsables de département.

**5. Documents**

Sensibilisation et formation

Programme de formation

Plan d’augmentation de la sensibilité

Authentification

Incidents

Plan de développement des compétences

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

A.6.3 Sensibilisation, enseignement et formation en sécurité de l’information

Le personnel de l'organisation et les parties intéressées pertinentes doivent recevoir une sensibilisation, un enseignement et des formations en sécurité de l'information appropriés, ainsi que des mises à jour régulières de la politique de sécurité de l'information, des politiques spécifiques et des procédures de l'organisme pertinentes à leur fonction.

**7. Politique sensibilisation et formation**

Un programme de sensibilisation, d'éducation et de formation à la sécurité de l'information est établi conformément à la politique de sécurité de l'information de l'organisation, aux politiques et procédures spécifiques, cf. la procédure Sensibilisation et formation.

La sensibilisation, l'éducation et la formation à la sécurité de l'information ont lieu périodiquement selon le Programme de formation. La sensibilisation, l'éducation et la formation initiales peuvent s'appliquer au nouveau personnel et à ceux qui sont mutés à de nouveaux postes ou rôles avec des exigences de sécurité de l'information sensiblement différentes.

La compréhension et l’assimilation des connaissances de la part du personnel sont évaluées afin de tester le transfert de connaissances et l'efficacité du programme de formation, cf. le Plan d’augmentation de la sensibilité.

Le programme de sensibilisation à la sécurité de l'information a pour objectif de sensibiliser le personnel en lien avec les responsabilités de chacun en matière de sécurité de l'information et aux moyens utilisés.

Le programme de sensibilisation est planifié et tient compte :

* des rôles du personnel dans l'organisation, y compris le personnel interne et externe (par exemple, les consultants externes, le personnel des fournisseurs)
* des enseignements tirés des incidents de sécurité de l'information

Les activités du programme de sensibilisation sont programmées dans le temps et couvrent les nouveaux embauchés.

Le programme de sensibilisation inclut des activités de sensibilisation diverses comme :

* des campagnes spécifiques
* des brochures
* des affiches
* des bulletins d'information
* des sites Web éducatifs
* des séances d'information
* des modules d'apprentissage en ligne
* des courriels de rappel

La sensibilisation à la sécurité de l'information inclut :

* l'engagement de la direction par rapport à la sécurité de l'information
* les règles et obligations applicables :
  + politique de sécurité de l'information
  + politiques spécifiques
  + normes
  + lois
  + statuts
  + règlements
  + contrats
  + accords
* la responsabilité personnelle et les responsabilités générales de sécurisation et de protection de l’information
* les procédures de sécurité de l'information (Authentification, Incidents)
* les points de contact et les ressources pour obtenir des informations et des conseils sur les questions de sécurité de l'information

Le Plan de développement des compétences établit des formations appropriées pour les équipes techniques dont les rôles nécessitent des compétences et une expertise spécifiques. Les équipes techniques ont les compétences nécessaires pour configurer et maintenir le niveau de sécurité requis pour les appareils, les systèmes, les applications et les services. Quand une compétence fait défaut, les mesures pour les acquérir sont entreprises.

Le programme d'éducation et de formation prend différentes formes :

* cours magistraux
* cours autodidactes
* mentorat par des experts ou des consultants sur place
* rotation des membres du personnel pour suivre différentes activités
* recrutement de personnes déjà qualifiées
* embauche de consultants et d’experts

Les moyens pour se former peuvent être :

* en classe en centre de formation
* à distance
* sur le Web (en ligne)
* mixte (en présentiel et en ligne)

Le personnel technique maintient ses connaissances techniques et professionnelles à jour en :

* s'abonnant à des :
  + newsletters
  + magazines
* assistant à des :
  + conférences
  + événements

Lors de la composition du programme de sensibilisation, il est important non seulement de se concentrer sur le « quoi » et le « comment », mais aussi sur le « pourquoi » des activités.

Le personnel comprend l'objectif de la sécurité de l'information et l'effet potentiel, positif et négatif, sur l'organisation de son propre comportement.

La sensibilisation, l'éducation et la formation à la sécurité de l'information font souvent partie d'autres activités comme la gestion générale de l'information, les TIC, la sécurité, la confidentialité, la disponibilité.