



Sec-IT

**Mehr Sicherheit.
Mehr Wert.**

Anforderungskatalog

zur Bewertung und Zertifizierung von Rechenzentren

Version 1.1
Stand: 15.05.2014

© TÜV SÜD Sec-IT GmbH

Autor: Marko Hoffmann

Sitz: München
Amtsgericht München HRB 197 698
USt-IdNr. DE282283450
Informationen gemäß § 2 Abs. 1 DL-InfoV
unter www.tuev-sued.de/impressum

Geschäftsführer:
Herbert Huß

Telefon: +49 89 5791-3894
Telefax: +49 89 5155-1097
www.tuev-sued.de

TÜV[®]

TÜV SÜD Sec-IT GmbH
Ridlerstraße 65
80339 München
Deutschland



Inhalt

1	Organisatorische Anforderungen:	4
1.1	Verpflichtung auf die Anforderungen	4
1.2	Vermittlung der Anforderungen	4
1.3	Festlegung von Verantwortlichkeiten	4
1.4	Einsatz wirksamer Verfahren	4
1.5	Bereitstellung der erforderlichen Mittel	4
1.6	Bewertung der Konformität	4
1.7	Ständige Verbesserung	4
1.8	Lenkung von Dokumenten	4
1.9	Notfall- und Störungsmanagement	4
1.10	Risikomanagement	4
1.11	Dokumentation	5
1.12	Erreichbarkeit	5
1.13	Geplante Serviceunterbrechungen	5
1.14	Löschung und Vernichtung von Daten	5
2	Personelle Anforderungen	5
2.1	Rollen- bzw. Stellenbeschreibungen	5
2.2	Schulung	5
2.3	Recruiting, Eintritt, Änderung und Austritt von Mitarbeitern	5
2.4	Betriebsfremde Personen	6
3	Anforderungen an das Gebäude	6
3.1	Standort	6
3.2	Gebäudestruktur, Bauweise	6
3.3	Zutritt	6
3.4	Alarmsystem	6
3.5	Wartung, Dokumentation	6
4	Kommunikation	6
5	Stromversorgung	7
5.1	Auslegung, Planung, Ausführung	7
5.2	Netzeinspeisung, interne Versorgung	7
5.3	Notfallversorgung: USV, NEA	7
5.4	Monitoring und Dokumentation	7
5.5	Test und Wartung	7
6	Klima und Lüftung	7
6.1	Auslegung	7
6.2	Planung, Ausführung	7
6.3	Ausfallsicherheit	8
6.4	Monitoring und Dokumentation	8
6.5	Test und Wartung	8



Sec-IT

7	Brandschutz	8
7.1	Branderkennung und –meldung	8
7.2	Brandbekämpfung	8
7.3	Test, Wartung und Dokumentation.....	8
8	Blitzschutz/Potentialausgleich	8



1 Organisatorische Anforderungen

1.1 Verpflichtung auf die Anforderungen

Die für das Rechenzentrum und die dazugehörigen Geschäftsprozesse verantwortlichen Mitarbeiter verpflichten sich, alle Anforderungen aus diesem Katalog und alle relevanten gesetzlichen Bestimmungen zu erfüllen. Sie weisen die Übernahme dieser Verantwortung durch geeignete Maßnahmen nach.

1.2 Vermittlung der Anforderungen

Die in diesem Katalog aufgeführten Anforderungen werden in der Organisation allen davon betroffenen Mitarbeitern in angemessener Art und Weise vermittelt.

1.3 Festlegung von Verantwortlichkeiten

Zur Erfüllung aller Anforderungen sind Verantwortlichkeiten und Befugnisse in der Organisation vollständig und eindeutig festgelegt. Es existiert eine angemessene Stellvertreterregelung. Der Aufbau der Organisation ist dokumentiert.

1.4 Einsatz wirksamer Verfahren

Es sind Verfahren wirksam, die geeignet sind, die Anforderungen in der Organisation umzusetzen.

1.5 Bereitstellung der erforderlichen Mittel

Die notwendigen und geeigneten Mittel zur Erfüllung der Anforderungen werden bereitgestellt (z.B. geschultes Personal, erforderliche Infrastruktur).

1.6 Bewertung der Konformität

Die Organisation bewertet regelmäßig ihre Konformität bzgl. der Anforderungen, um deren Einhaltung nachhaltig sicherzustellen.

1.7 Ständige Verbesserung

Das Ergebnis der Bewertung von Kundenzufriedenheit und Konformität zu diesem Anforderungskatalog wird zur ständigen Verbesserung der Organisation verwendet.

1.8 Lenkung von Dokumenten

Das Unternehmen verwendet eine Dokumentenlenkung für betriebswichtige Dokumente und Aufzeichnungen, aus der zumindest Ersteller und Datum oder Revision des Dokuments / der Aufzeichnung hervorgehen.

1.9 Notfall- und Störungsmanagement

Um Schäden aus Störungen und Notfällen zu minimieren gibt es ein Konzept zum Umgang mit Störungen und Notfällen. Es enthält unter anderem Eskalationspläne, die auch die Kundenkommunikation abdecken. Die Eskalationspläne werden regelmäßig getestet, Auftretende Störungen und Notfälle sowie die daraufhin eingeleiteten Maßnahmen werden aufgezeichnet.

1.10 Risikomanagement

Die Organisation führt regelmäßig eine Risikoanalyse durch, in der die Risiken für den Betrieb des Rechenzentrums beschrieben sind und entsprechende Maßnahmen zur Beherrschung der Risiken zugeordnet werden. Das Restrisiko ist von der Leitung der Organisation zu freizugeben.



1.11 Dokumentation

Der Betrieb des Rechenzentrums wird dokumentiert. Dabei sind unter anderem folgende Dokumente zu führen:

- a) Betriebshandbücher oder adäquate Beschreibungen, die die grundlegenden Prozesse und Verfahren zum Betrieb des Rechenzentrums beschreiben.
- b) Weiterführende Dokumentation für wichtige Prozesse und Verfahren.
- c) Service-Level-Agreements mit Lieferanten
- d) Service-Level-Agreements mit Kunden
- e) Ein Verfahren zur geregelten Durchführung von Änderungen an Infrastruktur und Anlagen („Changemanagement“)
- f) Ein reaktives Incidentmanagement, das Sicherheitsvorfälle sowie Betriebsstörungen und Notfälle aufzeichnet und deren Behebung dokumentiert.
- g) Ein Kennzahlensystem mit Monitoring der SLA-Vorgaben aufgrund definierter Schwellwerte wird verwendet. Wesentliche Kennzahlen werden regelmäßig ausgewertet.

1.12 Erreichbarkeit

Betriebspersonal des Rechenzentrums ist rund um die Uhr („24/7“) erreichbar. Dies kann durch ständig besetzte Stellen oder durch Bereitschaftsdienste umgesetzt werden.

1.13 Geplante Serviceunterbrechungen

Notwendige Serviceunterbrechungen („Downtime“) werden geplant und internen Stellen sowie Kunden mit angemessener Vorlaufzeit mitgeteilt. Entsprechende Vorgaben sind definiert und dokumentiert.

1.14 Löschung und Vernichtung von Daten

Die Löschung und Vernichtung von Daten auf Papier oder Datenträgern läuft nach einem definierten Verfahren ab.

2 Personelle Anforderungen

2.1 Rollen- bzw. Stellenbeschreibungen

Die Verantwortung, Rechte und Pflichten sowie Vertretungsregelungen der Stelleninhaber müssen in entsprechenden Rollen- bzw. Stellenbeschreibungen klar definiert sein. Bei Entscheidungsträgern sind darüber hinaus auch die Befugnisse zu definieren.

2.2 Schulung

Der Schulungsbedarf der Mitarbeiter wird regelmäßig und systematisch festgestellt. Notwendige Schulungen werden durchgeführt und die Teilnahme daran dokumentiert. Außerdem wird der Erfolg von Schulungsmaßnahmen bewertet.

2.3 Recruiting, Eintritt, Änderung und Austritt von Mitarbeitern

Für auszuscribende Stellen existieren Anforderungsprofile. Bewerber werden hinsichtlich Ihrer Eignung für einen Einsatz in sicherheitskritischen Bereichen überprüft.

Es existiert ein definiertes Verfahren für Eintritt, Änderung und Austritt von Mitarbeitern. Darin ist eine geregelte Einschulung und Vergabe von Benutzerrechten berücksichtigt. Zur Nutzung überlassene Unternehmenswerte werden dokumentiert.



2.4 Betriebsfremde Personen

Der Aufenthalt von Kunden, Technikern, Fremdpersonal und Besuchern ist nachvollziehbar und erkennbar dokumentiert. Betriebsfremde Personen werden vor Betreten über notwendige Verhaltensregeln belehrt und vor dem Betreten von Sicherheitsbereichen angemessen überprüft. Techniker und Fremdpersonal erhalten Berechtigungen nur zeitlich befristet und nur soweit zur Erfüllung der Aufgaben notwendig. Besucher werden dauerhaft von einem Mitarbeiter oder einer berechtigten Person begleitet.

3 Anforderungen an das Gebäude

3.1 Standort

In der Risikobewertung (siehe 1.10) müssen geographische Risiken und nachbarliche Risiken enthalten sein (z.B. Risiken durch Hochwasser, Erdbeben, Flugverkehr, Explosionsgefährdungen, politische Risiken etc.)

3.2 Gebäudestruktur, Bauweise

Die Gebäudestruktur ist dem Zweck angemessen, unterschiedliche Funktionsbereiche sind räumlich getrennt, für Sicherheitszonen existiert ein angemessenes Konzept. Das Gebäude bietet einen grundlegenden EMV-Schutz (Faradayscher Käfig). Es gibt redundante Gebäudezugänge und zugehörige Sicherheitskontrollen.

Die Außenwände der IT-Fläche sind fensterlos. Bereiche unterschiedlicher Kunden sind durch geeignete Maßnahmen voneinander zugriffssicher getrennt. Für die Aufstellung von USV/Batteriesystem, Netzersatzanlage und IT-Racks gibt es entsprechende Eignungsnachweise bezüglich der Gebäudestatik.

3.3 Zutritt

Für den Notfall existieren zugängliche Parkplätze für Betriebspersonal bzw. Notdienst.

Der Zutritt zur IT-Fläche ist nur über die Authentisierung mit zwei unabhängigen Merkmalen möglich. (Zum Verlassen der IT-Fläche muss mindestens eines der Merkmale verwendet werden.)

Das Rechenzentrum verfügt über einen Zutrittsschutz, der in die Gebäudetechnik integriert ist und der Zutritte / verweigerte Zutritte, Verlassen / verweigertes Verlassen protokolliert.

Der Zutritt ist so zu regeln, dass jede Person bei Zutritt und Verlassen der IT-Fläche erfasst wird (z.B. über Vereinzelungsanlage, Videoaufzeichnung, Foto)

3.4 Alarmsystem

Das Rechenzentrum verfügt über eine an die Gebäudetechnik angeschlossene Einbruchmeldeanlage mit Alarmierung an 24/7 erreichbare Ziele.

3.5 Wartung, Dokumentation

Gebäudestruktur, Raumaufteilung und Gebäudetechnik sind auf aktuellem Stand dokumentiert. Die Gebäudetechnischen Einrichtungen werden regelmäßig getestet. Alle Anlagen und Einrichtungen der Gebäudetechnik werden regelmäßig und geplant gewartet.

4 Kommunikation

Die Kommunikationseinrichtungen des Rechenzentrums werden über die USV-Anlage notgespeist. Zueinander redundante Bereitstellungsanlagen werden redundant mit Energie versorgt. Die Anbindung an öffentliche Netze findet an mindestens zwei getrennten POPs statt. Eingangsleitungen in das Gebäude sind räumlich getrennt.



5 Stromversorgung

5.1 Auslegung, Planung, Ausführung

Ein Stromversorgungskonzept mit Ziel- und Zweckdefinition muss vorhanden sein, das für USV und NEA mindestens beinhaltet: Planungsunterlagen mit Redundanznachweisen, Prüfnachweise der geplanten Anlagen (Typ- und Stückprüfprotokolle), Schutzselektivitätsbetrachtungen für redundante Systeme. Energieverteiler und Leitungsführungen sind fachgerecht ausgeführt, wartungsfreundlich und gut erreichbar und bieten Reserven für Erweiterungen

5.2 Netzeinspeisung, interne Versorgung

An das öffentliche Stromnetz ist das Rechenzentrum mit einer n+1-Redundanz angebunden. Ein offener Ring wird hierbei akzeptiert. Versorgungsleitungen sind räumlich getrennt unterirdisch verlegt. Interne Versorgungsleitungen und Verteiler sind n+1-redundant ausgelegt, klima- und lüftungstechnische Anlagen werden n+1-redundant versorgt. Alle redundanten Systeme werden räumlich getrennt installiert. IT-Racks werden redundant versorgt.

5.3 Notfallversorgung: USV, NEA

Eine USV mit n+1-Redundanz ist vorhanden. Die USV ist nach EN 62040, das Batteriesystem nach EN 50272-2 ausgelegt.

Eine inselbetriebsfähige NEA nach IS 8528 mit n+1-Redundanz ist vorhanden. Die Redundanz kann z.B. durch Anschlussmöglichkeit für eine mobile NEA erreicht werden.

5.4 Monitoring und Dokumentation

Die Anlagen der Stromversorgung sind dokumentiert, die Dokumentation ist auf aktuellem Stand und beinhaltet unter anderem Zuleitung, Beschriftung, Kabelführung, Kennzeichnungen von Anlagen und Geräten.

An den Anlagen vor Ort und an zentraler Stelle sind aktuelle Kennzahlen ablesbar (Auslastung, USV-Kapazität, Phasenverteilung etc.)

5.5 Test und Wartung

Die Anlagen zur Sicherung der Energieversorgung werden je nach technischen Anforderungen regelmäßig getestet, die Testergebnisse sind zu dokumentieren und zu bewerten. Dabei erfolgt eine NEA Funktionsprobe monatlich, Tests von Umschalteneinrichtungen halbjährlich, sowie ein Black-Building-Test jährlich. Wartungen der Stromversorgung finden geplant und regelmäßig statt.

6 Klima und Lüftung

6.1 Auslegung

Das Klimatisierungssystem ist insgesamt n+1-redundant ausgelegt. Redundante Systeme sind räumlich getrennt, Redundanz kann ggf. auch durch Anschlussmöglichkeit für mobile Kälte hergestellt werden. Anlagen und Leitungsnetz sind mit Leckageerkennungssysteme und Kondenswasserführungen ausgestattet, das Rohrleitungssystem ggf. räumlich getrennt.

6.2 Planung, Ausführung

Ein Klimatisierungskonzept mit Ziel- und Zweckdefinition muss vorhanden sein, das für Kälte- und Lüftungsanlagen mindestens beinhaltet: Planungsunterlagen mit Redundanznachweisen, Prüfnachweise der geplanten



Anlagen (Typ- und Stückprüfprotokolle) Anlagen und Leitungsführungen sind fachgerecht ausgeführt, wartungsfreundlich und gut erreichbar und bieten Reserven für Erweiterungen

6.3 Ausfallsicherheit

Bei Ausfall der Gebäudeleittechnik muss nachweisbar ein Weiterbetrieb des Rechenzentrums erfolgen. Die Anlagen zu Kälte- und Lüftungsversorgung können auch ohne Gebäudetechnik manuell gesteuert werden. Steuerungsanlagen sind per redundanter USV abgesichert.

6.4 Monitoring und Dokumentation

Die Anlagen der Klimatisierung sind dokumentiert, die Dokumentation ist auf aktuellem Stand und beinhaltet unter anderem Zuleitung, Beschriftung, Kabelführung, Kennzeichnungen von Anlagen und Geräten.

An den Anlagen vor Ort und an zentraler Stelle sind aktuelle Kennzahlen und Anlagenbetriebszustände ablesbar und zumindest vor Ort einstellbar (Luftfeuchtigkeit und Temperatur). Bei Über-/Unterschreitung von Vorgabewerten wird eine besetzte Stelle alarmiert.

6.5 Test und Wartung

Die Anlagen zur Klimatisierung werden regelmäßig je nach technischer Anforderung getestet, die Testergebnisse sind zu dokumentieren und zu bewerten. Dabei wird die Umschaltung der Kälteanlagen halbjährlich getestet. Hinsichtlich Laufzeiten der Anlagen werden Hygieneverordnungen beachtet und ein Betriebsstundenmanagement eingesetzt. Wartungen der Klimatechnik finden geplant und regelmäßig statt

7 Brandschutz

Sämtliche gesetzlichen, behördlichen und versicherungstechnischen Brandschutzvorgaben werden eingehalten. Die Brandschutzausstattung des Gebäudes erfüllt die Empfehlungen des Bitkom-Leitfadens „Betriebssichere Rechenzentren“, Kapitel 6.2.3, Kategorie C.

7.1 Branderkennung und –meldung

Eine Brandmeldeanlage nach DIN 14675 ist in Betrieb. Die Erkennung erfolgt mit Sensoren zur Brandfrüherkennung, dabei ist eine Zweimelder-Abhängigkeit umgesetzt. Die Alarmierung erfolgt über die Gebäudetechnik an eine ständig besetzte Stelle.

7.2 Brandbekämpfung

Eine Brandlöschanlage mit geeignetem Löschmittel ist vorhanden. Alternativ kann durch eine Brandvermeidungsanlage / Sauerstoffreduzierungsanlage das Schutzziel erreicht werden.

7.3 Test, Wartung und Dokumentation

Die Brandschutzanlagen sind dokumentiert, die Dokumentation ist auf aktuellem Stand. Wartungen der Brandschutztechnik finden geplant und regelmäßig statt. Die Anlagen zum Brandschutz werden regelmäßig entsprechend bauaufsichtlichen Vorgaben getestet, die Testergebnisse sind zu dokumentieren und zu bewerten.

8 Blitzschutz/Potentialausgleich

Ein Blitzschutzkonzept ist vorhanden, das auch einen EMV-Schutz berücksichtigt. Hierbei werden die verschiedenen Blitzschutz zonen im Rechenzentrum unterschieden.

Ein Blitzschutzsystem nach EN 62305 Teil 1 bis 4 ist vorhanden, es beinhaltet außerdem einen EMV-gerechten Potentialausgleich. Der



Sec-IT

Potentialausgleich für die IT-Anlagen erfolgt
gemäß EN 50310