Certificate

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

PostFinance AG
Mingerstrasse 20
3030 Bern, Switzerland

to confirm that its dual site data center

Bern-Engehalde [RZ1] and Zofingen [RZ2]

fulfils all requirements for high protection of the Trusted Site Infrastructure criteria catalogue

TSI.STANDARD V4.2
Dual Site Level 3

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.

Infra-structure TÜViT® 2019 Trusted Site

Certificate ID: 66537.19

Certificate valid until 2021-12-31

Essen, 2019-11-07

Dr. Christoph Sutter
Head of Certification Body

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Langemarckstr. 20
45141 Essen, Germany
www.tuvit.de

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 1.0 as of 2015-08-24, TÜV Informationstechnik GmbH

Evaluation Report

- German document: "Prüfbericht – Trusted Site Infrastructure (TSI.STANDARD) – Dual Site, Bern-Engehalde [RZ1] und Zofingen [RZ2]", version 1.0 as of 2019-10-23, TÜV Informationstechnik GmbH tionstechnik GmbH

Evaluation Requirements

- "TSI.STANDARD Criteria Catalogue, TSI.STANDARD V4.2" as of 2019-01-01, TÜV Informationstechnik GmbH

The Evaluation Requirements are summarized at the end.

Evaluation Target

The target of evaluation is the dual site data center "Bern-Engehalde [RZ1] und Zofingen [RZ2]" of PostFinance AG.

The dual site data center consists of data centers:

- Bern-Engehalde [RZ1] und
- Zofingen [RZ2].

It is detailed in the evaluation report.

Evaluation Result

The result is “Dual Site Level 3”. The result is valid under the condition that the IT systems are set up and operated redundantly in both data centers.

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 2 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.