

SUPPORT D'AUDIT · HYGIÈNE INFORMATIQUE

Les 42 mesures du Guide d'hygiène informatique de l'ANSSI

Chaque mesure expliquée, ses points de contrôle au niveau standard et renforcé, les preuves à demander et une case de statut. Pour mener un audit ou une auto-évaluation, puis bâtir le plan d'action.

42

mesures, en 10 thèmes

39

mesures au niveau standard

22

mesures au niveau renforcé

Comment s'en servir

- 1 Faire l'état des lieux** avec l'outil de suivi (pages suivantes) : pour chaque mesure, le niveau standard est-il atteint ? Puis, le cas échéant, le niveau renforcé ?
- 2 Justifier chaque réponse** avec la fiche de la mesure : points de contrôle à cocher, preuves à demander, constat.
- 3 Traiter d'abord le niveau standard.** Les mesures où il n'est pas atteint forment le premier plan d'action. Quand un référentiel de l'ANSSI renvoie au guide, c'est ce niveau qui est attendu, sauf mention contraire.
- 4 Viser ensuite le niveau renforcé**, une fois le standard atteint partout.

Lire les cases



Case vide : le niveau existe pour la mesure.
Cochez-la quand il est atteint.



Case hachurée : l'ANSSI ne définit pas ce niveau pour la mesure. Rien à évaluer.

Statut dans les fiches : **atteint** (tous les points vérifiés, preuve à l'appui), **partiel**, **non atteint**, ou **sans objet** (la mesure ne s'applique pas au périmètre, à justifier).

Audit

Entité

Périmètre audité

Interlocuteurs

Auditeur

Date(s)

Outil de suivi

Le tableau de l'ANSSI, mesure par mesure. Cochez la case quand le niveau est atteint ; les cases hachurées sont sans objet.

I Sensibiliser et former		STANDARD	RENFORCÉ	OBSERVATIONS
1	Former les équipes opérationnelles à la sécurité des systèmes d'information			
2	Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique			
3	Maîtriser les risques de l'infogérance			
II Connaître le système d'information		STANDARD	RENFORCÉ	OBSERVATIONS
4	Identifier les informations et serveurs les plus sensibles et maintenir un schéma du réseau			
5	Disposer d'un inventaire exhaustif des comptes privilégiés et le maintenir à jour			
6	Organiser les procédures d'arrivée, de départ et de changement de fonction des utilisateurs			
7	Autoriser la connexion au réseau de l'entité aux seuls équipements maîtrisés			
III Authentifier et contrôler les accès		STANDARD	RENFORCÉ	OBSERVATIONS
8	Identifier nommément chaque personne accédant au système et distinguer les rôles utilisateur/administrateur			
9	Attribuer les bons droits sur les ressources sensibles du système d'information			
10	Définir et vérifier des règles de choix et de dimensionnement des mots de passe			
11	Protéger les mots de passe stockés sur les systèmes			
12	Changer les éléments d'authentification par défaut sur les équipements et services			
13	Privilégier lorsque c'est possible une authentification forte			

IV Sécuriser les postes		STANDARD	RENFORCÉ	OBSERVATIONS
14	Mettre en place un niveau de sécurité minimal sur l'ensemble du parc informatique			
15	Se protéger des menaces relatives à l'utilisation de supports amovibles			
16	Utiliser un outil de gestion centralisée afin d'homogénéiser les politiques de sécurité			
17	Activer et configurer le pare-feu local des postes de travail			
18	Chiffrer les données sensibles transmises par voie Internet			

V Sécuriser le réseau		STANDARD	RENFORCÉ	OBSERVATIONS
19	Segmenter le réseau et mettre en place un cloisonnement entre ces zones			
20	S'assurer de la sécurité des réseaux d'accès Wi-Fi et de la séparation des usages			
21	Utiliser des protocoles sécurisés dès qu'ils existent			
22	Mettre en place une passerelle d'accès sécurisé à Internet			
23	Cloisonner les services visibles depuis Internet du reste du système d'information			
24	Protéger sa messagerie professionnelle			
25	Sécuriser les interconnexions réseau dédiées avec les partenaires			
26	Contrôler et protéger l'accès aux salles serveurs et aux locaux techniques			

VI Sécuriser l'administration		STANDARD	RENFORCÉ	OBSERVATIONS
27	Interdire l'accès à Internet depuis les postes ou serveurs utilisés pour l'administration du système d'information			
28	Utiliser un réseau dédié et cloisonné pour l'administration du système d'information			
29	Limiter au strict besoin opérationnel les droits d'administration sur les postes de travail			

VII Gérer le nomadisme		STANDARD	RENFORCÉ	OBSERVATIONS
30	Prendre des mesures de sécurisation physique des terminaux nomades			
31	Chiffrer les données sensibles, en particulier sur le matériel potentiellement perdable			
32	Sécuriser la connexion réseau des postes utilisés en situation de nomadisme			
33	Adopter des politiques de sécurité dédiées aux terminaux mobiles			

VIII Maintenir à jour le système d'information		STANDARD	RENFORCÉ	OBSERVATIONS
34	Définir une politique de mise à jour des composants du système d'information			
35	Anticiper la fin de la maintenance des logiciels et systèmes et limiter les adhérences logicielles			

IX Superviser, auditer, réagir		STANDARD	RENFORCÉ	OBSERVATIONS
36	Activer et configurer les journaux des composants les plus importants			
37	Définir et appliquer une politique de sauvegarde des composants critiques			
38	Procéder à des contrôles et audits de sécurité réguliers puis appliquer les actions correctives associées			
39	Désigner un référent en sécurité des systèmes d'information et le faire connaître auprès du personnel			
40	Définir une procédure de gestion des incidents de sécurité			

X Pour aller plus loin		STANDARD	RENFORCÉ	OBSERVATIONS
41	Mener une analyse de risques formelle			
42	Privilégier l'usage de produits et de services qualifiés par l'ANSSI			

Les 42 mesures, une par une

Pour chaque mesure : ce qu'elle protège, ce qu'il faut vérifier à chaque niveau, les preuves à demander, puis le statut et le constat.

I SENSIBILISER ET FORMER

1

Former les équipes opérationnelles à la sécurité des systèmes d'information

STANDARD

L'enjeu. Administrateurs, développeurs, chefs de projet et responsable sécurité ont des accès privilégiés : une mauvaise pratique de leur part (compte trop puissant, mot de passe faible, compte personnel utilisé pour un service) ouvre une faille.

POINTS DE CONTRÔLE · NIVEAU STANDARD

- ☐ Formation sécurité à la prise de poste, puis à intervalles réguliers.
- ☐ Programme couvrant législation, risques et menaces, maintien en condition de sécurité, authentification, durcissement, cloisonnement et journalisation.
- ☐ Contenu adapté au métier (développement sécurisé, intégration de la sécurité dans les projets, référentiels pour le responsable sécurité).
- ☐ Clauses de formation régulière à la sécurité dans les contrats des prestataires et infogérants.

Preuves à demander : Plan de formation et attestations des deux dernières années · Clauses des contrats d'infogérance

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____

2

Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique

STANDARD

RENFORCÉ

L'enjeu. Chaque utilisateur est un maillon de la chaîne : il doit connaître, dès son arrivée, les enjeux, les règles et les bons réflexes.

POINTS DE CONTRÔLE · NIVEAU STANDARD

- ☐ Sensibilisation dès l'arrivée, puis régulière et adaptée aux publics.
- ☐ Sujets couverts : enjeux de l'entité, informations sensibles, obligations légales, règles du quotidien (pas d'équipement personnel sur le réseau, pas de partage ni de réutilisation des mots de passe, signalement des événements suspects).
- ☐ Moyens présentés : verrouillage de session, outil de protection des mots de passe.

POINTS DE CONTRÔLE · NIVEAU RENFORCÉ

- ☐ Charte informatique rédigée, diffusée et signée par les utilisateurs.

Preuves à demander : Supports et calendrier de sensibilisation · Charte informatique et preuves de signature

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Renforcé ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____



3

Maîtriser les risques de l'infogérance

STANDARD

L'enjeu. Externaliser tout ou partie du système d'information crée des risques propres (actions à distance, hébergement mutualisé, contrat incomplet) qu'il faut traiter dès la rédaction des exigences.

POINTS DE CONTRÔLE · NIVEAU STANDARD

- ☐ Risques de l'infogérance évalués avant le choix du prestataire.
- ☐ Exigences imposées au contrat : réversibilité, droit d'audit, sauvegarde et restitution des données dans un format ouvert, maintien du niveau de sécurité dans le temps.
- ☐ Plan d'assurance sécurité (PAS) fourni par le prestataire.
- ☐ Pas de traitement d'informations sensibles sur des outils non maîtrisés.

Preuves à demander : Contrats d'infogérance et annexes sécurité · Plan d'assurance sécurité

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____

II CONNAÎTRE LE SYSTÈME D'INFORMATION

4

Identifier les informations et serveurs les plus sensibles et maintenir un schéma du réseau

STANDARD

L'enjeu. On ne protège bien que ce que l'on connaît : données sensibles, serveurs qui les portent et chemins réseau qui y mènent.

POINTS DE CONTRÔLE · NIVEAU STANDARD

- ☐ Liste des données sensibles (savoir-faire, données personnelles, contrats...) et des composants qui les hébergent.
- ☐ Schéma du réseau à jour : zones IP et plan d'adressage, équipements de routage et de sécurité, interconnexions avec l'extérieur et les partenaires.
- ☐ Serveurs sensibles localisés sur le schéma.

Preuves à demander : Inventaire des données et serveurs sensibles · Schéma réseau daté

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____



5

Disposer d'un inventaire exhaustif des comptes privilégiés et le maintenir à jour

STANDARD

L'enjeu. Les comptes à privilèges sont la première cible d'un attaquant : il faut savoir lesquels existent et qui les détient.

POINTS DE CONTRÔLE · NIVEAU STANDARD

- ☐ Inventaire des comptes administrateurs et des comptes aux droits supérieurs à ceux d'un utilisateur standard.
- ☐ Comptes pouvant lire les répertoires des responsables ou de tous les utilisateurs recensés.
- ☐ Utilisateurs de postes non administrés par le service informatique recensés.
- ☐ Revue périodique des comptes ; nomenclature claire des comptes de service et d'administration.

Preuves à demander : Inventaire des comptes privilégiés · Compte rendu de la dernière revue

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____

6

Organiser les procédures d'arrivée, de départ et de changement de fonction des utilisateurs

STANDARD

RENFORCÉ

L'enjeu. Les droits doivent suivre les mouvements de personnel : un départ ou un changement de poste qui laisse des accès ouverts est une porte dérobée.

POINTS DE CONTRÔLE · NIVEAU STANDARD

- ☐ Procédures définies avec les ressources humaines.
- ☐ Couvrent : création et suppression des comptes et boîtes aux lettres, droits ajoutés ou retirés au changement de fonction, badges et clés, équipements mobiles, transfert et changement des mots de passe.
- ☐ Tous les droits révoqués au départ.

POINTS DE CONTRÔLE · NIVEAU RENFORCÉ

- ☐ Procédures formalisées par écrit et mises à jour selon le contexte.

Preuves à demander : Procédures arrivée / départ / mutation · Échantillon de départs récents et date de clôture des comptes

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Renforcé ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____



7

Autoriser la connexion au réseau de l'entité aux seuls équipements maîtrisés

STANDARD

RENFORCÉ

L'enjeu. Chaque équipement connecté est un point d'entrée ; un appareil personnel ou de visiteur échappe au contrôle de l'entité.

POINTS DE CONTRÔLE - NIVEAU STANDARD

- ☐ Seuls les terminaux maîtrisés par l'entité se connectent aux réseaux, filaires ou sans fil.
- ☐ Solution prévue pour les appareils personnels et visiteurs (par exemple un Wi-Fi dédié, séparé).

POINTS DE CONTRÔLE - NIVEAU RENFORCÉ

- ☐ Authentification des postes sur le réseau (802.1X ou équivalent).

Preuves à demander : Règle d'accès au réseau · Configuration du Wi-Fi invités · Configuration 802.1X le cas échéant

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Renforcé ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____

III AUTHENTIFIER ET CONTRÔLER LES ACCÈS

8

Identifier nommément chaque personne accédant au système et distinguer les rôles utilisateur/administrateur

STANDARD

RENFORCÉ

L'enjeu. Un compte nominatif permet d'attribuer une action et de repérer un compte compromis ; séparer le compte d'administration limite l'exposition des privilèges.

POINTS DE CONTRÔLE - NIVEAU STANDARD

- ☐ Comptes nominatifs ; comptes génériques marginaux et rattachés à un petit nombre de personnes.
- ☐ Comptes génériques et de service gérés au moins aussi strictement que les comptes nominatifs.
- ☐ Chaque administrateur dispose d'un compte d'administration distinct, avec un secret différent, utilisé seulement pour administrer et depuis un environnement dédié.

POINTS DE CONTRÔLE - NIVEAU RENFORCÉ

- ☐ Journalisation des connexions réussies et échouées des comptes.

Preuves à demander : Extrait de l'annuaire (comptes génériques, comptes d'administration) · Paramètres d'audit des connexions

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Renforcé ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____

9

Attribuer les bons droits sur les ressources sensibles du système d'information

STANDARD

L'enjeu. Répertoires sensibles, bases de données et boîtes aux lettres sont précieux pour un attaquant : leur accès doit être restreint à qui en a besoin.

POINTS DE CONTRÔLE · NIVEAU STANDARD

- ☐ Liste des ressources sensibles et, pour chacune, la population autorisée.
- ☐ Accès contrôlé : utilisateur authentifié et membre de la population autorisée.
- ☐ Pas de copie dans des emplacements moins protégés (exports de configuration, documentation technique, bases métier).
- ☐ Revue régulière des droits d'accès.

Preuves à demander : Matrice des droits sur les ressources sensibles · Compte rendu de revue des droits

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____

10

Définir et vérifier des règles de choix et de dimensionnement des mots de passe

STANDARD

L'enjeu. Un mot de passe facile à deviner ou réutilisé d'un service à l'autre, en particulier entre messagerie personnelle et professionnelle, ouvre l'accès.

POINTS DE CONTRÔLE · NIVEAU STANDARD

- ☐ Règles de choix et de longueur des mots de passe définies et expliquées aux utilisateurs.
- ☐ Blocage des comptes après plusieurs échecs de connexion.
- ☐ Connexions anonymes désactivées.
- ☐ Robustesse des mots de passe auditée avec un outil.

Preuves à demander : Politique de mots de passe · Paramètres de verrouillage · Résultat du dernier audit de robustesse

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____

11 Protéger les mots de passe stockés sur les systèmes

STANDARD

L'enjeu. Post-it, fichier de mots de passe, courriel à soi-même ou mémorisation dans le navigateur : autant de cibles pour un attaquant.

POINTS DE CONTRÔLE · NIVEAU STANDARD

- ☐ Coffre-fort de mots de passe fourni et utilisé.
- ☐ Mots de passe stockés chiffrés ; aucun en clair (papier, fichier, courriel).
- ☐ Mot de passe maître robuste, mémorisé par l'utilisateur.

Preuves à demander : Outil de coffre-fort déployé · Constat sur poste (fichiers, navigateur) par échantillon

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____

12 Changer les éléments d'authentification par défaut sur les équipements et services

STANDARD

RENFORCÉ

L'enjeu. Les identifiants par défaut sont connus des attaquants, même s'ils ne sont pas publics.

POINTS DE CONTRÔLE · NIVEAU STANDARD

- ☐ Identifiants et mots de passe par défaut changés dès l'installation.
- ☐ Nouveaux mots de passe conformes aux règles des mesures 10 et 11.
- ☐ Identifiant impossible à changer (secret « en dur ») signalé au fournisseur.

POINTS DE CONTRÔLE · NIVEAU RENFORCÉ

- ☐ Renouvellement régulier des éléments d'authentification changés.

Preuves à demander : Procédure de mise en service des équipements · Contrôle par échantillon (imprimantes, bornes Wi-Fi, interfaces d'administration)

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Renforcé ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____

13

Privilégier lorsque c'est possible une authentification forte

STANDARD

RENFORCÉ

L'enjeu. Un mot de passe seul se vole ; un second facteur rend le vol inutile.

POINTS DE CONTRÔLE - NIVEAU STANDARD

- ☐ Authentification à deux facteurs différents : ce que je sais, ce que je possède, ce que je suis.

POINTS DE CONTRÔLE - NIVEAU RENFORCÉ

- ☐ Carte à puce privilégiée ou, à défaut, mot de passe à usage unique avec jeton physique.

Preuves à demander : Couverture de l'authentification forte (part des comptes, accès concernés) · Méthodes autorisées

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Renforcé ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____

IV SÉCURISER LES POSTES

14

Mettre en place un niveau de sécurité minimal sur l'ensemble du parc informatique

STANDARD

RENFORCÉ

L'enjeu. L'utilisateur est souvent la porte d'entrée : chaque équipement (postes, serveurs, imprimantes, téléphones) doit atteindre un socle commun.

POINTS DE CONTRÔLE - NIVEAU STANDARD

- ☐ Applications et modules de navigateur limités au nécessaire.
- ☐ Pare-feu local et antivirus sur les postes.
- ☐ Partitions de données utilisateur chiffrées.
- ☐ Exécution automatique (autorun) désactivée.
- ☐ Postes en dérogation (impossible à mettre à jour) isolés du reste du système.

POINTS DE CONTRÔLE - NIVEAU RENFORCÉ

- ☐ Données vitales sauvegardées régulièrement sur des supports déconnectés, restauration vérifiée périodiquement.

Preuves à demander : Configuration de référence des postes · État de chiffrement et d'antivirus du parc · Liste des dérogations

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Renforcé ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____

15

Se protéger des menaces relatives à l'utilisation de supports amovibles

STANDARD

RENFORCÉ

L'enjeu. Clés USB et disques externes propagent des codes malveillants et emportent des données.

POINTS DE CONTRÔLE - NIVEAU STANDARD

- ☐ Risques des supports amovibles traités et expliqués aux utilisateurs.
- ☐ Branchement de clés inconnues proscrit ; clés non maîtrisées analysées par l'antivirus avant usage.

POINTS DE CONTRÔLE - NIVEAU RENFORCÉ

- ☐ Exécution de programmes depuis les supports amovibles interdite (AppLocker, montage noexec).
- ☐ Procédure de mise au rebut, jusqu'à la destruction sécurisée.

Preuves à demander : Règle d'usage des supports amovibles · Stratégie de restriction logicielle · Procédure de destruction

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Renforcé ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____

16

Utiliser un outil de gestion centralisée afin d'homogénéiser les politiques de sécurité

STANDARD

L'enjeu. La sécurité vaut celle du maillon le plus faible : les politiques doivent s'appliquer partout, vite, depuis un point central.

POINTS DE CONTRÔLE - NIVEAU STANDARD

- ☐ Outil de gestion centralisée (par exemple Active Directory, Intune) couvrant le plus d'équipements possible, postes et serveurs.
- ☐ Politiques de sécurité (mots de passe, navigateurs, restrictions de connexion, durcissement) déployées depuis cet outil.
- ☐ Capacité à reconfigurer rapidement le parc en cas de crise.

Preuves à demander : Taux d'équipements gérés · Liste des stratégies de sécurité appliquées

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____



17

Activer et configurer le pare-feu local des postes de travail

STANDARD

RENFORCÉ

L'enjeu. Un attaquant qui contrôle un poste cherche à rebondir vers les autres ; les flux de poste à poste sont rares en bureautique.

POINTS DE CONTRÔLE · NIVEAU STANDARD☐ Pare-feu local activé sur tous les postes de travail.**POINTS DE CONTRÔLE · NIVEAU RENFORCÉ**

- ☐ Ports d'administration des postes (TCP 135, 445, 3389 ; 22 sous Unix) bloqués, sauf depuis les ressources identifiées.
- ☐ Flux entrants bloqués par défaut, liste blanche des seuls flux nécessaires.
- ☐ Flux bloqués journalisés.

Preuves à demander : Stratégie de pare-feu déployée · Règles entrantes autorisées · Exemple de journal des flux bloqués

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Renforcé ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____

18

Chiffrer les données sensibles transmises par voie Internet

STANDARD

L'enjeu. Sur Internet, on ne maîtrise pas le trajet des données : un courriel ou un dépôt dans le cloud peut être intercepté.

POINTS DE CONTRÔLE · NIVEAU STANDARD

- ☐ Données sensibles chiffrées avant envoi par courriel ou dépôt en ligne.
- ☐ Secret de déchiffrement transmis par un autre canal (en main propre, par téléphone).

Preuves à demander : Outil de chiffrement mis à disposition · Consigne d'envoi des données sensibles

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____

V SÉCURISER LE RÉSEAU

19 Segmenter le réseau et mettre en place un cloisonnement entre ces zones

STANDARD

L'enjeu. Sur un réseau « à plat », la compromission d'un poste met en péril toutes les machines, jusqu'aux serveurs critiques.

POINTS DE CONTRÔLE · NIVEAU STANDARD

- ☐ Réseau découpé en zones aux besoins de sécurité homogènes (serveurs d'infrastructure, serveurs métier, postes utilisateurs, postes d'administration, téléphonie...).
- ☐ Zones séparées par VLAN et sous-réseaux, filtrage entre zones par pare-feu.
- ☐ Flux d'administration cloisonnés en priorité.
- ☐ À défaut, cloisonnement prévu à chaque extension ou renouvellement du réseau.

Preuves à demander : Schéma des zones · Matrice des flux entre zones · Règles du pare-feu interne

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____

20 S'assurer de la sécurité des réseaux d'accès Wi-Fi et de la séparation des usages

STANDARD

L'enjeu. Le Wi-Fi déborde des locaux et ses réglages par défaut sont faibles : une intrusion par radio doit rester contenue.

POINTS DE CONTRÔLE · NIVEAU STANDARD

- ☐ Flux venant du Wi-Fi filtrés et limités au nécessaire.
- ☐ Chiffrement robuste (WPA2 avec AES-CCMP au minimum) et authentification centralisée, si possible par certificat machine.
- ☐ Pas de mot de passe unique partagé ; à défaut, complexe, renouvelé, jamais diffusé à des tiers.
- ☐ Bornes administrées de façon sécurisée (interface dédiée, mot de passe par défaut changé).
- ☐ Wi-Fi personnel et visiteurs séparé de celui de l'entité (SSID, VLAN, accès Internet distincts).

Preuves à demander : Configuration des SSID · Mode de chiffrement et d'authentification · Règles de filtrage du Wi-Fi

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____



21

Utiliser des protocoles sécurisés dès qu'ils existent

STANDARD

L'enjeu. Beaucoup de protocoles historiques circulent en clair ; leurs versions sécurisées existent.

POINTS DE CONTRÔLE - NIVEAU STANDARD

- ☐ Protocoles chiffrés utilisés sur Internet comme sur le réseau interne (HTTPS, IMAPS, SMTPS, POP3S...).
- ☐ SSH à la place de Telnet et RLOGIN.

Preuves à demander : Relevé des services et des protocoles utilisés

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____

22

Mettre en place une passerelle d'accès sécurisé à Internet

STANDARD

RENFORCÉ

L'enjeu. Les terminaux ne doivent pas accéder directement à Internet : sites piégés, fichiers malveillants et fuites passent par là.

POINTS DE CONTRÔLE - NIVEAU STANDARD

- ☐ Pare-feu au plus près de l'accès Internet.
- ☐ Serveur mandataire (proxy) qui authentifie les utilisateurs et journalise les requêtes.

POINTS DE CONTRÔLE - NIVEAU RENFORCÉ

- ☐ Analyse antivirus des contenus et filtrage par catégories d'URL.
- ☐ Procédures de maintien en condition de sécurité de la passerelle ; redondance selon le besoin.
- ☐ Résolution DNS publique directe désactivée sur les postes, déléguée au mandataire.
- ☐ Postes nomades connectés d'abord au système d'information pour naviguer à travers la passerelle.

Preuves à demander : Architecture de la sortie Internet · Configuration du mandataire · Exemple de journal

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Renforcé ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____

23

Cloisonner les services visibles depuis Internet du reste du système d'information

STANDARD

L'enjeu. Un site web ou un serveur de messagerie hébergé en interne est attaqué en continu ; sa compromission ne doit pas ouvrir le reste du système.

POINTS DE CONTRÔLE · NIVEAU STANDARD

- ☐ Services exposés administrés par des personnes compétentes et disponibles, sinon hébergement externalisé.
- ☐ Infrastructure d'hébergement Internet physiquement séparée du reste du système.
- ☐ Flux de ces services filtrés à part ; flux entrants via un mandataire inverse (reverse proxy).

Preuves à demander : Liste des services exposés · Schéma de la zone exposée (DMZ) · Configuration du mandataire inverse

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____

24

Protéger sa messagerie professionnelle

STANDARD

RENFORCÉ

L'enjeu. La messagerie est le premier vecteur d'infection : pièces jointes piégées, liens malveillants, fraude au virement.

POINTS DE CONTRÔLE · NIVEAU STANDARD

- ☐ Utilisateurs sensibilisés à l'hameçonnage ; vérification par un autre canal en cas de doute.
- ☐ Mesures organisationnelles contre la fraude (validation des virements).
- ☐ Redirection vers une messagerie personnelle interdite ; accès distant sécurisé proposé.
- ☐ Analyse antivirus en amont des boîtes aux lettres.
- ☐ Chiffrement TLS entre serveurs de messagerie et entre postes et serveurs.

POINTS DE CONTRÔLE · NIVEAU RENFORCÉ

- ☐ Serveurs de boîtes aux lettres non exposés directement, relais dédié en coupure d'Internet.
- ☐ Service anti-spam.
- ☐ Enregistrements DNS de messagerie configurés (MX, SPF, DKIM, DMARC).

Preuves à demander : Règles de transfert externe · Configuration antivirus et anti-spam · Enregistrements SPF, DKIM, DMARC

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Renforcé ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____

25

Sécuriser les interconnexions réseau dédiées avec les partenaires

STANDARD

RENFORCÉ

L'enjeu. Un lien direct avec un fournisseur ou un client fait entrer son niveau de sécurité dans le vôtre : le partenaire est réputé non sûr.

POINTS DE CONTRÔLE - NIVEAU STANDARD

- ☐ Liaison par Internet protégée par un tunnel site à site, de préférence IPsec.
- ☐ Filtrage IP par pare-feu au plus près de l'entrée des flux.
- ☐ Matrice des flux réduite au besoin, tenue à jour, et configuration qui la respecte.

POINTS DE CONTRÔLE - NIVEAU RENFORCÉ

- ☐ Équipement de filtrage dédié aux connexions partenaires.
- ☐ Détection d'intrusion sur ces flux.
- ☐ Contact à jour chez le partenaire pour réagir en cas d'incident.

Preuves à demander : Liste des interconnexions · Matrice des flux partenaires · Contacts sécurité des partenaires

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Renforcé ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____

26

Contrôler et protéger l'accès aux salles serveurs et aux locaux techniques

STANDARD

L'enjeu. Un accès physique contourne la plupart des protections logiques.

POINTS DE CONTRÔLE - NIVEAU STANDARD

- ☐ Salles serveurs et locaux techniques fermés par serrure ou badge.
- ☐ Prestataires accompagnés, sauf accès strictement tracé et limité dans le temps.
- ☐ Revue régulière des droits d'accès ; retrait des droits ou changement des codes au départ d'une personne ou d'un prestataire.
- ☐ Prises réseau des zones ouvertes au public désactivées ou restreintes.

Preuves à demander : Liste des personnes habilitées · Journal des accès · État des prises réseau en zones publiques

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____

VI SÉCURISER L'ADMINISTRATION

27 Interdire l'accès à Internet depuis les postes ou serveurs utilisés pour l'administration du système d'information

STANDARD

RENFORCÉ

L'enjeu. Naviguer ou lire ses courriels depuis un poste d'administration expose directement les privilèges les plus élevés.

POINTS DE CONTRÔLE - NIVEAU STANDARD

- ☐ Aucun accès Internet depuis les postes et serveurs d'administration.
- ☐ Poste distinct (ou bureautique virtualisée distante) pour les usages Internet des administrateurs.
- ☐ Pas d'accès à l'administration depuis un poste bureautique.

POINTS DE CONTRÔLE - NIVEAU RENFORCÉ

- ☐ Mises à jour récupérées depuis une source sûre, contrôlées puis transférées vers l'environnement d'administration (support dédié ou zone d'échange).

Preuves à demander : Règles de filtrage des postes d'administration · Procédure de transfert des mises à jour

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Renforcé ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____

28 Utiliser un réseau dédié et cloisonné pour l'administration du système d'information

STANDARD

RENFORCÉ

L'enjeu. Sans réseau d'administration séparé, un poste utilisateur compromis peut rebondir vers les interfaces d'administration.

POINTS DE CONTRÔLE - NIVEAU STANDARD

- ☐ Réseau d'administration cloisonné du réseau bureautique.
- ☐ Au minimum par VLAN ; mieux, par tunnels IPsec (cloisonnement logique chiffré).

POINTS DE CONTRÔLE - NIVEAU RENFORCÉ

- ☐ Cloisonnement physique du réseau d'administration.

Preuves à demander : Schéma du réseau d'administration · Mode de cloisonnement retenu

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Renforcé ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____



29

Limiter au strict besoin opérationnel les droits d'administration sur les postes de travail

STANDARD

L'enjeu. Un utilisateur administrateur de son poste donne à tout code malveillant qu'il exécute les mêmes droits.

POINTS DE CONTRÔLE - NIVEAU STANDARD

- ☐ Aucun utilisateur administrateur de son poste, quelle que soit sa position.
- ☐ Magasin d'applications validées pour répondre aux besoins.
- ☐ Droits d'administration des postes réservés aux administrateurs, pendant leurs interventions.
- ☐ Délégation ponctuelle tracée, limitée dans le temps et retirée à échéance.

Preuves à demander : Membres du groupe Administrateurs local (échantillon) · Registre des délégations

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____

VII GÉRER LE NOMADISME

30

Prendre des mesures de sécurisation physique des terminaux nomades

STANDARD

RENFORCÉ

L'enjeu. Portables, tablettes et téléphones se perdent et se volent ; ils contiennent des données et ouvrent l'accès au système.

POINTS DE CONTRÔLE - NIVEAU STANDARD

- ☐ Utilisateurs sensibilisés à la vigilance en déplacement.
- ☐ Terminaux banalisés (aucune marque de l'entité).
- ☐ Filtre de confidentialité sur les écrans.

POINTS DE CONTRÔLE - NIVEAU RENFORCÉ

- ☐ Secrets de déchiffrement ou d'authentification sur un support externe (carte à puce, jeton USB) conservé à part.

Preuves à demander : Consignes aux voyageurs · Dotation en filtres de confidentialité

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Renforcé ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____



31

Chiffrer les données sensibles, en particulier sur le matériel potentiellement perdable

STANDARD

L'enjeu. Un matériel perdu ne doit rien livrer : seules des données chiffrées y sont stockées.

POINTS DE CONTRÔLE · NIVEAU STANDARD

- ☐ Données chiffrées sur tout matériel nomade : portables, téléphones, clés USB, disques externes.
- ☐ Chiffrement complet du disque en priorité, puis archives ou fichiers selon le besoin.
- ☐ Secret de déchiffrement unique et robuste.

Preuves à demander : État du chiffrement des portables et téléphones · Règle pour les supports amovibles

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____

32

Sécuriser la connexion réseau des postes utilisés en situation de nomadisme

STANDARD

RENFORCÉ

L'enjeu. En déplacement, la connexion au système d'information traverse Internet et des réseaux non maîtrisés.

POINTS DE CONTRÔLE · NIVEAU STANDARD

- ☐ Tunnel VPN, de préférence IPsec, vers une passerelle de l'entité.
- ☐ Tunnel établi automatiquement et non désactivable : aucun flux hors du tunnel.
- ☐ Exception encadrée pour les portails captifs (ou partage de connexion d'un téléphone de confiance).

POINTS DE CONTRÔLE · NIVEAU RENFORCÉ

- ☐ Authentification forte pour le VPN (certificat sur carte à puce ou jeton, ou mot de passe à usage unique).

Preuves à demander : Configuration du client VPN · Mode d'authentification au VPN

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Renforcé ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____



33

Adopter des politiques de sécurité dédiées aux terminaux mobiles

STANDARD

RENFORCÉ

L'enjeu. Téléphones et tablettes mêlent souvent vie personnelle et professionnelle et portent courriels, fichiers et contacts.

POINTS DE CONTRÔLE · NIVEAU STANDARD

- ☐ Usages personnels et professionnels non mutualisés sur un même terminal.
- ☐ Gestion centralisée des terminaux mobiles (MDM) privilégiée : déverrouillage imposé, applications validées.
- ☐ À défaut, terminal configuré avant remise et utilisateur sensibilisé.

POINTS DE CONTRÔLE · NIVEAU RENFORCÉ

- ☐ Assistant vocal intégré désactivé.

Preuves à demander : Politique MDM · Taux de terminaux gérés

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Renforcé ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____

VIII MAINTENIR À JOUR LE SYSTÈME D'INFORMATION

34

Définir une politique de mise à jour des composants du système d'information

STANDARD

L'enjeu. Chaque faille publiée devient une porte d'entrée ; l'ANSSI demande d'appliquer les correctifs dans le mois qui suit leur publication.

POINTS DE CONTRÔLE · NIVEAU STANDARD

- ☐ Veille sur les vulnérabilités (CERT-FR, éditeurs).
- ☐ Correctifs de sécurité appliqués dans le mois suivant leur publication.
- ☐ Politique déclinée en procédures : inventaire des composants, sources d'information, outils de déploiement, qualification et déploiement progressif.
- ☐ Composants obsolètes isolés (filtrage réseau strict, secrets dédiés).

Preuves à demander : Politique de mise à jour · Rapport de conformité des correctifs · Liste des composants obsolètes isolés

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____



35

Anticiper la fin de la maintenance des logiciels et systèmes et limiter les adhérences logicielles

STANDARD

L'enjeu. Un logiciel hors support ne reçoit plus de correctifs : ses failles restent ouvertes.

POINTS DE CONTRÔLE - NIVEAU STANDARD

- ☐ Inventaire des systèmes et applications avec leurs dates de fin de support.
- ☐ Solutions choisies avec un support couvrant leur durée d'utilisation ; parc homogène.
- ☐ Dépendances entre logiciels limitées.
- ☐ Clauses de suivi des correctifs et d'obsolescence dans les contrats.
- ☐ Délais et ressources de migration identifiés pour chaque logiciel en fin de vie.

Preuves à demander : Inventaire logiciel avec fins de support · Plan de migration des composants en fin de vie

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____

IX SUPERVISER, AUDITER, RÉAGIR

36

Activer et configurer les journaux des composants les plus importants

STANDARD

RENFORCÉ

L'enjeu. Sans journaux, on ne détecte pas une tentative d'accès et on ne reconstitue pas un incident.

POINTS DE CONTRÔLE - NIVEAU STANDARD

- ☐ Composants critiques identifiés : équipements réseau et de sécurité, serveurs critiques, postes sensibles.
- ☐ Journalisés au minimum : paquets bloqués par les pare-feu, authentifications et autorisations (succès et échecs), arrêts inopinés, erreurs de protocole, flux aux interconnexions.
- ☐ Événements de sécurité conservés au moins un an (plus si la réglementation l'impose).
- ☐ Même source de temps (NTP) pour tous les composants.

POINTS DE CONTRÔLE - NIVEAU RENFORCÉ

- ☐ Journaux centralisés sur un dispositif dédié : recherche automatisée, archivage long, traces protégées de l'effacement.

Preuves à demander : Liste des sources journalisées · Durée de conservation · Configuration NTP · Outil de centralisation le cas échéant

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Renforcé ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____



37

Définir et appliquer une politique de sauvegarde des composants critiques

STANDARD

RENFORCÉ

L'enjeu. Après un incident ou une intrusion, des sauvegardes saines et conservées en lieu sûr conditionnent la reprise de l'activité.

POINTS DE CONTRÔLE · NIVEAU STANDARD

- ☐ Politique de sauvegarde formalisée et tenue à jour.
- ☐ Contenu : données vitales et serveurs concernés, types de sauvegarde (dont hors ligne), fréquence, procédure d'exécution, stockage et restrictions d'accès, tests de restauration, destruction des supports.
- ☐ Restaurations testées (systématiques, ponctuelles ou générales).

POINTS DE CONTRÔLE · NIVEAU RENFORCÉ

- ☐ Exercice de restauration au moins une fois par an, avec une trace des résultats.

Preuves à demander : Politique de sauvegarde · Preuve d'une copie hors ligne · Compte rendu du dernier test de restauration

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Renforcé ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____

38

Procéder à des contrôles et audits de sécurité réguliers puis appliquer les actions correctives associées

RENFORCÉ

L'enjeu. Un audit mesure l'écart entre la règle et la pratique ; il révèle des failles sans jamais prouver leur absence.

POINTS DE CONTRÔLE · NIVEAU RENFORCÉ

- ☐ Audit du système d'information au moins une fois par an, interne ou par une société spécialisée.
- ☐ Audits techniques et organisationnels selon le périmètre.
- ☐ Actions correctives identifiées, planifiées et suivies à intervalles réguliers.
- ☐ Indicateurs d'avancement remontés à la direction.

Preuves à demander : Rapports des derniers audits · Plan d'action et son état d'avancement

Renforcé ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____



39

Désigner un référent en sécurité des systèmes d'information et le faire connaître auprès du personnel

STANDARD

L'enjeu. Les utilisateurs doivent savoir à qui s'adresser ; la sécurité a besoin d'un responsable soutenu par la direction.

POINTS DE CONTRÔLE · NIVEAU STANDARD

- ☐ Référent sécurité désigné et soutenu par la direction.
- ☐ Connu de tous les utilisateurs.
- ☐ Missions : définir les règles, vérifier leur application, sensibiliser et planifier la formation, centraliser et traiter les incidents.
- ☐ Référent formé à la sécurité et à la gestion de crise.

Preuves à demander : Lettre de désignation · Communication interne · Formations suivies

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____

40

Définir une procédure de gestion des incidents de sécurité

STANDARD

L'enjeu. Une mauvaise réaction aggrave un incident et efface les traces utiles à l'analyse.

POINTS DE CONTRÔLE · NIVEAU STANDARD

- ☐ Signes d'alerte connus (connexion impossible, activité inhabituelle, alertes antivirus répétées...).
- ☐ Bon réflexe : déconnecter la machine du réseau sans l'éteindre ni la redémarrer, puis prévenir la hiérarchie et le référent sécurité.
- ☐ Recours prévu à un prestataire de réponse aux incidents (PRIS).
- ☐ Éradication, changement des mots de passe compromis, registre centralisé des incidents, dépôt de plainte possible.

Preuves à demander : Procédure de gestion des incidents · Registre des incidents · Contact du prestataire de réponse aux incidents

Standard ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____

X POUR ALLER PLUS LOIN

41 Mener une analyse de risques formelle

RENFORCÉ

L'enjeu. Chaque mesure a un coût : l'analyse de risques vérifie qu'elle réduit au bon niveau un risque identifié.

POINTS DE CONTRÔLE · NIVEAU RENFORCÉ

- ☐ Démarche formalisée : contexte, appréciation des risques (vraisemblance, gravité), traitement.
- ☐ Plan de traitement des risques validé au plus haut niveau.
- ☐ Méthode dédiée, EBIOS Risk Manager recommandée par l'ANSSI.

Preuves à demander : Analyse de risques datée · Plan de traitement validé par la direction

Renforcé ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____

42 Privilégier l'usage de produits et de services qualifiés par l'ANSSI

RENFORCÉ

L'enjeu. La qualification de l'ANSSI atteste une évaluation approfondie, technique et organisationnelle, du produit ou du prestataire.

POINTS DE CONTRÔLE · NIVEAU RENFORCÉ

- ☐ Produits qualifiés privilégiés dans les achats de sécurité.
- ☐ Prestataires qualifiés privilégiés : audit (PASSI), réponse aux incidents (PRIS), détection (PDIS), cloud (SecNumCloud).

Preuves à demander : Politique d'achat · Liste des produits et prestataires de sécurité utilisés, avec leur qualification

Renforcé ☐ Atteint ☐ Partiel ☐ Non atteint ☐ Sans objet

Constat _____

Synthèse

Nombre de mesures atteintes par thème, à reporter depuis l'outil de suivi.

N°	Thème	Standard atteint	Renforcé atteint
I	Sensibiliser et former	____ / 3	____ / 1
II	Connaître le système d'information	____ / 4	____ / 2
III	Authentifier et contrôler les accès	____ / 6	____ / 3
IV	Sécuriser les postes	____ / 5	____ / 3
V	Sécuriser le réseau	____ / 8	____ / 3
VI	Sécuriser l'administration	____ / 3	____ / 2
VII	Gérer le nomadisme	____ / 4	____ / 3
VIII	Maintenir à jour le système d'information	____ / 2	—
IX	Superviser, auditer, réagir	____ / 4	____ / 3
X	Pour aller plus loin	—	____ / 2
	Total	____ / 39	____ / 22

Plan d'action

D'abord les mesures dont le niveau standard n'est pas atteint.

Mesure	Action	Responsable	Échéance	Priorité

Faire l'état des lieux avec nous

Une heure d'entretien gratuit avec un expert DMC DEFENSE pour situer votre organisation et repérer les écarts prioritaires.

Demander un audit gratuit

dmc-defense.com/fr/contact

Source : ANSSI, Guide d'hygiène informatique, version 2.0, septembre 2017 (Licence Ouverte Etalab). Titres des mesures repris du guide ; explications et points de contrôle rédigés par DMC DEFENSE. Document d'information, non contractuel. Guide complet : messervices.cyber.gouv.fr/documents-guides/guide_hygiene_informatique_anssi.pdf