

#Firma#

A 7.2

Richtlinie: Physischer Zutritt zu Arbeitsbereichen mit Informationswerten

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

Hintergrund und Zweck.....	4
Geltungsbereich.....	4
Umgesetzte Schutzmaßnahmen im Unternehmen.....	4
Zutrittsregelungen im Detail.....	5
Mitarbeitende.....	5
Gäste und Externe.....	5
Technische Infrastruktur der Zutrittskontrolle.....	6
Schutz des Arbeitsplatzes und sensibler Informationen.....	6
Verantwortung und Kontrolle.....	7
Prüfung und Auditfähigkeit.....	7
Erweiterte Szenarien: Remote Work und Projekträume.....	7

Hintergrund und Zweck

Die Informationssicherheit umfasst nicht nur den Schutz digitaler Systeme, sondern beginnt bereits mit der physischen Kontrolle des Zugangs zu den Orten, an denen Informationen verarbeitet oder gespeichert werden. Das betrifft Arbeitsplätze ebenso wie Serverräume oder technische Infrastruktur.

Ein unbefugter Zutritt zu sensiblen Bereichen kann dazu führen, dass Informationen:

- eingesehen, entwendet oder manipuliert werden (z. B. Dokumente, Hardware, Monitore),
- Systeme sabotiert oder unautorisiert manipuliert werden (z. B. Netzwerke, Server),
- Schutzmaßnahmen umgangen werden (z. B. Firewalls, Zugangskontrollen),
- regulatorische Anforderungen verletzt werden (z. B. DSGVO, ISO-Zertifizierung, Kundenverträge).

Der Schutz des physischen Zugangs ist daher integraler Bestandteil eines ganzheitlichen ISMS. Diese Maßnahme sichert die erste Verteidigungslinie, die darüber entscheidet, ob digitale Sicherheitsmaßnahmen überhaupt greifen können.

Geltungsbereich

Diese Richtlinie betrifft alle physischen Zugänge zu Räumen, Gebäuden und Einrichtungen, in denen Informationen, IT-Systeme oder sicherheitsrelevante Prozesse vorkommen. Dazu zählen:

- Büroräume (auch bei geteilten Flächen, z. B. Coworking)
- Meetingräume mit technischer Infrastruktur
- Technik- und Serverräume
- Archivräume mit Papierunterlagen
- Zutrittsgeschützte Bereiche in IT-Dienstleister- oder Hostingumgebungen (z. B. RZs, Colocations)
- Remote-Arbeitsplätze, sofern dort schützenswerte Informationen verarbeitet werden

Umgesetzte Schutzmaßnahmen im Unternehmen

In der Organisation sind elektronische Zutrittssysteme auf Basis von Dongles (transponderbasiert) im Einsatz. Diese erfüllen folgende Sicherheitsfunktionen:

- Personalisierte Zugangsmittel: Jeder Mitarbeitende erhält einen individuellen Dongle mit eindeutiger ID.
- Zonenbasierte Zutrittsfreigaben: Zugangsrechte sind räumlich differenziert (z. B. Eingang vs. Serverraum).
- Zeitliche Einschränkungen: Bei Bedarf wird der Zugang auf bestimmte Tageszeiten oder Wochentage begrenzt.
- Automatische Protokollierung: Jeder Zutritt (Öffnungsversuch, Erfolg, Fehlversuch) wird in einem zentralen System mit Zeitstempel und Benutzerkennung dokumentiert.

- Zentrale Sperrung: Bei Verlust oder Ausscheiden wird der Dongle sofort deaktiviert.

Diese Lösung erfüllt die Anforderungen an Zugangssteuerung, Revisionsfähigkeit und Reaktionsgeschwindigkeit und stellt damit ein robustes Mittel zur Zutrittssicherheit dar.

Zutrittsregelungen im Detail

Mitarbeitende

- Mitarbeitende erhalten ihren Dongle nach Rollenprüfung und Freigabe durch IT oder Office-Management.
- Die Berechtigungen werden im Zutrittsverzeichnis dokumentiert.
- Zutritt wird ausschließlich zu den für die Tätigkeit relevanten Bereichen gewährt.
- Verlust oder Defekt eines Dongles muss unverzüglich gemeldet werden.
- Beim Austritt aus dem Unternehmen ist die Rückgabe verpflichtend, andernfalls wird der Dongle zentral gesperrt.

Gäste und Externe

- Gäste erhalten nur in Begleitung Zutritt oder auf Basis einer temporären Zutrittsfreigabe mit Einschränkung (z. B. Techniker: Zugang nur zum Serverraum, befristet auf einen Tag).
- Jeder Zutritt von Externen wird im Besucherverzeichnis dokumentiert (Name, Firma, Uhrzeit, verantwortliche Person, Unterschrift Regelungen gesehen und akzeptiert).
- Externe erhalten keinen Zugang zu Büroarbeitsplätzen ohne vorherige Zustimmung und Sicherheitsunterweisung.

Technische Infrastruktur der Zutrittskontrolle

Funktion	Umsetzung
Zugangstechnologie	RFID-/Transponder-basierte Dongles mit individueller Kennung oder Schlüssel
Steuerungseinheit	Zentrale Zutrittsdatenbank mit Nutzer-, Raum- und Zeitprofilen und Schlüsselliste
Protokollierung	Log-System mit Exportfunktion für Audits (Speicherzeitraum: mindestens 6 Monate)
Integration	Verknüpfung mit HR-Austrittsprozess (Personio) und IT-Offboarding
Notfallzugänge	Durch definierte Schlüssel bei Ausfall des Systems – Dokumentation erforderlich

Schutz des Arbeitsplatzes und sensibler Informationen

Auch innerhalb physisch gesicherter Bereiche müssen Informationswerte am Arbeitsplatz geschützt werden:

- Vertrauliche Dokumente werden nicht offen liegen gelassen („Clean Desk Policy“)
- Displays werden wenn nötig mit Sichtschutzfolien versehen
- Arbeitsplätze mit Kundendaten, HR-Themen oder sicherheitsrelevanter Funktion sind besonders zu schützen (z. B. IT-Admin, Projektleitung)
- Papierunterlagen werden außerhalb der Arbeitszeit in abschließbaren Containern oder Schränken aufbewahrt
- Besuchende oder Externe dürfen keine Einsicht in Bildschirme oder Unterlagen erhalten

Verantwortung und Kontrolle

Rolle	Aufgabe
Geschäftsführung	Genehmigung und Kontrolle der Zutrittspolitik
IT-Leitung	Einrichtung, Wartung und Protokollierung des elektronischen Zutrittssystems
Office-Management	Ausgabe und Rücknahme von Zutrittsmedien, Verwaltung Besucherverzeichnis
ISB	Kontrolle der Richtlinienkonformität, Prüfung der Zutrittslogs bei Vorfällen
Mitarbeitende	Einhaltung der Vorgaben, keine Weitergabe von Dongles oder Schlüsseln, sofortige Meldung bei Verlust

Prüfung und Auditfähigkeit

- Zutrittsrechte werden jährlich überprüft (Vergleich der aktuellen Berechtigungen mit der Organisationsstruktur)
- Logs des Zutrittssystems werden bei sicherheitsrelevanten Vorfällen durch ISB/IT ausgewertet
- Auditnachweise: Exportierte Zutrittsprotokolle, Freigabevermerke, Rückgabeprotokolle, Besucherdokumentation
- Die Effektivität der Maßnahmen wird jährlich im Rahmen des ISMS-Reviews bewertet

Erweiterte Szenarien: Remote Work und Projekträume

Auch wenn physische Kontrolle in Remote-Arbeitsumgebungen eingeschränkt ist, gilt:

- Laptops und mobile Geräte müssen bei Abwesenheit gegen physischen Zugriff geschützt werden (z. B. im abschließbaren Fach)
- In geteilten Wohnungen ist sicherzustellen, dass Dritte keine Einsicht in arbeitsbezogene Informationen erhalten
- Kein Arbeiten in öffentlich einsehbaren Bereichen ohne Sichtschutz (Café, Zug, Flughafen etc.) bei Zugriff auf interne Daten