swisscom

Service Description

Enterprise Service Cloud - Managed OS Service

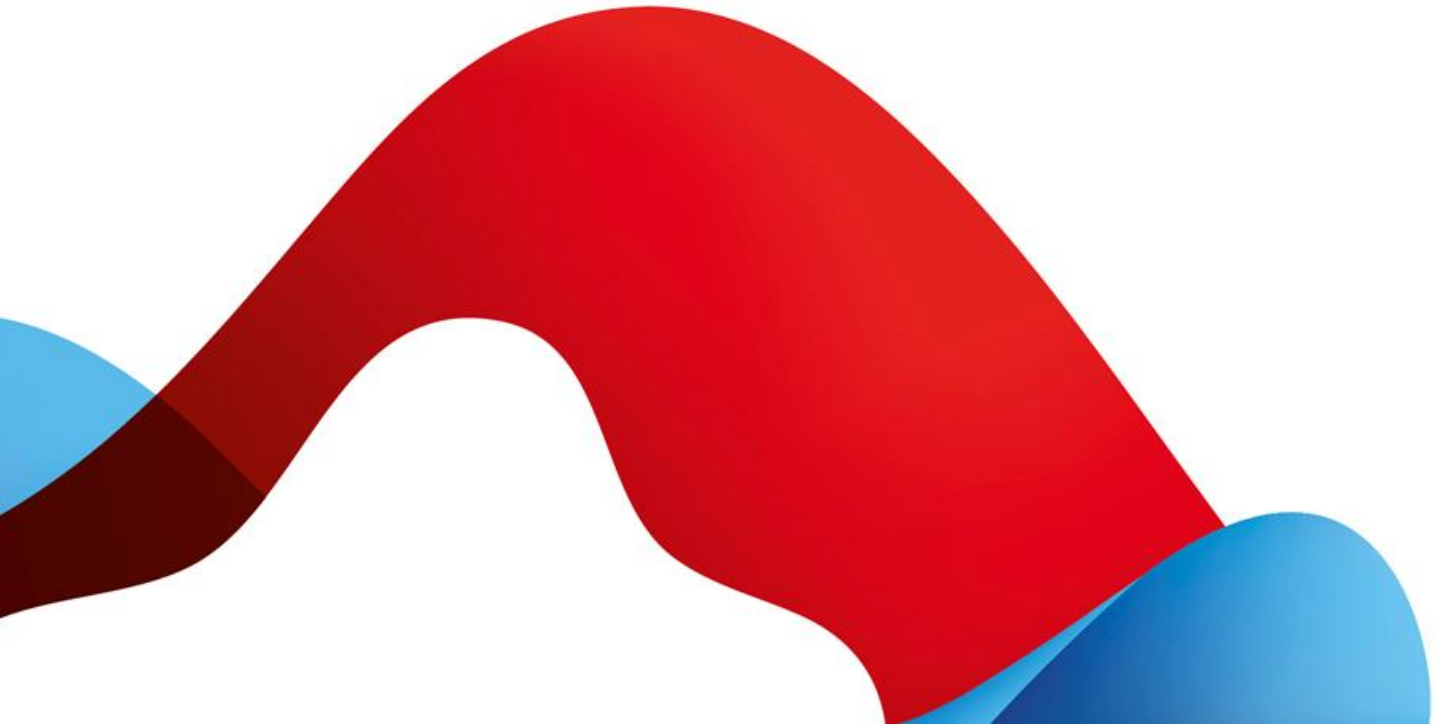


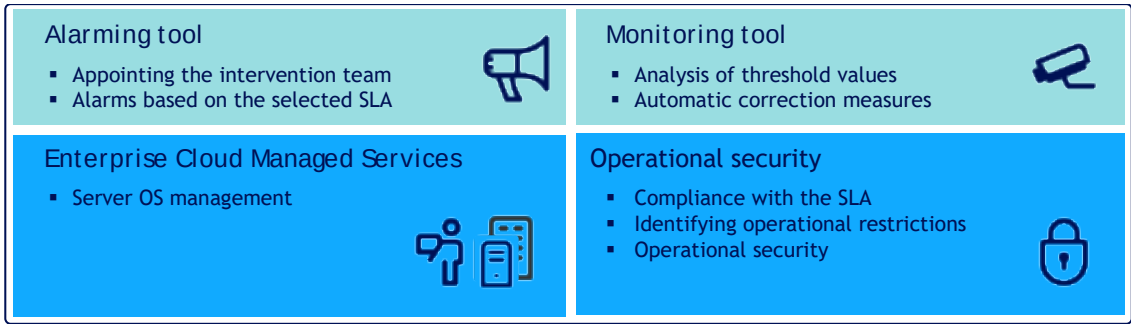
Table of contents

1 Service Overview

The *"Managed OS Service"* enables the Customer to transfer operational tasks within the E*nterprise Service Cloud* environment at operating system level to Swisscom. These include backup/restore functionalities, antivirus and malware protection, patching, hardening accordint to "good practices" and monitoring of system-relevant parameters (monitoring and alarms) as well as incident and problem management up to OS level. The use of Managed OS components meets high quality standards and is suitable for business-critical applications.

The Managed OS service consists of services shown in the graphic below and is distinguished by the following characteristics:

- Swisscom ensures the secure and reliable functioning of the operating system and thus enables the Customer to use IT resources in a targeted way at application level.
- High-quality service levels, including their reporting, form a stable basis for the operation of business applications.
- All operational services are carried out by Swisscom employees in Switzerland.



The Managed OS service is based on the "Enterprise Service Cloud" service. It follows that the purchase of Enterprise Service Cloud is a precondition for the purchase of the Managed OS Service.

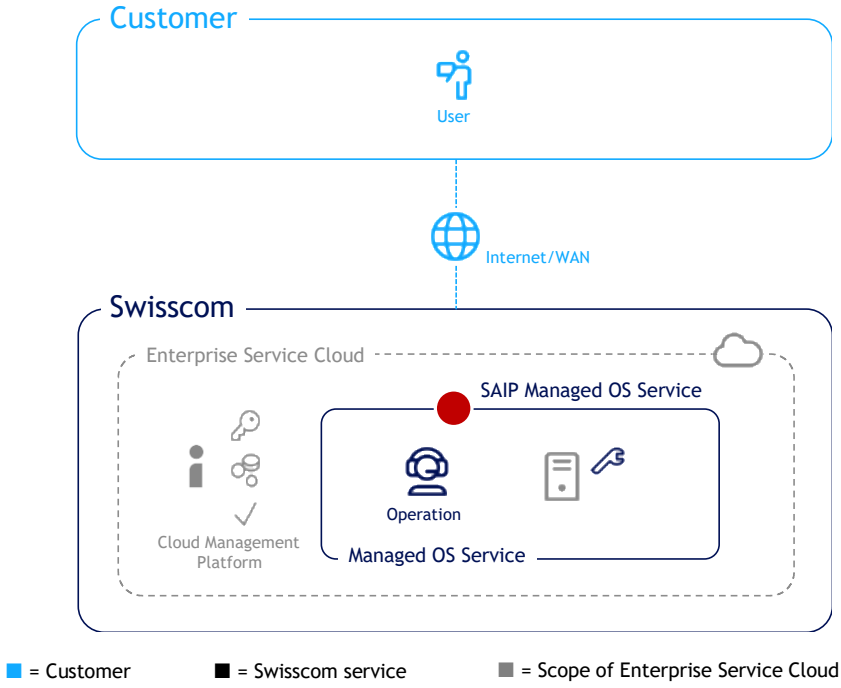
The Managed OS services can be purchased on the basis of Swisscom standard templates (blueprints) made available in the Enterprise Service Cloud service catalogue. The service is available for the Windows Server and Linux Red Hat operating systems.

2 Definitions

2.1 The Service Access Interface Point (SAIP)

The Service Access Interface Point (SAIP) is the contractually agreed, geographical and/or logical point at which a service is delivered to the service user. It is also the point at which a service is monitored and the service level provided is documented. In relation to this service description's scope of service, this is located on the virtual server's virtual network adapter on which the service is operated.

The following schematic diagram shows the services and service components of Managed OS Services:



The availability of the cloud management platform and cloud infrastructure is defined in the Enterprise Service Cloud service description.

2.2 Service-specific definitions

Term	Description
Agent	An agent (technical agent) is a software component installed on the target system (VM). The task of the agent is the performance of defined actions, such as the surveillance of monitoring metrics.
Customer Maintenance Mode	The Customer can, via self-service, set a VM containing the Managed OS service to Customer Maintenance Mode. In this mode the Customer can carry out actions which have an impact on the availability status of a VM, such as a restart of the VM.
Provider Managed Mode	"Provider Managed Mode" is the standard setting in which Swisscom provides the service for the Managed OS service.
Temp Admin	The Customer can, via self-service, set a VM containing the Managed OS service to "Temp Admin". In this mode, the Customer has temporary administration rights to the VM and can install applications.
VM	A virtual machine (VM) describes the software-related technical encapsulation of one computer system within another. The virtual machine replicates the computing architecture of a server that actually exists as hardware.

3 Variants and options

Standard variant	Enterprise Service Cloud Managed OS service
Antivirus and malware protection	●
Patching and security updates	●
Backup	●
Monitoring and alerts	●
Incident rectification	●
Temporary administration rights on the VM	●
Security reporting	○

● = Standard (included in the price) ○ = For an additional fee

3.1 Definition of the service specifications and options

The *Managed OS service* contains the operating service on the VM up to operating system level (without application operation) including rectification of faults on the virtual server selected.

The service is provided only for VMs based on Swisscom standard templates (blueprints). The service can be purchased via self-service from the cloud service catalogue by selecting a *Provider Managed Windows* or *Provider Managed Linux Red Hat* (blueprints) service.

Specification	Definition
Antivirus and Malware protection	Swisscom will ensure the protection of the server against viruses and malware. The malware/antivirus protection is implemented and operated via the agent in the respective OS. The servers are effectively protected against viruses and malware through the targeted use of antivirus/malware software.
Patching and security updates	Operating system patches (only minor releases) and security updates are provided for the Customer by Swisscom in accordance with the instructions. When ordering, the Customer selects a defined time window for each VM during which Swisscom is entitled to install system updates and restart the VM if necessary. The time windows available for selection are distributed over several weeks per month. The distribution of new deployment packages is started in the first week of a month. The time windows distributed over various weeks each month enable the Customer to ensure a staggered distribution of patches. (e.g. in week 1 distribution on test systems, week 2 distribution on integration systems and week 3 distribution on production systems)
Backup	Image-based backup to back up the VM (snapshot of the VM and save the data as backup in a remote location). Ability to restore the VM on demand. Standard Backup Policy daily snapshot with 30 days retention time. Supplementary use of agent-based backup to back up MS SQL databases and transaction logs to consistently restore databases.
Monitoring and event management	As part of the service, monitoring is carried out at operating system level to identify instances of threshold values being exceeded and corresponding alerts are sent to the persons responsible for operations at Swisscom. The monitored threshold values are documented in the “technical product description”.
Incident rectification	Rectification of faults at operating system level and ensuring availability according to the agreed service level. If the resolution of the incident requires the involvement of the customer, Swisscom will contact the customer. (No rectification of faults for software components/applications that are installed on the operating system by the Customer.)

Specification	Definition
Temporary administration rights on the VM	When ordering the Managed OS service, the Customer loses their permanent administration rights at operating system level. The Customer can apply for administration rights to the VM for the installation of applications on the VM via self-service. An automated process enables the setting of a password and therefore privileged access to the VM within minutes. The service levels are not active in "Temp Admin" mode. Once the work has been completed, the Customer can once again start the process for the switch to "Provider Managed Mode" via self-service. To verify that the system meets the security requirements and operating system settings, Swisscom carries out automated compliance checks. The results of the checks can be viewed by the Customer in a report. If divergent settings are discovered during the checks, they must be rectified by the Customer. The VM can be set to "Provider Managed Mode" only after successful performance of the checks. The service levels are reactivated only after the successful switch to "Provider Managed Mode". If the Customer has to carry out only one action which has an impact on the availability status of the VM, the Customer can set the VM to "Customer Maintenance Mode" status via self-service. This status allows, for example, the restarting of a VM and prevents the triggering of false monitoring alerts. Once the action has been carried out, the Customer can easily switch the VM back to "Provider Managed Mode" without the additional performance of compliance checks. The service levels are likewise not active in the "Customer Maintenance Mode" and are reactivated only once the status has been set to "Provider Managed Mode". The details on the VM change of status and the defined compliance checks are documented in the technical product description.
Security reporting	The security reporting provides status information on patch management, malware protection and hardening. The report can be requested by the customer and is provided in pdf format on a monthly basis.

4 Service provision and responsibilities

4.1 Managed OS service

Non-recurring services

Activities (S = Swisscom/C = Customer)	S	C
Provisioning of the service		
1. Ordering of the "Managed OS" service in the self-service portal or via API with the appropriate OS derivative. This is done through the ordering of a blueprint which contains Managed OS services (e.g. Managed Windows).		✓
2. Provision and switch of the virtual server to "Managed OS" mode.	✓	
3. Installation of the required agents on the VM for the provision of the Managed OS service.	✓	
4. Creation of the required provider firewall rules to ensure communication with peripheral systems (monitoring server, logging server, patching server, backup server, malware protection management server).	✓	
5. Connection of the virtual server to the required peripheral systems (monitoring server, logging server, patching server, backup server, malware protection management server).	✓	
6. Takeover of operation by Swisscom.	✓	
7. Designation of a technical contact person who can be contacted by[1] Swisscom if necessary.		✓

[1] The contact details of a team/role are preferred rather than an individual person. E-mail and telephone contact must be possible.

Activities (S = Swisscom/C = Customer)	S	C
Termination of the service		
1. Deletion of the VM or de-selection of the “Managed OS” service in the self-service portal of the VM concerned.		✓
2. Responsibility for timely data back-up. (The applicable licence provisions of the respective software provider must be adhered to.)		✓
3. The customer can order the immediate deletion of backup data by means of a service request from Swisscom. Without an order, backup data will be stored until the end of the retention period agreed in accordance with the backup policy.		✓
4. Release of Swisscom from all contractual obligations relating to data storage.		✓

Recurring services

Activities (S = Swisscom/C = Customer)	S	C
Standard services		
1. Availability management: Ensuring availability in accordance with the agreed service levels of the server managed up to operating system level.	✓	
2. Antivirus and malware management: Swisscom ensures responses to the latest threats and the appropriate updating of signature files.	✓	
3. Patching: Swisscom automatically carries out the patching of the operating system during the maintenance windows defined by the Customer. Details on OS patching (patching cycle, emergency patches etc.) can be found in the technical documentation.	✓	
4. Performance of major upgrades (change of operating system).		✓
5. Monitoring and event management: Monitoring of the resources for the server infrastructure components: vCPU, memory and storage. The following responsibilities will apply within the scope of the service:	✓	
▪ Monitoring of faults at operating system level	✓	
▪ Monitoring of faults for software components based on the operating system		✓
▪ Monitoring of the OS drive and its correct size	✓	
▪ Monitoring of the size of added virtual disks		✓
6. Alerts: If the monitoring threshold values are exceeded, an alert is sent to the operating organisation of Swisscom and the incident management process is triggered.	✓	
7. Incident and problem management: Fault rectification and problem resolution to restore agreed service levels. (Fault reports are generated by the monitoring tools or can be reported by the Customer via the standard incident management process.) If the rectification of incidents requires the support of the Customer (for example, due to dependency on installed applications), Swisscom makes contact with the technical contact person designated by the Customer. The service level will be suspended until the Customer responds. Swisscom will also inform the technical Customer contact person if the resolution of an incident required the modification of assigned system resources (e.g. vCPU, memory, storage).	✓	
8. Connectivity management: Operation of the necessary components for the connection between the server systems and the storage.	✓	

Activities (S = Swisscom/C = Customer)	S	C
9. Migration to the subsequent OS versions (performance of major upgrades/change of operating system): Servers will be switched over to supported OS variants in the life cycle if the existing OS is excluded from the support cycle of the manufacturer. The Customer will be responsible for migrations of this kind.		✓

Licences

Provisioning obligations (S = Swisscom/C = Customer)	S	C
Provision of licences		
1. Swisscom ensures the correct licensing of the operating system for each VM within the framework of the Enterprise Service Cloud. For details, see the Enterprise Service Cloud service description.	✓	
2. The Customer is responsible for the correct licensing of additionally installed software.		✓

5 Service Level and Service Level Reporting

5.1 Service Level

The following service levels generally relate to the agreed Support Time. Definitions of terms (Operation Time, Support Time, Availability, Security and Continuity) and the description of the measurement method and reporting are based on the other contractual elements (e.g. “SLA definitions”).

The following service levels are provided for the service variants (see section 3). If several possible service levels are available for each variant, the service level is selected in the service contract.

		Managed OS Service		
Service level & target values		**Basic**	**Standard**	**Advanced**
Operation Time				
Operation Time	Mo-Su 00:00-24:00		●	
Provider Maintenance Window	Dependent on the time window (at VM level) selected by the Customer in the cloud portal		●	
Support Time				
Support Time	Mo-Fr 07:00-18:00	●	–	–
	Mo-Su 00:00-24:00	–	●	●
Fault Acceptance	Mo-Su 00:00-24:00	●	●	●
Availability				
Service Availability	99.9% - Self-service portal and cloud management API	●	●	●
	99.5% - Operating system	●	–	–
	99.9% - Operating system	–	●	●
Security				
	Basic (ITSLB)	●	●	●

Service level & target values		Managed OS Service		
		Basic	Standard	Advanced
Continuity				
ICT Service Continuity (ICTSC) [2]	RTO Best Effort | RPO Best Effort	●	●	–
	RTO 4 h | RPO Near to 0	–	–	●
ICT Business Continuity (ICTBC) [3]	Offered according to separate service description ICT Business Continuity	–	–	○

● = Standard (included in the price) ○ = For an additional fee – = Not available

Remarks:

- The service level variant "Basic", "Standard" and "Advanced" is selected when ordering a blueprint of the Managed OS. The service level of the VM also determines the service level for the Managed OS service (e.g.: If the Customer selects the standard service level for the VM, the standard service level also applies to the Server OS Management service).
- The "Advanced" service level variant contains the service continuity services at VM level. Neither recovery at application level nor its regular "failover tests" are part of this service.
- Outages resulting from software faults by the operating system manufacturer result in the suspension of the guaranteed service level.

5.2 Service Level Reporting

As part of the service, the Customer receives the following standard service level reports. Further reports can be provided, subject to charge, as part of the advanced reporting service after assessing the feasibility of the Customer's requirements.

Service Level Report		Enterprise Service Cloud Managed OS Services	Reporting period
Availability	Availability in % of the service at the SAIP during the measurement period	●	Monthly
Security	Customer notification in the event of knowingly deviating from ITSLB and not automatically correctable security breaches.	●	In the event of a security violation

● = Standard (included in price)

[2] ICT Service Continuity for instantiated objects (i.e. VMs) requires that the customer has purchased the Backup option for the objects that need to be restored in the event of a disaster.

[3] Customer instances can also be secured using the ICT Business Continuity service. This involves the services for IT Business Continuity being governed in a separate contract with a separate service contract in addition to the scope of service of the Enterprise Service Cloud. If the ICTBC service is used, a customer-specific restart plan is produced for the solution and subjected to a customer-specific IT Business Continuity Test in accordance with the agreed scope of service on a regular basis. ICTBC tests for instantiated customer objects can be carried out in the cloud at a virtualisation level. (Example: For a VM to run the "Power Off" command and force a restart of the VM in the second data centre.) Switching off lower-level hardware components for the ICTBC test is not possible in the Shared Cloud Environment for individual customer tests.

6 Billing and quantity report

6.1 Billing

The prices of the Managed OS service are determined on the basis of a period of usage of at least one hour. Services are billed to the Customer retroactively for the previous month. The values for the effectively used Managed OS services are calculated pro rata on an hourly basis based on the VM status started and invoiced based on the current price list. Computing resources, amount of storage and backup data as well as licenses are charged according to the Enterprise Service Cloud service description.

Price position	Unit/period	Minimum purchase Billing	Maximum purchase Billing	Quantity included
Managed OS Service	No. VM/hour	1	Unlimited	–

6.2 Quantity report

For the Swisscom Managed OS service, reports on the following data and information on the services rendered are provided together with the monthly invoice: The resources and services used will be billed to the Customer retroactively for the previous month. The values for the effectively used resources are calculated pro rata on an hourly basis and invoiced based on the current price list.

Quantity report **Product services/options**	**Reporting information on billing**
Managed OS Service	Total volume Managed OS Services

7 Special provisions

7.1 Lifecycle management

Swisscom reserves the right to upgrade the virtualisation infrastructure hardware and software quarterly in line with the latest releases and versions. The system costs are borne by Swisscom. Expenses incurred for any modifications to Customer applications and upgrades to Customer software, for example, are charged to the Customer.

Swisscom reserves the right to install the standard patching for all systems on the infrastructure during any maintenance windows. If the services provided by Swisscom include third-party products, the Customer will also respect the terms and conditions of use and licence terms and conditions associated with these. Swisscom will be entitled to enforce these terms and conditions vis-à-vis the Customer.

7.2 Miscellaneous

- Unless it explicitly transfers these tasks to Swisscom, the Customer will be responsible for the set-up of the virtual servers and complete operation (incl. maintenance, monitoring, patching, support etc.) of its Customer solutions from operating system level. This includes the required middleware, databases and applications.
- End-to-end availability measurement and availability guarantees for applications and appliances are not included.
- The “Managed OS Service” is available only for OS versions that still at least receive “Extended Support” from the manufacturer and are listed in the service catalogue. If a previously supported version is excluded from the service catalogue, Swisscom will provide notification of this 6 months in advance. It is the Customer’s responsibility to migrate applications to a supported operating system version according to the service catalogue during the transitional period. At the end of the period indicated, the status of VMs no longer supported by Swisscom for Managed OS services according to the service catalogue will be set to “Temp Admin”. Operating system services must be performed by the Customer from this point in time for these VMs and Swisscom will be released from the provision of Managed OS operating services on these VMs.

- In addition to the other disclaimers of warranty, Swisscom also excludes any warranty in the following cases:
  - Restricted availability due to insufficient measurement of resources (e.g. Java settings, incorrect configuration of middleware) by the Customer.
  - Outages for which Swisscom is not directly responsible, in particular external DNS routing problems, virtual attacks on Swisscom's network infrastructure (DDoS/viruses) and outages experienced by parts of the Internet outside Swisscom's control which lead to misinterpretations by the Customer.
  - Outages for which the Customer is at fault, in particular outages caused by incoming/outgoing hacker attacks (DDoS) as a consequence of erroneous or insufficient maintenance of the Customer's own software
  - Outages resulting from software errors of the manufacturer's operating system.
  - Outages that occur because the systems have not been installed, operated and maintained in
  - Temporary freezing of the operating system can occur during the automated image backup process (only with selected backup policy) where this is based on a VMware Snapshot. (This behaviour depends on the application installed).
- The Customer is responsible for all specifications concerning the storage and deletion of its data:
  - The accuracy of the content saved by the Customer
  - The compliance of the stored content with legal requirements (e.g. Swiss Data Protection Act)
  - Deletion of, or amendments to, data by the Customer itself
  - The accuracy of the Customer's instructions to Swisscom regarding storage periods and data deletion
- Swisscom will set up and operate an Active Directory Resource Domain in a business group managed by Swisscom for the operation of Managed OS services. VMs using the Managed OS service must be part of this resource domain. The Customer will allow the resource domain to connect to its active directory using "one-way trust".
- The Customer cannot directly access hardware interfaces or disk drives. (Access to serial ports, parallel ports, the firewire connection, USB, CD/DVD-ROM are available on a virtual basis.)
- The Customer is obliged not to stop or change installed VMware tools.
- Customer-specific software or Customer data must be installed or deposited on its own drive. The operating system drives (e.g. C: or /) are reserved for the provider.
- No local administrator accounts may be created while in Customer Maintenance Mode. Swisscom reserves the right to remove this from the administrators group when switching to the Provider Managed Mode.
- To guarantee the virus protection service, no other virus protection solutions may be installed by the Customer.
- To enable Swisscom to provide the antivirus, monitoring, alerting and security patching services, additional software solutions, such as configuration management agents, will be deployed. These are under the control of the provider and cannot be stopped, deactivated or otherwise manipulated. Identical configuration management tools must be determined on a customer-specific basis.
- Provider rules cannot be changed, deleted or interfered with in the local firewall of the Managed OS.
- The Swisscom Security Team regularly issues new requirements concerning the security settings of the operating systems. Examples may include the deactivation of old encryption ciphers. Such changes are published for the introduction in the Blueprint by means of release notes and, if required, communicated for existing instances by means of a regular change process. Such changes can be made in the blueprint without prior notice.
- The compliance checks may be supplemented with other checks without notice. Results of the compliance checks can be seen when changing variant to Provider Managed.
- Swisscom reserves the right to reverse changes made by the Customer to the operating system configuration which result in security or operating restrictions and which are not identified by compliance checks. The implementation of such configuration changes is carried out in consultation with the Customer.

- Swisscom reserves the right to amend this service description on a unilateral basis at any time. Amendments that are necessary due to the service being extended or that do not negatively affect contractual use of the service by the Customer shall be announced as part of the release notes sent to all subscribers by e-mail. Where an amendment negatively affects contractual use of the service by the Customer (esp. if functionalities cease to be available), Swisscom shall inform the Customer about the details of the amendment and the date on which it will take effect at least six months in advance. In this case, both parties agree to seek an amicable solution to the consequences of such amendment, and to do so in good faith. If the parties fail to come to an agreement regarding the consequences of the contractual modification, the Customer shall be granted the right to terminate the relevant service contract in writing with effect from the date on which the amendment is set to take effect, subject to two weeks' notice. No further claims may be made by the Customer.

7.3 Data protection provisions

7.3.1 Data processing by third parties in Switzerland or abroad

The data transmitted to Swisscom by the Customer (customer data) within the scope of service provision is stored in Switzerland by Swisscom. Customer data is not accessed directly within the framework of the provision of the service. Swisscom employees may require access to technical system data as part of service provision. If necessary, information (such as dump files, SOS reports or system-specific log files) can be made available to third parties commissioned by Swisscom for the purpose of error analysis. It is ensured that only technical information (such as IP addresses, host names) is transmitted. Should it be necessary to transmit further information – which may contain customer data (e.g. from a memory dump) – this requires the Customer's prior written consent in each individual case. For its part, the Customer shall ensure that no customer data (e.g. from software components for which the Customer is responsible) is written to system-specific log files.