**1 Informationssicherheits-Richtlinie**

**Inhalt**

[1 Sicherer Umgang mit personenbezogenen Daten 2](#_Toc520323568)

[2 Hardware (HW) 2](#_Toc520323569)

[2.1 Notebooks/mobile Endgeräte 2](#_Toc520323570)

[2.2 Netzwerkanschluss 2](#_Toc520323571)

[3 Software (SW) 3](#_Toc520323572)

[3.1 Anschaffungen von Software 3](#_Toc520323573)

[3.2 Software-Installation 3](#_Toc520323574)

[4 Passwörter 3](#_Toc520323575)

[5 Verlassen des Arbeitsplatzes 3](#_Toc520323576)

[6 Internet-Anwendungen (E-Mail, Web) 4](#_Toc520323577)

[6.1 Abwehr von Schadprogrammen (Firewall/Virenschutz) 4](#_Toc520323578)

[6.2 Nutzungsrichtlinien 4](#_Toc520323579)

[7 Datenträger/Übertragungsmedien 5](#_Toc520323580)

[8 Datenspeicherung/Datensicherung 5](#_Toc520323581)

[9 E-Mail-Archivierung 5](#_Toc520323582)

[10 VPN (Virtual Private Network) 5](#_Toc520323583)

[11 Schutzmaßnahmen 5](#_Toc520323584)

[11.1 Videounterstützte Überwachung 5](#_Toc520323585)

[11.2 Zwei-Faktor-Authentifizierung 5](#_Toc520323586)

[11.3 E-Mail-Nutzung 5](#_Toc520323587)

[11.4 Social Engineering/CEO Fraud 6](#_Toc520323588)

[12 Drucken und Einscannen von Dokumenten 6](#_Toc520323589)

[13 Entsorgung von Dokumenten und Datenträgern 6](#_Toc520323590)

[14 Produktionsaufzeichnungen 6](#_Toc520323591)

[15 Auditierung/Überprüfung 6](#_Toc520323592)

[16 Anwendung auf Mobiltelefone 6](#_Toc520323593)

[17 Folgen des Zuwiderhandelns 6](#_Toc520323594)

(Funktions-)Bezeichnungen, die in der männlichen Form genannt werden, beziehen sich auf weibliche und männliche Personen gleichermaßen. Dienstnehmer sind berechtigt, diese (Funktions-)Bezeichnung in der geschlechtsspezifischen Form zu verwenden. Diese Richtlinien stellen verbindliche Anordnungen für alle Mitarbeiter der ---XXXXXXXX--- und deren verbundenen Unternehmen dar, die im Rahmen ihrer Dienstverhältnisse die IT-Infrastruktur samt IT-Systemen für die Abwicklung von Geschäftsprozessen nutzen.

# Sicherer Umgang mit personenbezogenen Daten

Personenbezogene Daten sind all jene Informationen, die sich auf eine natürliche Person beziehen oder zumindest beziehbar sind und so Rückschlüsse auf deren Persönlichkeit erlauben. Besonders schützenswerte personenbezogene Daten sind Informationen über die ethnische und kulturelle Herkunft, politische, religiöse und philosophische Überzeugungen, Gesundheit, Sexualität und Gewerkschaftszugehörigkeit. Diese Daten dürfen nur nach schriftlicher Zustimmung oder mit gesetzlicher Erlaubnis an Dritte weitergegeben werden.

# Hardware (HW)

Im ---XXXXXXXX----Netzwerk dürfen ausnahmslos nur IT-Systeme betrieben werden, die durch die ---XXXXXXXX----IT-Abteilung beschafft wurden oder aber deren Inbetriebnahme durch die IT-Abteilung vorab schriftlich freigegeben wurde. Der Betrieb von systemfremder Hardware (HW) ist ausdrücklich und ausnahmslos untersagt. Die Weitergabe und die Umverteilung von HW unter den einzelnen Mitarbeitern erfolgen ausschließlich durch oder nach schriftlicher Freigabe durch die IT-Abteilung. Dazu zählt auch das Um- und Ausstecken von Netzwerkkabeln. Derartige Maßnahmen sind nach Durchführung durch die IT- Abteilung vom jeweiligen Mitarbeiter durch Unterzeichnung eines IT-Mitarbeiterdatenblattes zu bestätigen.

## Notebooks/mobile Endgeräte

Bei Notebooks und mobilen Endgeräten hat der Mitarbeiter zusätzlich nach den Regeln der Sorgfaltspflicht dafür Sorge zu tragen, dass das Gerät sicher verwahrt und nicht von Unbefugten benutzt werden kann. Jedes Notebook muss im Büro außerhalb der Geschäftszeiten sowie bei Verwendung auf Messen, Veranstaltungen etc. mit einem dafür vorgesehenen Notebook-Lock gesichert oder sicher verwahrt werden. Das Gerät ist vor Diebstahl und unbefugter Inbetriebnahme zu schützen. Das Gerät darf nicht im Auto von außen sichtbar oder offen im Hotelzimmer liegen bleiben.

Besonders schützenswerte Firmendaten dürfen nicht auf dem Notebook gespeichert werden, sofern das Gerät nicht vom Hersteller oder IT-Dienstleister mit Festplattenverschlüsselung ausgestattet ist. Die Nutzung mobiler Endgeräte, insbesondere Mobiltelefone, während der Inbetriebnahme eines Firmenfahrzeuges ist nur zum Zwecke der Navigation und/oder mit Freisprecheinrichtung erlaubt. Diebstahl, Verlust oder Beschädigung sind unverzüglich telefonisch der IT-Abteilung zu melden.

Die Nutzung privater Cloud-Speicher für Unternehmensdaten ist untersagt. Die Nutzung privater mobiler Endgeräte für betriebliche Zwecke (auch als BYOD – bring your own device bezeichnet) ist grundsätzlich untersagt. Zur Sicherstellung der Einhaltung wird im Unternehmen ein regelmäßiger Netzwerkscan/eine regelmäßige Inventarisierung vorgenommen.

## Netzwerkanschluss

Der Anschluss von Hardware an das Netzwerk ist nur mit vorheriger ausdrücklicher Genehmigung durch die IT-Abteilung erlaubt. Es ist strengstens untersagt, selbstständig Hardware an das Netzwerk an- bzw. abzuschließen. Dies gilt auch und insbesondere für Notebooks von Gästen. Für diese steht ein Gäste-WLAN zur Verfügung.

# Software (SW)

## Anschaffungen von Software

Die Beschaffung jeglicher Software (SW) wird ausschließlich nach Freigabe durch den Vorgesetzten durch die IT-Abteilung durchgeführt. Für den Einsatz der SW werden in allen Bereichen des Unternehmens entsprechende Software-Lizenzen benötigt. Die ---XXXXXXXX--- untersagt in jedem Fall die Verwendung von nicht durch obigen Beschaffungsprozess erworbener Software sowie von Software ohne gültige Lizenz.

## Software-Installation

Die Mitarbeiter sind nicht mit einer Systemberechtigung zur Installation von Software auf den benutzten Endgeräten ausgestattet. In Ausnahmefällen kann ein solches Recht nach Freigabe durch den Vorgesetzten durch die IT-Abteilung gewährt werden. In jedem Fall ist aber die Installation von SW nur nach ausdrücklicher Genehmigung gestattet. Die Nutzung von Software (Starten von Anwendungen auch ohne Installation), die nicht durch die IT-Abteilung geprüft und freigegeben wurde, ist verboten.

# Passwörter

Der Zugriff zu den IT-Systemen wird durch Benutzerkonten mit Passwort gesichert und kontrolliert. Benutzerkonten sind – abgesehen von den firmenrelevanten Zugriffen auf externe Onlineservices oder dezidiert als Firmenkonten gelieferte Zugangsdaten – stets personenbezogen. Die Zugangsdaten für Web-Portale oder sonstige Dienste, die eine Autorisierung vorsehen, müssen in sicherer Form gespeichert werden. E-Mail oder Dateiablage ist hier nicht zulässig. Passwörter sind in jedem Fall geheim zu halten. Dem Mitarbeiter ist es daher ausnahmslos untersagt, sein Passwort an andere Personen weiterzugeben oder in irgendeiner Form durch andere Personen zugänglich zu notieren. Das Passwort ist in nicht lesbarer Form abzuspeichern. Die Verwaltung und Speicherung der Passwörter ist ausschließlich im von der IT-Abteilung vorgegebenen Software-Tool (z.B. KeyPassX) erlaubt. Es ist dahingehend Sorge zu tragen, dass das Passwort bei der Eingabe nicht „von den Fingern“ abgelesen werden kann. Jeder Mitarbeiter ist für sein Passwort und alle Eingaben in die IT-Systeme, die unter diesem Benutzerkonto getätigt werden, verantwortlich.

Sollte der Verdacht bestehen, dass das persönliche Passwort nicht mehr sicher ist, so ist das Passwort unverzüglich zu ändern und dieser Verdacht umgehend der IT-Abteilung mitzuteilen.

Es ist untersagt, mit einem fremden Benutzerprofil zu arbeiten, es sei denn, es handelt sich um ein allgemeines Benutzerkonto, welches speziell für diesen Zweck freigegeben wurde. Im Falle eines Verstoßes gegen diese Vorschriften trägt der Verfügungsberechtigte über das jeweilige Benutzerkonto die Verantwortung für sämtliche daraus resultierende Schäden. Darüber hinaus ist darauf zu achten, wer in den Bildschirm einsehen kann, wenn vertrauliche Informationen bearbeitet werden. Dies gilt sowohl innerhalb der Firma, insbesondere aber bei der Verwendung von Notebooks außerhalb des Unternehmens (bei Kunden, auf Workshops, auf öffentlichen Plätzen, bei Konferenzen etc.).

# Verlassen des Arbeitsplatzes

Beim Verlassen des Arbeitsplatzes während der Dienstzeit ist immer die Bildschirmsperre (Bildschirmschoner) zu aktivieren oder eine Systemabmeldung durchzuführen. Wird der Arbeitsplatz für längere Zeit verlassen (z.B. Dienstschluss, Dienstreise etc.) ist der PC bzw. das Notebook herunterzufahren oder in den Ruhezustand zu versetzen und abzusperren. Ebenso ist dafür Sorge zu tragen, dass unberechtigte Personen (z.B. Reinigungspersonal, unbefugte Mitarbeiter oder Besucher) keinen Zugriff auf Hardcopy-Dokumente haben. Netzwerkdrucker und -scanner dürfen nicht abgeschaltet werden. Im Abwesenheitsfall ist der Mitarbeiter verpflichtet, eine Abwesenheitsnachricht einzurichten.

# Internet-Anwendungen (E-Mail, Web)

Der Internetzugang und das E-Mail-System werden nur für die dienstliche Nutzung zur Verfügung gestellt, jegliche private Nutzung ist untersagt. Über die dienstlichen E-Mail-Adressen eingehende private E-Mails sind wie private schriftliche Post zu behandeln. Eingehende private, aber fälschlich als Dienstpost behandelte E-Mails sind den betreffenden Beschäftigten unverzüglich nach Bekanntwerden ihres privaten Charakters zur alleinigen Kenntnis zu geben. Private E-Mails sind von Beschäftigten nach Kenntnisnahme des privaten Charakters unverzüglich zu löschen.

Das Downloaden von ausführbaren Programmen aus dem Internet sowie das Ausführen von Bildschirmschonern und anderen Programmen, die als Attachments zu E-Mails empfangen werden, ist aus Sicherheitsgründen (Viren, Würmer, etc.) ausdrücklich untersagt. Der Versand von Dokumenten mit vertraulichem oder kritischem Inhalt muss entsprechend sensibel erfolgen. E-Mails, für die aufgrund ihres Inhalts gesetzliche Aufbewahrungsfristen gelten, müssen für eben diesen Zeitraum gespeichert werden.

Ist der Mitarbeiter im Urlaub oder kann krankheitsbedingt nicht seiner Arbeit nachgehen, hat er (soweit möglich) den Abwesenheitsagenten in der E-Mail-Anwendung zu aktivieren oder aktivieren zu lassen. Bei längerer Abwesenheit sowie bei Ausscheiden eines Mitarbeiters ist ---XXXXXXXX--- berechtigt, eine Weiterleitung von E-Mails bei Abwesenheit und/oder einen Zugriff auf empfangene bzw. versandte betriebliche E-Mails einzurichten, wenn dies für betriebliche Zwecke erforderlich ist und eine Abwesenheitsmitteilung nicht ausreicht. Der Mitarbeiter muss damit rechnen, dass dadurch auch private E-Mails versehentlich gelesen werden können. Mit Beendigung des Beschäftigungsverhältnisses steht die E-Mail-Adresse des jeweiligen Mitarbeiters nicht mehr für diesen zur weiteren Nutzung zur Verfügung. Die Mitarbeiter sind angehalten, ihre außerbetrieblichen Kommunikationspartner über diesen Umstand zu informieren.

## Abwehr von Schadprogrammen (Firewall/Virenschutz)

Auf jedem Endgerät muss eine Abwehr von Schadprogrammen (z.B. durch Firewall und/oder Virenschutz) sichergestellt werden. Es ist untersagt installierte Abwehr-Tools zu deaktivieren oder zu deinstallieren. Bei jedem Virenverdacht auf dem Datenbestand ist sofort die IT-Abteilung zu verständigen. Der Versuch, das Virus selbst zu löschen, ist zu unterlassen. Es ist strengstens untersagt, Viren selbst zu generieren oder bewusst weiterzuleiten.

Der Mitarbeiter stimmt dem Betrieb von Firewalls, Virensuchprogrammen sowie Filtern zur Abwehr von Spam-Mails und anderen unerwünschten Inhalten auf den IT-Systemen ausdrücklich zu. Er stimmt ferner der aus technischen Gründen erforderlichen Überprüfung von Logfiles durch die IT-Abteilung zu. Der Mitarbeiter wird ausdrücklich darauf hingewiesen und stimmt zu, dass im Falle eines Missbrauches der von ---XXXXXXXX--- seinen Mitarbeitern zur Verfügung gestellten Telekommunikationsinfrastruktur durch Aufzeichnungen des Datenverkehrs die Identität des verantwortlichen Mitarbeiters ermittelt werden kann.

## Nutzungsrichtlinien

Alle Internet-Systeme (inklusive PC und Software) sind Eigentum der ---XXXXXXXX--- und sind jederzeit zu Geschäftszwecken und im Interesse des Dienstgebers zu benutzen. Benutzer von Internet-Systemen repräsentieren das Unternehmen nach außen, ein verantwortungsvolles und professionelles Auftreten im Internet wird vorausgesetzt.

Zu beachten ist, dass sich der Mitarbeiter, wann immer er sich im Internet bewegt, über seine IP-Adresse eindeutig als Repräsentant des Unternehmens ausweist. Es darf kein mit dem Gesetz in Konflikt stehendes Material abgerufen, gespeichert oder weitergeleitet werden. Vor allem der Besuch von unseriösen Webseiten beeinträchtigt die Datensicherheit. Zu beachten ist, dass Chats und Newsgroups öffentliche Foren sind. Alle Anfragen, Diskussionsbeiträge etc. werden gespeichert und können von jedem beliebigen Benutzer abgefragt werden. So wäre es für einen Mitbewerber sehr einfach nachzuforschen, welche Interessensgebiete verfolgt werden. Es ist darauf zu achten, dass bei Zitaten und Downloads aus dem Internet keine Urheberrechte verletzt werden. Zu beachten ist außerdem, dass das Internet internationale Dienste anbietet und mitunter auch internationales Recht zur Anwendung kommt.

# Datenträger/Übertragungsmedien

Für den Austausch von Daten dürfen nur die von der IT-Abteilung freigegebenen Speicher- und Übertragungsmedien verwendet werden. Der Einsatz von externen physischen Datenträgern und von Übertragungsmechanismen (wie z.B. Bluetooth, WLAN etc.) hat mit äußerster Sorgfalt zu erfolgen. Vertrauliche Informationen dürfen ausschließlich verschlüsselt gespeichert und übertragen werden. Der Mitarbeiter ist für die Sicherheit dieser Daten alleine verantwortlich. ---XXXXXXXX--- behält es sich vor, Datenträger und/oder Übertragungsmedien zu sperren. Das Übertragen und Speichern von firmenrelevanten Informationen auf systemfremde HW – dazu zählen auch private PCs oder Notebooks – ist untersagt. Dies gilt auch für das Versenden von firmenrelevanten Informationen auf einem eigenen, privaten E-Mail-Account.

# Datenspeicherung/Datensicherung

Für die regelmäßige und automatische Datensicherung müssen die Dateien auf dem jeweiligen Netzlaufwerk vom Mitarbeiter abgelegt werden. Für alle Informationen, die auf lokalen Festplatten und Geräten gespeichert wurden, kann die Sicherheit nicht gewährleistet werden. Aus diesem Grund werden alle Mitarbeiter ausdrücklich angewiesen, firmenrelevante Informationen ausschließlich auf den zugewiesenen Netzwerklaufwerken bzw. nach Umstieg auf eine Firmen-Cloudlösung in der ausgewählten Cloud zu speichern. Die Datensicherung auf lokalen Festplatten und Geräten ist lediglich temporär für die Präsentation von Daten z.B. bei Kunden erlaubt. Das Speichern von privaten Informationen auf ---XXXXXXXX----HW oder -Netzlaufwerken ist nicht gestattet.

# E-Mail-Archivierung

Aus technischen und rechtlichen Gründen werden E-Mails der Mailbox automatisch nach Erreichen eines definierten Alters in ein Archivsystem übernommen.

# VPN (Virtual Private Network)

Nach Freigabe durch den Vorgesetzten ist es möglich, ein Notebook mit einem VPN-Zugang ausstatten zu lassen.

# Schutzmaßnahmen

## Videounterstützte Überwachung

Zu besseren Absicherung der Infrastruktur wird von ---XXXXXXXX--- in definierten Unternehmensbereichen ein videounterstütztes Überwachungssystem eingesetzt. Zur Auswertung der Daten werden technische und infrastrukturelle Vorkehrungen getroffen. Die Wahl der Aufstellungsplätze wurde unter Berücksichtigung der Datenschutzrichtlinie getroffen. Der Mitarbeiter stimmt der videounterstützen Überwachung ausdrücklich zu.

## Zwei-Faktor-Authentifizierung

Es wird empfohlen, die Sicherheit von besonders schützenswerten Daten und den Zugang zu diesen mit einer Zwei-Faktor-Authentifizierung umzusetzen.

## E-Mail-Nutzung

Der Mitarbeiter ist verpflichtet eingehende E-Mails mit äußerster Sorgfalt zu prüfen. E-Mails, die im Bezug auf Absender, Betreffzeile und/oder Dateianhang verdächtig erscheinen, sind unverzüglich an die IT-Abteilung mit dem Hinweis auf Spam/Phishing/Virus weiterzuleiten und anschließend sofort zu löschen. Keinesfalls darf ein verdächtiger Anhang vom Mitarbeiter selbst geöffnet werden.

## Social Engineering/CEO Fraud

Es ist untersagt unter Umgehung der firmeninternen Prozesse für Vorgesetzte oder Kollegen Zahlungsvorgänge oder ähnliche Tätigkeiten durchzuführen. Verdächtige Anfragen und Aufforderungen sind an den Vorgesetzten zu melden.

# Drucken und Einscannen von Dokumenten

Der Mitarbeiter ist verpflichtet, jederzeit den korrekten Drucker zu verwenden und ausgedruckte vertrauliche Informationen umgehend aus dem Drucker zu entfernen. Darüber hinaus sollte sparsam und gewissenhaft beim Ausdrucken vorgegangen werden.

# Entsorgung von Dokumenten und Datenträgern

Sämtliche Dokumente und Datenträger (USB Stick, Festplatte, SD-Karte, CD/DVD etc.) müssen am Ende ihrer Nutzungsdauer sicher über die IT-Abteilung entsorgt werden.

# Produktionsaufzeichnungen

Die Mitarbeiter in den Entwicklungs- und Produktionsstätten werden in Kenntnis gesetzt und stimmen hiermit ausdrücklich zu, dass, insbesondere zum Zwecke der Qualitätssicherung und zum Zwecke der technologischen und innovativen Entwicklung des Unternehmens, unterschiedliche Auswertungen in digitaler Form, z.B. Messdaten von Produktionsmaschinen, regelmäßig durchgeführt werden.

# Auditierung/Überprüfung

Alle Mitarbeiter werden darauf hingewiesen und stimmen zu, dass alle Systeme elektronisch auf die Einhaltung der oben angeführten Regeln hin überprüft werden können. Unregelmäßige Stichproben können unangekündigt im Auftrag der Geschäftsleitung durchgeführt werden.

# Anwendung auf Mobiltelefone

Die Vorschriften dieser Richtlinie gelten - soweit anwendbar - auch für mobile Geräte, die ---XXXXXXXX--- dem Mitarbeiter zur Verfügung gestellt werden, insbesondere für Mobiltelefone. Der Mitarbeiter ist dafür verantwortlich, dass seine Nutzung die Freieinheiten des für ihn freigeschalteten Tarifs nicht übersteigt. Sofern sich der Mitarbeiter im Ausland aufhält, ist er verpflichtet, rechtzeitig vor Abreise von der IT-Abteilung passende Pakete freischalten zu lassen. Bei Verlust bzw. Diebstahl des Mobiltelefons ist unverzüglich die IT-Abteilung zu verständigen, damit das Mobiltelefon gesperrt werden kann. Die private Nutzung von Mobiltelefonen im Rahmen der Freieinheiten des Tarifs ist bis auf Weiteres gestattet. Der Mitarbeiter stimmt ausdrücklich der regelmäßigen Protokollierung von Anruflisten zu.

# Folgen des Zuwiderhandelns

Die Einhaltung der IT-Richtlinie wird überprüft und kontrolliert, um das Unternehmen vor strafrechtlicher Verfolgung und Schaden zu schützen. Wird ein Verstoß eines Mitarbeiters gegen diese Richtlinien festgestellt, so kann der Zugang zu den zur Verfügung gestellten Systemen ohne Vorankündigung durch die IT-Abteilung gesperrt werden. Im Zuge dieser Maßnahme werden sowohl der Mitarbeiter als auch der Vorgesetzte umgehend davon in Kenntnis gesetzt. Eine Sperre kann nur in Abstimmung mit dem Vorgesetzten aufgehoben werden. Der Mitarbeiter hat außerdem mit entsprechenden dienstrechtlichen Folgen zu rechnen.

Dieses Dokument wurden von einer Expertengruppe der Cybersicherheit-Plattform (CSP) erstellt.

Alle Angaben erfolgen trotz sorgfältigster Bearbeitung ohne Gewähr. Eine Haftung der Wirtschaftskammern Österreichs, der CSP oder der Mitglieder der Expertengruppe ist ausgeschlossen.

Bei allen personenbezogenen Bezeichnungen gilt die gewählte Form für alle Geschlechter!

Stand: März 2024