TÜVIT

Certificate

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

noris network AG
Thomas–Mann–Straße 16–20
90471 Nürnberg, Germany

Certificate validity:
2023-07-25 – 2025-06-24

to confirm that its security area

Nürnberg Süd (NBG6 BA2)

fulfils all requirements of

ISO/IEC 22237-1, –3 and –4
Availability Class 4,
Granularity Level 2

using Trusted Site Infrastructure Criteria catalogs TSI.STANDARD V4.3 and V4.5 of TÜV Informationstechnik GmbH. The requirements are summarized in the appendix to the certificate.

The appendix is part of the certificate with the ID 661007.23 and consists of 4 pages.

Essen, 2023-07-25

Dr. Christoph Sutter, Head of Certification Body

To Certificate

TÜVNORDGROUP

Appendix to the certificate
with the ID: 661007.23
page 1 of 4

Certification scheme

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

- German document: "Zertifizierungsprogramm (nicht akkreditierter Bereich) der Zertifizierungs-stelle 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), Nürnberg Süd (NBG6 BA2)", Version 2.0 as of 2023-07-07, TÜV Informationstechnik GmbH

Evaluation requirements

The evaluation requirements are defined in the following standards:

- ISO/IEC 22237-1, Information technology — Data centre facilities and infrastructures —Part 1: General concepts, 2021-10

- ISO/IEC 22237-3, Information technology — Data centre facilities and infrastructures —Part 3: Power Distribution, 2021-10

- ISO/IEC 22237-4, Information technology — Data centre facilities and infrastructures —Part 4: Environmental control, 2021-10

and were checked applying the evaluation requirements:

- "TSI.STANDARD Criteria Catalog" V4.3 and V4.5 as of 2023-07-01, 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 "Nürnberg Süd (NBG6 BA2)" of noris network AG. It is detailed in the evaluation report.

Appendix to the certificate
with the ID: 661007.23
page 2 of 4

Evaluation result

The evaluation target fulfils all applicable requirements of the above-mentioned standards with regard to

- Availability Class 4,

- Granularity Level 2.

Summary of the Evaluation Requirements

The requirements for Trusted Site Infrastructure, TSI.STANDARD V4.5, which contain the requirements of ISO/IEC:

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.

Appendix to the certificate
with the ID: 661007.23
page 3 of 4

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   ISO/IEC 22237

The supplementary requirements for holistic coverage of ISO/IEC 22237-1, -3, -4 have been implemented.

Appendix to the certificate
with the ID: 661007.23
page 4 of 4

To achieve availability class X, all ISO/IEC 22237 requirements relevant in level X as well as the TSI requirements in the areas of POW and ACV must be achieved at least in the corresponding TSI level X.

Granularity level 2 according to ISO/IEC 22237-3 and -4 is confirmed if the TSI requirements are fulfilled in one of the levels 2, 3 or 4 together with the corresponding ISO/IEC 22237 requirements.

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.