Politique de gestion des accès et de la MFA

Politique | Français · Modèle à adapter | v3.0 · 2026-10-16

Version du modèle : 3.0. La politique prévoit une PME d'environ 80 personnes avec informatique éventuellement externalisée. Elle distingue propriétaire métier et exécutant technique, sans supposer une équipe identité dédiée. Les fonctions peuvent être cumulées avec suppléance et contrôle adapté. Les clauses ne valent exigences internes qu'après adoption et ne décrivent pas un état de mise en œuvre déjà acquis.

Mode d'emploi. Les sections 1–5 présentent les règles générales. Appliquer le périmètre et les catégories des sections 6 et 8 avant de provisionner ; utiliser la section 7 pour les mouvements de personnel. Les sections 9–10 encadrent récupération et urgence avant toute intervention correspondante. La section 11 guide la revue ; la section 12 prépare l'adoption. Les développements sont des références à utiliser avant l'action, pas des étapes à lire après sa réalisation.

Type : politique à faire approuver. Ce modèle fixe des règles internes proposées pour attribuer, vérifier et retirer les accès. Il devient une politique de votre organisation après adaptation et approbation. Il ne constitue ni une attestation de conformité ni une sélection automatique de niveau d'assurance réglementaire.

Objet. Maintenir des accès justifiés, attribuables et révocables pendant leur cycle de vie, avec une authentification adaptée au risque. Après adoption, « doit » et « exige » expriment les exigences internes approuvées ; avant adoption, toutes les clauses restent des propositions. Le propriétaire complète les paramètres, fait confirmer les moyens disponibles et retire toute affirmation d'application qui n'a pas été vérifiée.

Approbation, champ et responsabilités

Champ	Valeur à renseigner
Organisation, référence et version	[À RENSEIGNER : organisation, référence, version]
Propriétaire et approbateur	[À RENSEIGNER : responsable identité, direction]
Approbation et prochaine révision	[À RENSEIGNER : dates]
Services et populations couverts	[À RENSEIGNER : salariés, tiers, cloud, accès distants]
Référentiel des identités et demandes	[À RENSEIGNER : systèmes et procédure]
Circuit d'exception et urgence	[À RENSEIGNER : responsables, contacts]

Les responsables métier justifient le besoin ; les propriétaires de ressources autorisent les droits ; l'équipe identité applique et trace les changements. Les RH ou donneurs d'ordre transmettent les mouvements autorisés. La sécurité définit les exigences et examine les exceptions. Chaque titulaire protège ses moyens d'authentification et signale perte ou sollicitation inattendue.

Les identités techniques et comptes partagés doivent être inventoriés séparément. Quand une interaction nominative est possible, l'organisation privilégie un compte individuel. Toute impossibilité doit être documentée avec responsable, traçabilité compensatoire et date de réexamen. L'usage d'un compte ne prouve pas automatiquement l'identité de la personne agissante.

1. Accorder un accès justifié

Toute demande précise ressource, droits, motif, bénéficiaire, propriétaire et durée. Le demandeur ne valide pas seul son propre accès sensible. Les profils de droits sont définis par rôle et limités au besoin. Un accès temporaire comporte une expiration vérifiable. La copie intégrale des droits d'un collègue ne remplace pas l'analyse du besoin.

☐ Vérifier l'identité et le rattachement du bénéficiaire.

☐ Obtenir l'accord du propriétaire de la ressource.

☐ Identifier les incompatibilités de fonctions : [À RENSEIGNER : règles].

☐ Fixer début, fin éventuelle et modalités d'utilisation.

☐ Confirmer les droits réellement appliqués, avec référence de demande.

Les accès d'administration utilisent des identités et moyens adaptés au risque, distincts des usages ordinaires lorsque cela est possible. Éviter les privilèges permanents inutiles ; définir l'élévation temporaire et sa journalisation dans [À RENSEIGNER : procédure d'administration].

2. Définir la couverture MFA

L'organisation impose une MFA sur [À RENSEIGNER : ressources et catégories prioritaires], avec calendrier de couverture et contrôle des exceptions. La méthode doit être compatible avec le service, la population et les risques. Les mécanismes résistants au phishing sont privilégiés pour les accès sensibles lorsqu'ils sont disponibles et déployables.

Le NIST distingue les niveaux d'assurance et les propriétés des authentificateurs. Un code saisi manuellement ou une notification approuvée ne doit pas être présenté comme équivalent à une authentification résistante au phishing. Choisir une méthode nécessite de vérifier ses propriétés réelles, pas seulement l'étiquette « MFA » affichée par un produit.

Catégorie	Exigence locale	Responsable et contrôle
Administration et accès distant	[À RENSEIGNER : méthodes admises, restrictions]	[À RENSEIGNER : propriétaire, preuve de couverture]
Applications métier	[À RENSEIGNER : périmètre et déploiement]	[À RENSEIGNER : propriétaire, fréquence]
Services incompatibles	[À RENSEIGNER : compensation, exception datée]	[À RENSEIGNER : décideur et réexamen]

Désactiver les chemins d'authentification qui contournent les exigences après analyse des dépendances. Vérifier aussi les accès directs aux applications, comptes externes et moyens de récupération. Une règle configurée mais non appliquée ne démontre pas la couverture.

3. Enrôler et récupérer sans affaiblir

L'enrôlement initial, l'ajout d'un moyen et la récupération exigent une vérification d'identité proportionnée au risque. Le support ne collecte pas les mots de passe ou codes MFA. Une demande urgente provenant du compte concerné ne suffit pas à autoriser une réinitialisation. Utiliser [À RENSEIGNER : canal indépendant et contrôles] et tracer l'opérateur.

Prévoir une solution de secours maîtrisée pour la perte d'un authentificateur. Les comptes d'urgence sont limités, protégés, surveillés et testés selon [À RENSEIGNER : scénario et périodicité]. Leur activation déclenche une revue. Les secrets et codes de récupération sont stockés dans un dispositif autorisé, séparément des tickets ordinaires.

4. Réviser et retirer

☐ Lors d'un changement de rôle, organiser une transition approuvée, retirer les droits devenus inutiles et borner tout chevauchement temporaire ; vérifier les accès essentiels après changement.

☐ Lors d'un départ, coordonner les retraits selon l'heure autorisée.

☐ Examiner groupes, droits directs, délégations, accès tiers et applications.

☐ Traiter sessions et tokens selon les mécanismes réellement disponibles.

☐ Faire attester les accès sensibles par leurs propriétaires à [À RENSEIGNER : fréquence].

☐ Affecter une échéance et un propriétaire aux anomalies détectées.

Pour un compte suspect, appliquer le playbook de réponse adapté. Le retrait de droits doit être contrôlé dans les services concernés ; les sessions applicatives peuvent nécessiter une action distincte. Conserver la preuve du résultat, pas uniquement celle de la demande.

5. Exceptions, suivi et exercice

Toute exception décrit ressource, risque, justification, mesure compensatoire, décideur, expiration et contrôle. Une dérogation renouvelée sans examen n'est pas une maîtrise du risque. Suivre la couverture MFA effective, les comptes sans propriétaire, les droits expirés et les récupérations inhabituelles sans inventer de cible universelle.

Testez un départ, une mutation et une perte de moyen MFA. Le contrôleur doit retrouver qui a approuvé, ce qui a changé et comment le résultat a été vérifié. Réviser la politique après incident, changement majeur ou à l'échéance prévue. Les règles de conservation des traces et les obligations applicables sont définies avec les fonctions compétentes.

Exigences de contrôle après adoption

Référence interne proposée	Exigence et élément de preuve
ACC-01 — Attribution	Tout accès sensible doit avoir un propriétaire, une justification et une autorisation conservées.
ACC-02 — Authentification	Le propriétaire doit contrôler la couverture effective des exigences MFA et leurs contournements possibles.
ACC-03 — Cycle de vie	Les mouvements de personnel et les accès temporaires doivent déclencher une vérification des droits et du résultat des retraits.
ACC-04 — Exception	Toute dérogation doit avoir un décideur acceptant le risque, une expiration, une compensation et une preuve de réexamen.
ACC-05 — Assurance interne	Les écarts doivent être suivis jusqu'à correction vérifiée ou acceptation explicite du risque résiduel.

Le propriétaire du processus présente à [À RENSEIGNER : instance et fréquence] la couverture contrôlée, les accès sans propriétaire, les exceptions échues et les retraits non vérifiés. Chaque indicateur précise son périmètre et ses limites ; une population non testée n'est pas comptée comme conforme. Les preuves restent accessibles uniquement aux personnes habilitées, pour une durée justifiée localement.

Une exception arrivée à expiration est réexaminée par l'autorité désignée ; sa reconduction n'est pas implicite. Si la suppression immédiate menace une activité essentielle, cette autorité décide d'une transition bornée et de protections adaptées. Les modifications de la politique sont approuvées, versionnées et communiquées aux exploitants concernés avant leur application, sauf procédure d'urgence expressément prévue.

6. Périmètre d'adoption et délégations

Le propriétaire doit établir la liste des annuaires, applications SaaS, accès distants, consoles d'administration, sauvegardes et services externalisés couverts. Les accès fournisseurs et le télétravail sont inclus lorsque l'organisation les autorise. Les équipements personnels, environnements industriels et relations contractuelles particulières doivent recevoir une règle adaptée ; la politique ne permet aucune intervention hors des droits détenus.

Pour une petite structure, le responsable administratif peut notifier les mouvements, le dirigeant ou propriétaire métier autoriser les droits et le prestataire les appliquer. Le MSSP peut observer des événements sans pouvoir changer les comptes. Chaque responsabilité doit avoir un titulaire, un

suppléant, un canal de secours et une limite de délégation. Une tâche sans exécutant confirmé constitue un écart d'adoption, pas une capacité disponible.

Décision	Responsable interne	Exécutant et contrôle
Ouvrir ou modifier un accès	Propriétaire de la ressource	Prestataire ou administrateur ; droits effectivement appliqués vérifiés
Accorder un privilège ou accès fournisseur	Sponsor métier et autorité désignée	Administrateur ; périmètre, durée et traçabilité contrôlés
Restreindre en urgence	Coordinateur dans sa délégation	Exécutant habilité ; conséquences et accès essentiels vérifiés
Accepter une exception	Autorité de risque nommée	Propriétaire du contrôle ; compensation et réexamen démontrés

Si le prestataire est indisponible, le coordinateur utilise les contacts de secours et le circuit contractuel. Il consigne l'impossibilité d'agir et sollicite le décideur métier. Les moyens temporaires doivent être autorisés et réalisables ; il est interdit, dans le modèle adopté, de transformer un accès partagé non maîtrisé en solution permanente parce que le support ne répond pas.

7. Arrivées, mobilités et départs

L'événement déclencheur doit provenir d'une fonction autorisée : RH, direction ou sponsor d'un prestataire. Une demande directe par messagerie ne suffit pas pour un accès sensible sans validation indépendante du besoin. La fiche précise identité stable, rôle, ressources, date d'effet, propriétaire et limite éventuelle. L'équipe d'exécution confirme les droits créés, refusés et encore en attente.

Étape	Action et autorisation	Preuve et traitement d'échec
Arrivée	Vérifier identité, besoin et profil approuvé ; préparer enrôlement	Demande liée aux droits réels ; si besoin non validé, ne pas ouvrir l'accès sensible
Mobilité	Comparer ancien et nouveau rôle ; décider le chevauchement nécessaire	Droits retirés/ajoutés tracés ; tout maintien temporaire a propriétaire et fin
Départ	Appliquer l'heure et le périmètre autorisés avec métier et IT	Retraits et sessions ciblées contrôlés ; les services inaccessibles restent ouverts au suivi
Fin de mission fournisseur	Confirmer sponsor, comptes, délégations et secrets exposés	Accès retirés et ressources transférées ; incertitudes soumises à l'autorité de risque

Avant un départ, déterminer qui reprend les données et responsabilités opérationnelles sans remettre le mot de passe de la personne sortante à son remplaçant. Préserver les données nécessaires selon les règles approuvées, puis contrôler boîtes partagées, délégations, groupes et applications. La suppression d'un compte n'est pas une méthode universelle de conservation ni une preuve que tous les droits externes ont disparu.

En cas de conflit entre retrait urgent et continuité, le propriétaire métier décide d'un accès alternatif autorisé ou d'une interruption assumée. Toute transition conserve un terme, une liste de droits et un contrôle. Une réactivation ultérieure doit être traitée comme une nouvelle décision : vérifier le besoin actuel au lieu de restaurer aveuglément tous les anciens droits.

8. Comptes privilégiés, techniques, partagés et fournisseurs

Les comptes privilégiés doivent être liés à une tâche d'administration justifiée, avec un environnement d'usage et des traces adaptés. Le titulaire doit distinguer son activité habituelle de son activité d'administration. Si une élévation temporaire est disponible et retenue, documenter approbation,

activation, durée et résultat. Si elle ne l'est pas, une exception précise comment le privilège permanent est contrôlé.

Une identité technique doit avoir un propriétaire métier, un responsable technique et une liste de dépendances. Décrire son usage, ses droits, son mécanisme d'authentification, le stockage du secret ou certificat et son renouvellement. Ne pas déclarer toutes les identités « couvertes par MFA » parce que les comptes interactifs le sont ; la protection doit être vérifiée selon le mécanisme réellement utilisé.

Catégorie	Paramètres à renseigner	Contrôle attendu
Service ou application	[À RENSEIGNER : usage, propriétaire, dépendances, mécanisme]	Secret protégé, droits limités, renouvellement et arrêt testables
Compte partagé exceptionnel	[À RENSEIGNER : justification, titulaires autorisés, traçabilité]	Accès aux secrets maîtrisé, usage attribuable au niveau possible, sortie des titulaires suivie
Fournisseur	[À RENSEIGNER : sponsor, contrat, systèmes, horaires ou durée]	Accès activé selon besoin, actions observables et retrait confirmé
Administration	[À RENSEIGNER : tâches, droits, environnement, approbation]	Séparation des usages, examen des privilèges et anomalies

Un prestataire ne doit pas réutiliser un accès d'une personne partie sans décision. Les comptes génériques imposés par un équipement sont documentés avec les compensations possibles : accès réseau limité, coffre contrôlé, journal d'intervention ou supervision. L'autorité de risque approuve les limites de traçabilité. Aucune compensation ne doit être présentée comme équivalente à une identité individuelle si elle ne permet pas cette attribution.

9. Enrôlement MFA, perte et récupération

Avant déploiement, le propriétaire doit choisir les méthodes admises, identifier les personnes ayant des besoins d'accessibilité et prévoir le remplacement d'un moyen perdu. Tester les applications prioritaires et les chemins alternatifs. L'absence d'un moyen compatible reçoit une exception ou une solution de travail approuvée ; elle ne justifie pas une désactivation durable et invisible de l'exigence.

Entrée	Action autorisée	Preuve et limite
Nouvel utilisateur	Vérifier identité et remettre les instructions par un canal maîtrisé	Enrôlement attendu confirmé ; aucun secret dans le ticket
Moyen perdu ou téléphone remplacé	Vérification indépendante, évaluation de compromission, récupération approuvée	Ancien moyen traité, nouveau moyen contrôlé, opérateur identifié
Sollicitation inattendue	Signalement et examen du compte selon playbook	Décision de restriction ou explication ; absence de validation par défaut
Support indisponible	Secours défini et arbitrage métier	Demande suivie ; pas d'accès sensible improvisé hors délégation

La récupération ne doit pas devenir un chemin moins contrôlé que l'usage prévu. Le support applique les vérifications définies localement et refuse de fonder une réinitialisation sensible sur l'urgence seule ou un message du compte concerné. Si l'identité ne peut pas être établie par les moyens approuvés, escalader et proposer une activité alternative, sans demander de codes MFA utilisables.

10. Accès d'urgence et remise sous contrôle

Le propriétaire doit définir les scénarios d'urgence : indisponibilité de l'identité, perte des moyens ordinaires ou impossibilité d'administrer un service critique. Désigner les personnes autorisées, les

conditions d'activation, la garde des moyens et les accès de secours réellement nécessaires. Vérifier que leur récupération ne dépend pas exclusivement du service qu'ils doivent secourir.

Le guide Microsoft sur les comptes d'urgence Entra recommande notamment des dépendances d'authentification distinctes, une garde protégée, une surveillance des usages et une revue après utilisation. Ces principes éclairent le modèle ; les paramètres propres à Entra, nombres de comptes et périodicités de ce fournisseur ne sont pas des valeurs universelles à recopier.

☐ Le décideur enregistre le motif, le périmètre et l'opérateur avant activation lorsque l'urgence le permet.

☐ Les moyens sont remis uniquement aux personnes habilitées par le canal prévu.

☐ L'opérateur consigne les changements et préserve les traces disponibles.

☐ Un destinataire indépendant est informé par le mécanisme retenu ; toute panne de notification reste visible.

☐ Après usage, contrôler les droits, moyens exposés, accès temporaires et fonctionnement normal.

☐ Révoquer, remplacer ou remettre sous garde les moyens selon leur nature et la procédure approuvée.

☐ Un relecteur examine nécessité, autorisation et résultat ; une personne seule ne s'auto-attribue pas une assurance indépendante.

11. Recertification, exceptions et preuve

La revue des accès doit partir de la population réelle des comptes et ressources, pas uniquement des demandes récentes. Le propriétaire de ressource reçoit compte, droits, sponsor, dernière information d'usage disponible et exceptions. Il décide maintenir, modifier, retirer ou instruire. Une absence de réponse n'équivaut pas à une approbation ; le coordinateur relance puis soumet la décision au circuit d'escalade.

Fiche de revue à dupliquer	Valeur à renseigner
Population et couverture	[À RENSEIGNER : systèmes, comptes, exclusions, date d'extraction]
Décision et autorité	[À RENSEIGNER : droits, besoin, propriétaire, maintien/retrait]
Exécution	[À RENSEIGNER : prestataire, référence, date, résultat]
Écart	[À RENSEIGNER : impossibilité, compensation, risque accepté, fin]

Le dossier d'exception réunit l'exigence non satisfaite, les ressources, le motif, les alternatives étudiées, la compensation testée, l'autorité acceptant le risque et l'expiration. Préciser le déclencheur de réexamen anticipé : changement de mission, incident ou nouvelle capacité disponible. Le responsable contrôle la correction ou obtient une nouvelle décision ; il ne supprime pas le constat pour améliorer un indicateur.

12. Adoption et exercice fictif

L'adoption suit quatre passages : inventaire et responsabilités acceptés ; demandes et mouvements testés ; MFA, récupération et urgence vérifiées sur un périmètre représentatif ; écarts présentés à l'approbateur avec moyens et plan de traitement. Un document signé sans exécutants ni accès disponibles ne constitue pas une recette réussie. La date d'effet doit être compatible avec les décisions encore nécessaires.

Atelier-80, entreprise entièrement fictive, fait évoluer une salariée des ventes vers la finance. Le sponsor demande des droits comptables ; le prestataire propose de copier un profil existant. Le propriétaire finance refuse la copie globale, valide les tâches nécessaires et autorise un chevauchement limité pour achever des commandes. La décision fictive EX-A1 précise droits, contrôle métier, responsable et fin.

Cas fictif	Décision	Preuve de recette
Mobilité ventes vers finance	Retirer les droits sans besoin, borner le chevauchement autorisé	Comparaison avant/après et opération métier testée
Départ d'un intervenant fournisseur	Sponsor confirme fin ; prestataire retire comptes et délégations	Résultats vérifiés, service externe non confirmé suivi séparément
Perte d'un moyen MFA	Support vérifie par le parcours indépendant puis récupère	Ancien moyen traité, nouveau validé, aucun code dans le ticket
Test d'accès d'urgence	Activation autorisée dans le périmètre prévu	Usage observable, revue effectuée, moyens remis sous contrôle

L'exercice échoue si le prestataire conserve seul le pouvoir d'accepter le risque métier, si un compte technique n'a pas de propriétaire ou si un refus d'accès conduit à partager un secret. Il est accepté lorsque les décisions et résultats sont retrouvables, les inconnues explicites et les corrections affectées. La direction conserve la décision sur les exceptions restantes avant la mise en application générale.

Références de travail

Consulter également Microsoft, gestion des comptes d'accès d'urgence. Les prescriptions techniques doivent être adaptées au fournisseur, aux accès détenus et aux contraintes locales.

NIST SP 800-63B-4 : authentificateurs, assurance et récupération ; ce référentiel n'impose pas automatiquement ses exigences à toute organisation. Microsoft : révocation des accès : exemple de limites des tokens et sessions. Les règles internes proposées doivent être testées avec vos fournisseurs et adaptées aux contraintes d'accessibilité, de continuité et de sécurité.