Charte d'utilisation des Systèmes d'Information et Protection des Données

Version du 10 septembre 2024

Applicable au 1er mars 2025 - UES Capgemini France

Contrôle du document

Nom du document	Charte d'utilisation des Systèmes d'information et de la Protection des Données
Date de délivrance	24 janvier 2022
Classification du document	Interne
Auteur du document	Direction des Affaires Sociales UES/ Direction Juridique/ GroupIT / Equipe Cybersécurité
Propriétaire du document	UES Capgemini
Distribution du document	Tout utilisateur des SI de l'UES Capgemini

Approbateurs du document

Approbateur	**Version**	**Date**
Gaël COENEN, DRH de l'UES Capgemini	1.0	24 janvier 2022
Bruno LAFORGE, DRH de l'UES Capgemini	2.0	10 septembre 2024

Modifications du document

Version	**Délivrée en**
1.0	24 janvier 2022
2.0	10 septembre 2024

Table des matières

CE DOCUMENT COMPORTE 14 PAGES, PAGE DE GARDE INCLUSE

1. Définitions :

On désignera par « **Groupe Capgemini** » l'ensemble du Groupe de Sociétés Capgemini contrôlées, directement ou indirectement, par Capgemini SE.

On désignera par « **UES Capgemini** » les sociétés comprises dans son périmètre et défini dans l'accord du 11 janvier 2019 et ses éventuels avenants.

On désignera par « **Tiers** » toute société en relation avec le Groupe Capgemini : clients, sous-traitants, fournisseurs, partenaires, etc.

On désignera par **« Actif »,** tout moyen technique ou système, quel qu'en soit le support acheté, loué, construit ou utilisé pour créer, collecter, stocker et/ou traiter des données/informations. Ces systèmes, comprennent, notamment, les infrastructures, les réseaux informatiques, les équipements informatiques, les logiciels, les applications et les services en ligne, les systèmes d'exploitation, les supports de stockage, la messagerie électronique, la messagerie vocale, le téléphone, les tablettes et équipements numériques, les serveurs de fichiers, les bases de données, etc…

On désignera par **« Information »** toute information structurée ou non structurée du Groupe Capgemini ou de ses Tiers (devant être traitée par l'utilisateur de l'UES Capgemini dans le cadre d'une prestation de services) sous forme de courriels, de documents électroniques, d'applications, de bases de données, de logiciels, etc.

On désignera par « **Employé(s)** » tout salarié de l'UES Capgemini, permanent ou temporaire, au moment de l'utilisation de la présente Charte.

On désignera par « **Utilisateur(s)** », toute personne ayant accès aux systèmes d'information du Groupe Capgemini ou de ses Tiers, qu'il s'agisse d'Employés, de sous-traitants, de consultants ou tout autre personne travaillant pour le compte de l'UES Capgemini, y compris tout le personnel affilié à des Tiers et ce, quel que soit leur statut permanents ou temporaires.

2. Objet du document

Cette charte d'utilisation du système d'information et protection des données, (ci-après appelée Charte), est issue de la Politique d'utilisation acceptable définie par le Groupe Capgemini. Elle est adaptée aux exigences et aux impératifs légaux et réglementaires français. Elle a pour objectifs :

- De distinguer les utilisations autorisées et les utilisations non autorisées des Actifs, conformément aux dispositions des Politiques du Groupe Capgemini relatives à la protection des informations, de la propriété intellectuelle, des données personnelles et à l'utilisation des Actifs du Groupe Capgemini et des Tiers ;
- De préciser, en complément des modules de formation obligatoires les règles principales de sécurité qui doivent être adoptées par chaque Utilisateur lors de l'utilisation des Actifs du Groupe Capgemini et des Tiers.

Cette Charte n'est pas exhaustive et elle exige que les Employés, en tant qu'Utilisateurs des Actifs, se conforment également aux autres Chartes et Politiques du Groupe Capgemini en vigueur, lesquelles sont accessibles depuis l'Intranet du Groupe Capgemini.

Aucune clause dudit document n'a pour but de déroger aux accords collectifs d'entreprise ni d'apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir et proportionnées au but recherché conformément à la législation en vigueur.

Cette Charte ne fait pas obstacle à l'application de toute autre disposition spécifique (notamment les exigences supplémentaires de sécurité d'un Tiers du Groupe Capgemini) et procédures additionnelles dès lors qu'elles sont portées à la connaissance de l'Employé et de manière générale de l'Utilisateur, notamment pour des groupes d'Utilisateurs dont la mission comporte des contraintes particulières (défense nationale, secret bancaire…).

3. Champs d'application

La présente Charte s'applique à l'ensemble des Utilisateurs et à tous les Actifs et dispositifs connectés à un réseau du Groupe Capgemini ou hébergés sur un site du Groupe Capgemini.

4. Responsabilité

Chaque Utilisateur est responsable de l'usage qu'il fait du matériel et des ressources de l'entreprise mis à sa disposition pour l'exercice de sa fonction. Une utilisation sécurisée des Actifs nécessite la participation et le soutien de tous les Utilisateurs ayant accès aux informations et systèmes d'informations du Groupe Capgemini et de ses Tiers.

Il est de la responsabilité de tous les Utilisateurs de prendre connaissance de la présente Charte, de s'y conformer et de mener leurs activités de manière professionnelle et responsable.

L'élaboration, la rédaction et la mise en place de la présente Charte sont sous la responsabilité de GroupIT.

D'autres acteurs comme les responsables de projets et leurs équipes peuvent avoir la charge de contrôles spécifiques lorsque les Actifs sont fournis par des Tiers.

5. Sécurisation de l'espace de travail

Le collaborateur est responsable de la sécurisation de son espace de travail physique et virtuel, individuel et collectif. Ainsi, la bonne utilisation des Actifs implique un ensemble de règles de conduite à mettre en œuvre. A ce titre, tout Utilisateur veille à :

- Utiliser des Actifs ayant été approuvés par GroupIT ou tout autre service compétent ;
- Maintenir le bon fonctionnement des contrôles de sécurité mis en place par GroupIT (chiffrement, backup, authentification, antivirus, économiseurs d'écran, etc.) ;
- Utiliser des câbles de sécurité permettant d'attacher les postes de travail afin de se prémunir de tout risque de vol ;
- Maintenir son espace de travail rangé de manière à n'y laisser aucune information confidentielle (mot de passe, documents sensibles, etc.) ;
- Effacer les informations confidentielles des tableaux blancs, des notes papier ainsi que tout autre support après chaque réunion ;
- Conserver les documents et dossiers physiques classés confidentiels dans des armoires fermées à clés ;

- Eliminer toute information sensible de manière sécurisée selon la politique de classification des données (Cf. article 8 de la présente Charte) ;
- Utiliser un destructeur de document ;
- Assurer la collecte sécurisée des documents à partir de l'imprimante (prendre tous les originaux, détruire les copies inutiles, etc.), en utilisant les moyens mis à leur disposition par le Groupe Capgemini notamment l'utilisation des badges ;
- Utiliser les logiciels mis à disposition dans le portail d'entreprise et dans le catalogue des services GroupIT ;
- Se conformer aux demandes d'exceptions dans le portail de services GroupIT pour l'utilisation de logiciels et matériels non standards ;
- Assurer la continuité de l'activité et le bon fonctionnement du service, en son d'absence. A défaut, l'Administrateur pourra, à titre exceptionnel et sous réserve de l'autorisation de la hiérarchie de l'Utilisateur, avoir un accès provisoire aux données professionnelles de l'Utilisateur. Ce dernier est alors obligatoirement informé de cet accès, au plus tard à son retour d'absence ;
- Se conformer aux directives de GroupIT applicables en cas d'absence prolongée afin de garantir la sécurité des systèmes d'information. A ce titre l'Utilisateur peut voir sa messagerie suspendue (absence supérieure à un mois), et peut être amené à restituer le matériel (absence supérieure à 3 mois) qui lui a été fourni par le Groupe Capgemini.

6. Accès au système d'information et au réseau

Chaque Utilisateur est responsable des accès que GroupIT lui attribue (réseaux, systèmes d'information, etc.) et veille à ce titre à :

- Sécuriser tous les Actifs mis à sa disposition à l'aide d'un mot de passe complexe, de données biométriques, d'un code PIN, ou tout autre dispositif d'authentification forte fourni par GroupIT ;
- Garder les mots de passe et les dispositifs d'authentification strictement confidentiels ;
- Définir différents mots de passe pour les différents types d'accès aux systèmes ;
- Changer son mot de passe selon les règles édictées par le Groupe Capgemini, soit régulièrement et au plus tard tous les trois mois, ou immédiatement s'il pense que quelqu'un l'a vu le taper ou s'il pense qu'il peut être compromis (en cas de réponse à un spam ou d'attaque informatique par exemple) ;
- Verrouiller systématiquement son poste de travail lorsque l'on s'en éloigne (ordinateurs portables et ordinateurs de bureau), sans quitter le site du Groupe Capgemini, du Tiers, ou du télétravail ;
- Eteindre son poste de travail dès lors que l'Utilisateur cesse de travailler.

Il est interdit aux Utilisateurs :

- D'utiliser un poste de travail ou un équipement mobile fourni par le Groupe Capgemini pour se connecter directement au réseau d'un Tiers sans un mode de connexion préalablement approuvé par le Groupe et le Tiers et/ou une solution d'isolation ;
- De provoquer une atteinte à la sécurité du Groupe Capgemini ou à d'autres ressources réseau, notamment en accédant sans autorisation aux données, aux serveurs ou aux comptes ou encore en autorisant l'accès ou en diffusant des Informations à des personnes non autorisées ;
- Contourner l'authentification des Utilisateurs sur n'importe quel périphérique, ou de surveiller le trafic du réseau ;

- De provoquer l'interruption des services du Groupe Capgemini ou d'autres ressources du réseau, y compris, notamment, les floods ICMP(1), l'usurpation de paquets, le déni de service, les dépassements de tas ou de tampon, et le routage frauduleux ;
- D'effectuer un balayage de ports ou un scan de sécurité sur le réseau du Groupe Capgemini ou d'un Tiers, sauf autorisation préalable des équipes cybersécurité du Groupe Capgemini ou du Tiers ;
- D'introduire des systèmes (tels que des honeypots, des honeynets(2)), ou toute autre technologie similaire sur le réseau du Groupe Capgemini.

(1) floods ICMP : saturation la bande passante d'un routeur réseau ou d'une adresse IP ciblée, surcharge de la capacité d'un terminal à transmettre le trafic au prochain tronçon en aval en le submergeant de paquets ICMP élaborés.
(2) honeypots, honeynets : leurre prenant l'apparence d'un système réel, avec des vulnérabilités fictives et exploitables.

7. Classification des données et des informations

Chaque Utilisateur doit marquer les documents qu'il créé avec la classification appropriée (les logos ci-après peuvent être utilisés également) en fonction des Informations contenues et doit respecter le niveau de confidentialité prévu sur les documents auxquels il accède tel que prévu ci-dessous :

SEC0-Public : Informations destinées au grand public et dont le partage ne présente aucun risque. Il s'agit des contenus accessibles à tous, comme les informations publiées sur le site internet de Capgemini.

SEC1-Company Confidential : Informations créées et détenues par Capgemini destinées uniquement à un usage interne.

SEC2-Company Restricted : Informations à destination d'un groupe défini et limité d'employés de Capgemini.

SEC2-Customer Restricted : Informations à destination d'un groupe défini et limité d'employés de Capgemini en lien avec un ou plusieurs clients.

SEC3-Company Sensitive : Informations strictement confidentielles, réglementées, et dont la diffusion pourrait porter préjudice à Capgemini ou à un tiers.

Ces mesures de protection s'appliquent à tous les documents, originaux ou copies, sur support physique ou dématérialisé.

8. Messagerie professionnelle et utilisation d'internet

Tout Utilisateur est responsable de la bonne utilisation des Actifs qui sont mis à sa disposition, dont les messageries professionnelles, et à ce titre, il doit :

- Respecter les règles du Groupe Capgemini relatives à la classification (cf. article 7 de la présente Charte) et la protection de l'information en vigueur lors d'envoi de messages confidentiels ;
- Adapter les options de chiffrement, d'interdiction de transfert ou de partage des courriels et leurs pièces jointes selon le niveau de confidentialité ;
- Adopter un comportement prudent et vigilant face aux attaques d'hameçonnage de courriels malveillant tentant d'amener l'utilisateur à divulguer un mot de passe ou tout autre type d'information confidentielle ;
- Faire preuve de vigilance lorsque les courriels reçus proviennent de domaines externes et tout particulièrement s'ils ne présentent pas de bandeau rouge explicite. Il est donc nécessaire de s'assurer de la validité de l'émetteur et en cas de doute, de solliciter l'équipe SPAM (Bouton « Report Spam » présent dans Outlook ou toute autre procédure prévue à cet effet) et de ne pas ouvrir les pièces jointes ;
- Saisir dans le portail de service GroupIT, toute demande d'exception pour les domaines externes considérés comme SPAM par les outils de sécurité du Groupe ;
- Respecter la Charte éthique du Groupe Capgemini dans ses communications.

Par ailleurs, il est interdit aux Utilisateurs :

- D'envoyer des informations ou des documents concernant ou appartenant au Groupe Capgemini ou ses Tiers vers une boîte de messagerie privée ;
- D'envoyer des informations ou des documents appartenant à un Tiers depuis une adresse tierce fournie par le Tiers, vers toute autre boîte de messagerie professionnelle (y compris la sienne) sans l'autorisation expresse et préalable du Tiers concerné ;
- De créer ou transférer des courriels en masse, c'est-à-dire à portée collective, que ce soit pour des raisons professionnelles ou personnelles qui ne soient pas justifiées par l'exercice des fonctions ou le projet sur lequel est affecté l'Utilisateur ;
- D'envoyer des spams par courriel, SMS, appels, messagerie instantanée, messagerie vocale ou toute autre forme de communication électronique ;
- De transférer des fausses alertes (hoaxes en anglais) et rumeurs (informations non vérifiées susceptibles d'induire d'autres Utilisateurs en erreur) ;
- D'utiliser le système de messagerie du Groupe Capgemini pour insulter, perturber ou offenser un groupe ou une personne quelconque ou d'une façon contraire aux Politiques, Chartes et directives du Groupe Capgemini ;
- De falsifier, présenter de façon erronée, supprimer ou remplacer l'identité de l'expéditeur d'une communication électronique et/ou le contenu de celle-ci afin d'induire le destinataire en erreur concernant l'expéditeur ;
- D'utiliser 'Capgemini', ou tout autre marque ou dénomination sociale d'une société du Groupe Capgemini, en nom de domaine (ex : @capgemini.com) notamment depuis une messagerie externe (Gmail, etc) ;
- De s'abonner, avec leur adresse de messagerie du Groupe Capgemini ou d'un Tiers, à des listes de diffusion qui ne sont pas liées à leur activité professionnelle.

De manière générale, les Utilisateurs doivent réserver l'utilisation des services de messagerie du Groupe Capgemini ou celle de ses Tiers à l'activité professionnelle sous réserve de la tolérance rappelée à l'article 12 de la présente Charte.

Les règles définies ci-dessus s'appliquent également lors de l'utilisation des messageries mises à la disposition des Utilisateurs par les Tiers de Capgemini.

Lorsqu'ils utilisent Internet, les Utilisateurs doivent :

- Télécharger des fichiers uniquement à partir de sites fiables et réputés, pouvant être identifiés à partir de diligences raisonnables (par ex. vérification du caractère sécurisé du site, taper le nom du site sur un moteur de recherche éventuellement associé avec le mot 'fraude ' ou 'arnaque', …), maintenir actifs le blocage des pop-ups et l'antivirus tels que configurés par le Groupe Capgemini ;
- Limiter l'usage des données ou des informations personnelles sur des sites web à vocation professionnelle ;
- Garder séparés les liens entre leurs données personnelles et leur profil professionnel en gérant :
  - les activités personnelles en utilisant leur adresse de messagerie personnelle,
  - les activités professionnelles au moyen de leur adresse professionnelle ;
- Vérifier l'URL des sites visités, utiliser HTTPS et faire attention aux fautes de frappe dans l'URL associée (les attaquants pouvant utiliser de fausses URL similaires pour entraîner l'Utilisateur sur des sites malveillants). En cas de doute sur un lien présent dans un courriel, vérifier sans cliquer sur le lien, l'orthographe du nom du site en positionnant le curseur au-dessus du lien.

Les Utilisateurs d'Internet ne doivent pas :

- Saisir leurs informations d'identification sur un site Web à moins d'être sûr de sa légitimité ;
- Se livrer à des activités illégales ou se rendre sur des sites hébergeant des contenus illégaux, offensants ou inappropriés (par exemple à caractère violent, pornographique, pédophile, raciste, antisémite, jeux, paris en ligne, etc.) ;
- Utiliser des outils de transfert de fichier publics ;
- Publier sur Internet des données ou des informations relatives au Groupe Capgemini ou à ses Tiers.

9. Déplacement, télétravail

Dans le cadre d'éventuels déplacements, lors d'une connexion à domicile ou depuis un lieu extérieur à l'entreprise, les Utilisateurs doivent continuer à assurer la sécurité et la confidentialité des Actifs. Ils doivent notamment :

- S'assurer que les Actifs (ordinateurs portables, smartphones ou dispositifs d'authentification contenant des données concernant le Groupe Capgemini ou ses Tiers) sont sécurisés ;
- Se connecter au réseau du Groupe Capgemini depuis des sites distants par le biais de mécanismes d'authentification et d'autorisation mis en place par GroupIT ;
- Ne jamais laisser d'ordinateurs portables sans surveillance dans des voitures, ni dans des lieux publics tels que les aéroports, trains, restaurants, salons d'hôtel, etc. ;
- S'assurer que les informations affichées à l'écran ne sont pas visibles par des tiers (filtre de courtoisie, luminosité plus faible, etc.) ;
- En cas d'utilisation d'un équipement personnel, respecter scrupuleusement l'utilisation des containers sécurisés ou tout autre dispositif fournis par le Groupe Capgemini protégeant ses applications et ses données ;

- Se conformer aux règles du Groupe Capgemini relatives au télétravail à l'étranger disponibles sur l'intranet.

Les Utilisateurs doivent se conformer à la politique de voyage définie par le Groupe Capgemini et disponible sur l'intranet :

- Celle-ci définit une liste de pays très sensibles dans lesquels il est interdit d'emmener tout Actif appartenant au Groupe Capgemini ou ses Tiers, et depuis lesquels il est strictement interdit de se connecter au réseau du Groupe Capgemini avec par exemple un ordinateur, un appareil personnel ou un périphérique enrôlé dans le SI du Groupe Capgemini. Pour ce dernier cas, il est obligatoire de procéder à son désenrôlement avant de l'emporter (Suppression de l'appareil dans le portail d'entreprise) ;
- Pour les autres pays, voyager pour des raisons personnelles avec des Actifs du Groupe Capgemini ou de ses Tiers, nécessite un accord préalable du manager et du Chief Information Security Officer (CISO) de son entité.

10. Utilisation des réseaux sociaux et des sites/espaces ouverts

Compte tenu de l'importance des plates-formes sociales en ligne et des risques d'atteinte à la confidentialité des données liés à leur usage, le Groupe Capgemini considère essentiel de prendre en compte l'impact de ces dernières sur les activités professionnelles des Employés.
Les réseaux sociaux visés dans le présent article concernent tout site internet permettant aux Utilisateurs de partager ou échanger des informations, des photos ou des vidéos (ex : blogs, wikis, réseaux sociaux et tout autre médias sociaux utilisés au sein du Groupe Capgemini ou à l'extérieur).
Pour chaque contribution apportée sur les plates-formes sociales (y compris Yammer, LinkedIn ou équivalent) faisant référence ou ayant éventuellement une incidence sur le Groupe Capgemini, les Utilisateurs doivent :

- S'assurer que toute publication et toute référence au Groupe Capgemini, à ses salariés, à ses Tiers, n'enfreignent, ni les clauses de confidentialité et de loyauté inscrites dans leur contrat de travail, ni les accords de confidentialité signés dans le cadre de leur mission ;
- S'assurer d'avoir l'accord de la Direction Communication pour toute publication concernant le Groupe Capgemini, ses Tiers, les projets et desdits Tiers si la publication les concerne ;
- Respecter, conformément à sa formation et aux instructions de la présente charte une neutralité au sein de l'entreprise ainsi qu'à l'extérieur lors de l'utilisation des outils et moyens de communication appartenant au Groupe Capgemini (exemples : signature de courriel, avatar, photo, etc.) ;
- S'exprimer à la première personne et non au nom de la société.

Ne doivent pas :

- Publier des informations (activités, photos, etc.) à propos de leurs collègues ou toute autre personne liée directement ou indirectement à leur activité professionnelle sans leur autorisation ;
- Proférer d'insulte ou publier du contenu à caractère insultant, haineux, diffamatoire, dénigrant, menaçant, discriminatoire ou encore pornographique ;
- Transférer des fausses informations, des insinuations et/ou rumeurs (informations non vérifiées pouvant induire d'autres Utilisateurs en erreur) susceptibles ou non de nuire à l'image et/ou la réputation d'un Utilisateur et/ou du Groupe Capgemini ;
- S'identifier de manière anonyme ou sous de faux noms ;

- Publier sur un forum/groupe de discussions ou une liste de diffusion à l'aide d'une adresse de messagerie du Groupe Capgemini représentant le Groupe Capgemini auprès du public ;
- Détourner le nom de « Capgemini » et son logo ;
- S'abonner à des réseaux sociaux à des fins personnelles en utilisant leur adresse de messagerie professionnelle ;
- Télécharger des logiciels publiés sur les réseaux sociaux par des sociétés ou personnes inconnues.

De manière générale, chaque Utilisateur doit respecter les lois et les réglementations en vigueur, et plus particulièrement les lois régissant les droits de propriété intellectuelle, les droits d'auteur et les marques commerciales.

11. Données à caractère personnel

Le Groupe Capgemini a mis en place des Règles d'Entreprise Contraignantes (REC) - ou Binding Corporate Rules (BCR), lesquelles sont annexées au règlement intérieur de l'UES Capgemini.

Par ailleurs, le Groupe Capgemini traite des données à caractère personnel des Utilisateurs conformément à la réglementation en vigueur. Le Groupe Capgemini tient à la disposition des Utilisateurs une notice d'information sur les traitements de données à caractère personnel disponible sur l'Intranet du Groupe Capgemini.

12. Usage personnel des Actifs

L'utilisation des Actifs mis à disposition par le Groupe Capgemini ou ses Tiers doit être réservée à l'activité professionnelle des Utilisateurs. Toutefois, un usage personnel est toléré dès lors qu'il respecte les conditions de la présente Charte, qu'il est occasionnel et raisonnable, qu'il n'entrave pas la productivité, qu'il ne porte pas atteinte à l'image du Groupe Capgemini, de ses Tiers ou de tout autre personne physique ou morale, qu'il respecte la législation en vigueur et qu'il n'engage pas la responsabilité des Employés de l'une ou des entités du Groupe Capgemini.

L'Utilisateur qui souhaite utiliser, à des fins privées, les Actifs mis à disposition par le Groupe Capgemini, est tenu de l'indiquer clairement et explicitement par l'utilisation du terme « personnel » ou « privé ». Cette mention doit obligatoirement apparaître dans le nom des fichiers ou répertoires ou dans le sujet des messages concernés. Toutes les informations qui ne sont pas clairement identifiées comme « personnel » ou « privé », sont considérées comme des informations professionnelles.

Le Groupe Capgemini ne pourra pas être tenu responsable de la perte de données personnelles ou relevant de la vie privée enregistrées par l'employé sur un Actif mis à sa disposition.

13. Signalement des incidents

Il peut arriver que le Groupe Capgemini ou un de ses Tiers soit victime d'un incident technique ou de sécurité. Dans ce cadre, les Utilisateurs sont les premiers à agir et doivent sans délai signaler :

- Tout incident de sécurité au Chief Information Security Officer (CISO) et à leur manager hiérarchique ;
- Tout incident technique à GroupIT Help Desk et à leur manager hiérarchique direct.

Ces règles pourront évoluer en fonction des process définis par le Groupe Capgemini. En cas de modification, les salariés en seront informés.

14. Comportements et pratiques non autorisés

En complément des comportements interdits décrits ci-avant, et en raison d'impératifs de sécurité, de prévention ou de contrôle du réseau, les pratiques suivantes sont strictement interdites aux Utilisateurs :

- Exporter ou importer des logiciels, des informations techniques, des logiciels de chiffrement ou des technologies en violation des lois internationales ou régionales en matière de contrôle des exportations et potentiellement des restrictions en matière de propriété intellectuelle ou de licence ;
- Introduire intentionnellement du code malveillant, y compris, notamment, des virus, des vers, des chevaux de Troie, du mail-bombing, des logiciels espions, des adwares, des ransomwares et des enregistreurs de frappe ;
- Enfreindre la loi sur les droits d'auteur, y compris, notamment, reproduire ou transmettre illégalement des images, de la musique, des vidéos et des logiciels protégés par le droit d'auteur ;
- Utiliser des systèmes fournis par le Groupe Capgemini ou ses Tiers afin de réaliser un gain financier à des fins personnelles ;
- Héberger un site internet personnel sur des appareils du Groupe Capgemini ou de ses Tiers ;
- Utiliser de manière abusive tout matériel professionnel du Groupe Capgemini ou d'un Tiers à des fins personnelles qui aurait pour conséquence de perturber les actifs (ex : activation de canal Web diffusant des mises à jour fréquentes sur les ordinateurs tels que les actualités, résultats sportifs, jeux en ligne, etc.) ;
- Installer et utiliser des machines virtuelles sur les postes de travail ;
- Transférer vers un dispositif externe tout document appartenant au Groupe Capgemini ou ses Tiers sans autorisation préalable en toute circonstance (changement de projet, départ de l'entreprise …) ;
- Modifier la configuration de son poste de travail sans autorisation préalable formelle de son N+1 et validation de GroupIT et/ou Group Cybersécurité ;
- Utiliser son poste de travail pour perpétrer toute forme de fraude, et/ou de piratage de logiciels, de films ou de musique, pirater des sites web non autorisés et/ou mettre en péril la sécurité des systèmes de communication électronique du Groupe Capgemini.
- …

15. Contrôles et Alertes à l'utilisateur

Afin de contrôler le fonctionnement, maintenir et garantir la sécurité du système d'information et des Actifs, des contrôles sont opérés par GroupIT :

Systèmes de maintenance et filtrage :

- De manière périodique sur le poste de travail
  - Audit des logiciels installés
  - Etat du logiciel d'encryptage
  - Etat du logiciel EDR (ou Antivirus)

  - Etat du logiciel de Management de Configuration Système
- De manière automatique sur le réseau
  - Filtrage des adresses internet
  - Filtrage des adresses des courriels dans le cadre de la lutte contre le spam (courriels non sollicités)

Ces contrôles sont réalisés de manière automatique afin d'assurer la sécurité du Système d'information et des Actifs. Ces types de contrôles automatiques sont susceptibles d'évoluer afin de faire face aux évolutions technologiques et aux risques cyber.

Sur les systèmes automatiques de traçabilité :

Les Utilisateurs sont informés que des fichiers de journalisation (fichiers logs) recensent les connexions et tentatives de connexion des Utilisateurs sur les Actifs. Conformément aux dispositions en vigueur, ces fichiers peuvent comporter notamment les données suivantes : dates, postes de travail et objet de l'évènement. Le Groupe Capgemini est le seul utilisateur de ces informations qui sont effacées à l'issue d'un délai de 1 an.

GroupIT pourra effectuer des vérifications et contrôles ponctuels de l'utilisation des Actifs, dans le respect des limites prévues par la loi.

Les appareils interférant avec d'autres appareils ou Utilisateurs du réseau du Groupe Capgemini devront être déconnectés sans délai sur demande d'un membre de GroupIT ou de l'équipe Cybersécurité.

16. Dégradation et restitution du matériel

Chaque Utilisateur doit prendre soin du matériel mis à sa disposition afin d'éviter toute dégradation accidentelle. Cela inclut les PC et accessoires fournis ainsi que tous les Actifs mis à disposition sur les sites (bureaux, salles de réunion…)

L'accès aux salles de réunion dépend de sa nature (bubbles, bureaux de réflexion, cabine téléphoniques, salles de réunion) et peut nécessiter une réservation préalable via l'outil de messagerie. Ces espaces doivent être restitués propres, rangés et conformes à l'usage initial : aucune intervention sur le câblage et les branchements n'est autorisée et le déplacement de tout ou partie des équipements présents dans l'espace est strictement interdit.

Au départ de l'Utilisateur du Groupe Capgemini ou à la fin d'une mission, les Actifs confiés doivent être restitués en bon état de fonctionnement.

Toute dégradation doit être signalée à GroupIT dans les meilleurs délais.

Toute dégradation volontaire pourra être sanctionnée.

17. Application de la Charte

Le manquement aux règles et mesures de sécurité de la présente Charte est susceptible d'engager la responsabilité de l'Utilisateur et d'entraîner à son encontre des rappels ou mises en garde, des limitations ou suspensions d'utiliser tout ou partie des systèmes d'information et de communication, voire des sanctions disciplinaires, proportionnées à la gravité des faits reprochés.

Tout Employé enfreignant la présente Charte peut faire l'objet de mesures disciplinaires pouvant aller jusqu'au licenciement, nonobstant toute poursuite judiciaire possible en vertu des lois.

Toute infraction à la présente Charte par un Utilisateur autre que les Employés, peut entraîner la résiliation de son contrat ou de son affectation au sein du Groupe Capgemini ou de son accès à tout ou partie du système d'information du Groupe Capgemini, nonobstant toute action en justice et recours en vertu des lois.

18. **Publicité**

La présente Charte a été soumise à l'avis du CSE Central de l'UES Capgemini pour les dispositions relevant de ses compétences.

La présente Charte est annexée au règlement intérieur de l'UES Capgemini. Elle est soumise aux mêmes procédures de consultation, de communication, de publicité et de dépôt que celles du règlement intérieur.

Toute modification ultérieure serait, conformément au Code du travail, soumise à la même procédure.

L'entrée en vigueur de la présente Charte est fixée au 1er mars 2025

Fait à Issy-les-Moulineaux, le 10 septembre 2024