**Hygiène informatique - Grille de suivi**

| Règle | Échéance | État | | |
|---|---|---|---|---|
| | | Réalisé | En cours | Planifié |
| **1) Disposer d'une cartographie précise de l'installation informatique et la maintenir à jour.** | | | | |
| 1.1) Établir la liste des briques matérielles et logicielles utilisées. | | | | |
| 1.2) Établir un schéma d'architecture réseau sur laquelle sont identifiés les points névralgiques (connexions externes, serveur hébergeant des données et/ou des fonctions sensibles, etc.). | | | | |
| **2) Disposer d'un inventaire exhaustif des comptes privilégiés et le maintenir à jour.** | | | | |
| 2.1) Établir la liste des utilisateurs qui disposent d'un compte administrateur sur le système d'information. | | | | |
| 2.2) Établir la liste des utilisateurs qui disposent de privilèges suffisants pour lire la messagerie des dirigeants de la société. | | | | |
| 2.3) Établir la liste des utilisateurs qui disposent de privilèges suffisants pour lire la messagerie de l'ensemble des utilisateurs | | | | |
| 2.4) Établir la liste des utilisateurs qui disposent de privilèges suffisants pour accéder aux répertoires de travail des dirigeants. | | | | |
| 2.5) Établir la liste des utilisateurs qui disposent de privilèges suffisants pour accéder aux répertoires de l'ensemble des utilisateurs. | | | | |
| 2.6) Établir la liste des utilisateurs qui disposent d'un poste non administré par le service informatique. | | | | |
| **3) Rédiger des procédures d'arrivée et de départ des utilisateurs (personnel, stagiaires, etc.).** | | | | |
| 3.1) Décrire les mécanismes de gestion (création/destruction) des comptes informatiques et l'attribution des droits associés à ses comptes sur le système d'information, y compris pour les partenaires et les prestataires externes. | | | | |
| 3.2) Décrire les mécanismes de gestion du contrôle d'accès aux locaux. | | | | |
| 3.3) Décrire les mécanismes de gestion des équipements mobiles. | | | | |
| 3.4) Décrire les mécanismes de gestion du contrôle des habilitations. | | | | |
| **4) Limiter le nombre d'accès internet au strict nécessaire.** | | | | |
| 4.1) Identifier l'ensemble des accès internet existants. | | | | |
| 4.2) Mutualiser au maximum ces accès en les mettant à niveau du point de vue de la sécurité. | | | | |
| 4.3) Surveiller les accès de manière centralisée et permanente. | | | | |

**Hygiène informatique - Grille de suivi**

| Règle | Échéance | État | | |
|---|---|---|---|---|
| | | Réalisé | En cours | Planifié |
| 4.4) Pour chaque accès à Internet, utiliser des passerelles d'interconnexion sécurisées. | | | | |
| **5) Interdire la connexion d'équipements personnels au système d'information de l'entreprise.** | | | | |
| 5.1) Si le travail à distance est nécessaire, fournir des moyens professionnels pour permettre de tels usages. | | | | |
| 5.2) Sécuriser plus particulièrement ces moyens et leur mode d'accès au système d'information de l'entreprise. | | | | |
| **6) Connaître les modalités de mises à jour de l'ensemble des composants logiciels utilisés.** | | | | |
| 6.1) Recenser l'ensemble des composants de base du système d'information. | | | | |
| 6.2) Pour chacun, définir leur criticité dans le système d'information. | | | | |
| 6.3) Identifier les technologies innovantes non encore maîtrisées en interne. | | | | |
| 6.4) Remplacer ces technologies par celles sous maîtrise interne ou acquérir les compétences. | | | | |
| **7) Se tenir informé des vulnérabilités de ces composants et des mises à jour nécessaires.** | | | | |
| 7.1) Élaborer la liste des différentes sources (éditeurs, CERTs) diffusant les vulnérabilités des composants du système d'information. | | | | |
| 7.2) Indiquer ceux susceptibles de diffuser de correctifs en précisant les modalités pratiques. | | | | |
| **8) Définir une politique simple de mise à jour et l'appliquer strictement.** | | | | |
| 8.1) En fonction du niveau de criticité de chaque composant dans le système d'information, définir précisément pour chacun sa fréquence de mise à jour. | | | | |
| 8.2) Identifier les différents acteurs responsables des mises à jour. | | | | |
| 8.3) Mettre en œuvre une plateforme de test représentative du système d'information. | | | | |
| 8.4) Définir un plan de qualification des correctifs afin de vérifier les non-régressions fonctionnelles du système d'information et des applications métier qu'il héberge. | | | | |
| **9) Identifier nominativement chaque personne ayant accès au système.** | | | | |
| 9.1) Mettre en œuvre un processus d'enrôlement des utilisateurs dans le système d'information. | | | | |
| 9.2) Mettre en œuvre un processus de suppression de compte à chaque départ d'un utilisateur. | | | | |
| **10) Respecter les bonnes pratiques de choix et de dimensionnement des mots de passe.** | | | | |
| 10.1) Proscrire la réutilisation de mots de passe (a fortiori la réutilisation de mots de passe privés pour des usages professionnels et vice versa). | | | | |
| 10.2) Déterminer une taille de mot de passe minimale à respecter. Une taille de douze caractères est un bon choix en l'absence d'analyse. | | | | |

**Hygiène informatique - Grille de suivi**

| Règle | Échéance | État | | |
|---|---|---|---|---|
| | | Réalisé | En cours | Planifié |
| 10.3) Proscrire les mots de passe liés aux identités des utilisateurs (mot de passe composé d'un nom de société, d'une date de naissance, etc.). | | | | |
| 10.4) Ne jamais autoriser un tiers à générer un mot de passe pour votre entité. | | | | |
| 10.5) Renouvelez vos mots de passe avec une fréquence raisonnable. Une fréquence de 90 jours est un bon compromis pour les systèmes contenant des données sensibles. | | | | |
| 10.6) Modifier systématiquement les mots de passe par défaut. | | | | |
| | | | | |
| **11) Mettre en place des moyens techniques permettant de faire respecter les règles relatives aux mots de passe** | | | | |
| 11.1) Bloquer les comptes dont le mot de passe n'a pas été changé depuis 6 mois. | | | | |
| 11.2) Imposer techniquement de bonnes règles de constitution de mot de passe. | | | | |
| 11.3) Rendre impossible techniquement la saisie d'un nouveau mot de passe semblable aux 5 derniers mots de passe saisis. | | | | |
| | | | | |
| **12) Ne pas conserver les mots de passe sur les systèmes informatiques.** | | | | |
| 12.1) Ne pas autoriser les utilisateurs ou les administrateurs à stocker les mots de passe dans un fichier sur un poste informatique particulièrement exposé au risque (ex. : en ligne sur Internet). | | | | |
| 12.2) Ne pas autoriser les utilisateurs à s'adresser leurs propres mots de passe sur leur messagerie personnelle. | | | | |
| 12.3) Configurez les logiciels, y compris les navigateurs web, pour qu'ils ne se « souviennent » pas des mots de passe choisis. | | | | |
| | | | | |
| **13) Supprimer ou modifier systématiquement les éléments d'authentification par défaut (mots de passe, certificats) sur les équipements (commutateurs réseau, routeurs, serveurs, imprimantes).** | | | | |
| 13.1) Modifier les éléments d'authentification par défaut des équipements (commutateurs réseau, routeurs, serveurs, imprimantes) à chaque installation. | | | | |
| 13.2) Définir la fréquence de renouvellement de ces mots de passe pour chaque type d'équipement. | | | | |
| 13.3) Mettre en œuvre des dispositifs de contrôle permettant de s'assurer que ces mots de passe sont régulièrement modifiés. | | | | |
| | | | | |
| **14) Privilégier lorsque c'est possible une authentification forte par carte à puce.** | | | | |
| 14.1) Idéalement, utiliser des certificats stockés sur la carte à puce pour s'authentifier aux applications sensibles. | | | | |
| 14.2) Formaliser le processus permettant de garantir que l'utilisateur d'une carte à puce en est bien le propriétaire. | | | | |

**Hygiène informatique - Grille de suivi**

| Règle | Échéance | État | | |
|---|---|---|---|---|
| | | Réalisé | En cours | Planifié |
| **15) Mettre en place un niveau de sécurité homogène sur l'ensemble du système d'information.** | | | | |
| 15.1) Désactiver les services applicatifs inutiles. | | | | |
| 15.2) Restreindre les privilèges utilisateurs. | | | | |
| **16) Interdire techniquement la connexion des supports amovibles.** | | | | |
| 16.1) A minima désactiver l'exécution des autoruns depuis des supports amovibles. | | | | |
| **17) Utiliser un outil de gestion de parc permettant de déployer des politiques de sécurité et les mises à jour sur les équipements.** | | | | |
| 17.1) Mettre en œuvre des solutions permettant d'appliquer de manière centralisée les politiques de sécurité et les mises à jour. | | | | |
| 17.2) Paramétrer ces solutions pour que le déploiement soit le plus automatisé. | | | | |
| **18) Gérer les terminaux nomades selon la même politique de sécurité que les postes fixes.** | | | | |
| 18.1) Identifier l'ensemble des terminaux nomades. | | | | |
| 18.2) Mettre en œuvre sur ces terminaux une politique de sécurité identique à celle des postes fixes. | | | | |
| **19) Maîtriser les connexions à distance sur les postes clients.** | | | | |
| 19.1) Toute opération de téléassistance doit s'effectuer dans le contexte de l'utilisateur, avec ses droits, et sans que son mot de passe ne soit communiqué au téléassistant. | | | | |
| 19.2) La téléassistance du poste de travail doit s'effectuer de manière visuelle par affichage partagé entre l'utilisateur et le téléassistant. L'utilisateur doit être en mesure de voir les opérations effectuées par le téléassistant. | | | | |
| 19.3) L'opération de téléassistance sur le poste de travail de l'utilisateur doit respecter le consentement de ce dernier. Elle ne doit être possible que suite à l'acceptation explicite de l'utilisateur (dans le cas d'une offre d'assistance) ou à l'initiative de ce dernier (demande d'assistance). Toute connexion arbitraire à un poste de travail utilisateur par un téléassistant doit être impossible. | | | | |
| 19.4) L'authentification des téléassistants sur les postes distants doit idéalement être réalisée à l'aide de certificats individuels délivrés par une IGC de confiance (ou bien à l'aide de tickets Kerberos délivrés suite à une authentification par certificat individuel par exemple). | | | | |
| 19.5) L'offre d'assistance, lorsqu'elle est utilisée, ne doit être possible que par des téléassistants dûment autorisés à le faire. Cette restriction pourrait par exemple consister en une liste blanche de groupes ou de comptes utilisateurs autorisés à offrir une téléassistance. | | | | |

| Règle | Échéance | État | | |
|---|---|---|---|---|
| | | Réalisé | En cours | Planifié |
| 19.6) Dans le cadre d'une offre de téléassistance, l'utilisateur téléassisté doit être en mesure de vérifier l'identité du téléassistant qui lui est présentée préalablement à toute acceptation. L'identité de ce dernier peut être prouvée par exemple par la présentation d'un certificat X509 ou du compte Active directory utilisé. | | | | |
| 19.7) La solution de téléassistance doit se présenter sous la forme d'une application pouvant être démarrée par l'utilisateur plutôt qu'un service lancé automatiquement au démarrage du poste de travail. | | | | |
| 19.8) Les postes de téléassistance doivent être dédiés à ces opérations, isolés d'Internet et, en permanence à jour de leurs correctifs de sécurité. | | | | |
| 19.9) La solution de téléassistance doit reposer sur des protocoles sécurisés, les mécanismes de sécurité implémentés doivent permettre :<br>- une authentification mutuelle entre les postes de téléassistant et téléassisté ;<br>- un échange de clés de session éphémères à la manière de TLS ;<br>- une protection contre le rejeu ou les attaques de type « man in the middle ». | | | | |
| 19.11) La téléassistance ne doit pouvoir être opérée que depuis des adresses IP sources bien identifiées comme étant celles des postes des téléassistants. Des mesures de sécurité au niveau du réseau doivent donc être mises en œuvre. | | | | |
| 19.12) L'ensemble des opérations de téléassistance effectuées doit être journalisé, idéalement en les distinguant de toute autre action effectuée sur le poste de travail. | | | | |
| **20) Chiffrer les données sensibles, en particulier sur les postes nomades et les supports perdables.** | | | | |
| **21) Auditer ou faire auditer fréquemment la configuration de l'annuaire central (active directory en environnement Windows).** | | | | |
| 21.1) Vérifier l'absence de compte dormant. | | | | |
| 21.2) S'assurer de l'attribution d'un compte individuel par utilisateur du SI. | | | | |
| 21.3) Lister les autres types objets gérés par l'annuaire. | | | | |
| 21.4) Identifier les droits (lecture, écriture) définis pour chaque type d'objet qui ne seraient pas justifiés. | | | | |
| **22) Ne pas mettre en place de réseau non cloisonné.** | | | | |
| 22.1) Pour les postes ou les serveurs contenant des informations importantes pour la vie de l'entreprise, créer un sous-réseau protégé par une passerelle spécifique. | | | | |
| **23) Interdire la navigation sur internet depuis les comptes d'administration.** | | | | |
| **24) Pour chaque accès à Internet, utiliser des passerelles d'interconnexion sécurisées.** | | | | |
| 24.1) Identifier les flux autorisés à traverser la passerelle et en déduire son architecture. | | | | |

**Hygiène informatique - Grille de suivi**

| Règle | Échéance | État | | |
|---|---|---|---|---|
| | | Réalisé | En cours | Planifié |
| 24.2) Disposer d'une politique de mise à jour la plus efficace et rapide possible pour l'ensemble des composants de la passerelle. | | | | |
| 24.3) Superviser en temps réel la passerelle et analyser les alertes. Toute connexion non prévue entre deux équipements doit être considérée comme une possible tentative d'attaque. | | | | |
| 24.4) Ne pas utiliser le protocole DNS pour résoudre les noms de machine au sein de la passerelle. Les machines doivent communiquer au niveau IP par la seule connaissance de leurs adresses respectives. | | | | |
| 24.5) Proscrire l'utilisation du protocole ARP dans la passerelle et configurer les associations adresses Ethernet et adresses IP en dur sur chaque machine. | | | | |
| 24.6) Diversifier les technologies utilisées dans la passerelle dans la limite de la maintenabilité du parc. | | | | |
| **25) Vérifier qu'aucun équipement du réseau ne comporte d'interface d'administration accessible depuis l'internet.** | | | | |
| **26) Éviter l'usage de technologies sans fil (Wifi).** | | | | |
| 26.1) Si de telles technologies doivent être employées, la segmentation de l'architecture réseau doit permettre de limiter les conséquences d'une intrusion depuis la voie radio à un périmètre déterminé. | | | | |
| 26.2) Avoir recours à un chiffrement des réseaux Wifi reposant sur WPA Entreprise (EAP-TLS avec chiffrement WPA2 CCMP). | | | | |
| **27) Définir concrètement les objectifs de la supervision des systèmes et des réseaux.** | | | | |
| 27.1) Générer une alerte pour toute connexion d'un utilisateur hors de ses horaires habituels de travail. | | | | |
| 27.2) Générer une alerte pour tout transfert massif de données vers l'extérieur de l'entreprise. | | | | |
| 27.3) Générer une alerte pour toutes tentatives de connexions successives ou répétées sur un service. | | | | |
| **28) Déterminer les mécanismes de journalisation devant être activés.** | | | | |
| 28.1) Définir également les procédures de vérification de ces journaux qui permettront de générer une alerte dès lors que l'un des objectifs prioritaires n'est pas rempli. | | | | |
| **29) Utiliser un réseau dédié à l'administration des équipements ou au moins un réseau logiquement séparé du réseau des utilisateurs.** | | | | |
| 29.1) Le cloisonnement logique doit idéalement reposer sur un tunnel Ipsec, | | | | |

**Hygiène informatique - Grille de suivi**

| Règle | Échéance | État | | |
|---|---|---|---|---|
| | | Réalisé | En cours | Planifié |
| **30) Ne pas donner aux utilisateurs de privilège d'administration. Ne faire aucune exception.** | | | | |
| **31) N'autoriser l'accès à distance au réseau professionnel, y compris pour l'administration, que depuis des postes professionnels mettant en œuvre des mécanismes d'authentification forte et protégeant l'intégrité et la confidentialité des échanges à l'aide de moyens robustes (privilégier ceux qui sont qualifiés par l'ANSSI).** | | | | |
| 31.1) Privilégier pour cela des moyens robustes qualifiés par l'ANSSI. | | | | |
| **32) Utiliser impérativement des mécanismes de contrôle d'accès aux locaux robustes.** | | | | |
| **33) Gérer rigoureusement les clés permettant l'accès aux locaux et les codes d'alarme.** | | | | |
| 33.1) Récupérer systématiquement les clés ou les badges d'un employé à son départ définitif de l'entreprise. | | | | |
| 33.2) Changer fréquemment les codes de l'alarme de l'entreprise. | | | | |
| 33.3) Ne jamais donner de clé ou de code d'alarme à des prestataires extérieurs (agents de ménage, etc.), sauf s'il est possible de tracer ces accès et de les restreindre techniquement à des plages données. | | | | |
| **34) Ne pas laisser de prise d'accès au réseau interne accessibles dans les endroits publics.** | | | | |
| 34.1) Ne pas laisser des imprimantes ou photocopieurs multifonctions connectés au réseau dans un couloir. | | | | |
| 34.2) Sécuriser les connexions réseau des écrans d'affichage diffusant des flux d'information. | | | | |
| 34.3) Contrôler l'utilisation des prises réseau dans une salle de conférence. | | | | |
| **35) Définir des règles en matière de gestion des impressions papier.** | | | | |
| 35.1) Détruire en fin de journée les documents oubliés sur l'imprimante ou la photocopieuse. | | | | |
| 35.2) Broyer les documents plutôt que de les mettre à la corbeille à papier. | | | | |
| **36) Ne jamais se contenter de traiter l'infection d'une machine sans tenter de savoir si le code malveillant a pu se propager ailleurs dans le réseau.** | | | | |
| **37) Disposer d'un plan de reprise ou de continuité d'activité informatique tenu régulièrement à jour.** | | | | |
| 37.1) Analyser les conséquences sur l'activité d'une perte de l'accès à internet pendant deux jours. | | | | |
| 37.2) Analyser l'impact d'une perte des données stockées sur les serveurs. | | | | |
| 37.3) Analyser l'impact d'une perte des données stockées sur les postes utilisateurs. | | | | |
| **38) Mettre en place une chaîne d'alerte connue de tous les intervenants.** | | | | |

**Hygiène informatique - Grille de suivi**

| Règle | Échéance | État | | |
|---|---|---|---|---|
| | | Réalisé | En cours | Planifié |
| 38.1) Pour chaque utilisateur, lui communiquer les coordonnées de la personne à avertir en cas d'incident sur le système d'information (dysfonctionnement, ralentissement, etc.). | | | | |
| **39) Sensibiliser les utilisateurs aux règles d'hygiène informatique qui les concernent.** | | | | |
| 39.1) Chaque utilisateur doit se voir rappeler tous les ans que les données stockées sur les serveurs. | | | | |
| 39.2) Chaque utilisateur doit se voir rappeler tous les ans que la sécurité de ces informations repose entre autres sur l'exemplarité de leur comportement et le respect des règles élémentaires d'hygiène informatique (non-contournement de la politique de sécurité, verrouillage de la session lorsque l'utilisateur quitte sa position informatique, non-connexion d'équipements personnels au réseau de l'entreprise, non-divulgation d'authentifiant à un tiers, signalement des événements suspects). | | | | |
| **40) Faire réaliser des audits de sécurité périodiques (au minimum tous les ans). Chaque audit doit être associé à un plan d'action.** | | | | |