Zertifikat

Die Zertifizierungsstelle der TÜV NORD CERT GmbH
bescheinigt hiermit dem Unternehmen

noris network AG
Thomas-Mann-Straße 16-20
90471 Nürnberg

für den Sicherheitsbereich

Nürnberg Süd (NBG6 BA2)

die Erfüllung aller Anforderungen

ISO/IEC 22237-1, -2, -3, -4, -6
Verfügbarkeitsklasse 4
Schutzklassen 1-4
Granularitätsniveau 2

unter Verwendung des Trusted Site Infrastructure Kriterienkatalogs TSI.STANDARD V4.6 der TÜV NORD CERT GmbH. Die Anforderungen sind in der Anlage zum Zertifikat zusammenfassend aufgelistet.

Die Anlage ist Bestandteil des Zertifikats und besteht aus 5 Seiten.

Zertifikats-ID: 661196.25

gültig von 16.04.2025 bis 24.06.2027

Zum Zertifikat

Essen, 16.04.2025

Zertifizierungsstelle der TÜV NORD CERT GmbH

TÜV NORD CERT GmbH
Am TÜV 1, 45307 Essen
tuev-nord-cert.de

TÜV®

Zertifizierungsprogramm

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

- „Zertifizierungssystem für IT-Zertifikate (nicht akkreditierter Bereich) der Zertifizierungsstelle der TÜV NORD CERT GmbH“, D503-CP-001, Rev. 00/09.24, TÜV NORD CERT GmbH

Evaluierungsbericht

- „Evaluierungsbericht – Trusted Site Infrastructure (TSI.STANDARD), Nürnberg Süd (NBG6 BA2)“, Version 1.0 vom 16.04.2025, TÜV NORD CERT GmbH

Evaluierungsanforderungen

Die Evaluierungsanforderungen sind definiert in den Normen:

- ISO/IEC 22237-1, Information technology — Data centre facilities and infrastructures —Part 1: General concepts, 2021-10
- ISO/IEC 22237-2, Information technology — Data centre facilities and infrastructures —Part 2: Building construction, 2024-02
- 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
- ISO/IEC 22237-6, Information technology — Data centre facilities and infrastructures —Part 6: Security systems, 2024-02

und wurden überprüft unter Verwendung der Evaluierungsanforderungen:

- „TSI.STANDARD Kriterienkatalog“, TSI.STANDARD V4.6 vom 01.11.2024, TÜV NORD GmbH

Die Evaluierungsanforderungen sind am Ende zusammenfassend aufgeführt. Hierbei sind die für den Evaluierungsgegenstand nicht anwendbaren Anforderungen ausgegraut.

Evaluierungsgegenstand

Evaluierungsgegenstand ist der Sicherheitsbereich „Nürnberg Süd (NBG6 BA2)“ der noris network AG. Dieser wird im Evaluierungsbericht detailliert beschrieben.

Evaluierungsergebnis

Der Evaluierungsgegenstand erfüllt alle anwendbaren Anforderungen der oben genannten Normen bezüglich

- Verfügbarkeitsklasse 4
- Schutzklassen 1-4
- Granularitätsniveau 2

Zusammenfassung der Evaluierungsanforderungen

Evaluierungsanforderungen für Trusted Site Infrastructure, TSI.STANDARD V4.6, welche die Anforderungen der ISO/IEC 22237 enthalten:

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 zueinander 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 Raumlufttechnische 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 ISO/IEC 22237

Die ergänzenden Anforderungen zur ganzheitlichen Abdeckung der ISO/IEC 22237-1, -2, -3, -4, -6 sind umgesetzt.

Zur Erreichung der Verfügbarkeitsklasse X müssen sowohl alle im Level X relevanten ISO/IEC 22237-Anforderungen als auch die TSI-Anforderungen in den Bereichen POW und ACV mindestens im korrespondierenden TSI Level X erreicht werden.

Das Granularitätsniveau 2 gemäß ISO/IEC 22237-3 und -4 wird bestätigt, wenn die TSI-Anforderungen in einem der Level 2, 3 oder 4 zusammen mit den entsprechenden ISO/IEC 22237-Anforderungen erfüllt sind.

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.

E Energie-Effizienz (EFF – Energy Efficiency)

Der Wert für die Power Usage Effectivness (PUE) der Rechenzentrumsinfrastruktur wurde korrekt ermittelt und liegt unter 1,5. Die Ergebnisse zu den kontinuierlichen Messungen über 12 Monate für den Gesamtenergiebedarf und den IT-Energiebedarf sowie eine Dokumentation für das Messkonzept liegen vor.