CHARTE ADMINISTRATEUR DES SYSTÈMES D'INFORMATION

2017

GUSTAVE ROUSSY
CANCER CAMPUS
GRAND PARIS

CYCLE DE VIE DU DOCUMENT

HISTORIQUE DU DOCUMENT

Version	Date	Description	Détails
1.0	10/2016	Charte Administrateur des Systèmes d'Information (version initiale)	

AUTEUR

Fonction	Nom	Date
Référent Sécurité des Systèmes d'Information / Architecte technique SI	LEMOINE Cédric	10/2016

CONCERTATION / AVIS

Fonction	Nom	Date
Directoire	EGGUERMONT Alexander VARNIER Frédéric DUCREUX Michel MORICE Philippe FIZAZI Karim SOLARY Eric SCHLUMBERGER Martin CALVO Fabien MONTARON Anne BOURASSIN Philippe BENHAMOU Ellen DEUTCH Eric	04/2017
Comité de Direction	VARNIER Frédéric DUCREUX Michel MONTARON Anne BOURASSIN Philippe MEZAOUR Naima PUSTILCOV Ilia STEPANIAN Stéphane DAHER Valérie BIGOURDAN Philippe BRIERE Virginie MONS Muriel	02/2017

Fonction	Nom	Date
Direction de la recherche	SOLARY Eric BOUCARD David BOURSIN Yannick	03/2017
Direction de l'enseignement	SCHLUMBERGER Martin CROUAN Antoine GRELLIER Elodie	03/2017
Direction des Systèmes d'information	MEZAOUR Naima BUSET Marc TAHAR Mouheb GAVOILLE André DARLY Jimmy	01/2017
Direction des Ressources Humaines	BOURASSIN Philippe ALAYRAC Caroline	02/2017
Service des Affaires Juridiques	VEROTTE Nelly CHEVALLOT Sabine	02/2017
Comité d'Hygiène, de Sécurité et des Conditions de Travail		04/2017
Comité d'Entreprise		04/2017

VALIDATION

Fonction	Nom	Date
Directeur Général	EGGERMONT Alexander VARNIER Frédéric	04/2017

LISTE DE DIFFUSION DU DOCUMENT

Fonction	Nom	Date
Tout Administrateur des Systèmes d'Information de Gustave Roussy		12/06/2017

SOMMAIRE

Article 1 : Objet et champ d'applications

Ce document constitue la charte Administrateur du Système d'Information de Gustave Roussy.

Dans la présente charte, sont désignés les termes suivants :

- **Moyens informatiques** : Ce sont les moyens matériels (ordinateurs, serveurs, imprimantes, tablettes, smartphones) et logiciels mis à disposition dans le cadre des fonctions occupées et/ou missions, au sein de Gustave Roussy.
- **Système d'Information :** Ensemble des éléments et règles participant à la gestion, au stockage, au traitement, au transport et à la diffusion de l'information au sein de l'Établissement, en provenance et vers ses partenaires externes.
- **Utilisateur** : toute personne, quel que soit son statut, ayant accès ou utilisant les moyens informatiques professionnels dans le cadre de son emploi, d'une prestation ou d'un stage au sein de l'Établissement de Santé.
- **Administrateur** : tout personnel ayant des droits étendus sur tout ou partie du Système d'Information (SI), disposant de par ses fonctions et/ou ses missions, d'habilitations permettant d'intervenir sur :
  - Les composants d'infrastructure des SI (exemples : serveurs, réseaux, infrastructure de stockage et sauvegarde, infrastructure téléphonique)
  - Les Bases de données
  - Les Equipements de sécurité des SI
  - Les postes de travail et leurs périphériques
  - Le développement d'applications/logiciels ou interfaces

Cette charte est applicable à :

- L'ensemble des personnels de la Direction des Systèmes Informations hors service des archives Médicales,
- Les administrateurs localisés au sein des pôles et services, quel que soit leur statut (salariés et non-salariés, stagiaires, personnel intérimaire),
- Aux personnels extérieurs exerçant une mission au sein de la DSI (tout prestataire d'infogérance, consultants, sous-traitants, fournisseurs, formateurs…) utilisant les moyens informatiques de l'établissement sur site et/ou à distance.

L'objectif de la charte est de définir les bons usages, les droits et devoirs de chaque Administrateur sur le Système d'Information de Gustave Roussy, au regard de la Politique de Sécurité du Système d'Information (PSSI) de l'établissement, et des obligations législatives et réglementaires de la sécurité de l'information dans les établissements de santé.

Les responsables de chaque direction et département s'engagent à identifier les utilisateurs internes et externes ayant potentiellement des droits étendus sur le SI, et communiquer la liste de ces personnes au Référent Sécurité du Système d'Information (RSSI).

En tant qu'Utilisateur du Système d'information, l'Administrateur s'engage à respecter la charte Utilisateur du Système d'Information, ainsi que cette présente charte pendant la durée de son contrat ainsi qu'à sa cessation.

La liste des Administrateurs est maintenue à jour par le RSSI, dans le document ***« C2-liste-Administrateurs.xls »***

Article 2 : Droits et Obligations

n°	règles
Politique de Sécurité	
1	L'Administrateur s'engage à respecter les règles de la charte utilisateur et la Politique de Sécurité du Système d'Information (PSSI). Il relève et signale au RSSI, toute anomalie ou risque de sécurité SI.
Comptes informatiques et mots de passe	
2	L'Administrateur dispose de deux types de comptes : un compte « standard », pour le fonctionnement de routine et un compte dit « administrateur » avec des droits étendus. Il s'engage à utiliser son compte administrateur dans les strictes conditions de nécessité de service.
3	L'Administrateur s'engage à ne créer aucune dépendance entre ses comptes personnels et la fonction d'un composant du Système d'Information. Des comptes spécifiques dédiés doivent être utilisés pour le fonctionnement des composants des SI (exemple : taches planifiées). Une vigilance particulière doit être observée sur les plateformes de test
4	L'Administrateur doit s'assurer que tous les comptes et mots de passe génériques qu'il utilise pour l'administration des différents systèmes soient dûment documentés et enregistrés dans un référentiel de mots de passe, défini et accessible à tout moment par sa hiérarchie et les personnels habilités. Le mot de passe d'accès à ce référentiel est hautement sensible. Il doit être mémorisé par les personnes habilitées à accéder au référentiel, et ressaisi à chaque accès. En aucun cas, il ne doit être inscrit sur un papier ou dans un fichier, quelle que soit la sécurité associée à ce fichier.
5	En cas de nécessité de création d'un compte générique, L'Administrateur s'engage à respecter les mêmes règles de constitution d'un mot de passe individuel (cf. charte utilisateurs). Les comptes génériques de services ne doivent être connus et utilisés par les prestataires dans les conditions de production.
6	L'Administrateur s'engage à respecter le principe du moindre privilège pour tout compte de services.

n°	règles
7	En aucun cas, L'Administrateur ne doit demander les mots de passe à un utilisateur.
8	L'Administrateur doit s'assurer de l'identité de son interlocuteur, lors de la réinitialisation d'un mot de passe (perdu, oublié ou compromis). Cette réinitialisation doit, si le système le permet, être paramétrée de façon à forcer un changement du mot de passe par l'utilisateur, à la prochaine utilisation du système.
Locaux et Outils utilisés	
9	L'Administrateur s'engage à respecter scrupuleusement les procédures liées à l'accès aux locaux informatiques et à signaler toute altération constatée d'équipements au RSSI. L'Administrateur considère ses espaces de travail comme sensibles et y met en œuvre la sécurité nécessaire (armoires, cubes et tiroirs fermés, coffres, locaux sécurisés) dans la mesure du possible.
10	L'Administrateur doit s'assurer de façon régulière que son poste de travail dispose bien de protections actives et à jour contre les programmes malveillants. L'Administrateur doit veiller à utiliser uniquement des outils réputés fiables sur le plan de la sécurité. Il évitera ainsi d'installer sur son poste et/ou sur un poste ayant des accès privilégiés, des outils risquant de comporter des logiciels espions, chevaux de Troie et autres programmes malveillants.
11	L'Administrateur doit éviter d'accéder à internet via sa session avec droits étendus.
12	L'Administrateur doit tester toute évolution ou correction logicielle sur un environnement de test (relevant de son champ d'intervention) avant une mise en production.
13	L'Administrateur s'interdit toute installation de logiciels et/ou outils non conformes sur le SI de l'Etablissement. Il s'engage à choisir en priorité les outils homologués par l'ANSSI, ou à défaut des outils standards du marché sous licence. L'usage de certains outils « gratuits » pertinents peut être autorisé, le RSSI peut être consulté en cas de doutes.
14	Dans le cas d'une nécessité de prise de main à distance, L'Administrateur s'engage à n'utiliser que les systèmes d'accès distants homologués par la DSI et mis en œuvre à cet effet.
Confidentialité et Réserve	
15	L'Administrateur s'engage à ne pas accéder aux données désignées explicitement comme privées, sauf dans le cadre d'une enquête judiciaire, et sur demande formelle de l'établissement.
16	Pour des raisons de continuité de service, et selon les dispositions institutionnelles, l'Administrateur a le droit de consulter des données professionnelles d'un utilisateur absent momentanément ou bien définitivement.

n°	règles
17	L'Administrateur a le devoir de configurer et d'administrer les systèmes qu'il gère dans le sens d'une meilleure sécurité, dans l'intérêt de l'établissement, des utilisateurs, et en accord avec le RSSI.
18	En cas de demande d'un utilisateur, L'Administrateur est tenu de confirmer ses accès, en toute transparence. Il doit cependant respecter les règles de confidentialités et de réserve de cette charte.
Surveillance	
19	L'Administrateur a le droit d'accéder, sur les systèmes qu'il administre, à des informations nécessaires à ses missions de maintien en condition opérationnel (diagnostic et d'administration, analyse de logs), en respectant scrupuleusement la confidentialité de ces informations.
20	L'Administrateur s'interdit la mise en œuvre de procédure de surveillance ciblée sur une ou plusieurs personnes sans l'accord de sa hiérarchie, du RSSI, et dans le cadre strict du maintien en conditions opérationnelles des SI.
Relation avec les tiers	
21	L'Administrateur s'engage à informer son service de la venue d'un prestataire, et que ce dernier n'accède qu'aux informations nécessaires à son intervention.
22	Dans la mesure du possible, l'Administrateur ne doit pas laisser un prestataire extérieur ou un utilisateur extérieur à la DSI seul dans les locaux techniques de la DSI. Il s'engage à respecter la procédure d'accès en salle.
23	L'Administrateur doit, dans la mesure du possible, assurer une surveillance des prestataires connectés en télémaintenance.
24	L'Administrateur doit remettre un ou plusieurs comptes par fournisseur. Ces comptes doivent être supprimés ou désactivés à la fin du contrat avec le prestataire. Ces comptes doivent respecter le principe du moindre privilège.
25	L'Administrateur ne doit pas remettre, ni permettre à des sociétés prestataires/éditeurs des extractions de données comportant des informations sensibles (qu'elles soient ou non nominatives), sauf contrat spécifique de confidentialité signé entre les parties, et en accord avec le RSSI.
26	Sauf validation du RSSI, l'Administrateur n'autorise pas la connexion de matériel du prestataire sur le réseau local de Gustave Roussy. Le prestataire devra utiliser une connexion sécurisée ou un matériel fourni par Gustave Roussy

n°	règles
Alerte	
27	L'Administrateur s'engage à signaler au RSSI tout risque, et tout incident susceptible de porter atteinte à la sécurité du Système d'Information.
Sécurité dans les demandes et dans les projets	
28	L'Administrateur fait preuve de vigilance quant au traitement des demandes, et s'assure de leur bonne provenance et de leur cohérence. Il suit la procédure de traitement des incidents
29	Toute mise en place ou évolution dans les modalités ou technologies de sécurité des SI doit faire l'objet d'une validation du RSSI.

Article 3 : Entrée en vigueur

Conformément à l'article L. 6162-7 du Code de la santé publique, la Direction Générale de Gustave Roussy a arrêté la présente charte après avis et concertation (se conférer à la partie « cycle de vie du document » en page 2 et 3).

Cette Charte est annexée au Règlement intérieur et est diffusée aux personnels qualifiés Administrateur.

La Charte Administrateur des Systèmes d'Information entre en vigueur à compter de la date de publication mentionnée dans la partie « liste de diffusion du document » en page 3.
Elle sera modifiée en fonction du contexte législatif et réglementaire et des évolutions des nouvelles technologies.

GUSTAVE ROUSSY
CANCER CAMPUS
GRAND PARIS

114, rue Édouard-Vaillant
94805 Villejuif Cedex - France

www.gustaveroussy.fr