Axe : 8 - Protection des données

Objectif : RGPD : R1 - Réaliser un état des lieux et mettre en place une organisation projet

Critère	Réponse	Commentaire
Etre sensibilisé à la protection des données et comprendre ses enjeux (consulter le guide RGPD)	Oui	
Identifier les flux de données à caractère personnel utilisées par votre structure (nature, emplacement, logiciel, prestataire, ...) ainsi que le responsable de la collecte de ces données dans votre structure. Ce document vous servira ensuite de tableau de suivi général.	En cours	recensement terminé
Recenser les mesures de sécurité à mettre en place en remplissant la partie Diagnostic de sécurité de ce référentiel (SECURITE)	Non renseigné	
Désigner un pilote pour mettre en oeuvre la gouvernance des données personnelles de votre structure	Non renseigné	
Etablir un plan d'actions prévisionnel en lien avec les personnes concernées	Non renseigné	

Objectif : RGPD : R2 - Cartographier vos traitements de données personnelles

Critère	Réponse	Commentaire
Recenser les traitements sur des données à caractère personnel avec l'aide des responsables de la collecte de ces données (utiliser la fiche traitement prévue à cet effet ou télécharger les traitements déjà identifiés par d'autres établissements)	Non	
S'assurer que les sous-traitants existants et futurs sont conformes aux exigences du RGPD contractuellement et par le biais de contrôles	Oui	
Analyser les risques d'impact sur la protection des données	Oui	

Objectif : RGPD : R3 - Prioriser les actions à mener

Critère	Réponse	Commentaire
Prévoir les modalités d'exercice des droits des personnes concernées par les traitements identifiés(droit d'accès, de rectification, droit à la portabilité, retrait du consentement...)	Non renseigné	
Respecter les règles de sécurité qui permettent de protéger vos données personnelles (voir chapitre SECURITE)	Oui	
Valider et tester les procédures permettant de répondre aux demandes d'exercice des droits des personnes prévus par le RGPD. En particulier droits d'accès, de rectification, de suppression des données de droit à l'oubli, de droit à la portabilité ou de limitation de traitement	Oui	

Objectif : RGPD : R4 - Documenter les procédures mises en place

Critère	Réponse	Commentaire
Les documents prouvant votre conformité sont enregistrés dans le coffre-fort. En effet, pour prouver sa conformité RGPD en cas de contrôle, il faut justifier d'une documentation précise et détaillée de tous les points évoqués précédemment : quels sont les traitements, comment sont collectées les données, comment sont-elles sécurisées, quels risques existent, quels sont les processus mis en place, etc...	Oui	
La procédure en cas de contrôle de la CNIL a été communiquée aux personnes concernées (accueil, standard, DPD, ...)	Oui	

Objectif : SECURITE : S01 - Sensibiliser les utilisateurs

Critère	Réponse	Commentaire

Sensibiliser le personnel travaillant sur des données à caractère personnel aux risques liés aux libertés et à la vie privée	En cours
Documenter vos procédures d'exploitation. Concrètement, toute action sur un traitement de données à caractère personnel, qu'il s'agissed'opérations d'administration ou de la simple utilisation d'une application, doit être expliquée dans unlangage clair et adapté à chaque catégorie d'utilisateurs, dans des documents auxquels ces derniers peuventse référer.	Non
Annexer une charte informatique au règlement intérieur	Non
Porter une mention visible et explicite sur chaque page des documents papier ou électroniques qui contiennent des données sensibles	Non
Prévoir la signature d'un engagement de confidentialité	Non renseigné
Organiser des séances de formation et de sensibilisation à la sécurité de l'information	Non renseigné

Objectif : SECURITE : S02 - Authentifier les utilisateurs

Critère	Réponse	Commentaire
Définissez-vous un identifiant (login) unique à chaque utilisateur ? (et interdire les comptes partagés entre plusieurs utilisateurs.Dans le cas où l'utilisation d'identifiants génériques ou partagés est incontournable, exiger une validationde la hiérarchie et mettre en œuvre des moyens pour les tracer)	Non renseigné	
Adoptez-vous une politique de mot de passe utilisateur rigoureuse ?	Non renseigné	
Obligez-vous l'utilisateur à changer son mot de passe après réinitialisation?	Non renseigné	
Limitez-vous le nombre de tentatives d'accès aux comptes utilisateurs sur les postes de travail et bloquez-vous temporairement le compte lorsque la limite est atteinte ?	Non renseigné	

limite est atteinte ?	
Imposez-vous un renouvellement du mot de passe selon une périodicité pertinente et raisonnable.	Non renseigné

Objectif : SECURITE : S03 - Gérer les habilitations

Critère	Réponse	Commentaire
Réaliser une revue annuelle des habilitations. (afin d'identifier et de supprimer les comptes non utilisés et deréaligner les droits accordés sur les fonctions de chaque utilisateur)	Non renseigné	
Établir régulièrement une politique de contrôle d'accès (documentation, réexamen) ?	Non renseigné	
Définir des profils d'habilitation dans vos applications. (dans les systèmes en séparant les tâches et les domaines de responsabilité,afin de limiter l'accès des utilisateurs aux seules données strictement nécessaires à l'accomplissement deleurs missions)	Non renseigné	
Supprimer les permissions d'accès obsolètes. (dès qu'ils ne sont plus habilités à accéder à un local ouà une ressource informatique, ainsi qu'à la fin de leur contrat)	Non renseigné	

Objectif : SECURITE : S04 - Tracer les accès et gérer les incidents

Critère	Réponse	Commentaire
Tenir un système de journalisation. (c'est-à-dire un enregistrement dans des « fichiers journaux »ou « logs ») des activités des utilisateurs, des anomalies et des événements liés à la sécurité)	Non renseigné	
Examiner périodiquement les journaux d'événements pour y détecter d'éventuelles anomalies	Non renseigné	

Informer tous les utilisateurs de la mise en place du système de journalisation. (après information et consultation des représentants du personnel)	Non renseigné
Protéger les équipements de journalisation et les informations journalisées	Non renseigné
Notifier les personnes concernées des accès frauduleux à leurs données. (pour qu'elles puissent en limiter les conséquences)	Non renseigné

Objectif : SECURITE : S05 - Sécuriser les postes de travail

Critère	Réponse	Commentaire
Prévoir un mécanisme de verrouillage automatique de session en cas de non-utilisation du poste pendant un temps donné	Non renseigné	
Utiliser des systèmes d'exploitation à jour	Non renseigné	
Limiter les accès administrateurs	Non renseigné	
Mettre à jour les applications lorsque des failles critiques ont été identifiées et corrigées	Non renseigné	
Diffuser à tous les utilisateurs la conduite à tenir et la liste des personnes à contacter en cas d'incident de sécurité ou de survenance d'un événement inhabituel touchant aux systèmes d'information et de communication de l'organisme	Non renseigné	
Installer un «pare-feu» (firewall) logiciel sur les postes (et limiter l'ouverture des ports de communication à ceuxstrictement nécessaires au bon fonctionnement des applications installées sur le poste de travail)	Non renseigné	
Utiliser des antivirus régulièrement mis à jour et prévoir une politique de mise à jour régulière des logiciels	Non renseigné	

Favoriser le stockage des données des utilisateurs sur un espace de stockage régulièrement sauvegardé accessible via le réseau de l'organisme plutôt que sur les postes de travail. Dans le cas où des données sont stockées localement, fournir des moyens de synchronisation ou de sauvegarde aux utilisateurs et les former à leur utilisation	Non renseigné
Limiter la connexion de supports mobiles (clés USB, disques durs externes, etc.) à l'indispensable	Non renseigné
Interdire l'exécution d'applications téléchargées ne provenant pas de sources sûres	Non renseigné
Désactiver l'exécution automatique (« autorun ») depuis des supports amovibles	Non renseigné
Limiter l'usage d'applications nécessitant des droits de niveau administrateur pour leur exécution	Non renseigné
Effacer de façon sécurisée les données présentes sur un poste préalablement à sa réaffectation à une autre personne	Non renseigné
Effectuer une veille de sécurité sur les logiciels et matériels utilisés dans le système d'information del'organisme	Non renseigné
Pour l'assistance sur les postes de travail, les outils d'administration à distance doivent recueillir l'accord de l'utilisateur avant toute intervention sur son poste, par exemple en répondant à un message s'affichant à l'écran. L'utilisateur doit également pouvoir constater si la prise de main à distance est en cours et quand elle se termine, par exemple grâce à l'affichage d'un message à l'écran.	Non renseigné
Limiter le nombre de tentatives d'accès à un compte	Non renseigné
Installer les mises à jour critiques des systèmes d'exploitation sans délai en programmant une vérification automatique hebdomadaire	Non renseigné

Objectif : SECURITE : S06 - Sécuriser l'informatique mobile

Critère	Réponse	Commentaire
Prévoir des mécanismes de protection contre le vol (par ex. câble de sécurité, marquage visible du matériel) et de limitation de ses impacts (par ex. verrouillage automatique, chiffrement)	Non renseigné	
Mettre en œuvre des mécanismes maîtrisés de sauvegardes ou de synchronisation des postes nomades, pourse prémunir contre la disparition des données stockées	Non renseigné	
Prévoir des moyens de chiffrement des postes nomades et supports de stockage mobiles (ordinateur portable, clés USB, disque dur externes, CD-R, DVD-RW, etc.)	Non renseigné	
Concernant les smartphones, en plus du code PIN de la carte SIM, activer le verrouillage automatique du terminal et exiger un secret pour le déverrouiller (mot de passe, schéma, etc.)	Non renseigné	
Positionner un filtre de confidentialité sur les écrans des postes utilisés dans des lieux publics	Non renseigné	
Sensibiliser les utilisateurs aux risques spécifiques liés à l'utilisation d'outils informatiques mobiles (ex : volde matériel) et aux procédures prévues pour les limiter	Non renseigné	
Limiter le stockage des données sur les postes nomades au strict nécessaire, et éventuellement l'interdire lors de déplacement à l'étranger (voir le « Passeport de conseils aux voyageurs » publié par l'ANSSI	Non renseigné	
Lorsque des appareils mobiles servent à la collecte de données en itinérance (ex : assistants personnels, smartphones, ordinateurs portables, etc.), chiffrer les données sur le terminal. Prévoir aussi un verrouillage de l'appareil au bout de quelques minutes d'inactivité et la purge des données collectées sitôt qu'elles ont été transférées au système d'information de l'organisme.	Non renseigné	

Objectif : SECURITE : S07 - Protéger le réseau informatique interne

Critère	Réponse	Commentaire
Limiter les accès Internet en bloquant les services non nécessaires (VoIP, pair à pair, etc.)	Non renseigné	
Imposer un VPN pour l'accès à distance ainsi que, si possible, une authentification forte de l'utilisateur (carte à puce, boitier générateur de mots de passe à usage unique (OTP), etc.)	Non renseigné	
Gérer les réseaux Wi-Fi. Ils doivent utiliser un chiffrement à l'état de l'art (WPA2 ou WPA2-PSK avec un mot de passe complexe) et les réseaux ouverts aux invités doivent être séparés du réseau interne	Non renseigné	
S'assurer qu'aucune interface d'administration n'est accessible directement depuis Internet. La télémaintenance doit s'effectuer à travers un VPN	Non renseigné	
Limiter les flux réseau au strict nécessaire en filtrant les flux entrants/sortants sur les équipements (pare-feu, proxy, serveurs, etc.). Par exemple, si un serveur web utilise obligatoirement HTTPS, il faut autoriser uniquement les flux entrants sur cette machine sur le port 443 et bloquer tous les autres ports	Non renseigné	

Objectif : SECURITE : S08 -Sécuriser les serveurs

Critère	Réponse	Commentaire
Installer les mises à jour critiques sans délai que ce soit pour les systèmes d'exploitation ou pour les applications, en programmant une vérification automatique hebdomadaire	Non renseigné	
Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées. Utiliser des comptes de moindres privilèges pour les opérations courantes.	Non renseigné	
Adopter une politique spécifique de mots de passe pour les administrateurs.	Non	

Changer les mots de passe, au moins, lors de chaque départ d'un administrateur et en cas de suspicion de compromission	renseigné
Effectuer des sauvegardes et les vérifier régulièrement	Non renseigné

Objectif : SECURITE : S09 - Sécuriser les sites web

Critère	Réponse	Commentaire
Limiter le nombre de composants mis en œuvre, en effectuer une veille et les mettre à jour	Non renseigné	
Limiter les ports de communication strictement nécessaires au bon fonctionnement des applications installées. Si l'accès à un serveur web passe uniquement par HTTPS, il faut autoriser uniquement les flux réseau IP entrants sur cette machine sur le port 443 et bloquer tous les autres ports	Non renseigné	
Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées. En particulier, limiter l'utilisation des comptes administrateurs aux équipes en charge de l'informatique et ce, uniquement pour les actions d'administration qui le nécessitent	Non renseigné	
Si des cookies non nécessaires au service sont utilisés, recueillir le consentement de l'internaute après information de celui-ci et avant le dépôt du cookie	Non renseigné	

Objectif : SECURITE : S10 - Sauvegarder et prévoir la continuité d'activité

Critère	Réponse	Commentaire
Utiliser un onduleur pour protéger le matériel servant aux traitements essentiels	Non renseigné	
Stocker les sauvegardes sur un site extérieur, si possible dans des coffres ignifugés et étanches	Non renseigné	

Tester régulièrement la restauration des sauvegardes et l'application du plan de continuité ou de reprisede l'activité	Non renseigné
Effectuer des sauvegardes fréquentes des données, que celles-ci soient sous forme papier ou électronique. Il peut être opportun de prévoir des sauvegardes incrémentales27 quotidiennes et des sauvegardes complètes à intervalles réguliers	Non renseigné

Objectif : SECURITE : S11 - Archiver de manière sécurisée

Critère	Réponse	Commentaire
Mettre en œuvre des modalités d'accès spécifiques aux données archivées du fait que l'utilisation d'une archive doit intervenir de manière ponctuelle et exceptionnelle	Non renseigné	
Définir un processus de gestion des archives : quelles données doivent être archivées, comment et où sont-elles stockées, comment sont gérées les données descriptives ?	Non renseigné	
S'agissant de la destruction des archives, choisir un mode opératoire garantissant que l'intégralité d'une archive a été détruite	Non renseigné	

Objectif : SECURITE : S12 - Encadrer la maintenance et la destruction des données

Critère	Réponse	Commentaire
Enregistrer les interventions de maintenance dans une main courante	Non renseigné	
Supprimer de façon sécurisée les données des matériels avant leur mise au rebut, leur envoi en réparation chez un tiers ou en fin du contrat de location	Non renseigné	
Recueillir l'accord de l'utilisateur avant toute intervention sur son poste	Non renseigné	

Objectif : SECURITE : S13 - Gérer la sous-traitance

Critère	Réponse	Commentaire
Obtenir des conditions de restitution et de destruction des données	Non renseigné	
Prévoir une clause spécifique quant aux données personnelles dans les contrats des sous-traitants	Non renseigné	
Prendre et documenter les moyens (audits de sécurité, visite des installations, etc.) permettant d'assurer l'effectivité des garanties offertes par le sous-traitant en matière de protection des données	Non renseigné	

Objectif : SECURITE : S14 - Sécuriser les échanges avec d'autres organismes

Critère	Réponse	Commentaire
Si vous êtes amené à utiliser le fax, mettre en place les mesures suivantes : installer le fax dans un local physiquement contrôlé et uniquement accessible au personnel habilité ;- faire afficher l'identité du fax destinataire lors de l'émission des messages ;- doubler l'envoi par fax d'un envoi des documents originaux au destinataire ;- préenregistrer dans le carnet d'adresse des fax (si la fonction existe) les destinataires potentiels.	Non renseigné	
Chiffrer les données avant leur enregistrement sur un support physique à transmettre à un tiers (DVD, clé USB, disque dur portable)	Non renseigné	

Objectif : SECURITE : S15 - Protéger les locaux

Critère	Réponse	Commentaire
Restreindre les accès aux locaux au moyen de portes verrouillées	Non renseigné	

Mettre en place des détecteurs de fumée ainsi que des moyens de lutte contre les incendies, et les inspecter annuellement	Non renseigné
Protéger physiquement les matériels informatiques par des moyens spécifiques (système anti-incendie dé-dié, surélévation contre d'éventuelles inondations, redondance d'alimentation électrique et/ou de climatisation,etc.).	Non renseigné