

## **Servicebeschreibung STACKIT Cloud**

### **1 Allgemeines**

#### **1.1 Einführung**

Unter der Marke STACKIT erbringt die Schwarz Digits Cloud GmbH & Co. KG, Am Campus 1, 74177 Bad Friedrichshall, Registergericht Stuttgart, HRA 741347 („**STACKIT**“) als nationaler Anbieter professionelle Infrastructure- & Platform-as-a-Service Leistungen („**STACKIT Cloud Services**“) auf Basis moderner Open-Source-Technologien und etablierter De-facto-Standards. Diese werden als Public Cloud Variante ausschließlich gegenüber Unternehmern, juristischen Personen des öffentlichen Rechts und öffentlich-rechtlichen Sondervermögen („**Kunden**“) bereitgestellt. STACKIT ist der Cloud-Service Provider der Schwarz Gruppe.

#### **1.2 Standorte der Rechenzentren und Standards**

Die STACKIT Cloud Services werden in Rechenzentren von STACKIT in Deutschland, Österreich sowie künftig ggf. auch weiteren Mitgliedsstaaten der europäischen Union bereitgestellt und betrieben. Verfügbare Zertifizierungen und Testate werden unter <https://stackit.com/de/zertifikate> aufgeführt. Als europäischer Cloud Service Provider unterliegt STACKIT der europäischen Datenschutzgrundverordnung (EU-DSGVO).

#### **1.3 Geltungsbereich**

Die vorliegende allgemeingültige Servicebeschreibung („**Servicebeschreibung**“) bildet neben den separat geregelten Nutzungsbedingungen sowie den vom Kunden ausgewählten Leistungsschein(en) einen wesentlichen Vertragsbestandteil des Vertrags über den Bezug eines STACKIT Cloud Services.

Im Falle von Widersprüchen zwischen den Nutzungsbedingungen, der Servicebeschreibung und dem geltenden Leistungsschein hat der Leistungsschein insoweit Vorrang vor der Servicebeschreibung und den Nutzungsbedingungen; die Servicebeschreibung hat insoweit Vorrang vor den Nutzungsbedingungen.

#### **1.4 Änderung der Servicebeschreibung**

Für den Fall, dass dies aus triftigem Grund erforderlich ist und die Ergänzung oder Änderung der Servicebeschreibung den Kunden nicht unzumutbar benachteiligen, insbesondere weil sich das Verhältnis von Leistung und Gegenleistung nicht überwiegend zu Ungunsten des Kunden verschiebt, ist STACKIT berechtigt, die Servicebeschreibung mit Wirkung für die Zukunft ganz oder teilweise zu ändern. Hierunter fallen insbesondere regulatorische oder rechtliche Gründe, Gründe der Sicherheit, Weiterentwicklung, Optimierung und Hinzufügung von Leistungsinhalten, technische Anpassungen und die Sicherstellung der Funktionsfähigkeit des Portals. Grundsätzlich werden dem Kunden im Fall der Änderung der Servicebeschreibung die Änderungen per E-Mail mindestens acht (8) Wochen vor dem Wirksamwerden der neuen Servicebeschreibung mitgeteilt. Änderungen gelten als genehmigt, wenn der Kunde den Änderungen nach Zugang der Änderungsmitteilung und bis zum Wirksamwerden der Änderungen nicht ausdrücklich widerspricht. Der Kunde wird in der Änderungsmitteilung gesondert auf diese Rechtsfolge, den Fristbeginn, die Frist und den Zeitpunkt des Inkrafttretens der Änderung hinweisen. Für den Fall,

dass der Kunde der Änderung widerspricht, steht STACKIT ein Sonderkündigungsrecht mit sofortiger Wirkung hinsichtlich des jeweiligen STACKIT Cloud Services zu, sofern dieser von der Änderung betroffen ist.

Sofern eine Änderung der Servicebeschreibung lediglich bestehende Leistungen von STACKIT gegenüber dem Kunden (optional) erweitert bzw. neu hinzufügt, ist STACKIT berechtigt, die Änderungen auch innerhalb einer verkürzten Frist gegenüber dem Kunden mitzuteilen; in diesen Fällen steht dem Kunden kein Widerspruchsrecht zu.

## **2 Service Level Agreement**

### **2.1 Leistungsübergabepunkt**

Die Leistungsverantwortung für zu erbringende STACKIT Cloud Services seitens STACKIT endet am Internet-Übergabepunkt zwischen dem jeweiligen durch STACKIT betriebenen Rechenzentrum und dem Internet Service Provider der jeweiligen Region.

### **2.2 Betriebszeiten**

Die Betriebszeiten der STACKIT Cloud Services sind Montag bis Sonntag, „7x24h“, an 365 Tagen im Jahr (ausgenommen geplante Wartungsarbeiten).

### **2.3 Verfügbarkeit**

Die generelle Verfügbarkeit eines STACKIT Cloud Service beträgt – nach Abzug der Ausgeschlossenen Ereignisse gemäß Ziffer 2.4 – 99,9% (99,5% für nicht redundant ausgelegte STACKIT Cloud Services) im Kalendermonat, sofern nicht in dem jeweiligen, dem STACKIT Cloud Service zugrundeliegenden Leistungsschein etwas Abweichendes geregelt ist („**Verfügbarkeit**“). Verfügbarkeitsangaben gelten nicht für die Verfügbarkeit kundeneigener Komponenten oder Komponenten Dritter (Software auch Hardware).

Die kalendermonatlich erzielte Verfügbarkeit wird wie folgt berechnet:

Verfügbarkeit in % = (Gesamte Serviceminuten - Gesamte Ausfallminuten) / (Gesamte Serviceminuten) x 100

- Die Verfügbarkeit bezieht sich immer auf einen Kalendermonat, wird kalendermonatlich erhoben und als Prozentsatz ausgewiesen.
- „Gesamte Serviceminuten“ ist zu verstehen als Gesamtanzahl an Kalendermonatsminuten (Berechnung: 60 Minuten x 24 Stunden x Anzahl Kalendertage im Monat)
- „Gesamte Ausfallminuten“ ist zu verstehen als die Anzahl an Minuten pro Monat, in der der vertraglich geschuldete STACKIT Cloud Service nicht erbracht wurde. Von dem Wert der gesamten Ausfallminuten sind die Anzahl an Minuten pro Monat abzuziehen, die als Ausgeschlossenen Ereignisse im Sinne der Ziff. 2.4 nicht in die Berechnung der Verfügbarkeit mit einfließen.

Die Verfügbarkeit des STACKIT Portals und des STACKIT Application Programming Interface (API) unterliegt keiner Verfügbarkeitszusage durch STACKIT. STACKIT strebt jedoch eine Verfügbarkeit für das STACKIT Portal und das STACKIT Application Programming Interface (API) von jeweils 99,9% im Kalendermonatsdurchschnitt an. Ausfälle, Störungen oder sonstige Nichterreichbarkeiten des STACKIT Portals oder des STACKIT Application Programming Interface (API), beeinflussen die Berechnung der Verfügbarkeit eines STACKIT Cloud Service nicht.

## 2.4 **Ausgeschlossene Ereignisse**

Ausgeschlossene Ereignisse bezeichnen insbesondere solche Zeiträume, in denen aufgrund nachfolgend aufgeführter Ausfälle und Störungen ein vertragsgemäßes Zurverfügungstellen der STACKIT Cloud Services nicht gewährleistet werden kann („**Ausgeschlossene Ereignisse**“). Ausgeschlossene Ereignisse gelten nicht als Ausfallzeit. Zu Ausgeschlossenen Ereignissen zählen insbesondere:

- Ausfälle und Störungen die nicht von STACKIT zu vertreten sind, insbesondere DNS-, Routingprobleme oder nicht autorisierte Einwirkungen von Dritten, wie bspw. virtuelle Angriffe auf die Netz- bzw. Mailinfrastruktur (z.B. DoS, Viren oder Spam).
- Ausfälle und Störungen, die sich aufgrund der Durchführung von Gegenmaßnahmen gegen nicht autorisierte Einwirkungen oder aufgrund von Security Incidents ergeben.
- Ausfälle und Störungen von Dienstleistungen Dritter außerhalb der Kontrolle von STACKIT bzw. die nicht auf die von STACKIT bereitgestellte Leistung zurückzuführen sind oder der Netzwerkstruktur außerhalb des Einflussbereichs von STACKIT liegen.
- Ausfälle und Störungen, die durch den Kunden verursacht wurden. Hierzu zählen beispielsweise:
  - Fehlerhafte Eingaben oder Nichteinhaltung von Anweisungen.
  - Handlungen oder Unterlassungen des Kunden welche die vorgeschriebenen und/oder gebuchten Kontingente (Quota) überschreiten.
  - Handlungen oder Unterlassungen des Kunden, erforderliche Konfigurationen vorzunehmen und/oder einzuhalten.
- Ausfälle und Störungen, die auf höherer Gewalt beruhen. Höhere Gewalt ist dabei ein Ereignis, das für keine der Parteien unter Anwendung äußerster, billigerweise zu erwartender Sorgfalt vorhersehbar war; höhere Gewalt kann in diesem Sinne insbesondere folgende Ereignisse umfassen: Brände, Explosionen, Stromausfälle, Erdbeben, Überschwemmungen, schwere Stürme, Streiks, Embargos, Arbeitskämpfe, Handlungen von Zivil- oder Militärbehörden, Krieg, Terrorismus (einschließlich Cyber-Terrorismus), Epidemien und Pandemien, Handlungen oder Unterlassungen von Internet Providern, Handlungen oder Unterlassungen von Aufsichtsbehörden oder Verwaltungseinrichtungen (einschließlich der Verabschiedung von Gesetzen oder Regelungen oder anderer Regierungshandlungen, die die Bereitstellung von STACKIT Cloud Services beeinträchtigen).

- Ausfälle und Störungen, welche aufgrund von Wartungsarbeiten gem. Ziffer 2.8 erfolgen.

STACKIT Cloud Services, die dem Kunden kostenlos zur Verfügung gestellt bzw. explizit als Testversion, Beta oder in ähnlicher Weise bezeichnet und vertrieben werden, unterliegen keiner Verfügbarkeitszusage. Ausfälle oder Störungen, welche durch die Nutzung derartiger Services durch den Kunden auftreten, werden als ausgeschlossene Ereignisse gewertet.

## 2.5 Unterstützte Softwareversionen

STACKIT Cloud Services können zum Zeitpunkt des Abschlusses eines Vertragsverhältnisses spezifische Softwareversionen aufweisen („**Hauptversionen**“). Um die STACKIT Cloud Services sowie die Leistungserbringung gegenüber dem Kunden sicher und aktuell zu halten, behält sich STACKIT vor, die Hauptversionen der eingesetzten Software durch Nachfolgeversionen („**Nachfolgeversionen**“) – auch für bereits abgeschlossene Vertragsverhältnisse – zu ersetzen.

In einem solchen Fall gilt insbesondere das Folgende:

- STACKIT informiert die betroffenen Kunden über die anstehende Änderung und das Ende des Unterstützungszeitraumes von Hauptversionen im Rahmen der Release-Notes unter <https://docs.stackit.cloud/display/STACKIT/Release+Notes> („**Release-Notes**“).
- Die von der Änderung betroffene Hauptversion wird für weitere mindestens 180 Kalendertage, gerechnet ab der Ankündigung der Änderung von STACKIT im Rahmen der Release-Notes unterstützt und im Anschluss zeitnah sukzessive auf die Nachfolgeversion migriert („**Übergangszeitraum**“).
- Innerhalb dieses Übergangszeitraums sind auch weiterhin Vertragsabschlüsse basierend auf der Hauptversion möglich, welche zum Ende des Übergangszeitraums aber ebenfalls auf die Nachfolgeversion umgestellt werden müssen. Kunden sind daher angehalten, sich im Rahmen der Release-Notes über etwaige angekündigte Änderungen der Hauptversionen bereits vor Abschluss eines Abonnements über einen STACKIT Cloud Service zu informieren; gegenüber Kunden, welche den von einer Änderung betroffenen STACKIT Cloud Service innerhalb des Übergangszeitraums abonnieren oder verlängern, steht der betroffene STACKIT Cloud Service in der abonnierten Hauptversion nur bis zum Ende des Übergangszeitraums zur Verfügung, was je nach dem Zeitpunkt des Abschlusses eines Abonnements deutlich weniger als 180 Kalendertage entsprechen kann.
- Sofern angeboten, technisch möglich und vom Kunden gewünscht, hat der Kunde auch bereits vor Ende des Übergangszeitraums die Möglichkeit, von einer Änderung betroffene Hauptversionen auf die Nachfolgeversionen zu migrieren bzw. – je nach STACKIT Cloud Service – durch STACKIT migrieren zu lassen. Ein Anspruch des Kunden auf vorzeitige Migration besteht jedoch nicht.
- Nach Ablauf des Übergangszeitraums stellt STACKIT noch nicht vom Kunden migrierte Hauptversionen sukzessive zeitnah auf die Nachfolgeversionen um.

- In einigen Fällen der Migration der Hauptversion auf die Nachfolgeversion kann es vorkommen, dass STACKIT eine automatische ordnungsgemäße Migration (insbesondere der Kundendaten) ohne die Mitwirkungshandlungen des Kunden nicht möglich ist. In diesen Fällen wird STACKIT die betroffenen Kunden über etwaige erforderliche Mitwirkungshandlungen im Rahmen der Release-Notes informieren. Der Kunde hat bis zum Ende des Übergangszeitraums – gerechnet ab Veröffentlichung der erforderlichen Mitwirkungshandlungen innerhalb der Release-Notes – Zeit, die erforderlichen Mitwirkungshandlungen vorzunehmen.
- Nach Ablauf des Übergangszeitraums wird die Hauptversion nicht mehr von STACKIT unterstützt und kann gegebenenfalls auch nicht mehr vom Kunden verwendet werden; STACKIT ist berechtigt, sofern und soweit technisch für STACKIT möglich, eine automatische Migration der Hauptversion auf die Nachfolgeversion durchzuführen, auch wenn der Kunde zuvor nicht die erforderlichen Mitwirkungshandlungen vorgenommen hat; dadurch kann es insbesondere zu Datenverlusten und Funktionsverlusten oder -einschränkungen des betroffenen STACKIT Cloud Service sowie in Zusammenhang mit diesem verwendeter kundeneigener Hard- und Software bzw. Hard- und Software von Dritten kommen. STACKIT übernimmt, ausgenommen in den Fällen der Ziffer 15.1 der Nutzungsbedingungen, keine Haftung für Schäden, welche dem Kunden durch eine nicht durchgeführte Migration oder eine automatische Migration entstehen.
- Nach Umstellung einer Software von deren Hauptversion auf die Nachfolgeversion ist sodann die Nachfolgeversion als (neue) Hauptversion im Sinne dieser Ziffer zu verstehen.

## 2.6 Service Deprecation

Jeder STACKIT Cloud Service unterliegt einem von STACKIT festgelegten Produktlebenszyklus. STACKIT wird die Einstellung des betroffenen STACKIT Cloud Services oder einer wesentlichen Funktionalität eines Services (**“Deprecation”**) mindestens 360 Kalendertage vor dem Einstellungszeitpunkt über die Release-Notes ankündigen. Mit dem Wirksamwerden der Deprecation steht der jeweils betroffene Service bzw. die betroffene Funktionalität nicht mehr zur Nutzung durch den Kunden zur Verfügung.

Im Rahmen der Ankündigung über die Release-Notes informiert STACKIT über etwaige nachfolgende Produkte.

## 2.7 Backup

Eine Datensicherung durch STACKIT findet nur dann statt, wenn dies entweder a) im Leistungsscheinen beschrieben ist oder b) sofern im Rahmen des Abschlusses bzw. der Konfiguration des jeweiligen Abonnements über den STACKIT Cloud Service über das Portal oder die STACKIT API durch den Kunden die Backup-Funktion (sofern vorhanden) aktiviert wurde.

Findet ein Backup statt, richtet sich die Datensicherung des entsprechenden STACKIT Cloud Services nach den nachfolgenden Standards, sofern im individuellen Leistungsschein nichts Abweichendes geregelt bzw. durch Kunden nichts Abweichendes konfiguriert worden ist:

Backup Parameter	Ausprägung
Recovery Point Objective (RPO)	4 h
Recovery Time Objective (RTO)	4 h
Retention Period (RP)	14 Tage, tagesgenaue Aufbewahrung nach den ersten 4 h

- „Recovery Point Objective“ (RPO): Das RPO bzw. der maximal zulässige Datenverlust, umfasst die Vorgabe, wie alt der Stand der letzten aktuellen, konsistenten Datensicherung sein darf. Im Falle eines Datenverlustes und bei einer notwendigen Datenrücksicherung kann auf diesen Sicherungsstand zurückgegriffen werden.
- „Recovery Time Objective“ (RTO): Das RTO bzw. die maximale Wiederherstellungszeit, beschreibt den Zeitraum, in dem eine Datenrücksicherung auf ein funktional bereitstehendes System, inkl. Betriebssystemdaten und benötigten (Applikations-)Daten, konsistent anhand der Rücksicherung wiederhergestellt werden kann.
- „Retention Period“ (RP): Die RP beschreibt die maximale Dauer der Aufbewahrung von Sicherungen.

## 2.8 Wartungsarbeiten

STACKIT führt regelmäßig Wartungsarbeiten (beispielsweise in Form von Updates, Patches, Bug Fixes oder Hardwaretausch und Hardwareerweiterungen) zur Gewährleistung der Funktion, Qualität und Sicherheit der STACKIT Cloud Services durch.

Wartungsarbeiten, welche voraussichtlich keine Beeinträchtigung der Nutzbarkeit der STACKIT Cloud Services für den Kunden zur Folge haben (**„nicht-disruptive Wartungsarbeiten“**), können von STACKIT zu jeder Zeit auch ohne vorherige Ankündigung durchgeführt werden.

Wartungsarbeiten, welche voraussichtlich eine Beeinträchtigung der Nutzbarkeit der STACKIT Cloud Services für den Kunden zur Folge haben (**„disruptive Wartungsarbeiten“**), kündigt STACKIT in der Regel zwei Wochen vor deren Durchführung über die STACKIT Cloud Status-Website an. Für dringende Wartungsarbeiten, beispielsweise aufgrund von sicherheitsrelevanten Änderungen, kann die Ankündigung auch deutlich kurzfristiger erfolgen oder je nach Einzelfall komplett entfallen. STACKIT empfiehlt den Kunden, sich regelmäßig über Wartungsarbeiten auf der STACKIT Cloud Status-Website zu informieren.

Während der Durchführung von disruptiven Wartungsarbeiten kann der Zugang zu STACKIT Cloud Services vorübergehend eingestellt oder beschränkt sein, insbesondere wenn dies nach der Art der durchzuführenden Wartungsarbeiten zwingend erforderlich ist.

Ausfallzeiten, die aufgrund von durchgeführten disruptiven Wartungsarbeiten entstehen, sind als Ausgeschlossene Ereignisse im Sinne der Ziffer 2.4 zu behandeln.

## 2.8 Service Payback

Sollte die vereinbarte Verfügbarkeit für STACKIT Cloud Services nicht wie beschrieben eingehalten werden, erhält der Kunde im Rahmen der nachfolgenden Abwicklung eine Gutschrift in Form eines Guthabens auf sein Kundenkonto („**Service Payback**“):

- Der Kunde muss zur Geltendmachung eines Service Payback innerhalb von zwei (2) Wochen nach Zugang der Rechnung des betroffenen STACKIT Cloud Services in Textform unter der Angabe von Kundennummer, Rechnungsnummer und des betroffenen STACKIT Cloud Service geltend machen, dass die vereinbarte Verfügbarkeit des STACKIT Cloud Service nicht eingehalten worden ist. Eine nicht innerhalb von zwei (2) Wochen eingegangene Geltendmachung kann nicht berücksichtigt werden.
- Erfolgt die Geltendmachung berechtigterweise, erhält der Kunde für die nachfolgende Abrechnungsperiode eine Gutschrift des Service Payback auf sein Kundenkonto.
- Die Höhe des Service Payback bezieht sich stets auf den anteiligen Rechnungsbetrag des STACKIT Cloud Service, dessen zugesagte Verfügbarkeit nicht eingehalten wurde.
- Im Falle der Ablehnung eines vom Kunden geltend gemachten Service Payback obliegt es dem Kunden, den Verstoß gegen die vereinbarte Verfügbarkeit eines STACKIT Cloud Services darzulegen.
- Gutgeschriebenes Service Payback wird mit Vergütungsansprüchen für die Erbringung von STACKIT Cloud Services im nachfolgenden Abrechnungszeitraum verrechnet, sodass sich das zu zahlende Entgelt des Kunden entsprechend mindert.
- Eine Auszahlung oder anderweitige Erstattung des gutgeschriebenen Service Paybacks ist ausgeschlossen.
- Es gelten folgende Service Paybacks, sofern nicht im Leistungsschein des STACKIT Cloud Service eine abweichende Regelung getroffen wurde:

Verfügbarkeit (Monat)	Service Payback
< vertraglich vereinbarter Verfügbarkeitswert in %* *siehe Ziffer 2.3.	10%
< 99,0%	20%
< 98,5%	50%
< 95,0%	100%

2.8 Weitergehende Ansprüche des Kunden auf Minderung der Vergütung sind ausgeschlossen. Etwaige Schadenersatzansprüche des Kunden bleiben unberührt. Erhaltenes Service Payback ist im Falle der Geltendmachung eines Schadenersatzanspruches auf diesen anzurechnen.

### 3 Incidents & Security Incidents

#### 3.1 Informationen

STACKIT stellt Kunden regelmäßig Informationen über Störungen über die STACKIT Cloud Status-Website ([status.stackit.cloud](https://status.stackit.cloud)) zur Verfügung.

Bei Sicherheitsvorfällen (auch „Security Incidents“) werden die jeweils vom Security Incident betroffenen Kunden direkt informiert.

STACKIT empfiehlt den Kunden, sich kontinuierlich über den Status von Incidents & Security Incidents auf der STACKIT Cloud Status-Website zu informieren.

### 3.2 **Analysemöglichkeit durch STACKIT**

Für STACKIT Cloud Services, die durch STACKIT bereitgestellt und durch den Kunden, der die STACKIT Cloud Services bezieht, genutzt werden, können durch STACKIT Maßnahmen im eigenen Ermessen ergriffen werden, um Schwachstellen sowohl im Verantwortungsbereich von STACKIT, als auch im Verantwortungsbereich des Kunden frühzeitig aufzudecken. Im Verantwortungsbereich des Kunden liegen dabei insbesondere sämtliche Hardware, Applikationen und Software Dritter, die nicht durch STACKIT bereitgestellt werden („**Verantwortungsbereich des Kunden**“).

Werden Security Incidents im Verantwortungsbereich des Kunden durch STACKIT oder externe Dienstleister von STACKIT erkannt, wird der Kunde über diese informiert. Je nach Schweregrad des Security Incident ist der Kunde verpflichtet, für seinen Verantwortungsbereich zeitnah geeignete Maßnahmen zur Vermeidung des Security Incident zu ergreifen (z.B. durch das Patchen einer betroffenen Anwendung). Wird der Verantwortungsbereich des Kunden beispielsweise nicht mit den neuesten Patches oder Workarounds abgesichert, beherbergt der Verantwortungsbereich Sicherheitsrisiken für STACKIT oder den Kunden selbst, oder wird die Qualität der STACKIT Cloud Services durch ein Security Incident im Verantwortungsbereich des Kunden negativ beeinflusst oder gefährdet, behält sich STACKIT entsprechende Gegenmaßnahmen gemäß Ziffer 3.4 vor.

### 3.3 **Datenerhebung für Analysemöglichkeiten durch STACKIT**

Zur Erkennung möglicher Security Incidents im Verantwortungsbereich des Kunden können Log-Daten der Kundensysteme oder Perimeter (bspw. Firewalls, Switches, Router) regelbasiert nach Anomalien und potenziellen Security Incidents ausgewertet werden. Auch können entsprechende Schwachstellen-Scans (pro- und reaktiv) für im Internet verfügbare Systeme durchgeführt werden.

### 3.4 **Mögliche Gegenmaßnahmen bei Security Incidents**

Zum Schutz des Kunden sowie der STACKIT Cloud Services, behält sich STACKIT vor, bei Verdachtsfällen oder nachgewiesenen Security Incidents und entsprechendem Schweregrad entsprechende Maßnahmen ohne vorherige Ankündigung oder Rücksprache mit dem Kunden zu ergreifen („**Gegenmaßnahmen**“). Selbstverständlich erfolgt hierzu spätestens im Nachgang eine separate Information des Kunden. Zu den Gegenmaßnahmen gehören insbesondere:

- Betroffene Systeme und STACKIT Cloud Services vom Netz zu trennen, herunterzufahren oder zu pausieren, um Schaden an Systemen und STACKIT Cloud Services zu vermeiden.
- Forensische Analyse möglicher betroffener Systeme und STACKIT Cloud Services (insbesondere, um dadurch Erkenntnisse für die Strafverfolgung, die Kritikalitäts- oder Schadensbewertung zu gewinnen).

- Andere Aktivitäten zur Vermeidung oder Reduktion von Beeinträchtigungen anderer Kunden-Systeme der STACKIT Cloud Services oder externen Systemen.

### **3.5 Technische Änderungen zur Lösung von Security Incidents**

Über vorgenommene technische Änderungen, die zur Lösung von Security Incidents aus der Sicht von STACKIT erforderlich waren und umgesetzt wurden, wird der Kunde zeitnah informiert. Sollte der Kunde diesen technischen Änderungen nicht innerhalb eines Zeitraums von 14 Kalendertagen beginnend ab Zugang der Information beim Kunden begründet widersprechen, so gelten diese technischen Änderungen als vom Kunden akzeptiert.

Ein Widerspruchsrecht des Kunden besteht nur dann, wenn sich der Leistungsumfang des STACKIT Cloud Services nach der vorgenommenen technischen Änderung nicht nur unwesentlich verschlechtert hat oder die Nutzung des STACKIT Cloud Services oder die Zugriffsmöglichkeit auf den STACKIT Cloud Service durch den Kunden aufgrund der vorgenommenen technischen Änderung nicht mehr vereinbarungsgemäß möglich ist.

Im Falle eines wirksamen Widerspruchs räumt der Kunde STACKIT die Möglichkeit zur Nachbesserung ein. Im Rahmen der Nachbesserung wird STACKIT wirtschaftlich angemessene Maßnahmen ergreifen, eine kundenverträglichere Lösung im Hinblick auf die Behebung des Security Incidents zu erreichen. Falls STACKIT die Nachbesserung begründet verweigert (z.B. aufgrund technischer Undurchführbarkeit, Fortbestehens des Security Incidents oder wirtschaftlicher Unangemessenheit) oder der Widerspruchgrund des Kunden nach der Nachbesserung weiterhin besteht, so wird STACKIT den betroffenen STACKIT Cloud Service mit den vorgenommenen technischen Änderungen weiterhin erbringen und dem Kunden steht das Recht der außerordentlichen Kündigung des betroffenen abonnierten STACKIT Cloud Services mit sofortiger Wirkung zu.

## **4 Support**

STACKIT erbringt gegenüber seinen Kunden Supportleistungen in Bezug auf die STACKIT Cloud Services gemäß den Bedingungen der in **Anhang A Support Pläne** zu dieser Servicebeschreibung geregelten Inhalte.

## ANHANG A: Support Pläne

### A.1 Allgemein

STACKIT bietet für den Bezug von STACKIT Cloud Services Supportleistungen an, die in dem vorliegenden Anhang A Support Pläne spezifiziert werden. Die Regelungen dieses Anhang A gelten dabei grundsätzlich für jeden von STACKIT zur Verfügung gestellten Support Plan (vgl. Ziffer A.5), sofern nicht zwischen STACKIT und dem Kunden abweichende Regelungen innerhalb eines gesonderten Supportvertrages festgelegt werden.

Jeder STACKIT Cloud Service unterliegt standardmäßig dem STACKIT Essential Support (**“SES”**); der SES bedarf keiner gesonderten Buchung/Beauftragung durch den Kunden.

### A.2 Supportanfragen

A.2.1 Anfragen des Kunden werden anhand des Anfrageninhalts in die Kategorien geschäftskritischer Incident, Incident und Service Request (insgesamt **„Supportanfragen“**) unterteilt.

A.2.1.1 Ein geschäftskritischer Incident liegt vor, wenn durch eine Störung eines vom Kunden genutzten STACKIT Cloud Service

- wesentliche Funktionen des Geschäftsbetriebs des Kunden komplett oder teilweise ausgefallen sind;
- dem Kunden ein schwerer Schaden (z.B. finanziell oder Reputation) droht; oder
- gesetzliche Verpflichtungen des Kunden nicht mehr eingehalten werden können (nachfolgend **„geschäftskritischer Incident“**).

A.2.1.2 Ein Incident liegt vor, wenn ein vom Kunden genutzter STACKIT Cloud Service eine Störung, d.h. eine Abweichung vom vereinbarten Leistungsgegenstand aufweist und diese Abweichung negative Auswirkungen auf die Nutzung des STACKIT Cloud Services durch den Kunden hat (**„Incident“**).

A.2.1.3 Ein Service Request liegt vor, wenn der Kunde allgemeine Service- oder Supportanfragen stellt, welchen keine Störung eines genutzten STACKIT Cloud Services zugrunde liegt (**„Service Request“**).

A.2.2 Im Rahmen der Übermittlung der Supportanfrage des Kunden kann der Kunde eine Einschätzung der Kategorie seiner Anfrage unter Begründung der Sachlage angeben.

A.2.3 Erfolgt keine Angabe der Kategorie durch den Kunden, wird STACKIT die Kategorie anhand der vom Kunden übermittelten Informationen selbst einschätzen.

A.2.4 In jedem Fall bleibt STACKIT berechtigt, kundenseitig vorgenommene Zuordnungen der Kategorien anderweitig einzustufen, sofern die übermittelten Informationen zur Begründung der vom Kunden vorgenommenen Einschätzung aus der Sicht von STACKIT vernünftigerweise nicht angemessen oder ausreichend sind.

A.2.5 STACKIT unternimmt situationsbedingt wirtschaftlich angemessene Maßnahmen und Anstrengungen, um Supportanfragen in angemessener Zeit zu lösen.

### A.3 Allgemeine Mitwirkungspflichten des Kunden bei Supportanfragen

A.3.1 Die ordnungsgemäße Erbringung der im Rahmen des Supports vereinbarten Leistungen ist STACKIT nur dann möglich, wenn der Kunde im Rahmen von Supportanfragen die angeforderten angemessenen Mitwirkungen erfüllt.

Im Rahmen seiner Mitwirkungspflichten wird der Kunde insbesondere:

- Vor der Meldung einer Supportanfrage umfassend prüfen, ob er mit den ihm bestehenden Möglichkeiten und Informationsquellen selbstständig in der Lage ist, eine Lösung herbeizuführen;
- Vor der Meldung von Incidents und geschäftskritischen Incidents prüfen, ob die Ursache der Störung in seinem Verantwortungsbereich liegt;
- Für die Kommunikation über Supportanfragen Personal einsetzen, welches sowohl mit den STACKIT Cloud Services als auch der relevanten Kundenumgebung technisch vertraut ist. Der Kunde wird in diesem Zusammenhang sicherstellen, dass er STACKIT je Supportanfrage einen oder mehrere qualifizierte und in ausreichendem Maße entscheidungsbefugte Ansprechpartner benennt. Der Kunde gewährleistet für die Bearbeitungsdauer einer Supportanfrage die schriftliche, sowie telefonische Verfügbarkeit von mindestens einem dieser Ansprechpartner, welcher nach Aufforderung durch STACKIT die Mitwirkungspflichten des Kunden erbringt;
- Bei der Meldung von Supportanfragen alle für die Bearbeitung relevanten Informationen zur Verfügung stellen. Hierzu zählen insbesondere eindeutige Kennungen zur Identifikation der Projekte oder Services, auf welche sich die Anfrage bezieht, detaillierte Beschreibungen des beobachteten Zustands betroffener Services, die klare Formulierung der Erwartungshaltung des Zielzustandes, eine umfassende Darstellung etwaiger zur Reproduktion von Fehlern notwendigen Schritte, die Beschreibung bisher unternommener Aktivitäten seitens des Kunden, sowie die Bereitstellung relevanter Logs;
- Die Klassifizierung eines Incidents als geschäftskritisch sorgfältig abwägen. Sofern der Kunde einen geschäftskritischen Incident identifiziert, wird er bereits bei der Meldung eine für STACKIT nachvollziehbare Erklärung über die Auswirkung auf seinen Geschäftsbetrieb abgeben. Sofern STACKIT auf Grundlage dieser Erklärung nach sorgfältiger Einstufung nicht zu der Erkenntnis kommen kann, dass die Auswirkungen des Incidents der in Ziffer A.2.1.1 aufgeführten Definition von geschäftskritisch entspricht, behält STACKIT sich das Recht vor, die Klassifizierung anzupassen;
- Bei einem Incident oder einem geschäftskritischen Incident, welcher auf eine aktuell bestehende Großstörung der STACKIT Plattform (Major Incident) zurückzuführen ist, wird STACKIT den Kunden hierüber informieren. Die weitere Kommunikation zum Entstörungsverlauf der Großstörung bis zu dessen Abschluss erfolgt über die STACKIT Statusseite. In einem solchen Fall wird der Kunde sich fortlaufend über den Status mittels der Statuswebseite informieren.

A.3.2 Vorstehende Aufzählung der Mitwirkungspflichten ist nicht abschließend. Im jeweiligen Einzelfall können weitere angemessene Mitwirkungen des Kunden erforderlich sein, um eine Supportanfrage adäquat bearbeiten zu können. STACKIT wird den Kunden insoweit rechtzeitig über erforderliche Mitwirkungshandlungen informieren. Sollte der Kunde seinen Mitwirkungspflichten nicht in erforderlicher, von STACKIT angeforderter angemessener Qualität oder Umfang nachkommen, behält STACKIT sich das Recht vor, die Bearbeitung einer Supportanfrage bis zur Erbringung der erforderlichen Mitwirkungshandlung durch den Kunden zu unterbrechen oder – sofern auch nach Aufforderung seitens STACKIT keine Erbringung der erforderlichen Mitwirkungshandlung des Kunden erfolgt – die Bearbeitung der Supportanfrage zu beenden.

#### A.4 Zugriff auf Cloud Services des Kunden

Um Supportanfragen des Kunden adäquat bearbeiten zu können kann es erforderlich sein, dass STACKIT auf die vom Kunden bezogenen STACKIT Cloud Services Zugriff nehmen muss. Der Kunde stimmt mit Übermittlung einer Supportanfrage an STACKIT zu, dass STACKIT ausschließlich im erforderlichen Umfang zur Bearbeitung der jeweiligen Supportanfrage Zugriff nehmen darf; unberührt bleiben vertragliche sowie gesetzliche Verpflichtungen von STACKIT, welche in diesem Zusammenhang weiterhin einzuhalten sind.

#### A.5 Support Pläne

A.5.1 STACKIT bietet seinen Kunden die Wahl zwischen verschiedenen Support Plänen, die sich im Umfang der erbrachten Supportleistungen, den Servicezeiten und den Reaktions- und Antwortzeiten unterscheiden.

Diese sind aktuell:

- STACKIT Essential Support („**SES**“)
- STACKIT Ultimate Support („**SUS**“)

A.5.2 Der SES ist automatisch Bestandteil jedes vom Kunden gebuchten STACKIT Cloud Service und wird ohne Mehrkosten durch STACKIT erbracht. Der SUS ist ausschließlich nach Kontaktaufnahme des Kunden mit STACKIT und Abschluss eines gesonderten SUS-Vertrags kostenpflichtig abschließbar.

#### A.6 Übersichtstabelle der Leistungsinhalte SES Support Plan

Nachfolgende Tabelle stellt eine Übersicht des Umfangs der Supportleistungen des SES dar. Eine Übersicht über die Leistungen der anderen optionalen Support Pläne befindet sich auf der Webseite von STACKIT bzw. in den zugehörigen Vertragsdokumenten des jeweiligen Supportplans.

Art des Service Supports	SES
--------------------------	-----

<b>Verfügbare Support Kanäle</b>	
Support-Team mit Sitz in Europäischen Union	<input checked="" type="checkbox"/>
Support über Portal	<input checked="" type="checkbox"/>
Support über Telefon <b>10</b>	<input checked="" type="checkbox"/>
Zugang zu Knowledge Database (docs.stackit.cloud) <b>20</b>	<input checked="" type="checkbox"/>
Zugang zu Status Webseite (status.stackit.cloud) <b>30</b>	<input checked="" type="checkbox"/>
Zugang zu Help Center (support.stackit.cloud)	<input checked="" type="checkbox"/>
Verfügbarkeit der Supportkanäle 24/7	<input checked="" type="checkbox"/>
<b>Zeiten</b>	
Servicezeiten <b>40</b> Montag – Freitag, 08:00 – 18:00 Uhr <b>50</b>	<input checked="" type="checkbox"/>
Reaktionszeit in Minuten - innerhalb der Servicezeiten <b>60</b>	angestrebt: 15
Antwortzeit bei geschäftskritischen Incidents in Minuten - innerhalb der Servicezeiten <b>70</b>	angestrebt: 240
Antwortzeit bei Incidents in Minuten <b>70</b>	best effort
Antwortzeit bei Serviceanfragen in Minuten <b>70</b>	best effort
<b>Service Level für Supportzeiten (Support-SLA)</b>	
Vereinbarung zur Einhaltung der Reaktionszeit <b>60</b>	best effort
Vereinbarung zur Einhaltung der Antwortzeit <b>70</b>	best effort
<b>Zusätzliche Services</b>	
Monatliche Support-SLA-Berichte	keine monatlichen Support-SLA-Berichte

**10** Hotline-Nummer: +49 7132 30-474747

**20** Knowledge Base Dokumentation, Release Notes, Tutorials, FAQ und bekannte Probleme

**30** Zur Benachrichtigung über geplante Wartungsarbeiten oder wichtige Vorfälle

**40** Servicezeiten sind die vertraglich vereinbarten Wochentage und Zeitfenster, innerhalb derer die STACKIT (Service-)Leistungen erbringt und Supportanfragen bearbeitet.

**50** CE(S)T [Central European (Summer) Time], Feiertage in Baden-Württemberg ausgenommen

**60** Reaktionszeit ist die Zeitspanne vom Eingang der Supportanfrage des Kunden bei STACKIT bis zum Start der Bearbeitung der Supportanfrage

**70** Antwortzeit ist die Zeitspanne ab Eingang der Supportanfrage bei STACKIT bis zur ersten qualifizierten Antwort. Sie beinhaltet eine konkrete Rückmeldung auf die Supportanfrage mit entweder

- einer Lösung,
- einer Problemanalyse oder
- eines nächsten Handlungsschrittes