Informationssicherheitsrichtlinie für Gebäude und Betriebsmittel

OA1002-04

Group24 AG (group24)

INHALTSVERZEICHNIS

STAMMDATEN

Referenz-Nummer:	OA1002-02
Dokumententitel:	Informationssicherheitsrichtlinie für Gebäude und Betriebsmittel
Fachlich Verantwortlicher:	Max Oing
Zuständiger Bereich:	
Geltungsbereich:	group 24
Gültig von:	01.11.2022
Gültig bis:	31.12.2024
Verantwortlicher Prüfer:	Christian Hornhues / Marc Eismann
Wiedervorlage Datum:	01.10.2024
Dokumentenkategorie	Intern

ÄNDERUNGSVERZEICHNIS

Version	Datum	Autor	Inhalte der Änderung
0.1	15.09.2022	Sandra Kiemes	Erstellung
0.2	20.09.2022	Andreas Heit	Anpassung / Aufbereitung group24
0.3	24.10.2022	Andreas Heit	Review mit Fachabteilung
1.0	30.11.2022	Sandra Kiemes	Finalisierung

REVIEWNACHWEIS UND FREIGABE

Version	Datum	Teilnehmer	Inhalte des Reviews
1.0	30.11.2022	Christian Hornhues / Marc Eismann	Prüfung Ersterstellung und Freigabe
1.1	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 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.

2 GEFÄHRDUNGSANALYSE FÜR GEBÄUDE

Für die Gebäude und Liegenschaften der group24 müssen Gefährdungsanalysen erstellt werden, aus denen angemessene Maßnahmen zur Sicherheit der Gebäude abgeleitet werden.

Für jedes Gebäude müssen Sicherheitsbereiche und für die Sicherheitsbereiche angemessene Informationssicherheitsmaßnahmen definiert werden.

Für Liegenschaften der group24 ist das Office Management verantwortlich.

Für Rechenzentren liegt die Verantwortung bei der für den jeweiligen Betreibern/ Cloud Anbieter.

3 PHYSISCHE SICHERHEITSBEREICHE

Die im Rahmen einer Risikoanalyse als kritisch eingestuften datenverarbeitenden Einrichtungen müssen in Sicherheitsbereichen untergebracht sein, die durch angemessene Sicherheitsbarrieren und Zugangskontrollsystemen geschützt sind.

Die group24 definiert vier Sicherheitsbereiche:

- Sicherheitsbereich A (Grün):

  Öffentliche Gebäudeaußenbereiche und Außenanlagen mit öffentlichem Charakter

- Sicherheitsbereich B (Grau):

  Nicht öffentliche Gebäudebereiche mit geringem Schutzbedarf (Basis-Schutzbedarf)

- Sicherheitsbereich C (Gelb):

  Nicht öffentliche Gebäudebereiche mit mittlerem Schutzbedarf (erhöhtem Basis-Schutzbedarf), z.B. für IT- und Technikräume, Lager

- Sicherheitsbereich D (Rot):

  Gebäude mit hohem Schutzbedarf: Rechenzentrum

Lage und Stärke der Sicherheitsgrenzen sind risikoorientiert gemeinsam zwischen der Abteilung Office Management und dem betroffenen Fachbereich festzulegen.

3.1 Informationssicherheitsmaßnahmen

3.1.1 Sicherheitsbereich A

Der öffentliche Bereich ist dauerhaft oder überwiegend für jeden zugänglich, diese Bereiche sind videoüberwacht.

3.1.2 Sicherheitsbereich B

Der Sicherheitsbereich B ist teilweise video- oder anders überwacht. Für Sicherheitsbereiche ab Sicherheitsbereich B gilt:

1. Eingänge sind an das Zutrittskontrollsystem anzuschließen. Der Zutritt darf nur autorisierten Personen ermöglicht werden.
2. Zutrittskontrollsysteme müssen die Identität der Personen und Datum und Uhrzeit des Zutritts von Sicherheitsbereichen erfassen.
3. Besucher und Besucherinnen werden vom Fachbereich im öffentlichen Bereich abgeholt, zum Fachbereich begleitet und wieder zum öffentlichen Bereich zurück gebracht.
4. Alle Mitarbeitenden und Personen, die innerhalb der group24 tätig sind, sind verpflichtet, die Brandschutzordnung zur Kenntnis zu nehmen und sie zu befolgen.

5. Externe Mitarbeitende bekommen nur befristeten Zugang ausschließlich zu den erforderlichen Bereichen.

3.1.3 Sicherheitsbereich C

Für Sicherheitsbereiche ab Stufe „C“ gilt zusätzlich:

Der Zugang zu Sicherheitsbereichen C ist durch eine zusätzliche Zutrittskontrolle zu sichern.

Bei öffentlichen Zugängen, Anlieferungs- und Ladezonen müssen die folgenden Regelungen risikoorientiert berücksichtigt werden:

- Zugang zur Anlieferungs- und Ladezone eines Gebäudes von außerhalb darf nur identifizierten und berechtigten Personen erlaubt sein.
- Die Anlieferungs- und Ladezone muss so gestaltet sein, dass Lieferungen ausgeladen werden können, ohne dass das Lieferpersonal Zutritt zu anderen Bereichen des Gebäudes erhält.
- Die Außentüren einer Anlieferungs- und Ladezone sollen gesichert sein, wenn die Türen zum inneren Bereich geöffnet sind.
- Eingehendes Material sollte auf potenzielle Bedrohungen hin untersucht werden bevor dieses Material aus der Anlieferungs- und Ladezone zu seinem Bestimmungsort gebracht wird.

Alle Mitarbeitenden und Personen, die Zutritt zum Sicherheitsbereich Stufe „C“ – „Lager“ erhalten – müssen eine separate Sicherheitseinweisung erhalten.

3.1.4 Sicherheitsbereich D

Für Sicherheitsbereiche der Stufe „D“ (Rechenzentren) gilt zusätzlich:

1. Nicht besetzte Sicherheitsbereiche der Sicherheitsstufe „D“ müssen verschlossen und regelmäßig kontrolliert werden. Dies kann bspw. durch das Office Management, einen Wachdienst oder durch bewegungsgesteuerte Videokameras erfolgen.
2. Die Rechenzentren der group24 müssen über Einbruchmeldesysteme verfügen, die alle Zugänge (Außentüren und ggf. Fenstern) überwachen. Diese Systeme müssen regelmäßig getestet werden. Räumlichkeiten, die nicht von Mitarbeitern besetzt sind, sollten einer permanenten Überwachung unterliegen, gleiches gilt für Computer- und Kommunikationsräume.
3. Rechenzentren der group24 sind unauffällig zu halten. Abweichend von Standard dürfen innerhalb von Rechenzentren durch Schilder Hinweise auf informationsverarbeitende Einrichtungen gegeben werden.
4. Der Zutritt zu Rechenzentren muss angekündigt werden.
5. Eine Liste autorisierter Personen für den Zutritt zu Rechenzentren ist zu führen und gemeinsam mit dem Rechenzentrumsbetreiber aktuell zu halten. Die Liste ist regelmäßig zu kontrollieren.
6. Zutrittskontrollsysteme müssen die Identität der Personen und Datum und Uhrzeit des Zutritts und des Verlassens von Sicherheitsbereichen erfassen.

7. Nur autorisierte Personen sollten Kenntnis über die Rechenzentren (Need-to-know Prinzip) besitzen. Arbeiten in Rechenzentren sind risikoorientiert zu überwachen. Dies kann bspw. durch einen Mitarbeiter der group24 oder bewegungsgesteuerte Videokameras erfolgen.

4 GERÄTE UND BETRIEBSMITTEL

4.1 Platzierung

Geräte und Betriebsmittel sollen so platziert und geschützt werden, dass das Risiko durch Bedrohungen aus der Umgebung, durch Katastrophen als auch die Gelegenheit für unerlaubten Zugriff reduziert wird.

Dabei müssen die folgenden Regelungen zum Schutz der Betriebsmittel beachtet und risikoorientiert umgesetzt werden:

1. Betriebsmittel müssen so platziert werden, dass unnötiger Zugang zu persönlichen Arbeitsplätzen minimiert wird.

   D.h. Betriebsmittel, zu denen viele Mitarbeitende Zugang benötigen (z.B. Drucker, Kopierer, Büromaterial), dürfen nicht an Arbeitsplätzen aufgestellt werden, bei denen vertrauliche Daten verarbeitet werden.

   Betriebsmittel, zu denen ausschließlich ausgewählte Mitarbeitende Zugang benötigen, sind in nur den ausgewählten Mitarbeitenden zugänglichen Räumen aufzustellen. Beispiele sind Server und Netzwerkkomponenten, die in Technikräumen mit Zutrittssicherung oder in Rechenzentren stehen.

2. Informationsverarbeitende Einrichtungen, die sensitive Daten verarbeiten, (z.B. Server, Netzwerkkomponenten, Speicherkomponenten, PCs, Smartphones, Tablets) müssen so platziert werden, dass das Risiko einer Einsicht durch Unbefugte während der Nutzung minimiert wird.

3. Betriebsmittel der Informationsverarbeitung benötigen einen speziellen Schutz und sind grundsätzlich in Rechenzentren zu betreiben.

   Ausnahmen:

   - Clients und Drucker der Office Infrastruktur (Desktop-PCs, Notebooks) dürfen in Büroräumen oder Druckerräumen betrieben werden.
   - Mobile Geräte (Notebooks, Smartphones, Tablets, Handys) sowie Arbeitsplatzausstattungen von Heimarbeitsplätzen dürfen auch außerhalb der group24 Gebäude betrieben werden.
   - Komponenten der Group24 Gebäude-Netzwerkinfrastruktur sind in Technikräumen mit Zutrittsschutz zu betreiben.
   - Weitere Ausnahmen, z.B. in Ausnahmefällen Test- und Entwicklungs-Server in Technikräumen im group24 Gebäude, sind nur mit Einzel-Zustimmung der Informationssicherheitsbeauftragten zulässig.

4. Potentielle Risiken durch physische Bedrohungen, wie z. B. Diebstahl, Feuer, Explosivstoffe, Rauch, Wasser (oder Versagen der Wasserversorgung), Staub, Vibration, chemische Effekte, Störungen der elektrischen Versorgung, Störungen der Kommunikation, elektromagnetische Abstrahlung und Vandalismus, sind, wenn vorhanden, durch entsprechende Baumaßnahmen zu reduzieren.

5. Umweltbedingungen wie Temperatur und Luftfeuchtigkeit müssen in Rechenzentren und Technikräumen geregelt und überwacht werden.

6. Alle Gebäude sollten mit Blitzableitern versehen sein. Alle Versorgungsleitungen für Strom und Kommunikation sollten mit Überspannungsschutz ausgestattet sein.

7. Betriebsmittel, die sensitive Informationen verarbeiten, sollten gegen Abstrahlung geschützt sein, um den derartigen Abfluss von Informationen zu verhindern. Diese Regelung ist risikoorientiert umzusetzen.

4.2 Versorgungseinrichtungen

Um Betriebsmittel vor Stromausfällen und Ausfällen anderer Versorgungseinrichtungen zu schützen, müssen die folgenden Maßnahmen für Ver- und Entsorgungseinrichtungen in Bürogebäuden risikoorientiert umgesetzt werden.

Für Rechenzentren müssen alle Maßnahmen umgesetzt werden:

1. Alle unterstützenden Ver- und Entsorgungseinrichtungen, z. B. Strom, Wasser, Abwasser, Heizung/Lüftung und Klima, müssen entsprechend den Anforderungen ausgelegt sein. Diese Versorgungseinrichtungen müssen regelmäßig hinsichtlich ihrer Funktionstüchtigkeit geprüft und angemessen getestet werden, um so das Risiko einer Fehlfunktion oder eines Ausfalls zu minimieren. Die Stromversorgung muss gemäß den Anforderungen der Hersteller dimensioniert sein.

2. Um einen unterbrechungsfreien Betrieb bzw. ein ordnungsgemäßes Herunterfahren von Anwendungen sicherzustellen, ist der Einsatz einer unterbrechungsfreien Stromversorgung vorgeschrieben. Maßnahmenpläne für einen Ausfall der Stromversorgung müssen auch den Ausfall einer unterbrechungsfreien Stromversorgung einbeziehen.

   Die unterbrechungsfreie Stromversorgung (USV) müssen regelmäßig auf eine angemessene Dimensionierung (Stromkapazität) überprüft werden. Sie müssen gemäß Herstellerangaben getestet werden.

3. Eine Notbeleuchtung muss, für den Fall eines Stromausfalls, bereitgestellt sein.

4. Die Wasserversorgung muss zuverlässig und angemessen dimensioniert sein, um Klima-, Befeuchtungsgeräte und Brandschutzeinrichtungen zu versorgen. Fehlfunktionen des Wasserversorgungssystems können die Geräte beschädigen und Brandschutzeinrichtungen in ihrer Funktion und Leistungsfähigkeit beeinträchtigen. Ein Alarmierungssystem, das Fehlfunktionen in den Versorgungseinrichtungen erkennt, muss im Bedarfsfall ausgewählt und installiert werden.

5. Telekommunikationseinrichtungen müssen redundant über zwei unterschiedliche Routen an den Telekommunikationsdienstanbieter angebunden sein, um sicherzustellen, dass beim Ausfall einer Anbindung die Kommunikation noch möglich ist. Sprachdienste müssen gegebenenfalls den gesetzlichen Anforderungen an eine Notfallkommunikation genügen.

4.3 Verkabelung

Um Versorgungsleitungen für Strom und Telekommunikation, die Daten transportieren oder Informationssysteme versorgen, vor Abhören und Beschädigung zu schützen müssen die folgenden Regelungen für die Sicherheit der Verkabelung berücksichtigt und angemessen umgesetzt werden:

1. Strom und Telekommunikationsleitungen zu informationsverarbeitenden Einrichtungen müssen, wo möglich, unterirdisch verlegt oder anders geschützt werden;
2. Netzkabel müssen, z. B. durch Verwendung eines Kabelkanals oder durch Vermeidung von Strecken, die über öffentliche Bereiche führen, vor unbefugtem Abhören und Beschädigung geschützt werden;
3. Stromkabel müssen von Kommunikationskabeln getrennt geführt werden, um Interferenzen zu vermeiden;
4. Um Fehlbedienungen, z. B. falsches Patchen von Netzverbindungen, zu vermeiden, müssen klar identifizierbare Markierungen an Kabeln und Geräten vorhanden sein;
5. Um die Wahrscheinlichkeit von Fehlern zu reduzieren, muss die gesamte Verkabelung (inklusive Patch- Felder) ausführlich dokumentiert werden;
6. Für sensitive oder kritische Systeme müssen die folgenden, zusätzlichen Maßnahmen in Erwägung falls möglich gezogen werden:
    - Einsatz von armierten Kabelkanälen und verschlossenen Verteilerräumen und -schränken an Verbindungs- und Endpunkten
    - Einsatz von Glasfaser
    - Abschirmung der Verkabelung gegen elektromagnetische Abstrahlung

- technisches Abtasten (Scannen) und Inspektion der Verkabelung nach unerlaubt angeschlossenen Geräten
- kontrollierter Zugang zu Patch-Feldern und Verteilerräumen
- Portsecurity im Netzwerk des Rechenzentrums

4.4 Instandhaltung

Die folgenden Regelungen für die Instandhaltung müssen risiko- und kostenorientiert umgesetzt werden:

1. Geräte müssen gemäß der vom Hersteller empfohlenen Spezifikationen und Intervalle gepflegt werden.
2. Das Ziel der nachhaltigen, wirtschaftlichen und werterhaltenden Nutzung muss verfolgt werden.
3. Eingehalten werden müssen in der zum Zeitpunkt des Vertragsabschlusses geltenden Fassung:
   - allgemein anerkannte Technik-Regeln
   - DIN-Vorschriften
   - Gewerbe- und Brandschutzbestimmungen
   - Vorschriften zum Umweltschutz und zur Arbeitssicherheit
   - Unfallverhütungsvorschriften
   - Herstellerhinweise
   - VDI-, VDE- und VDS-Bestimmungen
   - alle Vorschriften der Berufsgenossenschaft
4. Reparaturen und Wartungsmaßnahmen dürfen nur von dafür zugelassenem Wartungspersonal durchgeführt werden.
5. Alle vermuteten und tatsächlichen Fehler sowie alle getroffenen vorbeugenden und Fehlerbehebenden Maßnahmen sollten dokumentiert werden.
6. Angemessene Maßnahmen müssen getroffen werden, wenn für Geräte Wartung vorgesehen ist. Dabei muss berücksichtigt werden, ob die Wartung durch eigenes Personal oder durch Externe ausgeführt wird. Wenn notwendig müssen sensitive Informationen vorher entfernt werden oder das Wartungspersonal für diese Arbeit genügend vertrauenswürdig sein.
7. Alle Anforderungen, die als Auflagen von Versicherungen oder zur Sicherstellung von Gewährleistungen (Garantien) vorgegeben sind, müssen erfüllt werden.
8. Herstellerempfehlungen zum Schutz von Betriebsmitteln müssen Beachtung finden.

4.5 Entfernung (Mitnahme) von Betriebsmitteln, Informationen oder Software aus dem Standort

Die Entfernung (Mitnahme) von Betriebsmitteln, Informationen oder Software aus dem Standort ist nur zu dienstlichen Zwecken zulässig und muss genehmigt werden.

Die Ausgabe von mobilen Geräten erfolgt durch die group24. Mobile Geräte dürfen auch explizit außerhalb der group24 Gebäude für dienstliche Zwecke genutzt werden. Es muss keine weitere Genehmigung im Einzelfall erfolgen.

4.6 Entsorgung

Bei Betriebsmitteln (bspw. Fotokopierer) und Geräten, die Speichermedien enthalten, muss vor der Entsorgung überprüft werden, ob alle sensitiven Daten und die lizenzierte Software entfernt oder sicher überschrieben wurden.

Die Entsorgung der Betriebsmittel ist in der OA1002-02 Löschkonzept geregelt.

5 VERBINDLICHKEIT DER REGELUNGEN

5.1 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.

5.2 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.

6 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.

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.