ADGC

Politique de cybersécurité

Adoptée le 2 février

2023

1. Introduction

Le risque de failles de sécurité peut avoir un impact néfaste sur les systèmes, l'infrastructure technologique et la réputation de l'ADGC. Par conséquent, l'Association créée cette politique pour aider à décrire les mesures de sécurité mises en place pour s'assurer que les informations restent sécurisées et protégées.

Elle s'inscrit également dans une perspective de prévention et s'appuie sur la collaboration de ses ressources et la communauté qui gère les actifs informatiques dans le but d'en assurer une gestion sécuritaire et responsable.

2. Objectifs

Les objectifs de cette politique sont de :

a) protéger les données et l'infrastructure
b) sensibiliser les ressources et décrire les protocoles et les directives qui régissent les mesures de cybersécurité
c) définir les règles pour l'utilisation par l'entreprise et l'utilisation personnelle
d) énumérer le processus disciplinaire de l'entreprise pour les violations de la politique.

3. Champ d'application

Cette politique s'applique à tous les travailleurs à distance, aux employés permanents et à temps partiel, aux fournisseurs, aux stagiaires et/ou à toute personne ayant accès aux systèmes électroniques, aux informations, aux logiciels et/ou au matériel de l'entreprise.

4. Données confidentielles

La définition des « données confidentielles » est la suivante :

- Informations financières non divulguées et classifiées
- Informations sur les membres et les administrateurs
- Les mots de passe, les affectations et les informations personnelles des employés
- Les contrats de l'entreprise et les dossiers juridiques.

5. Sécurité des appareils

Utilisation par l'entreprise

Pour assurer la sécurité de tous les appareils et de l'information fournis par l'entreprise, les employés doivent :

- Garder tous les appareils fournis par l'entreprise protégés par un mot de passe. Cela inclut les tablettes, les ordinateurs et les appareils mobiles
- Sécuriser tous les appareils pertinents à la fin des heures de travail
- S'abstenir de partager des mots de passe privés avec des collègues, des connaissances personnelles, des cadres supérieurs et/ou des administrateurs
- Mettre régulièrement à jour les appareils avec les derniers logiciels de sécurité
- S'abstenir de toute utilisation illicite (destruction du matériel, actes portant atteinte à l'intégrité des données, harcèlement, activités commerciales personnelles, jeu de hasard, activités illégales, toute activité liée à du matériel sexuellement explicite)
- Assurer la protection des actifs informatiques sous leur responsabilité.

Utilisation personnelle

Il est reconnu que les employés peuvent être amenés à utiliser des appareils personnels pour accéder aux systèmes de l'entreprise. Dans ces cas, les employés doivent signaler cette information à la direction. Pour assurer la protection des systèmes de l'entreprise, tous les employés sont tenus de :

- Assurer que tous les appareils personnels utilisés pour accéder aux systèmes liés à l'entreprise sont protégés par un mot de passe
- Installer un logiciel antivirus complet
- Mettre régulièrement à niveau le logiciel antivirus
- Verrouiller tous les appareils s'ils sont laissés sans surveillance
- Toujours utiliser des réseaux sécurisés et privés.

6. Sécurité du courrier électronique

La protection des systèmes de courrier électronique est une priorité élevée, car les courriels peuvent conduire à des vols de données, des escroqueries et transporter des logiciels malveillants. Par conséquent, les ressources doivent :

- Vérifier la légitimité des courriels (adresse électronique et le nom de l'expéditeur)
- Éviter d'ouvrir des courriels suspects, des pièces jointes et de cliquer sur des liens
- Porter une attention aux erreurs grammaticales significative
- Contactez la direction ou le service informatique concernant tout courriel suspect
- Alerter immédiatement le service informatique concernant toute violation, logiciel malveillant et/ou escroquerie.
    - Pour rejoindre Solutions MC :
    - Téléphone : (514) 929-2547
    - Courriel : soutien@solutionsmc.ca

7. Transfert de données

L'Association reconnaît les risques de sécurité liés au transfert de données confidentielles en interne et/ou en externe. Pour minimiser les risques de vol de données, nous demandons à tous les employés de :

- S'abstenir de transférer des informations classifiées aux parties extérieures
- Transférer des données confidentielles via le réseau
- Obtenir l'autorisation nécessaire de la haute direction
- Vérifier le destinataire des informations et s'assurer qu'il a mis en place les mesures de sécurité appropriées
- S'en tenir à la loi sur la protection des données et à l'accord de confidentialité.

8. Sécurité logicielle, réseau et web

- Authentification à double / 2FA
- Les portables requièrent une authentification au démarrage des sessions
- Les appareils se mettent en veille après une période d'inactivité
- La base de données est hébergée sur Microsoft Azur, une base infonuagique hautement sécurisée
- Nul ne peut accéder à la base de données autrement que via l'adresse IP fixe de l'employé étant celle du lieu habituel de travail
- Système automatique de mise à jour des logiciels et antivirus
- Système de surveillance des équipements externe.

9. Sécurité du site web ADGC

- Conforment à l'initiative de centralisation de gestion des noms de domaine visant à assurer la légitimité des sites web et normaliser les pratiques en matière de gestion de domaine pour en assurer la sécurité, le domaine adgcq.com a été transféré dans le portefolio Desjardins.
- Le site de l'ADGC est sécurisé par un certificat SSL (Secure Sockets Layer) Entrust correspondant aux normes de sécurité Desjardins.

10. Action disciplinaire

La violation de cette politique peut entraîner une action disciplinaire, pouvant aller jusqu'au licenciement. Les protocoles disciplinaires sont basés sur la gravité de la violation. Les violations involontaires ne justifient qu'un avertissement verbal, les violations fréquentes de même nature peuvent donner lieu à un avertissement écrit et les violations intentionnelles peuvent entraîner une suspension et/ou un licenciement, selon les circonstances du cas.