Ordre des géologues du Québec

Politique globale de sécurité des systèmes et des données

Adoptée le 10 décembre 2024

1. Préambule

L'utilisation des appareils personnels pour effectuer des tâches professionnelles, la gestion des courriels et la protection des mots de passe sont des éléments essentiels pour la sécurité des informations au sein de notre organisation. Cette politique a pour but de définir des règles et des pratiques visant à assurer la sécurité des données sensibles, la confidentialité des communications électroniques, ainsi que l'intégrité de nos systèmes informatiques.

2. Objectif

Cette politique vise à :

- Encadrer l'utilisation des appareils personnels pour les activités professionnelles afin de protéger les données de l'organisation.
- Assurer des connexions sécurisées pour l'accès aux systèmes de l'organisation.
- Garantir la sécurité des courriels envoyés et reçus dans le cadre professionnel.
- Définir des règles strictes pour la gestion des mots de passe afin de prévenir l'accès non autorisé aux systèmes et données sensibles.

3. Portée

La portée de cette politique inclut tous les employés, collaborateurs externes, partenaires, et toute personne ayant accès aux systèmes, aux courriels ou aux données de l'Ordre.

4. Énoncé de la politique

4.1 Connexions sécurisées

4.1.1 Exigences de connexion :

L'accès aux systèmes et aux données doit être protégé par des mécanismes d'authentification sécurisés (mots de passe forts, authentification multifactorielle (MFA), ou authentification biométrique).

L'utilisation de mots de passe complexes est exigée. Les mots de passe doivent être changés régulièrement et ne doivent pas être partagés (voir la section suivante sur la gestion des mots de passe).

4.1.2 Exigences de connexion :

Pour assurer la sécurité du routeur internet à la maison, il est demandé de réviser les paramètres de cet appareil. Pour cela, vous pouvez suivre les différentes étapes qui se trouvent dans le document ici.

Depuis la maison, il est conseillé de se connecter à un réseau Wi-Fi isolé du reste des appareils de la maison pour travailler. Cela nécessite de créer un accès invité dans les paramètres de sécurité de son routeur.

Les connexions à des réseaux Wi-Fi publics ou non sécurisés sont déconseillées. Il est impératif d'utiliser un VPN fourni par l'organisation pour sécuriser les connexions depuis l'extérieur.

4.1.3 Gestion des sessions :

Verrouillage automatique : Les postes de travail doivent être configurés pour se verrouiller automatiquement après une période d'inactivité. Les utilisateurs doivent également verrouiller manuellement leurs sessions lorsqu'ils s'éloignent de leur poste de travail.

Déconnexion : Les utilisateurs doivent se déconnecter de leurs sessions lorsqu'ils ont terminé de travailler, surtout dans des environnements partagés ou publics.

4.1.4 Départs :

En cas de départ d'un employé, les accès aux systèmes informatiques et aux courriels doivent être révoqués immédiatement.

4.2 Gestion des mots de passe

4.2.1 Création et gestion des mots de passe :

Les mots de passe doivent comporter au minimum 12 caractères et inclure des lettres majuscules, des lettres minuscules, des chiffres et des caractères spéciaux. Ils ne doivent pas être facilement devinables et avoir de lien direct avec l'individu (nom de l'organisation, date importante ou date de naissance ...).

Un gestionnaire de mots de passe est recommandé pour faciliter la gestion des mots de passe complexes. Cet outil permet également de générer aléatoirement des mots de passe, et de les mémoriser.

Chaque utilisateur doit utiliser un mot de passe distinct et unique pour chaque compte professionnel. Les utilisateurs ne peuvent pas utiliser de mots de passe liés au travail pour leurs propres comptes personnels.

4.2.2 Changement et protection des mots de passe :

Les mots de passe doivent être modifiés tous les 6 mois. En cas de soupçon de compromission, un changement immédiat est requis.

Les mots de passe ne doivent pas être partagés et doivent être stockés dans des gestionnaires de mots de passe approuvés, et non sur des supports non sécurisés.

Les mots de passe ne devraient pas être insérés dans des courriels, des messages texte ou d'autres formes de communication électronique ni être révélés par téléphone à quiconque.

L'usage de la fonction « *Mémoriser le mot de passe* » des navigateurs est interdit.

4.2.3 Double facteur d'authentification (2FA) :

Le double facteur d'authentification est un code que l'on reçoit habituellement par texto, qui permet de vérifier que la personne qui est en train de se connecter à la plateforme en ligne est bel et bien la bonne personne, et ce, même si le bon mot de passe a été donné.

Le double facteur d'authentification est exigé pour l'accès à nos systèmes professionnels. Les applications recommandées pour l'authentification sont Google Authenticator ou Microsoft Authenticator.

4.3 Utilisation des appareils personnels

4.3.1 Séparation des utilisations personnelles et professionnelles :

Les appareils personnels utilisés pour des tâches professionnelles doivent être séparés des sessions personnelles. Il est recommandé de créer des sessions distinctes pour les activités professionnelles et pour l'utilisation personnelle.

Si l'appareil personnel servant aux tâches professionnelles de l'employé est partagé par quelqu'un d'autre que lui, il est impératif de cloisonner la session de travail des autres sessions de l'ordinateur. Pour cela, il suffit de créer une session qui sera dédiée au travail, et d'utiliser une session distincte pour l'utilisation personnelle.

4.3.2 Sécurité des appareils :

Chaque appareil personnel doit être sécurisé par un mot de passe, un NIP, une empreinte digitale ou une reconnaissance faciale.

L'appareil doit se verrouiller automatiquement après une période d'inactivité.

L'installation d'un antivirus est obligatoire et il doit être activé en tout temps.

Les appareils doivent être régulièrement mis à jour pour inclure les derniers correctifs de sécurité.

Il est strictement interdit de travailler depuis des logiciels piratés. L'organisation met à disposition tous les logiciels officiels nécessaires aux tâches des équipes.

4.3.3 Stockage des données :

En tout temps, l'organisation demeure propriétaire des informations professionnelles consultées sur l'appareil personnel de l'employé.

Aucune donnée organisationnelle ne doit être stockée sur l'appareil personnel de l'employé. Les données doivent être conservées dans les systèmes de l'organisation ou sur des plateformes sécurisées (Connexence, Microsoft 365, Constellio).

4.3.4 Responsabilité en cas de perte ou vol :

En cas de perte ou de vol de l'appareil, l'employé doit immédiatement informer le département informatique.

L'employé sera tenu responsable de tout accès non autorisé aux données professionnelles.

4.3.5 Imprimante :

Bien qu'il soit permis d'imprimer depuis son appareil personnel, les documents imprimés contenant des informations sensibles devraient être détruits.

4.4 Gestion des courriels

4.4.1 Envoi et réception de courriels :

Les informations sensibles ne doivent pas être envoyées par courriel. Il est préférable d'utiliser des outils de stockage partagés sécurisés (par exemple, OneDrive, Google Drive) pour le partage de documents sensibles. Seul le destinataire doit avoir accès au dossier partagé. Après réception de l'information sensible depuis ce dossier partagé, il est demandé d'enregistrer le(s) document(s) dans nos systèmes internes, de supprimer l'information du dossier partagé et de désactiver le partage du dossier.

Les informations considérées comme sensibles incluent, mais ne se limitent pas aux données personnelles identifiables (DPI), aux Informations financières, aux données de santé, aux informations confidentielles sur les clients ou sur l'organisation.

Si un courriel doit être utilisé pour transmettre des informations sensibles, il doit être protégé par un mot de passe robuste.

Aucune information sensible ne doit être conservée dans une boîte courriel. Toute information sensible devrait être transférée dans nos dossiers d'organisation puis supprimée définitivement de la boîte courriel.

Soyez vigilant concernant les courriels suspects et ne jamais répondre ou cliquer sur des liens dans des messages douteux.

Éviter d'envoyer des courriels en copie conforme (cc). Pour les courriels destinés à plusieurs personnes qui ne se connaissent pas nécessairement, utilisez la copie conforme invisible (cci) pour préserver la confidentialité.

Tout utilisateur soupçonnant que de l'information a été partagée ou communiquée par erreur doit signaler l'incident à son gestionnaire.

Les courriels doivent être utilisés principalement pour des fins professionnelles.

L'utilisation personnelle des courriels professionnels doit être minimale et ne pas interférer avec les tâches de l'organisation.

4.4.2 Accès et authentification des courriels :

Les comptes de courriels doivent être protégés par des mots de passe sécurisés, conformément aux points précédents sur les mots de passe.

L'accès aux courriels doit être limité aux personnes autorisées.

5. Sensibilisation et formation

Tous les employés doivent suivre des formations régulières sur la sécurité des systèmes d'information, la gestion des mots de passe, l'utilisation sécurisée des appareils personnels et des courriels.

Nexxo fournira des rappels périodiques et des mises à jour sur les menaces potentielles et les mesures de sécurité recommandées.

6. Non-conformité et sanctions

Tout manquement à cette politique peut entraîner des sanctions disciplinaires, y compris la suspension ou la résiliation des droits d'accès aux systèmes de l'Ordre, ainsi que des mesures plus sévères en cas de violation des règles de sécurité.

7. Révision et mise à jour

Cette politique sera révisée tous les deux ans ou en cas de changement significatif dans les menaces de sécurité ou la réglementation.

8 Contact

Pour toute question relative à cette politique, veuillez contacter dirgen@ogq.qc.ca.

9. Historique des versions

Numéro de version	Date de révision	Description des modifications	Auteurs des modifications
1.0	10 décembre 2024	Version initiale	Rédaction : Alain Cromp Révision : Charlotte Athurion