IT-Sicherheitsrichtlinie

Stand 12.05.2025 Version 2.0

1 Einleitung

IT-Sicherheit geht uns alle an und unterliegt den Vorgaben der DSGVO sowie weiteren relevanten Datenschutzgesetzen. Diese IT-Sicherheitsrichtlinie definiert verbindliche Regeln und Maßnahmen zur sicheren Nutzung der IT-Ausstattung und zum Schutz der Unternehmensdaten.

Eine stabile und sichere IT-Infrastruktur ist die Grundlage für unseren täglichen Arbeitsablauf. Ein Ausfall oder eine Beeinträchtigung kann schwerwiegende unternehmensweite monetäre und imageschädigende Folgen haben. Die von uns eingesetzten technischen Schutzmaßnahmen wie Firewalls oder Virenscanner bieten zwar einen wichtigen Grundschutz, können jedoch nicht jede Bedrohung vollständig erkennen oder abwehren.

Für die Aufrechterhaltung und kontinuierliche Verbesserung unseres Sicherheitsniveaus müssen alle Mitarbeitenden jederzeit verantwortungsvoll handeln und die technischen Sicherheitsregeln strikt einhalten. Nur so lassen sich Angriffe wirksam verhindern und Schäden minimieren.

Deshalb ist ein sicherheitsbewusster und verantwortungsvoller Umgang mit der IT-Ausstattung und unseren Systemen unverzichtbar, um Risiken effektiv zu minimieren. Gemeinsam sorgen wir dafür, dass unsere Daten und Systeme sicher bleiben.

2 Geltungsbereich

Die Richtlinie gilt für alle Mitarbeitenden der Abacus Experten GmbH (nachfolgend „*Unternehmen*“ genannt) sowie für externe Dienstleister, die Zugriff auf die IT-Systeme oder Daten des Unternehmens haben. Weitere Vereinbarungen, wie z. B. der jeweilige Arbeitsvertrag oder andere einschlägige Richtlinien, bleiben hiervon unberührt und gelten zusätzlich.

3 Grundsätzliche Informationen im Umgang mit IT-Systemen

3.1 Generelle Verbote

Unzulässig ist jede Nutzung des Internets, die geeignet ist, den Interessen des Arbeitgebers oder dessen Ansehen in der Öffentlichkeit zu schaden, die Sicherheit des Unternehmensnetzes zu beeinträchtigen oder die gegen geltende Rechtsvorschriften verstößt. Dies gilt vor allem für

- das Abrufen oder Verbreiten von Inhalten, die gegen persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen,
- das Abrufen oder Verbreiten von beleidigenden, verleumderischen, verfassungsfeindlichen,
- rassistischen, sexistischen, gewaltverherrlichenden oder pornografischen Äußerungen oder Abbildungen.

3.2 Protokollierung der Aktivitäten

Zur Überprüfung der Einhaltung der Regelungen dieser Vereinbarung führt eine von der Geschäftsführung beauftragte Person regelmäßige Stichproben in den Protokolldateien durch. Diese werden 24/7 automatisch durch die internen Protokollsysteme erfasst.

Die bei der Nutzung der Internetdienste anfallenden personenbezogenen Daten werden nicht zur Leistungs- und Verhaltenskontrolle verwendet. Sie unterliegen der Zweckbindung dieser Vereinbarung und den einschlägigen datenschutzrechtlichen Vorschriften.

Ergibt die Auswertung der Protokolle einen Hinweis auf Missbrauch, werden die Mitarbeiter hierauf in allgemeiner Form hingewiesen. Ferner erfolgt der Hinweis, dass fortgesetzter Missbrauch die vollständige personenbezogene Auswertung der Protokolle nach sich zieht und (arbeits-)rechtliche Konsequenzen zur Folge hat. Die personenbezogene Auswertung der Protokolle darf nur in Anwesenheit des zuständigen Datenschutzbeauftragten erfolgen.

4 IT-Ausstattung

4.1 Beschaffung

Die Beschaffung der IT-Ausstattung (Hard- und Software) erfolgt ausschließlich durch das Unternehmen. Alle Beschaffungs- und Implementierungsprozesse werden vom Unternehmen dokumentiert, um Nachvollziehbarkeit, Sicherheit und eine langfristige Administrierbarkeit sicherzustellen. Dabei werden Kriterien berücksichtigt, die sich an den Anforderungen des Gesamtkonzepts zur IT-Sicherheit sowie an der Stabilität und Effizienz des Gesamtsystems orientieren.

Die IT-Ausstattung, die Ihnen zur Ausübung Ihrer beruflichen Tätigkeit überlassen wird, ist sorgfältig zu behandeln. Sie sind dafür verantwortlich, diese vor Verlust, Diebstahl, Beschädigung oder Missbrauch zu schützen und sicherheitsrelevante Vorfälle unverzüglich dem Unternehmen zu melden.

4.2 Installation, Konfiguration und Betrieb

Der IT-Abteilung ist für die Installation, Konfiguration und den Betrieb der eingesetzten Software verantwortlich. Alle Schritte erfolgen ausschließlich nach vorheriger schriftlicher und dokumentierter Freigabe durch die zuständigen Vorgesetzten. Dies gewährleistet, dass installierte Software legal, lizenziert, korrekt konfiguriert und virenfrei ist.

Installation von Software: Die Installation oder Nutzung von Fremdsoftware (z. B. Downloads oder private Programme) auf Unternehmensgeräten ist ohne vorherige Prüfung und Freigabe durch die IT-Abteilung untersagt. Bitte senden Sie dazu eine E-Mail an: helpdesk@abacus-it-experten.de

Konfigurationsänderungen: In unseren IT-Systemen sind Konfigurationen der Endgeräte zentral gesteuert und können nicht durch die Benutzer verändert oder gelesen werden. Manuelle Konfigurationsänderungen sind stets durch unsere IT-Abteilung durchzuführen und zu protokollieren. Andernfalls stellen solche Änderungen einen Verstoß gegen diese Richtlinie dar.

Betrieb: Der Zugang zu tätigkeitsbezogener Software erfolgt in der Regel über individuelle Benutzerkonten, die durch persönliche Passwörter geschützt sind. Die Beantragung des Zugangs erfolgt über den Vorgesetzten, der die notwendigen Schritte koordiniert.

Passwörter werden Ihnen über einen sicheren Kommunikationsweg bereitgestellt und müssen unverzüglich nach Erhalt gemäß den Vorgaben geändert werden.

Stellen Sie sicher, dass die IT-Ausstattung außerhalb des Arbeitsortes stets sicher aufbewahrt wird und unbefugten Dritten nicht zugänglich ist. Arbeiten Sie regelmäßig mobil, wird empfohlen die Geräte durch Taschen oder Hüllen zu schützen.

5 Private Nutzung der IT-Ausstattung

Die IT-Ausstattung darf unter den nachfolgenden Voraussetzungen privat genutzt werden:

Zeitliche Einschränkung: Die private Nutzung (IT-Ausstattung ohne E-Mail-Account) ist nur außerhalb der Arbeitszeit erlaubt.

Sicherheitsanforderungen: Die private Nutzung darf keine sicherheitskritischen Risiken verursachen. Insbesondere ist die Installation unerlaubter Software und der Zugriff auf potenziell unsichere Webseiten und Dienste untersagt.

Zusammengefasste Verbote sind:

- Abruf kostenpflichtiger Informationen oder Dienste (z. B. Spiele oder Online-Plattformen) für private Zwecke.
- Aufrufen oder Versenden von Inhalten, die gegen Menschenwürde oder rechtliche Vorgaben verstoßen (z. B. pornografische, rassistische, extremistische, verfassungsfeindliche Inhalte).
- Nutzung der IT-Ausstattung für illegale Zwecke, einschließlich Urheberrechts- und Datenschutzverstöße.
- Installation von Software ohne Genehmigung der IT-Abteilung oder des Unternehmens.
- Download oder Speicherung privater Medieninhalte (z. B. Filme, Musik, Spiele) sowie privater Spiele auf Unternehmensgeräten.
- Teilnahme an interaktiven Spielen, Online-Plattformen oder Chatrooms zu privaten Zwecken.
- Verbreitung von Kettenmails/-nachrichten, Spam sowie belästigenden E-Mails oder Nachrichten.

Weitere Regelungen:

Die Nutzung der IT-Ausstattung für berufliche Nebentätigkeiten ist nicht erlaubt. Eine Ausnahme ist nur mit schriftlicher Genehmigung der Geschäftsführung möglich.

Private Kontakte auf IT-Geräten, insbesondere mobilen Endgeräten, müssen so gespeichert werden, dass sie jederzeit problemlos vom Mitarbeitenden gelöscht werden können – insbesondere vor der Rückgabe des Geräts.

Private Daten dürfen nur gespeichert werden, wenn sie weder gegen geltendes Recht verstoßen noch Urheberrechte verletzen. Das Unternehmen übernimmt keine Haftung für die Sicherheit, Vertraulichkeit oder Verfügbarkeit dieser Daten. Auf Anweisung sind private Daten unverzüglich zu löschen. Die Speicherung privater Daten auf unternehmensseitig bereitgestellten Netzlaufwerken oder Cloud-Diensten ist untersagt.

Der berufliche E-Mail-Account ist ausschließlich für berufliche Zwecke zu nutzen. Private E-Mails müssen über externe Anbieter (z. B. Webmail-Dienste) abgewickelt werden.

Freiwilligkeit der Erlaubnis zur privaten Nutzung: Die Erlaubnis zur privaten Nutzung der IT-Ausstattung ist eine freiwillige Leistung. Es besteht hierauf kein Rechtsanspruch, auch nicht für die Zukunft, soweit keine individuelle, gesonderte Absprache (§ 305b BGB) mit Ihnen vorliegt. Somit kann die Geschäftsführung die Erlaubnis zur privaten Nutzung jederzeit entziehen.

6 Nutzung privater Hard- und Software

Die Nutzung privater Hard- und Software für geschäftliche Zwecke ist untersagt. Lediglich private Bildschirme, Mäuse, Tastaturen, Webcams und Headsets sind im mobilen Arbeiten erlaubt. Auch die Nutzung privater Speichermedien für geschäftliche Zwecke ist nicht erlaubt. Bei Bedarf werden entsprechende Speichermedien durch das Unternehmen zur Verfügung gestellt.

7 Absicherung des IT-Systemzugangs

7.1 Zutritts- und Zugangskontrolle

Mitarbeitende müssen ihre persönlichen Zutritts- und Zugangskennungen (z. B. Benutzerkonten, Zugangsschlüssel oder Ausweise) stets sorgfältig schützen und sicherstellen, dass sie nicht in die Hände unberechtigter Dritter gelangen.

Die Weitergabe oder unautorisierte Nutzung von Zutritts- oder Zugangskennungen an Dritte einschl. Kollegen/innen ist verboten. Wenn ein Verdacht auf Missbrauch besteht oder Zugriffsrechte nicht mehr benötigt werden, ist dies unverzüglich zu melden und die Deaktivierung zu veranlassen.

7.2 Passwörter

Sicherheitsmaßnahmen beim Umgang mit Passwörtern:

- Passwörter dürfen nicht an Dritte einschl. Kollegen/innen weitergegeben werden, es sei denn, es handelt sich um genehmigte geteilte Accounts mit gesonderter Sicherheitsfreigabe.
- Passwörter sind auf Anforderung der IT-Abteilung oder bei Verdacht auf Missbrauch unverzüglich zu ändern.
- Für jeden Account muss ein einzigartiges Passwort verwendet werden. Die Verwendung desselben Passworts für mehrere Konten ist nicht gestattet.
- Voreingestellte Passwörter müssen unmittelbar nach der Ersteinrichtung geändert werden.
- Passwörter sind vertraulich zu behandeln und sicher aufzubewahren. Die Nutzung eines von der IT-Abteilung freigegebenen Passwort-Managers ist empfohlen. Haftnotizen mit Passwörtern oder ähnliches sind unzulässig.
- Bei der Eingabe von Passwörtern ist darauf zu achten, dass Dritte diese nicht einsehen können.
- Das gezielte Ausforschen, Testen oder die unbefugte Nutzung fremder Zugriffsberechtigungen sind strikt untersagt.
- Falls elektronische oder physikalische Zugangs- oder Zutrittsberechtigungen nicht mehr benötigt werden, ist deren Deaktivierung umgehend zu veranlassen.

Verbindliche Passwortrichtlinie:

- Passwörter müssen mindestens zwölf Zeichen lang sein.
- Die Kombination aus leicht erratbaren Informationen (z. B. Geburtstagen, Abteilungen, Tel.-Durchwahlen, Namen von Familienangehörigen oder Haustieren sowie gängigen Tastaturmustern wie ‚1234abcd') ist unzulässig.
- Jedes Passwort muss aus mindestens drei der folgenden vier Zeichenarten bestehen:
    - Großbuchstaben.
    - Kleinbuchstaben.
    - Sonderzeichen (z. B. !, $, %).
    - Ziffern.

Mehrfaktor-Authentifizierung (MFA):

Multi-Faktor-Authentifizierung (MFA) ist eine Authentifizierungsmethode, bei der der Benutzer zwei oder mehr Verifizierungsfaktoren angeben muss, um Zugang zu einer Ressource wie einer Anwendung, einem Online-Konto oder einem VPN zu erhalten.

Sofern technisch möglich, wird die Mehrfaktor-Authentifizierung (MFA) für alle relevanten Systeme und Anwendungen verpflichtend eingesetzt. Wo MFA eingesetzt wird, ist sie aktiv zu halten und darf nicht deaktiviert werden.

7.3 Rollen- und Berechtigungssystem durch die IT

Das Rollen- und Berechtigungssystem ist eine zentrale datenschutzrechtliche Maßnahme des Unternehmens. Es stellt sicher, dass ausschließlich berechtigte Personen auf die ihrer Zugriffsberechtigung entsprechenden Daten in einem Datenverarbeitungssystem zugreifen können. Zugleich gewährleistet es, dass personenbezogene Daten bei der Verarbeitung, Nutzung sowie nach der Speicherung nicht unbefugt gelesen, kopiert oder entfernt werden können.

Das Rollen- und Berechtigungskonzept ist verbindlich von der Geschäftsführung und dem IT-Verantwortlichen festzulegen. Es muss mit den zuständigen Stellen im Unternehmen – insbesondere dem leitenden Management – abgestimmt sein und soll die tatsächlichen Berechtigungen und Arbeitsabläufe im Umgang mit Daten möglichst vollständig und realitätsnah abbilden.

Zugriffsberechtigungen wie Lesen, Ändern oder Vollzugriff sind ausschließlich über Sicherheitsgruppen (z. B. Rollen- oder Ressourcengruppen) zu steuern. Dabei sind etablierte Best Practices anzuwenden.

8 Absicherung mobiler Endgeräte

8.1 Anforderung an die Mitarbeitenden:

Mobile IT-Geräte (Notebooks, Smartphones etc.) stellen durch ihre mobile Verwendung ein erhöhtes Sicherheitsrisiko dar. Diese Geräte sind für Diebe ein attraktives Ziel.

Bitte beachten Sie folgende Punkte:

- Lassen Sie das Gerät nicht unbeaufsichtigt.
- Überlassen Sie das Gerät nicht anderen Personen.
- Achten Sie bei Passworteingabe am Gerät auf Ihren Sichtschutz.

- Verwenden Sie Ihren privaten Cloud-Speicher nicht für Unternehmensdaten.
- Installieren Sie nur Anwendungen, die Ihnen als vertrauenswürdig und sicher bekannt sind und von der IT-Abteilung freigegeben wurden.
- Melden Sie einen Diebstahl oder Verlust sofort der IT-Abteilung.

8.2 Anforderung an die IT-Abteilung

- Installation einer Speicherverschlüsselung nach Stand der Technik mit zentraler Aufbewahrung der Wiederherstellungsschlüssel.
- Installation von Anti-Schadsoftware-Lösungen mit zentraler Verwaltung/Monitoring.
- Zentrale Steuerung von Softwareupdates für die Betriebssysteme.
- Einrichtung der Möglichkeit der Fernlöschung.

9 E-Mail-Nutzung und Datenaustausch

E-Mail-Zertifikate zur Absicherung der Kommunikation:

Im Unternehmen werden E-Mail-Zertifikate standardmäßig eingesetzt, um die Sicherheit der E-Mail-Kommunikation zu erhöhen:

- Authentizität: Die Echtheit des Absenders wird sichergestellt.
- Integrität: Unbefugte Änderungen an der Nachricht werden erkannt.
- Manipulationsschutz: Gefälschte Absender und nachträgliche Manipulationen werden erschwert.

Weitere Hinweise zur Sicherheit:

E-Mail-Zertifikate schützen ausschließlich vor Manipulationen und gefälschten Absendern. Der Inhalt einer E-Mail wird dadurch jedoch nicht automatisch verschlüsselt und kann bei ungesicherter Übertragung potenziell mitgelesen werden.

Wenn vertrauliche oder sensible Daten per E-Mail versendet werden, muss eine von der IT-Abteilung freigegebene Verschlüsselungsmethode angewendet werden.

Zulässig sind:

- Passwortschutz von Microsoft Office-Dateien (Word, Excel, PowerPoint) direkt in der Datei.
- Passwortschutz von PDF-Dateien über die Verschlüsselungsfunktion von Adobe Acrobat Pro.

Alternative für besonders sensible Daten:

Der Versand vertraulicher Daten per E-Mail ist möglichst zu vermeiden. Stattdessen ist eine sichere, Ende-zu-Ende-verschlüsselte Ablage innerhalb der vom Unternehmen hierfür freigegebenen Microsoft 365-Dienste zu nutzen.

10 Datenaustausch via Cloud-Dienste

Der interne Datenaustausch erfolgt vorrangig über die vom Unternehmen bereitgestellten Microsoft 365-Dienste, die den unternehmensinternen Sicherheitsanforderungen entsprechen:

- Microsoft Teams.
- OneDrive for Business.
- SharePoint.

Diese Dienste bieten eine Ende-zu-Ende-Verschlüsselung während der Übertragung sowie eine Speicherverschlüsselung.

Darüber hinaus ist der Datenaustausch über folgende aktuell freigegebene Cloud-Dienste zulässig:

- Adobe Acrobat Pro.
- Zapflow.
- Ideanote.
- Timebutler.
- Circula.
- Deskbird.
- ELO.
- LucaNet.
- Factorial.

Richtlinie zur Nutzung anderer Cloud-Dienste:

Die Nutzung nicht freigegebener Cloud-Dienste ist untersagt. Falls ein weiterer Cloud-Dienst aus beruflichen Gründen erforderlich ist, muss vorab die Freigabe durch den KI- und Cloud-Compliance-Ausschuss erfolgen. Die Nutzung von KI-Diensten wird in einer separaten KI-Sicherheitsrichtlinie geregelt.

11 Datenaustausch via Speichermedium

Falls Daten auf externe (nicht private) Speichermedien (z. B. USB-Stick, externe Festplatte) übertragen werden müssen, gilt:

- Vertrauliche Informationen sind immer verschlüsselt abzulegen.
- Die Verschlüsselung erfolgt mit einem Passwort und nach Stand der Technik.
- Die Speicherung unverschlüsselter sensibler Daten auf Speichermedien ist nicht zulässig.
- Es dürfen nur firmeneigene oder vom der IT-Abteilung freigegebene Speichermedien verwendet werden.

12 Externe Einwahl ins Unternehmensnetzwerk

12.1 Zugriff auf Unternehmensressourcen

Der Zugriff auf Unternehmensressourcen ist ausschließlich mit vom Unternehmen bereitgestellter und administrierter Hardware zulässig. Diese unternehmenseigenen Geräte dürfen nur über sichere und ausdrücklich erlaubte Netzwerkverbindungen gemäß Kapitel 12.2 auf Unternehmensressourcen zugreifen.
Die Nutzung unverschlüsselter oder allgemein frei zugänglicher Netzwerke ist untersagt. Der Zugriff auf Netzlaufwerke über Mobiltelefone ist nicht gestattet.

12.2 Zulässige Netzwerkverbindungen und Sicherheitsstufen

Für den Zugriff auf Unternehmensressourcen sind nur bestimmte Netzwerkverbindungen zulässig. Die Sicherheitsstufen sind nach Priorität gegliedert**:**

12.2.1. Bevorzugte Standardverbindungen (ohne VPN erlaubt)

Diese Verbindungen bieten das höchste Sicherheitsniveau und können ohne VPN uneingeschränkt genutzt werden.

- Private Heimnetzwerke, sofern folgende Anforderungen erfüllt sind:
    - Anschluss per Kabel / LAN.
    - WLAN mit mindestens WPA2- oder WPA3-Verschlüsselung mit sicherem Passwort.
    - Regelmäßige Aktualisierung der Router-Firmware durch die Mitarbeitenden.
- Mobiler Hotspot über das Diensthandy.

12.2.2 Öffentliche, verschlüsselte Netzwerke (nur mit VPN erlaubt)

Diese Verbindungen bieten ein eingeschränktes Sicherheitsniveau und dürfen nur in Ausnahmefällen genutzt werden, beispielsweise wenn keine stabile Mobilfunkverbindung verfügbar ist.

<u>Mögliche Zugangsarten:</u>

- Hotel-WLANs mit WPA2 oder höher.
- Netzwerke in Konferenzräumen oder bei Partnerunternehmen mit WPA2 oder höher.

<u>Anforderungen:</u>

- Der Zugriff auf Unternehmensressourcen ist nur mit aktiver VPN-Verbindung gestattet, die vor dem Zugriff hergestellt und während der gesamten Nutzung aufrechterhalten werden muss.
- Das WLAN-Netzwerk muss mindestens WPA2- oder WPA3-verschlüsselt sein und durch ein individuelles Kennwort geschützt sein.

12.2.3 Nutzung des WLANs der Deutschen Bahn (nur mit VPN erlaubt)

Das öffentliche WLAN in ICE-Zügen (WIFIonICE) bietet ein erhöhtes Sicherheitsrisiko, da es nicht WPA2-verschlüsselt ist. Es darf nur in Ausnahmefällen genutzt werden, wenn keine stabile Mobilfunkverbindung und kein öffentliches, verschlüsseltes Netzwerk verfügbar sind.

- **Da die Deutsche Bahn Client Isolation einsetzt** - eine Sicherheitsmaßnahme, die direkte Verbindungen zwischen Geräten im Netzwerk verhindert - **und die Nutzung zwingend mit aktiver VPN-Verbindung erfolgen muss**, ist die Verwendung von WIFIonICE unter diesen Bedingungen erlaubt.
- **Der Zugriff auf Unternehmensressourcen ist nur mit aktiver VPN-Verbindung gestattet.**

12.2.4 Nutzung von Microsoft 365-Diensten (VPN bei bevorzugten Standardverbindungen nicht erforderlich)

Microsoft 365-Dienste (z. B. Teams, OneDrive, SharePoint) können im Rahmen der in Abschnitt 12.2.1 beschriebenen bevorzugten Standardverbindungen ohne VPN genutzt werden.

Dies ist zulässig, da:

- die Datenübertragung stets TLS-verschlüsselt erfolgt,
- und die gespeicherten Daten zusätzlich mit AES-256 geschützt sind.

Wird auf Microsoft 365-Dienste über öffentliche Netzwerke gemäß Abschnitt 12.2.2 oder 12.2.3 zugegriffen, so ist zwingend eine aktive VPN-Verbindung erforderlich.

12.3 Aufbau der VPN-Verbindung

Die VPN-Verbindung wird von der IT-Abteilung bereitgestellt und vorkonfiguriert. Befolgen Sie die Anleitungen der IT-Abteilung, um die Verbindung störungsfrei aufzubauen.

Hinweis:

VPN muss aktiv sein, sobald interne Unternehmensressourcen (z. B. Netzlaufwerke) genutzt werden. Microsoft 365-Dienste (z. B. Teams, OneDrive, SharePoint) sind nur unter den in Kapitel 12.2.4 genannten Bedingungen von der VPN-Pflicht ausgenommen.

12.4 Geografische Einschränkungen beim Zugriff

Der Zugriff auf Unternehmensressourcen ist innerhalb des Europäischen Wirtschaftsraums (EWR), der Schweiz und Großbritanniens ohne zusätzliche Genehmigung erlaubt. Der Zugriff aus allen anderen Ländern ist grundsätzlich gesperrt und nur nach vorheriger, expliziter Freigabe durch die IT-Abteilung zulässig.

Vor einer Freigabe erfolgt durch die IT-Abteilung eine individuelle Sicherheitsprüfung. Je nach Ergebnis dieser Prüfung legt die IT-Abteilung erforderliche Sicherheitsmaßnahmen fest, z. B.:

- Nutzung einer gehärteten VPN-Verbindung.
- Zusätzliche Authentifizierungsverfahren.

Die Freigabe erfolgt ausschließlich temporär, wird dokumentiert und archiviert.

Der Antrag auf Freigabe ist mindestens fünf Arbeitstage vor Reiseantritt per E-Mail an die IT-Abteilung zu stellen und muss eine nachvollziehbare geschäftliche Begründung enthalten.

13 Clear Desk Policy

Unter der Clear Desk Policy versteht man, dass Mitarbeitende alle vertraulichen Dokumente, die sich auf ihrem Arbeitsplatz befinden, verschließen. Unberechtigte Personen (Reinigungspersonal, unbefugte Kolleginnen und Kollegen, Besucher oder Mitbewohner) dürfen keinen Zugriff darauf erhalten.

Bitte beachten Sie folgende Punkte:

- Bei Verlassen des Arbeitsplatzes müssen alle Ausdrucke, Kopien oder dergleichen so verstaut werden, dass diese Dokumente nicht für Dritte zugänglich sind (Schreibtisch, verschließbaren Kästen, Datenträgersafe).
- Lassen Sie keine Ausdrucke im Drucker/Kopierer liegen.
- Bewahren Sie unter keinen Umständen Passwortnotizen an Ihrem Arbeitsplatz auf.
- Sperren Sie Ihren Computer, wenn Sie Ihren Arbeitsplatz verlassen. Unbeaufsichtigte, nicht gesperrte Computer sind ein hohes Sicherheitsrisiko. Unbefugte könnten so Zugang zu vertraulichen Daten erhalten.

14 Vorsicht bei Social Engineering

Unter Social Engineering versteht man das Manipulieren von Personen, um unbefugt Zugang zu vertraulichen Informationen oder IT-Systemen zu erhalten. Vorwiegend wird dieser Angriff per Telefon oder E-Mail durchgeführt. Social Engineers geben sich gerne als Mitarbeiterinnen oder Mitarbeiter aus. Möglicherweise geben sie vor, eine Behörde, ein wichtiges Kundenunternehmen oder die IT-Abteilung zu vertreten. Ihre Opfer werden durch firmeninternes Wissen oder Kenntnisse spezieller Fachbegriffe getäuscht, die sie sich zuvor durch Telefonate oder Gespräche mit anderen Kollegen erworben haben. Beim Angriff appellieren sie dann als „gestresster Kollege“ an Ihre Hilfsbereitschaft oder drohen als „Kunde“ mit dem Verlust eines Auftrages.

Bitte beachten Sie folgende Punkte:

- Seien Sie bei Telefonanrufen oder E-Mails skeptisch, speziell wenn der Wunsch oder der Auftrag der Kollegin oder des Kollegen außergewöhnlich ist.
- Falls möglich, besprechen Sie die Angelegenheit mit Ihrem Kollegen oder mit Ihrer Kollegin persönlich.
- Fragen Sie bei einer verdächtigen E-Mail bei der IT-Abteilung nach.
- Bedenken Sie, dass Social Engineering sehr oft angewandt wird, aber meistens lange Zeit unentdeckt bleibt.
- Geben Sie keine vertraulichen Informationen per Telefon oder E-Mail weiter.
- Nutzen Sie einen Schredder oder Datentonne zur sicheren Vernichtung von Daten.
- Alte Arbeitsgeräte mit Datenspeichern oder Datenspeicher selbst werden zur sicheren Vernichtung an die IT-Abteilung übergeben.

Warnungen oder Fehlermeldungen, die nicht von Ihnen verursacht wurden oder die Sie nicht selbst beheben können, sind unverzüglich der IT-Abteilung zu melden.

15 Datenspeicherung und -sicherung

Zentrale Datenspeicherung und Sicherung:

Geschäftliche Daten, die für mehrere berechtigte Personen zugänglich sein sollen, müssen auf den freigegebenen Netzlaufwerken oder innerhalb der vom Unternehmen bereitgestellten Microsoft 365-Dienste (z. B. Teams, OneDrive, SharePoint) gespeichert werden.

Alle genannten Speicherorte werden täglich entweder durch die IT-Abteilung oder durch automatisierte, verschlüsselte Backup-Lösungen gesichert und gewährleisten so einen zuverlässigen Schutz vor Datenverlust oder versehentlicher Löschung.

Lokale Speicherung auf Endgeräten:

Daten, die ausschließlich lokal auf einem Endgerät gespeichert werden, sind nicht in die zentrale Sicherung eingebunden. Datenverluste durch Geräteausfall, Diebstahl oder Cyberangriffe (z. B. Ransomware) sind in diesen Fällen nicht rückgängig zu machen.

Falls eine temporäre lokale Speicherung notwendig ist (z. B. für die Arbeit unterwegs), müssen diese Daten spätestens bis zum Tagesende auf ein freigegebenes Netzlaufwerk oder in die Microsoft 365-Dienste (z. B.: Teams, OneDrive, SharePoint) übertragen werden.

Diese Maßnahme stellt sicher, dass:

- Daten in die zentrale Backup-Strategie eingebunden sind.
- Eine Wiederherstellung im Falle eines Datenverlusts möglich ist.
- Berechtigte Kolleginnen und Kollegen jederzeit Zugriff auf aktuelle Daten haben.

16 Verhalten am (mobilen) Arbeitsplatz

Die Nutzung von IT-Systemen außerhalb des Unternehmensstandorts (z. B. im Homeoffice, auf Reisen oder bei Kunden) erfordert besondere Sicherheitsvorkehrungen. Für diese Anwendungsfälle gilt ergänzend die „Richtlinie mobiles Arbeiten“, deren Einhaltung verpflichtend ist.

17 Meldung von Sicherheitsvorfällen

Schwerwiegende Sicherheitsvorfälle (z. B. Datenverlust, Phishing-Angriffe, Malware-Infektionen) müssen sofort durch die feststellenden Mitarbeitenden, spätestens innerhalb von 2 Stunden, gemeldet werden. Alle anderen sicherheitsrelevanten Ereignisse sind spätestens innerhalb von 24 Stunden zu melden.

Die Meldung muss innerhalb obiger Fristen an die IT-Abteilung und die Geschäftsleitung erfolgen.

Das weitere Vorgehen wird durch die Geschäftsleitung und die IT-Abteilung abgestimmt, um Schäden zu minimieren und angemessene Maßnahmen einzuleiten. Soweit von dem betroffenen Mitarbeitenden oder durch andere Mitarbeitende Maßnahmen umzusetzen sind, wird dies entsprechend mitgeteilt.

Beispiele für meldepflichtige Sicherheitsvorfälle:

- Verdacht auf kompromittierte Zugangsdaten (z. B. Benutzername, Passwort könnte Dritten bekannt sein).
- Unbefugter Zugriff auf interne, vertrauliche oder personenbezogene Daten.
- Ungewöhnliche Aktivitäten (z. B. unautorisierte Zugriffsversuche, verdächtige Systemmeldungen).
- Cyberangriffe oder technische Fehler, die zu Datenverlust oder einer Systembeeinträchtigung führen (z. B. Malware, Ransomware, Phishing).
- Verdacht auf Manipulation oder unautorisierte Veränderung von Unternehmensdaten.

18 Austritt eines Mitarbeitenden

Beim Ausscheiden aus dem Unternehmen sind alle Unternehmenswerte, einschließlich der bereitgestellten IT-Ausstattung, Zugangsmedien, Unternehmensdaten und vertraulichen Dokumente, vollständig, unbeschädigt und spätestens am letzten Arbeitstag zurückzugeben. Die Rückgabe wird durch die IT-Abteilung dokumentiert. Der ausscheidende Mitarbeitende ist verantwortlich, eigene private Daten vor der Rückgabe vollständig von allen geschäftlichen Geräten und Speichermedien zu entfernen.

19 Änderungsvorbehalt

Das Unternehmen behält sich das Recht vor, diese IT-Sicherheitsrichtlinie jederzeit zu ändern oder zu ergänzen, insbesondere sofern gesetzliche, organisatorische oder technische Anforderungen dies erforderlich machen. Die jeweils aktuelle Version wird den Mitarbeitenden in geeigneter Form (z. B. über das Netzlaufwerk oder per E-Mail) zur Verfügung gestellt und ist für alle verbindlich. Alle Mitarbeitenden sind verpflichtet, sich regelmäßig über den aktuellen Stand der Richtlinie zu informieren und die darin enthaltenen Änderungen unverzüglich umzusetzen.

20 Verstöße gegen die IT-Sicherheitsrichtlinie

Verstöße gegen die im Unternehmen geltenden Vorgaben, einschließlich der IT-Sicherheitsrichtlinie, können arbeitsrechtliche (disziplinarische Maßnahmen wie z. B. Abmahnung oder auch Beendigung des Arbeitsverhältnisses) sowie gegebenenfalls strafrechtliche Konsequenzen nach sich ziehen.