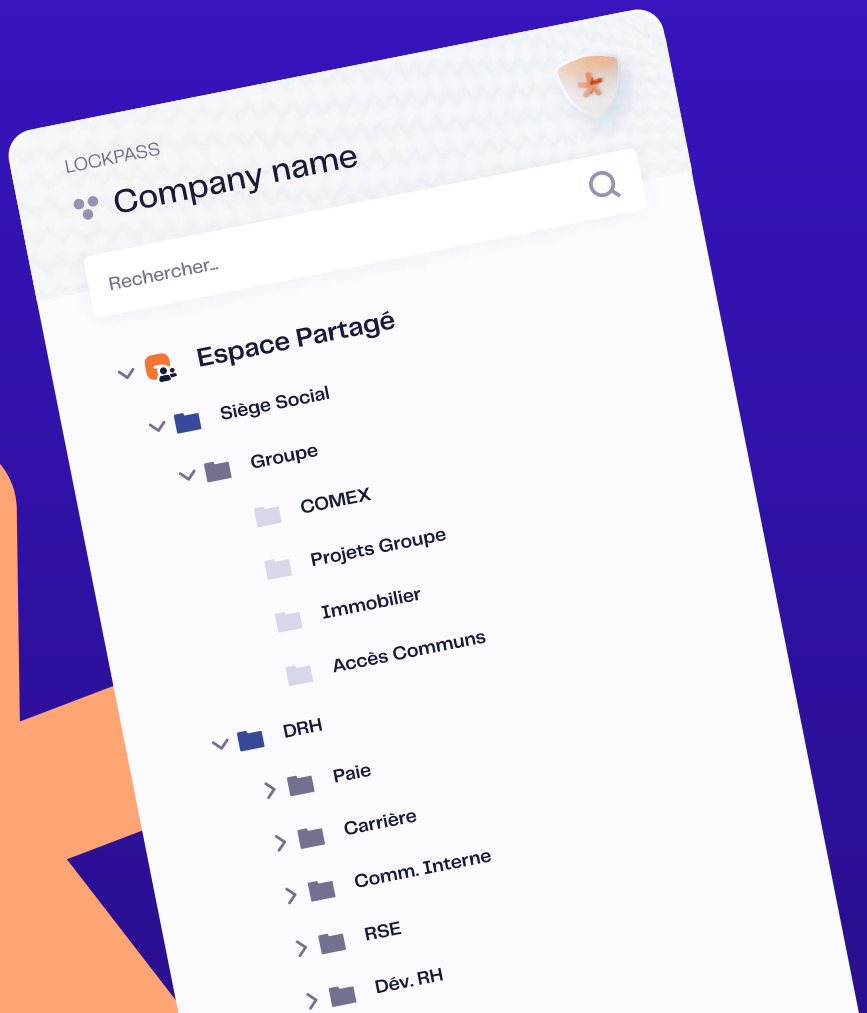
LOCKPASS par LOCKSELF

Mots de passe en entreprise : comment structurer son gestionnaire ?



Sommaire

01

Comprendre l'importance d'une arborescence de mots de passe adaptée

Structurer vos mots de passe : un levier de sécurité et d'efficacité 2

Comment le partage par catégorie optimise la gestion des accès ? 3

02

Facteurs à prendre en compte pour construire l'arborescence de mots de passe de son entreprise

Des besoins différents selon la taille de l'entreprise 5

Votre structure organisationnelle façonne l'arborescence 6

L'impact du secteur d'activité sur votre gestion des mots de passe 7

03

10 modèles d'arborescence de mots de passe adaptés à votre structure

Arborescence par département (ou fonction) 9

Arborescence par site 10

Arborescence par client ou projet 11

Arborescence pour la DSI 12

Meilleures pratiques pour la gestion des mots de passe en entreprise 14

01

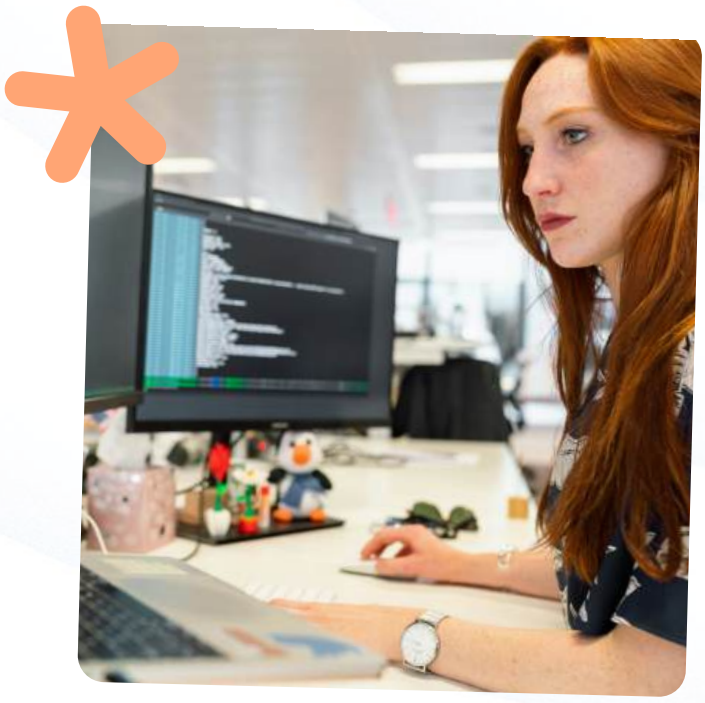
Comprendre l'importance d'une arborescence de mots de passe adaptée

Structurer vos mots de passe : un levier de sécurité et d'efficacité

La gestion des mots de passe en entreprise est un enjeu majeur pour assurer la sécurité des données, notamment avec la multiplication des cybermenaces et des exigences réglementaires.

Une fois votre gestionnaire de mots de passe professionnel choisi pour gérer la sécurité des accès, une autre question se pose : comment organiser vos mots de passe en fonction de la structure de votre entreprise ?

L'arborescence de votre gestionnaire de mots de passe n'est pas seulement une question d'organisation : c'est un véritable système structurant qui façonne la manière dont les utilisateurs interagissent avec les ressources de l'entreprise.



Elle permet de **classifier les mots de passe** selon des critères adaptés à la réalité de votre entreprise : les rôles de chacun (direction, it, finance...), les missions spécifiques (projets, clients, outils), et les niveaux de privilège (administrateurs, utilisateurs standards, ou encore invités).

Cette structuration évite les accès non pertinents, limite les risques de fuites, et **garantit que chaque collaborateur n'a accès qu'aux informations nécessaires à son périmètre.**

Exemple concret : Si tous les collaborateurs ont accès aux identifiants d'un compte bancaire ou d'un serveur critique, ce mot de passe devient hautement exposé. Mais si seuls deux ou trois collaborateurs, bien identifiés, y ont accès via une arborescence structurée, la surface d'exposition est réduite, donc le risque aussi.

Après avoir interrogé de nombreux clients utilisant notre gestionnaire de mots de passe LockPass, nous avons identifié des **modèles d'arborescences** – pour structurer les mots de passe professionnels – qui s'adaptent à chaque organisation, en fonction de leur structure, secteur d'activité et taille d'entreprise.

L'arborescence devient **un outil stratégique**, au croisement de la cybersécurité et de l'efficacité opérationnelle.

Sécurité

La structure de votre arborescence doit pouvoir assurer la sécurité de votre entreprise avec des **droits d'accès granulaires** selon les niveaux hiérarchiques et les besoins métiers.

Accessibilité

Pour que vos équipes puissent **facilement retrouver un mot de passe** en fonction de leur projet, la structure et la solution choisies doivent être fluides et intuitives.

Évolutivité

L'arborescence devra **s'adapter à la croissance de votre entreprise** et à l'apparition de nouveaux changements organisationnels : nouveaux employés, création de départements, expansion géographique ou acquisitions.

Les outils de sécurité comme les **gestionnaires de mots de passe professionnels** permettent de renforcer cette stratégie.

Comment le partage par catégorie optimise la gestion des accès ?

L'une des plus grandes forces de LockPass réside dans son **modèle de partage par catégorie** avec une approche hautement personnalisée pour gérer les accès au sein de l'organisation.

Cette architecture constitue un socle technique pour déployer efficacement les **politiques de sécurité**, en permettant l'application de règles spécifiques en fonction du **niveau de sensibilité des données associées à chaque catégorie**.

Par ailleurs, LockPass répond à la question : **« Qui a accès à quoi, et quand ? »**, et trace toutes les actions effectuées (connexions, accès, modifications, suppressions, ajouts ou partages). Un atout déterminant pour les entreprises engagées dans une démarche de certification, notamment **ISO 27001**, où la traçabilité et la maîtrise des accès sont des critères incontournables.

02

Facteurs à prendre en compte pour construire l'arborescence de mots de passe de son entreprise

Facteurs à prendre en compte pour créer une arborescence de mots de passe (1/2)

Avant d'**adopter un modèle d'arborescence**, il est donc essentiel de bien comprendre les spécificités de votre entreprise : qui doit accèder à quoi, à quelle fréquence, avec quel niveau de sensibilité, et dans quel but. Plusieurs facteurs vont influencer votre choix.

Des besoins différents selon la taille de l'entreprise

Petites entreprises

Pour une petite structure, une arborescence légère, avec peu de niveaux, est souvent la solution la plus efficace. L'objectif : faciliter la gestion des accès avec un bon niveau de sécurité.

Exemple d'arborescence :
📁 Comptabilité → Accès au compte bancaire, logiciel de facturation, Urssaf
📁 Marketing → Accès au CRM, réseaux sociaux, hébergeur web
📁 Clients → Accès aux portails ou outils utilisés pour les clients
📁 Site → Accès partagés avec tous les collaborateurs (code wifi, portail, local....)

Moyennes, grandes entreprises

Dans les structures de taille intermédiaire ou large, les enjeux ne sont plus seulement la simplicité, mais aussi :

- la segmentation par service, entité, filiale, ou équipes réparties par pays,
- la gestion des droits d'accès granulaires,
- et la conformité réglementaire (NIS2, DORA, ISO 27001, etc.).

🔐 Chaque dossier est lié à des groupes d'utilisateurs avec des droits adaptés.

Facteurs à prendre en compte pour créer une arborescence de mots de passe (2/2)

Votre structure organisationnelle façonne l'arborescence

La manière dont votre entreprise est structurée détermine en grande partie la façon dont vous devez organiser vos mots de passe et gérer les accès. **L'arborescence doit refléter la réalité opérationnelle**. On distingue généralement deux types de structures : centralisée et décentralisée, avec parfois des modèles hybrides.

Structure centralisée

Le contrôle des accès est concentré au niveau de la direction ou d'un service unique (souvent la DSI). **Il décide qui a accès à quoi**, selon les rôles et responsabilités des collaborateurs.

Les équipes ont peu d'autonomie dans la création ou le partage de nouveaux accès.

🎯 **Objectifs** : maîtrise, cohérence, conformité, uniformité des règles de sécurité

⚠️ **Point de vigilance** :
Moins de réactivité sur le terrain

🗂️ **Exemple d'arborescence adaptée** :

- Groupe
  - Direction
  - IT
  - RH
  - Finance
  - Commercial

Structure décentralisée

Chaque entité (filiale, département, pays...) gère ses propres accès. Les règles de sécurité sont déclinées localement, en respectant une politique globale. Les administrateurs locaux ont un pouvoir décisionnel : création, partage, modification, attribution d'accès.

🎯 **Objectifs** : agilité, responsabilisation, autonomie locale, réactivité opérationnelle.

⚠️ **Point de vigilance** :
Risque d'hétérogénéité des pratiques

🗂️ **Exemple d'arborescence adaptée** :

- Groupe
  - Filiale France
    - RH
    - IT
    - Marketing
  - Filiale Canada
    - RH
    - Juridique
  - Filiale Espagne
    - Technique
    - Commercial

L'impact du secteur d'activité sur votre gestion des mots de passe

🏥 Secteurs réglementés (finance, santé...)

Les entreprises qui traitent des informations sensibles – telles que des **données personnelles**, des **informations financières** ou des **données médicales** – sont soumises à une surveillance des autorités de régulation, qui imposent des **normes de sécurité**.

Par conséquent, la gestion des accès aux systèmes d'information doit être pensée en fonction des responsabilités spécifiques de chaque collaborateur, afin d'éviter que des personnes non autorisées aient accès à des informations sensibles.

💼 Secteurs de services (ESN, expertise comptable)

Les entreprises de services gèrent des projets pour des clients divers, ce qui rend la gestion des accès particulièrement complexe. Elles doivent jongler avec des **équipes multidisciplinaires** souvent mobilisées sur plusieurs projets simultanément.

De plus, les **accès aux ressources et aux informations sont souvent temporaires ou limités** en fonction des missions. L'un des principaux enjeux est de trouver un équilibre entre protéger les informations sensibles relatives à chaque client et faciliter l'accès aux équipes projet.

🌍 Secteurs avec une structure géographique (logistique, hôtellerie, retail)

Ces secteurs peuvent avoir un **réseau d'établissements répartis dans plusieurs villes, régions ou pays** (boutiques, usines, bureaux, entrepôts) avec des équipes locales ayant des besoins d'accès distincts.

L'arborescence est souvent organisée pour donner un **accès localisé et spécifique aux équipes** travaillant dans ces zones (par exemple, aux outils de gestion des stocks, aux systèmes de caisse) mais aussi de garantir que les employés n'aient pas accès à des informations concernant d'autres sites ou filiales qui ne relèvent pas de leur responsabilité.

03

10 modèles d'arborescence de mots de passe adaptés à votre structure

Ces templates sont pensés pour s'adapter à la réalité de la gestion des accès en entreprise Ils sont faits pour être ajustés en fonction des spécificités de votre structure, de vos équipes, de vos projets et de votre secteur.

Chaque modèle peut être affiné pour répondre à vos besoins spécifiques.

10 modèles d'arborescence de mots de passe adaptés à votre structure

Arborescence par fonction ou département

Le modèle le plus simple à adopter

Ce modèle est idéal pour les **entreprises de taille petite à moyenne** où la hiérarchie est relativement légère. Il s'agit d'une **structure hiérarchique qui permet une organisation par département**.

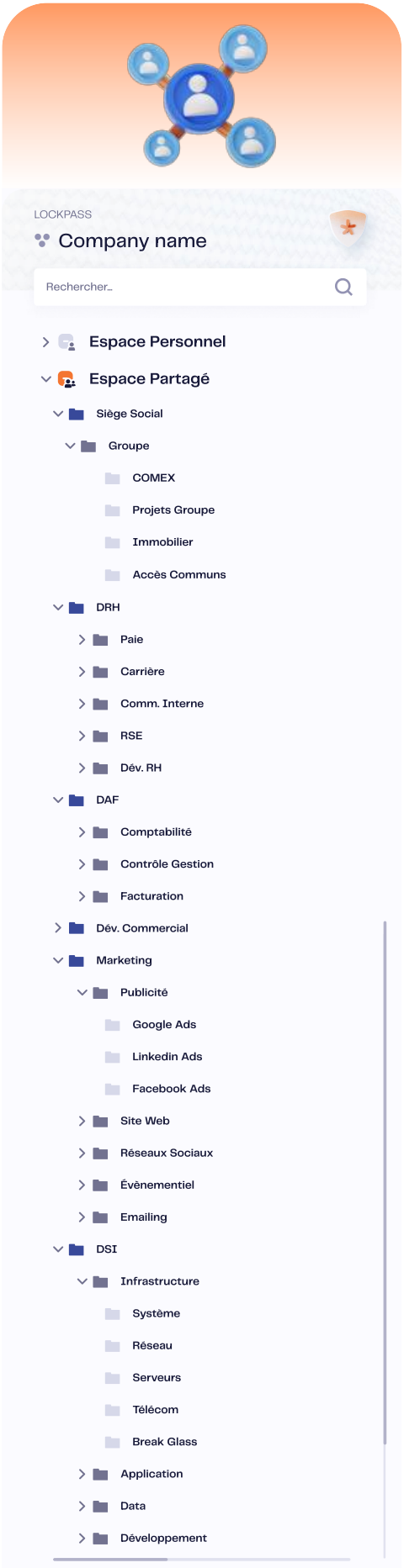
- **Niveau 1** : Regroupe les dirigeants et les équipes stratégiques (siège social, comex, direction générale), responsables de la gestion globale de l'entreprise.

- **Niveau 2** : Accès par départements fonctionnels : Ressources Humaines (RH), Commercial (Sales), Informatique (IT), Marketing, etc. avec ses propres droits d'accès à des ressources spécifiques.

- **Niveau 3** : Dans les départements, l'accès est affiné en fonction des pôles spécifiques ou des équipes qui travaillent sur des projets distincts. Par exemple, au sein du département RH, on peut avoir des sous-niveaux comme Recrutement, Paie, Formation, etc.

- **Accès restreint** par outils ou données spécifiques (en fonction du niveau d'accès utilisateur : Administrateurs (accès complet à tous les outils et données) / Utilisateurs standard (accès limité selon les outils et données nécessaires à leur fonction).

Télécharger le template



Arborescence par site

Pour les entreprises avec des opérations nationales ou internationales

Pour les entreprises opérant sur plusieurs sites, régions ou pays, il est souvent préférable d'opter pour une **structure géographique**. Cela permet de gérer l'accès en fonction des zones géographiques, en garantissant la sécurité globale des données et des systèmes.

- **Niveau 1** : Accès groupe et équipes stratégiques de l'entreprise (siège social, directions et sous-directions)

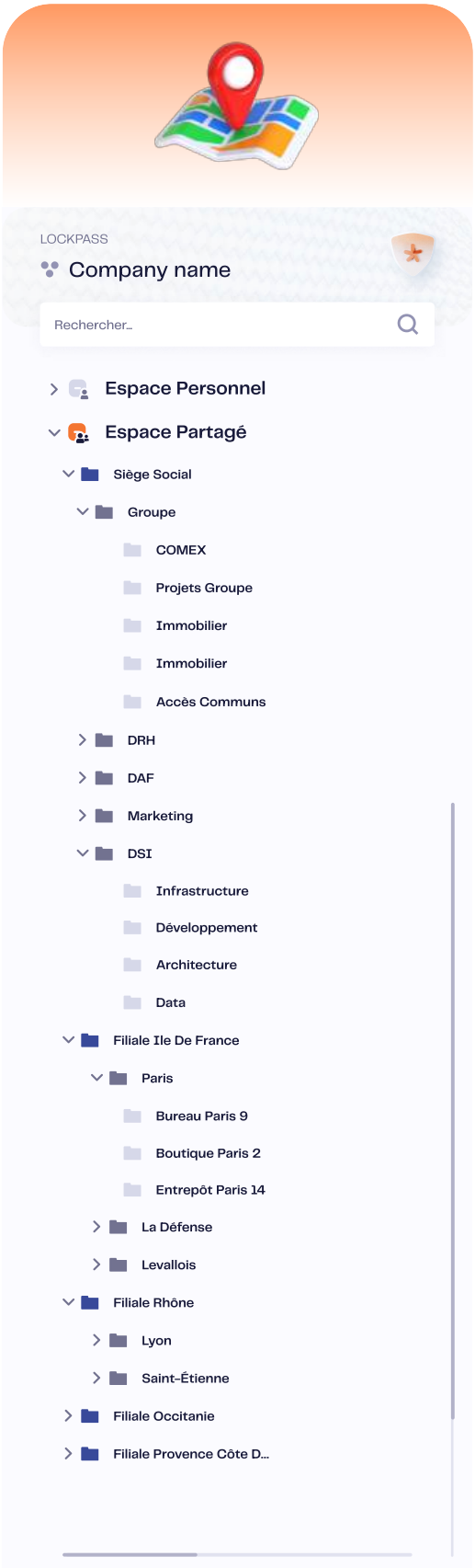
- **Niveau 2** : Accès par filiale régionale (pays, région, ville).

Niveau optionnel : Accès par type de site. Ce niveau permet de spécialiser davantage l'accès en fonction du site (Bureau, Usine, Entrepôt, Boutique)

- **Niveau 3** : Accès par pôle ou par équipe. Ce niveau affine encore les droits d'accès en fonction des équipes qui exercent des missions spécifiques dans chaque filiale. Par exemple, dans une filiale régionale, il peut y avoir des équipes dédiées à la logistique, au service client, à la comptabilité, ou à la production.

- **Accès restreint** par outils ou données spécifiques en fonction du niveau d'accès utilisateur : Admin, Utilisateur standard...).

–> **Modèle déclinable** pour donner de l'autonomie en local. Les responsables de chaque filiale peuvent gérer les accès des employés et les catégories de partage au niveau local, en suivant les lignes directrices et la politique de sécurité définie par le groupe (**structure décentralisée**).



Télécharger le template

Arborescence par client ou projet

Le modèle idéal pour les ESN, cabinets comptables, agences ou consultants.

Dans les structures où les équipes gèrent plusieurs comptes clients ou projets en simultané (comme les **ESN**, les **cabinets d'expertise comptable**, les **agences** ou les **freelances**), une **arborescence organisée par client ou par projet** permet une gestion cloisonnée et sécurisée des accès. Chaque mot de passe ou ressource est rattaché à un périmètre bien défini.

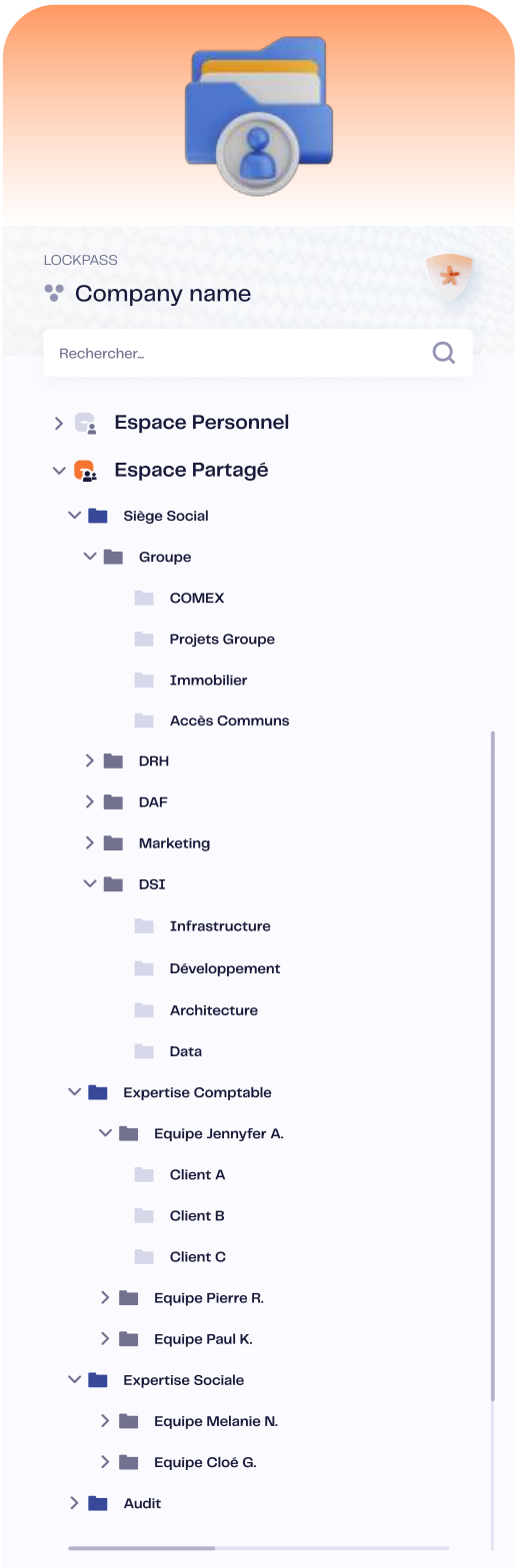
- **Niveau 1** : Accès groupe. Inclut le siège social, la direction générale et les services transverses (RH, finance, juridique)

Niveau optionnel : Accès par filiale régionale (pays, région, ville). Pertinent pour les cabinets ou ESN présents dans plusieurs régions ou pays pour segmenter les accès selon l'organisation géographique.

- **Niveau 2** : Accès communs aux outils partagés pour tous les clients ou projets : CRM, logiciels métiers communs, documentation interne, templates, etc. Idéal pour les équipes transverses.

- **Niveau 3** : Accès restreint aux équipes concernées : consultants affectés, gestionnaires de compte, collaborateurs dédiés. Chaque client ou projet a son propre espace dédié.

- **Accès restreint** par outils ou données spécifiques aux clients ou aux projets (en fonction du niveau d'accès utilisateur : Admin, Utilisateur standard, Modérateur...).



Télécharger le template

💡Retrouvez nos templates Spécial Experts-Comptables et Spécial ESN à la page 13.

Arborescence pour la DSI

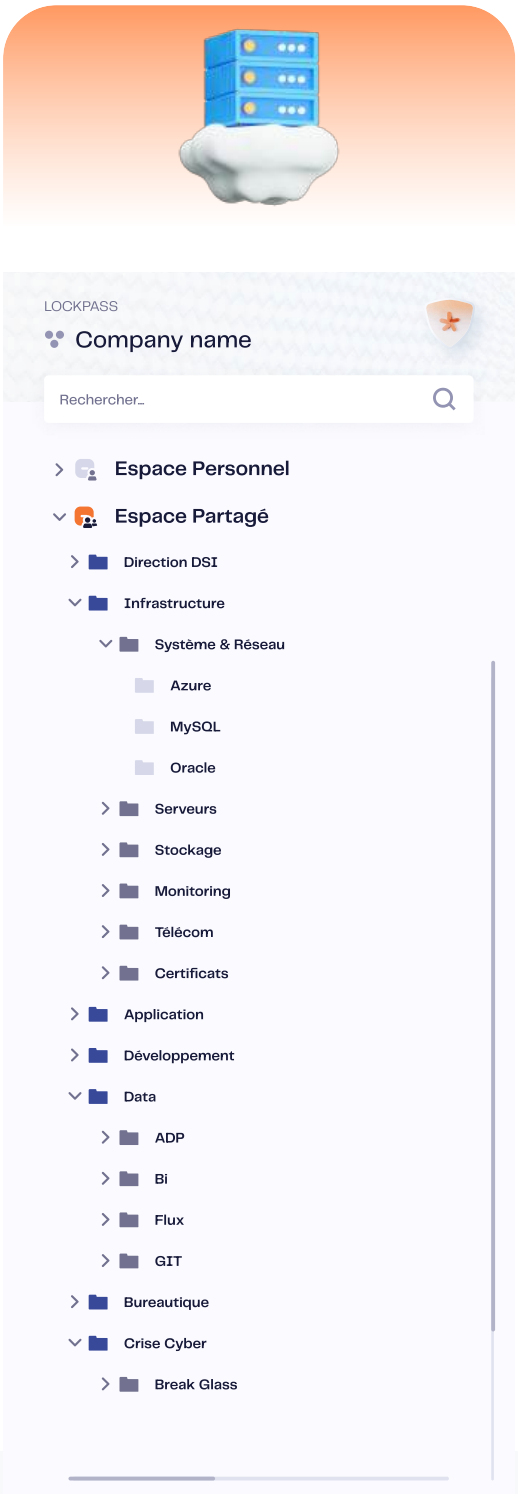
Pour une gestion plus techique

Pour les entreprises ayant une **DSI** (Direction des Systèmes d'Information) ou un **département IT**, une arborescence dédiée à la gestion des mots de passe des infrastructures et applications peut être appropriée.

- **Niveau 1** : Accès communs du SI. Ce niveau regroupe les accès généraux au système d'information (SI) de l'entreprise.
- **Niveau 2** : Accès par environnement/équipe. À ce niveau, les accès sont divisés par environnements spécifiques (Applications, Infrastructures, Architecture, Sécurité, Centre de service...)
- **Niveau 3** : Accès par sous-environnement. Ce niveau affine davantage les accès en fonction des sous-domaines au sein de chaque environnement (Serveurs, Cybersécurité, Réseau...)

-> **Modèle déclinable avec une DSI externalisée** par comptes clients

- **Niveau 4** : Accès par comptes clients
- **Accès restreint** par outils ou données spécifiques (en fonction du niveau d'accès utilisateur : Admin, Utilisateur standard...).



Télécharger le template

💡**Conseil pratique : N'oubliez pas les "break glass account"** (ou "compte de bris de glace"). En cas de cyberattaque ou de perte d'accès, ces comptes d'urgence permettent de reprendre le contrôle sans exposer le système à de nouveaux risques.

La bibliothèque d'arborescence de catégories de mots de passe LockSelf

Général

- Par département — Télécharger le template
- Par zone géographique — Télécharger le template
- Par client — Télécharger le template
- Pour la DSI — Télécharger le template

Spécial Experts-Comptables

- Par expertise — Télécharger le template
- Par clients — Télécharger le template
- Pour les cabinets multi-sites — Télécharger le template

Spécial ESN

- Par expertise — Télécharger le template
- Par clients — Télécharger le template
- Pour les ESN multi-sites — Télécharger le template

Meilleures pratiques pour la gestion des mots de passe en entreprise

Une fois l'arborescence mise en place, il est essentiel de suivre quelques bonnes pratiques pour optimiser la gestion des mots de passe.

📌 Nomenclature claire

- Une nomenclature standardisée pour faciliter la lecture, la recherche et l'usage quotidien :
  - Privilégiez des noms explicites
  - Évitez les abréviations internes peu claires ou trop génériques
  - Intégrez les mots-clés pour faciliter la recherche dans l'outil.

🎯 **Objectif : une arborescence compréhensible et facilite la recherche !**

🛡️ Accès au moindre privilège

- Adoptez une approche au "moindre privilège" : chacun accède uniquement aux mots de passe dont il a besoin pour travailler, rien de plus.

Avec LockSelf, cette gestion peut être automatisée grâce à l'interconnexion avec votre annuaire d'entreprise : les groupes et rôles définis dans l'annuaire sont synchronisés automatiquement dans le gestionnaire de mots de passe.

🔄 Révisions régulières

- Planifiez un audit pour vous assurer que l'arborescence reste adaptée aux besoins de l'entreprise (nouveaux projets, changements d'équipe, fusions de services).

💡 Conseil pratique : Les espaces personnels

Dans le cadre du respect du RGPD, les administrateurs n'ont pas accès aux **espaces personnels** des collaborateurs. Pour éviter que ces derniers y enregistrent des mots de passe à usage privé, **certaines entreprises choisissent de désactiver ces espaces**.

À la place, elles mettent en place des **dossiers individuels** : des espaces sécurisés et contrôlés par les administrateurs, attribués à chaque utilisateur. Ces dossiers permettent aux collaborateurs de stocker en toute sécurité leurs **identifiants professionnels personnels**, c'est-à-dire les accès liés à des outils ou ressources internes, mais **spécifiques à chaque utilisateur**, qui respectent la politique de sécurité globale de l'entreprise.

LockPass

Le gestionnaire centralisé de mots de passe qui s'intègre dans les habitudes de travail de vos collaborateurs et permet de reprendre le contôle sur le "Qui a accès à quoi".

Testez Lockself – 14 jours d'essai gratuit

Plus de **3 000 entreprises** nous font confiance et renforcent leur cybersécurité avec LockSelf.

france•tv · bouygues TELECOM · Primobox · BNP PARIBAS REAL ESTATE

SNCF · Eau du Ponant Société Publique Locale · ASSISTANCE PUBLIQUE HÔPITAUX DE PARIS · EY Building a better working world

LOCKSELF