Politique de réponse aux incidents et plan opérationnel

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

Version du modèle : 3.0. Type : politique et plan d'exécution. Profil proposé : PME d'environ 80 personnes, avec exploitation informatique et surveillance éventuellement externalisées. Ce profil est une hypothèse d'adaptation, non une description de votre entreprise. Les décisions métier, l'acceptation du risque et les communications restent attribuées à des personnes internes nommées.

Après adaptation et adoption, « doit » et les consignes opérationnelles expriment des exigences internes sur le périmètre approuvé. Avant adoption, elles restent des propositions. Le propriétaire doit compléter les paramètres, vérifier les moyens et contrats, obtenir les signatures et diffuser une version contrôlée. Ce modèle ne confère aucun pouvoir supplémentaire et ne garantit ni conformité, ni absence d'incident, ni délai de reprise.

1. Périmètre et décisions d'adoption

La politique couvre les signalements concernant identités, terminaux, réseaux, applications, données, services hébergés et fournisseurs utilisés pour les activités retenues. Le propriétaire doit rapprocher inventaire, contrats et responsables métiers. Les équipements personnels, comptes externes, services non administrés et systèmes industriels doivent avoir une règle explicite : autorisation d'enquête, interlocuteur et limites. Une exclusion ne doit pas devenir une disparition de l'inventaire.

Paramètre	Décision à compléter	Approbateur	Preuve attendue
Entité et activités prioritaires	[À RENSEIGNER : services, sites, données, exclusions]	Direction	Périmètre daté et responsables
Pilote et suppléance	[À RENSEIGNER : titulaires, délégations, contacts]	Direction	Acceptation des rôles
Couverture et fournisseurs	[À RENSEIGNER : horaires assurés, contrats, recours]	Responsable interne	Confirmation et test des contacts
Paramètres de réponse	[À RENSEIGNER : cibles par gravité, suivi, conservation]	Autorités compétentes	Justification locale, sans délai universel
Contrôle documentaire	[À RENSEIGNER : version locale, effet, révision, signatures]	Propriétaire et direction	Version approuvée accessible

Avant la date d'effet, le propriétaire doit vérifier que chaque intervenant connaît ses pouvoirs, que la collecte prévue est possible et que les changements urgents peuvent être autorisés. Si une capacité manque, il doit proposer un périmètre réduit ou une exception explicite. Un contrat de surveillance ne démontre pas une capacité de confinement ou de reconstruction.

Le responsable métier doit décrire le service minimum acceptable et les effets d'une interruption. Cette description doit inclure les dépendances : identité, réseau, prestataire, application et données. Le pilote doit pouvoir retrouver ces informations hors incident. Les paramètres non décidés doivent rester visibles dans un registre d'écarts, avec propriétaire et décision attendue.

2. Responsabilités, décisions et absence

Le pilote interne dirige chaque incident. Le MSSP peut qualifier et enquêter ; l'infogérant peut exécuter les changements. Ces fournisseurs doivent recevoir une mission précise. Ils ne décident pas seuls d'arrêter une activité, de communiquer à un tiers ou d'accepter un risque métier. Une personne peut cumuler des rôles compatibles, mais chaque décision sensible doit garder un responsable identifiable.

Fonction	Pouvoir ou tâche	Limite	Absence
Direction ou délégataire	Activer la crise, arbitrer les interruptions, accepter le risque	Pas de conclusion technique sans éléments	Suppléant nominatif
Pilote interne	Prioriser, affecter, enregistrer les décisions et demander les moyens	Délégations et sûreté	Relève consignée avec le suppléant
Propriétaire métier	Décrire l'impact et valider le service repris	Ne déclare pas seul la compromission éliminée	Responsable de secours désigné
MSSP ou analyste	Fournir faits, hypothèses, périmètre et contrôles	Aucune mesure hors mandat	Escalade contractuelle et relais interne
Infogérant ou exploitant	Exécuter et vérifier les changements autorisés	Aucun effacement improvisé	Autre opérateur habilité ou expertise approuvée
Juridique, protection des données, communication	Examiner obligations et messages	Aucun délai légal déduit du modèle	Conseil de secours et sollicitation tracée

L'annuaire doit distinguer contact opérationnel, escalade fournisseur et décideur interne. Il doit rester accessible si la messagerie, l'annuaire ou le poste habituel est indisponible. Le pilote doit vérifier l'identité d'un intervenant par un moyen indépendant avant de lui accorder un accès. Une personne absente ne doit pas conserver une tâche critique sans transfert accepté.

Le propriétaire doit faire tester la suppléance avant adoption : le remplaçant retrouve la délégation, reçoit un signalement et affecte une tâche sans utiliser le compte personnel du titulaire. Les limites découvertes doivent entraîner une correction ou une décision de risque. Une délégation de remplacement ne doit pas être improvisée à partir d'un message non vérifié.

3. Signalement, qualification et gravité

Toute personne doit pouvoir signaler une activité suspecte par [À RENSEIGNER : canaux et secours]. Le destinataire doit ouvrir un dossier, enregistrer heure et fuseau, déclarant, service, symptôme et actions déjà réalisées. Il ne doit pas demander de mot de passe, code MFA, cookie ou token utilisable. Un message suspect doit être conservé par le canal prévu, sans diffusion ordinaire.

Le pilote doit séparer impact constaté, impact plausible et inconnues. L'analyste doit indiquer les sources consultées et leur couverture temporelle. Un événement observé n'est pas automatiquement un incident ; sa qualification dépend des éléments analysés. L'absence de logs ou d'alerte ne prouve pas l'absence d'activité. Les détails du signalement doivent rester accessibles aux intervenants autorisés.

Niveau proposé	Conditions à apprécier	Décision interne	Preuve et réévaluation
Critique	Propagation plausible, privilèges structurants atteints ou activité essentielle menacée	Direction appelée ; coordination de crise envisagée	Faits, inconnues, périmètre, prochain contrôle
Majeur	Compromission crédible avec impact contenu mais significatif	Pilote mobilise métier, MSSP et exploitation	Mesures et critères d'aggravation
Limité	Signal localisé, impact faible et contrôle plausible	Analyse proportionnée affectée	Justification du périmètre et résultat
Non qualifié	Éléments insuffisants ou contradictoires	Priorité conservatoire décidée ; collecte suivante nommée	Information manquante et réexamen

Cette grille est un choix organisationnel à approuver. Le pilote doit considérer étendue, données, privilèges, dépendances et récupérabilité, plutôt qu'un score isolé. La priorité peut évoluer avec justification. Une atteinte à la sûreté suit les procédures compétentes. Mobilisation et rendez-vous

doivent être fixés localement selon gravité, couverture et moyens financés ; aucune valeur universelle n'est introduite.

Le MSSP doit transmettre un résumé exploitable, pas seulement une alerte : fait observé, source, cible, période, confiance argumentée, inconnues et contrôle proposé. Si le rapport manque d'identifiant ou de périmètre, le pilote doit demander ces éléments et conserver une priorité provisoire. Le manque d'information ne doit pas être transformé en classement sans suite.

4. Activation, canal indépendant et fournisseurs

À l'activation, le pilote doit nommer responsable, suppléant, équipes, canal et prochain rendez-vous. Il doit confirmer qui peut demander une isolation, suspendre un compte, arrêter un service ou engager une expertise. Si le canal ordinaire semble compromis, il doit utiliser le canal indépendant testé. La coordination de secours ne doit pas réintroduire les secrets sur un système suspect.

Chaque demande fournisseur doit préciser référence, cible, action autorisée, exclusions, résultat attendu et moyen de retour. Le pilote doit obtenir une acceptation humaine ou opérationnelle de la tâche, pas seulement un accusé automatique. Il doit vérifier au contrat horaires, droits, traces, sous-traitants et escalade. Une prestation indisponible est une limite de réponse, jamais une action accomplie.

Blocage	Action du pilote	Preuve	Escalade
Fournisseur sans réponse	Utiliser l'escalade et rechercher un relais autorisé	Tentatives et capacité manquante	Direction pour ressources et risque d'attente
Décideur absent	Appeler le suppléant ; mesures préautorisées seulement	Délégation et heure	Autorité interne de secours
Autorisation ambiguë	Faire reformuler objectif, cible et limites	Accord nominatif	Aucun élargissement tacite
Conflit de sûreté	Suspendre l'action et consulter l'exploitant compétent	Motif et protection alternative	Métier et fonction de sûreté

Les accès temporaires accordés à un expert doivent être nominatifs, limités et suivis. Le pilote doit définir leur retrait et demander la restitution des éléments. Les fichiers échangés doivent utiliser un dépôt approuvé. La clôture de mission doit confirmer ce qui a été fait, ce qui manque et qui conserve les traces ; elle ne clôt pas automatiquement l'incident.

5. Confinement et contrôle du résultat

Avant une mesure, le responsable doit préciser menace, bénéfice attendu, effets métier, dépendances et preuves potentiellement perdues. L'opérateur doit recevoir une cible vérifiable, les consignes d'arrêt et le retour possible. Le pilote doit décider si la collecte précède l'action. L'urgence peut justifier de protéger d'abord ; les preuves devenues indisponibles doivent alors être consignées.

Mesure	Entrée et autorité	Exécution et preuve	Résultat manquant
Isolation de terminal	Identifiant confirmé, délégation du pilote	Opérateur isole et contrôle la portée réseau	Confinement non confirmé ; autre contrôle recherché
Restriction de compte	Compte stable, services et impact	Équipe identité agit ; responsables applicatifs vérifient	Aucune conclusion sur tous les accès depuis une seule console
Restriction de service	Dépendances et décision métier	Exploitant applique et teste le mode dégradé	Revoir impact et protection
Protection des sauvegardes	Dépôts et identités connus	Équipe sauvegarde vérifie accès et copie préservée	Capacité de reprise incertaine escaladée

Une commande terminée ou un ticket fermé ne démontre pas l'effet souhaité. Le pilote doit chercher un contrôle indépendant lorsque possible : état réel, test autorisé ou confirmation du propriétaire. Une mesure temporaire doit avoir propriétaire, durée décidée et critère de retrait. Un retour arrière doit être évalué : il peut réouvrir une exposition.

Si le contrôle montre une portée différente, l'opérateur doit arrêter l'élargissement et prévenir le pilote. Celui-ci doit distinguer échec technique, cible incorrecte et limitation de visibilité. Le métier doit être informé de l'impact confirmé. Une protection alternative doit rester autorisée et vérifiable ; l'équipe ne doit pas empiler des mesures dont les effets ne sont plus compris.

6. Enquête, preuve et relève

L'analyste doit établir les questions : accès initial plausible, opérations observées, privilèges touchés, systèmes exposés et étendue inconnue. Il doit séparer heure d'événement, réception et observation, avec les corrections d'horloge explicites. Une relation temporelle ou une adresse partagée ne suffisent pas à attribuer une action à une personne. Toute conclusion doit renvoyer aux éléments et aux limites.

Le dépositaire doit référencer chaque pièce, consigner provenance, collecte, opérateur, accès et transferts, puis contrôler l'intégrité selon la méthode adaptée. Les originaux doivent être protégés ; l'analyse utilise des copies lorsque possible. Exports et captures peuvent contenir des données sensibles. Leur collecte doit rester autorisée et proportionnée, avec stockage et durée justifiés.

Contrôle	Responsable et entrée	Résultat utilisable	Échec à signaler
Recherche de logs	Analyste ; question, source, période	Requête conservée, résultat et couverture	Catégorie absente, expiration, droits insuffisants
Acquisition spécialisée	Expert habilité ; objectif et autorité	Méthode, supports, intégrité, limites	Acquisition impossible ou altération connue
Attribution technique	Analyste et propriétaire de source	Identifiants concordants, contexte historique	Rapprochement seulement supposé
Relève	Pilotes sortant et entrant	Priorités reformulées et actions acceptées	Pièce inaccessible ou responsabilité non reprise

Une hypothèse contredite doit être révisée sans effacer la conclusion précédente. Le pilote conserve le motif du changement. Le dossier distingue « non trouvé dans les sources consultées », « source indisponible » et « activité exclue par un contrôle précis ». Un assistant ou ticket ordinaire ne doit pas recevoir de secrets bruts ou de données dont le partage n'est pas autorisé.

La relève doit couvrir mesures actives, décisions attendues, urgence et prochaine vérification. L'entrant doit vérifier l'accès aux pièces utiles et reformuler ses actions. Si le transfert échoue, le sortant doit nommer le point bloquant au pilote ; une invitation à une réunion ou un lien envoyé ne constitue pas une acceptation de responsabilité.

7. Obligations, communication et décisions externes

Le pilote doit solliciter la fonction compétente lorsque l'incident peut concerner données personnelles, engagements contractuels, activité réglementée ou tiers. Il doit fournir faits, territoire, entités, catégories de données, services, dates et inconnues. Le référent doit documenter applicabilité, destinataires, échéances retenues et point de départ pertinent. Ce modèle n'impose aucun délai de notification universel.

La communication doit séparer constat, mesure et incertitude. Le porte-parole interne valide le public destinataire et le canal avec les fonctions compétentes. Les messages évitent attribution prématurée, garantie de suppression de données ou rétablissement non vérifié. Le pilote conserve version approuvée, destinataires et heure. Une demande externe doit être vérifiée avant transmission d'éléments sensibles.

Le dossier doit enregistrer la décision de notifier ou non, la personne consultée et la prochaine réévaluation si les faits changent. Une absence de décision ne doit pas être présentée comme une

décision négative. Les échanges avec assureur, autorités ou partenaires doivent suivre les habilitations et contrats applicables ; le prestataire technique ne doit pas improviser une position juridique pour l'entreprise.

8. Récupération et clôture conditionnelle

Le pilote prépare avec métier et exploitation une proposition : service minimum, ordre des dépendances, environnement, accès traités, contrôles, tests et conditions d'arrêt. L'accès initial peut rester partiellement incertain ; cette limite exige une décision explicite. Corriger un défaut ne démontre pas la disparition de toute persistance ou de tout accès hostile.

Passage	Preuve attendue	Décideur	Réserve ou rejet
Reconstruction	Administration, dépendances et supports vérifiés	Pilote et exploitant	Moyen suspect non réutilisé sans décision
Reprise pilote	Données et opération métier testées ; surveillance disponible	Métier et pilote	Périmètre limité ou mode dégradé
Élargissement	Résultats du pilote, écarts, risques restants	Autorité de reprise	Suspension si signes suspects
Fin de récupération	Critères atteints, tâches attribuées	Direction ou délégataire	Clôture différée ou risque accepté

L'opérateur vérifie les éléments de restauration avant usage et les services après restauration. Le métier teste une opération représentative, pas seulement l'ouverture d'une page. Le pilote fixe la surveillance renforcée et ses critères de fin. Si un signe suspect réapparaît, il suspend l'élargissement et réévalue ; une nouvelle alerte ne prouve pas à elle seule une récidive.

La clôture doit préciser ce qui est expliqué, ce qui reste incertain et les corrections affectées. Les mesures temporaires et accès experts doivent être retirés ou transférés à un propriétaire durable. Les preuves doivent recevoir une décision de conservation. Le retour d'expérience doit couvrir le dispositif, les contrats et la coordination, sans réduire l'analyse à une erreur supposée d'une personne.

9. Exemple fictif complet

La PME fictive Atelier Rivage emploie environ 80 personnes et externalise l'exploitation. Le MSSP signale une règle de transfert inconnue et une connexion contestée sur un compte de comptabilité. Le responsable administratif devient pilote ; un suppléant reprend la conduite en cas d'absence. Cette organisation illustre une adaptation, sans constituer une expérience client ou un modèle obligatoire.

Moment logique	Fait ou décision fictifs	Responsable	Pièce ou résultat
Signalement	Règle inconnue confirmée ; lien de session inconnu	Analyste MSSP	E-01 export, portée indiquée
Activation	Niveau majeur provisoire ; utilisateur joint par numéro vérifié	Pilote	D-01, canal indépendant
Confinement	Restriction autorisée sur identité et application	Opérateurs mandatés	D-02, deux contrôles ; autre application inconnue
Enquête	Suppression autorisée de la règle ; historique MFA recherché	Infogérant : règle ; MSSP : analyse	E-02, catégorie manquante consignée
Reprise	Accès nécessaire sur terminal vérifié ; surveillance bornée	Métier et pilote	D-03, risque résiduel accepté ; action fournisseur ouverte

L'exercice est accepté si un second intervenant retrouve E-01, distingue connexion reconnue et opération contestée, et explique la réserve sur l'application non vérifiée. Il doit identifier l'autorité de reprise et le prochain contrôle. « MFA présente, dossier clos » ou « mot de passe changé, tous les accès coupés » sont des conclusions refusées dans cet exemple.

10. Annexes et recette d'adoption

Registre vierge	Valeur à adapter	Vérification	Propriétaire
Dossier et périmètre	[À RENSEIGNER : référence, services, période]	Identifiants confirmés	[À RENSEIGNER]
Gravité et inconnues	[À RENSEIGNER : faits, hypothèses, niveau]	Réexamen planifié	[À RENSEIGNER]
Coordination	[À RENSEIGNER : pilote, suppléant, canal, rendez-vous]	Contacts testés	[À RENSEIGNER]
Mesure et autorité	[À RENSEIGNER : cible, accord, résultat]	Effet contrôlé ou réserve	[À RENSEIGNER]
Reprise et clôture	[À RENSEIGNER : critères, risque restant]	Acceptation nominative	[À RENSEIGNER]

☐ Un signalement hors outil habituel atteint une personne responsable.

☐ Le suppléant retrouve la délégation et obtient une acceptation fournisseur.

☐ Une isolation fictive possède cible, accord, effet attendu et contrôle.

☐ Une pièce est retrouvée, une hypothèse contestée et une relève acceptée.

☐ Les obligations sont examinées sans importer un délai d'une autre juridiction.

☐ Le métier peut refuser une reprise aux dépendances non vérifiées.

11. Exceptions, assurance et révision

Toute exception doit identifier exigence, périmètre, risque, compensation, décideur, responsable, expiration et prochain contrôle. Le demandeur explique pourquoi la règle ne peut être appliquée. L'autorité accepte ou refuse explicitement ; le fournisseur ne doit pas accepter un risque métier sans délégation. Une exception expirée doit être corrigée ou réexaminée, jamais renouvelée tacitement.

Le propriétaire examine à [À RENSEIGNER : instance et cadence] incidents sans pilote, actions échues, mesures non vérifiées, lacunes contractuelles et exercices. Chaque écart reçoit responsable et preuve de résolution. Rapidité apparente, qualité d'analyse et récupération doivent être distinguées ; le nombre de dossiers clos ne démontre pas seul l'efficacité du dispositif.

Chaque révision enregistre auteur, motif, approbateur et changements. Le propriétaire conserve décisions et contrôles selon [À RENSEIGNER : dépôt, droits, durée justifiée], diffuse la version approuvée et retire les copies remplacées. L'exercice est rejoué après changement majeur ou échec significatif. Fréquence ordinaire, conservation et cibles de mobilisation restent des paramètres locaux approuvés.

Sources et limites

Le NIST SP 800-61 révision 3, avril 2025 traite rôles, tiers, qualification, preuves et récupération, notamment §2.2 et RS.MA, RS.AN, RS.CO, RC.RP. L'ANSSI, anticiper et gérer une crise cyber distingue conduite stratégique et réponse technique.

Matrices, délégations, exemples et critères ci-dessus sont des choix opérationnels proposés, non des prescriptions universelles de ces sources. Ils doivent être validés avec métiers, fournisseurs et conseils compétents. Le plan ne remplace ni la sûreté, ni la continuité, ni une expertise spécialisée ou une analyse juridique propre à la situation.