Leitlinie Informationssicherheit

Informationssicherheitsbereich

Exported on 12/15/2023

Table of Contents

1 Inhaltsverzeichnis 4
2 Informationen zum Dokument 5
2.1 Freigegebene Version 5
3 1. Informationen und Rahmenbedingungen zur Richtlinie 6
3.1 1.1 Allgemeines 6
3.2 1.2 Anwendungsbereich 6
3.3 1.3 Kontext der Organisation 7
3.4 1.4 Interessierte Parteien und deren Anforderungen 7
3.4.1 1.4.1 Kunden 7
3.4.2 1.4.2 Geschäftsführung 8
3.4.3 1.4.3 Gesellschafter 8
3.4.4 1.4.4 Mitarbeiter 8
3.4.4.1 1.4.4.1 Festangestellte Mitarbeiter 8
3.4.4.2 1.4.4.2 Freiberufliche Mitarbeiter 8
3.4.5 1.4.5 Partnerunternehmen 8
3.4.5.1 1.4.5.1 Vertriebspartner 8
3.4.5.2 1.4.5.2 Technologiepartner 8
3.4.6 1.4.6 Lieferanten 9
3.4.6.1 1.4.6.1 Vertriebssoftwarelieferanten 9
3.4.6.2 1.4.6.2 Cloud-Softwarelieferanten 9
3.4.6.3 1.4.6.3 Sonstige Lieferanten 9
3.4.7 1.4.8 Gesetzgeber 9
3.4.8 1.4.9 Behörden 9
3.4.9 1.4.10 Untermieter 9
3.5 1.5 Referenzierte Dokumente 10
3.6 1.6 Kommunikation, Überprüfung und Verbesserung 10
4 2. Grundsätze Informationssicherheit 12

4.1 2.1 Abgrenzung Informationssicherheit - Datenschutz 12
4.2 2.2 Informationssicherheitsziele 12
4.2.1 2.2.1 Informationssicherheit ist integraler Bestandteil unseres Handelns ... 13
4.2.2 2.2.2 Informationssicherheit ist immer Up to Date 13
4.2.3 2.2.3 Need-to-know-Prinzip 14
4.2.4 2.2.4 Sichere Kommunikation auf allen Wegen mit allen Partnern 14
5 3. Verantwortung und Rollen 15
5.1 3.1 Verantwortung Führungskräfte 15
5.2 3.2 Verantwortung Mitarbeiter 15
5.3 3.3 Informationssicherheitsbeauftrager (ISB) 15
5.4 3.4 Datenschutzbeauftragter(DSB) 16
5.5 3.5 Weitere Rollen im Umfeld Datenschutz und Informationssicherheit 16
5.5.1 3.5.1 Informationsrisikomanagement 16
5.5.2 3.5.2 Governance 16
5.5.3 3.5.3 Compliance 16
5.5.4 3.5.4 Informationssicherheits-Managementsystem (ISMS) 17
5.5.5 3.5.5 IT-Verantwortliche 17
5.5.6 3.5.6 Krisenstab 17
5.6 3.6 Sicherheitsüberprüfung für Rollen mit entsprechender Kritikalität 18
6 4. Verstöße 19
7 5. Verpflichtungserklärung 20
8 Historie dieses Dokumentes 21
8.1 Freigabehistorie 21
8.2 Versionshistorie 24

1 Inhaltsverzeichnis

2 Informationen zum Dokument

2.1 Freigegebene Version

Freigegebene Version	13
Datum der Freigegebenen Version	13.12.2023
Freigabe erteilt durch	swenig
Klassifikation	öffentlich
Dokumentenart	b) Richtlinie

Referenz zu ISO27001

Anforderung	**Referenz ISO27001**
Ein ISMS ist etabliert.	4, 5.1, 5.2
Informationssicherheitsziele sind festgelegt.	6.2
Richtlinie zur Informationssicherheit ist erstellt, veröffentlicht und verteilt.	A.5.1
Das Management muss die Informationssicherheitspolitik, Richtlinien und Verfahren unterstützen.	A.5.4
Mitarbeiter werden über die Risiken beim Umgang mit Informationen und deren Verarbeitung geschult und sensibilisiert.	A.6.3

3 1. Informationen und Rahmenbedingungen zur Richtlinie

3.1 1.1 Allgemeines

Zielsetzung dieser Leitlinie ist die Definition des Zwecks, der Ausrichtung, der Grundlagen und der grundsätzlichen Regeln für das Informationssicherheitsmanagement (ISMS). Die Leitlinie gilt für die dab Gruppe. Diese umfasst die Unternehmen

- dab: Daten – Analysen & Beratung GmbH
- dab: data driven services GmbH.

Die Leitlinie stellt die Umsetzung der gesetzlichen Vorgaben und darüber hinaus die Selbstverpflichtungen der dab zum Datenschutz und zur Informationssicherheit dar. Inhalt und Umsetzung dieser Leitlinie sind integrale Bestandteile der Geschäftspolitik. Die Verlässlichkeit der eingesetzten Produkte und Services sowie eine hohe Sicherheit und Verfügbarkeit der Daten/Informationen sichern die Leistungsfähigkeit und die Wettbewerbsposition des Unternehmens, das Vertrauen der Kunden, Geschäftspartner sowie das Ansehen in der Öffentlichkeit.

Die Einhaltung und Umsetzung der Richtlinie liegt in der Verantwortung der Geschäftsführung. Spezielle Aufgaben in diesem Zusammenhang werden von der Geschäftsführung delegiert (siehe Kapitel 3). Die Geschäftsführung stellt sicher, dass sie von allen Mitarbeitern, Partner und ggf. weiteren Personen oder Einrichtungen, d.h. allen interessierten Parteien in geeigneter Weise zur Kenntnis gegeben wird.

Die **dab: Daten – Analysen & Beratung GmbH** entwickelt und vertreibt eigene Software sowie Fremdsoftware. Zudem bietet sie Beratungsdienstleistungen.

Die **dab: data driven services GmbH** konzentriert sich auf die Erbringung von Beratungs- und Dienstleistungen auf der Grundlage der von der dab: Daten-Analysen & Beratung GmbH entwickelten Software.

3.2 1.2 Anwendungsbereich

Die dab hat den Umfang der Zertifizierung spezifiziert und dies wird auf dem ISO27001:2022 Zertifikat wie folgt aufgezeichnet:

„Der Geltungsbereich der ISO 27001-Zertifizierung umfasst die Softwareentwicklung, den Vertrieb eigener Softwareprodukte, den Vertrieb von Fremdsoftware sowie die Erbringung von Beratungsdienstleistungen. Dies beinhaltet alle damit verbundenen Prozesse, Technologien und Personalressourcen. Der Anwendungsbereich erstreckt sich speziell auf den Standort in der Hans-Obser-Straße 12, 94469 Deggendorf, und bezieht sich auf die dortigen Betriebs- und Geschäftsprozesse, IT-Infrastrukturen, Datenverarbeitungssysteme und Sicherheitsmaßnahmen, die direkt mit diesen Aktivitäten in Verbindung stehen.“

Das Zertifikat gilt für den folgenden geographischen Standort:

Hans-Obser-Straße 12, 94469 Deggendorf

3.3 1.3 Kontext der Organisation

Der Kontext der Organisation wird im Mitarbeiterhandbuch beschrieben.

3.4 1.4 Interessierte Parteien und deren Anforderungen

Die Leitlinie zur Informationssicherheit ist Aufforderung und Verpflichtung zu gesetzeskonformen Verhalten und verantwortungsbewusstem Umgang mit der Informations-Infrastruktur dab Gruppe für alle, die diese Infrastruktur nutzen. Sie wird allen Mitarbeitern, Partnern und ggf. weiteren Personen oder Einrichtungen, d.h. allen interessierten Parteien in geeigneter Weise zur Kenntnis gegeben.

Interessierte Parteien der Gruppe sind (ergänzen und nichtzutreffendes löschen):

- Kunden
- Geschäftsführung
- Gesellschafter
- Festangestellte Mitarbeiter
- Freiberufliche Mitarbeiter
- Gesetzgeber
- Behörden
- Vertriebspartner (Bizcon, DataConsulting, RSM)
- Technologiepartner (Diligent, Microsoft minit, ehemals PAF, ABBYY)
- Vertriebssoftwarelieferanten (Diligent)
- Cloud-Softwarelieferanten (Anbieter)
- Sonstige Lieferanten
- Untermieter

Die interessierten Parteien erwarten von der dab Gruppe, dass die Informationssicherheit einen hohen Stellenwert in den Geschäftsprozessen der dab Gruppe hat und gelebt wird.

3.4.1 1.4.1 Kunden

Die Kunden der dab Gruppe stellen vielfältige Anforderungen an die dab Gruppe. Im Vorfeld zu abgeschlossenen Verträgen erwarten sie, dass im Rahmen von NDAs die Vertraulichkeit gewahrt wird. Innerhalb der Kundenbeziehungen erwarten sie die Einhaltung der SLAs sowie den Schutz ihrer Daten in Bezug auf Vertraulichkeit, Verfügbarkeit und Integrität. Zur Nachweisbarkeit, dass Informationssicherheit umfassend umgesetzt und gelebt wird und somit ein wirksames Informationssicherheitsmanagementsystem (ISMS) eingeführt wurde, wird die ISO 27001 Zertifizierung gefordert.

3.4.2 1.4.2 Geschäftsführung

Die Geschäftsführung hat ein vertragliches Interesse daran, dass die ISO 27001 umgesetzt und gelebt wird. Sie ist für die Einhaltung des ISMS verantwortlich.

3.4.3 1.4.3 Gesellschafter

Die Gesellschafter haben ein wirtschaftliches Interesse daran, dass die ISO 27001 umgesetzt und gelebt wird.

3.4.4 1.4.4 Mitarbeiter

Jeder Mitarbeiter ist dafür verantwortlich, dass die Ziele der Informationssicherheit, Vertraulichkeit, Verfügbarkeit und Integrität für alle Werte der dab Gruppe entsprechend den geltenden Richtlinien und Prozessen eingehalten werden und das ISMS aufrechterhalten wird. Bei informationssicherheitsrelevanten Vorgängen ist umgehend der Informationssicherheitsbeauftragte (ISB) zu informieren. Im Rahmen der Arbeitsverträge und ggfs. von vertraglichen Zusätzen, werden die Mitarbeiter auf die Einhaltung der Vertraulichkeit verpflichtet. Gleiches gilt auch für freiberufliche Mitarbeiter.

3.4.4.1 1.4.4.1 Festangestellte Mitarbeiter

3.4.4.2 1.4.4.2 Freiberufliche Mitarbeiter

3.4.5 1.4.5 Partnerunternehmen

Die Partnerunternehmen der dab Gruppe werden vertraglich zur Einhaltung der Vertraulichkeit verpflichtet. Darüber hinaus werden SLAs zur Vereinbarung der Verfügbarkeit geschlossen.

3.4.5.1 1.4.5.1 Vertriebspartner

Vertriebspartner sind Unternehmen, welche Softwareprodukte und Dienstleistungen der dab Gruppe vertreiben. Die Vertriebspartner der dab Gruppe sind daran interessiert, dass die dab Gruppe funktionierende Produkte und Dienstleistungen anbietet, die sie vertreiben können. Die ISO:27001 sorgt für die Sicherheit der verarbeiteten Daten. Die Einhaltung beider normen sichert die Wettbewerbsfähigkeit und bietet einen wirtschaftlichen Vorteil.

3.4.5.2 1.4.5.2 Technologiepartner

Technologiepartner sind Unternehmen, welche die Softwareprodukte der dab Gruppe in die eigenen Lösungen integriert hat. Sie sind daran interessiert, dass ein ISMS im Sinne der ISO:27001 existiert, um Ausfälle der Software zu verhindern. Sowie die gesetzlichen Anforderungen erfüllt und für eine Lösung ohne Datenlecks sorgt. Nicht konforme Produkte i.S.d. Normen können einen negativen Einfluss auf den Ruf und die wirtschaftliche Lage des Technologiepartners haben.

3.4.6 1.4.6 Lieferanten

Mit den Lieferanten der dab Gruppe werden zur Einhaltung der Vertraulichkeit NDAs und ggfs. TOMs zur Beschreibung der technischen und organisatorischen Maßnahmen und damit zur Gewährleistung der Verfügbarkeit, Integrität und Vertraulichkeit in Bezug auf die Verwendung personenbezogener Daten, abgeschlossen.

3.4.6.1 1.4.6.1 Vertriebssoftwarelieferanten

Vertriebssoftwarelieferanten sind Partner, deren Software die dab Gruppe vertreibt. Sie sind daran interessiert, dass die Sicherheit der Software hoch ist, die Verkaufsprozesse gut strukturiert und die Beratungsleistungen professionell sind, um einen sicheren Absatzmarkt zu haben. Ebenso sollen durch ein funktionierendes ISMS Sicherheitslücken vermieden werden, welche zu einem Imageschaden oder Verdienstausfall führen.

3.4.6.2 1.4.6.2 Cloud-Softwarelieferanten

Auch die Cloud-Softwarelieferanten der dab-Gruppe profitieren von einer hohen Sicherheit in allen Prozessen der dab Gruppe sowie einer stetigen Verbesserung dieser. Sie stellen die Arbeitswerkzeuge zur Verfügung und sind daher an einer wachsenden, sicheren Partnerschaft interessiert.

3.4.6.3 1.4.6.3 Sonstige Lieferanten

3.4.7 1.4.8 Gesetzgeber

Mit der Umsetzung des ISMS im Rahmen der ISO 27001 kommt die dab Gruppe der gesetzlichen Verpflichtung nach, die Ziele des Datenschutzes und der Informationssicherheit in Bezug auf Vertraulichkeit, Verfügbarkeit und Integrität zu gewährleisten.

3.4.8 1.4.9 Behörden

Datenschutzverletzungen und Informationssicherheitsvorfälle werden vom DSB einer Prüfung unterzogen. Ggfs. handelt es sich um eine meldepflichtige Datenpanne bei der Aufsichtsbehörde. Jede Datenschutzverletzung und jeder Informationssicherheitsvorfall werden dokumentiert. Erhebliche Informationssicherheitsvorfälle werden dem BSI gemeldet. Neue, untypische Sicherheitsvorfälle und Auffälligkeiten meldet der ISB ggfs. nach Rücksprache mit der Geschäftsführung und dem DSB dem Bundesamt für Sicherheit in der Informationstechnik (BSI).

3.4.9 1.4.10 Untermieter

Der Untermieter der dab Gruppe erwartet eine eindeutige Trennung der Infrastruktur der dab Gruppe von der Infrastruktur des Untermieters, damit seine Daten hinsichtlich Vertraulichkeit, Verfügbarkeit und Integrität geschützt sind.

3.5 1.5 Referenzierte Dokumente

- Richtlinie für Benutzer - Informationssicherheitsbereich - dab: Intranet (dab-europe.com)
- Richtlinie Clear Desk Policy - Informationssicherheitsbereich - dab: Intranet (dab-europe.com)
- Richtlinie Informationssicherheit auf Reisen - Informationssicherheitsbereich - dab: Intranet (dab-europe.com)
- Richtlinie Verhaltenskodex - Informationssicherheitsbereich - dab: Intranet (dab-europe.com)
- Richtlinie zur Zutrittssteuerung - Informationssicherheitsbereich - dab: Intranet (dab-europe.com)
- Richtlinie Klassifizierung von Informationen - Informationssicherheitsbereich - dab: Intranet (dab-europe.com)
- Richtlinie zur Dokumentenentsorgung - Informationssicherheitsbereich - dab: Intranet (dab-europe.com)
- Richtlinie Risiko- und Chancenmanagement - QMS - dab: Intranet (dab-europe.com)
- Cloud Policy - Informationssicherheitsbereich - dab: Intranet (dab-europe.com)
- Konzept zur Schulung & Sensibilisierung der Mitarbeiter - Informationssicherheitsbereich - dab: Intranet (dab-europe.com)
- Richtlinie Business Continuity Management - Informationssicherheitsbereich - dab: Intranet (dab-europe.com)
- Richtlinie für Passwörter - Informationssicherheitsbereich - dab: Intranet (dab-europe.com)
- Richtlinie für Sicherheitsprüfung und Abnahme in Entwicklung sowie Trennung von Entwicklung, Prüf und Produktionsumgebung - Informationssicherheitsbereich - dab: Intranet (dab-europe.com)
- Richtlinie Informationssicherheitsvorfälle - Informationssicherheitsbereich - dab: Intranet (dab-europe.com)
- Richtlinie Softwareentwicklung - Informationssicherheitsbereich - dab: Intranet (dab-europe.com)
- Richtlinie Sicherheit in der Softwareentwicklung - Informationssicherheitsbereich - dab: Intranet (dab-europe.com)
- Richtlinie zum Umgang mit Risiken der Übermittlung personenbezogener Daten in unsichere Drittländer - Informationssicherheitsbereich - dab: Intranet (dab-europe.com)
- Richtlinie zur Informationssicherheit in externen Kundenprojekten - Informationssicherheitsbereich - dab: Intranet (dab-europe.com)
- Verfahrensanweisung Pascom - Informationssicherheitsbereich - dab: Intranet (dab-europe.com)
- Verfahrensanweisung Softwarebeschaffung - Informationssicherheitsbereich - dab: Intranet (dab-europe.com)

3.6 1.6 Kommunikation, Überprüfung und Verbesserung

Die Leitlinie muss allen betroffenen Mitarbeitern gegenüber kommuniziert werden. Dies erfolgt durch eine Veröffentlichung in Confluence unter Leitlinie Informationssicherheit - Informationssicherheitsbereich - dab: Intranet (dab-europe.com) (see page 4)

Zusätzlich wird die Leitlinie Informationssicherheit in dem Slack Channel dab_info angepinnt.

Das Erreichen und die Verbesserung des angestrebten Informationssicherheits- und Datenschutzniveaus werden durch eine kontinuierliche Revision der Regelungen und Überprüfung von deren Einhaltung sichergestellt. Die Leitlinie zur Informationssicherheit wird einmal jährlich auf ihre Aktualität und Wirksamkeit

hin überprüft und gegebenenfalls angepasst. Im Besonderen wird die Leitlinie anlassbezogen, z.B. bei Änderungen der Bedrohungslage aufgrund aktueller Ereignisse oder der Einführung neuer Technologien bei der dab Gruppe überprüft und angepasst.

Für den Aufbau, die Umsetzung und die kontinuierliche Verbesserung des ISMS, wird der **PDCA-Zyklus** verfolgt:

- Plan (Planung und Konzeption des ISMS)
- Do (Umsetzung und Betrieb)
- Check (Überwachung und Kontrolle)
- Act (Kontinuierliche Verbesserung).

Zur Bewertung des ISMS, stellt der ISB entsprechende Kennzahlen auf, welche regelmäßig erhoben werden. Mit Hilfe von regelmäßigen Reports an das Management und der jährlich durchzuführenden Managementbewertung, wird ein stabiles Berichtswesen aufgebaut, welches das ISMS sicherstellt und auf interne und externe Audits vorbereitet.

4 2. Grundsätze Informationssicherheit

4.1 2.1 Abgrenzung Informationssicherheit - Datenschutz

Informationssicherheit ist eine grundlegende Voraussetzung für ein effektives Datenschutz-Management im Unternehmen. Sie umfasst neben der Sicherheit von IT-Systemen und aller darin gespeicherten und damit verarbeiteten Daten auch die Sicherheit von nicht-elektronisch verarbeiteten Informationen und von nicht personenbezogenen Daten. Ein wesentlicher Bestandteil der Informationssicherheit und des Datenschutzes ist die Datensicherheit.

Sie verfolgt das Ziel, im Prozess der Datenverarbeitung die Daten vor Verlust, Zerstörung, Verfälschung, unbefugter Kenntnisnahme und unberechtigter Verarbeitung zu schützen. Durch den sicheren Umgang mit Informationen und den Schutz der Systeme und Anwendungen werden die relevanten gesetzlichen und regulatorischen Anforderungen erfüllt, Werte (Assets) im Unternehmen geschützt und letztendlich Geschäftsrisiken minimiert.

Im Gegensatz dazu geht es beim Datenschutz darum, den Umgang mit personenbezogenen Daten zu regeln und die Einhaltung der gesetzlichen Anforderungen, insbesondere das Recht auf „informationelle Selbstbestimmung“, sicherzustellen. Die für die Verarbeitung Verantwortlichen müssen Risiken für die Rechte und Freiheiten natürlicher Personen, die die Verarbeitung personenbezogener Daten mit sich bringt, bewerten und durch geeignete Maßnahmen managen.

4.2 2.2 Informationssicherheitsziele

Das übergeordnete Ziel der Informationssicherheit ist, einen anhaltenden geschäftlichen Erfolg und einen kontinuierlichen Geschäftsbetrieb sicherzustellen. Daher erfolgt die Sicherstellung der Informationssicherheit im ureigenen Interesse der dab Gruppe, aber auch im Sinne der Kunden, Mitarbeiter und Geschäftspartner.

Um Beeinträchtigungen der Informationssicherheit zu minimieren ist das Management von angemessenen Sicherheitsmaßnahmen unter Berücksichtigung einer großen Bandbreite von Bedrohungen erforderlich.

- Die dab Gruppe schützt ihre eigene Arbeitsfähigkeit, Vertrauenswürdigkeit und Zuverlässigkeit.
- Die dab Gruppe schützt die Vertraulichkeit der verarbeiteten und gespeicherten Informationen der Kunden, Geschäftspartner und Mitarbeiter.
- Die dab Gruppe schützt vertrauliche Informationen wie z.B. Geschäftsprozesse, Vertragsdaten oder sonstige Geschäftsgeheimnisse.
- Die dab Gruppe gewährleistet die Verfügbarkeit ihrer IT-Systeme, Programme und Informationen.
- Die dab Gruppe schützt die Integrität ihrer IT-Systeme, Programme und Informationen.
- Die dab Gruppe schützt ihre Reputation, um mit Kunden, Geschäftspartnern und Mitarbeitern weiterhin erfolgreich zusammenzuarbeiten.
- Die dab Gruppe verhindert Missbrauch, zweckwidrige Nutzung und Nutzung durch Unbefugte ihrer IT-Systeme, Programme und Informationen.

Das Schutzziel **Vertraulichkeit** stellt sicher, dass bestimmt Informationen wie z.B. geschäftskritische Informationen und Know-How aber auch personenbezogene Daten der Mitarbeiter, Kunden und Partner nur durch berechtigte Personen, Instanzen oder Prozesse eingesehen werden können. Das Schutzziel **Integrität** sorgt für vollständige und unversehrte Daten (korrekt, unveränderbar oder unleugbar geloggt), Daten tragende Systeme und Daten verarbeitende Prozesse. Das Schutzziel **Verfügbarkeit** garantiert berechtigten Nutzern den Zugriff auf Informationen und Daten tragende Systeme zu dem jeweils erforderlichen Zeitpunkt. Das heißt zusammengefasst, dass alle Geschäftsdaten und Systeme zum erforderlichen Zeitpunkt, ausschließlich den berechtigten Nutzern vollständig und unbeschädigt und unverändert zur Verfügung stehen.

Informationssicherheitsziele werden bei Bedarf durch die Geschäftsführung angepasst, z.B. im Rahmen oder nach der jährlichen Managementbewertung des ISMS.

Weitere Grundsätze können sein:

- Einhaltung gesetzlicher / regulatorischer Anforderungen
- Standards und Regeln
- Schutz vor Angriffen und Notfällen
- Gewährleistung der Wirtschaftlichkeit.

4.2.1 2.2.1 Informationssicherheit ist integraler Bestandteil unseres Handelns

Informationssicherheit ist integraler Bestandteil und Voraussetzung für den Geschäftsbetrieb. Alle unternehmenseigenen und anvertrauten Informationen, vor allem personenbezogene Daten, sowie Ressourcen werden gegenüber unbefugten vorsätzlichen oder versehentlichen Zugriffen und Veränderungen geschützt.

Als schützenswerte Grundwerte werden die unter 2.2 erläuterten Schutzziele **Vertraulichkeit**, **Verfügbarkeit** sowie **Integrität** der Informationen definiert. Dies gilt sowohl auf den eigenen Systemen als auch auf den Systemen, die im Auftrag des Unternehmens von Dritten bzw. Dienstleistern betrieben werden. Darüber hinaus verantwortet jeder Mitarbeiter die Sicherheit der Information, welche er in seinem Geschäftsprozess nutzt, z.B. beim Umgang mit übermittelten Dokumenten oder Druckstücken.

Dabei erfolgt die Umsetzung der Informationssicherheit risikoorientiert mit geeigneten, nutzerfreundlichen Maßnahmen auf dem Stand der Technik unter Berücksichtigung der Kosteneffizienz. Durch den sicheren Umgang mit Informationen und dem Schutz unserer Systeme und Anwendungen werden die relevanten gesetzlichen und regulatorischen Anforderungen erfüllt, Risiken minimiert und wirtschaftliche Schäden vermieden.

4.2.2 2.2.2 Informationssicherheit ist immer Up to Date

In einer Zeit sich ständig verändernder Bedrohungen (z.B. Angriffe von außen) ist Aktualität eine wesentliche Voraussetzung für Informationssicherheit. Dies gilt sowohl für die Kenntnisse über Bedrohungen und Risiken als auch für die informationsverarbeitenden Prozesse und Ressourcen.

Nur über eine frühzeitige Identifizierung neuer Bedrohungen können die Risiken für das Unternehmen beurteilt werden [Richtlinie Risikomanagement] sowie eine zeitnahe und angemessene Reaktion erfolgen. Ein ausreichender und angemessener Schutz (Widerstandsfähigkeit / Resilienz) vor Angriffen und Notfällen ist

zu gewährleisten. Um im Notfall adäquat reagieren zu können, sind geeignete Notfall- und Wiederanlaufpläne zu entwickeln, zu testen und regelmäßig zu aktualisieren.

Damit der Schutz zielgerichtet erfolgen kann, werden die wesentlichen Werte (Assets) im Unternehmen identifiziert und durch ein angemessenes Berechtigungs- und Zugriffsmanagement Richtlinie Identity und Access Management - Informationssicherheitsbereich - dab: Intranet (dab-europe.com) - verbunden mit entsprechenden technischen und organisatorischen Maßnahmen auf dem Stand der Technik - geschützt. Dabei wird ganzheitlich der gesamte „Lebenszyklus“ der Information an allen Nutzungsorten betrachtet.

Durch kontinuierliche Awareness-Maßnahmen zur Informationssicherheit werden alle Mitarbeiter geschult und sind damit auch gegenüber neuen Bedrohungen sensibilisiert.

4.2.3 2.2.3 Need-to-know-Prinzip

Informationen werden sicher und unverfälscht ausschließlich den Berechtigten zur Verfügung gestellt. Hierbei wird konsequent eine restriktive Rechtevergabe nach dem Need-to-know-Prinzip angewandt: Benutzern (Mitarbeiter oder Technik) werden ausschließlich die zur Ausführung der (fachlichen) Aufgabe erforderlichen Berechtigungen und Zugriffsrechte erteilt.

4.2.4 2.2.4 Sichere Kommunikation auf allen Wegen mit allen Partnern

In den letzten Jahren hat mobile Kommunikation vermehrt Einzug in den Geschäftsbetrieb gehalten. Aufgrund von Art und Umfang der anfallenden Daten können dabei vielfältige Bedrohungen und Risiken entstehen. Aber auch die Komplexität – verursacht durch eine Vielzahl von installierten Applikationen und zahlreichen Ökosystemen - bildet einen entscheidenden Einflussfaktor für die potenzielle Bedrohungslage. Für eine vertrauenswürdige Kommunikation spielt Informationssicherheit deshalb eine große Rolle.

Das von uns angestrebte Sicherheitsniveau auf dem jeweiligen Stand der Technik wird dabei konsequent auf allen Kommunikationswegen umgesetzt. Dies gilt sowohl für die Kommunikation nach „außen“, z.B. mit Kunden und (Geschäfts-)Partnern, als auch für den Informationsfluss innerhalb der dab Gruppe verantwortlich dafür sind alle Führungskräfte und Mitarbeiter, insbesondere bei technischen Anwendungen der jeweilige Eigentümer.

5 3. Verantwortung und Rollen

Für die Durchsetzung der Regeln der Informationssicherheit und zur Einhaltung des Datenschutzes ist die Geschäftsführung verantwortlich. Sie stellt dazu die notwendigen finanziellen und personellen Ressourcen bereit. Die Geschäftsführung ist dafür verantwortlich, die Beschäftigten entsprechend ihren Aufgaben und Verantwortlichkeiten zu Themen des Datenschutzes und der Informationssicherheit zu sensibilisieren und zu befähigen.

Es wird ein Datenschutzbeauftragter bestellt, dem die Erfüllung der gesetzlich zugewiesenen Aufgaben obliegt. Zur Umsetzung eines Informationssicherheitsmanagements wird ein Informationssicherheits-beauftragter bestellt. Die Geschäftsführung unterstützt die ständige Verbesserung des Sicherheitsniveaus.

5.1 3.1 Verantwortung Führungskräfte

Führungskräfte sind in ihren Zuständigkeitsbereichen verantwortlich für die Implementierung von Informationssicherheitsmaßnahmen und -verfahren sowie deren Einhaltung und Überwachung im Sinne eines aktiven Risikomanagements.

Die Mitarbeiter sind über die Ziele und Maßnahmen der Informationssicherheit und des Datenschutzes zu informieren.

Verantwortlicher im Sinne des Datenschutzes ist derjenige, der über die Verarbeitung von personenbezogenen Daten entscheidet.

5.2 3.2 Verantwortung Mitarbeiter

Alle Mitarbeiter müssen durch ihr verantwortungsvolles Handeln die Gesetze, Vorschriften, Richtlinien, Anweisungen und vertraglichen Verpflichtungen bezogen auf den Datenschutz und die Informationssicherheit einhalten. Sie sind verpflichtet, verantwortungsbewusst mit den genutzten IT-Systemen, IT-Anwendungen und Daten/Informationen umzugehen.

5.3 3.3 Informationssicherheitsbeauftrager (ISB)

Das Unternehmen hat die Funktion eines Informationssicherheitsbeauftragten (ISB) eingerichtet. Zweck der Funktion ist die Steuerung und Weiterentwicklung des Informationssicherheits-Managements (ISMS). Die Funktion umfasst die Wahrnehmung aller Belange der Informationssicherheit innerhalb des Unternehmens und gegenüber Dritten. Sie stellt sicher, dass die in der Strategie sowie in der Informationssicherheitsleitlinie des Unternehmens niedergelegten Ziele und Maßnahmen hinsichtlich der Informationssicherheit sowohl intern als auch bei Bedarf gegenüber Dritten transparent gemacht und deren Einhaltung überprüft und überwacht werden.

5.4 3.4 Datenschutzbeauftragter(DSB)

Der Datenschutzbeauftragte ist das innerbetriebliche Kontrollorgan in allen Datenschutzfragen. Er wirkt auf die Einhaltung der datenschutzrechtlichen Vorschriften hin. Darüber hinaus unterstützt er die Leitung des Unternehmens sowie die Mitarbeiter bei der Identifikation von datenschutzrechtlichen Belangen sowie der Planung und Umsetzung von Maßnahmen zum Datenschutz.

5.5 3.5 Weitere Rollen im Umfeld Datenschutz und Informationssicherheit

Die folgenden Rollen sind für ein funktionierendes Datenschutz- und Informationssicherheits-Management wichtig und arbeiten eng mit den dortigen Funktionen zusammen. Die Beschreibung dieser Rollen ist in dieser Leitlinie auf, die im Zusammenhang mit dem Datenschutz und der Informationssicherheit zu erledigenden Aufgaben beschränkt. Weiterführende Informationen sind in den jeweiligen Richtlinien zu finden.

5.5.1 3.5.1 Informationsrisikomanagement

Das Informationsrisikomanagement ist u.a. für die Feststellung und Analyse, Bewertung, Dokumentation und Steuerung von Informations-Risiken verantwortlich [Richtlinie Risikomanagement]. Die Erfüllung dieser Aufgabe erfordert die regelmäßige Abstimmung zwischen dem Informations-Risikomanagement-Manager, dem Informationssicherheitsbeauftragten und dem Datenschutzbeauftragten.

5.5.2 3.5.2 Governance

Als wesentlicher Bestandteil der Unternehmensführung schafft die Governance die Voraussetzungen und einen Ordnungsrahmen für eine optimale Unterstützung der Unternehmensziele durch die Informationstechnologie (IT). Die Governance sorgt für definierte und verbindliche Prozess-, Organisations- und Führungsstrukturen. Sie stellt sicher, dass die IT einen transparenten und messbaren Beitrag zur Unternehmensstrategie und den Unternehmenszielen leistet. Governance sorgt dafür, dass die vorhandenen Ressourcen verantwortungsvoll eingesetzt sowie Risiken angemessen überwacht und gesteuert werden.

Die Informationstechnologie (Anwendungen und Infrastrukturen) soll die Geschäftsziele des Unternehmens optimal unterstützen. Ihr kommt eine Schlüsselrolle für den Geschäftserfolg zu.

Governance sorgt für die synchrone Entwicklung (Alignment) der Geschäftsstrategie mit der IT-Strategie. Sie stellt sicher, dass die IT-Zielbilder aus der Unternehmensstrategie abgeleitet werden. Der IT-Strategie-Prozess sorgt dafür, dass die Überprüfung und ggf. Anpassung der IT-Strategie jährlich erfolgt, um Veränderung aktiv und nachhaltig zu steuern.

5.5.3 3.5.3 Compliance

Der Compliance Officer (CO) berät die Geschäftsführung bei der Steuerung der Compliance-Organisation im gesamten Unternehmen. Der CO ist zentraler Ansprechpartner für Compliance-Themen, sowohl für intern als auch nach extern. Er steuert und koordiniert den Compliance-Prozess und wirkt damit an allen

zusammenhängenden Aufgaben, insbesondere bei Aufbau bzw. Fortführung einer Compliance-Organisation, angelehnt an das Prinzip eines Compliance Management System mit den drei Säulen: Prävention, Kontrolle und Reaktion.

5.5.4 3.5.4 Informationssicherheits-Managementsystem (ISMS)

Das ISMS folgt der Leitlinie Informationssicherheit, der Strategie und den Compliance-Vorgaben und setzt diese im verantworteten IT-Umfeld um. Zudem spezifiziert und erweitert das ISMS die unternehmensweiten Vorgaben um die für das Unternehmen erforderlichen, IT-spezifischen Richtlinien, Vorgaben, Methoden und Kontrollmechanismen. Das Informations-Sicherheitsmanagement stellt sicher, dass alle als schützenswert definierten Werte wie Informationen, Daten, IT-Services, Applikationen, Infrastruktur usw. im verantworteten IT-Umfeld entsprechend ihrem unternehmensspezifischen Schutzbedarf an Vertraulichkeit, Integrität und Verfügbarkeit geschützt und entsprechend behandelt werden. Ferner schließt das IT-Sicherheitsmanagement aktuelle Sicherheitslücken, analysiert Sicherheitsvorfälle und entwickelt die Sicherheitsstrategie zur Abwehr von Cyber-Angriffen weiter. Die Erfüllung dieser Aufgaben erfordert die regelmäßige Abstimmung mit dem Informationssicherheitsbeauftragten.

5.5.5 3.5.5 IT-Verantwortliche

Der IT-Verantwortliche trägt die End-to-End-Verantwortung für die Umsetzung (Start, Betrieb, Wartung und Support) der IT-Services gemäß den vereinbarten SLAs. Er stellt sicher, dass die Sicherheitsanforderungen eingehalten werden, insbesondere die Einhaltung der relevanten Gesetze und Richtlinien, der Zugriff auf die IT-Services (Konzept, Erteilen/Entzug von Berechtigungen), das Festlegen des erforderlichen Sicherheits- und Kontrollumfanges incl. der Einhaltung und Kontrollen sowie das Festlegen des Schutzbedarfes anhand der Schutzwürdigkeit in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit. Ferner ist er für die Erstellung, Aktualisierung und den Test eines Wiederanlaufplans für den IT-Service, die Gestaltung und Entwicklung des IT-Service (Servicedesign), Bereitstellung und Weiterentwicklung des IT-Service (Servicebetrieb) sowie die Steuerung des IT-Service (Planung, Preisgestaltung, Controlling & Reporting sowie kontinuierliche Verbesserung) zuständig.

5.5.6 3.5.6 Krisenstab

Der Krisenstab ist ein Gremium, das im Falle einer Krise eine befristete Funktion übernimmt und während der Krise Weisungsbefugnis gegenüber den Fachabteilungen hat. Seine Aufgaben sind:

- Ausrufung bzw. Beendigung der Krise
- Übernahme von befristeten Funktionen mit Weisungsbefugnis gegenüber den Fachabteilungen wie z. B. Überstunden- und Mehrarbeitsregelungen in Kraft setzen
- Entscheidung über die Anwendung der Verfahren aus dem Notfallhandbuch oder über die Anwendung der Verfahren, die für die Aktivierung der Fallback-Systeme erforderlich sind

Die hierzu erforderlichen Regelungen sind schriftlich im Notfallhandbuch festgehalten und von der Geschäftsführung autorisiert. Die genaue Zusammensetzung des Krisenstabs bezüglich beteiligter Rollen und Mitarbeiter (Rollenausführende nebst Vertretern) wird im Notfallhandbuch festgelegt.

5.6 3.6 Sicherheitsüberprüfung für Rollen mit entsprechender Kritikalität

In Bezug auf Positionen mit erheblicher Kritikalität müssen Hintergrundchecks im Rahmen des Datenschutzrechts stattfinden.

Diese zusätzliche Sicherheitsmaßnahme trägt dazu bei, potenzielle Risiken weiter zu minimieren und die Vertraulichkeit sowie Integrität unserer Informationssysteme zu stärken.

6 4. Verstöße

Bei einem Verstoß gegen diese Leitlinie ist der betreffende Mitarbeiter auf diesen Verstoß hinzuweisen und die Führungskraft des Mitarbeiters zu informieren. Ein Verstoß kann zu arbeits-, zivil- und gegebenenfalls strafrechtlichen Konsequenzen führen.

7 5. Verpflichtungserklärung

Sie als Benutzer der Informations-Infrastruktur der dab Gruppe bestätigen die Kenntnisnahme der vorstehenden Regelungen, verpflichten sich zu deren Einhaltung und bestätigen durch die nachfolgende Unterschrift oder Bestätigung in HR-Works den Erhalt dieses Dokumentes in schriftlicher oder digital Fassung, der in der digitalen Personalakte aufbewahrt wird.

Ferner sind Sie als Nutzer verpflichtet, sich in regelmäßigen Abständen über das ISMS zu informieren. Die Dokumentation des ISMS ist verfügbar unter dab Gruppe

_____

Name des Mitarbeiters

_____ _____

Datum Unterschrift des Mitarbeiters

Richtlinie für Benutzer

Informationssicherheitsbereich

Exported on 12/15/2023

Table of Contents

1 Inhaltsverzeichnis 3
2 Informationen zum Dokument 4
2.1 Freigegebene Version 4
3 2. Zielsetzung, Geltungsbereich, Zuständigkeit 5
4 2. Inhalt 6
4.1 2.1 Ansprechpartner für Informationssicherheit 6
4.2 2.2 Untersagte Aktivitäten 6
4.3 2.3 Sanktionsmaßnahmen 7
4.4 2.4 Verantwortlichkeiten der Benutzer 7
4.5 2.5 Umgang mit sensible Informationen 7
4.5.1 2.5.1 Verwendung von Besprechungsräumen und Schutz vertraulicher Informationen 8
4.6 2.6 Mobiles Arbeiten 9
4.7 2.7 Besucherprozess 9
4.8 2.7.1 Besucheranmeldung 9
4.9 2.7.2 Besucherformular 10
4.10 2.7.3 Verwaltung der Besucherformulare 10
4.11 2.7.4 Paketanlieferung durch Postdienste 10
4.12 2.7.5 Lieferanten des täglichen Bedarfs 10
4.13 2.8 Sensible Bereiche 10
4.14 2.9 Zusatz IT-Mitarbeiter 10
4.15 2.10 Anlaufstelle für Meldung von IT-Verdachtsfällen 11
5 3. Verantwortlichkeiten 12
6 4. Verpflichtungserklärung 13
7 Historie dieses Dokumentes 14
7.1 Freigabehistorie 14
7.2 Versionshistorie 17

1 Inhaltsverzeichnis

2 Informationen zum Dokument

2.1 Freigegebene Version

Freigegebene Version	12
Datum der Freigegebenen Version	17.11.2023
Freigabe erteilt durch	ext_mwinterstetter
Klassifikation	öffentlich
Dokumentenart	b) Richtlinie

Referenz zu ISO27001

Anforderung	**Referenz ISO27001:2022**
Ein ISMS ist etabliert.	4, 5.1, 5.2
Mitarbeiter werden über die Risiken beim Umgang mit Informationen und deren Verarbeitung geschult und sensibilisiert.	7.2. A.1 8.1; 8.7: 8.22

3 2. Zielsetzung, Geltungsbereich, Zuständigkeit

Diese Richtlinie gibt einen kompakten Überblick über die Regeln, die Benutzer im Sinne einer unternehmensweiten Informationssicherheit einhalten müssen.

Informationssicherheit ist kein rein technisches Unterfangen darstellt, sind einige Regeln und Richtlinien zu beachten, die das Unternehmen beim Erreichen dieser Ziele unterstützen. Dabei sind die Hilfe und Aufmerksamkeit aller Mitarbeiter erforderlich.

Diese Richtlinie gilt mit ihrer Veröffentlichung für alle Mitarbeiter.

Die Richtlinie wird jährlich und anlassbezogen durch den Informationssicherheitsbeauftragten (ISB) geprüft und falls erforderlich angepasst. Änderungen werden mit der Veröffentlichung gültig.

4 2. Inhalt

Unser Unternehmen ist auf IT-gestützte Prozesse angewiesen. Daher ist es auch im Sinne der Geschäftspolitik notwendig ein hohes Niveau an Informationssicherheit zu gewährleisten. Das heißt die Verfügbarkeit, Integrität und Vertraulichkeit der Systeme und Daten ist sicherzustellen.

Ein wesentlicher Bestandteil unserer Sicherheit stellt das Verhalten und Wissen jedes Mitarbeiters um Informationssicherheit im Unternehmen dar.

Daher führen wir regelmäßig (i.d.R. jährlich) Awareness Trainings für den Bereich Informationssicherheit und Datenschutz durch.

Weitere Informationen sind den jeweils veröffentlichen Richtlinien und Arbeitsanweisungen zu entnehmen. Diese Richtlinie gibt einen Überblick.

4.1 2.1 Ansprechpartner für Informationssicherheit

Die dab Gruppe hat die Funktion eines Informationssicherheitsbeauftragten (ISB) extern mit Herrn Markus Winterstetter von aigner business solutions GmbH besetzt. Zweck der Funktion ist die Steuerung und Weiterentwicklung des Informationssicherheits-Managements. Die Funktion umfasst die Wahrnehmung aller Belange der Informationssicherheit innerhalb des Unternehmens und gegenüber Dritten. Sie stellt sicher, dass die in der Leitlinie für Informationssicherheit der dab Gruppe niedergelegten Ziele und Maßnahmen hinsichtlich der Informationssicherheit sowohl intern als auch – sofern und soweit geboten – gegenüber Dritten transparent gemacht und deren Einhaltung überprüft und überwacht werden.

Bei Fragen zur Informationssicherheit wenden Sie sich bitte an Herrn Winterstetter, unseren ISB.

Im Falle von Abwesenheit wird Herr Winterstetter vertreten durch Herrn Jörg Sondermann von aigner business solutions GmbH.

Meldungen zu Informationssicherheit gehen an markus.winterstetter@aigner-business-solutions.com

Im Vertretungsfalle gehen die Meldungen an joerg.sondermann@aigner-business-solutions.com.

Bei verdächtigen Vorfällen, Ereignissen, E-Mails oder Anrufen, auch wenn Sie unsicher sind, wenden Sie sich bitte unverzüglich an den ISB unter Schilderung des Sachverhalts.

Weiteres siehe Richtlinie zum Umgang mit Informationssicherheitsvorfällen.

4.2 2.2 Untersagte Aktivitäten

Folgende Aktivitäten sind untersagt:

- Nutzung privater Endgeräte im betrieblichen Umfeld.
- Private Nutzung des betrieblichen E-Mail-Postfaches.
- Nutzung der privaten E-Mail-Adresse im betrieblichen Umfeld.
- Private Nutzung des betrieblichen Internetanschlusses. Eine Ausnahme besteht, wenn die Beschäftigten im Vorfeld dem Arbeitgeber eine Einwilligung gemäß Anlage Nutzungsvereinbarung privater Internetzugang gegeben haben. Dann kann die private Nutzung des betrieblichen

Internetzugangs in geringfügigem Umfang in den Pausen sowie vor und nach der Arbeitszeit und maximal für 60 Minuten pro Tag erfolgen.
- Installation und Nutzung von nicht freigegebenen Datenträgern/Applikationen/Apps (Lizenz- und Urheberrecht beachten).
- Entfernen von Datenträgern / Geräten vom Standort ohne Genehmigung.
- Nutzung von WhatsApp für die geschäftliche Kommunikation und Dokumentation.
- Austausch von Kundendaten oder vertraulichen und geheimen Unternehmensinformationen mittels Slack.
- Verstoß gegen die Regelungen zur mobilen Arbeit.

Zur Trennung zwischen betrieblichen und privaten Zwecken, existiert auf dem Diensthandy ein betrieblicher und ein privater Bereich.

4.3 2.3 Sanktionsmaßnahmen

Bei einem Verstoß gegen interne Richtlinien und Arbeitsanweisungen kann dies für den Mitarbeiter zu arbeits-, zivil- und gegebenenfalls strafrechtlichen Konsequenzen führen.

4.4 2.4 Verantwortlichkeiten der Benutzer

Alle Mitarbeiter müssen verantwortungsvoll handeln und die Gesetze, Vorschriften, Richtlinien, Anweisungen und vertraglichen Verpflichtungen bezogen auf den Datenschutz und die Informationssicherheit einhalten. Sie sind verpflichtet, verantwortungsbewusst mit den genutzten IT-Systemen, IT-Anwendungen und Daten/ Informationen umzugehen.

Der Benutzer darf sein Passwort keiner dritten Person mitteilen. Besteht der Verdacht einer missbräuchlichen Nutzung des Benutzerkontos, ist der ISB zu informieren und das Passwort umgehend zu ändern.

Das Passwort muss gemäß der Passwort-Richtlinie vergeben werden.

Wir verfolgen eine Clean Desk Policy, d.h. auf dem Schreibtisch dürfen keine Unterlagen bei Abwesenheit des Benutzers frei zugänglich sein. Weiteres siehe Richtlinie Clean Desk.

Die Nutzung von externen Geräten im Netz erfolgt über den Gast-WLAN-Zugang. Im Gast-WLAN gibt es einen freien Internetzugang.

Im Umgang mit Externen sowie Kommentaren in der Öffentlichkeit - auch auf Social-Media-Kanälen - verhalten wir uns professionell und achten darauf, betriebliche und private Kommentare strikt zu trennen.

Bei neuen Vorhaben oder Projekten sind Datenschutz und Informationssicherheit bereits von Beginn an zu integrieren, um so den Vorgaben der Geschäftsleitung und unserer Informationssicherheitspolitik zu folgen.

4.5 2.5 Umgang mit sensible Informationen

Die Vertraulichkeitsstufe wird auf Basis folgender Kriterien festgelegt:

- Wert der Information – basierend auf den in der Risikoeinschätzung festgestellten Auswirkungen

- Sensibilität und Kritikalität der Information – basierend auf dem für jede Information während der Risikoeinschätzung kalkulierten höchsten Risiko
- Rechtliche und vertragliche Verpflichtungen – basierend auf den gesetzlichen, amtlichen, vertraglichen Verpflichtungen

Beschreibung	**Klassifizierungsstufen**
Die Information ist öffentlich und frei zugänglich. Kein Schaden möglich.	**Öffentlich**
Der potenzielle Schaden ist geringfügig, kurzfristiger Natur und auf eine einzelne Entität begrenzt.	**Intern**
Der potenzielle Schaden ist beträchtlich oder mittelfristiger Natur oder nicht auf eine einzelne Entität begrenzt.	**Vertraulich**
Der potenzielle Schaden ist für das Unternehmen existenzbedrohlich oder langfristiger Natur oder nicht auf eine einzelne Entität begrenzt.	**Geheim**

Die Vertraulichkeitsstufe ist beim jeweiligen Dokument zu erfassen. Details sind der Richtlinie Klassifizierung von Informationen zu entnehmen.

4.5.1 2.5.1 Verwendung von Besprechungsräumen und Schutz vertraulicher Informationen

Besprechungsräume in unserem Unternehmen dienen häufig als Orte für den Austausch von vertraulichen Informationen und sensiblen geschäftlichen Diskussionen. Um die Integrität und Vertraulichkeit dieser Informationen zu gewährleisten, ist es von größter Bedeutung, angemessene Sicherheitsvorkehrungen zu treffen.

Bei der Nutzung von Besprechungsräumen ist sicherzustellen, dass Rollos oder Vorhänge vorhanden sind und diese stets heruntergelassen werden, um sicherzustellen, dass keine unbefugten Personen von außen Einblick in die Räume haben.

Mitarbeiter und Besprechungsteilnehmer sind angehalten, die Rollos oder Vorhänge stets herunterzulassen, wenn vertrauliche Informationen besprochen werden, und sicherzustellen, dass keine Beamer Inhalte, Bildschirme oder Whiteboards von außen sichtbar sind.