

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH
bescheinigt hiermit dem Unternehmen

Flughafen München GmbH
Nordallee 25
85356 München

für den Sicherheitsbereich

Rechenzentrum RZ1

die Erfüllung aller Anforderungen für erweiterten Schutzbedarf des
Prüfkatalogs

Trusted Site Infrastructure TSI V2.0
Level 2 (erweitert)

der TÜV Informationstechnik GmbH. Die Anforderungen sind in der
Anlage zum Zertifikat zusammenfassend aufgelistet.

Die Anlage ist Bestandteil des Zertifikats und besteht aus 4 Seiten.

Dieses Zertifikat gilt nur in Verbindung mit dem zugehörigen
Prüfbericht, Version 1.1 vom 11.02.2008.

Dieses Zertifikat ist bis zum 31.12.2009 gültig.



Zertifikat-Registrier-Nr.:
TUVIT-TSI6645.08

Essen, 11.02.2008

gez. Dr. Sutter
Zertifizierungsstelle

TÜV Informationstechnik GmbH
Unternehmensgruppe TÜV NORD
Langemarckstraße 20
45141 Essen
www.certuvit.de

Zertifikat

Prüfbericht

TÜV[®]

Prüfbericht – Trusted Site Infrastructure zum Rechenzentrum RZ1 der Flughafen München GmbH, Version 1.1 vom 11.02.2009, TÜV Informationstechnik GmbH

Prüfergebnis

Das Ergebnis lautet „Level2 (erweitert)“. Hierbei werden in den Bewertungsaspekten ENV, FIR, SEC und ORG alle Anforderungen des nächst höheren Levels erreicht.

Prüfanforderungen

Zusammenfassung der Anforderungen für Trusted Site Infrastructure (TSI), Version 2.0

1 Umfeld (ENV – Environment)

Gefährdungspotenziale aus dem Umfeld sind zu meiden. Die Standortentscheidung des Objekts ist u.a. unter den Gesichtspunkten Wasser-, Explosions-, Trümmer-, Erschütterungs- und Schadstoffgefährdung zu treffen.

2 Bauliche Gegebenheiten (CON – Construction)

Die Gebäudekonstruktion sowie Fenster und Türen bieten einen Zutritts-, Brand- und Trümmerschutz. Das Gebäude ist gegen Blitzeinschlag geschützt. Der Sicherheitsbereich liegt abseits öffentlicher Zugänge und gefährlicher Produktionsprozesse und bildet einen eigenen Brandabschnitt. Die Trassenverläufe im Gebäude sind abgesichert. Eine Trennung zwischen Grob- und Feintechnik ist erfolgt.

3 Brandmelde- und Löschtechnik (FIR – Fire Prot. / Alarm / Extinguishing Systems)

TÜV®

Eine Brandmeldeanlage ist im gesamten Sicherheitsbereich installiert und bei der Feuerwehr aufgeschaltet. Benachbarte Räume, doppelter Fußboden, abgehängte Decken und Luftkanäle sind in die Brandüberwachung einbezogen. Neben der Alarmierung werden Abschaltfunktionen und Schadensbegrenzungsmaßnahmen ausgelöst, z.B. durch eine Gaslöschanlage. Eine zusätzliche Versorgung mit geeigneten Handfeuerlöschern ist gegeben.

4 Sicherheitssysteme (SEC – Security)

Es existiert eine Zugangskontrollanlage (ZKA). Ein Einbruchschutz ist mehrstufig gegeben, dabei werden alle sicherheitskritischen Bereiche mittels einer Einbruchmeldeanlage überwacht. Die Anlage ist notstromversorgt und durchgeschaltet zu einer ständig besetzten Sicherheitszentrale.

5 Energieversorgung (POW – Power Supply)

Der Nachweis einer nach einschlägigen DIN-Normen und VDE-Vorschriften erfolgten Elektroinstallation ist erbracht. Es existieren angepasste Aufteilungen und Absicherungen der Stromkreise. Sie sind gegen Überspannung geschützt. Eine Notstromversorgung der IT- wie auch der Sicherheitssysteme ist gegeben.

6 Raumluftechnische Anlagen (ACV – Air Conditioning and Ventilation)

Die Abwärme der IT-Geräte wie auch der Infrastrukturkomponenten wird durch Kühlung hinreichend abgefangen. Ein Staubschutz und die Einhaltung von Luftfeuchtwerten sind gegeben. Feuer- und Rauchklappen sind gemäß Brandschutzkonzept eingebaut. Die Einhaltung der Klimavorgaben werden fernüberwacht. Ausfälle sind durch eine redundante Auslegung abgefangen.

7 Organisation (ORG – Organization)

Alle Sicherheitseinrichtungen werden einem regelmäßigen Funktionstest unterzogen. Regelmäßige Wartungen an Verschleißteilen der Infrastrukturkomponenten bzw. IT-Hardware sind in einem Wartungsplan festgelegt. Die Kommunikation nach draußen ist auch beim Ausfall der TK-Anlage sichergestellt. Die Datensicherungsmedien werden brand- und zugriffsgeschützt getrennt vom Sicherheitsbereich aufbewahrt.

8 Dokumentation (DOC – Documentation)

Es existiert eine Dokumentation der Infrastrukturmaßnahmen (DIM) bzw. ein Sicherheitskonzept. Ebenso gibt es Regelungen für das Zugangskontrollsystem, das Zutrittsberechtigte definiert und die Verfahren zur Ausgabe der Schlüssel, Codekarten, etc. beschreibt. Lagepläne für das Gebäude und alle Infrastrukturkomponenten liegen vor. Ein mit der Feuerwehr abgestimmtes Brandschutzkonzept ist vorhanden. Ein Notfallkonzept bzw. Alarmplan liegen vor.

L Level

- Level1 Mittlerer Schutzbedarf (entspricht den Infrastrukturanforderungen der BSI Grundschutzkataloge)
- Level2 Erweiterter Schutzbedarf (mit ergänz. Anforderungen bei o.g. Bewertungsaspekten)
- Level3 Hoher Schutzbedarf (vollständige Redundanzen kritischer Versorgungssysteme – No Single Point of Failures, klimatische Grenzwerteinhaltung gem. EN 1047-2)
- Level4 Sehr hoher Schutzbedarf (zusätzlich ausgeprägte Zutrittssicherung, keine benachbarten Gefährdungspotenziale, bei Alarmmeldungen minimale Interventionszeiten)