TÜVIT

Certificate

TÜVIT
TÜV NORD GROUP
TSI.STANDARD
Infrastructure
2023
tuvit.de ID: 66959.23

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

GlobalConnect Netz GmbH
Wendenstraße 377
20537 Hamburg, Germany

Certificate validity:
2023-07-04 – 2025-07-04

to confirm that its security area

DC Hamburg 04

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

TSI.STANDARD V4.4
Level 2 (extended)

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

The appendix is part of the certificate with the ID 66959.23 and consists of 4 pages.

Certificate extension
by 3 month

Certification Body of
TÜV NORD CERT GmbH

Essen, 2023-07-04

Joachim Faulhaber, Deputy Head of Certification Body

To Certificate

TÜV Informationstechnik GmbH
Am TÜV 1 ▪ 45307 Essen, Germany
tuvit.de

TÜVNORDGROUP

Certification scheme

The certification body of TÜV Informationstechnik GmbH performs its certifications based on 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: “Evaluierungsbericht – Trusted Site Infrastructure (TSI.STANDARD), DC Hamburg 04”, Version V1.0 as of 2023-06-26, TÜV Informationstechnik GmbH

Evaluation requirements

- “TSI.STANDARD Criteria Catalog, TSI.STANDARD V4.4” as of 2023-01-01, TÜV Informationstechnik GmbH

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

Evaluation target

Evaluation target is the security area “DC Hamburg 04” of GlobalConnect Netz GmbH. It is detailed in the evaluation report.

Evaluation result

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

Summary of the Evaluation Requirements

The evaluation requirements for Trusted Site Infrastructure, TSI.STANDARD V4.4:

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 Level 2-4	both data centers individually reach at least one Level underneath the Dual Site Level.

E EFF - Energy Efficiency

The value for the Power Usage Effectivness (PUE) of the data center infrastructure was correctly determined and is below 1.5. The results of the continuous measurements over 12 months for the total energy demand and the IT energy demand as well as documentation for the measurement concept are available.