|  |  |
| --- | --- |
| Version: | 1.0 |
| Status: | Freigegeben |
| Dokumentenklassifizierung: | intern |

Standard "physische Sicherheit"

1. Januar 2020

Allgemeine Informationen zum vorliegenden Dokument

|  |  |  |
| --- | --- | --- |
| Bezeichnung | Inhalt | Bearbeitungshinweis |
| Eigentümer |  | [verantwortlich für die Erstellung und Pflege des Dokuments = Abteilungsleitung] |
| Autor |  | [operative Verantwortung für das Dokument] |
| Status | Freigegeben | [Einstufung des aktuellen Dokumentenstatus <Entwurf, Finaler Entwurf, Final/Freigegeben>] |
| Klassifizierung | intern | [Einstufung der Dokumentenvertraulichkeitoffen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS200008 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung (vergeben] |
| Name des Dokuments |  | [Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.] |
| Version  | 1.0 | [zweistellige Versionsnummer] |
| Veröffentlichungsform | digital | [Veröffentlichungsform Papier, digital] |
| Speicherort |  | [Ablageort des Dokumentes] |
| Freigabe am | <TT.MM.YYYY> | [Datum der Freigabe durch den Eigentümer] |
| Freigabe bis | <TT.MM.YYYY> | [Datum der Freigabe bis durch den Eigentümer] |
| Revisionszyklus | Alle zwei Jahre | [Revisionszyklus alle 1, 2 Jahre] |
| Archivierungszeitraum | 10 Jahre | [Archivierungszeitraum nach Ablauf 5, 10 Jahre] |

# Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Beschreibung | Autor | Datum |
| 0.1 | initiale Erstellung |  |  |
| 0.2 – 0.8 | draft |  |  |
| 0.9 | final draft |  |  |
| 1.0 | final/freigegeben |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhaltsverzeichnis

[Allgemeine Informationen zum vorliegenden Dokument 2](#_Toc75592802)

[Dokumentenhistorie 3](#_Toc75592803)

[Inhaltsverzeichnis 4](#_Toc75592804)

[Allgemeine Festlegungen 6](#_Toc75592805)

[Ziel / Zweck 6](#_Toc75592806)

[Geltungsbereich 6](#_Toc75592807)

[Zuständigkeiten 6](#_Toc75592808)

[Genehmigungs- und Änderungsverfahren 7](#_Toc75592809)

[Standard physische Sicherheit 7](#_Toc75592810)

[Physische Sicherheit 7](#_Toc75592811)

[Gebäudeauswahl 7](#_Toc75592812)

[Sicherheitszonen eines Gebäudes 7](#_Toc75592813)

[Sicherheitszone 0 (Farbcodierung - weiß) 8](#_Toc75592814)

[Sicherheitszone 1 (Farbcodierung - grau) 8](#_Toc75592815)

[Sicherheitszone 2 (Farbcodierung - grün) 8](#_Toc75592816)

[Sicherheitszone 3 (Farbcodierung - orange) 8](#_Toc75592817)

[Sicherheitszone 4 (Farbcodierung - rot) 9](#_Toc75592818)

[Anforderungen an die Gebäude und Räumlichkeiten 9](#_Toc75592819)

[Gebäudesicherung 10](#_Toc75592820)

[Einhaltung der übergeordneten Richtlinien 10](#_Toc75592821)

[Perimeterschutz 10](#_Toc75592822)

[Schutz vor Wassergefährdungen 10](#_Toc75592823)

[Schutz der Fenster und Türen 11](#_Toc75592824)

[Gewährleistung des Brandschutzes 11](#_Toc75592825)

[Brand-Sicherheitszonen 11](#_Toc75592826)

[Brandmeldeanlagen 12](#_Toc75592827)

[Geräte 12](#_Toc75592828)

[Übungen 12](#_Toc75592829)

[Installation von Löschsystemen 12](#_Toc75592830)

[Umsetzung des Zutrittsschutzes 12](#_Toc75592831)

[Allgemeine Zutrittsbestimmungen 12](#_Toc75592832)

[Zutritt zum Gebäude 12](#_Toc75592833)

[Zutritt zwischen den Sicherheitszonen 13](#_Toc75592834)

[Verwaltung von Zutrittsberechtigungen 13](#_Toc75592835)

[Zentrale Zutrittskontrollsysteme 13](#_Toc75592836)

[Klimatisierung 14](#_Toc75592837)

[Vorgaben für die Aufstellung von IT-Systemen 14](#_Toc75592838)

[Vorgaben für Serverräume 14](#_Toc75592839)

[Vorgaben für IT-Schränke 16](#_Toc75592840)

[Stromversorgung 16](#_Toc75592841)

[Stromeinspeisung 16](#_Toc75592842)

[Vorgaben für USV und Notstromversorgung 17](#_Toc75592843)

[Blitz- und Überspannungsschutz 17](#_Toc75592844)

[Versorgung mit Netzdiensten und Telekommunikation 18](#_Toc75592845)

[Fernanzeige von Störungen 18](#_Toc75592846)

[Schutz bei der Gebäudereinigung 18](#_Toc75592847)

[Ausnahmeregelungen 18](#_Toc75592848)

# Allgemeine Festlegungen

## Ziel / Zweck

Dieser Standard beschreibt die Schutzmaßnahmen zur betrieblichen und umgebungsbezogenen Sicherheit. Es sollen einheitliche Maßstäbe der physischen und organisatorischen Sicherheit für die Gebäude der <Institution> festgelegt werden.

Der Standard für physische Sicherheit umfasst insbesondere die Anforderungen an den kontrollierten Zutritt zu Einrichtungen sowie die Zuständigkeit, Organisation und Verfahrensweise für die Erteilung von Zutrittsrechten.

Die Vorgaben des Dokuments haben zum Ziel, den unautorisierten Zutritt, Zugriff sowie Zugang zu verhindern und daraus resultierend die Sicherheit von Personen als auch den Schutz von Informationen vor Diebstahl, Zerstörung sowie Verfälschung und sonstigen Missbrauch zu gewährleisten.

## Geltungsbereich

Die Vorgaben des Dokumentes sind für alle Prozessverantwortlichen der <Institution> verbindlich und entsprechend durch die zuständigen Rollenträger umzusetzen.

Anzuwenden sind die Vorgaben für alle durch die <Institution> verantworteten Geschäftsprozesse, Hard- und Softwarekomponenten sowie ihren Konfigurationen. Die Umsetzung dieser Arbeitsanweisung ist durch die entsprechenden Führungskräfte sicherzustellen.

Die im Folgenden beschriebenen Vorgaben sind hingegen nicht bindend für Prozessverantwortliche von Geschäftsprozessen, die nicht durch die <Institution> wahrgenommen werden. In diesen Fällen besitzen die beschriebenen Vorgaben einen empfehlenden Charakter, auf eine Einhaltung muss durch die <Institution> hingewirkt werden.

Interne Regelungen sind geschlechterneutral zu formulieren. Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche personenbezogenen Bezeichnungen in männlicher Form werden verallgemeinernd verwendet und beziehen sich stets auf alle Geschlechter.

## Zuständigkeiten

Zuständig für die Einhaltung der in diesem Dokument aufgeführten Pflichten und Anforderungen sind:

* Eigene Mitarbeitende und beauftragte Dienstleister, welche administrative Arbeiten an IT- Systemen und Anwendungen von der <Institution> durchführen,
* Eigene Mitarbeitende und beauftragte Dienstleister, welche Applikationsbetreuung mit administrativem Charakter (z. B. Versionspflege, Benutzerverwaltung) betreiben. Die Kontrolle der korrekten Umsetzung der Vorgaben erfolgt durch den <Bereich ???> bei der <Institution>.

## Genehmigungs- und Änderungsverfahren

Der Standard physische Sicherheit (Gebäudesicherheit) wird durch den <Informationssicherheitsbeauftragter> verantwortet. Die Pflege dieses Dokuments unterliegt dem <Bereich ???> vertreten durch den <Informationssicherheitsbeauftragter>. Änderungen werden ausschließlich von dieser Person oder seinem Stellvertreter vorgenommen. Eine Genehmigung und Freigabe erfolgt durch den <Informationssicherheitsbeauftragter>.

# Standard physische Sicherheit

## Physische Sicherheit

### Gebäudeauswahl

Bei der Auswahl von Standorten und Gebäuden sind die folgenden Aspekte hinsichtlich Informationssicherheit zu berücksichtigen:

* Erreichbarkeit in Notfällen
* Beeinträchtigungen aufgrund von Unfällen oder Erschütterungen durch naheliegende Verkehrswege (Hauptstraßen, Eisenbahn, U-Bahn oder Flughafen)
* Beeinträchtigungen der Informationstechnologie durch naheliegende Sendeeinrichtungen
* Existierende Gefährdungen
* Gefährdung durch Hochwasser bei Flüssen
* Unfälle durch naheliegende Kraftwerke oder Fabriken
* Beeinträchtigungen des Zugangs (z. B. durch regelmäßige Massenveranstaltungen, Sperrungen, höhere Gewalt)
* Anordnung der Eingänge und Ladezonen

Für die Erschließung eines neuen Gebäudes ist eine entsprechende Planung unter Berücksichtigung, Bewertung und Behandlung der Risiken zu erstellen.

## Sicherheitszonen eines Gebäudes

Zur Gewährleistung eines Sicherheitsniveaus, welches den Anforderungen der an einem Standort verarbeiteten und gespeicherten Informationen genügt, werden alle Räumlichkeiten einzelnen Sicherheitszonen zugewiesen. Für diese gelten allgemeingültige und ggf. besondere Anforderungen.

* Es werden insgesamt fünf Zonen festgelegt, die sich teilweise nochmals in Zonen für klassische Büros, Technikräume oder Dokumentenarchive unterteilen.
* Grundsätzlich gilt, dass die Zonen geschachtelt werden und ein Übergang immer nur aus der direkt darunterliegenden Zone realisiert werden sollte (Zwiebelprinzip).
* Die Berechtigungen zum Zutritt zu den einzelnen Zonen sind restriktiv zu handhaben.
* An jedem Zonenübergang sollte die Autorisierung der Nutzer für den Zutritt abgeprüft werden.

Die Klassifizierung ergibt sich primär aus dem Schutzbedarf der an einem Standort (Gebäude) betriebenen Teilsysteme oder physisch gelagerten Dokumente, welche die jeweils höchste Schutzbedarfsklasse an den betrachteten Standort vererben. Sofern benötigt, kann für einen Standort eine zusätzliche bzw. eigenständige Sicherheitszone etabliert werden.

### Sicherheitszone 0 (Farbcodierung - weiß)

Die Sicherheitszone 0 definiert sich als öffentlich frei zugänglicher Bereich. Hierzu zählen zum Beispiel Zuwege zum Gebäude auf eigenen oder angemieteten Grundstücken, Eingangs- oder Empfangsbereiche oder direkte Standortumgebungen. Auch wenn diese Bereiche öffentlich sind, werden sie angemessen überwacht, bspw. durch:

* Kameraüberwachung unter Einhaltung der gesetzlichen Vorschriften,
* Einsichtnahme durch Empfangsdienst,
* Hinterfragung von Veränderungen (z. B. bei Baustellen).

### Sicherheitszone 1 (Farbcodierung - grau)

Die Sicherheitszone 1 bildet der jeweilige Empfangs- und Wartebereich in den Gebäuden. Hier findet die Zugangskontrolle aller Personen statt. Diese kann erfolgen durch:

* Überwachung durch den Empfangsdienst
* Zutrittskontrolle zum Gebäude sowie den weiteren Räumlichkeiten höherer Sicherheitszonen
* Einbruchmeldeanlage

### Sicherheitszone 2 (Farbcodierung - grün)

Die Sicherheitszone 2 ist ausschließlich Mitarbeitenden der <Institution> sowie am jeweiligen Standort eingesetztem Personal externer Firmen und Dienstleistern vorbehalten. Hierzu zählen die Flure und Büros der Mitarbeitenden sowie die Technikräume (Räume mit Druckern und Multifunktionsgeräten).

Mitarbeiter externer Firmen und Dienstleistungserbringer benötigen eine explizite Zutrittsberechtigung. Besucher sollten ständig begleitet werden. Betriebsfremde Personen dürfen diesen Bereich ohne Berechtigung und ohne Begleitung nicht betreten.

Anforderungen an die Sicherheitszone 2 sind:

* Zutrittskontrollsystem (bspw. Codeschloss, Kartenschloss, personelle Überwachung und in begründeten Ausnahmefällen auch mechanische Schlüsselschließanlage)
* Brandmeldeanlage
* Allgemeine und funktionelle Kennzeichnung der Räume gemäß Verwendung

### Sicherheitszone 3 (Farbcodierung - orange)

Der Zutritt zu Sicherheitszone 3 ist einem eindeutig identifizierbaren und benannten Kreis von Mitarbeitenden der <Institution> vorbehalten, deren direkte Tätigkeit einen Zugang zu den dort gelagerten Dokumenten oder aufgestellten IT-Systemen erfordert. Dies betrifft insbesondere:

* Bereiche für die Dokumentenarchivierung
* Serverräume
* Räume für technische Infrastruktur (z. B. Stromversorgung, Klimatisierung)

Des Weiteren ist bei dieser Sicherheitszone darauf zu achten, dass die Anforderungen aus der DIN ISO 11799 eingehalten werden.

### Sicherheitszone 4 (Farbcodierung - rot)

Der Zutritt zu Sicherheitszone 4 ist einem eindeutig identifizierbaren und benannten Kreis von Mitarbeitenden der <Institution> vorbehalten, deren direkte Tätigkeit einen Zugang zu den dort gelagerten Informationen, Dokumenten oder aufgestellten IT-Systemen erfordert. Dies betrifft insbesondere:

* Bürobereiche für die Geschäftsführung
* Bürobereiche für die Personalabteilung
* Bürobereiche für das Finanzwesen inklusive Buchhaltung
* Bürobereiche für die Administratoren
* Serverräume
* Räume für technische Infrastruktur (z. B. Stromversorgung, Klimatisierung)

Externe Dienstleister benötigen eine explizite Genehmigung ihres beauftragenden Ansprechpartners für den Zutritt zu bzw. den Aufenthalt in Räumlichkeiten dieser Sicherheitszone.

## Anforderungen an die Gebäude und Räumlichkeiten

Die Gebäude verfügen über eine eigene Zutrittssteuerung. Nicht empfohlen wird zum Beispiel die Verwendung einfacher mechanischer Schlüsselprinzipien für Zonenübergänge sowie ungeschützten Durchgänge zu anderen Sicherheitszonen, Klinken an Türaußenseiten. Dies bedeutet,

* den grundsätzlichen Verschluss der Räume beim Verlassen, den gesonderten Verschluss von Dokumenten im Raum (abschließbarer Sicherheitsschrank oder Tresor)
* die Begleitung und Beaufsichtigung nicht dauerhaft zutrittsberechtigter Personen (Handwerker, Mitarbeitende externer Firmen, Besucher)

Für Räume mit zentraler Informationstechnik (z. B. Rechenzentren, Serverräume oder Räume für technische Infrastruktur) gilt zusätzlich (soweit für den jeweiligen Raum-Typ relevant und technisch möglich):

* Unauffällige äußere Kennzeichnung bei Räumen mit technischer Infrastruktur (z. B. Server- oder Technikräume)
* Keine allgemeine Bekanntmachung der Funktion des Raumes
* Keine Lagerung von Gefahrstoffen oder hohen Brandlasten (z. B. Verpackungen, Druckerpapier)
* Protokollierung aller Zutritte
* Doppelboden (oder alternative sichere Kabelführungen)
* Klimatisierung
* Gesicherte Versorgung mit Strom
* Geeignete Löschtechnik (bspw. Handfeuerlöscher, Löschanlagen, Sauerstoffreduzierung)
* Erweiterte Schutzmaßnahmen an Wänden, Decken, Böden, Türen und Fenstern (bzw. entsprechende Alternativen)

## Gebäudesicherung

### Einhaltung der übergeordneten Richtlinien

Für alle Gebäude sind die geltenden örtlichen Bestimmungen der Bauordnung und des Brandschutzes einzuhalten.

### Perimeterschutz

Jedes Gebäude mit Technikbereichen der <Institution> sollte von einer Umzäunung umfriedet sein, sofern es bautechnisch umsetzbar ist. Der Zaun wird so gestaltet, dass er frei einsehbar ist.

Für Gebäudestandorte wird eine dauerhaft besetzte Sicherheitszentrale installiert bzw. die vorhandene genutzt. Ist dies nicht möglich, erfolgt eine Aufschaltung auf einen Wachdienst.

Außerhalb der Arbeitszeiten erfolgt mindestens eine Begehung durch das Sicherheitspersonal, das eine Zustandskontrolle der Perimeter durchführt (z. B. Prüfung aller Außentüren und -fenster, Aktivierung der Alarmanlage).

Bei Rechenzentren bzw. Serverräumen mit multiplen Serversystemen wird das Gelände zusätzlich mittels Kameratechnik überwacht, die auf die örtlichen Gegebenheiten abzustimmen ist und das gesamte Gelände dauerhaft einsehen kann.

* Es erfolgt eine Aufschaltung auf die Sicherheitszentrale bzw. die Hauptpforte.
* Zusätzlich erfolgen außerhalb der Geschäftszeiten regelmäßige Rundgänge durch Sicherheitspersonal mit Zustandskontrollen der Perimeter.
* Die direkte Umgebung von Gebäuden sollte zur Dunkelheit ausreichend ausgeleuchtet sein.

### Schutz vor Wassergefährdungen

Das Gebäude wird hinreichend vor Gefährdungen durch eindringendes Wasser wie z. B. Hochwasser, Regenwasser oder Grundwasser geschützt. Dies gilt nicht nur für die Sicherstellung des Zugangs, der jederzeit möglich sein sollte, sondern auch für die Konzeptionierung aller Versorgungsleitungen und entsprechender Verteiler, die für den Betrieb des Standorts unerlässlich sind.

Räume der Sicherheitszone 3 (Dokumentenarchiv) und Räume der Sicherheitszone 4 (kritischen IT-Systemen) sind vor eintretendem Wasser, auch aus einer evtl. installierten Sprinkleranlage hinreichend zu schützen und Feuchtigkeitsmelder zu installieren. Es dürfen keine wasserführenden Leitungen (Frisch-, Brauch- oder Abwasser) direkt neben, in oder über solchen Räumen installiert werden. Dies gilt über alle Etagen hindurch.

Nur die notwendigen Zuführungen und Abführungen (insbesondere Kondenswasserleitungen) der Klimatechnik dürfen in oder an die Räume geführt werden, wobei hier auf einen möglichst gefährdungsarmen Leitungsweg geachtet wird. In diesen Bereichen sollten Meldesysteme vor austretendem Wasser warnen und es sollte eine sofortige Verriegelung der betroffenen Leitung möglich sein.

### Schutz der Fenster und Türen

Fensterflächen, Türen (Haupteingangs-, Flucht-, Nebeneingangs-, Kellertüren o.ä. und deren Rahmen mit direktem Kontakt zum Außenbereich), sowie Zonenübergangstüren im Gebäude samt eventueller zonenbegrenzender Fensterflächen werden mit einer hohen bis sehr hohen Widerstandsklasse ausgelegt.

Ein Rechenzentrum, ein Serverraum oder Raum für technische Infrastruktur sollte über keine Fensterflächen verfügen. Sind diese dennoch vorhanden, sind die Fenster durchbruchhemmend mindestens der Klasse RC-4 (DIN EN 1627:2010-09) entsprechend auszulegen. Die Außentüren, idealerweise auch die der Innentüren, und die Fenster werden durchbruchhemmend ausgelegt.

Grenzen die Sicherheitszonen 1 oder 2 aus bautechnischer Grundlage direkt an den Außenbereich werden die Fenster immer durchbruchhemmend ausgelegt. Dies gilt ebenso für die verwendeten Rahmen, die auch über eine entsprechend angemessene Verankerung im Mauerwerk verfügen.

Für die Standorte wird eine Einbruchmeldeanlage für das gesamte Gebäude installiert. Alle Meldungen laufen bei der dauerhaft besetzten Sicherheitszentrale auf. Wenn keine Sicherheitszentrale vorhanden ist, laufen die Meldungen bei einem Wachdienst auf. Meldungen außerhalb der regulären Arbeitszeit können zusätzlich eine direkte Aufschaltung zur örtlichen Polizei erhalten.

## Gewährleistung des Brandschutzes

### Brand-Sicherheitszonen

Es werden Brand-Sicherheitszonen entsprechend des Brandschutzkonzeptes bzw. der Brandschutzverordnung eingerichtet.

* Trennende Türen dürfen nicht verstellt oder dauerhaft offengehalten werden. Wenn sie aus betriebstechnischer Sicht offengehalten werden, sind sie mit einem selbstschließenden Mechanismus im Gefahrenfall ausgestattet.
* Durchbrüche in Brandwänden sind sachgerecht zu verschließen.

Decken, Böden, Wände und Türen von Rechenzentren mit multiplen Serversystemen müssen eine Brand-Widerstandsfähigkeit von mindestens 90 Minuten (siehe DIN 4102-5) erfüllen können. Für die Decken, Böden, Wände und Türen von Serverräumen ist sicherzustellen, dass diese eine Brand-Widerstandsfähigkeit von mindestens 30 Minuten erfüllen können. Die Türen von Rechenzentren und Serverräumen müssen zusätzlich über einen Rauchschutz verfügen und Sie sollen im Brandfall für eine Zeitdauer von etwa 10 Minuten die Rettung gewährleisten.

### Brandmeldeanlagen

Im gesamten Gebäude wird für den vorbeugenden Brandschutz eine Meldetechnik installiert, die regelmäßig gewartet wird.

### Geräte

Zur Verfügung gestellte, aber potentiell gefährliche Geräte, wie z. B. Kaffeemaschinen, Wasserkocher usw., dürfen durch Mitarbeitende nicht außerhalb der dafür eingerichteten Bereiche und ohne qualifizierte Abnahme in Betrieb genommen werden.

### Übungen

Mit den Mitarbeitenden sollten regelmäßige Brandschutzübungen durchgeführt werden. Sofern die Räumlichkeiten sich über mehrere Etagen erstrecken, werden pro Etage Ersthelfer bestimmt und mit dem nötigen Fachwissen ausgebildet. Während der Übungen wird auch die Funktionalität der Sicherheitstüren und -fenster getestet.

### Installation von Löschsystemen

Das Rechenzentrum bzw. Dokumentenarchive müssen grundsätzlich über geeignete Löschsysteme verfügen. Darüber hinaus sind in allen Zonen entsprechende Handfeuerlöscher in hinreichender Menge und Größe griffbereit vorzuhalten. Sowohl das automatische Löschsystem als auch die Handfeuerlöscher werden einem regelmäßigen Wartungsprozess unterzogen. Die Mitarbeitenden des Rechenzentrums sind in den Umgang mit mit den Löschsystemen bzw. Handfeuerlöschern einzuweisen.

## Umsetzung des Zutrittsschutzes

### Allgemeine Zutrittsbestimmungen

Handelt es sich um eigene Gebäude oder um Gebäude wo die <Institution> der alleinige Mieter ist, ist ein Betreten außerhalb der Zeit von 06:30 bis 21:30 Uhr an Werktagen nur mit einer genehmigungspflichtigen Zutrittsberechtigung möglich. Die Genehmigung kann in Abstimmung mit der Gebäudesicherheit durch die Vorgesetzten erfolgen. In Gebäuden mit mehreren Mietern oder Nutzern ist dies anzustreben.

### Zutritt zum Gebäude

Der Zutritt zum Gebäude erfolgt über einen Haupteingang, der in den Geschäftszeiten mit einem Empfangsdienst besetzt wird. An kleineren Standorten kann auf den Empfangsdienst verzichtet werden, wenn die nachfolgenden Regelungen eingehalten werden.

* Der Außenbereich eines Gebäudes wird vom Innenbereich mit einer auch dauerhaft verschließbaren Tür abgeschottet.
* Die Tür wird entsprechend der geltenden Normen (DIN EN 1627:2010-09) ausgelegt und verfügt über eine hohe bis sehr hohe Widerstandsklasse.
* Ein Zutritt von Personen erfolgt nur nach erfolgreicher Zutrittskontrolle (personalisierte Zugangskarten).
* Jeder Mitarbeitende des Standorts ist zur Einhaltung und Überwachung dieser Richtlinie zu verpflichten.

## Zutritt zwischen den Sicherheitszonen

Der Zutritt aus dem öffentlichen Bereich (Sicherheitszone 0) in geschützte Bereiche der Sicherheitszonen 1 bis 4 wird mit geeigneten Zutrittskontrollsystemen gesteuert. An den Schnittstellen zwischen allen Sicherheitszonen werden weitere Zutrittskontrollsysteme installiert, wobei die Sicherheitszone 1 bei Standorten mit Rechenzentrum grundsätzlich mit einem Vereinzelungssystem ergänzt sein soll. Die Nutzung des am Standort vorhandenen Zutrittskontrollsystems wird für alle Mitarbeitende verbindlich geregelt. Insbesondere werden die Mitarbeitenden darauf verpflichtet, keine Unberechtigten durch Kontrollabschnitte mitzunehmen, wenn keine entsprechenden technischen Einrichtungen dies verhindern können.

### Verwaltung von Zutrittsberechtigungen

Die Ausgabe von Schlüsseln, Schlüsselkarten, Token oder ähnlichem sowie die Vergabe von Zutrittsberechtigungen an Mitarbeitende und Mitarbeitende externer Firmen sind zentral zu registrieren. Nicht ausgegebene Schlüssel, Schlüsselkarten, Token etc. werden in einem abschließbaren Schrank aufbewahrt. Ausscheidende Mitarbeitende geben am letzten Tag ihrer offiziellen Anwesenheit alle Schlüssel, Schlüsselkarten, Token oder ähnliches ab. Ihre Berechtigungen werden unverzüglich deaktiviert oder gelöscht.

### Zentrale Zutrittskontrollsysteme

Bei der Verwendung von zentralisierten Zutrittskontrollsystemen werden für alle Mitarbeitenden, externen Dienstleister und Besucher Profile mit den berechtigten Zutrittszonen erstellt und im Zutrittskontrollsystem hinterlegt. Zutrittsrechte zu Räumlichkeiten der Sicherheitszone 3 und 4 sind für Besucher nicht zu vergeben.

Jeder Zutritt in Räume ab Sicherheitszone 2 sollte innerhalb und außerhalb der regulären Geschäfts- oder Arbeitszeiten protokolliert werden. Des Weiteren sollten alle nicht erlaubten Zutrittsversuche protokolliert werden.

Bei Räumen mit multiplen Serversystemen (Rechenzentrum) wird ein Alarm an die Sicherheitszentrale gemeldet. Alle protokollierten Ereignisse werden regelmäßig ausgewertet. Auffälligkeiten wird unverzüglich nachgegangen. Bei der Auswahl eines Zutrittskontrollsystems werden zunächst interne Vorgaben und anschließend soweit notwendig vorhandene Zertifizierungen von unabhängigen Stellen maßgeblich zur Beurteilung berücksichtigt.

## Klimatisierung

Alle Technikräume, in denen eine vorgegebene Betriebstemperatur notwendig ist, werden mit einer hinreichend ausgelegten Klimaanlage ausgestattet. Für die zu klimatisierenden Bereiche wird ein Leistungsprofil erarbeitet, in welchem die Anforderungen an die Klimatechnik und die Art der Klimatisierung abgestimmt werden. Neuinstallationen dürfen nur nach Prüfung des Leistungsprofils auf Problemsituationen, wie Wärmestau, Wärmelast usw. erfolgen.

Bei der Auslegung und Ausgestaltung der Klimaanlage werden folgende Randwerte betrachtet:

* Leistungsreserven für Wachstum,
* Berücksichtigung hoher Außentemperaturen,
* Redundanz des Systems oder von Systemteilen,
* Schutz vor Manipulation oder Zerstörung, insbesondere der außen installierten Komponenten wie Rückkühler, Ansaugstutzen etc.,
* Kürzeste Leitungsführung im klimatisierten Bereich.

Für die installierte Klimatechnik wird mit dem Dienstleister ein Wartungsvertrag vereinbart. Bei Räumen mit multiplen IT-Systemen (Rechenzentrum) sind angemessene Reaktionszeiten festzulegen.

## Vorgaben für die Aufstellung von IT-Systemen

Zum Schutz vor unautorisiertem physischem Zugriff müssen alle Serversysteme und aktiven Netzkomponenten (Firewalls, Router/Switches) in einem Serverraum untergebracht werden. Aktive Netzkomponenten für die Etagenverteilung sind alternativ adäquat geschützt (z. B. verschlossener IT-Schrank) in einem geeigneten Technikraum unterzubringen.

In diesen Räumlichkeiten gelten ein grundsätzliches Rauchverbot sowie ein Verbot der Mitnahme oder des Verzehrs von Nahrungsmitteln.

### Vorgaben für Serverräume

Wird der Serverraum innerhalb eines Gebäudes oder der Bürofläche der <Institution> eingerichtet, sollte neben den zuvor aufgeführten Maßnahmen bzw. Regelungen zudem die Ergänzungen oder Abweichungen in diesem Kapitel berücksichtigt werden.

Der Serverraum hat sich in einem eigenen Brandschutzbereich befindet. Dabei sollen bereits bei der Auswahl des Serverraumes auch die Gefährdungen im Auge behalten werden, die sich durch die Umgebung ergeben könnten.

Bei der Stromversorgung soll darauf geachtet werden, dass der Serverraum über angepasste Stromkreise verfügt. Wenn möglich, sollte er an einen eigenen Stromkreis angeschlossen werden, getrennt von anderen Anlagen. Ansonsten sollten Steckdosenleisten mit Spannungsfilter eingesetzt werden. Falls der Strom ausfällt, ist für eine unterbrechungsfreie Stromversorgung (USV) zu sorgen. In Betracht kann die Anschaffung von USV-Anlagen gezogen werden, die zumindest das kontrollierte Herunterfahren der Systeme gewährleistet.

Ist auch ein langfristiger Stromausfall nicht tolerierbar, wäre der Einsatz eines Notstromgenerators sinnvoll, der im Notfall anspringt und ein Aufrechterhalten der Systeme sicherstellt.

Der Serverraum sollte über einen Doppelboden oder über Kabelkanalanlagen verfügen. In dem Hohlraum des Doppelbodens können Verkabelungen versteckt werden, was zu einer Erhöhung der Sicherheit führt.

Der Serverraum muss vor Hitze, Feuer und Brand geschützt werden. Deswegen sind Klimaanlagen zu installieren, wenn der normale Luft- und Wärmeaustausch eines Raumes nicht ausreicht. Ferner sollen nicht nur Rauchmelder vorhanden sein, sondern auch Brandmeldeanlagen. Diese können Brände in den IT-Anlagen in einem frühen Stadium erkennen. Bei hochwertigen IT-Anlagen können automatische Löschanlagen das teure Anschaffen neuer Anlagen verhindern. Ansonsten sollte in jedem Serverraum ein Handfeuerlöscher (z. B. Kohlendioxid, Argon, Stickstoff, FM 200) vorhanden sein.

Zusätzlich ist darauf zu achten, dass der Serverraum kein Abstellplatz ist und entzündliche Gegenstände aus Papier, Plastik o.ä. (z. B. Wasserkästen, Kartons, Akten) eine Gefahrenquelle darstellen.

Die IT-Anlagen sollten auch vor Wasser geschützt werden. Sind Fenster in dem Serverraum vorhanden, sollte darauf geachtet werden, dass kein Wasser (z. B. insbesondere Regen) in den Serverraum eindringen kann. Ferner sollte darauf geachtet werden, dass keine wasserführenden Leitungen in dem Serverraum vorhanden sind.

Ein Serverraum sollte stets verschlossen sein. Damit unbefugte Dritte den Serverraum nicht sofort entdecken können, sollte auf eine Beschilderung des Raumes verzichtet werden.

Um den Serverraum gegen Einbrüche abzusichern, sollten zudem Türen, Fenster und andere Eingangs- und Einstiegsmöglichkeiten so gesichert werden, dass sie auch zeitintensiveren Einbruchsmethoden standhalten.

Ergänzend zu den Angaben in Kapitel „Schutz der Fenster und Türen“ gelten für den Serverraum die Vorgaben bei Erreichbarkeit der Fenster aus dem öffentlichen Raum. Sofern Fenster vom öffentlichen Raum aus erreichbar sind, müssen sie z. B. durch Gitter, Schlösser, Sicherheitsglas oder Anti-Einbruch-Fensterfolie gesichert werden. Auch Luken, Lichtschächte und ähnliche Gebäudeteile können Einstiegsmöglichkeiten bieten und sind entsprechend zu sichern.

Fenster müssen zusätzlich mit abschließbaren Fenstergriffen ausgerüstet sein.

Durch eine Videoüberwachung des Eingangsbereichs kann die Sicherheit gesteigert werden. Hierbei ist aber auf eine datenschutzkonforme Aufzeichnung zu achten. Die Tür(en) zum Serverraum sind geschlossen zu halten.

In einem schriftlichen Berechtigungskonzept muss geregelt werden, welche Personen Zutritt zum Serverraum benötigen und erhalten. Dabei soll der Zutritt nur denjenigen vorbehalten sein, die zur Durchführung ihrer Aufgaben einen Zutritt bzw. Zugriff auf die IT-Anlagen benötigen. Ebenso sollte ein Berechtigungskonzept beschreiben, wer organisatorisch und technisch die Berechtigungen vergibt.

Es sollte festgehalten werden, wer wann einen Schlüssel (bzw. Chipkarte) zum Serverraum erhalten hat und wie viele Schlüssel (bzw. Chipkarten) vorhanden und vergeben sind. Auch sollte ein Schlüssel (bzw. Chipkarte) als Reserve für den Fall gesichert aufbewahrt werden, falls der Zutritt zum Serverraum notwendig wird und keine Person mit einem entsprechenden Schlüssel anwesend ist.

Nicht vergessen werden sollte, eine entsprechende Anweisung zu erteilen, wie sich berechtigte Personen bei Schlüsselverlust (bzw. Chipkartenverlust) zu verhalten haben und wem sie diesen melden müssen, damit entsprechende Maßnahmen in die Wege geleitet werden können.

### Vorgaben für IT-Schränke

Es sind LAN-Schränke entsprechend den Gegebenheiten (stehend oder wandhängend) und den Erfordernissen zu verwenden. Für die Größe ist unbedingt der Bedarf der nächsten 5 Jahre mit einzukalkulieren.

Es muss bei den Schränken auf eine gute Zugänglichkeit geachtet werden. Die Türen müssen sich vollständig öffnen lassen. Bei Datenschränken ist auf der Vorder- und Rückseite ein Abstand von 120 cm einzuhalten.

An Schränken, die an einer Ecke eines Raumes oder mit einer Seite an einer Wand stehen, sind die Türen so anzubringen, dass der Türanschlag zur Wand angebracht wird, sodass die Tür zur Wand hin öffnet.

Alle Schranktüren müssen sich problemlos öffnen lassen.

Die Gehäuse der Datenschränke sind Pulverbeschichtet, RAL7035.

In jedem Datenschrank ist eine Steckdosenleiste mit mind. sieben Anschlüssen ohne Schalter mit 16 A Absicherung (separat) einzubauen. Ein integrierter Feinschutz ist vorzusehen.

Bei Bedarf (hohe Wärmelast) sind zusätzlich Ventilatoren im Dach und Temperaturfühler im Schrank einzuplanen.

Alle Schranktüren sind mit 180° Scharnieren sowie Komfortgriffen zur Installation eigener Profilhalbzylinder auszurüsten. Schränke sind mit einer Schließung zu versehen.

Jeder Datenschrank ist in den Potentialausgleich nach DIN/ VDE einzubinden (min. 25mm2). Es gelten die in den DIN EN 50174 und DIN EN 50310 (VDE 0800 Teil 2-310) festgelegten Bestimmungen für Potentialausgleich und Erdung.

Unter jedem Patchfeld sowie an beiden Seiten sollten Kabelführungsbügel angebracht werden. Die vertikalen Kabelbügel sollten untereinander nicht mehr als 30 cm Abstand haben.

Alle Verlegekabel sind in den Schränken so zu verlegen, dass der Einbau oder Ausbau von Komponenten in den Schränken nicht behindert wird. Die Kabelzuführung zu den Schränken kann von oben, unten oder seitlich erfolgen. Die Verlegekabel sind ausreichend zu befestigen. Jedes Kabel hat auf einer Klemme, einem Anschluss oder einer Dose zu enden.

Die Beschriftung der Datenschränke erfolgt zweckmäßigerweise am oberen Rand der vorderen Datenschranktüren. Die Beschriftung muss gut lesbar sein.

## Stromversorgung

### Stromeinspeisung

Es ist regelmäßig zu überprüfen, ob die Absicherung und Auslegung der Stromkreise noch den tatsächlichen Bedürfnissen genügen. Elektrotechnische Anlagen werden nach deren Installation durch einen Sachverständigen in den vorgeschriebenen Intervallen überprüft. Für kritische Standorte (insbesondere Rechenzentren) ist eine redundante Einspeisung vorzusehen.

### Vorgaben für USV und Notstromversorgung

Zum Schutz vor Schäden durch plötzlichen Stromausfall müssen alle Serversysteme und aktiven Netzkomponenten (Firewalls, Router/Switches) an ein System zur unterbrechungsfreien Stromversorgung (USV) angeschlossen werden.

Die Stützzeit der USV muss so lang ausgelegt sein, dass alle Systeme geordnet heruntergefahren werden können. Typische Werte für die Stützzeit liegen bei 30 bis 60 Minuten. Der doppelte Ansatz der Shutdown-Zeit bewirkt ein Sicherheitspolster. Da die USV die letzte Bastion gegen den Stromausfall ist, kommt ihr große Bedeutung für die Sicherstellung der Verfügbarkeit zu.

* Sie hat denselben Schutzbedarf wie die durch die USV versorgte IT.
* Wenn die USV-versorgten IT-Systeme redundant ausgelegt sind, sollten auch USV-Systeme redundant vorhanden sein.

Wie bei allen anderen elektrischen Geräten ist auch bei USV-Systemen darauf zu achten, dass sie in den vom Hersteller genannten Temperaturbereichen betrieben werden. Dies ist bei der Dimensionierung der Kühlung zu berücksichtigen. Um die Schutzwirkung einer USV aufrechtzuerhalten, muss sie regelmäßig gewartet werden. Dafür sind die vom Hersteller vorgesehenen Wartungsintervalle der USV einzuhalten. Bei höheren Verfügbarkeitsanforderungen ist eine Netzersatzanlage (NEA) einzurichten. Sowohl die USV als auch die NEA sind regelmäßig zu testen.

### Blitz- und Überspannungsschutz

Die Gebäude der <Institution> verfügen über einen Blitz- und Überspannungsschutz mit den folgenden Anforderungen:

* Der Blitz- und Überspannungsschutz wird für den direkten Einschlag eines Blitzes sowie für die Einkopplung aufgrund der enormen elektrischen Felder gestaltet.
* Der Blitzschutz teilt sich in den äußeren und inneren Blitzschutz auf und wird nach geltender Norm DIN EN 62305 / VDE 0185 umgesetzt.
* Der äußere Blitzschutz dient im Wesentlichen dem Schutz des Gebäudes. (z. B. Blitzableiter)
* Zum Schutz von IT-Systemen wird ein gestaffelter innerer Blitzschutz, bestehend aus Grobschutz (bis ca. 6000 V), Mittelschutz (bis ca. 2000 V) und Feinschutz realisiert. Der Grobschutz muss blitzstromtragfähig sein.
* Bei der Installation ist auf ein zentrales Potential zu achten, damit die Wirksamkeit der Überspannungsschutzeinrichtungen gegeben ist.
* Für die Standorte sollten Blitzschutzzonen eingerichtet werden, die sich an den vorhandenen Sicherheitszonen orientieren.

## Versorgung mit Netzdiensten und Telekommunikation

Die Versorgung mit Netzdiensten und Telekommunikation wird dauerhaft sichergestellt.

* Die Einspeisung erfolgt soweit technisch möglich über zwei unterschiedliche und unabhängige Leitungswege in das lokale Netz.
* Verteiler- oder Übergabestellen werden mindestens in Räumen der Sicherheitszone 2 installiert.

Auf im freien Gelände installierte Verteiler wird verzichtet und eine Verlagerung angestrebt. Ist dies aus technischen Gründen nicht möglich, werden zusätzliche Maßnahmen zum Schutz der Verteiler vor Beschädigung oder Manipulation getroffen und als Ersatzleitungsweg eine nicht-terrestrische Verbindung bevorzugt. Dies gilt ebenso für Leitungswege, die einer besonderen Gefährdung ausgesetzt sind.

Die Einspeisungen werden von der Energieversorgung getrennt geführt. Ebenso wird auf die Trennung der Leitungswege im Haus geachtet. Zentrale Netz- und Telekommunikationsräume sind mindestens der Sicherheitszone 2 zugeordnet.

Trassen, Kabelkanäle und Steigepfade werden vor direktem Zugriff und vor Brandgefahren hinreichend geschützt.

Das interne Netz wird nach Möglichkeit mit zwei Steigepfaden (sekundäre Verkabelung) ausgelegt und die Etagen vom Etagenverteiler (Sicherheitszone 2) redundant versorgt.

## Fernanzeige von Störungen

Meldeanlagen, Serversysteme, aktive Netzkomponenten sowie wesentliche Unterstützungselemente wie USV und Klimatisierung sind mit einem Überwachungssystem zu versehen, um Fehlfunktionen frühzeitig erkennen zu können. In kritischen Bereichen ist sicherzustellen, dass Alarmmeldungen auch unverzüglich angenommen und bearbeitet werden können. Sofern kein externer Wartungsdienst beauftragt ist, muss ggf. eine Rufbereitschaft eingerichtet werden.

## Schutz bei der Gebäudereinigung

Die Reinigung von Informationstechnik und technische Anlagen sind grundsätzlich aus der allgemeinen Gebäudereinigung auszuschließen. Diese erfolgt nur durch entsprechend geschultem Personal. In kritischen Bereichen (z. B. Räumen mit Servern oder technischen Anlagen) sind Reinigungskräfte grundsätzlich zu begleiten und zu beaufsichtigen.

## Ausnahmeregelungen

Aufgrund baulicher oder technischer Gegebenheiten oder anderer übergeordneter Zwänge ist eine Abweichung von den hier definierten Vorgaben teilweise unumgänglich. Dies können zum Beispiel andere Zonenübergänge oder Lösungen über andere technische Maßnahmen sein. Die hier definierten Maßnahmen gelten als Richtlinie und müssen für jeden betrachteten Einzelfall geprüft und gegebenenfalls angepasst werden.