	Retour au Dossier Organisationnel Liste des procédures Proc#138 - Arrivée d'un collaborateur ou d'un stagiaire
Sujets connexes	Documentation proton

Notice d’utilisation de Proton Pass : Guide de bonnes pratiques d’usage

1. Objectif de Proton Pass

Proton Pass est un gestionnaire de mots de passe sécurisé développé par Proton. Il permet :

- de stocker et gérer ses mots de passe de manière chiffrée et confidentielle
- de générer automatiquement des mots de passe forts et uniques
- de synchroniser ses identifiants sur tous ses appareils (ordinateur, mobile, tablette)
- de sécuriser l’accès aux comptes professionnels et personnels

2. Bonnes pratiques d’usage

Gestion des mots de passe

- Utiliser Proton Pass pour tous les comptes professionnels sensibles
- Créer des mots de passe longs et complexes via le générateur intégré
- Ne jamais réutiliser le même mot de passe sur plusieurs services
- Mettre à jour régulièrement les mots de passe importants (administration, messagerie, etc.)

Organisation

- Classer les identifiants par dossiers (ex. : *Comptes Pro*, *Comptes Perso*)
- Utiliser des étiquettes pour retrouver rapidement les accès
- Partager uniquement les identifiants nécessaires avec les collègues de confiance
- Supprimer les comptes ou identifiants obsolètes

3. Bonnes pratiques techniques

- Activer l’authentification à deux facteurs (2FA) sur Proton Pass et sur les comptes critiques
- Installer l’extension Proton Pass sur les navigateurs pour remplir automatiquement les identifiants
- Utiliser l’application mobile Proton Pass pour un accès sécurisé en déplacement
- Garder l’application et l’extension à jour pour bénéficier des dernières protections

4. Respect et éthique

- Ne pas stocker de mots de passe non liés à l'activité professionnelle dans l'espace commun (si usage partagé)
- Ne jamais communiquer un mot de passe en clair par email ou messagerie instantanée
- Respecter la confidentialité des identifiants partagés via Proton Pass

5. Cas d'usage recommandés

Recommandé :

- Stockage sécurisé des identifiants professionnels
- Génération de mots de passe uniques pour chaque service
- Partage contrôlé des accès avec un collaborateur
- Accès centralisé aux mots de passe depuis tout appareil

Non destiné à :

- Le stockage de fichiers ou documents (préférer Proton Drive ou KDrive)
- L'échange de mots de passe en clair
- L'usage en dehors du cadre défini par l'entreprise

6. Utilisation en ligne

On privilégiera l'utilisation de Proton Pass via l'interface officielle (web ou extension de navigateur) :

- **Accès universel** : disponible partout avec un simple compte Proton
- **Sécurité renforcée** : chiffrement de bout en bout, Proton n'a pas accès aux données
- **Mises à jour automatiques** : pas besoin de configurer un outil tiers
- **Support simplifié** : assistance Proton disponible en cas de problème

7. Utilisation sur mobile

Il est recommandé d'utiliser l'**application mobile Proton Pass** pour smartphones et tablettes :

- **Synchronisation native** : mots de passe accessibles partout en temps réel
- **Remplissage automatique** : identifiants insérés directement dans les applications mobiles
- **Authentification forte** : prise en charge du Face ID, Touch ID ou code PIN
- **Sécurité optimale** : toutes les données restent chiffrées sur l'appareil et dans le cloud Proton

From:
https://wiki-logeas.fr/certif/ - **dokuwiki-certif**

Permanent link:
https://wiki-logeas.fr/certif/doku.php?id=certif:outils:proton&rev=1755607796

Last update: **2025/08/19 14:49**