#09

Politique **Sécurité de l'information**

Responsabilité sociétale des entreprises

Ce feuillet est consacré à la mise en garde face aux différentes cyber-attaques et les bonnes pratiques à mettre en place.

1. QU'EST-CE QUE LA SECURITE DES SYSTEMES D'INFORMATIONS ?

Cela consiste à assurer la sécurité de l'ensemble de nos biens (site, personne, matériel, réseau, logiciel et organisation).

2. LES DIFFERENTS TYPES D'ATTAQUE

Il existe 4 types principales d'attaques que nous subissons chez Altyor :

- **Ransomware** : cryptage des données
- **Phishing** : envoi d'emails contrefaits
- **Spear phishing** : phishing qui se base sur le réseau personnel / professionnel
- **Attaque au président** : consiste à convaincre le collaborateur d'une entreprise à effectuer un virement à un tiers

3. LES REGLES ESSENTIELLES

- ☑ **Choisir avec soin ses mots de passe**
- ☑ **Choisir l'accès Wi-Fi d'Altyor**
- ☑ **Être aussi prudent avec son smartphone ou sa tablette qu'avec son ordinateur**
- ☑ **Protéger ses données lors de ses déplacements (mot de passe)**
- ☑ **Être prudent lors de l'utilisation de sa messagerie**
- ☑ **Télécharger ses programmes sur les sites officiels des éditeurs (toujours demander la validation du SI)**
- ☑ **Être vigilant lors d'un paiement sur Internet**
- ☑ **Séparer les usages personnels des usages professionnels**
- ☑ **En cas de doute toujours remonter l'information au SI**

4. NOS ENGAGEMENTS

Altyor s'engage à :

- Collecter, utiliser et divulguer de manière responsable, équitable et transparente les données personnelles (toute information relative à une personne pouvant être identifiée directement ou indirectement) des employés, conformément aux lois, normes et normes applicables.
- Traiter les données aux fins légitimes spécifiées explicitement à la personne concernée lorsque le Groupe les a collectées.
- Collecter et traiter uniquement autant de données que nécessaire aux fins spécifiées. Les données personnelles sont principalement utilisées pour les ressources humaines, l'informatique, la santé et la sécurité au travail, les relations de travail, la gestion des infrastructures et les audits.
- Utiliser des mesures organisationnelles, techniques et administratives raisonnables pour protéger les données personnelles sous son contrôle.

5. COMMENT REMONTER L'INFORMATION ?

Votre alerte sera traitée dans les plus brefs délais via votre manager, le service IT, le service RH ou de façon anonyme via :

https://altyor.fr/engagements-rse/

Sanction : il est important de remonter les informations d'attaques, sinon cela peut être considéré comme une faute professionnelle

6. REPORTING

Altyor s'engage à surveiller ses performances en matière de cybersécurité et, à cette fin, suit les indicateurs suivants :

- Nombre d'incidents de sécurité informatique confirmés
- Nombre d'incidents signalés par le biais de la procédure d'alerte

7. PERIMETRE

Cette politique s'applique à toutes les entités du groupe Altyor et toutes les parties prenantes externe du groupe.

8. RESPONSABILITE

Le comité RSE est responsable de la définition de la politique cybersécurité. Le département IT est en charge de veiller à sa bonne application.

9. COMMUNICATION

Cette politique est communiquée chaque année à tous les employés par les canaux habituels de l'entreprise, y compris les règles internes de l'entreprise et l'intranet de l'entreprise, et est présentée à tous les nouveaux membres du personnel lors de leur intégration. Cette politique est également distribuée aux parties prenantes externes et est disponible sur le site web d'Altyor.

10. CONTACT

Pour plus d'informations, veuillez contacter Alexis Lutun alutun@altyor.com ou envoyer un courriel à contact@altyor.com.

11. TABLEAU DE L'HISTORIQUE DES REVISIONS

Cette politique est revue chaque année ou en cas de changement de la politique gouvernementale connexe ou de changements importants dans les activités de l'entreprise.

La présente politique a été approuvée pour la dernière fois le 22 décembre 2023 par Yanis Cottard, Président du groupe Altyor.

Version de la politique	Description de la modification	Date de la modification
A	N/A	Janvier 2023
B	Ajout des KPI dans la politique	Juillet 2023
C	Changement de nom de politique « Sécurité des informations » et ajout de nos engagements envers les collaborateurs	Décembre 2023