Guide d'accompagnement vers la mise en conformité au RGPD

Le présent document a été conçu à partir des recommandations officielles de la CNIL et de l'ANSSI

Rappel liminaire : il est bon de garder présent à l'esprit deux définitions avant de commencer le travail de mise en conformité : la définition de ce qu'est une « donnée personnelle » et un « traitement de données personnelles ».

- **«données à caractère personnel»** : *toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;*

- **«traitement»** : *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utili sation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rappro chement ou l'interconnexion, la limitation, l'effacement ou la destruction;*

1. Recenser les traitements de données à caractère personnel, automatisés ou non et les données traitées (ex : fichiers client, contrats) ainis que les supports sur lesquels elles reposent :

- **les matériels** (ex : serveurs, ordinateurs portables, disques durs) ;
- **les logiciels** (ex : système d'exploitation, logiciel métier) ;
- **les canaux de communication** (ex : fibre optique, Wi-Fi, Internet) ;
- **les supports papier** (ex : document imprimé, photocopie).

2. Évaluer les risques causés par chaque traitement en s'interrogeant sur ces hypothèses est leurs conséquences potentielles :

Risques	Impacts sur les personnes	Principales sources de risques	Principales menaces	Mesures existantes ou prévues	Gravité	Vraisemblance
Accès illégitime à des données						
Modification non désirée de données						
Disparition de données						

- **Prendre** des mesures appropriées
- **Auditer** ces mesures

3. Archiver & détruisez de manière sécurisée

- **Définir un processus de gestion des archives et de destruction ds données :** quelles données doivent être archivées/détruites, comment et où sont-elles stockées, comment sont gérées les données descriptives ?
- **Mettre en œuvre des modalités d'accès spécifiques** aux données archivées
- **Détruire les archives/données** selon un mode opératoire sécurisé.

4.Sensibiliser & former les utilisateurs

> **La sécurité des données personnelles** recoupe beaucoup celle du système informatique de l'entreprise. Au même titre que vous formez vos personnels à la sécurité du SI, vous devez le sensibiliser à la protection des données personnelles.

I - Sensibiliser et former	
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

> **Informez les personnels par voie d'affichage** (voir documents fournis en annexe) :

> **Établissez une charte informatique & sur les données personnelles contraignante :** ce document rédigé par un juriste peut compléter le règlement intérieur ou s'y annexer. Il s'imposera aux personnels.

> **Prévoyez la signature d'engagements de confidentialité** pour les personnes appelées à manipuler les données personnelles :

Exemple d'engagement de confidentialité pour les personnes ayant vocation à manipuler des données à caractère personnel :

Je soussigné/e Monsieur/Madame _____, exerçant les fonctions de _____ au sein de la société _____ (ci-après dénommée « la Société »), étant à ce titre amené/e à accéder à des données à caractère personnel, déclare reconnaître la confidentialité desdites données.

Je m'engage par conséquent, conformément aux articles 34 et 35 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ainsi qu'aux articles 32 à 35 du règlement général sur la protection des données du 27 avril 2016, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin de protéger la confidentialité des informations auxquelles j'ai accès, et en particulier d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.

Je m'engage en particulier à :
- ne pas utiliser les données auxquelles je peux accéder à des fins autres que celles prévues par mes attributions ;
- ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;
- ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de mes fonctions ;
- prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;
- prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité physique et logique de ces données ;
- m'assurer, dans la limite de mes attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;
- en cas de cessation de mes fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.

Cet engagement de confidentialité, en vigueur pendant toute la durée de mes fonctions, demeurera effectif, sans limitation de durée après la cessation de mes fonctions, quelle qu'en soit la cause, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel.

J'ai été informé que toute violation du présent engagement m'expose à des sanctions disciplinaires et pénales conformément à la réglementation en vigueur, notamment au regard des articles 226-16 à 226-24 du code pénal.

Fait à xxx, le xxx, en xxx exemplaires

Nom :
Signature :

5. Authentifiez les utilisateurs

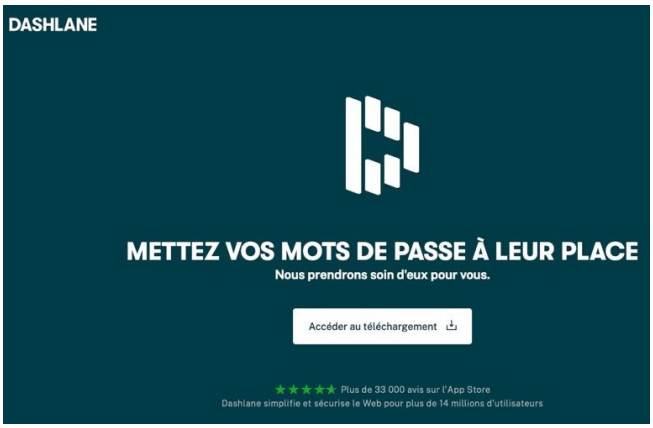
III - Authentifier et contrôler les accès	
8	Identifier nommément chaque personne accédant au système et distinguer les rôles utilisateur/administrateur
9	Attribuer les bons droits sur les ressources sensibles du système d'information
10	Définir et vérifier des règles de choix et de dimensionnement des 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

> **Un utilisateur = un identifiant.** Pas de compte partagé.

> Veillez à rendre obligatoire l'identification de l'utilisateur avant le début d'une session de travail sur un matériel informatique. L'authentification d'un utilisateur est qualifiée de forte lorsqu'elle a recours à une combinaison d'au moins deux de ces catégories :

- **ce que l'on sait,** par exemple un mot de passe
- **ce que l'on a,** par exemple une carte à puce
- **une caractéristique qui nous est propre,** par exemple une empreinte digitale, ou la manière de tracer une signature manuscrite

> **Imposez une politique de mots de passe suffisamment complexe** en ayant recours à un logiciel gestionnaire de mots de passe comme Dashlane par exemple (https://www.dashlane.com/fr)



6. Gérez les habilitations

> **Limitez l'accès aux seules données** dont un utilisateur a besoin
> **Définissez les profils d'habilitation** et révisez-les périodiquement.
> **Supprimer les autorisations** à la fin d'un contrat ou d'un usage.

> **Établissez, documentez et réexaminez régulièrement** une politique de contrôle d'accès qui comprendra :

IV - Sécuriser les postes	
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

> les procédures à appliquer systématiquement à l'arrivée ainsi qu'au départ ou au changement d'affectation d'une personne ayant accès aux données à caractère personnel ;

> les conséquences prévues pour les personnes ayant un accès légitime aux donnés en cas de non-respect des mesures de sécurité ;

> les mesures permettant de restreindre et de contrôler l'attribution et l'utilisation des accès au traitement

> **Sécurisez** les postes de travail : ils constituent le principal point de vulnérabilité de votre entreprise.

- **Verrouillage automatique de session** en cas de non-utilisation du poste pendant un temps donné.
- Installation d'un « **pare-feu** » (« **firewall** »)
- Utilisation d'**antivirus régulièrement mis à jour**
- Politique de **mise à jour régulière des logiciels**
- **Stockage régulier de sauvegarde accessible via le réseau de l'organisme** plutôt que sur les postes de travail.
- **Limiter la connexion de supports mobiles**
- **Désactiver l'exécution automatique** (« autorun ») depuis des supports amovibles.
- **Interdire l'exécution d'applications téléchargées** ne provenant pas de sources sûres.
- **Limiter l'usage** d'applications nécessitant des droits de niveau administrateur pour leur exécution.
- **Effacer de facon sécurisée les données** présentes sur un poste

> En matière d'**assistance sur les postes de travail :**

- **Recueil préalable de l'accord de l'utilisateur** avant toute intervention

7. Gérer les incidents

- En cas d'accès d'atteinte à vos systèmes, d'accès frauduleux ou d'usage illicite de ceux-ci, **vous devez pouvoir retracer l'incident pour le traiter.**

- Mettez en place **un système de journalisation** des activités des utilisateurs, des anomalies et des événements liés à la sécurité : ces journaux doivent conserver les évènements sur une période glissante **ne pouvant excéder six mois** (sauf obligation légale, ou risque particulièrement important) ;

- **la journalisation doit concerner, au minimum, les accès des utilisateurs** en incluant leur identifiant, la date et l'heure de leur connexion, et la date et l'heure de leur déconnexion ;

- **Informer les utilisateurs** de la mise en place d'un tel système, après information et consultation des représentants du personnel.

- **Protéger les équipements de journalisation et les informations journalisées** contre les accès non autorisés, notamment en les rendant inaccessibles aux personnes dont l'activité est journalisée.

- **Notifier** toute violation de données à caractére personnel à la VNIL et, aux personnes concernées pour qu'elles puissent en limiter les conséquences.

IX - Superviser, auditer, réagir	
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

8. Gérer l'informatique mobile de vos collaborateurs

VII - Gérer le nomadisme	
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

> **Sensibiliser les utilisateurs** aux risques spécifiques liés à l'utilisation d'outils informatiques mobiles (ex : vol de matériel) et aux procédures prévues pour les limiter.

> **Mise en place de sauvegardes ou de synchronisation des postes nomades**, pour se prémunir contre la disparition des données stockées.

> **Prévoir des moyens de chiffrement des postes nomades** et supports de stockage mobiles

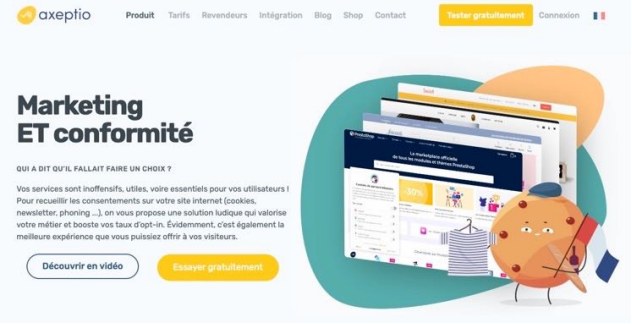
- **Sur les Smartphones,** activer le verrouillage automatique du terminal et exiger un code pour le déverrouiller
- **Utiliser un filtre de confidentialité sur les écrans** utilisés dans les lieux publics.

9. Protéger le réseau informatique & les Sites Web

- **Limiter les accès Internet** en bloquant les services non nécessaires
- **Gérer les réseaux Wi-Fi.** Ils doivent utiliser un chiffrement conforme à l'état de l'art
- **Séparer** le réseau « invités »
- **Utiliser un VPN** pour l'accès à distance
- **Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées**.

V - Sécuriser le réseau	
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

- **Mettre en œuvre le protocole TLS** sur tous les sites web
- **Rendre l'utilisation de TLS obligatoire pour toutes les pages d'authentification**, de formulaire ou sur lesquelles sont affichées ou transmises des données à caractère personnel non publiques.
- **Limiter les ports de communication strictement nécessaires** au bon fonctionnement des applications installées.
- **Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées**.
- **Utilier des logiciels de recueil de consentement** conformes aux exigences du RGPD comme Axeptio (www.axeptio.eu)



10. Gérer la sous-traitance

> **Qu'est-ce qu'un sous-traitant ?**

Les sous-traitants sont notamment vos partenaires commerciaux. Le RGPD les définit comme suit : *« la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement »*

> On se place donc dans l'hypothèse où vous avez la qualité de **Responsable de traitement**

> **Vérifiez que votre sous-traitant présente des garanties suffisantes** en matière de protection des données personnelles et de sécurité informatique. Interrogez-le sur ces points.

> Réservez-vous dans les contrats avec le sous-traitant **les moyens de vérifier ses compétences** (audits de sécurité, visite des installations, etc.)

> Chaque cas de sous-traitance de données personnelles doit donner lieu à **l'établissement d'un contrat spécifique ou d'une clause dédiée dans le contrat conclu.**

11. PRÉVOIR LA CONTINUITÉ D'ACTIVITÉ

- **Un plan de continuité ou de reprise d'activité** anticipant les éventuels incidents doit être préparé.
- **Rédiger un plan de reprise et de continuité d'activité informatique** même sommaire, incluant la liste des intervenants.
- **Lister les personnes à alerter** en cas d'incident.
- **Tester régulièrement la restauration** des sauvegardes et l'application du plan de continuité ou de reprise de l'activité.
- **Utiliser un onduleur**
- **Prévoir une redondance matérielle**

12. Protéger les locaux

Les exigences de sécurité posées par le RGPD ne se limitent pas au numérique. L'accès aux données personnelles détenues par l'entreprise ou leur destruction peut aussi se faire de manière physique. La sécurisation des locaux c'est sans doute la plus simple des mesures à prendre pour entamer une procédure de mise en conformité.

- L'accès aux locaux doit être contrôlé pour **éviter ou ralentir un accès direct, non autorisé, que ce soit aux fichiers papiers ou aux matériels informatiques, notamment aux serveurs.**

- Alarmes anti-intrusion, détecteurs de fumée, moyens de lutte contre les incendies… sont à enviager.

- Protection des clés permettant l'accès aux locaux et les codes d'alarme.

- Distinguer les zones des bâtiments selon les risques (par exemple prévoir un contrôle d'accès dédié pour la salle informatique). Selon la taille et l'activité de l'entreprise : liste des personnes ou catégories de personnes autorisées à pénétrer dans chaque zone, règles et moyens de contrôle d'accès des visiteurs, au minimum en faisant accompagner les visiteurs, en dehors des zones d'accueil du public par une personne appartenant à l'organisme.

13. Évaluez votre entreprise :

FICHES		MESURE	
1	Sensibiliser les utilisateurs	Informez et sensibilisez les personnes manipulant les données	☐
		Rédigez une charte informatique et donnez lui une force contraignante	☐
2	Authentifier les utilisateurs	Définissez un identifiant (login) unique à chaque utilisateur	☐
		Adoptez une politique de mot de passe utilisateur conforme à nos recommandations	☐
		Obligez l'utilisateur à changer son mot de passe après réinitialisation	☐
		Limitez le nombre de tentatives d'accès à un compte	☐
3	Gérer les habilitations	Définissez des profils d'habilitation	☐
		Supprimez les permissions d'accès obsolètes	☐
		Réaliser une revue annuelle des habilitations	☐
4	Tracer les accès et gérer les incidents	Prévoyez un système de journalisation	☐
		Informez les utilisateurs de la mise en place du système de journalisation	☐
		Protégez les équipements de journalisation et les informations journalisées	☐
		Prévoyez les procédures pour les notifications de violation de données à caractère personnel	☐
5	Sécuriser les postes de travail	Prévoyez une procédure de verrouillage automatique de session	☐
		Utilisez des antivirus régulièrement mis à jour	☐
		Installez un « pare-feu » (*firewall*) logiciel	☐
		Recueillez l'accord de l'utilisateur avant toute intervention sur son poste	☐
6	Sécuriser l'informatique mobile	Prévoyez des moyens de chiffrement des équipements mobiles	☐
		Faites des sauvegardes ou des synchronisations régulières des données	☐
		Exigez un secret pour le déverrouillage des smartphones	☐
7	Protéger le réseau informatique interne	Limitez les flux réseau au strict nécessaire	☐
		Sécurisez les accès distants des appareils informatiques nomades par VPN	☐
		Mettez en œuvre le protocole WPA2 ou WPA2-PSK pour les réseaux Wi-Fi	☐
8	Sécuriser les serveurs	Limitez l'accès aux outils et interfaces d'administration aux seules personnes habilitées	☐
		Installez sans délai les mises à jour critiques	☐
		Assurez une disponibilité des données	☐

FICHES		MESURE	
9	**Sécuriser les sites web**	Utilisez le protocole TLS et vérifiez sa mise en œuvre	☐
		Vérifiez qu'aucun mot de passe ou identifiant ne passe dans les url	☐
		Contrôlez que les entrées des utilisateurs correspondent à ce qui est attendu	☐
		Mettez un bandeau de consentement pour les *cookies* non nécessaires au service	☐
10	**Sauvegarder et prévoir la continuité d'activité**	Effectuez des sauvegardes régulières	☐
		Stockez les supports de sauvegarde dans un endroit sûr	☐
		Prévoyez des moyens de sécurité pour le convoyage des sauvegardes	☐
		Prévoyez et testez régulièrement la continuité d'activité	☐
11	**Archiver de manière sécurisée**	Mettez en œuvre des modalités d'accès spécifiques aux données archivées	☐
		Détruisez les archives obsolètes de manière sécurisée	☐
12	**Encadrer la maintenance et la destruction des données**	Enregistrez les interventions de maintenance dans une main courante	☐
		Encadrez par un responsable de l'organisme les interventions par des tiers	☐
		Effacez les données de tout matériel avant sa mise au rebut	☐
13	**Gérer la sous-traitance**	Prévoyez une clause spécifique dans les contrats des sous-traitants	☐
		Prévoyez les conditions de restitution et de destruction des données	☐
		Assurez-vous de l'effectivité des garanties prévues (audits de sécurité, visites, etc.)	☐
14	**Sécuriser les échanges avec d'autres organismes**	Chiffrez les données avant leur envoi	☐
		Assurez-vous qu'il s'agit du bon destinataire	☐
		Transmettez le secret lors d'un envoi distinct et via un canal différent	☐
15	**Protéger les locaux**	Restreignez les accès aux locaux au moyen de portes verrouillées	☐
		Installez des alarmes anti-intrusion et vérifiez-les périodiquement	☐
16	**Encadrer les développements informatiques**	Proposez des paramètres respectueux de la vie privée aux utilisateurs finaux	☐
		Évitez les zones de commentaires ou encadrez-les strictement	☐
		Testez sur des données fictives ou anonymisées	☐
17	**Utiliser des fonctions cryptographiques**	Utilisez des algorithmes, des logiciels et des bibliothéques reconnues	☐
		Conservez les secrets et les clés cryptographiques de manière sécurisée	☐

ANNEXES

I - Outil de suivi de sécurité informatique
II - Affichages destinés aux locaux de l'entreprise

I - Sensibiliser et former	
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 - Connaitre le système d'information	
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	
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	
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	
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	
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	
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	
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	
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

La sécurité du numérique à portée de clic

4
SAUVEGARDES : L'ATOUT SÉRÉNITÉ.

Pour préserver vos données, effectuez des sauvegardes régulières sur un support externe déconnecté.

12
IDENTITÉ NUMÉRIQUE : ATTENTION, DOSSIER !

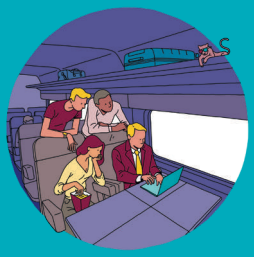
Une fois sur Internet, vos données vous échappent et font le bonheur des adeptes de l'« ingénierie sociale » (usurpation d'identité, espionnage…). Faites-vous discret…

2
MISES À JOUR : ~~JE LE FERAI DEMAIN !~~

La mise à jour des logiciels et applications corrige les vulnérabilités appréciées des attaquants. N'attendez plus !

7
NOMADISME : FAITES RIMER MOBILITÉ ET SÉCURITÉ.

En déplacement, attention et discrétion doivent guider l'usage que vous faites de vos appareils mobiles. N'emportez que l'essentiel !



5
WI-FI, CLÉS USB, ETC. : N'OUVREZ PAS LA PORTE À N'IMPORTE QUI !

Les services ou équipements qui vous sont offerts peuvent avoir été configurés à des fins malveillantes. Par prévoyance, évitez-les ou demandez l'avis d'un spécialiste.

10
PAIEMENT EN LIGNE : ÉVITEZ LES FRAIS.

Soyez vigilants lors de vos achats sur Internet. Gardez en tête quelques bons réflexes : vérifiez que figure la mention « https:// » dans la barre d'adresse du site consulté et dans certains cas, un cadenas.

6
ORDINATEUR, TÉLÉPHONE, TABLETTE : MÊME COMBAT !

Vos appareils mobiles aussi sont vulnérables ! Qu'attendez-vous pour les protéger ?

9
TÉLÉCHARGEMENT : GARE AUX ARNAQUES !

Restez prudents lorsque vous téléchargez programmes et logiciels, préférez les sites officiels.

1
MOTS DE PASSE : FAITES PREUVE D'IMAGINATION…

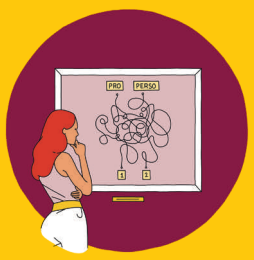
Aimez-les complexes, uniques, secrets et régulièrement renouvelés !

8
MESSAGERIE : MÉFIEZ-VOUS DES APPARENCES…

Les courriels, les pièces jointes ou les liens qu'ils contiennent réservent parfois de mauvaises surprises… Les incohérences de fond ou de forme et les requêtes indiscrètes sont à prendre avec des pincettes !

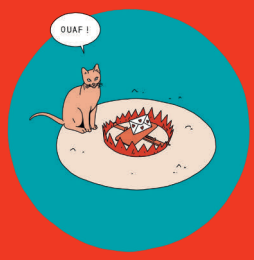
11
SÉPARATION DES USAGES : UN JEU D'ENFANT ?

Pour limiter l'effet boule de neige d'une action malveillante, séparez vos usages professionnels et personnels (messagerie, équipements…).



3
PRIVILÈGES : À QUOI BON AVOIR TOUS LES DROITS ?

Un compte administrateur vous ouvre tous les droits (configuration de votre ordinateur, réseaux, etc.). Préférez le compte utilisateur pour vos usages courants (navigation, bureautique, etc.), c'est plus sûr.



ANSSI

#TousSecNum

En savoir plus avec le guide des bonnes pratiques de l'informatique :
www.ssi.gouv.fr/guide-bonnes-pratiques/

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

LES RÉSEAUX SOCIAUX

Mémo

ADOPTER LES **BONNES PRATIQUES**

10 CONSEILS POUR VOTRE SÉCURITÉ SUR LES RÉSEAUX SOCIAUX

1. Protégez l'accès à vos comptes
2. Vérifiez vos paramètres de confidentialité
3. Maîtrisez vos publications
4. Faites attention à qui vous parlez
5. Contrôlez les applications tierces
6. Évitez les ordinateurs et les réseaux Wi-Fi publics
7. Vérifiez régulièrement les connexions à votre compte
8. Faites preuve de discernement avec les informations publiées
9. Utilisez en conscience l'authentification avec votre compte de réseau social sur d'autres sites
10. Supprimez votre compte si vous ne l'utilisez plus

POUR EN SAVOIR PLUS OU VOUS FAIRE ASSISTER, RENDEZ-VOUS SUR:
www.cybermalveillance.gouv.fr

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

LES MOTS DE PASSE

Mémo

ADOPTER LES **BONNES PRATIQUES**

10 CONSEILS POUR GÉRER VOS MOTS DE PASSE

1. Utilisez un mot de passe différent pour chaque service
2. Utilisez un mot de passe suffisamment long et complexe
3. Utilisez un mot de passe impossible à deviner
4. Utilisez un gestionnaire de mots de passe
5. Changez votre mot de passe au moindre soupçon
6. Ne communiquez jamais votre mot de passe à un tiers
7. N'utilisez pas vos mots de passe sur un ordinateur partagé
8. Activez la double authentification lorsque c'est possible
9. Changez les mots de passe par défaut des différents services auxquels vous accédez
10. Choisissez un mot de passe particulièrement robuste pour votre messagerie

POUR EN SAVOIR PLUS OU VOUS FAIRE ASSISTER, RENDEZ-VOUS SUR:
www.cybermalveillance.gouv.fr

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

LES APPAREILS MOBILES Mémo

ADOPTER LES **BONNES PRATIQUES**

10 CONSEILS POUR SÉCURISER VOTRE APPAREIL MOBILE

1. Mettez en place les codes d'accès
2. Chiffrez les données de l'appareil
3. Appliquez les mises à jour de sécurité
4. Faites des sauvegardes
5. Utilisez une solution de sécurité contre les virus et autres attaques
6. N'installez des applications que depuis les sites ou magasins officiels
7. Contrôlez les autorisations de vos applications
8. Ne laissez pas votre appareil sans surveillance
9. Évitez les réseaux Wi-Fi publics ou inconnus
10. Ne stockez pas d'informations confidentielles sans protection

POUR EN SAVOIR PLUS OU VOUS FAIRE ASSISTER, RENDEZ-VOUS SUR:
www.cybermalveillance.gouv.fr

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

LES SAUVEGARDES

Mémo

ADOPTER LES **BONNES PRATIQUES**

10 CONSEILS POUR ÉVITER DE PERDRE VOS DONNÉES

1. Effectuez des sauvegardes régulières de vos données
2. Identifiez les appareils et supports qui contiennent des données
3. Déterminez quelles données doivent être sauvegardées
4. Choisissez une solution de sauvegarde adaptée à vos besoins
5. Planifiez vos sauvegardes
6. Déconnectez votre support de sauvegarde après utilisation
7. Protégez vos sauvegardes (perte, vol, casse...)
8. Testez vos sauvegardes
9. Vérifiez le support de sauvegarde
10 Pro. Sauvegardez les logiciels indispensables à l'exploitation de vos données

POUR EN SAVOIR PLUS OU VOUS FAIRE ASSISTER, RENDEZ-VOUS SUR:
www.cybermalveillance.gouv.fr

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

LES MISES À JOUR

Mémo

ADOPTER LES **BONNES PRATIQUES**

10 CONSEILS POUR GÉRER VOS MISES À JOUR

1. Pensez à mettre à jour sans tarder l'ensemble de vos appareils et logiciels
2. Téléchargez les mises à jour uniquement depuis les sites officiels
3. Identifiez l'ensemble des appareils et logiciels utilisés
4. Activez l'option de téléchargement et d'installation automatique des mises à jour
5. Pro — Définissez les règles de réalisation des mises à jour
6. Planifiez les mises à jour lors de périodes d'inactivité
7. Méfiez-vous des fausses mises à jour sur Internet
8. Pro — Informez-vous sur la publication régulière des mises à jour de l'éditeur
9. Pro — Testez les mises à jour lorsque cela est possible et faites des sauvegardes
10. Pro — Protégez autrement les appareils qui ne peuvent pas être mis à jour

POUR EN SAVOIR PLUS OU VOUS FAIRE ASSISTER, RENDEZ-VOUS SUR:
www.cybermalveillance.gouv.fr

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

LES USAGES PRO-PERSO Mémo

ADOPTER LES **BONNES PRATIQUES**

10 CONSEILS POUR SÉCURISER VOS USAGES PRO ET PERSO

1. Utilisez des mots de passe différents pour tous les services professionnels et personnels auxquels vous accédez
2. Ne mélangez pas votre messagerie professionnelle et personnelle
3. Ayez une utilisation raisonnable d'Internet au travail
4. Maîtrisez vos propos sur les réseaux sociaux
5. N'utilisez pas de service de stockage en ligne personnel à des fins professionnelles
6. Faites les mises à jour de sécurité de vos équipements
7. Utilisez une solution de sécurité contre les virus et autres attaques
8. N'installez des applications que depuis les sites ou magasins officiels
9. Méfiez-vous des supports USB
10. Évitez les réseaux Wi-Fi publics ou inconnus

POUR EN SAVOIR PLUS OU VOUS FAIRE ASSISTER, RENDEZ-VOUS SUR:
www.cybermalveillance.gouv.fr

LES RANÇONGICIELS

EXTORSION D'ARGENT

Vous ne pouvez plus accéder à vos fichiers et on vous demande une rançon ? Vous êtes victime d'une attaque par rançongiciel (*ransomware*, en anglais) !

BUT

Réclamer le paiement d'une rançon pour rendre l'accès aux fichiers verrouillés.

TECHNIQUE

Blocage de l'accès à des données par envoi d'un message contenant des liens ou pièces jointes malveillantes ou par intrusion sur le système.

COMMENT RÉAGIR ?

- Débranchez la machine d'Internet et du réseau local
- En entreprise, alertez le support informatique
- Ne payez pas la rançon
- Déposez plainte
- Identifiez et corrigez l'origine de l'infection
- Essayez de désinfecter le système et de déchiffrer les fichiers
- Réinstallez le système et restaurez les données
- Faites-vous assister par des professionnels

Pour en savoir plus ou vous faire assister, rendez-vous sur cybermalveillance.gouv.fr

LIEN UTILE

www.nomoreransom.org/fr/index.4html

L'HAMEÇONNAGE

CYBERCRIMINEL

VOL DE DONNÉES

Vous recevez un message ou un appel inattendu, voire alarmant, d'une organisation connue et d'apparence officielle qui vous demande des informations personnelles ou bancaires ? Vous êtes peut-être victime d'une attaque par hameçonnage (*phishing* en anglais) !

BUT

Voler des informations personnelles ou professionnelles (identité, adresses, comptes, mots de passe, données bancaires…) pour en faire un usage frauduleux.

TECHNIQUE

Leurre envoyé *via* un faux message, SMS ou appel téléphonique d'administrations, de banques, d'opérateurs, de réseaux sociaux, de sites d'e-commerce…

VICTIME

COMMENT RÉAGIR ?

- Ne communiquez jamais d'information sensible suite à un message ou un appel téléphonique
- Au moindre doute, contactez directement l'organisme concerné pour confirmer
- Faites opposition immédiatement (en cas d'arnaque bancaire)
- Changez vos mots de passe divulgués/compromis
- Déposez plainte
- Signalez-le sur les sites spécialisés (voir liens utiles)

Pour en savoir plus ou vous faire assister, rendez-vous sur cybermalveillance.gouv.fr

LIENS UTILES

- Signal-spam.fr
- Phishing-initiative.fr
- Info Escroqueries
  0 805 805 817 (gratuit)

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

NOS CONSEILS POUR VOTRE SÉCURITÉ NUMÉRIQUE

ADOPTER LES BONNES PRATIQUES

LES MOTS DE PASSE

Votre mot de passe doit être différent pour chaque service, suffisamment long et complexe, et impossible à deviner. Ne le communiquez jamais à un tiers. Pour votre messagerie, il doit être particulièrement robuste.

LA SÉCURITÉ SUR LES RÉSEAUX SOCIAUX

Protégez l'accès à vos comptes, vérifiez vos paramètres de confidentialité et maîtrisez vos publications. Faites attention à qui vous parlez. Vérifiez régulièrement les connexions à votre compte.

LA SÉCURITÉ DES APPAREILS MOBILES

Mettez en place les codes d'accès. Appliquez les mises à jour de sécurité et faites des sauvegardes, évitez les réseaux Wi-Fi publics ou inconnus. Ne laissez pas votre appareil sans surveillance.

LES SAUVEGARDES

Pour éviter de perdre vos données, effectuez des sauvegardes régulières. Identifiez les appareils et supports qui contiennent des données et déterminez lesquelles doivent être sauvegardées. Choisissez une solution adaptée à vos besoins. Protégez et testez vos sauvegardes.

LES MISES À JOUR

Mettez à jour sans tarder l'ensemble de vos appareils et logiciels. Téléchargez les mises à jour uniquement depuis les sites officiels et activez l'option de téléchargement et d'installation automatique des mises à jour.

LES USAGES PRO-PERSO

Utilisez des mots de passe différents pour tous les services professionnels et personnels auxquels vous accédez. Ne mélangez pas votre messagerie professionnelle et personnelle et n'utilisez pas de service de stockage en ligne personnel à des fins professionnelles.

RETROUVEZ L'ENSEMBLE DES CONSEILS SUR CES THEMATIQUES DANS NOS FICHES PRATIQUES

COMPRENDRE LES RISQUES ET RÉAGIR

L'HAMEÇONNAGE

VOL DE DONNÉES

Vous recevez un message ou un appel inattendu, voire alarmant, d'une organisation connue et d'apparence officielle qui vous demande des informations personnelles ou bancaires ? Vous êtes peut-être victime d'une attaque par hameçonnage (*phishing* en anglais) !

BUT
Voler des informations personnelles ou professionnelles (identité, adresses, comptes, mots de passe, données bancaires…) pour en faire un usage frauduleux.

TECHNIQUE
Leurre envoyé *via* un faux message, SMS ou appel téléphonique d'administrations, de banques, d'opérateurs, de réseaux sociaux, de sites d'e-commerce…

LES RANÇONGICIELS

EXTORSION D'ARGENT

Vous ne pouvez plus accéder à vos fichiers et on vous demande une rançon ? Vous êtes victime d'une attaque par rançongiciel (*ransomware*, en anglais) !

BUT
Réclamer le paiement d'une rançon pour rendre l'accès aux fichiers verrouillés.

TECHNIQUE
Blocage de l'accès à des données par envoi d'un message contenant des liens ou pièces jointes malveillantes ou par intrusion sur le système.

L'ARNAQUE AU FAUX SUPPORT TECHNIQUE

ESCROQUERIE FINANCIÈRE

Votre ordinateur est bloqué et on vous demande de rappeler un support technique ? Vous êtes victime d'une arnaque au faux support !

BUT
Inciter la victime à payer un pseudo-dépannage informatique et/ou la faire souscrire à des abonnements payants

TECHNIQUE
Faire croire à un problème technique grave impliquant un risque de perte de données ou d'usage de l'équipement (par écran bloqué, téléphone, SMS, courriel etc.).

CYBERCRIMINEL

VICTIME

COMMENT RÉAGIR ?

Hameçonnage
- Ne communiquez jamais d'information sensible suite à un message ou un appel téléphonique
- Au moindre doute, contactez directement l'organisme concerné pour confirmer
- Faites opposition immédiatement (en cas d'arnaque bancaire)
- Changez vos mots de passe divulgués/compromis
- Déposez plainte
- Signalez-le sur les sites spécialisés

Rançongiciels
- Débranchez la machine d'Internet et du réseau local
- En entreprise, alertez le support informatique
- Ne payez pas la rançon
- Déposez plainte
- Identifiez et corrigez l'origine de l'infection
- Essayez de désinfecter le système et de déchiffrer les fichiers
- Réinstallez le système et restaurez les données
- Faites-vous assister par des professionnels

Arnaque au faux support technique
- Ne répondez pas
- Conservez toutes les preuves
- Redémarrez votre appareil
- Purgez le cache, supprimez les cookies et réinitialisez les paramètres de votre navigateur
- Désinstallez tout nouveau programme suspect
- Faites une analyse antivirus
- Changez tous vos mots de passe
- Faites opposition auprès de votre banque si vous avez payé
- Déposez plainte

En partenariat avec l'Agence nationale de la sécurité des systèmes d'information

POUR EN SAVOIR PLUS OU VOUS FAIRE ASSISTER, RENDEZ-VOUS SUR :
www.cybermalveillance.gouv.fr

Avec la participation des membres du dispositif :

LES FAUX SUPPORTS TECHNIQUES

ESCROQUERIE FINANCIÈRE

Votre ordinateur est bloqué et on vous demande de rappeler un support technique ? Vous êtes victime d'une arnaque au faux support !

BUT

Inciter la victime à payer un pseudo-dépannage informatique et/ou la faire souscrire à des abonnements payants.

TECHNIQUE

Faire croire à un problème technique grave impliquant un risque de perte de données ou d'usage de l'équipement (par écran bloqué, téléphone, SMS, courriel etc.).

COMMENT RÉAGIR ?

- Ne répondez pas
- Conservez toutes les preuves
- Redémarrez votre appareil
- Purgez le cache, supprimez les cookies et réinitialisez les paramètres de votre navigateur
- Désinstallez tout nouveau programme suspect
- Faites une analyse antivirus
- Changez tous vos mots de passe
- Faites opposition auprès de votre banque si vous avez payé
- Déposez plainte

Pour en savoir plus ou vous faire assister, rendez-vous sur cybermalveillance.gouv.fr

LIENS UTILES

- Internet-signalement.gouv.fr
- Info Escroqueries
  0 805 805 817 (gratuit)