A1 M365 Standard Managed Service

Servicebeschreibung

Erstellung:	02.06.2025
Änderung:	
Version:	1.0
Status:	Final

Inhalt

1. Allgemeines

Diese Servicebeschreibung erläutert die Nutzung von *A1 Microsoft 365 Standard Managed Service*, das Ihnen als Kunde über den A1 Marketplace angeboten und bereitgestellt wird. Sofern hier nicht Abweichendes geregelt wird, kommen die AGB-Solutions der A1 Telekom Austria AG (A1) zur Anwendung.

A1 Microsoft 365 Standard Managed Service bietet Kunden einen monatlich definierten Zugriff auf A1 Experten Know-How und Lösungskompetenz im Rahmen eines Managed Services für die Microsoft 365 (M365) Umgebung mit einem definierten Service Level Agreement. Zusätzlich wird der bestehende Tenant zu Beginn der Serviceerbringung in einem gemeinsamen Workshop mit A1 Experten auf Basis der Kundenanforderungen bzw. A1 Best Practices abgesichert.

Das Service richtet sich an Unternehmen mit mindestens einer Lizenz, welche ihren Tenant grundsätzlich selbst verwalten. Bei Bedarf können Sie gezielt Unterstützung durch einen Experten in Anspruch nehmen, ohne auf ihre Eigenständigkeit zu verzichten.

Folgende Leistungen sind im A1 M365 Standard Managed Service enthalten:

- A1 Security Best Practices Information
- Tenant-Absicherung
- Emergency Access Admin
- Definiertes Incident Management
- Microsoft Case Einmeldung, Nachverfolgung und Kommunikation

2. Voraussetzungen

- Bestehender oder neuer Microsoft 365 Tenant mit mindestens einer aktiven Lizenz
- Freigabe für die Betreuung des Microsoft 365 Tenants durch A1 Operation Experts (GDAP Relationship) – wird im Rahmen des Servicesetups überprüft und ggf. angefordert
- Kontaktperson mit Namen, E-Mail-Adresse und Telefonnummer als zuständigen Ansprechpartner auf Kundenseite
- Liste von Personen welche berechtigt sind, Supportanfragen einzumelden (Name, Telefonnummer, E-Mail-Adresse)

Zur Klarstellung wird festgehalten:

Microsoft Cloudservices (M365) sind nicht Teil dieses Services und liegen nicht in der Verantwortung von A1. A1 hat keinen Einfluss auf diese Services.

Es liegt in Ihrer Verantwortung, eingesetzte Hard- und Software auf aktuellem Stand zu halten. Lösungen auf Hard- und Software, deren Support nach der jeweiligen policy des Herstellers/Lieferanten beendet wurde, werden durch A1 nicht mehr unterstützt.

Bestehen Sie auf dem Einsatz solcher Hard- und Software, entfallen sämtliche Zusagen der A1 aus diesem Vertrag. Die Serviceerbringung erfolgt „best effort", allfällige Leistungsstörungen sind nicht von A1 zu verantworten.

A1 haftet nicht für eventuelle aus der unterlassenen Aktualisierung resultierende Nachteile oder Schäden.

Ergeben sich aus solcher Hard- und Software erhöhte Betriebsaufwände, sind diese nicht vom gegenständlichen Angebot umfasst. A1 würde in einem derartigen Fall Services gegen gesondertes Angebot und Entgelt erbringen.

Lizenzbereitstellung erforderliche Rechte

Die Lizenzbereitstellung ist nicht Gegenstand dieses Services.

Erforderliche Lizenzen können auf Basis eines gesonderten Vertrages von A1 über den A1 Market Place zu den dort genannten Bedingungen bezogen werden. A1 Marketplace ist ein Business Online Shop, der auf A1.net integriert ist.

Nach der Erstbestellung können Sie Ihre Marketplace Produkte in der A1 Marketplace Administration selbst verwalten und bei Bedarf weitere Produkte bestellen.

Falls die Beschaffung von Lizenzen direkt von Ihnen oder über einen Marktbegleiter erfolgt, liegt die Provisionierung von Lizenzen und Subscriptions in Ihrem alleinigen Verantwortungsbereich.

3. Leistungen im Rahmen von A1 M365 Standard Managed Service

Die Nutzung von Microsoft 365 Services ermöglicht ein mobiles Arbeiten nach modernsten Sicherheitsstandards. Diese Services sind jedoch für eine breite Masse an Kunden und eher auf Kompatibilität vorkonfiguriert. Um dieses Software-As-A-Service (kurz SaaS) optimal und vor allem sicher einzusetzen, benötigt es Expertise.
Das A1 M365 Standard Managed Service bietet eine individuelle Anpassung auf die Bedürfnisse der Kunden mit optimierten Sicherheitseinstellungen und Unterstützung durch A1 Experten.
Im Folgenden werden die Bestandteile des Service beschrieben.

3.1. A1 Security Best Practices Information

Der Kunde erhält ein Dokument mit allgemeinen Sicherheitsempfehlungen zur Absicherung seiner M365 Umgebung (A1 Security Tipps für die Tenantabsicherung). Anhand dieses Dokuments kann der Kunde selbst die Maßnahmen umsetzen oder diese durch A1 umsetzen lassen.

3.2. Tenant Setup Service (Tenantabsicherung)

Zu Beginn der Serviceerbringung werden die Tenant Konfigurationen mit dem Kunden abgestimmt, um sicherzustellen, dass die Konfiguration auf die Kundenanforderungen abgestimmt und nach A1 Best Practices erfolgt ist. Dabei spielt es keine Rolle, ob es sich um einen neuen oder bereits vorhandenen Tenant handelt.

- Berechtigungsstruktur für A1 Support
  Zugriff für A1 Administratoren sollte über das Microsoft Cloud Solution Provider (CSP) Portal erfolgen und ebendort werden auch die Rollen über GDAP zugewiesen. Falls das nicht möglich ist (z.B. Kunde ist aus technischen Gründen nicht im CSP Portal), dann sind im Tenant bzw. EntraID entsprechende Gruppen anzulegen (Vorschlag: oA1-<Service>-Admins, oA1-Exchange-Admins). Über diese Gruppen werden die jeweiligen Admin-User und Rollen (bevorzugt: wenn Lizenzen vorhanden, Nutzung von Privileged Identity Management) vergeben.

- Organisation Wide Settings
  Im M365 Admin Portal können grundlegende und organisationsweite Einstellungen für diverse Features und Applikationen geändert werden. Die Konfigurationsmöglichkeiten in diesem Portal sind eingeschränkt und beinhalten oft nur die Möglichkeit eine Funktion ein- oder auszuschalten.

- Konfiguration der *Enterprise Collaboration* Settings, weitere Einstellungen werden im Arbeitschritt *„Tenant hardening*" durchgeführt

- Tenant hardening
  Eine Reihe an Einstellungen, die grundlegende Tenantsicherheit betreffen, werden gemäß A1 Best Practices gesetzt. Beispielsweise Password Reset Policy, Application Registrations, Tenant Creation und andere.

- Enterprise Applications
  Jede Anwendung, die auf Cloud Services zugreifen möchte, muss zuvor registriert und zugelassen werden.

- License Administration
  Um Cloud Services nutzen zu können, müssen je nach gewünschter Funktionalität und Ausprägung Lizenzen beschafft werden. Diese Lizenzen werden den Mitarbeitern direkt oder auf Basis einer Gruppenmitgliedschaft (empfohlen) zugewiesen. Initiales Einrichten von Gruppen für die verwendeten Microsoft 365 Lizenzen.

- Public Domain Administration
  Öffentliche Domains, welche in der Cloud verwendet werden sollen, müssen zuerst dem Tenant hinzugefügt werden. Je nach aktivierten und verwendeten Services sind DNS-Einträge und andere Anpassungen in der öffentlichen DNS-Verwaltung des Kunden nötig. Einrichtung der beim Kunden bestehenden Domains.

- Microsoft 365 Archive
  Konfiguration von Microsoft 365 Archive, wenn die Voraussetzungen vom Kunden erfüllt werden (Subscription, Billing, …).

- Tenant-Settings Abzug
  Abzug der Tenant Settings zu Dokumentationszwecken.

- Accountübergabe an den Kunden
  Übergabe von bis zu 5 administrativen Accounts mit den vom Kunden vorgegebenen benötigten Rechten laut Microsoft Standardrollen.

3.3. Emergency Access Admin

Sperrt sich der Kunde irrtümlich aus seinem Tenant aus oder verliert/vergisst sein Admin Passwort, kann A1 ihn mit Hilfe eines eigenen (Global) Admin Accounts wieder berechtigen. Im Normalfall wird hierfür der CSP Benutzer herangezogen. Das funktioniert nur, wenn der Kunde eine Verwaltung seines Tenants über den CSP Tenant bestätigt und ein A1 Experte Zugriff auf den Tenant hat. Sperrt der Kunde den CSP Account aus oder widerruft die GDAP Bestätigung für den CSP Tenant, so hat A1 auch im Notfall keinen Zugriff auf den Kundentenant und kann damit nicht unterstützen.

3.4. Definiertes Incident Management

A1 M365 Standard Managed Service umfasst Plattform Support für folgende Komponenten der Microsoft 365 Umgebung:

- Tenant, Security & Identity
- SharePoint Online & OneDrive
- Exchange Online
- Power Platform (Power Apps, Power Automate, Power BI)
- Microsoft Teams
- Intune (für Windows, iOS, Android)
- Defender for Endpoint (für Windows Client OS) – Remote Unterstützung bei Konfigurationsthemen, kein remote/lokaler Client Support

Für die oben gelisteten Komponenten ist monatlich die Einmeldung von bis zu 4 Plattform Fehlern als Incident bei A1 inkludiert die im Rahmen des Service Level Agreements behoben werden. Der Referenzzeitraum beträgt dabei 6 Monate, d.h. es sind bis zu 24 Incidents pro Halbjahr inkludiert, Durchrechnungszeitraum immer Jänner-Juni; Juli-Dezember.

Wenn das Limit erreicht ist, werden nachfolgende Incidents kostenpflichtig auf Basis Best Effort abgearbeitet. Etwaige Requests, die der Kunde einmeldet, werden kostenpflichtig auf Basis Best Effort abgearbeitet.

Beschreibung Incident und Einmeldung

Stößt der Kunde auf ein Fehlverhalten in der Microsoft 365 Plattform und ist dieses Fehlverhalten nicht auf Drittanbieterkomponenten zurückzuführen, so kann er diesen Fehler als Incident bei A1 einmelden.

Bei der Einmeldung eines Incidents sind seitens Kunden verpflichtend folgende Informationen anzugeben

1. Microsoft Fehler ID (Diese wird bei Microsoft 365 Plattform Fehlern angezeigt) falls vorhanden
2. Microsoft Fehlerbeschreibung (Diese wird bei Microsoft 365 Plattform Fehlern angezeigt) oder eine Erklärung des Fehlerbilds
3. Beschreibung (inkl. Screenshots) mit folgenden Informationen, sodass eine Nachstellung des Fehlers möglich ist
    - Für die Nachstellung benötigte URLs
    - Für die Nachstellung benötigte Eingabeinformationen
    - Welche Aktionen wurden zuvor gesetzt
    - Bei welcher Aktion trat der Fehler auf
    - Was hätte gemäß Erwartung passieren sollen
    - Wann wurde der Fehler zum ersten Mal bemerkt (bzw. bis wann trat er sicher nicht auf)

Die Einmeldung des Incidents erfolgt:

- Per E-Mail an tech.business-service@a1.net
- Per Telefon unter 0800 664 410

3.5. Microsoft Case Einmeldung

Für Fehler, die direkt im Bereich der Plattform von Microsoft 365 liegen und nicht durch A1 behoben werden können, übernimmt A1 das Microsoft Case Management inkl. Nachverfolgung und Kommunikation. Sollte zur Behebung des eingemeldeten Incidents ein Microsoft Case erforderlich sein, wird der vereinbarte SLA unterbrochen.

4. Service Level Agreement

Der Servicegrad für die Serviceleistung ist in der Beilage Service Level Agreement (SLA) A1 Managed Cloud Service definiert.

Service Desk
Zur Aufrechterhaltung eines störungsfreien Betriebs hat A1 geeignete Prozesse des IT Service Managements nach dem Rahmenwerk von ITIL (IT Infrastructure Library) implementiert. Auftretende Störungen (Incidents) werden erfasst, verfolgt und einer Lösung zugeführt. Ebenso werden mit diesen Prozessen von Ihnen gemeldete Anträge auf Systemänderungen (Change Requests) abgewickelt.

Der Service Desk von A1 nimmt hier, als zentraler Zugang (Single Point of Contact) für Ihren IT-Administrator, eine wesentliche Rolle zur Entgegennahme und Bearbeitung von Störungen ein.

Die Erreichbarkeit ist gegeben unter:
- Rufnummer: 0800 664 410
- E-Mail-Adresse: tech.business-service@a1.net

Service Level Agreement

Fehlerbehebung

Service Level	Fehlerkategorie	Servicezeit	Reaktionszeit	Lösungszeit
5x9/8h	Kritische Fehler	Mo-Fr, 8-17 Uhr, werktags	2h	8h
	Hauptfehler		nächster Werktag	nächster Werktag
	Nebenfehler		nächster Werktag	5 Werktage

Die Verfügbarkeit der Microsoft Cloudservices (Microsoft 365) liegt im Verantwortungsbereich von Microsoft. Es gelten die Vereinbarungen, welche direkt zwischen Kunden und Microsoft abgeschlossen wurden. A1 hat keinen Einfluss auf diese Verfügbarkeit.

5. RACI-Matrix

Serviceverantwortlichkeiten

Tätigkeit \ Verantwortungsbereich	Kunde	A1	Nicht inkludiert (=Zusatz-kosten)
Setup			
M365 – A1 Best Practices Info	I	R	
Basisabsicherung			
Abstimmung der Tenantabsicherung	I/C/A	R	
Ausrollen der Basisabsicherung/Tenant Setup	I	R	
Incidents			
Qualifizierte Einmeldung eines Incidents	R	I	
Lösung eines Incidents	I/C	R	
Microsoft Case Management	I/C	R	

R – Responsible, A – Accountable, C – Consulted, I – Informed

6. Begriffsdefinition

6.1. Best Effort

Eine Umsetzung nach Best Effort erfolgt nach besten Bemühungen seitens A1 jedoch ohne zugesichertes Service Level Agreement.

6.1. Microsoft Case

Kann ein Fehler von A1 nicht behoben werden, weil es sich um einen Fehler in der Microsoft 365 Plattform handelt, so muss dieses Fehlverhalten bei Microsoft als sogenannter „Case" eingemeldet werden. Über eine Case-Nummer erfolgt eine transparente Dokumentation eines Case bei Microsoft von der Eröffnung bis zum Abschluss.

6.2. Request

Bei einem Request handelt es sich um einen Auftrag seitens Kunden an A1 (Im Gegensatz zu einem Incident). Im Rahmen von A1 M365 Standard Managed Service sind Requests kostenpflichtig. Dabei muss seitens Kunden immer folgende Information angegeben werden

- Ansprechpartner
- Anforderungsbeschreibung

6.3. Tenant

Um Cloud-Dienste bereitstellen zu können, muss ein Tenant erstellt werden. Für die Erstellung sind einige Angaben wie Kontaktperson, Firmenname etc. erforderlich. Zusätzlich ist auch ein Domänenname festzulegen, welcher im Nachhinein nicht mehr geändert werden kann.

Microsoft selbst vergleicht einen Microsoft 365 Tenant beispielsweise mit einer Wohnung, die in einem Haus gemietet wird, wo der Mieter beispielsweise bestimmt, was hineinkommt und wer Zugriff erhält, etc. nur, dass ein M365 Tenant keinem fixen physischen Server zugeordnet ist.

Das Wort Tenant kann auf Deutsch wahrscheinlich am besten mit dem Wort „Mandant" übersetzt werden. Innerhalb eines Tenants werden also alle Apps, Benutzer, Lizenzen und Inhalte (Daten) für diesen Mandanten verwaltet.

6.1. Microsoft 365 (M365)

Microsoft 365 ist die cloudbasierte Produktivitätsplattform von Microsoft. Sie umfasst beispielsweise Module wie Microsoft Teams, Exchange Online, SharePoint Online, OneDrive, Power Platform.

6.1. Incidentmanagement

Beim Incident Management geht es um die schnellstmögliche Wiederherstellung des normalen Servicebetriebs und die Minimierung der negativen Auswirkungen auf den Geschäftsbetrieb. Das Incident Management umfasst die Entgegennahme von Incidents, das Routing an die entsprechenden Experts und die Behebung des Fehlers (inkl. Eröffnung eines Microsoft Cases im Bedarfsfall) im Rahmen des definierten Service Level Agreements sowie die Kundenkommunikation im Rahmen der Lösung.