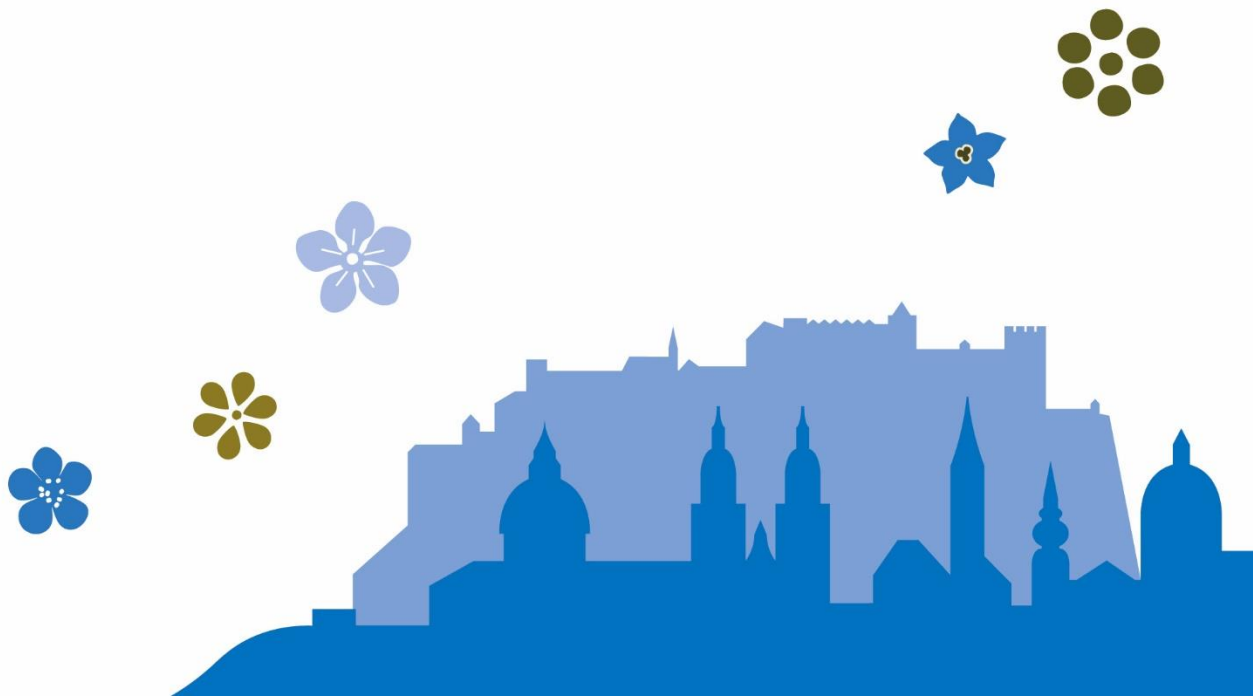
SalzburgMilch

LEITLINIE FÜR IT-NUTZER DER SALZBURGMILCH GMBH

VERSION 1.0 • STAND 01.02.2025



1. FORMELLE ANFORDERUNGEN AN DIE LEITLINIE

1.1. Ziel und Zweck

1.1.1. Die Leitlinie für IT-Nutzer der SalzburgMilch GmbH (in der Folge kurz „Leitlinie“) dient als interner Mitarbeiterleitfaden hinsichtlich der Nutzung von bereitgestellter IT-Hard- und Software und stellt ein verbindliches Regelwerk für sämtliche Beschäftigte dar. Die Leitlinie soll insbesondere Bewusstsein für potenzielle Sicherheitsrisiken schaffen, Kontaktpersonen benennen und klare Handlungsanweisungen geben. Damit soll die interne Aufrechterhaltung der IT-Sicherheit und Prävention von Fällen der Cyberkriminalität gewährleistet werden.

1.1.2. Für eine bessere Lesbarkeit dieses Dokuments wird ausschließlich die männliche Form verwendet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

1.2. Rechtlicher Rahmen

Die Leitlinie basiert auf den geltenden österreichischen und europäischen Datenschutzbestimmungen, insbesondere der Datenschutzgrundverordnung (DSGVO) und dem österreichischen Datenschutzgesetz (DSG). Die Leitlinie stützt sich weiters auf die geltenden Bestimmungen des Arbeitnehmerschutz- und Betriebsverfassungsrechts sowie einschlägigen Grundrechten, insbesondere aus der Grundrechtecharta (GRC). Darüber hinaus basiert diese Leitlinie auf den OECD-Leitsätzen für multinationale Unternehmen zu verantwortungsvollem unternehmerischem Handeln.

1.3. Organisatorischer und zeitlicher Geltungsbereich der Leitlinie

Die Leitlinie ist für sämtliche Mitarbeiter der SalzburgMilch GmbH verbindlich. Es gilt immer die aktuelle Version der Leitlinie. Für Sachverhalte, die die Heranziehung einer früheren Version der Leitlinie notwendig machen, ist die für diesen Zeitraum geltende Leitlinie heranzuziehen.

1.4. Erstellung, Erlass und Aktualisierung der Leitlinie

1.4.1. Die Leitlinie wurde erstmals durch die IT-Abteilung in Abstimmung mit der Abteilung Compliance erstellt und nach erfolgter schriftlicher Genehmigung durch einen Prokuristen und die Geschäftsführung erstmals durch IT-Abteilung erlassen. Die Leitlinie wird regelmäßig, zumindest einmal jährlich, durch die IT-Abteilung in Abstimmung mit der Abteilung Compliance auf deren Aktualität hin geprüft.

1.4.2. Sollte eine weitreichende inhaltliche Änderung der Leitlinie (z.B. im Fall einer gänzlich neuen Formulierung wesentlicher für die Leitlinie relevanter Bestandteile) notwendig sein, wird die neue Version der Leitlinie durch die IT-Abteilung in Abstimmung mit der Abteilung Compliance erstellt und nach Freigabe durch einen Prokuristen und die Geschäftsführung erlassen. In diesem Fall ist eine neue Versionsnummer zu vergeben. Die schriftliche Freigabe wird durch die Abteilung Compliance archiviert. Redaktionelle Änderungen an der Leitlinie, worunter auch geringfügige inhaltliche Änderungen an der Leitlinie zu verstehen sind, sind durch die IT-Abteilung ohne Freigabe durch die Geschäftsführung bzw. ohne weitere Abstimmung mit der Abteilung Compliance möglich und wird in diesem Fall lediglich eine neue Subversionsnummer vergeben.

1.5. Verteilung und Abrufbarkeit der Leitlinie

Die Leitlinie wird nach erfolgter Genehmigung bzw. im Fall der Änderung nach Kapitel 1.4.2. eigenständig durch die IT-Abteilung / Abteilung Compliance am Laufwerk Z: (Ordner „Policies“) bereitgestellt und an alle verantwortlichen Heads ausgeschickt.

1.6. Verantwortung und Rückfragemöglichkeit

Die inhaltliche Verantwortung der Leitlinie obliegt der IT-Abteilung. Die organisatorische Verantwortung obliegt der Abteilung Compliance. Für allfällige Rückfragen zur Auslegung einzelner Bestimmungen aus oder im Zusammenhang mit der Leitlinie steht die IT-Abteilung zur Verfügung.

2. EINFÜHRUNG

2.1. Informationstechnologie (IT) wird in immer mehr Geschäftsprozessen der SalzburgMilch GmbH in praktisch allen funktionalen Bereichen eingesetzt. IT ist sowohl auf Verwaltungs-, als auch Produktionsebene bei der Durchführung vieler Aufgaben behilflich. Die Effizienz und wirtschaftliche Realisierbarkeit von vielen Prozessen ist heute zur Gänze von der IT abhängig.

2.2. Um sicherzustellen, dass alle IT-Systeme effizient funktionieren und um die Mitarbeiter in die Lage zu versetzen, die Arbeit ordnungsgemäß durchzuführen und externe Anforderungen, wie sie von gesetzlichen Regelungen und anderen Verpflichtungen (Risikomanagement) vorgegeben sind, zu erfüllen, muss die SalzburgMilch die Nutzung von IT-Ressourcen (IT-Hardware,

-Software und -Dienstleistungen), die den Mitarbeitern zur Verfügung gestellt werden, bestimmten Richtlinien unterwerfen. Diese Richtlinien sind Gegenstand dieses Dokuments.

3. UMSETZUNG DIESER LEITLINIE

3.1. Diese Leitlinie stellt eine verpflichtende Referenz für jeden Mitarbeiter dar, der in der SalzburgMilch GmbH tätig ist. Das heißt jeder, der IT-Ressourcen benutzt, ist verpflichtet, diese IT-Richtlinien einzuhalten; leitende Führungskräfte und Heads sind im Rahmen ihrer Aufsichtsführung für deren Umsetzung in der Praxis verantwortlich.

3.2. Die IT-Abteilung ist über jeden Verstoß gegen die Bestimmungen dieser Leitlinie in Kenntnis zu setzen.

3.3. Die Nichteinhaltung von Bestimmungen dieser IT-Richtlinien kann zu einer Einschränkung der Nutzung von IT-Ressourcen, zu deren zeitweiligem Verbot oder auch dazu führen, dass dem Zuwiderhandelnden deren Nutzung vollständig untersagt wird.

3.4. Jeder Mitarbeiter ist im Rahmen seiner arbeitsrechtlichen Treuepflicht der SalzburgMilch gegenüber zur Wahrung der Vorgaben dieser Leitlinie verpflichtet. Es wird darauf hingewiesen, dass Verhalten entgegen den Bestimmungen dieser Leitlinie sowie darüberhinausgehendes (straf-)rechtlich relevantes Verhalten für Mitarbeiter arbeitsrechtliche Folgen (bis hin zur Entlassung) hat. Die SalzburgMilch behält sich darüber hinaus ausdrücklich vor, gegebenenfalls zivil- / strafrechtliche Schritte einzuleiten.

4. ALLGEMEINE RICHTLINIEN BEI DER NUTZUNG VON IT-RESSOURCEN

4.1. Allgemeine Richtlinien

4.1.1. **Geschäftliche Nutzung**: Im Allgemeinen sind alle IT-Systeme des Unternehmens nur für eine geschäftliche Nutzung vorgesehen.

4.1.2. **Verbot der Nutzung Dritter**: Die Nutzung firmeneigener IT-Ressourcen durch nicht befugte Dritte ist grundsätzlich verboten.

4.1.3. **Verbotene Inhalte**: Um einen Benutzerzugriff auf gefährliche Websites oder Webseiten mit sexuellen, rassistischen oder anderen unangemessenen Inhalten zu verhindern, kann die Internet-Nutzung durch spezielle IT-Technologien kontrolliert werden.

4.1.4. **Beschaffung von Hard- und Software**: Die IT-Abteilung oder in einer bestimmten Situation ausdrücklich autorisierte Personen sind die einzigen, denen es gestattet ist, IT-Hardware und -Software zu beschaffen und IT-Dienstleistungen in Auftrag zu geben. Die Beschaffung von IT-Hardware und -Software unterliegt den Anforderungen eines allgemeinen IT-Systemkonzepts der SalzburgMilch GmbH in Hinsicht auf die reibungslose Administration der gesamten Systemlandschaft. Eine wesentliche Konsequenz, die sich daraus ergibt, ist die, dass persönliche Wünsche nach spezieller IT-Ausstattung nicht berücksichtigt werden, wenn sie der standardisierten Strategie für die IT-Beschaffung nicht entsprechen.

4.1.5. **Freigabe von fremder Hard- und Software**: Die Installation und Nutzung von nicht freigegebener Hard- oder Software sowie Clouddiensten ist strengstens untersagt. Von der IT-Abteilung ist stets eine Nutzungsfreigabe einzuholen. Bereits erteilte Freigaben für andere Abteilungen oder Kollegen sind Einzelfallentscheidungen und nicht automatisch für alle Anwender gültig.

4.1.6. **Ausnahmen für die Nutzung von nicht freigegebener Hardware**: Der Datenaustausch über USB-Speichermedien aus vertrauenswürdigen Quellen (z. B. durch die IT gescannte USB-Memory-Sticks, die ausschließlich in Systemen der SalzburgMilch wiederverwendet werden) ist gestattet.

4.1.7. **Reparatur von Hardware**: IT-Hardware wird ausschließlich von der IT-Abteilung oder ihren autorisierten Partnern repariert.

4.1.8. **Verteilung und Veröffentlichung von geschützten / unternehmensinternen Daten**: Ohne die vorherige Genehmigung durch die IT-Abteilung dürfen IT-Systeme nicht für die Verteilung oder Veröffentlichung rechtlich geschützten Materials (z.B. urheberrechtlich geschützte Materialien, Patente, usw.) oder interner Unternehmensdaten (insbesondere firmenvertrauliches Material oder Geschäftsgeheimnisse) verwendet werden. Es ist zu beachten, dass auch die Nutzung einer Cloudsoftware bereits als Datenverteilung und -weitergabe gelten kann. Gleiches gilt für die Nutzung von KI-Programmen wie z.B. ChatGPT oder Co-Pilot.

4.1.9. **Umgang mit KI-Tools**: Der Einsatz von KI-Tools und KI-Programmen bedarf einer Datenschutzprüfung und Rücksprache mit der IT-Abteilung, sowie einer individuellen Unterweisung im Umgang mit den Tools. Des Weiteren müssen sich alle Mitglieder der Geschäftsleitung sowie Führungskräfte und Anwender von KI-Software und Tools regelmäßigen KI-Schulungen unterziehen.

4.1.10. **Dienstreisen und Homeoffice**: Es dürfen nur notwendige elektronische Geräte mitgenommen werden. Sicherheitsfunktionen

müssen vor Reiseantritt aktiviert werden (Verschlüsselung, Bildschirmsperre, keine Nutzung öffentlicher WLANs ohne VPN, Sichtschutz für Bildschirm, usw.). Für betrieblichen Zugriff dürfen ohne Notwendigkeit keine fremden Geräte genutzt werden (z.B. Webmailnutzung im Internet-Café). Alle gespeicherten Passwörter und sensible Daten müssen entfernt werden und für eine sichere Kommunikation ist ein VPN zu nutzen.

4.1.11. Bei der Nutzung von Firmengeräten im Home-Office gelten erhöhte Vorsichtsmaßnahmen, da die gewohnten Sicherheitsstandards wie bei Anwesenheit in den Betriebsstätten der SalzburgMilch im privaten Bereich (etwa in der Privatwohnung) in der Regel nicht eingehalten werden können. Es gilt daher erhöhte Vorsicht beim Klick auf Links, sowie dem Öffnen von unerwarteten E-Mails unbekannter Personen und / oder Unternehmen.

4.1.12. Alle IT- Arbeitsmittel und Arbeitsunterlagen sind so zu verwahren und zu nutzen, dass eine Einsicht oder ein Zugriff durch dritte Personen (einschließlich Haushaltsangehörige) ausgeschlossen ist. IT-Arbeitsmittel und Arbeitsunterlagen sind stets gesichert zu verwahren und zu transportieren.

4.1.13. **Schutz der Arbeitsgeräte**: Die Sicherheit des Arbeitsgeräts vor (physischen) Schäden jeglicher Art ist jederzeit zu gewährleisten; so ist dieses auch vor Dritten (z.B. Familienmitgliedern) zu schützen. Eine Nutzung durch Dritte ist ausdrücklich untersagt. Regelmäßige Updates der Geräte sind schnellstmöglich durchzuführen, hierzu erfolgt meist eine Aufforderung in Form einer Systemmeldung. Ebenfalls ist die Verwendung von Virenschutz und Firewall obligatorisch. Passwörter dürfen nicht in Textdateien oder Dokumenten gespeichert werden, ebenso dürfen diese nicht auf Zetteln notiert werden, da sich hierfür verschlüsselte Kennwortmanager besser eignen. Die IT-Abteilung stellt bei Bedarf die entsprechende Software und Einschulung bereit.

4.1.14. **Nutzung von Apps und Sprachassistenten**: Zur jeweiligen beruflichen Tätigkeit des Mitarbeiters nicht unbedingt notwendige APPs und Dienste wie Sprachassistenten sind aus Datenschutzgründen verpflichtend zu löschen bzw. zu deaktivieren. Für die Nutzung von zusätzlicher Software und APPs für berufliche Zwecke bedarf es einer ausdrücklichen schriftlichen Freigabe durch den Head und Rücksprache mit der IT-Abteilung, welche nach sorgfältiger Prüfung und Abwägung die letzte Entscheidung trifft.

4.1.15. **Bei Beendigung des Beschäftigungsverhältnisses**: Jeder Mitarbeiter, der das Unternehmen verlässt, ist verpflichtet, seinem Nachfolger und Vorgesetzten alle bis zu diesem Zeitpunkt gespeicherten firmeneigenen Daten verfügbar zu machen. Der Mitarbeiter muss alle Kopien dieser Daten, die nicht in der IT-Infrastruktur von der SalzburgMilch GmbH gespeichert sind, unwiderruflich vernichten und alle Gegenstände seiner IT-Ausrüstung in gutem Zustand an die IT-Abteilung zurückzugeben. Alle firmeneigenen und persönlichen Daten werden auch nach dem Ende des Beschäftigungsverhältnisses geheim gehalten.

5. PASSWÖRTER, BENUTZERPROFILE UND ZUGRIFFSRECHTE

5.1. Passwörter

5.1.1. Passwörter müssen eine Länge von mindestens acht Zeichen aufweisen und komplex sein, d.h. sie müssen mindestens folgende Kriterien beinhalten: Zahl, Sonderzeichen, GROSS-/kleinschreibung. Es sollte sich dabei nicht um einen alltäglichen Begriff handeln (wie etwa Vor- oder Nachname). Passwörter müssen regelmäßig (mindestens alle 42 Tage) und können max. einmal pro Tag geändert werden. Wenn möglich zwingt das Authentifizierungssystem den Benutzer zur Einhaltung dieses Zeitraums. Das IT-System führt eine Passworthistorie der letzten 24 Kennwörter, die nicht wiederverwendet werden dürfen. Die fünfte Fehleingabe des Passwortes, führt zu einer Systemsperre von 30 Minuten.

5.1.2. Alle administrativen Passwörter für die Verwaltung von internen IT-Systemen müssen der IT-Abteilung bekannt sein (personalisierte Passwörter der Benutzer sind hiervon ausgenommen).

5.2. Benutzerprofile und Zugriffsrechte

5.2.1. Der Zugang zu IT-Services und -Systemen des Unternehmens wird beantragt, indem der Vorgesetzte der entsprechenden Person das zum jeweiligen Zeitpunkt gültige Antragsverfahren durchführt. Auch Änderungen von Benutzerrechten und die Löschung von Zugriffsrechten bei Beendigung des Beschäftigungsverhältnisses müssen beantragt werden.

5.2.2. Für den erstmaligen Zugriff auf ein IT-System / einen IT-Service stellt die IT-Abteilung einem IT-Benutzer ein vorläufiges Passwort zur Verfügung, das der Benutzer nach dem ersten Einloggen in das System ändern muss. Dieses lautet im Regelfall: Start123$.

5.2.3. Mitarbeiter, die auf irgendeine Art und Weise Zugriff auf Daten erhalten, für die sie nicht ausdrücklich autorisiert sind, müssen die IT-Abteilung von diesem Umstand in Kenntnis setzen. Sie dürfen diese Daten weder lesen noch anderweitig nutzen.

5.2.4. Mitarbeitern ist es nicht gestattet, Zugangsdaten (Benutzernamen, Passwörter) zu verwenden, für die sie nicht ausdrücklich autorisiert (z.B. Zugangsdaten von KollegInnen während des Urlaubs) sind oder ihre eigenen Passwörter anderen Personen

mitzuteilen.

5.2.5. Dritten, d.h. nicht firmenzugehörigen Personen (einschließlich Haushaltsangehörigen), ist der Zugriff auf sensible und geschäftskritische Daten (inkl. Bildschirmeinsicht) durch Mobilgeräte, wie z.B. Laptops und USB-Festplatten, so weit wie technisch und praktisch durchführbar unmöglich zu machen oder falls dies nicht möglich ist, zumindest zu erschweren (z.B. mithilfe von Verschlüsselungsmechanismen).

5.2.6. Jeder Benutzer muss beim Einloggen zu Beginn einer Sitzung die ihm zugewiesene Benutzerkennung (User ID) eingeben. Wenn er seinen Arbeitsplatz für längere Zeit verlässt, muss er sich aus allen Systemen, in denen er zum jeweiligen Zeitpunkt tätig ist, ausloggen. Verlässt er seinen Arbeitsplatz nur vorübergehend, muss er seine Workstation sichern (z. B. sperren, passwortgeschützter Bildschirmschoner, Standbymodus, etc.). In bestimmten Situationen ist die IT-Abteilung befugt, einen Benutzer remote auszuloggen.

6. CYBERSICHERHEIT

6.1. Allgemeines

6.1.1. E-Mails von / an die SalzburgMilch GmbH und deren Standorte werden automatisch im Hintergrund verschlüsselt, wenn die E-Mail gesendet wird (VPN-Tunnel). Im Prinzip ist die Datenübertragung vom lokalen Computer-Netzwerk der SalzburgMilch bzw. an diese Empfängernetzwerke vor Angriffen geschützt.

6.1.2. Die IT-Abteilung führt eine tägliche Datensicherung aller Daten durch, die auf den Serversystemen des Unternehmens gespeichert sind. Es ist zu beachten, dass die auf dem PC / Laptop lokal gespeicherten Daten in diese Datensicherung nicht mit einbezogen werden. Wichtige Daten müssen immer auf einem Serversystem gespeichert werden (z.B. auf dem Dateiserver).

6.2. Richtlinien für Mitarbeiter

6.2.1. **Sicherheitsprogramme**: Benutzer dürfen die von der IT-Abteilung eingerichteten Sicherheitsprogramme (wie zum Beispiel Virenscanner) nicht absichtlich umgehen oder deaktivieren.

6.2.2. **Übermittlung großer Dateien**: Es dürfen keine großen Dateien (mehr als 5 MB) an E-Mails angehängt werden, selbst wenn die Mitteilung an einen Empfänger im eigenen Haus geschickt wird. Dateien, die an mehrere Personen gerichtet sind, müssen in Projektordnern abgelegt werden. Die IT-Abteilung ist dabei behilflich die Größe von Dateien zu reduzieren.

6.2.3. **Mails**: Da E-Mail-Nachrichten (genauso wie beispielsweise Rechnungsunterlagen) zum kaufmännischen Schriftverkehr zählen, sollte das Löschen von E-Mails sorgsam abgewogen werden. Sollten gesetzliche Aufbewahrungsfristen bestehen, sind die Mails an einem sicheren Ort als Datei abzulegen und nach Ablauf der Aufbewahrungsfrist unbedingt zu löschen. Sollte keine gesetzliche Aufbewahrungsfrist Anwendung finden, gilt das Datenminimierungsprinzip. Abgearbeitete Mails sind daher ehestmöglich zu löschen. Geschäftliche E-Mail-Adressen dürfen Dritten aus Datenschutzgründen nur mitgeteilt oder übermittelt werden, wenn dies für den geregelten Geschäftsablauf innerhalb der SalzburgMilch unbedingt notwendig ist. Zu beachten ist: je mehr Personen eine Mailadresse kennen, desto höher ist die Gefahr des Erhalts von Spam-Mails.

6.2.4. **Verdächtige Mails**: Mails mit verdächtigem Betreff, unbekannten Absendern oder mit verdächtigen Inhalten dürfen keinesfalls geöffnet bzw. beinhaltete Verlinkungen geöffnet werden (Gefahr eines Virenangriffs). Im Zweifelsfall haben sich Nutzer an die IT-Abteilung zu wenden.

6.2.5. **In sicherheitskritischen Fällen**: Die IT-Abteilung ist von jedem sicherheitskritischen Ereignis (z. B. unerwartete Deaktivierung eines Zugriffscodes/Passwortes, unerklärliches Verhalten von Programmen, Datenverlust, verdächtige Mails) umgehend in Kenntnis zu setzen.

6.2.6. **Schulungen**: In regelmäßigen Intervallen sind vorgegebene Schulungen aus diversen IT-Bereichen zu absolvieren (z.B. Cybersecurity-Awareness, Phishing, Office, etc.)

7. PRIVATNUTZUNG UND PRIVATE DATEN AUF FIRMENSYSTEMEN

7.1. Die **Privatnutzung** der von der SalzburgMilch GmbH bereitgestellten IT-Ausrüstung (einschließlich PC / Laptop, Büro- und Mobiltelefon) ist **nicht gestattet**. Privatnutzung bedeutet jegliche Nutzung der Geräte außerhalb des jeweiligen beruflichen Kontexts, daher bspw. Empfangen / Versenden privater Mails und Telefonate, private Internet- und Social Media-Nutzung, etc.

7.2. Abweichend davon kann die Erlaubnis zur Privatnutzung eines oder mehrerer spezifizierter IT-Ausrüstung in Ausnahmefällen erteilt werden. Hierzu bedarf es entweder einer gesonderten vertraglichen Vereinbarung (etwa im Rahmen des Dienstvertrages) oder einer ausdrücklichen schriftlichen Genehmigung des jeweiligen Vorgesetzten in Abstimmung mit der IT-Abteilung.

Unbeschadet dessen ist die Gewährung einer Privatnutzung an dritte Personen (insbesondere auch Haushaltsangehörige) in jedem Fall strikt untersagt.

7.3. **Private Daten und Informationen**, einschließlich Mediendateien, wie private Fotos, Videos, Memes, „lustige Bilder“ etc. dürfen **nicht** auf den Systemen der SalzburgMilch GmbH abgespeichert werden. Auch allfällig bereits bestehende abgespeicherte private Dateien und Informationen auf den Firmensystemen sind vom Nutzer eigenverantwortlich zu löschen. Zu diesen Systemen zählen beispielsweise Server, PCs, Laptops, Tablets und Mobiltelefone.

7.4. Die IT-Abteilung behält sich vor, bei etwaigen ihr zu Kenntnis kommenden Verstöße, Dateien / Informationen, die damit in Verbindung stehen, ohne Vorwarnung und Begründung zu löschen.

8. VERTRAULICHE INFORMATIONEN

Sollen bestimmte berufsbezogene vertrauliche Nachrichten (z.B. Mails) und Dateien, welche im Zusammenhang mit der beruflichen Tätigkeit entstehen (z.B. eigene Notizen), auch im Notfall oder Vertretungsfall nicht mit anderen geteilt werden, so ist für diese Daten ein eigener Ordner im Outlook und am persönlichen Laufwerk mit der Beschriftung VERTRAULICH anzulegen und diese Daten dorthin zu verschieben.

9. ZUGRIFF AUF DATEN DURCH DIE SALZBURGMILCH

9.1.1. Unter strenger Einhaltung der geltenden gesetzlichen Bestimmungen (darunter die des Arbeits- und Betriebsverfassungsrechts) sowie Wahrung der Persönlichkeitsrechte der Mitarbeiter behält sich die SalzburgMilch das Recht vor, zu Wartungs-, Prüf-, Test- und Kontrollzwecken auf alle elektronischen Daten zuzugreifen, die auf firmeneigenen IT-Systemen gespeichert sind und diese zu analysieren.

9.1.2. Zur Gewährleistung der IT-Sicherheit und zu Zwecken der Fehleranalyse führt die IT-Abteilung ein Protokoll der Daten der verschiedenen IT-Systeme, für die sie zuständig ist, um rasch auf Sicherheitsvorfälle und IT-Störungen reagieren zu können.

9.1.3. Die bereitgestellten IT-Anlagen sind von Mitarbeitern stets mit größter Sorgfalt zu behandeln. Bei Beschädigung oder Verlust von IT-Ausrüstung ist umgehend die IT-Abteilung zu benachrichtigen. Für vorsätzliche oder grob fahrlässige Beschädigung oder Verlust von IT-Ausrüstung aus Fahrlässigkeit haftet der jeweilige Mitarbeiter im Rahmen der Bestimmungen des Dienstnehmerhaftpflichtgesetzes (DHG).

SalzburgMilch

SalzburgMilch GmbH • Milchstraße 1 • A-5020 Salzburg
+43 (0)662 / 24 55-0 • office@milch.com • www.milch.com