

Charte informatique des administrateurs à hauts privilèges

TOYOTA MOTOR MANUFACTURING FRANCE — Réf. TMMF-IS-CHARTE-ADMIN-001 — v2.0

PREAMBULE

La présente charte a pour objet de définir les principales prérogatives, les engagements et la responsabilité des administrateurs à hauts privilèges, quel que soit leur statut et leur position géographique (Cas du travail à distance)

Dans le cadre de l'exercice de leurs missions, les administrateurs sont susceptibles d'accéder à des informations ou données d'autres utilisateurs. Ces informations pouvant revêtir un caractère confidentiel, les administrateurs sont tenus à une obligation stricte de confidentialité et ne peuvent accéder à ces données que dans la mesure nécessaire à l'accomplissement de leurs fonctions.

Les administrateurs restent soumis à l'ensemble des règles et obligations prévues par la Charte informatique de TMMF. Toutefois, en raison de la nature particulière de leurs missions et de l'étendue des droits qui leur sont conférés, ils sont également tenus de respecter les dispositions spécifiques énoncées dans la présente charte.

Ainsi, cette charte complète les dispositions de la Charte informatique de TMMF. En cas de contradiction entre la charte des systèmes d'information et la charte administrateur, les dispositions de la charte administrateur priment.

Au sens de cette charte est considéré comme administrateur toute personne disposant de droits lui permettant d'installer, configurer, maintenir, superviser ou administrer une application, un équipement ou tout ou partie des systèmes d'information de TMMF.

Les administrateurs peuvent être des Toyota Members de TMMF ou des salariés d'entreprise extérieures dûment habilités à intervenir. Dans ce dernier cas, l'entreprise extérieure doit faire valider la présente charte par le ou les salariés concernés.

1. Les droits des administrateurs

Dans le cadre des missions qui lui sont confiées et en raison des privilèges dont il dispose, l'administrateur est autorisé à exercer les actions suivantes :

- Créer, modifier, suspendre et supprimer des comptes et profils utilisateurs, conformément aux règles de gestion des droits d'accès définies par TMMF, afin d'assurer une gestion sécurisée des accès aux systèmes d'information ;
- Superviser, analyser et contrôler régulièrement les journaux d'évènement (les logs) des systèmes, applications et équipements informatiques dans le but de détecter les anomalies (activité suspecte, dysfonctionnement ou tentative d'intrusion), et de mettre en œuvre les mesures correctives nécessaires ;
- Assurer l'assistance et le support technique auprès des utilisateurs, afin de résoudre les problèmes rencontrés sur les systèmes informatiques ;
- Installer, déployer, configurer, mettre à jour et maintenir les outils, logiciels, applications et équipements nécessaires au bon fonctionnement des systèmes d'information, que ce soit individuellement ou au moyen d'outils d'administration centralisée ;

- Mettre en œuvre des mesures conservatoires, correctives ou d'urgence nécessaire à la protection des systèmes d'information en cas d'incident de sécurité, de cyberattaque ou de comportement susceptible de compromettre l'intégrité, la confidentialité ou la disponibilité des ressources informatiques ;
- Filtrer, surveiller, vérifier et contrôler, dans le respect des dispositions légales et des politiques internes applicables, l'utilisation des ressources informatiques mises à disposition des utilisateurs, notamment afin de prévenir les usages non conformes ou présentant un risque pour la sécurité des systèmes d'information ;
- Conformément aux règles de gouvernance, protéger, isoler, arrêter ou reconfigurer les comptes utilisateurs, les matériels ou les applications informatiques qui pourraient compromettre la sécurité des systèmes d'information, ou qui seraient susceptibles de porter atteinte à l'intégrité et à la disponibilité des services informatiques ;
- Assurer un support technique aux utilisateurs, leur fournissant l'assistance nécessaire pour résoudre les problèmes rencontrés sur les systèmes informatiques, et contribuant à la formation continue des utilisateurs ;
- Participer à la mise en œuvre des mesures de protection des systèmes d'information, y compris par l'installation régulière de patches de sécurité et la mise à jour des versions des logiciels utilisés chez TMMF ;
- Gérer les incidents de sécurité informatique. En cas d'attaque, se référer à « La procédure d'escalade », en alertant les parties prenantes concernées, en mettant en œuvre des actions correctives immédiates, et en documentant l'incident pour analyse post-mortem ;
- Gérer les accès privilégiés (comptes « super-utilisateur » ou « root »), en s'assurant qu'ils sont attribués et utilisés uniquement selon les nécessités professionnelles, et qu'une traçabilité complète des actions est effectuée ;
- Veiller à ce que des sauvegardes régulières des données et des systèmes critiques soient effectuées et testées ainsi qu'à la mise en œuvre des opérations de restauration en cas de perte de données ou de panne majeure, en suivant les procédures établies ;
- Documenter et maintenir à jour toutes les informations nécessaires au bon fonctionnement des outils, logiciels et / ou matériel informatique ;
- Contrôler la performance des systèmes d'information afin de détecter toute dégradation ou anomalie susceptible de nuire au bon fonctionnement des services informatiques ;
- Autoriser, modifier, restreindre ou supprimer les accès au réseau de l'entreprise, qu'il soit filaire ou autre (Wi-Fi par exemple) ;
- Participer à la mise en œuvre, aux tests et à la mise à jour régulière du plan de continuité d'activité (PCA) et du plan de reprise ;
- Sensibiliser les utilisateurs aux bonnes pratiques en matière de sécurité informatique ;

2. Les devoirs des administrateurs

Compte tenu des privilèges qui lui sont accordés et des responsabilités qui lui incombent, l'administrateur s'engage à respecter les règles suivantes :

- Utiliser exclusivement les outils, logiciels et équipements validés par TMMF ou, à défaut, obtenir une autorisation préalable avant toute mise en œuvre d'une solution non référencée, conformément aux standards et politiques de l'entreprise ;
- Ne pas installer ou utiliser sur les matériels informatiques un logiciel, progiciel ou application sans qu'une licence d'utilisation appropriée n'ait été préalablement souscrite ;
- Respecter les droits de propriété intellectuelle et s'interdire tout développement, d'outils ou produits à partir d'éléments appartenant à des tiers en violation des droits qui leur sont attachés, ce qui constitue une contrefaçon engageant la responsabilité des administrateurs ;
- Préserver strictement la confidentialité en s'interdisant de communiquer à quiconque des codes d'accès ;
- Ne pas demander les codes d'accès des utilisateurs sauf circonstance exceptionnelle, par exemple dans le cadre d'un dépannage effectué en présence de la personne concernée ;
- Veiller à la protection et à la sécurité du poste de travail à partir duquel il exerce ses fonctions ;
- Respecter une obligation stricte de confidentialité et de discrétion professionnelle. À ce titre, il s'engage à ne divulguer à aucun tiers les informations, données, documents ou connaissances auxquels il aurait eu accès dans le cadre de ses missions, quel qu'en soit le support ou le mode de communication ;
- Appliquer rigoureusement les politiques de sécurité, procédures, normes et directives en vigueur au sein de TMMF, et contribuer à leur diffusion auprès des utilisateurs lorsque cela relève de ses attributions ;
- Informer les utilisateurs concernés des interruptions planifiées ou non planifiées des services informatiques ;
- Assurer la traçabilité des opérations réalisées et tenir à jour l'historique des incidents, interventions et actions correctives mises en œuvre ;
- Utiliser ses droits d'accès privilégiés dans la limite de ses attributions et missions, et ne modifier les configurations et droits d'accès des utilisateurs que dans le respect des procédures définies ;
- Ne mettre en œuvre aucun outil de chiffrement ou de protection sans l'accord préalable de la direction informatique ;
- Prendre les mesures appropriées en cas de risque d'attaque ou d'attaque subie et en référer immédiatement, conformément aux procédures d'escalade en vigueur ;
- Alerter la Direction informatique de tout usage anormal des systèmes d'information, qu'elle émane d'une personne interne ou externe à l'entreprise ;
- Ne pas accéder aux données identifiées comme « personnelles » ou « privées » des utilisateurs sans leur autorisation expresse. S'il est constaté un accès aux données identifiées

comme « personnelles » ou « privées » à la suite d'un incident, ne pas faire usage de ces données personnelles, sauf en cas de demande expresse du Responsable de la Sécurité des Systèmes d'Information (« CISO ») ou du Responsable du développement et de l'implémentation des politiques et procédures de sécurité des systèmes d'information (« ISO ») ;

- Ne pas porter atteinte à la vie privée des utilisateurs et au secret de leurs correspondances privées ;
- Réserver l'utilisation des outils, matériels et solutions mis à disposition dans le cadre de sa mission d'administrateur à hauts privilèges à des fins strictement professionnelles ;
- Tracer et conserver un historique de toutes les actions réalisées sur le poste de travail des utilisateurs via un compte administrateur ;
- Ne pas réaliser de tests de pénétration ou d'autres tests sur la sécurité des systèmes d'information sans l'accord préalable et écrit du Directeur des Systèmes d'Information ou de la Direction Générale de TMMF ;
- Collaborer à la réalisation d'audits de sécurité internes et externes, permettant d'évaluer la robustesse des systèmes d'information et de mettre en place des actions correctives ou préventives suite aux résultats de ces audits.

3° Evolution de la charte

Chaque personne destinataire de la présente charte est invitée à transmettre à TMMF toute proposition de modification ou d'ajout dont elle a pu constater l'intérêt dans le cadre de ses missions ou dans l'exercice de ses fonctions, lesquelles justifient l'attribution de droits étendus.

Dans le cadre de la démarche d'amélioration continue qui anime TMMF, la présente charte sera régulièrement mise à jour et portée à la connaissance de toute personne concernée sur support papier ou électronique.

4° Engagements de l'administrateur à hauts privilèges

Cases à lire et cocher avant signature :

☐ J'ai pris connaissance des règles applicables dans le cadre de cette charte de l'administrateur à hauts privilèges et m'engage à les respecter.

☐ Je m'engage à suivre les différentes formations imposées par TMMF.

☐ Je reconnais avoir été informé que tout manquement aux obligations définies dans cette charte constitue une violation de la réglementation relative à la protection des données personnelles (RGPD), ainsi qu'aux règles internes établies par TMMF notamment celles prévues au Règlement Intérieur.

Le non-respect de la présente charte engage la responsabilité de l'administrateur qui s'expose à des sanctions disciplinaires, administratives et pénales. En cas de non-respect de la charte, TMMF se réserve par ailleurs le droit de suspendre ou de supprimer tout ou partie des droits d'accès et privilèges de l'administrateur.

Nom, Prénom : _____

Matricule (si salarié TMMF) : _____

Date : _____

Parapher les pages et signature accompagnée de la mention manuscrite « Lu et approuvé, bon pour accord »
