Anlage 3 zum Vwxyz/Debitor

Service Level Agreement

Bereitstellung von Systemen in der dSecureCloud - IaaS

für

Auftraggeber

Straße

Ort

nachfolgend Auftraggeber

Version: 1.4
Stand: 19.10.2018

Inhaltsverzeichnis

1 Einleitung

Dataport (nachfolgend Auftragnehmer) stellt mit dem Infrastructure-as-a-Service (IaaS) in der dSecureCloud eine „On Demand“ Lösung für die Bereitstellung von Servern für Trägerländer (nachfolgend Auftraggeber) bereit. IaaS in der Dataport Cloud wurde entwickelt, um eine wirtschaftliche und zugleich flexible Bereitstellungsform für virtuelle Server anzubieten. Sie unterscheidet sich in ihrem Leistungsumfang stark vom „Full Service Support“.

Mittels eines Self-Service-Portals kann ein Anwender virtuelle Systeme (VM) nach seinem eigenen Bedarf bereitstellen. Hierbei ist es ihm möglich, Ressourcen seinen benötigten Servern zuzuweisen, als auch aus einer vorgegebenen Auswahl ein Betriebssystem auszuwählen. Die Bereitstellung des virtuellen Servers erfolgt vollautomatisiert, jedoch ohne Konfiguration des Betriebssystems oder betriebssystemnaher Komponenten.

Über einen Proxy Zugang wird die Erreichbarkeit des virtuellen Servers ins Internet hergestellt. Aus dem jeweiligen Clientnetz sind die Server direkt per RDP (Microsoft Windows) oder SSH (Linux), ohne einen eToken oder den Zugang zu einer Adminplattform, zu erreichen. Die Erreichbarkeit der virtuellen Server ist nur untereinander möglich. Zusätzliche Freischaltungen müssen beim Dataport Policymanagement eingereicht werden und unterliegen einem Genehmigungsvorbehalt. Freischaltungen in weitere RZ-Bereiche sind nicht möglich.

Der IT-Grundschutzkonforme Betrieb der Virtualisierungsinfrastruktur wird vom Auftragnehmer für die Verarbeitung von Daten mit dem Schutzbedarf „normal“ gewährleistet. Die virtuellen Systeme selbst, sind im Gegensatz zum „Full Service Support“, ungehärtet und werden vom Auftragnehmer nicht betreut. Sicherheitspatche von Betriebssystem und betriebssystemnaher Software müssen vom Anwender selbstständig installiert werden. Ein Virenschutz für die VMs wird bereitgestellt. Ein Monitoring findet nur für die zugrunde liegende Virtualisierungsinfrastruktur statt, nicht jedoch für die vom Anwender betreuten Server. Es bestehen jedoch keinerlei Verfügungsansprüche für die vom Anwender betriebenen virtuellen Server.

Störungen des Self-Service-Portals können über den User-Help-Desk eröffnet werden, während die Anwender-VMs keinem Support durch den Auftragnehmer unterliegen. Die Option auf eine vollständige Datensicherung und Wiederherstellung der Systeme ist möglich.

2 Allgemeine Leistungen

2.1 Basisleistungen

Die Basisleistungen stellen die Grundlage des Infrastructure-as-a-Service (IaaS) innerhalb der dSecureCloud dar. Mit dem Self-Service-Portal stellt sich der Auftraggeber seine benötigten virtuellen Server mit den von ihm benötigten Ressourcen flexibel selbst bereit. Zu den Ressourcen, die vom Auftraggeber wählbar sind, gehören RAM, CPU Cores, Kapazität sowie Partitionierung von Storage als auch die Wahl der Betriebssystemplattform.

Die Bereitstellung des virtuellen Servers erfolgt vollautomatisiert über die vom Auftragnehmer bereitgestellten Server-Templates. Es findet keine Konfiguration des Betriebssystems oder möglicher betriebssystemnaher Komponenten durch den Auftragnehmer statt. Der Server wird eigenverantwortlich vom Auftraggeber betreut.

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Bereitstellung der Server-Templates zur Erstellung von virtuellen Servern in der Cloud	**V, D, B**	**I**
Erstellung eines virtuellen Servers über das Self-Service-Portal	**I**	**V, D, B**
Konfiguration des virtuellen Servers nach Erstellung über das Self-Service-Portal	**I**	**V, D, B**
Ressourcenerweiterung des virtuellen Servers (RAM, Cores, Festplatten)	**I**	**V, D, B**

2.1.1 Grundschutzkonformer Betrieb

Alle Systeme der dSecureCloud Virtualisierungsinfrastruktur erfüllen die Anforderungen des grundschutzkonformen Betriebs des BSI für die Verarbeitung von Daten mit dem Schutzbedarf „normal“.. Der grundschutzkonforme Betrieb der Virtualisierungsinfrastruktur wird vom Auftragnehmer gewährleistet.

Der sichere Betrieb für die vom Auftraggeber eigenadministrierten virtuellen Server in der dSecureCloud wird nicht vom Auftragnehmer gewährleistet.

Für das Update- und Patchmanagement für die Virtualisierungsinfrastruktur der dSecureCloud ist der Auftragnehmer verantwortlich.

Im Quartalszyklus werden die Servertemplates für Neubereitstellungen für die vom Auftraggeber nutzbaren Betriebssysteme vom Auftragnehmern auf ein aktuelles Patch- und Updatelevel gehoben.

Nach dem Zeitpunkt der Bereitstellung der virtuellen Systeme verpflichtet sich der Auftraggeber aktuelle Sicherheitspatche und Updates für das Betriebssystem und betriebssystemnaher Software auf seinen betreuten virtuellen Servern innerhalb der dSecureCloud selbstständig zu beziehen und zu installieren.

Der Auftragnehmer behält sich das Recht vor, kundenbetreute Maschinen stillzulegen, wenn diese ein Sicherheitsrisiko (zum Beispiel Teil eines Bot-Netzes, Viren- oder Malwarebefall) darstellen oder nach wiederholter Aufforderung keine sicherheitsrelevanten Patche eingespielt werden.

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Grundschutzkonformer Betrieb der dSecureCloud Infrastruktur	**V, D, B**	**I**
Sicherer Betrieb der virtuellen Server innerhalb der dSecureCloud nach Bereitstellung, inkl. Einspielung von Patches und Updates	**I**	**V, D**

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Anpassung der Templates für Neubereitstellungen auf aktuelles Patch- & Updatelevel (pro Quartal)	**V, D, B**	
Planung von systemspezifischen Wartungsarbeiten an der dSecureCloud Infrastruktur	**V, D**	**I**

2.1.2 Datenschutz

Der Auftraggeber ist allein verantwortlich für die Art der Nutzung der bereitgestellten virtuellen Systeme inklusive der verwendeten Daten. Verarbeitet der Auftraggeber auf den bereitgestellten virtuellen Systemen des Auftragnehmers personenbezogene Daten, so ist der Auftraggeber ist bezüglich der Verarbeitung dieser personenbezogenen Daten Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Der Auftraggeber ist ebenfalls für die Einhaltung der in Kapitel IV der DSGVO und ggfs. ergänzend geltender nationaler Datenschutzvorschriften verantwortlich, insbesondere für

- die Rechtmäßigkeit der Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten,
- sofern die Verarbeitung auf der Grundlage einer Einwilligung erfolgt, die Einholung und Dokumentation von Einwilligungserklärungen, die Dokumentation von Widerrufserklärungen und die Umsetzung der im Falle eines Widerrufs erforderlichen Maßnahmen,
- die Prüfung, ob gemäß Art. 35 DSGVO eine Datenschutz-Folgeabschätzung durchzuführen ist, und falls ja, für die Durchführung derselben,
- die Dokumentation der zum Schutz der Daten getroffenen Maßnahmen, soweit diese in nicht von dem Auftragnehmer im Rahmen der in diesem SLA geregelten Leistungen umzusetzen sind,
- die Wahrung der Rechte der Betroffenen insbes. des Rechts auf Berichtigung, Löschung, Einschränkung,
- die Einhaltung von Löschfristen und zulässiger Speicherdauer.

Die datenschutzrechtliche Verantwortung des Auftragnehmers zur Umsetzung der Maßnahmen gemäß Art. 32 und 28 DSGVO ist auf den in diesem SLA geregelten Leistungsumfang beschränkt.

2.1.3 Virenschutz

Der Auftragnehmer gewährleistet für die Virtualisierungsinfrastruktur einen Virenschutz.

Für die vom Auftraggeber betreuten virtuellen Server ist der Virenschutz innerhalb der dSecureCloud optional.

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Virenschutz der dSecureCloud Infrastruktur	**V, D, B**	**I**
Bereitstellung des Virenschutzagenten der virtuellen Server innerhalb der dSecureCloud	**V, I, B**	**D**
Betrieb und Betreuung des Virenschutzagenten auf virtuellen Server innerhalb der dSecureCloud		**V,D,B**

2.1.4 Monitoring

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Monitoring der Dataport Infrastruktur	**V, D, B**	**I**
Störungsfreier Betrieb des Self-Service-Portals	**V, D, B**	**I**
Steuerung und Überwachung der virtuellen Systeme. Proaktives Erkennen und Vermeiden von Störungen	**I**	**V, D**

Die virtuellen Server des Auftraggebers innerhalb der **d**SecureCloud unterliegen nicht dem Monitoring des Auftragnehmers. Der Auftraggeber ist eigenverantwortlich für den Zustand und den störungsfreien Betrieb seiner Server.

Die Überwachung für die virtuelle Infrastruktur, wie auch das Self-Service-Portal, werden vom Auftragnehmer betreut und gewährleistet.

2.1.5 Verfügbarkeit

Der Auftraggeber hat gegenüber dem Auftragnehmer keinerlei Verfügbarkeitsansprüche auf seinen in der **d**SecureCloud eigenadministrierten Servern.

Die Verfügbarkeit der Virtualisierungsinfrastruktur und des Self-Service-Portals wird analog zum Standard des Dataport Servicekatalogs zugesichert.

2.1.6 Zugang

Aus dem jeweiligen Clientnetz sind die Server direkt per RDP (Remote Desktop Protokoll, Microsoft Windows) oder SSH (Secure Shell, Linux) zu erreichen. Über einen Proxyserver wird der Zugang zu dem vom Auftraggeber in der **d**SecureCloud administrierten Server hergestellt.

Es wird kein Zugang zu einer Administrationsplattform benötigt.

2.1.7 Netzkommunikation

Die Erreichbarkeit für die vom Auftraggeber in der **d**SecureCloud betreuten virtuellen Server ist nur untereinander möglich. Zusätzliche Freischaltungen müssen beim Dataport Policymanagement eingereicht werden und unterliegen einem Genehmigungsvorbehalt (siehe 3.4.2).

Freischaltungen in weitere RZ-Bereiche sind nicht möglich.

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Erreichbarkeit der virtuellen Server innerhalb der **d**SecureCloud	**V, I**	**D**
Beantragung zusätzlicher Freischaltungen	**I**	**V, D**
Umsetzung zusätzlicher Freischaltung nach erfolgter Prüfung	**V, D**	**I**

2.1.8 Verschlüsselung

Für die Wahrung der Vertraulichkeit der vom Auftraggeber in der dSecureCloud verarbeiteten Daten ist ausschließlich der Auftraggeber verantwortlich; dieser hat eine ggfs. erforderliche Verschlüsselung eigenverantwortlich vorzunehmen. Sofern die vom Auftraggeber in der dSecure Cloud verarbeiteten Daten aus Gründen der Sicherheit oder des Geheimschutzes eine Verschlüsselung erfordern, ist der Auftraggeber hierfür verantwortlich.

2.1.9 Authentisierung

Die Authentisierung der vom Auftraggeber betriebenen virtuellen Server innerhalb der **d**SecureCloud erfolgt mittels lokaler Benutzer-Accounts. Weitere Authentisierungsdienste werden nicht angeboten.

2.1.10 Löschung von Daten

Im Falle einer Vertragskündigung ist der Auftraggeber dafür verantwortlich, die von ihm in der dSecure Cloud gespeicherten Daten rechtzeitig vor Beendigung des Vertrages anderweitig zu sichern. Unabhängig vom Kündigungsgrund und von der Vertragspartei, welche die Kündigung ausgesprochen hat, löscht der Auftragnehmer alle Daten des Auftraggebers einschließlich eventuell noch gemäß Tz 3.4.1 vorhandenen Datensicherungen spätestens 30 Tage nach Beendigung des Vertrages.

Eine Wiederherstellung von Daten ist nach dieser Löschung ausgeschlossen.

Ausgenommen von der Löschung sind Daten, die vom Auftragnehmer zu Abrechnungszwecken über diese Frist hinaus benötigt werden oder soweit sie einer gesetzlichen Aufbewahrungspflicht unterliegen.

Für die Löschung der betriebenen virtuellen Server innerhalb der **d**SecureCloud während der Vertragslaufzeit ist der Auftraggeber verantwortlich.

2.1.11 Offenlegung von Daten des Auftraggebers

Der Auftragnehmer wird Daten, die der Kunde in der dSecureCloud gespeichert hat, Dritten (insbesondere Strafverfolgungsbehörden) nur offenlegen, sofern der Auftragnehmer hierzu gesetzlich verpflichtet ist. Ist der Auftragnehmer gesetzlich zur Offenlegung verpflichtet, wird er den Auftraggeber unverzüglich darüber informieren und ihm eine Kopie der Verfügung (z.B. Anordnung zur Beschlagnahme oder Durchsuchung) zukommen lassen, sofern dies nicht gesetzlich verboten ist. Der Auftragnehmer ist gegenüber dem Auftraggeber nicht zur Einlegung von Rechtsbehelfen oder Rechtsmitteln gegen solche Verfügungen verpflichtet.

2.1.12 Berichtswesen und Rechnungsstellung

Der Auftragnehmer stellt über das Self-Service-Portal ein automatisiertes Berichtswesen dem Auftraggeber zur Verfügung. Der aktuelle Ressourcenverbrauch und die entstandenen Aufwände sind jederzeit einsehbar.

Die Rechnungsstellung erfolgt kalendermonatlich nachträglich. Auf der Rechnung werden nur die im Leistungszeitraum entstandenen Gesamtaufwände je im Preisblatt (Anlage 2) angegebener Position

ausgewiesen. Detaillierte Aufschlüsselungen pro Tag kann der Auftraggeber dem Self-Service-Portal entnehmen.

2.1.13 Protokollierung

Innerhalb des Self-Service-Portals findet eine Protokollierung statt. Durch Firewalls geblockte Netzwerkkommunikation wird ebenfalls protokolliert.

Eine regelmäßige Auswertung erfolgt nicht, sondern nur im Bedarfsfall, wie zum Beispiel dem Verdacht, dass ein Sicherheitsrisiko (s. 2.1.1) vorliegt.

2.2 Leistungsgegenstand

2.2.1 Leistungsmerkmale eines virtuellen Servers in der dSecureCloud

Folgende Leistungsmerkmale stehen dem Auftraggeber bei der Erstellung und dem Betrieb seiner virtuellen Server in der Dataport Cloud zur Verfügung:

Leistungsmerkmal	Min.	Max.
CPU	1 Cores	8 Cores
RAM	1 GB	64 GB
Storage	abhängig vom Betriebssystem *(Linux 20GB, Windows 32GB)*	64 TB
SCSI-Controller	1	4
Anzahl an virtuellen Festplatten	1	60

2.2.2 Betriebssysteme in der dSecureCloud

Folgende Betriebssysteme stehen dem Auftraggeber bei der Erstellung eines Servers in der dSecureCloud zur Auswahl:

Hersteller	Betriebssystem
Microsoft	Windows Server
Microsoft	Windows Client
Linux	SUSE Linux Enterprise Server
Linux	Ubuntu Server

Von den genannten Betriebssystemen werden nur diese bereitgestellt, die sich im regelhaften Support durch den Hersteller befinden. Die Versionen werden vom Auftragnehmer regelmäßig aktualisiert und sind im Self-Service-Portal einsehbar. Bereits bereitgestellte Betriebssysteme können auch nach Entfernung

aus dem Self-Service-Portal weiterbetrieben werden, sofern sie keine Gefahr für andere Systeme darstellen (s. 2.1.1).

2.3 Mitwirkungsleistungen und Pflichten des Auftraggebers

Die Mitwirkungsleistungen Beistellleistungen und Pflichten des Auftraggebers sind in den jeweiligen Abschnitten der Leistungsbeschreibung und optionalen Leistungen ausgewiesen.

Der Auftragnehmer weist darauf hin, dass das BSI die Erstellung einer Cloud-Sicherheitsrichtlinie für Cloud-Nutzer durch den Auftraggeber empfiehlt.

Zusätzlich gelten für den Auftraggeber folgende Pflichten:

a) Der Auftraggeber versichert, dass er und diejenigen, die über ihn, in seinem Auftrag, mit seinem Wissen oder seiner Duldung die dScecure Cloud nutzen oder auf diese zugreifen können, keine Inhalte auf dem vertragsgegenständlichen Speicherplatz speichern und in das Internet einstellen werden, deren Bereitstellung, Veröffentlichung oder Nutzung gegen geltendes Recht oder Rechte Dritter oder behördliche Anordnungen verstößt; dies gilt insbesondere für ehrverletzende, volksverhetzende oder rechtsradikale Inhalte sowie für die Verbreitung von Spam oder Malware.

b) Der Auftraggeber prüft eigenverantwortlich die Einhaltung aller für ihn im Zusammenhang mit der Nutzung der Leistung relevanten und anwendbaren rechtlichen Vorschriften, Gesetze und Verordnungen und stellt deren Einhaltung sicher.

c) Der Auftraggeber ist verpflichtet die Betriebssysteme und Applikationen innerhalb seiner virtuellen Maschinen gegen Angriffe Dritter und Missbrauch zu schützen, sowie frei von Schadsoftware zu halten.

d) Der Auftraggeber ist verpflichtet innerhalb seiner virtuellen Maschinen die VMwareTools oder openVMTools für die Gastbetriebssystemunterstützung nur nach Aufforderung durch den Auftragnehmer zu deinstallieren.

e) Der Auftraggeber ist für die Einhaltung von Lizenzanforderungen hinsichtlich der von ihm oder auf seine Veranlassung in der dSecure Cloud installierten Software verantwortlich. Er hält Dataport diesbezüglich von jeglichen Ansprüchen Dritter frei.

Ein Verstoß des Auftraggebers gegen die in diesem SLA geregelten Pflichten berechtigt Dataport, den Vertrag mit sofortiger Wirkung zu kündigen und die vom Kunden in der dSecureCloud gespeicherten Daten nach Maßgabe von Tz 2.1.10 zu löschen.

3 Leistungsbeschreibung

3.1 Anforderungen an die Infrastruktur des Auftraggeber

Für den Fall, dass sich die Anforderungen an die dezentrale Infrastruktur ändern, gehen die dadurch erforderlich werdenden Anpassungen zu Lasten des Auftraggebers. Der Auftraggeber stellt sicher, dass seine dezentrale Infrastruktur den laufenden Betrieb ermöglicht.

3.1.1 Netzwerk-Anbindung und Firewall

Für Dienststellen der Verwaltung des Landes Schleswig-Holstein, des Landes Sachsen-Anhalts, der Freien und Hansestadt Hamburg und der Hansestadt Bremen wird ein Zugang zum jeweiligen Landesnetz vorausgesetzt.

3.2 Lizenzleistungen

Der Auftragnehmer gewährleistet die Lizenzleistung für die jeweilig zur Verfügung stehenden Betriebssysteme (s.2.2.2). Für alle weiteren Lizenzleistungen ist der Auftraggeber verantwortlich.

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Betriebssystemlizenzen	**V,D**	
Lizenzen für optional angebotene Dienste Datensicherung und Virenschutz, sofern genutzt	**V,D**	
Fachanwendung		**V,D**
Middleware		**V, D**

3.3 Leistungsabgrenzung

Der Zugang zu den Dataport Basisdiensten für die virtuellen Server des Auftragsgebers innerhalb der dSecureCloud sowie die Administration dieser virtuellen Server durch den Auftragnehmer sind nicht Bestandteil dieser Leistungsbeschreibung.

Seitens des Auftragnehmers werden keine weiteren Serverrollen (z.B. Datenbanken, Webservices etc.) bereitgestellt und/oder betreut.

Störungen innerhalb der automatisiert erstellten Anwender-VMs unterliegen nicht dem Support von Dataport. Störungen an der Virtualisierungsinfrastruktur und des Self-Service-Portals können über den User Help Desk eröffnet werden. Siehe hierzu Punkt 4.

3.4 Optionale Leistungen

Die nachfolgenden Leistungen können von allen Auftraggebern zusätzlich zu den Basisleistungen gebucht werden:

3.4.1 Datensicherung

Als optionale und zusätzlich zu berechnende Leistung bietet der Auftragnehmer innerhalb der dSecureCloud eine Datensicherung für die vom Auftraggeber eigenadministrierten Server an.

Die Option der Datensicherung kann bei der Neuerstellung eines vom Auftraggeber betreuten Servers oder auch bei einem in der dSecureCloud bestehenden System aktiviert werden. Der Auftraggeber kann zwischen einer täglichen oder wöchentlichen Sicherung wählen.

Die Aufbewahrungszeit der Datensicherung beträgt 14 Tage. Ein Restore kann nur für den gesamten virtuellen Server angewendet werden, nicht jedoch auf Fileebene.

Die Anforderung einer Datenrücksicherung von einem seiner optional zur Datensicherung verwalteten Server erfolgt ebenfalls innerhalb der Servicezeiten über den User-Help-Desk von Dataport.

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Definition von Backup Anforderungen und Aufbewahrungszeiträumen	**V, D**	**I**
Definition von Backup mit Zeitplänen, Vorgehensweisen, Parametern	**V, D**	**I**
Implementierung der Full-VM Sicherung	**V, D**	**I**
Durchführung der Datensicherung	**V, D**	**I**
Durchführung von Recovery Maßnahmen entsprechend der bestehenden Richtlinien	**V, D**	**I**

3.4.2 Erweiterte Netzkommunikation

Die selbstadministrierten Server des Auftraggebers innerhalb der dSecureCloud sind untereinander erreichbar. Für den Fall, dass die einfache Netzkommunikation nicht ausreicht und eine Kommunikation in erweiterte Bereiche notwendig wird, steht dem Auftraggeber die optionale Möglichkeit einer erweiterten Netzkommunikation zur Verfügung.

Die erweiterte Netzkommunikation muss über zusätzliche Freischaltungen beim Dataport Policymanagement eingereicht werden und unterliegt einem Genehmigungsvorbehalt. Für die Beantragung einer erweiterten Netzkommunikation entstehen keine weiteren Aufwände. Für umzusetzende Maßnahmen können zusätzliche Aufwände entstehen, die nicht Bestandteil dieser Vereinbarung sind.

3.4.3 Zusatzservice Erreichbarkeit über öffentliche Netzwerke

Die Server der dSecureCloud sind in ihrer Standard-Konfiguration nur über die Landesnetze erreichbar. Für Zugriffe von außerhalb der Landesnetze kann für jede virtuelle Maschine zusätzlich ein erweiterter Service, der die Erreichbarkeit über öffentliche Netzwerke sowie die Filterung mittels virtueller Firewalls sicherstellt, bestellt werden. In diesem ist weiterhin die optionale Buchung eines öffentlichen DNS-Eintrags enthalten.

Durch Providerwechsel kann es zu einer Änderung der öffentlichen IP-Adressen kommen. Der Auftragnehmer wird den Auftraggeber rechtzeitig informieren. Alle hieraus entstehenden Aufwände sind vom Auftraggeber selbstständig durchzuführen.

3.4.4 Virenschutz

Für die vom Auftraggeber betreuten virtuellen Server ist der Virenschutz innerhalb der dSecureCloud optional. Der Auftraggeber entscheidet eigenverantwortlich, ob er den Service vom Auftragnehmer nutzen möchte.

Die Ressourcen für den Virenschutzclient werden jedem Auftraggeber auf ihren eigens administrierten Servern zur Installation bereitgestellt. Das Angebot ist im Service enthalten und unterliegt keiner gesonderten Berechnung.

4 Leistungskennzahlen

4.1 Leistungsausprägung

4.1.1 Betriebszeiten

4.1.1.1 Onlineverfügbarkeit

Die zentrale Infrastruktur steht ganztägig zur Verfügung, d.h. an sieben Tagen in der Woche, 24 Stunden pro Tag – ausgenommen der unten angegebenen Einschränkungen (z.B. Wartungsfenster).

4.1.1.2 Servicezeit - Betreuter Betrieb[1]

- Montag bis Donnerstag 08.00 Uhr bis 17.00 Uhr
- Freitag 08.00 Uhr bis 15.00 Uhr

In diesen Zeiten erfolgt die Überwachung und Betreuung der Systeme durch Administratoren des Auftragnehmers. Es stehen Ansprechpartner mit systemtechnischen Kenntnissen für den Betrieb und zur Störungsbehebung zur Verfügung. Im Problem- und Störungsfall wird das entsprechende Personal des Auftragnehmers über das Call-Center des Auftragnehmers informiert.

4.1.1.3 Servicezeit - Überwachter Betrieb

- alle Zeiten außerhalb des betreuten Betriebes

Auch außerhalb des betreuten Betriebes stehen die Systeme den Anwendern grundsätzlich zur Verfügung. Die zentrale Infrastruktur wird automatisiert überwacht. Festgestellte Fehler werden automatisch in einem Trouble-Ticket-System hinterlegt. Ansprechpartner stehen während des überwachten Betriebes nicht zur Verfügung.

4.1.2 Wartungsarbeiten

Die regelmäßigen, periodisch wiederkehrenden Wartungs- und Installationsarbeiten erfolgen i. d. R. außerhalb der definierten Servicezeiten des betreuten Betriebes. Derzeit ist ein Wartungsfenster in der Zeit von Dienstag 19:00 Uhr bis Mittwoch 06:00 Uhr definiert. In dieser Zeit werden Wartungsarbeiten durchgeführt und das Arbeiten ist nur sehr eingeschränkt möglich. In Ausnahmefällen (z.B. wenn eine größere Installation erforderlich ist) werden diese Arbeiten nach vorheriger Ankündigung an einem Wochenende vorgenommen.

4.1.3 Support

Der Auftragnehmer übernimmt den Support für die Virtualisierungsinfrastruktur und das Self-Service-Portal.

Die automatisch durch den Auftraggeber erstellten VMs unterliegen nicht dem Support des Auftragnehmers. Der Auftragnehmer übernimmt des Weiteren keine verfahrensbezogenen fachlichen Supportleistungen.

[1] Gilt nicht für gesetzliche Feiertage, sowie 24.12. und 31.12.

4.1.4 Störungsannahme[2]

Die Störungsannahme erfolgt grundsätzlich über das Call-Center/den User-Help-Desk des Auftragnehmers.

Im Rahmen der Störungsannahme werden grundsätzlich Melderdaten sowie die Störungsbeschreibung erfasst und ausschließlich für die Störungsbehebung gespeichert. Der Störungsabschluss wird dem meldenden Anwender bekannt gemacht.

4.1.5 Incident-Management

Betriebsstörungen werden als Incidents im zentralen Trouble Ticket System (TTS) aufgenommen. Jeder Incident und dessen Bearbeitungsverlauf werden im TTS dokumentiert. Aus dem TTS lässt sich die Zeit der Störungsbearbeitung von der Aufnahme bis zum Schließen des Tickets mit der Störungsbehebung bestimmen.

Generell unterbrechen die Zeiten außerhalb des betreuten Betriebes die Bearbeitungszeit. Ebenso wird die Störungsbearbeitung unterbrochen durch höhere Gewalt oder durch Ereignisse, die durch den Auftraggeber oder den Nutzer zu verantworten sind (z.B. Warten auf Zusatzinformationen durch den Nutzer, Unterbrechung auf Nutzerwunsch, etc.).

Folgende Prioritäten werden für die Störungsbearbeitung im Rahmen der beauftragten Leistungen definiert:

Priorität	Auswirkung	Dringlichkeit	Bearbeitung
Niedrig (bisher 4)	Incident betrifft einzelne Benutzer. Die Geschäftstätigkeit ist nicht eingeschränkt.	Ersatz steht zur Verfügung und kann genutzt werden, oder das betroffene System muss aktuell nicht genutzt werden. Tätigkeiten, deren Durchführung durch den Incident behindert wird, können später erfolgen.	Priorität Niedrig führt zur Bearbeitung durch den Auftragnehmer und unterliegt der Überwachung des Lösungsfortschritts. Die Reaktionszeit (Beginn der Bearbeitung oder qualifizierter Rückruf) ergibt sich aus der Serviceklasse.
Mittel (bisher 3)	Wenige Anwender sind von dem Incident betroffen. Geschäftskritische Systeme sind nicht betroffen. Die Geschäftstätigkeit kann mit leichten Einschränkungen aufrechterhalten werden.	Ersatz steht nicht für alle betroffenen Nutzer zur Verfügung. Die Tätigkeit, bei der der Incident auftrat, kann später oder auf anderem Wege evtl. mit mehr Aufwand durchgeführt werden.	Priorität Mittel führt zur standardmäßigen Bearbeitung durch den Auftragnehmer und unterliegt der Überwachung des Lösungsfortschritts. Die Reaktionszeit (Beginn der Bearbeitung oder qualifizierter Rückruf) ergibt sich aus der Serviceklasse.
Hoch (bisher 2)	Viele Anwender sind betroffen. Geschäftskritische Systeme sind betroffen. Die Geschäftstätigkeit kann eingeschränkt aufrechterhalten werden.	Ersatz steht kurzfristig nicht zur Verfügung. Die Tätigkeit, bei der der Incident auftrat, muss kurzfristig durchgeführt werden.	Priorität Hoch führt zur bevorzugten Bearbeitung durch den Auftragnehmer und unterliegt besonderer Überwachung des Lösungsfortschritts. Die Reaktionszeit (Beginn der Bearbeitung oder qualifizierter Rückruf) ergibt sich aus der Serviceklasse.
Kritisch	Viele Anwender sind	Ersatz steht nicht zur	Priorität Kritisch führt zur

[2] Gilt nicht für gesetzliche Feiertage, sowie 24.12. und 31.12.

(bisher 1)	betroffen. Geschäftskritische Systeme sind betroffen. Die Geschäftstätigkeit kann nicht aufrechterhalten werden.	Verfügung. Die Tätigkeit, bei der der Incident auftrat, kann nicht verschoben oder anders durchgeführt werden.	umgehenden Bearbeitung durch den Auftragnehmer und unterliegt intensiver Überwachung des Lösungsfortschritts. Die Reaktionszeit (Beginn der Bearbeitung oder qualifizierter Rückruf) ergibt sich aus der Serviceklasse.

5 Erläuterungen

5.1 Begriffsfestlegungen

Betriebsmodus	Begriffsdefinition
Betriebszeit (ungetreuer Betrieb)	Die Betriebszeit ist der Zeitraum, in der die vereinbarten Ressourcen vom Auftragnehmer zur Verfügung gestellt und automatisiert überwacht werden.
Servicezeit	Servicezeiten beschreiben Zeiträume, in denen definierte Services zur Verfügung stehen.
Supportzeit (betreuter Betrieb)	Die Servicezeit „Supportzeit (betreuter Betrieb)“ beschreibt die Zeiträume, in denen die Ressourcen vom Auftragnehmer bedient und Störungen und Anfragen bearbeitet werden.
Wartungsfenster	Regelmäßiges Zeitfenster für Wartungsarbeiten an den Systemen, in dem die Systeme nicht oder nur eingeschränkt für den Auftraggeber nutzbar sind. Sollte in Sonderfällen ein größeres oder weiteres Wartungszeitfenster beansprucht werden, so erfolgt dies in direkter Absprache mit dem Auftraggeber. Der Auftraggeber wird nur in begründeten Fällen die Durchführung von Wartungsmaßnahmen einschränken. Der Auftragnehmer wird in diesen Fällen unverzüglich über sich ggf. daraus ergebenden Mehraufwand und Folgen informieren.
Ausfallzeit	Die Ausfallzeit ist die Zeitspanne, die nach Eintritt der Nichtverfügbarkeit während der zugesagten Servicezeit vergeht, bis ein System (bzw. Systemcluster) mit allen Komponenten wieder für den Regelbetrieb zur Verfügung steht. Gemessen wird die Ausfallzeit in Stunden innerhalb der vereinbarten Servicezeiten.
Reaktionszeit	Die Reaktionszeit ist die Zeitspanne innerhalb der vereinbarten Servicezeiten zwischen der Feststellung einer Störung durch den Dienstleister bzw. Meldung einer Störung durch den Auftraggeber über den vereinbarten Weg (Service Desk) bis zum Beginn der Störungsbeseitigung. Die Reaktionszeit beginnt mit der Aufnahme der Störung in das Ticketsystem des Auftragnehmers.
Messzeitraum	Der Zeitraum, auf den sich eine Leistungskennzahl bezieht und in dem die tatsächlich erbrachte Qualität der Leistung gemessen wird. Sofern nicht anders angegeben beziehen sich alle angegebenen Metriken jeweils auf einen Messzeitraum von einem Kalenderjahr.

5.2 Erläuterung VDBI

V = Verantwortlich	“V” bezeichnet denjenigen, der für den Gesamtprozess verantwortlich ist. „V“ ist dafür verantwortlich, dass „D“ die Umsetzung des Prozessschritts auch tatsächlich erfolgreich durchführt.
D = Durchführung	“D” bezeichnet denjenigen, der für die technische Durchführung verantwortlich ist.
B = Beratung	“B” bedeutet, dass die Partei zu konsultieren ist und z.B. Vorgaben für Umsetzungsparameter setzen oder Vorbehalte formulieren kann. „B“ bezeichnet somit ein Mitwirkungsrecht bzw. eine Mitwirkungspflicht.
I = Information	“I” bedeutet, dass die Partei über die Durchführung und/oder die Ergebnisse des Prozessschritts zu informieren ist. „I“ ist rein passiv.