Leitlinie zur Informationssicherheit

OA1002

group24 AG (group24)

INHALTSVERZEICHNIS

1 Einleitung 4
1.1 Ziel des Sicherheitsmanagements 4
1.2 Verantwortung des Managements 4
2 Organisation der Sicherheit 5
2.1 Sicherheitsleitlinie 5
2.2 Sicherheitsrichtlinien 5
2.3 Operative Vorgabendokumente 6
2.4 Aufzeichnungen 6
2.5 Struktur der ISMS-Dokumente 6
3 Rollen und Verantwortlichkeiten 7
3.1 Höchste Kontrollinstanz 7
3.2 Führungskräfte 7
3.3 Mitarbeiter 7
3.4 Betreiber 8
4 Prinzipien 9
5 Verbindlichkeit der Regelungen 10
5.1 Verbindlichkeit der Regelungen 10
5.2 Ausnahmeregelung 10
6 Verstöße und Sanktionen 11

STAMMDATEN

Referenz-Nummer:	OA1002
Dokumententitel:	Leitlinie zur Informationssicherheit
Fachlich Verantwortlicher:	Andreas Badry
Zuständiger Bereich:	Informationssicherheit
Geltungsbereich:	group24
Gültig von:	02.11.2022
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	16.09.2022	Andreas Badry	Anpassung auf die group24
0.4	22.09.2022	Andreas Badry	Anpassung auf die group24

REVIEWNACHWEIS UND FREIGABE

Version	Datum	Teilnehmer	Inhalte des Reviews
V1.0	31.10.2022	Christian Hornhues / Marc Eismann	Ersterstellung
V1.1	15.11.2023	Christian Hornhues / Marc Eismann	Review 2023

1 EINLEITUNG

Die vorliegende Organisationsanweisung definiert die Sicherheitspolitik der group24 und beschreibt die Rollen und Verantwortlichkeiten in der Informationssicherheitsorganisation. Weiter werden Verantwortlichkeiten für Anwender und Betreiber festgelegt (siehe Anlagen Sicherheitsgrundsätze).

1.1 Ziel des Sicherheitsmanagements

Die group24 bietet ihren Kunden Dienstleistungen im Bereich Consulting und Managed Service an.

Folglich sind der Erhalt der Vertraulichkeit, Integrität und Authentizität der Kundendaten sowie die Einhaltung gesetzlicher Vorgaben an den Schutz personenbezogener Daten oberste Ziele des Informationssicherheits-Managementsystems (ISMS) der group24, das nach ISO/IEC 27001 (2013) aufgebaut wird.

1.2 Verantwortung des Managements

Der Vorstand der group24 beauftragt das ISMS mit der Identifikation und dem verantwortungsvollen Umgang mit wesentlichen Risiken sowohl für die group24 selbst als auch für deren Kunden. Hierfür stellt der Vorstand die notwendigen personellen und sachlichen Ressourcen zum Betrieb und zur Weiterentwicklung des ISMS zur Verfügung. Der Vorstand überzeugt sich regelmäßig von der ordnungsgemäßen Arbeit des ISMS, unter anderem durch regelmäßige Berichtsmeetings.

2 ORGANISATION DER SICHERHEIT

2.1 Sicherheitsleitlinie

Die Sicherheitsleitlinie ist eine Richtungsvorgabe für die Umsetzung von Sicherheit in der group24. Sie ist die Grundlage für alle nachgeordneten Sicherheitsrichtlinien, -konzepte, -vorgaben und -empfehlungen und weiterführenden Organisationsanweisungen.

Die Sicherheitsleitlinie basiert auf folgenden Vorgaben:

1. Alle Maßnahmen zur Wahrung der Sicherheit müssen dem Risiko und den zu schützenden Werten angemessen sein. Um die Angemessenheit zu gewährleisten, sind regelmäßig die Risiken und Schwachstellen zu identifizieren sowie geeignete Sicherheitsmaßnahmen auszuwählen und zu realisieren.

2. Die Sicherheitskultur ist von dem Grundsatz geprägt, dass die Eigenverantwortung jedes einzelnen Mitarbeiters und präventive Maßnahmen Vorrang vor unangemessenen Kontrollen und permanenter Überwachung haben.

3. Regelungen zur Sicherheit werden schriftlich festgehalten und allen Mitarbeitern zur Kenntnis gebracht werden.

4. Die Mitarbeiter müssen über die Bedeutung der Sicherheit für das Unternehmen und für ihren Arbeitsbereich unterrichtet und sensibilisiert werden.

5. Sicherheitsvorfälle und Schäden werden quantifiziert und an den Informationssicherheitsbeauftragten (ISB) gemeldet. Allen wesentlichen Sicherheitsvorfällen muss nachgegangen werden. Zugrunde liegende Mängel werden ermittelt und eine Beseitigung der Mängel forciert.

6. Die Einhaltung der Sicherheitsleitlinie wird durch die jeweils zuständigen Prüfverantwortlichen (z.B. IT-Sicherheit, Datenschutz) oder die Revision überprüft.

2.2 Sicherheitsrichtlinien

In den Sicherheitsrichtlinien werden die Mindestanforderungen an die Sicherheit in der group24 definiert. Jede Einheit kann bei Bedarf innerhalb ihres Zuständigkeitsbereichs weitreichendere Vorgaben erstellen und umsetzen. Eine Aussetzung einzelner Sicherheitsrichtlinien bzw. einzelner Vorgaben einer Richtlinie ist nur in Ausnahmefällen temporär in Abstimmung mit der Geschäftsführung möglich.

Die Sicherheitsrichtlinien werden als Anlage zu diesem Dokument geführt und werden sowohl thematisch als auch zielgruppenspezifisch verfasst.

2.3 Operative Vorgabendokumente

In operativen Vorgabendokumenten - namentlich Handlungsanweisungen, Verfahrensanweisungen und Sicherheitskonzepte - werden die Vorgaben der Sicherheitsleitlinie und -richtlinien weiter konkretisiert, sofern dies erforderlich ist.

2.4 Aufzeichnungen

In Aufzeichnungen wird die Umsetzung von Maßnahmen dokumentiert. Hierbei handelt es sich um Protokolle, Prüfnachweise, die Business Impact Analyse (BIA) und den Risikokatalog.

2.5 Struktur der ISMS-Dokumente

Die ISMS-Dokumente sind hierarchisch aufgebaut. Alle Dokumente unterliegen der Sicherheitsleitlinie, darunter gibt es die weiteren, oben aufgeführten, Dokumentebenen. Die ISMS-Dokumentenpyramide ist unten grafisch dargestellt.

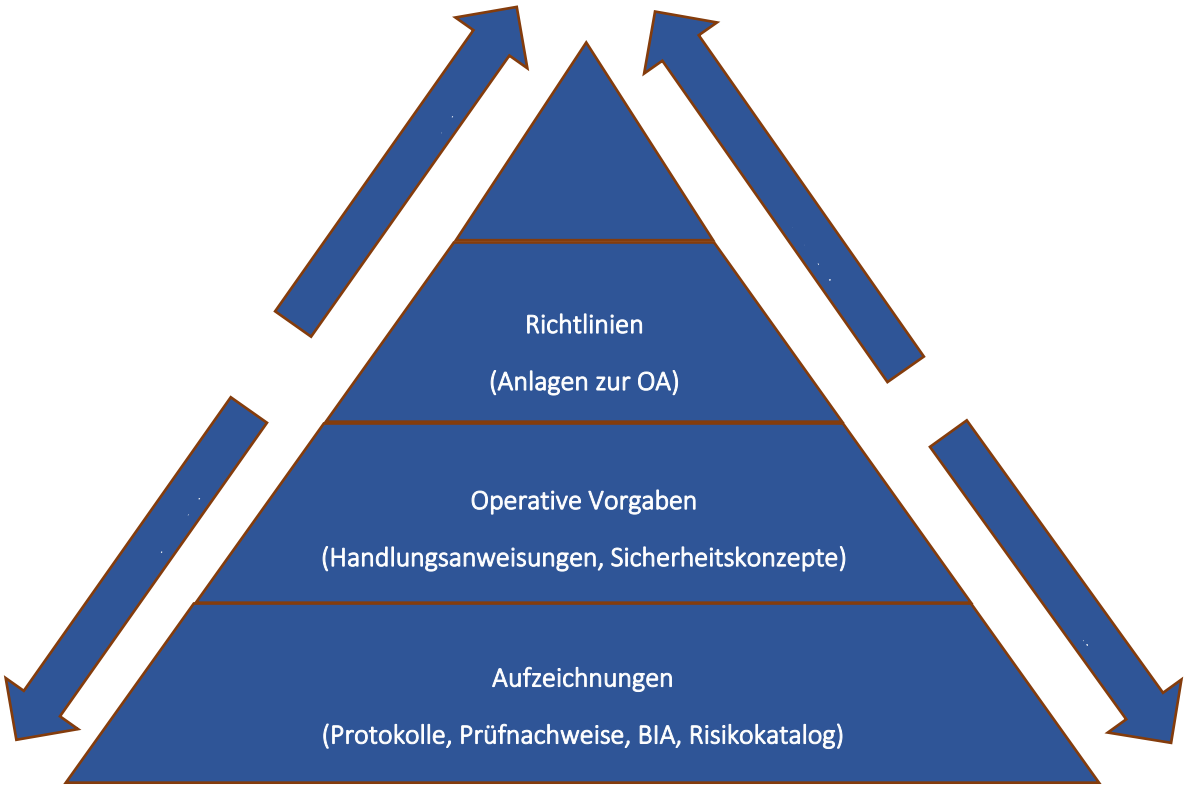

Abbildung 1: Struktur der ISMS-Dokumente

3 ROLLEN UND VERANTWORTLICHKEITEN

Voraussetzung für einen funktionierenden Sicherheitsprozess ist ein geeigneter organisatorischer Rahmen, in dem die jeweiligen Rollen und Verantwortlichkeiten verbindlich festgelegt werden. Dabei kann das Erreichen der angestrebten Sicherheitsziele und die Durchsetzung sowie die Aufrechterhaltung eines angemessenen Sicherheitsniveaus nur durch ein geplantes und organisiertes Vorgehen aller Beteiligten gewährleistet werden.

3.1 Höchste Kontrollinstanz

Die Verantwortung für die Sicherheit in der group24 liegt bei der höchsten Kontrollinstanz.

Diese gibt die Sicherheitspolitik der group24 vor, legt die Grundsätze der Sicherheit fest, fördert die Sicherheitskultur und unterstützt die Umsetzung der Sicherheitspolitik in allen Unternehmensbereichen der group24. Sie delegiert soweit erforderlich die notwendigen Zuständigkeiten und Kompetenzen zur Koordination und Kontrolle des Sicherheitsprozesses.

3.2 Führungskräfte

Zur Wahrung der Sicherheit ist die aktive Mitwirkung der Mitarbeiter mit Führungsfunktion unerlässlich. Führungskräfte müssen darauf achten, dass die in ihrem Verantwortungsbereich eingeführten Sicherheitsmaßnahmen eingehalten werden. Sie haben bezüglich der Einhaltung der Sicherheitspolitik Vorbildfunktion und sorgen für die Sensibilisierung und Schulung ihrer Mitarbeiter. Sie organisieren die Einführung und Durchsetzung von Sicherheitsmaßnahmen innerhalb ihres Zuständigkeitsbereichs – ggf. in Zusammenarbeit mit den jeweils zuständigen Verantwortlichen.

- Notfallmanager – Andreas Badry
- IT-Sicherheitsbeauftragten – Andreas Badry
- Datenschutzbeauftragten – Marcel Konrads

3.3 Mitarbeiter

Jeder Mitarbeiter der group24 ist persönlich verantwortlich für die Einhaltung der Sicherheitsgrundsätze. Jeder Mitarbeiter muss die Sicherheitsgrundsätze kennen, verstehen und in seiner Funktion und Zuständigkeit umsetzen. Im Rahmen der jährlichen Mitarbeitergespräche weisen die Führungskräfte die Mitarbeiter auf die Sicherheitsgrundsätze und die Notwendigkeit der Kenntnisnahme hin. Unterlagen und Anweisungen zu diesem Themenkomplex stehen den Mitarbeitern zur Verfügung.

Zu den Aufgaben eines Mitarbeiters gehört es darüber hinaus, Sicherheitsvorfälle, Fehler, Schwachstellen oder Bedrohungen so früh wie möglich dem, IT-Sicherheitsbeauftragten zu melden, um die Evaluation und Quantifizierung der Vorfälle zu ermöglichen. Als Anwender

von sicherheitsrelevanten Einrichtungen, Systemen oder Prozessen sind dabei für alle Mitarbeiter insbesondere die Sicherheitsgrundsätze für Anwender relevant.

3.4 Betreiber

Betreiber von sicherheitsrelevanten Einrichtungen, Systemen oder Prozessen haben eine zentrale Bedeutung bei der Umsetzung und Aufrechterhaltung von Sicherheitsmaßnahmen in der group24. Dabei macht es keinen Unterschied, ob der Betrieb durch eine Einheit innerhalb der group24 oder durch externe Dienstleister erbracht wird. Für Betreiber sind dabei insbesondere die Sicherheitsgrundsätze für Betreiber bindend. In den Verträgen mit externen Dienstleistern wird die Einhaltung der Sicherheitsgrundsätze verbindlich fixiert

4 PRINZIPIEN

Hieraus leitet die group24 drei Prinzipien zur Umsetzung der Informationssicherheit und des Notfallmanagements. Diese sind:

- Die Vermeidung von Unterbrechungen und Inkonsistenzen der eingesetzten informationstechnischen Infrastrukturen spielt eine maßgebliche Rolle bei der Durchführung der Arbeitsvorgänge. Deswegen werden die für die Erbringung eingesetzten informationstechnischen Infrastrukturen so betrieben, dass Ausfälle einzelner Komponenten im Rahmen des Notfallmanagements toleriert werden können (Prinzip der Verfügbarkeit und Fehlerfreiheit).
- Technische und organisatorische Maßnahmen stellen sicher, dass die Auswirkungen von Unregelmäßigkeiten in Daten oder Fehlfunktionen in informationstechnischen Infrastrukturen vermieden werden, nicht unbemerkt bleiben und zeitlich begrenzt werden (Prinzip der Integrität).
- Der Schutz sensibler Daten und informationstechnischer Infrastrukturen wird dadurch gewährleistet, dass diese ausschließlich Berechtigten zugänglich gemacht werden (Prinzip der Vertraulichkeit).

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 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.

6 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.

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 der group24. 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.

Unterschriften – Vorstand der group24 AG

Marc Eismann _____

Christian Hornhues _____