GRANDE COURONNE

REPUBLIQUE FRANCAISE
LIBERTE - EGALITE- FRATERNITE

SEANCE ORDINAIRE DU CONSEIL D'ADMINISTRATION DU 02 AVRIL 2024

37 membres en exercice
17 présents – 12 pouvoirs – 29 votants
Convocation adressée et publiée le 26 mars 2024

L'an deux mille vingt-trois, le 02 avril à 10 heures 30, le Conseil d'Administration, légalement convoqué, s'est assemblé en partie au lieu ordinaire de ses séances, sous la présidence de Daniel LEVEL, Maire de la commune déléguée de Fourqueux (78).

Etaient présents :

Marie-Hélène AUBERT Vice-présidente du Conseil départemental des Yvelines, Maire de Jouy-en-Josas (78) - Laurence BACLE Adjointe au Maire de Villiers-Saint-Frédéric (78) - Marie-Josée BEAULANDE Maire d'Eaubonne (95) - Myriam BRENAC Maire de Chavenay (78) - François-Gilles CHATELUS Adjoint au Maire de Versailles (78) - Michel DELAMAIRE Adjoint au Maire de Feucherolles (78) - Huguette FOUCHE Conseillère régionale, Adjoint au Maire de Montesson (78) - Nicolas KOWBASIUK Adjoint au Maire de Taverny (95) - Christian LAGIER Vice-Président de la Communauté d'agglomération de Plaine Vallée, Maire de Piscop (95) - Laurent LAMBERT Vice-Président de la Communauté d'Agglomération de Cergy-Pontoise, Adjoint au Maire de Pontoise (95) - Florence MARY Adjointe au Maire de Soisy sous Montmorency (95) - Anne PELLETIER LE BARBIER Maire de Bièvres (91) - Denise PLANCHON Vice-Présidente de la Communauté de Communes Cœur d'Yvelines, Maire de Neauphle-le-Vieux (78) - Martine QUIGNARD Maire de Lainville-en-Vexin (78) - Nadine RIBERO Adjointe au Maire d'Athis-Mons (91) - Sylvain TANGUY Maire du Plessis-Pâté (91)

Pouvoirs :

Laetitia BOISSEAU Conseillère départementale du Val d'Oise (95) donne pouvoir à Daniel LEVEL Maire de la commune déléguée de Fourqueux (78) - Dominique BOUGRAUD Présidente déléguée du Conseil départemental de l'Essonne (91) donne pouvoir à Anne PELLETIER LE BARBIER Maire de Bièvres (91) - Martine CINOSI – GIRARD Conseillère départementale de l'Essonne (91) donne pouvoir à Laurence BACLE Adjointe au Maire de Villiers-Saint-Frédéric (78) - Grégory GARESTIER Conseiller départemental des Yvelines – Maire de Maurepas (78) donne pouvoir à Michel DELAMAIRE Adjoint au Maire de Feucherolles (78) - Josette JEAN Conseillère départementale des Yvelines, Maire de Condé-sur-Vesgre (78) donne pouvoir à Marie-Hélène AUBERT Vice-présidente du Conseil départemental des Yvelines, Maire de Jouy-en-Josas (78) - Raoul JOURNO Adjoint au Maire du Plessis-Bouchard (95) donne pouvoir à Laurent LAMBERT Vice-Président de la Communauté d'Agglomération de Cergy-Pontoise, Adjoint au Maire de Pontoise (95) - Jean-René MARTEL Adjoint au Maire d'Herblay (95) donne pouvoir à Nicolas KOWBASIUK Adjoint au Maire de Taverny (95) - Sylvie PESLERBE Adjointe au Maire d'Asnières-sur-Oise (95) donne pouvoir à Denise PLANCHON Vice-Présidente de la Communauté de Communes Cœur d'Yvelines, Maire de Neauphle-le-Vieux (78) - Alexandra ROSETTI Vice-Présidente de la Communauté d'Agglomération de Saint-Quentin-en-Yvelines, Maire de Voisins-le-Bretonneux (78) donne pouvoir à Myriam BRENAC Maire de Chavenay (78) - Abdoulaye SANGARE Adjoint au Maire de Cergy (95) donne pouvoir à Nadine RIBERO Adjointe au Maire d'Athis-Mons (91) - Dominique VEROTS Maire de Saint-Pierre-du-Perray (91) donne pouvoir à Florence MARY Adjointe au Maire de Soisy sous Montmorency (95) - Francisque VIGOUROUX Maire d'Igny (91) donne pouvoir à Sylvain TANGUY Maire du Plessis-Pâté (91).

Absents, excusés :

Benjamin CHKROUN Conseiller régional, Adjoint au Maire d'Enghien-les-Bains (95) - Gabriel CRUZILLAC Adjoint au Maire d'Arpajon (91) - Nathalie JAQUEMET Adjointe au Maire de Bougival (78) - Françoise NORDMANN Maire de Beauchamp (95) - Cédric PEMBA-MARINE Maire du Port-Marly (78) - Éric TONDU Maire de Maulette (78) - Jean-François VIGIER Vice-Président de la Communauté d'agglomération Paris-Saclay, Maire de Bures-sur-Yvette (91).

Délibération n° 2024-25 portant sur l'adoption de la Charte informatique

Le président,
Certifie sous sa responsabilité le caractère exécutoire de cet acte
Informe que la présente délibération peut faire l'objet d'un recours pour excès de pouvoir devant le Tribunal Administratif, dans un délai de 2 mois à compter de la présente publication

Publié le 04 avril 2024

Délibération 2024 – 25

Objet

Adoption de la Charte informatique

Le CIG met en œuvre un système d'information et de communication, nécessaire à l'exercice de ses missions, comprenant notamment un réseau informatique et téléphonique. Il offre aux agents une ouverture vers l'extérieur et leur permet de disposer de moyens de communication électronique, de ressources informatiques, informationnelles, numériques et technologiques.

Ces outils se révèlent être des vecteurs de modernisation du CIG, si leur utilisation est faite à bon escient, dans le respect des usages et de la législation en vigueur. A l'inverse, une mauvaise utilisation de ces outils peut engendrer des risques d'atteinte à la confidentialité, à la disponibilité, à l'intégrité de l'information et du système d'information. Celle-ci peut donc avoir des conséquences graves, techniques mais également juridiques et de nature à engager la responsabilité civile et/ou pénale de l'établissement et de ses agents.

La présente charte, validée par le Comité Social Territorial en date du 29 juin 2023, s'inscrit dans une démarche d'information, de sensibilisation, de responsabilisation des utilisateurs des moyens de communication électronique et du système d'information du CIG. Elle a pour objet de fixer les règles générales et permanentes d'utilisation du système d'information professionnel et des outils numériques confiés aux agents. En particulier, elle définit les conditions d'accès et les règles d'utilisation d'outils informatiques (ordinateurs, téléphones, logiciels, etc.). Elle a également pour objet de sensibiliser les utilisateurs aux risques d'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées.

La présente charte s'applique à tous les personnels employés par l'établissement, quel que soit leur statut, ainsi qu'aux utilisateurs invités.

Le Conseil d'administration,

- Vu le Code général des collectivités territoriales ;
- Vu le Code général de la fonction publique ;
- Vu le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) ;
- Vu la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;
- Vu le décret n°2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;
- Vu l'avis du Comité social territorial du 29 juin 2023 ;
- Vu le projet de charte annexé ;
- Considérant la nécessité, pour le CIG, de maintenir l'intégrité de son système d'information ;
- Considérant la volonté du CIG d'être en mesure de garantir un niveau de performance satisfaisant à tous les utilisateurs des ressources informatiques, numériques et de communication ;
- Vu l'exposé du président ;

Après en avoir délibéré,
A l'unanimité des votants,

- Approuve la Charte informatique pour les utilisateurs du système d'information du CIG ;
- Autorise son annexion au Règlement intérieur du CIG.

Pour extrait conforme,

Le président

Daniel LEVEL
Maire de la commune déléguée de Fourqueux

Conseil d'administration du 02 avril 2024

Charte informatique CIG

Sommaire

INTRODUCTION

La présente charte a été approuvée par le Comité Social Territorial du 29/06/2023 et entre en vigueur à compter de son adoption par le conseil d'administration.

Le Centre Interdépartemental de Gestion de la Grande Couronne met en œuvre un Système d'Information et de communication nécessaire à l'exercice de ses missions. Il met ainsi à disposition des agents des outils informatiques et de communication.

La présente charte définit les conditions d'accès et les règles d'utilisation sécurisées des moyens informatiques et des outils de communication du CIG. Elle a également pour objet de sensibiliser les utilisateurs aux risques liés à l'utilisation de ces ressources en termes d'intégrité, de confidentialité et de disponibilités des informations traitées.

Ces risques imposent à l'agent le respect de règles de sécurité et de bonne conduite. L'imprudence, la négligence ou la malveillance d'un utilisateur peuvent en effet avoir des conséquences graves de nature à engager la responsabilité civile ou pénale de l'agent ainsi que celle du CIG.

Certains documents peuvent renforcer ou compléter les règles générales de la charte, il appartient à l'utilisateur de prendre connaissance de ces textes dans le cadre de ses missions.

CHAMP D'APPLICATION DE LA CHARTE

La présente charte s'applique à tous les agents du CIG ainsi que l'ensemble des personnes habilitées par un donneur d'ordre du CIG qui utilisent les ressources informatiques et les moyens de communication dans l'exercice de leurs missions.

L'utilisation à titre privé de ces outils est tolérée, mais doit être raisonnable et ne doit pas perturber le bon fonctionnement du service. La charte est systématiquement remise à tout nouvel arrivant, soit par voie numérique, soit en main propre au format papier.

Des actions de communication interne sont organisées régulièrement afin d'informer et sensibiliser les utilisateurs aux pratiques recommandées.

LEXIQUE

Utilisateur
Désigne les fonctionnaires, agents contractuels, apprentis ou encore stagiaires du CIG utilisant les ressources du Système d'Information, ainsi que les éventuels salariés de sociétés extérieures.

Système d'Information
Ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) qui permet de regrouper, classifier, traiter et diffuser de l'information sur un environnement donné.

Administrateur système et réseau
Membre de la DSI en charge des ressources informatiques. Ses missions principales permettent le maintien en condition opérationnelle des infrastructures informatiques. Il a également un rôle de supervision des infrastructures techniques du CIG (moyens d'accès internet et téléphonique, serveurs bureautiques, de messagerie), il intervient physiquement ou à distance sur les postes utilisateurs en cas de problème ou d'incident. Il est soumis au secret professionnel en ce qui concerne les données personnelles ou confidentielles dont il pourrait être amené à prendre connaissance dans l'exercice de ses fonctions.

Administrateur fonctionnel / métier
Membre du CIG ayant dans son périmètre de responsabilité un accès privilégié à une application métier lui permettant d'administrer tout ou partie de l'application (exemple : création de compte utilisateur ou affectation de droits). Il est également soumis au secret professionnel concernant la confidentialité des données (fiches de paie…).

Ressources / moyens / actifs / outils informatiques
Tous les équipements et logiciels informatiques du CIG, gérés par la DSI, interconnectés ou non entre eux, postes de travail (PC fixe ou portable), imprimantes, téléphones (fixe, virtuel, ou mobile), réseau, Internet, messagerie, logiciels métiers, etc…

Internet
Interconnexion mondiale de réseaux reposant sur un protocole appelé « Internet » et dont les applications les plus utilisées sont le courriel et les consultations de sites (Web).

Intranet
Réseau informatique utilisé et accessible uniquement à l'intérieur d'une organisation.

Courriel
Message électronique.

Réseau
Ensemble d'ordinateurs et d'équipements informatiques qui communiquent grâce à une technique commune de transmission.

REGLES GENERALES D'UTILISATION DU SYSTEME D'INFORMATION DU CIG

Chaque agent accède aux outils informatiques nécessaires à l'exercice de son activité professionnelle dans les conditions suivantes définies par le CIG.

1. Les acteurs de l'infrastructure informatique modalités d'intervention de la DSI

La Direction responsable du Système d'Information (DSI) est en charge de définir, de maintenir et de faire évoluer le Système d'Information pour satisfaire aux besoins du CIG.
Elle est composée de 3 services :

- Le Service Exploitation et Assistance Utilisateurs : assure l'assistance utilisateur, la sécurité et le maintien en condition opérationnelle du Système d'Information du CIG ;
- Le Service Applicatif et Projets : assure l'assistance utilisateur sur les applications métier et l'escalade aux éditeurs si besoin, suit les demandes d'évolution et prend en charge les demandes de nouveaux outils et projets informatiques ;
- Le Service SIRH : assure l'assistance utilisateurs à destination des services utilisant les solutions informatiques de gestion des ressources humaines du CIG.

Le Délégué à la protection des données (DPD),
Le délégué à la protection des données est un agent du CIG dont le rôle est de veiller à ce que les responsables de traitement respectent leurs obligations en matière de protection des données et que les personnes concernées soient informées de leurs droits et de leurs obligations au titre du règlement (UE) 2018/1725.

Le Responsable de la Sécurité des Systèmes d'Information (RSSI)
Le responsable de la sécurité des systèmes d'information est un agent du CIG qui travaille avec l'ensemble des directions et services afin d'assurer au mieux la continuité, la disponibilité et l'intégrité des Systèmes d'Information ainsi que le respect des réglementations applicables. Il collabore activement avec le DPD en assurant la sensibilisation des agents aux risques cyber.

2. L'authentification

L'accès aux principales ressources informatiques (connexion au poste de travail, accès aux serveurs bureautiques, connexion GLPI…) repose sur l'utilisation d'un identifiant de compte fourni à l'utilisateur lors de son arrivée au CIG. Un mot de passe est associé à cet identifiant de connexion. Les moyens d'authentification sont personnels et confidentiels. Le mot de passe doit être composé de 12 caractères minimums combinant chiffres, lettres (majuscule et minuscule) et caractères spéciaux. Il ne doit comporter ni le nom, ni le prénom, ni l'identifiant d'ouverture de la session de travail. Au bout de 365 jours sans modification, le mot de passe expire et les agents sont invités à le renouveler. Les mots de passe utilisateurs étant chiffrés pour des raisons de sécurité, les administrateurs n'ont pas de moyen technique d'accéder ou de prendre connaissance de ces derniers.
Les mêmes préconisations relatives à la complexité et au changement des mots de passe doivent être appliquées pour les mots de passe des applications.

3. Les règles de sécurité et devoirs de l'utilisateur

Tout utilisateur doit respecter les règles de sécurité suivantes :

- Conserver ses informations d'authentification individuelle de manière sécurisée (ne jamais confier ou écrire son identifiant / mot de passe sur un support accessible librement type post-it, cahier ou répertoire consultable facilement…) ;
- Ne pas installer de logiciels sans autorisation de la DSI[1] ;
- Ne pas apporter volontairement des perturbations au bon fonctionnement des ressources informatiques et des réseaux que ce soit par des manipulations anormales du matériel ou par l'introduction de logiciels parasites (virus, malware, chevaux de Troie, logiciel de scan, etc.) ;
- Ne pas copier, modifier, altérer les logiciels installés par la DSI ;
- Laisser toutes analyses antivirales s'exécuter librement ;
- Ne pas copier de données professionnelles sur un support externe, à des fins de sauvegarde, sans avoir sécurisé ce dernier par un chiffrement des données ;
- Utiliser le logiciel NetExplorer pour transmettre ou recevoir tout document contenant des données personnelles ou sensibles vers l'extérieur ;
- Ne pas utiliser des sites de transfert de fichiers hébergés sur Internet ne respectant pas le RGPD (type Dropbox, Skydrive, Wetransfer, MegaUpload, FTP, etc…) mais privilégier l'utilisation de NextExplorer, Swiss Transfer, drop.infini.fr, lufi.ethibox.fr, drop.chapril.org… ;
- Verrouiller son ordinateur dès qu'il quitte son poste de travail (touche « Windows » + « L ») ;
- Signaler à la DSI toute violation ou tentative de violation suspectée de son compte réseau et de manière générale tout dysfonctionnement constaté ;
- Avertir la DSI si l'agent se rend compte qu'il accède à des ressources informatiques dont il n'a pas la nécessité dans le cadre de ses missions (répertoire sur le réseau, accès à une application) ;
- Laisser l'exécution des programmes de mises à jour.

Parallèlement à ces règles, tout utilisateur :

- Est responsable du matériel qui lui est confié et doit en respecter l'intégrité ;
- Est responsable du bon usage de ses identifiants, mots de passe, droits d'accès attribués ;
- Est responsable de l'information qui lui est confiée et doit prendre toutes les précautions nécessaires afin de préserver l'intégrité et la confidentialité des données qu'il traite ou échange ;
- Doit respecter les consignes de sécurité énoncées dans la présente charte.

En outre, il convient de rappeler que les visiteurs ne peuvent avoir accès au Système d'Information du CIG sans l'accord préalable de la DSI.

[1] Les agents du service Conseil en Informatique et Communication ne sont pas concernés par cette restriction car dans le cadre de leurs missions, ils ont la nécessité d'installer régulièrement des applications sur leur ordinateur.

LE ROLE DES ADMINISTRATEURS ET LES MESURES DE CONTRÔLE

Afin de superviser le fonctionnement et de garantir la sécurité du Système d'Information du CIG, différents dispositifs sont mis en place.

1. Le rôle des administrateurs

L'administrateur du Service Exploitation assure et maintient la sécurité du Système d'Information, notamment par l'installation du système d'exploitation des postes de travail et des mises à jour nécessaires.

Il accompagne les utilisateurs dans l'utilisation des moyens informatiques et de communication notamment par l'information, l'assistance à la résolution de problèmes techniques, et l'information des contraintes de service liées au maintien du bon fonctionnement des moyens informatiques et de communication (ex : interruption de service, maintenance…). Les administrateurs peuvent être sollicités depuis l'application de gestion des demandes et des incidents (https://glpi.cigversailles.fr). Il est également possible de les contacter par courriel (pole.exploitation@cigversailles.fr) ou par téléphone (01 39 49 70 00 depuis l'extérieur ou au 70 00 depuis le CIG). Dans le cadre du bon suivi des interventions, il est préférable de les solliciter principalement par GLPI.

Il intervient sur les outils d'administration du Système d'Information.

Il peut avoir momentanément accès aux ressources informatiques indispensables à la poursuite de l'activité du service, si possible après avoir informé l'utilisateur ou sur sollicitation du supérieur, et à l'exclusion de l'accès aux données clairement identifiées comme personnelles.

Il analyse les éléments source de problèmes techniques.

La prévention et la résolution de problèmes techniques autorisent les administrateurs à analyser un certain nombre d'éléments relatifs aux flux réseaux et aux volumes stockés et notamment :

- Les fichiers stockés (format, taille, date, contenus…) ;
- Les ressources matérielles et logicielles ;
- Les connexions au réseau (identifiants, dates et heures de connexions…) ;
- Les échanges via le réseau ;
- Les connexions Internet (identifiants de connexion, volumes de données transférées, dates et heures de connexion…) ;
- Les messages stockés (fréquence, taille des fichiers transmis…).

En revanche, les administrateurs n'ont aucun moyen d'accéder aux mots de passe des utilisateurs.

Dans ce cadre, la confidentialité des données sera respectée (devoir de réserve et secret professionnel des agents publics).

2. Les mesures de contrôle

Afin de se conformer aux dispositions légales en vigueur, le CIG met en place des outils de collecte d'informations des données transitant sur son Système d'Information.
Ces mesures de contrôle n'ont pas pour but de réaliser un suivi individuel et régulier de l'activité des utilisateurs mais permettent d'identifier de manière pro-active tout dysfonctionnement éventuel ou facilitent le diagnostic et la résolution d'incident(s) en cours.

Contrôles automatisés
Le Système d'Information et de communication s'appuie sur des fichiers journaux (« logs ») ou des fichiers de traces (cookies par exemple), créés en grande partie automatiquement par les équipements informatiques et de télécommunication ou à l'occasion de l'utilisation de services informatiques internes ou externes. Ces fichiers sont stockés sur les postes informatiques, sur les serveurs et sur les équipements réseaux. Ils permettent d'assurer le bon fonctionnement du système, en protégeant la sécurité des informations du CIG, en détectant des erreurs matérielles ou logicielles et en contrôlant les accès et l'activité des utilisateurs et des tiers accédant au Système d'Information.

A des fins d'exploitation informatique ou d'obligation légale, sont notamment surveillées et conservées pendant 3 à 12 mois les données relatives :

- À l'utilisation des logiciels pour contrôler l'accès, les modifications et suppressions de fichiers ;
- Aux connexions entrantes et sortantes au réseau interne ;
- À la consultation de sites Internet ;
- Aux flux de messagerie ;
- Aux tentatives d'intrusion ;
- Aux téléchargements de fichiers.

Procédure de contrôle manuel
En cas de dysfonctionnement constaté par la DSI ou en cas de violation de la Charte, l'administrateur est habilité à procéder à un contrôle manuel et à une vérification de toutes opérations effectuées par un ou plusieurs utilisateurs.

RESSOURCES INFORMATIQUES ET REGLES SPECIFIQUES

1. Le poste de travail

Le CIG met à disposition de chaque utilisateur un poste de travail doté des outils informatiques nécessaires à l'accomplissement de ses fonctions et dont il est responsable. Lors de l'arrivée d'un nouvel agent au CIG, le responsable de service sollicite les moyens informatiques à fournir à l'agent pour la bonne exécution de ses missions.

En cas de perte du matériel, il incombe à l'utilisateur de prévenir **sans délai** la DSI.

En dehors des trajets effectués par l'agent, la conservation de l'ordinateur dans le véhicule (coffre ou habitacle) n'est pas autorisée.

En dehors des déplacements internes sur site, le poste doit être protégé par un équipement adapté à son transport (sacoche, sac à dos…).

Afin de minimiser les risques de perte ou de vol, l'utilisateur doit s'assurer de la sécurité physique de son pc (utilisation de câble antivol, mise sous clé du pc), surtout lorsqu'il s'absente de son bureau.

L'utilisation de matériel personnel (clavier / souris sans fil, casque audio…) est autorisée après validation de la DSI.

2. Messagerie

Le CIG met à disposition des agents une messagerie accessible depuis Internet. En cas d'absence d'un agent, une redirection des mails par message d'absence ou transfert automatique des mails vers une autre adresse mail interne doit être organisée. Ce choix est défini par chaque responsable de service.

Une vigilance particulière doit être portée lors de l'utilisation de la messagerie pour ne pas engager indûment la responsabilité du CIG. Par ailleurs, la messagerie ne se substitue pas au courrier papier, notamment lorsque le contenu du message doit comporter le visa de l'autorité territoriale, ou de la personne habilitée à cet effet conformément aux délégations de signature en vigueur.

La messagerie du CIG ne doit pas être utilisée pour faire des envois vers l'extérieur de messages « en masse » afin d'éviter toute saturation de l'outil en interne et pour que les serveurs de messagerie du CIG ne soient pas inscrits automatiquement sur liste noire au niveau mondial.
En cas de besoin ponctuel, le service communication possède les outils permettant de faire des envois en masse.

L'utilisation de raccourcis ou liens pointant vers un fichier bureautique accessible par l'ensemble des destinataires est à privilégier plutôt que de transmettre les pièces jointes par mail afin d'éviter la démultiplication des données et la saturation des boîtes aux lettres.

Dans le cadre de l'usage de la messagerie professionnelle, l'utilisateur doit signaler toute erreur ou correction à effectuer vis-à-vis de la constitution des groupes de distribution par défaut du CIG.

D'autre part, l'utilisateur ne doit pas :

- Mettre en œuvre une redirection automatique ou réplication de messages vers une adresse électronique externe. Le transfert de messages, ainsi que leurs pièces jointes, à caractère professionnel sur des messageries personnelles est interdit ;
- Utiliser la messagerie d'autrui sans l'autorisation expresse de la personne concernée et sans que la situation ne la réclame ;
- Relayer des chaines, tout canular ou informations non vérifiées.

- Transmettre par mail, que ce soit dans le corps du mail ou par pièce jointe, des données personnelles sensibles telles que le numéro de sécurité sociale, des données de santé, des pièces d'identité, des bulletins de salaire et autres données aussi confidentielles. Cette transmission doit passer par des moyens sécurisés (fichier partagé sur le réseau en interne et solutions de transfert sécurisé – NetExplorer - pour les envois externes).

L'utilisation à des fins personnelles de la messagerie est tolérée. Il est cependant fortement recommandé de préfixer l'objet de ces messages par le texte « Personnel » ou « Privé » afin d'identifier clairement ce message comme n'étant pas à caractère professionnel.

Chaque boite aux lettres dispose d'un espace de stockage de 5 Go. Il est vivement recommandé d'archiver ses messages afin d'éviter toute saturation et toute perte d'information. Une fiche d'assistance utilisateur indiquant la procédure est disponible auprès de la DSI. Il incombe donc à chacun de gérer son archivage.

En cas d'absence ou de départ d'un agent et afin d'assurer une continuité de service, la DSI est autorisée à accéder à la messagerie professionnelle d'un agent sur sollicitation du supérieur hiérarchique.

Le système de messagerie est protégé par un logiciel antispam et par un antivirus. Cependant, il est possible qu'un courriel malveillant puisse passer ces éléments de protection. En cas de doute sur la légitimité d'un message reçu, l'utilisateur doit respecter les règles suivantes :

- Ne pas ouvrir de documents ou cliquer sur un lien dont l'origine est inconnue ;
- Ne jamais répondre à une demande d'informations personnelles par courriel quel qu'en soit l'expéditeur ;
- Ne jamais communiquer de données à caractère personnel (données bancaires, numéro de sécurité sociale) ou permettant un accès aux systèmes d'information (mot de passe et identifiant) ;
- Signaler immédiatement tout message suspect au Service Exploitation par courriel ou par téléphone.

Rappel :
L'accès au poste informatique ou à la messagerie
L'employeur doit respecter le secret des correspondances privées. Une communication électronique émise ou reçue par un agent peut avoir le caractère d'une correspondance privée. La violation du secret des correspondances est une infraction pénalement sanctionnée par l'article L.432-9 du Code pénal.

La Cour de cassation a affirmé, dans un arrêt du 2 octobre 2001 (arrêt « Nikon »), qu'un employeur ne saurait prendre connaissance de messages personnels d'un employé sans porter atteinte à la vie privée de celui-ci (article 9 du code civil) et au principe du secret des correspondances (article 226-15 du code pénal), quand bien même une utilisation à des fins privées aurait été proscrite par l'employeur.

Pour autant, le principe du secret des correspondances connaît des limites dans la sphère professionnelle. Il peut également être levé dans le cadre d'une instruction pénale ou par une décision de justice.

***Tout ce qui n'est pas identifié comme « personnel » est réputé être professionnel de sorte que l'employeur peut y accéder librement**.*
La Cour de cassation considère qu'un message envoyé ou reçu depuis le poste de travail mis à disposition par l'employeur revêt un caractère professionnel (Cour de cassation, 30 mai 2007).

Il appartient à l'employé d'identifier les messages qui sont personnels. À défaut d'une telle identification, les messages sont présumés être professionnels*.*
La nature personnelle d'un message peut figurer dans l'objet du message ou dans le nom du répertoire dans lequel il est stocké.
Source CNIL Juin 2017

3. Les imprimantes et copieurs

Des imprimantes et des copieurs sont mis à disposition des utilisateurs. Ils doivent faire l'objet d'une utilisation raisonnable en respectant quelques principes de base :

- N'imprimer ou ne photocopier que si nécessaire ;
- Conserver le paramétrage par défaut, soit le noir et blanc et le recto/verso ;
- Imprimer en mode économie d'encre ;
- Ne pas imprimer les courriels ;
- Utiliser l'aperçu avant impression pour éviter les erreurs ;
- Utiliser le mode « impression sécurisée » sur les copieurs afin de respecter la confidentialité des documents comportant des données à caractère personnel ou sensible.

4. Internet et réseaux sociaux

Le CIG est considéré comme un Fournisseur d'Accès Internet (FAI) puisqu'il fournit un accès à Internet quel que soit le biais (filaire ou wifi) à ses utilisateurs. La navigation sur Internet s'effectue avec l'adresse IP publique du CIG, engageant de fait la responsabilité du Président en cas d'usage délictueux.

De ce fait, le CIG est tenu de respecter les obligations suivantes :

- L'identification et la journalisation des informations de connexion et de navigation (durée, sites visités, téléchargements) ainsi que leur conservation sur une année (obligation applicable depuis la Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme) ;
- Le filtrage de la navigation, par le blocage de sites dont la consultation est illicite et punie par la loi ;
- Les informations enregistrées peuvent être examinées en réponse à une demande actée d'une autorité administrative ou judiciaire compétente ;
- Le constat de toute utilisation illégale pourra donner lieu, après décision actée de l'autorité administrative ou judiciaire, à la suppression des accès et/ou à des sanctions disciplinaires ;
- Le CIG se réserve le droit de bloquer l'accès aux sites dont le contenu est jugé illégal, offensant ou sans rapport avec les missions de l'utilisateur.

Malgré l'outil de filtrage, chaque utilisateur est seul responsable de la décision d'accéder à un site Internet. Le fait que l'accès à un site en particulier ne soit pas bloqué ne signifie pas que l'accès à ce site est autorisé et conforme à la réglementation applicable.

Les utilisateurs peuvent consulter les sites Internet présentant un lien direct et nécessaire avec leur activité professionnelle. Toutefois, une utilisation ponctuelle, pour un motif personnel, des sites

Internet dont le contenu n'est pas contraire à la loi, l'ordre public et ne mettant pas en cause l'intérêt et la réputation du CIG est admise.

Si certains sites non accessibles s'avèrent présenter un intérêt professionnel, il convient d'avertir la DSI en suivant les instructions présentes sur la page de blocage.

5. Accès réseaux et wifi invités

La connexion des postes de travail du CIG se fait principalement par le réseau filaire (Ethernet) lorsque le pc est relié à sa station de travail ou à un adaptateur USB.

Cependant, des bornes wifi sont réparties sur l'intégralité des bâtiments permettant de conserver une connexion au réseau du CIG depuis un autre bureau ou une salle de réunion.

Le réseau wifi est strictement réservé aux agents du CIG et apparait sur le poste de travail en "WiFiCIG". Afin de sécuriser ce réseau wifi, celui-ci est activé uniquement les jours ouvrés de 06h00 à 21h30.

Un second réseau nommé : "WiFiCIG_Invité" est mis à la disposition du public, accueilli au sein du CIG, les jours ouvrés de 07h30 à 19h00. Ce réseau permet, d'une manière ponctuelle, d'accéder uniquement au réseau internet sans possibilité de se connecter aux ressources informatiques du CIG.

La procédure de demande de connexion au réseau invité est la suivante :

- Lors de la sélection du réseau WiFiCIG_Invité, une clé d'accès est demandée à l'invité ;
- Une fois la clé saisie, l'invité saisit l'adresse du "sponsor" (l'agent du CIG l'ayant convié) ;
- L'agent du CIG reçoit un courriel afin de valider la demande d'accès au réseau WiFiCIG_Invité ;
- Une fois la demande d'accès validée, l'invité peut utiliser l'accès internet.

A noter :

Il est de la responsabilité de l'agent de s'assurer de la légitimité de la demande d'accès.

Les courriels de demande d'accès doivent être conservés **pendant 1 an** afin de permettre l'identification de l'invité en cas de poursuite pour utilisation frauduleuse de la connexion.

Afin de garantir la légitimité des accès à ce réseau, il est préférable d'éviter de saisir une adresse courriel pointant vers une liste de distribution.

6. Applications métiers

Les agents du CIG utilisent des applications métiers qui peuvent contenir des données confidentielles, nominatives ou appartenant à des collectivités.

La gestion et l'utilisation de ces applications doivent obéir aux mêmes règles de sécurité énoncées au paragraphe « Les règles générales d'utilisation du Système d'Information du CIG », notamment en matière d'authentification et de confidentialité.

Les règles de mots de passe (longueur de caractère, complexité, renouvellement…) de ces applications sont de la responsabilité des administrateurs métiers.

7. Téléphonie

Le CIG met à disposition des utilisateurs, pour l'exercice de leur activité professionnelle, des téléphones fixes, mobiles, logiciel (application MiCollab) et clé 4G.

Toute utilisation effectuée en dehors du forfait (type appels ou sms surtaxés…) doit être autorisée par le responsable de l'agent.

L'utilisation du téléphone à titre privé est admise à condition qu'elle demeure raisonnable et n'empêche pas l'agent de mener à bien ses missions habituelles (ex : dépassement de forfait « data » de l'abonnement).

Des statistiques globales peuvent être réalisées sur l'ensemble des appels entrants et sortants. Elles vérifient que les consommations n'excèdent pas les limites des contrats passés avec les opérateurs et permettent d'analyser l'activité téléphonique par service à des fins d'amélioration des processus métiers.

Néanmoins, en cas de consommation excessive ou d'anomalie, la DSI peut être amenée à déterminer l'auteur ou l'origine du ou des appels. En cas d'abus, une refacturation peut être effectuée directement auprès de l'utilisateur.

L'utilisation des périphériques de type Smartphone est soumises aux règles complémentaires suivantes :

- Il est obligatoire de protéger son téléphone mobile par un système de verrouillage (mot de passe, code PIN, schéma de déverrouillage…) ;
- Le code PIN opérateur par défaut (0000, 1234…) doit être impérativement modifié ;
- Ces équipements ne doivent pas être « débridés » ;
- Il est interdit d'utiliser les stations de recharge USB des lieux public (aéroport, gare…) afin d'éviter toute exfiltration de données de l'appareil. Il est recommandé de ne charger son téléphone qu'à partir d'un chargeur depuis une prise électrique classique ;
- Les applications de confiance doivent être téléchargées à partir des plateformes officielles de téléchargement (Google Play Store, AppStore, plateformes internes de type Intranet applicatif…) ;
- L'utilisateur doit être le seul à utiliser son équipement si des données professionnelles sont stockées (messagerie, fichiers…). Il lui est interdit de prêter ou de donner à un tiers son matériel ;
- L'utilisateur doit signaler au plus tôt au Service Exploitation, la perte ou le vol d'un terminal mobile contenant des données professionnelles ou y donnant accès ;
- L'utilisateur doit contacter l'opérateur téléphonique correspondant pour suspendre la ligne en cas de perte ou de vol. Une grande vigilance est à observer quant au vol ou à la perte des équipements mobiles : notamment lors des déplacements ;
  En cas de vol, l'utilisateur doit porter plainte dans les meilleurs délais ;
- L'utilisateur a l'obligation de se rapprocher de son supérieur afin de prévenir le Service Exploitation en cas de déplacement à l'étranger afin d'obtenir l'autorisation d'utiliser ses équipements mobiles dans le pays concerné.

8. Stockage et accès aux données informatiques, responsabilité de l'information confiée

La mise en œuvre du système de sécurité comporte des dispositifs de sauvegarde des informations permettant d'assurer l'intégrité et la restauration des données sauvegardées.
L'organisation mise en place des sauvegardes répond à une stratégie permettant de sécuriser les données de manière optimale, à savoir : 3 copies identiques sur 2 médias de stockage différents dont 1 copie hors site.

Les données stockées sur les postes informatiques (disque dur C:\ ou D:\ par exemple), ou sur des supports externes (disque, clé USB…) ne sont pas sauvegardés par la DSI. En cas de panne importante de ces matériels, toutes ces données peuvent être perdues. Cette perte et l'absence de possibilité de récupération seront de la seule responsabilité de l'utilisateur.

Les données numériques et l'information en général constituent le patrimoine immatériel du CIG et sa principale richesse. Chaque utilisateur est responsable de l'information qui lui est confiée et doit prendre toutes les précautions nécessaires afin de préserver l'intégrité et la confidentialité des données qu'il traite ou échange.

Chaque agent dispose d'un répertoire de travail dont l'accès est individuel sur le réseau (R:\). Les données sont donc accessibles exclusivement par l'utilisateur et ne peuvent être mises à disposition d'autres utilisateurs (sauf cas exceptionnel, pour raison de service, sur demande motivée du supérieur hiérarchique).

Dans le cadre de ses missions, un utilisateur peut avoir accès à des données confidentielles ou sensibles (données de santé, données sociales ou médico-sociales, données financières, etc.).

Dans ce cadre, l'utilisateur doit :

- Veiller à ce que leur intégrité et leur confidentialité soient strictement respectées et qu'elles ne soient pas détournées de l'usage et de la finalité prévus ;
- Prendre toutes les précautions de sécurité requises lors du transit d'informations confidentielles au sein du CIG et à l'extérieur (chiffrer les données au moment de leur envoi par mail ou utiliser des moyens de transmission sécurisés tels que NetExplorer ou toute autre application de partage (cf. partie 4 : « Les règles de sécurité et devoirs de l'utilisateur »).

Les utilisateurs ne doivent pas :

- Tenter d'accéder à des informations ou à des applications en dehors des droits qui leur sont attribués. En cas de détection d'une faille, chaque utilisateur doit le signaler immédiatement au Service Exploitation et en informer sa hiérarchie ;
- Utiliser de données professionnelles à des fins personnelles ;
- Laisser l'accès à son environnement de travail à des personnes non habilitées ;
- Tenter de lire, modifier, copier ou détruire des données autres que celles qui appartiennent directement à l'utilisateur.

Chaque utilisateur doit procéder à la protection des informations professionnelles qui lui sont confiées. Il doit veiller à leur enregistrement sur des emplacements protégés et sauvegardés (serveurs, réseaux de stockage de données, arborescence bureautique du service).

L'enregistrement de données sur le poste en local doit rester une exception et ne saurait constituer une règle de classement et de gestion de ces informations.

Toute copie de film, série, musique n'ayant pas un caractère professionnel est strictement interdite sur l'ensemble des répertoires bureautiques et sur le poste de travail de l'utilisateur.

Afin d'assurer un fonctionnement optimal des infrastructures bureautiques, les données informatiques présentes dans les répertoires réseaux peuvent être analysées automatiquement ou manuellement par les administrateurs de la DSI et sont sauvegardées régulièrement.

La DSI informe que la suppression par un utilisateur d'un fichier sur un serveur n'est pas absolue et qu'il peut en rester une copie sur le dispositif de sauvegarde pendant 1 an au maximum.

De plus, il revient à chaque utilisateur et à chaque service de trier régulièrement les données enregistrées, afin de ne garder que les données utiles et conformes aux durées d'utilité administrative listées dans les circulaires du Service Interministériel des Archives de France et en sollicitant le service archives en cas de besoin.

9. Accès à distance

Le CIG met à disposition de ses agents des outils permettant un accès au Système d'Information en distanciel (VPN) depuis les ordinateurs portables professionnels.

L'ensemble des règles décrites dans les articles précédents concernant l'utilisation des ressources sont applicables. Dans le cas d'utilisation du service d'accès à distance, afin de limiter le risque de divulgation d'information, des précautions particulières et supplémentaires s'imposent :

- Les utilisateurs sont seuls responsables de la sécurité physique des équipements mis à leur disposition ;
- Être vigilant afin de ne pas divulguer d'information confidentielle lors d'une consultation à distance (regard indiscret d'un tiers, échange visio dans un lieu ne permettant pas de garantir la confidentialité des échanges, etc.) ;
- Se déconnecter systématiquement et complètement du service d'accès à distance après utilisation ;
- Protéger contre le vol les équipements mobiles et accessoires ;
- Respecter les règles encadrant l'usage du poste de travail.

CONDUITE A TENIR EN CAS DE CYBERATTAQUE

En cas de suspicion de cyberattaque (comportement inhabituel de l'ordinateur, chiffrement de données locales ou sur le réseau, envoi de courriel non initié par l'agent…), il est important de réagir dans les plus brefs délais :

- Déconnecter l'équipement informatique suspect du réseau du CIG (débranchement du câble réseau et/ou déconnexion du wifi) afin de l'isoler du reste des infrastructures ;
- Laisser votre équipement allumé afin de conserver toute éventuelle trace pouvant disparaitre en cas d'arrêt électrique ;
- Contacter le Service Exploitation (7000) afin que les administrateurs prennent en compte cet incident et puisse le traiter avec le RSSI.

PROTECTION DES DONNEES A CARACTERE PERSONNEL

Dans le cadre de l'exercice de ses missions, chaque agent doit respecter la règlementation en vigueur relative à la protection des données notamment les dispositions du règlement UE 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

L'agent doit :

- Ne pas utiliser les données personnelles à d'autres fins que celles pour lesquelles elles ont été collectées ;
- Ne pas conserver les données personnelles au-delà de la durée nécessaire aux finalités pour lesquelles celles-ci ont été collectées et dans la limite maximale fixée par l'instruction DGP/SIAF/2014/006 des archives de France ;
- Respecter les mesures de sécurité listées dans cette charte puisqu'en plus de permettre la sécurité du système d'information, elles permettent de garantir la sécurité, l'intégrité et la confidentialité des données personnelles collectées et notamment d'empêcher qu'elles ne soient déformées, endommagées, perdues, détournées, corrompues, divulguées, transmises ou communiquées à des personnes non autorisées ;
- Ne pas transmettre à un tiers les données personnelles collectées ;
- Transmettre, dans les meilleurs délais, les demandes d'exercice des droits des personnes concernées au Délégué à la Protection des Données du CIG.

ECO-RESPONSABILITE

Afin d'assurer un usage éco-responsable des ressources informatique, il est recommandé de :

- Ne pas laisser allumés ses écrans en mettant en place une extinction automatique (veille) ;
- Eteindre son ordinateur et ses écrans à l'issue de sa journée de travail ;
- Penser à désactiver régulièrement les fonctions non nécessaires dans certaines situations (wifi, Bluetooth, connexion « data » ou GPS du téléphone…) afin de préserver la batterie de son périphérique ;
- Limiter l'envoi des mails aux seuls destinataires ayant la nécessité d'en connaître ;
- Archiver ou supprimer régulièrement les messages ou documents ;
- S'assurer de la réelle nécessité d'imprimer un document numérique.

PROCEDURE APPLICABLE LORS DU DEPART D'UN AGENT

Sous couvert de son responsable, lors de son départ, l'utilisateur doit restituer à la DSI les matériels (pc portable, smartphone et accessoires…) mis à sa disposition. Il doit préalablement effacer ses fichiers et données privées et s'assurer de la bonne transmission des données professionnelles éventuellement présentes sur son ordinateur ou son répertoire personnel (fichiers, messages…) à son responsable.

Toute copie de documents professionnels est interdite.

Le compte utilisateur est désactivé dès le lendemain de son départ.

Les comptes et les données privées de l'utilisateur sont supprimés des infrastructures (hors sauvegarde) dans un délai de 2 mois au maximum après son départ.

RESPONSABILITES ET SANCTIONS

L'utilisateur doit respecter les règles définies dans la présente Charte et agir dans le respect de la réglementation applicable. En cas de non-respect de ces règles, d'agissements frauduleux, fautifs ou dommageables, l'utilisateur pourra être tenu pour personnellement responsable et faire l'objet de poursuites disciplinaires, civiles ou pénales.

Dans le cas de tentatives ou d'agissements frauduleux sur des sites distants accédés via Internet et si la responsabilité du CIG était recherchée à côté de celle de l'utilisateur, le CIG se réserve le droit d'appliquer à l'utilisateur les sanctions disciplinaires appropriées et d'exercer un recours contre l'intéressé.

ENTREE EN VIGUEUR DE LA CHARTE

La présente charte est annexée au règlement intérieur du CIG et s'applique de fait à l'agent lors de son arrivée. Elle est disponible en téléchargement sur les répertoires bureautiques et l'intranet du CIG.

Elle est complétée par des fiches de bonnes pratiques relatives aux types d'utilisation et d'administration des ressources informatiques.

Elle sera réactualisée régulièrement afin de tenir compte du contexte juridique, technologique et organisationnel en constante évolution.