# Clarté sécurité

**PILIER #3**

**5 réflexes pour éviter la catastrophe et dormir (vraiment) tranquille**

Un guide Arkonium – Clarté, Structuration, Scalabilité

# POURQUOI LA CLARTÉ SUR LA SÉCURITÉ CHANGE TOUT

Quand la sécurité est floue ou reléguée à plus tard, chaque étape du projet devient un pari risqué :
une mauvaise gestion des accès, une sauvegarde absente, une fuite de données…

## 3 bénéfices concrets si tu t'y prends tôt :

**Tu dors tranquille** : tu sais que tes données sont protégées, tes accès maîtrisés, et que tu peux restaurer en cas de pépin.

**Tu inspires confiance** : tes clients, partenaires ou équipes voient que tu prends leur sécurité au sérieux.

**Tu évites la double peine** : anticiper, c'est gagner du temps, de l'argent, et préserver la réputation de ton projet.

**La sécurité, ce n'est pas un bonus :**
**c'est ta vraie bouée de sauvetage.**

***"La sécurité, c'est comme une fondation invisible :***
***personne ne la voit… jusqu'au jour où elle sauve tout."***

# DÉFINIR LES ACCÈS : ÉVITER LES ERREURS HUMAINES

*Donner le même accès à tout le monde, c'est ouvrir la porte à toutes les erreurs : suppression accidentelle, fuite de données, ou mauvaise manipulation. Une gestion par rôles limite l'impact d'une faute ou d'un piratage.*

Prends le temps de lister tous les rôles présents sur ton projet.
Pour chaque rôle, demande-toi :
– De quels accès a-t-il vraiment besoin ?
– Y a-t-il un droit trop large ou inutile à retirer ?

Vérifie que personne n'a plus de droits "par défaut" que nécessaire.

- [ ] Les rôles sont clairement définis
- [ ] Chaque rôle a des droits limités
- [ ] Un audit d'accès est prévu régulièrement

Quels accès ou rôles dois-tu revoir en priorité ?

_____

_____

_____

# CHIFFRER LES DONNÉES SENSIBLES : PROTÉGER TON ACTIF

*Stocker des mots de passe ou des infos critiques en clair, c'est s'exposer à une fuite massive en cas de faille. Le chiffrement protège même si un attaquant accède à la base.*

***"Ce qui n'est pas chiffré est déjà public."***

Fais le point sur toutes les données sensibles de ton projet (mots de passe, emails, paiements...).

Pour chacune, vérifie si elle est chiffrée ou protégée côté serveur.
Teste la récupération ou la modification d'une donnée pour t'assurer du bon fonctionnement.

- [ ] Les mots de passe ne sont jamais stockés en clair
- [ ] Les données critiques sont chiffrées ou anonymisées
- [ ] Un process de vérification régulière existe

Quelle donnée sensible dois-tu mieux protéger aujourd'hui ?

_____

_____

_____

# LIMITER LES DROITS : RÉDUIRE LA SURFACE D'ATTAQUE

*Chaque membre ou service doit avoir juste ce qu'il faut pour travailler ni plus, ni moins. Accorder trop de droits multiplie la surface d'attaque et les erreurs humaines.*

Liste tous les accès accordés à chaque personne ou service (développeur, prestataire, script…).

Pour chaque accès, pose-toi la question :
– Cet accès est-il vraiment nécessaire à sa mission ?
– Pourrais-tu le limiter à la lecture seule ou à une durée précise ?

- [ ] Aucun compte "admin" n'est utilisé par défaut
- [ ] Les accès "lecture seule" sont privilégiés
- [ ] Les accès sont limités dans le temps ou surveillés

Quel accès pourrais-tu réduire ou supprimer dès cette semaine ?

_____

_____

_____

# RÉVOQUER LES ACCÈS SANS DÉLAI : FERMER LES PORTES

*Un collaborateur (dev, prestataire...) qui quitte l'équipe doit immédiatement perdre ses accès. Sinon, tu gardes une porte ouverte vers tes données et ton infra, sans surveillance.*

**"Un accès oublié, c'est une brèche assurée."**

Prends le temps de simuler le départ d'un membre de l'équipe ou d'un prestataire.
Liste toutes les actions à effectuer pour couper ses accès (comptes, API, outils).
Teste la suppression d'un compte pour vérifier qu'il ne reste aucune "porte ouverte".

- [ ] Une procédure de départ existe et est connue
- [ ] Les accès sont coupés dès l'annonce du départ
- [ ] Un contrôle post-départ est fait (logs, audit)

Quels accès ou comptes dois-tu penser à révoquer en priorité ?

_____

_____

_____

# TESTER TES SAUVEGARDES : ASSURER LA REPRISE RAPIDE

*Sauvegarder ne suffit pas. Ce qui compte, c'est pouvoir restaurer.*
*Et personne n'a envie de découvrir que "la sauvegarde ne fonctionne pas" après une panne.*

Teste une restauration complète, sur un environnement isolé.
Observe le temps nécessaire, les éventuelles erreurs, et documente la procédure.

- [ ] J'ai une procédure de restauration testée récemment
- [ ] J'ai simulé une perte de données et pu revenir à un état stable
- [ ] Je sais combien de temps cela prend, et qui peut l'exécuter

Quelle est la date de ma prochaine vérification de restauration ?

_____

_____

_____

# AUTO-ÉVALUATION : OÙ EN ES-TU SUR LA CLARTÉ SÉCURITÉ ?

Réponds honnêtement à ces 5 questions.
Coche une case par question :

As-tu une liste claire de tous les accès (comptes, API, prestataires) à ton projet ?

☐ Oui ☐ Partiellement ☐ Non

Les droits de chaque rôle sont-ils limités au strict nécessaire (“least privilege”) ?

☐ Oui ☐ Partiellement ☐ Non

Toutes les données sensibles sont-elles chiffrées ou protégées (mots de passe, infos clients, etc.) ?

☐ Oui ☐ Partiellement ☐ Non

Un départ d’équipe déclenche-t-il automatiquement une révocation complète des accès ?

☐ Oui ☐ Partiellement ☐ Non

Les accès et droits sont-ils revus et mis à jour régulièrement (audit ou contrôle trimestriel) ?

☐ Oui ☐ Partiellement ☐ Non

**4-5 “Oui”** : continue, tu as de la clarté produit !
**<4 “Oui”** : reprends une étape, ou demande de l’aide si besoin.

**Chaque “Non” est une opportunité d’améliorer la sécurité de ton projet. Relis les étapes précédentes ou demande un diagnostic externe si besoin : la prévention vaut mieux que la réparation !**

# CHECKLIST : LES ÉTAPES CLÉS À VALIDER

Coche chaque étape lorsque tu l'as validée.
Reviens sur cette liste à chaque nouvelle version, ou dès que tu ressens un doute sur la clarté technique de ton projet.

- [ ] Les rôles et accès sont définis et documentés
- [ ] Les droits de chaque rôle ont été revus et limités au nécessaire
- [ ] Les accès critiques sont audités au moins une fois par trimestre
- [ ] Les données sensibles (mots de passe, infos clients) sont chiffrées
- [ ] Un process de révocation des accès existe et a été testé récemment
- [ ] Tous les accès d'ex-membres ou prestataires ont été supprimés
- [ ] Un inventaire de tous les comptes et API existe et est à jour
- [ ] Les accès admin sont réservés à un minimum de personnes
- [ ] Un contrôle post-départ est effectué (logs, audit, vérification)

**Seule l'action fait progresser la sécurité de ton projet.**
**Un petit pas chaque semaine = des risques divisés par dix à long terme.**

# À ÉVITER ABSOLUMENT !

Même les meilleurs projets se plantent sur ces points.
Anticipe, et tu éviteras beaucoup de temps (et d'argent) perdus !

### Oublier de révoquer les accès après un départ

Résultat : Un ex-collaborateur ou prestataire peut encore accéder, modifier ou supprimer tes données, parfois des mois plus tard.

### Stocker des données sensibles en clair

Résultat : Une fuite, un piratage ou une mauvaise manipulation, et toutes tes infos critiques (mots de passe, emails…) sont lisibles.

### Donner des droits admin "par défaut"

Résultat : Une erreur ou un compte compromis, et tout le projet peut être mis à terre en une minute.

### Penses que "ce n'est pas pour moi, je suis trop petit"

Résultat : Les PME, side-projects et SaaS early-stage sont justement les cibles préférées : automatisées, rapides à attaquer, peu protégées.

Si tu évites ces pièges, tu fais déjà partie des 20 % qui construisent sur du solide.

Relis ce livret à chaque nouvelle embauche, changement d'équipe, ou avant de lancer une nouvelle fonctionnalité critique.

# Envie d’aller plus loin ?

Besoin d’un regard neuf sur ton architecture,
d’un coup de pouce pour organiser tes environnements ou automatiser tes tests ?
Profite d’un échange gratuit pour faire le point et repartir avec des actions concrètes.

**Réserve ton créneau ici :** **30 minutes de call gratuit**

**Ou contacte-moi par email :** arkonium.contact@gmail.com

Je suis Arnaud, fondateur d’Arkonium.

J’accompagne les porteurs de projets et équipes tech à structurer, sécuriser et faire grandir leurs idées sans bullshit.

Passionné par la clarté, la structuration et la transmission.

Ma mission : t’aider à transformer le flou en projet solide et pérenne

Merci d’avoir lu ce mini-guide
et bravo pour ton engagement à bâtir sur de bonnes bases !

**Structurer. Sécuriser. Scaler.**