Formation et sensibilisation

**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**

**5.1 Intégration du personnel**

**5.2 Formation au poste**

**5.3 Cycle de formation**

**5.4 Plan de développement des compétences**

**5.5 Sensibilisation du personnel**

**5.6 Entretien annuel d’évaluation**

Historique

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

**1. Objet**

**1.1 Finalité**

La présente procédure 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.

**1.2 Domaine d'application**

Le domaine d’application de la procédure « Sensibilisation et formation » 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

**2. Responsabilité**

Le responsable du personnel a l’autorité de l’écriture et de la mise à jour de cette procédure. Il est garant de son application.

**3. Documents**

Sélection des candidats

Gérer le contrat de travail

Termes et conditions d’embauche

Description de fonction

Programme de formation

Dispenser la formation

Attestation de présence

Sensibilisation et formation

Appliquer la discipline

Règles disciplinaires

Décisions de la revue de direction

Plan de développement des compétences

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

§ 7.3 Sensibilisation

Les personnes effectuant un travail sous le contrôle de l’organisation doivent:

a) être sensibilisées à la politique de sécurité de l’information ;

b) avoir conscience de leur contribution à l’efficacité du système de management de la sécurité de l’information, y compris aux effets positifs d’une amélioration des performances de la sécurité de l’information ; et

c) avoir conscience des implications de toute non-conformité aux exigences requises par le système de management de la sécurité de l’information.

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

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

**5. Déroulement**

**5.1 Intégration du personnel**

Les activités de sélection des candidats sont précisés dans la procédure Sélection des candidats. Lors de l’embauche (après signature du contrat de travail, cf. le processus Gérer le contrat de travail) de tout employé (permanent ou intérimaire), le responsable du personnel et le responsable hiérarchique présentent les points clés du fonctionnement de l’entreprise (Termes et conditions d’embauche) et de la politique sécurité de l’information. Le nouvel embauché est sensibilisé à des règles avant sa prise de fonction :

* règles déontologiques
* règles de sécurité de l’information
* identification des risques et les conséquences des phénomènes d'électricité statique
* maintien de la propreté et entretien premier niveau de son poste de travail
* 5 S (rangement)

Le nouvel embauché reçoit son équipement personnel, sa carte de pointage, son badge. Avec l'aide de son responsable il fait le tour des départements. Il est informé du système de management de la sécurité de l’information (SMSI) et des procédures, processus et politiques liés directement à son travail.

La formation de base a pour but de former le nouvel employé au fonctionnement du poste qui lui est attribué en accord avec sa fiche Description de fonction. Cette formation est dispensée en interne, en salle de formation ou sur le poste de travail, par un formateur, un chef de groupe, un agent de maîtrise ou le responsable opérationnel.

**5.2 Formation au poste**

Lorsqu’une personne doit prendre en charge un nouveau poste de travail (ou une nouvelle machine) ou qu'elle n'a pas occupé ce poste depuis un temps jugé trop important par le chef de groupe, une formation doit être réalisée en totalité ou en partie au poste de travail, cf. le processus Dispenser la formation. Le formateur est alors un agent de maîtrise, un technicien ou un chef de groupe qui va apporter à la personne les connaissances de base lui permettant de tenir son poste. Cette formation permet au chef de groupe de connaître très rapidement le nom des personnes accréditées à travailler sur un poste.

**5.3 Cycle de formation**

Il s’agit de la mise en place, la réalisation et le suivi des formations effectuées en interne ou en externe concernant tous les secteurs de l’entreprise selon le Programme de formation.

Toute action de formation fait l'objet d'un enregistrement archivé par le département du personnel. Après la formation, une Attestation de présence est remplie et donné au département du personnel afin de valider la présence des personnes conviées et de valider ou non leur formation. En cas de formation externe, le diplôme obtenu est inclus dans le dossier personnel de chaque employé.

**5.4 Plan de développement des compétences**

En fonction de la politique de l'entreprise, de ses objectifs de redéploiement stratégique ou simplement de sa démarche continue de progrès, des besoins concrets de formation sont identifiés par la direction et enregistrés dans les Décisions de la revue de direction.

Le suivi des actions de formation, au cours de l'année, permet éventuellement de réviser les moyens mis en place et de mieux les adapter.

Le suivi est assuré par le département du personnel. Chaque responsable lui transmet les coordonnées de l’organisme de formation externe qu’il a choisi ou la fiche pédagogique qu’il a bâtie en interne, avant le début de la formation. Ensuite, chaque formateur ou responsable de département fournit au département du personnel le dossier complet de formation après réalisation de celle-ci, soit :

* le programme
* la liste des personnes ayant participées (cf. Attestation de présence)

Afin de s'assurer que la formation a été profitable, une mesure d'efficacité est réalisée. Le suivi de chaque formation est fait par le chef de département de la personne ayant été formée auprès d'un organisme externe ou en interne 3 mois après la formation.

**5.5 Sensibilisation du personnel**

La politique Sensibilisation et formation précise les droits et obligations du personnel liés aux activités de sensibilisation et de formation. L'accessibilité du serveur (manuel sécurité de l’information, processus, procédures et politiques) permet la diffusion de tous les documents, ce qui contribue à sensibiliser le personnel aux différents aspects du SMSI. Lors des audits, exercices et tests évaluant la capacité à réagir, il est rappelé l'importance du respect des procédures et les risques encourus dans le cas contraire. Les divers affichages, en particulier ceux de la politique de sécurité et les autres politiques contribuent également à la sensibilisation du personnel.

La démarche de sensibilisation à la sécurité de l'information garantit l’atteinte d’un niveau de compréhension de base des questions de sécurité de l'information, telles que les obligations et restrictions découlant des diverses politiques, procédures, directives, lois, règlements et conditions contractuelles en vigueur selon le processus Appliquer la discipline et le document Règles disciplinaires.

Les messages sur lesquels la communication est centrée sont les suivants :

* la sécurité de l’information :
  + enjeux
  + principes
  + responsabilités
  + règles
  + menaces
  + vulnérabilités
* les lois, règlements, chartes, accords
* l’organisation de la sécurité :
  + processus
  + procédures
  + politiques
* les droits et les obligations

Le personnel est sensibilisé à ne pas tenir de conversation confidentielle dans des lieux publics et sur des réseaux de communication non sécurisés.

**5.6 Entretien annuel d’évaluation**

L'entretien annuel d'évaluation du personnel est conduit en début d'année et fait partie du Plan de développement des compétences. Pour les employés la fiche est remplie par le responsable hiérarchique (responsable du département). Pour les cadres c'est le directeur qui conduit les entretiens sauf quand cela est fait par le responsable du département.