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

Sicherheitsrichtlinie "Bürogebäude"

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 Dokumentenvertraulichkeit  offen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300058 | [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](#_Toc83717825)

[Dokumentenhistorie 3](#_Toc83717826)

[Inhaltsverzeichnis 4](#_Toc83717827)

[Allgemeine Festlegungen 5](#_Toc83717828)

[Ziel / Zweck 5](#_Toc83717829)

[Geltungsbereich 6](#_Toc83717830)

[Zuständigkeiten 6](#_Toc83717831)

[Genehmigungs- und Änderungsverfahren 6](#_Toc83717832)

[Aufbau des Dokuments 7](#_Toc83717833)

[Sicherheitsrichtlinie „Bürogebäude" 8](#_Toc83717834)

[Basismaßnahmen 8](#_Toc83717835)

[Allgemeines Gebäude 8](#_Toc83717836)

[Büroarbeitsplatz 9](#_Toc83717837)

[Besprechungs-, Veranstaltungs- und Schulungsräume 9](#_Toc83717838)

[Raum sowie Schrank für technische Infrastruktur 10](#_Toc83717839)

[Standardmaßnahmen 10](#_Toc83717840)

[Allgemeines Gebäude 10](#_Toc83717841)

[Büroarbeitsplatz 12](#_Toc83717842)

[Besprechungs-, Veranstaltungs- und Schulungsräume 13](#_Toc83717843)

[Raum sowie Schrank für technische Infrastruktur 14](#_Toc83717844)

[Maßnahmen bei erhöhtem Schutzbedarf 14](#_Toc83717845)

[Allgemeines Gebäude 14](#_Toc83717846)

[Büroarbeitsplatz 16](#_Toc83717847)

[Besprechungs-, Veranstaltungs- und Schulungsräume 16](#_Toc83717848)

[Raum sowie Schrank für technische Infrastruktur 16](#_Toc83717849)

# Allgemeine Festlegungen

## Ziel / Zweck

Ein Rechenzentrum ist innerhalb der <Institution> wie folgt definiert:

* Wird die IT der <Institution> innerhalb eines Gebäudes oder einer Liegenschaft verteilt in mehreren Bereichen betrieben und sind diese Bereiche untereinander und zu den IT-Benutzern hin durch hauseigene LAN-Verbindungen angeschlossen, ist mindestens der funktional bedeutendste dieser Bereiche als Rechenzentrum zu behandeln. Des Weiteren sind Bereiche, von deren ordnungsgemäßem Betrieb 50 % und mehr Nutzer abhängig sind oder aus denen heraus 50 % und mehr an Diensten und Daten (gemessen an der Gesamtheit der Bereiche) bereitgestellt werden, als Rechenzentrum zu behandeln.
* Hat die <Institution> nur einen zentralen IT-Betriebsbereich, ist dieser gemeinsam mit den erforderlichen Supportbereichen grundsätzlich immer wie ein Rechenzentrum entsprechend dem Schutzbedarf zu behandeln. Unter „IT-Betriebsbereich“ sind Räume zu verstehen, in denen die Hardware aufgebaut ist und betrieben wird, die der Bereitstellung von Diensten und Daten dient. Das Rechenzentrum umfasst neben dem IT-Betriebsbereich alle weiteren technischen Supportbereiche (z. B. Stromversorgung, Kälteversorgung, Löschtechnik, Sicherheitstechnik), die dem bestimmungsgemäßen Betrieb und der Sicherheit dienen.
* Ist die IT der <Institution> an mehreren räumlich voneinander getrennten Standorten angesiedelt und sind diese durch andere als hauseigene LAN-Verbindungen miteinander gekoppelt, ist jeder der Standorte entsprechend separat zu betrachten und zu behandeln.
* Ein IT-Betriebsbereich, in dem für kritische Geschäftsprozesse (Prozesse, deren Störung oder Ausfall zu wesentlichen Beeinträchtigungen der Erledigung primärer Aufgaben führen) erforderliche IT angesiedelt ist, ist immer als Rechenzentrum zu behandeln, unabhängig von Größe.
* IT-Betriebsbereiche, aus denen heraus Dienste oder Dienstleistungen für Dritte erbracht werden, sind immer als Teil eines Rechenzentrums zu betrachten. Dabei ist es unerheblich, ob dies gegen Entgelt erfolgt oder nicht.
* Besteht ein begründetes Interesse, einen IT-Betriebsbereich gemeinsam mit seinem Supportbereich abweichend von den vorgenannten Regelungen als Serverraum zu behandeln, ist dies samt den sich daraus ergebenden Reduzierungen von Sicherheitsanforderungen zu begründen.

Weicht ein Rechenzentrum von dieser Definition ab, wird der betrachtete IT-Betriebsbereich als Serverraum bezeichnet. Diese Definition orientiert sich ausschließlich an der Bedeutung der IT-Struktur für die Aufgabenerfüllung der <Institution> und steht damit im methodischen Einklang mit der DIN EN 50600.

Soll ein Serverraum abgesichert werden, können die Anforderungen dieser Sicherheitsrichtlinie entsprechend reduziert werden. Dies muss jedoch stichhaltig und nachvollziehbar begründet werden und es müssen mindestens die Basis-Anforderungen umgesetzt werden.

Ziel dieser Sicherheitsrichtlinie ist es zu beschreiben, welche Anforderungen zu erfüllen sind, um ein Rechenzentrum aus Sicht der Informationssicherheit optimal zu nutzen. Für die Erstellung dieser Sicherheitsrichtlinie wurde auf die Vorgaben des BSI Bausteines INF.1 „Allgemeines Gebäude" und INF.2 „Rechenzentrum“ zurückgegriffen.

Ein Büroraum ist der Bereich innerhalb der <Institution>, in dem sich ein oder mehrere Mitarbeitende aufhalten, um dort ihre Aufgaben zu erfüllen. In dieser Sicherheitsrichtlinie werden die typischen Gefährdungen und Anforderungen bezüglich der Informationssicherheit für einen Büroraum auf Basis der Vorgaben aus dem BSI Bausteines INF.7 "Büroarbeitsplatz" definiert.

## 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

Die Sicherheitsrichtlinie „Bürogebäude“ 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>.

## Aufbau des Dokuments

Das vorliegende Dokument ist wie folgt aufgebaut:

* Kapitel Basismaßnahmen: Beschreibung der Kernmaßnahmen, die für das Anforderungsmanagement zwingend erforderlich sind.
* Kapitel Standardmaßnahmen: Definition von Maßnahmen zur Erreichung eines vollumfänglichen Standardabsicherungsschutzniveaus für einen Schutzbedarf von „Normal“ in den Informationssicherheitsschutzzielen Vertraulichkeit, Integrität und Verfügbarkeit.
* Kapitel Maßnahmen bei erhöhtem Schutzbedarf: Erläuterung von Maßnahmen die einen erhöhten Schutzbedarf (Schutzbedarfe „Hoch“, „Sehr hoch“) gewährleisten. Der Einsatz ist je Anwendungsfall im Rahmen einer Verhältnismäßigkeitsprüfung abzuwägen.

# Sicherheitsrichtlinie „Bürogebäude"

## Basismaßnahmen

Die nachfolgenden Basismaßnahmen sind vorrangig zur Gewährleistung der sicherheitstechnischen Anforderungen aus der Leitlinie umzusetzen.

### Allgemeines Gebäude

#### Planung der Gebäudeabsicherung (INF.1.A1)

Das System der Einbruchhemmung muss wie eine Kette wirken und ist nur so gut wie das schwächste Glied. Aus diesem Grunde muss die Einbruchshemmung bereits bei der Gebäudeplanung beginnen. Unter Berücksichtigung der innerhalb des Bürogebäudes betriebenen Services und deren Schutzbedürfnisse (Verfügbarkeit, Vertraulichkeit und Integrität) muss von den Verantwortlichen für die Planung der Gebäudeabsicherung festgelegt werden, wie dieses unter Anwendung der internen und gesetzlichen Vorgaben abzusichern ist.

#### Angepasste Aufteilung der Stromkreise (INF.1.A2)

Es muss regelmäßig überprüft werden, ob die Absicherung und Auslegung der Stromkreise noch den tatsächlichen Bedürfnissen des Bürogebäudebetriebes genügen. Bei der Absicherung und Auslegung der Stromkreise muss ebenfalls der voraussichtliche Bedarf für die nächsten zwei Jahre mit einfließen.

#### Einhaltung von Brandschutzvorschriften (INF.1.A3)

Die bestehenden Brandschutzvorschriften sowie die Auflagen der Bauaufsicht müssen von der <Institution> als Betreiber des Bürogebäudes bzw. vom Vermieter des Gebäudes eingehalten werden. Die Fluchtwege müssen vorschriftsmäßig ausgeschildert und freigehalten werden. Bei der Brandschutzplanung sollte die örtliche Feuerwehr hinzugezogen werden. Es muss ein IT-bezogenes Brandschutzkonzept erstellt und umgesetzt werden, dass die fehlenden IT bezogenen Anforderungen aus der Bauordnung zum Brandschutz enthält.

Unnötige Brandlasten müssen vermieden werden.

Es muss eine Brandschutzbeauftragte bzw. einen Brandschutzbeauftragten oder eine mit dem Aufgabengebiet betraute und geschulte Person benannt sein.

Branderkennung in Gebäuden (INF.1.A4)

Das Bürogebäude muss mit einer ausreichenden Anzahl von Rauchmeldern und einer Brandmeldezentrale (BMZ) ausgestattet sein. Alle Rauchmelder müssen auf der MBZ aufgeschaltet sind. Zusätzlich muss eine Alarmierung bei erkanntem Rauch im Bürogebäude ausgelöst werden. Die Funktionsfähigkeit aller Rauchmelder bzw. aller Komponenten einer Brandmeldeanlage müssen regelmäßig überprüft werden. Ebenfalls muss regelmäßig kontrolliert werden, dass die Fluchtwege benutzbar und frei von Hindernissen sind, damit das Bürogebäude in einer Gefahrensituation schnell geräumt werden kann.

Handfeuerlöscher (INF.1.A5)

Zur Sofortbekämpfung von Bränden müssen Handfeuerlöscher in der jeweils geeigneten Brandklasse (DIN EN 3 Tragbare Feuerlöscher) in ausreichender Zahl und Größe im Bürogebäude zur Verfügung stehen. Die Handfeuerlöscher müssen regelmäßig geprüft und gewartet werden. Die Mitarbeitenden sollten im Rahmen von Brandbekämpfungsschulungen in die Benutzung der Handfeuerlöscher eingewiesen werden.

#### Geschlossene Fenster und Türen (INF.1.A6)

Im Bürogebäude müssen Fenster und Türen geschlossen werden. Dafür muss eine entsprechende Anweisung erlassen werden. Es muss regelmäßig überprüft werden, ob die Fenster und Türen verschlossen sind. Brand- und Rauchschutztüren dürfen unter Berücksichtigung der Implementierungsart nicht dauerhaft offengehalten werden bzw. müssen bei Erkennung eines Brandes automatisch sich schließen.

#### Zutrittsregelung und -kontrolle (INF.1.A7)

Der Zutritt zu schutzbedürftigen Gebäudeteilen und Räumen muss geregelt und kontrolliert werden. Die Zahl der zutrittsberechtigten Personen muss für jeden Bereich auf ein Mindestmaß reduziert werden. Weitere Personen dürfen erst Zutritt erhalten, nachdem geprüft wurde, ob dies notwendig ist. Alle erteilten Zutrittsberechtigungen müssen dokumentiert werden. Die Zutrittskontrollmaßnahmen müssen regelmäßig auf ihre Wirksamkeit überprüft werden.

#### Rauchverbot (INF.1.A8)

In den Räumen des Bürogebäudes muss ein striktes Rauchverbot gelten.

### Büroarbeitsplatz

#### Geeignete Auswahl und Nutzung eines Büroraumes (INF.7.A1)

Als Büroraume müssen hierfür geeignete Räume genutzt werden. Die Büroräume müssen für den Schutzbedarf bzw. das Schutzniveau der dort verarbeiteten Informationen angemessen ausgewählt und ausgestattet sein. Büroräume mit Publikumsverkehr dürfen nicht in sicherheitsrelevanten Bereichen des Bürogebäudes sich befinden. Die Arbeitsstättenverordnung für die Einrichtung eines Büroraumes umgesetzt werden (<http://www.gesetze-im-internet.de/arbst_ttv_2004/index.html>).

#### Geschlossene Fenster und abgeschlossene Türen (INF.7.A2)

Wenn Mitarbeitende ihre Büroräume verlassen, müssen alle Fenster verschlossen werden. Befinden sich vertrauliche Informationen in dem Büroraum, müssen beim Verlassen die Türen abgeschlossen werden. Dies sollte insbesondere in Bereichen mit Publikumsverkehr beachtet werden.

Alle Mitarbeitenden der <Institution> müssen dazu verpflichtet werden, die Anweisungen einzuhalten und die internen Vorgaben dieser Sicherheitsrichtlinie umzusetzen. Zusätzlich sollte regelmäßig geprüft, ob beim Verlassen die Fenster und die Türen abgeschlossen wurden. Ebenso muss darauf geachtet werden, dass Brand- und Rauchschutztüren tatsächlich geschlossen sind oder automatsch geschlossen werden können.

### Besprechungs-, Veranstaltungs- und Schulungsräume

#### Sichere Nutzung von Besprechungs-, Veranstaltungs- und Schulungsräumen (INF.10.A1)

In den Besprechungs-, Veranstaltungs- und Schulungsräumen vorhandene IT-Systeme müssen angemessen gegen Diebstahl gesichert werden. Wer die in den Räumen dauerhaft vorhandenen IT- und sonstigen Systeme administriert muss festgelegt werden. Ob und unter welchen Bedingungen Besucher mitgebrachte IT-Systeme in Besprechungs-, Veranstaltungs- und Schulungsräumen verwenden dürfen bzw. sich wie an die bereitgestellten Netzzugänge und eventuellen Telekommunikationsschnittstellen anbinden dürfen, muss festgelegt werden.

#### Beaufsichtigung von Besuchern (INF.10.A2)

Besucher müssen außerhalb von Besprechungs-, Veranstaltungs- und Schulungsräumen, welche ausdrücklich nicht für den Zutritt von Besuchern der <Institution> vorgesehen sind, beaufsichtigt werden. Mitarbeiter müssen dazu sensibilisiert werden, fremde Personen nicht unbeaufsichtigt zu lassen.

Geschlossene Fenster und Türen (INF.10.A3)

Die Fenster und Türen der Besprechungs-, Veranstaltungs- und Schulungsräume müssen beim Verlassen verschlossen werden. In regelmäßigen Abständen muss geprüft werden, ob die Fenster und Türen nach Verlassen der Räume verschlossen wurden. Ebenso muss darauf geachtet werden, dass vorhandene Brand- und Rauchschutztüren tatsächlich geschlossen werden.

### Raum sowie Schrank für technische Infrastruktur

#### Planung der Raumabsicherung (INF.5.A1)

Für einen Raum für technische Infrastruktur müssen angemessene technische und organisatorische Vorgaben definiert und umgesetzt werden. Dabei muss der für den Raum ermittelte Schutzbedarf und hieraus abgeleitet, dass zu erreichende Schutzniveau berücksichtigt werden. Bei der Planung müssen sowohl gesetzliche Regelungen und Vorschriften als auch potenzielle Gefährdungen durch Umwelteinflüsse, Einbruch und Sabotage beachtet werden.

#### Lage und Größe des Raumes für technische Infrastruktur (INF.5.A2)

Der Raum für technische Infrastruktur darf kein Durchgangsraum sein. Es muss sichergestellt sein, dass ausreichend Fläche für Fluchtwege und Arbeitsfläche vorhanden ist.

#### Zutrittsregelung und -kontrolle (INF.5.A3)

Der Raum für technische Infrastruktur muss gegen unberechtigten Zutritt geschützt werden. Es muss geregelt werden, welche Personen für welchen Zeitraum, für welche Bereiche und zu welchem Zweck den Raum betreten dürfen. Dabei muss sichergestellt sein, dass keine unnötigen oder zu weitreichenden Zutrittsrechte vergeben werden. Alle Zutritte zum Raum für technische Infrastruktur sollten von der Zutrittskontrolle individuell erfasst werden.

#### Schutz vor Einbruch (INF.5.A4)

Der Raum muss entsprechend dem zu realisierenden Schutzniveau vor Einbruch geschützt werden. Je nach erforderlichem Sicherheitsniveau des Raumes für technische Infrastruktur sollten geeignete raumbildende Teile wie Wände, Decken und Böden sowie Fenster und Türen mit entsprechenden Widerstandsklassen nach DIN EN 1627 ausgewählt werden.

#### Vermeidung sowie Schutz vor elektromagnetischen Störfeldern (INF.5.A5)

Elektromagnetische Felder müssen in unmittelbarer Nähe zum Raum für technische Infrastruktur vermieden werden. Es muss ein ausreichender Abstand zu großen Maschinen wie z. B. Aufzugsmotoren eingehalten werden.

#### Minimierung von Brandlasten (INF.5.A6)

Brandlasten innerhalb und in der direkten Umgebung des Raumes für technische Infrastruktur müssen auf ein Minimum reduziert werden. Es muss auf brennbare Materialien für raumbildende Teile verzichtet werden.

#### Verhinderung von Zweckentfremdung (INF.5.A7)

Der Raum für technische Infrastruktur darf nicht zweckentfremdet werden.

## Standardmaßnahmen

Gemeinsam mit den Basismaßnahmen sind die folgenden Standardmaßnahmen zum Erzielen eines normalen Schutzbedarfs zu betrachten und sollten grundsätzlich umgesetzt werden.

### Allgemeines Gebäude

#### Sicherheitskonzept für die Gebäudenutzung (INF.1.A9)

Es sollte ein Sicherheitskonzept für die Gebäudenutzung als Bürogebäude erstellt, regelmäßig auf Aktualität und bei Bedarf aktualisiert werden. Das Sicherheitskonzept für das Gebäude sollte mit dem Gesamt-Sicherheitskonzept der <Institution> abgestimmt und regelmäßig aktualisiert werden.

#### Einhaltung einschlägiger Normen und Vorschriften (INF.1.A10)

Bei der Planung, der Errichtung und dem Umbau des Bürogebäudes sowie beim Einbau von technischen Einrichtungen sollten alle relevanten Normen und Vorschriften berücksichtigt werden.

#### Abgeschlossene Türen (INF.1.A11)

Beschäftigte im Bürogebäude sollten die Räumlichkeiten abschließen und sollten ihre Arbeitsunterlagen wegschließen, wenn sie den Raum verlassen und der Raum für unberechtigte Personen zugänglich ist. Es sollte sporadisch überprüft werden, ob diese Regelungen umgesetzt werden.

#### Schlüsselverwaltung (INF.1.A12)

Für alle Schlüssel des Bürogebäudes muss ein Schließplan vorliegen. Die Herstellung, Aufbewahrung, Verwaltung und Ausgabe von Schlüsseln sollten zentral geregelt werden. Reserveschlüssel sollten vorgehalten und gesichert, aber für Notfälle griffbereit aufbewahrt werden. Nicht ausgegebene Schlüssel sollten sicher aufbewahrt werden. Jede Schlüsselausgabe muss dokumentiert werden.

#### Regelungen für Zutritt zu Verteilern (INF.1.A13)

Der Zutritt zu den Verteilern aller Versorgungseinrichtungen in einem Bürogebäude muss im Bedarfsfall schnell möglich sein. Der Zutritt zu Verteilern muss auf einen engen Kreis von Berechtigten beschränkt sein.

#### Blitzschutzeinrichtungen (INF.1.A14)

Das Bürogebäude der <Institution> muss über einen Blitz- und Überspannungsschutz mit den folgenden Anforderungen verfügen:

* 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 das Bürogebäude sollten Blitzschutzzonen eingerichtet werden, die sich an den vorhandenen Sicherheitszonen orientieren.

#### Lagepläne der Versorgungsleitungen (INF.1.A15)

Es sollten aktuelle Lagepläne aller Versorgungsleitungen für das Bürogebäude der <Institution> existieren. Es sollte innerhalb der <Institution> geregelt sein, wer die Lagepläne aller Versorgungsleitungen führt und aktualisiert. Die Pläne sollten so aufbewahrt werden, dass ausschließlich berechtigte Personen darauf zugreifen können, sie aber im Bedarfsfall schnell verfügbar sind.

#### Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile (INF.1.A16)

Lagehinweise auf schutzwürdige Bereiche sollten innerhalb des Bürogebäudes vermieden werden. Schutzwürdige Gebäudebereiche dürfen von außen nicht leicht einsehbar sein.

#### Baulicher Rauchschutz (INF.1.A17)

Der bauliche Rauchschutz sollte nach Installations- und Umbauarbeiten überprüft werden. Es muss regelmäßig überprüft werden, ob die Rauchschutz-Komponenten noch funktionieren.

#### Brandschutzbegehungen (INF.1.A18)

Brandschutzbegehungen müssen mindestens ein- bis zweimal im Jahr stattfinden. Bei Brandschutzbegehungen sollten festgestellte Mängel unverzüglich behoben werden.

#### Frühzeitige Information des Brandschutzbeauftragten (INF.1.A19)

Die Brandschutzbeauftragten sollten über Arbeiten an Leitungstrassen, Fluren, Flucht- und Rettungswegen informiert werden. Die Brandschutzbeauftragten sollten die ordnungsgemäße Ausführung von Brandschutzmaßnahmen kontrollieren.

#### Alarmierungsplan und Brandschutzübungen (INF.1.A20)

Es muss ein Alarmierungsplan für die im Brandfall zu ergreifenden Maßnahmen erstellt werden. Der etablierte Alarmierungsplan sollte periodisch überprüft und bei Bedarf aktualisiert werden. Durch regelmäßige Brandschutzübungen sollten die im Brandfall zu ergreifenden Maßnahmen und der Alarmierungsplan verifiziert und bei Bedarf an aktuelle Erfordernisse angepasst werden.

### Büroarbeitsplatz

#### Fliegende Verkabelung (INF.7.A3)

Die Stromanschlüsse und Zugänge zum Datennetz (LAN) im Büroraum sollten sich in der Nähe des Ortes befinden, wo die IT-Geräte aufgestellt sind.

#### Zutrittsregelungen und -kontrolle (INF.7.A4)

Es sollte gewährleistet sein, dass Unberechtigte die Büroräume nicht betreten können. Hierfür sollte ein Konzept erstellt und umgesetzt werden. Regelmäßig sollte überprüft werden, ob die ergriffenen Maßnahmen wirksam sind.

#### Ergonomischer Arbeitsplatz (INF.7.A5)

Die Arbeitsplätze aller Mitarbeitenden sollten ergonomisch eingerichtet sein. Vor allem die Bildschirme müssen so aufgestellt sein, dass ein ergonomisches und ungestörtes Arbeiten möglich ist. Dabei sollte beachtet werden, dass Unbefugte Bildschirme der Mitarbeitenden nicht einsehen können. Die Bildschirmarbeitsschutzverordnung (BildscharbV) muss umgesetzt werden. Alle Arbeitsplätze sollten für eine möglichst fehlerfreie Bedienung der IT individuell verstellbar sein.

#### Aufgeräumter Arbeitsplatz (INF.7.A6)

Jeder Mitarbeitende sollte dazu angehalten werden, seinen Arbeitsplatz aufgeräumt zu hinterlassen. Benutzer sollten darauf achten, dass Unbefugte keinen Zugang zu IT-Anwendungen erhalten oder vertrauliche Informationen einsehen können. Alle Mitarbeitenden sollten angehalten werden, regelmäßig ihre Arbeitsplätze sorgfältig zu überprüfen und sicherzustellen, dass keine vertraulichen Informationen frei zugänglich sind. Vorgesetzte sollten sporadisch die Arbeitsplätze daraufhin überprüfen, ob schutzbedürftige Informationen offen zu gänglich sind.

#### Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger (INF.7.A7)

Die Mitarbeitenden sollten angewiesen werden, dass alle vertrauliche Dokumente und Datenträger verschlossen aufzubewahren, sofern diese nicht verwendet werden. In den Büroräumen oder in deren Umfeld sollten hierfür geeignete Behältnisse aufgestellt werden.

### Besprechungs-, Veranstaltungs- und Schulungsräume

#### Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen (INF.10.A4)

Bei der Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen sollte die Lage der Räume im Bürogebäude berücksichtigt werden. Insofern Besprechungs-, Veranstaltungs- und Schulungsräumen, ausschließlich von Besuchern oder zusammen mit Besuchern genutzt werden, sollten diese nicht in der Nähe von Räumen sein, in denen regelmäßig vertrauliche Informationen bearbeitet oder bereitgestellt werden. Es sollte für jeden bzw. übergreifen für alle Besprechungs-, Veranstaltungs- und Schulungsraum festgelegt werden, wie vertraulich die Informationen sein dürfen, die in diesen Räumen besprochen, bereitgestellt oder verarbeitet werden.

#### Fliegende Verkabelung (INF.10.A5)

Um eine fliegende Verkabelung zu vermeiden, sollten sich die Stromanschlüsse in den Besprechungs-, Veranstaltungs- und Schulungsräumen dort befinden, wo Beamer, Laptops oder andere Verbraucher aufgestellt werden. Zudem sollten Verkabelungen, die über den Boden verlaufen, geeignet abgedeckt oder besser durch einen Doppelboden geführt werden.

#### Einrichtung sicherer Netzzugänge (INF.10.A6)

In den Besprechungs-, Veranstaltungs- und Schulungsräumen sollte sichergestellt werden, dass mitgebrachte IT-Systeme der Besucher nicht über das Datennetz (LAN) mit internen IT-Systemen der <Institution> direkt verbunden wird.

#### Auf Informationen auf IT-Systemen im LAN der <Institution> sollten ausschließlich dafür vorgesehene und berechtigte IT-Systeme zugreifen können. Netzzugänge für Besucher müssen vom LAN der <Institution> mindestens logisch getrennt werden, um so ein unberechtigtes Mitlesen des internen Datenaustausch durch unberechtigte Dritte verhindern zu können.

Netzanschlüsse in Besprechungs-, Veranstaltungs- oder Schulungsräumen sollten so abgesichert werden, dass verhindert wird, dass IT-Systeme in Besprechungs-, Veranstaltungs- und Schulungsräumen gleichzeitig eine Verbindung zum Intranet der <Institution> und zum Internet aufbauen können.

Zusätzlich sollte die Stromversorgung aus einer Unterverteilung heraus getrennt von anderen Räumen aufgebaut werden.

#### Sichere Konfiguration von Schulungs- und Präsentationsrechnern (INF.10.A7)

Dedizierte Schulungs- und Präsentationsrechner sollten mit einer Minimalkonfiguration versehen werden. Es sollte festgelegt sein, welche Anwendungen auf Schulungs- und Präsentationsrechnern in der jeweiligen Veranstaltung genutzt werden können. Die Schulungs- und Präsentationsrechner sollten nur an ein separates, vom LAN der <Institution> getrenntes VLAN angeschlossen werden. Auf alle anderen Netze der <Institution> sollte nur restriktiv zugegriffen werden können.

#### Erstellung eines Nutzungsnachweises für Räume (INF.10.A8)

Je nach Nutzungsart der Besprechungs-, Veranstaltungs- und Schulungsräume sollte ersichtlich sein, wer die Räume zu welchem Zeitpunkt genutzt hat. Für Räumlichkeiten, in denen Schulungen an IT-Systemen oder besonders vertrauliche Besprechungen durchgeführt werden, sollten ebenfalls Nutzungsnachweise erstellt werden. Es sollte überlegt werden, für Besprechungs-, Veranstaltungs- und Schulungsräume, die für jeden Mitarbeiter zugänglich sind, ebenfalls entsprechende Nutzungsnachweise einzuführen.

### Raum sowie Schrank für technische Infrastruktur

#### Vermeidung von unkontrollierter elektrostatischer Entladung (INF.5.A8)

Im Raum für technische Infrastruktur sollte ein ableitfähiger Fußbodenbelag nach DIN EN 14041 verlegt werden.

#### Stromversorgung (INF.5.A9)

Die Energieverteilung des Gebäudes, in dem sich der Raum für technische Infrastruktur befindet, sollten als TN-S- System ausgeführt sein.

#### Einhaltung der Lufttemperatur und -feuchtigkeit (INF.5.A10)

Es sollte sichergestellt werden, dass die Lufttemperatur und Luftfeuchtigkeit im Raum für technische Infrastruktur innerhalb der Grenzen liegen, die in den Datenblättern der darin betriebenen Geräte genannt sind. Dafür sollte eine geeignete raumlufttechnische Anlage eingesetzt werden. Diese sollte ausreichend dimensioniert sein.

#### Vermeidung von Leitungen mit gefährdenden Flüssigkeiten und Gasen (INF.5.A11)

Im Raum für technische Infrastruktur sollte es nur Leitungen geben, die für den Betrieb der Technik im Raum unbedingt erforderlich sind. Leitungen wie Abwasserleitungen, Frischwasserleitungen, Gas- und Heizungsrohre sowie Leitungen für Treibstoff oder Ferndampf sollten nicht durch den Raum geführt werden.

#### Schutz vor versehentlicher Beschädigung von Zuleitungen (INF.5.A12)

Zuleitungen wie z. B. Schutzrohre oder Kabelkanäle außerhalb des Raumes für technische Infrastruktur sollten gegen versehentliche Beschädigung geschützt werden.

#### Schutz vor Schädigung durch Brand und Rauchgase (INF.5.A13)

Unabhängig von den für den Raum geltenden baurechtlichen Brandschutz-Vorgaben sollten alle raumbildenden Teile sowie Türen und Fenster gleichwertig rauchdicht sein. Sie sollten Feuer und Rauch für mindestens 30 Minuten standhalten. Brandlasten im Bereich der Leitungstrassen sollten vermieden werden.

#### Minimierung von Brandgefahren aus Nachbarbereichen (INF.5.A14)

Der Raum sollte nicht in unmittelbarer Nähe zu anderen Räumlichkeiten mit brennbaren Materialien liegen.

#### Blitz- und Überspannungsschutz (INF.5.A15)

Es sollte ein Blitz- und Überspannungsschutzkonzept nach dem Prinzip der energetischen Koordination (siehe DIN EN 62305) erstellt und umgesetzt werden. Der Raum für technische Infrastruktur sollte mindestens der Blitzschutzzone 2 (LPZ 2) zugeordnet werden. Die Blitz- und Überspannungsschutzeinrichtungen sollten regelmäßig und anlassbezogen auf ihre Funktion überprüft und, falls erforderlich, ersetzt werden.

#### Einsatz einer unterbrechungsfreien Stromversorgung (INF.5.A16)

Es sollte geprüft werden, welche Geräte an einer USV angeschlossen werden sollen. Falls eine USV erforderlich ist, sollte die Stützzeit der USV so ausgelegt sein, dass alle versorgten Komponenten sicher herunterfahren können. Es sollte berücksichtigt werden, dass die Batterien von USV-Anlagen altern.

Bei relevanten Änderungen sollte überprüft werden, ob die vorhandenen USV-Anlagen noch ausreichend dimensioniert sind. Die Batterie der USV sollte im erforderlichen Temperaturbereich gehalten werden.

Die USV sollte regelmäßig gewartet und auf Funktionsfähigkeit getestet werden. Dafür sollten die vom Hersteller vorgesehenen Wartungsintervalle eingehalten werden.

Inspektion und Wartung der Infrastruktur (INF.5.A17)

Für alle Komponenten der baulich-technischen Infrastruktur sollten mindestens die vom Systemhersteller empfohlenen oder durch Normen festgelegten Intervalle und Vorschriften für Inspektion und Wartung eingehalten werden. Kabel- und Rohrdurchführungen durch brand- und rauchabschnittbegrenzende Wände sollten daraufhin geprüft werden, ob die Schotte normgerecht und unversehrt sind. Inspektionen und Wartungsarbeiten müssen geeignet protokolliert werden.

## Maßnahmen bei erhöhtem Schutzbedarf

Gemeinsam mit den Basismaßnahmen und den Standardmaßnahmen sind zum Erzielen eines erhöhten Schutzbedarfs die hier aufgeführten Maßnahmen zu betrachten und sollten grundsätzlich umgesetzt werden. Ist dies aus wirtschaftlichen bzw. organisatorischen Gründen nicht möglich, so ist dies mit dem Sicherheitsmanagement zur weiteren Begegnung von Risiken für die Infrastruktur der <Institution> zu begründen und abzustimmen. Im Folgenden werden die Maßnahmen bei erhöhtem Schutzbedarf aufgeführt. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

### Allgemeines Gebäude

#### Unabhängige elektrische Versorgungsstränge (INF.1.A21 - A)

Die IT-Systeme im Bürogebäude sollten über zwei voneinander unabhängige Versorgungsstränge gespeist werden.

#### Sichere Türen und Fenster (INF.1.A22 - A)

Das System der Einbruchhemmung sollte wie eine Kette wirken und ist nur so gut wie das schwächste Glied. Aus diesem Grunde muss die Einbruchshemmung bereits bei der Gebäudeplanung beginnen. Der Zutritt zum Bürogebäude sollte über einen Haupteingang erfolgen, der in den Geschäftszeiten mit einem Empfangsdienst besetzt sein sollte. An kleineren Standorten kann auf den Empfangsdienst verzichtet werden, wenn die nachfolgenden Regelungen eingehalten werden.

* Der Außenbereich eines Bürogebäudes wird vom Innenbereich mit einer auch dauerhaft verschließbaren Tür abgeschottet.
* Die Tür und etwaige Fenster in den leicht zugänglichen Etagen des Bürogebäudes werden entsprechend der geltenden Normen (DIN EN 1627:2010-09) ausgelegt und verfügt über eine hohe bis sehr hohe Widerstandsklasse. Hieraus ableitend muss in der Kette der zu durchquerenden Türen, um in die Räumlichkeiten des Bürogebäudes und an die IT-System zu gelangen mindestens ein 20-minütiger Einbruchswiderstand realisiert werden.
* Ein Zutritt von Personen erfolgt nur nach erfolgreicher Zutrittskontrolle (personalisierte Zugangskarten).
* Jeder Mitarbeitende des Bürogebäudes ist zur Einhaltung und Überwachung dieser Richtlinie zu verpflichten.

#### Bildung von Sicherheitszonen (INF.1.A23 - A)

Räume ähnlichen Schutzbedarfs sollten in Sicherheitszonen zusammengefasst werden, um vergleichbare Risiken einheitlich behandeln und Kosten für erforderliche Sicherheitsmaßnahmen reduzieren zu können. Es muss ein Sicherheitszonenkonzept für Gebäude und Grundstück entwickelt und dokumentiert werden.

#### Selbsttätige Entwässerung (INF.1.A24 - A)

Alle von Wasser gefährdeten Bereiche sollten mit einer selbsttätigen Entwässerung ausgestattet sein. Es sollte regelmäßig geprüft werden, ob die aktiven und passiven Entwässerungseinrichtungen noch funktionieren.

#### Geeignete Standortauswahl (INF.1.A25 - A)

Wird ein Bürogebäudestandort geplant oder ausgewählt, muss geprüft werden, welche Bedingungen aus dem Umfeld Einfluss auf die Informationssicherheit haben könnten. Es sollte eine Übersicht über standortbedingte Gefährdungen geben. Diesen Gefährdungen müssen mit zusätzlichen kompensierenden Maßnahmen entgegengewirkt werden.

#### Pförtner- oder Sicherheitsdienst (INF.1.A26 - A)

Die Aufgaben des Pförtner- bzw. Sicherheitsdienstes sollten klar dokumentiert sein. Die Pförtner sollten alle Personenbewegungen an der Pforte und an allen anderen Eingängen beobachten bzw. kontrollieren. Alle Mitarbeiter und Besucher des Bürogebäudes sollten sich bei den Pförtnern ausweisen können. Besucher sollten zu den Besuchten begleitet bzw. an der Pforte abgeholt werden. Die Pförtner sollten über die etablierten Prozesse rechtzeitig darüber informiert werden, wenn sich Zutrittsberechtigungen ändern.

#### Einbruchschutz (INF.1.A27 - A)

Es sollten ausreichende und den örtlichen Gegebenheiten angepasste Maßnahmen zum Einbruchschutz umgesetzt werden. Bei der Planung, der Umsetzung und im Betrieb sollte beim Einbruchschutz darauf geachtet werden, dass er gleichwertig und durchgängig ist. Hieraus ableitend muss in der Kette der zu durchquerenden Türen, um in die Räumlichkeiten des Bürogebäudes und an die IT-System zu gelangen mindestens ein 20-minütiger Einbruchswiderstand realisiert werden.

Der Einbruchswiderstand sollte regelmäßig durch fachkundige Personen begutachtet und dokumentiert werden.

#### Klimatisierung durch raumlufttechnische Anlagen (INF.1.A28 - A)

In Rechenzentren sollte die Luftversorgung durch raumlufttechnische Anlagen (RLT-Anlagen) sichergestellt werden. Die RLT-Anlagen sollten auf die tatsächliche Nutzung und Wärmelast des Bürogebäudes ausgelegt und regelmäßig gewartet werden.

#### Organisatorische Vorgaben für die Gebäudereinigung (INF.1.A29 - CI)

Es muss kontrolliert werden, ob die Verantwortlichen Mitarbeiter für die Reinigung bzw. die Mitarbeiter der beauftragten Reinigungsfirma die ausgegebenen Zutrittsmittel (bspw. RFID-Karten, Schlüssel bzw. Ausweise) vertragsgemäß verwenden. Die Reinigungskräfte sollten über den Umgang mit der IT ausreichend informiert sein. Reinigungskräfte müssen in besonders sensitiven Bereichen des Bürogebäudes bei der Arbeit beaufsichtigt werden.

### Büroarbeitsplatz

#### Einsatz von Diebstahlsicherungen (INF.7.A8 - CA)

Insofern der Zutritt zu Räumen nicht geeignet beschränkt werden kann, sollten für alle IT-Systeme Diebstahlsicherungen eingesetzt werden. In Bereichen mit Publikumsverkehr muss generell eine Diebstahlsicherung genutzt werden.

### Besprechungs-, Veranstaltungs- und Schulungsräume

#### Zurücksetzen von Schulungs- und Präsentationsrechnern (INF.10.A9 - CA)

Es sollte ein Verfahren festgelegt werden, um Schulungs- und Präsentationsrechner nach der Nutzung auf einen vorher definierten Zustand zurückzusetzen. Durch Benutzer vorgenommene Änderungen sollten dabei vollständig entfernt werden.

#### Mitführverbot von Mobiltelefonen (INF.10.A10 - C)

Mobiltelefone/Smartphones sollten nicht zu streng vertraulichen Besprechungen und Gesprächen mitgeführt werden. Falls erforderlich, sollte dies durch Mobilfunk-Detektoren überprüft werden.

### Raum sowie Schrank für technische Infrastruktur