TÜVNORD

Certificate

The certification authority of TÜV NORD CERT GmbH hereby certifies the company

Equinix (Germany) GmbH
Rebstöcker Straße 33
60326 Frankfurt am Main

for the security area

IBX MU4.1

the fulfillment of all requirements

EN 50600
Availability Class 3, Protection Classes 1-3, Granularity Level 2

using the Trusted Site Infrastructure Criteria Catalog TSI.STANDARD V4.5 of TÜV NORD CERT GmbH. The requirements are summarized in the annex to the certificate.

The annex is part of the certificate and consists of 6 pages.

Certificate ID: 661150.24 valid from 07.10.2024 to 07.10.2026

Zum Zertifikat

Essen, 07.10.2024 Dr.-Ing. Poldrack

Certification body of TÜV NORD CERT GmbH

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

TÜV®

Certification Program

The certification authority of TÜV NORD CERT GmbH conducts certifications based on the following certification program:

- "Certification System for IT Certificates (Non-Accredited Area) of the Certification Authority of TÜV NORD CERT GmbH," D503-CP-001, Rev. 00/09.24, TÜV NORD CERT GmbH

Evaluation Report

- “Evaluation Report – Trusted Site Infrastructure (TSI.STANDARD), IBX MU4.1”, Version 1.0 from 07.10.2024, TÜV NORD CERT GmbH

Evaluation Requirements

The evaluation requirements are defined in the standards:

- DIN EN 50600-1 (VDE 0801-600-1), Information Technology – Facilities and Infrastructures of Data Centers – Part 1: General Concepts; German version EN 50600-1:2019-08
- DIN EN 50600-2-1 (VDE 0801-600-2-1), Information Technology – Facilities and Infrastructures of Data Centers – Part 2-1: Building Construction; German version EN 50600-2-1:2021-09
- DIN EN 50600-2-2 (VDE 0801-600-2-2), Information Technology – Facilities and Infrastructures of Data Centers – Part 2-2: Power Supply and Distribution; German version EN 50600-2-2:2019-08
- DIN EN 50600-2-3 (VDE 0801-600-2-3), Information Technology – Facilities and Infrastructures of Data Centers – Part 2-3: Environmental Condition Control; German version EN 50600-2-3:2019-08
- DIN EN 50600-2-4 (VDE 0801-600-2-4), Information Technology – Facilities and Infrastructures of Data Centers – Part 2-4: Telecommunications Cabling Infrastructure; German version EN 50600-2-4:2015-07
- DIN EN 50600-2-5 (VDE 0801-600-2-5), Information Technology – Facilities and Infrastructures of Data Centers – Part 2-5: Security Systems; German version EN 50600-2-5:2021-09
- DIN EN 50600-3-1 (VDE 0801-600-3-1), Information Technology – Facilities and Infrastructures of Data Centers – Part 3-1: Information for Management and Operation; German version EN 50600-3-1:2016-08

- DIN EN 50600-4-2, Information Technology – Facilities and Infrastructures of Data Centers – Part 4-2: Key Figures for Energy Used; German version EN 50600-4-2:2016 + AC:2017 + A1:2019

and were reviewed using the evaluation requirements:

- "TSI.STANDARD Criteria Catalog", TSI.STANDARD V4.5 from 01.07.2023, TÜV NORD CERT GmbH

The evaluation requirements are summarized at the end. The requirements that are not applicable to the evaluation subject are grayed out.

Evaluation Subject

The evaluation subject is the security area "IBX MU4.1" of Equinix (Germany) GmbH. This is described in detail in the evaluation report.

Evaluation Result

The evaluation subject meets all applicable requirements of the above-mentioned standards regarding

- Availability Class 3,
- Protection Classes 1-3,
- Granularity Level 2.

Summary of Evaluation Requirements

Evaluation requirements for Trusted Site Infrastructure, TSI.STANDARD V4.5, which include the requirements of DIN EN 50600:

1. **Environment (ENV – Environment)**

   Hazards from the environment have been avoided. The site decision of the facility was made considering risks such as water, explosion, debris, vibration, and pollutant hazards.

2. **Construction (CON – Construction)**

   The building construction, including windows and doors, provides access, fire, and debris protection. The building is protected against lightning strikes. The security area is separate from public access and hazardous production processes, forming its own fire section. There is a separation between coarse and fine technology. There is structural fire and water protection.

3. **Fire Alarm and Extinguishing Systems (FIR – Fire Alarm & Extinguishing Systems)**

   A fire alarm system is installed throughout the security area and connected to an alarm receiving center. Adjacent rooms, raised floors, suspended ceilings, and air ducts are included in the fire monitoring. In addition to alarm signaling, shutdown functions and damage limitation measures are triggered, for example, by a gas extinguishing system. Additional suitable portable fire extinguishers are available.

4. **Security Systems (SEC – Security Systems & Organization)**

   There is an access control system (ACS). Multi-tiered burglary protection is in place, with all security-critical areas monitored by a burglar alarm system (BAS). The system is powered by a main and auxiliary energy source. Alarms are transmitted to a continuously staffed security center.

5. **Cabling (CAB – Cabling)**

   Communication and data cables are installed according to DIN EN 50174-2 with the necessary distance from each other and from power cables on separate cable trays. Data cables are not routed through hazardous areas or are specially protected. WAN paths run without intersections, and a connection to at least 2 providers (Level 3) is established.

6. **Power Supply (POW – Power Supply)**

   Documentation of the electrical installation in accordance with relevant DIN standards and VDE regulations has been provided. There are appropriate distributions and protections of the circuits. They are protected against overvoltage. Failures are mitigated by redundant design. There is an emergency power and UPS supply for IT and security systems. Tests for commissioning have been conducted.

7. **Air Conditioning and Ventilation Systems (ACV – Air Conditioning & Ventilation)**

   The waste heat of the IT devices and infrastructure components is sufficiently dissipated through cooling. It is ensured that air temperature, humidity, and dust load adhere to appropriate limits. Fire and smoke dampers are installed according to the fire protection concept. Compliance with climate requirements is monitored remotely. Failures are mitigated by redundant design. Tests for commissioning have been conducted.

8. **Organization (ORG – Organization)**

   All security systems undergo regular functional testing. Regular maintenance of wear parts of infrastructure components or IT hardware is defined in a maintenance plan. Data backup media are stored in a fire- and access-protected manner, separate from the security area.

9. **Documentation (DOC – Documentation)**

   There is documentation of the infrastructure measures (DIM) or a security concept. Additionally, there are regulations for the access control system, defining entitled persons and describing the procedures for issuing keys, code cards, etc. Site plans for the building and all infrastructure components as well as schematics and data sheets are available. A fire protection concept exists. An emergency plan or alarm plan is also in place.

10. **EN 50600**

    The supplementary requirements for comprehensive coverage of DIN EN 50600 have been implemented.

    To achieve Availability Class X, all relevant EN 50600 requirements at Level X and the TSI requirements in the areas of POW, ACV, and CAB must be met at least at the corresponding TSI Level X.

    The Granularity Level 2 according to EN 50600-2-2 and -2-3 is confirmed when the TSI requirements are met in one of Level 2, 3, or 4 together with the corresponding EN 50600 requirements.

Four different protection classes are defined. Each area and supply path of the data center is assigned a protection class. They describe physical safeguards against the following events:

- Unauthorized access
- Burglary
- Internal environmental events
- External environmental events

Regarding Unauthorized access/Burglary, at least three protection classes must be implemented.

L Level

Level 1	Medium protection requirement (corresponds to the infrastructure requirements of the BSI-Grundschutzkataloge in the module server room)
Level 2	Extended protection requirement (redundancies of critical supply systems, with additional requirements for the aforementioned evaluation aspects)
Level 3	High protection requirement (complete redundancies of critical supply systems – No Single Point of Failures for important central systems)
Level 4	Very high protection requirement (additionally enhanced access security, no adjacent hazard potentials, minimal intervention times in case of alarm notifications)
Dual Site Level 2-4	Both data centers individually meet at least the level below the Dual Site Levels.

E Energy Efficiency (EFF – Energy Efficiency)

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