

CHARTE INFORMATIQUE

SOMMAIRE

GLOSSAIRE	4
PREAMBULE	5
1. Rôles et responsabilités	6
1.1. Direction	6
1.2. Responsable de la Sécurité des Systèmes d'Information	6
1.3. Utilisateurs	6
2. Champ d'application	6
3. Périmètre géographique	7
4. Accès aux systèmes d'information	7
4.1. Droits d'accès	7
4.2. Authentification	8
4.3. Verrouillage de session	8
4.4. Revue des droits d'accès	8
4.5. Destruction des données	8
5. Conditions d'usage	8
5.1. Installations logicielles	9
5.2. Supports de stockage amovibles	9
5.3. Outils de communication approuvés	9
5.4. Stockage des données professionnelles	9
6. Matériels / logiciels informatiques	9
6.1. Acquisition	9
6.2. Perte ou vol	10
6.3. Destruction	10
7. Propriété intellectuelle	10
8. Limitation des droits d'accès	10
8.1. Usage d'Internet	10
8.2. Dispositifs de sécurité réseau	11
9. Règles de sécurité	11
10. Droit à la déconnexion	11
11. Contrôle des systèmes d'information	11
12. Historisation des accès	12
13. Mesures d'urgence et de restriction	12
14. Pannes ou dysfonctionnements	12
15. Réseaux sociaux	13
16. Télétravail et usage à distance	13

17	Incident de sécurité	13
17.1	Définition	13
17.2	Signalement	14
17.3	Obligations des utilisateurs	14
18	Absence temporaire et départ de l'entreprise	14
19	Intelligence artificielle (IA)	15
20	Enregistrement des réunions	15
21	Protection des informations	15
21.1	Accès aux locaux	15
21.2	Bureau Propre (Clear Desk)	15
22	Sauvegarde des données	16
23	Comportements attendus	16
24	Demandes particulières et contacts	16

GLOSSAIRE

Les termes techniques utilisés dans la présente Charte sont définis ci-dessous :

TERME	DEFINITION
Authentification Multi-Facteurs (MFA)	Méthode d'identification exigeant au moins deux formes d'identification pour accéder à un système réduisant ainsi le risque de compromission (ex : mot de passe + code sur téléphone).
Chiffrement	Procédé visant à transformer des données en un format illisible pour toute personne ne disposant pas de la clé de déchiffrement.
Confidentialité	Principe garantissant que l'information n'est accessible qu'aux personnes autorisées (1er pilier de la sécurité de l'information) Elle implique également une obligation de non-divulgaration, avec un niveau de communication et de transfert strictement limité aux seules personnes concernées.
Disponibilité	Principe garantissant que les systèmes et données sont accessibles quand les utilisateurs en ont besoin (2e pilier).
Hameçonnage (Phishing)	E-mail frauduleux imitant un tiers de confiance pour soutirer des identifiants ou des informations sensibles.
Incident de Sécurité	Tout événement compromettant ou susceptible de compromettre la confidentialité, l'intégrité ou la disponibilité des informations d'un système ou d'un réseau.
Ingénierie Sociale	Manipulation psychologique visant à tromper un utilisateur pour qu'il divulgue des informations ou réalise une action non souhaitée.
Intégrité	Principe garantissant que les données n'ont pas été altérées ou modifiées de manière non autorisée (3e pilier).
ISO/IEC 27001:2022	Norme internationale définissant les exigences pour gérer la sécurité de l'information (SMSI) — version la plus récente.
Logiciel Malveillant (Malware)	Programme informatique conçu pour nuire à un système (virus, ransomware, spyware, etc.) ou en exploiter les vulnérabilités.
Moindre Privilège	Principe de sécurité selon lequel chaque utilisateur ne dispose que des droits strictement nécessaires à l'exercice de ses fonctions (limitation des droits d'accès).
Pare-feu (Firewall)	Dispositif de sécurité qui filtre le trafic réseau afin d'empêcher les accès non-autorisés et de protéger le réseau interne contre les menaces extérieures.
Ransomware	Type de Logiciel malveillant (Malware) qui bloque l'accès à un système ou chiffre des données, en exigeant le paiement d'une rançon pour en permettre la restitution ou le déchiffrement.
Repeat Offender	Programme interne de remédiation renforcée destiné aux utilisateurs présentant des comportements récurrents non conformes aux règles de sécurité de l'organisation.
RGPD (Règlement Général sur la Protection des Données)	Règlement européen (UE 2016/679) encadrant la collecte, le traitement et le stockage des données personnelles imposant des obligations aux organisations et assurant la protection des droits des personnes concernées.
RSSI (Responsable de la Sécurité des Systèmes d'Information)	Responsable de la politique de sécurité informatique au sein de l'organisation.
Shadow IT	Utilisation de systèmes, applications ou services informatiques sans validation préalable du service IT, pouvant introduire des risques importants pour la sécurité
SMSI (Système de Management de la Sécurité de l'Information)	Ensemble des politiques et processus mis en place pour gérer la sécurité de l'information (norme ISO 27001).

Station Blanche	Dispositif physique permettant de scanner la clé USB de l'utilisateur afin de détecter et prévenir l'introduction de logiciels malveillants et autres menaces.
Support Amovible	Périphérique de stockage portable (clé USB, disque dur externe, carte SD) pouvant constituer un vecteur fréquent de propagation de logiciels malveillants (type malwares).
VPN (Virtual Private Network)	Mécanisme de connexion sécurisée reposant sur un tunnel chiffré entre le poste utilisateur et le réseau de l'entreprise, obligatoire pour les accès à distance.
Vishing	Appels téléphoniques frauduleux visant à usurper l'identité d'une entité de confiance afin d'obtenir des informations confidentielles (Phishing par téléphone).
Matériel Informatique	Ensemble des équipements physiques utilisés pour le traitement, le stockage ou la transmission de l'information, constituant des actifs du système d'information nécessitant une protection adéquate.
Sauvegarde en local	Copie de données stockée sur un support physique indépendant et déconnecté du réseau de l'entreprise (exemple : disque dur externe, clé USB, disque dur du PC,...)

PREAMBULE

Compte-tenu de l'importance grandissante de la digitalisation et des outils numériques dans le quotidien des activités tant administratives qu'en lien avec la production d'une part, et des exigences réglementaires d'autre part, TMMF a décidé de se doter d'une charte informatique et de mettre en place une gouvernance pour renforcer la cybersécurité et la gestion des risques liés aux systèmes d'information.

La présente charte des systèmes d'information a pour objet de définir les règles d'utilisation des systèmes d'information et des moyens de communication mis à la disposition des utilisateurs dans le cadre de leur activité professionnelle.

Annexée au règlement intérieur, elle produit les mêmes effets et s'impose à l'ensemble des utilisateurs concernés. Les règles qu'elle définit visent à assurer un niveau élevé de sécurité, de confidentialité, d'intégrité et de performance dans l'utilisation des systèmes d'information et de communication. Ces règles peuvent être complétées et déclinées dans des documents opérationnels (fiches pratiques, procédures internes ou manuels utilisateurs / administrateurs...).

Cette charte ne saurait toutefois prévoir de manière exhaustive l'ensemble des situations susceptibles de se présenter dans le cadre de l'utilisation de ces outils.

En conséquence, il appartient à chaque utilisateur d'adopter un comportement responsable, conforme aux règles de sécurité en vigueur, ainsi qu'à l'esprit et aux principes énoncés par la présente charte, y compris dans les situations qui n'y sont pas expressément prévues.

1. Rôles et responsabilités

1.1. *Direction*

La Direction s'engage à soutenir la politique de sécurité des systèmes d'information, d'allouer les ressources nécessaires pour la mise en œuvre et promouvoir une culture de la sécurité à tous les niveaux de l'organisation.

1.2 *Responsable de la Sécurité des Systèmes d'Information*

Un Responsable de la Sécurité des Systèmes d'Information (RSSI) est désigné. Il est l'interlocuteur principal pour toute question relative à la sécurité informatique. A ce titre, ses missions incluent notamment :

- La définition et la mise à jour de la politique de sécurité
- La gestion et le suivi des incidents de sécurité
- La réalisation d'audits et de contrôles périodiques
- La sensibilisation, le conseil et la formation des utilisateurs.

1.3 *Utilisateurs*

Chaque utilisateur est responsable de l'usage des ressources informatiques mises à sa disposition et doit adopter un comportement conforme aux règles de sécurité de l'organisation.

A ce titre, il doit notamment :

- Respecter l'ensemble des dispositions de la présente Charte
- Signaler immédiatement tout incident ou anomalie de sécurité
- Participer aux actions de sensibilisation et aux formations obligatoires
- Protéger la confidentialité des informations auxquelles il a accès

2. Champ d'application

La présente charte s'applique à toute personne accédant à tout ou partie des systèmes d'information de l'entreprise.

Elle s'applique à l'ensemble des matériels, systèmes et services informatiques/numériques mis à disposition par l'entreprise, ainsi qu'aux données qu'ils traitent ou hébergent.

Elle couvre également tout équipement personnel utilisé dans un cadre professionnel.

L'accès aux outils bureautiques via un équipement personnel est autorisé sous réserve du respect des règles de sécurité et des modalités de connexion définies par l'entreprise.

Cet usage est strictement encadré et n'est autorisé qu'à condition :

- de ne procéder à aucun téléchargement ou stockage de données professionnelles sur l'équipement personnel ;
- et de ne pas tenter de contourner les mesures de sécurité mises en place.

Toute demande particulière ou dérogation doit être soumise préalablement à la Direction informatique et faire l'objet d'une validation écrite.

L'utilisation de matériel personnel pour tout autre usage professionnel non prévu est interdite, sauf autorisation expresse de la Direction informatique. Cette autorisation peut être soumise à des règles d'approbation particulières ou au déploiement de mesures de sécurité spécifiques.

3. Périmètre géographique

La présente charte s'applique sans restriction géographique dès lors qu'un outil, un service ou une ressource mise à disposition par l'entreprise est utilisé ou consulté.

Elle s'applique notamment dans les locaux de l'entreprise ou en dehors de celle-ci (déplacements professionnels, télétravail...)

Il est rappelé que le télétravail est organisé dans le cadre d'un accord d'entreprise, il représente un mode d'organisation du travail par lequel l'activité professionnelle du collaborateur est réalisée de façon volontaire en dehors des locaux de l'entreprise, au moyen des outils d'information et de communication mis à sa disposition.

Pour des raisons de sécurité, le travail à distance doit être réalisé exclusivement à l'aide des outils et équipements de travail fournis ou autorisés par l'entreprise. Les utilisateurs s'engagent à respecter les règles applicables en matière de sécurité et de confidentialité des données, ainsi que les dispositions de l'accord sur le télétravail.

4. Accès aux systèmes d'information

L'accès aux outils et services informatiques est soumis à une identification et une authentification préalable de chaque utilisateur.

Les règles d'accès à tout ou partie des systèmes d'information sont définies par la Direction informatique. Les modalités pratiques sont précisées dans les documents internes applicables (fiches pratiques, procédures ou manuels utilisateurs).

Il est strictement interdit :

- De partager ou communiquer les éléments qui permettent d'accéder à toute ou partie des systèmes d'information de l'entreprise ;
- De contourner ou de tenter de contourner les dispositifs de sécurité visant à identifier ou authentifier les utilisateurs.

Toute suspicion de compromission des accès ou des identifiants doit être signalée sans délai à la Direction informatique afin de permettre la mise en œuvre des mesures de sécurité appropriées.

4.1 Droits d'accès

Les droits d'accès aux systèmes d'information sont attribués selon quatre principes de minimisation visant à en limiter l'usage au strict nécessaire :

- Moindre privilège : les accès sont strictement limités aux besoins nécessaires à l'exercice des fonctions ;
- Besoin d'en connaître : l'accès aux informations est réservé aux seules personnes habilitées dans le cadre de leurs missions ;

- Séparation des tâches : les droits critiques sont distribués entre plusieurs personnes afin de prévenir tout risque d'abus ou d'erreur ;
- Formation et sensibilisation : l'attribution des accès est conditionnée à la participation aux actions de sensibilisation et formation à la sécurité de l'information définies par l'entreprise.

4.2 Authentification

Les identifiants, mots de passe ainsi que tous les autres moyens d'authentification sont strictement personnels et confidentiels. Leur partage, leur communication à un tiers ou leur exposition sont formellement interdits.

Les règles relatives aux exigences sécurité (création, renouvellement...) des mots de passe sont définies par la Politique de mots de passe établie par la Direction informatique et doivent être strictement respectées.

En cas de suspicion de compromission, les mesures appropriées doivent être prises sans délai, notamment la modification du mot de passe et l'information de la Direction informatique.

4.3 Verrouillage de session

Les sessions utilisateur doivent être verrouillées systématiquement en cas d'absence de l'utilisateur, même de courte durée, afin de garantir la confidentialité des informations affichées et de prévenir tout accès non autorisé aux systèmes d'information.

4.4 Revue des droits d'accès

Les droits d'accès font l'objet d'une revue au minimum une fois par an, ainsi qu'à chaque changement de fonction déclaré dans les outils de gestion du personnel. Cette revue vise à s'assurer de l'adéquation des habilitations avec les fonctions exercées et à supprimer tout accès devenu non justifié.

4.5 Destruction des données

La destruction des données doit être réalisée de manière sécurisée conformément aux règles définies par la Direction informatique, afin de garantir leur confidentialité et d'éviter toute récupération non autorisée.

5 Conditions d'usage

Les systèmes d'information, les moyens de communication électroniques et les ressources numériques mis à disposition par l'entreprise sont destinés à un usage professionnel dans le cadre de l'exécution des missions confiées aux utilisateurs.

Un usage personnel limité peut être toléré, sous réserve qu'il demeure raisonnable, ponctuel, conforme aux dispositions légales et réglementaires en vigueur et qu'il ne porte atteinte ni à la sécurité des systèmes d'information, ni à la disponibilité des ressources, ni au bon fonctionnement de l'entreprise.

Tout document, email, fichier, dossier ou contenu à caractère personnel doit être clairement identifié par une mention explicite telle que « Personnel » ou « Privé ». À défaut d'une telle identification, les contenus concernés seront présumés avoir un caractère professionnel et pourront être consultés par l'entreprise dans le cadre de ses prérogatives de gestion, de contrôle et de sécurité, conformément aux dispositions légales applicables.

Les contenus identifiés comme « Personnel » ou « Privé » bénéficient d'une protection particulière au titre du respect de la vie privée et du secret des correspondances. Leur consultation et utilisation par l'entreprise ne peut intervenir que dans les conditions particulières prévues par la loi et la jurisprudence.

5.1 Installations logicielles

Il est strictement interdit d'installer des logiciels non autorisés sur les équipements de l'organisation. Toute installation de logiciel doit faire l'objet d'une demande préalable et d'une validation par la Direction informatique.

5.2 Supports de stockage amovibles

L'utilisation de supports de stockage amovibles est strictement encadrée.

Seuls les supports préalablement autorisés par la Direction informatique peuvent être utilisés.

L'usage de tout support externe non validé est interdit, en raison des risques qu'il peut faire peser sur la sécurité et l'intégrité des systèmes d'information.

5.3 Outils de communication approuvés

Seuls les outils de communication validés par la Direction informatique peuvent être utilisés dans le cadre professionnel. L'utilisation d'application de messagerie personnelle pour échanger des données professionnelles est interdite.

5.4 Stockage des données professionnelles

Le stockage de données professionnelles sur des services de stockage en ligne (cloud) non autorisé par la Direction informatique est interdit. Les données professionnelles doivent être conservées exclusivement sur les espaces de stockage mis à disposition ou validés par l'entreprise, afin de garantir leur sécurité, leur confidentialité et leur disponibilité.

6 Matériels / logiciels informatiques

6.1 Acquisition

Toute acquisition de matériel ou de logiciel informatique doit faire l'objet d'une demande préalable auprès de la hiérarchie et d'une validation par la Direction informatique, afin de garantir la conformité, la sécurité et la compatibilité avec les systèmes d'information de l'entreprise.

Tout matériel ou logiciel non conforme aux règles de l'entreprise ou non autorisé pourra être isolé, désactivé ou retiré par la Direction informatique, y compris sans notification préalable, dans un objectif de sécurité et de protection des systèmes d'information.

6.2 Perte ou vol

En cas de perte ou de vol d'un équipement informatique ou de communication, l'utilisateur doit en informer sans délai sa hiérarchie ainsi que le service informatique conformément aux procédures en vigueur, et ce, afin que les mesures de sécurité appropriées puissent être mises en œuvre, notamment pour prévenir tout risque d'accès non autorisé aux données de l'entreprise.

6.3 Destruction

Le matériel informatique est sous la responsabilité de la Direction informatique. Tout équipement en fin de vie doit être restitué au service informatique pour destruction ou revalorisation selon les règles définies.

7 Propriété intellectuelle

Conformément aux dispositions du Code de la propriété intellectuelle, les droits sur les logiciels créés par un salarié dans l'exercice de ses fonctions ou d'après les instructions de l'employeur appartiennent à l'entreprise.

Les logiciels, applications, contenus, documents, bases de données ainsi que toute autre ressource protégée par des droits de propriété intellectuelle, appartenant à l'entreprise ou à des tiers, ne peuvent être copiés, reproduits, modifiés ou diffusés sans l'autorisation préalable.

Les utilisateurs sont tenus de respecter les droits de propriété intellectuelle de l'entreprise et des tiers.

8 Limitation des droits d'accès

L'entreprise se réserve le droit de restreindre ou de filtrer l'accès à certains outils, services, sites web ou contenus, afin de garantir un service de sécurité optimal.

8.1 Usage d'Internet

L'accès à Internet est mis à disposition à des fins professionnelles. Il est interdit d'accéder à des contenus illicites, notamment à caractère pornographique, incitant à la haine ou portant atteinte à la dignité humaine.

8.2 Dispositifs de sécurité réseau

Les dispositifs de sécurité réseau mis en place par l'entreprise ne doivent en aucun cas être contournés, désactivés ou altérés. Tout manquement ou tentative de contournement constitue une violation des règles de sécurité et peut faire l'objet de mesures disciplinaires.

9 Règles de sécurité

Les règles de sécurité applicables sont définies et mises à jour par la Direction informatique.

Toutefois, la sécurité des systèmes d'information repose sur la responsabilité collective de l'ensemble des utilisateurs, qui doivent adopter un comportement vigilant et conforme aux règles en vigueur.

En cas de doute sur un contenu indésirable, aucune action risquée ne doit être entreprise. La situation doit être signalée sans délai à la Direction informatique.

De même, toute attaque ou suspicion d'attaque (phishing, malware, etc.) doit être immédiatement remontée afin de permettre la mise en œuvre des mesures de sécurité appropriées (Application du principe Stop – Call –Wait).

10 Droit à la déconnexion

TMMF respecte le droit à la déconnexion et à la vie privée des members.

Le droit à la déconnexion vise à réguler l'usage des outils numériques professionnels pour protéger le temps de repos, la vie personnelle et la santé.

Sauf en cas d'urgence ou de nécessité impérieuse de service, le salarié n'est pas tenu de répondre aux appels et différents messages qui lui sont destinés pendant les jours et heures de repos, ainsi que durant les périodes de suspension du contrat de travail.

De ce fait, les outils numériques ne doivent pas être utilisés, pour exercer une activité professionnelle pendant ces périodes.

11 Contrôle des systèmes d'information

L'entreprise se réserve le droit de procéder à des contrôles réguliers portant sur l'usage des systèmes d'information, ainsi que sur le respect des dispositions de la présente charte et des documents associés (fiches pratiques, procédures ou manuels utilisateurs/administrateurs).

Ces contrôles peuvent être réalisés :

- par des moyens humains, notamment par les équipes habilitées (administrateurs, équipes informatiques) ;
- par des dispositifs automatisés.

Ces contrôles peuvent être effectués de manière planifiée ou aléatoire, en fonction des besoins de sécurité.

12 Historisation des accès

Le service informatique, responsable de la qualité et de la sécurité des systèmes d'information, est habilité à exercer des opérations de surveillance, de contrôle et de maintenance sur l'ensemble des ressources informatiques mises à disposition des utilisateurs.

Les utilisateurs sont informés que les administrateurs, par leurs fonctions, ont accès à l'ensemble des informations relatives à leur utilisation des systèmes d'information (messagerie, connexions internet, fichiers stockés sur les espaces réseau, imprimantes, postes de travail ...), et ce dans le strict cadre de leurs missions professionnelles, auxquelles s'ajoute une obligation de confidentialité.

Des dispositifs de surveillance et de journalisation sont déployés en continu (pare-feu, antivirus, systèmes de détection d'intrusion, proxys, filtres de contenu ...) permettant de tracer les authentications, les accès aux ressources, le trafic réseau et les échanges par messagerie.

Ces contrôles, qui peuvent être systématiques, par échantillonnage ou ciblés, visent à prévenir les incidents de sécurité, détecter les usages non conformes et protéger le patrimoine informationnel de TMMF.

Les journaux d'événements ainsi collectés sont conservés dans le respect de la réglementation en vigueur (RGPD, loi Informatique et Libertés ...) et peuvent, le cas échéant, être transmis aux autorités compétentes sur réquisition ou exploités dans le cadre d'une procédure disciplinaire ou judiciaire.

Toute demande d'accès aux données à caractère personnel issues de ces journaux peut être exercée auprès du Délégué à la protection des données (DPO), dans les conditions prévues par la réglementation en vigueur.

13 Mesures d'urgence et de restriction

L'entreprise se réserve le droit de suspendre, sans préavis, tout ou partie de l'accès aux systèmes d'information.

Elle peut également être amenée, notamment pour des raisons de sécurité, à imposer des mesures particulières aux utilisateurs.

14 Pannes ou dysfonctionnements

Les pannes, dysfonctionnements et, plus généralement, tout service d'assistance aux utilisateurs relèvent exclusivement du service informatique. À ce titre, il est strictement interdit de faire appel à un prestataire ou à une ressource externe non autorisée.

Le stockage de données professionnelles sur des équipements personnels est, par principe, interdit, sauf autorisation expresse de la Direction informatique. Dans les cas exceptionnels où un tel stockage est autorisé, et en cas de panne ou de dysfonctionnement de l'équipement, toute intervention d'un tiers doit être précédée soit de la suppression des données professionnelles, soit de la mise en œuvre de mesures limitant l'accès à ces données, afin d'en garantir la confidentialité et la protection.

15 Réseaux sociaux

L'usage des réseaux sociaux est libre en dehors du réseau interne de TMMF. Néanmoins, et dans le respect de la liberté d'expression, aucun contenu publié sur les réseaux sociaux ou sur tout autre espace numérique public ne doit être de nature à porter atteinte aux intérêts de l'entreprise, de ses dirigeants, de ses salariés ou de ses partenaires.

Il est en outre strictement interdit de divulguer, sous quelque forme que ce soit, des informations confidentielles ou sensibles relatives à l'entreprise.

16 Télétravail et usage à distance

Les règles définies dans la présente charte demeurent pleinement applicables dans le cadre du télétravail et de tout usage à distance. Le télétravail est organisé conformément aux dispositions prévues par le « Guide du télétravail chez TMMF » et par l'Accord télétravail.

L'utilisation d'un équipement informatique professionnel mis à disposition par l'entreprise, affecté de manière nominative, est autorisée en situation de télétravail ou de déplacement professionnel, sous réserve de la sécurisation de la connexion par l'usage du VPN de l'entreprise.

L'accès aux systèmes d'information s'effectue exclusivement au moyen du compte nominatif de l'utilisateur, et le matériel doit être physiquement sécurisé.

Dans le cadre d'un usage à distance, il convient de veiller à ne pas afficher d'informations confidentielles dans des lieux publics (notamment les transports ou espaces partagés) et, plus généralement, à garantir la confidentialité des informations affichées à l'écran. Le verrouillage de la session est requis dès que l'utilisateur n'est pas devant l'écran.

L'usage à distance expose les systèmes d'information à des risques accrus, notamment en cas de perte, de vol ou d'accès frauduleux au matériel. À ce titre, les équipements ne doivent jamais être laissés sans surveillance et une vigilance renforcée est attendue. L'entreprise peut, le cas échéant, définir des règles spécifiques.

L'utilisation de filtres de confidentialité est fortement recommandée dans les environnements publics.

Enfin, l'utilisation de matériels ou de services informatiques depuis l'étranger est susceptible d'engendrer des coûts supplémentaires. Toute utilisation dans ce contexte doit faire l'objet d'une information préalable de la Direction informatique, afin d'obtenir les consignes nécessaires.

17 Incident de sécurité

17.1 Définition

Constitue un incident de sécurité tout événement susceptible de compromettre la confidentialité, l'intégrité ou la disponibilité des informations ou des systèmes d'information, notamment :

- La perte ou vol d'un équipement ou d'un support contenant des données
- Un accès non autorisé à un système ou à des données
- Une infection par un logiciel malveillant (virus, ransomware, etc.)
- La réception d'un email frauduleux (phishing) ou toute tentative d'escroquerie

- La divulgation accidentelle d'informations confidentielles
- La reproduction numérique de document ou d'emails contenant des données ayant un caractère confidentiel ou sensible par leur nature

17.2 Signalement

Tout incident ou suspicion d'incident de sécurité doit être signalé sans délai à la Direction informatique via les canaux définis.

17.3 Obligations des utilisateurs

En cas d'incident, les utilisateurs sont tenus de :

- cesser immédiatement toute action susceptible d'aggraver la situation ;
- préserver les éléments de preuve disponibles (messages, fichiers, journaux, captures d'écran, etc.) ;
- ne pas tenter de résoudre l'incident par leurs propres moyens ;
- coopérer pleinement avec les équipes informatiques afin de permettre l'analyse et le traitement de l'incident.

18 Absence temporaire et départ de l'entreprise

En cas d'absence, les accès aux outils informatiques demeurent actifs. Toutefois, lesdits outils ne doivent pas être utilisés pendant les jours et heures de repos ainsi que pendant les périodes de suspension du contrat de travail (congrés...).

Pour des raisons de continuité de service, l'entreprise peut être amenée à permettre l'accès, par d'autres utilisateurs, aux dossiers, documents et communications professionnelles, y compris à la messagerie professionnelle.

En cas de départ de l'entreprise, l'ensemble des accès aux systèmes d'information est coupé. Tout accès ultérieur aux données ou documents est réalisé exclusivement sur demande.

Par ailleurs, l'entreprise se réserve le droit lorsque les circonstances le justifient, dans le respect de ses intérêts légitimes de protection, de mettre en œuvre des mesures de contrôle ciblées visant à prévenir ou détecter d'éventuels accès, extractions, transferts ou suppressions non autorisés de données.

Ces contrôles sont strictement limités à ce qui est nécessaire et proportionné au but recherché. Ils sont réalisés dans le respect des droits et libertés des utilisateurs ainsi que de la réglementation applicable en matière de protection des données personnelles.

Au plus tard à la date effective du départ, l'utilisateur est tenu :

- de restituer l'ensemble des matériels mis à disposition en bon état de fonctionnement ;
- de supprimer tout document, fichier ou contenu de nature privée présent sur les matériels mis à disposition.

19 Intelligence artificielle (IA)

L'utilisation de l'intelligence artificielle doit impérativement respecter les règles définies par la Direction Informatique.

L'usage des outils d'intelligence artificielle est strictement limité à ceux expressément autorisés par la Direction Informatique et doit se conformer aux règles et modalités précisées dans les fiches pratiques et/ou les manuels utilisateurs en vigueur.

Dans ce cadre, tout utilisateur s'engage à respecter les principes d'éthique, de transparence et de confidentialité, notamment en veillant à :

- anonymiser systématiquement les informations saisies et supprimer toute donnée à caractère personnel ;
- s'abstenir d'utiliser ces outils pour des activités ou traitements sensibles ;
- ne pas communiquer ni intégrer de données confidentielles ;
- ne pas générer ou diffuser de contenus illicites, discriminatoires ou offensants ;
- ne pas porter atteinte à l'image, à la réputation ou aux intérêts de TMMF ;
- exercer un esprit critique et s'assurer de la fiabilité et de l'exactitude des informations générées avant l'utilisation.

20 Enregistrement des réunions

L'enregistrement de réunion, qu'elle soit en présentiel ou en distanciel, n'est possible qu'avec l'autorisation de l'ensemble des participants.

21 Protection des informations

21.1 Accès aux locaux

L'accès aux différents locaux de l'entreprise contenant des équipements informatiques ou zones sécurisées est strictement réservé aux personnes habilitées.

Par ailleurs, les visiteurs sont soumis à des règles d'accès strictes.

21.2 Bureau Propre (Clear Desk)

Afin de garantir la confidentialité des informations et de prévenir tout accès non autorisé, les règles suivantes doivent être respectées :

- verrouiller systématiquement le poste de travail lors de toute absence, même de courte durée ;
- ne laisser aucun document sensible ou confidentiel visible en cas d'absence ;
- ranger les documents confidentiels dans des espaces de stockage sécurisés ;
- ne pas afficher d'informations confidentielles dans des lieux publics.

22 Sauvegarde des données

Les données professionnelles doivent être stockées sur les serveurs ou les espaces de stockage officiels mis à disposition par l'organisation, afin d'en garantir la sauvegarde, la sécurité et la disponibilité.

Les utilisateurs sont responsables de s'assurer que leurs fichiers et données professionnels sont correctement enregistrés sur les espaces partagés mis à disposition par l'organisation.

Des tests de restauration sont réalisés périodiquement par le service informatique afin de vérifier l'intégrité et la disponibilité des sauvegardes.

Le stockage des données professionnelles exclusivement en local sur un poste de travail est proscrit, en raison de l'absence de garanties suffisantes en matière de disponibilité et de sécurité.

23 Comportements attendus

Chaque utilisateur est tenu d'adopter au quotidien les comportements suivants :

- respecter la présente charte ;
- faire preuve d'une vigilance constante face aux tentatives de manipulation, de fraude ou d'ingénierie sociale ;
- signaler sans délai aux équipes informatiques tout email, appel ou message suspect, sans y répondre ni interagir avec son contenu ;
- adopter une attitude de prudence systématique avant toute action impliquant des données sensibles ou des accès aux systèmes d'information ;
- participer activement aux actions de sensibilisation, aux formations et aux exercices de simulation organisés par le service informatique ;
- ne jamais communiquer ses identifiants, mots de passe ou tout autre moyen d'authentification, y compris à une personne se présentant comme membre du service informatique.

En cas de manquement constaté aux dispositions de la présente charte, le service informatique est tenu d'en informer la Direction. Selon la gravité des faits, les droits d'accès de l'utilisateur pourront être suspendus et tout logiciel illicite ou fichier suspect supprimé sans délai, outre la possibilité d'engager une procédure disciplinaire et/ou judiciaire.

24 Demandes particulières et contacts

Toute demande particulière relative à l'utilisation des systèmes d'information, notamment toute demande de dérogation aux dispositions de la présente charte, doit être formulée par écrit et adressée à la Direction informatique. La demande doit être motivée et validée par le responsable hiérarchique de l'utilisateur concerné.

La Direction informatique se réserve le droit d'accepter ou de refuser la demande au regard des exigences de sécurité, de conformité et de bon fonctionnement des systèmes d'information. Toute autorisation accordée peut être limitée dans le temps et soumise à des conditions spécifiques.

Pour toute question relative à l'utilisation des systèmes d'information, aux règles définies par la présente charte, les utilisateurs peuvent contacter la Direction informatique.

Pour toute question relative à la protection des données à caractère personnel ou à l'exercice des droits associés, les utilisateurs peuvent contacter le Délégué à la protection des données (DPO).