

Service Description – STACKIT Cloud

1 General

1.1 Introduction

Under the STACKIT brand, Schwarz Digits Cloud GmbH & Co. KG, Am Campus 1, 74177 Bad Friedrichshall, Germany, Registry Court Stuttgart, HRA 741347 ("**STACKIT**"), is a national provider of professional Infrastructure- & Platform-as-a-Service services ("**STACKIT Cloud Services**") based on state-of-the-art open source technologies and established de facto standards. These services are provided as a public cloud option exclusively to traders, legal persons under public law and special funds under public law ("**Customers**"). STACKIT is the Cloud Service provider for Schwarz Group.

1.2 Data Center Locations and Standards

STACKIT Cloud Services are provided and operated in STACKIT data centers located in Germany, Austria and potentially other member states of the European Union in the future. Available certifications and letters of attestation are listed under <https://stackit.com/en/certificates>. As a European Cloud Service provider, STACKIT is subject to the EU General Data Protection Regulation (GDPR).

1.3 Scope of Application

This generally applicable service description ("**Service Description**") forms an integral part of the agreement on the purchase of any STACKIT Cloud Services in addition to the Terms of Use and the Customer's selected Service Certificate(s).

In the event of conflicts between the Terms of Use, the Service Description and the applicable Service Certificate, the Service Certificate shall be controlling over the Service Description and the Terms of Use; the Service Description shall be controlling over the Terms of Use.

1.4 Amendment of the Service Description

If there is a valid reason to amend or supplement the Service Description and such amendment or addition does not unreasonably disadvantage the Customer, in particular because the cost/benefit ratio does not disproportionately shift to the detriment of the Customer, STACKIT shall be entitled to amend the Service Description, in whole or in part, with prospective effect. Such valid reasons shall include in particular regulatory or legal reasons, security reasons, enhancing, optimizing or adding services, making technical adjustments and ensuring the functionality of the portal.

If the Service Description is amended, the Customer shall be notified of the amendments by e-mail at least eight (8) weeks before the new Service Description enters into effect. Amendments shall be deemed approved if the Customer, after having received the notice of amendment, does not expressly object to them on or before the date on which they enter into effect. The Customer will be specifically advised in the notice of amendment of this legal consequence, the start of the period, the deadline and the date on which the amendment enters into force. In the event that the Customer objects to the amendment, STACKIT shall be entitled to a special right of termination with immediate effect with regard to those STACKIT Cloud Services affected by the amendment.

Where a amendment to the Service Description merely extends or adds to the existing services STACKIT provides to the Customer (on an optional basis), STACKIT is entitled to notify the customer of such amendments within a shorter period; in such cases, the Customer has no right to object.

2 Service Level Agreement

2.1 Service Transfer Point

The service responsibility for the STACKIT Cloud Services to be provided on the part of STACKIT ends at the Internet transfer point between the respective data center operated by STACKIT and the Internet service provider of the respective region.

2.2 Operating Hours

The operating hours for the STACKIT Cloud Services are Monday to Sunday, "24/7", 365 days a year (excluding scheduled maintenance work).

2.3 Availability

The general availability of any STACKIT Cloud Service is 99.9% (99.5% for non-redundant STACKIT Cloud Services) per calendar month – after deducting the Excluded Events pursuant to clause 2.4 – unless otherwise stipulated in the respective Service Certificate on which the STACKIT Cloud Service is based ("**Availability**"). The information on Availability does not apply to the availability of the Customer's own components or third-party components (software and hardware).

Availability per calendar month shall be calculated as follows:

Availability in % = (Total Service Minutes – Total Downtime Minutes) / (Total Service Minutes) x 100

- Availability always refers to a calendar month, is calculated on a calendar month basis, and is reported as a percentage.
- "Total Service Minutes" means the total number of calendar month minutes (calculation: 60 minutes x 24 hours x number of calendar days in the month)
- "Total Downtime Minutes" means the number of minutes per month in which the STACKIT Cloud Service owed was not provided. The number of minutes per month that are not included in the calculation of Availability as Excluded Events within the meaning of clause 2.4 shall be deducted from the value of the Total Downtime Minutes.

The availability of the STACKIT Portal and the STACKIT Application Programming Interface (API) is not subject to any Availability commitment by STACKIT. However, STACKIT aims to achieve an average monthly Availability of 99.9% for both the STACKIT Portal and the STACKIT Application Programming Interface (API). Downtime, disruptions or other instances where the STACKIT portal or the STACKIT Application Programming Interface (API) is unavailable shall not affect the calculation of the availability of any STACKIT Cloud Service.

2.4 Excluded Events

Excluded Events refer in particular to periods in which the contractual provision of the STACKIT Cloud Services cannot be achieved due to the following instances of downtime and disruptions ("**Excluded Events**"). Excluded Events do not count as downtime. Excluded Events include in particular:

- Downtime and disruptions for which STACKIT is not responsible, in particular DNS and routing problems or unauthorized interference from third parties, such as virtual attacks on the network or mail infrastructure (e.g., DoS, viruses or spam).
- Downtime and disruptions resulting from the implementation of countermeasures against unauthorized interference or due to security incidents.
- Downtime and disruptions of third-party services beyond the control of STACKIT or which are not attributable to the service provided by STACKIT or the network structure outside STACKIT's sphere of control.
- Downtimes and disruptions caused by the Customer. These include, for example:
 - Incorrect entries or non-compliance with instructions.
 - Actions or omissions of the Customer which exceed the prescribed and/or booked quotas.
 - Acts or omissions of the Customer to make and/or comply with required configurations.
- Downtime and disruptions due to force majeure. Force majeure is an event that could not have been foreseen by either party using the utmost care that could reasonably be expected; force majeure in this sense may include in particular the following events: Fires, explosions, power outages, earthquakes, floods, severe storms, strikes, embargoes, labor disputes, acts of civil or military authorities, war, terrorism (including cyber-terrorism), epidemics and pandemics, acts or omissions of Internet providers, acts or omissions of regulatory or administrative bodies (including the enactment of laws or regulations or other governmental actions affecting the provision of STACKIT Cloud Services).
- Downtime and disruptions that occur due to maintenance work in accordance with clause 2.8.

No Availability commitment is given for STACKIT Cloud Services that are provided to the Customer free of charge or explicitly designated and marketed as a trial or beta version or the like. Downtime or disruptions that occur due to the Customer's use of such services are deemed to be Excluded Events.

2.5 Supported Software Versions

STACKIT Cloud Services may have specific software versions ("**Major Versions**") at the time a contractual relationship is entered into. In order to keep the STACKIT Cloud Services and the provision of services to the Customer secure and up-to-date, STACKIT reserves the right to replace the Major Versions of the software used with successor versions ("**Successor Versions**"), including for contractual relationships already entered into.

In such case, the following shall apply in particular:

- STACKIT shall notify affected Customers about the upcoming change and the end of the support period for Major Versions in the release notes at <https://docs.stackit.cloud/display/STACKIT/Release+Notes> ("**Release Notes**").
- The Major Version affected by the change will be supported for at least another 180 calendar days, calculated from STACKIT's announcement of the change in the Release Notes, and then successively migrated to the Successor Version in a timely manner ("**Transition Period**").
- During this Transition Period, it will still be possible to enter into agreements based on the Major Version, but these will also have to be migrated to the Successor Version when the Transition Period ends. Customers are therefore advised to consult the Release Notes to find out about any announced changes to Major Versions before purchasing a subscription to a STACKIT Cloud Service; for Customers subscribing or renewing a subscription to the STACKIT Cloud Service affected by a change during the Transition Period, the affected STACKIT Cloud Service will only be available in the subscribed Major Version until the Transition Period ends, which, depending on when the subscription is taken out, may be significantly less than 180 calendar days.
- Provided this is offered, technically feasible and requested by the Customer, the Customer will have the option, even before the Transition Period ends, to migrate affected Major Versions to the Successor Versions or – depending on the STACKIT Cloud Service – to have STACKIT perform the migration. However, the Customer has no claim to any such early migration.
- Once the Transition Period ends, STACKIT will successively migrate Major Versions not yet migrated by the Customer to the Successor Versions in a timely manner.
- In some cases where the Major Version is migrated to the Successor Version, STACKIT may not be able to properly perform an automatic migration (particularly of customer data) without the Customer's assistance. In those cases, STACKIT will notify the affected Customers in the Release Notes if any cooperative action is required. The Customer then has until the end of the Transition Period – calculated from the date on which the required cooperative actions are published in the Release Notes – to carry out the required cooperative actions.

- Once the Transition Period ends, STACKIT will no longer provide support for the Major Version and the Customer may also not be able to use it any longer; if and to the extent technically feasible, STACKIT may perform an automatic migration of the Major Version to the Successor Version, even if the Customer has not carried out the cooperative actions beforehand; this may, in particular, result in data loss and loss of functionality or functional limitations of the affected STACKIT Cloud Service, as well as of the Customer's own hardware and software or third-party hardware and software used in connection with it. STACKIT assumes no liability for loss or damage incurred by the Customer as a result of any failure to perform or have performed any (automatic) migration, except in those cases set out in clause 15.1 of the Terms of Use.
- Once the software has been migrated from its Major Version to the Successor Version, the Successor Version becomes the (new) Major Version for purposes of this clause.

2.6 Service Deprecation

Every STACKIT Cloud Service is subject to a product life cycle defined by STACKIT. STACKIT will announce the discontinuation of the affected STACKIT Cloud Service or an essential functionality of a service ("**Deprecation**") in the Release Notes at least 360 calendar days before the discontinuation date. Once Deprecation enters into effect, the affected service or functionality will no longer be available for use by the Customer.

STACKIT will provide information about any successor products (if any) in the announcement made in the Release Notes.

2.7 Backup

STACKIT will only perform a data backup if this is either a) specified in the Service Certificate or b) the backup function (where available) was activated by the Customer when purchasing or configuring the relevant subscription to the STACKIT Cloud Service via the portal or the STACKIT API.

When a backup is performed, the data backup for the relevant STACKIT Cloud Service is carried out in accordance with the following standards, unless otherwise stipulated in the individual Service Certificate or configured by the Customer:

Backup Parameters	Value
Recovery Point Objective (RPO)	4 hrs.
Recovery Time Objective (RTO)	4 hrs.
Retention Period (RP)	14 days, daily retention after the first 4 hrs.

- "Recovery Point Objective" (RPO): The RPO or the maximum acceptable amount of data loss, covers the requirement of how old the status of the last current, consistent data backup may be. In the event of a data-loss incident and any necessary data restore, this backup status can be reverted to.

- "Recovery Time Objective" (RTO): The RTO or the maximum acceptable recovery time, describes the period of time in which a data restore to a functionally available system, including operating system data and required (application) data, can be consistently recovered on the basis of the restore.
- "Retention Period" (RP): The RP describes the maximum period for the retention of backups.

2.8 Maintenance Work

STACKIT carries out regular maintenance work (e.g., in the form of updates, patches, bug fixes or hardware replacements and hardware extensions) to ensure the function, quality and security of the STACKIT Cloud Services.

STACKIT may carry out maintenance work that is not likely to impair the usability of the STACKIT Cloud Services for the Customer ("**Non-disruptive Maintenance Work**") at any time, even without prior notice.

STACKIT generally announces maintenance work that is likely to impair the usability of the STACKIT Cloud Services for the Customer ("**Disruptive Maintenance Work**") on the STACKIT Cloud Status website two weeks before it is carried out. For urgent maintenance work, involving security-related changes for example, the announcement can also be made at much shorter notice or, depending on the individual case, without prior notice. STACKIT recommends that Customers regularly check the status of maintenance work on the STACKIT Cloud Status website.

While Disruptive Maintenance Work is being carried out, access to STACKIT Cloud Services may be temporarily suspended or restricted, especially if this is absolutely necessary due to the nature of the maintenance work to be carried out.

Downtimes resulting from Disruptive Maintenance Work carried out shall be treated as Excluded Events within the meaning of clause 2.4.

2.9 Service Payback

If the agreed availability of STACKIT Cloud Services is not provided as described, the Customer shall receive a credit to their Customer account ("**Service Payback**"):

- In order to assert a Service Payback claim, the Customer must provide notification in text form within two (2) weeks of receipt of the invoice for the affected STACKIT Cloud Services, stating the Customer number, invoice number and the affected STACKIT Cloud Service, that the agreed Availability has not been provided. Any claim not received within two (2) weeks cannot be considered.
- If the claim is justified, the Customer will receive a Service Payback credit to their Customer account for the following billing period.
- The amount of the Service Payback always relates to the pro rata invoice amount for the STACKIT Cloud Service with respect to which the agreed Availability was not complied with.

- If a Customer's Service Payback claim is rejected, it is the Customer's responsibility to demonstrate the breach of the agreed Availability of a STACKIT Cloud Service.
- Credited Service Payback is offset against remuneration claims for the provision of STACKIT Cloud Services in the subsequent billing period, so that the Customer's fee to be paid is reduced accordingly.
- A payout or other reimbursement of the credited Service Payback is excluded.
- The following Service Paybacks apply, unless otherwise stipulated in the STACKIT Cloud Service Service Certificate:

Availability (month)	Service Payback
< contractually agreed Availability %*	10%
* See clause 2.3.	
< 99.0%	20%
< 98.5%	50%
< 95.0%	100%

Any further claims of the Customer for a reduction of the remuneration shall be excluded. Any claims for damages on the part of the Customer shall remain unaffected. Any Service Payback received shall be offset against any claim for damages asserted.

3 Incidents & Security Incidents

3.1 Information

STACKIT regularly provides Customers with information about incidents via the STACKIT Cloud status website (status.stackit.cloud).

In the event of security incidents, the Customers affected by the security incident are notified directly.

STACKIT recommends that Customers continuously check the status of Incidents & Security Incidents on the STACKIT Cloud Status website.

3.2 Analysis by STACKIT

For STACKIT Cloud Services provided by STACKIT and used by the Customer who purchased the STACKIT Cloud Services, STACKIT can take measures at its own discretion to detect vulnerabilities at an early stage, both in STACKIT's area of responsibility and in the Customer's Area of Responsibility. In particular, the Customer shall be responsible for all hardware, applications and software of third parties that are not provided by STACKIT ("**Customer's Area of Responsibility**").

If security incidents in the Customer's Area of Responsibility are detected by STACKIT or external service providers of STACKIT, the Customer will be informed of these. Depending on the severity of the security incident, the Customer is obligated to take suitable measures to prevent the security incident in its area of responsibility in a timely manner (e.g., by patching an affected application). If, for example, the Customer's Area of Responsibility is not secured with the latest patches or workarounds, if the area of responsibility harbors security risks for STACKIT or the Customer itself, or if the quality of the STACKIT Cloud Services is adversely affected or jeopardized by a Security Incident in the Customer's Area of Responsibility, STACKIT reserves the right to take appropriate countermeasures in accordance with clause 3.4.

3.3 Data Collection for Purposes of Analysis by STACKIT

To detect possible security incidents in the Customer's Area of Responsibility, log data from Customer systems or perimeters (e.g., firewalls, switches, routers and others) can be analyzed for anomalies and potential security incidents based on rules. Appropriate vulnerability scans (proactive and reactive) can also be carried out for systems available on the Internet.

3.4 Possible Countermeasures for Security Incidents

To protect the Customer and the STACKIT Cloud Services, STACKIT reserves the right to take appropriate measures without prior notice or consultation with the Customer in the event of suspected or proven security incidents and corresponding severity ("**Countermeasures**"). The Customer will receive separate notification in this respect subsequently at the latest. The Countermeasures include in particular:

- Disconnect affected systems and STACKIT Cloud Services from the network, shut them down or pause them to prevent damage to systems and the STACKIT Cloud Services.
- Forensic analysis of possible affected systems and STACKIT Cloud Services (in particular to gain insights for law enforcement, criticality or damage assessment).
- Other activities to avoid or reduce interference with other Customer systems of the STACKIT Cloud Services or external systems.

3.5 Technical Modifications for the Purpose of Resolving Security Incidents

The Customer will be informed without delay of technical modifications deemed necessary and implemented by STACKIT for the purpose of resolving security incidents. If the Customer fails to raise justified objection to such technical modifications within 14 calendar days of receiving notice thereof, such technical modifications will be deemed accepted by the Customer.

The Customer will only have a right to object if the scope of the STACKIT Cloud Services is substantially reduced or the Customer is no longer able to use or access the STACKIT Cloud Services after such technical modification as contractually agreed due to the technical modification made.

In the event of a valid objection, the Customer shall grant STACKIT the opportunity for remediation. As part of such remediation, STACKIT shall use commercially reasonable efforts to achieve a solution that is more acceptable to the Customer with regard to resolving the Security Incident. If STACKIT justifiably refuses the remediation (e.g., due to technical infeasibility, continuation of the Security Incident, or commercial unreasonableness), or if the Customer's grounds for objection persist following the remediation, STACKIT shall continue to provide the affected STACKIT Cloud Service with the implemented technical modifications, and the Customer shall have the right to extraordinary termination of the affected subscribed STACKIT Cloud Service with immediate effect.

4 Support

STACKIT shall provide support services to its Customers in relation to the STACKIT Cloud Services accordance with the terms and conditions set out in **Appendix A: Support Plans** to this Service Description.

APPENDIX A: Support Plans

A.1 General

STACKIT offers support services for the purchase of STACKIT Cloud Services, which are specified in this Appendix A: Support Plans. The provisions of this Appendix A shall apply to every support plan provided by STACKIT (see clause A.5), unless deviating provisions are agreed between STACKIT and the Customer in a separate agreement for support services.

Every STACKIT Cloud Service is covered by STACKIT Essential Support ("**SES**") as the standard support plan; the SES does not require a separate booking or order by the Customer.

A.2 Support Requests

A.2.1 Customer requests are divided into the categories of business-critical incident, incident, and service request (collectively "**Support Requests**") based on the content of the request.

A.2.1.1 A business-critical incident is when, as a result of a disruption in a STACKIT Cloud Service used by the Customer,

- a partial or total failure of essential functions of the Customer's business operations occurs;
- the Customer is at risk of incurring significant loss or damage (e.g., financial or reputational); or
- the Customer can no longer comply with its statutory obligations (hereinafter "**Business-critical Incident**")

A.2.1.2 An incident is when a service used by the Customer is disrupted, i.e., it deviates from the agreed service and this deviation has an adverse effect on the use of the STACKIT Cloud Service by the Customer ("**Incident**").

A.2.1.3 A Service Request occurs when the Customer submits general service or support inquiries that are not based on a disruption of a utilized STACKIT Cloud Service ("**Service Request**").

A.2.2 When submitting the Support Request, the Customer may provide an assessment of the category of its request, along with a justification of the circumstances.

A.2.3 If no category is specified by the Customer, STACKIT shall assess the category itself based on the information provided by the Customer.

A.2.4 In any event, STACKIT reserves the right to reclassify the category assignments made by the Customer if the information submitted to justify the Customer's assessment is not appropriate or sufficient from STACKIT's reasonable perspective.

A.2.5 STACKIT shall make every commercially reasonable effort under the given circumstances to resolve Support Requests within a reasonable period of time.

A.3 General Obligations of the Customer to Provide Cooperative Assistance with Support Requests

A.3.1 The proper performance of the agreed support services by STACKIT is only possible if the Customer complies with its duty to provide reasonable cooperative assistance with regard to Support Requests.

Within the scope of its duties of cooperation, the Customer shall in particular:

- Check extensively before submitting a Support Request whether it is capable, based on the resources and information available to it, of resolving the issue itself.
- Check before reporting Incidents and Business-critical Incidents whether the cause of the disruption lies within its area of responsibility.
- Assign personnel for communication regarding Support Requests who are technically familiar with both the STACKIT Cloud Services and the relevant Customer environment. In this context, the Customer shall ensure that it appoints one or more qualified contact persons with sufficient decision-making authority for each Support Request. For the processing duration of a Support Request, the Customer ensures the availability—both in writing and by telephone—of at least one such contact person, who shall fulfill the Customer's cooperation obligations upon STACKIT's request.
- Provide all information relevant to the processing when submitting Support Requests. This includes, in particular, unique identifiers for the projects or services to which the request relates, detailed descriptions of the observed state of the affected services, a clear formulation of the expected target state, a comprehensive outline of any steps required to reproduce the errors, a description of the activities undertaken by the Customer to date, and the provision of relevant logs.
- Carefully consider classifying an incident as business-critical. If the Customer identifies a Business-critical Incident, it must provide STACKIT with a clear explanation of the impact on its business operations when reporting the incident. If, after careful consideration of the explanation provided, STACKIT is unable to conclude that the impact of the incident meets the definition of "business-critical" set out in clause A.2.1.1, STACKIT reserves the right to change the classification.
- In the event of an Incident or a Business-critical Incident that can be attributed to an ongoing major disruption of the STACKIT platform (Major Incident), STACKIT shall inform the Customer accordingly. Further communication regarding the resolution progress of the major disruption until its conclusion shall take place via the STACKIT status page. In such cases, the Customer shall continuously monitor the status via the status website.

A.3.2 The foregoing list of duties of cooperation is not exhaustive. In individual cases, the Customer may be required to provide additional cooperative assistance in order to process a Support Request properly. STACKIT shall inform the Customer in a timely manner of any cooperative action that is required. Should the Customer fail to meet its duties of cooperation to the necessary extent in the quality or scope as required by STACKIT, STACKIT reserves the right to suspend the processing of a Support Request until the necessary cooperative assistance is provided by the Customer and, should the Customer fail to provide the necessary cooperative assistance even after being requested to do so by STACKIT, cease processing the Support Request.

A.4 Access to the Customer's Cloud Services

In order to process Support Requests of the Customer properly, it may be necessary for STACKIT to access the STACKIT Cloud Services utilized by the Customer. By submitting a Support Request to STACKIT, the Customer consents to such access by STACKIT solely to the extent necessary to process the respective Support Request. This does not affect contractual and statutory obligations on the part of STACKIT, which it must continue to meet in this context.

A.5 Support Plans

A.5.1 STACKIT offers its Customers a variety of support plans to choose from, which vary in terms of the scope of support services provided, service hours, and reaction and response times.

These are currently:

- STACKIT Essential Support ("SES")
- STACKIT Ultimate Support ("SUS")

A.5.2 SES is automatically included with every STACKIT Cloud Service booked by the Customer and is provided by STACKIT at no additional cost.
SUS can only be purchased after the Customer has contacted STACKIT and entered into a separate agreement for SUS services.

A.6 Overview of the SES Support Plan

The following table provides an overview of the scope of SES support services. An overview of the services of the other optional support plans is available on STACKIT's website or in the associated contract documents.

Type of Service Support	SES
-------------------------	-----

Available support channels	
Support team based in the European Union	✓
Support via portal	✓
Support via telephone 10	✓
Access to Knowledge Database (docs.stackit.cloud) 20	✓
Access to Status Website (status.stackit.cloud) 30	✓
Access to Help Center (support.stackit.cloud)	✓
Availability of support channels 24/7	✓
Hours	
Service hours 40 Monday - Friday, 8:00 a.m. - 6:00 p.m. 50	✓
Reaction time in minutes - during service hours 60	target: 15
Response time in minutes for Business-critical Incidents - during service hours 70	target: 240
Response time in minutes for Incidents 70	best efforts
Response time in minutes for Service Requests 70	best efforts
Service level for support times (support SLA)	
Agreement on Compliance with Reaction Times 60	best efforts
Agreement on Compliance with Response Times 70	best efforts
Additional Services	
Monthly support SLA reports	No monthly support SLA reports

10 Hotline: +49 7132 30-474747

20 Knowledge Database documentation, Release Notes, tutorials, FAQs and known issues

30 For notification of scheduled maintenance work or important incidents

40 Service hours are the contractually agreed days of the week and time windows during which STACKIT provides its services and processes Support Requests.

50 CE(S)T [Central European (Summer) Time], excluding public holidays in Baden-Württemberg

60 Reaction time is the period of time from receipt of the Customer's Support Request by STACKIT until processing of the Support Request begins

70 Response time is the period of time from receipt of the Support Request by STACKIT until the first qualified response.

It contains a specific response to the Support Request with either

- a solution,
- a problem analysis, or
- a next step for action