



ALLGEMEINE LIEFER- UND LEISTUNGSBEDINGUNGEN

ifa Managed Security

Allgemeine Liefer- und Leistungsbedingungen

ifa Managed Security (iMS)

Versionierung

Version	Datum	Inhalt	Person/Gremium
1.0	17.06.2020	Geltungsdatum / Veröffentlichung	ifa systems AG
1.1	13.07.2020	Anpassung Managed Backup und Managed Endpoint Zeiten	MBA

Allgemeine Liefer- und Leistungsbedingungen

ifa Managed Security (iMS)

Inhalt

Versionierung.....	1
1. ifa Managed Security (iMS).....	3
1.1. Übersicht iMS.....	3
1.2. iMS Module.....	3
2. Allgemeines.....	4
2.1. Geltungsbereich.....	4
2.2. Änderungen der allgemeinen Liefer- und Leistungsbedingungen.....	4
3. iMS Managed Endpoint.....	5
3.1. Leistungen.....	5
3.2. Mengestufen und -staffeln.....	6
4. iMS Managed Firewall.....	7
4.1. Leistungen.....	7
4.2. Mengestufen und -staffeln.....	8
5.1. Leistungen.....	8
5.2. Mengestufen und -staffeln.....	10
6. Vertragslaufzeiten und Kündigungsfristen.....	10
6.1. Vertragslaufzeiten.....	10
6.2. Vertragsverlängerung.....	10
6.3. Kündigung.....	10
7. Gebühren und Preise.....	11
7.1. iMS-Preise.....	11
7.2. Zahlungsmodalitäten.....	11
7.3. Sonstige Gebühren.....	11
8. Mitwirkungspflichten des Kunden.....	11
9. Leistungsbeschränkungen.....	12
10. Haftung.....	13
11. Vertraulichkeit.....	13
12. Datenschutz.....	14
13. Allgemeine Bestimmungen.....	14
Anhang 1 – Aufstellung der Überwachungswerte.....	15
Anhang 2 – Third-Party-Patchmanagement.....	16

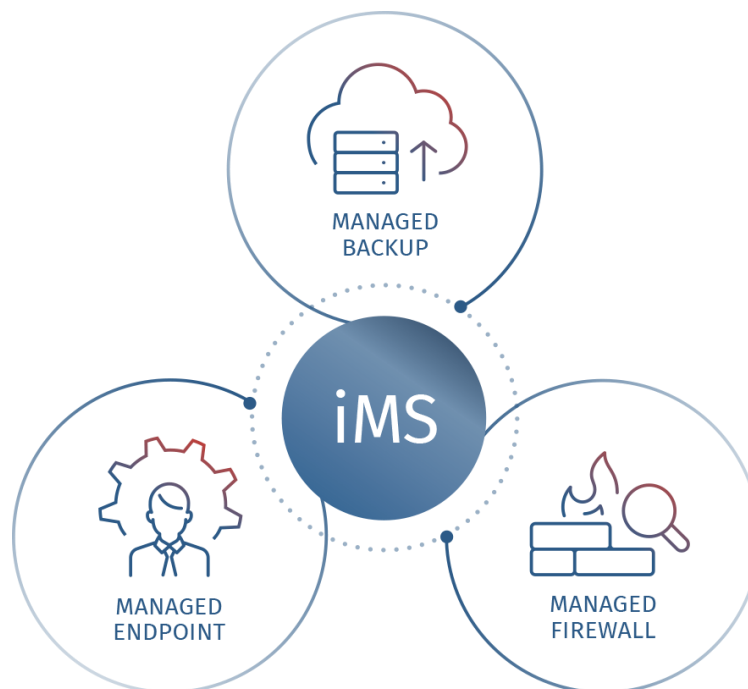
Allgemeine Liefer- und Leistungsbedingungen

ifa Managed Security (iMS)

1. ifa Managed Security (iMS)

1.1. Übersicht iMS

ifa Managed Security ist ein Paket aus intelligenten Sicherheitslösungen und Dienstleistungen für Ihre IT-Infrastruktur, das sich aus drei Modulen zusammensetzt:



1.2. iMS Module

- i. **iMS Managed Endpoint**
iMS Managed Endpoint bietet die Leistungs- und Sicherheitsüberwachung Ihrer IT-Infrastruktur wie Server, Workstations oder Netzwerkgeräte durch erfahrene ifa-Techniker. iMS Managed Endpoint bietet kontinuierliche und professionelle Überwachung, Pflege und Wartung Ihrer Server und Workstations in Verbindung mit intelligenten „self-healing“-Regeln. Automatisierte Störungsmeldungen bei kritischen & sicherheitsrelevanten Vorfällen direkt an unsere Mitarbeiter beschleunigen die Lösungsfindung und reduzieren Arbeitszeitverluste.
- ii. **iMS Managed Firewall**
iMS Managed Firewall liefert Ihnen hochwertige Firewall-Lösungen inklusive Einrichtung, Verwaltung und Monitoring durch geschulte ifa-Mitarbeiter. Die Firewalls bieten mehr Transparenz über risikoreiche Aktivitäten, verdächtigen Datenverkehr und komplexe Bedrohungen in Ihrem Netzwerk. Leistungsstarke Next-Gen-Schutztechnologien wie „Deep Learning“ und „Intrusion Prevention“ schützen Ihr Netzwerk auch vor neuen und unbekanntem Bedrohungen. Auch ein Webfilter gegen gefährliche und ungewollte Downloads ist Teil des Lieferumfangs sowie ein leistungsfähiges VPN-Gateway für sichere Remote-Arbeitsplätze oder Homeoffice-Szenarien.

Allgemeine Liefer- und Leistungsbedingungen

ifa Managed Security (iMS)

iii. **iMS Managed Backup**

iMS Managed Backup ist eine hybride Backup-Lösung mit einem lokalen Backup-Speicher in Ihrer Praxis oder Klinik und Langzeitarchivierung von Quartalssicherungen in der Cloud. Der lokale Speicher ermöglicht die schnelle Sicherung und Wiederherstellung von Daten des letzten Monats, unabhängig von der Cloud und dem Internet. Die Langzeitarchivierung in der Cloud ist kostengünstig und skaliert unendlich ohne Bänderwechsel. Der Backup-Zustand wird durch unsere Mitarbeiter überwacht und Probleme können frühzeitig und schnell gelöst werden. Alle Backups werden vollständig in der Praxis verschlüsselt und eine starke Segmentierung bietet hohen Schutz vor Crypto-Trojanern.

2. Allgemeines

2.1. Geltungsbereich

Diese allgemeinen Liefer- und Leistungsbedingungen („ALB“) gelten für alle zwischen dem Kunden und der ifa systems AG abgeschlossenen Verträge über „ifa Managed Security“-Dienstleistungen („iMS“) und ggfs. Software und Hardware im Zusammenhang mit diesen Dienstleistungen.

Der Vertrag kommt durch rechtsverbindliche Signatur eines Angebots durch den Kunden in Verbindung mit einer Auftragsbestätigung oder der Leistungserbringung durch die ifa systems AG zustande. Maßgeblich für den Umfang der Leistungserbringung sind die im Angebot bzw. der Auftragsbestätigung zwischen den Parteien festgelegten Leistungsbestandteile. Individuelle Dienstleistungsverträge mit ergänzenden oder abweichenden Bedingungen haben Vorrang vor diesen allgemeinen Bedingungen.

Entgegenstehende oder von diesen Geschäftsbedingungen abweichende Geschäftsbedingungen des Kunden werden nicht Vertragsbestandteil, auch wenn die ifa systems AG diesen nicht ausdrücklich widerspricht. Dies gilt auch dann, wenn die ifa systems AG Leistungen an den Kunden in Kenntnis entgegenstehender oder abweichender Bedingungen vorbehaltlos erbringt oder in Einzelkorrespondenz auf solche Bedingungen verwiesen wird.

2.2. Änderungen der allgemeinen Liefer- und Leistungsbedingungen

Es gelten jeweils die ALB in ihrer bei Beauftragung durch den Kunden unter www.ifasystems.de/agb abrufbaren Fassung. Änderungen der ALB werden schriftlich, in der Regel per E-Mail, mitgeteilt. Wird der Änderung nicht binnen 3 Wochen schriftlich widersprochen, gelten die Änderungen als anerkannt.

3. iMS Managed Endpoint

3.1. Leistungen

Im Rahmen von Managed Endpoint stellt ifa die Verwaltung von **Monitoring, Patchmanagement und Antivirus** der im Vertrag enthaltenen Systeme und Geräte. Um dies zu gewährleisten, werden Software-Agents von Solarwinds MSP auf den Geräten installiert. Die Verwaltung umfasst folgende Bereiche:

- **Überwachung** aller relevanten Werte von Windows-, Mac-, Linux- und Netzwerkgeräten: - Basis für alle weiteren Leistungen innerhalb des iMS Managed Endpoint Moduls:
 - Laufendes Monitoring der betreuten Systeme und Alarmierung bei auftretenden Problemen - vgl. Anhang 1 zur Aufstellung der Überwachungswerte
 - Analyse von Störungsmeldungen und Aufbereitung als Info für den Kunden
 - Inventarisierung der überwachten Systeme

- **Patchverwaltung** zur Aktualisierung der betreuten Systeme und Anwendungen, inklusive automatisiertem Rollout und Neustart.
 - Das Patchmanagement beinhaltet Betriebssysteme und Standardsoftware inklusive der gängigen Drittanbietersoftware nach dem Standard der ifa systems AG; vgl. Anhang 2 für eine Auflistung der im Third-Party-Patchmanagement unterstützten Produkte und Hersteller.
 - Die Patches werden je nach Klassifizierung freigegeben und installiert. Es werden folgende Klassifizierungen unterschieden:
 - Kritisch: Definition Updates
 - Hoch: Critical Updates, Security Updates
 - Medium: Service Packs, Third-Party-Patches, Update Rollups, Updates, Upgrades
 - Niedrig: Anwendungen, Treiber, Feature Packs, Tools

 - Die Freigabe der Patches erfolgt nach Wichtigkeit der Klassifizierungen:
 - Kritisch: werden sofort freigegeben und installiert
 - Hoch: werden sofort freigegeben und während des nächsten Wartungsfensters installiert
 - Medium: werden nach 7 Tagen freigegeben und innerhalb des nächsten Wartungsfensters installiert
 - Niedrig: werden bei Workstations sofort freigegeben und während des nächsten Wartungsfensters installiert. Bei Servern werden Patches nicht automatisch und nur bei Bedarf installiert.

 - Die Installation der Patches erfolgt innerhalb der definierten Wartungsfenster:
 - Bei Workstations:
 - Wartungsfenster 1: Kritische und wichtige Patches werden täglich, außer mittwochs, jeweils um 10:00 und 16:00 Uhr installiert. Das Wartungsfenster ist 60 Minuten lang.

Allgemeine Liefer- und Leistungsbedingungen

ifa Managed Security (iMS)

- Wartungsfenster 2: Kritische und wichtige Patches werden mittwochs um 02:00 Uhr installiert. Das Wartungsfenster ist 60 Minuten lang.
- Wartungsfenster 3: Alle anderen Patches werden täglich um 13:00 und 17:00 Uhr installiert. Das Wartungsfenster ist jeweils 60 Minuten lang.
- Bei Servern werden wöchentlich alle freigegebenen Patches installiert. Das Wartungsfenster ist 180 Minuten lang und beginnt um 02:00.
- Automatisierte Neustarts:
 - Bei Workstations erhält der Nutzer eine Benachrichtigung, falls ein Neustart notwendig ist. Alle Workstations werden planmäßig donnerstags um 03:00 Uhr neu gestartet, falls der Neustart durch den Nutzer nicht erfolgt ist und das Betriebssystem einen Neustart zum Abschluss des Patchvorgangs benötigt.
 - Bei Windows-Servern erfolgt der Neustart bis zu einmal wöchentlich, sofern das Betriebssystem dies zum Abschluss der Installation benötigt.
- **Antivirus-Software** wird installiert, regelmäßig aktualisiert und überwacht:
 - Bei Windows-Clients:
 - Integrierter Viren- und Webschutz mit Signatur- und Verhaltensanalyse, Anti-Phishing-Filter auf Basis von Bitdefender
 - Bis zu stündlicher Aktualisierung der Virensignaturen,
 - automatisierte Aktualisierung der Software bei Bedarf
 - Planmäßige tägliche Quick Scans um 12:00 Uhr
 - Planmäßige wöchentliche Full Scans freitags um 16:00
 - Bei Windows-Servern:
 - Integrierter Virenschutz und Verhaltensanalyse auf Basis von Bitdefender
 - Planmäßiger Quick Scan montags bis donnerstags um 18:00 Uhr
 - Planmäßiger Full Scan freitags um 18:00 Uhr
 - Sofortiges Updaten der Virensignatur bei Veröffentlichung

Für alle iMS Managed-Endpoint-Dienstleistungen gilt:

- Sofortige Benachrichtigung der ifa-Techniker bei kritischen und sicherheitsrelevanten Ereignissen
- Reaktion auf kritische und sicherheitsrelevante Ereignisse innerhalb von vier Stunden während unserer Servicezeiten von 8 bis 17 Uhr an Werktagen
- Innerhalb der Servicezeiten ist die Service-Hotline der ifa systems AG für den Kunden verfügbar; eine Gewährleistung für die Erreichbarkeit wird nicht übernommen. Außerhalb der Servicezeiten steht eine Notfall-Hotline zur Verfügung.
- Direkter Remote-Zugriff auf alle iMS-Endpoints über den iMS-Softwareagenten

3.2. Mengenstufen und -staffeln

Windows Server:

Allgemeine Liefer- und Leistungsbedingungen

ifa Managed Security (iMS)

Mengeneinheiten werden jeweils pro Server abgerechnet. Darüber hinaus werden keine Mengenstaffel oder sonstige Leistungsstufen angeboten. Vertragslaufzeiten werden über 24 und 36 Monate angeboten. Es gilt die jeweils gültige Preisliste für „ifa Managed Security“-Produkte und -Dienstleistungen.

Windows Workstations:

Mengeneinheiten werden jeweils pro Workstation abgerechnet, es gilt folgende Mengenstaffel:

- < 5 Workstations
- 5 – 20 Workstations
- > 20 Workstations

Vertragslaufzeiten werden über 24 und 36 Monate angeboten. Es gilt die jeweils gültige Preisliste für „ifa Managed Security“-Produkte und -Dienstleistungen.

4. iMS Managed Firewall

4.1. Leistungen

Im Rahmen von iMS Managed Firewall stellt die ifa systems AG die Grundsicherung des Netzwerks der betreuten Systeme und übernimmt dazu die Bereitstellung, Einrichtung und Konfiguration sowie die laufende Verwaltung der Firewalls. Diese Komplettlösung umfasst folgende Bereiche:

- Network Protection
 - Firewall: Netzwerk- und Anwendungsverkehr mit zonenbasierten Richtlinien und Benutzeridentität-Awareness; Anpassung der Auslieferungskonfiguration an die kundenspezifischen Anforderungen (z. B. IP BPX)
 - Intrusion Prevention System (IPS): Konfiguration eines IPS für ein- und ausgehende Verbindungen nach Best Practice
 - Advanced Threat Protection: Konfiguration der Advanced Threat Protection mit DNS, IPS, Web- und Datenverkehrsfiltren nach Best Practice
 - Web Protection: Konfiguration des richtlinienbasierten Webfilters für den Internetverkehr nach Best Practices inklusive HTTP-Scanning
 - Web Protection, um unsicheres Surfen und Downloads zu vermeiden.
 - VPN: an Kundenumgebung angepasste VPNs (IPsec, SSL usw.) nach Best Practice inklusive Site-to-Site und Client-to-Site; Software-VPN-Lizenzen erfordern keine zusätzliche Lizenz
- Regelmäßige Updates und Backups der Komplettlösung inkl. Appliance, EnterpriseGuard Subscription, Enhanced Support
- Automatisierte Installation von kritischen Hotfixes für das Firewall-Betriebssystem ohne Neustart des Geräts
- Überwachung der Sicherheit, Performance und Verfügbarkeit der Firewall, Schutzfunktionen und VPN-Tunnel

Allgemeine Liefer- und Leistungsbedingungen

ifa Managed Security (iMS)

Für alle „iMS Managed Firewall“-Lösungen und -Dienstleistungen gilt:

- Sofortige Benachrichtigung der ifa-Techniker bei kritischen und sicherheitsrelevanten Ereignissen
- Reguläre Updates des Firewall-Betriebssystems werden innerhalb des Wartungsfensters von drei Stunden zum nächsten Sonntag um 23:00 Uhr bereitgestellt und automatisch installiert.
- Eine Reaktion auf kritische Ereignisse erfolgt innerhalb von vier Stunden während unserer Servicezeiten von 8 bis 17 Uhr an Werktagen.
- Innerhalb der Servicezeiten ist die Service-Hotline der ifa systems AG für den Kunden verfügbar; eine Gewährleistung für die Erreichbarkeit wird nicht übernommen. Außerhalb der Servicezeiten steht eine Notfall-Hotline zur Verfügung.

4.2. Mengenstufen und -staffeln

Die einzelnen Firewall-Modelle sind auf der Homepage des Herstellers unter <https://www.sophos.com/de-de/products/next-gen-firewall/tech-specs.aspx> zu ersehen.

Die jeweiligen Mengenstufen- und -staffeln richten sich nach der Anzahl der Workstations bzw. Geräte im Netzwerk und werden im individuellen Kundenangebot festgelegt.

Vertragslaufzeiten werden über 24 und 36 Monate angeboten. Es gilt die jeweils gültige Preisliste für „ifa Managed Security“-Produkte und -Dienstleistungen.

5. iMS Managed Backup

5.1. Leistungen

Im Rahmen von iMS Managed Backup stellt die ifa systems AG eine vollständige, hybride „Backup-as-a-Service“-Lösung und überwacht die Backups der betreuten Systeme. Die Lösung bezieht sich standardmäßig auf einen physikalischen Server beziehungsweise Hypervisor. Die hybride Backup-Architektur umfasst einen Netzwerkspeicher („NAS“) als lokales Backup und einen Cloud-Speicher sowie die verschlüsselte Übertragung der Backup-Dateien zwischen dem NAS und der Cloud.

- Image-basiertes Backup des gesamten Servers beziehungsweise aller virtuellen Maschinen
- Hybrides Backup:
 - Alle Daten werden komprimiert und mit dem AES 256 bit Algorithmus verschlüsselt
 - Tägliches inkrementelles Backup um 21:00 Uhr
 - Monatliches Vollbackup am ersten Samstag des Monats um 02:00 Uhr
 - Aufbewahrungsrichtlinien (Minimum bzw. standardmäßig vorkonfiguriert):
 - Managed Backup S
 - Lokal: 30 Tage tagesgenau
 - Cloud: 30 Tage tagesgenau
 - Managed Backup M
 - Lokal: 60 Tage monatsgenau, 30 Tage tagesgenau

- Cloud: 60 Tage monatsgenau, 30 Tage tagesgenau
 - Managed Backup L/Unlimited
 - Lokal: 90 Tage monatsgenau, 30 Tage tagesgenau
 - Cloud: 90 Tage monatsgenau, 30 Tage tagesgenau
 - Kunden-individuelle Aufbewahrungsregelungen sind auf Basis einer schriftlichen Mitteilung des Kunden möglich
- Quartalsbackup:
 - Alle ifa-Daten werden komprimiert und mit dem AES 256 bit Algorithmus verschlüsselt.
 - Voll-Backup am ersten Samstag des Quartals um 02:00 Uhr
 - Aufbewahrungsrichtlinien:
 - Bis zu 10 Jahre, sofern genügend Speicher erworben wurde
- Netzwerkspeicher:
 - Die ifa systems AG liefert, installiert und konfiguriert einen Netzwerkspeicher entsprechend den Vorgaben des Kunden bzw. wie im jeweiligen Auftrag festgelegt.
- Cloud-Speicher / zu sicherndes Datenvolumen bzw. zu buchende Speichermenge:
 - Die ifa systems AG stellt dem Kunden zum Speichern seines Backup-Datenvolumens Speicherplatz auf ihrer Cloud-Backup-Plattform zur Verfügung.
 - Das zu sichernde Datenvolumen wird bei Auftragserteilung durch den Kunden festgelegt. Zusätzlicher Speicherbedarf kann dynamisch entsprechend dem Bedarf des Kunden hinzugefügt werden.
 - Überschreitet der Kunde das von ihm gebuchte Speicherkontingent, indem er z. B. mehr Daten sichert als im festgelegten Datenvolumen definiert, so werden automatisch im nächsten Monat weitere Pakete hinzugefügt, bis die Datenmenge gedeckt ist.
- Wiederherstellung der gesicherten Daten:
 - Mithilfe eines ifa-Technikers können die Schritte zur Datenwiederherstellung eingeleitet werden.
 - Der Kunde kann jederzeit eine Wiederherstellung seiner gesicherten und verschlüsselten Backup-Daten eigenständig durchführen.
 - Für den Zugriff auf das Cloud-Archiv des Quartalsbackups gelten folgende Abrufbedingungen:
 - Bis 210 Tage nach der Archivierung in die Cloud dauert der Zugriff auf das Archiv bis zu 12 Stunden
 - Ab 210 Tage nach der Archivierung in die Cloud dauert der Zugriff auf das Archiv bis zu 48 Stunden

Für alle „iMS Managed Backup“-Lösungen und -Dienstleistungen gilt:

- Sofortige Benachrichtigung der ifa-Techniker bei kritischen und sicherheitsrelevanten Ereignissen
- Reaktion auf kritische und sicherheitsrelevante Ereignisse innerhalb von vier Stunden während unserer Servicezeiten von 8 bis 17 Uhr an Werktagen

Allgemeine Liefer- und Leistungsbedingungen

ifa Managed Security (iMS)

- Innerhalb der Servicezeiten ist die Service-Hotline der ifa systems AG für den Kunden verfügbar. Eine Gewährleistung für die Erreichbarkeit wird nicht übernommen. Außerhalb der Servicezeiten steht eine Notfall-Hotline zur Verfügung.

5.2. Mengestufen und -staffeln

- S Basic: NAS mit 4 TB Nettospeicher + 1 TB Cloudspeicher inkl.
 - 24 Monate Laufzeit
 - 36 Monate Laufzeit
- M Advanced: NAS mit 8 TB Nettospeicher + 5 TB Cloudspeicher inkl.
 - 24 Monate Laufzeit
 - 36 Monate Laufzeit
- L Pro: NAS mit 16 TB Nettospeicher + 25 TB Cloudspeicher inkl.
 - 24 Monate Laufzeit
 - 36 Monate Laufzeit
- XL Unlimited: NAS mit 16 TB Nettospeicher + unbegrenzter Cloudspeicher inkl.
 - 36 Monate Laufzeit
- Die Abrechnung zusätzlichen Speicherplatzes erfolgt je weiterer TB-Cloudspeicher
- Zusätzliche Archivordner für die Datensicherung werden je weiterem Archiv berechnet
- Zusätzliche Server zur Archivierung werden je weiterem Server berechnet
- Zusätzliche Workstations zur Archivierung werden je weiterer Workstation berechnet

Es gilt die jeweils gültige Preisliste für „ifa Managed Security“-Produkte und -Dienstleistungen.

6. Vertragslaufzeiten und Kündigungsfristen

6.1. Vertragslaufzeiten

Die Vertragslaufzeit für sämtliche iMS-Produkte wird ab dem Datum der Auftragsunterzeichnung wirksam und für eine anfängliche Dauer von vierundzwanzig (24) oder sechsunddreißig (36) Monaten geschlossen, wie im jeweiligen Auftrag ausgewiesen.

6.2. Vertragsverlängerung

Die Vereinbarung wird automatisch zum Ende der ursprünglichen Vertragslaufzeit für einen Zeitraum von zwölf (12) Monaten verlängert, wenn sie nicht durch die ifa systems AG oder durch den Kunden mindestens 30 Tage vor Vertragsende der Vereinbarung schriftlich gekündigt wird.

6.3. Kündigung

ifa und/oder der Kunde haben das Recht, diesen Vertrag unter einer der folgenden Bedingungen zu kündigen:

- a. Wenn eine der Parteien zahlungsunfähig oder insolvent erklärt wird

Allgemeine Liefer- und Leistungsbedingungen

ifa Managed Security (iMS)

- b. Wenn der Anwender innerhalb von dreißig (30) Tagen ab Erhalt der Rechnung der ifa systems AG nicht zahlt und/oder anderweitig gegen diesen Vertrag verstößt
- c. Wenn die ifa systems AG ihre Verpflichtungen aus dieser Vereinbarung nicht ausführen kann und dieser Ausfall nach einem Zeitraum von dreißig (30) Tagen nach schriftlicher Mitteilung weiterhin besteht

Jede Kündigung bedarf der Schriftform.

7. Gebühren und Preise

7.1. iMS-Preise

- a. Es gilt jederzeit die jeweils gültige Preisliste für „ifa Managed Security“-Produkte und -Dienstleistungen, sowie die im Angebot bzw. der Auftragsbestätigung festgelegten Preise. Alle Preise der ifa systems AG verstehen sich zzgl. der jeweils gültigen gesetzlichen Mehrwertsteuer.
- b. Die ifa systems AG behält sich das Recht vor, die Preise einzelner Komponenten entsprechend von Preisänderungen, die aus dem Erwerb von Software- und Dienstleistungskomponenten von Unterauftragnehmern resultieren, bei der Verlängerung des Vertrags anzupassen.
- c. Eine solche Preisanpassung ist dem Kunden mindestens 60 Tage vor Wirksamkeit durch die ifa systems AG schriftlich, in der Regel per E-Mail, mitzuteilen.

7.2. Zahlungsmodalitäten

- a. Die Rechnungsstellung erfolgt jeweils am ersten Werktag des Monats.
- b. Alle verbrauchsbasierten Artikel und Zusatzdienstleistungen werden zum 15. des Monats ermittelt und am ersten Werktag des Folgemonats in Rechnung gestellt.

7.3. Sonstige Gebühren

- a. Von der ifa systems AG erbrachte Zusatzleistungen, die nicht Bestandteil des ALB sind, erfolgen, wenn nicht ausdrücklich abweichend schriftlich vereinbart, zu dem jeweils gültigen Vergütungssatz der ifa systems AG gemäß Preisliste zzgl. Mehrwertsteuer.
- b. Die ifa systems AG wird den Kunden vor Erbringung der kostenpflichtigen Leistungen darauf hinweisen, dass es sich um kostenpflichtige Leistungen handelt.

8. Mitwirkungspflichten des Kunden

Es liegt in der Verantwortung des Kunden, ifa unverzüglich über alle Ereignisse / Vorfälle zu informieren, die sich auf die Leistungen im Rahmen dieser Vereinbarung und/oder auf ergänzende Servicebedürfnisse auswirken könnten.

- a. Der Kunde stimmt zu, dass er ifa über alle Änderungen, Installationen oder Dienste an dem Netzwerk informiert, die von Personen durchgeführt werden, die nicht von ifa eingesetzt sind, um ifa bei der Bereitstellung einer effizienten und effektiven Netzwerkunterstützung zu helfen.

- b. Die ifa systems AG nutzt Remote-Einwahl und ggf. vor-Ort-Unterstützungsservices in Übereinstimmung mit dieser Vereinbarung. Die Vertreter von ifa müssen vollen Netzzugriff haben und der Anwender muss vollen Zugriff auf das Netzwerk bereitstellen, um die erforderlichen Überwachungsdienstleistungen und/oder ergänzenden Dienstleistungen zu gewährleisten. Alle Dienstleistungen im Sinne dieser Vereinbarung gelten während der Geschäftszeiten.
- c. Der Anwender wird einen Vertreter bestimmen, der alle Netzwerkzugriffe autorisieren kann. Wenn immer möglich, soll der Vertreter anwesend sein, wenn ein Servicemitarbeiter von ifa vor Ort ist. Diese Kontaktinformationen werden im Anhang A dargestellt, und es liegt in der Verantwortung des Anwenders, ifa über alle Änderungen innerhalb dieser Vertretung dreißig (30) Tage im Voraus zu informieren.
- d. ifa ist verpflichtet, einen Dienst nur an dem/den in dieser Vereinbarung definierten Standort(en) anzubieten, wie sie im jeweiligen Auftrag aufgeführt sind. Wenn der Kunde beabsichtigt, umzuziehen, einen Standort hinzuzufügen oder einen Standort aufzugeben, muss eine entsprechende Mitteilung an ifa dreißig (30) Tage im Voraus erfolgen. ifa behält sich in diesem Fall das Recht vor, Servicebedingungen neu zu verhandeln. Dieses Recht umfasst auch das Recht, einen Dienst an einem neuen Standort zu verweigern. Die Aufgabe eines Standortes hat keinen Einfluss auf die Mindestlaufzeit von vierundzwanzig (24) Monaten.
- e. Der Anwender gewährleistet eine stabile Internetverbindung mit entsprechender Upload- und Download-Rate, die für die jeweiligen Komponenten von iMS ausreichend ist.
 - a. Die Internetverbindung sollte aus technischen Gründen für die Komponente iMS Managed Backup mindestens 40 Mbit/s Upload-Geschwindigkeit betragen.

9. Leistungsbeschränkungen

- a. Kosten für Verbrauchsmaterial, Ersatzteile, Hardware, Software, Netzwerk-Upgrades und die damit verbundenen Dienste liegen außerhalb des Geltungsbereiches dieser Vereinbarung.
- b. Alle zusätzlichen, kostenpflichtigen Server-, Netzwerkgeräte- und Software-Upgrades liegen nicht im Geltungsbereich dieser Vereinbarung.
- c. Herstellergarantien und -Arbeitsdienste liegen nicht im Geltungsbereich dieser Vereinbarung.
- d. Periodische Neustarts für Geräte wie Firewalls, Router und Server sind erforderlich, um kritische Updates und Konfigurationsänderungen anzuwenden und zu aktivieren. Diese Neustarts erfolgen nach Absprache mit ifa und dem Kunden.
- e. Die Unterstützung von Anwendungssoftware ist auf die Produkte der Hersteller begrenzt, die in der Serviceleistung aufgeführt sind.
- f. Die Sicherung der Daten liegt in der Verantwortung des Nutzers. Eine Wiederherstellung von verlorenen Daten, die durch einen System-Hardwareausfall verursacht wurde, liegt explizit außerhalb des Geltungsbereiches dieser Vereinbarung.

10. Haftung

- a. Die ifa systems AG haftet grundsätzlich nur bei Vorsatz und grober Fahrlässigkeit und bei eigenem Verschulden.
- b. Die ifa systems AG haftet für leicht fahrlässiges Verhalten nur, soweit dies eine nicht unerhebliche Verletzung einer vertragswesentlichen Pflicht bedeutet. Eine vertragswesentliche Pflicht ist eine Verpflichtung, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht und auf deren Einhaltung der Auftraggeber regelmäßig vertraut und vertrauen darf.
- c. Bei einer Haftung wegen Vorsatz oder grober Fahrlässigkeit, bei Personenschäden oder nach dem Produkthaftungsgesetz gelten die gesetzlichen Verjährungsfristen. Ansonsten gilt für alle Ansprüche auf Schadensersatz oder Ersatz vergeblicher Aufwendungen des Auftraggebers bei vertraglicher und außervertraglicher Haftung eine Verjährungsfrist von einem Jahr. Die Verjährungsfrist beginnt gemäß den gesetzlichen Bestimmungen. Sie beginnt jedoch spätestens mit Ablauf von 5 Jahren ab Entstehung des Anspruchs.
- d. Die Haftung ist grundsätzlich beschränkt auf denjenigen Aufwand, der zur Beseitigung des Schadens erforderlich ist; z. B. werden bei Datenverlusten nur die Kosten der Wiederherstellung ersetzt.
- e. Eine Haftung ist ausgeschlossen für den Fall, dass ein Schaden durch die Nicht-Erfüllung von Mitwirkungspflichten verursacht wurde, z. B. durch die nicht ordnungsgemäße Durchführung von Datensicherungen.
- f. Eine Haftung für Fehler an einer Software Dritter ist ausgeschlossen.
- g. Gewinnausfallschäden werden nicht ersetzt.
- h. Eine verschuldensunabhängige Haftung nach § 536a Abs. 1 BGB ist ausgeschlossen.
- i. Die Haftung nach dem Produkthaftungsgesetz bleibt unberührt.

11. Vertraulichkeit

- a. Die Parteien werden die Bestimmungen des Vertrags und sonstige vertrauliche Informationen vertraulich behandeln und nicht an Dritte weitergeben, es sei denn, eine solche Weitergabe von Informationen ist aufgrund gesetzlicher oder vertraglicher Bestimmungen erforderlich oder die Weitergabe dieser Informationen wurde schriftlich durch die jeweils andere Partei freigegeben.
- b. Bei Tätigkeiten im Rahmen der Betreuung von IT-Netzwerken in Augenkliniken und Augenarztpraxen wird der ifa-Mitarbeiter zum Erfüllungsgehilfen des verantwortlichen Arztes. Er

Allgemeine Liefer- und Leistungsbedingungen

ifa Managed Security (iMS)

unterliegt damit einer Schweigepflicht und hat die für Mediziner geltenden Regeln der Vertraulichkeit bei insbesondere sensiblen Patientendaten zu beachten.

- c. Bei Eingriffen in Netzwerke, Neuinstallationen, Erweiterungen, Fehlersuche und Reparaturen greift der ifa-Mitarbeiter auf patientenbezogene Daten nur insoweit zu, als dies für den spezifischen Auftrag notwendig bzw. wirtschaftlich sinnvoll ist. Das gilt für Einsätze vor Ort wie auch für übernommene bzw. zugesandte Datenbestände auf Datenträgern.
- d. Die Geheimhaltungspflicht endet frühestens mit Ablauf des fünften Jahres nach Beendigung der Vertragsbeziehung.

12. Datenschutz

- a. Personenbezogene Daten werden von der ifa systems AG in Übereinstimmung mit dem in Deutschland geltenden Datenschutzrecht verarbeitet. Soweit die ifa systems AG eine Auftragsverarbeitung gemäß Art. 28 DSGVO vornimmt, schließen die Parteien eine Auftragsdatenverarbeitungsvereinbarung ab.
- b. Der Kunde sichert zu, dass für sämtliche an die ifa systems AG oder deren Unterauftragnehmer im Rahmen des Vertrags übermittelten oder zugänglich gemachten personenbezogenen Daten (inklusive solcher von Mitarbeitern und Patienten sowie sonstigen Lieferanten und Dritten) eine Zustimmung oder gesetzliche Erlaubnis zur Nutzung und sonstigen Bearbeitung im Rahmen des Vertrags vorliegt.

13. Allgemeine Bestimmungen

- a. Sollten eine oder mehrere Bestimmungen dieses Vertrags unwirksam sein, so bleiben die übrigen Bestimmungen hiervon unberührt. Regelungen, die aufgrund ihrer Unwirksamkeit wegfallen, sind durch gesetzeskonforme Regelungen zu ersetzen, deren Inhalt durch Auslegung zu ermitteln ist.
- b. Sämtliche Änderungen und Ergänzungen des Vertrags oder vergleichbare Erklärungen bedürfen der Schriftform. Dies gilt insbesondere für Kündigungen, Mahnungen oder Fristsetzungen.
- c. Es gilt ausschließlich deutsches Recht. Als Gerichtstand ist Köln vereinbart.

Allgemeine Liefer- und Leistungsbedingungen

ifa Managed Security (iMS)

Anhang 1 – Aufstellung der Überwachungswerte

Folgende Werte werden im Rahmen des iMS Managed Endpoint Monitoring mindestens überwacht:

- Alle relevanten Werte von Windows-, Mac-, Linux- und Netzwerkgeräten:
 - Bei Windows Workstations:
 - Agenten-Status
 - Konnektivität zwischen Probe und Device
 - CPU-Usage
 - Disk Usage: C: Partition
 - Memory Usage
 - Status Windows Firewall
 - Windows Service - ifa Component Registration Service
 - LocalIP
 - Bei Windows-Servern:
 - Agenten-Status
 - Clock Drift
 - Konnektivität zwischen Probe und Device
 - CPU-Usage
 - Disk Usage: alle Partitionen
 - Memory Usage
 - Uptime
- Zusätzlich je nach Server-Rolle:
 - Bei Domain Controllern:
 - Active Directory
 - DNS
 - DNS Performance
 - DHCP
 - DHCP Performance
 - Windows Eventlog: DNS, DHCP
 - Bei Hyper-V Hosts:
 - Hyper-V Health
 - Replikationsstatus
 - Bei Terminalservern:
 - Aktive Sessions
 - TCP Availability
 - Bei Fileservern:
 - Windows-Services:
 - File Server Ressource Manager
 - Remote Storage Server
 - Server for NFS

Allgemeine Liefer- und Leistungsbedingungen

ifa Managed Security (iMS)

Anhang 2 – Third-Party-Patchmanagement

Folgende Produkte werden im Rahmen des Third-Party-Patchmanagement mindestens unterstützt (in alphabetischer Reihenfolge):

- 7-Zip
- Adobe Acrobat, Reader, Flash, Shockwave
- AdoptOpenJDK
- Apple iTunes, QuickTime, Safari
- Foxit Reader
- Google Chrome, Earth
- Oracle Java
- KeePass
- Microsoft Windows & Server, Office, Skype, SQL-Server, .NET Framework, Active Directory Rights Management Services Client, ASP.NET Web Frameworks, Bing, Visual Studio, Exchange Server, Forefront TMG, Microsoft Advanced Threat Analytics, Microsoft Azure Information Protection Client, Microsoft Dynamics CRM, Microsoft Monitoring Agent, MS Security Essentials & Defender, Network Monitor 3, Silverlight, System Center Operations Manager, Works, Zune
- Mozilla Firefox & Thunderbird
- Notepad ++
- Opera
- PuTTY
- WinRAR
- TeamViewer
- VLC Media Player
- WinZip
- Zoom