



# 360° IT Service

Server Datensicherung Client **Mobile** IT-Struktur

Wartungskonzepte von Schneider + Wulf

**Leistungsbeschreibung 360° IT Service Modul Mobile**

## Vorbemerkung

Wenn im Folgenden die Worte 'mobile Geräte' genutzt werden, sind hiermit Smartphones oder Tablets auf Basis von iOS, Android und Windows Phone gemeint.

Die Leistungsbeschreibung behandelt ausschließlich Firmengeräte, private Geräte sind ausgeschlossen.

Die Mindest-Vertragslaufzeit beträgt 36 Monate.

Falls bei einzelnen Leistungen Managed Service-Leistungen von Dritten genutzt werden sollten, so sichert der Auftragnehmer zu, dass diese Services in der Bundesrepublik Deutschland gehostet sind.

## Voraussetzungen

Die zuverlässige, sichere und kostengünstige Betreuung der mobilen Geräte innerhalb dieses Betreuungskonzeptes basiert auf bestimmten Voraussetzungen der IT-Infrastruktur beim Kunden. Dies umfasst:

- Die mobilen Geräte müssen über eine dauerhafte Internet-Verbindung verfügen
- Für Punkt **m05 COD Standard** | Einsatz von Exchange Online, Office 365 oder Exchange Server 2013 CU3 und höher
- Für den Punkt **m05 COD Premium** | Einsatz mobiles Gerät: Android ab V4.2, iOS ab V8 | Einsatz Server: Exchange Server 2010 oder höher

## Gültigkeit Service-Bedingungen

Nachrangig zu den Regelungen dieser Leistungsbeschreibung gelten die Service-Bedingungen in der jeweils aktuellen Version, abrufbar unter

<https://share.schneider-wulf.de/index.php/s/bHCG1SWddYwFBZz> Kennwort: 12M\$!%&82IT

Außerdem gelten nachrangig für die eingesetzten Software-Produkte die Lizenz- und Nutzungsbedingungen der jeweiligen Hersteller.

Weiterhin gelten nachrangig die allgemeinen Geschäftsbedingungen, jederzeit abrufbar unter

<https://share.schneider-wulf.de/index.php/s/bHCG1SWddYwFBZz> Kennwort: 12M\$!%&82IT

## Disclaimer

Unsere Angebote, bereitgestellte Dokumente sowie Mitteilungen sind ausschließlich für Sie bestimmt und müssen vertraulich behandelt werden. Die Weitergabe sowie Vervielfältigung unserer Unterlagen sowie die Verwertung und Mitteilung ihres Inhaltes an Dritte ist nicht gestattet, soweit dieses von uns nicht schriftlich freigegeben worden ist. Zuwiderhandlungen verpflichten zu Schadensersatz.

## Leistungsbeschreibung 360° IT Service Modul Mobile

### m01 Web-Zugriff auf mobile Geräteverwaltung inklusive Zugriff auf Berichte

Dem Kunden wird ein Zugang auf die Verwaltungskonsole zur Verfügung gestellt. Der Kunde kann über den Zugang lesenden Zugriff auf eine Übersicht seiner mobilen Geräte nehmen sowie auf Inventarisierungsberichte zugreifen.

### m02 Geräte-Inventarisierung

Tägliche automatische Aktualisierung der Auflistung der installierten Hardware- und Software-Komponenten der Clients in der vom Auftragnehmer für den Kunden bereitgehaltenen Verwaltungskonsole. Für die vorgenannte Funktionalität werden je nach Betriebssystem des mobilen Gerätes bis zu zwei Applikationen auf dem mobilen Gerät installiert, die eine Internet-Verbindung benötigen.

Sofern das mobile Gerät die folgenden Daten zum Abruf bereitstellt, werden diese Daten in der Verwaltungskonsole bereitgestellt:

- **Standard-Paket** | Gerätetyp, Hersteller, Version Betriebssystem, IMEI-Nummer, Seriennummer, Gesamtspeicher, Aktuell genutztes Mobilfunknetzwerk, Status Daten-Roaming, Wi-Fi MAC-Adresse
- Zusätzlich bei **Premium-Paket** | Modell, Letztes Betriebssystem-Update, UDID, Verfügbarer Speicher, Mobilfunkvertragspartner

### m03 Fernwartungsmöglichkeit nach Benutzerfreigabe

Die Fernwartungsfunktion ermöglicht einen Zugriff auf den Bildschirm des mobilen Geräts in folgender Art und Weise:

- Android-basierte mobile Geräte | Bildschirmübertragung und -steuerung
- iOS-basierte mobile Geräte | Übertragung von benutzergenerierten Screenshots
- Windows Phone-basierte mobile Geräte | Keine Übertragung möglich

Die Fernwartungsfunktion wird durch den Techniker des Auftragnehmers zum mobilen Gerät durchgeführt. Möchte der Kunde selbst Fernwartungen auf den mobilen Geräten seiner Mitarbeiter durchführen, so fällt ein Aufpreis von 30,00 € monatlich an.

Die Fernwartungs-Software unterstützt die zeitnahe Problemanalyse und -lösung durch Techniker des Auftragnehmers aus der Ferne über eine nach dem üblichen Standard gesicherte Internet-Verbindung. Der Auftragnehmer versichert, diesen Zugang mit hoher Sorgfalt zu verwalten und versichert weiterhin, sämtliche in Kontakt mit den Systemen des Kunden kommenden Mitarbeiter im Hinblick auf die Einhaltung des Bundesdatenschutzgesetzes BDSG zu verpflichten.

Der Nutzer, der Support erhalten möchte, startet die Fernwartungs-App und erhält vom Support-Techniker einen einmaligen Sitzungs-Code, den er in die App eingibt. Im Anschluss erhält der Support-Techniker einen Zugriff auf den Bildschirm des Nutzers.

Die benötigten Lizenzen zur Nutzung der Fernwartungs-Software auf den mobilen Geräten sind enthalten.

## **m04** Auto Config für WLAN

Der Kunde übergibt die WLAN-Zugangsdaten an den Auftragnehmer, der sie dann für den Kunden im Verwaltungssystem hinterlegt. Folgende WLAN-Verschlüsselungstypen werden unterstützt:

- **Standard-Paket** | Android und iOS: WEP, WPA | Windows: WEP, WPA, WPA2
- **Premium-Paket** | Android: WEP, WPA | iOS: WEP, WPA, WPA2 | Windows: WPA, WPA2

Bei Buchung des Premium-Pakets kann der Kunde die vom Auftragnehmer bereitgestellte Verwaltungskonsole nutzen, um selbst die WLAN-Konfigurationen für seine mobilen Geräte vorzudefinieren.

## **m05** Container-Lösung für Mail, Kontakte, Kalender (Trennung privater und geschäftlicher Daten)

### **Standard-Paket**

Bereitstellung einer von Microsoft angebotenen OWA App. Die geschäftlichen Daten in Form von Mails, Kontakten und Kalendereinträgen werden über die OWA App bereitgestellt. Dadurch werden sie nicht über den Smartphone-integrierten Mail Client zugänglich gemacht, sodass Dritt-Applikationen auf die geschäftlichen Daten keinen Zugriff nehmen können. Das bedeutet weiterhin, dass keine konsolidierte Sicht auf privaten und geschäftlichen Terminkalender möglich ist.

Es erfolgt eine Zwischenspeicherung von vorher definierten Ordnern. Die zwischengespeicherten Objekte der App sind nicht verschlüsselt gespeichert. Es gilt die Nutzungsvereinbarung von Microsoft für die OWA App.

### **Premium-Paket**

Bereitstellung einer verschlüsselten Container-Lösung für die mobilen Geräte. Das bedeutet, dass Firmendaten in Form von Mails, Kontakten und Kalendereinträgen über eine spezielle App abrufbar sind und nicht über den Smartphone-integrierten Mail Client zugänglich sind. Dadurch werden sie nicht über den Smartphone-integrierten Mail Client zugänglich gemacht, sodass Dritt-Applikationen auf die geschäftlichen Daten keinen Zugriff nehmen können. Das bedeutet weiterhin, dass keine konsolidierte Sicht auf privaten und geschäftlichen Terminkalender möglich ist.

Es erfolgt eine Zwischenspeicherung der synchronisierten Elemente. Die zwischengespeicherten Objekte der App sind verschlüsselt gespeichert. Es gilt die Nutzungsvereinbarung des App-Herstellers.

## m06 Sperr-Service für Remote-Sperrung und -Löschung des mobilen Gerätes

Bereitstellung einer telefonischen Hotline sowie einer Mail-Adresse zur Mitteilung eines Sperr- oder Löschauftrags. Dieser Auftrag wird spätestens innerhalb eines Werktages durchgeführt. Der Auftrag wird mit hoher Dringlichkeit priorisiert abgearbeitet. Der Sperr- oder Löschbefehl wird an das mobile Gerät abgesendet. Um den Befehl umzusetzen, benötigt das mobile Gerät eine Internet-Verbindung und ausreichenden Akkuladestand. Der Vorgang kann nicht mehr rückgängig gemacht werden.

Bei Buchung des Standard-Paketes wird eine Gebühr von 30,00 € pro Auftrag an den Kunden verrechnet.

Bei Buchung des Premium-Paketes kann der Kunde die vom Auftragnehmer bereitgestellte Verwaltungskonsole nutzen, um den Sperr- oder Löschbefehl selbst abzusetzen.

## m07 App-Inventarisierung

Bereitstellung eines über das Internet zugänglichen Verwaltungssystems, in dem die installierten Software-Programme der mobilen Geräte dargestellt werden.

- **Standard-Paket** | App-Name und App-Versionsnummer werden pro mobilem Gerät dargestellt
- Zusätzlich bei **Premium-Paket** | Anwendungs- und Datengröße der einzelnen Apps

## m08 Automatische Überwachung der Einhaltung von App-Richtlinien

Auf Basis einer vom Kunden zu stellenden Applikationsliste (Blacklist) wird alle 30 Minuten automatisch geprüft, ob eine Applikation auf einem mobilen Gerät installiert ist, welche auf der Blacklist steht, also gegen die internen Nutzungsrichtlinien verstößt.

## m09 Alarmierung bei Regelverstoß gegen App-Richtlinien

Bei einem Ereignis gemäß Punkt **m08** erfolgt eine Alarmierung per Mail an den Benutzer. Zusätzlich erfolgt eine Alarmierung an eine pro Richtlinie definierbare Mail-Adresse (beispielsweise IT-Beauftragter oder Vorgesetzter) und/oder an eine pro Richtlinie definierbare SMS-Mobilfunknummer.

## m10 Antivirus-Lizenz

Es erfolgt die Bereitstellung einer Antivirus-Lizenz für mobile Geräte mit dem Betriebssystem Android. Der Antivirus-Schutz beinhaltet einen Echtzeit-Scanner, geplante Geräte-Scans sowie regelmäßige Signatur-Updates. Ein 100%iger Anti-Virus-Schutz ist nicht möglich. Der Auftragnehmer wird nach den üblichen Standards Maßnahmen zum Schutz der mobilen Geräte beim Kunden durchführen.

## **m11** Einstellung für gefilterte Web-Suche

Der Auftragnehmer bietet dem Kunden im Rahmen der Einrichtung gemäß Punkt **m13** an, die Suchmaschine Google im mobilen Browser zu konfigurieren um nur noch gefilterte Suchergebnisse zu erhalten. SafeSearch ist eine Filtertechnik, die beispielsweise Websites mit pornographischem oder gewaltverherrlichendem Inhalt aus den Ergebnissen der Suche ausschließt.

## **m12** Bereitstellung eines firmeneigenen App Store

Dem Kunden wird ein Firmen-eigener App-Katalog pro Betriebssystem (iOS, Android, Windows) bereitgestellt. Die Applikationen, die im Katalog für die Benutzer sichtbar sind, können pro Gruppe oder Abteilung definiert werden.

Zusätzlich können kundeneigene Applikationen in die Verwaltungskonsole integriert und über den App-Katalog auf die einzelnen mobilen Geräte verteilt werden - hierbei wird dann kein öffentlicher App Store genutzt.

## **m13** Einrichtungsgebühr pro Gerät

Nachdem die Voraussetzungen wie auf Seite 1 dieses Dokuments beschrieben erfüllt sind, werden die mobilen Geräte durch den Auftragnehmer mit den notwendigen Applikationen und Richtlinien versehen und konfiguriert. Dazu wird der Kunde die Geräte an einem Standort zentral bereitstellen.

## **m14** Stundensatz für weitere Leistungen

Stundensätze, Fahrtkosten und etwaige Zuschläge für Leistungen außerhalb des Service-Zeitraums Montag bis Freitag zwischen 08:00 und 17:00 Uhr ergeben sich aus der jeweils aktuellen Dienstleistungspreisliste. Diese ist abrufbar unter

<https://share.schneider-wulf.de/index.php/s/bHCG1SWddYwFBZz> Kennwort: 12M\$!%&82IT

## Firmenprofil Schneider & Wulf EDV-Beratung

Messbar herausragender Service seit 1988 - störungsfreie und leistungsstarke IT-Lösungen. Jährlich erarbeiten wir in mehr als 300 Kundenprojekten und weit über 5.000 Supports für aktuell 1.700 KMU mit 20 bis 250 PC-Arbeitsplätzen zukunftssichere IT-Infrastrukturen, die einfach funktionieren.

Mit Standorten in Frankfurt am Main und im hessischen Babenhausen operieren wir im Rhein-Main-Gebiet, aber auch deutschland- und europaweit am Markt.

Unsere Erfahrung spiegelt sich in unserer Ausrichtung wieder: Wir sind immer für unsere Kunden da - so unbürokratisch wie möglich, dabei jedoch immer aufmerksam, strukturiert und absolut professionell - bei 100%iger Kostentransparenz.

Um störungsfreie und leistungsstarke IT-Lösungen zu gewährleisten, arbeiten wir präventiv statt reaktiv. Das bedeutet: Wir vermeiden und beheben Störungen, bevor sie zum Problem werden.

Adressiert werden inhabergeführte KMU, deren Entscheider verstanden haben, dass IT kein notwendiges Übel, sondern ein wichtiger Baustein erfolgreicher Unternehmensplanung ist.

## Kontakt

Schneider & Wulf EDV-Beratung GmbH & Co KG  
Im Riemen 17 | 64832 Babenhausen  
[www.schneider-wulf.de](http://www.schneider-wulf.de) | [info@schneider-wulf.de](mailto:info@schneider-wulf.de)  
Fon +49 6073 6001-0 | Fax +49 6073 6001-99