Charte d'administration des systèmes d'information

Annexe du règlement intérieur
Unité Economique et Social LEROY MERLIN FRANCE

Version du 20 juillet 2018

PREAMBULE

Pour servir nos ambitions, nous agissons en nous appuyant sur un socle commun, des valeurs de confiance et d'autonomie permettant à chaque collaborateur d'être acteur dans un monde qui change, d'être ouvert, connecté, utile et de se réaliser.

Pour y parvenir, ensemble, nous innovons, testons, expérimentons, interagissons avec nos communautés, ce qui implique plus de technologie, plus d'échanges et de partage de données. En résumé, à la fois plus de numérique et d'humain.

Dans le même temps, les réglementations nationales et européennes évoluent vers un renforcement de la protection des systèmes d'information et particulièrement des données à caractère personnel des clients-habitants comme des collaborateurs.

Dans ce contexte, la sécurité des systèmes d'information est essentielle au soutien de nos ambitions. C'est un facteur de confiance pour :

- Les clients-habitants, collaborateurs, partenaires, acteurs de notre écosystème ;
- L'image de marque de notre Entreprise, et sa capacité à répondre aux projets de ses clients-habitants ;
- Et, au final, l'Entreprise elle-même.

En tant qu'administrateur des systèmes d'information, je suis particulièrement concerné par la sécurité des systèmes d'information et j'y contribue au quotidien.

Le présent document a pour objet de me faire connaître et comprendre les principales règles d'administration des systèmes d'information de l'Entreprise.

Il me permet, en tant que collaborateur-administrateur des systèmes d'information, de contribuer à la réalisation de nos ambitions en adoptant un comportement responsable et des pratiques respectueuses de la sécurité des systèmes d'information.

Un système d'information est un ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information.

Une ressource peut désigner un matériel (ordinateur, imprimante, serveur, équipement réseau, périphérique…), un logiciel (système d'exploitation, logiciel bureautique…), une application (Pyxis, Saveo…), un service interne (messagerie électronique, Younity, partage de fichiers, accès Internet…), un service externe (offre d'hébergement, service Cloud…) ou tout simplement une information (sous forme unitaire ou de base de données).

La sécurité des systèmes d'information est l'ensemble des moyens et mesures techniques, organisationnels, juridiques et humains visant à prévenir, détecter ou réagir à un impact sur une ressource d'un système d'information concernant :

- sa disponibilité, c'est-à-dire son usage aux moments choisis
- son intégrité, c'est-à-dire sa capacité à rester exacte, complète et fiable
- sa confidentialité, c'est-à-dire son accès qu'aux personnes, entités ou Ressources autorisées
- sa traçabilité, c'est-à-dire sa capacité à prouver l'origine et la date de toute action réalisée

CHAMP D'APPLICATION

Ce document, associé au règlement intérieur des différents sites, s'applique aux entreprises de l'unité économique et sociale Leroy Merlin (UES Leroy Merlin, ci-après l'Entreprise) ainsi qu'aux administrateurs de ses systèmes d'information.

> On appelle ici Administrateur, toute personne physique ayant des accès de modifications sur les mécanismes de fonctionnement technique, applicatif ou de sécurité d'un matériel, logiciel, application, ou service des Systèmes d'Information de l'Entreprise. Il peut donc s'agir de développeurs, responsables applicatifs, administrateurs réseaux, systèmes, base de données, web, sécurité, administrateurs fonctionnels métiers…

1- Je suis intègre et loyal

En tant qu'administrateur des systèmes d'information de l'Entreprise, je limite mes actions aux seules ressources sous ma responsabilité, dans le respect de la finalité de ma mission, et sans jamais abuser de mes privilèges. En particulier, je ne cherche pas à obtenir des informations sensibles, à modifier les configurations et les droits d'accès, en dehors des besoins liés à ma mission. Je ne contourne pas les procédures ou mécanismes de sécurité établis. Je recueillie l'accord préalable d'un Utilisateur avant toute prise en main à distance sur son équipement professionnel.

> Le terme « utilisateur » représente ici toute personne physique :
>
> - travaillant au service de l'Entreprise, quel que soit son statut ou son contrat : dirigeant, salarié à temps plein ou temps partiel, personnel intérimaire, stagiaire…
> - ayant accès aux Systèmes d'Information de l'Entreprise, à tout ou partie de ses données, et par tout type d'équipement (clé USB, ordinateurs, serveurs…).

Cette prise en main ne doit être menée que dans les cas où le bon fonctionnement ou la sécurité des systèmes d'information ne pourraient être assurés par d'autres moyens moins intrusifs. Enfin, je m'interdis d'accéder sans l'autorisation de l'utilisateur à l'un de ses équipements personnels.

Je ne prends jamais connaissance des données personnelles d'un utilisateur, sauf sur sa demande formelle, et n'autorise quiconque à y accéder, sauf cas particuliers prévus par la loi ou habilitations formelles et légitimes préalablement déclarées.

Je ne divulgue jamais les informations auxquelles j'aurais pu avoir accès lors de l'exercice de mes fonctions, à moins qu'une disposition législative ne l'impose ou qu'elles mettent en cause la charte « Confiance et transparence dans l'usage des systèmes d'information », le règlement intérieur, le bon fonctionnement des systèmes d'information, leur sécurité ou les intérêts de l'Entreprise.

Je m'interdis d'utiliser les informations en ma possession à des fins personnelles ou illégales. Si je suis incité ou si je fais l'objet de pressions visant à enfreindre la loi, je n'accède pas à la demande et remonte auprès de mon responsable (ou du service juridique) toute requête me paraissant inappropriée.

2- Je protège les identifiants et authentifiants des ressources sous ma responsabilité

Je respecte les règles de création et de renouvellement des mots de passe concernant mes comptes d'administration ou les comptes des ressources sous ma responsabilité. Ces mots de passe doivent être strictement différents (d'autant plus vis-à-vis de mon compte utilisateur).

> 13 caractères minimum, des minuscules, majuscules, chiffres, et caractères spéciaux. Pas de prénom, année de naissance, ou mot du dictionnaire. A renouveler chaque année.

Je ne prête jamais mon compte d'administration ni ne communique le mot de passe associé. Ce compte est personnel et confidentiel. Je garde secret les mots de passe des ressources sous ma responsabilité en dehors des personnes strictement habilitées.

Je change sans délai les authentifiants par défaut (comme les mots de passe) sur les équipements (routeurs, imprimantes…) ou comptes de services (bases de données…) dont j'ai la charge. Ces authentifiants devront présenter des garanties de sécurité notamment en respectant des règles de création et de renouvellement.

J'utilise la solution de coffre-fort électronique mis à disposition par l'Entreprise pour stocker les mots de passe des ressources sous ma responsabilité. En cas de coffre-fort électronique partagé (au sein d'une équipe, d'un projet…), je veille à changer le mot de passe du coffre-fort électronique à chaque départ ou mobilité d'une personne préalablement habilitée.

3- J'assure la sécurité des ressources sous ma responsabilité

Je mets en œuvre l'ensemble des bonnes pratiques, politiques, procédures opérationnelles et standards techniques de sécurité sur les ressources sous ma responsabilité (politique de gestion des mises à jour, politique de gestion des mots de passe…).

Je m'interdis de dégrader la sécurité des ressources sous ma responsabilité ou de générer de nouvelles dettes de sécurité.

> Par exemple, je ne désactive pas l'antivirus, je n'empêche pas l'installation de mises à jour de sécurité, je ne configure pas un mot de passe faible…

Je m'assure qu'aucune donnée sensible ou à caractère personnel ne soit copiée d'un environnement de production, vers des environnements de moindre sécurité (développement, recette…).

Je prends toute disposition nécessaire pour assurer le bon fonctionnement et la sécurité des ressources sous ma responsabilité mais aussi des équipements que j'utilise pour réaliser ma mission (comme mon poste de travail).

Je chiffre l'ensemble des périphériques de stockage que j'utilise pour mes tâches d'administration (disques durs, clés USB…)

4- Je respecte les bonnes pratiques d'administration

Je réalise toutes mes actions d'administration via mon compte nominatif dédié à ces usages (compte d'administration ADM) et dans le cadre strict de ma mission.

Je n'utilise jamais des comptes non-nominatifs (comptes ROOT, SA…) en dehors de bastions d'administration. Toute action d'administration doit pouvoir être identifiée nominativement.

> Bastion d'administration : Passerelle d'accès obligatoire pour les actions d'administration de ressources. Ce composant permet d'assurer l'authentification nominative des administrateurs SI, des accès adaptés à leurs fonctions et la traçabilité des actions réalisées.

J'utilise uniquement des protocoles et des outils d'administration sécurisés comportant des mécanismes de chiffrement et, si possible, une authentification forte.

> Authentification forte : Procédure d'authentification qui requiert l'usage d'au moins deux authentifiants de nature différente. Par exemple : un mot de passe combiné à un code reçu par SMS.

Lors de tout changement ou correctif, je respecte le processus de gestion des changements de l'Entreprise. Notamment, je m'assure de tester préalablement la modification avant mise en production ou généralisation.

Je m'assure, avant de donner l'accès à une personne sur une ressource, que la demande a été formellement validée par le responsable du demandeur (ou commanditaire de la prestation) ainsi que par le propriétaire métier de la ressource concernée.

Je revois régulièrement les droits des utilisateurs et administrateurs affectés aux ressources sous ma responsabilité.

5- Je supervise les ressources sous ma responsabilité

J'active la traçabilité des ressources (systèmes d'exploitation, services applicatifs…) sous ma responsabilité. Je m'assure également de la transmission de ces traces vers l'infrastructure de centralisation/corrélation d'évènements de l'Entreprise. Je m'interdis de désactiver, supprimer ou altérer des traces.

Je m'assure de la mise en place d'une supervision régulière de bon fonctionnement et de sécurité des ressources sous ma responsabilité, avec contrôles de masse et non nominatifs. Si aucune anomalie n'attire mon attention, les contrôles s'arrêtent à ce stade. Si, à l'occasion des contrôles, mon attention est attirée par une anomalie, un comportement inhabituel ou inapproprié ou un dysfonctionnement, j'effectue des vérifications complémentaires manuelles susceptibles de contenir des traces nominatives. En cas de menace avérée, j'isole toute donnée ou ressource qui mettrait en péril le bon fonctionnement ou la sécurité des systèmes d'information.

6- Je gère les alertes et incidents de sécurité

J'informe le département sécurité des systèmes d'information de toute faille, comportement anormal, alerte ou incident de sécurité que je découvre ou dont j'ai connaissance.

Je mets tout en œuvre pour permettre la résolution rapide d'un incident (par exemple : isoler ou arrêter des comptes utilisateurs, équipements, flux ou fichiers pouvant compromettre la sécurité d'ensemble des systèmes d'information).

Je préserve, conserve et sauvegarde les traces nécessaires à la résolution d'un incident et à toute investigation ultérieure, y compris judiciaire, dans des conditions permettant de garantir leur intégrité. En cas de doute, je contacte le département sécurité SI.

7- Je m'assure du respect du secret des correspondances

Dans le cadre de la gestion des incidents, je peux être amené à voir des messages identifiés comme « personnel » ou « privé » ou classés dans un dossier intitulé « personnel » ou « privé » sur la messagerie professionnelle des utilisateurs. Dans cette hypothèse, je suis tenu à une obligation de confidentialité m'imposant de ne pas divulguer le contenu des correspondances qui auraient ainsi été portées à ma connaissance à mon employeur ou à un tiers en dehors de tout risque ou évènement particulier.

8- J'accède aux salles informatiques

Je m'interdis de prêter mon badge nominatif d'accès aux salles informatiques, Il m'est strictement personnel.

En cas d'usage de badge non-nominatif ou de clés, j'assure leur sécurité par le stockage au coffre. Je vérifie l'identité et la légitimité d'une personne avant de lui prêter un badge non-nominatif ou une clé. Je complète enfin une feuille d'émargement pour assurer la traçabilité des accès. Je m'assure que la personne ayant bénéficié de ce prêt a bien rendu les clés ou badges non-nominatifs après utilisation.

Je ne laisse jamais la porte d'une salle informatique ouverte ou déverrouillée.

Je déclare immédiatement la perte d'un badge ou d'une clé, d'autant plus si il/elle permet l'accès à une salle informatique. Le badge sera alors désactivé ou la serrure changée.

9- Que se passe-t-il si je ne respecte pas ce document ?

Les règles contenues dans ce document sont essentielles au bon fonctionnement et à la sécurité des systèmes d'information de l'Entreprise.

Leur non-respect engage ma responsabilité personnelle et peut entraîner des sanctions de natures différentes, qui ne sont pas exclusives les unes des autres :

- Sanctions disciplinaires définies par le règlement intérieur du site de rattachement,
- Poursuites civiles et/ou pénales engagées à la demande de l'Entreprise en cas de manquement grave et avéré aux lois en vigueur.

ADOPTION ET PUBLICITE DU PRESENT DOCUMENT

Ce document a été adopté après information et consultation des instances représentatives du personnel de l'UES Leroy Merlin. Il est applicable à compter du **30 septembre 2018.**

La présente charte est portée à la connaissance de chaque administrateur des systèmes d'information par toute vois jugée nécessaire par l'entreprise et sous toute forme de communication utile, conformément au code du travail.

Ce document est publié sur le site intranet de l'Entreprise. Des actions de sensibilisation et de communication sont organisées régulièrement afin de rappeler les règles décrites ici. En cas de questions sur certaines parties du document, je peux contacter à tout moment mon manager ou mon département RH.