Politique de sauvegarde et de restauration avec plan de test

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

Version du modèle : 3.0. Type : politique et procédure opérationnelle. Profil proposé : PME d'environ 80 personnes, dont l'exploitation, l'hébergement ou les sauvegardes peuvent être externalisés. Ce profil n'affirme rien sur votre environnement. L'entreprise doit garder des propriétaires internes pour les objectifs métier, l'acceptation des écarts et l'autorisation de reprise, même si un fournisseur réalise toutes les opérations techniques.

Après adaptation et adoption, « doit » et les consignes constituent des exigences internes sur le périmètre approuvé. Avant adoption, elles restent des propositions. Les fréquences, durées, objectifs RPO/RTO, fenêtres et critères doivent être décidés localement. Le modèle ne garantit ni conformité, ni récupération complète, ni délai de reprise. Une tâche réussie n'établit pas, seule, qu'un service pourra être restauré.

1. Objet, périmètre et décisions d'adoption

La politique doit couvrir données, configurations, applications et moyens nécessaires aux activités prioritaires. Le propriétaire doit identifier ce qui doit être reconstruit, ce qui doit être récupéré et ce qui peut être réinstallé depuis une source maîtrisée. Le périmètre doit inclure services externalisés, postes contenant des données uniques, annuaires, clés, catalogues et procédures lorsqu'ils sont nécessaires à la reprise retenue.

L'équipe doit distinguer sauvegarde, réplication, disponibilité et archivage. Ces mécanismes peuvent contribuer à des objectifs différents ; leur présence ne les rend pas interchangeables. Un fournisseur qui conserve des répliques ne promet pas automatiquement la restauration attendue après suppression, compromission ou erreur. Le contrat et un test représentatif doivent confirmer les capacités réellement utilisables.

Paramètre	Décision locale	Autorité	Preuve
Activités et périmètre	[À RENSEIGNER : services, données, dépendances, exclusions]	Direction et métiers	Cartographie et responsables
Objectifs métier	[À RENSEIGNER : perte et interruption acceptables]	Propriétaires métiers	Arbitrages approuvés
Stratégie de copie	[À RENSEIGNER : fréquences, supports, séparation, durées]	Responsable interne	Capacité et protections vérifiées
Reprise et test	[À RENSEIGNER : scénarios, ordre, critères, fenêtres]	Métier et exploitation	Procédure et résultats
Contrôle documentaire	[À RENSEIGNER : version, effet, approbateur, revue]	Direction	Document approuvé accessible

Une exclusion doit avoir motif, propriétaire, risque et action. Le propriétaire doit vérifier les informations avant effet : un service nouveau, une donnée déplacée ou un catalogue absent peut modifier la reprise. Il doit maintenir les écarts visibles. Une liste de tâches de sauvegarde ne suffit pas à décrire les services protégés.

2. Responsabilités et recours en cas d'absence

Fonction	Responsabilité	Décision réservée	Absence ou défaut
Direction ou délégataire	Arbitrer moyens et risque résiduel	Accepter l'écart aux objectifs	Suppléant interne nommé
Propriétaire métier	Décrire priorité, données et opération à reprendre	Valider service minimum et résultat	Remplaçant connaissant l'activité
Responsable interne	Tenir stratégie, couverture, contrats et preuves	Accepter la recette et demander correction	Suppléant avec accès aux procédures
Infogérant ou équipe sauvegarde	Exécuter, contrôler, restaurer et fournir les preuves	Action dans mandat seulement	Escalade et opérateur habilité
Sécurité ou pilote d'incident	Évaluer compromission et sûreté de reprise	Recommander protection et conditions	Relais identifié
Propriétaire de données et fonctions compétentes	Définir sensibilité, accès et conservation	Autoriser usages et contraintes	Conseil ou responsable de secours

Le responsable interne doit vérifier au contrat : périmètre, données exclues, horaire de soutien, accès de restauration, délais de mise à disposition, restitution, coûts et dépendances de capacité. Il doit faire confirmer l'acceptation des tâches et des preuves attendues. Un engagement du fournisseur ne doit pas être transformé en objectif métier démontré sans test de bout en bout.

Le suppléant doit pouvoir retrouver l'annuaire, les instructions, l'autorité et le moyen d'obtenir les secrets autorisés sans utiliser le compte du titulaire absent. Les documents généraux ne doivent pas contenir ces secrets. Une dépendance à la même messagerie ou au même annuaire que les systèmes sinistrés doit être examinée ; le mode de secours doit être testé, pas seulement décrit.

3. Définir RPO/RTO à partir de l'activité

Le métier doit expliquer quelle perte de données il peut supporter et combien de temps l'activité peut rester interrompue. Le responsable doit traduire ces besoins en objectifs locaux et préciser le point de départ de la mesure. RPO désigne ici l'objectif de perte de données ; RTO l'objectif de temps de reprise. Les valeurs ne doivent pas être choisies uniquement d'après les options affichées par un logiciel.

L'exploitant doit examiner si fréquence, cohérence applicative, volume, capacité, bande passante, clés et accès permettent d'atteindre ces objectifs. Le test doit inclure préparation et dépendances selon le périmètre de mesure approuvé. Si la capacité est insuffisante, il doit présenter l'écart et les options. La direction doit arbitrer moyens, priorité ou risque ; l'objectif ne doit pas être modifié silencieusement pour correspondre au dernier résultat.

Activité	Besoin à exprimer	Vérification technique	Décision si écart
Traitement de commandes	Données nécessaires, perte acceptable, service minimum	Copie cohérente et opération représentative	Moyen supplémentaire ou mode dégradé accepté
Identité et administration	Accès indispensables aux autres reprises	Annuaire, comptes de secours et autorité	Revoir ordre et dépendances
Données hébergées	Période, granularité et accès disponibles	Export/restauration effectivement réalisables	Contrat, autre protection ou risque accepté
Données locales uniques	Sources non synchronisées et responsable	Inclusion ou récupération contrôlée	Supprimer l'unicité ou documenter exclusion

Chaque service doit avoir une fiche : propriétaire, composants, dépendances, objectifs, copies, durée, ordre, méthode et test. Les valeurs doivent être validées conjointement par métier et technique. Une

restauration plus rapide mais incohérente peut ne pas répondre au besoin ; un fichier récent sans application ou clé disponible ne constitue pas un service repris.

4. Concevoir les copies et leur séparation

La stratégie doit déterminer quelles copies répondent aux scénarios : suppression involontaire, panne, perte de site et compromission. Elle doit identifier le contrôle administratif capable de les modifier ou supprimer. Une copie hors site mais connectée n'est pas une copie hors ligne. L'équipe doit vérifier les droits et les chemins d'accès réels, notamment ceux du fournisseur et des identités de production.

Une protection présentée comme immuable doit être examinée : mécanisme, durée configurée, personnes pouvant la changer, suppression du compte, clés et conditions du fournisseur. Le terme ne doit pas être utilisé comme garantie absolue. La stratégie peut combiner protection contre modification et copie déconnectée selon le risque ; le choix et les limites doivent être approuvés et testés dans les conditions autorisées.

Protection	Question à vérifier	Preuve	Échec à traiter
Séparation réseau	Un accès de production atteint-il le dépôt ?	Configuration et contrôle autorisé	Restreindre ou accepter le risque explicitement
Identités distinctes	Le compte compromis pourrait-il supprimer les copies ?	Rôles et test de refus	Revoir privilèges et secours
Protection contre modification	Qui change la règle et pendant quelle période ?	Paramètres, droits et essai prévu	Corriger la protection ou limiter la promesse
Copie hors ligne	Quand est-elle réellement déconnectée et récupérable ?	Inventaire, garde et test de lecture	Organiser rotation ou autre stratégie

La sensibilité des copies doit suivre celle des données. Le chiffrement doit être accompagné d'une gestion des clés récupérables et d'accès autorisés. Le responsable doit considérer vol de support, corruption, changement de fournisseur et perte d'identité. La protection d'une copie ne dispense pas de contrôler les données qu'elle contient ni de savoir comment les restaurer.

5. Protéger les moyens de sauvegarde et la chaîne de reprise

L'infrastructure de sauvegarde doit être administrée avec des identités dédiées et des privilèges limités. Les rôles de consultation, exploitation, configuration et suppression doivent être distingués lorsque les capacités le permettent. Les changements et opérations sensibles doivent être journalisés. Les composants doivent suivre la politique de correctifs ; protéger les données sans maintenir le logiciel de sauvegarde laisse une dépendance critique non traitée.

Le responsable doit conserver les éléments permettant de reconstruire le dispositif : procédures, catalogue, configurations, binaires autorisés, licences, matériel ou capacité, mécanismes d'import et récupération des clés. Les moyens de secours doivent être protégés, mais utilisables par les personnes habilitées. Une copie chiffrée dont la clé n'est pas récupérable ne démontre aucune capacité de restauration.

Étape de dépendance	Entrée nécessaire	Contrôle	Responsable
Accès de secours	Identité, délégation et moyen d'authentification	Connexion autorisée sans système sinistré	Responsable interne
Infrastructure	Réseau, temps, stockage et administration maîtrisés	Ressources disponibles et isolées si nécessaire	Exploitant
Outil et catalogue	Installation et références des copies	Copie retrouvée et lisible	Équipe sauvegarde

Étape de dépendance	Entrée nécessaire	Contrôle	Responsable
Clés et données	Autorité, clé et point cohérent	Déchiffrement et intégrité contrôlés	Dépositaire et opérateur
Application	Versions, paramètres et dépendances	Fonction technique puis opération métier	Propriétaires technique et métier

L'ordre dépend du service ; cette chaîne est un modèle à adapter, non une séquence universelle. Le pilote doit rechercher les dépendances circulaires, par exemple une procédure ou un secret accessible uniquement depuis l'application à restaurer. Il doit faire tester l'accès alternatif et affecter la correction. Une dépendance non résolue doit rester une réserve explicite de reprise.

6. Exécuter les sauvegardes et traiter les échecs

L'opérateur doit contrôler les tâches, les données effectivement incluses, la fraîcheur et les anomalies de volume, durée ou configuration. Une tâche verte peut ignorer un volume ou une application. Le contrôle doit comparer le périmètre réel à la fiche de service et prendre en compte les changements récents. Les messages fournisseur doivent être reliés aux services concernés, pas seulement archivés.

Observation	Action	Preuve à garder	Escalade
Tâche échouée	Identifier état, cause et copie encore disponible	Erreur, service, dernière copie utile	Responsable interne et métier selon exposition
Tâche réussie mais contenu douteux	Comparer inclusions et données attendues	Écart de périmètre et contrôle	Ne pas annoncer protection complète
Copie trop ancienne	Comparer à l'objectif approuvé	Dernier point cohérent et perte potentielle	Décision de protection ou risque accepté
Changement inattendu	Vérifier autorisation et effet	Configuration, auteur et historique	Sécurité si compromission plausible

Chaque échec doit recevoir propriétaire, action et point de réexamen. Une nouvelle tâche réussie doit être vérifiée avant fermeture. Si le service dépasse l'objectif approuvé, le métier doit connaître la perte potentielle et décider avec l'autorité compétente. Une relance répétée sans analyse ne doit pas masquer une absence durable de copie utilisable.

Le fournisseur doit confirmer ce qu'il a fait et ce qu'il a vérifié. S'il est indisponible, le responsable utilise l'escalade et le relais prévus. Les moyens alternatifs ne doivent pas exposer les données par un export non autorisé. Le risque d'attente et les capacités manquantes doivent être soumis à une personne interne, pas acceptés tacitement par silence.

7. Choisir et autoriser une restauration

Toute demande doit préciser service, données, motif, point souhaité, destination et autorité. Le responsable doit vérifier le besoin, les droits du demandeur et le risque d'écraser des données récentes. Une restauration vers un autre utilisateur ou système doit être spécifiquement autorisée. La récupération ne doit pas devenir un moyen de contourner les restrictions d'accès normales.

L'opérateur doit identifier la copie, son âge, les dépendances et sa cohérence applicative. Le pilote doit approuver environnement, fenêtre, impact, critères de succès et arrêt. La version source et les données actuelles utiles doivent être préservées selon la situation. La décision doit séparer restauration de test, récupération d'un élément et reprise complète ; ces niveaux n'ont pas la même preuve attendue.

Branche	Autorité et préparation	Contrôle de résultat	Réserve
Élément supprimé	Propriétaire de données ; destination séparée si adaptée	Contenu et accès validés	Ne prouve pas reconstruction du service

Branche	Autorité et préparation	Contrôle de résultat	Réserve
Panne technique	Métier et exploitation ; dépendances et capacité	Application et opération représentative	Effets sur données récentes
Compromission	Pilote d'incident ; environnement maîtrisé	Vérifications de sécurité et reprise conditionnelle	Copie possiblement contaminée
Demande fournisseur	Mandat, périmètre et protection du transfert	Réception lisible, complète selon demande	Capacité ou délai non confirmé

8. Reprise après compromission

Le pilote d'incident doit coordonner préservation, protection des sauvegardes et reconstruction. Les copies peuvent contenir des implants ou des configurations hostiles ; leur ancienneté ou leur lisibilité ne suffit pas à les déclarer saines. Le choix doit utiliser les faits disponibles sur la période compromise et consigner les inconnues. Une vérification antivirus seule ne constitue pas une garantie d'innocuité.

L'équipe doit privilégier une reconstruction maîtrisée selon les capacités : sources d'installation vérifiées, configurations examinées, données contrôlées avant import et administration indépendante des accès suspects. Le pilote doit décider des restrictions nécessaires et de la surveillance. Les mesures d'isolement de l'infrastructure de sauvegarde doivent être préparées avec les opérateurs et leurs effets connus, plutôt qu'improvisées pendant la crise.

Gate de reprise	Preuve attendue	Autorité	Si insuffisant
Préparer	Administration, environnement et copie identifiés	Pilote et exploitant	Reporter ou limiter le périmètre
Restaurer	Méthode, clés et point justifiés	Opérateur mandaté	Conserver erreur et réévaluer
Vérifier	Intégrité, accès, données et fonction métier	Technique et métier	Réparer, changer de point ou mode dégradé
Reconnecter	Accès suspects traités, risques et surveillance	Autorité de reprise	Ne pas élargir sans décision
Terminer	Critères atteints, actions restantes affectées	Direction ou délégataire	Risque résiduel explicitement accepté

La reprise ne remplace pas l'enquête ni le traitement des accès hostiles. Le métier doit comprendre ce qui a été récupéré et ce qui manque. Le pilote doit définir les conditions d'arrêt si un signe suspect apparaît. Une reconstruction techniquement terminée ne doit pas être déclarée service nominal avant la validation convenue.

9. Tester la capacité, pas seulement une copie

Le programme doit couvrir des scénarios représentatifs des risques : fichier, application, dépendance d'identité, perte des outils habituels et reprise cyber lorsque pertinente. Le propriétaire doit choisir les tests avec métier et exploitation, définir fréquence et périmètre localement et expliquer les exclusions. Un test de fichier ne doit pas être présenté comme une reconstruction complète.

L'autorisation doit préciser données utilisées, environnement, risques d'envoi réel, accès temporaires, consignes d'arrêt et suppression de fin. Les tests doivent éviter réactivation de comptes suspects, messages vers de vrais destinataires ou écrasement de production. Les opérateurs doivent noter début et fin des étapes selon le périmètre mesuré ; le résultat doit inclure les attentes et interventions, pas seulement la copie des octets.

☐ Vérifier mandat, scénario, périmètre et personnes de secours.

☐ Retrouver procédure, catalogue, copie, clés et capacité sans dépendance bloquante.

☐ Confirmer séparation du test et protection des données.

☐ Exécuter les étapes et conserver erreurs, durées et ajustements.

☐ Vérifier données, accès et opération métier.

☐ Comparer perte et temps observés aux objectifs approuvés.

☐ Affecter les écarts et prévoir un nouveau contrôle.

☐ Retirer accès temporaires, supprimer données de test et confirmer la clôture.

Le compte rendu doit permettre à une autre personne de comprendre ce qui a réellement été démontré. Les résultats doivent identifier service, point, environnement, opérateur, contrôleur, critères, écarts et décision. Le métier doit approuver ou refuser l'acceptation. Un test non concluant peut être utile s'il révèle une dépendance précise et entraîne une correction vérifiée.

10. Scénario fictif de reprise complète

Atelier Rivage, PME fictive d'environ 80 personnes, doit reprendre son traitement de commandes après une compromission suspectée. Le métier a fixé ses propres objectifs dans la fiche, sans valeur universelle. L'infogérant dispose des copies, mais la procédure initiale dépend d'une messagerie indisponible. Le suppléant utilise la copie contrôlée de secours. Aucun résultat ne représente une expérience client.

Étape fictive	État constaté	Décision et responsable	Preuve
Préparation	Catalogue disponible ; messagerie indisponible	Pilote utilise le canal et la procédure de secours	D-01, accès autorisé testé
Choix de copie	Point récent dans la période suspecte	Sécurité réserve son usage ; autre point examiné	E-01, justification et inconnues
Reconstruction	Outil et clés récupérés dans l'environnement séparé	Infogérant exécute sous mandat	E-02, lecture et déchiffrement
Test métier	Commande de test fonctionne ; pièce jointe absente	Métier refuse le nominal et accepte un mode dégradé limité	D-02, écart affecté
Validation	Donnée manquante récupérée et contrôle rejoué	Autorité décide élargissement avec surveillance	D-03, contrôle et risque restant

L'exercice est accepté si le remplaçant explique le choix de copie, retrouve l'autorité de déchiffrement et démontre pourquoi le premier résultat n'était pas une reprise complète. Il doit distinguer traitement sauvegardé, donnée récupérée et service validé. Il doit identifier la correction du manque et la prochaine vérification, plutôt que déclarer le test réussi parce que l'outil a terminé.

11. Annexes adaptables et exceptions

Fiche vierge de service	Valeur locale	Responsable	Vérification
Besoin et dépendances	[À RENSEIGNER : activité, minimum, ordre, fournisseurs]	[À RENSEIGNER]	Métier et technique
Objectifs	[À RENSEIGNER : RPO/RTO, point de départ, justification]	[À RENSEIGNER]	Approbation interne
Copies et accès	[À RENSEIGNER : fréquence, séparation, clés, durée]	[À RENSEIGNER]	Tests de lecture et refus

Fiche vierge de service	Valeur locale	Responsable	Vérification
Restauration	[À RENSEIGNER : méthode, destination, contrôles, arrêt]	[À RENSEIGNER]	Résultat technique et métier
Test et écarts	[À RENSEIGNER : scénario, observations, décision, suite]	[À RENSEIGNER]	Recette et correction

Exception	Exemple fictif rempli	À adapter	Décideur
Exigence non satisfaite	Copie déconnectée non disponible pour un service secondaire	[À RENSEIGNER]	Autorité interne
Compensation	Copie protégée et accès restreints testés ; limitation conservée	[À RENSEIGNER]	Sécurité et métier consultés
Risque et sortie	Destruction par privilège excessif reste possible ; changement planifié	[À RENSEIGNER]	Acceptation nominative
Expiration et contrôle	Date locale obligatoire avant signature ; réexamen après changement	[À RENSEIGNER]	Propriétaire de l'action

Une exception doit préciser cause, périmètre, risque, compensation vérifiée, responsable, expiration et réexamen. Le fournisseur ne doit pas accepter seul un écart aux objectifs métier. À l'échéance, correction ou nouvelle décision est exigée ; la reconduction tacite est exclue. Une protection supposée ne doit pas être qualifiée de compensation vérifiée.

12. Surveillance, application et révision

Le propriétaire doit présenter à [À RENSEIGNER : instance et cadence] services non couverts, copies anciennes, échecs, capacités insuffisantes, tests échus et exceptions. Chaque indicateur précise population, période et limites. Les niveaux « tâche exécutée », « donnée récupérée » et « service repris » doivent rester distincts. Un statut inconnu ne doit pas être compté comme conforme.

Une restauration non autorisée, un accès excessif ou un échec ignoré doit être examiné avec les fonctions compétentes. Le responsable doit protéger les données, affecter la correction et vérifier les suites. Ce modèle ne crée aucune sanction automatique. Les réponses doivent respecter règles internes, contrats et obligations applicables, tout en conservant les éléments utiles à l'analyse.

La révision doit suivre incident, test non concluant ou changement de dépendance, identité, clé, fournisseur ou objectif. Auteur, motif, approbateur et version remplacée sont conservés dans [À RENSEIGNER : dépôt, droits, durée]. Les opérateurs et suppléants doivent recevoir les instructions approuvées. L'entreprise doit vérifier restitution et récupération lors d'une sortie de contrat, avant de perdre les moyens techniques nécessaires.

Sources et limites

Le guide ANSSI Sauvegarde des systèmes d'information, version 1.1 du 27 novembre 2025, notamment §2 et R1–R32, traite objectifs, séparation, identités, tests, ordre de reprise et risque des copies compromises. Le NIST SP 800-34 révision 1, publié en 2010, apporte un cadre de planification et de tests à adapter aux technologies actuelles.

Les rôles, tableaux, exemples et critères proposés sont des choix organisationnels, non une garantie d'atteinte des objectifs ni une certification. Les mécanismes du fournisseur, la cohérence applicative, la sûreté et les obligations doivent être vérifiés dans votre environnement. Les besoins peuvent exiger d'autres capacités que la sauvegarde seule.