

#Firma#

A 7.1

Richtlinie zur physischen Sicherheit

Version	0.9
Autor	#Autor#
Besitzer der Richtlinie	#Besitzer#
Genehmigt von	#Genehmigt#
Datum der Genehmigung	#Datum#
Überprüfung	Jährlich
Status des Dokuments	In Arbeit
Vertraulichkeitsstufe	INTERN
Klassifizierung	Richtlinie (Level 3)
Dokument Kontakt	#Dokumentkontakt#
Anwendbarkeit	Das ISMS gilt für alle Standorte und Abteilungen der #Firma#

Versionshistorie:

Datum	Version	Erstellt von	Beschreibung der Änderung
#Datum#	0.90	Notivia GmbH	Basisstruktur des Dokuments

Dokumentenmitwirkende	Abteilung	Position	Name

Genehmigungsstufe	Rolle	Datum/Version	Name
Steering Committee			
Geschäftsführung			
Management			

Inhalt

Einführung.....	4
Sichere Bereiche.....	4
Sicherheit von Papier und Ausrüstung.....	5
Verwaltung des Lebenszyklus der Ausrüstung.....	6

Einführung

Der Schutz der physischen Umgebung ist eine wichtige Aufgabe im Bereich der Informationssicherheit. Die Vernachlässigung von Maßnahmen zur physischen Zugangskontrolle kann selbst die sorgfältigsten technischen Sicherheitsvorkehrungen zunichte machen.

Diese Richtlinie bezieht sich auf alle Systeme, Personen und Prozesse, die die Informationssysteme der Organisation umfassen. Dazu gehören Vorstandsmitglieder, Direktoren, Mitarbeiter, Lieferanten und andere externe Parteien, die Zugang zu den Systemen von der #Firma# haben.

Die folgenden Richtlinien und Protokolle sind für dieses Dokument von Bedeutung:

- Richtlinien für mobile Geräte

Sichere Bereiche

Die Sicherheit von Informationen erfordert eine sorgfältige Aufbewahrung in Übereinstimmung mit der zugewiesenen Klassifizierung. Um ein optimales Maß an Sicherheit zu erreichen, muss eine umfassende Risikobewertung durchgeführt werden, um die erforderlichen Schutzmaßnahmen zur Sicherung der gespeicherten Informationen zu bestimmen.

Um die physische Sicherheit zu gewährleisten, muss man sich auf das Gebäude selbst konzentrieren und zunächst die Anfälligkeit des Geländes bewerten. Die Prüfung der Sicherheit eines Gebäudes muss auch die Einrichtung von Kontrollmechanismen umfassen, die für die Klassifizierung der untergebrachten Informationen und Geräte geeignet sind.

Folgende Maßnahmen sind ergriffen:

- Aktivierung von Alarmen außerhalb der Betriebszeiten
- Schlösser an notwendigen Stellen
- Fenstergitter in den unteren Etagen
- Ausstattung der zugänglichen Türen mit Zugangskontrollmechanismen (beschränkt auf autorisiertes Personal)
- Implementierung der CCTV-Überwachung
- Bewegungsmelder in Fluren und Sicherheitsbereichen wie HR-Büro
- Einrichtung eines bemannten Empfangsbereichs
- Gegenmaßnahmen gegen mögliche Schäden wie Feuer, Überschwemmung und Vandalismus

Personal, das sich in Sicherheitszonen aufhält, ist verpflichtet, Personen, die sich nicht ordnungsgemäß ausweisen können, zur Rede zu stellen.

Besucher, die die Sicherheitsbereiche betreten, müssen immer in Begleitung von berechtigten Personen sein.

Die Schlüsselverwaltung für Sicherheitsbereiche, in denen sich IT-Geräte und abschließbare IT-Schränke befinden, wird zentral von der internen IT überwacht. Im Falle von Verstößen oder unüblichen Abgängen von Mitarbeitern ist sofortiges Handeln erforderlich. Alle Identifizierungs- und Zugangsinstrumente (Ausweise,

Schlüssel usw.) müssen unverzüglich von dem ausscheidenden Mitarbeiter zurückgefordert werden.

Sicherheit von Papier und Ausrüstung

Nicht-elektronische Informationen, einschließlich papierbasierter Dokumente, erfordern einen zugewiesenen Eigentümer und eine bestimmte Klassifizierung. Um dieses Material zu schützen, müssen geeignete Maßnahmen zur Informationssicherheit ergriffen werden, die sich an den Bestimmungen des Verfahrens zum Umgang mit Assets orientieren.

In offenen Büroumgebungen müssen Papierdokumente durch eine Kombination aus Kontrollen auf Gebäudeebene und spezifischen Sicherheitsmaßnahmen geschützt werden. Zu den praktikablen Ansätzen gehören unter anderem die folgenden:

- Gesicherte Aktenschränke mit getrennt vom Schrank aufbewahrten Schlüsseln
- Verwendung von verschlossenen Tresoren
- Aufbewahrung in einem sicheren Bereich mit Zugangskontrollen

Bei der strategischen Platzierung der allgemeinen Computerausrüstung müssen physische Kriterien beachtet werden:

- Reduzieren Sie die Exposition gegenüber Umweltrisiken wie Hitze, Feuer, Rauch, Wasser, Staub und Vibration
- Verringern Sie das Diebstahlrisiko, indem Sie z. B. Gegenstände wie Laptops bei Bedarf an den Schreibtischen befestigen.
- Positionieren Sie Arbeitsstationen mit sensiblen Daten so, dass Unbefugte sie nicht einsehen können.

Die Datenspeicherung muss in erster Linie auf Netzwerk-Dateiservern oder genehmigten Cloud-Speichern erfolgen, sofern verfügbar. Diese Praxis gewährleistet die Wiederherstellbarkeit und den Erhalt der Integrität im Falle einer Kompromittierung von Informationen durch unerlaubten Zugriff, Verlust oder Beschädigung.

Server, die außerhalb des zentralen Rechenzentrums auf dem Gelände von der #Firma# stehen, müssen sich in einer physisch sicheren Enklave befinden.

Um Unterbrechungen und Datenverluste aufgrund von Stromausfällen zu vermeiden, müssen geschäftskritische Systeme durch unterbrechungsfreie Stromversorgungen (USV) geschützt werden.

Ein umfassendes Inventar, das von der internen IT geführt wird, muss relevante Ausrüstung umfassen. Es müssen Verfahren eingerichtet werden, die eine Aktualisierung des Inventars bei Erhalt oder Veräußerung von Assets gewährleisten. Jedes Gerät sollte eine Sicherheitskennzeichnung tragen und eine eindeutige Asset-Kennung besitzen. Diese Asset-Kennung muss im Inventar der #Firma# ordnungsgemäß dokumentiert werden.

Kabel, die Daten übertragen oder lebenswichtige Informationsdienste unterstützen, müssen gegen Abhören oder Beschädigung abgeschirmt werden (min. Kat 5). Die Verlegung von Netzkabeln durch öffentliche Räume sollte, wann immer möglich, auf Leerrohre beschränkt werden.

Verwaltung des Lebenszyklus der Ausrüstung

Die interne IT ist dafür verantwortlich, dass die IT-Ausrüstung von der #Firma# in Übereinstimmung mit den Anweisungen des Herstellers und allen dokumentierten

internen Protokollen gewartet wird. Diese Sorgfalt ist für die Aufrechterhaltung des optimalen Betriebszustands der Geräte unerlässlich.

Das mit der Wartung beauftragte Personal muss Folgendes tun:

- Bestimmen Sie die empfohlenen Wartungsintervalle und Spezifikationen
- Einrichtung eines reaktionsschnellen Abrufverfahrens für den Fall von Störungen
- Stellen Sie sicher, dass nur autorisierte Techniker Aufgaben im Zusammenhang mit der Ausrüstung übernehmen
- Berücksichtigen von Versicherungsvoraussetzungen
- Relevante Ereignisse sind zu dokumentieren

Die Aufbewahrung der Servicehistorie eines Geräts ist von Bedeutung und erleichtert fundierte Entscheidungen über den Zeitplan für den Austausch. Die Wartungsanweisungen des Herstellers müssen förmlich dokumentiert werden und für das Support-Personal zur Durchführung von Reparaturen leicht zugänglich sein.

Für Geräte, die wiederverwendet oder entsorgt werden sollen, ist eine umfassende Löschung oder Vernichtung aller Daten und Software obligatorisch. In Fällen, in denen die Geräte an eine andere Organisation weitergegeben werden sollen, muss die Datenlöschung mit genehmigten, angemessen sicheren Softwaretools durchgeführt werden, insbesondere wenn die Geräte im Rahmen eines Leasingvertrags zurückgegeben werden sollen.

Ausrüstungslieferungen müssen von einer autorisierten Person durch ein nachvollziehbares formales Verfahren bestätigt werden. Dieses Verfahren muss die Übereinstimmung zwischen den gelieferten Gegenständen und dem auf dem Lieferschein aufgeführten Bestand sicherstellen. Die tatsächlich erhaltenen Assets müssen akribisch aufgezeichnet werden.

Ladebereiche und Lagerräume müssen gegen unbefugtes Betreten gesichert werden, und alle Zugriffe müssen protokolliert werden.

Die anschließende Entfernung der Ausrüstung muss nach einem strukturierten, nachvollziehbaren Verfahren erfolgen.

Die Informationssicherheitsprotokolle unterliegen routinemäßigen, unabhängigen Audits, und alle empfohlenen Sicherheitsverbesserungen werden bei Bedarf ordnungsgemäß umgesetzt.

Aktuelle Situation in den Standorten:

- xxxx
-