Informationssicherheitsrichtlinie für Mitarbeiter

OA1002-02

Group24 AG (group24)

INHALTSVERZEICHNIS

STAMMDATEN

Referenz-Nummer:	OA1002-02
Dokumententitel:	Informationssicherheitsrichtlinie– Mitarbeiter
Fachlich Verantwortlicher:	Andreas Badry
Zuständiger Bereich:	Informationssicherheit
Geltungsbereich:	group24 AG
Gültig von:	02.11.2022
Gültig bis:	31.12.2024
Verantwortlicher Prüfer:	Christian Hornhues
Wiedervorlage Datum:	01.10.2024
Dokumentenkategorie	Intern

ÄNDERUNGSVERZEICHNIS

Version	Datum	Autor	Inhalte der Änderung
0.1	22.06.2022	Sandra Kiemes (extern)	Initiale Erstellungen
0.2	08.09.2022	Andreas Badry	Anpassung auf die group24
0.3	09.09.2022	Andreas Badry	Anpassung auf die group24
0.4	20.10.2022	Andreas Badry	Anpassung auf die group24
0.9	28.10.2022	Andreas Badry	Anpassung 2.3 Umgang mit privaten Daten

REVIEWNACHWEIS UND FREIGABE

Version	Datum	Teilnehmer	Inhalte des Reviews
V1.0	31.10.2022	Christian Hornhues	Prüfung Ersterstellung und Freigabe
V1.1	15.11.2023	Christian Hornhues	Review 2023

1 EINLEITUNG

1.1 Ziel und Zweck

Ziel und Zweck dieses Dokumentes ist es, allen (internen und externen) Mitarbeiter/innen der group24 eine Organisationsanweisung zur Benutzung der DV-/IT-Systemen in die Hand zu geben, damit sie sich bei der Benutzung von DV-/IT-Systemen, insbesondere des Internets, verantwortungsbewusst im Sinne des Unternehmens verhalten können. Angesichts des Risikopotentials sind die folgenden Weisungen für alle Mitarbeiter/innen verbindlich und strikt zu befolgen.

1.2 Hintergrund der Sicherheitsmaßnahmen

Die Unternehmens-IT besonders die Cloud-Services sind eine rasant wachsende und verändernde Umgebung mit allen Vor- und Nachteilen eines offenen weltweiten Netzes. Nützliche wie auch unwichtige Informationen, auch krimineller Natur, sind verfügbar. Die erste Priorität der unternehmensweiten Sicherheit bezogen auf IT-Services ist, Mitarbeitern/innen eine Nutzungsmöglichkeit zu bieten bei gleichzeitiger Sicherstellung des Schutzes der Unternehmens-IT und Informationen sowie der Berücksichtigung von Kundenvorgaben und -Interessen.

1.3 Gefahrenpotential

Es ist wichtig, sich der Tatsache bewusst zu sein, dass

- die IT auch von Personen benutzt wird, die nicht immer das Wohl des Unternehmens im Auge haben;
- alle ausgetauschten Informationen von einer Vielzahl unbekannter Personen (Kriminelle, Spione, Saboteure, Geheimdienste etc.) gelesen und missbraucht werden können;
- Computer-Viren, Computer-Würmer, Trojanische Pferde oder sonstige Schädlinge unkontrolliert verbreitet und große materielle und immaterielle Schäden verursachen können.

1.4 Sicherheitsmaßnahmen des Unternehmens

Ein Schutz vor den möglichen Gefahrenpotentialen in unserem Unternehmen kann nur dann gewährleistet werden, wenn alle betroffenen Mitarbeiterinnen und Mitarbeiter des Unternehmens mit Zugang zu den IT-Services diese Arbeitsanweisung beachten und danach handeln.

1.5 Persönlicher und räumlicher Geltungsbereich

Diese Arbeitsanweisung gilt für alle Mitarbeiterinnen und Mitarbeiter des Unternehmens. Dazu gehören alle beschäftigten Personen (interne und externe), Auszubildende und Aushilfen, mit denen das Unternehmen Verträge zur Leistungserbringung vereinbart hat. Neue Versionen ersetzen die alten Versionen dieses Dokuments vollständig, sofern dies nicht anders ausgewiesen ist.

1.6 Aushändigung

Diese Arbeitsanweisung und Nutzungsvereinbarung wird an alle Mitarbeiter in zweifacher Ausfertigung ausgehändigt, unabhängig davon, ob sie zurzeit bereits eine Zugangsberechtigung zu DV-/IT-Systemen besitzen.

2 UMGANG MIT DATEN UND DATENKLASSIFIKATION

2.1 Allgemeines

Alle Daten der group24 müssen entsprechend dem potenziellen Risiko, das die Daten für die group24, für Kunden und Kundinnen der group24 und alle anderen betroffenen Parteien, wie z.B. Mitarbeitende oder Dienstleister, bei missbräuchlicher Nutzung darstellen, in Datenklassen eingeteilt werden.

Die Daten werden klassifiziert, um sie mit angemessenen Richtlinien und Prozessen zu schützen.

Jede/r Mitarbeitende ist für die Klassifikation und den Schutz ihrer/seiner Daten verantwortlich.

Die Daten werden jeweils einer der drei folgenden Datenklassen zugeteilt:

Öffentlich

Öffentliche Daten sind Daten, aus denen kein Risiko für die group24, deren Kunden, Kundinnen oder andere betroffene Parteien erwachsen kann.
Beispiele: Daten, die von der group24 für die Öffentlichkeit erzeugt oder von externen Stellen veröffentlicht wurden, wie z.B. Pressemeldungen oder der Internetauftritt.

Intern

Interne Daten sind Daten, aus denen nur ein geringes Risiko für die Group24, deren Kunden, Kundinnen oder andere betroffene Parteien erwachsen kann.

Dies ist die Standardklasse für alle Daten der group24, wenn diese nicht offensichtlich öffentlich sind.

Interne Daten können der ganzen group24 zugänglich gemacht werden und können, falls erforderlich, und mit angemessenen Vorsichtsmaßnahmen auch Geschäftspartnern zur Verfügung gestellt werden.

Beispiele für interne Daten sind Richtlinien, Prozesse, etc.

Vertraulich

Vertrauliche Daten sind Daten, aus denen ein mittleres bis hohes Risiko für die group24, deren Kunden, Kundinnen oder andere betroffene Parteien erwachsen kann.

Vertrauliche Daten sind Daten mit Schutzbedarf, die nach dem Need-to-Know-Prinzip zu behandeln sind.

Beispiele sind unveröffentlichte Umsatzzahlen, Kundenverträge, Mitarbeiterdaten, etc.

Das Teilen sensibler bzw. als vertraulich klassifizierter Unternehmensdaten erfolgt ausschließlich durch autorisierte Personen.

Explizite und implizite Kennzeichnung

- Explizite Kennzeichnung

Explizite Kennzeichnungen müssen im Dokument oder in der Datei gut sichtbar und verständlich sein. Die Klassifizierung muss ohne großen Aufwand abgerufen werden können.

- Implizite Kennzeichnung

Daten werden implizit gekennzeichnet, indem ihre Klassifikationen in einer begleitenden Information (Schreiben, Mail, mündlich) jeder Person zur Verfügung gestellt werden, die mit diesen klassifizierten Informationen oder Materialien umgehen muss, ohne dass eine explizite Kennzeichnung erfolgt.

Die implizite Kennzeichnung ist nicht auf einzelne Materialien oder Informationen begrenzt, sondern kann ganze Gruppen an Informationen, Informations- oder Materialarten umfassen.

2.2 Umgang mit Unternehmensdaten

Unternehmensdaten sind ausschließlich in der entsprechenden Ordnerstruktur in Teams, SharePoint Online, Dynamics bzw. auf dem persönlichen Laufwerk in OneDrive zu speichern.

Es muss sichergestellt werden, dass die zu berechtigende Person nur auf die für sie bestimmten Daten zugreifen kann.

2.3 Umgang mit privaten Daten auf group24 Geräten

Private Daten auf group24 Geräten dürfen nur auf der internen Festplatte des Rechners in einer separat und als privat gekennzeichneter Struktur abgelegt werden. Die privaten Daten müssen unter C:\Users*jeweiliger Mitarbeitername*\Documents\PRIVAT abgespeichert werden. Der Ordner ist vom Mitarbeiter zu erstellen. Bei Mobiltelefonen oder Tablets ist dies analog anzuwenden und sicherzustellen, dass die privaten Daten keinen Einzug in die Dateiservices halten.

2.4 Drucken

Dokumente dürfen beim Druck nicht unbeaufsichtigt bleiben oder danach im Drucker liegen gelassen werden. Beim Ausdruck von Dokumenten ist auf die Klassifizierung der Daten zu achten (bspw. Verwendung von Wasserzeichen / Hinweis auf Vertraulichkeit der Daten).

3 IDENTITÄTS- UND BERECHTIGUNGSMANAGEMENT

Für den Zugriff auf Daten und IT-Anwendungen und Zutritt zu Räumen benötigen Mitarbeitende in Abhängigkeit von ihrem jeweiligen Aufgabengebiet Berechtigungen.

3.1 Beantragung und Genehmigung

Beim Beantragen und Genehmigen von Berechtigungen gilt:

Es sind die Prinzipien der minimalen Rechtevergabe – Need-to-know und Least-Privilege – zu beachten, d.h. die Berechtigungen sind auf den für die Aufgabenerfüllung erforderlichen Umfang zu beschränken.

Rechtliche Anforderungen und vertragliche Verpflichtungen zum Zugriffsschutz auf Daten und Services sind zu berücksichtigen.

Für einen reinen Löschantrag, also einen Berechtigungsantrag, der den Berechtigungsumfang ausschließlich reduziert, ist eine Genehmigung von einer der folgenden Stellen ausreichend:

- die Person, deren Berechtigungen gelöscht werden sollen, bzw. für technische oder nicht personalisierte Benutzerkonten die Person, die für das Benutzerkonto verantwortlich ist
- die (ggfs. vorherige) Führungskraft
- die Informationssicherheit

Für die Einrichtung, Änderung, Deaktivierung oder Löschung von Berechtigungen sind die pro System definierten Genehmigungsprozesse einzuhalten.

3.2 Austritt und interner Wechsel

Bei Austritt oder internem Wechsel ist die Führungskraft dafür verantwortlich, dass der Personalprozess initiiert wird. Bei internem Wechsel ist für die Löschung der bestehenden Berechtigungen die abgebende Führungskraft und für die Beantragung die abgebende Führungskraft verantwortlich. Dazu gehören auch Berechtigungen auf Verzeichnissen und IT-Anwendungen.

3.3 Rezertifizierung von Berechtigungen

Zugangs- und Zugriffsberechtigungen sind regelmäßig zu überprüfen (zu rezertifizieren).

Die Informationssicherheitsbeauftragten stoßen alle Rezertifizierungen an.

Berechtigungen werden jährlich rezertifiziert.

Für die Rezertifizierung der Berechtigungen ist die Führungskraft des berechtigten Mitarbeitenden verantwortlich (für technische oder nicht personalisierte Benutzerkonten ist dies die Führungskraft der Person, die für das Benutzerkonto verantwortlich ist).

3.4 Nutzung von Berechtigungen

Unabhängig von der Art der Berechtigungsvergabe (automatisch, durch Antrag, durch Delegation) darf eine zugewiesene Berechtigung nur unter Berücksichtigung der internen Regelungen des Unternehmens sowie der gesetzlichen Anforderungen genutzt werden. Insbesondere erfolgt durch die Erteilung einer Berechtigung keine automatische Erweiterung von Kompetenzen und Zeichnungsberechtigungen.

3.5 Passwörter und Token

Passwörter und Token sind sicher zu verwahren (bei Passwörtern z.B. keine Klartext-Eingabe von Passwörtern, keine Zuschauer bei der Passworteingabe) und dürfen nicht weitergegeben werden.

- Bei Anzeichen einer möglichen Kompromittierung eines Passworts ist dieses unverzüglich zu ändern und der internen IT und dem Informationssicherheitsbeauftragten sind zu informieren.
- Passwörter dürfen nicht notiert oder gespeichert werden (z. B. auf Papier, in einer Datei oder auf einem Mobilgerät), außer in geneeigneten Aufbewahrungsmethoden, wie z. B. dem Passwortverwaltungssystem LastPass.

4 MELDUNG VON INFORMATIONSSICHERHEITSVORFÄLLEN

4.1 Informationssicherheitsvorfall

Ein Informationssicherheitsvorfall ist die Bedrohung oder der Verlust von schützenswerten Informationen – entweder indem die Informationen uns nicht mehr zur Verfügung stehen (Verlust der Verfügbarkeit), indem Informationen verfälscht werden (Verlust der Integrität) oder Personengruppen bekannt werden, die diese eigentlich nicht kennen dürften (Verlust der Vertraulichkeit). Sollte der Verdacht bestehen, dass der Schutz oder die Sicherheit von Daten in irgendeiner Weise gefährdet sein könnten, hat sich der Mitarbeiter unverzüglich an den Datenschutzbeauftragten, Informationssicherheitsbeauftragen und seinen Vorgesetzten zu wenden.

Beispiele:

- Cyber-Angriffe (zum Beispiel Phishing-E-Mails oder E-Mails mit Anhängen oder Links, die evtl. Schadsoftware enthalten)
- Diebstahl, Untreue, Unterschlagung (dolose Handlung)
- Datenverlust, deren Wiederbeschaffung oder erneute Produktion Kosten oberhalb der Bagatellgrenze erzeugt
- Datenschutzvorfälle

Wenn eine Schwachstelle in einem System entdeckt wurde und ein Schaden oberhalb der Bagatellgrenze entsteht bzw. zu erwarten ist.

Vorfälle müssen die Bagatellgrenze von 10.000,- Euro Schaden übersteigen, um als Informationssicherheitsvorfall weiterbearbeitet zu werden.

Informationssicherheitsvorfälle müssen umgehend gemeldet werden:

- an die Informationssicherheitsbeauftragten
- Es muss ein Ticket / Incident erstellt werden (Weclapp Ticket)

Die Informationssicherheitsbeauftragten melden Informationssicherheitsvorfälle mit Personalbezug der Bereichsleitung Personal.

4.2 Virenbefall

Folgende Anzeichen können auf einen Virenbefall hindeuten:

- Häufige Programmabstürze
- Programmdateien vergrößern sich
- Unerklärliches Systemverhalten (hohe Last, Verringerung des Speicherplatzes,…)
- Unerklärliche und/oder spontane Systemmeldungen

- Nutzung unbekannter Dienste
- Veränderte Dateiinhalte

Bei einem solchen Verdacht wenden Sie sich umgehend an den User Help Desk und folgen Sie den Anweisungen des Service Desk.

Das betroffene System darf bis zur Klärung des Sachverhaltes nicht weiter verwendet werden.

Zuwiderhandlungen („Ich will aber sehen, was passiert“) können neben arbeitsrechtlichen auch strafrechtliche Konsequenzen und Schadensersatzforderungen nach sich ziehen.

5 NUTZUNGSREGELN

5.1 Allgemeines

5.1.1 Mobiles Arbeiten

Das Arbeiten auf group24 und Kunden-Systemen ist, nur mit einem corporate device erlaubt.

Es ist darauf zu achten, dass die von ihm gewählte Arbeitsstätte für die Erbringung der ihm zugewiesenen Arbeitsaufgabe geeignet ist. Es ist darauf zu achten, dass das eigene Heimnetzwerk nicht als öffentlich gekennzeichnet ist und vor Manipulation geschützt wird.

Beim Arbeiten an öffentlichen Orten, ist darauf zu achten, dass keine Gefahr besteht, das Daten durch dritte eingesehen oder gehört werden können.

Für die Nutzung, den Schutz und die Pflege von Hard- und Software beim mobilen Arbeiten gelten die Vorgaben aus Kapitel 3.

Für die Nutzung von IT-Systemen der group24 und Kundensystemen gelten die Vorgaben aus den Kapiteln 5.3.

Für den Umgang mit Daten gelten die Vorgaben aus dem gesamten Kapitel 2.

5.1.2 Privatnutzung

Die private Nutzung der Systeme der group24 ist – mit Ausnahme von (Mobil-) Telefonen (zum Telefonieren) und Webmailern – grundsätzlich untersagt. Dies gilt insbesondere für die Bearbeitung und Ablage privater Dokumente auf den Systemen der group24. Auch das personalisierte Onedrive dient ausschließlich zur Ablage dienstlicher Daten.

Die Speicherung von privaten Informationen (Kontakte, Termine oder sonstige) in Outlook ist – sofern dies die Arbeitsweise des Nutzers unterstützt – zulässig. Die Speicherung wird dann als dienstlich veranlasst angesehen und die Daten werden entsprechend behandelt.

Alle auf den Systemen der group24 abgelegten Daten werden als dienstlich veranlasst angesehen und unterliegen daher keinem besonderen Persönlichkeitsschutz. Insbesondere besteht auch kein Anspruch auf Aushändigung solcher.

5.2 Umgang mit Hardware und Software

5.2.1 Verantwortlichkeit für IT-Geräte

Jedes IT-Gerät (z.B. Notebook, Tablet, Desktop-Rechner, Smartphone) ist einem Benutzer bzw. einer Benutzergruppe zugeordnet. Besitzer des IT-Geräts ist derjenige, dem das IT-Gerät zur

Nutzung ausgehändigt wurde. Der Besitzer trägt die Verantwortung für die Beachtung der Vorschriften und Arbeitsanweisungen des jeweiligen IT-Geräts

Die zur Verfügung gestellten IT-Geräte sind pfleglich zu behandeln und nach Beendigung des Arbeitsverhältnisses an den Vorgesetzten oder die interne IT der group24 zu übergeben.

group24 behält sich vor, jederzeit Ad hoc Überprüfungen von IT-Geräten durchzuführen.

Jedes IT-Gerät darf nur die vom Unternehmen oder vom Bereichsleiter/Vorgesetzten zugelassene bzw. genehmigte Hardware beinhalten. Dem Mitarbeiter ist es gestattet für ihre beruflichen Tätigkeiten notwendige Software nach zu installieren oder runterzuladen.

Dabei trägt er die Verantwortung dafür, dass die Software weder Rechte Dritter verletzt noch eine Gefährdung für die Netzsicherheit der group24 darstellt. Die group24 behält sich das Recht vor im Einzelfall Software zu verbieten und die Löschung zu veranlassen. Die group24 behält sich ferner vor, Anwendungen und Funktionen über Richtlinien automatisiert zu aktivieren bzw. zu deaktivieren. Es ist zu beachten die Software aktuell gehalten wird.

5.2.2 Nutzung privater Mobiltelefone/Tablets

Das Anmelden an den Unternehmensaccount mit dem privaten Mobiltelefon in Microsoft 365 ist für den beruflichen Austausch gestattet. Das Verwenden des privaten Mobiltelefons zur Multi-Faktor Authentifizierung ist ebenfalls gestattet.

Die Verwendung des group24-WLANS ist nur mit group24 eigenen Geräten gestattet.

Damit sind private Geräte nur im Gast WLAN gestattet.

5.2.3 Nutzung unternehmenseigener Telefonie

Sowohl Festnetz (Teamscall) als auch Mobiltelefone der group24 werden den Mitarbeitern zur betrieblichen Nutzung überlassen und dienen lediglich dem Unternehmenszweck.

Dual-Sim Geräte können gleichsam für den privaten und geschäftlichen Gebrauch genutzt werden, eine Trennung der Daten eingerichtet wird.

Die Nutzung von Social Media Plattformen wie z.B. Whatsapp, Facebook etc. ist auf Firmentelefonen im Firmenprofil gestattet. Die Nutzung dieser Apps kann von Seiten der group24 durch technische Verfahren verhindert werden.

5.2.4 Nutzung unternehmenseigener SIM-Karten

SIM-Karten werden den Mitarbeitern/innen zur Nutzung im Rahmen der beruflichen Tätigkeit überlassen.

Da das Überschreiten des vereinbarten monatlichen Datenvolumens zu Mehrkosten führt, sind alternative Kommunikationswege, soweit möglich und sinnvoll, zu nutzen.

Alle Tarife der group24 beinhalten eine Flatrate innerhalb von Deutschland und Europa zu deutschen Mobil- bzw. Festnetz-Anschlüssen. Davon ausgenommen sind Anrufe zu Sonderrufnummer und Auslandsgesprächen.

5.2.5 Schutz vor unbefugter Nutzung

Jede/r Mitarbeiterin/Mitarbeiter hat ihr/sein IT-Gerät vor unbefugter Nutzung zu schützen. Hierzu gehört insbesondere die Auswahl eines sicheren Benutzerpasswortes oder bei mobilen Geräten eine sichere Sperrfunktion. Als sichere Sperrfunktionen gelten u.a. auch Windows Hello oder Fingerabdrücke. Der Rechner ist bei jedem Verlassen des Arbeitsplatzes zu sperren (Windowstaste+L) und die automatische Sperrfunktion ist bei mobilen Geräten auf eine Sperre nach spätestens nach 10 Minuten zu setzen.

Notebooks sind beim Verlassen des Arbeitsplatzes nach Beendigung des Arbeitstages sicher zu verschließen.

5.2.6 Schutz vor unbefugtem Zugriff

Aufgrund der sich schnell verändernden Technologien muss jeder neue Dienst durch die group24 auf Sicherheitsrelevanz überprüft werden, bevor er zum Einsatz kommt.

Für die Zulassung gibt der Benutzer darüber hinaus folgende Verpflichtungserklärungen ab:

- der Benutzer handelt im Sinne und im Interesse des Unternehmens,
- der Benutzer ist sich über die Gefahren und Risiken bewusst.

5.2.7 Technische Überprüfung

Die group24 IT wird vor dem Erreichen dieser Frist den Mitarbeiter über die anstehende Prüfung informieren. Zum Prüftermin sind die elektrischen Geräte vollständig inkl. Zubehör (u.a. Netzteil, Netzkabel) mitzubringen.

5.2.8 Rückgabe von IT-Ausstattung

Die von der group24 zur Verfügung gestellte IT-Ausstattung ist bei Beendigung des Arbeits- oder Vertragsverhältnisses spätestens am letzten Arbeitstag in gepflegtem Zustand und vollständig zurückzugeben. Dies beinhaltet neben dem Gerät auch alle zur Verfügung gestelltes Zubehör, wie Ladekabel, Adapterkabel, Headset, Webcam, Dockingstations, Monitor usw.

Zusätzlich zur IT-Ausstattung sind ebenfalls die zur Verfügung gestellten Schlüssel und Zugangsmedien zu Räumlichkeiten der group24 bzw. Kunden zurückzugeben.

Die Rückgabe der IT-Ausstattung erfolgt persönlich und entlastend ausschließlich an die group24 zu den Service-Zeiten von 8-17 Uhr am Geschäftsstandort der group24.

5.2.9 Störungen/Defekte/Verluste

Störungen, Defekte bzw. Verluste an/von der group24 zur Verfügung gestellten IT Geräten oder IT-Services sind unverzüglich nach dem Bekanntwerden an die group24 IT per email technik@group24.de oder Tel. +49 25422008060 Group24 (Mo-Fr 8-17 Uhr, außer an Feiertagen in NRW) zu melden.

Bei Beschädigungen an stromführenden Geräteteilen oder bei sonstigen Beschädigungen, die einen sicheren Betrieb nicht mehr gewährleisten, ist das Gerät sofort außer Betrieb zu nehmen.

Reparaturaufträge oder Ersatzbeschaffungen dürfen erst nach Freigabe durch die group24 erfolgen.

5.2.10 Nutzung von Datenträgern

Die Speicherung von Unternehmensdaten auf lokalen oder externen Datenträgern ist ohne ausdrückliche Genehmigung nicht gestattet.

Sollte es nötig sein, dass Unternehmensdaten oder insbesondere Kundendaten auf dem Notebook oder einen USB-Stick gespeichert werden, sind diese durch geeignete Maßnahmen (z.B. Bitlocker) zu verschlüsseln. Ausgenommen davon sind öffentliche Daten, wie z.B. Unternehmenspräsentationen.

5.3 Umgang mit IT-Services

Zu den IT-Services im Sinne dieser Vereinbarung gehören verschiedene von der group24 zur Verfügung gestellte IT-Services, dazu zählen unter anderem Microsoft 365 (Office, Mail, Teams, SharePoint usw.), DATEV, Kenjo, Internetzugang, Weclapp, usw.

Der Benutzer ist nach dem Vorgabe des Berechtigungskonzepts in der Lage, die zugelassenen Dienste während der Arbeitszeit entsprechend seiner beruflichen Tätigkeit in Anspruch zu nehmen.

5.3.1 Allgemeines

Folgende allgemeine Regelungen sind zum Umgang mit dem IT-Services bzw. IT-Systeme definiert.

- Nach Beendigung der Arbeit mit dem System ist dieses ordnungsgemäß abzumelden oder herunterzufahren.
- Notebooks sind zusätzlich vor Diebstahl gesichert zu verwahren
- Geschäftsrelevante Daten sind in den zentralen Verzeichnissen abzulegen. Auf Notebooks dürfen die Daten nur kurzfristig gespeichert werden, da sie dort nicht gesichert und im Vertretungsfall für die Kollegen nicht einsehbar sind.

- Alle Versuche, unberechtigt auf geschützte Informationen zuzugreifen oder diese zu löschen oder zu verändern sind untersagt
- Die Systeme der group24 dürfen keinesfalls zur Belästigung anderer oder gar zur Durchführung illegaler Aktivitäten verwendet werden
- Die Nutzung fremder Geräte im Netzwerk der group24 ist nicht gestattet.
- Zum Schutz der group24 vor schädlichen Einflüssen gelten folgende Bestimmungen:
    - Veränderungen an Systemen erfolgen ausschließlich durch die für den IT-Betrieb verantwortlichen Einheiten. Insbesondere ist es verboten eigene Software zu verändern, sowie Geräte oder Bauteile ein- oder auszubauen oder zu verändern.
    - Das Ausführen von fremden, nicht autorisierten Programmen ist untersagt. Dazu gehören insbesondere Spielprogramme.

5.3.2 Nutzung des E-Mail Accounts

Der von der group24 zur Verfügung gestellte E-Mail Account ((Erster Buchstabe des Vornamen).Nachnamw@group24.de) ist lediglich für berufliche Zwecke zu nutzen. Eine private Nutzung dieses E-Mail Accounts ist aus datenschutzrechtlichen Gründen untersagt. Die group24 behält sich vor, bei evtl. längerer Abwesenheit (z.B. Krankheit) oder Ausscheiden des Mitarbeiters, die E-Mails weiterzuleiten oder Einsicht in das Postfach zu nehmen.

Es gelten folgende Grundsätze:

- Die Übertragung vertraulicher Informationen zur weiteren Bearbeitung durch Mitarbeiter außerhalb der group24 (beispielsweise am privaten Rechner) ist nicht erlaubt.
- Die Übertragung vertraulicher Informationen an Geschäftspartner darf ausschließlich im Rahmen der vertraglich vereinbarten Geschäftsbeziehung erfolgen.
- Das Erzeugen oder Weiterleiten von Kettenbriefen ist weder intern noch extern erlaubt. Warnmeldungen werden in der group24 von der internen IT weitergeben.
- E-Mails, die Sie unaufgefordert erhalten und deren Inhalt verdächtig ist (indem Sie beispielsweise aufgefordert werden, unbedingt den Anhang zu öffnen oder eine Webseite zu besuchen), sollten Sie löschen oder im Zweifelsfall vom Informationsicherheitsbeauftragten zu analysieren.

Des Weiteren findet eine automatisierte E-Mail Spamfilterung statt, aus der Absender, Empfänger, Betreff und Uhrzeit der E-Mail hervorgehen.

Eine dauerhafte Sensibilität gegenüber möglicher Phishing Angriffe ist durch konsequente Prüfung der Mails zu gewährleisten.

5.3.3 Nutzung des Internets

Eine private Nutzung des Internets ist in Pausenzeiten außerhalb der Arbeitszeit gestattet.

Der Zugriff auf jugendgefährdende, extremistische, pornografische, rassistische Inhalte oder Inhalte die gegen geltendes Recht der BRD verstoßen, ist untersagt. In den Geschäftsräumen wird der Zugriff auf bestimmte Bereiche des Internets durch Firewall-Regeln automatisiert gesperrt. Der Zugang zu gesperrten Bereichen kann bei berechtigtem dienstlichen Interesse über den Vorgesetzten beantragt werden.

Der Mitarbeiter hat dafür Sorge zu tragen, dass durch die Nutzung der Dienste keine Gefährdung für die group24 (z.B. durch Schadsoftware oder Freigabe von Daten) entsteht.

5.3.4 Nutzung von Teams

5.3.4.1 Ziel- und Zweckbestimmung

Teams soll dazu dienen die Kommunikation und den Informationsaustausch zwischen den Mitarbeitern der group24 zu fördern und zu vereinfachen.

Durch Teams soll der Zugriff auf Vorlagen, Anträge etc. für Mitarbeiter erleichtert und eine zentrale Informationsplattform geschaffen werden.

Die Inhalte von Teams sollten weitestgehend von den Mitarbeitern, den Bereichen selbst gestaltet werden.

5.3.4.2 Zugriff auf Teams

Auf Teams kann sowohl über die Webadresse https://teams.microsoft.com/, als auch über die dazugehörigen Apps zugegriffen werden. Die Zugangsdaten sind vertraulich zu behandeln und dürfen nicht an Dritte weitergegeben werden.

5.3.4.3 Kollaboration in Teams

Für den Umgang mit Daten in Teams gelten die Vorgaben aus dem Kapitel 2.

Die Erstellung neuer Teams kann beim IT-Support der group24 beauftragt werden.

Die Zusammenarbeit mit Externen oder eine Zusammenarbeit zwischen Fachbereichen in Teams ist nur über explizit dafür erstellte Teams zulässig.

5.3.4.4 Video- und Telefonkonferenzen

Videokonferenzen sind ausschließlich über Teams abzuhalten. Ausnahmen sind ausschließlich dann einzuräumen wen es die Situation eines Kunden nicht zulässt.

Bei Videokonferenz mit Externen ist immer ein group24 Hintergrund zu verwenden.

Beim Hinzuziehen anderer Personen ist sicherstellen, dass im Chat keine Inhalte lesbar sind oder besprochen werden, auf die hinzugefügte Personen keinen Zugriff haben dürfen. Bei aufeinanderfolgenden Konferenzen mit verändertem Teilnehmerkreis muss die alte Konferenz verlassen und das Gespräch in der neuen fortgeführt werden. Es ist sicherzustellen, dass der Konferenzraum nicht durch Teilnehmer für andere belange genutzt wird und keine Inhalte in die Historie geraten die mit den besprochenen geschäftlichen Inhalten nicht in Zusammenhang stehen.

Screensharing ist umsichtig zu nutzen, es dürfen keine nicht für den Teilnehmerkreis bestimmten Daten offenbart werden. Falls möglich soll nur das aktuell besprochene Dokument oder genutzte Programm und nicht der ganze Screen freigegeben werden.

Die Übergabe der Steuerung bei Screensharing darf nicht bei Freigabe des gesamten Desktops erfolgen.

5.3.5 Nutzung von Kundensystemen

Die Nutzung des Internets und Anwendungen beim Kunden hat sich grundsätzlich auf die beim Kunden vorgefundenen und von diesem ausdrücklich zur Verfügung gestellten Zugriffsmöglichkeiten zu beschränken, um auf diesem Wege eine durch Mitarbeiter von group24 verursachte Erhöhung des Risikopotentials auszuschließen.

Während der Arbeitszeit gilt die Beschränkung der Nutzung auf die beruflichen Tätigkeiten des Mitarbeiters. Sollte festgestellt werden, dass die beim Kunden verwendeten Sicherheitsvorkehrungen unzureichend sind, ist die Nutzung umgehend einzustellen. Der Kunde, der Vorgesetzte/Bereichsleiter und/oder der Vorstand von group24 sind auf geeignetem Wege umgehend zu informieren, damit die erkannten Sicherheitslücken vom Kunden, group24 oder Dritten beseitigt werden können.

Eine Nutzung der IT Services ist nur nach Zustimmung des Kunden erlaubt. Gleichermaßen bedarf die Nutzung des Internets zu privaten Zwecken und mit technischen Einrichtungen des Kunden dessen vorherige Zustimmung. Im Rahmen der Nutzung des Internets zu privaten Zwecken vor Ort beim Kunden ist jeder Mitarbeiter aufgefordert, ein Höchstmaß an Fingerspitzengefühl zu zeigen. Sollte es nicht möglich sein, für Außenstehende eindeutig ersichtlich zu machen, dass eine Nutzung zu privatem Zweck außerhalb der Arbeitszeit erfolgt, ist auf die Nutzung zu verzichten.

6 SENSIBILISIERUNG UND SCHULUNG

Alle Mitarbeitenden der group24 nehmen an einem intern Schulungsprogramm teil und lesen Aktualisierungen der Richtlinien und Verfahren, die für ihr berufliches Arbeitsgebiet relevant sind, um ein angemessenes Bewusstsein für Informationssicherheit zu bekommen.

Alle Mitarbeitenden werden zweimal Jährlich in einer -Schulung im Bereich Informationssicherheit und Datenschutz geschult. Alle Mitarbeitenden sind verpflichtet, die Schulung im vorgegebenen Zeitfenster (Schulungszyklus) durchzuführen.

7 VERBINDLICHKEIT DER REGELUNGEN

7.1 Verbindlichkeit der Regelungen

Die im Anhang aufgeführten, veröffentlichten und in Kraft gesetzten Dokumente gelten als Anlage zu dieser OA und sind für alle Mitarbeiter verbindlich.

Sie sind insoweit Bestandteil dieser Organisationsanweisung.

7.2 Ausnahmeregelung

Sollte eine gültige Regelung für einzelne Systeme oder Prozesse, aus welchen Gründen auch immer, nicht umsetzbar sein, so kann der Informationssicherheitsbeauftragte für dieses System bzw. diesen Prozess eine Ausnahme von den Regeln genehmigen. Die Entscheidung des Informationssicherheitsbeauftragten erfolgt risikobasiert.

Diese Ausnahmen sind zentral vom Informationssicherheitsbeauftragten zu dokumentieren.

8 VERSTÖßE UND SANKTIONEN

Verstöße gegen diese Sicherheitslinie und die darunter liegenden Sicherheitsgrundsätze sind nicht tolerierbar. Sie können daher zu Disziplinarmaßnahmen, arbeitsrechtlichen Maßnahmen oder gar zu Straf- und/oder zivilrechtlichen Verfahren führen.

Die Zugangsberechtigung zu den IT Services wird widerrufen, wenn die IT Services mindestens fahrlässig und unzulässig für solche Zwecke eingesetzt wird, die das Unternehmen materiell bzw. immateriell schädigen oder schädigen können.

Bei schweren Verstößen oder Missbrauchsfällen bei der Nutzung der IT-Services und bereitgestellter Hardware können neben der Sperre des Zugangs weitere disziplinäre und arbeitsrechtliche Maßnahmen eingeleitet werden.

Zum schweren Verstoß gehört die grobe Fahrlässigkeit bzw. der Missbrauch bezogen auf die Nutzung, die Speicherung und die Weitergabe der folgenden Inhalte:

- pornographisches Material sowie sittenwidrige, obszöne und respektlose Angebote,
- menschenverachtende und rassistische Propagandadaten,
- Sekten-Propaganda bzw. -Mitgliederwerbung jeder Art,
    - Der Zugang zum Dark-Net sowie zum Deep Web
- Das Erwerben von Inhalten oder Gütern, die gegen geltendes Recht, insbesondere der BRD verstoßen.

Zu den schweren Verstößen zählen ferner die Verwendung, Nutzung und Speicherung (und sei es auch lediglich zur Weitergabe an Dritte) von urheberechtlich geschützten Daten wie beispielsweise Computerprogrammen, E-Books, Musik und Filmen, sowie die fahrlässige oder mutwillige Beschädigung von Hardware und DV-/IT-Systemen.

Bei schweren Verstößen oder Missbrauchsfällen bei der Nutzung von DV-/IT-Systemen kann ein Entzug der Nutzung von DV-/IT-Systemen erfolgen. Daraus eventuell resultierende notwendige Maßnahmen, wie z. B. Versetzungen, sind im Einzelfall möglich. Ferner muss bei Verstößen gegen diese Arbeitsanweisung mit arbeitsrechtlichen Konsequenzen bis hin zur fristlosen Kündigung gerechnet werden, die bei schweren Verstößen auch ohne vorherige Abmahnung ausgesprochen werden kann.