META10 AG
Haldenstrasse 5
6340 Baar
phone: 041 500 11 00
email: info@meta10.com
web: www.meta10.com

META10 Secure Cloud

SLA – Service Level Agreement

Inhaltsverzeichnis

META10 AG
Haldenstrasse 5
6340 Baar
phone: 041 500 11 00
email: info@meta10.com
web: www.meta10.com

4.1. Service Level

Es existieren zwei Service Level, Standard und Extended, aus denen der Kunde bei Abschluss des Vertrages die für ihn beste Variante auswählen kann.

Der «Standard Service Level» ist ohne Aufpreis in der META10 Secure Cloud enthalten. Der «Extended Service Level» kann gegen Aufpreis aktiviert werden, und bietet erweiterte Leistungen im Bereich Verfügbarkeit, Garantie und Support.

Wählt der Kunde den «Extended Service Level», muss der kostenpflichtige «Extended Support Level» obligatorisch dazu aktiviert werden.

Die verfügbaren Service Level unterscheiden sich wie folgt:

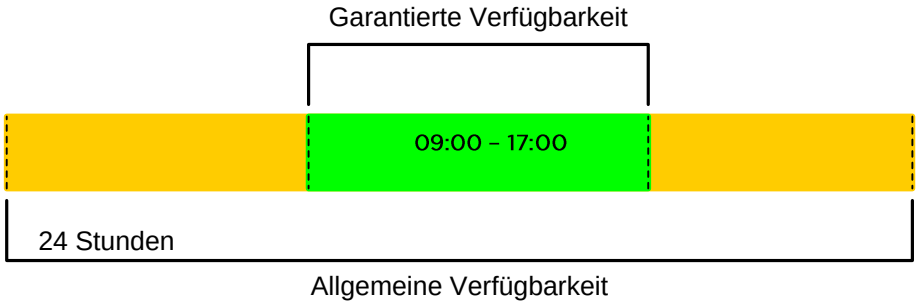
Funktion	Standard Service Level	Extended Service Level
Allgemeine Verfügbarkeit 365 Tage / 24 Std.	✓	✓
Garantierte Verfügbarkeit 09:00 – 17:00 Uhr	✓	✓
Garantierte Verfügbarkeit 07:00 – 19:00 Uhr		✓
CashBack bei Überschreiten der maximal erlaubten Ausfallzeiten		✓
Erweiterte Support Hotline		✓
Garantierte Reaktionszeit bei Anfragen		✓
Persönlicher Key Account Betreuer		✓
«Extended Support Level» obligatorisch (kostenpflichtig)		✓

4.2. Verfügbarkeit

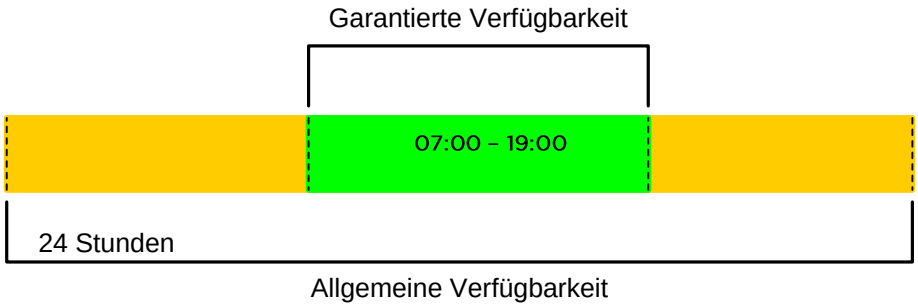
4.2.1 Zeitfenster

Bei der Verfügbarkeit wird zwischen einer allgemeinen und garantierten Verfügbarkeit unterschieden:

Standard Service Level:



Extended Service Level:



4.2.2 Allgemeinde Verfügbarkeit

Die META10 Secure Cloud Infrastruktur steht den Anwendern grundsätzlich während 365 Tagen im Jahr, 24 Stunden pro Tag zur Verfügung (365/24 Betrieb). Allerdings wird die Verfügbarkeit nur während der definierten Zeitspanne der „Garantierten Verfügbarkeit“ auch garantiert.

4.2.3 Garantierte Verfügbarkeit

Standard Service Level:

Im Zeitfenster von Montag – Freitag von 09:00 – 17:00 wird eine Verfügbarkeit von 99.5% garantiert. Zu den restlichen Zeiten gilt die allgemeine Verfügbarkeit.

Extended Service Level:

Im Zeitfenster von Montag – Freitag von 07:00 – 19:00 wird eine Verfügbarkeit von 99.5% garantiert. Zu den restlichen Zeiten gilt die allgemeine Verfügbarkeit.

Zur Überprüfung wird die Verfügbarkeit durch geeignete Programme und/oder Verfahren von META10 überwacht und dem Kunden jährlich mitgeteilt.

Das Zeitfenster bezieht sich auf die lokale Zeit in der Schweiz.

Folgende Unterbrüche sind von der garantierten Verfügbarkeit ausgeschlossen:

- Wartungsfenster
- Unterbrüche der Internetverbindung
- Unterbrüche durch Fehler in der lokalen IT Infrastruktur des Kunden, z.B. PC, Firewall, Smartphone, etc.
- Software von Drittanbietern welche wegen Programmier- oder Kompatibilitätsfehler vollständig oder teilweise nicht benutzbar ist
- Cyberattacke
- Höhere Gewalt

Für die Berechnung der garantierten Verfügbarkeit werden 100% wie folgt definiert:

Der Zeitraum, in dem die Services gemäss Vereinbarung und dem abgemachten Level der Verfügbarkeit zur Verfügung stehen sollten, abzüglich der Ausfallzeiten, welche META10 nicht zu vertreten hat und abzüglich der geplanten und angekündigten Wartungsfenster.

Der Zeitraum, über welchen die Verfügbarkeit gemessen wird, sind 12 Monate.

4.2.4 CashBack

→ Ein CashBack gilt nur für Kunden mit einem vereinbarten Extended Service Level.

Berechnung:

Für jedes Prozent, um welches die garantierte Verfügbarkeit unterschritten wird, erhält der Kunde eine Gutschrift von 3% des monatlichen Mietbetrages für den betreffenden Monat. Die Gutschrift wird von der nächsten Rechnung in Abzug gebracht.

Unterschreitung der garantierten Verfügbarkeit in % = Nicht Verfügbarkeit des Service in Std. / (Garantierte Verfügbarkeit in Std. / 100)

Gutschrift = Unterschreitung % * 3 * monatliche META10 Secure Cloud Miete

Sind die Services nur teilweise nicht verfügbar (z.B. durch Ausfall einer einzelnen Applikation oder Ausfall des Email Systems), so fällt dies erst ab dem Zeitpunkt unter die Berechnung der garantierten Verfügbarkeit, an welchem die Geschäftsfähigkeit des Kunden analog einem Totalausfall erheblich eingeschränkt wird.

Bei längerem Wegfall eines wichtigen Teil-Service erhält der Kunde für die prozentuale Ausfallzeit (Ausfallzeit in Std. / (garantierte Verfügbarkeit in Std. / 100)) die für diesen Teil-Service im entsprechenden Monat bezahlte Gebühr anteilsmässig als Gutschrift der nächsten Rechnung abgezogen.

Handelt es sich bei dem Teil-Service um eine Applikation eines Drittherstellers, kann META10 für Probleme im Zusammenhang mit Fehlern oder Kompatibilitätsproblemen in der Applikation keine Garantie übernehmen. Solche Fehler werden nicht als von META10 verantwortete Ausfallzeiten deklariert und sind daher auch nicht Rückvergütungsberechtigt. Solche Fehler werden sofort dem Dritthersteller gemeldet und nach zur Verfügung stellen von Lösungen des Drittherstellers in der META10 Secure Cloud installiert.

Die Summe aller Gutschriften pro Monat ist auf die monatliche META10 Secure Cloud Miete begrenzt.

4.2.5 Weitergehende Haftung

Jede weitere Haftung oder Verpflichtung im Zusammenhang mit der Erbringung von Leistungen sowie Einsatz und Gebrauch des Arbeitsresultates und die damit erzielten Resultate, insbesondere für indirekte oder Folgeschäden wie entgangener Gewinn, Arbeitsausfall, Personalkosten, nicht realisierte Einsparungen, Mehraufwendungen des Auftraggebers, Rekonstruktion und Wiederherstellung von Daten, oder Ansprüche Dritter, wird ausdrücklich ausgeschlossen.

4.2.6 Wartungsfenster

Die META10 AG führt regelmässige Wartungsfenster durch, welche der Pflege der META10 Secure Cloud dienen. Die Wartungsfenster werden den Kunden im Voraus angekündigt. Während einem Wartungsfenster kann es zu Unterbrüchen in der Verbindung und dem Bereitstellen der META10 Secure Cloud kommen.

Die Wartungsfenster dienen zum Durchführen von Softwareaktualisierungen, Austauschen von Hardware, Anpassen von Konfigurationen, Erneuern von Infrastruktur, etc., und sind zwingend nötig um den reibungslosen Betrieb der META10 Secure Cloud sicherstellen zu können.

Die Wartungsfenster werden auf der Webseite www.meta10.info vorangekündigt. Die META10 AG kann davon abweichende Wartungsfenster (ausserterminlich) durchführen. Diese werden durch entsprechende Ankündigung per Email und auf der Website dem Kunden angezeigt.

4.3. Verantwortlichkeiten

4.3.1 META10 Secure Cloud Infrastruktur

Die META10 Secure Cloud Infrastruktur liegt in der Verantwortung der META10 AG.

4.3.2 Lokale Infrastruktur

Die lokale IT Infrastruktur wie PCs, Drucker, Scanner, Switch, Router, Internetverbindung, usw. , liegt in der Verantwortung des Kunden. Unterstützung im Bereich der lokalen IT Infrastruktur durch META10 ist kostenpflichtig.

4.4. Patches, Updates und Upgrades

4.4.1 Updates von gemieteter Standard Software

Die vom Kunden per Miete eingesetzte Standard Software wird in der META10 Secure Cloud laufend aktualisiert. Bei der gemieteten Standard Software handelt es sich um die Betriebssysteme, Microsoft Office,

Backupsysteme, Sicherheitssysteme, Überwachungssysteme, sowie alle sonstige Software welche zur Bereitstellung des Standardservices benötigt wird. Ausgeschlossen davon sind jegliche für den Kunden individuell betriebene Software, unter anderem sind dies alle Applikationen unter dem Begriff MyApp, sowie jede andere Software welche im Auftrag des Kunden installiert, betrieben und upgedatet wird.

Bei den Updates wird zwischen Patches, Updates und Upgrades unterschieden.

- Patches sind die laufenden Aktualisierungen der Software anhand vom Softwarehersteller entdeckter Fehler oder Defekte, z.B. Patch von Outlook zur Bekämpfung von Viren oder Spam.
- Updates (oder Service Packs) sind Verbesserungen der Software in der aktuellen Version. Oftmals enthalten Updates mehrere zusammengefasste Patches, welche sich seit dem letzten Update angesammelt haben.

Alle Patches und Updates werden normalerweise immer auf eines der regelmässig stattfindenden Wartungsfenster gelegt. Ist eine Aktualisierung ausserhalb eines Standard-Wartungsfensters nötig, kann das Wartungsfenster auch kurzfristig durchgeführt werden, im Notfall ohne vorherige Ankündigung (z.B. bei wichtigen Patches wegen Cyberbedrohungen, etc.).

Während Updates kann der Kunde die Systeme welche upgedatet werden nicht benutzen.

4.4.2 Updates von individueller Software

Unter individueller Software wird jegliche für den Kunden individuell betriebene Software verstanden, unter anderem sind dies alle Applikationen unter dem Begriff MyApp, sowie jede andere Software welche im Auftrag des Kunden installiert, betrieben und upgedatet wird. Dies sind z.B. auch PDF Programme oder Internetbrowser welche der Kunde individuell für sich installieren liess.
Das Patchen, updaten und upgraden jeglicher individuellen Software ist im Abo Preis nicht enthalten, sondern separat und kostenpflichtig.

4.4.2.1 Vorgehen

Der Kunde sendet an den CustomerService genügend früh eine schriftliche Anfrage seine individuelle Software zu aktualisieren. Darin nennt er genau um welche Software es sich handelt, auf welche Version aktualisiert werden soll, sowie seinen Wunschtermin.
META10 schätzt den Aufwand ab und plant dann in Abstimmung mit dem Kunden ein individuelles Aktualisierungsdatum ein und teilt dies dem Kunden mit.

4.4.2.2 Voraussetzungen

META10 überprüft die für eine Aktualisierung nötigen Voraussetzungen. Müssen für eine Aktualisierung einer Software auch nötige Voraussetzungen vorgängig aktualisiert werden, teilt dies META10 dem Kunden mit. Dabei wird dem Kunden, wenn möglich auch der daraus resultierende Zusatzaufwand und die Zusatzkosten kommuniziert. Falls sich nötige Anpassungen der Voraussetzungen erst nach einem Update zeigen, werden dies dem Kunden angezeigt und der Kunde muss die nötigen Anpassungen in Auftrag geben. Die daraus entstehenden Kosten sind vom Kunden zu tragen, auch dann, wenn META10 aus Versehen dem Kunden die nötigen Voraussetzungen nicht vorgängig mitgeteilt hat oder mitteilen konnte.

Beispiele von nötigen Voraussetzungen welche auch aktualisiert werden müssen:
- neue Betriebssystemversion
- neue Microsoft Office Version
- neue SQL Server Version
- neue .NET Version
- mehr CPU, Ram oder Diskspace
- zusätzliche Lizenzen
- zusätzliche Server

Alle für eine Aktualisierung nötigen Voraussetzungen welche angepasst werden müssen, sind in jedem Fall kostenpflichtig.

4.4.2.3 Vorbereitung

Jede Aktualisierung der Software muss vorbereitet werden und braucht deshalb eine entsprechende Vorlaufzeit. Üblicherweise kann daher eine Aktualisierung nicht «auf die Schnelle» durchgeführt werden, son-

dern benötigt zwischen einigen Tagen bis Wochen Vorlaufzeit. Daher muss der Kunde gewünschte Aktualisierungen im Voraus genügend früh anzeigen um eine geordnete Vorbereitung und Bearbeitung zu ermöglichen.

4.4.2.4 Zeitpunkt

Updates von individueller Software erfolgen während den normalen Öffnungszeiten des META10 CustomerService. Daher muss der Kunde einen Zeitpunkt wählen wo er das entsprechende System nicht benutzt. Wünscht der Kunde die Durchführung ausserhalb der normalen Öffnungszeiten, ist dies nur gegen Zusatzkosten und in Abstimmung mit META10 möglich.

4.4.2.5 Testsystem

Der Kunde hat die Möglichkeit für individuelle Software eine Testumgebung gegen entsprechendes Entgelt betreiben zu lassen. Etwaige Aktualisierungen einer Software können dann unabhängig vom produktiven System auf dem Testsystem installiert werden, und durch den Kunden getestet werden. Nach erfolgreichem Test und Freigabe durch den Kunden, wird dann separat das Produktivsystem aktualisiert.

4.4.2.6 Direktes Aktualisieren des Produktivsystems

Kunden welche kein Testsystem betreiben sind damit einverstanden, dass eine direkte Aktualisierung des Produktivsystems Probleme verursachen kann, und damit zu Ausfällen des Produktivsystems führen kann. Die Kunden ohne Testsystem sind sich dem bewusst und nehmen das Risiko in Kauf zwecks Einsparung der Kosten eines Testsystems.

Entstehen bei der Aktualisierung des Produktivsystems Probleme, sind alle daraus entstehenden Zusatzaufwendungen kostenpflichtig.

4.4.2.7 Aufwand

Der gesamte Aufwand zur Aktualisierung, inkl. Vor- und Nacharbeiten, werden dem Kunden über die Supportrechnung fakturiert, und sind in jedem Fall kostenpflichtig.
Treten während oder nach einer Aktualisierung Probleme auf die wegen der Aktualisierung entstanden sind, fallen alle daraus entstehenden Aufwendungen zu Lasten des Kunden.
Kann eine Aktualisierung nicht erfolgreich eingespielt werden, und für den Kunden muss die Software auf den Stand vor der Aktualisierung zurückgesetzt werden, sind alle Aufwendungen für die Durchführung der Aktualisierung sowie für die Zurücksetzung in jedem Fall kostenpflichtig.
Treten nach einer Aktualisierung einer Software Probleme auf, ist der Kunden dafür vollumfänglich verantwortlich.

4.5. Software Maintenance

Für die in der META10 Secure Cloud eingesetzte Software ist grundsätzlich ein Maintenance Vertrag obligatorisch. Alle von META10 eingesetzte Microsoft Software hat automatisch einen Maintenance Vertrag und wird laufend erneuert. Für Branchensoftware ist durch den Kunden grundsätzlich mit dem jeweiligen Hersteller der Applikation ein Maintenance- / Updatevertrag abzuschliessen. Nur in Ausnahmefällen kann eine Software des Kunden ohne laufende Maintenance in der META10 Secure Cloud betrieben werden, und nur wenn die META10 dazu explizit schriftlich zustimmt. Jeglicher Aufwand im Zusammenhang mit dem Betrieb und den Updates gehen zu Lasten des Kunden.

4.5.1 Verantwortung für Lizenzen

Alle in der META10 Secure Cloud gemieteten Software-Lizenzen liegen in der Verantwortung der META10. Die Lizenzen für nicht im META10 gemietete Software, sowie die Lizenzen für lokale Infrastruktur, liegen in der Verantwortung des Kunden.

4.6. Internetverbindung

Die META10 AG übernimmt keine Garantie oder Gewährleistung dafür, dass die Internetverbindung zwischen dem Standort des Kunden und dem Standort der Rechenzentren der META10 AG ununterbrochen funktioniert. Unterbrüche der Internetverbindung im Rechenzentrum der META10 AG werden sofort dem Internetprovider der META10 AG gemeldet und vom Provider so schnell wie möglich behoben.

Unterbrüche der Internetverbindung beim Standort des Kunden liegen in der Verantwortung des Kunden und sind durch ihn bei seinem jeweiligen Internetprovider zu melden. Für die Behebung eines solchen Unterbruchs ist der Kunde und sein Internetprovider zuständig. Unterstützung des Kunden oder Internetproviders durch META10 ist für den Kunden kostenpflichtig.

Der Kunde ist verpflichtet eine den Anforderungen für einen reibungslosen Betrieb genügende Internetverbindung bei einem Internetprovider zu beziehen. Ist seine verwendete Internetverbindung nur von ungenügender Qualität, ist z.B. instabil oder hat Unterbrüche, so übernimmt die META10 AG keine Garantie für die Funktionsfähigkeit der META10 Secure Cloud.

4.6.1 Beanspruchung der Internetverbindung

Wird die Internetverbindung in die META10 Secure Cloud durch den Kunden übermässig beansprucht, ist die META10 AG berechtigt den Zugriff und/oder die Bandbreite für diesen Kunden einzuschränken. Folgende Aktivitäten können beispielsweise zu übermässiger Beanspruchung der Internetverbindung führen:

- Up- und Downloads grosser Datenmengen
- Versand von Massenemails an mehr als 50 Empfänger
- Versand von Emails mit grossen Attachements
- Datentransfers grosser Datenmengen zwischen der META10 Secure Cloud und dem lokalen PC

4.7. User Account

4.7.1 Arten von User Accounts

Jeder Benutzer welcher Zugriff auf die META10 Secure Cloud haben möchte, benötigt dazu einen META10 Secure Cloud User Account. Es stehen zwei Arten von User Accounts zur Verfügung:

- Desktop User Account - Account mit Zugriff auf einen Remote Desktop
- Application User Account - Account mit Zugriff auf eine Remote Applikation

Der User Account wird normalerweise auf den Benutzer ausgestellt, welcher damit arbeitet.

Jeder Benutzer erhält seinen persönlichen User Account. Das für den User Account zur Verfügung gestellte Login ist persönlich und muss vom Benutzer mit entsprechender Sorgfalt behandelt werden. Dazu gehören das ändern des Initialkennwortes nach der Aufschaltung, sowie das regelmässige ändern des Kennwortes alle paar Monate. Für einen etwaigen Missbrauch seiner Logindaten wegen mangelnder Sorgfalt durch den Benutzer, lehnt META10 jegliche Haftung ab.

4.8. Aktivieren und Deaktivieren von User Accounts und Modulen

4.8.1 Auftragserteilung

Useraccounts und Module können vom Kunden monatlich auf den 1. des Monats deaktiviert oder aktiviert werden. Die Auftragserteilung durch den Kunden kann schriftlich, per Email, oder mündlich erfolgen.

Die Aufschaltung von Services generiert die entsprechenden Aktivierungs- und Servicekosten. Bei Abschaltung des Service reduzieren sich die Servicekosten um den entsprechenden Betrag.

Der aktuelle Leistungsumfang wird jeweils in der monatlich erstellten Faktura ausgewiesen.

Der Kunde hat nach Erhalt der Rechnung 30 Tage Zeit Anpassungen mitzuteilen. Danach gilt der in der Rechnung aufgeführte Leistungsumfang als vom Kunden akzeptiert.

4.8.2 Einschränkungen

Bei Software von Microsoft können Module monatlich aktiviert oder deaktiviert werden. Die bei Vertragsabschluss der META10 Secure Cloud definierte Anzahl User Accounts kann monatliche Anpassungen nach oben oder unten erfahren. Aufschaltungen von Services werden ab dem Monat der effektiven Aufschaltung in Rechnung gestellt. Gewünschte Abschaltungen von Services, welche vor dem 1. des jeweiligen Monats schriftlich gemeldet werden, werden im Folgemonat nicht mehr in Rechnung gestellt, ausser der Kunde hat den entsprechenden Service weiter verwendet.

Module von Drittherstellern können normalerweise nicht auf monatlicher Basis deaktiviert werden, da der jeweilige Dritthersteller eine Mindestlaufzeit vorschreibt (meist zwischen 3 – 12 Monaten). Bei Deaktivierung eines solchen Moduls laufen die Kosten weiter bis zum frühestmöglichen Kündigungstermin welche durch den Dritthersteller vorgegeben werden.

Wird vom Kunden erworbene und in der META10 Secure Cloud einmal deaktivierte Software wieder reaktiviert, muss auf die zu diesem Zeitpunkt in der META10 Secure Cloud aktuelle Version dieser Software upgedatet werden. Die Kosten für das Update gehen zu Lasten des Kunden. Etwaige Datentransfers oder Datenkonvertierungen gehen zu Lasten des Kunden.

4.9. Support

4.9.1 Supportzeiten

Den Benutzern der META10 Secure Cloud steht zu den üblichen Bürozeiten von

08:30 – 12:00 Uhr und von 13:30 – 17:00 Uhr ein Support unter der Tel-Nr. 041 500 11 05 oder Email customerservice@meta10.com zur Verfügung.

Kunden mit einem «Extended Support Level» steht von Mo – So von 07:00 – 19:00 ein Pikettdienst per Messenger für Notfälle zur Verfügung.

4.9.2 Reaktionszeiten

Für Kunden mit einem «Standard Service Level» Vertrag wird die Reaktionszeit nicht garantiert.

Für Kunden welche einen «Extended Service Level» Vertrag abgeschlossen haben, wird folgende Reaktionszeit auf Supportanfragen garantiert.

Prio.	Definition	Reaktionszeit	Meldung per	Innerhalb Zeitraum
1	Störfälle welche den Kunden hindern seine Geschäftstätigkeit fortzusetzen, weil alle oder die wichtigsten Teile der benötigten Applikationen und/oder Daten nicht zur Verfügung stehen.	Max. 60 min.	Pikett	Garantierte Verfügbarkeit Mo - Fr
2	Störfälle welche die Geschäftstätigkeit des Kunden stark behindern, weil wichtige Funktionen oder Leistungen nicht zur Verfügung stehen.	Max. 4 Std.	Pikett	Offizielle Supportzeiten Mo - Fr
3	Störfälle welche die Geschäftstätigkeit des Kunden wenig behindern.	Max. 48 Std.	Telefon Email	Offizielle Supportzeiten Mo - Fr

Als Reaktionszeit gilt die Zeit, welche seit der Meldung des Kunden an META10 maximal verstreichen darf, bis META10 sich beim Kunden meldet. Störfälle mit Prio 1 und 2 müssen über den Pikettservice eingehen damit die Reaktionszeit garantiert werden kann.

Es können Anfragen auch per Email auf customerservice@meta10.com eingereicht werden, allerdings können dann die Reaktionszeiten für Ereignisse mit Prio 1 und 2 nicht garantiert werden.

Trifft eine Anfrage ausserhalb des für die Reaktionszeit definierten Zeitraums ein, so wird die Reaktionszeit ab dem nächsten aktiven Zeitraum an gerechnet. Endet der Zeitraum der Reaktionszeit während eine Anfrage noch nicht beantwortet wurde, so wird die Reaktionszeit mit Beginn des nächsten aktiven Zeitraums an weitergerechnet.

Beispiel 1: Trifft eine Anfrage Prio 2 am Montag um 22:00 Uhr ein, wird die Reaktionszeit ab den offiziellen Supportzeiten am darauffolgenden Dienstagmorgen gerechnet.

Beispiel 2: Trifft eine Anfrage Prio 1 am Donnerstag um 16:45 Uhr ein, so werden die 15 Minuten bis 17:00 Uhr zur Reaktionszeit gezählt. Am Freitagmorgen läuft die Reaktionszeit ab 8:30 Uhr weiter und es muss bis 9:15 Uhr reagiert werden, damit die vereinbarte Reaktionszeit eingehalten worden ist.

4.9.3 Supportumfang

Der Support erstreckt sich über alle von META10 gelieferten Leistungen oder Produkte im Rahmen der in diesem Vertrag gewählten Konfigurationen.

Folgender Support ist in den monatlichen Gebühren enthalten:

- Anfragen bei Fehler oder Problemen innerhalb der Funktionalität der META10 Secure Cloud
- Anfragen bei Fehler oder Problemen beim Zugriff auf der META10 Secure Cloud

Der Support für folgende Anfragen ist in den monatlichen Gebühren **nicht** enthalten. Die META10 AG nimmt solche Anfragen entgegen und löst diese in Absprache mit dem Kunden. Der Aufwand für diesen Support wird in einem Ticketing- und Aufwanderfassungs-System erfasst und dem Kunden zusammen mit dem Protokoll periodisch in Rechnung gestellt:

- Probleme welche auf Benutzerfehler zurückzuführen sind
- Fragen zur Benutzung und Bedienung von installierter Software, z.B. Microsoft Word, Excel, Powerpoint, Outlook, winVS, Sage, Abacus, Proffix, usw.
- Einrichten von zusätzlichen Konfigurationen, z.B. Anbinden zusätzlicher Mailboxen, Anbinden von Postfächern über POP3 oder IMAP, Einrichten von Signaturen o.ä. in Outlook, etc.
- Support im Zusammenhang mit Emailproblemen welche nichts mit META10 zu tun haben, z.B. falsche Empfängeradresse, Problem im Emailsystem des Empfängers, etc.
- Einrichten von vom Standard abweichenden Konfigurationen, z.B. Zugriffsrechte auf dem Filesystem
- Einschleusen von Viren oder sonst schädlicher Software in die META10 Secure Cloud durch den Kunden
- Zurückspielen von durch den Kunden gelöschten oder veränderten Daten vom Backup
- Installation oder Updates spezieller Software oder Konfigurationen, welche nicht in der META10 Secure Cloud als Standard enthalten sind
- Fragen oder Probleme des Kunden in Bezug auf seine lokale IT Infrastruktur, z.B. PCs, Notebooks, Drucker, Scanner, Smartphone, Tablet, etc.
- Fragen oder Probleme des Kunden in Bezug auf sein lokales Netzwerk und seine Internetverbindung

Der Support der installierten Applikationen ist grundsätzlich nicht in den META10 Gebühren enthalten. Für einzelne Applikationen kann jedoch ein separater Supportvertrag abgeschlossen werden.

Die aufgelaufenen Supportkosten werden periodisch abgerechnet.

Der Kunde kann als zusätzlichen Service ein Monatsabo „Lokaler Support“ abschliessen. Für die Leistungen des lokalen Supports gelten der SLA unter www.meta10.com/SLA-lokal

4.9.4 Extended Support Level

Der Extended Support Level steht allen Kunden zur Verfügung, welchen diesen Zusatzservice aktiviert haben und bezahlen.

Der Extended Support Level umfasst folgende Zusatzleistungen:

- Support Hotline – Pikettdienst - Mo – So 07:00 – 19:00 Uhr
- Support Hotline – Pikettdienst - per Messenger Service
- Optional und wenn vereinbart ein Key Account Betreuer

4.9.4.1 Support Hotline - Pikettdienst

Mit dem Extended Support Level steht dem Kunden eine Support Hotline in Form eines Pikettdienstes per Messenger zur Verfügung. Der Kunde kann den Pikettdienst zur Meldung von wichtigen und dringenden Problemen nutzen.

Wie wird der Pikettdienst richtig genutzt:

1. Senden Sie über den für Sie eingerichteten Messenger eine Nachricht und beschreiben das Problem kurz und prägnant
2. Sie können die Nachricht auch mit Bildern und Videos ergänzen
3. Der Pikettdienst wird so schnell wie möglich auf Ihre Nachricht reagieren und Ihnen den Erhalt quittieren. Danach wird der Fall vom Pikettdienst einem Supportmitarbeiter zugeteilt. Dieser kümmert sich um die Meldung und versucht das Problem zu lösen
4. Wenn nötig wird der Supportmitarbeiter Sie anrufen um das Problem zu lösen.

Falsche Nutzung des Pikettdienstes:

1. Meldungen welche «normale» Supportfälle sind oder betreffen, und nicht als Notfall deklariert werden können
2. Eine Nachricht wie «Bitte anrufen», ohne Beschreibung des Problems
3. Versuch per Messenger anzurufen
4. Sehr unklare Beschreibung des Problems, z.B. durch Pauschalaussagen wie «mein Computer geht nicht»
5. Unprofessionelles Verhalten, z.B. Kraftwörter, etc.

Bei falscher Nutzung des Pikettdienstes ist META10 berechtigt solche Anfragen des Kunden zu ignorieren oder den Kunden auf eine korrekte Nutzung hinzuweisen.

Reaktionszeit:

Der Pikettdienst arbeitet nach dem «Best Effort» Prinzip, d.h. es wird so schnell wie möglich reagiert, aber keine definierte Reaktionszeit garantiert. In der Regel wird auf Meldungen innert 30 Minuten reagiert, in 80% der Fälle in unter 10 Minuten.

Für Kunden mit einem aktiven «Extended Service Level» wird die Reaktionszeit anhand dieses SLA während den üblichen Supportöffnunsgzeiten von Mo – Fr garantiert. Die Reaktionszeiten ausserhalb dieser Öffnungszeiten werden nach dem «Best Effort» Prinzip erbracht.

Wer ist berechtigt den Pikettdienst zu nutzen:

Im Service kann der Kunde bis zu 2 Benutzer in den Messengerdienst aufschalten. Die Aufschaltung von weiteren Teilnehmern ist gegen Aufpreis möglich.

4.9.4.2 Key Account Betreuer

Kunden mit einem Extended Support Level steht, optional und wenn vereinbart, ein Key Account Betreuer zur Verfügung. Dieser behandelt Anliegen welche nicht dem Support zugeordnet werden können oder welche der Support oder Pikettdienst nicht selber lösen kann.

Der Key Account Betreuer ist aber in keinem Fall die direkte Anlaufstelle für Supportanfragen oder Pikettanfragen. Alle Supportanfragen sind immer an die offiziellen Supportkanäle zu richten.

Falls der Kunde trotzdem Supportanfragen an den Key Account Betreuer richtet, ist der Key Account Betreuer berechtigt solche Anfrage kommentarlos an den Support weiterzuleiten.

Wegen Abwesenheit durch Projekte, Ferien oder Krankheit, kann die Bearbeitung von Supportanfragen durch einen Key Account Betreuer nicht garantiert werden.

4.10.Speicherplatz

4.10.1 Menge

Der verfügbare Speicherplatz ist pro Service und Benutzer vorgegeben. Bei Erreichen einer Speicherlimite bei einem Service und/oder Benutzer, muss entweder ein kostenpflichtiges Upgrade auf einen Service mit mehr Speicherplatz durchgeführt werden, oder der Benutzer muss die Datenmenge im entsprechenden Service durch löschen von Daten reduzieren.

4.10.2 Private Daten

Private Daten wie z.B. Fotos, Videos oder Musikdateien, sind auf den lokalen Geräten zu speichern und nicht ins META10 zu transferieren. Die META10 Umgebung steht für die Speicherung geschäftlicher Daten zur Verfügung. META10 kann den Kunden darauf hinweisen private Daten zu entfernen, bzw. zu löschen. Dieses Vorgehen dient auch der Sicherheit, da private Daten viel häufiger von Schadsoftware befallen sind als geschäftliche Daten. Sollte der Kunde trotzdem private Daten speichern, ist META10 berechtigt den dafür benötigten Speicherplatz in Rechnung zu stellen.

4.10.3 Physische Limiten

Die Services haben physische Limiten welche nicht überschritten werden können. Bei Erreichen einer solchen Limite muss der Speicherplatz zwingend reduziert werden, z.B. durch Archivierung von «alten» Daten.

Beispiel ist ein Exchange Postfach, welches auf 50 GB oder 100 GB limitiert ist. Bei Erreichen der Limite muss der Benutzer die Daten in seinem Postfach reduzieren.

4.10.4 Fair User Limiten

Bei Services ohne physische Limiten gilt das Fair Use Prinzip. Sollte ein Benutzer mit einem Service übermässig Speicherplatz beanspruchen, oder Daten speichern welche nicht in die Cloud gehören, ist META10 berechtigt von ihm die Reduktion des belegten Speicherplatzes durch löschen von Daten zu verlangen, oder den zusätzlichen Speicherplatz in Rechnung zu stellen. Beispiel: Ein Benutzer arbeitet lokal mit vielen Daten. Er nutzt seinen Cloud Account um dort die Daten als Backup zu sichern, damit er sich die Kosten einer Backuplösung sparen kann. Dies würde beispielsweise wegen Verstoss des Fair Use Prinzip nicht zugelassen.
META10 ist jederzeit berechtigt Anpassungen an der Speicherplatz und Transfer Limiten und dem Fair Use Prinzip anzupassen.

4.11. Datensicherheit

4.11.1 Im Allgemeinen

Alle Daten des Kunden, welche in der META10 Secure Cloud gespeichert sind, sind durch technische Sicherheitsmassnahmen vor fremdem Zugriff durch Dritte geschützt.

Die META10 AG betreibt eine den aktuellen technischen Möglichkeiten entsprechende Sicherheitsinfrastruktur, um Zugriffe durch Dritte zu verhindern. Dies beinhaltet u.a. gewartete Firewalls, Antivirensysteme, Antispamsysteme, Patchmanagement, Datenverschlüsselung, gehärtete Windows Syssteme sowie Intrusion Detection Systeme.

Die META10 AG gibt jedoch keine Garantie dafür ab, dass Zugriffe durch Hacker oder Cracker zu 100% ausgeschlossen werden können.

Wird durch die META10 AG ein Angriff durch Hacker oder Cracker auf die Systeme in den Datacentern festgestellt, werden umgehend Gegenmassnahmen getroffen und die Kunden über den Angriff informiert.

4.11.2 Standort der Datacenter

Die Datacenter der META10 AG befinden sich alle in der Schweiz.

4.11.3 Zugriff auf fremde Daten

Sollte trotz aller Sicherheitsmassnahmen der META10 AG ein Benutzer in der META10 Secure Cloud auf Daten Zugriff erhalten, welche nicht für ihn bestimmt sind, hat er den Zugriff auf diese Daten sofort einzustellen und unverzüglich die META10 AG zu benachrichtigen. Eine Verwendung oder Weitergabe von fremden Daten durch den Kunden ist auf jeden Fall rechtswidrig und kann durch die META10 AG oder den Besitzer der entsprechenden Daten rechtlich geahndet werden.

4.11.4 Passwörter

Jeder Benutzer erhält einen Benutzernamen und ein Passwort und muss sich damit in der META10 Secure Cloud anmelden.

Bei Weitergabe der Zugangsdaten (Benutzernamen und Passwörter) durch den Kunden an Dritte, haftet der Kunde für daraus entstehenden Schaden.

4.11.5 Änderung der Passwörter

META10 ist berechtigt die Benutzer periodisch zur Eingabe eines neuen Passworts aufzufordern. Der Benutzer muss sein Passwort zwingend ändern, was der Sicherheit dient.

4.11.6 Multi Faktor Authentifizierung (MFA)

Eine MFA für den Zugriff auf den Remote Desktop oder eine Remote App in der META10 Secure Cloud ist zwingend und obligatorisch.

META10 stellt eine MFA jedem Benutzer zur Verfügung. Der Benutzer muss die MFA per APP oder SMS über ein Smartphone nutzen. Dazu muss jeder Benutzer META10 bei der Anmeldung ein ihm zugeordnetes Smartphone angeben.

Es sind keine Ausnahmen erlaubt, d.h. ein Arbeiten ohne MFA ist verboten.

4.11.7 Verschlüsselung

Der Datentransfer zwischen dem PC des Anwenders und der META10 Secure Cloud wird normalerweise verschlüsselt, solange das Endgerät des Anwenders die Verschlüsselung unterstützt.

Der Transfer der Daten direkt von einem Scanner in die META10 Secure Cloud per FTP Protokoll ist nicht verschlüsselt. Falls ihr Scanner das SFTP Protokoll unterstützt kann dieses verwendet werden und damit ist die Kommunikation verschlüsselt. Falls kein SFTP vom Scanner des Kunden möglich ist, kann zwischen dem Standort des Kunden und der META10 Secure Cloud eine VPN Site-to-Site Verbindung aufgebaut und darüber gescannt werden. Ein VPN Tunnel hat aber zusätzliche Kosten in der META10 Secure Cloud und beim Kunden zur Folge, welche durch den Kunden getragen werden müssen.

4.12. Datensicherung

Alle Daten welche der Kunde auf den dafür vorgesehenen Datenspeichern auf den File- und Applikationsservern in der META10 Secure Cloud speichert, werden täglich gesichert (Company Laufwerk, Home Laufwerk, Applikationsserver und Datenbanken). Der Zustand einzelner Dateien oder Datenbanken kann damit durch die META10 AG von einem älteren Zustand rekonstruiert werden. Speichert der Kunde Daten ausserhalb der dafür vorgesehenen Speicherorte, auch unbewusst, befinden sich diese evtl. nicht im Backup. Die Verantwortung für das Speichern der Daten am richtigen Speicherort liegt beim Kunden.

Der Kunde wählt bei Abschluss des SLA den Backup Level für die gesamte Firma. Dabei muss der Backup Level für die Gesamtzahl der Accounts gelöst werden.

«Standard Backup Level – 30 Tage»

- Die täglich gesicherten Daten werden für die Dauer von 30 Tagen aufbewahrt

«Extended Backup Level – 12 Monate»

- Die täglich gesicherten Daten werden für die Dauer von 30 Tagen aufbewahrt
- Danach wird pro Monat eine Sicherung der Daten für 1 Jahr aufbewahrt

«Extended Backup Level – 10 Jahre»

- Die täglich gesicherten Daten werden für die Dauer von 30 Tagen aufbewahrt
- Danach wird pro Monat eine Sicherung der Daten für 1 Jahr aufbewahrt

- Danach wird pro Jahr eine Sicherung für 10 Jahre aufbewahrt

META10 übernimmt keine Garantie dass die Backup-Datenträger immer lesbar bleiben.

Microsoft erstellt von den Daten in der Azure Cloud, wie Microsoft 365, OneDrive, Sharepoint, Teams, usw., KEINE Backups. Nutzt ein Kunde Microsoft Azure und möchte auch von seinen Daten die er dort gespeichert hat eine Datensicherung, stellt META10 dafür den Service «Cloud Backup» zur Verfügung. Nur Kunden welche diesen Service beziehen, und dabei Microsoft Azure einbeziehen, haben damit auch ein Backup der Daten bei Microsoft Azure.

Nutzt der Kunde einen Exchange Server bei META10 (Exchange OnPremise), werden die Daten darin redundant gespeichert. Gelöschte Emails werden pro Benutzer in den Ordner «Gelöschte Elemente» abgelegt, und kann der Benutzer von dort wieder zurückholen. Werden vom Benutzer Emails innerhalb des Ordners «Gelöschte Elemente» gelöscht, oder beim Löschvorgang «unwiederuflich» gelöscht, landen diese Emails in einem «speziellen» Ordner «Wiederherstellbare Elemente». Der Benutzer oder META10 kann gelöschte Emails von diesem Ordner wieder zurückholen.

Bei diesem Verfahren handelt es sich nicht um ein klassisches Backup, sondern entspricht dem von Microsoft empfohlenen Vorgehen in Exchange Server. Microsoft Exchange Online arbeitet nach dem gleichen Prinzip.

4.12.1 Wiederherstellung von Daten

Das Wiederherstellen von Daten auf Kundenwunsch, z.B. wegen Überschreiben oder Löschen von Daten durch den Kunden, ist kostenpflichtig und wird nach Aufwand verrechnet.

Das Wiederherstellen von Systemen und Daten, welche weder auf Wunsch, noch aus Verschulden des Kunden erfolgen, sind nicht kostenpflichtig.

4.12.2 Lokale Daten

Daten welche der Benutzer auf seiner lokalen IT Infrastruktur speichert, z.B. auf seinem Notebook, werden durch die Datensicherung in der META10 Secure Cloud **nicht** gesichert. Der Benutzer hat die Möglichkeit lokale Daten vom PC in die META10 Secure Cloud zu kopieren oder umgekehrt.

Die Verantwortung für lokal auf dem PC gespeicherte Daten liegt beim Kunden.

4.13. Viren und Trojaner

Der Kunde ist verpflichtet jegliche Vorfälle zu melden welche die Sicherheit der Secure Cloud beeinträchtigen könnten, z.B. das Öffnen von «auffälligen» Emails oder Attachements, das Öffnen von «auffälligen» Webseiten oder das Öffnen oder Ausführen von «auffälligen» Dateien auf dem Filesystem. Mit auffällig ist gemeint, wenn der Benutzer etwas von der Norm Abweichendes oder Unübliches bemerkt, z.B. Emailabsender, Text in der Email, sonstige Hinweise auf manipuliertes Email, Warnmeldungen oder Fehlermeldungen, Auffälliges Verhalten von Applikationen, Auffälliger Inhalt auf Webseiten, auffälliges Verhalten seines PC oder seiner Session nach dem Besuchen von Webseiten, usw.

Nach der Meldung eines «auffälligen» Vorfalls durch den Kunden ist META10 berechtigt den Zugriff des Benutzers zu sperren und den Account in Quarantäne zu nehmen. META10 analysiert nach der Prüfung der Meldung des Kunden ob ein Full Scan des Dateisystems nötig ist, und führt dieses bei Bedarf aus. Während dieser Zeit kann der Benutzer nicht auf seinen Account zugreifen und muss warten bis die Sicherheits Checks abgeschlossen sind.

Werden durch den Kunden Viren und/oder Trojaner oder andere Schadsoftware in die META10 Secure Cloud eingeschleust, sei dies z.B. durch das Kopieren von Dateien, durch das Öffnen von Email oder durch das Öffnen von Webseiten, so haftet der Kunde für das Beseitigen der Schadsoftware und etwaige durch die Schadsoftware entstandene Schäden oder Ausfälle seiner META10 Secure Cloud Umgebung.

Die META10 Secure Cloud setzt aktuelle Antiviren und Antispamsysteme ein, kann aber keine Garantie abgeben, dass zu jedem Zeitpunkt und jeder Situation alle Schadsoftware automatisch erkannt und eliminiert

wird. Daher ist der Kunde verpflichtet, Dateien, Emails oder Webseiten mit entsprechender Vorsicht zu öffnen.

META10 kann von Kunden das obligatorische lösen und durchführen eines kostenpflichtigen Security Awareness Trainings verlangen.

Setzt der Kunde Outlook mit einem POP oder IMAP Account ein, liegt die Verantwortung für die Antiviren- und Antispamsoftware beim Kunden.

Treten in der META10 Secure Cloud Umgebung eines Kunden Viren oder Trojaner auf, ist die META10 berechtigt den Zugriff des Kunden temporär zu sperren, bis die Schadsoftware bereinigt wurde.

Alle Aufwendungen von META10 im Zusammenhang mit dem Prüfen und/oder Bereinigen von Auffälligen Meldungen, oder beim prüfen und/oder Bereinigen von Malware ist kostenpflichtig.

4.14. Einbindung fremder Emailserver

Innerhalb von META10 können fremde Emailserver eingebunden werden. Jedoch muss der Zugriff verschlüsselt über IMAP Port 993, POP3 Port 995 oder SMTP Port 465 erfolgen. Alle anderen Zugriffe, vor allem unverschlüsselte Zugriffe, sind nicht erlaubt.

4.15. Zugriff auf externe Webseiten / Webdienste

Die META10 Secure Cloud ist über verschiedene Ebenen abgesichert. Der Zugriff auf Webseiten wird über ein Sicherheitssystem überwacht und der Zugriff auf bestimmte Webseiten automatisch blockiert, z.B. wenn diese Malware beinhalten, oder gesperrten Kategorien entsprechen. Ausserdem ist der Zugriff über andere Protokolle als HTTP und HTTPS aus Sicherheitsgründen nicht möglich. Benötigen Sie für geschäftliche Zwecke Zugriff auf eine Webseite oder einen Webdienst, welcher gesperrt ist, kontaktieren Sie den META10 CustomerService. Grundsätzlich empfehlen wir Ihnen in diesem Fall aber von Ihrem lokalen PC aus zuzugreifen.

5. Cloud Apps

Für folgende Cloud Apps gelten vom Standard abweichende Vereinbarungen.

Bei folgenden Services steht im Standard keine separate Datensicherung zur Verfügung:

- META10 Cloud Services: METAdrive, Hosted Exchange
- Microsoft Cloud Services: Alle Cloud Services von Microsoft, wie Office 365 oder Teams

METAdrive ist komplett verschlüsselt und daher hat META10 keinen Zugriff auf den Dateninhalt. Es ist daher nicht möglich Daten aus dem METAdrive von einem Backup zurückzuspielen. Wenn Sie allerdings METAdrive auf ihr Homelaufwerk in der META10 Cloud synchronisieren, wird dieser Speicherort vom META10 Backup erfasst und gesichert. Die Verantwortung zur Aufschaltung des METAdrive sync und dem durchführen des sync liegt beim Kunden.

Microsoft Exchange hat kein übliches separates Backup, sondern es wird die «Recycle Bin» Funktion von Exchange genutzt, über welche der Benutzer 30 Tage zurück gelöschte Objekte wiederherstellen kann.

Office 365 von Microsoft beinhaltet kein Backup. META10 bietet optional dem Kunden den Service Cloud-Backup, mit welchem Office 365 Accounts gesichert werden können. Der Kunde muss diesen kostenpflichtigen Service aufgeschaltet haben, damit Office 365 Accounts gesichert werden.

6. SLA Version

Die aktuelle Version des SLA wird unter der URL www.meta10.com/sla zur Verfügung gestellt. Die SLA können durch META10 jederzeit angepasst werden.

META10 AG
Haldenstrasse 5
6340 Baar
phone: 041 500 11 00
email: info@meta10.com
web: www.meta10.com

7. AGB

Es gelten die AGB unter www.meta10.com/agb