CHARTE DE SENSIBILISATION DES UTILISATEURS À LA SÉCURITÉ

Bonnes pratiques, authentification et protection des données

Référence	PCG-SMSI-021
Version	1.1
Date	29/06/2026
Classification	Public
Rédacteur	Romain PONSOT — RSSI
Approbateur	Romain PONSOT — Direction

Suivi des versions

Version	Date	Auteur	Description
1.0	18/06/2026	R. PONSOT	Création initiale
1.1	29/06/2026	R. PONSOT	Reclassement en document Public ; titre précisé (sensibilisation des utilisateurs). Mise à jour suite à l'audit interne IMSM.

1. Objet

La présente charte sensibilise aux bonnes pratiques de sécurité de l'information les utilisateurs de l'application ponsotconseilgestion.com, conformément à la mesure A.6.3 de l'Annexe A de la norme ISO/IEC 27001:2022.

Contrôle	Intitulé	Couverture
A.6.3	Sensibilisation, enseignement et formation	Bonnes pratiques de mots de passe, double authentification, vigilance hameçonnage, protection des données et confidentialité

2. Périmètre

Cette charte s'adresse au Responsable de la Sécurité de l'Information (auto-formation) ainsi qu'à l'ensemble des utilisateurs de l'application au sein des cabinets clients : Associé, Collaborateur, Stagiaire et Secrétaire.

3. Mots de passe

- Un mot de passe est obligatoire pour créer un compte et accéder à l'application.
- Il doit comporter au minimum 8 caractères dont au moins une majuscule, une minuscule, un chiffre et un caractère spécial.
- Le mot de passe ne doit jamais être réutilisé sur d'autres services ni partagé ; l'usage d'un gestionnaire de mots de passe est recommandé.
- Après 10 tentatives échouées, le compte est temporairement verrouillé.

4. Double authentification (2FA)

La double authentification ajoute un second facteur au mot de passe : un code temporaire à usage unique (TOTP), valable 30 secondes, généré par une application d'authentification (Google Authenticator, Authy, 1Password…).

- Elle est obligatoire pour le compte administrateur (super_admin) et activable par tout utilisateur depuis le menu « Sécurité » de son profil.
- À la première activation, l'utilisateur scanne un QR code ; ensuite, le code à 6 chiffres est demandé à chaque connexion.
- En cas de perte du téléphone, la double authentification est réinitialisée par l'administrateur, qui impose un nouvel enrôlement.

5. Hameçonnage (phishing)

Les avocats et leurs cabinets sont des cibles privilégiées d'attaques par hameçonnage. Les réflexes attendus :

- vérifier l'expéditeur et se méfier des messages urgents ou inhabituels ;
- ne jamais cliquer sur un lien ni ouvrir une pièce jointe suspecte ;
- ne jamais communiquer ses identifiants, son mot de passe ou un code de double authentification ;
- en cas de doute, signaler le message (section 7).

6. Protection des données et confidentialité

Les données traitées sont couvertes par le secret professionnel de l'avocat. Les utilisateurs doivent en préserver la confidentialité et respecter la classification (Public / Interne / Confidentiel).

- Aucune donnée sensible (coordonnées bancaires, informations clients) ne doit être exposée ou transmise en dehors de l'application.
- Les informations publiées sont disponibles sur les pages statiques du site : /confidentialite (politique de confidentialité), /mentions-legales, /cgu et /cookies.

7. Signalement

Tout incident, comportement suspect ou perte de moyen d'authentification doit être signalé sans délai au responsable de la sécurité informatique :

Référent : Romain Ponsot

@: contact@ponsotconseilgestion.com

T: 00 33 (7) 87 28 92 95

Approbation

La présente charte de sensibilisation est approuvée par le responsable du SMSI. Il engage l'organisation à mettre en œuvre les audits selon le modèle de revue de direction établis aux présentes et dans les délais impartis.

Rôle	Nom	Date	Signature
Responsable SMSI (Direction)	Romain Ponsot	02/07/2026