AEGIREN · RESSOURCE GRATUITE

Sécuriser Microsoft 365 dans une PME

15 contrôles à vérifier vous-même — sans inscription, sans e-mail à laisser

Aegiren — sécurité des accès et de l'identité **Version** v1.0 **Mise à jour** 16 juillet 2026 **Diffusion** libre — partagez-la

À qui elle s'adresse

Vous dirigez une structure de 5 à 80 personnes sous Microsoft 365. Vous n'avez pas d'informaticien à demeure, ou une seule personne qui fait déjà tout. Vous vous demandez si vos comptes sont correctement protégés, sans savoir par quel bout regarder.

Cette checklist répond à cette question. Quinze points, chacun avec **l'endroit exact où aller voir** dans vos portails d'administration, ce qui distingue une situation saine d'une situation à corriger, et pourquoi cela compte.

Ce dont vous avez besoin : un compte administrateur, ou un compte disposant du rôle *Lecteur général* (`Global Reader`), qui permet de tout consulter sans rien modifier. **Comptez une heure.** Vous ne modifierez rien en suivant ce document : il ne fait que regarder.

Ce que cette checklist n'est pas : un audit. Elle couvre l'essentiel de ce qui provoque des incidents dans les petites structures, pas la totalité des réglages de Microsoft 365. Elle ne remplace ni un regard indépendant, ni un plan d'action priorisé.

Pourquoi les accès, et pas autre chose

La grande majorité des compromissions de petites entreprises ne commencent pas par une faille technique exotique. Elles commencent par **un compte** : un mot de passe réutilisé, un message d'hameçonnage crédible, un compte d'ancien salarié jamais désactivé, un administrateur sans double authentification. L'attaquant n'entre pas par effraction, il se connecte.

C'est une bonne nouvelle : l'essentiel des mesures ci-dessous sont **gratuites**, incluses dans votre abonnement, et se règlent en quelques heures.

Comment noter

Pour chaque point, attribuez-vous une couleur.

- **Vert** — la situation décrite comme saine est vérifiée.
- **Orange** — c'est partiellement en place, ou vous n'êtes pas certain.
- **Rouge** — la situation décrite comme à risque correspond à la vôtre.

Un rouge n'est pas une catastrophe, c'est une tâche. Ce qui compte, c'est de savoir lesquels vous avez.

Note sur les portails. Microsoft renomme régulièrement ses écrans. Les chemins ci-dessous sont ceux en vigueur ; si un libellé a changé, la fonction se retrouve en recherchant son nom dans la barre du portail concerné.

`entra.microsoft.com` — centre d'administration Microsoft Entra (identités, accès)
`admin.microsoft.com` — centre d'administration Microsoft 365 (utilisateurs, licences)
`security.microsoft.com` — portail Microsoft Defender (sécurité, messagerie)
`purview.microsoft.com` — portail Microsoft Purview (audit, conformité)

---

1. Le Secure Score

La question : Microsoft calcule en permanence une note de sécurité pour votre environnement. Quelle est la vôtre, et l'avez-vous déjà regardée ?

Où vérifier : portail Defender → *Gestion de l'exposition* → *Degré de sécurisation* (Secure Score).

Pourquoi ça compte : c'est le seul chiffre que Microsoft vous donne gratuitement sur votre propre posture, assorti de recommandations classées par gain. Un score bas signale que les réglages par défaut n'ont jamais été resserrés — or les réglages par défaut privilégient la facilité d'usage, pas la sécurité.

VERT Vous connaissez votre score, vous le suivez, et les recommandations à fort gain ont été traitées.
ROUGE Vous découvrez l'écran, ou le score est inférieur à 50 %.

---

2. Les comptes dormants

La question : combien de comptes actifs n'ont pas servi depuis plus de quatre-vingt-dix jours ?

Où vérifier : centre Entra → *Identité* → *Utilisateurs* → *Tous les utilisateurs*, en affichant la colonne de dernière connexion. L'historique complet des connexions nécessite une licence Entra ID P1 ; à défaut, recoupez avec votre liste de personnes réellement présentes.

Pourquoi ça compte : un compte inutilisé reste une porte ouverte, et c'est souvent celle qui a le mot de passe le plus ancien et le moins de protections. Le compte d'un salarié parti il y a deux ans n'alertera personne s'il est utilisé un dimanche soir. Vous payez également une licence pour chacun.

VERT Aucun compte actif sans connexion depuis quatre-vingt-dix jours, et vous faites une revue trimestrielle.
ROUGE Vous trouvez des comptes de personnes qui ont quitté l'entreprise, encore actifs.

---

3. Les administrateurs

La question : combien de personnes sont *Administrateur général* de votre environnement ?

Où vérifier : centre Entra → *Identité* → *Rôles et administrateurs* → *Administrateur général*.

Pourquoi ça compte : l'administrateur général peut tout faire — lire n'importe quelle boîte, réinitialiser n'importe quel mot de passe, supprimer n'importe quelle donnée. Chaque compte de ce

type est une clé du royaume. Il est fréquent d'en découvrir six ou huit dans une PME de quarante personnes, souvent parce que le prestataire précédent n'a jamais été retiré.

VERT Deux administrateurs généraux au maximum, dont un compte de secours peu utilisé, et les administrateurs disposent d'un compte dédié séparé de leur compte de messagerie quotidien.
ROUGE Plus de trois administrateurs généraux, ou des comptes d'administration servant aussi à lire les e-mails et naviguer sur internet.

---

4. La double authentification

La question : la double authentification est-elle imposée à **tout le monde**, et par quel mécanisme ?

Où vérifier : centre Entra → *Protection* → *Méthodes d'authentification*, puis l'onglet d'activité d'inscription. Vérifiez aussi si les *Paramètres de sécurité par défaut* sont activés (Entra → *Identité* → *Vue d'ensemble* → *Propriétés*).

Pourquoi ça compte : c'est la mesure au meilleur rapport effort/protection qui existe. Sans second facteur, un seul mot de passe volé suffit à prendre le contrôle d'une boîte — celle du dirigeant, celle de la comptabilité. Attention au piège fréquent : la double authentification activée « pour les administrateurs seulement », ou proposée sans être obligatoire.

Toutes les méthodes ne se valent pas : l'application d'authentification vaut mieux que le SMS, qui reste vulnérable au détournement de ligne.

VERT Cent pour cent des comptes, administrateurs en premier, avec l'application d'authentification comme méthode principale.
ROUGE Des comptes sans double authentification, ou une activation laissée au choix de chacun.

---

5. Les règles d'accès conditionnel

La question : existe-t-il des règles qui décident d'autoriser ou de bloquer une connexion selon son contexte ?

Où vérifier : centre Entra → *Protection* → *Accès conditionnel* → *Stratégies*. Nécessite une licence Entra ID P1, incluse dans Business Premium.

Pourquoi ça compte : sans ces règles, toutes les connexions sont traitées de la même façon — celle de votre comptable depuis le bureau comme celle d'un inconnu depuis l'autre bout du monde à trois heures du matin. Un socle de base tient en quatre règles : double authentification pour tous, blocage des anciens protocoles, protection renforcée des administrateurs, et réaction aux connexions jugées risquées.

VERT Un socle de règles est en place, testé, et un compte de secours en est exclu pour éviter de se verrouiller dehors.
ROUGE Aucune règle, ou uniquement les *Paramètres de sécurité par défaut* alors que vous disposez d'une licence permettant mieux.

---

6. L'authentification héritée

La question : les anciens protocoles de messagerie sont-ils encore autorisés à se connecter ?

Où vérifier : centre Entra → *Surveillance* → *Journaux de connexion*, en filtrant sur l'application cliente pour ne garder que les clients d'authentification héritée. Regardez les trente derniers jours.

Pourquoi ça compte : ces vieux protocoles — POP, IMAP, SMTP en authentification simple — **ne savent pas gérer la double authentification**. Tant qu'ils sont ouverts, ils constituent un contournement de toutes vos protections, et ce sont eux que visent en priorité les attaques automatisées par essai de mots de passe.

VERT Aucune connexion héritée sur trente jours, et un blocage explicite en place.
ROUGE Des connexions héritées apparaissent, ou vous n'avez jamais vérifié.

---

7. Les transferts de messagerie et l'anti-hameçonnage

La question : un utilisateur peut-il faire suivre automatiquement tous ses e-mails vers une adresse extérieure ? Et vos protections anti-hameçonnage sont-elles réglées ?

Où vérifier : portail Defender → *Stratégies et règles* → *Stratégies contre les menaces* → *Anti-courrier indésirable sortant* pour le transfert automatique, et *Anti-hameçonnage* pour la protection. Vérifiez aussi les règles de boîte aux lettres dans le centre d'administration Exchange.

Pourquoi ça compte : la règle de transfert discrète est **la signature classique d'une boîte compromise**. L'attaquant qui prend la main sur une messagerie crée une règle qui lui expédie une copie de tout, puis se retire : il continue de tout lire sans jamais se reconnecter. C'est le mécanisme central de la fraude au virement.

VERT Le transfert automatique vers l'extérieur est bloqué, et la protection anti-hameçonnage est renforcée pour les dirigeants et la comptabilité.
ROUGE Le transfert externe est autorisé sans contrôle, ou vous découvrez des règles de transfert que personne n'a créées sciemment.

---

8. Le partage externe des fichiers

La question : qui peut recevoir un lien vers vos documents, et ces liens expirent-ils ?

Où vérifier : centre d'administration SharePoint → *Stratégies* → *Partage*.

Pourquoi ça compte : le réglage le plus permissif produit des liens accessibles **à toute personne qui les possède, sans aucune authentification**. Un lien de ce type transféré, retrouvé dans une boîte compromise ou simplement oublié dans un vieil e-mail reste valable indéfiniment. Beaucoup d'organisations découvrent des centaines de liens anonymes actifs dont plus personne ne connaît l'existence.

VERT Le partage est limité aux personnes authentifiées, les liens ont une date d'expiration, et les partages sensibles ont été revus.
ROUGE Le partage « tout le monde » est autorisé, sans expiration.

---

9. Le départ d'un collaborateur

La question : quand quelqu'un quitte l'entreprise, que se passe-t-il exactement, et qui le fait ?

Où vérifier : nulle part — c'est le seul point de cette liste qui ne se lit pas sur un écran. Prenez la dernière personne partie et vérifiez son compte.

Pourquoi ça compte : entre le dernier jour et la désactivation effective, il s'écoule souvent des semaines. Or désactiver un compte ne suffit pas : tant que les **sessions ouvertes** ne sont pas révoquées, l'accès depuis un téléphone personnel déjà connecté peut se poursuivre. Une procédure écrite couvre le blocage de la connexion, la révocation des sessions, la réinitialisation du mot de passe, le devenir de la boîte et le transfert des documents.

VERT Une procédure écrite existe, elle est appliquée le jour du départ, et le compte de la dernière personne partie est correctement traité.
ROUGE Rien d'écrit, ou vous trouvez des comptes d'anciens collaborateurs encore actifs.

---

10. Le journal d'audit

La question : le journal d'audit unifié est-il activé, et depuis combien de temps conservez-vous les traces ?

Où vérifier : portail Purview → *Audit*. Si l'écran propose de démarrer l'enregistrement, c'est qu'il est éteint.

Pourquoi ça compte : c'est votre boîte noire. Sans elle, en cas d'incident, il est **impossible** de savoir quels fichiers ont été consultés, quels e-mails ont été lus, ni depuis quand. Vous ne pouvez ni mesurer les dégâts, ni répondre à votre assureur, ni notifier correctement une violation de données. L'activation prend quelques minutes, elle est gratuite, et elle n'a aucun impact sur les utilisateurs — mais elle n'est pas rétroactive : ce qui n'a pas été enregistré est perdu.

VERT Le journal est actif, et vous connaissez la durée de conservation associée à vos licences.
ROUGE Le journal est désactivé, ou vous l'ignorez.

---

11. Les mots de passe et leur réinitialisation

La question : un utilisateur peut-il réinitialiser son mot de passe seul et de façon sécurisée ? Et imposez-vous encore un changement périodique ?

Où vérifier : centre Entra → *Protection* → *Réinitialisation du mot de passe*, et *Méthodes d'authentification* → *Protection par mot de passe* pour la liste des termes interdits.

Pourquoi ça compte : deux idées ont changé. D'abord, la réinitialisation en libre-service, bien configurée avec double vérification, est **plus sûre** qu'un appel au support où l'on reconnaît la voix du demandeur — c'est ce coup de téléphone que l'ingénierie sociale exploite. Ensuite, l'expiration forcée tous les trois mois est aujourd'hui **déconseillée** par Microsoft comme par l'ANSSI : elle pousse mécaniquement vers `Printemps2026!` puis `Ete2026!`. Un mot de passe long, unique, jamais expiré, associé à une double authentification, protège nettement mieux.

VERT La réinitialisation en libre-service est active avec deux méthodes de vérification, les mots de passe n'expirent plus, et les termes évidents liés à votre entreprise sont interdits.
ROUGE Pas de libre-service, ou une expiration forcée toujours en vigueur.

12. La sauvegarde de vos données

La question : si tous vos e-mails et fichiers étaient supprimés ou chiffrés aujourd'hui, comment les récupéreriez-vous dans six mois ?

Où vérifier : cherchez si une solution de sauvegarde tierce est en place. Ce n'est pas une fonction native de Microsoft 365 : si personne ne peut nommer l'outil, il n'y en a pas.

Pourquoi ça compte : c'est le malentendu le plus coûteux du cloud. Microsoft garantit la **disponibilité de sa plateforme**, pas la **récupération de vos contenus** face à vos propres incidents — c'est le modèle de responsabilité partagée, écrit dans vos conditions de service. Ce que vous avez n'est pas une sauvegarde mais une **corbeille à rétention limitée**, de l'ordre de trente à quatre-vingt-treize jours selon les éléments. Elle récupère un fichier effacé la semaine dernière ; elle ne restaure rien trois mois après un sinistre. Et un rançongiciel moderne chiffre précisément les fichiers **synchronisés** vers OneDrive et SharePoint.

VERT Une sauvegarde tierce couvre la messagerie, OneDrive, SharePoint et Teams, avec une durée de conservation définie — et **une restauration a déjà été testée**.
ROUGE Aucune sauvegarde tierce, ou une sauvegarde dont personne n'a jamais vérifié qu'elle se restaure.

13. Les appareils

La question : vos données professionnelles sont-elles accessibles depuis des appareils personnels non gérés ?

Où vérifier : centre d'administration Intune → *Appareils* → *Conformité*. À défaut de licence Intune, la question reste valable : sur quels téléphones et ordinateurs vos e-mails sont-ils réellement consultés ?

Pourquoi ça compte : un ordinateur familial non chiffré, sans mise à jour et partagé avec des adolescents peut aujourd'hui télécharger l'intégralité d'un espace documentaire. En cas de perte ou de vol, sans chiffrement du disque ni verrouillage, les données sont lisibles directement.

VERT Des règles de conformité minimales — chiffrement, verrouillage, système à jour — conditionnent l'accès aux données.
ROUGE N'importe quel appareil peut se connecter et synchroniser sans condition.

14. Les invités externes

La question : combien de personnes extérieures ont un accès à votre environnement, et depuis quand ?

Où vérifier : centre Entra → *Identité* → *Utilisateurs*, en filtrant sur le type d'utilisateur *Invité*.

Pourquoi ça compte : chaque prestataire, expert-comptable, stagiaire ou partenaire invité sur un espace Teams y reste. La mission se termine, l'invitation demeure. Il n'est pas rare de trouver dans une PME de cinquante personnes plusieurs dizaines d'invités, dont beaucoup travaillent désormais ailleurs — et l'accès d'un invité échappe entièrement à votre contrôle de sécurité, puisqu'il dépend de la protection de son propre compte.

VERT La liste des invités est connue, justifiée, et revue au moins deux fois par an.
ROUGE Vous découvrez le nombre, ou des invités de missions terminées depuis longtemps.

15. Les connexions à risque

La question : que se passe-t-il quand Microsoft détecte une connexion suspecte — depuis un pays inhabituel, une adresse anonymisée, ou avec un mot de passe apparu dans une fuite publique ?

Où vérifier : centre Entra → *Protection* → *Identity Protection* → *Utilisateurs à risque* et *Connexions à risque*. Les règles automatiques nécessitent une licence Entra ID P2 ; la consultation des détections reste possible sans.

Pourquoi ça compte : Microsoft détecte ces signaux pour vous. Sans règle associée, la détection s'affiche sur un écran que personne n'ouvre, et il ne se passe rien. Avec une règle, une connexion risquée déclenche automatiquement une demande de double authentification ou un changement de mot de passe — c'est-à-dire une réaction en pleine nuit, sans intervention humaine.

VERT Les détections sont exploitées, et des règles automatiques réagissent aux risques élevés.
ROUGE Personne n'a jamais ouvert cet écran.

Et maintenant ?

Comptez vos couleurs.

Cinq rouges ou plus. C'est fréquent et ce n'est pas une raison de paniquer : cela signifie surtout que vos réglages sont restés ceux d'origine. Commencez par les points 4, 3, 6 et 12 — la double authentification, le nombre d'administrateurs, les anciens protocoles et la sauvegarde. Ces quatre-là ferment l'essentiel du risque réel, et les trois premiers sont gratuits.

Entre un et quatre rouges. Votre socle tient. Traitez-les dans l'ordre où ils apparaissent ci-dessus : la liste est classée par impact décroissant.

Aucun rouge, quelques oranges. Vous êtes au-dessus de la moyenne de votre catégorie. Le sujet devient alors la régularité — une revue trimestrielle des comptes, des invités et des partages — plutôt que la configuration.

Une remarque honnête pour finir. Cette liste vous dit *où* vous en êtes. Elle ne vous dit pas ce qui, dans votre situation particulière, mérite d'être traité en premier, ni ce que coûte réellement chaque correction. C'est précisément ce travail — regarder, comparer à un référentiel, noter, prioriser — que je fais pour des structures de votre taille, en quelques heures étalées sur deux semaines, à distance, et restitué par écrit.

Si vous voulez en parler, ou simplement poser une question sur un point de cette liste : **contact@aegiren.com**. Répondre à une question ne vous engage à rien.

Référentiels. Cette checklist s'appuie sur le *CIS Microsoft 365 Foundations Benchmark* et sur le *Guide d'hygiène informatique* de l'ANSSI, adaptés à la réalité d'une structure de 5 à 80 postes.

Aegiren — Votre Microsoft 365, audité, durci, documenté.
Rédigé par Mithra · v1 · 2026 · aegiren.com