POLITIQUE DE CYBERSECURITÉ

---

1. EXPOSÉ DE LA POLITIQUE ET OBJECTIF

La politique de cybersécurité de notre Société décrit nos directives et dispositions pour préserver la sécurité de nos données et de notre infrastructure technologique.

Plus nous nous appuyons sur la technologie pour collecter, stocker et gérer les informations, plus nous devenons vulnérables à de graves violations de la sécurité. Les erreurs humaines, les attaques de pirates informatiques et les dysfonctionnements du système pourraient causer d'importants dommages financiers et mettre en péril la réputation de notre Société.

Pour cette raison, nous avons mis en place plusieurs mesures de sécurité. Nous avons également préparé des instructions qui peuvent aider à atténuer les risques de sécurité. Nous avons exposé ces deux dispositions dans la présente politique.

2. CHAMP D'APPLICATION

Cette politique s'applique à tous nos employés, Administrateurs, Dirigeants, aux employés des filiales et des sociétés affiliées, contractants et à toute personne ayant un accès permanent ou temporaire à nos systèmes et matériels.

3. ÉLÉMENTS DE LA POLITIQUE

A. Données confidentielles

Les données confidentielles sont secrètes et précieuses. Des exemples courants sont :

- Informations financières non publiées
- Données des clients/partenaires/contractants/prestataires de services
- Contrats privés ou conventions gouvernementales
- Données géologiques et techniques
- Données concernant nos opérations minières, nos opérations d'exploration, nos résultats financiers.

- Date et informations concernant les financements, les financements éventuels, les fusions et acquisitions, les partenariats, etc.

Tous les employés doivent prendre toutes les mesures nécessaires pour protéger toutes les données de la Société, y compris les informations spécifiquement confidentielles et faire tout ce qui est nécessaire afin d'éviter les failles de sécurité.

B. Protéger les appareils personnels et ceux de la Société

Lorsque les employés utilisent leurs appareils numériques pour accéder aux courriels ou aux comptes de la Société, ils introduisent un risque de sécurité pour nos données. Nous conseillons à nos employés de sécuriser à la fois leur ordinateur, tablette et téléphone portable personnels et ceux fournis par la Société. Ils peuvent le faire en :

- S'assurant que tous les appareils et systèmes sont protégés par un mot de passe, idéalement avec un authentificateur à deux facteurs si possible.
- Choisissant un mot de passe approprié pour tous les appareils, logiciels, sites et services. Les mots de passe de type MOTDEPASSE123 NOM PRÉNOM ne sont pas autorisés. Vous devez utiliser un mot de passe approprié et qui n'est pas simple à deviner ou à pirater.
- Protégeant tous les appareils par un mot de passe.
- S'assurant que le logiciel antivirus fourni par la Société est à jour sur votre ordinateur.
- Veillant à ne pas laisser leurs appareils exposés ou sans surveillance sans les verrouiller.
- Installant les mises à jour de sécurité des navigateurs, des systèmes d'exploitation et des logiciels systèmes tous les mois ou dès que les mises à jour sont disponibles.
- Utilisant le VPN fourni par la Société lorsque vous accédez à Internet via des réseaux publics.
- Ne se connectant aux comptes et systèmes de la Société que par des réseaux sécurisés et privés.

Nous conseillons également à nos employés d'éviter d'accéder aux systèmes et comptes internes depuis les appareils d'autres personnes, des ordinateurs publics (par exemple: un cybercafé), ou de prêter leurs appareils à d'autres personnes.

C. Protéger les courriels

Les courriels contiennent souvent des escroqueries et des logiciels malveillants (par exemple des chevaux de troie). Pour éviter les infections virales ou le vol de données, nous demandons aux employés de:

- Éviter d'ouvrir les pièces jointes et de cliquer sur les liens lorsque le contenu n'est pas expliqué de manière adéquate (par exemple, "regardez cette vidéo, elle est incroyable").
- Se méfier des titres "pièges à clic" (offrant des prix ou des conseils, par exemple).
- Vérifier l'adresse électronique et le nom des personnes dont ils ont reçu un message pour vous assurer qu'ils sont légitimes, et en cas de doute, ne répondez pas et ne renvoyez pas de SMS, mais entamez une nouvelle conversation avec la personne que vous soupçonnez d'être à l'origine

du problème en utilisant un moyen de communication que vous savez être le sien (son téléphone, un autre e-mail, Teams, en personne, etc.).
- Chercher des incohérences ou des indices (par exemple, des fautes de grammaire, des majuscules, un nombre excessif de points d'exclamation, etc.).

Si un employé n'est pas certain qu'un courriel qu'il a reçu est sûr, il peut s'adresser à nos fournisseurs de services informatiques sur it@ayagoldsilver.com

D. Gérer correctement les mots de passe

Les fuites de mots de passe sont dangereuses car elles peuvent compromettre l'ensemble de notre infrastructure. Non seulement les mots de passe doivent être sécurisés pour ne pas être facilement piratés, mais ils doivent également rester secrets. C'est pourquoi nous demandons à nos employés de:

- Choisir des mots de passe comportant au moins huit caractères (y compris des lettres majuscules et minuscules, des chiffres et des symboles) et éviter les informations qui peuvent être facilement devinées (par exemple, les anniversaires).
- Mémoriser les mots de passe au lieu de les écrire. Si les employés doivent écrire leurs mots de passe, ils sont tenus de garder le document papier ou numérique confidentiel et de le détruire lorsque leur travail est terminé.
- Ne pas échanger les informations d'identification que lorsque cela est absolument nécessaire. Lorsqu'il n'est pas possible de les échanger en personne, les employés doivent préférer le téléphone au courriel, et seulement s'ils reconnaissent personnellement leur interlocuteur.
- Choisir un mot de passe différent entre votre mot de passe de messagerie et votre mot de passe de connexion au réseau/à l'ordinateur.
- Changer leurs mots de passe chaque année.

E. Transférer les données en toute sécurité

Le transfert de données présente un risque pour la sécurité. Les employés doivent :

- Éviter de transférer des données sensibles (par exemple, des informations sur les clients, des dossiers d'employés) vers d'autres appareils ou comptes, sauf en cas de nécessité absolue. Lorsque le transfert massif de telles données est nécessaire, nous demandons aux employés de demander l'aide de notre service informatique.
- Partager les données confidentielles sur le réseau/système de la Société et non sur un Wi-Fi public.
- S’assurer que les destinataires des données sont des personnes ou des organisations dûment autorisées et disposent de politiques de sécurité adéquates.
- S’assurer que la transmission des données à des tiers autorisés se fait via un système de la Société qui assure la sécurité des données, comme les services de partage de données de la Société (par exemple, le one-drive de la Société, Dropbox) et non via un système de transfert personnel (par exemple, le one-drive personnel, we transfer, etc.).

- Signaler les escroqueries, les atteintes à la vie privée et les tentatives de piratage.

Notre fournisseur de services informatiques doit être informé des escroqueries, des brèches et des logiciels malveillants afin de pouvoir mieux protéger notre infrastructure. C'est pourquoi nous demandons à nos employés de signaler dès que possible à nos spécialistes les attaques perçues, les courriels suspects ou les tentatives d'hameçonnage. Notre fournisseur de services informatiques s'occupera d'enquêter rapidement, résoudre le problème et envoyer une alerte à l'échelle de la Société si nécessaire.

Notre fournisseur de services informatiques est chargé de conseiller les employés sur la manière de détecter les courriels frauduleux. Nous encourageons nos employés à les contacter pour toute question ou préoccupation.

F. Mesures supplémentaires

Pour réduire la probabilité de violations de la sécurité, nous demandons également à nos employés de :

- Éteindre leurs écrans et verrouiller leurs appareils lorsqu'ils quittent leur bureau.
- Signaler tout équipement volé ou endommagé dès que possible à leur supérieur et à notre fournisseur de services informatiques.
- Changer les mots de passe de tous les comptes en une seule fois lorsqu'un appareil est volé.
- Signaler une menace perçue ou une éventuelle faiblesse de sécurité dans les systèmes de la Société.
- S'abstenir de télécharger des logiciels suspects, non autorisés ou illégaux sur leur équipement de la Société.
- Éviter d'accéder à des sites Web suspects.

Nous attendons également de nos employés qu'ils se conforment à notre Politique d'utilisation des médias sociaux & d'Internet.

Notre fournisseur de services informatiques doit :

- Installer des pare-feu, des anti-virus, des logiciels anti-malware et des systèmes d'authentification d'accès.
- Informer régulièrement les employés des nouveaux courriels frauduleux ou virus et des moyens de les combattre.
- Mener une enquête approfondie sur les violations de la sécurité.
- Suivre les dispositions de cette politique comme le font les autres employés.

Notre Société disposera de tous les boucliers physiques et numériques pour protéger les informations.

G. Employés à distance

Les employés à distance doivent également suivre les instructions de cette politique. Étant donné qu'ils accèdent à distance aux comptes et aux systèmes de notre Société, ils sont tenus de respecter toutes les normes et tous les paramètres de cryptage et de protection des données, et de veiller à la sécurité de leur réseau privé.

Nous les encourageons à demander conseil à notre fournisseur de services informatiques.

4. ACTION DISCIPLINAIRE

Nous attendons de tous nos employés qu'ils respectent cette politique et ceux qui sont à l'origine de violations de la sécurité s'exposent à des mesures disciplinaires:

- Première infraction à la sécurité, non intentionnelle et à petite échelle : Nous pouvons émettre un avertissement verbal et demander à l'employé de revoir les politiques de sécurité et/ou de revoir le matériel de formation sur la sécurité.
- Violations intentionnelles, répétées ou à grande échelle (qui cause un grave dommage financier ou autre) : Nous appliquerons des mesures disciplinaires plus sévères pouvant aller jusqu'au licenciement. Nous examinerons chaque incident au cas par cas.

En outre, les employés qui ne respectent pas nos instructions de sécurité seront soumis à une discipline progressive, même si leur comportement n'a pas entraîné de violation de la sécurité.

Prenez la sécurité au sérieux

Chacun, qu'il s'agisse de nos clients, de nos partenaires, de nos employés ou de nos sous-traitants, doit avoir le sentiment que ses données sont en sécurité. La seule façon de gagner cette confiance est de protéger de manière proactive nos systèmes et nos bases de données. Nous pouvons tous y contribuer en étant vigilants et en faisant de la cybersécurité une priorité.