

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH  
bescheinigt hiermit dem Unternehmen

**R-KOM GmbH & Co. KG**  
**Prinz-Ludwig-Straße 9**  
**93055 Regensburg**

für den Sicherheitsbereich

**RZ2**

die Erfüllung aller Anforderungen für erweiterten Schutzbedarf des  
Trusted Site Infrastructure Kriterienkatalogs

**TSI.STANDARD V4.2**  
**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 5 Seiten.  
Dieses Zertifikat gilt nur in Verbindung mit dem Prüfbericht.



**22**  
Zertifikatsgültigkeit:  
21.12.2020 – 31.07.2022

Certificate ID: 66660.20

© TÜVIT – TÜV NORD GROUP – www.tuvit.de

Essen, 21.12.2020

  
Joachim Faulhaber  
stellv. Leiter Zertifizierungsstelle

**TÜV Informationstechnik GmbH**

TÜV NORD GROUP

Langemarckstraße 20

45141 Essen

www.tuvit.de

**Zertifikat**

## Zertifizierungsprogramm

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH führt Zertifizierungen auf Basis des folgenden Zertifizierungsprogramms durch:

- „Zertifizierungsprogramm (nicht akkreditierter Bereich) der Zertifizierungsstelle der TÜV Informationstechnik GmbH“, Version 1.1 vom 01.03.2020, TÜV Informationstechnik GmbH

## Prüfbericht

- „Prüfbericht – Trusted Site Infrastructure (TSI.STANDARD), RZ2“, Version 1.0 vom 17.12.2020, TÜV Informationstechnik GmbH

## Prüfanforderungen

- „TSI.STANDARD Kriterienkatalog, TSI.STANDARD V4.2“ vom 01.01.2019, TÜV Informationstechnik GmbH

Die Prüfanforderungen sind am Ende zusammenfassend aufgeführt. Hierbei sind die für den Prüfgegenstand nicht anwendbaren Prüfanforderungen ausgegraut.

## Prüfgegenstand

Gegenstand der Prüfung ist der Sicherheitsbereich „RZ2“ der R-KOM GmbH & Co. KG. Dieser wird im Prüfbericht detailliert beschrieben.

## Prüfergebnis

Das Ergebnis lautet „Level 2 (erweitert)“. Hierbei werden in den Bewertungsaspekten FIR und CAB alle Anforderungen des nächst höheren Levels erreicht.

## **Zusammenfassung der Prüfanforderungen**

Prüfanforderungen für Trusted Site Infrastructure, TSI.STANDARD V4.2:

### **1 Umfeld (ENV – Environment)**

Gefährdungspotenziale aus dem Umfeld sind gemieden. Die Standortentscheidung des Objekts ist unter Berücksichtigung der Risiken u. a. von Wasser-, Explosions-, Trümmer-, Erschütterungs- und Schadstoffgefährdung erfolgt.

### **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. Eine Trennung zwischen Grob- und Feintechnik ist erfolgt. Es besteht ein baulicher Brand- und Wasserschutz.

### **3 Brandmelde- und Löschtechnik (FIR – Fire Alarm & Extinguishing Systems)**

Eine Brandmeldeanlage ist im gesamten Sicherheitsbereich installiert und zu einer Alarmempfangsstelle 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 Systems & Organization)**

Es existiert eine Zugangskontrollanlage (ZKA). Ein Einbruchschutz ist mehrstufig gegeben, dabei werden alle sicherheitskritischen Bereiche mittels einer Einbruchmeldeanlage (EMA) überwacht. Die Anlage wird von einer Haupt- und einer Zusatzenergiequelle gespeist. Die Alarme werden an eine ständig besetzte Sicherheitszentrale übertragen.

#### **5 Verkabelung (CAB – Cabling)**

Kommunikations- und Datenkabel sind gemäß DIN EN 50174-2 mit dem nötigen Abstand zu einander und zu Stromkabeln auf getrennten Kabelführungen verlegt. Datenkabel werden nicht durch Bereiche mit Gefährdung geführt oder sind speziell geschützt. WAN-Trassen verlaufen kreuzungsfrei, und ein Anschluss an mindestens 2 Provider (ab Level 3) ist realisiert.

#### **6 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. Ausfälle sind durch eine redundante Auslegung abgefangen. Eine Notstrom- und USV-Versorgung der IT- wie auch der Sicherheitssysteme ist gegeben. Tests zur Inbetriebsetzung sind erfolgt.

## **7 Raumluftechnische Anlagen (ACV – Air Conditioning & Ventilation)**

Die Abwärme der IT-Geräte wie auch der Infrastrukturkomponenten wird durch Kühlung hinreichend abgefangen. Es ist sichergestellt, dass Lufttemperatur, Luftfeuchte und Staubbelastung entsprechende Grenzen einhalten. Feuer- und Rauchklappen sind gemäß Brandschutzkonzept eingebaut. Die Einhaltung der Klimavorgaben wird fernüberwacht. Ausfälle sind durch eine redundante Auslegung abgefangen. Tests zur Inbetriebsetzung sind erfolgt.

## **8 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 Datensicherungsmedien werden brand- und zugriffsgeschützt getrennt vom Sicherheitsbereich aufbewahrt.

## **9 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 sowie Schemata und Datenblätter liegen vor. Ein Brandschutzkonzept ist vorhanden. Ein Notfallkonzept bzw. Alarmplan liegen vor.

## 10 Rechenzentrumsverbund (DDC – Dual Site Data Center)

Der Rechenzentrumsverbund besteht aus zwei TSI geprüften Rechenzentren, die einzeln mindestens die Levelstufe unterhalb des Dual Site Levels erreicht haben. Die Rechenzentren befinden sich in getrennten Gebäuden mit getrennter Versorgung, haben eine redundante Daten-netzverbindung und unterscheiden sich in der Größe um max. 30%. Bei Dual Site Level 4 haben die Rechenzentren einen Mindestabstand von mehreren Kilometern, abhängig von der Risikobetrachtung.

### L Level

- |                     |   |
|---------------------|---|
| Level 1             | Mittlerer Schutzbedarf (entspricht den Infrastrukturanforderungen der BSI-Grundschutzkataloge im Baustein Serverraum)   |
| Level 2             | Erweiterter Schutzbedarf (Redundanzen kritischer Versorgungssysteme, mit ergänzenden Anforderungen bei o. g. Bewertungsaspekten)                              |
| Level 3             | Hoher Schutzbedarf (vollständige Redundanzen kritischer Versorgungssysteme – No Single Point of Failures bei wichtigen zentralen Systemen)                    |
| Level 4             | Sehr hoher Schutzbedarf (zusätzlich ausgeprägte Zutrittssicherung, keine benachbarten Gefährdungspotenziale, bei Alarmmeldungen minimale Interventionszeiten) |
| Dual Site Level 2-4 | Beide Rechenzentren erreichen einzeln mindestens die Levelstufe unterhalb des Dual Site Levels.   |

The certification body of TÜV Informationstechnik GmbH hereby awards this certificate to the company

**R-KOM GmbH & Co. KG**  
**Prinz-Ludwig-Straße 9**  
**93055 Regensburg, Germany**

to confirm that its security area

**RZ2**

fulfils all requirements for extended protection of the Trusted Site Infrastructure Criteria Catalog

**TSI.STANDARD V4.2**  
**Level 2 (extended)**

of TÜV Informationstechnik GmbH. The requirements are summarized in the appendix to the certificate.

The appendix is part of the certificate and consists of 5 pages.

The certificate is valid only in conjunction with the evaluation report.

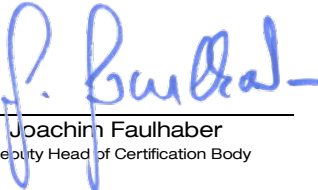


Certificate validity:  
2020-12-21 – 2022-07-31

Certificate ID: 66660.20

© TÜVIT – TÜV NORD GROUP – www.tuvit.de

Essen, 2020-12-21

  
Joachim Faulhaber  
Deputy Head of Certification Body

**TÜV Informationstechnik GmbH**

TÜV NORD GROUP

Langemarckstr. 20

45141 Essen, Germany

www.tuvit.de

**Certificate**

## **Certification Scheme**

The certification body of TÜV Informationstechnik GmbH performs its certification on the basis of the following certification scheme:

- German document: “Zertifizierungsprogramm (nicht akkreditierter Bereich) der Zertifizierungsstelle der TÜV Informationstechnik GmbH”, version 1.1 as of 2020-03-01, TÜV Informationstechnik GmbH

## **Evaluation Report**

- German document: “Prüfbericht – Trusted Site Infrastructure (TSI.STANDARD), RZ2”, version 1.0 as of 2020-12-17, TÜV Informationstechnik GmbH

## **Evaluation Requirements**

- “TSI.STANDARD Criteria Catalog, TSI.STANDARD V4.2“ as of 2019-01-01”, TÜV Informationstechnik GmbH

The Evaluation Requirements are summarized at the end. Not applicable requirements are printed in grey.

## **Evaluation Target**

The target of evaluation is the security area “RZ2” of R-KOM GmbH & Co. KG. It is detailed in the evaluation report.

## **Evaluation Result**

The result is “Level 2 (extended)”. All requirements of the evaluation aspects FIR and CAB of the next higher level are fulfilled.



## **Summary of the Evaluation Requirements**

The requirements for Trusted Site Infrastructure, TSI.STANDARD V4.2:

### **1 ENV – Environment**

Surrounding hazard potentials have been avoided. The decision on the location is based on risk assessments according e. g. floods, explosions, seismic events, shock waves, danger of collapse or pollutants.

### **2 CON – Construction**

Walls, doors and windows offer protection against access, fire and debris. The building is protected against lightning. The security area is located in a separate fire protection area and not directly adjacent to the public and dangerous next-door production processes. IT and technical equipment are separated. A constructive fire and water prevention is given.

### **3 FIR – Fire Alarm & Extinguishing Systems**

A fire alarm system has been installed in the complete security area and linked to an alarm receiving centre. Adjacent rooms, raised floors, suspended ceilings and air ducts are included in the fire monitoring. Apart from signalling an alarm, damage containment measures such as a gas extinguishing system in the security area are triggered. Furthermore appropriate hand fire extinguishers are available.

### **4 SEC – Security Systems & Organization**

An access control system including appropriate access rules does exist. The protection against breaking and entering features several levels, and all security sensitive areas are

monitored by means of an intrusion detection system. The security systems are fed by a main and an additional power source. The alarms are transmitted to a permanently manned security control room.

## **5 CAB - Cabling**

Communication and data cables are laid with the necessary distance to each other and to power cables on separate cable routings in accordance with EN 50174-2. Data cables are not laid in any hazardous areas or they are specially protected. WAN trays are crossing-free, and connections to at least 2 providers are given from Level 3.

## **6 POW - Power Supply**

The electrical installations are realized in accordance with the relevant standards and regulations. They are protected against over voltage and realized with adapted separations and with protection of the electric circuits. Failure of power components is handled by a redundant layout. The IT components and the security control room are connected to an emergency power unit and UPS systems. Commissioning procedures have been performed.

## **7 ACV - Air Conditioning & Ventilation**

Air conditioning for the IT systems and infrastructure components is sufficiently given. It has been ensured that air temperature, humidity and dust content comply with specified limits. Dampers are installed according to the fire protection concept. The measured values are remotely controlled. Failure of air conditioning components are handled by a redundant layout. Commissioning procedures have been performed.

## **8 ORG - Organization**

Periodical functional tests are carried out for all safeguards. A maintenance schedule defines methods and intervals for the wear parts of the infrastructure components. The data backup media is stored and protected against fire and access in an area separate from the security area.

## **9 DOC - Documentation**

A DIM (Documentation of Infrastructure Measures) or a security concept has been provided. Rules of conduct exist, i.e. covering access control with respect to authorization or key / smart card distribution. Up-to-date drawings are available for the building and all infrastructure components, as well as schematics and data sheets. Furthermore a fire protection concept does exist and has been coordinated with the local fire brigade. Additionally emergency or recovery concepts are provided.

## **10 DDC - Dual Site Data Center**

The dual site data center consists of two TSI audited data centers, which individually have reached at least one Level underneath the Dual Site Level. The data centers are located in separate buildings with separate supplies, have a redundant network connection and deviate by size at the most by 30%. For Dual Site Level 4 the data centers have a minimum distance of several kilometres, depending on the risk assessment.

## **L Level**

- Level 1 Medium protection requirements (corresponds to the infrastructure requirements of the “IT-Grundschutz Catalogues” published by the German Federal Office for Information Security (BSI))
- Level 2 Extended protection requirement (redundancies of critical supply systems, with supplementary requirements for the aforementioned assessment aspects)
- Level 3 High protection requirement (complete redundancies of critical supply systems – no single point of failures in important central systems)
- Level 4 Very high protection requirements (advanced access control, no adjacent hazard potentials, with minimal intervention times in the case of alarms)
- Dual Site both data centers individually reach at least one Level 2-4 Level underneath the Dual Site Level.