Règlement d'utilisation informatique

Migros

Responsable du document (document owner)	Ruf, Lukas-MGB
Auteur-e du document	Marques, Raphael-MGB
Version du document	v1.0
Date du document	01.07.2021
Cycle de révision	Annuel
Date d'entrée en vigueur	1.7.2021
Statut	Freigegeben

Lukas Ruf
M0560320 Mail
2021.09.09
08:18:54 +02'00'

Historique du document

Vers.	Date	Personne	Modifications
0.1	22.12.2020	Raphael Marques	Document initial issu du modèle
0.2	30.12.2020	Raphael Marques	Reprise des informations les plus importantes à partir des règlements précédents. Première ébauche
0.3	14.1.2021	Raphael Marques	Review Björn Sieger, Dario Quattrocchi
0.4	15.1.2021	Raphael Marques	Ajout du chapitre sur l'internet et les courriels, nettoyage pour la révision
0.5	17.2.2021	Raphael Marques	Intégration des retours de la revue interne CU
0,6	19.3.2021	Raphael Marques	Intégration de la revue des parties prenantes
0.7	3.5.2021	Raphael Marques	Intégration des retours d'information du Conseil de la sécurité de l'information
0.8	21.6.2021	Lukas Ruf	Révision pour la Conférence spécialisée IT et le CT
1.0	28.6.2021	Lukas Ruf	Validation après consultation effectuée

Sommaire

1. Introduction

Migros s'engage à créer un environnement sûr pour ses collaboratrices et collaborateurs, ses informations et ses biens. Toutes les informations provenant de clients, de partenaires et de tiers doivent être protégées de manière adéquate. Migros s'appuie sur les normes de la branche et sur une approche fondée sur les risques pour la mise en œuvre des contrôles et des mesures de sécurité.

2. Contenu et objectifs

L'objectif de ce Règlement d'utilisation informatique est de définir des principes généraux pour:

- le maintien de la confidentialité, de l'intégrité et de la disponibilité des informations et des biens
- la protection de tous les biens contre les menaces – internes ou externes, intentionnelles ou accidentelles – selon une approche fondée sur le risque
- le respect des exigences légales, réglementaires, opérationnelles et contractuelles

Le Règlement d'utilisation informatique comporte une partie principale et des annexes. La partie principale définit les principes. Le contenu du document principal a un impact direct sur les pratiques des membres du personnel et décrit ce à quoi il faut veiller dans l'utilisation des ressources informatiques (matériel et logiciels) et des données. Les annexes contiennent des sujets complémentaires, des explications ou des clarifications relatives aux principes de la partie principale.

Dans le Règlement d'utilisation informatique, on entend par ressources informatiques tout le matériel informatique et les logiciels. Il s'agit entre autres de l'ordinateur portable, du téléphone mobile, mais aussi du serveur, de l'équipement du réseau comme le routeur, de la palette Office, de SAP et des données qui y sont enregistrées.

3. Domaine d'application

Le Règlement d'utilisation informatique, qui fait partie de la Réglementation de sécurité, s'applique aux collaboratrices et collaborateurs de l'ensemble du groupe Migros dans le cadre de la Gouvernance nationale de la sécurité de l'information, c'est-à-dire à tout le personnel interne et externe de toutes les sociétés du groupe Migros, à l'exception de la Banque Migros. Au sens du présent Règlement d'utilisation de l'informatique, les entreprises du groupe Migros sont toutes les coopératives Migros et la Fédération des coopératives Migros, ainsi que toutes les entreprises qu'elles contrôlent individuellement ou conjointement, directement ou indirectement.

Le règlement représente un ensemble de documents qui définissent des principes, des exigences, des procédures et des standards contraignants en matière de sécurité des informations. Tous les documents publiés dans le règlement peuvent être consultés sur security.migros.net.

Le Règlement d'utilisation informatique remplace le Règlement d'utilisation de la FCM[1]publié précédemment ainsi que tous les documents dérivés de ce règlement dans les entreprises M.

[1] https://m-security.migros.net/InformationSecurity/download/attachments/4620300/Nutzungsreglement_MGB_1.3.pdf?api=v2

3.1 Politique applicable à l'ensemble du groupe et aux entreprises

Les entreprises du groupe Migros peuvent renforcer et préciser le règlement d'utilisation informatique du groupe Migros (également appelé «Politique pour le groupe» dans ce contexte) dans le cadre d'une politique spécifique à l'entreprise. En cas de conflit entre une politique spécifique à une entreprise et les politiques pour le groupe, ces dernières prévalent et l'emportent sur la politique de l'entreprise.

3.2 Intégration dans le Règlement Migros

Le Règlement d'utilisation informatique fait partie du Règlement Migros. Le Règlement Migros est enregistré sur security.migros.net. Le Règlement d'utilisation informatique est du type «Politique».

4. Révision, mise à jour et maintenance

Le Règlement d'utilisation informatique est revu au moins une fois par année. Il peut être modifié par le groupe CISO du groupe en fonction des besoins de protection de Migros si de nouvelles menaces ou vulnérabilités sont identifiées ou si le profil de risque de l'entreprise évolue.

5. Exceptions

Des exceptions au Règlement d'utilisation informatique sont possibles dans certaines circonstances, par exemple lorsqu'il est impossible d'en respecter les exigences en raison des conditions locales.

6. Application

Si une violation ou un soupçon avéré de violation de ce règlement d'utilisation est constaté, les mesures suivantes peuvent être prises:

- Blocage préventif de l'accès aux équipements de travail concernés, p. ex. verrouillage du compte utilisateur/utilisatrice correspondant
- Blocage des données d'abus et d'usage illicite ainsi que leur sauvegarde et archivage à des fins de preuve
- Suppression des données d'abus et d'usage illicite, si cela est requis pour des motifs de sécurité et que rien ne s'oppose légalement à une conservation de ces données

Le comportement d'une collaboratrice ou d'un collaborateur illégal ou contraire à cette politique représente une violation des obligations prévues par le droit du travail et peut entraîner des mesures disciplinaires (y compris le licenciement), des conséquences civiles et/ou pénales ainsi que des demandes de dommages et intérêts. En cas de soupçon motivé d'acte punissable (par exemple pédopornographie, incitation à la haine raciale, etc.), un signalement à l'autorité compétente peut être effectué. Les pertes, dommages et coûts engendrés par

une conduite illégale ou contraire aux politiques, y compris les frais de clarification et d'enquête, de justice, d'avocat et de sanction, peuvent être facturés à la collaboratrice ou au collaborateur fautif.

7. Utilisation des ressources informatiques de Migros

Les collaboratrices et les collaborateurs disposent de ressources informatiques mises à disposition pour un usage professionnel. L'utilisation de ces ressources informatiques est fondamentalement de la responsabilité des collaboratrices et des collaborateurs mêmes. La responsabilité d'une utilisation sûre et précautionneuse de ces ressources informatique leur incombe.

7.1 Pratiques interdites

Les pratiques suivantes sont interdites:

- Quitter le poste de travail sans verrouiller ou fermer la session
- Toute utilisation non autorisée des ressources informatiques, des informations de Migros, des informations sur les clients et/ou les partenaires
- La participation intentionnelle ou par négligence à des activités susceptibles de mettre en danger la sécurité des informations, les ressources informatiques ou les réseaux de Migros, de ses partenaires ou de ses clients
- La violation des droits de propriété intellectuelle d'une personne ou d'une entreprise
- Les tentatives non autorisées de modifier la configuration de sécurité des ressources informatiques de Migros, ou de contourner ou désactiver les restrictions de sécurité afin d'accéder à des informations ou à des zones protégées
- L'utilisation des ressources informatiques de Migros pour télécharger, stocker, transmettre ou diffuser/distribuer des contenus répréhensibles. Les contenus répréhensibles comprennent le matériel pornographique, offensant, discriminatoire, raciste ou diffamatoire
- L'utilisation des ressources informatiques de Migros pour créer, télécharger, stocker, vendre, distribuer, copier ou échanger des logiciels, informations, musiques ou autres fichiers multimédias illégaux, protégés par des droits d'auteur ou sans licence
- La suppression ou la destruction non autorisée, intentionnelle ou par négligence grave, d'informations, de communications ou de données de Migros
- L'installation ou l'utilisation de tout logiciel d'application ou de services en nuage qui n'ont pas été autorisés par Group IT Migros
- L'utilisation d'outils, applications et dispositifs de tout genre ou les exploits (exploitation des vulnérabilités) pour causer des dommages à Migros.
- Le stockage, l'exécution ou la distribution de tout logiciel malveillant
- L'utilisation de comptes privés auprès de services en nuage autorisés (p. ex. le compte privé Microsoft 365)

7.2 Utilisation privée des ressources informatiques de Migros

Les appareils et équipements de communication de Migros mis à disposition de l'utilisatrice ou de l'utilisateur peuvent être utilisés de façon limitée à des fins privées. L'utilisation à des fins privées des ressources informatiques de Migros ne compte pas comme temps de travail.

L'utilisation à des fins privées des ressources informatiques de Migros est soumise aux restrictions suivantes:

- Les fichiers privés ne peuvent pas être stockés sur les systèmes de Migros
- L'utilisation privée d'un équipement de Migros ne doit pas avoir d'impact négatif sur la productivité de la collaboratrice ou du collaborateur ni sur la disponibilité du système

- L'utilisation privée de ces dispositifs et technologies est soumise aux mêmes règles que leur utilisation professionnelle.
- L'utilisation privée des ressources informatiques de Migros qui servent principalement au traitement, au stockage de masse et à l'échange d'informations et de données de Migros (p. ex. serveurs, composants de réseau, appareils IoT) n'est pas autorisée

7.3 Téléchargement, installation et utilisation des logiciels

Tous les logiciels et applications utilisés sur les ressources informatiques de Migros doivent être obtenus par l'intermédiaire du service informatique officiel (p. ex. Group IT Migros) et faire l'objet d'une licence correspondante pour un usage professionnel.

7.4 Protection des ressources informatiques de Migros

Les ressources informatiques de Migros doivent être protégées par les collaborateurs et les collaboratrices avec le soin requis contre le vol et les dommages (sur le lieu de travail, en déplacement et à domicile). Les collaborateurs et les collaboratrices doivent s'assurer que l'écran est verrouillé au moment de quitter le poste de travail et qu'au moins un mot de passe est nécessaire pour continuer à travailler. Il en va de même pour les équipements informatiques privés s'ils contiennent des données professionnelles ou si de telles données peuvent y être stockées ou consultées. Voir également le chapitre 8.1. La perte d'un appareil doit être immédiatement signalée au Service desk (servicedesk@mgb.ch).

7.5 Utilisation des imprimantes et des photocopieuses

Les documents doivent, dans la mesure du possible et si l'équipement est disponible, être imprimés de façon sûre dans les locaux de l'entreprise. Tous les documents imprimés doivent être immédiatement retirés de l'imprimante. Si des documents à contenu confidentiel ou secret sont trouvés vers une imprimante, ils doivent être immédiatement remis à leur auteur ou détruits.

7.6 Signalement des cas d'urgence

Le groupe Migros gère diverses infrastructures de services, plusieurs sont locales et l'une est centrale pour la Fédération des coopératives (servicedesk@mgb.ch). Si une urgence survient dans l'utilisation des ressources informatiques, elle doit être signalée immédiatement, soit auprès d'un service desk de l'entreprise ou soit auprès de celui de la Fédération des coopératives Migros servicedesk@mgb.ch).

Les incidents techniques suspects (p. ex., l'infection possible d'un ordinateur par des virus, l'hameçonnage, le piratage, etc.) doivent être signalés immédiatement, c'est-à-dire dès la survenue des soupçons, à security@migros.ch et aux service desks locaux.

7.7 Sécurité en dehors des locaux de l'entreprise

Les collaborateurs et les collaboratrices en déplacement respecteront les points suivants:

- Il convient d'être particulièrement attentif lors de la discussion d'informations confidentielles dans les lieux publics (aéroports, gares, restaurants, parcs, trains et autres lieux à forte fréquentation). Les informations secrètes ne doivent jamais être discutées dans les lieux publics.
- Les tiers ne doivent pas pouvoir lire des informations confidentielles ou secrètes affichées sur l'écran d'un ordinateur portable. Si nécessaire, le département informatique peut organiser un pare-vue (technique de floutage).

- Pour les WLAN publics, le VPN doit toujours être utilisé.

7.8 Utilisation d'internet

Les collaboratrices et les collaborateurs de Migros utilisent internet pour obtenir des informations, échanger des données et des documents avec des partenaires commerciaux, des clients, des autorités et d'autres instances, en tenant compte des exigences de sécurité de l'information, et pour se procurer des services et des biens, en tenant compte des règles de signature en vigueur. Les collaboratrices et les collaborateurs de Migros doivent utiliser internet de manière à protéger Migros des risques juridiques, réglementaires et opérationnels ainsi que des risques pour la réputation de Migros. L'utilisation privée d'internet pendant les heures de travail doit être réduite au minimum.

Toute utilisation illégale ou inappropriée d'internet est interdite. Cela inclut notamment:

- l'accès à tout type de site de jeu (p. ex. les jeux de hasard) ou de commerce boursier privé
- l'accès à des sites web au contenu obscène ou illégal

7.9 Messagerie électronique

Une boîte aux lettres personnelle ne peut être utilisée que par la collaboratrice ou le collaborateur concerné. Les courriels professionnels importants, qui doivent être accessibles à d'autres personnes, doivent être stockés dans des endroits convenus sur les lecteurs prévus à cet effet.

La redirection automatique vers des adresses électroniques externes est interdite. Dans des cas spécifiques, une redirection externe peut être configurée. Toute demande doit être adressée à servicedesk@mgb.ch ou au service desk de l'entreprise M concernée.

La collaboratrice ou le collaborateur a l'obligation d'activer un message d'absence en cas d'absence ou de départ de l'entreprise. Si le courrier entrant doit être transféré vers la personne suppléante, cela doit être convenu par les deux personnes au préalable. Dans des circonstances particulières (par exemple, en cas de maladie de la collaboratrice ou du collaborateur), Migros se réserve le droit d'établir un message d'absence, en tenant compte des aspects liés à la protection des données.

La prudence est de mise dans le cas de courriels dont l'expéditeur est douteux ou dont l'objet est formulé de manière inhabituelle, ainsi que dans le cas de formulations étranges dans le texte. Ces courriels doivent être supprimés immédiatement. Pour des raisons de sécurité, il ne faut pas ouvrir les pièces jointes de ces courriels ni cliquer sur les liens.

Selon la directive «Rapports et enquêtes», les données et documents électroniques des collaboratrices et collaborateurs liés à l'entreprise peuvent être enregistrés et consultés dans le cadre d'une enquête interne. Par conséquent, tous les éléments d'Outlook (courriels, entrées de calendrier, tâches, discussions dans Teams et contacts) sont conservés pendant 10 ans à des fins spécifiques et avec une protection d'accès.

8. Utilisation des ressources informatiques privées

8.1 Utilisation professionnelle de ressources informatiques privées

Les ressources informatiques privées (p. ex. le propre smartphone) peuvent être utilisées pour un usage professionnel. La collaboratrice ou le collaborateur n'a pas droit à bénéficier du support ou de l'assistance pour ses ressources de travail privées.

Les ressources informatiques privées ne peuvent être connectées qu'au réseau du groupe Migros prévu à cet effet. L'utilisatrice ou l'utilisateur est responsable de la sécurité de son équipement informatique privé. Les données professionnelles stockées localement sur l'appareil doivent être supprimées immédiatement après leur utilisation.

Les ressources informatiques privées, si utilisées à des fins professionnelles, doivent être protégées contre tout accès non autorisé par un mot de passe ou une protection biométrique et un cryptage du lecteur. Les mises à jour des logiciels (c'est-à-dire systèmes d'exploitation, applications, apps, etc.) doivent être effectuées dès qu'elles sont mises à disposition par le fabricant du logiciel.

9. Gestion des données Migros

9.1 Classification des données

Ce Règlement d'utilisation informatique prévoit le classement des données professionnelles dans les catégories suivantes:

- Données publiques: les données sont consultables par tout le monde.
- Données internes: les données sont consultables par tout le personnel de Migros.
- Données confidentielles: les données peuvent être consultées par un groupe restreint de collaboratrices et de collaborateurs de Migros et requièrent une protection accrue. Il existe des restrictions d'autorisation pour un groupe spécifique et les données doivent être traitées avec une diligence accrue. Il s'agit par exemple de données personnelles ou financières.
- Données secrètes: les données ne sont accessibles qu'à un petit groupe de personnes connues par leur nom et sont pleinement protégées. Les données sont cryptées individuellement au niveau du fichier. Les grosses transactions de fusion et acquisition sont, par exemple, des données secrètes.

À côté des catégories des données d'entreprise, nous trouvons les données privées qui, techniquement, ne sont pas traitées séparément. Les données des utilisateurs/utilisatrices, des collaborateurs/collaboratrices, qui n'ont pas de lien direct avec Migros, sont considérées comme données privées, selon une présomption réfragable. Les données privées ne doivent pas être enregistrées sur les systèmes Migros.

9.2 Gestion des données

Les collaborateurs et collaboratrices doivent traiter les données/informations de manière responsable.

Les données/informations doivent être traitées consciencieusement et avec soin, ne doivent être divulguées ou rendues accessibles qu'aux personnes qui en ont besoin pour l'accomplissement de leur fonction et de leurs tâches, doivent être protégées de manière adéquate à tout moment et ne peuvent être utilisées que conformément aux dispositions légales et aux règles internes applicables.

Les collaborateurs et collaboratrices sont tenus de veiller au respect des dispositions légales et des règlements internes applicables dans leur sphère d'influence.

Le traitement des données personnelles est notamment soumis à la directive de protection des données et à d'autres exigences en matière de protection des données prescrites par le service de conformité légale FCM.

Les données d'entreprise sont enregistrées exclusivement sur des supports dont les technologies de stockage sont fournies et approuvées par Migros ou ses partenaires mandatés. Si, conformément au

chapitre 8.1, des ressources informatiques privées sont utilisées, le collaborateur ou la collaboratrice doit s'assurer que les données sur son appareil privé sont effacées immédiatement après leur utilisation.

La personne quittant l'entreprise doit nettoyer le support de stockage personnel avant son départ. Ce faisant, les données privées doivent être supprimées et les autres données doivent être déplacées après consultation de la supérieure ou du supérieur hiérarchique. Après le départ de la collaboratrice ou du collaborateur, l'accès au support de stockage de données personnel est bloqué.

Une personne propriétaire du répertoire doit être définie pour chaque emplacement de stockage. Elle est responsable de la définition initiale des personnes autorisées à accéder aux données ainsi que de leur mise à jour continue.

Les données d'entreprise non publiques ne peuvent être enregistrées que sous forme cryptée sur des clés de mémoire et des supports de données externes (par exemple, CD, DVD, clés de mémoire, disques durs externes/disques durs USB, et similaires). Après utilisation, ces données doivent être supprimées du support de données. Les CD et DVD contenant des données d'entreprise doivent être éliminés ou recyclés de manière sécurisée après usage.

9.3 Gestion des mots de passe

Les connexions aux ressources informatiques de Migros sont possibles uniquement avec l'identifiant personnel et le mot de passe. Les règles de mot de passe suivantes s'appliquent:

- Le mot de passe, le login et les certificats sont personnels et doivent être tenus secrets vis-à-vis de tiers. Il est donc interdit de communiquer ou de rendre accessible son mot de passe personnel à une autre personne. Il est interdit de noter les mots de passe ou les codes PIN, sauf si le support écrit est conservé dans un endroit verrouillé (p. ex. dans une enveloppe déposée dans un coffre-fort).
- Le mot de passe doit au minimum satisfaire aux exigences de la norme relative aux mots de passe (voir MSS001, chapitre «Mots de passe interdits»).
- Le mot de passe ne doit pas être facile à deviner. Cela signifie, par exemple, qu'il ne doit pas contenir l'identifiant, le nom de l'organisation, d'autres informations personnelles, des numéros de téléphone, des mots de passe courants (par exemple «Motdepasse», «Passe1234», etc.).
- Les mots de passe utilisés dans le groupe Migros ne peuvent pas être utilisés dans d'autres institutions et dans les applications externes à Migros (par exemple, comptes de courrier électronique privés, portails web externes, etc.).
- Au sein du groupe Migros, le même mot de passe peut être utilisé plusieurs fois tant qu'il est utilisé dans le cadre du même rôle.
- Si l'on soupçonne qu'un mot de passe est connu de tiers, la personne est tenue de le changer immédiatement.
- Si un mot de passe est modifié, il ne doit pas correspondre à un mot de passe utilisé précédemment.
- Les mots de passe ne peuvent pas être transmis en texte clair (p. ex. dans un courriel)
- Lors de la saisie du mot de passe, il faut s'assurer que personne n'observe la saisie.
- Les mots de passe initiaux doivent impérativement être modifiés après la première connexion.
- Les mots de passe et les identifiants prédéfinis, par exemple ceux fournis par le fabricant lors de la livraison du matériel informatique, doivent être remplacés par des mots de passe individuels et, si possible, des identifiants avant que le système ou le matériel ne soit mis en service.

- Chaque collaboratrice et collaborateur est responsable des transactions effectuées sous son identifiant.
- L'accès à distance à des fins de support doit être confirmé par l'utilisateur ou l'utilisatrice lorsque la connexion est établie. Pendant la session à distance, les activités de l'opérateur/opératrice doivent être surveillées et, une fois le travail terminé, la collaboratrice ou le collaborateur doit s'assurer que la session à distance a été correctement fermée.

9.4 Enregistrement et analyse des données électroniques

Migros peut utiliser des systèmes qui génèrent des journaux et des messages d'avertissement pour maintenir l'exploitation, la sécurité, l'intégrité et la disponibilité des ressources informatiques, des données/informations, pour garantir la qualité des services, pour respecter et contrôler les dispositions légales et/ou les règles internes applicables, pour contrôler le respect des conditions de licence, pour la facturation et pour le contrôle des coûts, ainsi que pour identifier des perturbations opérationnelles ou abus et y remédier.

Les collaboratrices et les collaborateurs prennent connaissance du fait que Migros enregistre des données sur l'utilisation des ressources informatiques, en particulier les données de trafic et journal sur l'utilisation d'internet ou des courriels, des informations comparables sur les appels téléphoniques sortants ou entrants et les données de journalisation sur les accès/mutations/suppressions de fichiers, et qu'elle dispose de données d'utilisation générales pour tous les comptes et peut les analyser aux fins susmentionnées. L'analyse est en principe effectuée sous forme anonyme ou pseudonymisée.

En cas d'incidents ou de cas suspects graves, des analyses visant la personne peuvent être effectuées ou d'ultérieures données enregistrées en consultation avec le département des ressources humaines et le service de conformité légale et dans le respect du principe de proportionnalité. Pour de plus amples informations sur la sécurisation et la consultation des données et des documents, se référer la directive Signalements et enquêtes internes.

Les données sont conservées sous forme personnelle aussi longtemps qu'elles sont nécessaires à la réalisation du but spécifique pour lequel elles ont été collectées ou s'il existe un intérêt légitime à les conserver. Cela peut être le cas notamment si les données personnelles sont nécessaires pour faire valoir ou défendre des revendications, pour des raisons de preuve, à des fins d'archivage et pour assurer la sécurité informatique. Les données enregistrées sont également conservées sous forme de données personnelles tant qu'elles sont soumises à une obligation légale de conservation ou qu'il existe une autre raison exceptionnelle valable en vertu du droit applicable. Une période de conservation de dix ans, par exemple, s'applique à certaines données. Pour d'autres données, des périodes de conservation plus courtes s'appliquent, par exemple pour les enregistrements d'opérations effectuées dans internet (données de journal).

10. Autres documents utiles

Outre les dispositions générales sur le respect de la sécurité de l'information, il existe d'autres règlements qui s'appliquent à tout le personnel. En plus des principes directeurs, des politiques, des directives, des normes et des dispositions, toutes les annexes au Règlement d'utilisation informatique sont également contraignantes pour toutes les collaboratrices et tous les collaborateurs de Migros. Tous les documents sont enregistrés sur security.migros.net.

D'autres documents relatifs à la conformité légale sont disponibles sur l'intranet. Les documents pertinents des RH sont publiés ici.

Des informations ultérieures sur le traitement des données personnelles sont contenues dans la Déclaration de protection des données pour les collaboratrices et les collaborateurs.

Annexe Accès à distance

Migros

Responsable du document (propriétaire du document)	Ruf, Lukas-MGB
Auteur-e du document	Marques, Raphael-MGB
Version du document	v1.0
Date du document	01.07.2021
Cycle de révision	Tous les ans
Date d'entrée en vigueur	1.7.2021
Statut	Validé

Lukas Ruf
M0560320 Mail
2021.09.09
08:17:44
+02'00'

Historique du document

Vers.	Date	Personne	Modifications
0.1	22.12.2020	Raphael Marques	Document initial issu du modèle
0.2	2.2.2021	Dario Quattrocchi	Intégration des dispositions
0.4	5.2.2021	Raphael Marques	Cleanup pour la révision
0.5	17.2.2021	Raphael Marques	Intégration du retour issu de la révision en interne
0.6	18.3.2021	Raphael Marques	Intégration des retours issus de la révision des parties prenantes
0.7	3.5.2021	Raphael Marques	Intégration des retours de l'Information Security Board
0.8	21.6.2021	Lukas Ruf	Révision pour la Conf. Spéc. IT et le CT
1.0	28.6.2021	Lukas Ruf	Validation après consultation

Sommaire

1. Accès à distance – Remote access

L'accès à distance (remote access en anglais) permet aux collaborateurs et collaboratrices internes et externes se trouvant hors de l'entreprise de travailler comme s'ils étaient connectés au réseau du groupe Migros. Une telle connexion à distance peut être établie au moyen d'un Virtual Private Network (VPN) ou par le biais d'un accès au serveur Citrix.

En cas d'accès avec un équipement tiers (p. ex. PC, ordinateur portable, tablette ou smartphone privé), il faut tenir compte des restrictions pour la sauvegarde en local des documents d'entreprise (voir annexe Appareils mobiles et points de terminaison).

1.1 Exploitation et installation

Les collaboratrices et collaborateurs eux-mêmes sont responsables du bon fonctionnement de leur WLAN privé. L'accès externe ne peut se faire que par l'intermédiaire de dispositifs dotés d'une protection antivirus et de systèmes d'exploitation à jour, ainsi que de versions de programme à jour et corrigées.

1.2 Accès par le serveur CITRIX

Le personnel interne et externe peut accéder par le biais d'une interface web aux services du groupe Migros et aux données de l'entreprise au moyen d'une connexion Citrix. Dans le cas d'une connexion Citrix, seul le contenu de l'écran est transféré du serveur au dispositif de travail privé. Les données restent mémorisées dans le réseau interne du groupe Migros, ce qui permet de garantir un niveau maximal de sécurité des données et l'accès aux données et systèmes protégés.

Les ordinateurs de Migros sont déjà munis de l'application permettant un accès Citrix; en cas d'utilisation sur un appareil tiers, le récepteur Citrix requis doit être téléchargé depuis http://www.citrix.com/receiver et installé selon les instructions.

Le stockage en local de données de l'entreprise est uniquement autorisé en cas d'utilisation d'outils informatiques de Migros; il est interdit sur les outils informatiques privés. L'impression de données de l'entreprise doit s'effectuer dans les locaux de Migros et est autorisée sur des imprimantes privées uniquement dans des cas exceptionnels. En cas d'impression sur des imprimantes privées, la même prudence est de mise pour le traitement de données de l'entreprise que dans les locaux de Migros.

Une fois connectés, les collaboratrices et collaborateurs sont automatiquement déconnectés après une longue période d'inactivité. La session Citrix est toutefois maintenue. Après un certain temps d'inactivité, la session Citrix est elle aussi terminée et les documents qui n'ont pas été sauvegardés sont perdus.

1.3 Accès via la connexion VPN

Une connexion VPN permet de connecter un poste de travail externe au réseau interne du groupe Migros. Les collaboratrices et collaborateurs peuvent ainsi accéder aux données d'entreprise, aux courriels professionnels, etc. Un logiciel spécial est requis pour établir une telle connexion. Il est préinstallé sur les outils informatiques de Migros.

Par principe, l'accès à distance par VPN n'est pas autorisé sur des appareils tiers. Les exceptions doivent faire l'objet d'une demande auprès de la CU Security&Risk via le processus d'exception

(«Demande d'exception»). Dans des cas motivés, des partenaires externes (p. ex. des fournisseurs avec mandat de support) reçoivent un accès à distance si celui-ci satisfait aux mêmes exigences de sécurité que les appareils d'entreprise de Migros. Les partenaires externes doivent installer et paramétrer eux-mêmes le client VPN selon les instructions. Les utilisatrices et utilisateurs accédant de l'extérieur au réseau du groupe Migros avec des appareils tiers s'engagent à garantir un niveau de sécurité adéquat sur leur équipement (antivirus, pare-feu, protection par mot de passe, cryptage des fichiers, logiciel de sécurité à jour et correctifs, etc.)

Une connexion VPN suppose une connexion stable à internet. L'authentification auprès du réseau interne se déroule en deux étapes:

1. saisie du nom d'utilisateur et du mot de passe
2. saisie d'un mot de passe à usage unique généré dynamiquement (OTP - One-Time-Password, voir annexe Appareils mobiles et points de terminaison)

Une fois connectés, les collaboratrices et collaborateurs sont automatiquement déconnectés après une longue période d'inactivité.

Annexe Services en nuage (cloud services)

Migros

Responsable du document (propriétaire du document)	Ruf, Lukas-MGB
Auteur-e du document	Marques, Raphael-MGB
Version du document	v1.0
Date du document	01.07.2021
Cycle de révision	Annuel
Date d'entrée en vigueur	1.7.2021
Statut	Validation

Lukas Ruf
M0560320 Mail
2021.09.09
08:15:00 +02'00'

Historique du document

Vers.	Date	Personne	Modifications
0.1	22.12.2020	Raphael Marques	Document initial issu du modèle
0.2	2.2.2021	Raphael Marques / Dario Quattrocchi	Traitement des contenus et révision initiale
0.4	5.2.2021	Raphael Marques	Cleanup pour la révision
0.5	17.2.2021	Raphael Marques	Intégration de retours de la CU révision interne
0.6	18.3.2021	Raphael Marques	Intégration des retours des parties prenantes
0.7	3.5.2021	Raphael Marques	Intégration des retours de l'Information Security Board
0.8	21.6.2021	Lukas Ruf	Révision pour la Conf. Spéc. IT et le CT
1.0	28.6.2021	Lukas Ruf	Validation après consultation

Sommaire

1. Introduction

Cette directive vise à garantir que les services en nuage ne soient pas utilisés sans que Enterprise Architecture et la CU Security&Risk (partie de Group IT FCM) soient au courant et aient donné leur accord. Il est impératif que les membres du personnel ne puissent pas ouvrir de comptes de services en nuage ni conclure de contrats en la matière sans que Enterprise Architecture ait été impliqué et ait donné son accord. C'est nécessaire pour préserver l'intégrité et la confidentialité des données ainsi que la sécurité du réseau de l'entreprise.

Migros met tout en œuvre pour que les membres du personnel puissent effectuer leurs tâches de la manière la plus efficace possible grâce à l'utilisation de la technologie. La directive ci-après vise à établir une procédure permettant aux membres du personnel d'utiliser les services en nuage sans mettre en péril les données de l'entreprise ni les outils informatiques.

2. Services en nuage chez Migros

Migros acquiert de nombreux services en nuage pour la fourniture de divers services informatiques. Cette directive porte sur les types de services en nuage suivants:

- Software as a Service (SaaS): l'application et l'application partielle sont fournies par le fournisseur de services en nuage. Ici, Migros configure l'application. Migros utilise de nombreuses applications Software as a Service de différents fournisseurs de services en nuage.
- Function as a Service: des fonctions spécifiques (par exemple, les réseaux IA) sont fournies par le fournisseur de services en nuage. Migros prend en charge la logique, les paramètres d'entrée, les données et la configuration. Diverses plateformes de différents fournisseurs de services en nuage sont utilisées chez Migros.
- Platform as a Service (PaaS): l'infrastructure informatique et la plateforme (par exemple Kubernetes) sont mises à disposition par le fournisseur de services en nuage. Migros exploite son propre code au sein des plateformes. Diverses plateformes de différents fournisseurs de services en nuage sont utilisées chez Migros.
- Infrastructure as a Service (IaaS): l'infrastructure informatique est mise à disposition par un fournisseur de services en nuage. Migros exploite les applications et autres composants logiciels au sein même du nuage. Pour l'IaaS, Migros s'appuie sur deux fournisseurs agréés de services en nuage (Microsoft Azure et Google Cloud Platform).

Cette directive inclut tous les concepts opérationnels pour le nuage mentionnés et futurs.

L'utilisation de services en nuage doit être conforme aux dispositions légales en vigueur, aux règlements internes ainsi qu'aux conditions d'utilisation du prestataire concerné. Migros définit quelles données/informations peuvent être enregistrées ou non dans le nuage. La CU Security & Risk octroie la validation de sécurité, et la CU Enterprise Architecture la validation de l'architecture. Ces deux validations sont nécessaires pour une autorisation. L'autorisation est régie via le Cloud Enabling & Orchestration Board.

Tous les modules complémentaires en provenance d'une place de marché au sein de services en nuage agréés doivent répondre au minimum aux mêmes normes de sécurité que le service en nuage lui-même. Si des services en nuage supplémentaires sont nécessaires pour un module complémentaire, ils doivent explicitement avoir été validés comme nouveau service en nuage.

3. Utilisation des services en nuage au sein de Migros

L'utilisation de services en nuage non approuvés et utilisés à titre privé (par exemple, Dropbox, WeTransfer ou Google Translate) avec des données Migros non «publiques» est interdite.

Migros exploite et consomme des services en nuage officiels qui peuvent être utilisés de façon illimitée pour les activités désignées. L'utilisation de services en nuage, non exploités et utilisés par Migros, requiert une autorisation d'Enterprise Architecture ainsi qu'une validation de sécurité par la CU Security&Risk. Pour toute question à propos de services en nuages, les membres du personnel doivent s'adresser à leur service informatique local ou au Cloud Enabling & Orchestration Board

4. Utilisation de Microsoft 365

L'utilisation des instances officielles de Microsoft 365 de Migros est autorisée dans le cadre des fonctions définies. Il est interdit d'utiliser des comptes Office 365 privés pour le traitement, le stockage ou la transmission de données de Migros.

Annexe Points de terminaison et appareils mobiles

Migros

Responsable du document (propriétaire du document)	Ruf, Lukas-MGB
Auteur-e du document	Marques, Raphael-MGB
Version du document	v1.0
Date du document	01.07.2021
Cycle de révision	Tous les ans
Date d'entrée en vigueur	1.7.2021
Statut	Freigegeben

Lukas Ruf
M0560320 Mail
2021.09.09
08:15:55 +02'00'

Historique du document

Vers.	Date	Personne	Modifications
0.1	22.12.2020	Raphael Marques	Document initial issu du modèle
0.2	28.1.2021	Dario Quattrocchi	Regroupement de l'annexe «Appareils mobiles» et «Points de terminaison», révision par Raphael Marques
0.4	5.2.2021	Raphael Marques	Cleanup pour la révision
0.5	17.2.2021	Raphael Marques	Intégration du retour à partir de la révision en interne
0.6	18.3.2021	Raphael Marques	Intégration du retour des parties prenantes
0.7	3.5.2021	Raphael Marques	Intégration des retours de l'Information Security Board
0.8	21.6.2021	Lukas Ruf	Révision pour la Conf. Spéc. IT et le CT
1.0	28.6.2021	Lukas Ruf	Validation après consultation

Sommaire

1. Ressources informatiques privées et de Migros

Vous trouverez ci-après les dispositions qui régissent l'utilisation des outils informatiques privés et des outils informatiques de Migros. Sont concernés les outils informatiques utilisés directement par les membres du personnel de Migros (également appelés points de terminaison).

Ces points de terminaison sont par exemple des ordinateurs portables, smartphones, stations de travail avec moniteurs, etc.

1.1 Points de terminaison

Les points de terminaison, c'est-à-dire les ordinateurs, les mobiles professionnels (téléphones mobiles et smartphones) et les tablettes professionnelles, sont la propriété de Migros et doivent être restitués à Migros lorsque la personne quitte l'entreprise.

Ces appareils sont gérés par Migros et les actions suivantes peuvent donc être effectuées sur l'appareil concerné sans information préalable de la collaboratrice ou du collaborateur:

- Restrictions à l'installation d'applications
- Installation obligatoire d'un code PIN ou de procédures d'authentification équivalentes
- Suppression de l'appareil en raison d'un incident de sécurité (par exemple, en cas de perte de l'appareil)
- Copie de toutes les données sur l'appareil et analyse de ces données par un-e expert-e en sécurité
- Autres activités administratives nécessaires pour l'activité

1.1.1 Traitement et sauvegarde des données

Les données sur tous les lecteurs réseau, les bibliothèques SharePoint et le stockage des données dans le cloud sont correctement sécurisées grâce à des sauvegardes et à la redondance. C'est pourquoi ces technologies doivent, dans la mesure du possible, être utilisées pour stocker les données.

Stockage dans Microsoft Teams	Les données qui sont créées et partagées dans un projet ou une équipe peuvent être stockées dans l'espace de stockage dédié de Microsoft Teams.
Sharepoint	Les bibliothèques SharePoint de Migros peuvent être utilisées comme les archives Microsoft Teams pour enregistrer et partager des fichiers conformément aux autorisations SharePoint.
Office 365 One Drive	Office 365 OneDrive peut être utilisé pour l'archivage personnel. En outre, l'archivage est synchronisé localement, ce qui rend les fichiers également disponibles en cas de coupure de la connexion internet.

1.1.2 Logiciels antivirus

Un concept antivirus à plusieurs niveaux, faisant appel à plusieurs solutions, est appliqué pour assurer une protection contre les virus informatiques. Le but est de prévenir une intrusion ainsi qu'une propagation de telles menaces.

En cas de suspicion de programme malveillant, d'incohérences ou de doute, il faut informer immédiatement security@migros.ch ou le service informatique local.

1.1.3 Gestion des mots de passe et des codes PIN

Les informations sur les accès (notamment les mots de passe) doivent être conservées de manière cryptée (p. ex. avec un outil de gestion des mots de passe).

Si des certificats sont installés localement, ceux-ci doivent être protégés séparément par un mot de passe. Le mot de passe doit être saisi dans le dialogue de l'installation.

1.1.3.1 Gestion des mots de passe et des codes PIN personnels

Les collaborateurs et collaboratrices sont responsables de la gestion correcte des mots de passe et des codes PIN:

- Il est recommandé de changer de mot de passe régulièrement (p. ex. chaque année) pour la connexion au poste de travail personnel (PC, ordinateur portable).
- Il est interdit de noter les mots de passe ou les codes PIN, à moins que ceux-ci ne soient mis en sécurité dans un endroit verrouillé (p. ex. dans une enveloppe déposée dans un coffre-fort).
- Les mots de passe et les PIN (à l'exception du mot de passe initial) sont personnels et ne doivent en aucun cas être divulgués, même à d'autres membres de l'entreprise. Cette règle doit aussi être respectée vis-à-vis des collaboratrices et des collaborateurs du Service desk.
- Lors de la saisie du mot de passe ou du code PIN, il faut s'assurer que personne ne peut en prendre connaissance.
- Les mots de passe initiaux (lors de l'octroi de droits de mots de passe attribués) doivent impérativement être changés lors de la première connexion.
- Un nouveau mot de passe ou PIN doit être différent des mots de passe ou codes PIN précédemment utilisés.
- Les mots de passe ne peuvent pas être enregistrés dans des documents normaux. Les mots de passe doivent être gérés dans un outil de gestion des mots de passe. Il convient de s'assurer que cet outil assure la sauvegarde cryptée des mots de passe. Les mécanismes de verrouillage appliqués par l'outil doivent satisfaire aux exigences actuelles. En cas de doute, il est possible de demander conseil et assistance à l'organisation Security&Risk (partie de Group IT FCM).
- Les mots de passe ne doivent jamais être envoyés par courriel. Font exception les mots de passe initiaux.
- Les mots de passe de l'entreprise doivent uniquement être utilisés pour les systèmes du groupe Migros (et non à des fins privées ou pour se connecter sur des sites web tiers).

1.1.3.2 Gestion des mots de passe fonctionnels

L'authentification pour des comptes utilisateur impersonnels est effectuée par un mot de passe fonctionnel, qui est en général connu de plusieurs personnes. Les règles ou restrictions suivantes doivent être observées en ce qui concerne les mots de passe fonctionnels:

Les comptes utilisateurs impersonnels disposent de droits d'accès limités.

Un compte utilisateur impersonnel ne permet pas d'accéder au réseau interne du groupe Migros depuis internet.

Les mots de passe fonctionnels ne peuvent pas être transmis à des externes.

1.1.3.3 Gestion des mots de passe administratifs fonctionnels

Dès que les personnes quittent l'entreprise ou changent de fonction, tous les mots de passe qu'elles connaissaient pour les comptes fonctionnels avec privilèges doivent être modifiés.

1.1.3.4 Gestion des certificats

Selon le logiciel utilisé sur le poste de travail du groupe Migros, l'utilisateur ou l'utilisatrice reçoit un certificat numérique personnel. Ce certificat personnel ne doit pas être transmis.

Les dispositions d'utilisation y compris les questions de responsabilité pour les certificats du groupe Migros se trouvent dans les directives d'exécution (CP&CPS) sur http://www.migros.ch/pki.

En cas de changement d'adresse électronique, la collaboratrice ou le collaborateur concerné reçoit automatiquement un nouveau certificat. Pour l'installation sur des appareils tiers, un nouveau PIN doit être demandé.

1.1.3.5 Gestion des mots de passe à usage unique (One-time password, OTP)

Les mots de passe à usage unique sont générés à chaque procédure d'authentification et ne sont acceptés qu'une seule fois pour se connecter. Comme les mots de passe changent constamment, ils constituent un élément de sécurité plus élevé que les mots de passe statiques (comme une liste à biffer).

Mots de passe à usage unique générés par un logiciel

Les mots de passe sont générés par un logiciel. Le mot de passe unique peut être généré à l'aide d'une application d'authentification ou être transmis à la collaboratrice ou au collaborateur par SMS. Une notification Push via l'app Authenticator constitue également un mot de passe unique autorisé.

En cas d'envoi par SMS, aucun frais n'est facturé au collaborateur ou à la collaboratrice.

Mots de passe à usage unique basés sur une solution matérielle

Les mots de passe uniques peuvent également être générés par une solution matérielle. Ce mode de génération de mots de passe est utilisé pour protéger des composants et applications critiques, et requiert un hard token (boîtier).

1.1.4 Vol ou perte

Le vol ou la perte d'appareils doivent être signalés sans délai au service informatique. Migros fera en sorte que les données de l'entreprise sur l'appareil concerné soient supprimées. En outre, dans le cas d'un appareil d'entreprise, le blocage immédiat de la carte SIM est demandé auprès du fournisseur de réseau.

1.1.5 Accès non autorisé

Si un accès non autorisé aux données de l'entreprise via un appareil est suspecté, cela doit être immédiatement signalé au département informatique conformément aux directives de signalement.

1.1.6 Appareils jailbreakés ou enracinés

Il n'est pas permis de trafiquer un appareil de l'entreprise en utilisant le jailbreak ou des méthodes équivalentes. Dès lors, il est interdit d'utiliser des jailbreaks, des appareils enracinés ou des logiciels/micrologiciels enracinés pour accéder aux fonctions système.

1.1.7 Copies piratées et contenus illégaux

Aucun contenu piraté ou illégal ne peut être chargé sur les ressources informatiques de Migros.

1.1.8 Envoi de données de l'entreprise

Les données de l'entreprise ne peuvent être envoyées que par l'intermédiaire de l'adresse électronique de l'entreprise. Si un utilisateur ou une utilisatrice soupçonne que des données d'entreprise ont été envoyées via un compte de messagerie électronique privé (dans le texte du courriel ou en pièce jointe), le département informatique doit en être immédiatement informé.

1.1.9 Sauvegarde et synchronisation du contenu des appareils

Les utilisatrices et les utilisateurs ne peuvent sauvegarder ou synchroniser le contenu des appareils (tels que les fichiers multimédia) que lorsqu'ils le font à des fins professionnelles.

1.2 Appareils mobiles et tablettes privées à des fins professionnelles

Les appareils mobiles privés peuvent être utilisés à des fins professionnelles. Il convient de noter que certaines autorisations doivent être accordées à Migros en raison de l'utilisation professionnelle. En autorisant l'appareil privé, les directives relatives aux appareils sont appliquées à l'appareil en question:

- L'appareil doit être verrouillé par un code PIN, des données biométriques, un mot de passe ou un schéma de balayage
- Le support de mémoire (p. ex. disque) doit être crypté.
- Les données d'entreprise peuvent être supprimées ou faire l'objet d'une enquête par l'employeur sans préavis (par exemple, si la sécurité de l'appareil n'est plus garantie)
- Le jailbreaking et les méthodes équivalentes sont interdites et peuvent empêcher l'accès aux données d'entreprise

Selon l'entreprise, différentes technologies sont utilisées pour pouvoir utiliser un appareil privé à des fins professionnelles. Le membre du personnel doit utiliser une méthode autorisée par l'entreprise Migros (Active Sync via Exchange, Secure Container, systèmes de gestion des appareils mobiles).

Il supporte entièrement tous les coûts liés à l'appareil mobile, aux accessoires mobiles (adaptateurs, etc.) et à l'itinérance.

L'utilisation privée pendant les heures de travail doit être réduite au minimum. Elle ne doit pas interférer avec l'activité professionnelle.