Notre position

La sécurité de l'information

MTN est présent dans plus de 22 pays répartis sur deux continents. MTN s'appuie sur ses informations, qui sont sous diverses formes, pour fournir des services à ses clients. Par conséquent, la sécurité de l'information est essentielle à nos opérations quotidiennes et à notre succès.

Notre position sur la sécurité de l'information

L'information est un atout et doit donc être correctement protégée. La sécurité de l'information protège les biens informationnels contre un large éventail de menaces pour assurer la continuité des opérations, minimiser les dommages aux activités et maximiser le rendement des investissements.

La sécurité de l'information est régie par les objectifs de contrôle suivants :

a) La confidentialité, qui concerne la protection des informations sensibles contre les accès non autorisés.

b) L'intégrité, qui se rapporte à l'exactitude et à l'exhaustivité des informations, ainsi qu'à la validité des informations conformément aux valeurs et aux attentes de l'entreprise.

c) La disponibilité, qui se rapporte à l'information disponible au bon moment pour le processus commercial. Elle traite également de la sauvegarde des ressources nécessaires et des capacités associées.

Notre portée et notre applicabilité en matière de sécurité de l'information

La portée de la sécurité de l'information englobe toutes les installations de MTN, les fonctions du Groupe et des sociétés d'exploitation, les biens informationnels, les employés, les entrepreneurs et les tiers.

Elle s'applique aux éléments suivants :

a) Toutes les informations, y compris, mais sans s'y limiter, les informations sur les clients, les informations relatives aux employés de MTN et à l'entreprise générées, traitées et stockées par diverses unités fonctionnelles de MTN pour mener ses activités et réaliser sa prestation de services.

b) Tous les biens informationnels qui traitent les informations à MTN. Les biens informationnels peuvent inclure, sans s'y limiter, des ressources matérielles, des ressources logicielles, des actifs de services, des ressources humaines et des actifs papier.

c) Tous les employés, entrepreneurs et membres du personnel de tiers de MTN qui accèdent aux installations de traitement de l'information de MTN. Les installations de traitement de l'information de MTN comprennent, sans s'y limiter, le campus de MTN, les installations, les bureaux, les zones de travail, les zones sécurisées, les salles d'infrastructure critiques et salles de télécommunications.

Nos responsabilités en matière de sécurité de l'information

Les responsabilités en matière de sécurité de l'information sont décrites ci-dessous :

a) Tous les employés, entrepreneurs et l'ensemble du personnel de tiers doivent se conformer à la Politique de sécurité de l'information de MTN Group et aux procédures, normes et directives associées.
b) L'ensemble du personnel, des entrepreneurs et du personnel de tiers impliqués dans le stockage et le traitement des informations à MTN ont la responsabilité de signaler les informations et les incidents de sécurité liés à la cybersécurité, ainsi que toute faiblesse identifiée.
c) L'ensemble du personnel, des entrepreneurs et du personnel de tiers impliqués dans le stockage et le traitement des informations à MTN doivent soutenir toutes les mesures prises pour atténuer les risques liés à la sécurité de l'information et y participer activement, le cas échéant.

Notre organisation en matière de sécurité de l'information

La Politique de sécurité de l'information de MTN Group définit les responsabilités, pouvoirs et relations appropriés pour mettre en œuvre et gérer de façon cohérente la sécurité de l'information à MTN. L'organisation de la sécurité de l'information est représentée par toutes les unités opérationnelles et par toutes les unités fonctionnelles de soutien pertinentes afin d'assurer une coordination structurée des activités liées à la sécurité de l'information.

Notre politique de gestion des biens
La politique de gestion des biens précise l'importance des informations ou des biens informationnels, y compris l'identification du propriétaire des biens, la classification des biens et la détermination des cotes de confidentialité, d'intégrité et de disponibilité des biens.
Notre sécurité des ressources humaines
Les biens informationnels doivent être physiquement protégés contre tout accès non autorisé, toute utilisation abusive, tout dommage ou tout vol. Le campus de MTN et les installations de traitement de l'information doivent être adéquatement protégés contre les menaces physiques et environnementales.
Notre sécurité physique
Les biens informationnels doivent être physiquement protégés contre tout accès non autorisé, toute utilisation abusive, tout dommage ou tout vol. Le campus de MTN et les installations de traitement de l'information doivent être adéquatement protégés contre les menaces physiques et environnementales.

Notre politique de sécurité des opérations

La politique de sécurité des opérations établit des contrôles appropriés qui doivent être mis en œuvre pour empêcher l'accès non autorisé, l'utilisation abusive ou la défaillance des systèmes et équipements d'information et afin de garantir la confidentialité, l'intégrité et la disponibilité des informations traitées par les systèmes d'information, les applications, équipements et périphériques réseau ou stockées dans ceux-ci.
Notre politique de sécurité des communications

La politique de sécurité des communications couvre les implications associées à l'utilisation des services réseau, y compris la communication entre les OpCos de MTN, les tiers et les transactions en ligne entre autres.
Notre politique de contrôle d'accès

a) La Politique de contrôle d'accès définit les contrôles à mettre en œuvre et à maintenir pour protéger les biens informationnels contre les accès logiques non autorisés qui représentent un risque important pour l'organisation.
b) L'accès aux informations ou aux biens informationnels, aux installations de traitement de l'information, aux systèmes, aux équipements d'application et aux périphériques réseau doit être limité conformément aux exigences commerciales valides, à la responsabilité professionnelle de l'utilisateur et aux exigences de sécurité de l'information. Des procédures formelles seront mises en place pour contrôler l'attribution des droits d'accès.

Notre politique d'acquisition, de développement et de maintenance des systèmes d'information

La politique d'acquisition, de développement et de maintenance des systèmes d'information définit les exigences de sécurité à déterminer et à intégrer pendant le développement et la maintenance d'applications, de logiciels, de produits et/ou de services.

Notre Politique de gestion des incidents liés à la sécurité de l'information
La politique de gestion des incidents liés à la sécurité de l'information fournit des instructions pour élaborer et mettre en œuvre les Procédures de gestion des incidents liés à la sécurité de l'information pour les systèmes d'information, les applications, les équipements et les périphériques réseau, améliorant ainsi la sensibilisation des utilisateurs à la sécurité, à la détection précoce et à l'atténuation des incidents de sécurité et suggérant des mesures qui peuvent être prises pour réduire les risques liés aux incidents de sécurité.

Notre processus de gestion de la continuité des opérations
Un processus de gestion de la continuité des opérations doit être mis en œuvre afin de minimiser l'impact sur l'organisation et la reprise après une perte d'information ou de biens informationnels, de systèmes, d'applications, d'équipements et de périphériques réseau résultant d'événements prévus (par exemple, une grève du travail ou un ouragan) ou imprévus (catastrophes naturelles telles qu'un tremblement de terre, des accidents, des pannes d'électricité et des défauts d'équipement) à un niveau acceptable.

Ce processus doit identifier les processus opérationnels critiques et intégrer les exigences en matière de gestion de la sécurité de l'information relatives à la continuité des opérations à d'autres exigences de continuité liées à des aspects tels que les opérations, la dotation en personnel, les matériaux, le transport et les installations. Pour plus de détails, veuillez-vous reporter au cadre ou à la boîte à outils de MTN Group et des Départements Gestion de la continuité des opérations des OpCos.
Notre politique de conformité

La politique de conformité fournit des directives pour la conception et la mise en œuvre de contrôles appropriés afin de respecter les lois, les réglementations et les exigences légales et contractuelles locales de MTN. La conception, l'exploitation, l'utilisation et la gestion des systèmes d'information doivent être soumises aux lois et réglementations locales, ainsi qu'aux exigences de sécurité légales et contractuelles.

Vous pouvez faire connaître toutes vos observations ou préoccupations en appelant nos lignes d'assistance client dans le pays et par courriel à l'adresse cybersecurity@mtn.com.