IT-Nutzungsreglement

Migros

Dokumentenverantwortlicher (Document Owner)	Ruf, Lukas-MGB
Dokumentenautor	Marques, Raphael-MGB
Dokumentenversion	V1.3
Dokumentendatum	12.03.2024
Überprüfungsturnus	Jährlich
Datum des Inkrafttretens	30.06.2023
Status	Freigegeben

Dokumentenhistorie

Ver.	Datum	Person	Anpassungen
0.1	22.12.2020	Raphael Marques	Initiales Dokument aus Template
0.2	30.12.2020	Raphael Marques	Übernehmen der wichtigsten Informationen aus vorherigen Reglementen. Erste Draft-Version.
0.3	14.01.202	Raphael Marques	Review Björn Sieger, Dario Quattrocchi
0.4	15.01.2021	Raphael Marques	Erweiterung um Internet & E-Mail-Kapitel, Cleanup für Review
0.5	17.02.2021	Raphael Marques	Einarbeitung CU Interne Review-Runde
0.6	19.03.2021	Raphael Marques	Einarbeitung Stakeholder Review
0.7	03.05.2021	Raphael Marques	Einarbeitung Feedback Information Security Board
0.8	21.06.2021	Lukas Ruf	Revision für FAKO IT und TA
1.0	28.06.2021	Lukas Ruf	Freigabe nach Vernehmlassung erfolgt
1.1	01.10.2021	Dario Quattrocchi	Kleine Anpassungen («Verallgemeinerungen»)
1.1	09.01.2022	Lukas Ruf	Freigabe
1.1.1	14.12.2022	Dario Quattrocchi	Kapitel 7.5 und 7.6 neu hinzugefügt, Anpassung von Links, Anpassung & Ergänzung 8.1 Abs. 1
1.1.2	23.01.2023	Lukas Ruf	Revision v1.2 unter Berücksichtigung der Anforderungen an die Datensicherheit gem. revidierter Datenschutzverordnung.
1.1.3	28.02.2023	Dario Quattrocchi	Kapitel 7.11 Ergänzung zur Weiterleitung von E-Mails an externe E-Mail-Adressen.
1.2	08.03.2023	ISB	Vernehmlassung durch ISB
1.2	27.06.2023	Group CISO	Freigabe nach Vernehmlassung TA erfolgt
1.3	06.03.2024	Thomas Haas	Präzisierungen von Formulierungen innerhalb der Kapitel 7.4, 7.5, 7.11 sowie 9.3.
1.3	13.03.2024	Group CISO	Freigabe der Präzisierungen

Inhaltsverzeichnis

1. Einführung

Die Migros verpflichtet sich dazu, eine sichere Umgebung für Ihre Mitarbeitende, Informationen und Vermögenswerte zu schaffen. Hierbei müssen alle Informationen, welche von Kunden, Partnern und Drittparteien stammen, adäquat geschützt werden. Die Migros setzt auf Branchenstandards und auf einen risikobasierten Ansatz zur Umsetzung von Sicherheitskontrollen und Massnahmen.

2. Inhalte und Ziele

Ziel dieses IT-Nutzungsreglements ist die Definition allgemeiner Prinzipien, um:

- die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Vermögenswerten zu wahren.
- alle Vermögenswerte vor Bedrohungen – ob intern oder extern, absichtlich oder versehentlich – anhand eines risikobasierten Ansatzes zu schützen.
- sicherzustellen, dass gesetzliche, behördliche, betriebliche und vertragliche Anforderungen erfüllt werden.

Das IT-Nutzungsreglement gliedert sich in ein Hauptdokument und Anhänge. Im Hauptdokument sind Prinzipien definiert. Die Inhalte des Hauptdokuments haben direkten Einfluss auf das Handeln der Mitarbeitenden und beschreiben, was beim Umgang mit IT-Mitteln (jegliche Hard- und Software) sowie beim Umgang mit Daten zu beachten ist. Weiterführende Themen, Erklärungen oder Präzisierungen zu den Prinzipien im Hauptdokument sind in den Anhängen zu finden.

Unter IT-Mitteln wird im IT-Nutzungsreglement jegliche Hard- uns Software umschrieben. Hierbei zählt z.B. der Laptop, das Mobiltelefon aber auch ein Server, ein Netzwerk-Gerät ein Router, Office, Word, SAP sowie der darin gespeicherten Daten.

3. Geltungsbereich

Das IT-Nutzungsreglement als Teil des Migros Security Regelwerks gilt für Mitarbeitenden der gesamten Migros im Rahmen der Nationalen Information Security Governance, d.h. für alle internen und externen Mitarbeitenden aller Unternehmen der Migros Gemeinschaft ohne die Migros Bank. Dritte, welche von der Migros bereitgestellte oder betriebene Arbeitsmittel, Services und Dienstleistungen verwenden, sind ebenfalls verpflichtet, das Nutzungsreglement einzuhalten. Als Unternehmen der Migros gelten im Sinne dieses IT-Nutzungsreglements alle Migros Genossenschaften und der Migros-Genossenschafts-Bund sowie alle von diesen einzeln oder gemeinsam, direkt oder indirekt kontrollierten Unternehmen sowie die Migros-Stiftungen.

3.1 Migros-weite und unternehmensspezifische Weisungen

Gesellschaften innerhalb der Migros können das Migros-weite IT-Nutzungsreglement (in diesem Kontext auch «Migros-weite Weisung» genannt) verschärfen und präzisieren im Rahmen einer unternehmensspezifischen Weisung. Bei Widerspruch einer unternehmensspezifischen Weisung zur Migros-weiten Weisung, hält die Migros-weite Weisung Gültigkeit und wird höher gewichtet.

3.2 Eingliederung in das Migros Security Regelwerk

Das IT-Nutzungsreglement ist Teil des Migros Security Regelwerks. Das Migros Security Regelwerk ist unter isms.migros.net hinterlegt. Das Migros Security Regelwerk stellt eine Sammlung von Dokumenten dar, welche verbindliche Prinzipien, Anforderungen, Prozeduren und Standards für die Informationssicherheit definiert. Alle publizierten Dokumente im Regelwerk sind unter isms.migros.net zu finden. Das IT-Nutzungsreglement ist vom Dokumenttyp «Weisung».

4. Überprüfung, Aktualisierung und Pflege

Das IT-Nutzungsreglement wird mindestens jährlich überarbeitet. Es kann zum Schutz der Migros nach Bedarf durch den Group CISO der Migros abgeändert werden, wenn neue Bedrohungen oder Schwachstellen erkannt werden, oder sich das Risikoprofil des Unternehmens wandelt.

5. Ausnahmen

Ausnahmen von diesem IT-Nutzungsreglement sind unter bestimmten Umständen möglich, z.B. Unmöglichkeit, den Vorgaben aufgrund lokaler Gegebenheiten nachzukommen.

6. Durchsetzung

Wird ein Verstoss oder ein konkreter Verdacht eines Verstosses gegen dieses Nutzungsreglements festgestellt, so können folgende Massnahmen angeordnet werden:

- Vorsorgliche Sperrung des Zugangs zu Arbeitsmitteln, die davon betroffen sind, z.B. Sperrung des entsprechenden Benutzerkontos
- Blockierung missbräuchlicher und rechtswidriger Daten sowie deren Sicherung und Aufbewahrung zu Beweiszwecken
- Löschung missbräuchlicher und rechtswidriger Daten, soweit dies aus Sicherheitsgründen erforderlich ist und einer Beweissicherung aus rechtlicher Sicht nicht entgegensteht

Ein weisungswidriges oder widerrechtliches Verhalten von Mitarbeitenden stellt einen Verstoss von arbeitsrechtlichen Pflichten dar und kann arbeitsrechtliche Disziplinarmassnahmen (einschliesslich Entlassung), zivil- und/oder strafrechtliche Konsequenzen sowie Schadenersatzansprüche zur Folge haben. Bei begründetem Verdacht auf eine strafbare Handlung (z.B. Kinderpornographie, Rassismus, etc.) kann Anzeige bei der zuständigen Behörde erstattet werden. Die durch ein weisungswidriges
oder widerrechtliches Verhalten verursachten Verluste, Schäden und Kosten, einschliesslich Aufklärung,- Untersuchungs-, Gerichts-, Anwalts- und Sanktionierungskosten können den fehlbaren Mitarbeitenden überwälzt werden.

7. Umgang mit Migros IT-Mitteln

Den Mitarbeitenden werden für den geschäftlichen Gebrauch u.a. IT-Mittel zur Verfügung gestellt. Die Nutzung dieser IT-Mittel steht grundsätzlich in der Eigenverantwortung der Mitarbeitenden. Sie tragen die Verantwortung für einen sicheren und sorgfältigen Umgang mit diesen IT-Mitteln.

7.1 Verbotene Handlungen

Die folgenden Handlungen sind verboten:

- Das Verlassen der Arbeitsstation ohne Bildschirmsperren oder Abmelden des Benutzers.
- Jede unbefugte Nutzung von IT-Mitteln, Migros-, Kunden- und/oder Partnerinformationen.
- Die absichtliche oder fahrlässige Teilnahme an Aktivitäten, welche die Informationssicherheit, die IT-Mittel oder Netzwerke von der Migros, ihrer Partner oder Kunden gefährden.
- Die Verletzung der Rechte des geistigen Eigentums einer Person oder eines Unternehmens.
- Unbefugte Versuche, die Sicherheitskonfiguration eines Migros IT-Mittels zu verändern oder die Sicherheitseinschränkungen zu umgehen oder zu deaktivieren, um sich Zugriff auf geschützte Informationen oder Bereiche zu verschaffen.
- Die Verwendung von Migros IT-Mitteln, um anstössige Inhalte herunterzuladen, zu speichern, zu übermitteln oder zu verbreiten / verteilen. Anstössige Inhalte sind u. a.

pornographische, beleidigende, diskriminierende, rassistische oder diffamierende Materialien.

- Die Verwendung von Migros IT-Mitteln, um illegale, urheberrechtlich geschützte oder nicht lizenzierte Software, Informationen, Musik oder andere Multimediadateien zu erstellen, herunterzuladen, zu speichern, zu verkaufen, zu verteilen, zu kopieren oder auszutauschen.
- Das vorsätzliche oder grobfahrlässige, unbefugte Löschen oder Vernichten von Migros-Informationen, Kommunikationen oder Datensätzen.
- Die Verwendung jeder Art von Tools, Anwendungen und Geräten oder Exploits (Ausnutzung von Schwachstellen), um der Migros Schaden zuzufügen.
- Das Speichern, Ausführen oder Verbreiten von jeglicher Schadsoftware.
- Der Einsatz von privaten Konten bei freigegebenen Cloud Services (z.B. privates Microsoft 365 Konto)

7.2 Private Nutzung von Migros IT-Mitteln

Migros-Endbenutzergeräte und Kommunikationseinrichtungen dürfen zur privaten Nutzung eingeschränkt verwendet werden. Die private Nutzung von Migros IT-Mitteln gilt nicht als Arbeitszeit.

Es existieren folgende Einschränkungen beim privaten Gebrauch von Migros IT-Mittel:

- Private Dateien dürfen nicht auf Migros Systemen gespeichert werden.
- Jegliche private Nutzung von Migros Geräten darf sich nicht negativ auf die Produktivität des Mitarbeitenden und die Systemverfügbarkeit auswirken.
- Die private Nutzung dieser Geräte und Technologien unterliegt den gleichen Vorschriften wie die geschäftliche Nutzung.
- Die private Nutzung von Migros IT-Mitteln, die primär für die Verarbeitung, die Massenspeicherung und den Austausch von Migros Informationen und Daten eingesetzt werden (z.B. Server, Netzwerkkomponenten, IoT Geräte), ist nicht erlaubt.

7.3 Herunterladen, Installieren und Nutzen von Software oder Cloud-Services

Sämtliche Softwareprogramme und Anwendungen auf Migros IT-Mitteln müssen über die offizielle IT-Stelle (z. B. Migros Group IT) bezogen und entsprechend für eine geschäftliche Nutzung lizenziert werden. Die Installation bzw. Nutzung von Anwendungs-Software oder Cloud Services, die nicht von der Migros Group IT oder dem jeweiligen M-Unternehmen freigegeben wurden, ist verboten.

7.4 Schutz von Migros IT-Mitteln

Migros IT-Mittel sind von Mitarbeitenden mit der nötigen Sorgfalt gegen Diebstahl und Beschädigung zu schützen (am Arbeitsplatz, unterwegs und zu Hause). Mitarbeitende müssen sicherstellen, dass der Bildschirm beim Verlassen der Arbeitsstation gesperrt, und mindestens ein Passwort für die Weiterarbeit benötigt wird. Gleiches gilt für private IT-Mittel, wenn diese geschäftlichen Daten enthalten bzw. solche darauf gespeichert oder abgerufen werden können, siehe hierzu auch Kapitel 8.1. Der Verlust eines Gerätes ist umgehend dem/der jeweiligen Servicedesk/Hotline (im MGB z.B. über IT Self-Service-Portal) zu melden.

7.5 Tragen des Firmen Badge

Die Identifikation von Mitarbeitenden innerhalb von Gebäuden / Räumlichkeiten oder Arealen der Migros erfolgt durch den persönlichen Firmen Badge. Der persönliche Firmen Badge ist innerhalb von Gebäuden / Räumlichkeiten oder auf einem Areal der Migros sichtbar zu tragen. Ausnahmen bilden speziell gekennzeichnete Räumlichkeiten (z.B. hygienische Produktion) oder falls für die Mitarbeitenden einer M-Genossenschaft oder eines M-Unternehmens andere Zutrittsmechanismen (z.B. «Schlüsselanhänger»-Badge) existieren.

7.6 Clean-Desk Policy

Beim Verlassen des Arbeitsplatzes muss folgendes sichergestellt werden:

- Alle Dokumente / Datenträger mit vertraulichen und sensitiven Geschäftsinformationen müssen beim Verlassen des Arbeitsplatzes vom Schreibtisch entfernt werden. Dazu gehören unter anderem: USB-Sticks, Visitenkarten und gedruckte Dokumente.
- Der Computer / das Notebook ist zu sperren beim Verlassen des Arbeitsplatzes.
- Falls eine Aufbewahrung nötig ist, müssen sensible und vertrauliche Dokumente sicher und verschlossen verstaut werden (z.B. in einem abgeschlossenen Kasten/Spind).
  Falls eine Aufbewahrung nicht notwendig ist, müssen die Dokumente unverzüglich auf sichere Weise vernichtet werden (z.B. mit dem Schredder oder Reisswolf). Jeglicher Papiermüll, der sensible oder vertrauliche Informationen enthält, muss in den dafür bereitgestellten Shreddern entsorgt werden. Unter keinen Umständen sollten solche Daten in den üblichen Müll gelangen.

7.7 Umgang mit Drucker und Kopierer

Dokumente müssen, soweit vorhanden und möglich, über sicheres Drucken in den Geschäftsräumen ausgedruckt werden. Alle ausgedruckten Dokumente müssen umgehend vom Drucker entfernt werden. Werden bei einem Drucker Dokumente mit vertraulichem oder geheimem Inhalt gefunden, sind diese umgehend dem Urheber auszuhändigen oder zu vernichten.

7.8 Meldung von Notfällen

Die Migros Gruppe betreibt verschiedene lokale und eine für den Genossenschaftsbund zentrale Serviceinfrastruktur (jeweiliger Servicedesk oder jeweilige Hotline: im MGB z.B. über IT Self-Service-Portal). Tritt im Umgang mit IT-Mittel ein Notfall auf, muss dieser sofort gemeldet werden. Das kann ein Service Desk im Unternehmen sein, oder derjenige im Migros-Genossenschafts-Bund (IT Self-Service-Portal).

Verdächtige technische Zwischenfälle (z.B. mögliche Infektion eines Computers durch Viren, Phishing, Hacking, usw.) sind umgehend, d.h. sofort bei Verdachtsfeststellung, an den jeweiligen Servicedesk oder an die zentrale Security-Hotline security@migros.ch zu melden.

7.9 Sicherheit ausserhalb von Unternehmensräumlichkeiten

Reisende Mitarbeitende achten auf folgende Punkte:

- An öffentlichen Orten (an Flughäfen und Bahnhöfen, im Restaurant, im Park, im Zug und anderen dicht bevölkerten Orten) ist besondere Vorsicht geboten, wenn vertrauliche

Informationen diskutiert werden. Geheime Informationen dürfen nicht in der Öffentlichkeit besprochen werden.

- Beim Arbeiten mit dem Notebook sollen keine vertraulichen oder geheimen Informationen von Dritten eingesehen werden können. Bei Bedarf kann über die IT ein entsprechender Sichtschutz (Privacy Filter) organisiert werden.
- Werden Verbindungen zu öffentlichen oder privaten WLANS hergestellt, muss der Datenaustausch mittels einer vertrauensvollen Verbindung (z.B. VPN) geschützt werden.

7.10 Internetnutzung

Das Internet dient den Mitarbeitenden der Migros für die Informationsbeschaffung, den Austausch von Daten und Dokumenten mit Geschäftspartnern, Kunden, Behörden und weiteren Stellen unter Berücksichtigung der Informationssicherheitsanforderungen, sowie für die Beschaffung von Dienstleistungen und Waren unter Berücksichtigung der gültigen Unterschriftenregelungen. Die Mitarbeitenden der Migros haben das Internet auf eine Weise zu benützen, die Migros vor rechtlichen, regulatorischen und operationellen Risiken sowie Risiken für den Ruf der Migros schützt. Die private Nutzung des Internets ist während der Arbeitszeit auf ein Minimum zu beschränken.

Jede widerrechtliche oder unangemessene Benutzung des Internets ist verboten. Hierzu zählen u.a.:

- Zugriffe auf jegliche Art von Spielseiten (z.B. Glücksspielen) oder privater Börsenhandel
- Aufruf von Webseiten mit anstössigem oder gesetzwidrigem Inhalt

7.11 E-Mail

Eine persönliche Mailbox darf nur vom jeweiligen Mitarbeitenden benutzt werden. Wichtige, geschäftliche E-Mails, welche für andere Personen einsehbar sein müssen, sind an vereinbarten Orten in den dafür vorgesehenen Datenspeichern abzuspeichern.

Das automatische Um- oder Weiterleiten an externe oder interne E-Mail-Adressen ist grundsätzlich verboten. Bei spezifischen Anwendungsfällen kann eine externe oder interne Weiterleitung eingerichtet werden, diese bedarf allerdings einer Ausnahmebewilligung (Exception-to-Policy). Hierbei gilt:

Die automatische Weiterleitung von E-Mails darf einzig von einer internen, persönlichen E-Mail-Adresse auf eine einzige, direkt zur Person zugehörige persönliche E-Mail-Adresse eingerichtet werden.

Verboten ist die automatische E-Mail-Weiterleitung:

1) von einer Funktions-/Sammel-Mail-Adresse an externe
2) von einer internen zu mehreren externen
3) von einer internen zu Personen ohne Vertragsbeziehung mit M-Unternehmen

Mitarbeitende sind verpflichtet, bei Abwesenheiten oder Austritt eine Abwesenheitsmeldung einzurichten. Sollen die Maileingänge durch eine Stellvertretung geführt werden, so erfolgt dies nach vorgängiger bilateraler Absprache. Bei besonderen Umständen (z. B. Krankheit des Mitarbeitenden) behält sich die Migros das Recht vor, eine Abwesenheitsmeldung unter Berücksichtigung der Datenschutzaspekte einzurichten.

Vorsicht ist geboten bei Mails mit zweifelhaftem Absender oder merkwürdigen Formulierungen in der Betreffzeile sowie generell merkwürdiger Formulierung im Text. Solche Mails sind umgehend zu löschen. Falls im E-Mail-Programm (z.B. Outlook) ein Meldebutton für Spam/Fishing-Mails existiert, soll ein verdächtiges E-Mail mittels Anklickens desselben gemeldet werden. Bei solchen Mails dürfen aus Sicherheitsgründen Anhänge nicht geöffnet und Links nicht angeklickt werden.

Geschäftsbezogene elektronische Daten und Dokumente von Mitarbeitenden können im Rahmen einer internen Untersuchung gesichert und durchsucht werden. Deshalb werden alle Outlook-Elemente (E-Mails, Kalender-Einträge, Aufgaben, Teams-Chats und Kontakte) während 10 Jahren zweckgebunden und zugriffsgesichert aufbewahrt.

8. Umgang mit privaten IT-Mitteln

8.1 Geschäftliche Nutzung von privaten IT-Mitteln

Private IT-Mittel (z.B. das eigene Smartphone) dürfen für geschäftliche Zwecke verwendet werden. Der Mitarbeitende hat keine Ansprüche auf Support oder Unterstützung zu privaten Arbeitsmitteln. Die M-Unternehmen können abweichende Regelungen betreffend Entschädigung sowie Support- und Installationsleistungen vorsehen.

Private IT-Mittel dürfen ausschliesslich in das dafür vorgesehene Netzwerk der Migros Gruppe angeschlossen werden. Der Benutzer ist in der Verantwortung die Sicherheit der privaten IT-Mittel sicherzustellen. Geschäftliche Daten, welche lokal auf dem Gerät abgelegt sind, müssen nach Gebrauch umgehend gelöscht werden.

Private IT-Mittel müssen, wenn sie für geschäftliche Zwecke genutzt werden, durch einen Passwort-Schutz oder einen biometrischen Schutz sowie Verschlüsselung des Speichers gegen unberechtigten Zugang geschützt werden. Updates von Software (d.h. Betriebssystemen, Applikationen, Apps, etc.) sollen vorgenommen werden, sobald diese vom Software-Hersteller bereitgestellt werden.

Bei privaten IT-Mittel (z.B. Laptop oder Tablet) muss beim Zugriff auf Daten innerhalb des Migros-Netzwerks sichergestellt werden, dass der Verbindungsaufbau in das Netzwerk der Migros mittels einer vertrauensvollen Verbindung (z.B. VPN) sowie einer Multi-Faktor-Authentisierung durchgeführt wird. Hiervon ausgenommen ist die blosse Verwendung von Exchange Funktionalitäten mit privaten IT-Mitteln (z.B das eigene Smartphone), sofern dies über eine von dem Migros-Unternehmen erlaubte Methode (z.B. Active Sync, Outlook App) erfolgt.

9. Umgang mit Migros Daten

9.1 Datenklassifizierung

Im Kontext dieses IT-Nutzungsreglements werden geschäftliche Daten in folgende grundsätzliche Klassen gegliedert:

- Öffentliche Daten: Die Daten sind für alle einsehbar.
- Interne Daten: Die Daten sind für alle Mitarbeitenden der Migros einsehbar.
- Vertrauliche Daten: Die Daten sind für einen eingeschränkten Kreis von Mitarbeitenden der Migros einsehbar und besitzen einen erhöhten Schutzbedarf. Es gibt Einschränkungen der Berechtigung auf eine bestimmte Gruppe und die Daten müssen mit erhöhter Sorgfalt behandelt werden. Beispiele sind Personen- oder Finanzdaten.
- Geheime Daten: Die Daten sind nur einem kleinen, namentlich bekannten Kreis von Personen zugänglich und werden umfassend geschützt. Die Daten werden einzeln verschlüsselt auf Datei-Ebene. Beispiele von geheimen Daten sind Informationen über grosse M&A Transaktionen.

Neben den Klassen für Geschäftsdaten gibt es private Daten, welche nicht gesondert technisch gehandhabt werden. Bei Daten der Nutzenden/Mitarbeitenden, die in keinem direkten Zusammenhang

zur Migros stehen, besteht die widerlegbare Vermutung, dass es sich um private Daten handelt. Private Daten dürfen nicht auf Migros Systemen gespeichert werden.

9.2 Umgang mit Daten

Die Mitarbeitenden sollen mit Daten/Informationen verantwortungsvoll umgehen.

Daten/Informationen sind gewissenhaft und sorgfältig zu behandeln, nur denjenigen Personen bekannt zu geben oder zugänglich zu machen, welche diese für die Erfüllung ihrer Funktion und Aufgaben benötigen, jederzeit angemessen zu schützen und dürfen nur in Übereinstimmung mit anwendbaren gesetzlichen Vorschriften sowie anwendbaren internen Regelwerken verwendet werden.

Die Mitarbeitenden sind verpflichtet, in ihrem Einflussbereich für die Einhaltung der anwendbaren gesetzlichen Vorschriften sowie anwendbaren internen Regelwerken zu sorgen.

Bei der Bearbeitung von Personendaten gelten insbesondere die Richtlinie zum Datenschutz sowie weitere Datenschutzanforderungen gemäss Legal & Compliance MGB.

Geschäftsdaten werden ausschliesslich auf den von der Migros oder in ihrem Auftrag bereitgestellten und freigegebenen Speichertechnologien gespeichert. Werden gemäss Kapitel 8.1 private IT-Mittel eingesetzt, so muss die Löschung der Daten auf dem privaten Gerät nach dem Gebrauch umgehend durch den Mitarbeitenden sichergestellt werden.

Vor Austritt eines Mitarbeitenden ist die persönliche Datenablage zu bereinigen. Dabei sind private Daten zu löschen und die restlichen Daten in Absprache mit dem Vorgesetzten zu verschieben. Nach dem Austrittstermin ist der Zugriff auf persönliche Datenablagen gesperrt.

Für jeden Speicherort ist ein Verzeichnisverantwortlicher zu definieren. Er ist verantwortlich für die erstmalige Definition der Zugriffsberechtigten sowie für deren laufende Mutationen im Betrieb.

Nicht öffentliche Geschäftsdaten dürfen nur verschlüsselt auf Memory-Sticks und externen Datenträgern (z.B. CD, DVD, Memory-Sticks, externen Festplatten / USB-Harddisks und ähnliches) abgelegt werden. Nach Verwendung der Daten sind diese wieder vom Memory-Stick zu löschen. CDs und DVDs mit Geschäftsdaten sind nach Gebrauch sicher zu entsorgen.

9.3 Umgang mit Passwörtern

Anmeldungen an den Migros IT-Mitteln sind ausschliesslich mit der persönlichen Benutzer ID und dem persönlichen Passwort vorzunehmen (Ausnahmen bilden hier die Verwendung von generischen Benutzerkonten in bestimmten Ausnahmefällen z.B. bei den Filialen). Des Weiteren ist es verboten, sich mit dem Account eines anderen Mitarbeitenden an einem System oder Applikationen anzumelden. Es gelten die nachfolgenden Passwortregeln:

- Das Passwort, der Login und die Zertifikate sind persönlich und gegenüber Dritten geheim zu halten. Es ist somit verboten, sein persönliches Passwort jemand anderem mitzuteilen oder zugänglich zu machen. Passwörter und PINs dürfen nicht aufgeschrieben werden, ausser sie werden sicher verschlossen (z.B. in einem Couvert in einem Safe) aufbewahrt.
- Das Passwort muss mindestens die Anforderungen des Passwort-Standards (siehe MSS001, Abschnitt «Verbotene Passwörter») erfüllen.
- Das Passwort darf nicht leicht zu erraten sein. Das heisst, es darf beispielsweise nicht die Benutzer ID, den Organisationsnamen, andere persönliche Informationen, Telefonnummern, gängige Passwörter (z.B. «Passw0rt», «Pass1234», etc.) enthalten.

- Passwörter, welche in der Migros Gruppe verwendet werden, dürfen nicht bei anderen Institutionen und Migros externen Anwendungen verwendet werden (z.B. bei privaten E-Mail Accounts, bei externen Webportalen, etc.).
- Innerhalb der Migros Gruppe darf dasselbe Passwort mehrmals verwendet werden, solange man es in derselben Rolle braucht.
- Wenn der Verdacht besteht, dass ein Passwort Dritten bekannt geworden ist, sind Mitarbeitende verpflichtet, das Passwort sofort zu ändern.
- Wird ein Passwort gewechselt, darf es nicht einem vorher bereits verwendeten Passwort entsprechen.
- Passwörter dürfen nicht im Klartext übertragen werden (z.B.: in einem E-Mail)
- Passwörter dürfen nur unbeobachtet eingegeben werden.
- Initialpasswörter müssen zwingend nach der ersten Anmeldung geändert werden.
- Voreingestellte Passwörter und Benutzer-IDs, z. B. des Herstellers bei Auslieferung von IT-Mitteln, müssen vor der produktiven Inbetriebnahme des Systems oder Gerätes durch individuelle Passwörter und, wenn möglich, Benutzer-ID ersetzt werden.
- Jede und jeder Mitarbeitende sind für alle unter ihrer Benutzer-ID ausgelösten Transaktionen verantwortlich.
- Ein Remotezugriff zwecks Support muss beim Verbindungsaufbau zwingend durch den Benutzer bestätigt werden. Während einer Remotesession sind die Tätigkeiten des Supporters zu überwachen und nach Abschluss der Arbeiten auch die korrekte Abmeldung der Remotesession sicherzustellen.

9.4 Protokollierung und Auswertung von elektronischen Daten

Die Migros kann insbesondere zur Aufrechterhaltung des Betriebes, der Sicherheit, der Integrität und Verfügbarkeit von IT-Mitteln, Daten/Informationen zur Gewährleistung der Dienstleistungsqualität, zur Einhaltung und Kontrolle der anwendbaren gesetzlichen Vorschriften und/oder internen Regelwerken, zur Kontrolle der Einhaltung von Lizenzbedingungen, zu Abrechnungszwecken und zur Kostenkontrolle sowie zur Ermittlung und Behebung von Betriebsstörungen oder Missbräuchen Systeme einsetzen, die Protokolle und Warnmeldungen erzeugen.

Die Mitarbeitenden sind sich bewusst, dass die Migros Daten über die Nutzung von IT-Mitteln, insbes. Verkehrs- und Logdaten aus der Nutzung von Internet oder E-Mail, vergleichbare Angaben über ausgehende oder eingehende Telefonanrufe sowie Logdaten betr. Dateizugriffe/-mutationen/-löschungen aufzeichnet und über generelle Nutzerdaten aller Konten verfügt und diese zu den genannten Zwecken auswerten kann. Die Auswertung erfolgt grundsätzlich in anonymisierter oder pseudonymisierter Form.

Bei entsprechenden Vorfällen oder schwerwiegenden Verdachtsfällen können in Absprache mit der Personalabteilung und Legal & Compliance, unter Einhaltung des Grundsatzes der Verhältnismässigkeit, Daten personenbezogen ausgewertet oder zusätzliche Aufzeichnungen durchgeführt werden. Für weiterführende Informationen zur Sicherung sowie Durchsicht von Daten und Dokumenten wird auf die Richtlinie betreffend Meldung und interne Untersuchungen verwiesen.

Die Daten werden in personenbezogener Form gespeichert, solange es für den konkreten Zweck, für den sie erhoben wurden, erforderlich ist oder ein berechtigtes Interesse an der Speicherung besteht. Das kann insbesondere dann der Fall sein, wenn Personendaten benötigt werden, um Ansprüche durchzusetzen oder abzuwehren, aus Beweisgründen, zu Archivierungszwecken und zur Gewährleistung der IT-Sicherheit. Die aufgezeichneten Daten werden zudem in personenbezogener Form gespeichert, solange sie einer gesetzlichen Aufbewahrungspflicht unterliegen oder ein anderer nach anwendbarem Recht gültiger Ausnahmegrund besteht. Für bestimmte Daten gilt z.B. eine

zehnjährige Aufbewahrungsfrist. Für andere Daten gelten jeweils kürzere Aufbewahrungsfristen, zum Beispiel für Aufzeichnungen bestimmter Vorgänge im Internet (Log-Daten).

10. Weiterführende Dokumente

Neben den allgemeinen Bestimmungen zur Einhaltung der Informationssicherheit gibt es weiterführende Regelungen, die für alle Mitarbeitende Gültigkeit haben. Neben allen Leitlinien, Weisungen, Richtlinien, Standards und Bestimmungen gelten auch alle Anhänge zum IT-Nutzungsreglement für alle Mitarbeitenden der Migros als verbindlich. Alle Dokumente liegen unter isms.migros.net vor.

Weitere Dokumente von Legal & Compliance sind im Intranet zu finden. Relevante Dokumente von Seiten HR werden hier publiziert.

Weitere Informationen zur Bearbeitung von Personendaten sind in der Datenschutzerklärung für Mitarbeitende zu finden.