Informationssicherheitsrichtlinie - Löschkonzept

OA1002-1

group24 AG (group24)

INHALTSVERZEICHNIS

STAMMDATEN

Referenz-Nummer:	OA1001-01
Dokumententitel:	Informationssicherheitsrichtlinie - Löschkonzept
Fachlich Verantwortlicher:	Tobias Affeldt
Zuständiger Bereich:	Technical Department
Geltungsbereich:	group24 AG
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	28.07.2022	Andreas Badry	Anpassung auf die group24.
0.2	18.08.2022	Andreas Badry	Anpassung auf die group24.
0.3	30.08.2022	Andreas Badry	Aktualisierung des geforderten Standards zur Überschreibung des Datenträgers. (VSITR) Weiter kleinere Anpassungen.
1.1	01.11.2023	Cihat Dokumaci	Anpassung Verantwortlichkeit, Formatierung

REVIEWNACHWEIS UND FREIGABE

Version	Datum	Teilnehmer	Inhalte des Reviews
V1.0	31.10.2022	Christian Hornhues / Marc Eismann	Gesamt-Review und Freigabe
V1.1	15.11.2023	Christian Hornhues / Marc Eismann	Review 2023

1 EINLEITUNG

Die vorliegende Richtlinie beschreibt und bildet die Grundlage für eine ordnungsgemäße und sichere Entsorgung von Datenträgern in der group24.

Dieses Dokument gilt für alle Mitarbeiter der group24.

Dieses Dokument ist Bestandteil der OA1001-Datenschutzrichtlinie und dient zur Dokumentation zum Informationssicherheits-Managementsystem nach ISO27001.

1.1 Ziel und Zweck

Ziel des Dokuments ist es, die formalen Anforderungen zur sicheren Entsorgung von Datenträgern im Rahmen des Informationssicherheitsmanagementsystems nach ISO27001 zu beschreiben und festzulegen.

Damit vertrauliche oder schützenswerte Daten nach dem Entsorgen eines Datenträgers nicht an unautorisierte Personen gelangen, werden diese Komponenten nach bestimmten formalen Verfahren entsorgt.

Dieses Dokument regelt die Vorgehensweise für eine sichere Entsorgung.

1.2 Gültigkeitsbereich

Dieses Dokument gilt für alle Mitarbeiter der group24, die Dokumente und Datenträger sowie IT-Systeme mit Datenträgern im Rahmen des im „ISO27001 Geltungsbereich“ relevanten Dienstleistungen entsorgen oder für eine Wiederverwendung oder Abverkauf vorbereiten müssen.

1.3 Zuständigkeiten

Für die Umsetzung und Aufrechterhaltung der Prozesse und Verfahren in diesem Dokument, zur Entsorgung von Datenträgern im Sinne der ISO27001 A.8.3.2, ist der Informationssicherheitsbeauftragter verantwortlich.

Der Kontrollverantwortliche zur Qualitätssicherung, Nachvollziehbarkeit und Ordnungsmäßigkeit der Entsorgungsverfahren ist der Informationssicherheitsbeauftragte der group24.

1.4 Abkürzungen und Definitionen

Kürzel	Bedeutung
IS-Team	Informationssicherheits-Team
DS-GVO	Europäische Datenschutz-Grundverordnung
HDD	Hard Disk Drive, Festplatte
SLA	Service Level Agreement, Dienstgütevereinbarung

SSD	Solid State Disc/Drive, Halbleiterlaufwerk, Festplatte aus Speicherchips
HGB	Handelsgesetzbuch, der Kern des Handelsrechts in Deutschland, gültig für Kaufleute
EStG	Einkommensteuergesetz, Regelung der Besteuerung des Einkommens natürlicher Personen
KStG	Körperschaftsteuergesetz, Regelung der Besteuerung des Einkommens juristischer Personen
GewStG	Gewerbesteuergesetz, Regelung der Besteuerung des Gewerbeertrags
AO	Abgabenordnung, für alle Steuerarten geltenden Regelungen über das Besteuerungsverfahren
BGB	Bürgerliches Gesetzbuch, Regelungen der Rechtsbeziehungen zwischen Privatpersonen
ZPO	Zivilprozessordnung, Regelung der gerichtlichen Verfahren in Zivilprozessen

2 BERÜCKSICHTIGUNG VON RICHTLINIEN UND DATENSCHUTZGESETZEN

Für den Entsorgungsprozess sind die folgenden Vorgaben und Richtlinien zu beachten:

- Europäische Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Landesdatenschutzgesetze relevanter Bundesländer
- Gesetzliche Aufbewahrungsfristen aus dem Handelsrecht (HGB), aus steuerrechtlichen Vorschriften (EStG, KStG, GewStG, AO) sowie zivilrechtliche Vorschriften (BGB, ZPO), die ggf. einer Entsorgung entgegenstehen.
- Interne Richtlinien und Vorgaben

Diese Richtlinie stellt die Mindestanforderungen an eine sichere Entsorgung von Datenträgern dar.

3 DEFINITION VON DATENTRÄGERN

Informationen können auf papiergebundenen sowie elektronischen Medien gespeichert werden. In diesem Dokument wird zwecks Vereinfachung der Begriff „Datenträger“ verwendet.

Als Datenträger werden Komponenten oder Geräte verstanden, auf denen Informationen (Daten) gespeichert werden können. Datenträger können insbesondere sein, oder enthalten sein in:

3.1 Papier

Papiergebundene Informationsträger, wie

- Akten
- Ausdrucke
- Schriftverkehr
- Fotos
- Faxe
- Kopien
- Aufzeichnungen
- Systemdokumentationen

3.2 Digitale Datenträger

Digitale Datenträger, wie

- Intern verbaute Festplatten
- Extern anschließbare Festplatten
- SSD
- Datensicherungsbänder/Backup-Tapes
- Optische Datenträger wie CDs, DVDs und BluRays
- Disketten
- Memory Sticks / USB Sticks
- Flashspeicher (z.B. SD-Karten)

3.3 IT-Systeme / Trägersysteme

An oder in Geräte gebundene Datenträger in

- Router / Switches
- Fat Clients

- Notebooks
- Server
- Smartphones / Tablets
- Digitalkameras
- Diktiergeräte
- Multifunktionsgeräte
- Drucker
- Scanner
- Faxgeräte

4 GEFÄHRDUNGSLAGE

Bei der Entsorgung von unverschlüsselten Informationen müssen sowohl schutzbedürftige Informationen auf Papier als auch solche betrachtet werden, die auf digitalen Datenträgern (elektronisch, magnetisch, optisch) oder in IT-Systemen gespeichert sind.

Analoge Datenträger wie Mikrofilm, etc. werden bei der group24 nicht verwendet. Fällt dennoch ein derartiger Datenträger zur Entsorgung an, so erfordert dies eine Einzelfall-Behandlung durch den Informationssicherheitsbeauftragten und / oder den Datenschutzbeauftragten der group24.

Bei der Entsorgung von IT-Systemen sind alle IT-Systeme mit integrierten Speichermedien zu berücksichtigen, insbesondere auch Netzwerkkomponenten wie Access Points, Router und Switches sowie ggf. Multifunktionsdrucker und Kopierer.

Dabei gilt es zu bedenken, dass mechanisch beschädigte Datenträger mit forensischen Methoden selbst dann noch ausgelesen werden können, wenn Standard-Betriebssysteme diese als nicht lesbar anzeigen und keinen Zugriff auf die Daten ermöglichen.

Wenn nicht oder nur unzureichend gelöschte Datenträger weitergegeben oder ausgesondert werden, kann eine Wiederherstellung von noch enthaltenen Informationen dem Unternehmen erhebliche Schäden verursachen. Ein besonderes Risiko stellen dabei Authentisierungsinformationen für den Zugriff auf group24 Ressourcen, hochsensible Unternehmensdaten und personenbezogene Informationen dar.

5 GRUNDSÄTZE

Alle unverschlüsselten Datenträger sind, mangels gesicherter Informationen über die Kritikalität der dort gespeicherten Informationen, als HOCH KRITISCH einzustufen und somit nachhaltig sicher unter Anwendung formaler Verfahren zu entsorgen. Im Folgenden die Grundsätze für eine sichere Entsorgung von Datenträgern:

5.1 Nachvollziehbarkeit

Der Lebenszyklus von Datenträgern muss über den gesamten Weg von Erhalt / Erfassung bis zur Bereitstellung für den Entsorger (inkl. einer vorherigen Löschung und ggf. physischen Zerstörung) nachvollziehbar sein.

Dies wird durch eine Dokumentation am Asset im Assetmanagement sowie durch Ablage des Entsorgungsbelegs sichergestellt.

5.2 Physische Zerstörung

Für physisch bei der group24 zerstörtes Material muss die Zerstörungstechnik (z.B. Aktenvernichter, Festplatten- / CD- / Bänder- Schredder) gewährleisten, dass die Gewinnung von Informationen aus dem zerstörten Material nicht mehr praktikabel ist.

Gleiches gilt für Zerstörung durch beauftragte Entsorgungs-Dienstleister.

Die Zerstörung der Datenträger für interne Zwecke ist auf Basis des Status des Assets im Assetmanagement sowie im SharePoint jederzeit nachvollziehbar.

Die Zerstörung der Datenträger von Kunden ist auf Basis des Status des Assets im SharePoint für den jeweiligen Kunden jederzeit nachvollziehbar.

5.3 Datenlöschung durch Überschreiben

Bevor ein unverschlüsselter Datenträger im Rahmen von Entsorgung oder Abverkauf den Einflussbereich der group24 verlässt, und nicht physikalisch zerstört wird, müssen die Daten auf diesem Datenträger durch ein sicheres Löschverfahren (softwaretechnisch) nachhaltig unleserlich gemacht werden.

Als sicheres Löschverfahren gilt der VSITR- Standard des Bundesamtes für Sicherheit in der Informationstechnik, muss ein Datenträger in sieben Durchgängen überschrieben werden. Bei den ersten 6 Durchgängen wird jeweils das Bitmuster des vorherigen Durchgangs umgekehrt. Durch diese Umkehrung der Bits sollen Datenreste destabilisiert werden, die sich eventuell noch an den Rändern der zum Schreiben der Daten verwendeten Spur befinden können. Gleiches gilt für die Löschung durch beauftragte Entsorgungs-Dienstleister.

5.4 Abverkauf / Wiederverwertung

Unverschlüsselte Datenträger, die an group24 IT zum Abverkauf oder Verwertung zurückgegeben bzw. außer Dienst gestellt werden und für eine Wiederverwendung aufbewahrt werden sollen, sind vor der Wiederverwendung grundsätzlich sicher durch mehrfaches Überschreiben gemäß Kapitel 5.3 zu löschen.

Unverschlüsselte Datenträger sind, sofern sie gesammelt werden („kritische Masse“), bis zur Verwertung sicher vor Zugriff und Abgriff durch geeignete Maßnahmen zu schützen. (Zugangsbeschränkter Lagerort, eingeschränkter Personenkreis)

Der Abverkauf oder die Wiederverwertung von Datenträgern, muss durch den Status im Assetmanagement jederzeit nachvollziehbar sein. Das Verfahren „Abverkauf Assets“ muss entsprechend der Vorgaben aus diesem Dokument berücksichtigen und erfüllen.

5.5 Reporting

Dem Kontrollverantwortlichen für informationssicherheitsrelevante Prozesse, zu denen auch die Inhalte aus diesem Dokument gehören, ist regelmäßig über die Vorgänge zur Entsorgung von Datenträgern zu berichten bzw. Einsicht zu gewähren.

Die Zyklen und Häufigkeit des Reporting bestimmt der Kontrollverantwortliche.

Inhaltlich soll über

- Anzahl und Art der entsorgten Datenträger
- Ergebnisse der Validierungsprüfung der Entsorgungsrückmeldungen
  - Übereinstimmung (Grün)
  - Unstimmige Rückmeldung (Rot)
- Ergebnisse von Dienstleisteraudits der Entsorger
- Auffälligkeiten im Rahmen der Entsorgung berichtet werden.

6 ENTSORGUNG

Im Scope der group24 wurden folgende Datenträger als relevant für dieses Dokument identifiziert:

- Verschlüsselte Datenträger (Festplatten) aus
  - Fat Clients
  - Laptops
  - Multifunktionsgeräten
- Nicht verschlüsselte Datenträger aus:
  - Servern
  - USB-Datenträger (Sticks, HDD)
  - Optische Datenträger (CD/DVD)
  - Papiergebundene Datenträger

Die folgenden Kapitel geben vor, wie die jeweilige Datenträgerart zu behandeln ist. Grundsätzlich gilt es dabei die Grundsätze aus Kapitel 5 zu berücksichtigen. In Zweifeln über Art und Umfang kann und soll das IS-Team hinzugezogen werden.

6.1 Papiergebundene Informationsträger

Grundsätzlich gilt: alle papiergebundenen Informationsträger sind vor der Entsorgung mit einem Aktenvernichter, der den Anforderungen zu hohem bzw. sehr hohem Schutzbedarf genügen muss, zu vernichten zu entsorgen.

6.2 Verschlüsselte digitale Datenträger

Die verschlüsselten Datenträger sind durch ihre besondere Eigenschaft einer Verschlüsselung der Daten grundsätzlich vor unautorisiertem Zugriff, nach Ausbau aus den Trägersystemen bzw. durch eigene Hardwareverschlüsselung, ausreichend geschützt. Diese Datenträger benötigen keine besondere Behandlung wie Löschen oder Schreddern.

Es muss jedoch sichergestellt sein, dass kein unautorisierter Zugriff auf die jeweilig zugehörigen Schlüssel mehr möglich ist.

Das Löschen bzw. Entfernen von Schlüsselmodulen wird durch die Software group24 sichergestellt.

(Löschen des Schlüssels, Entfernen von Schlüsselmodulen)

6.3 Unverschlüsselte digitale Datenträger

Da der Grundsatz gilt, dass alle Information auf Datenträgern als hoch kritisch anzusehen sind, sind digitale Datenträger unter Berücksichtigung der folgenden Vorgaben zu entsorgen:

- Alle nichtverschlüsselten Datenträger sind, sofern ein Löschen technisch noch möglich ist, vor einer Entsorgung durch mehrfaches Überschreiben zu löschen. In

Fällen wo das technisch nicht mehr umzusetzen ist, muss das IS-Team konsultiert werden.

- Alternativ zur Löschung durch Überschreiben kann auch eine physikalische Zerstörung mittels Schredder durchgeführt werden (bevorzugt).
- Optische Datenträger (CD, DVD) sind vor einer Entsorgung zu zerstören. (z.B. per geeignetem Aktenvernichter/Schredder oder Entsorgungs-Dienstleister).

Die Löschung / Zerstörung von Datenträgern ist im Assetmanagement zu dokumentieren.

Die Entsorgung sonstiger digitaler Datenträger (z.B. USB-Sticks, Speicherkarten) ist mit dem ISB abzustimmen.

Um den Aufwand der Entsorgung zu minimieren, werden die Datenträger zunächst verschlossen aufbewahrt (Büro Interne IT) und ab einer ausreichenden Menge über entsprechende Dienstleister entsorgt.

6.4 IT-Systeme

Datenträger, wie Festplatten in IT-Systemen, die nicht verschlüsselt sind, sind gemäß Kapitel 6.3 zu behandeln. Sollen bei der Entsorgung eines IT-Systems die enthaltenen digitalen Datenträger für eine mögliche Wiederverwendung (als Ersatzteil, Abverkauf) aufbewahrt werden, so sind diese vor der Einlagerung sicher durch Überschreiben zu löschen und in der Asset-Verwaltung (z.B. per Seriennummer oder Label) zu erfassen. In Wartungsfällen für Server, bei denen ein Defekt einer unverschlüsselten Festplatte vorliegt, kann die Herausgabe der defekten Festplatte in unbeschädigter Form zur Bedingung für die Wartungsleistung (Festplattenersatz) gemacht werden. Da sich defekte Festplatten zudem häufig nicht mehr sicher löschen lassen, kann sich daraus ein Sicherheitsproblem ergeben.

Um diesem Fall vorzubeugen, sind schon bei der Beschaffung von IT-Systemen z.B. das Einbehalten oder Zerstören von unverschlüsselten defekten Festplatten für den Fall einer Wartung mit dem Lieferanten abzustimmen („keep your harddrive on fail“) und im Rahmen der Kaufentscheidung zu berücksichtigen.

In Wartungsfällen, in denen die Herausgabe einer unverschlüsselten defekten Festplatte, die sich nicht mehr sicher löschen lässt, an den Wartungsdienstleister in unbeschädigter Form verlangt wird, ist das IS-Team zu konsultieren.

Auf IT-Systemen mit integriertem OS (z.B. Access-Points, Switche, Router, Appliance, sowie Thin Clients) sind, sofern technisch möglich, alle Konfigurationen vor einer Entsorgung zu löschen bzw. auf den Werkszustand zurückzusetzen.

Ist ein Zurücksetzen oder Löschen nicht möglich, sind je nach Einzelfall mit dem ISB Alternativmaßnahmen (z.B. Speicherchips zerstören) abzustimmen.

6.5 Notebooks / Fat Clients

Alle Notebooks und Fat Clients im Scope der group24 besitzen grundsätzlich BitLocker verschlüsselte Festplatten. Die Aktivierung von Bitlocker erfolgt bei allen weiteren Geräten durch die Einführung von

Mobile Device Management (ist bereits im Rollout). Hier erfolgt auch eine Protokollierung/Mitteilung über den aktuellen Status des Gerätes.

Notebooks bzw. Fat Clients werden oft intern wiederverwendet, weitergegeben oder verkauft.

Um die Sicherheit der Daten auf den Festplatten vor Weitergabe lückenlos zu gewährleisten, kümmert sich das group24 IT mit einem etablierten Verfahren um den Wechsel des BitLocker-Schlüssels und das Formatieren der Festplatte. Alle Schritte lassen sich im verwendeten Tool Azure Portal nachvollziehen. Wenn gewünscht können dort auch Protokolle zum Reporting gezogen werden.

In Ausnahmefällen werden Fat Clientsauch nicht verschlüsselt betrieben. In dem Falle gilt Kapitel 5.3.

6.6 Mobile Endgeräte (Smartphones / Tablets)

Mobile Endgeräte wie Smartphones und Tablets sind mit aktiver Geräte- bzw. Dateiverschlüsselung zu betreiben. Vor der Entsorgung sind derartige Endgeräte dann lediglich (per Factory Reset) zurückzusetzen, so dass ein sicheres Löschen des Verschlüsselungsschlüssels stattfindet.

Bei Endgeräten, die keine Geräte- bzw. Dateiverschlüsselung bieten, (z.B. Altbestand) ist die Entsorgung im Einzelfall mit dem IS-Team abzustimmen.

Herausnehmbare Speicherkarten aus den mobilen Endgeräten müssen gemäß den Grundsätzen in diesem Dokument einer sicheren Entsorgung bzw. Wiederverwertung zugeführt werden.

6.7 Multifunktionsdrucker und Kopierer

Multifunktionsdrucker und Kopierer werden im Falle eines Defekts oder bei Außerbetriebnahme bzw. Austausch durch ein Serviceunternehmen für Bürosysteme gewartet bzw. abgeholt.

Es muss sichergestellt sein, dass im Rahmen der Wartung durch Fremdunternehmen kein unbefugter Zugriff auf die Informationen auf den internen Speichermedien erfolgt. Um das zu gewährleisten, kann beispielsweise ein Mitarbeiter während der Wartungsarbeiten darauf achten, dass keine Daten kopiert werden.

Sollen enthaltene Speichermedien (durch Austausch oder Außerbetriebnahme) das Unternehmen verlassen, so ist vorher deren sichere Löschung mit dem Informationssicherheit-Team zu koordinieren und sicherzustellen.

In den Fällen, wo die Datenträger einer Verschlüsselung unterliegen, ist sicherzustellen, dass der Schlüssel zuverlässig und nachweislich aus den Geräten entfernt wird.

7 ENTSORGUNGSDIENSTLEISTER

7.1 Verpflichtung nach DSGVO

Mit dem Entsorgungsdienstleister, der einen Zugriff auf Informationen haben könnten, müssen gemäß Art. 28 Abs. 3 lit b DSGVO verpflichtet werden, das heißt ein Vertrag zur Auftragsverarbeitung abgeschlossen werden.

Falls zu entsorgende Informationsträger (Dokumente, Datenträger) schon bei der Group24 einer physischen Zerstörung unterzogen werden oder verschlüsselt sind, also noch vor der Übergabe der Informationsträger an den Entsorgungsdienstleister, ist eine Verpflichtung nach DSGVO beim Dienstleister nur optional.

7.2 Vereinbarungen

Grundsätzlich sind mit den Entsorgungsdienstleistern Vereinbarungen zu treffen, die die Rahmenbedingungen zur sicheren Entsorgung oder Wiederverwendung von Datenträgern festschreiben.

Zertifizierte Dienstleister sind bei der Vergabe von Aufträgen zu bevorzugen.

7.3 Nachweise

Die Löschung oder Zerstörung eines Datenträgers muss durch ein Lösch- bzw. Zerstörungsprotokoll des Dienstleisters dokumentiert werden. Löschungen bzw. Zerstörungen multipler Datenträger können auch durch ein sogenanntes „Sammelzertifikat“ nachgewiesen werden.

Auf den Protokollen müssen die Seriennummern der Datenträger zur Überprüfung ausgewiesen werden.

Die Seriennummern dürfen dem Entsorger vorab NICHT mitgeteilt werden, damit dieser gezwungen wird, die Seriennummern selbst zu erfassen und die Nachfolgeprozesse der group24 somit eine Kontrollmöglichkeit über die Validität der „Meldung zur Löschung / Zerstörung“ haben. (interne Seriennummer-Liste vs. Meldeliste des Entsorgers).

8 ANHANG

8.1 DSGVO Art. 17 – Recht auf Löschung

Der Artikel 17 DSGVO definiert das Recht auf Löschung ("Recht auf Vergessenwerden").

8.2 SLAs zur sicheren Entsorgung von Datenträgern über Dienstleister

Anforderungen an Dienstleister die mit der Entsorgung oder Verwendung von Datenträgern der Group24 beauftragt werden.

8.2.1 Verpflichtung nach DSGVO

Der Entsorgungsdienstleister verpflichtet sich, konform zur DSGVO zu arbeiten, Datenträger nachhaltig sicher zu löschen und im Rahmen seines Verwertungsprozesses sicherzustellen, dass kein unautorisierter Zugriff auf die Datenträger erfolgen kann. Es wird ein Vertrag über die Auftragsverarbeitung mit dem Entsorgungsdienstleister abgeschlossen.

8.2.2 Sichere Löschung der Informationen

Der Entsorgungsdienstleister verpflichtet sich, als sicheres Löschverfahren ein dreifaches Überschreiben mit beliebigen Zufallsdaten mittels einer geeigneten Software („Wipe-Tool“) durchzuführen.

8.2.3 Sichere Zerstörung der Datenträger

Der Entsorgungsdienstleister verpflichtet sich, durch geeignete Zerstörungstechnik und Partikelgröße sicher zu stellen, dass die Gewinnung von Informationen aus dem zerstörten Material nicht mehr praktikabel ist.

8.2.4 Nachweis und Protokollierung

Der Entsorgungsdienstleister verpflichtet sich, die Löschung oder Zerstörung eines Datenträgers durch ein Protokoll zu dokumentieren. Löschungen oder Zerstörungen multipler Datenträger können auch durch ein sogenanntes „Sammelzertifikat“ nachgewiesen werden.

Auf den Protokollen müssen die Seriennummern der Datenträger zur Überprüfung ausgewiesen werden.

8.2.5 Meldepflichten

Der Entsorgungsdienstleister verpflichtet sich, durch interne Kontrollmaßnahmen sicherzustellen, dass Unstimmigkeiten hinsichtlich Art und Menge der zu entsorgenden Datenträger, sowie Problemen, die den Schutz der Daten gefährden, unverzüglich an die Group24 gemeldet werden.

8.2.6 Auditvorbehalt

Der Entsorgungsdienstleister verpflichtet sich, der Group24 regelmäßige interne Prüfungen (Audits) seiner Entsorgungsverfahren zu ermöglichen.

Mögliche Prüfpunkte können sein:

- Löschprotokolle der genutzten Software
- Schutz beim Transport der Datenträger
- Schutz bei der Lagerung der Datenträger
- Zugriffsberechtigter Personenkreis zu den Datenträgern

9 VERBINDLICHKEIT DER REGELUNGEN

9.1 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.

9.2 Ausnahmeregelung

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

Diese Ausnahmen sind zentral vom IT Security Manager zu dokumentieren.

10 VERSTÖSSE UND SANKTIONEN

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.