Politique de sécurité de l'information:

Département TI :

Action Travail des femmes

7000 Av du Parc suite bureau 404, Montréal, QC H3N

Téléphone : 514-768-7233

www.atfquebec.ca

700-407 Rue McGill, Montréal, QC, Canada

Téléphone : 514-463-1748 |Support : 514-819-0353

support@gcs-technologie.com | www.gcstechnologie.com

Préparé par : Luidgi Patrizio Samedi | GCS TECHNOLOGIE |

Réseautique - Intégration - Gestion - Conception
Consultation - Développement – Support

3 Février 2023

1. Objectif :

La Politique de sécurité de l'information de ATF (ci-après, la Politique) définit des principes et rôles et responsabilités pour protéger les employés (ci-après, les employés), ses infrastructures technologiques et son information comme actif stratégique.

Elle indique les attentes de ATF liées à la protection de l'information de ATF eu égard des employés qui conçoivent, développent ou utilisent des systèmes d'information. Cette politique respecte les normes et la législation applicable en matière de sécurité de l'information.

Cette politique est basée sur deux axes importants :

1- Protection de l'information

2- Comportement du responsable face aux risques associés à l'information

L'entreprise doit restreindre l'accès aux données confidentielles et sensibles pour éviter qu'elles ne soient perdues ou compromises, de façon à ne pas nuire à nos clients, à ne pas encourir de sanctions pour non-conformité et à ne pas nuire à notre réputation. Parallèlement, nous devons faire en sorte que les utilisateurs puissent accéder aux données qui leur sont nécessaires pour travailler efficacement.

Il n'est pas attendu de cette politique qu'elle élimine tous les vols de données. Son principal objectif est plutôt de sensibiliser les utilisateurs et d'éviter les scénarios de perte accidentelle, c'est pourquoi elle décrit les exigences de prévention des fuites de données.

2. Champ d'application

Cette politique de sécurité des données s'applique à toutes les données clients, données personnelles ou autres données de l'entreprise définies comme sensibles par la politique de classification des données de l'entreprise. Elle s'applique donc à tous les serveurs, bases de données et systèmes informatiques qui traitent ces données, y compris tout appareil régulièrement utilisé pour le courrier électronique, l'accès au Web ou d'autres tâches professionnelles. Tout utilisateur qui interagit avec les services informatiques de l'entreprise est également soumis à cette politique.

3. Politique

3.1- Principes

L'entreprise fournira à tous ses employés et à ses sous-traitants l'accès aux informations dont ils ont besoin pour effectuer leur travail aussi efficacement que possible.

3.2- Généralité

a. Chaque utilisateur sera identifié par un ID utilisateur unique, afin que tous puissent être tenus pour responsables de leurs actions.

b. L'utilisation des identités partagées n'est autorisée que là où elles sont appropriées, par exemple pour les comptes de formation ou les comptes de service.

c. Chaque utilisateur doit lire la présente politique de sécurité des données, ainsi que les directives de Connexion et de déconnexion, et signer une déclaration stipulant qu'ils comprennent les conditions d'accès.

d. Les enregistrements des accès des utilisateurs peuvent être utilisés comme éléments probants dans le cadre d'une enquête sur incident de sécurité.

e. Les accès doivent être accordés selon le principe du moindre privilège, ce qui signifie que chaque programme et chaque utilisateur obtiendra seulement les privilèges qui lui sont nécessaires pour effectuer son travail.

3.3 Autorisation de contrôle d'accès

L'accès aux ressources et aux services informatiques de l'entreprise sera accordé par le biais d'un compte d'utilisateur unique et d'un mot de passe complexe.

Les mots de passe sont gérés par le centre d'assistance informatique. Les exigences relatives à la longueur, à la complexité et à l'expiration des mots de passe sont indiquées dans la politique des mots de passe de l'entreprise.
Le contrôle d'accès basé sur les rôles sert à sécuriser les accès à toutes les ressources basées sur fichiers dans les domaines d'Active Directory.

3.4 Accès aux réseaux

a. Un accès aux réseaux doit être accordé à tous les employés et sous-traitants, selon les procédures de contrôle d'accès de l'entreprise et le principe du moindre privilège.

b. Tous les employés et sous-traitants bénéficiant d'un accès distant aux réseaux de l'entreprise doivent être authentifiés par le mécanisme d'authentification du VPN uniquement.

c. Les réseaux doivent être séparés selon les recommandations issues des recherches de sécurité sur les réseaux de l'entreprise. Les administrateurs réseaux doivent regrouper les services et systèmes informatiques et les utilisateurs selon les besoins de cette séparation.

d. Des contrôles de routage des réseaux doivent être mis en place pour appliquer la politique de contrôle d'accès.

3.5 Responsabilités des utilisateurs

a. Tous les utilisateurs doivent verrouiller leur écran chaque fois qu'ils quittent leur bureau, pour réduire le risque d'accès non autorisé.

b. Tous les utilisateurs doivent veiller à ne laisser aucune information sensible ou confidentielle autour de leur poste de travail.

c. Tous les utilisateurs doivent tenir leurs mots de passe confidentiels et ne pas les partager.

3.6 Accès aux applications et aux informations

a. Tous les employés et sous-traitants de l'entreprise doivent bénéficier d'un accès aux données et aux applications nécessaires à leur fonction professionnelle.

b. Tous les employés et sous-traitants ne doivent accéder aux données et systèmes sensibles qu'en cas de nécessité professionnelle et avec l'accord de la direction.

c. Les systèmes sensibles doivent être physiquement ou logiquement isolés afin d'en restreindre l'accès au personnel autorisé uniquement.

3.7 Accès aux informations confidentielles et restreintes

a. L'accès aux données classées comme « confidentielles » ou « restreintes » doit être limité aux personnes autorisées dont les responsabilités professionnelles l'exigent, tel que déterminé par la Politique de sécurité des données ou la direction.

b. Le service de sécurité informatique est responsable d'instaurer les restrictions d'accès.

4. Directives techniques

Les directives techniques spécifient toutes les exigences relatives aux contrôles techniques utilisés pour accorder l'accès aux données.

Voici un exemple :

Les méthodes de contrôle d'accès à utiliser incluent :

• Audit des tentatives de connexion à tout appareil connecté au réseau de l'entreprise

• Autorisations Windows NTFS pour les fichiers et dossiers

• Modèle d'accès basé sur les rôles

• Droits d'accès aux serveurs

• Autorisations relatives aux pares-feux

• Listes de contrôle d'accès aux zones du réseau et au réseau local virtuel

• Droits d'authentification Web

• Droits d'accès et listes de contrôle d'accès aux bases de données

• Chiffrements des données au repos et en transit

• Séparation des réseaux entreprises de surveiller et protéger leurs informations et réseaux les plus vulnérables.

5. Exigences de reporting

Cette section décrit les exigences de documentation des incidents.

a. Des rapports d'incidents quotidiens doivent être produits et traités par le service de sécurité informatique ou l'équipe d'intervention sur incident.

b. Des rapports d'incidents hebdomadaires détaillés doivent être produits par le service de sécurité informatique et envoyés au DSI.

c. Les incidents hautement prioritaires découverts par le service de sécurité informatique doivent être immédiatement remontés. Le DSI doit être contacté aussi vite que possible.

d. Le service de sécurité informatique doit également produire un rapport mensuel indiquant le nombre d'incidents de sécurité informatique et le pourcentage d'entre eux qui ont été résolus.

6. Propriété et responsabilités

Vous indiquez ici qui est propriétaire de quoi et qui est responsable de quelles actions et de quels contrôles.

- ✓ Les propriétaires de données sont des employés dont la principale responsabilité est de gérer les informations qu'ils possèdent ; il peut s'agir par exemple d'un cadre, un chef de service ou un chef d'équipe.
- ✓ L'administrateur de la sécurité des informations est un employé chargé par les responsables informatiques d'assurer un soutien administratif pour l'implémentation, la supervision et la

coordination des procédures et systèmes de sécurité, conformément aux ressources informatiques spécifiques.

- ✓ Les utilisateurs comprennent tous ceux qui ont accès aux ressources informatiques, par exemple les employés, les entités de confiance, les sous-traitants, les consultants, les employés à l'essai, les employés temporaires et les bénévoles.
- ✓ L'équipe d'intervention en cas d'incident doit être dirigée par un cadre et inclure des employés de services tels que, par exemple : infrastructure informatique, sécurité des applications informatiques, juridique, financier et ressources humaines.

7. Application

Tout utilisateur qui enfreint cette politique est passible de sanctions disciplinaires, pouvant aller jusqu'au licenciement. Tout partenaire ou sous-traitant tiers surpris en infraction peut voir sa connexion au réseau suspendue.

8. Définitions

Ce paragraphe définit tous les termes techniques utilisés dans la présente politique.

- ✓ Liste de contrôle d'accès (ACL) – Liste des règles ou des entrées de contrôle d'accès (ACE). Chaque ACE d'une ACL identifie une entité de confiance et précise ses droits d'accès autorisés, refusés ou contrôlés.
- ✓ Base de données – Ensemble organisé de données, généralement stocké et accessible électroniquement depuis un système informatique.
- ✓ Chiffrement – Processus de codage d'un message ou d'autres informations afin que seules les parties autorisées puissent y accéder.
- ✓ Pare-feu – Dispositif permettant d'isoler un réseau d'un autre. Les pares-feux peuvent être des systèmes autonomes ou inclus dans d'autres dispositifs, par exemple des routeurs ou des serveurs.
- ✓ Séparation du réseau – Division du réseau en unités logiques ou fonctionnelles appelées zones. Par exemple, vous pouvez avoir une zone pour les ventes, une zone pour le support technique et une autre zone pour la recherche, chacune ayant des besoins techniques différents.
- ✓ Contrôle d'accès basé sur les rôles (RBAC) – Mécanisme de contrôle d'accès neutre en termes de politique, défini selon les rôles et les privilèges.
- ✓ Serveur – Programme ou appareil informatique qui fournit des fonctionnalités à d'autres programmes ou appareils, appelés clients.
- ✓ Réseau privé virtuel (VPN) – Connexion à un réseau privé sécurisé via un réseau public.
- ✓ VLAN (réseau local virtuel) – Groupement logique d'appareils au sein d'un même domaine de

diffusion.

9. Documents connexes

- Politique des mots de passe
- Politique de prévention des données
- Gestion de maintenance

SUPPORT TECHNIQUE :

Contacter le département TI en cas de besoin de support.

Téléphone : 514-819-0353 ext.207

Cellulaire : 514-463-1748

Courriel : support@gcs-technologie.com

Contact : Luidgi Patrizio Samedi