Service Level Agreement (SLA)

1. Festlegung Verfügbarkeit und Betriebszeiten

Bei RIB (MTWO) sind folgende Bedingungen Vertragsgrundlage.

Incident Level	Priorität 1	Priorität 2	Priorität 3	Priorität 4
1st Level Support	Endkunde			
2nd Level Support	RIB			
3rd Level Support	RIB			
Supportzeiten	Werktags Mo-Fr 08:00 – 17:00 CET			
Reaktionszeiten für Produktiv Systeme innerhalb der Supportzeiten	1 h	2 h	1 d	2 d
Reaktionszeiten für nicht-Produktiv Systeme innerhalb der Supportzeiten	-	4 h	1 d	2 d
Information über aktuellen Bearbeitungsstatus	1 x pro h proaktiv	Alle 2 h	1 x pro d	1 x pro d
Backup und Retention Time	Application und Storage: Backup Vorhaltungszeit 8 Tage mit einem Full Backup pro Tag. Datenbank: Point in Time Restore mit Wiederherstellung von jedem beliebigen Datenbestand innerhalb der letzten 8 Tage.			
SLA-Verfügbarkeit	Produktiv Systeme: 99,5%. Nicht- Produktiv Systeme: 98,0% (sofern vorhanden)			
Redundanz	Single - Zone innerhalb der Azure location			

Definition und Geltungsbereich

Das SLA bezieht sich auf den Service, der aus Plattform Infrastruktur und Applikation besteht. Verfügbarkeit ist gegeben, wenn die Applikation erreichbar ist.
Die Serververfügbarkeitsgarantie gilt nicht während der Wartungs- und Release Management Zeitfenster.
Die Verfügbarkeit von RIB-Systemen wird am Ende eines jeden Monats wie folgt gemessen:
Verfügbarkeit in % = 100*(gesamte verfügbare Zeit - relevante Ausfallzeit) /gesamte verfügbare Zeit
Die gesamte verfügbare Zeit wird auf der Grundlage der vereinbarten Servicezeit (pro Quartal) abzüglich der im Voraus vereinbarten Wartungsarbeiten (Wartungsfenster, geplante Wartung) ermittelt. Die "relevante Ausfallzeit" ist definiert als die Zeitspanne (innerhalb der vereinbarten Betriebszeiten) zwischen der Meldung einer Störung und ihrer Behebung.

Verfügbarkeit und Betriebszeiten

Die Verfügbarkeit ist der Zeitraum, in dem die Plattform für die Anwendung mindestens bereitsteht. Der Zeitraum beträgt grundsätzlich 24x7 (24 Stunden pro Tag an 7 Tagen pro Woche). In dieser Zeit ist MTWO grundsätzlich erreichbar.
Darüber hinaus werden Kernbetriebszeiten und Nebenbetriebszeiten von iTWO definiert. Hiervon unberührt sind die vereinbarten Support Zeiten. Der Unterschied zwischen Kernzeiten und Nebenzeiten ist ausschließlich die Leistungsfähigkeit der angebotenen Service Infrastruktur.

- **Kernbetriebszeiten**: Mo-Fr 07:00-17:00. Das System steht mit voller Leistung zur Verfügung.
- **Nebenbetriebszeiten**: Zeit außerhalb der Kernbetriebszeit. Das System steht mit reduzierter Leistung zur Verfügung, da von einer verringerten Nutzerintensität in diesem Zeitraum ausgegangen wird. Der Zugriff der maximalen Anzahl von Nutzern ist dennoch möglich.

Wichtige Voraussetzungen für Managed Azure Services

Die erfolgreiche Bereitstellung und Implementierung der MTWO Azure Plattform basiert auf den folgenden Hauptvoraussetzungen:

- MTWO wird immer im Azure-Abonnement der RIB betrieben, da für MTWO ein bestimmtes Maß an administrativem Zugang erforderlich ist, um die erforderlichen Überwachungs- und Managementinstrumente zur Kostenkontrolle und zum Servicemanagement zu gewährleisten. Dies ist

ein wesentlicher Teil des Dienstes.

- Voraussetzung für die erfolgreiche Bereitstellung von Anwendungen ist, dass eine geeignete Internetverbindung von jeder der Benutzergruppen (unabhängig von der geographischen Verteilung) verfügbar ist. Für wichtige Kundenstandorte verfügt Microsoft Azure über dedizierte Zugriffsoptionen, die gegen zusätzliche Kosten zur Verfügung gestellt werden können. Ansonsten liegt es jedoch in der Verantwortung des Kunden, sicherzustellen, dass eine geeignete Konnektivität verfügbar ist, um die erforderliche Anwendungsleistung zu erbringen. Falls erforderlich, können wir Beratungsdienstleistungen bei der Evaluierung von Anbindungsoptionen für Microsoft Azure anbieten.

Security
Wir verwenden Richtlinien und Verfahren, um den unbefugten physischen und logischen Zugang zu den Diensten zu verhindern, um die Kundendaten bestmöglich zu schützen.
MTWO basiert auf einem der leistungsfähigsten und sichersten Plattformen der Welt: Microsoft Azure
Sichert Betrieb durch eine Vielzahl von Zertifizierungen, von denen hier nur einiger relevante genannt sind: ISO/IEC 27001:2013, BSI IT-Grundschutz, ISO/IEC 27017 und 27018, SOC 1 Typ II

Backup
Teil der Managed Azure Services ist ein tägliches Backup auf Applikations-Ebene. (d.h. nicht auf Workload-Ebene). Die Standardverweildauer beträgt 8 Tage mit 1 Vollsicherung pro Tag. Wiederherstellungen können für eine vollständige Applikation oder auf Dateibasis durchgeführt werden.

Data Restore
Daten können aus Sicherungen durch einen Request wiederhergestellt werden. Der Kunde kann die Wiederherstellung von Daten für ein bestimmtes Datum innerhalb der definierten Sicherungsaufbewahrungsrichtlinie (s. Backup wie oben beschrieben) anfordern. Die Wiederherstellungszeit kann je nach Größe der Sicherung variieren. Wiederherstellungszeiten sind von den garantierten Verfügbarkeitszeiten ausgeschlossen.

Monitoring
Ein Teil der Managed Azure Plattform ist die Überwachung der Dienste.
- Netzwerk-Schicht
- Gateway up
- Remote-Ping auf öffentliche IP's
- Gateway-Bandbreitenkapazität

Die oben genannten KPIs des Überwachungssystems werden für Produktionsumgebungen auf einer 24x7-Basis überwacht.

Patch Management
Sicherheits- und kritische Updates werden automatisch auf monatlicher Basis von Microsoft für alle Betriebssysteme bereitgestellt und gemäß regelmäßigen Wartungsplan angewendet.

Environment	**Zeit**
Produktiv Systeme	CET Mo-Fr 18:00-07:00 + Wochenende 24h
Nicht Produktiv Systeme	CET Mo-Fr 08:00-18:00

Release Management
Um sicherzustellen, dass die einzelnen Services immer miteinander kompatibel sind und in Summe die bestimmungsgemäße Funktion liefern, umfasst das Release Management die eigentliche Anwendungssoftware in Kombination mit allen beteiligten Komponenten und Diensten von Microsoft Azure. Die RIB folgt dem Lebenszyklus der Microsoft Azure Services und bezieht diese in das Release Management ein. Die RIB ist verantwortlich für das Release Management und führt Releases entsprechend durch.

Environment	**Zeit**
Produktiv Systeme	CET Sa 18:00 - So 07:00
Nicht Produktiv Systeme	CET Mi 18:00 - Do 07:00 oder nach Vereinbarung

Die SLA und alle hierin enthaltenen Bestimmungen gelten nicht für Dienste, Anwendungen und/oder Versionen, die vom Anbieter als „End-of-Life“ erklärt wurden.

Jeglicher Support, der in Verbindung mit Diensten, Anwendungen und/oder Versionen am Ende der Lebensdauer geleistet wird, wird dem Kunden bei Supportanfragen in Rechnung gestellt.

2. Support

Der Kunde kann sich an den Support wenden, um Incidents zu lösen, Service Requests zu stellen oder Change Requests zu beantragen. Diese Anfragen müssen im Serviceportal registriert werden. Nur Benutzer des Kunden mit entsprechender Berechtigung können Incidents und Requests melden.

Incidents

Zur Registrierung, Verfolgung und Lösung von Incidents kann der Kunde diese melden. Innerhalb unseres SLAs führen wir eine proaktive Überwachung durch. Dies bewirkt, dass möglichen Probleme proaktiv an die Partner gemeldet werden können, so dass die Auswirkungen eines Problems minimiert werden können.

Incident levels werden nach Schweregrad definiert.

- Priorität 1- Kritisch: Das Problem verursacht einen vollständigen Verlust des Dienstes einschließlich Einschränkung der Systemverfügbarkeit und Datenintegrität, ohne dass ein Workaround verfügbar ist. Die Arbeit kann nicht fortgesetzt werden, da die Funktion des Dienstes die Arbeit nicht zulässt und der Betrieb für das Unternehmen geschäftskritisch ist. Die Mehrheit oder alle Benutzer sind betroffen. Priorität 1 Incidents gelten nur für Produktiv Systeme.
  Hinweis: Neben der Registrierung im Serviceportal ist auch die Priorität 1- Kritische Incidents telefonisch zu melden.

- Priorität 2 - Dringend: Die Hauptfunktionalität ist beeinträchtigt oder die Leistung ist stark beeinträchtigt. Das Problem ist hartnäckig und betrifft viele Benutzer und/oder wichtige Funktionen. Es ist kein vernünftiger Workaround verfügbar.

- Priorität 3 - Hoch: Problem mit der Systemleistung oder Fehler, der einige, aber nicht alle Benutzer betrifft. Ein kurzfristiger Workaround ist verfügbar, aber nicht skalierbar.

- Priorität 4 - Mittel: Anfrage zu einem technischen Routineproblem; Fehler, der eine kleine Anzahl von Benutzern betrifft. Angemessener Workaround verfügbar. Die Lösung muss so schnell wie möglich erfolgen.

Bei der Aufnahme des Incidents wird die Priorität festgelegt. Die Priorität kann durch die RIB geändert werden, wenn sie nicht der beschriebenen Klassifizierung entspricht. Dies wird dokumentiert und im Serviceportal mit einer Benachrichtigung versehen.
Nur autorisierte Benutzer dürfen Incidents mit dem MTWO Service Center auf einer 24x7-Basis über das Serviceportal melden. Incident Berichte müssen auf Englisch eingegeben werden.

Requests

Service Requests
Service Requests sind in der Regel Anfragen bezüglich Informationen oder Beratung oder nach Standardaktion (wie z.B. rücksetzen eines Passworts), die in der Regel nicht mit einer Ausfallzeit verbunden sind oder eine schnelle Wiederherstellungszeit haben. Das MTWO-Servicecenter legt nach Rücksprache mit dem Auftraggeber fest, ob es sich bei der gemeldeten Anforderung um einen Service Request oder einen Change Request handelt. Service Requests werden nach Time and Material in Rechnung gestellt.

Change Requests
Änderungen von Service-Konfigurationen können über einen Change Request beantragt werden. Das MTWO Service Center wird nach Rücksprache mit den Parteien Änderungswünsche planen. Change Requests werden auf Time- and Material Basis in Rechnung gestellt. RIB ist nicht verpflichtet, der Ausführung eines Change Request zuzustimmen. Sollte die Ausführung eines Change Request abgelehnt

werden, wird dem Antragsteller umgehend eine Erläuterung gegeben.
Nur autorisierte Benutzer dürfen Change Request beim MTWO Service Center über das Serviceportal eingeben.
Dringende Change Request müssen telefonisch gemeldet werden.
Alle Änderungen, die außerhalb der normalen Supportzeit in der Primärregion ausgeführt werden müssen, sollten während der Supportzeit des Servicezentrums gemeldet werden, wobei eine ausreichende Vorlaufzeit für die ordnungsgemäße Planung der Aktivitäten zu berücksichtigen ist.

3. Wartung

RIB wird die Plattform und die Dienste in Übereinstimmung mit den folgenden Bestimmungen warten:

- Bestimmungen, Anweisungen, Garantiebedingungen, Handbücher und Wartungspläne der jeweiligen Anbieter
- Anweisungen von Lieferanten in Bezug auf Sicherheitsbenachrichtigungen
- Managed Services Richtlinien bezüglich Verfügbarkeit, Sicherheit, Integrität, Schutz persönlicher Daten und Vertraulichkeit von Daten im Allgemeinen

Wartungsaktivitäten werden innerhalb des beschriebenen Wartungsfensters durchgeführt. Die von Microsoft auf der Azure-Plattform durchgeführte Wartung ist von den Bestimmungen dieses SLA ausgenommen, Microsoft ist ausschließlich für alle Wartungsaktivitäten auf der Azure-Plattform verantwortlich.

Geplante Wartung
Geplante Wartungsarbeiten werden durchgeführt, um die Integrität, Verfügbarkeit und Konsistenz der Dienste zu gewährleisten. Sollte der Service im Rahmen der geplanten Wartung nicht verfügbar sein, wird diese Ausfallzeit nur in den dafür vorgesehenen Wartungsfenstern stattfinden. Die geplante Wartung umfasst unter anderem Sicherheitsupdates und Patches, wie sie von Microsoft zur Verfügung gestellt werden und automatisch auf einer monatlichen Basis angewendet werden.

Notfallwartung
Beinhaltet Notfall-Wartungsaktivitäten, um die die Integrität, Verfügbarkeit und Konsistenz der Dienste in einem Notfall wiederherzustellen oder zu gewährleisten. RIB unternimmt jeden angemessenen Versuch, die Parteien vor Beginn der Wartung zu informieren. Ist eine Benachrichtigung vor Beginn der Wartungsarbeiten nicht möglich, erfolgt die Benachrichtigung so schnell wie möglich nach Abschluss der Wartungsarbeiten.

Missbrauch
RIB kann vermutete Verstöße gegen diese Bestimmungen oder den Missbrauch von Diensten untersuchen und jede ungesetzlich erscheinende Aktivität den zuständigen Aufsichtsbehörden melden. Darüber hinaus behält sich RIB das Recht vor, Anwendungen, Systeme, Netzwerke und Daten zu untersuchen, um IP-Probleme, Viren, Würmer oder andere Software, die als schädlich angesehen werden können, aufzudecken. Dies gilt ebenso für Aktivitäten, bei denen der Verdacht auf Verstöße oder eine mutmaßlich unzulässige Nutzung besteht.
RIB kann den Zugang zu Ressourcen oder Diensten, von denen vermutet wird, dass sie gegen die Bestimmungen dieses SLA verstoßen, aussetzen, deaktivieren oder ändern. Im Falle solcher Verstöße oder des Missbrauchs von Diensten wird RIB, sofern möglich, die betroffenen Parteien vor dem Beginn solcher Maßnahmen zu benachrichtigen. Im Falle einer gerechtfertigten Aussetzung, Sperrung des Zugangs zu Ressourcen oder Services oder deren Änderung bleiben alle Vereinbarungen zwischen den Parteien sowie die Verpflichtungen der Parteien wie z.B., aber nicht ausschließlich, die Zahlung aller fälligen ausstehenden Beträge, in Kraft.

4. Bestimmungsgemäße Nutzung

Die bereitgestellten Dienste dürfen ausschließlich für den Zweck, für den sie bestimmt sind, genutzt werden, damit sie die Sicherheit, Verfügbarkeit und Integrität eines Netzwerks, Computers oder Kommunikationssystems nicht gefährden. Zu den verbotenen Nutzungen gehören unter anderem:

unbefugter Zugriff auf Systeme, Pentests ohne vorherige Koordination und Zustimmung durch RIB, Verletzung jeglicher Sicherheits- oder Authentifizierungsmaßnahmen, Überwachung von Daten oder Datenverkehr, Überlastung oder Datenüberflutung von Systemen oder Netzwerken, Betrieb von offenen Proxies, Open Mail Relays, offenen rekursiven Domain- Nameservern, Verteilung, Veröffentlichung, Versand oder Unterstützung des Versands von unerwünschten Massen-E-Mails oder anderen Nachrichten.

Bei der Nutzung der bereitgestellten Dienste gibt es Verantwortlichkeiten, die beim Kunden liegen. Dies ist z.B. die Berechtigung zur Benutzerverwaltung innerhalb der Anwendung und die Anwendungskonfiguration.

- Der Kunde darf selbst keine Dienste bereitstellen, ändern oder löschen. Beide Parteien sind dafür verantwortlich, dass geeignete Maßnahmen zum Schutz der Zugangsdaten und zur Gewährleistung einer ordnungsgemäßen Benutzerverwaltung getroffen werden.
- Beide Parteien sind dafür verantwortlich, dass Änderungen an Parametern und Konfigurationen der Dienste wie z.B. Integrationen o. ä. entsprechend autorisiert, bewertet, genehmigt und implementiert werden und das Monitoring, dass durch RIB erfolgt während dieser Änderungen deaktiviert wird. Andernfalls können überwachte Werte verfälscht werden, die die Leistung und Verfügbarkeit der Services dokumentieren.
- Der Kunde ist für die Kompatibilität der in seiner Verantwortung liegenden Hard- und Software-Landschaft in Bezug auf die von der RIB zur Verfügung gestellten Dienste verantwortlich.
- RIB ist vom Kunden unverzüglich über Verstöße gegen die Privatsphäre oder Vertraulichkeit, die unbefugte Verwendung von Zugangsdaten oder andere Sicherheitsverletzungen zu informieren.
- Der Kunde stellt sicher, dass qualifiziertes und autorisiertes Personal zur Verfügung steht, dass die von RIB durchzuführenden Supportaufgaben und Anweisungen ausführen und unterstützen kann.
- Die Parteien sind dafür verantwortlich, dass die autorisierten Benutzer gepflegt und auf dem neuesten Stand gehalten werden. Darüber hinaus sind die Parteien für alle Anfragen der von ihnen benannten autorisierten Benutzer verantwortlich.