



Charte d'utilisation des Systèmes d'Information

Charte Utilisateur

Ce document est intégré au règlement intérieur de l'établissement, en ce sens, l'ensemble des salariés de l'établissement ont l'obligation de respecter les éléments de ce document.

Pour les non-salariés de l'établissement, le document leur sera remis via un lien de redirection qui leur est transmis.

Description du document

Titre du document	Charte d'utilisation des Systèmes d'Information		
Propriétaire			
Classification	Interne		
Rédacteur	RSSI		
Statut	<input type="checkbox"/> Brouillon	<input checked="" type="checkbox"/> Relecture	<input type="checkbox"/> Approuvé

Diffusion

Entité	Prénom NOM	Fonction	Diffusion
Interne			Lecture

Historique des versions

Version	Opération	Intervenant	Date
1.0	Création	RSSI	XX/XX/XXXX
1.1	Modification	DSI adjoint / DPO	04/12/2024
1.2	Modification	Adjoint DRH / Responsable Relations sociales et Droit du travail	10/01/2025
1.3	Modification	DSI adjoint / DPO	15/01/2025
1.4	Modification	DSI adjoint / DPO	20/01/2025
1.5	Modification	Adjoint DRH / Responsable Relations sociales et Droit du travail	28/01/2025
1.6	Modification	DSI adjoint / DPO	29/01/2025
1.7	Modification	DSI adjoint / DPO	04/02/2025
1.8	Mise en forme finale	DSI adjoint	12/02/2025

Table des matières

PREAMBULE	4
DIFFUSION	4
1 PRINCIPES GENERAUX D'UTILISATION DES SYSTEMES D'INFORMATION	5
1.1 CHAMP D'APPLICATION	5
1.2 DEFINITIONS	5
1.3 RESPECT DES CONTRAINTES LEGALES	5
1.4 RESPECT DE LA PROPRIETE INTELLECTUELLE	6
1.5 RESPECT DE LA CONFIDENTIALITE DES INFORMATIONS	6
1.6 PROTECTION DES RESSOURCES ET DES BIENS DE GUSTAVE ROUSSY	6
1.7 PROTECTION DES CONDITIONS D'UTILISATION DES RESSOURCES INFORMATIQUES	6
1.8 PROTECTION DES DONNEES PRIVEES DE L'UTILISATEUR	7
1.9 DROIT A LA DECONNEXION	7
2 ACCES AUX SYSTEMES D'INFORMATION DE GUSTAVE ROUSSY	8
2.1 MATERIELS ET RESSOURCES	8
2.2 IDENTIFIANTS ET MOTS DE PASSE	8
2.3 ACCES AUX SI DE L'ETABLISSEMENT DEPUIS L'EXTERIEUR	9
2.4 MESSAGERIES	9
2.5 ACCES INTERNET ET NAVIGATION WEB	11
2.6 TELEPHONIE ET DISPOSITIFS CONNECTES	11
2.7 VPN	11
2.8 DISPOSITIFS DE STOCKAGE ET D'ECHANGE DE DONNEES	12
2.9 CONTROLES DE SECURITE	13
2.10 UTILISATION A TITRE PRIVE	13
3 CONTROLE DES ACCES PHYSIQUES	13
4 DEPART DE GUSTAVE ROUSSY	14
5 PROTECTION DES DONNEES A CARACTERE PERSONNEL	15
5.1 LES ENGAGEMENTS DE L'UTILISATEUR	15
5.2 LES ENGAGEMENTS DE GUSTAVE ROUSSY	15
5.3 LEXIQUE RGPD	16
6 SENSIBILISATION	16
7 SANCTIONS APPLICABLES	16
8 ENTREE ET VIGUEUR ET EVOLUTIONS	16

Préambule

La sécurité est l'affaire de tous.

La présente Charte a pour objet de formaliser les règles applicables à l'usage des Systèmes d'Information au sein de **Gustave Roussy**.

Elle définit les règles visant à garantir la disponibilité, l'intégrité, la confidentialité et la traçabilité des services et informations traitées et conservées sur les Systèmes d'Information (ou SI) de Gustave Roussy. Elle fixe également les règles en matière de contrôle et de surveillance des composants du Système d'Information mis à disposition des Utilisateurs (terme défini ci-dessous).

La Charte est remise selon les modalités suivantes :

- Concernant les salariés de Gustave Roussy : la Charte est annexée au règlement intérieur de Gustave Roussy remis au moment de leur embauche et disponible sur l'intranet ;
- Concernant les personnels non-salariés intervenant au sein de Gustave Roussy : la Charte leur est remise via un lien de redirection qui leur est transmis.

Le respect par tous les Utilisateurs des règles de sécurité des systèmes d'information contenues dans la Charte est opposable juridiquement. Ainsi les termes de la Charte s'impose à tous les Utilisateurs. Par conséquent, la violation d'une de ses stipulations expose son auteur à des sanctions pouvant aller jusqu'à la rupture du contrat.

Il est important de rappeler que des poursuites pénales et/ou civiles pourraient être engagées vis-à-vis de l'Utilisateur lui-même et/ou Gustave Roussy du fait d'action(s) pénalement répréhensibles effectuées avec ou sur le Système d'Information de Gustave Roussy.

Cette Charte s'inscrit dans la continuité des clauses du contrat liant l'Utilisateur à Gustave Roussy relatives au secret professionnel et à la non-divulgence d'informations confidentielles.

L'Utilisateur est informé de la nécessité de respecter les dispositions légales en matière de traitement de données à caractère personnel, conformément aux dispositions légales et réglementaires applicables à la protection des données personnelles, telles que celles du Règlement Général sur la Protection des Données (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 (RGPD) et de la loi n°78-17 du 6 janvier 1978 relative à l'informatique et aux libertés, telle qu'amendée par la loi 2004-801 du 6 août 2004 et par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles (Loi Informatique et Libertés) et de ses décrets d'application.

Diffusion

Cette charte est accessible sur l'intranet de l'établissement (elle est annexée au règlement intérieur de Gustave Roussy) et remise à tous les personnels extérieurs ayant besoin d'accéder au SI de l'établissement via un lien de redirection qui leur est transmis.

1 Principes généraux d'utilisation des Systèmes d'Information

1.1 Champ d'application

La Charte s'applique à toute personne amenée à utiliser les ressources informatiques et de télécommunications de Gustave Roussy indépendamment de son lieu d'accès et de son statut (*Ex. Salariés de Gustave Roussy, prestataire, stagiaire, etc...*).

1.2 Définitions

Les termes « Système d'Information » (ou SI) ou encore « Ressources Informatiques » désignent un ensemble organisé de ressources permettant l'accès, la collecte, le stockage, le traitement et la distribution de l'information. Il comprend notamment tous les ordinateurs, services et moyens de télécommunication de Gustave Roussy, les serveurs, les stations de travail, les portables, les smartphones, les tablettes, les dispositifs connectés, les réseaux téléphoniques, les logiciels, les messageries et les réseaux internes et externes.

Le terme « Utilisateur » désigne toute personne amenée à utiliser, consulter et à mettre en œuvre les ressources informatiques, de télécommunications et les systèmes d'information de Gustave Roussy indépendamment de son lieu d'accès et de son statut (*Exemple : salarié, stagiaire, etc...*).

Les termes « Responsable de la Sécurité des Systèmes d'Information » ou « RSSI » désignent la personne en charge de la protection des différents Systèmes d'Information de Gustave Roussy. Il évalue les risques, définit les politiques de sécurité et coordonne les activités de sécurité assumées par les différentes fonctions (administrateurs technique ou fonctionnel, métiers, etc..) afin de pouvoir assurer la disponibilité, l'intégrité, la confidentialité et la traçabilité des SI.

Les termes « Data Protection Officer », « Délégué à la Protection des Données » ou « DPO » désignent la personne en charge de la protection des données à caractère personnel au sein de Gustave Roussy.

Le terme « données sensible » désigne toutes données pouvant porter atteinte à la sécurité de l'établissement, aux objectifs stratégiques de Gustave Roussy, à sa réputation ou pouvant amener à un non-respect de réglementations en vigueur (*ex. RGPD – ayant une définition spécifique précisée plus bas*).

1.3 Respect des contraintes légales

Tout Utilisateur doit respecter la législation et réglementation en vigueur dont notamment celles relatives à la protection des données à caractère personnel, à la propriété intellectuelle et à la prohibition des publications à caractère injurieux, raciste, pornographique, diffamatoire ou de harcèlement sexuel ou moral.

L'Utilisateur ne doit, en aucun cas, consulter, stocker, publier, diffuser ou distribuer aux moyens des ressources de Gustave Roussy des documents, informations, images, vidéos :

- A caractère sexiste ou discriminatoire, violent, pornographique ou contraires aux bonnes mœurs.
- Susceptibles de porter atteinte au respect de la personne humaine et de sa dignité, ainsi qu'à la protection des mineurs.
- A caractère diffamatoire, ou susceptibles de porter atteinte à la vie privée des personnes.

Plus largement, il est strictement interdit d'accéder à des données ou services prohibés par la loi et/ou sanctionnés pénalement.

Toute tentative de désactivation (échouée ou non) ou de contournement des règles de sécurité mis en œuvre par Gustave Roussy peut être considéré comme une intrusion dans le SI de l'établissement.

1.4 Respect de la propriété intellectuelle

Les droits de propriété intellectuelle, ceux de Gustave Roussy ou ceux de tiers, doivent être respectés.

En ce sens, tout Utilisateur doit notamment :

- Utiliser les logiciels dans les conditions des licences souscrites (notamment effectuer les éventuelles copies de manière strictement conforme aux dispositions prévues).
- Ne pas reproduire, copier, diffuser, modifier ou utiliser tout document numérique protégé par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.
- Respecter le droit des marques.

L'Utilisateur s'interdit de porter atteinte d'une quelconque manière aux droits de propriété intellectuelle appartenant ou licenciés de Gustave Roussy ou à des tiers.

Les données et les programmes produits et/ou développés par l'Utilisateur ou fournis par Gustave Roussy dans le cadre de son activité professionnelle sont des actifs appartenant à Gustave Roussy.

1.5 Respect de la confidentialité des informations

Le respect de la confidentialité des données constituant un enjeu important de sécurité, l'Utilisateur s'engage à :

- Ne pas tenter de lire, copier, divulguer ou modifier les données d'un tiers sans y être autorisé.
- S'interdit toute tentative d'interception de données entre tiers.
- Prendre toutes les mesures nécessaires pour protéger la sécurité des données

En l'absence d'une autorisation écrite, toute tentative d'accès à des informations détenues par d'autres Utilisateurs est considérée comme illicite.

1.6 Protection des ressources et des biens de Gustave Roussy

L'Utilisateur doit respecter les consignes d'utilisation des matériels, logiciels et services mis à sa disposition. Il coopère avec les personnels et entités assurant le support de ces biens.

Des mesures de protection (*ex : antivol, antivirus, chiffrement, etc...*) sont mises en œuvre.

L'Utilisateur s'engage à ne pas entraver le bon fonctionnement de ces mesures de protection.

En cas d'identification ou de suspicion de faille ou d'un incident de sécurité, l'Utilisateur :

- **Le signale dès la survenance de l'évènement à sa hiérarchie ainsi qu'au support informatique.**
- **S'interdit d'exploiter ou de divulguer les éventuelles failles et incidents de sécurité, qu'il pourrait découvrir ou dont il pourrait avoir connaissance, et qui seraient présentes sur les ressources et applications de Gustave Roussy.**

1.7 Protection des conditions d'utilisation des ressources informatiques

L'Utilisateur s'interdit d'utiliser sciemment et indûment les Ressources et applications informatiques de Gustave Roussy de manière :

- A gêner l'accès ou l'utilisation des ressources par les autres Utilisateurs
- A perturber le fonctionnement des Ressources Informatiques
- A augmenter indûment les coûts de fonctionnement de ces Ressources
- A mettre en risque la sécurité des Systèmes d'Information (*ex. en désactivant les outils de sécurité*)
- A réaliser une activité illicite

1.8 Protection des données privées de l'Utilisateur

Les Administrateurs systèmes de Gustave Roussy gèrent les traces informatiques à l'aide de mécanismes de journalisation afin de s'assurer du bon fonctionnement et de la sécurité du système d'information dans le seul but de diagnostiquer les dysfonctionnements ou les incidents de sécurité affectant ces systèmes et ce, jusqu'à la date légale de destruction des journaux d'évènements.

Les informations de l'Utilisateur stockées dans le SI de Gustave Roussy (*ex : serveurs de fichiers, postes de travail, messagerie*) peuvent être consultées par les Administrateurs systèmes à des fins de sécurité, de risques d'actes de concurrence déloyale ou par la nécessité d'éviter les usages abusifs ou préjudiciables à Gustave Roussy.

Les informations privées que l'Utilisateur stocke et souhaite rendre confidentielles doivent présenter la mention « Personnel » ou « Privé » dans le nom du répertoire, du fichier ou de l'entête.

Ces informations doivent être stockées exclusivement sur le poste de travail personnel de l'Utilisateur. Il appartient à l'Utilisateur de procéder lui-même à la sauvegarde de ses fichiers identifiés comme « Personnel » ou « Privé ».

Dans le cadre de ses missions, le RSSI ou son équipe peuvent accéder aux données marquées « Personnel » ou « Privé » aux conditions suivantes :

- En présence de l'Utilisateur ou après que ce dernier ait été invité à être présent
- En l'absence de l'Utilisateur, et sans l'informer uniquement :
 - Dans le cadre d'une enquête judiciaire ou sur décision d'un juge
 - En cas d'évènement ou de risque particulier pour la sécurité de Gustave Roussy.

Dans le cadre de ses missions, le RSSI ou son équipe peuvent également accéder, même en l'absence de l'Utilisateur, à l'ensemble des fichiers enregistrés sur tout périphérique de stockage interne ou externe (*ex. clé USB, disque dur, etc...*) dès lors que ces derniers sont connectés à un ordinateur appartenant à l'entreprise et qu'ils ne sont pas identifiés comme personnels.

1.9 Droit à la déconnexion

Il est rappelé que le « droit à la déconnexion » est le droit de chaque salarié de ne pas être connecté à ses outils numériques professionnels et de ne pas être contacté pour un motif professionnel en dehors de ses heures de travail (y compris sur ses outils de communication personnels).

A ce titre l'Utilisateur s'engage à respecter les dispositions prévues à l'accord d'entreprise sur le droit à la déconnexion, et notamment :

- De respecter ses horaires de travail, ses temps de repos hebdomadaires et quotidiens et de suspension de son contrat de travail.
- Respecter les périodes de repos, congés et disponibilité de l'ensemble des Utilisateurs, périodes pendant lesquelles ils ne sont pas tenus de consulter leurs messages et de répondre aux sollicitations (à l'exception du personnel en astreinte).

En tout état de cause, les managers doivent s'abstenir de contacter leurs équipes en dehors de leurs horaires de travail habituels, ainsi que pendant leurs congés ou en cas d'arrêt maladie, sauf nécessité de service ou urgence caractérisée.

Dans tous les cas, l'usage de la messagerie électronique, du téléphone professionnel ou de tout autre outil numérique en dehors des horaires de travail doit être justifié par la gravité, l'urgence et/ou l'importance du sujet en cause.

2 Accès aux Systèmes d'Information de Gustave Roussy

Les Systèmes d'Information de Gustave Roussy mis à disposition de l'Utilisateur ne doivent en aucun cas être utilisés dans le cadre d'une activité illicite, quelle qu'elle soit.

2.1 Matériels et ressources

Gustave Roussy met à disposition de l'Utilisateur les moyens nécessaires à l'exécution de ses missions qui constituent un outil de travail.

Les règles suivantes sont applicables :

- Les matériels confiés à l'Utilisateur de Gustave Roussy le sont à des fins professionnelles.
- Chaque Utilisateur est responsable du matériel qui lui est confié et doit en prendre soin.
- L'utilisateur ne peut modifier le matériel mis à disposition par Gustave Roussy.
- L'utilisateur ne peut installer de composants logiciels non validé par la DTNSI et le RSSI.
- Toute perte ou vol d'un matériel doit être signalé sans délai à la DTNSI et sauf incapacité manifeste, dans les deux heures qui suivent la découverte de la perte ou du vol. Tout signalement effectué oralement doit être immédiatement confirmé par écrit à la DTNSI.
- A des fins de maintenance informatique, la DTNSI peut accéder à distance aux postes de travail. Cette intervention s'effectue avec l'autorisation expresse de l'Utilisateur.
- Dans le cadre de mises à jour et évolutions du système d'information, et lorsqu'aucun Utilisateur n'est connecté sur son poste de travail, le service informatique peut être amené à intervenir sur l'environnement technique du poste de travail.

Aucun matériel personnel (ex. ordinateur, clé USB, tablette, modem 4G, etc...) n'est autorisé à se connecter aux réseaux interne de Gustave Roussy et ne peut être utilisé pour traiter des informations professionnelles de Gustave Roussy.

L'utilisateur travaillant à distance (hors des locaux de Gustave Roussy et sur un réseau externe) pourra accomplir toutes ses missions en utilisant un bureau virtuel sécurisé fourni par la DTNSI (par exemple : Citrix). Cela lui permettra d'accéder à ses applications depuis n'importe quel appareil, y compris personnel.

Pour les Utilisateurs ayant un ordinateur portable mis à disposition par Gustave Roussy, le service informatique met à disposition un système antivol sur demande. Il est de la responsabilité de l'Utilisateur de s'assurer que l'ordinateur ne puisse être volé (ex. en utilisant correctement le système antivol ou en le mettant dans un tiroir fermé à clé) et ce même dans les locaux de Gustave Roussy.

Lors du départ de Gustave Roussy, l'utilisateur s'engage à rendre l'ensemble du matériel mis à sa disposition dans le cadre de l'exercice de ses missions.

L'Utilisateur doit également faire son maximum pour respecter les bonnes pratiques suivantes :

- Arrêter l'ordinateur au moins une fois par semaine
- Allumer et connecter son ordinateur au SI de Gustave Roussy au moins une fois par mois

2.2 Identifiants et mots de passe

Chaque Utilisateur dispose d'au moins un compte lui permettant de s'authentifier à l'aide d'un identifiant et d'un mot de passe pour accéder notamment à son poste de travail, aux applications, à sa messagerie ainsi qu'aux différents Systèmes d'Information.

Les règles concernant les identifiants et mots de passe sont :

- Les identifiants sont strictement personnels et inaccessibles.
- Les données d'authentification sont strictement personnelles et confidentielles. Elles ne doivent en aucun cas être communiquées à un tiers quel qu'il soit (*ex : collègue, supérieur hiérarchique, service informatique, etc...*).
- Il est rappelé que toute action réalisée à l'aide de ces données d'authentification est effectuée sous la responsabilité de l'Utilisateur et lui est imputable.
- L'utilisateur ne doit pas utiliser un mot de passe trivial (sont déconseillés : mot du dictionnaire, prénom ou nom dans le mot de passe, etc...)
- Les identifiants et mots de passe ne doivent pas être affichés sur papier ou support numérique.
- **L'Utilisateur ne doit pas utiliser un même mot de passe pour accéder à des environnements différents ou pour les différents comptes informatiques mis à sa disposition.**

Les droits d'accès par Utilisateur sont définis au strict nécessaire et au besoin d'en connaître. Toute demande de droits sur une solution (*ex. DPI*) doit être justifiée et validée au préalable par le responsable du périmètre.

2.3 Accès aux SI de l'établissement depuis l'extérieur

Gustave Roussy met à disposition des Utilisateurs la possibilité de se connecter depuis l'extérieur au SI de l'établissement via les outils dédiés à cet effet (*ex. Citrix, Webmail, messagerie sur smartphone, etc...*).

L'utilisation de ces accès externes n'est pas imposée aux Utilisateurs mais tout Utilisateur souhaitant utiliser ces services accepte de manière implicite de respecter les exigences de sécurité associées.

La principale mesure de sécurité à respecter par l'Utilisateur est l'utilisation d'une authentification multi-facteurs (ou MFA) nécessitant l'installation d'une application sur le smartphone (professionnel ou non) de l'Utilisateur, ou l'enregistrement d'un numéro de téléphone portable (professionnel ou non) ou d'une adresse mail non fournie par l'établissement (*ex. boîte email personnelle*). Le traitement de ces données est fondé sur l'intérêt légitime de Gustave Roussy à mettre en œuvre des dispositifs destinés à assurer la sécurité et le bon fonctionnement des applications informatiques et des réseaux.

Ces éléments sont nécessaires pour garantir la sécurité du SI de Gustave Roussy, de garantir l'identité des personnes accédant au SI de l'établissement et ainsi éviter l'usurpation d'identité.

L'utilisateur est informé que l'application de MFA ne dispose pas de droit particulier sur le smartphone de l'Utilisateur et ne récupère pas de données sur ce dernier.

2.4 Messageries

GUSTAVE ROUSSY met à disposition de l'Utilisateur différents systèmes de messagerie professionnelle (*ex : Outlook, Teams*).

Des mécanismes de sécurité sont déployés au niveau des services de messagerie afin de bloquer les menaces potentielles pour le Système d'Information de Gustave Roussy. De ce fait, certains messages ou fichiers joints peuvent être filtrés/bloqués ou encore analysés par l'équipe en charge de la sécurité du SI de l'établissement.

L'Utilisateur doit cependant rester vigilant quant à la réception de mails notamment ceux provenant d'expéditeurs inconnus, dont la forme ou le fond font suspecter un caractère malveillant. En cas de suspicion, l'Utilisateur doit en informer son support informatique et lui transférer le mail suspect en pièce jointe pour analyse. Il ne doit pas ouvrir les messages douteux, les pièces jointes suspectes, ni répondre à l'émetteur de ces messages ou cliquer sur les liens qui y sont présents et prévenir la DTNSI dans les meilleurs délais.

Il est rappelé que les systèmes de messagerie ne permettent pas de garantir par défaut la confidentialité des informations échangées. En ce sens, lors de l'envoi de données sensibles, il est nécessaire de protéger ces données par un mécanisme de chiffrement (*ex. En utilisant les outils permettant l'envoi/le dépôt sécurisés de données validés par le RSSI*).

Lors d'envois de données, en particulier sensibles, l'utilisateur s'assure que la liste des destinataires du message ne comporte pas de destinataire inapproprié.

L'usage d'une adresse électronique de type « gmail » pour communiquer avec un patient constitue une négligence dans la sécurisation des données à caractère personnel au sens du RGPD. Le personnel médical dispose d'une adresse se terminant par **@gustaveroussy.mssante.fr**. Cette adresse peut être fournie aux correspondants et permet de communiquer des informations de patients en toute sécurité.

Pour rappel, la transmission de données de santé par messagerie électronique (non MS-santé) et fax, à d'autres professionnels de santé, ne constituent pas un moyen suffisamment sécurisé pour transmettre des données de santé.

Toute utilisation à titre professionnel d'un compte de messagerie non professionnel ou n'appartenant pas à Gustave Roussy est strictement interdite.

La redirection automatique de messages professionnels vers une boîte email personnelle ou n'appartenant pas à Gustave Roussy est strictement interdit (*ex. redirection des emails vers une boîte personnelle, redirection vers une boîte emails d'un autre établissement*).

Il est rappelé à l'Utilisateur que toute adresse email mise à sa disposition est sous sa responsabilité, et l'adresse mail à son nom conserve son caractère professionnel. A cet égard, tout message reçu ou envoyé depuis la messagerie professionnelle mise à disposition par Gustave Roussy a par principe un caractère professionnel.

L'utilisation des systèmes de messagerie de Gustave Roussy à titre privé est tolérée mais doit rester exceptionnelle et ne doit en aucun cas perturber le fonctionnement global.

La diffusion de messages privés à usage commercial, politique ou de publicité est strictement interdite. De manière générale, la messagerie ne peut donc pas servir à diffuser des messages sans rapport avec l'activité professionnelle.

Il appartient aux Utilisateurs de procéder eux-mêmes à la sauvegarde de leur courrier électronique personnel.

Les messages électroniques échangés avec des tiers peuvent, le cas échéant former un contrat, engageant légalement l'Utilisateur ou Gustave Roussy. Ainsi, l'Utilisateur doit, en conséquence, être vigilant sur la nature des messages électroniques qu'il échange au même titre que pour les courriers traditionnels.

GUSTAVE ROUSSY tolère l'utilisation d'un smartphone ou d'une tablette personnelle pour consulter la messagerie professionnelle aux conditions exclusives suivantes :

- L'appareil doit être maintenu à jour
- L'appareil doit avoir un système de sécurité (*ex. code, empreinte, reconnaissance faciale*)
- **Seules les applications Microsoft peuvent être utilisées** (*Microsoft Outlook, Teams, etc...*) pour consulter les données de Gustave Roussy. Les autres applications ne sont pas autorisées.

Le non-respect de ces conditions pourra entraîner l'arrêt de la tolérance d'usage à l'Utilisateur.

La redirection automatique de mail vers une boîte mail externe est strictement interdite (même ponctuellement).

La bonne pratique consistant à utiliser le Webmail ou bien utiliser la messagerie électronique sur smartphone.

2.5 Accès internet et navigation Web

Gustave Roussy met à disposition de l'Utilisateur les moyens nécessaires à la navigation Web depuis ses locaux.

Afin de limiter les risques pour le Système d'Information, l'accès Internet mis à disposition par Gustave Roussy fait l'objet de mesures de sécurité, dont notamment : (accès depuis un PC GR en homeoffice)

- Filtrage basé sur des catégories de sites. En cas de blocage, une demande de déblocage peut être effectuée à la DTNSI dans la mesure où le besoin est légitimé par des besoins professionnels et que cela ne représente pas un risque pour le SI de Gustave Roussy.
- Authentification des Utilisateurs.
- Surveillance par l'antivirus des contenus téléchargés.
- Enregistrement de l'historique de la navigation.

Dans le cadre de ses missions, l'Utilisateur doit utiliser les solutions d'accès à Internet suivantes :

- Dans les locaux de Gustave Roussy : accès Internet professionnel mis à disposition.
- En dehors des locaux de Gustave Roussy : de préférence solutions de nomadisme professionnel, ou à défaut, points d'accès sécurisés (fournisseur de confiance et protection par mot de passe).
- En télétravail : utiliser uniquement le VPN fourni par Gustave Roussy pour accéder aux Systèmes d'Information de Gustave Roussy.

L'utilisation de services en mode Cloud non validés par Gustave Roussy est strictement interdite.

Le téléchargement de logiciels ou application est strictement interdit, sauf autorisation explicite de la DTNSI et du RSSI.

2.6 Téléphonie et dispositifs connectés

Dans le cadre des missions de l'Utilisateur, Gustave Roussy peut mettre à disposition de l'Utilisateur un dispositif connecté tel qu'un téléphone fixe, un téléphone mobile, une tablette, etc...

L'usage de ce type de dispositifs a pour objectif prioritaire la réalisation des missions de l'Utilisateur et sont destinés à un usage professionnel. Il doit se faire dans le respect des règles suivantes :

- Pas d'utilisation de services surtaxés ou payants (numéros surtaxés, communications à l'étranger hors-forfait, applications payantes) sans validation managériale.
- Respect des règles de vocabulaire, de style, de ton et de savoir-vivre.

Les dispositifs connectés et téléphones pouvant constituer un risque de sécurité pour le SI, il est nécessaire de respecter les points suivants :

- L'installation et la configuration d'applications (ex : *messagerie*) accédant ou manipulant des données de Gustave Roussy doivent se faire en accord avec les règles de sécurité de Gustave Roussy.
- La sécurité physique de ces périphériques doit être assurée par l'Utilisateur afin de garantir la disponibilité et la confidentialité des informations stockées.

2.7 VPN

Au même titre que les logiciels non validés par l'établissement, l'utilisation de VPN non fourni par l'établissement est strictement interdit sur son SI.

Un VPN permettant d'outrepasser un certain nombre de règle de sécurité, toute tentative d'installation ou d'utilisation peut être considéré comme une tentative de contournement des règles de sécurité ou comme une tentative d'intrusion dans le SI de l'établissement.

En cas de besoin de mise en œuvre de VPN avec un autre établissement de santé, ce besoin devra faire l'objet d'une demande spécifique.

2.8 Dispositifs de stockage et d'échange de données

Gustave Roussy met à disposition différentes ressources de stockage et d'échange de données réparties en plusieurs catégories :

- Ressources de stockage partagées (ex. SharePoint, Teams, serveurs de fichiers [lecteurs réseaux, etc...])
- Ressources de stockage personnelles (ex. OneDrive fourni par Gustave Roussy, lecteur réseau R:)
- Périphérique de stockage amovible (ex. clé USB, disque dur externe, etc...)
- Plateforme d'échange ponctuel

- **Pour les ressources de stockage partagées :**
L'utilisateur est informé que :
 - Chaque service dispose d'un environnement de stockage partagé sous la responsabilité du responsable de ce même service, cet environnement doit être utilisé pour les activités courantes (ex. partage de documents pour un projet)
 - L'attribution des droits d'accès doit se faire en fonction du besoin d'en connaître et est sous la responsabilité de chaque propriétaire de la ressource
 - Le stockage de données personnel sur ces ressources est strictement interdit

- **Pour les ressources de stockage personnelles :**
L'utilisateur est informé que :
 - Le partage de documents via l'espace de stockage personnel n'est pas autorisé (Le partage doit se faire via les plateformes dédiées).
 - Le stockage de données privées est toléré mais son usage doit être raisonnable. La DTNSI se réserve le droit de limiter le stockage ou de demander la suppression de ces données si l'usage dépasse le cadre raisonnable (ex. plusieurs dizaines de giga de photos de vacances).

- **Pour les périphériques de stockage amovible :**
Par défaut, l'usage de périphérique de stockage est strictement interdit et nécessite une autorisation préalable. Son usage doit faire l'objet d'une validation préalable auprès du RSSI et doit être justifié par l'impossibilité de faire autrement.

Lorsque l'usage est autorisé :
 - Les données sensibles stockées sur ces dispositifs doivent obligatoirement être chiffrées et protégées par un code
 - Ce type d'usage doit être une solution d'appoint ponctuelle et exceptionnelle. L'utilisation des plateformes d'échanges de Gustave Roussy devant être privilégié
 - Tout dispositif de stockage amovible pouvant contenir des fichiers et dont l'utilisateur ne connaît pas la provenance doit être considéré par défaut comme un risque pour le Système d'Information de Gustave Roussy. En ce sens, il est interdit d'en faire usage ou de le brancher sur le poste de travail ou sur le réseau de Gustave Roussy. En cas de doute, l'utilisateur doit s'adresser à la DTNSI pour mener les investigations nécessaires.
 - L'utilisation de dispositifs de stockage amovibles personnels dans un cadre professionnel est strictement interdite.

Les périphériques de stockage amovibles peuvent faire l'objet de blocage.

➤ **Pour les plateformes d'échange :**

Seules les plateformes d'échanges explicitement validées par le RSSI et la DPO sont autorisées.
Pour les échanges de données de santé, l'utilisation de plateforme certifiée HDS est obligatoire.

Enfin, de manière générale, le stockage et l'exploitation de données Gustave Roussy en dehors du SI de l'établissement est strictement interdit sauf si encadré par un contrat et validé par le RSSI, la DPO et la DTNSI.

2.9 Contrôles de sécurité

L'ensemble des ressources mis à disposition des Utilisateurs dispose de mécanismes de sécurité.

Ces derniers produisent notamment des journaux d'événements détaillés recensant notamment toutes les connexions et tentatives de connexions effectuées. Ces journaux sont conservés sur une période d'un an glissant maximum conformément à la réglementation en vigueur (durée de conservation en fonction de la solution).
Il est indiqué à l'Utilisateur que les ressources de stockage partagées permettent d'enregistrer les activités de chaque Utilisateur et les modifications de privilèges d'accès.

L'accès à ces journaux d'événements est limité aux personnes habilitées.

L'équipe du RSSI ou la DTNSI opère, sans avertissement, les investigations nécessaires à la résolution de dysfonctionnements qui mettent en péril son fonctionnement ou sa sécurité. Il peut en résulter une révision des mesures de sécurité et la mise en place d'une surveillance accrue.

En cas d'identification d'un risque pour la sécurité du système d'information et après validation du DPO et le RSSI, Gustave Roussy peut être amenée à consulter le contenu stocké sur les ressources mise à disposition des Utilisateurs.

L'utilisation de ces éléments de preuve ne pourra se faire qu'avec la validation de la Direction, du DPO et du RSSI. Il est important de rappeler que des poursuites pénales et/ou civiles pourraient être engagées vis-à-vis de l'Utilisateur lui-même et/ou Gustave Roussy du fait d'action(s) pénalement répréhensibles effectuées avec ou sur le Système d'Information de Gustave Roussy.

2.10 Utilisation à titre privé

L'utilisation à titre personnel de ressources mis à disposition de l'Utilisateur par Gustave Roussy est tolérée.

Cet usage doit cependant :

- Demeurer raisonnable et modéré dans le temps
- Respecter le cadre légal et réglementaire
- Respecter les règles de sécurité de Gustave Roussy
- Ne pas gêner l'activité de Gustave Roussy
- Ne pas porter atteinte à la sécurité et l'image de Gustave Roussy
- Ne pas mettre en péril les ressources des Systèmes d'Information de Gustave Roussy

3 Contrôle des accès physiques

L'accès aux locaux de Gustave Roussy fait l'objet de mesures de sécurité en conformité avec la politique de sécurité de Gustave Roussy.

La surveillance des accès est réalisée au travers des mécanismes suivants :

- Badges personnels

Les badges sont strictement personnels et permettent à l'Utilisateur de se déplacer dans les zones qui lui sont autorisées. Le système de contrôle d'accès trace les accès et tentatives d'accès aux différentes zones. L'accès à ces journaux d'événements est restreint aux seules personnes habilitées. L'utilisation de ces éléments de preuve ne pourra se faire qu'avec la validation de la Direction, du RSSI, et celle du DPO.

- Vidéosurveillance

Une vidéosurveillance est mise en place dans les zones stratégiques des différents bâtiments et est mis en œuvre conformément à la réglementation en vigueur.

L'accès aux enregistrements de ces dispositifs est restreint aux seules personnes habilitées. L'utilisation de ces éléments de preuve ne pourra se faire qu'avec la validation de la Direction, du Responsable de la sécurité, du Responsable des affaires juridiques et celle du DPO.

Le système de vidéosurveillance est géré par le responsable de la sécurité.

4 Départ de Gustave Roussy

En cas de départ définitif de Gustave Roussy, l'Utilisateur doit rendre l'intégralité du matériel mis à sa disposition dans le cadre de ses missions.

L'Utilisateur doit prendre les dispositions suivantes avant de rendre son matériel :

- Veiller à ce qu'aucun dossier ou fichier contenant des informations de nature personnelle ne subsiste sur le disque dur de son ordinateur et/ou sur les espaces de stockage mis à sa disposition sur le réseau informatique de Gustave Roussy à la date du départ effectif.
- Veiller à ce qu'aucun mail revêtant le caractère d'une correspondance privée ne subsiste dans la messagerie à la date du départ effectif.
- Veiller à mettre à disposition toutes les informations nécessaires à la continuité de son activité sur les espaces de travail collaboratif ou les transmettre directement.

Toute copie ou suppression de documents professionnels sans autorisation est strictement interdite.

L'Utilisateur s'engage à ne pas transmettre ses identifiants/mots de passe au moment de son départ.

À la suite de son départ, les fichiers et messages seront tous considérés comme ayant un objet professionnel et mis, à ce titre, à la disposition pleine et entière de Gustave Roussy. Dans le cas où leur caractère personnel et privé serait établi par la suite, ils seraient détruits.

Dans un souci de continuité d'activité et de non-perte d'information en cas de départ d'un salarié, les espaces de stockage dédiés à l'Utilisateur et la messagerie seront conservés durant 6 mois après le départ de salarié puis supprimés définitivement après ce délai.

Après le départ et en cas de demande d'accès à des informations professionnelles contenues dans l'espace de stockage dédié à l'Utilisateur ou dans sa messagerie, seules les données professionnelles seront transmises au supérieur hiérarchique.

Les comptes informatiques d'un Utilisateur étant strictement personnels et inaccessibles, aucun libre accès ne sera donné aux comptes d'un ancien Utilisateur afin notamment d'éviter toute tentative d'usurpation d'identité.

5 Protection des données à caractère personnel

L'Utilisateur est informé de la nécessité de respecter les dispositions légales et réglementaires en matière de traitement de données à caractère personnel, conformément aux dispositions légales et réglementaires applicables à la protection des données personnelles, telles que celles du Règlement Général sur la Protection des Données (RGPD) et de la loi n°78-17 du 6 janvier 1978 relative à l'informatique et aux libertés (Loi Informatique et Libertés). Tous les fichiers contenant des données à caractère personnel doivent s'y conformer.

5.1 Les engagements de l'Utilisateur

L'Utilisateur s'engage notamment à :

- Déclarer au DPO tout nouveau traitement de données à caractère personnel, pour lequel Gustave Roussy est responsable de traitement ou sous-traitant ;
- Ne collecter que les données strictement nécessaires au regard de la finalité poursuivie ;
- Soumettre ses traitements à la réalisation d'une analyse d'impact ;
- Prévenir dans les plus brefs délais le RSSI ou le DPO, en cas de violation de données afin de permettre le respect de l'obligation de notification auprès de l'autorité de contrôle dans les 72 heures maximum ;
- Transmettre dans les plus brefs délais au DPO toute demande d'exercice de droits venant des personnes concernées par les traitements afin de permettre à Gustave Roussy de respecter son obligation de réponse dans les délais réglementaires impartis ;
- Transmettre toute information susceptible d'aider dans le cadre d'un contrôle de la Commission Nationale de l'Informatique et Libertés ;
- Informer Gustave Roussy si l'Utilisateur ou l'un de ses sous-traitants, est tenu de procéder à un transfert de données vers un pays en dehors de l'Union européenne ;
- Ne faire aucune copie, extraction ni exploitation de données personnelles sauf à ce que cela soit nécessaire à l'exécution de ses fonctions et des finalités de ses autorisations ;
- Prendre toutes les mesures conformes aux usages, à l'état de l'art, aux bonnes pratiques et à la réglementation en vigueur dans le cadre de ses attributions et de ses autorisations afin d'éviter l'utilisation détournée ou frauduleuse de ces données et préserver la sécurité physique et logique de ces données ;
- Consulter et saisir les données à caractère personnel uniquement sur des outils sécurisés mis à disposition par Gustave Roussy ;
- Ne conserver les données à caractère personnel de patients, même pseudonymisées, uniquement sur le réseau privatif de Gustave Roussy ;
- En cas de cessation de ses fonctions, en informer Gustave Roussy et restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.

5.2 Les engagements de Gustave Roussy

En parallèle, chacun des Utilisateurs accepte la collecte de certaines de ses données à caractère personnel, dont notamment son nom, son prénom, et son service de rattachement en vue de son identification sur le système d'information par Gustave Roussy. Ce traitement est fondé sur la base légale du RGPD relatif à l'exécution du contrat de travail, à l'intérêt légitime.

Conformément aux dispositions applicables, chaque Utilisateur dispose d'un droit d'accès, de rectification, d'effacement (droit à l'oubli), de limitation, d'opposition et de portabilité de ses données relatives à l'ensemble des données collectées le concernant, y compris les données portant sur l'utilisation du système d'information. Ce droit s'exerce auprès du DPO (donneespersonnelles@gustaveroussy.fr). En cas de difficulté à exercer ces droits, il est possible d'introduire une réclamation auprès de la CNIL à l'adresse suivante : <https://www.cnil.fr/fr/plaintes>.

Par ailleurs, il est rappelé que l'envoi de données à caractère personnel, doit être « sécurisé ». En cas de doute concernant un envoi de données à caractère personnel à la suite d'une demande (interne ou externe), l'Utilisateur doit se rapprocher du DPO de Gustave Roussy pour vérifier la conformité du transfert.

5.3 Lexique RGPD

Responsable de traitement	La personne physique ou morale qui détermine les finalités et les moyens du traitement.
Sous-traitant	La personne physique ou morale qui traite des données à caractère personnel pour le compte du responsable du traitement.
Personnes concernées	La personne dont on collecte les données.
Traitement de données	Toute opération effectuée sur des données à caractère personnel à l'aide de procédés automatisés ou non. <i>Exemples</i> : la collecte, l'enregistrement, l'organisation, la structuration, la conservation, la modification, l'extraction, la consultation, la destruction, l'effacement...
Données à caractère personnel ou données personnelles	Toute information se rapportant à une personne physique identifiée ou identifiable. L'information permet une identification directe ou indirecte, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.
Données sensibles	Ces données révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale. Elles comprennent aussi le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.
Violation de données	Tout incident de sécurité, d'origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles.
Exercice de droits	Gustave Roussy a mis en place une procédure, processus de manière à garantir une réponse rapide aux demandes formulées par les personnes concernées afin que celles-ci puissent exercer pleinement leurs droits, notamment leur droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

6 Sensibilisation

Tout Utilisateur s'engage à suivre les campagnes de sensibilisations liées à la sécurité au travers des cursus mis à disposition par Gustave Roussy.

7 Sanctions applicables

Tout manquement aux règles de la présente charte est susceptible de faire l'objet de sanctions disciplinaires prévues au règlement intérieur dont l'importance sera notamment fonction de la gravité des manquements constatés.

Il est rappelé que le non-respect des lois applicables en matière de sécurité des Systèmes d'Information est susceptible de poursuites et sanctions pénales prévues par la loi.

8 Entrée et vigueur et évolutions

La Charte a été approuvée par le Directeur Général de Gustave Roussy.

Elle a été soumise au Comité Social et Economique pour avis, puis transmise à l'Inspection du Travail et déposée au secrétariat-greffe du Conseil des Prud'hommes de Créteil.

Elle est annexée au Règlement Intérieur de Gustave Roussy, et diffusée sur l'intranet.

La Charte pourra évoluer en fonction d'évolution technique et du droit.

Le RSSI comme la Direction pourront être amenés à mettre en place des consignes complémentaires afin de préserver la sécurité du SI de Gustave Roussy et ainsi assurer la pérennité du SI face aux menaces potentielles.

Elle entre en vigueur à compter du 12 mai 2025.