



territoire
d'énergie

LOIRE-ATLANTIQUE

CHA-OSID-001

Charte Informatique de
TE44

Etat du document

Version	Création	MaJ
1	12/04/2024	-

Historique des révisions

Version	Date	Objet
1	12/04/2024	Initialisation du document
2		
3		
4		
5		
6		
7		

Responsables

Rédacteur	Vérificateur	Approbateur
C. PINEAU	A.S. LAHMAR / C. HUMSKI	A. MIVIELLE

Critère de diffusion

- Restreint
- Confidentiel
- Interne
- Public

Sommaire

I.	INTRODUCTION	4
II.	PERIMETRE	5
III.	REFERENCE DOCUMENTAIRE	6
IV.	UTILISATION DES SYSTEMES D'INFORMATION ET DES OUTILS DE COMMUNICATION	6
	Moyens d'accès logiques	6
	Moyens d'accès physiques	7
	Messagerie électronique	7
	Accès Internet & Intranet	9
	Téléphonie	9
	Accès au Système d'Information à distance	10
	Utilisation des copieurs	10
	Fin d'utilisation et restitution des moyens	11
V.	PROTECTION DES LOCAUX ET DES RESEAUX	11
	Sécurité physique des locaux	11
	Supervision du réseau informatique	12
VI.	DONNEES PERSONNELLES A CARACTERE SENSIBLE	13
VII.	SANCTIONS APPLICABLES EN CAS DE NON-RESPECT	14

I. Introduction

Territoire d'Énergie Loire-Atlantique (TE44) met en œuvre un système d'information et de communication nécessaire à son activité, comprenant notamment un réseau informatique et téléphonique, ainsi que des équipements informatiques fixes et mobiles.

Les agents, dans l'exercice de leurs fonctions, sont conduits à accéder et à utiliser lesdits équipements informatiques, ainsi que les systèmes d'information et de communication mis à leur disposition.

L'utilisation du système d'information et de communication doit être effectuée exclusivement à des fins professionnelles, sauf exception prévue par la présente charte.

Par ailleurs, des tiers (salariés de structures hébergées, stagiaires, prestataires externes, partenaires...) peuvent également avoir accès aux équipements informatiques et aux systèmes d'information et de communication de TE44.

Dans un but de transparence à l'égard des utilisateurs, de promotion d'une utilisation loyale, responsable et sécurisée du système d'information et des équipements informatiques, la présente charte décrit les règles relatives à l'utilisation de ces ressources et ce, notamment dans le respect des règles spécifiques aux collectivités territoriales.

Cette charte a pour objectifs :

- De sensibiliser les utilisateurs aux risques liés à la sécurité informatique en matière de libertés et de vie privée, notamment lorsque leur activité implique de traiter des données à caractère personnel ;
- D'informer les utilisateurs sur :
 - Les usages permis des moyens informatiques mis à sa disposition ;
 - Les règles de sécurité en vigueur ;
 - Les mesures de contrôle mises en œuvre ;
 - Les sanctions éventuellement encourues ;
- De formaliser les règles générales de sécurité que les utilisateurs s'engagent à respecter en contrepartie de la mise à disposition des systèmes d'information et des équipements informatiques (droits et devoirs des utilisateurs).

Ces règles s'inscrivent dans une démarche responsable afin de protéger d'une part les conditions de fonctionnement, le patrimoine informationnel et l'image de marque de TE44, et d'autre part les libertés et la vie privée des personnes concernées que sont les agents et les tiers en lien avec TE44.

Le Directeur Organisation et Systèmes d'Information et Data (DOSID) ainsi que le Délégué à la Protection des Données personnelles (DPD) se tiennent à la disposition des utilisateurs qui souhaiteraient disposer d'informations ou de conseils complémentaires relatifs à l'usage des systèmes d'information et des équipements informatiques.

II. Périmètre

Personnel soumis aux présentes dispositions :

Les obligations décrites dans la présente charte s'appliquent à toute personne qui utilise les systèmes d'information de TE44. Il en est ainsi, notamment, des agents, des stagiaires, des intérimaires, des salariés de structures hébergées par TE44 et de manière générale, de tout utilisateur ayant obtenu des droits personnels d'utilisation.

Accès par des tiers aux systèmes d'information :

La présente charte devra être annexée au contrat de prestations conclus avec des tiers concernant l'informatique dans le cadre d'un contrat de sous-traitance.

Tout utilisateur extérieur à TE44 ayant été autorisé à accéder aux systèmes d'information de TE44 s'engage à respecter l'ensemble des dispositions de la présente charte.

Moyens informatiques et de communication électronique concernés :

La présente charte concerne l'ensemble des moyens informatiques et de communication électronique qui sont mis à la disposition des utilisateurs à des fins professionnelles exclusivement, ainsi que l'ensemble des moyens informatiques et de communication électronique qui sont la propriété personnelle de l'utilisateur, et pour lesquels celui-ci a obtenu une autorisation d'utilisation dans le cadre de son activité professionnelle.

Les systèmes d'information et de communication sont notamment constitués des éléments suivants :

- Ordinateurs portables ou fixes,
- Périphériques,
- Réseaux informatiques (serveurs, routeurs, connecteurs, bornes WIFI),
- Photocopieurs,
- Téléphones,
- Tablettes électroniques,
- Logiciels,
- Fichiers informatiques et bases de données,
- Espaces de stockage individuel,
- Messageries (courriel et instantanée),
- Connexions internet, intranet, extranet et VPN.

Les serveurs exposants des contenus applicatifs disponibles directement sur Internet (applications à destination des adhérents, site Internet TE44 etc.) disposent de leurs propres conditions d'utilisation et sont exclues du périmètre du présent document.

Déroghations possibles :

Toute demande de dérogation aux différents éléments définis dans le cadre de la présente Charte doit être présentée par écrit au Directeur Organisation, Systèmes d'Information et Données. L'arbitrage des demandes de dérogation est réalisé en concertation avec la direction générale.

III. Référence Documentaire

- Politique de Sécurité des Systèmes d'Information de TE44

IV. Utilisation des Systèmes d'Information et des outils de communication

L'accès à certains éléments du système d'information (comme la messagerie électronique ou téléphonique, les sessions sur les postes de travail, le réseau, certaines applications ou services interactifs) est protégé par des paramètres de connexion (identifiant, mot de passe, second facteur d'authentification ...).

Chaque utilisateur reçoit un droit d'accès individuel qui se matérialise par des moyens logiques (code utilisateur et mot de passe) ou physiques (badge, carte ...). Ces moyens sont personnels à l'utilisateur, il doit s'identifier personnellement et ne peut utiliser l'identité d'autrui (même avec l'accord de ce dernier).

Les droits d'accès sont révoqués lors d'un départ et peuvent être modifiés lors d'un événement le justifiant (changement de poste, détachement, etc.) ou s'il est constaté que l'utilisateur a enfreint l'une des obligations imposées par la présente charte.

Moyens d'accès logiques

Les moyens d'accès moyens logiques doivent être gardés confidentiels et ne peuvent être communiqués à aucun tiers quelle qu'en soit la justification (niveau hiérarchique, appartenance à l'équipe informatique etc.).

Les règles de tailles et de complexité des mots de passe sont inscrites dans la Politique de Sécurité des Systèmes d'Information de TE44. Ces dernières sont susceptibles d'évoluer afin de rester en conformité avec les référentiels de sécurité généraux et ces évolutions font l'objet de communications de la part du service Organisation et Systèmes d'Information et Data.

Les règles suivantes sont applicables pour l'ensemble des mots de passe utilisés

- Il est formellement interdit de stocker les mots de passe ailleurs que dans un coffre-fort numérique sécurisé. En particulier, la sauvegarde des mots de passe dans un fichier local, même protégé, ou par écrit sur un support physique est à proscrire ;
- Les mots de passe ne doivent en aucun cas être sauvegardés dans les navigateurs Internet ;
- Les mots de passe choisis doivent être différents pour chacun des systèmes mis à disposition de l'utilisateur ;
- Les mots de passe doivent être régulièrement changés. En particulier, il est impératif de modifier les mots de passe après tout soupçon de compromission.

Moyens d'accès physiques

Les moyens physiques doivent être conservés dans un espace personnel et sécurisé. Il est notamment formellement interdit de laisser les moyens d'accès physiques sans surveillance dans un véhicule. L'utilisateur s'engage à signaler immédiatement toute perte ou vol d'un moyen d'accès physique.

Lorsqu'ils sont choisis par l'utilisateur, les mots de passe doivent respecter le degré de complexité et les règles indiqués dans la Politique de Sécurité du Système d'Information de TE44.

Messagerie électronique

Principes généraux :

Chaque salarié dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique. Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un filtrage anti-spam. Les salariés sont invités à informer la direction informatique des dysfonctionnements qu'ils constateraient dans ce dispositif de filtrage.

L'attention des utilisateurs est attirée sur le fait qu'un message électronique a la même portée qu'un courrier manuscrit et peut rapidement être communiqué à des tiers. Il convient de prendre garde au respect d'un certain nombre de principes, afin d'éviter les dysfonctionnements du système d'information, de limiter l'envoi de messages non sollicités et de ne pas engager la responsabilité civile ou pénale de TE44 et/ou de l'utilisateur.

Les utilisateurs doivent veiller au respect des lois et règlements, et notamment à la protection des droits de propriété intellectuelle et des droits des tiers. Les correspondances électroniques des salariés doivent respecter les droits et obligations des agents publics, en particulier les obligations de neutralité, de laïcité, de secret et de discrétion professionnels, ainsi que le devoir de réserve.

Dans l'objectif d'une utilisation sobre des outils numériques, une limitation de la taille des messageries électroniques est mise en œuvre et l'utilisateur est invité à réaliser un tri des messages régulièrement ainsi qu'à privilégier, chaque fois que cela est possible, l'ajout d'un lien vers un document plutôt que l'ajout du document en pièce-jointe au message.

Envoi de messages électroniques :

Avant tout envoi, il est impératif de bien vérifier l'identité des destinataires du message et de leur qualité à recevoir communication des informations transmises. En présence d'informations à caractère confidentiel, de données à caractère personnel ou de données sensibles, ces vérifications doivent être renforcées ; en cas de besoin, un chiffrage des messages pourra être aussi proposé par le service Organisation et Systèmes d'Information et Data.

En cas d'envoi à une pluralité de destinataires, l'utilisateur doit respecter les dispositions relatives à la lutte contre l'envoi en masse de courriers non sollicités et notamment :

Accusé de réception en préfecture
044-200014926-20240620-BS-2024-10-DE
Date de réception préfecture : 24/06/2024

- La directive européenne n° 2002/58 du 12 juillet 2002 relative à la vie privée et aux communications électroniques ;
- La loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN), transposition de la directive "vie privée et communications électroniques" ;
- La loi n° 78 -17 du 6 janvier 1978 "informatique, fichiers et libertés" est applicable pour la collecte frauduleuse d'adresses électroniques.

Il doit également envisager l'opportunité de dissimuler certains destinataires, en les mettant en copie cachée, pour ne pas communiquer leur adresse électronique à l'ensemble des destinataires.

La signature des courriers électroniques fait l'objet d'une forme standardisée et gérée par le service Communication de TE44. Aucune modification de cette signature, de sa forme ou de son contenu n'est autorisée sans dérogation du service Communication.

Réception de messages électroniques :

L'utilisateur ne doit pas ouvrir, ni répondre à des messages électroniques tels que spam, messages électroniques répétés, tentatives manifestes d'hameçonnage, ni les transférer lorsque ceux-ci sont reçus à son insu sur leur messagerie électronique professionnelle ou ne présentent aucun rapport avec ses fonctions et ses attributions au sein de TE44. Il s'engage, dans pareil cas, à avertir le service Organisation et Systèmes d'Information et Data le plus rapidement possible.

Absences de l'utilisateur :

Lors d'une absence ou d'une indisponibilité planifiée (congrés, RTT, formation ...) et supérieure à deux jours consécutifs, l'utilisateur a pour obligation de paramétrer deux messages d'absences spécifiques, l'un pour les courriers internes et l'autres pour les courriers externes, indiquant à minima :

- Une phrase introductive comprenant une formule de politesse (ex : « Bonjour et merci pour votre courriel, ...)
- Les dates de début et de fin de son absence ou indisponibilité ;
- Les noms et coordonnées (adresse de messagerie et/ou numéro de téléphone) des agents à qui s'adresser en cas d'urgence.

L'utilisateur est informé et accepte qu'en cas d'absence prolongée le service Organisation et Systèmes d'Information et Data est autorisé, sur demande d'un responsable de service, à accéder à sa messagerie et à ses dossiers professionnels sans son consentement préalable.

En cas d'urgence ou pour des raisons motivées par la protection des intérêts et/ou de la qualité du service de TE44, le service Organisation et Systèmes d'Information et Data peut procéder à la réinitialisation des codes d'accès d'un utilisateur afin d'en obtenir l'accès.

Utilisation personnelle :

Les messages à caractère personnel sont tolérés s'ils respectent la législation en vigueur et sont en accord avec les principes édictés dans la présente charte.

Les messages reçus envoyés doivent être signalés par la mention « Privé », « Perso » ou « Personnel » dans leur objet et être classés dès l'envoi dans un dossier signalé par les mêmes mentions. Tout message ne respectant pas ces critères est présumé être à caractère professionnel.

Toutefois, les utilisateurs sont invités, dans la mesure du possible, à utiliser leur messagerie personnelle pour l'envoi de messages à caractère personnel plutôt que la messagerie de l'entreprise.

Accès Internet & Intranet

Dans le cadre de leur activité, les utilisateurs ont accès à Internet depuis le réseau informatique de TE44 via les terminaux informatiques qui leur sont fournis (PC, tablette, téléphone etc.). Le service Organisation et Systèmes d'Information et Data peut, pour des raisons de sécurité, limiter ou prohiber l'accès à certains sites. Celui-ci est habilité à imposer les versions et configurations des navigateurs ainsi qu'à restreindre ou interdire le téléchargement de certains fichiers.

Il est rappelé que les utilisateurs ne doivent en aucun cas se livrer à une activité illicite ou portant atteinte aux intérêts de TE44, y compris sur Internet.

Seule la consultation de sites ayant un rapport avec l'activité professionnelle est autorisée pendant le temps de travail.

En particulier, sont interdits :

- L'utilisation de l'Internet à des fins commerciales personnelles en vue de réaliser des gains financiers ou de soutenir des activités lucratives ;
- La création ou la mise à jour des pages personnelles et la consultation de réseaux sociaux personnels ;
- La consultation de sites de diffusion de médias (musique, vidéo ...) dont l'usage n'est pas strictement nécessaire dans le cadre des activités professionnelles ;
- La connexion à des sites Internet dont le contenu est contraire à l'ordre public, aux bonnes mœurs ou à l'image de marque de TE44, ainsi qu'à ceux pouvant comporter un risque pour la sécurité du système d'information.

Téléphonie

Principes généraux :

Pour leur activité professionnelle, les utilisateurs peuvent disposer d'un smartphone ou d'une tablette. L'utilisation de ces terminaux mobiles en connexion pour accès à des sites Internet ou à la messagerie électronique répond également aux règles édictées dans la présente charte.

Lorsque le smartphone fourni autorise l'utilisations de deux cartes SIM ou d'une carte SIM électronique (eSIM), l'ajout d'une carte SIM personnelle dans le smartphone est tolérée. En revanche, l'utilisation de la carte SIM professionnelle dans un terminal personnel est formellement interdite.

L'utilisateur est informé qu'un journal des communications entrantes et sortantes de son numéro professionnel est accessible par le service Organisation et Systèmes d'Information et Data. Ces relevés de communication peuvent faire l'objet d'un contrôle.

Les terminaux mobiles fournis par TE44 peuvent être enrôlés dans un système de gestion de la flotte mobile dans l'objectif de :

- Maîtriser le déploiement des applications mobiles
- Maîtriser la politique de mise à jour
- Géolocaliser le terminal

La géolocalisation du terminal ne peut être activée par les personnels du service Organisation et Systèmes d'Information et Data que dans les cas suivants :

- Perte ou vol du téléphone
- Nécessité de porter secours au détenteur
- Réquisition de l'autorité publique (services de police, gendarmerie)

Engagements de l'utilisateur :

L'utilisateur s'engage en outre à :

- Prévenir sans délai en cas de perte, vol ou faille de sécurité ;
- Mettre en œuvre tous les moyens de sécurité prévus par les fonctionnalités du smartphone, notamment le code d'accès (pin, verrouillage du terminal) ;
- Accepter systématiquement toutes les mises à jour proposées par le système du terminal ;
- Se déconnecter de toutes les applications après usage et ne pas rester connectés par défaut ;
- Conserver ses terminaux dans un espace personnel et sécurisé. Il est notamment formellement interdit de laisser les terminaux sans surveillance dans un véhicule.

Utilisation personnelle du smartphone :

L'utilisation à caractère personnel du smartphone est tolérée, à condition qu'elle reste raisonnable et qu'elle :

- Soit réalisée uniquement à partir de la France métropolitaine ;
- N'engendre aucun surcoût particulier pour TE44 ;
- Soit réalisée dans le cadre strict de la législation ;
- Ne présente aucun risque pour la sécurité du terminal et du système d'information.

Accès au Système d'Information à distance

L'ensemble des dispositions de la présente charte sont applicables aux utilisateurs accédant aux systèmes d'information et de communication de TE44 à distance.

L'accès à distance du Système d'Information par du matériel informatique personnel est formellement interdite.

Utilisation des copieurs

Des copieurs multifonction sont mis à disposition des utilisateurs du système d'information de TE44.

Accusé de réception en préfecture
044-200014926-20240620-BS-2024-10-DE
Date de réception préfecture : 24/06/2024

Dans un souci de sobriété, il est demandé aux utilisateurs de faire usage de l'impression seulement dans les cas où cela est strictement nécessaire. Dans la mesure du possible, les impressions recto/verso en noir et blanc doivent être privilégiées.

Lorsque l'utilisateur doit imprimer un document à diffusion confidentielle ou restreinte, il lui appartient d'être vigilant et de récupérer le document immédiatement lors de son impression. L'usage de la fonction d'impression confidentielle des copieurs est fortement recommandé.

L'usage ponctuel et raisonnable des copieurs à des fins personnelles est toléré par TE44.

Fin d'utilisation et restitution des moyens

Lors de son départ de TE44, l'utilisateur doit respecter la procédure de départ et remettre l'ensemble des moyens informatiques et de communication électronique qui lui ont été attribués au service Organisation et Systèmes d'Information et Data. Il est formellement interdit de conserver du matériel informatique, des moyens logiques ou physiques permettant d'accéder au système d'information ou aux locaux de TE44.

En outre, il est formellement interdit pour l'utilisateur de conserver des données appartenant à TE44 ou relatives à son service au sein de TE44, quelle que soit leur forme (fichiers, documents papier etc.) et ce même s'il a contribué à leur établissement.

Sauf nécessité liée à la continuité du service et pour un temps raisonnable qui ne saurait excéder trois mois, le compte messagerie et les identifiants de l'utilisateur sont désactivés le jour de son départ. Les données de messagerie peuvent être conservées par TE44 pendant une durée maximum de deux ans après le départ du salarié.

Dans le cas où le compte messagerie est toujours actif après le départ d'un utilisateur, une redirection des messages vers un autre utilisateur peut être mise en place.

V. Protection des locaux et des réseaux

Dans l'intérêt légitime de sécurité de TE44, les locaux sont équipés des systèmes de protection et de contrôle d'accès. Une supervision globale du réseau informatique est également assurée de manière permanente.

Sécurité physique des locaux

La sécurité physique des locaux est assurée par :

- Des lecteurs de badges contrôlant l'accès aux locaux depuis l'extérieur ;
- Des contrôles d'accès physiques aux locaux techniques sensibles (salle serveur etc.) ;

Accusé de réception en préfecture
044-200014926-20240620-BS-2024-10-DE
Date de réception préfecture : 24/06/2024

- Des caméras positionnées en périphérie extérieure des locaux ainsi que dans les espaces de circulation intérieurs ;
- Un système d'alarme.

Objet du traitement :

Les données recueillies par les systèmes de sécurité physique sont conservées sur des enregistreurs dédiés au sein de la salle serveur de TE44. Les données enregistrées dans ce dispositif ne sont pas utilisées à des fins de surveillance du personnel ni de contrôle des horaires.

La base légale du traitement est l'intérêt légitime (cf. article 6.1.f du Règlement européen sur la protection des données).

Catégories de personnes concernées :

Les collaborateurs de TE44 sont tous concernés par ces dispositifs. Les visiteurs occasionnels des locaux de la société sont également susceptibles d'être filmés.

Destinataires :

Les images peuvent être visionnées, en cas d'incident, par le personnel habilité de TE44 (service Ressources Humaines et Moyens Généraux) et par les forces de l'ordre. Les personnels de la société en charge de la maintenance du matériel peuvent également accéder aux images, à cette seule fin.

Durée de conservation :

Les données collectées sont conservées pendant 90 jours. En cas d'incident lié à la sécurité des personnes et des biens, les images de vidéosurveillance peuvent néanmoins être extraites du dispositif. Elles sont alors conservées sur un autre support le temps du règlement des procédures liées à cet incident et accessibles aux seules personnes habilitées dans ce cadre.

Supervision du réseau informatique

La supervision du réseau informatique et de ses actifs est assurée par :

- Les systèmes de gestion du trafic entrant et sortant (pare-feu) ;
- Les systèmes de gestion des informations et des événements de sécurité (SIEM) ;
- Les outils de gestion et de supervision des postes fixes et mobiles.

Objet du traitement :

Les données recueillies par les systèmes de gestion et de supervision sont conservées sur des serveurs dédiés au sein d'un infocentre sécurisé et situé sur le territoire français. Les données enregistrées par ces dispositifs sont utilisées à des fins d'anticipation des incidents informatiques ainsi qu'en cas de doute concernant le respect des règles édictées dans la présente charte.

La base légale du traitement est l'intérêt légitime (cf. article 6.1.f du Règlement européen sur la protection des données).

Catégories de personnes concernées :

Tous les utilisateurs du réseau informatique TE44 sont concernés par ces dispositifs, y compris les utilisateurs occasionnels (sous-traitants, stagiaires etc.).

Destinataires :

Les données recueillies par les dispositifs de supervision du réseau informatique peuvent être exploitées par le personnel technique habilité de TE44 (Administrateur Système et Technicien Système) ainsi que par les sous-traitants de TE44 intervenants dans les domaines de la sécurité informatique et de la gestion des infrastructures.

En cas d'incident, ces données peuvent être transmises aux forces de l'ordre ou aux autorités nationales en charge du suivi et de l'accompagnement en période de crise (Agence Nationale de la Sécurité des Systèmes d'Information, etc.).

Durée de conservation :

Les données collectées sont conservées pendant 1 an.

VI. Données personnelles à caractère sensible

La Loi n° 78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés, dite Loi Informatique et Libertés, l'ordonnance n° 2018-1125 du 12 décembre 2018, ainsi que le Règlement Général sur la Protection des Données (RGPD) définissent les conditions dans lesquelles des traitements de données à caractère personnel peuvent être opérés.

Conformément à ces dispositions, l'utilisateur peut être désigné comme Responsable d'un Traitement (RT) par le Délégué à la Protection des Données personnelles (DPD) de TE44.

A cet égard, le RT s'engage à informer les utilisateurs à :

- Ne pas utiliser les données à caractère personnel auxquelles ils peuvent accéder à des fins autres que celles prévues par leurs 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 lorsque cela n'est pas strictement nécessaire à l'exécution de leurs fonctions ;
- Prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de leurs 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 ;
- Assurer, dans la limite de leurs attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;
- Ne pas accéder, tenter d'accéder ou supprimer les données en dehors de leurs attributions ;

Accusé de réception en préfecture
044-200014926-20240620-BS-2024-10-DE
Date de réception préfecture : 24/06/2024

- Respecter les droits des personnes concernées (droit d'accès, de rectification, d'opposition, effacement...) conformément aux procédures mises en place ;
- Restituer intégralement, en cas de cessation de leurs fonctions, les données, fichiers informatiques et tout support d'information relatif à ces données.

VII. Sanctions applicables en cas de non-respect

Il convient de rappeler qu'en cas de manquement aux obligations mentionnées au précédent paragraphe, TE44 ainsi que le RT peuvent être passibles de sanctions importantes, qu'elles soient administratives, civiles ou pénales.

Indépendamment des sanctions précitées, les agents de TE44 qui ne respecteraient pas les dispositions prévues par la présente charte pourraient se voir sanctionnés disciplinairement dans les conditions prévues par la réglementation en vigueur.