Richtlinien
für die Nutzung von IT-Systemen, IT-Anwendungen und IT-Diensten und dem Umgang mit elektronischen Dokumenten

der Loewe Technology GmbH

Version: 1.1 **gültig ab:** 01.11.2023

Autoren: Stefan Bodenschatz
Julia Memmel

Kronach, 01.11.2023

Aslan Khabliev	Thomas Putz	Christian Alber
CEO	CTO	COO

INHALTSVERZEICHNIS

Rev.-Nr.	Revisions-datum	Betrifft Kapitel / Abschnitt	Änderungsbeschreibung
1.0	01.12.2020	Gesamtes Dokument	Überarbeitung, Anpassung an Loewe Technology GmbH
1.1	1.11.2023		

1 Verhaltensweisen zur IT-Sicherheit mit Richtliniencharakter

1.1 Vorbemerkung

Sicherheit und Datenschutz in der Informationstechnik dienen der Sicherstellung der drei Hauptgrundwerte der Informationssicherheit:

- **Verfügbarkeit** (IT-Systeme, Anwendungen und Informationen sind verfügbar, wenn sie gebraucht werden)
- **Integrität** (Die Informationen sind vollständig und richtig; unautorisierte Änderungen gespeicherter oder übertragener Daten werden ausgeschlossen bzw. erkannt)
- **Vertraulichkeit** (Zugang zu Informationen nur für Befugte)
- **Belastbarkeit der Systeme und Dienste** (die Widerstandsfähigkeit der IT im Fehlerfall, bei Störungen oder hoher Beanspruchung)

Diese Grundwerte werden ergänzt durch

- **Authentizität** (Herkunft von Informationen kann zweifelsfrei nachgewiesen werden)
- **Revisionsfähigkeit** (Änderungen an Daten können nachvollzogen werden)

von Daten und IT-Anwendungen.

Bei der Verarbeitung personenbezogener Daten sind darüber hinaus die Prinzipien der **Datenvermeidung, Datensparsamkeit und Erforderlichkeit** sowie der **Zweckbindung** (Personenbezogene Daten dürfen nur für den Zweck verwendet werden, zu dem sie erhoben wurden) zu beachten. Die eingesetzte Informationstechnik ist nicht aus sich heraus, sondern vielmehr wegen ihres Wertes für die Anwender und das Unternehmen schützenswert.

Die nachfolgenden Richtlinien sollen die möglichst störungsfreie, ungehinderte und sichere Nutzung der Kommunikations- und Datenverarbeitungsinfrastruktur von Loewe gewährleisten.

Ziel der IT-Sicherheitsmaßnahmen ist es, nicht nur die existierenden gesetzlichen Auflagen zu erfüllen, sondern zusätzlich die bei Loewe verarbeiteten, übertragenen und gespeicherten Daten und Anwendungen zu schützen sowie das Unternehmen soweit wie möglich vor finanziellen Schäden und Imageverlust zu bewahren.

Diese Richtlinie gilt für die Loewe Technology GmbH einschließlich aller

Tochtergesellschaften (als Loewe Gruppe bezeichnet).

Die Bestimmungen gelten in gleicher Weise, sofern nicht gesetzliche Vorgaben dagegenstehen, für alle Geschäftspartner von Loewe, die am Standort Kronach für Loewe Dienstleistungen erbringen und dafür teilweise Hardware, Software oder andere IT-Dienste in Anspruch nehmen (die sog. „Erfüllungsgehilfen“ von Loewe am Standort Kronach).

Zusätzlich zu den nachfolgend aufgeführten Richtlinien und speziellen gesetzlichen Vorgaben in Deutschland sind Betriebsvereinbarungen (z. B. über die Nutzung von E-Mail und Internet) sowie ergänzende Richtlinien bei den Auslandstöchtern, das EU-Recht und landespezifische Gesetze zu beachten.

Bei personenbezogenen Daten gilt darüber hinaus die Schulungspräsentation zum Datenschutz

Die Richtlinien wurden von dem Bereich IT in Zusammenarbeit mit dem IT-Sicherheits- und Datenschutzbeauftragten erarbeitet. Bei Fragen wenden Sie sich bitte an Ihre IT oder den IT-Sicherheits- bzw. Datenschutzbeauftragten

1.2 Änderungen und Ergänzungen im Überblick

- Konkretisierungen einzelner Bestimmungen
- Neuer Hauptpunkt: Netzwerk

1.3 Allgemeine IT-Sicherheit, Schutz von Informationen und Daten

- Benutzen Sie keine IT-Systeme oder IT-Komponenten ohne ausdrückliche Erlaubnis.

- Versuchen Sie nicht, auf Informationen zuzugreifen oder diese zu verändern, wenn Sie nicht explizit dazu berechtigt sind oder nicht sicher wissen, dass Sie dazu befugt sind. Der Zugriff auf Daten Dritter ohne deren Erlaubnis sowie die unberechtigte Manipulation von elektronischen Daten anderer sind verboten.

- Verändern Sie nie Informationen auf IT-Systemen, wenn Sie nicht explizit dazu berechtigt sind oder nicht sicher wissen, dass Sie dazu befugt sind. Insbesondere ist die unberechtigte Manipulation von elektronischen Daten anderer verboten.

- Falls eine Weitergabe von vertraulichen Informationen an Dritte notwendig ist, müssen Sie den Empfänger der Information zur vertraulichen Behandlung verpflichten. Dies betrifft in der Regel jeden Loewe-Geschäftspartner. Dazu steht im Dokumentenmanagementsystem SharePoint in der Rubrik „Workspace Loewe“ das Formular

Geheimhaltungsvereinbarung (Workspace Loewe -> 03 Corporate Company Documents“) bereit.

- Externe Mitarbeiter, die für Loewe tätig sind und Zugang zu Unterlagen und Daten erhalten, müssen schriftlich (im Rahmen von Geheimhaltungsverpflichtungen) auf die Einhaltung der geltenden Vorschriften, internen Regelungen und einschlägigen Gesetze verpflichtet werden.

- Legen Sie keine Dateien mit Informationen der Geheimhaltungsstufe „vertraulich“ oder höher und Dateien mit personenbezogenen Informationen im Sinn der Datenschutz-richtlinie in einem Speicherbereich ab, der allgemein zugänglich ist.

- Achten Sie generell beim Speichern von Informationen darauf, dass auf diese nicht von Unbefugten zugegriffen werden kann.

- Dokumente der Geheimhaltungsstufe „vertraulich“ oder höher und Dokumente, die personenbezogene Informationen im Sinn der Datenschutzrichtlinie enthalten und auf transportablen Datenmedien, wie USB-Sticks und –Festplatten, CDs, DVDs etc. abgelegt werden oder per Email versendet werden, müssen besonders geschützt werden, z.B. durch Datenverschlüsselung.

- Die Ablage von privaten Daten im Netzwerk und auf lokalen Datenträgern von Firmen-Endgeräten ist generell verboten.

  Sollten Sie dennoch private Daten dort ablegen oder bereits abgelegt haben, dann werden diese Daten analog zu Firmendaten behandelt. Beispielsweise dürfen private Daten von der IT gesichert oder archiviert werden und bei einem Ausscheiden aus dem Unternehmen auch ohne Rückfrage gelöscht werden. Ein Rechtsanspruch auf Herausgabe und/oder Löschung der privaten Daten ist ausgeschlossen und teilweise auch technisch nicht möglich (Stichwort: Archivierung).

  Die Ablage auf mobilen Firmen-Endgeräten ist eingeschränkt erlaubt (siehe da- zu Pkt. 2 für „Mobile Devices“).

1.4 Mobile Datenträger, mobile IT-Geräte und sonstige netzwerkfähige Geräte

- Bitte beachten Sie, dass fremde USB-Medien, z.B. von Geschäftspartnern oder Besuchern nicht an Loewe-PCs angeschlossen werden sollten. Ist es trotzdem unumgänglich, dann sind Sie bitte besonders aufmerksam und melden Sie jedes verdächtige Ereignis (es kommt z.B. eine Warnung des Virenscanners) unverzüglich der Loewe IT. Selbstverständlich birgt auch der umgekehrte Weg eine nicht zu vernachlässigende Gefahr, also der Anschluss von Loewe-Speichermedien an einen Besucher-PC, um z.B. Daten auf einen Loewe-PC zu übertragen. Auch hier ist besondere Aufmerksamkeit geboten.

- Es wird darauf hingewiesen, dass Laptops, Tablets, PDAs bzw. Mobiltelefone auf Dienstreisen oder auf der Fahrt zwischen Arbeitsplatz und Wohnort sicher zu transportieren und zu verschließen sind. Bitte beachten Sie in diesem Zusammenhang auch folgendes:

    - Die Zeit, in denen das Gerät unbeaufsichtigt ist, ist zu minimieren.
    - Bitte beschränken Sie die auf mobilen Geräten gespeicherten Daten aufs Nötigste.
    - Wird ein Gerät in einem Kraftfahrzeug aufbewahrt, so sollte es von außen nicht sichtbar sein, z. B. indem es im Kofferraum eingeschlossen wird.
    - In Hotelräumen sollten mobile Geräte nicht offen ausliegen. Das Verschließen des Gerätes in einem Schrank oder einem Koffer behindert Gelegenheitsdiebe.
    - Sie sollten Ihr mobiles Gerät niemals an firmenfremde Personen verleihen.
    - Der Internetzugang sollte nur dann aktiviert werden, wenn er auch genutzt wird.
    - Drahtlose Verbindungen wie Bluetooth oder WLAN (Wireless LAN) sollten generell nur dann aktiviert werden, wenn sie auch zum Einsatz kommen. Bei Bluetooth ist darauf zu achten, dass mit Ausnahme der Ersteinrichtung die Erkennbarkeit auf „nicht erkennbar“ eingestellt wird. Bei manchen Bluetooth-fähigen Geräten lässt sich die zur Absicherung verwendete PIN nämlich nicht ändern.
    - Bei öffentlichen WLAN-Zugängen (z.B. Flughafen, Bahnhof, Hotel, Café) achten Sie bitte darauf, sensible Daten auf Webseiten nur dann einzugeben, wenn Sie über eine https-Verbindung darauf zugreifen.
    - Achten Sie an öffentlichen Plätzen, dass niemand Einblick auf das Display Ihres Endgerätes hat, speziell, wenn dort vertrauliche Informationen angezeigt werden.

- Transportable Kommunikationsgeräte (z. B. Notebooks, Smartphones, Tablets oder andere PDAs) sind mit einem Passwort zu schützen, um z. B. nach Verlust des Gerätes einen direkten Zugriff auf die darauf gespeicherten Daten zu verhindern. Jeder Verlust ist unverzüglich der IT zu melden, um zeitnah eine Sperrung durchführen zu können.

- Alle nicht von der IT ausgegebenen und eingerichteten netzwerkfähigen Geräte dürfen bis zur expliziten Einzel- oder Gruppenfreigabe durch die IT nicht im Loewe LAN betrieben werden. Für Tests steht das sog. „Labornetz“ zur Verfügung. Dabei handelt es sich um ein separates Netzwerk mit einem Internetzugang via DSL.

2 Mobile Devices

Mobilgeräte, wie etwa Smartphones und Tablet-Computer, spielen inzwischen eine wichtige Rolle in der internen und externen Unternehmenskommunikation.

Sie bergen jedoch auch beträchtliche Sicherheitsrisiken: Werden keine hinreichenden Vorsichtsmaßnahmen getroffen, können sich Unbefugte über Mobilgeräte unter Umständen Zugriff auf die IT-Infrastruktur des Unternehmens verschaffen. Datenverluste und eingeschleuste Malware (Viren, Trojaner etc.) können die Folge sein.

2.1 Technische Anforderungen

- Auf den Geräten muss ein aktuelles Betriebssystem installiert sein

- Benutzerkennwörter zu den Geräten oder zu Anwendungen dürfen nur in verschlüsselten Kennwortspeichern aufbewahrt werden.

- Benutzer müssen für Ihre Anmeldung am PC (Domain Account) ein sicheres Kennwort wählen, das den Anforderungen der Kennwortrichtlinie von Loewe genügt.

- Das Sperrkennwort zu dem mobilen Endgerät muss mindestens aus 6 Zahlen bestehen, aber einfache Kombinationen wie z.B. 11111,12345 etc. nicht. Hinweis: nach 10 Falscheingaben werden alle Daten auf dem Gerät gelöscht.

2.2 Pflichten der Benutzer

- Abhanden gekommene oder gestohlene Geräte müssen der IT-Abteilung und dem Datenschutzteam umgehend gemeldet werden und Diebstahl bei der Polizei angezeigt werden. Nutzen Sie dazu den bekannten Kommunikationskanal: servicedesk@loewe.de und datenschutz@loewe.de. Ihnen sollte bewusst sein, dass wir als Unternehmen unter bestimmten Voraussetzungen eine gesetzliche Informationspflicht sowohl an die Datenschutzaufsichtsbehörde als auch an die Betroffenen selbst haben, sollten Daten (vor allem Gesundheits-, Bank- oder Kreditkartendaten) einem Dritten unbefugt zur Kenntnis gelangen.

- Vermutet ein User, dass ein unbefugter Zugriff über Mobilgeräte auf Unternehmensdaten erfolgt ist oder erkennt er eine Sicherheitslücke, muss er dies der IT-Abteilung und dem Datenschutzteam mitteilen. Nutzen Sie auch hier servicedesk@loewe.de oder datenschutz@loewe.de.

- Die Umgehung der vom Hersteller vorgesehenen Sicherheitsfunktionen durch Jailbreak oder Rooting ist ausnahmslos nicht gestattet. Der Einsatz von Geräten mit manipulierter Firmware ist verboten.

- Es dürfen keine Raubkopien oder illegale Inhalte auf die Geräte geladen und dort benutzt werden.

- Apps aus nicht vertrauenswürdigen Quellen dürfen niemals installiert werden.
  Die Installation von „nicht dienstlichen“ Apps aus einer vertrauenswürdigen Quelle wird aktuell toleriert. Die Kosten für den Erwerb, sowie mögliche Folgekosten sind vom Anwender selbst zu tragen. Die IT kann auch keinen Support für „nicht dienstliche“ Apps übernehmen. Bitte denken Sie immer daran, dass das Installieren einer unbekannten Anwendung unter Sicherheitsaspekten grundsätzlich problematisch sein kann. Es können dadurch auch Sicherheitsfunktionen deaktiviert oder Daten erfasst und weitergeleitet werden, die für die spezielle Anwendung gar nicht notwendig sind.

- Betriebssystem- und Sicherheitsupdates sind zeitnah durchzuführen.

- Von der Firma beschaffte Geräte dürfen nur an unternehmenseigene Computer angeschlossen werden. Bei privat beschafften Geräten sind Firmendaten, die auf nicht firmeneigenen Computern (z.B. Heim-PC) abgelegt werden, unbedingt zu verschlüsseln (z.B. verschlüsseltes Backup).

- Bei der Verknüpfung von privaten und Unternehmens-E-Mail-Konten ist stets Vorsicht geboten. Unternehmensdaten dürfen nur über die Unternehmens-E-Mail-Adresse versendet werden. Hegt ein User den Verdacht, dass Unternehmensdaten über ein persönliches E-Mail-Konto (im E-Mail-Text oder als Attachment) verschickt wurden, so muss er die IT-Abteilung via servicedesk@loewe.de umgehend darüber in Kenntnis setzen.

- Ein Austausch von Mails zwischen privater und dienstlicher Mailbox ist nicht erlaubt.

- Cloud-Dienste, wie z.B. iCloud, Dropbox oder WeTransfer, dürfen für die Ablage und den Austausch von Firmendaten nicht genutzt werden. Sofern eine Verschlüsselung der im Cloud-Speicher abgelegten Daten bereits lokal am Endgerät erfolgt und die Daten nicht unverschlüsselt in den Cloud-Speicher übertragen und dort abgespeichert werden, kann die Nutzung geduldet werden (z.B. Boxcryptor). Dies ist aber mit der IT im Vorfeld abzustimmen.

  Zum einfachen Datenaustausch steht die „**Loewe-Cloud“**-Lösung zur Verfügung. Hier werden die Daten im Loewe eigenen Rechenzentrum gehostet.

- Die regelmäßige Durchführung von Backups des dienstlichen mobilen Endgerätes obliegt dem Nutzer. Der IT-Abteilung hilft bei evtl. auftretenden Problemen.

- Die Nutzung für private Apps, Emails etc. wird toleriert, solange für Loewe keinerlei Schaden entsteht und keine der anderen Bestimmungen in der Richtlinie verletzt wird.

- Die Weitergabe bzw. Nutzung der Geräte durch Dritte (Familie, Freunde, Firmenfremde), auch kurzfristig, ist untersagt.

- Es darf keine direkte Verbindung zum internen Firmennetzwerk hergestellt werden. Erlaubt ist nur der Zugriff über mobile Datenfunkverbindungen (z.B. UMTS) oder über das dafür vorgesehene WLAN.

2.3 Private mobile Endgeräte („**B**ring **Y**our **O**wn **D**evice**” – BYOD)**

Privat beschaffte mobile Endgeräte, die zu dienstlichen Zwecken eingesetzt werden, unterliegen den gleichen Richtlinien wie von der Firma beschaffte Geräte.

Beim Einsatz von privaten Notebooks und PCs ist der Zugriff auf Loewe-Daten und Loewe-Applikationen nur über Einrichtungen gestattet, bei denen sichergestellt werden kann, dass die Firmendaten nicht auf das Endgerät gelangen und dort abgespeichert werden (Office 365) .

Ausnahmen hiervon dürfen nur gemacht werden, wenn eine Internet-Anbindung an die zentralen IT-Systeme und damit eine Speicherung auf den IT-Systemen nicht möglich ist. In diesen Fällen dürfen personenbezogene Daten auf den von den Beschäftigten verwendeten Geräten gespeichert werden, wenn sichergestellt ist, dass die Daten auf den verwendeten Datenträgern verschlüsselt gespeichert werden. Beschäftigte, die nicht sicher sind, ob ihre verwendeten Datenträger verschlüsselt speichern, könnten dies beim IT-Support nachfragen.

Die so gespeicherten Daten sind unverzüglich nach Zugriff auf das Firmennetzwerk wieder zu löschen. Falls erforderlich sind die Daten auf den zentralen Systemen zu aktualisieren. Temporäre Speicher sind ebenfalls regelmäßig zu löschen.

Eine Speicherung oder Weiterleitung an weitere Orte die nicht unter der Kontrolle des Unternehmens liegen (Dropbox, Nextcloud, Owncloud, OneDrive, iCloud, Google Drive oder

vergleichbare Angebote) ist nicht zulässig.

Mobile Endgeräte ermöglichen die schnelle und einfache Erstellung von bildlichen Darstellungen / Kopien von Unterlagen, Orten, Menschen. Diese Fotografien sind auf das betrieblich erforderliche Maß zu begrenzen. Die rechtlichen Vorgaben zum Recht am eigenen Bild werden durch die Nutzung der betrieblich bereitgestellten Hardware an das Unternehmen abgetreten.

Eine Abbildung natürlicher Personen ohne Einwilligung ist nicht zulässig.

Hiermit wird ausdrücklich darauf hingewiesen, dass mobile Geräte auf Dienstreisen oder auf der Fahrt zwischen Arbeitsplatz und Wohnort sicher zu transportieren und ggf. zu verschließen sind.

3 Netzwerk

Das IT-Netzwerk im Unternehmen ist mit dem zentralen Nervensystem des menschlichen Körpers vergleichbar. Das Rechenzentrum entspricht quasi dem Gehirn, in dem alle Informationen zusammenlaufen. Störungen in einem Segment können Probleme in einem ganz anderen Bereich hervorrufen. Ohne Netzwerk funktioniert von der Entwicklung über die Pforte bis zur Fertigung kein Bereich. Entsprechend wichtig für einen reibungslosen Geschäftsbetrieb sind daher Sicherheit und Verfügbarkeit.

3.1 Allgemein

Generell sind alle Veränderungen am Netzwerk verboten, welche nicht ausdrücklich erlaubt oder mit der IT abgesprochen sind.

3.1.1 Beispiele für untersagte Aktionen

- Testen aller Netzwerkdosen, um in ein Netzwerk zu gelangen
- Anschließen von unbekannten bzw. nicht durch die IT eingerichteten Geräten
- Nutzung von Netzwerken ohne entsprechende Berechtigung
- Eigens errichtete Insellösungen jeglicher Art, die nicht von der IT genehmigt wurden

3.1.2 Folgende Tätigkeiten sind mit von der IT verwalteten Geräten erlaubt

- IP-Telefone, Notebooks und PCs können selbst an das Netzwerk angeschlossen werden, sofern die Netzwerkdose eindeutig beschriftet ist und entsprechende Kenntnisse vorhanden sind

- Notebooks oder PCs können an ein vorhandenes IP-Telefon angeschlossen werden

3.2 WLAN

3.2.1 Firmen WLAN

Das Firmen-WLAN wird auf allen Geräten ausschließlich von der IT eingerichtet. Einzige Ausnahmen stellen hier die sog. Labor LAN´s und das Gäste WLAN dar.

3.2.2 Labor LAN´s

- Dürfen nur für den vorgesehenen Verwendungszweck verwendet werden.
- Der Zugang (WPA2-KEY) wird entweder von der IT oder von hierzu befugten Anwendern aus dem Fachbereich ausgegeben bzw. eingetragen. Die Herausgeber sind für einen gewissenhaften Umgang selbst verantwortlich.
- Stellen in der Regel eine Heimsituation nach und haben keinerlei Sicherheitsmechanismen die über den Heimanwenderbereich hinausgehen. Von daher ist ein gewissenhafter Umgang Voraussetzung.

3.2.3 Gäste WLAN

- Diese Lösung dient ausschließlich dafür, Besuchern von Loewe einen Internetzugriff zur Verfügung zu stellen.
- Ausgewählten Mitarbeitern mit einem Windows AD-Account ist es generell erlaubt als Sponsor für einen Gastzugang zu fungieren. Diese freizügige Regelung setzt einen gewissen- haften Umgang voraus. Sollten die Regularien nicht eingehalten werden, kann dies ohne Information oder Ankündigung unterbunden werden.
- Bitte stellen Sie die Richtigkeit der Daten sicher. Wir sind verpflichtet diese korrekt zu erfassen.
- Genehmigen Sie keine Anfragen, bei denen Sie nicht sicher sind. Sie tragen dafür die Verantwortung.
- Es ist verboten eigene Geräte freizuschalten. Bei Bedarf kontaktieren sie bitte den Servicedesk
- Es ist ebenso untersagt, Geräte für einen längeren Zeitraum freizuschalten. Bei einer Dauer über 5 Werktage ist die IT zu informieren.

4 Urheberrechtsschutz, Lizenzschlüssel und sonstige IT-Sicherheitseinrichtungen

- Von der IT-Infrastruktur bereitgestellte Software, Dokumentationen und Daten dürfen weder kopiert noch an Dritte weitergegeben werden, sofern dies nicht zur Erfüllung Ihrer

betrieblich bedingten Aufgaben erforderlich ist und auch nicht zu anderen als den erlaubten Zwecken genutzt werden.

- Bei der Benutzung von Software, Dokumentationen und sonstigen Daten sind die gesetzlichen Vorgaben, insbesondere zum Urheberrechtsschutz und Copyright, einzuhalten und die Lizenzbedingungen, unter denen Software, Dokumentationen und Daten zur Verfügung gestellt werden, zu beachten.

- Die Ermittlung und Erzeugung von Lizenzschlüsseln (z.B. von Software) und deren unbefugte Weiterverwendung ist untersagt.

- Zentral von der IT installierte oder eingerichtete Sicherheitsmechanismen, wie Antivirensoftware, Personal Firewalls, Profileinstellungen etc. dürfen nicht deaktiviert oder verändert werden. Dies gilt besonders für mobile Endgeräte (iPhone, iPad, etc.).

- Die Beschädigung oder Störung von elektronischen Diensten ist verboten (z. B. Denial-of-Service-Attacken).

- Der Einsatz von sog. Netzwerkscannern oder anderen Netzwerk-Analysetools ist generell verboten. Ausnahmen können nach Rücksprache mit der IT gewährt werden, falls dem Einsatz eine dienstliche Anforderung zugrunde liegt, deren Erfüllung nicht mit anderen Mitteln erreicht werden kann.

- Es gibt eine Reihe weiterer Programme und Tools, deren Installation und/oder Einsatz aus sicherheits- und/oder datenschutzrechtlichen Gründen einer besonderen Genehmigung der IT bedürfen. Nutzen Sie daher nur die Programme und Tools, die Ihnen von der IT zur Verfügung gestellt wurden. Sollten Sie darüber hinaus ein anderes Programm oder Tool einsetzen wollen, wenden Sie sich an die IT.

5 Benutzerkonten und Passwörter

- Lassen Sie ungesicherte IT-Systeme nicht unbeobachtet. Nutzen Sie stattdessen die angebotenen Sicherheitsmechanismen, wie z. B. Bildschirmschoner mit Passwortschutz.

- Halten Sie Ihre Passwörter vertraulich und geben Sie diese nicht weiter.

- Wechseln Sie Ihre Passwörter mindestens einmal jährlich.
- Wählen Sie keine Passwörter, die Sie schon einmal in der Vergangenheit verwendet haben.
- Nutzen Sie keine Passwörter, die leicht zu erraten sind.
- Die minimale Länge für Passwörter beträgt 12 Zeichen.
- Jedes Passwort muss mindestens eine Ziffer, einen Klein- und einen Großbuchstaben enthalten.
- Die erneute Wiederverwendung eines Passwortes ist nicht erlaubt.
- Hinweis: Sollten Sie Smartphones oder Tablet-Computer nutzen, dann sollten Sie auf Sonderzeichen verzichten, da bei mobilen Geräten die Eingabe von bestimmten Sonderzeichen oft nur sehr schwer oder gar nicht möglich ist.
- Sollten Sie Ihre Passwörter aufschreiben, dann verwahren Sie sie an einem sicheren Ort. Hierzu gibt es auch IT-Lösungen, wie Passwortsafes. Informationen dazu erhalten Sie ebenfalls vom IT-Benutzerservice.
- Achten Sie darauf, dass niemand bei der Eingabe des Passworts mitlesen oder Ihre Tastatureingabe verfolgen kann.
- Fremde Benutzerkennungen und Passwörter dürfen weder ermittelt noch genutzt werden. Insbesondere ist der Einsatz von Passwortermittlungsprogrammen in jeglicher Form verboten.
- Die Weitergabe von Zugangsberechtigungen an Dritte ist verboten.

6 Internet, Email und Dienste im WWW

- Öffnen Sie keine Email-Anhänge von unbekannten Absendern oder Emails mit verdächtigen Inhalt (z.B. Schreibfehler); denken Sie auch daran, dass Email-Absender-Adressen leicht zu fälschen sind.
- Online-Veröffentlichungen mit unternehmensbezogenen Informationen auf Social Sites wie Facebook, Xing etc., in Communities, Foren, Blogs, Wikis und anderen Formen

der Online Kommunikation dürfen ausschließlich durch die verantwortlichen Personen der Aufgabengebiete „Presse und Public Relations“ und „Marketing“ erfolgen. Private Online-Veröffentlichungen zu unternehmensrelevanten Themen sind hiervon ausgenommen, wenn sie als privat gekennzeichnet sind und die Regelungen von Loewe eingehalten werden.

- Die Nutzung von nicht von der IT freigegebenen Webspaces (z.B. Dropbox) für die Ablage von Firmendaten ist verboten. Dies gilt insbesondere für Daten der Geheimhaltungsstufe „vertraulich“ und „streng vertraulich“. Ebenso ist für andere „Public Cloud“-Dienste eine explizite Freigabe durch die IT erforderlich.

- Die generelle Weiterleitung von Firmen-Emails an private Email-Accounts ist nicht gestattet.

- Die Nutzung des Dienstes Outlook Anywhere auf Privat-PCs ist grundsätzlich untersagt. Falls Sie zwingend Zugang auf Ihre Emails von einem privaten PC benötigen, stehen hierfür Office 365 zur Verfügung.

- Der Mitarbeiter darf den Internetzugang am Arbeitsplatz ausschließlich für dienstliche Zwecke nutzen. Jede private Nutzung während und außerhalb der Arbeitszeit ist untersagt.

- Der Mitarbeiter darf personalisierte oder allgemeine eMail-Adressen des Arbeitgebers ausschließlich für dienstliche Zwecke benutzen. Er darf diese Adressen insbesondere nur für dienstliche Zwecke bekannt geben. Dem Mitarbeiter ist die private eMail-Nutzung während und außerhalb der Arbeitszeiten untersagt.

Denken Sie daran:

- Sie sind für alles verantwortlich

    - was unter Ihrem Benutzernamen und Ihrem Passwort und/oder
    - was durch Ihre oder die Ihnen überlassenen Endgeräte passiert.

- Die Nutzung der IT-Dienste und –Zugänge wird protokolliert und solange gespeichert, wie es für die Erfüllung der jeweiligen Aufgabe erforderlich ist.

- Sollten Sie auf ein System oder einen Prozess stoßen, an deren Konformität mit der IT-Benutzerrichtlinie oder deren Einklang mit den getroffenen Maßnahmen zur Sicherstellung der Daten- und Informationssicherheit Sie zweifeln, informieren Sie bitte zeitnah den Datenschutzkoordinator - oder die IT . Ein Ausnutzen erkannter Sicherheitsmängel bzw. administrativer Mängel ist verboten.

7 Homeoffice / mobiles Arbeiten

Es wird ausschließlich die von Loewe bereitgestellte oder genehmigte Hard- und Software genutzt. Ausnahmen zur Nutzung bestimmter privater Geräte sind nach vorheriger Absprache mit der IT-Abteilung und ggf. Vorgaben zur Benutzung/Bedienung sowie im Rahmen der Bring Your Own Device Regelung (BYOD) möglich und bleiben stets auf das einzelne Gerät beschränkt.

Alle Mitarbeiter sind verpflichtet, alle sie oder ihre Tätigkeit betreffenden Richtlinienvorgaben oder Anweisungen im Umgang mit personenbezogenen Daten auch bei der Arbeit im „Homeoffice / mobilem Arbeiten“ einzuhalten. Dies gilt insbesondere für Vorgaben, die die Sicherheit personenbezogener Daten betreffen.

Daten sind grundsätzlich nicht auf lokalen Festplatten oder Datenspeichern von Endgeräten zu speichern, die nicht im Eigentum oder Besitz der Firma stehen.

Die Speicherung von Daten hat grundsätzlich in den Verzeichnissen/Ordnern von Servern bzw. zentralen IT-Systemen der Firma zu erfolgen, die für den Benutzer freigegeben sind. Ausnahmen hiervon dürfen nur gemacht werden, wenn eine Internet-Anbindung an die zentralen IT-Systeme und damit eine Speicherung auf den IT-Systemen nicht möglich ist. In diesen Fällen dürfen personenbezogene Daten auf den von den Beschäftigten im „Home-Office/mobilem Arbeiten“ verwendeten Geräten gespeichert werden, wenn sichergestellt ist, dass die Daten auf den verwendeten Datenträgern verschlüsselt gespeichert werden. Beschäftigte, die nicht sicher sind, ob ihre verwendeten Datenträger verschlüsselt speichern, könnten dies beim IT-Support nachfragen.

Beschäftigte, die im „Homeoffice / mobilem Arbeiten“ arbeiten, haben sicherzustellen, dass andere Personen keinen Zugang zu den im Zusammenhang mit der Beschäftigung verarbeiteten Daten erhalten. Dies gilt insbesondere für Personen, die in demselben Haushalt leben.

Beschäftigte müssen daher beim Verlassen des „Homeoffice / mobilem Arbeiten“ -Arbeitsplatzes unverzüglich eine Bildschirmsperre aktivieren, die nur mit einem Passwort aufgehoben werden kann, das dem Beschäftigten bekannt ist.

Dokumente sollten grundsätzlich nicht im „Homeoffice / mobilem Arbeiten“ ausgedruckt werden. Sollte dies für die Erledigung von betriebsbedingten Aufgaben zwingend erforderlich sein, hat der Beschäftigte Sorge dafür zu tragen, dass die ausgedruckten Informationen auch direkt vor Ort geeignet vernichtet werden können.

Besonders schutzbedürftige Informationen sollten nach Möglichkeit nur an Orten im „Homeoffice / mobilem Arbeiten“ verarbeitet werden, die von Dritten nicht einzusehen sind. Sollte dies nicht möglich sein, muss der Nutzer einen Ort bzw. Platz zur Verarbeitung von Daten wählen, der gewährleistet, dass der Bildschirm nicht von Dritten eingesehen werden kann.

8 Benutzerkonten und Passwörter – Regelungen für ausscheidende Mitarbeiter

Für ausscheidende Mitarbeiter gibt es ein Austrittsformular im „Workspace Loewe“ unter Corporate Company Documents. In diesem „Laufzettel“ sind alle Stellen aufgeführt, die Sie vor Ihrem Ausscheiden bei Loewe aufsuchen müssen, um sich dort die Abmeldung bzw. Rückgabe von Gegenständen bescheinigen zu lassen. In Bezug auf die auch nach Ihrem Ausscheiden zu gewährleistende IT-Sicherheit ist folgendes zu beachten:

Das Austrittsformular sollte mindestens eine Woche vor dem Austritt (d.h. eine Woche vor dem Austrittsdatum oder eine Woche vor dem Freistellungsdatum, je nachdem, welches Datum zuerst kommt) in der IT vorliegen. Dieses Datum entspricht im Nachfolgenden dem Tag des Beschäftigungsendes.

Sofern bei Vorlage des Austrittsformulars keine abweichenden Vereinbarungen in Abstimmung mit Ihrem Vorgesetzten getroffen wurden, gilt für Ihre Benutzerkonten und Daten folgende Regelung:

- Deaktivierung des **Windows Benutzerkontos,** wird am Tag des Beschäftigungsendes deaktiviert und nach weiteren 90 Tagen gelöscht.

- Die Daten auf dem **persönlichen Laufwerk M:** des Mitarbeiters werden am nächsten Werktag nach dem Beschäftigungsende des Mitarbeiters archiviert und für 6 Monate aufbewahrt.

- Die Daten im **Postfach** des Mitarbeiters werden am nächsten Werktag nach dem Beschäftigungsende des Mitarbeiters archiviert und nach 90 Tagen gelöscht.

- Die **Email-Adresse** wird am nächsten Werktag nach dem Beschäftigungsende des Mitarbeiters deaktiviert.

- Zugänge für **SAP, SAP-Subsysteme, CRM und alle weiteren Systeme** werden zum Beschäftigungsende deaktiviert.

- **Telefonnummer und Voice Mail** werden am nächsten Werktag nach dem Beschäftigungsende des Mitarbeiters deaktiviert und gelöscht.

- **Personalisierte FTP- und AdHoc-Transfer-Zugänge, sowie Zugänge zu „privaten Clouds“** werden am nächsten Werktag nach dem Beschäftigungsende des Mitarbeiters gelöscht.

9 Definition Geheimhaltungsstufen von Dokumenten

„Streng vertraulich“

Firmenvertrauliche Informationen, deren unerwünschte Offenlegung oder Weitergabe an Dritte einen sehr schweren Schaden für die Geschäftszwecke und Ziele des Hauses, gravierende rechtliche Konsequenzen oder eine schwere Schädigung des Ansehens nach sich ziehen können. Dies sind üblicherweise Informationen, die für den Erfolg und das Weiterbestehen des Unternehmens von größter Bedeutung sind, z.B.:

- Firmenstrategien
- technologische, strategische Planungen
- Informationen über geplante Firmenübernahmen oder Firmenverkäufe
- Wirtschafts- und Budgetpläne
- Informationen über Produktionsverfahren und Innovationen
- bisher nicht veröffentlichte Produkt- und Entwicklungspläne
- Informationen gleicher Vertraulichkeit von Geschäftspartnern
- Informationen über Krisensituationen
- personenbezogene Daten i.S.d. Bundesdatenschutzgesetzes und der DSGVO

„Vertraulich“

Firmenvertrauliche Informationen, deren unerwünschte Offenlegung oder Weitergabe an Dritte einen erheblichen finanziellen Schaden, rechtliche Konsequenzen oder eine Schädigung des Ansehens nach sich ziehen kann. Hier werden in der Regel alle Informationen eingeordnet, die für den technischen oder finanziellen Erfolg des Unternehmens von Bedeutung sind. Insbesondere sind dies alle Informationen, deren Kenntnis für Mitbewerber von Wert sein kann, z.B.:

- Sicherung der Wettbewerbsfähigkeit, wie Marketingdaten
- Patentunterlagen vor ihrer Offenlegung
- Kunden- und Lieferantendaten
- Strategische Planungen, Firmenpolitik, Umsatzdaten vor der offiziellen Bekanntgabe
- neue Produkte und deren Freigabedaten vor offizieller Bekanntgabe
- Geschäftsanbahnungen, Revisionsergebnisse
- Vertragsentwürfe, Verträge und Vereinbarungen mit vertraulichem Inhalt

- Entwicklungs- und Konstruktionsunterlagen
- Softwarelösungen und -Produkte, insbesondere deren Source Codes
- vertrauliche Informationen Dritter (v.a. im Rahmen von Geheimhaltungsvereinbarungen)
- Informationen über Sicherheitsmaßnahmen sowie schwerwiegende Schwachstellen
- Informationen über die internen Netzwerktopologien (EDV)

„Offen“

Alle Dokumente, die nicht in die Kategorien „streng vertraulich“ oder „vertraulich“ fallen.

10 Anmerkung

Die obige Auflistung für „streng vertrauliche“ und „vertrauliche“ Informationen ist nur als Orientierungsbeispiel zu sehen und erhebt keinen Anspruch auf Vollständigkeit. Es muss jeder Bereich selbst die vorhandenen internen Informationen und Dokumente den erwähnten Vertraulichkeitsstufen zuordnen und diese deutlich mit der jeweiligen Vertraulichkeitsstufe kennzeichnen.

11 Allgemeine Gesetze

Auf die folgenden Gesetze und Paragraphen wird hinsichtlich etwaiger Verstöße und möglichen Konsequenzen besonders hingewiesen:

- **Bundesdatenschutzgesetz (BDSG)**
- **Datenschutzgrundverordnung (DSGVO)**
- **Strafgesetzbuch (StGB):**
  - Ausspähen von Daten (§ 202a)
  - Datenveränderung (§ 303a) und Computersabotage (§ 303b)
  - Computerbetrug (§ 263)
  - Verbreitung pornographischer Schriften (§ 184), insbesondere Verbreitung, Erwerb und Besitz kinderpornographischer Darstellungen Schriften (§ 184)

- Verbreitung von Propagandamitteln verfassungswidriger Organisationen (§ 86) und Volksverhetzung (§ 130)

- **Urhebergesetz (UrhG)**

  - strafbare Urheberrechtsverletzungen, z. B. durch urheberrechtswidrige Vervielfältigung von Software (§§ 106 ff.).

Glossar:

App (allgemein) = Abkürzung für Applikation (Anwendungsprogramm)
App (speziell) = Anwendungsprogramm, das über ein Onlineportal bezogen werden kann
CD = Compact Disc
Cloud = IT-Infrastrukturen werden dynamisch über das Intranet/Internet zur Verfügung gestellt
DVD = Digital Versatile Disc
EU = Europäische Union
IT = Informationstechnologie
IT-System = jedes informationsverarbeitende System, speziell auch Arbeitsplatzcomputer
IT-Komponente = Teil eines IT-Systems
Jailbreak = das Entfernen von Nutzungsbeschränkungen bei mobilen Endgeräten, die durch den Hersteller aus Sicherheitsgründen gesperrt sind (s.a. Rooting)
Notebook = Transportabler Computer
Personal Firewall = lokal auf dem PC/Notebook installierter Schutz gegen unberechtigte Angriffe aus dem Internet
Private Cloud = Bereitstellung erfolgt ausschließlich über das firmeninterne Netz
Public Cloud = Bereitstellung erfolgt durch externe Anbieter über das Intranet
Smartphone = Ein Mobiltelefon, das mehr Computerfunktionalität und -konnektivität als ein herkömmliches fortschrittliches Mobiltelefon zur Verfügung stellt. Erste Smartphones vereinigten die Funktionen eines PDA bzw. Tablet-Computers mit der Funktionalität eines Mobiltelefons (Quelle: Wikipedia).
Tablet-Computer = Ein tragbarer, flacher Computer in besonders leichter Ausführung mit einem Touchscreen-Display, anders als beim Notebook ohne ausklappbare Tastatur. Aufgrund der leichten Bauart und dem berührungsempfindlichen Bildschirm zeichnen sich Tablet-PCs durch eine einfache Handhabung aus (Quelle: Wikipedia).
USB-Stick = Universal Serial Bus: Kleine mobile Datenspeicher

BDSG = Bundesdatenschutzgesetz
DSGVO = Datenschutzgrundverordnung
StGB = Strafgesetzbuch
UrhG = Urhebergesetz