

CHU DIJON			V 1.0
	Charte d'Utilisation du SIC pour les Administrateurs & Titulaires de profil à privilèges	Date Application 01/06/2017	Page 1 sur 11



CHU de Dijon Bourgogne

Charte d'Utilisation du Système d'Information et de Communication pour les Administrateurs & Titulaires de profil à privilèges

	Noms	Fonctions	Date
Créateur	Sébastien MOREY	RSSI	15/02/2017
Rédacteurs	Sébastien MOREY	RSSI	15/02/2017
Vérificateur	COSSI/Bertrand JEANMOUGIN	DSI	
Approbateur	Bertrand JEANMOUGIN	DSI	

Historique du document

Version	Date	Auteur	Changements
1.1	15/02/2017	S. MOREY	Corrections mineures
1.0	01/09/2014	G. SAGGIORO	Initialisation document

Historique Diffusion

Version	Date	Destinataires	Commentaires
1.0	A définir		

CHU DIJON			V 1.1
	Charte d'Utilisation du SIC pour les Administrateurs & Titulaires de profil à privilèges	Date Application 06/03/2017	Page 2 sur 11

Table des matières

PREAMBULE	3
1. Objet du document	4
2. Les droits des administrateurs	5
2.1. Utilisateurs aux droits étendus	5
2.2. Utilisation de logiciels/matériels spécifiques	5
3. Les devoirs des administrateurs	7
3.1. Respect de la Charte d'Utilisation du Système d'Information et de Communication	7
3.2. Des devoirs clairement identifiés	7
3.3. Un suivi imposé	8
3.4. Incidents de sécurité	8
3.5. Manipulation des données	8
3.6. Clause de confidentialité	9
3.7. Relation avec les tiers	9
4. Respect de la charte	10
Annexe : Formulaire d'engagement de l'ADMINISTRATEUR....	11

CHU DIJON			V 1.0
	Charte d'Utilisation du SIC pour les Administrateurs & Titulaires de profil à privilèges	Date Application TBA	Page 3 sur 11

PREAMBULE

La sécurité et le bon fonctionnement du Système d'Information et de Communication (SIC) sont l'affaire de tous et découlent d'une action à la fois collective et individuelle. Chacun doit être conscient de ses droits mais aussi de ses devoirs tant vis-à-vis des propriétaires des informations manipulées (les patients par exemple) que du CHU de Dijon Bourgogne.

La présente charte s'inscrit dans le cadre de la Politique Générale de Sécurité du Système d'Information (PGSSI), validée par la Direction Générale. Elle est de ce fait, un document de référence pour l'ensemble des entités du CHU de Dijon Bourgogne et constitue une annexe au règlement intérieur.

La présente charte ne peut couvrir de façon exhaustive tous les cas de figures possibles mais **fixe les principes généraux d'Utilisation du Système d'Information** permettant de protéger les ressources du CHU de Dijon Bourgogne.

Le Système d'Information et de Communication est considéré dans son ensemble, c'est-à-dire comme la totalité des moyens informatiques ou de télécommunications (postes de travail, dont les ordinateurs du biomédical, réseaux, Internet, téléphones, supports papier, ...) visant à créer, acquérir, traiter, stocker, archiver, diffuser ou détruire de l'Information en rapport avec l'activité professionnelle des Utilisateurs du SIC.

Les règles édictées dans ce document, s'appliquent également à l'ensemble des équipements informatiques non fournis par le CHU de Dijon Bourgogne et interagissant avec le SIC du CHU de Dijon Bourgogne. Il s'agit, à titre d'illustration des équipements personnels, ou fournis par des partenaires, et autorisés à être connectés au SIC du CHU de Dijon Bourgogne, comme décrit dans la suite du document.

Par ailleurs, la charte couvre le Système d'Information du CHU de Dijon Bourgogne, et non la sécurité dans son ensemble, c'est-à-dire la sécurité des personnes ou des moyens autres qu'informatiques (hygiène, sûreté des locaux et des outils de travail, respect de la législation du travail, ...).

CHU DIJON			V 1.0
	Charte d'Utilisation du SIC pour les Administrateurs & Titulaires de profil à privilèges	Date Application TBA	Page 4 sur 11

1. Objet du document

Cette charte a pour vocation de définir les droits et devoirs de l'ensemble des personnes, dénommées « **ADMINISTRATEURS** », responsables de l'administration des systèmes d'information.

Au sens utilisé dans le présent document, le terme « ADMINISTRATEURS » désigne tout intervenant, quel que soit son statut (agent, personnel temporaires, partenaire, fournisseur, ...) et quel que soit l'intitulé de son poste ou de sa fonction, qui a pour rôle et missions d'assurer le bon fonctionnement ou la sécurité des ressources du SIC du CHU de Dijon Bourgogne, placées sous sa responsabilité ou sur lesquels il intervient, au titre de son activité professionnelle, dans le cadre de ses droits d'accès étendus aux infrastructures techniques et applicatives.

Le terme « ADMINISTRATEURS » regroupe de façon non exhaustive les différents profils d'administrateurs suivants :

- Administrateur système ;
- Administrateur réseau ;
- Administrateur base de données ;
- Administrateur téléphonie ;
- Techniciens SAV
- Administrateurs fonctionnels / Titulaires de profils à privilèges des applications métiers
- Etc.

CHU DIJON			V 1.0
	Charte d'Utilisation du SIC pour les Administrateurs & Titulaires de profil à privilèges	Date Application TBA	Page 5 sur 11

2. Les droits des administrateurs

2.1. Utilisateurs aux droits étendus

Les ADMINISTRATEURS sont des utilisateurs possédant des privilèges étendus auxquels sont associés les droits présentés dans les chapitres suivants.

Tâche spécifique

L'ADMINISTRATEUR peut prendre les dispositions qui lui semblent nécessaires afin d'assurer le bon fonctionnement et la sécurité des composants du SI du CHU de Dijon Bourgogne, dans son périmètre de responsabilité. Il peut notamment effectuer les tâches suivantes, dans le cadre de procédures établies :

- Isoler, arrêter ou reconfigurer des comptes utilisateurs, des équipements ou des applications informatiques pouvant compromettre la sécurité de l'ensemble du SI du CHU de Dijon Bourgogne ;
- Procéder à des vérifications techniques sur des fichiers, des bases de données, de journalisation ou de configuration, afin de déceler tout anomalie ou incident de sécurité qui pourrait porter atteinte au bon fonctionnement ou à la protection du SI du CHU de Dijon Bourgogne ;
- Traiter (détection, analyse, éradication, filtrage, etc.) tous les flux informatiques présentant des risques potentiels de sécurité (virus, intrusion, utilisation d'un logiciel non autorisé, etc.).

Procédure spécifique

En cas de comportements anormaux identifiés, en lien avec l'activité des utilisateurs et du SI du CHU de Dijon Bourgogne, les ADMINISTRATEURS peuvent avoir à réaliser les actions suivantes, en conformité avec l'organisation et les procédures éventuellement en place :

- Interruption prolongée d'un service ;
- Interruption de toute tâche utilisateur, avec ou sans préavis, dans le cas où une utilisation excessive des ressources nuit au bon fonctionnement du système ;
- Archivage, compression ou suppression des données excessivement volumineuses ou sans un lien direct avec l'activité professionnelle (avec ou sans préavis si l'urgence de la situation le requiert) en cas de dégradation de service ;
- Interruption des sessions de travail inactives.

2.2. Utilisation de logiciels/matériels spécifiques

Les ADMINISTRATEURS possèdent entre autre le droit d'installer des logiciels pour leurs tâches d'administration. Il existe cependant des restrictions concernant ces logiciels et notamment :

CHU DIJON			V 1.0
	Charte d'Utilisation du SIC pour les Administrateurs & Titulaires de profil à privilèges	Date Application <i>TBA</i>	Page 6 sur 11

- Les ADMINISTRATEURS peuvent être amenés à utiliser des logiciels spécifiques, non autorisés par la liste blanche des applications aux utilisateurs du SI du CHU de Dijon Bourgogne. Ces logiciels doivent figurer dans une liste blanche des applications autorisées aux ADMINISTRATEURS mise à leur disposition pour l'accomplissement de leur fonction.
- Tout logiciel ne faisant pas partie de cette liste blanche des applications ADMINISTRATEURS doit être déclaré et validé par la Direction des Systèmes d'Information avant toute utilisation ;
- La modification de ces listes, ainsi que les dérogations susmentionnées, sont portées à la connaissance du RSSI du CHU de Dijon Bourgogne.
- Tout usage de logiciel d'analyse technique de fonctionnement ou permettant d'effectuer des scans sur tous les composants du SI du CHU de Dijon Bourgogne doit avoir reçu une dérogation du RSSI du CHU de Dijon Bourgogne avant opération par les ADMINISTRATEURS. Cette dérogation peut être permanente, elle est impérativement nominative.
- Toute réparation de panne ou prise de contrôle à distance d'un poste de travail utilisateur à l'aide d'un logiciel de télémaintenance nécessite obligatoirement l'accord de cet utilisateur si une session de cet utilisateur est active. Si nécessaire l'ADMINISTRATEUR procèdera à l'interruption de la session ;

CHU DIJON			V 1.0
	Charte d'Utilisation du SIC pour les Administrateurs & Titulaires de profil à privilèges	Date Application <i>TBA</i>	Page 7 sur 11

3. Les devoirs des administrateurs

3.1. Respect de la Charte d'Utilisation du Système d'Information et de Communication

En tant qu'utilisateur du SI du CHU de Dijon Bourgogne, les ADMINISTRATEURS doivent respecter la Charte d'Utilisation du Système d'Information et de Communication.

3.2. Des devoirs clairement identifiés

En regard des privilèges nécessaires accordés aux ADMINISTRATEURS, ces derniers doivent respecter des règles en termes de sécurité afin de réaliser leurs tâches d'administration et notamment :

- Chaque ADMINISTRATEUR doit documenter le résultat de ses actions de mise en œuvre ou modification de telle sorte que le CHU de Dijon Bourgogne ne soit pas dans un état de dépendance, ou de méconnaissance due à ces mêmes actions, lors de son départ ;
- L'ADMINISTRATEUR ne doit pas abuser de ses privilèges, et limite ses actions aux ressources informatiques dont il a la charge, dans le respect de la finalité de sa mission. En particulier, il ne modifie les configurations et les droits d'accès que dans le respect de procédures d'administration ou d'exploitation définies ;
- L'ADMINISTRATEUR ne doit pas prendre ses consignes d'une personne non autorisée ; il doit informer son responsable hiérarchique de toute demande non légitime, dans le cadre des procédures établies ; sa hiérarchie pourra l'autoriser à réaliser ce traitement ;
- L'ADMINISTRATEUR ne doit pas mettre en œuvre les requêtes lui paraissant contraire à la Politique Générale de Sécurité du SI du CHU de Dijon Bourgogne ou aux lois françaises, mais en référer à sa hiérarchie et au RSSI ;
- L'ADMINISTRATEUR ne doit pas contourner les procédures de sécurité établies, et en particulier ne désactive pas de sa propre initiative les mécanismes de traçabilité, et ne porte pas atteinte à l'intégrité des fichiers de journalisation ;
- Tout ADMINISTRATEUR doit garder strictement confidentiels les authentifiants de ses comptes personnels, ainsi que des comptes techniques dont il a connaissance pour exercer sa mission ;
- Les ADMINISTRATEURS doivent garantir le respect des procédures en vigueur et en particulier s'assurer de l'approbation préalable du propriétaire d'une application ou d'une information avant d'attribuer un droit d'accès à un utilisateur.

CHU DIJON			V 1.0
	Charte d'Utilisation du SIC pour les Administrateurs & Titulaires de profil à privilèges	Date Application TBA	Page 8 sur 11

3.3. Un suivi imposé

Dans le but de fournir un moyen de contrôle de leurs activités, les ADMINISTRATEURS ont pour obligation de respecter l'ensemble des règles suivantes :

- Toute opération impactant le périmètre de la sécurité (SI, application, infrastructure, etc.) doit obligatoirement donner lieu à un enregistrement (suivi, traces) ;
- Il est de la responsabilité des ADMINISTRATEURS d'établir et transmettre les rapports d'incidents, signalant notamment tout évènement mettant en cause la qualité et la sécurité des ressources informatiques du SI du CHU de Dijon Bourgogne, ainsi que toute infraction à la présente charte et à la Charte d'Utilisation du Système d'information et de Communication, dans le respect du processus établi de gestion des incidents de sécurité;
- Lors des gestes d'administration, l'ADMINISTRATEUR doit, le cas échéant, utiliser le compte individuel d'administration qui lui est fourni afin de permettre un suivi strict des modifications.

3.4. Incidents de sécurité

Dans le cas d'une détection d'incident de sécurité, l'ADMINISTRATEUR doit se conformer à la procédure de gestion d'incidents, et immédiatement joindre le support informatique afin d'enregistrer l'incident de sécurité et permettre d'informer le RSSI, ainsi que les personnels concernés de la DSI.

Le typage de l'incident de sécurité détecté pourra requérir de l'ADMINISTRATEUR la collecte et la conservation de preuves et traces nécessaires à la résolution de l'incident et à toute investigation ultérieure.

3.5. Manipulation des données

De par leur fonction, les ADMINISTRATEURS ont à manipuler des données plus ou moins sensibles. Les règles suivantes encadrent leur utilisation, et notamment les données à caractère personnel et les données de santé à caractère personnel des patients du CHU de Dijon Bourgogne :

- Les ADMINISTRATEURS ne doivent prendre connaissance que des informations pour lesquels ils nécessitent le besoin d'en connaître, ou sur dérogation formelle de leur hiérarchie directe ;
- L'ADMINISTRATEUR n'est pas autorisé à prendre connaissance des données personnelles d'utilisateurs (dont l'identifiant et mot de passe), sauf cas particuliers prévus par la loi (par exemple, commissions rogatoires, enquêtes judiciaires) ou habilitations formelles et légitimes préalablement déclarées ; s'il advient que l'ADMINISTRATEUR vienne à connaître le mot de passe associé à un identifiant utilisateur (par exemple dans la cadre d'une réinitialisation), cet ADMINISTRATEUR devra rappeler à l'utilisateur son devoir de changer le mot de passe ;
- L'ADMINISTRATEUR n'est pas autorisé à prendre connaissance des données de santé à caractère personnel, même au niveau des bases de données les contenant ;
- L'ADMINISTRATEUR doit respecter ses engagements de confidentialité et de non divulgation. Il ne doit pas utiliser les informations qu'il peut être amené à connaître dans le cadre de ces fonctions.

CHU DIJON			V 1.0
	Charte d'Utilisation du SIC pour les Administrateurs & Titulaires de profil à privilèges	Date Application TBA	Page 9 sur 11

- L'ADMINISTRATEUR n'est pas autorisé à extraire ou copier toute donnée issue du système d'information en dehors du strict exercice de sa mission. Toute extraction ou copie qui serait rendue nécessaire pour concourir au diagnostic d'un incident devra être effacée sous la responsabilité de l'administrateur et dans l'échéance maximale de la résolution de l'incident.

3.6. Clause de confidentialité

Au regard des informations auxquelles l'ADMINISTRATEUR a accès dans le cadre de sa mission et de ses compétences, il est indispensable de préciser le caractère de confidentialité absolue que doit revêtir l'exercice de son activité.

Il est rappelé que l'accès aux informations confidentielles (en raison de l'importance stratégique et du caractère confidentiel qu'elles revêtent) constitue une responsabilité qui n'est confiée qu'à un nombre de collaborateurs restreint et contrôlé.

Dès lors, il appartient aux ADMINISTRATEURS d'assurer que ces informations restent confidentielles et qu'aucunes données sensibles ne soient transmises ou accessibles (directement ou indirectement) par une tierce personne.

Le CHU de Dijon Bourgogne se réserve la possibilité de vérifier, à l'aide d'un système de surveillance, la conformité des habilitations et incidemment des droits d'accès associés, ainsi que la conformité de l'utilisation faite de ces différents comptes (identifiant / mot de passe), et notamment ceux confiés aux ADMINISTRATEURS.

3.7. Relation avec les tiers

De par sa fonction, l'ADMINISTRATEUR peut être amené à donner accès à des ressources informatiques à des Tiers opérant de manière ponctuelle. Dans ce cadre, il se doit de respecter les procédures en place au sein du CHU de Dijon Bourgogne (demande d'accès à une salle informatique, demande d'informations suite à un incident, demande de connexion particulière, etc.). S'il n'a pas à sa disposition une procédure concernant une demande particulière d'un Tiers, l'ADMINISTRATEUR doit systématiquement se référer à son responsable hiérarchique et au RSSI pour une prise de décision.

CHU DIJON			V 1.0
	Charte d'Utilisation du SIC pour les Administrateurs & Titulaires de profil à privilèges	Date Application TBA	Page 10 sur 11

4. Respect de la charte

Le non-respect ou la violation des règles et obligations de la présente Charte engage la responsabilité de l'ADMINISTRATEUR et constituera une faute susceptible de sanctions disciplinaires, telles que décrites par le processus défini dans le Règlement Intérieur et dans la Charte d'Utilisation du Système d'Information et de Communication.

Par ailleurs, le CHU de Dijon Bourgogne pourra être amené à communiquer aux autorités compétentes les actes délictueux commis par les ADMINISTRATEURS (par exemple : une activité illicite sur Internet). De même, dans le cadre d'une procédure judiciaire, les autorités compétentes peuvent être amenées à prendre connaissance notamment des fichiers de journalisation. En outre la responsabilité personnelle de l'ADMINISTRATEUR pourra être recherchée dans le cas :

- De dommages causés à un tiers ou au CHU de Dijon Bourgogne ;
- D'infractions pénales commises au sein du CHU de Dijon Bourgogne ou au moyen des ressources mises à sa disposition.

De plus, lorsque l'ADMINISTRATEUR en cause est un intervenant externe ou tout agent d'un prestataire ou d'un sous-traitant, le non-respect de la Charte par l'ADMINISTRATEUR fait l'objet d'une expulsion de ce dernier des locaux et du retrait immédiat de ses droits d'accès. La Direction des Achats est également informée.

Des sanctions à l'encontre des commettants, lorsqu'elles sont prévues par le contrat passé entre le CHU de Dijon Bourgogne et ce commettant, peuvent être mise en œuvre à la discrétion du CHU de Dijon Bourgogne.

CHU DIJON			V 1.1
	Charte d'Utilisation du SIC pour les Administrateurs & Titulaires de profil à privilèges	Date Application 06/03/2017	Page 11 sur 11

Annexe : Formulaire d'engagement de l'ADMINISTRATEUR

Le non-respect ou la violation des règles et obligations de la présente Charte engage la responsabilité de l'ADMINISTRATEUR et constituera une faute susceptible de sanctions disciplinaires, telles que décrites par le processus défini dans le Règlement Intérieur et dans la Charte d'Utilisation du Système d'Information et de Communication.

Par ailleurs, le CHU de Dijon Bourgogne pourra être amené à communiquer aux autorités compétentes les actes délictueux commis par les ADMINISTRATEURS (par exemple : une activité illicite sur Internet). De même, dans le cadre d'une procédure judiciaire, les autorités compétentes peuvent être amenées à prendre connaissance notamment des fichiers de journalisation. En outre la responsabilité personnelle de l'ADMINISTRATEUR pourra être recherchée dans le cas :

- De dommages causés à un tiers ou au CHU de Dijon Bourgogne ;
- D'infractions pénales commises au sein du CHU de Dijon Bourgogne ou au moyen des ressources mises à sa disposition.

De plus, lorsque l'ADMINISTRATEUR en cause est un intervenant externe ou tout agent d'un prestataire ou d'un sous-traitant, le non-respect de la Charte par l'ADMINISTRATEUR fait l'objet d'une expulsion de ce dernier des locaux et du retrait immédiat de ses droits d'accès. La Direction des Achats est également informée.

Des sanctions à l'encontre des commettants, lorsqu'elles sont prévues par le contrat passé entre le CHU de Dijon Bourgogne et ce commettant, peuvent être mise en œuvre à la discrétion du CHU de Dijon Bourgogne.

Nom et Prénom :

Direction ou pôle :

Fonction :

Déclare avoir pris connaissance et approuver les dispositions de la présente charte énoncées sur les pages précédentes et m'engage à les respecter. Dans le cas contraire, je ne pourrais pas m'opposer à l'application des sanctions prévues au règlement intérieur du CHU.

Le : / /

Signature