Service Level Agreement DC- and Cloud-Services (SLA)

§ 1 Scope of terms

The Service Level Agreement DC- and Cloud-Services (in the following 'SLA'), in addition to the terms of use DC- and Cloud-Services (in the following 'terms of use') and the supplementary general terms and conditions (in the following 'T&Cs'), create the foundation for the provision of services by the enterprises of the TechniData IT-Group (in the following 'TechniData') in the scope of data center and cloud products. The SLA only describes the minimal contents of the customer entitlement and supplements any existing product related descriptions of services. In the case of conflicts, these descriptions shall prevail over the SLA. The following order describes the rank order of the contractual documents:

I. Customer offer
II. Product- or service description
III. SLA
IV. Terms of use
V. T&Cs

§ 2 Provision of Services / Point of Transfer

The services under this SLA are provided to the customer via the internet for a limited period of time either within the scope of a rental or a services agreement. Usage of the services by the customer requires him to establish an appropriate internet connection which is not part of the service provision by TechniData unless ordered separately.
Point of transfer of the contractual services is the interface to the public internet (backbone) at the TechniData data center.

§ 3 Data center description & Quality characteristics

The TechniData data center is established in Möglingen/Baden-Württemberg and meets high demands to security and availability. The following description constitutes the agreed quality characteristics of the data center.

Building
The building was especially designed to accommodate and operate a data center. From the outside it is quite discreet and the outer walls of the IT surfaces are windowless. Different functional zones within the structure are separated from one another.

Access control and alarm system
The data center has an access control system integrated in the building services engineering that generates access protocols. Access to the data center is only granted by two factor authentication (alarm system & access control system).
The center also has an intrusion reporting system, including alarm to a security service with 24x7 availability, integrated within the building services engineering. The security service has predefined procedures in case of an alarm.
The presence of customers, technicians, foreign personnel and visitors is documented traceable. Outside visitors are briefed about necessary rules of behavior and pass an identity check before entering the secured premises. Technicians and foreign personnel may only enter temporarily and only to complete their assigned tasks. All visitors are continuously being accompanied by an authorized person.

WAN-connection
All communication devices of the data center are backed up by redundant power supplies. All connections to outside networks are also redundant. All lines entering the building are laid separately.

Power supply
The data center is connected to the public power supply by an 'open ring' for an increased fail safety. A UPS system with n+1 redundancy as well as an emergency power system is installed. All redundant systems are spaced apart and supplied separately.
The power redundancy units are tested regularly depending on their technical requirements. A test run of the emergency power system commences monthly. Switch units are tested every half year and a 'black-building-test' is done every year. Maintenance of the power supply is scheduled regularly.

Air conditioning
The air condition system is designed as n+1 redundant. The cooling and air venting systems can also be operated manually if necessary. The air conditioning is tested regularly depending on their technical requirement. The switching process of the cooling systems is tested at least once every half a year. All maintenance work is scheduled in advance and executed regularly.

Fire protection
All legal and official regulations as well as the insurance conditions regarding fire protection are met. A system with sensors for early fire detection and two sensor dependency technology is installed. Alarm is given by the building services engineering to a security center that implements procedures for an alarm scenario. A fire prevention system is also installed. Maintenance work for fire prevention is scheduled in advance and executed regularly.

System-Monitoring
For service provision, multiple monitoring tools are being used. All monitored system parameters are collected centrally and their status is controlled continuously. With the optional management option 'Advanced 24x7' or 'Professional 24x7', on call services are being alarmed even outside of the regular service hours.

Security-Management
The security installations of the data center fulfill today's technical requirements by a multilayered network structure. By an active patch management process, the security systems are continuously updated. Every customer receives an individual IP range that is separated to other IP ranges by VLAN. Anti-virus protection is established in every system. TechniData employs security checks regularly which check on every security system within the data center. The security checks are monitored by an information security officer.

Emergency- and risk management
A concept for the management of disruptions and emergency situations is in place to minimize their occurrence or effects. It contains escalation plans that also cover customer communications and are tested periodically. Any disruptions and emergency as well as the actions taken are documented.
TechniData employs risk analysis scenarios that describe the operation of the data center and applicable countermeasures to manage any risk imaginable.

DC-operation / documentation
The operation of the data center is documented by TechniData to ensure compliance to the quality characteristics and to detect any disruption as early as possible. To achieve this goal, the following documentation/information is created by TechniData:

- Operating manuals or appropriate adequate descriptions that depict the basic processes and procedures for data center operations.
- Advanced documentation for important processes and procedures.
- Service-Level-Agreements with suppliers.
- Service-Level-Agreements with customers.
- Procedures for a standardized handling of changes to the infrastructure and appliances ('change management').
- A reactive incident management that records security issues, disruptions and emergencies as well as the measures taken.
- A system of indicators including monitoring of SLA guidelines is in place. Essential indicators are analyzed regularly.

Certification
TechniData's high quality of standards is underlined by certifications such as ISO 9001 and ISO 27001. Even today enterprises within the TechniData-Group hold both of these certifications. The IT service management of TechniData is aligned to the de facto standard ITIL.

§ 4 Disruption- / Incident-Management

Fault clearance
TechniData fixes faults and disruptions of the provided infrastructure and services as quickly as possible within its operational capabilities. Prerequisite is the timely and adequate fulfillment of the customers' cooperation obligations necessary for the fault clearance. TechniData may use third parties to remedy any disruptions or faults. Other rights of the customer regarding faults of the contractual services and deliveries of TechniData remain unaffected within the contractual scope.

Definition of disruption
A disruption exists, if the infrastructure or the service is faulty or not available. Reaction time, in accordance with § 6 Section 3 below, begins when the disruption has been detected and reported by the technical surveillance institutions

(monitoring systems) or by the customer. Upon acknowledgement, TechniData opens up a 'fault-ticket'. During disruption management, the customer receives the reference number to this ticket which serves to quickly identify the process at later times.

Reception of disruptions and service requests
Reception of incidents as well as reception of service requests (service ordering) happens during service hours (see § 6 Section 2 below) by the ServiceDesk of TechniData.
Contact information for Service Desks of TechniData enterprises can be taken from their websites. The TechniData central ServiceDesk can be reached by the phone number +49 180 2007002. It is possible to ask for guidance to the correct contact there or directly pass on the relevant information.
The customer must use the provided contact methods to report an incident in order for TechniData to be able to uphold their contractually agreed reaction times.

Self-Service-Portal
The TechniData self-service-portal offers to the customers the possibility to relay specific questions in regards to services, problems, incidents and service requests to the TechniData ServiceDesk by a web based form system. The system also provides information to the current state or enables to add further information to prior requests made.
Key users of a customer may view all service tickets made by their organization unit and add additional information. Setup of users and key users and the relay of login data commences after receipt of order. The use of the portal is free of an additional charge.

§ 5 Service Level

TechniData offers a standardized service level that is referred to in the specific product- and service descriptions.

Standard

DC operation time	24x7 on 365 days a year
Service times	Monday to Friday 8:00 a.m. – 6:00 p.m.*
Reaction time to incidents	max. 45 minutes
System availability p.a.	99,5%
Scheduled service times p.a.	6

Premium

DC operation time	24x7 on 365 days a year
Service times	Monday to Friday 8:00 a.m. – 6:00 p.m.*
Reaction time to incidents	max. 45 minutes
System availability p.a.	99,9%
Scheduled service times p.a.	6

*) except public and bank holidays (nationwide) and 24.12. ,31.12.

§ 6 SLA definition of terms

1. DC operation time
Operation of infrastructure and services is provided on 365 days a year around the clock within the scope of system availability (see Sec. 4 below).

2. Service times
TechniData offers services, especially the reception and management of incident reports and service requests, within the defined service hours. Is there no other agreement, these service times are from Monday to Friday between 8 a.m. and 6 p.m. with the exception of public and bank holidays (nationwide holidays) as well as the 24th and 31st of December every year. Outside these service hours, TechniData will offer services only after prior arrangement.

3. Reaction time
Reaction time for the processing of disruptions is the time from acknowledgement of this disruption by TechniData (by means of monitoring systems) or the reception of a report, complete and in due form, by the customer by means of the intended ways of communication up to the start of processing it by TechniData. Reaction time is counted within the defined service times. Is the incident report made outside the service times, reaction time starts with begin of service hours of the next work day. Is it made within the service times, not yet spent reaction time at the end of the service day will resume being used up at beginning of the next service day. Times at that TechniData cannot provide its services due to reasons outside its responsibility and/or times in which TechniData is waiting for the completions of the customers' cooperation will not be considered when calculating the reaction time.

4. System availability
Principally, the ordered services are available during the operation period. Calculation base for system availability is the calendar year. Should the start to provide a service be at a date unequal to the beginning of a calendar year, that period of time lasting to the end of that calendar year is defined as a 'trunk' year; so is the beginning of the last calendar year of the contractual period to the end of the agreement. System availability within a 'trunk' year will be extrapolated over a full year.

Calculation of system availability over the course of a calendar year is based on the following formula:

$$\text{System availability} = \frac{\text{operation period} - \text{disruption times}}{\text{operation period}} \times 100$$

• **Operation period** = scheduled maintenance times (see Section 6) subtracted from yearly DC operation time
• **Disruption times** = sum of all times within the operation period of a calendar year in which the system or service was not available. Times of system unavailability may not be considered as disruption times due to the following reasons:

- Force majeure
- Other events or causes that are not attributable to TechniData (especially events caused by third parties that are of mechanical nature, other kinds of destructive forces on active components and/or the passive cable trays or failures in the employed standard software that the TechiData IT-infrastructure is based upon (i.e. MS Windows Server)
- Impairment of data transmission outside of the TechniData network (towards the interconnection point. See § 2), i.e. by line failure or other disruptions caused by other providers or telecommunication companies.
- Disruptions caused by the customer himself or caused on his behalf, i.e. changes in configuration of the used services that TechniData executes upon request of customer
- Delays in system access that are not caused by TechniData (i.e. denial of access to the technical institutions)
- Events that require restriction or blockage towards access to single infrastructural components and/or services due to imminent threat to data, hard- and/or software, due to dangers (i.e. virus, trojan) or due to substantial threat to the network security or integrity.
  TechniData will take into consideration the legitimate interests of the customer as far as possible, in case such a decision needs to be made. TechniData will inform the customer immediately about the measures taken and will do everything possible to clear the access restriction or blockage at the earliest possible.

If there is no complete system unavailability or impairment of the system availability that equals a complete unavailability, because the service is virtually unusable by the customer, this does not count as disruption time. In case of any other impaired system availability (i.e. bit error rate, packet loss, etc.) TechniData will try to restore the system availability as quickly as possible.

5. Scheduled maintenance
The customer is informed by TechniData of any scheduled service interruptions, for example, if any installation- or maintenance work is due, in written form, by facsimile or by E-Mail in due time, at least 5 working days in advance; in case of an unexpectedly occurring emergency maintenance (i.e. Security patch) this deadline may not be met. By default, six (6) scheduled maintenance events per calendar year are planned by TechniData. These are notified to the customer at the beginning of the year. Emergency maintenance serves as a measure to avoid or remedy disruptions and may be scheduled at short notice, according to the degree of urgency. TechniData will inform the customer immediately, should this affect any of his booked services.
If possible and viable, TechniData will schedule emergency maintenance events at times with low system load and will coordinate these times with the customer.

6. Legal consequences
The legal consequences of compliance failure to these service level regulations especially arise from the terms of use and the T&Cs.