**Richtlinie für Zulässige ICT-Nutzung**

1. Einführung

COMPANY gewährt ihren Mitarbeitenden Zugang zu einer Reihe von Informationen, Geräten, IT-Systemen und Dienstleistungen (zusammen "**Informations- und Technologieanlagen**"), damit sie ihre Arbeit effizient und effektiv ausführen können. Die vorliegende Richtlinie für die zulässige ICT-Nutzung (nachfolgend "**Richtlinie**") soll den Mitarbeitenden helfen, die Erwartungen der COMPANY in Bezug auf die verantwortungsvolle und sichere Nutzung dieser Informationen und technischen Mittel sowie die diesbezüglichen Verpflichtungen der Mitarbeitenden zu verstehen.

Effektive Sicherheit ist eine persönliche Verantwortung und eine Teamleistung, die die Beteiligung und Unterstützung aller Mitarbeitenden erfordert. Die unsachgemässe Nutzung von Informations- und Technologieanlagen setzt COMPANY, ihre Mitarbeitenden, Kunden, Lieferanten und andere Interessengruppen erheblichen Risiken aus, einschliesslich Malware und Hackerangriffen, Kompromittierung vertraulicher Informationen, rechtlicher und beruflicher Konsequenzen sowie finanzieller und rufschädigender Probleme.

Es liegt in der Verantwortung von jedem Mitarbeitenden, diese Richtlinie zu kennen, zu verstehen und zu befolgen und dementsprechend seine Tätigkeiten auszuführen.

Anträge betreffend Ausnahmen von dieser Richtlinie müssen per E-Mail an [[...]](mailto:infosec@swlegal.ch) eingereicht, mit [zuständigen Abteilung] abgestimmt und vom [Leitungsorgan] genehmigt werden, sofern in dieser Richtlinie nichts anders vorgesehen ist. Genehmigte Ausnahmen müssen dokumentiert werden.

1. Umfang

Diese Richtlinie gilt für:

alle Mitarbeitenden der COMPANY; und

alle Informations- und Technologieanlagen der COMPANY, unabhängig davon, ob sie der COMPANY gehören, von ihr geleast oder im Rahmen einer anderen Vereinbarung zur Verfügung gestellt werden.

Diese Richtlinie gilt sinngemäss auch für dritte Auftragnehmer und Dienstleister, wenn für die erbrachten Dienstleistungen Informations- und Technologieanlagen genutzt werden oder darauf zugegriffen wird. Die Mitarbeitenden müssen sicherstellen, dass alle relevanten Verpflichtungen und Bestimmungen dieser Richtlinie in Vereinbarungen mit Lieferanten und deren Mitarbeitenden und Auftragnehmern, die Zugang zu den Informations- und Technologieanlagen der COMPANY haben, aufgenommen werden.

1. Allgemeine Bestimmungen
   1. Einhaltung von gesetzlichen und vertraglichen Verpflichtungen

Jegliche Nutzung von Informations- und Technologieanlagen der COMPANY muss im Einklang stehen mit:

den Grundsätzen, Verfahren und Anweisungen der COMPANY;

allen einschlägigen gesetzlichen und regulatorischen Verpflichtungen;

spezifischen vertraglichen Pflichten aus Vertragsverhältnissen mit Kunden, Lieferanten und anderen Dritten hinsichtlich der akzeptablen Nutzung ihrer Informationen.

* 1. Verbotene Aktivitäten

Zusätzlich zu den an anderer Stelle in dieser Richtlinie dargelegten Sonderregelungen sind den Mitarbeitenden die folgenden Aktivitäten ausdrücklich untersagt, es sei denn, sie sind ausdrücklich genehmigt und für bestimmte Geschäftszwecke erforderlich (z. B. im Rahmen einer IT-Prüfung oder einer Untersuchung). Die folgende Liste erhebt keinen Anspruch auf Vollständigkeit:

Unbefugter Zugang zu Informationen, IT-Systemen, Geräten, Einrichtungen oder Bürobereichen.

Weitergabe vertraulicher Kunden-, persönlicher oder geschäftlicher Informationen an unbefugte Dritte.

Speicherung von vertraulichen Kunden-, persönlichen oder geschäftlichen Informationen auf ungesicherten (z. B. unverschlüsselten) Geräten oder Speichermedien.

Weitergabe vertraulicher Kunden-, persönlicher oder geschäftlicher Informationen über nicht autorisierte Nachrichtendienste oder soziale Medien (z. B. LinkedIn, XING, Twitter, Instagram oder Facebook).

Das Hochladen, Herunterladen, Kopieren, Speichern, Verbreiten, Installieren oder Verwenden von rechtlich geschütztem Material und damit die Verletzung von Urheberrechten oder anderer Rechter der COMPANY oder Dritter.

Der Zugriff auf, das Erstellen, Kopieren, Speichern, Übertragen oder Verbreiten von Material, das illegal, explizit sexuell, rassistisch, diskriminierend, verleumderisch, hasserfüllend, bedrohlich oder belästigend ist oder als solches angesehen werden könnte.

Erstellen, Kopieren, Übertragen oder Verbreiten von Material, das COMPANY in Verruf bringen könnte.

Anmeldung bei oder Nutzung von Online-Spielen, -Wetten oder -Geldmachern mit Hilfe der Informations- und Technologieanlagen der COMPANY.

Unerwünschtes Werbematerial, "Kettenbriefe" oder andere Junk-E-Mails mit Hilfe der Informations- und Technologieanlagen der COMPANY zu verbreiten.

Weitergabe von Passwörtern und anderer Informationen oder Geräten, die zur Authentifizierung verwendet werden.

Umgehung von Mechanismen zur Benutzerauthentifizierung (z. B. PIN-Schutz für Smartphones).

Deaktivierung oder der Versuch der Deaktivierung von Sicherheitswerkzeugen jeglicher Art (z. B. Anti-Malware, Verhinderung von Datenlecks, Protokollerfassung oder vollständige Festplattenverschlüsselung).

Einschleusen bösartiger Programme (z. B. Viren, Computerwürmer, Trojaner, Key Logger oder Passwort-Cracker).

Vorsätzliche Störung von Netzen und IT-Systemen.

* 1. Schulungen zur Informationssicherheit und Datenschutz

Alle Mitarbeitenden müssen bei ihrem Eintritt in COMPANY und danach mindestens einmal jährlich an Schulungen zur Informationssicherheit und zum Datenschutz teilnehmen.

* 1. Nichteinhaltung dieser Richtlinie

Jeder Verstoss gegen diese Richtlinie wird als Informationssicherheitsvorfall behandelt.

Als Folge eines Verstosses gegen diese Richtlinie kann COMPANY folgende Massnahmen ergreifen:

den Zugang des Mitarbeitenden zu den Informations- und Technologieanlagen der COMPANY einschränken oder entziehen.

Einleitung von Disziplinarmassnahmen gegen den Mitarbeitenden, was u. U. zur Entlassung führen kann.

Einleitung rechtlicher Schritte gegen den Mitarbeitenden und andere an dem Vorfall beteiligte Personen.

Weitergabe von Informationen, einschliesslich Personendaten, an Strafverfolgungsbehörden, soweit dies notwendig ist.

Weitere Massnahmen, die für angemessen erachtet werden.

* 1. Geltung und Ersetzung bestehender Richtlinien

Diese Richtlinie tritt am [...] in Kraft und ersetzt ab diesem Datum alle vorherigen einschlägigen Richtlinien. Falls zutreffend sind alle bestehenden Verweise auf frühere Richtlinien als Verweise auf die vorliegende Richtlinie in ihrer aktuellen Fassung zu verstehen.

1. Nutzung der Informations- und Technologiebestände der COMPANY
   1. Allgemeine Pflichten

|  |  |
| --- | --- |
| Vorübergehendes Nutzungsrecht | 1. COMPANY gewährt ihren Mitarbeitenden zeitlich begrenzten Zugang zu den Informations- und Technologieanlagen der COMPANY, die sie zur Erfüllung ihrer Arbeitsaufgaben benötigen. 2. Alle Eigentums- und Nutzungsrechte an diesen Informations- und Technologieanlagen verbleiben bei der COMPANY. |
| Verwendung für genehmigte Zwecke | 1. Die Mitarbeitenden dürfen die Informations- und Technologieanlagen der COMPANY nur für autorisierte Zwecke nutzen. 2. Die private Nutzung der Informations- und Technologieanlagen der COMPANY ist nur unter den in Abschnitt 4.5 unten zulässig. |
| Die Sorgfaltspflicht | 1. Die Mitarbeitenden sind verpflichtet, mit den Informations- und Technologieanlagen der COMPANY sorgfältig umzugehen und sie entsprechend ihrer Klassifizierung und Handhabung zu schützen (siehe Abschnitt 6 unten). 2. Die Mitarbeitenden dürfen ohne Genehmigung der [zuständige Abteilung] keine Änderungen an den Sicherheitseinstellungen von Informations- und Technologieanlagen vornehmen. 3. Störungen und Fehlfunktionen müssen der [zuständige Abteilung] gemeldet werden. |
| Diebstahl oder Verlust | 1. Bei Verlust oder Diebstahl von Papierdokumenten, die vertrauliche Kunden-, persönliche oder Geschäftsinformationen enthalten, oder eines Geräts, das solche Informationen enthält oder für den Zugriff darauf verwendet wurde (z. B. Laptops, Smartphones oder USB-Laufwerke), müssen die Mitarbeitenden unverzüglich ihren Vorgesetzten oder [zuständige Abteilung] informieren und einen Sicherheitsvorfall melden (siehe Abschnitt 8 unten). Dies gilt unabhängig davon, ob das Gerät Eigentum der COMPANY ist oder nicht. 2. COMPANY behält sich das Recht vor, alle Daten von einem verlorenen oder gestohlenen mobilen Gerät aus der Ferne zu löschen. |
| Rückgabe | 1. Bei Beendigung des Arbeitsverhältnisses (oder auf Verlangen der COMPANY auch früher) sind die Mitarbeitenden verpflichtet, der COMPANY alles zurückzugeben, was sie im Rahmen ihrer vertraglichen Pflichten hergestellt haben und was ihnen während der Dauer ihres Arbeitsverhältnisses anvertraut wurde. Insbesondere sind sie verpflichtet, alle Geräte, Software oder Informationen, die der COMPANY gehören, wie Schlüssel, Ausweise, Smartphones, Tablets, Laptops, USB-Sticks und ähnliche Geräte, sowie alle elektronischen Dateien und Papierdokumente zurückzugeben. Die Mitarbeitenden dürfen keine Kopien oder Auszüge davon behalten, weder in Papier- noch in elektronischer Form. 2. Bei Beendigung des Arbeitsverhältnisses (oder auf Verlangen der COMPANY auch früher) dürfen die Mitarbeitenden keine Online-Datenbanken und -Dienste mehr nutzen, zu denen sie von der COMPANY Zugang erhalten hatten. |

* 1. Workstations und virtuelle Desktops

|  |  |
| --- | --- |
| Workstations und virtuelle Desktops | 1. Die Mitarbeitenden erhalten eine Workstation oder einen Laptop, der Zugang zu einer vorkonfigurierten virtuellen Desktop-Umgebung bietet. |
| Fernzugriff | 1. Berechtigte Mitarbeitende können auf ihren virtuellen Desktop aus der Ferne zugreifen, indem sie die sichere Fernzugriffseinrichtung der COMPANY nutzen (siehe Abschnitt 6.3 unten). |

* 1. Laptops, Smartphones, Tablets und Wechselspeichermedien

|  |  |
| --- | --- |
| Definitionen | 1. Zu den mobilen Datenverarbeitungsgeräten gehören Laptops, Smartphones, iPads und andere Tablets, Digitalkameras, digitale Diktiergeräte und andere tragbare oder am Körper getragene Datenverarbeitungsgeräte. 2. Zu den Wechselspeichermedien gehören USB-Sticks, externe Festplatten, Speicherkarten, CDs/DVDs und andere tragbare Speichermedien. 3. Da diese Geräte und Medien mobil sind, besteht ein grösseres Risiko von Datenverlust, Diebstahl oder sonstigem unbefugten Zugriff, und sie erfordern zusätzliche Sicherheit und Schutz. |
| Laptops | 1. Allen Mitarbeitenden wird ein firmeneigener Laptop zur Verfügung gestellt werden. 2. Vertrauliche Kunden-, persönliche oder geschäftliche Daten dürfen nicht auf der lokalen Festplatte eines Laptops gespeichert werden, es sei denn, sie werden für arbeitsbezogene Zwecke benötigt und der Vorgesetzte eines Mitarbeitenden oder [zuständige Abteilung] genehmigen dies. |
| Smartphones und Tablets | 1. Den Mitarbeitenden wird ein firmeneigenes Smartphone oder Tablet zur Verfügung gestellt. |
| USB-Sticks und andere Wechselspeichermedien | 1. Vertrauliche Kunden-, persönliche oder geschäftliche Daten dürfen nicht auf USB-Sticks oder anderen Wechselspeichermedien gespeichert werden, es sei denn, sie werden für arbeitsbezogene Zwecke benötigt und der Vorgesetzte eines Mitarbeitenden oder [zuständige Abteilung] genehmigen dies. 2. Es dürfen nur von der COMPANY zur Verfügung gestellte Speichermedien mit mindestens 256-Bit-Verschlüsselung verwendet werden, die auf Anfrage beim IT-Helpdesk der COMPANY erhältlich sind. 3. Speichermedien müssen nach der Benutzung an den IT-Helpdesk der COMPANY zurückgegeben werden, um sie sicher zu reinigen oder zu entsorgen. |
| Private Geräte | 1. Die Mitarbeitenden dürfen keine geschäftlichen Daten auf privaten Computern, Laptop, Smartphones, Tablets oder Wechselspeichermedien speichern, es sei denn, sie werden für dienstliche Zwecke benötigt und wurden ausdrücklich von ihrem Vorgesetzten oder [zuständige Abteilung] dazu ermächtigt. Die privaten Geräte müssen mit den aktuellsten Sicherheits-Patches auf dem neusten Stand gehalten werden. Private Computer/Laptop müssen zudem über eine vollständige Laufwerksverschlüsselung verfügen. |

ODER

Nutzung privater Geräte/Bring Your Own Device (BYOD)

|  |  |
| --- | --- |
| Allgemeine Regel | 1. Zugelassene Mitarbeitende können einen privaten Computer (Laptop oder Desktop-Computer) oder ein mobiles Gerät (Smartphone, Tablet) verwenden, um sich mit ihrer virtuellen Desktop-Umgebung zu verbinden und auf bestimmte von der COMPANY bereitgestellte Anwendungen, Dienste und Ressourcen zugreifen zu können (E-Mail, Kalender, Kontakte, Aufgaben, Dateien, Videokonferenzen, Online-Datenbanken usw.). |
| Private Computer (Laptops und Desktop-Computer) | 1. Private Computer, die für den Zugang zu den Informations- und Technologieanlagen der COMPANY verwendet werden, müssen die folgenden Anforderungen erfüllen: 2. Einsatz der anwendbaren Sicherheits-Patches für das Betriebssystem. 3. Einsatz von Anti-Malware-Software sowie Installation der jeweils neustens Updates. 4. Persönliches Login, das den Passwortanforderungen in Abschnitt 5.2 unten entspricht. 5. Passwortgeschützter Bildschirmschoner mit automatischer Aktivierung oder Sperrung der Sitzung nach maximal 15 Minuten. 6. Die Mitarbeitenden dürfen keine geschäftlichen Daten auf privaten Computern speichern, es sei denn, sie werden für dienstliche Zwecke benötigt und sind ausdrücklich von ihrem Vorgesetzten oder [zuständige Abteilung] dazu ermächtigt, und die Speicherung auf dem Computer ist durch eine vollständige Laufwerksverschlüsselung geschützt. |
| Private Smartphones und Tablets | 1. Die Mitarbeitenden müssen ihr mobiles Gerät mit den neuesten Sicherheits-Patches auf dem neuesten Stand halten. 2. Ausserdem müssen sich die Mitarbeitenden beim [IT-Abteilung] vergewissern, dass das Gerät mit den aktuellen technischen Anforderungen kompatibel ist. |
| Private Speichermedien | 1. Vertrauliche, persönliche oder geschäftliche Informationen dürfen nicht auf privaten Wechseldatenträgern (USB-Sticks, CD/DVD usw.) gespeichert werden. Die Mitarbeitenden müssen stattdessen von der COMPANY zur Verfügung gestellte Speichermedien verwenden. |

* 1. Software und Online-Dienste

|  |  |
| --- | --- |
| Autorisiert Software | 1. Auf den von der COMPANY bereitgestellten IT-Systemen darf nur ordnungsgemäss lizenzierte Software verwendet werden, die von der [Leitung IT-Abteilung] genehmigt wurde. 2. Nicht autorisierte Software, die auf von COMPANY bereitgestellten IT-Systemen entdeckt wird, wird entfernt. |
| Vom Unternehmen bereitgestellte web- und cloudbasierte Anwendungen | 1. COMPANY bietet autorisierten Mitarbeitenden Zugang zu verschiedenen Web-Applikationen, die auf den firmeneigenen Servern in der Schweiz gehostet werden (z.B. FileCloud), sowie zu ausgewählten Diensten, die von Dritten gehostet werden (z.B. Webhosting, Videokonferenzen, E-Mail-Marketing, Online-Umfragen usw.). 2. Die Mitarbeitenden müssen alle besonderen Anweisungen für die zulässige Nutzung dieser Systeme befolgen. |
| Andere Cloud-basierte Anwendungen und Dienste | 1. Die Nutzung anderer Cloud-basierter Dienste und Anwendungen für dienstliche Zwecke muss vorab von der [zuständige Abteilung] genehmigt werden. |

* 1. Private Nutzung der Informations- und Technologiebestände des Unternehmens

|  |  |
| --- | --- |
| Allgemeine Regel | 1. Die Informations- und Technologieanlagen der COMPANY sind für arbeitsbezogene Zwecke bestimmt. Eine begrenzte private Nutzung ist zulässig, sollte jedoch in den Pausen oder ausserhalb der Arbeitszeit erfolgen und die Arbeitsverpflichtungen der Mitarbeitenden nicht beeinträchtigen. 2. Die Vertraulichkeit und Sicherheit der Informationen der COMPANY muss gewahrt werden, und die Mitarbeitenden müssen alle Verpflichtungen aus dieser und anderen einschlägigen Richtlinien einhalten. Insbesondere müssen sich die Mitarbeitenden aller in Abschnitt 3.2 aufgeführten verbotenen Handlungen enthalten. |
| Private E-Mails und elektronische Dateien | 1. Die von der COMPANY zur Verfügung gestellten E-Mail-Konten sollten grundsätzlich nicht für private Mitteilungen genutzt werden. Wenn das von der COMPANY zur Verfügung gestellte E-Mail-Konto verwendet wird, sollten private E-Mails in der Betreffzeile ausdrücklich als "privat" oder "persönlich" gekennzeichnet und mit der Empfindlichkeit "Privat" versandt werden. 2. Private elektronische Dateien sollten im Betreff, Dateinamen und/oder im Dokument als "privat" oder "persönlich" gekennzeichnet werden. 3. Private E-Mails und elektronische Dateien sollten im "Privaten" Arbeitsbereich des Mitarbeitenden abgelegt werden, um sie vor unbefugtem Zugriff zu schützen. Solche E-Mails und Dateien können jedoch auch nach der Löschung noch in den Archivierungs- und Sicherungssystemen der COMPANY vorhanden sein und unterliegen der allgemeinen Systemüberwachung und -prüfung durch COMPANY (siehe Abschnitt 9 unten). |
| Private  Dokumente | 1. Private Papierdokumente sollten getrennt von Geschäftsdokumenten aufbewahrt und gegebenenfalls als "privat" oder "persönlich" gekennzeichnet und in einer verschlossenen Schublade oder einem Schrank aufbewahrt werden. |

1. Zugangskontrolle
   1. Büroeinrichtungen

|  |  |
| --- | --- |
| Schlüssel und Ausweise | 1. Der Zugang zu den Büroräumen der COMPANY ist durch elektronische Schlüssel und Ausweise gesichert. 2. Die Mitarbeitenden müssen ihre Büroschlüssel und Ausweise sicher verwahren und dürfen sie mit niemandem teilen. Schlüssel und Ausweise dürfen nicht unbeaufsichtigt gelassen und nicht auf Dienstreisen oder in den Urlaub mitgenommen werden. 3. Bei Verlust oder Diebstahl von Büroschlüsseln oder Ausweisen müssen sich die Mitarbeitenden unverzüglich an die [zuständige Stelle] wenden. |
| Türen, Fenster | 1. Beim Verlassen des Büros nach Büroschluss oder an Wochenenden müssen die Mitarbeitenden die Fenster vollständig schliessen und die Bürotüren (sofern vorhanden) abschliessen. |
| Besucher und andere Dritte | 1. Die Mitarbeitenden dürfen unbefugten Besuchern oder sonstigen Dritten ohne Begleitung keinen Einlass in die zugangsbeschränkten Bürobereiche gewähren. |

* 1. Sicherheit von Benutzerkonten und Passwörtern

|  |  |
| --- | --- |
| Benutzerkonten | 1. Die Mitarbeitenden müssen sich mit dem ihnen zugewiesenen Benutzernamen und Passwort bei den IT-Systemen der COMPANY anmelden, unabhängig davon, welcher Arbeitsplatz oder welches Gerät verwendet wird. 2. Die Mitarbeitenden dürfen ihr Passwort nicht an andere weitergeben oder anderen erlauben, ihr Konto zu benutzen. 3. Ebenso dürfen die Mitarbeitenden nicht versuchen, das Passwort eines anderen Benutzers zu erfahren oder mit dessen Anmeldedaten auf das Konto eines anderen Benutzers zuzugreifen. |
| Passwortsicherheit | 1. Die Passwörter müssen die folgenden Komplexitätsanforderungen erfüllen: 2. Die Passwörter müssen mindestens 8 Zeichen lang sein. 3. Passwörter müssen mindestens drei der folgenden vier Arten von Zeichen enthalten:   Grossbuchstabe (A-Z)  Kleinbuchstabe (a-z)  numerisches Zeichen (0-9)  Sonderzeichen (z. B. $ # @ . ; %).   1. Passwörter dürfen keinen Teil des Benutzernamens enthalten. 2. Passwörter dürfen nicht aus leicht auffindbaren persönlichen Daten bestehen (z.B. Geburtsdatum, Adresse, Namen von Familienmitgliedern usw.). 3. Die Passwörter dürfen nicht mit einem der 12 vorherigen Passwörter identisch sein. 4. Die Passwörter müssen alle 90 Tage geändert werden. 5. Passwörter, die für Cloud- oder persönliche Konten (z.B. E-Banking, soziale Medien usw.) verwendet werden, dürfen nicht mit den Passwörtern identisch sein, die für die Anmeldung bei den IT-Systemen von COMPANY verwendet werden. 6. Passwörter dürfen nicht aufgeschrieben oder so aufbewahrt werden, dass andere sie sehen oder benutzen können (z. B. auf Papier, Aufklebern oder in Klartextdateien auf Computern oder mobilen Geräten). 7. Die Mitarbeitenden dürfen die Passworteingabe nicht durch automatische Anmeldung oder Passwortspeicherung in Webbrowsern oder Anwendungen umgehen. 8. Die Mitarbeitenden müssen ihr Passwort sofort ändern und einen Sicherheitsvorfall melden (siehe Abschnitt 8 unten), wenn es Anzeichen dafür gibt, dass das Passwort missbraucht worden sein könnte. |

* 1. Zugang zu IT-Systemen, Anwendungen und Informationen

|  |  |
| --- | --- |
| Allgemeine Regeln | 1. Die Mitarbeitenden sollen nur auf die für ihre Arbeit notwendigen Informations- und Technologieanlagen der COMPANY Zugang erhalten und diese nutzen dürfen (je nach Funktion, Verantwortlichkeit und Notwendigkeit) ("need to know" und "need to use" Prinzipien). 2. Die Mitarbeitenden dürfen nicht auf Informations- und Technologieanlagen der COMPANY zugreifen oder versuchen, darauf zuzugreifen, für die sie keine Zugangsberechtigung haben. Der Zugang zu einem bestimmten System bedeutet nicht, dass ein Mitarbeitender berechtigt ist, auf alle Daten in diesem System zuzugreifen oder sie zu nutzen. 3. Falls ein Mitarbeitender Informationen erhält oder versehentlich darauf zugreift, ohne eine entsprechende Befugnis zu haben, ist er verpflichtet, seinen Vorgesetzten oder [zuständige Abteilung] unverzüglich zu informieren. |
| Zugangsrechte  Definition | 1. Die Zugriffsrechte werden von [zuständige Abteilung] festgelegt. 2. Um Zugang zu Informations- und Technologieanlagen zu erhalten, müssen die Mitarbeitenden ein Zugangsantrag bei [zuständige Abteilung] stellen. 3. Die [zuständige Abteilung] kann die Zugriffsrechte eines Mitarbeitenden jederzeit einschränken oder widerrufen. |

1. Klassifizierung und Handhabung von Informationen
   1. Allgemeine Pflichten

|  |  |
| --- | --- |
| Klassifizierung von Informationen | 1. Alle Informationen werden als öffentlich, intern, vertraulich oder streng vertraulich eingestuft. 2. Die Informationen müssen entsprechend ihrer Klassifizierung geschützt werden. |

* 1. Clean-Desk-Policy

|  |  |
| --- | --- |
| Allgemeine Regel | 1. Im Interesse der Sicherheit und "Housekeeping" verlangt COMPANY von den Mitarbeitenden, dass sie ihren Arbeitsplatz stets aufräumen und in einwandfreiem Zustand erhalten. 2. Die folgenden Bestimmungen sollten sowohl bei der Arbeit im Büro als auch bei der Fernarbeit beachtet werden, auch wenn die Einstufung einer Information dies nicht unbedingt erfordert. |
| Regeln betr. Schreibtisch | 1. Die Schreibtische sollten am Ende eines jeden Arbeitstages von nicht benötigten Papierdokumenten und Speichermedien befreit werden. Vertrauliches Material sollte in verschlossenen Schubladen oder Schränken aufbewahrt werden. 2. Vertrauliches Material darf in den öffentlichen Bereichen der COMPANY (z. B. Empfangsbereich, Konferenzräume, Küchen, Toiletten) nicht unbeaufsichtigt gelassen werden. 3. Die Mitarbeitenden sollten den Gebrauch von gedruckten Dokumenten auf ein Minimum reduzieren und vertrauliche Ausdrucke unverzüglich aus den Druckern/Fotokopierern entfernen. 4. Nicht mehr benötigte Papierdokumente sollten sofort entsorgt werden. Vertrauliche Dokumente dürfen nicht in offenen Abfallbehältern entsorgt werden, sondern müssen geschreddert werden. Im Zweifelsfall sollte davon ausgegangen werden, dass ein Dokument vertraulich ist. |
| Regeln betr. Bildschirm | 1. Computerbildschirme sollten möglichst nicht im Blickfeld der Öffentlichkeit stehen und/oder durch technische Massnahmen vor unbefugten Blicken geschützt sein. 2. Die Computerbildschirme sollten immer gesperrt werden, wenn der Computer unbeaufsichtigt gelassen wird. 3. Bei der gemeinsamen Nutzung des Bildschirms (Besprechungen, Videokonferenzen, Fernunterstützung usw.) dürfen keine vertraulichen Informationen für Unbefugte sichtbar sein (in geöffneten Anwendungen, Dokumenten, Verknüpfungen auf dem Desktop, Verlauf der zuletzt geöffneten Dokumente usw.). Pop-up-Benachrichtigungen sollten ausgeschaltet werden. 4. Bei Videokonferenzen dürfen keine vertraulichen Informationen in der Umgebung des Mitarbeitenden sichtbar sein (auf Schreibtischen, Whiteboards usw.). |

* 1. Fernarbeit ("Home Office") und Reisen

|  |  |
| --- | --- |
| Verlagerung von Assets an einen anderen Standort | 1. Die Mitarbeitenden dürfen keine vertraulichen Dokumente oder IT-Geräte der COMPANY nachhause (oder andere externe Arbeitsorte) mitnehmen, es sei denn, dies ist für die Arbeitstätigkeit erforderlich und wurde von ihrem Vorgesetzten oder [zuständige Abteilung] ausdrücklich genehmigt. |
| Fernarbeit und "Home Office" | 1. Zugelassene Mitarbeitende können aus der Ferne auf ihren virtuellen Desktop zugreifen, indem sie die sichere Fernzugriffseinrichtung der COMPANY nutzen. Regelmässiges Arbeiten aus der Ferne (oder "Home-Office") ist in dem Umfang und unter den Bedingungen gestattet, die in der Home-Office-Richtlinie der COMPANY festgelegt sind. 2. Die Mitarbeitenden müssen sicherstellen, dass die Ausrüstung und die Umgebung, in der die Arbeit ausgeführt wird, angemessen sind und dass die Sicherheit der Informations- und Technologieanlagen der COMPANY jederzeit gewährleistet ist. 3. Private Computer, die für die Verbindung mit dem virtuellen Desktop der COMPANY verwendet werden, müssen die in Abschnitt 4.3 genannten Anforderungen erfüllen. 4. Die Mitarbeitenden dürfen nicht zulassen, dass andere Personen (einschliesslich Haushaltsmitglieder) ihren Computer benutzen, während sie mit den IT-Systemen der COMPANY verbunden sind. 5. Die Mitarbeitenden müssen sich an die Clean-Desk-Policy halten (Abschnitt 6.2 oben). Vertrauliche Papierdokumente und Speichermedien müssen vor unbefugter Offenlegung, Zugriff und Diebstahl geschützt werden. Sie müssen in einem verschlossenen Raum, einer Schublade oder einem Schrank aufbewahrt werden, wenn sie nicht gebraucht werden. 6. Die Mitarbeitenden dürfen keine vertraulichen Kunden-, persönlichen oder geschäftlichen Daten auf ihrem lokalen Computer speichern, es sei denn, dies ist für arbeitsbezogene Zwecke erforderlich und wurde von [zuständige Abteilung] ausdrücklich genehmigt. Vertrauliche Informationen dürfen nur auf Computern mit vollständiger Laufwerksverschlüsselung gespeichert werden. 7. Aktivitäten, die eine hohe Internet-Bandbreite beanspruchen (z.B. das Streaming von Videos), sollten innerhalb der Fernsitzung so weit wie möglich eingeschränkt werden. |
| Unterwegs | 1. Besondere Vorsicht ist geboten, wenn Mitarbeitende auf Reisen sind oder in öffentlichen Bereichen arbeiten. 2. Bei der Arbeit in Zügen, Flugzeugen oder anderen öffentlichen Räumen müssen die Mitarbeitenden darauf achten, dass ihnen keine andere Person "über die Schulter" schauen oder hören kann, wie sie vertrauliche Angelegenheiten besprechen. 3. Die Informations- und Technologiewerte von COMPANY dürfen in Autos, Restaurants, Zügen oder anderen öffentlichen Räumen nicht unbeaufsichtigt gelassen werden. Die Mitarbeitenden sollten Geräte, Speichermedien und Dokumente immer bei sich tragen und sie nach Möglichkeit wegschliessen. 4. Bei Flug-, Schiffs- oder Busreisen sollten die Mitarbeitenden die Informations- und Technologiegüter der COMPANY im Handgepäck mitnehmen. |

* 1. Weitergabe von Informationen an Dritte

|  |  |
| --- | --- |
| Allgemeine Regeln | 1. Informationen dürfen nur dann an Dritte weitergegeben werden, wenn dies von [zuständige Abteilung] ausdrücklich genehmigt wurde und den Anforderungen an die Klassifizierung und Handhabung entspricht. 2. Die grenzüberschreitende Übermittlung von Kunden-, personenbezogenen und anderen vertraulichen Informationen, kann besondere Vereinbarungen und eine spezielle Genehmigung des Kunden oder der betroffenen Person erfordern. |
| Physische Übertragung | 1. Papierdokumente und Speichermedien, die vertrauliche Kunden-, Personen- oder Geschäftsinformationen enthalten, dürfen nur persönlich, per Einschreiben oder per Kurierdienst übermittelt werden. 2. Vertrauliche elektronische Daten müssen auf einem von der COMPANY zur Verfügung gestellten verschlüsselten Speichermedium gespeichert werden. |
| Online-Übertragung | 1. Wann immer es möglich ist, sollten grosse Mengen vertraulicher Kunden-, persönlicher oder geschäftlicher Daten in elektronischer Form über die von der COMPANY bereitgestellte File-Sharing-Plattform oder einen autorisierte File-Sharing-Dienst eines Drittanbieters übertragen werden. 2. Einzelne Dateien können auch per E-Mail übermittelt werden (mit entsprechendem Schutz, siehe Abschnitt 7.1 unten). |

1. E-Mail, Internet und Online-Dienste
   1. E-Mail

|  |  |
| --- | --- |
| Verantwortung für E-Mail-Konten | 1. Sofern es für die Erfüllung der Arbeitsaufgaben notwendig ist, erhalten die Mitarbeitenden ein geschäftliches E-Mail-Konto. 2. Arbeitsbezogene Kommunikation muss über das von der COMPANY zur Verfügung gestellte E-Mail-Konto abgewickelt werden; die Nutzung privater E-Mail-Konten für geschäftliche Zwecke ist nicht gestattet. 3. Die Mitarbeitenden sind für alle Handlungen verantwortlich, die mit ihrem E-Mail-Konto verbunden sind, und dafür, dass die Sicherheit und der Ruf der COMPANY durch die Nutzung der E-Mail-Dienste der COMPANY nicht gefährdet werden. Insbesondere müssen sich die Mitarbeitenden aller in Abschnitt 3.2 oben aufgeführten verbotenen Aktivitäten enthalten. 4. Die gesamte Kommunikation muss auf professionelle Weise erfolgen. Die Mitarbeitenden müssen bei der Verwendung von E-Mails die gleiche Sorgfalt walten lassen wie bei der physischen Korrespondenz. |
| Empfang von E-Mails; Schutz vor Malware und Spam | 1. COMPANY hat verschiedene technische Sicherheitsmassnahmen eingeführt, um zu verhindern, dass bösartige und unerwünschte E-Mails in die Systeme der COMPANY gelangen. Alle E-Mails und Anhänge werden beim Empfang und bei der Speicherung auf den E-Mail-Systemen der COMPANY auf Schadsoftware überprüft. 2. Trotz dieser technischen Massnahmen besteht immer noch ein Restrisiko, dass bösartige E-Mails in die Postfächer der Mitarbeitenden gelangen, und die Mitarbeitenden müssen daher äusserst wachsam sein und beim Lesen von E-Mails ein gesundes Urteilsvermögen beweisen:   Die Mitarbeitenden dürfen keine verdächtigen E-Mails und Anhänge von unbekannten Absendern öffnen oder auf verdächtige Links in einer E-Mail klicken. Die Mitarbeitenden müssen einen Sicherheitsvorfall sofort melden (siehe Abschnitt 8 unten) und die Anweisungen der [zuständige Abteilung] befolgen.  Ungewöhnliche oder gefälschte Absender, ungewöhnliche Aufforderungen zu bestimmten Handlungen (z. B. zum Anklicken eines Links, zur Übermittlung von Informationen über COMPANY oder Mitarbeitende oder zu Zahlungen), ungewöhnliche Inhalte in der Signatur des Absenders, Schreibstil und Fehler sollten Verdacht erregen.  Offensichtliche Spam-E-Mails sollten gelöscht werden, ohne einen Sicherheitsvorfall zu melden. Die Mitarbeitenden sollten niemals auf Spam-E-Mails antworten, da dies dem Absender die Existenz einer gültigen E-Mail-Adresse bestätigen kann, was zu weiteren unerwünschten Mitteilungen führen kann.   1. COMPANY behält sich das Recht vor, externe Adressen für den Versand von E-Mails an COMPANY zu sperren, wenn diese unerwünschte oder "Junk-Mails" oder E-Mails mit bösartigem Inhalt versenden. |
| Versenden von E-Mails und Anhängen | 1. Ausgehende E-Mails und E-Mail-Anhänge müssen entsprechend ihrer Klassifizierung und Sensibilität angemessen geschützt werden. 2. Es ist verboten, vertrauliche Kunden-, persönliche oder geschäftliche Informationen an private E-Mail-Konten zu senden oder weiterzuleiten (manuell oder automatisch). 3. Die Mitarbeitenden müssen alle Empfänger überprüfen, bevor sie eine E-Mail versenden. 4. Anhänge, die an externe Empfänger gesendet werden, sollten um vertrauliche Metadaten bereinigt werden. Enthalten Anhänge vertrauliche Informationen, sollten sie in einer verschlüsselten Containerdatei (Zip-Datei) übermittelt oder über die File-Sharing-Dienste freigegeben werden. 5. E-Mails, die nur für den/die Empfänger sichtbar sein sollen, müssen mit der Empfindlichkeit "Privat" gesendet werden. Dadurch wird die E-Mail vor Benutzern mit delegiertem Zugriff auf das Empfängerpostfach (z.B. Assistenten) verborgen, wenn das Empfängerpostfach entsprechend konfiguriert ist. Die Mitarbeitenden müssen darauf achten, die E-Mail in einem Arbeitsbereich mit entsprechenden Zugriffsbeschränkungen abzulegen. |
| Interne E-Mails | 1. Interne E-Mails sollten auf das notwendige Mass beschränkt werden, insbesondere E-Mails an interne Verteilergruppen mit vielen Empfängern und beim Kopieren von Empfängern in Cc. Das Kopieren von Empfängern in Bcc sollte vermieden werden. |
| Private E-Mails | 1. Siehe Abschnitt 4.5 above. |

* 1. Internet

|  |  |
| --- | --- |
| Zugang zum Internet | 1. Der Internetzugang wird den Mitarbeitenden zur Verfügung gestellt, die einen legitimen geschäftlichen Bedarf haben. 2. Die Mitarbeitenden sind für alle Folgen verantwortlich, die sich aus der unbefugten oder unangemessenen Nutzung der Internetdienste der COMPANY ergeben. Insbesondere müssen sich die Mitarbeitenden aller in Abschnitt 3.2 aufgeführten verbotenen Aktivitäten enthalten. 3. COMPANY setzt Inhaltskontrollmechanismen ein, um den Zugang zu Webseiten mit bösartigen, illegalen oder unangemessenen Inhalten zu blockieren. Die Mitarbeitenden dürfen nicht versuchen, diese Inhaltskontrolle zu umgehen. 4. Video- und Audiostreaming und -downloads sollten nur dann verwendet werden, wenn sie für arbeitsbezogene Zwecke erforderlich sind. 5. Die Mitarbeitenden müssen Informationen, die sie über ungeprüfte Webseiten erhalten, als unzuverlässig betrachten. Solche Informationen dürfen erst dann für geschäftliche Zwecke verwendet werden, wenn ihre Authentizität und Richtigkeit überprüft worden ist. 6. Die Mitarbeitenden dürfen bei der Nutzung von Internetressourcen für ihre eigenen Arbeitsergebnisse keine Urheberrechte oder andere Rechte an geistigem Eigentum verletzen. Die Quellen müssen ordnungsgemäss angegeben werden. |
| Private Nutzung | 1. Siehe Abschnitt 4.5 oben. |

* 1. Soziale Medien

|  |  |
| --- | --- |
| Firmenkonten | 1. Firmenkonten in den sozialen Medien dürfen nur von [zuständige Abteilung] eingerichtet und betrieben werden oder müssen von dieser genehmigt werden. |
| Private Konten | 1. Die Mitarbeitenden sollten den Zugang zu persönlichen und geschäftlichen Informationen, die zur Erstellung von Datenprofilen, zum Social Engineering oder zur Identifizierung des Mitarbeitenden verwendet werden könnten (z.B. private und geschäftliche E-Mail-Adressen und Handynummern, Geburtsdatum, Bildungs- und Beschäftigungsgeschichte, Verbindungen usw.), angemessen beschränken. 2. Der Zugang zu privaten Fotos, Videos und Nachrichten sollte in angemessener Weise eingeschränkt werden. |
| Verbotene Aktivitäten | 1. Mitarbeitende dürfen nicht: 2. interne, vertrauliche oder geschützte Informationen weitergeben; 3. den Namen oder das Logo der COMPANY zur Bezeichnung von Gruppen, Webseiten usw. ohne vorherige Genehmigung der [zuständige Abteilung] verwenden; 4. sich an Aktivitäten zu beteiligen, die das Geschäft oder den Ruf der COMPANY, ihrer Mitarbeitenden, Kunden, Lieferanten oder anderer Interessengruppen schädigen könnten, oder an anderen in Abschnitt 3.2 oben aufgeführten Aktivitäten teilnehmen. 5. Inhalte, die gegen diese Grundsätze verstossen, müssen auf erste Aufforderung der [zuständige Abteilung] gelöscht werden. |

1. Meldung von Sicherheitsvorfällen

|  |  |
| --- | --- |
| Berichterstattung  Verpflichtung | 1. Die Mitarbeitenden müssen wachsam sein und jeden beobachteten oder vermuteten Sicherheitsvorfall, jedes Ereignis oder jede Schwachstelle unverzüglich melden. 2. Alle Sicherheitsvorfälle, Ereignisse und Schwachstellen sind per E-Mail an [...] zu melden. |
| Externe  Kommunikation | 1. Jegliche externe Kommunikation über Sicherheitsvorfälle ist der [zuständigen Abteilung] vorbehalten. |
| Beispiele für  Sicherheitsvorfälle | 1. Zu den Sicherheitsvorfällen gehören unter anderem:   Diebstahl oder Verlust von Papierdokumenten, die vertrauliche Kunden-, persönliche oder Geschäftsinformationen enthalten, oder eines Geräts, auf dem solche Informationen gespeichert sind oder das für den Zugriff auf solche Informationen verwendet wurde (z. B. Laptops, Smartphones oder USB-Laufwerke), unabhängig davon, ob das Gerät Eigentum der COMPANY ist oder nicht;  aktive, geplante oder zurückliegende Cyberangriffe auf die IT-Systeme der COMPANY;  unbefugte Änderungen an IT-Systemen, einschliesslich Malware-Infektionen, Verunstaltung von Webseiten usw.;  tatsächliche oder vermutete Kompromittierung des Passworts;  unbefugter oder unrechtmässiger Zugang zu Informationen, IT-Systemen oder Einrichtungen;  unbefugte oder unrechtmässige Entnahme, Weitergabe, Zerstörung, Veränderung oder Verwendung von Informationen;  unbefugter oder unrechtmässiger Zugang zu, die Nutzung oder Verbreitung von illegalen oder missbräuchlichen Inhalten;  ungeplante Nichtverfügbarkeit von kritischen IT-Systemen und -Diensten mit negativen Auswirkungen auf den Geschäftsbetrieb;  Verstösse gegen gesetzliche, regulatorische oder vertragliche Verpflichtungen in Bezug auf die Informationssicherheit und den Datenschutz, einschliesslich Verletzungen der Datensicherheit gemäss der EU-Datenschutzgrundverordnung (DSGVO) oder des Schweizer Datenschutzgesetzes (vgl. Richtlinie betr. internes Vorgehen bei Verletzung der Datensicherheit). |

1. Systemüberwachung und Auditing

|  |  |
| --- | --- |
| Zweck | 1. COMPANY wird den Zustand und die Nutzung von Systemen, Netzwerken und Anwendungen für folgende Zwecke überwachen und prüfen: 2. Planung und Verwaltung der Systemkapazität und -funktion; 3. Überprüfung der Einhaltung von Richtlinien und Verfahren; und 4. Aufdeckung, Untersuchung und Verhinderung der unbefugten und illegalen Nutzung. |
| Einhaltung der geltenden Gesetze | 1. Alle Systemüberwachungen und -prüfungen werden in Übereinstimmung mit den geltenden Gesetzen und nur in dem erforderlichen Umfang durchgeführt. 2. Soweit technisch möglich, erfolgt die Überwachung und Prüfung in anonymer Form und beschränkt sich auf relevante Metadaten und Sicherheitsprotokolle. Der Inhalt von E-Mails, Dateien und besuchten Webseiten wird nur mit dem Einverständnis der betroffenen Personen eingesehen oder wenn dies zur Untersuchung mutmasslich unbefugter oder rechtswidriger Handlungen oder für andere legitime Geschäftszwecke erforderlich und von [zuständige Abteilung] genehmigt wurde. |
| Autorisiert  Personen | 1. Die Überwachung und Prüfung werden von Personen durchgeführt, die von [zuständige Abteilung] speziell zu diesem Zweck ermächtigt wurden. 2. Die autorisierten Personen unterliegen strengen Vertraulichkeitsverpflichtungen und besonderen Regeln für den Umgang mit den Systemen und den von diesen Systemen erfassten oder verarbeiteten Informationen. 3. Der Zugang zu den Überwachungs- und Auditsystemen ist auf die autorisierten Personen beschränkt. 4. Die Überwachungs- und Prüfungstätigkeiten der autorisierten Personen werden ebenfalls überwacht und geprüft. |