POSA Source des Monts

Politiques de sécurité informatique

Document interne – Confidentiel

Version 1.21 – 30 octobre 2025

Adopté par le conseil d'administration : 10 février 2026

Table des Matières

Contenu

1. Politique de gestion des mots de passe

1.1 Contexte

POSA Source des Monts est un organisme à but non lucratif (OBNL) œuvrant dans la communauté de Chambly depuis 25 ans.

Ses employés, bénévoles et partenaires utilisent des systèmes informatiques, des adresses courriel et des plateformes collaboratives afin de soutenir la mission sociale de l'organisme.

La protection des données (dossiers des participants, informations des partenaires financiers, documents internes) est essentielle.

Comme les mots de passe représentent la première ligne de défense contre les intrusions, il est primordial d'établir une politique claire pour leur gestion.

1.2 Objectif de la politique

Garantir que l'accès aux systèmes, documents et plateformes de POSA Source des Monts soit protégé par des mots de passe robustes et confidentiels, réduisant ainsi les risques de vol de données, d'usurpation d'identité et de bris de confidentialité.

1.3 Directives

- Chaque utilisateur doit posséder un mot de passe unique, **personnel et confidentiel**.
- Les mots de passe doivent comporter au minimum 10 caractères, avec une **combinaison de lettres majuscules, minuscules, chiffres et symboles.**
- Les mots de passe doivent être changés au moins **une fois par année** ou immédiatement si une fuite ou un doute de compromission survient.
- Il est strictement interdit de partager ou d'écrire un mot de passe sur un support papier, dans un courriel ou par messagerie instantanée.
- Lorsqu'un employé, stagiaire ou bénévole quitte son rôle, son accès doit être révoqué sans délai.

1.4 Conséquences en cas de non-respect

- Perte ou vol de données sensibles.
- Retrait immédiat des accès informatiques.
- Mesures disciplinaires pouvant aller jusqu'à la cessation du lien d'engagement avec l'organisme.
- Signalement aux autorités compétentes en cas de négligence grave entraînant une fuite de données personnelles.

1.5 Responsabilités

- Direction : s'assurer que les règles sont connues et appliquées.
- Employés et bénévoles : respecter rigoureusement les consignes.
- Responsable informatique ou désigné : gérer les accès, révoquer rapidement les anciens comptes.

2. Politique de gestion sécurisée des courriels

2.1 Contexte

Le courriel demeure le moyen de communication le plus utilisé par POSA Source des Monts pour ses échanges internes et externes (participants, partenaires financiers, institutions publiques, donateurs).

Cependant, il s'agit aussi du principal vecteur d'attaques (hameçonnage, virus, usurpation).

Une politique claire est nécessaire pour protéger l'intégrité de l'organisme.

2.2 Objectif de la politique

Réduire les risques de cyberattaques, de perte de données et de bris de confidentialité en instaurant des pratiques sécurisées dans l'utilisation des courriels.

2.3 Directives

- Les adresses courriel de POSA Source des Monts doivent être utilisées uniquement pour des communications liées aux activités de l'organisme.
- Les utilisateurs doivent être vigilants face aux courriels suspects (liens douteux, pièces jointes inattendues, fautes grossières, demandes inhabituelles).
- Les informations sensibles (données personnelles, financières ou médicales) ne doivent jamais être transmises par courriel sans chiffrement ou méthode sécurisée approuvée.
- Une signature normalisée doit être utilisée pour représenter l'organisme.
- Les comptes de messagerie doivent être protégés par des mots de passe robustes et, lorsque possible, par l'authentification à deux facteurs (2FA).
- Les courriels frauduleux ou suspects doivent être signalés immédiatement à la direction.

2.4 Conséquences en cas de non-respect

- Risque de fraude financière ou de fuite d'information.
- Suspension de l'accès courriel en cas d'usage abusif.
- Mesures disciplinaires selon la gravité de l'incident.

2.5 Responsabilités

- Direction : sensibiliser les utilisateurs aux menaces et adopter des mesures de sécurité (filtrage, antivirus).
- Employés et bénévoles : appliquer les consignes, signaler rapidement tout incident.
- Responsable informatique : mettre en place des protections techniques (filtrage anti-spam, sauvegardes).

3. Politique de connexion sécurisée (VPN)

3.1 Contexte

Les employés et bénévoles accèdent aux systèmes de POSA Source des Monts depuis divers lieux : au bureau, en télétravail, ou parfois à partir d'événements communautaires.

Les risques de compromission (Wi-Fi publics, appareils non sécurisés) sont réels et peuvent menacer la confidentialité des informations.

3.2 Objectif de la politique

Assurer que toutes les connexions aux systèmes et aux données de POSA Source des Monts se fassent de façon sécurisée, minimisant les risques de piratage ou d'accès non autorisé.

3.3 Directives

- Tous les systèmes (ordinateurs, plateformes en ligne, dossiers partagés) doivent être protégés par un mot de passe conforme à la politique.
- L'authentification multi facteur (2FA) doit être activée lorsqu'elle est disponible.
- Les connexions en télétravail doivent se faire à partir de réseaux fiables (interdiction des Wi-Fi publics non sécurisés).
- Les postes de travail doivent se verrouiller automatiquement après 15 minutes d'inactivité.
- L'accès aux fichiers et aux applications est accordé uniquement selon le principe du moindre privilège (accès minimal nécessaire à la fonction).
- Les tentatives de connexion suspectes doivent être signalées immédiatement à la direction.

3.4 Conséquences en cas de non-respect

- Exposition de données confidentielles.
- Suspension de l'accès aux systèmes.
- Mesures disciplinaires pouvant aller jusqu'à la cessation du lien d'engagement.

3.5 Responsabilités

- Direction : veiller à l'application de la politique et autoriser les accès selon les rôles.
- Employés et bénévoles : sécuriser leur poste et signaler tout incident.
- Responsable informatique : surveiller les accès, détecter les anomalies, mettre à jour les protections.

4. Politique d'utilisation des appareils personnels (BYOD)

4.1 Contexte

Plusieurs employés et bénévoles de POSA Source des Monts utilisent leurs appareils personnels (téléphones, ordinateurs, tablettes) pour accéder aux courriels ou aux documents liés à l'organisme.

Bien que pratique, cette réalité augmente les risques de perte ou de fuite de données.

4.2 Objectif de la politique

Encadrer l'utilisation des appareils personnels pour assurer la sécurité des données de l'organisme et réduire les risques associés à leur usage.

4.3 Directives

- L'utilisation d'appareils personnels doit être autorisée par la direction.
- Tout appareil personnel utilisé pour accéder aux systèmes de POSA Source des Monts doit être protégé par :
  - un mot de passe ou code d'accès,
  - un antivirus à jour,
  - des mises à jour régulières du système.
- Il est interdit de stocker de façon permanente des données sensibles de l'organisme sur un appareil personnel.
- En cas de perte, vol ou compromission d'un appareil, l'utilisateur doit en informer la direction immédiatement.
- L'organisme se réserve le droit d'exiger la suppression des données de POSA Source des Monts présentes sur un appareil personnel lors de la fin d'un mandat.

4.4 Conséquences en cas de non-respect

- Risque de fuite d'informations confidentielles.
- Retrait de l'autorisation d'utiliser un appareil personnel.
- Mesures disciplinaires selon la gravité du manquement.

4.5 Responsabilités

- Direction : encadrer et autoriser l'utilisation des appareils personnels.
- Employés et bénévoles : protéger leurs appareils et respecter les règles.
- Responsable informatique : fournir les conseils techniques nécessaires et superviser la sécurité.

5. Politique d’utilisation de Messenger interne

5.1 Contexte

POSA Source des Monts utilise Messenger (ou une messagerie instantanée similaire) pour faciliter la communication rapide entre employés, bénévoles et direction.
Bien que pratique et conviviale, cette plateforme n’est pas conçue pour la transmission d’informations sensibles ou confidentielles. Une politique d’usage est donc essentielle pour assurer la cohérence, la sécurité et la confidentialité des échanges.

5.2 Objectif de la politique

Assurer que l’utilisation de Messenger interne demeure conforme aux valeurs de l’organisme, respecte la confidentialité des données et soutient un climat de travail professionnel et respectueux.

5.3 Directives

- Messenger doit être utilisé uniquement pour des communications liées aux activités de POSA Source des Monts.
- Les informations confidentielles (participants, dossiers internes, données financières) ne doivent jamais être partagées sur Messenger.
- Les utilisateurs doivent éviter de joindre des documents officiels (contrats, listes de bénéficiaires, rapports) sur la plateforme — ces fichiers doivent être transmis par les canaux sécurisés approuvés.
- Les groupes Messenger doivent être créés et gérés avec l’autorisation de la direction.
- Un langage professionnel et respectueux est obligatoire en tout temps.
- Les notifications de sécurité (tentatives d’hameçonnage, liens douteux) doivent être signalées immédiatement.
- Lorsqu’un employé ou bénévole quitte l’organisme, il doit être retiré de tous les groupes Messenger internes sans délai.

5.4 Conséquences en cas de non-respect

- Risque de fuite ou mauvaise diffusion d’informations.
- Retrait immédiat des groupes Messenger internes.
- Mesures disciplinaires pouvant aller jusqu’à la cessation du lien d’engagement

6. Section signature et attestation

Je

Soussigné(e), atteste avoir lu, compris et accepté les politiques de cybersécurité de POSA Source des Monts, Chambly.

Nom :

Fonction :

Date : 130 octobre 2025

Signature

X _____