

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

Bayer Business Services GmbH
Gebäude B151
51368 Leverkusen

to confirm that its security location

Bayer Data Center BDC 1.2

fulfills all requirements of the criteria catalogue

Trusted Site Infrastructure TSI V2.0
Level 3 (extended)

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

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

The certificate is valid only in conjunction with the corresponding
evaluation report, version 1.0 as of 2008-10-31.

The certificate is valid until 2010-10-31.



© 2008 TÜVIT GmbH - Member of TÜV NORD Group

Certificate-Registration-No.:
TUVIT-TSI6681.08

Essen, 2008-10-31

Dr. Christoph Sutter
Head of Certification Body

TÜV Informationstechnik GmbH
Member of TÜV NORD Group
Langemarckstr. 20
45141 Essen, Germany
www.certuvit.de

Certificate

Evaluation Report

TÜV[®]

„Prüfbericht – Trusted Site Infrastructure zum Bayer Data Center BDC 1.2 der Bayer Business Services GmbH“, Version 1.0, 2008-10-31, TÜV Informationstechnik GmbH

Evaluation Result

The result is „Level3 (extended)“. All requirements of the evaluation aspects FIR, POW, ACV and ORG of the next highest level are fulfilled.

Evaluation Criteria

Summary of the requirements for “Trusted Site Infrastructure” (TSI), version 2.0

1 ENV – Environment

There are no surrounding hazard potentials. The decision on the location must be based on the avoidance of 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. It has also been ensured that building sections threatened by water, EM/RF interference fields, and dangerous next-door production processes are avoided. The building is protected against lightning. The security area is located in a separate fire protection area and not directly adjacent to the public. IT and technical equipment are separated.

3 FIR – Fire Protection / Alarm / Extinguishing Systems

TÜV[®]

A fire alarm system has been installed in the complete security area and linked with the fire brigade. Adjacent rooms, raised floors, suspended ceilings and air ducts are included in the fire monitoring. Apart from signaling 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

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. These security systems are connected to the emergency power supply and to a permanently manned control room.

5 POW – Power Supply

The electrical installations are realized in accordance with the relevant DIN standards and VDE regulations. They are protected against over voltage and realized with adapted separations and with protection of the electric circuits. The IT- and the security systems are connected to an uninterruptible power supply. For the supply alternative possibilities exist.

6 ACV – Air Conditioning and Ventilation

Air conditioning in redundant design for the IT systems is given. It has been ensured that air temperature, humidity and dust content comply with specified limits. The measured values are remotely controlled. Dampers are installed according to the fire protection concept.

7 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 communication with the exterior is ensured, even if the PBX fails. The data backup media is stored and protected against fire and access in an area separate from the security area.

8 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 plans and documentation are available for the building and all infrastructure components. Furthermore a fire protection concept does exist and has been coordinated with the local fire brigade. Additionally emergency and recovery concepts are provided.

L Level

- Level1 medium protection requirements (according to the BSI infrastructure requirements of the baseline protection manual)
- Level2 extended protection requirements (extended requirements to all above mentioned aspects)
- Level3 high protection requirements (complete redundancy of essential components, no single point of failures, climate limits according to EN 1047-2)
- Level4 very high protection requirements (advanced access control, no adjacent hazard potentials, with minimal intervention time)