

Charte Informatique Utilisateurs à hauts privilèges

Date	Version	Auteur	Modification
27/10/2017	0.1	Advens	Création du fichier
09/11/2017	0.2	Talan	Modification / Ajout
16/01/2018	0.3	RSSI	Modification / Ajout suite remarques des IRP
05/02/2018	1.1	RSSI	Modifications
12/04/2018	1.2	RSSI	Modifications
17/05/2018	2.0	Comité validation documentation SMSI	Validé
07/01/2021	3.0	RSSI	Modification / Ajout suite remarques contraintes dev. Talan Labs et Opérations (§ 3.3 Exceptions particulières)

Document	SMSI_CHA_Charte utilisateurs à hauts privilèges_v3.0.pptx			
Classification	Non Confidentiel	Interne	Confidentiel	Secret
Propriétaire	Identité Pascal SCHMITT		Entité TALAN	Fonction RSSI
Diffusion	Date de diffusion 17/05/2018	Identité Patricia NICOLIN	Entité TALAN	Fonction Chef de Projet ISO
		Philippe DECONINCK	TALAN	DSI
		Martial JOURNIAUX	TALAN	RI
		Frédéric LECAN	TALAN	DAF
		Hugo CATHERINE	TALAN	DRH
		Laureline Taquet	TALAN	Juridique
		Ridha DEBBADI	TALAN Opération	Resp Secteur Telecom
		Meriem RIAHI	TALAN	Responsable Applicatif

TABLE DES MATIERES

1	Introduction	5
2	La fonction d'utilisateur à hauts privilèges	5
2.1	Définition et rôle	5
2.2	Les périmètres d'intervention	6
2.3	Les risques associés à ces droits d'accès privilégiés	6
3	Les droits et obligations de l'utilisateur à hauts privilèges	7
3.1	Ses droits	7
3.2	Ses obligations	8

3.3	Exceptions particulières	8
4	Bonnes pratiques de développement informatique.....	9
5	A retenir.....	10
6	Engagement et acceptation.....	11

1 INTRODUCTION

La présente charte, associée au règlement intérieur de Talan et à la charte d'usage des ressources informatiques et de télécommunication applicable à tout collaborateur, est avant tout un code de bonne conduite.

Elle est applicable à tous les utilisateurs du système d'information du Groupe Talan disposant de droits à hauts privilèges et a pour objectif de préciser leurs responsabilités en accord avec la Politique Générale de la Sécurité de l'information.

Elle vise à garantir un usage correct des ressources informatiques et assurer une meilleure sécurité durant le travail quotidien de ces utilisateurs.

Pour de plus amples informations ou questions, la Politique Générale et les Politiques Spécifiques de la Sécurité de l'information restent le document de référence de la sécurité au sein de Talan.

2 LA FONCTION D'UTILISATEUR A HAUTS PRIVILEGES

2.1 Définition et rôle

L'utilisateur à hauts privilèges a pour responsabilité de gérer techniquement, d'exploiter, de configurer, de maintenir et de sécuriser les ressources informatiques dont il a la charge. Sa mission consiste à assurer le fonctionnement optimal de ces ressources, qui doivent à tout moment pouvoir rendre les services pour lesquels elles ont été conçues, avec la qualité, la disponibilité et la performance requise.

Afin de conduire les actions quotidiennes d'administration, d'exploitation informatiques et de développement afférentes à sa mission (configuration, supervision, maintenance, évolution, support, etc.), l'utilisateur à hauts privilèges est doté de droits d'accès privilégiés aux ressources des systèmes d'information sous sa responsabilité.

2.2 Les périmètres d'intervention

Au sein de Talan, le rôle de l'utilisateur à hauts privilèges peut se décliner sous différents périmètres d'intervention, selon la ressource gérée :

- Administrateur (réseau, système, de messagerie, de base de données, bureautique, etc.),
- Développeur.

Cette charte s'applique quelle que soit l'étendue des droits à hauts privilèges conférés, qu'il s'agisse :

- D'utilisateurs internes tels que les administrateurs des réseaux et des systèmes d'information, de développeurs,
- De toute autre personne qui dispose d'un droit étendu sur un poste ou un serveur interne ou externe à Talan.

2.3 Les risques associés à ces droits d'accès privilégiés

L'utilisateur à hauts privilèges a un rôle de confiance. Sa démarche doit être impartiale et son action ne doit pas découler d'une action personnelle. Il convient de fixer les règles déontologiques qu'il s'engage à respecter.

Données confidentielles et données à caractère personnel

L'un des risques associés aux droits d'un utilisateur à hauts privilèges est l'accès à des informations dont il ne serait pas destinataire : comme notamment certaines données confidentielles (documents métiers, stratégiques) ou à caractère personnel, ou encore relatives aux activités des utilisateurs (les données d'utilisation de la messagerie et de l'intranet, les données de connexion aux ressources des systèmes d'information, etc.).

De plus, l'utilisateur à hauts privilèges ne peut aller consulter les informations qui auraient été catégorisées comme étant « personnelles » et/ou « privées », celles-ci ayant un caractère personnel pour l'utilisateur, la consultation de ces dernières irait à l'encontre du respect de la vie privée des personnes.

Réalisation d'actions dangereuses

La réalisation de ses actions peut devenir dangereuse et impacter la disponibilité, l'intégrité ou plus généralement la sécurité des systèmes d'information : modification ou contournement de mécanismes de protection, modification des comptes utilisateurs, destruction ou modification de fichiers, etc.

Gestion des mots de passe

L'utilisateur à hauts privilèges doit s'assurer de garder ses mots de passe confidentiels, et en assurer le renouvellement de manière régulière en accord avec la politique gestion de mot de passe du Groupe, pour ne pas risquer une usurpation de droits, qui pourrait entraîner de malveillances ou fraudes.

3 LES DROITS ET OBLIGATIONS DE L'UTILISATEUR A HAUTS PRIVILEGES

Pour mener à bien sa mission, l'utilisateur à hauts privilèges dispose de droits d'accès étendus sur les ressources des systèmes d'information.

Il est autorisé à prendre toutes les dispositions nécessaires au maintien de la sécurité et du fonctionnement des ressources dans son périmètre de responsabilité.

3.1 Ses droits

- ☑ Surveiller la bonne utilisation des ressources dans son domaine de responsabilité, notamment en ce qui concerne les volumes d'informations transmis et reçus, la gestion des espaces de stockage et la capacité des équipements,
- ☑ Traiter (détection, analyse, éradication, filtrage, etc.) tout flux informatique présentant des risques de sécurité (virus, intrusion, utilisation d'un logiciel interdit, etc.),
- ☑ Isoler ou arrêter des comptes utilisateurs, équipements, ressources ou systèmes informatiques, en cas de menace importante, ou sur demande explicite d'un supérieur hiérarchique, pouvant compromettre la sécurité de l'ensemble des systèmes d'information.

3.2 Ses obligations

L'utilisateur à hauts privilèges est soumis à plusieurs obligations relatives au secret professionnel et à la préservation des informations confidentielles auxquelles il a accès :

- ☑ N'accéder ou ne donner accès aux informations des SI qu'après autorisation explicite de la part de leur(s) propriétaire(s) et dans le strict respect des procédures formalisées ou dans les cas particuliers prévu par la loi,
- ☑ Respecter ses engagements de confidentialité. Ainsi, il ne divulgue aucune information dont il a pris connaissance dans le cadre de ses fonctions, en particulier lorsque celles-ci sont couvertes par le secret des correspondances ou relèvent de la vie privée des utilisateurs, et ne remettent en cause ni le bon fonctionnement des ressources des SI, ni leur sécurité ;
- ☑ Avoir un devoir d'information, de conseil et de mise en garde vis-à-vis des utilisateurs ;
- ☑ Informer immédiatement le RSSI de toute tentative d'intrusion sur un système, ou de tout comportement d'utilisateur pouvant compromettre la sécurité du système d'information ;
- ☑ Informer, dans la mesure du possible, les utilisateurs de toute intervention nécessaire, susceptible de perturber ou d'interrompre l'utilisation habituelle des moyens informatiques

3.3 Exceptions particulières

Il peut être autorisé qu'une certaine catégorie de développeurs des entités du groupe : Talan Labs et de Talan Opérations, puissent devenir administrateurs de leur poste et obtenir l'accès au mot de passe Bios de leur machine sur demande et validation managériale uniquement.

Dans ce cadre et uniquement dans celui-ci :

- ☑ Les demandes de droits d'administration et d'accès au mot de passe BIOS doivent être validées par le Directeur Talan Labs ou Opérations ainsi que le DSI et le RSSI du groupe
- ☑ Le mot de passe du BIOS ne doit pas être modifié par l'utilisateur (à des fins de réutilisation du matériel informatique par exemple)
- ☑ Les développeurs ne doivent en aucun cas connecter leur machine au réseau interne Talan (que ce soit au siège du groupe Talan, dans une agence, à l'international, par le biais d'une liaison VPN, ...)
- ☑ Les développeurs ne doivent en aucun cas connecter leur machine aux réseaux des clients ou sous-traitant de Talan
- ☑ Les développeurs ne doivent pas stocker de données confidentielles sur leur poste
- ☑ Les développeurs doivent impérativement disposer d'un disque dur machine chiffré selon les standards de cryptographie en vigueur au sein du groupe Talan (AES 256), Les informations confidentielles ou à caractère personnel doivent obligatoirement être stockées sur cet espace de stockage chiffré.
- ☑ Les développeurs bénéficiant de l'une de ces exceptions ne pourront pas faire appel au support IT Talan en cas d'incident sur leur machine concernée par ces hauts privilèges spécifiques
- ☑ Les développeurs bénéficiant de l'une de ces exceptions ne pourront pas installer d'applications prohibées par le groupe (« Black List » maintenue par la DSI en accord avec la sécurité du groupe)

- ☑ Avant de pouvoir récupérer disposer de leur machine, les développeurs ayant émis le souhait de bénéficier d'au moins l'une de ces exceptions, devront lire, accepter et signer la charte des utilisateurs à haut privilège, acceptant de se conformer notamment aux différents points cités ci-avant.

4 BONNES PRATIQUES DE DEVELOPPEMENT INFORMATIQUE

Comme évoqué précédemment, les développeurs, au même titre que les administrateurs, peuvent parfois disposer de pouvoirs et de droits d'accès privilégiés du fait de leur activité. Ainsi ils se doivent de respecter ou de faire respecter les règles suivantes, composant un recueil de bonnes pratiques de développement permettant d'assurer un niveau de sécurité initial commun :

- ☑ Ne pas utiliser de code (ou des parties de code) provenant de sources inconnues et non vérifiées. Par exemple, ne pas recopier du code pris sur des forums internet ou sur des sites Web. Le code provenant de sources connues et vérifiées n'est pour autant exempt de vulnérabilités. Il convient de tester également ce code lors de l'étape de revue de code afin de minimiser les risques encourus.
- ☑ Ne pas utiliser de code sous copyright. Utiliser du code sous copyright pris sur Internet ou sur d'autres applications est strictement interdit. Si du code Open-Source est utilisé, il faut être vigilant aux restrictions liées au licensing.
- ☑ Être vigilant lorsque le code est rendu public. Il se peut que cela soit nécessaire (contribution à des codes open-source par exemple). Lorsque cela arrive, il faut d'abord obtenir une validation du responsable.
- ☑ Supprimer tous les commentaires sensibles du code avant déploiement. Les commentaires sont très utiles pour les développeurs mais il est nécessaire de les supprimer avant le déploiement de l'application car ils peuvent contenir des informations potentiellement utiles pour les hackers (faille à corriger, mots de passe ou clés d'authentification par exemple).
- ☑ Être formé aux standards et pratiques de développement sécurisé. Les responsables des développeurs concernés, se devront d'intégrer aux parcours de formation de ceux-ci, des formations sécurité adaptées et qui répondent à l'utilisation de bonnes pratiques et de standards de développement sécurisé. Ces formations doivent être complétées par des mises à niveau régulières sur les nouvelles techniques et vulnérabilités existantes, ainsi qu'une veille régulière sur les problèmes de sécurité inhérents à des développements.
- ☑ L'OWASP (Open Web Application Security Project) fournit le Top 10 des plus grandes failles de sécurité identifiées et fournit donc un référentiel aux développeurs de bonnes pratiques de sécurité pour éviter ces failles de sécurité.

5 A RETENIR

Mission

L'utilisateur à hauts privilèges est doté de droits d'accès privilégiés aux ressources des systèmes d'information sous sa responsabilité, et doit en assurer le fonctionnement optimal.

Périmètre d'intervention

Au sein de Talan, le rôle d'utilisateur à hauts privilèges concerne les administrateurs (réseau, système, de messagerie, de base de données, bureautique, etc.), mais aussi les développeurs. Cette charte s'applique à tous les utilisateurs disposants de hauts privilèges qu'ils soient internes ou externes à Talan.

Risques associés

L'utilisateur à hauts privilèges doit agir dans une démarche impartiale, il devra ainsi respecter les informations auxquelles il pourrait avoir accès, notamment celles à caractère personnel. Il devra également s'assurer de ne pas réaliser d'actions potentiellement dangereuses, et s'assurer de la non divulgation de ses mots de passe et du renouvellement régulier de ces derniers.

Droits et devoirs

Dans le cadre de ses fonctions, l'utilisateur à hauts privilèges dispose d'un certain nombre de droits et devoirs, notamment : d'assurer le bon fonctionnement général du système d'Information, de faire respecter les consignes de sécurité, et de procéder à toutes vérifications ou traitements lui permettant d'assurer au mieux ses fonctions.

Par ailleurs, il est tenu au secret professionnel, il ne peut donc ainsi pas divulguer d'informations confidentielles.

Standards et bonnes pratiques de développement


Les développeurs, pouvant également être dotés de droits à hauts privilèges dans le cadre de leur activité, se doivent de respecter l'ensemble des règles énoncées liées à cette fonction, mais doivent également s'assurer du niveau de sécurité dans le cadre de leur développement.

6 ENGAGEMENT ET ACCEPTATION

Le collaborateur par sa signature du document reconnaît avoir lu et déclare avoir compris la présente charte et les règles déontologiques et de sécurité auxquelles il est également soumis. Il confirme être en accord avec toutes les dispositions du présent document, et s'engage à respecter toutes les règles y figurant.

Il s'engage également à fournir à la demande des ressources humaines, du RSSI ou toute autre personne ayant légitimité, son extrait de casier judiciaire, bulletin n°3. Une demande de ce type ne pourra être motivée que dans le cadre du respect d'une obligation réglementaire, juridique, légale ou à des fins de sécurité (Ex. : demande d'habilitation confidentielle ou secret défense.) et ne pourra en aucun cas avoir d'autres finalités. De fait, le collaborateur dispose du droit de ne pas fournir ce document au demandeur, conformément au droit du travail et au respect à sa vie privée. Un refus de sa part ne pourrait donc constituer un motif de sanction à son encontre. Par ailleurs, ce document ne saurait être conservé au-delà de la période légale de rétention autorisée par la Loi.

Dans l'hypothèse où la charte mise à jour serait portée à la connaissance du collaborateur par voie électronique, l'acceptation de la charte modifiée sera réalisée en ligne par chaque utilisateur à hauts privilèges dûment identifié au moyen de son identifiant et de son mot de passe et selon la procédure de double clic ayant la même valeur qu'une signature manuscrite.

Je soussigné(e), agissant en ma qualité d'utilisateur à hauts privilèges au sein de Talan, reconnais avoir été informé(e) des règles et m'engage à les respecter.

-- Fin du document --