

IBM MaaS360 (SaaS)

Nella presente Descrizione dei Servizi è descritto il Servizio Cloud che IBM fornisce al Cliente. Il termine "Cliente" indica l'azienda, i relativi utenti autorizzati e i destinatari del Servizio Cloud. L'Offerta applicabile applicabile e la PoE (Proof of Entitlement) sono forniti come Documenti d'Ordine separati.

1. Servizio Cloud

MaaS360 è una piattaforma cloud di facile utilizzo, avente tutte le funzionalità essenziali per una gestione end-to-end dei dispositivi mobili odierni che utilizzano i sistemi operativi iOS, Android, Windows e Blackberry. Di seguito è riportata una breve descrizione delle offerte del Servizio Cloud:

1.1 IBM MaaS360 Mobile Device Management (SaaS) e IBM MaaS360 Mobile Device Management (SaaS) Step up for existing customers

Le funzionalità principali di Mobility Device Management ("MDM") includono la registrazione del dispositivo, la configurazione, la gestione della policy di sicurezza e le azioni del dispositivo, come l'invio, l'individuazione, il blocco e la cancellazione dei messaggi. Le funzionalità MDM avanzate includono le regole di conformità automatizzate, le impostazioni di riservatezza Bring Your Own Device ("BYOD") e la reportistica ed i dashboard Mobility Intelligence.

1.2 IBM MaaS360 Mobile Application Management (SaaS) e IBM MaaS360 Mobile Application Management (SaaS) Step up for existing customers

MaaS360 Mobile Application Management consente di aggiungere le applicazioni e di distribuirle sui dispositivi supportati gestiti da MaaS360. Ciò include MaaS360 App Catalog, un'applicazione sul dispositivo che consente agli utenti di visualizzare, installare e di essere informati dell'aggiornamento di applicazioni gestite.

1.3 IBM MaaS360 Mobile Application Security (SaaS) e IBM MaaS360 Mobile Application Security (SaaS) Step up for existing customers

MaaS360 Mobile Application Security fornisce una protezione dati aggiuntiva per applicazioni aziendali che utilizzano Workplace SDK durante lo sviluppo o per consentire l'integrazione automatica del caricamento app iOS (.ipa), del profilo di fornitura e del certificato di firma. Mobile Application Security integra l'app con Productivity Suite. Tale soluzione abilita il single sign-on, l'accesso Intranet mediante Mobile Enterprise Gateway e l'applicazione delle impostazioni di sicurezza dei dati.

1.4 IBM MaaS360 Gateway for Apps (SaaS) e IBM MaaS360 Gateway for Apps (SaaS) Step up for existing customers

MaaS360 Gateway for Apps offre agli utenti esterni alla rete aziendale un percorso di accesso trasparente alle risorse delle applicazioni interne senza che sia necessaria una connessione VPN completa del dispositivo.

1.5 IBM MaaS360 Mobile Content Management (SaaS) e IBM MaaS360 Mobile Content Management (SaaS) Step up for existing customers

MaaS360 Mobile Content Management consente all'amministratore di aggiungere e distribuire documenti nei dispositivi supportati che sono gestiti da IBM MaaS360 Mobile Device Management. Include IBM MaaS360 Doc Catalogue, un contenitore protetto da password su dispositivo, che offre agli utenti un modo semplice di accedere, visualizzare e condividere documenti. Include un accesso continuo ai repository e al contenuto distribuito come, ad esempio, SharePoint, Box e Google Drive. L'accesso alle condivisioni di file riservati SharePoint e Windows è disponibile con MaaS360 Gateway for Documents. È possibile controllare, verificare e proteggere la versione dei documenti gestiti tramite MaaS360 mediante le opzioni della policy Data Loss Prevention (DLP) come, ad esempio, richiedere l'autenticazione, limitare la funzionalità di copia e incolla e bloccare l'apertura o la condivisione dei documenti in altre applicazioni.

1.6 IBM MaaS360 Mobile Document Sync (SaaS) e IBM MaaS360 Mobile Document Sync (SaaS) Step up for existing customers

MaaS360 Mobile Document Sync fornisce agli utenti la possibilità di sincronizzare il contenuto dell'utente su tutti i dispositivi mobili gestiti. Gli amministratori possono garantire che le policy come, ad esempio, la limitazione delle operazioni di taglia, copia e incolla e il blocco dell'apertura e condivisione del contenuto

in altre app o che siano attive per il contenuto dell'utente sui dispositivi. Il contenuto è archiviato in modo protetto sia nel cloud che nel dispositivo ed è possibile accedervi solo tramite MaaS360 Doc Catalogue.

1.7 IBM MaaS360 Mobile Document Editor (SaaS) e IBM MaaS360 Mobile Document Editor (SaaS) Step up for existing customers

MaaS360 Mobile Document Editor è una potente suite per ufficio che consente agli utenti di utilizzare i documenti aziendali quando sono fuori sede. MaaS360 Mobile Document Editor consente di:

- creare e modificare file .DOC, .PPT e .XLS.
- Creare e modificare moduli di presentazione per diapositive
- Lavorare facilmente con gli allegati delle email ed altri file di MaaS360 per iOS.

1.8 IBM MaaS360 Gateway for Documents (SaaS) e IBM MaaS360 Gateway for Documents (SaaS) Step up for existing customers

Con MaaS360 Gateway for Documents, le organizzazioni possono utilizzare MaaS360 Mobile Content Management per offrire inoltre ai dispositivi esterni alla rete aziendale un accesso trasparente ai siti di connessioni interne, ai siti SharePoint, alle condivisioni file Windows e ad altri sistemi di archiviazione file senza che sia necessaria una connessione VPN completa del dispositivo. L'utilizzo di MaaS360 Gateway for Documents richiede inoltre l'acquisto di MaaS360 Mobile Content Management. Supporta iOS 5.0 e Android 4.0 o versioni successive.

1.9 IBM MaaS360 Email Management (SaaS) e IBM MaaS360 Email Management (SaaS) Step up for existing customers

MaaS360 Email Management include importanti funzionalità per il supporto di Microsoft Exchange ActiveSync e Lotus Traveler.

- Exchange ActiveSync: fornisce supporto ai dispositivi mobili che si connettono a Microsoft Exchange sul protocollo ActiveSync. Tra le soluzioni offerte vi sono le principali funzioni di gestione dei dispositivi mobili, come ad esempio la capacità di configurare e creare dispositivi; garantire le policy ActiveSync (codice di accesso, blocco o accesso consentito all'email); intraprendere azioni sul dispositivo, come il blocco e la cancellazione, e preparare report dettagliati sugli attributi del dispositivo.
- Lotus Traveler: fornisce supporto ai dispositivi mobili che si connettono a IBM Lotus Notes® sul protocollo Lotus Traveler. Le funzionalità includono la possibilità di configurare, bloccare o consentire l'utilizzo di dispositivi, applicare le policy ai codici di accesso, cancellare i dispositivi e preparare dei report dettagliati sugli attributi del dispositivo.

1.10 IBM MaaS360 Secure Mobile Browser (SaaS) e IBM MaaS360 Secure Mobile Browser (SaaS) Step up for existing customers

MaaS360 Browser è un browser web completo che abilita l'accesso ai siti della intranet aziendale e garantisce la conformità delle policy dei contenuti, definendo le policy della sicurezza e di filtraggio del sito web, in modo che gli utenti accedano solo al contenuto web approvato basato su un numero di categorie di contenuto, come i siti di social networking, espliciti o malware. Inoltre, è possibile disabilitare i browser web nativi o di terze parti mediante la policy dell'applicazione o la creazione di blacklist quando in combinazione con MobileFirst Protect Devices. Sono consentite eccezioni con liste approvate (whitelist) di siti web, limitazioni dei cookie; funzionalità per copiare, incollare e stampare; e abilitazione della modalità Kiosk.

1.11 IBM MaaS360 Gateway for Browser (SaaS) e IBM MaaS360 Gateway for Browser (SaaS) Step up for existing customers

MaaS360 Gateway for Browser consente ai dispositivi supportati di accedere ai siti web interni approvati senza che sia necessaria una connessione VPN completa del dispositivo.

1.12 IBM MaaS360 for BlackBerry (SaaS) e IBM MaaS360 for BlackBerry (SaaS) Step up for existing customers

Fornisce supporto per i dispositivi mobili connessi al BlackBerry Enterprise Server ("BES") utilizzando le API BlackBerry. Le funzionalità includono azioni remote come l'invio di un messaggio, la reimpostazione del codice di accesso, l'assegnazione della policy BES e la cancellazione, nonché la creazione di report dettagliati sugli attributi del dispositivo. È richiesta l'installazione di MaaS360 Cloud Extender. Disponibile solo per dispositivi visualizzati o gestiti con MaaS360 tramite BES 5.0.

1.13 IBM MaaS360 Mobile Expense Management (SaaS) e IBM MaaS360 Mobile Expense Management (SaaS) Step up for existing customers

MaaS360 Mobile Expense Management consente all'amministratore di creare le policy di utilizzo dei dati e di assegnarle ai dispositivi supportati che sono gestiti da MaaS360 e assegnare tali policy a livello di dispositivo, di gruppo o a livello globale e configurare la messaggistica e le soglie degli avvisi per entrambe relativamente all'utilizzo di dati in roaming o in rete.

1.14 IBM MaaS360 Management Suite (SaaS) e IBM MaaS360 Management Suite (SaaS) Step up for existing IBM MaaS360 customers

Suite o Bundle di prodotti che include MaaS360 Mobile Device Management, MaaS360 Mobile Application Management, MaaS360 Content Service e MaaS360 Mobile Expense Management.

1.15 IBM MaaS360 Productivity Suite (SaaS) e IBM MaaS360 Productivity Suite (SaaS) Step up for existing customers

Suite o Bundle di prodotti che include MaaS360 Secure Mobile Mail, MaaS360 Mobile Application Management, MaaS360 Mobile Application Security, MaaS360 Content Service e MaaS360 Secure Mobile Browser.

1.16 IBM MaaS360 Secure Mobile Mail (SaaS) e IBM MaaS360 Secure Mobile Mail (SaaS) Step up for existing customers

MaaS360 Secure Mobile Mail fornisce un'applicazione di produttività per ufficio separata che consente agli utenti di accedere e gestire le email, il calendario e i contatti, con la possibilità di controllare le email e gli allegati per impedire la perdita di dati, limitando le operazioni di invio o spostamento del contenuto in altre applicazioni, applicare l'autenticazione, limitare le operazioni di taglia, copia e incolla, nonché vincolare gli allegati delle email alla sola consultazione.

1.17 IBM MaaS360 Gateway Suite (SaaS) e IBM MaaS360 Gateway Suite (SaaS) Step up for existing customers

MaaS360 Gateway Suite consente alle app supportate su iOS e Android di comunicare nuovamente in modo trasparente con le risorse sulla rete interna dell'azienda.

1.18 IBM MaaS360 Content Suite (SaaS) e IBM MaaS360 Content Suite (SaaS) Step up for existing customers

Suite o pacchetto di prodotti che include MaaS360 Mobile Content Management, MaaS360 Mobile Document Editor e MaaS360 Mobile Document Sync.

1.19 IBM MaaS360 Mobile Threat Management (SaaS)

MaaS360 Mobile Threat Management fornisce una sicurezza mobile migliorata con rilevamento malware mobile e rilevamento jailbreak/root avanzato. Con MaaS360 Mobile Threat Management, il Cliente sarà in grado di impostare e gestire le policy di conformità inerenti i malware rilevati ed altre vulnerabilità della sicurezza.

1.20 IBM MaaS360 Content Service (SaaS)

MaaS360 Content Service (SaaS) fornisce agli utenti la capacità di caricare documenti e pacchetti di applicazioni su MaaS360 Content Distribution system.

IBM MaaS360 fornisce a ciascun Cliente 1 GB di Storage. IBM MaaS360 fornisce anche 6 GB di utilizzo di larghezza di banda all'anno per ciascun dispositivo come pool condiviso di larghezza di banda. L'intero pool di larghezza di banda è condiviso da tutti i dispositivi. Tale assegnazione di storage di base e di larghezza di banda non aumenta indipendentemente dal numero di bundle di prodotti o di articoli della linea acquistati. I Clienti devono acquistare ulteriore storage e/o larghezza di banda in base alla quantità usata o necessaria oltre alla quantità di base fornita.

1.21 IBM MaaS360 Content Service Storage (SaaS)

MaaS360 Content Service Storage (SaaS) fornisce agli utenti la capacità di acquistare una quantità totale di storage per i dati disponibile per l'utilizzo con il servizio MaaS360 Content Service (SaaS).

1.22 IBM MaaS360 Content Service Bandwidth (SaaS)

MaaS360 Content Service Bandwidth (SaaS) fornisce agli utenti la capacità di acquistare la quantità totale di larghezza di banda disponibile per l'utilizzo con il servizio MaaS360 Content Service (SaaS).

1.23 IBM MaaS360 Professional (SaaS)

Fornisce alle aziende di piccole e medie dimensioni un modo facile e veloce per configurare da remoto smartphone e tablet, applicare le policy della sicurezza, eseguire il push di app e documenti e proteggere i dati sui dispositivi aziendali e personali. Il Cliente può accedere alle opportune funzionalità di gestione della mobilità della propria azienda in modo rapido, semplice e conveniente.

1.24 IBM MaaS360 Laptop Management (SaaS)

Fornisce al Cliente la possibilità di iscriversi, configurare, gestire e creare report sui dispositivi basati sui sistemi OS X e Windows PC nonché su smartphone e tablet. Le organizzazioni possono mantenere la coerenza dei profili e delle policy di sicurezza tra i dispositivi di proprietà aziendale e di proprietà dei dipendenti all'interno della stessa console di gestione MaaS360.

1.24.1 Windows

MaaS360 Laptop Management (SaaS) per i PC basati su Windows fornisce la reportistica OTA (Over The Air) sulla gestione dell'inventario e delle iscrizioni riguardanti l'hardware, il sistema operativo e le informazioni sul software. Il modulo di reportistica sulla sicurezza degli endpoint fornisce una reportistica interattiva e l'analisi dei dati per le applicazioni fornite dal Cliente quali, ad esempio, le applicazioni anti-virus, di backup/ripristino, per la crittografia dei dati e i firewall personali, nonché le patch mancanti del sistema operativo. Il modulo di protezione dei dati fornisce la reportistica interattiva e l'analisi dei servizi di sicurezza, inclusa la crittografia dei dati, la prevenzione della perdita di dati, il backup/ripristino e altre applicazioni integrate. Supporta i sistemi Windows XP SP3, Windows Vista, Windows 7, Windows 8+ e Windows 8+ Pro (inclusi i sistemi a 32-bit e 64-bit, dove applicabile).

Le azioni del dispositivo includono:

- invio messaggi al dispositivo
- blocco del dispositivo
- individuazione di un dispositivo (richiede MaaS360 Laptop Location)
- arresto/avvio/riavvio dei Servizi
- chiusura/riavvio
- cancellazione dell'unità disco
- configurazione delle impostazioni delle patch
- distribuzione del software

1.24.2 Mac OS X

MaaS360 Laptop Management (SaaS) for Mac OS X fornisce la reportistica OTA (Over The Air) sulla gestione dell'inventario e delle iscrizioni riguardanti l'hardware, il sistema operativo e le informazioni sul software. Il modulo di reportistica sulla sicurezza degli endpoint fornisce una reportistica interattiva e l'analisi dei dati per le applicazioni fornite dal Cliente quali, ad esempio, le applicazioni anti-virus, di backup/ripristino, per la crittografia dei dati e i firewall personali, nonché le patch mancanti del sistema operativo. Il modulo di protezione dei dati fornisce la reportistica interattiva e l'analisi per i servizi di sicurezza dei dati, inclusa la crittografia dei dati. Il modulo di gestione della configurazione consente la gestione remota di un numero di impostazioni del dispositivo e dell'utente, che include: password, email, VPN e Wi-Fi. Supporta il sistema Mac OS X, versione 10.7.3 o successive.

Le azioni del dispositivo includono:

- blocco del dispositivo
- cancellazione dell'unità disco
- modifica della policy del dispositivo

1.25 IBM MaaS360 Laptop Location (SaaS)

MaaS360 Laptop Location (SaaS) ha abilitato la capacità di individuare i computer portatili e i tablet supportati. MaaS360 segnala la posizione delle coordinate del Wi-Fi o dell'indirizzo IP e converte questi dati in un indirizzo facilmente riconoscibile. Quando un dispositivo è online, è possibile recuperarne la posizione corrente. MaaS360 memorizza le posizioni documentate nel corso del tempo e, pertanto, la cronologia delle posizioni è disponibile per la revisione. Richiede MaaS360 Laptop Management (SaaS) for Windows. Supporta i sistemi Windows XP SP3, Windows Vista, Windows 7, Windows 8+ e Windows 8+ Pro (inclusi i sistemi a 32-bit e 64-bit, dove applicabile).

1.26 IBM MaaS360 Laptop Lifecycle Management (SaaS)

Fornisce le funzionalità dell'offerta MaaS360 Laptop Management (SaaS) e aggiunge le seguenti funzionalità:

- consente al Cliente di caricare i pacchetti sulla piattaforma MaaS360 Content Service (SaaS) e di pianificare la distribuzione dei carichi utili (payload) nei dispositivi gestiti dal servizio MaaS360 Laptop Management (SaaS) per Microsoft Windows. Il Cliente controlla tutti gli aspetti della distribuzione, incluse le istruzioni di installazione e di destinazione su un dispositivo, un gruppo o a livello globale. Il Cliente è responsabile della creazione dei file di packaging e di installazione. IBM non fornisce supporto per la creazione del pacchetto di installazione.

1.27 IBM MaaS360 Laptop Security (SaaS)

Fornisce alle organizzazioni la capacità di mantenere la coerenza dei profili e delle policy di sicurezza tra i dispositivi di proprietà aziendale e di proprietà dei dipendenti all'interno della stessa console di gestione.

1.28 IBM MaaS360 Essentials Suite (SaaS)

Questa suite consente al Cliente di visualizzare e controllare i dispositivi mobili e le app accedendo all'organizzazione del Cliente. La suite offre la gestione dei dispositivi mobili, delle applicazioni e delle spese del gruppo aziendale da un'unica schermata.

1.29 IBM MaaS360 Deluxe Suite (SaaS)

Questa suite include tutte le funzionalità di MaaS360 Essentials Suite e aggiunge un'applicazione separata di produttività per uffici molto sicura affinché gli utenti accedano e gestiscano le relative email, agende, contatti e chat.

1.30 IBM MaaS360 Premier Suite (SaaS)

Questa suite include tutte le funzionalità di MaaS360 Deluxe Suite e aggiunge la sicurezza delle applicazioni mobili, un browser per dispositivi mobili sicuro e la gestione del contenuto dei dispositivi mobili.

1.31 IBM MaaS360 Enterprise Suite (SaaS)

Questa suite include tutte le funzionalità di MaaS360 Premier Suite e aggiunge la gestione delle minacce dei dispositivi mobili, un editor di documenti e la sincronizzazione dei documenti.

2. Descrizione della Sicurezza

Questo Servizio Cloud si conforma ai principi IBM sulla sicurezza e riservatezza dei dati per i servizi IBM SaaS che sono disponibili alla pagina web <http://www-03.ibm.com/software/sla/slabdb.nsf/sla/dsp> e ad eventuali condizioni aggiuntive fornite in questo articolo. Eventuali modifiche delle policy di IBM sulla sicurezza dei dati non avranno un impatto negativo sulla sicurezza del Servizio Cloud.

Il presente Servizio Cloud è certificato 'US-EU Safe Harbor'.

3. Service Level Agreement ("SLA")

IBM fornisce il seguente Service Level Agreement ("SLA") di disponibilità per il Servizio Cloud, come specificato nella PoE. Lo SLA non costituisce una garanzia e non si applica al Software di Abilitazione. Lo SLA è disponibile solo per il Cliente e si applica per essere utilizzato esclusivamente negli ambienti di produzione.

3.1 Crediti di Disponibilità

Il Cliente deve registrare un ticket di assistenza di Severità 1 mediante l'help desk del supporto tecnico IBM, entro le 24 ore successive dal momento in cui il Cliente determina che un evento ha avuto un impatto negativo sulla disponibilità del Servizio Cloud. Il Cliente deve fornire ad IBM ragionevole assistenza nella diagnosi e risoluzione di qualsiasi problema.

La richiesta di rimedio per il ticket di assistenza per il mancato adempimento dello SLA dovrà essere inoltrata entro tre giorni lavorativi dal termine del Mese Contrattuale. Il rimborso per una richiesta di rimedio valida relativa allo SLA sarà un credito di cui verrà dato atto in una fattura successiva per il Servizio Cloud in base al periodo di tempo durante il quale l'elaborazione del sistema di produzione per il Servizio Cloud non è disponibile ("Tempo di Fermo"). Il Tempo di Fermo è misurato dal momento in cui il Cliente segnala l'evento fino a quando il Servizio Cloud viene ripristinato e non include il tempo relativo ad un'interruzione pianificata o annunciata per manutenzione; cause al di fuori del controllo di IBM; problemi con i contenuti, le tecnologie, i progetti o le istruzioni del Cliente o di terzi; errori nelle

configurazioni di sistema e di piattaforme non supportate o altri errori del Cliente; oppure incidenti di sicurezza causati dal Cliente o da test di sicurezza del Cliente. IBM applicherà il rimborso più elevato in base alla disponibilità cumulativa del Servizio Cloud durante ciascun mese contrattuale, come mostrato nella tabella seguente. Il rimborso totale rispetto ad un mese contrattuale non può superare il 10 per cento di un dodicesimo (1/12) del corrispettivo annuale per il Servizio Cloud.

3.2 Livelli di Servizio

Disponibilità del Servizio Cloud in un mese contrattuale

Disponibilità in un mese contrattuale	Credito di Disponibilità (% del Costo* dell'abbonamento mensile per il mese contrattuale oggetto di una richiesta di rimedio)
Meno del 99,8%	2%
Meno del 98,8%	5%
Meno del 95,0%	10%

* Se il Cliente ha acquistato il Servizio Cloud da un Business Partner IBM, il costo dell'abbonamento mensile sarà calcolato in base al listino prezzi al momento in vigore per il Servizio Cloud attivo nel mese contrattuale che è oggetto della richiesta di rimedio, scontato del 50%. IBM applicherà uno sconto direttamente al Cliente.

La disponibilità, espressa come percentuale, viene calcolata nel seguente modo: il numero totale di minuti in un mese contrattuale, meno il numero totale di minuti del Tempo di Fermo in un mese contrattuale, diviso per il numero totale di minuti in un mese contrattuale.

Esempio: 425 minuti del Tempo di Fermo totale in un mese contrattuale

43.200 minuti totali in un Mese Contrattuale di 30 (trenta) giorni - 425 minuti di Tempo di Fermo = 42.775 minuti <hr/> 43.200 minuti totali	= 2% Credito di Disponibilità per il 99,0% di disponibilità in un mese contrattuale
---	---

4. Supporto Tecnico

Il supporto tecnico per il Servizio Cloud viene fornito tramite chat, email e telefono.

IBM renderà disponibile la Guida al Supporto IBM Software as a Service che fornisce le informazioni di contatto del supporto tecnico, altre informazioni e procedure.

Severità	Definizione di Severità
1	Problemi o errori con il servizio che interrompono o impediscono all'intera popolazione del Cliente di eseguire le normali operazioni aziendali. Problemi o errori causati dal servizio con un impatto catastrofico sulle normali operazioni aziendali.
2	Problemi o errori con il servizio che interrompono o impediscono ad una percentuale significativa della popolazione del Cliente di eseguire le normali operazioni aziendali. Problemi o errori causati dal servizio con un forte impatto sulle normali operazioni aziendali.
3	Problemi o errori con il servizio che interrompono o impediscono ad una piccola percentuale della popolazione del Cliente di eseguire le normali operazioni aziendali. Problemi o errori causati dal servizio con un impatto significativo sulle normali operazioni aziendali.
4	Problemi o errori con il servizio che interrompono o impediscono ad un singolo utente di eseguire le normali operazioni aziendali. Problemi o errori causati dal servizio con un impatto minore sulle normali operazioni aziendali.

5. Informazioni sulle Titolarità e sulla Fatturazione

5.1 Calcolo dei Corrispettivi

Il Servizio Cloud è disponibile in base al calcolo dei corrispettivi specificato nel Documento d'Ordine:

- a. **Utente Autorizzato** – è un'unità di misura che consente di ottenere il Servizio Cloud. Il Cliente deve ottenere autorizzazioni separate, dedicate per ciascun Utente Autorizzato specifico che accede al Servizio Cloud in qualsiasi modo, direttamente o indirettamente (ad esempio: tramite un programma multiplexing, dispositivo o server applicativo) tramite qualsiasi mezzo. È necessario ottenere titolarità sufficienti a coprire il numero totale di Utenti Autorizzati ai quali è stato concesso l'accesso al Servizio Cloud durante il periodo di misurazione specificato nella PoE o nel Documento della Transazione del Cliente.
- b. **Gigabyte** – è un'unità di misura che consente di ottenere il Servizio Cloud. L'unità Gigabyte è uguale a 2 elevato alla trentesima potenza (1.073.741.824 byte). È necessario ottenere titolarità sufficienti a coprire il numero totale di Gigabyte elaborati dal Servizio Cloud durante il periodo di misurazione specificato nel Documento d'Ordine o nella PoE del Cliente.
- c. **Dispositivo Client Gestito** – è un'unità di misura che consente di ottenere il Servizio Cloud. Un Dispositivo Client è un dispositivo informatico per singolo utente, un sensore per scopi speciali oppure un dispositivo di telemetria che richiede o accetta per il funzionamento una serie di comandi, procedure o applicazioni o che fornisca dati ad un altro sistema di computer generalmente definito come server oppure gestito dal server. Più Dispositivi Client possono condividere l'accesso ad un server comune. Un Dispositivo Client può avere alcune capacità di elaborazione o essere programmabile per consentire ad un utente di lavorare. Il Cliente deve ottenere le titolarità Dispositivo Client Gestito per ogni Dispositivo Client gestito dal Servizio Cloud durante il periodo di misurazione specificato nella PoE del Cliente o nel Documento d'Ordine.
- d. **Dispositivo Client** – è un'unità di misura che consente di ottenere il Servizio Cloud. Un Dispositivo Client è un dispositivo informatico per singolo utente, un sensore per scopi speciali oppure un dispositivo di telemetria che richiede o accetta per il funzionamento una serie di comandi, procedure o applicazioni o che fornisca dati ad un altro sistema di computer generalmente definito come server oppure gestito dal server. Più Dispositivi Client possono condividere l'accesso ad un server comune. Un Dispositivo Client può avere alcune capacità di elaborazione o essere programmabile per consentire ad un utente di lavorare. Il Cliente deve ottenere titolarità per ciascun Dispositivo Client che esegue, fornisce dati, utilizza i servizi forniti da, o che accede al Servizio Cloud in qualche altro modo, durante il periodo di misurazione specificato nella PoE del Cliente o nel Documento d'Ordine.

5.2 Corrispettivi Mensili Parziali

Un Corrispettivo Mensile Parziale così come specificato nel Documento d'Ordine può essere valutato proporzionalmente.

5.3 Corrispettivi di sovrapprezzo

Se l'utilizzo effettivo del Servizio Cloud da parte del Cliente durante il periodo di misurazione supera la titolarità per cui è autorizzato, il Cliente dovrà corrispondere un sovrapprezzo, secondo quanto stabilito nel Documento d'Ordine.

6. Opzioni di Durata e Rinnovo

La durata del Servizio Cloud inizia nella data in cui IBM comunica al Cliente che l'accesso al Servizio Cloud è disponibile, così come documentato nella PoE. Nella PoE sarà specificato se il Servizio Cloud sarà rinnovato automaticamente, se procederà sulla base di un uso continuativo o se terminerà alla scadenza.

6.1 Rinnovo Automatico

In caso di rinnovo automatico, salvo comunicazione scritta da parte del Cliente di non voler rinnovare almeno 90 (novanta) giorni prima della data di scadenza del periodo contrattuale, il Servizio Cloud sarà rinnovato automaticamente per la durata contrattuale specificata nella presente PoE.

LA QUANTITÀ DELLE TITOLARITÀ DI RINNOVO SARÀ UGUALE AL MAGGIORE FRA IL VALORE DELLA QUANTITÀ DELL'ORDINE ORIGINALE, ED IL VALORE DELL'UTILIZZO MENSILE RIPORTATO PER IL MESE ANTECEDENTE ALL'EMISSIONE DELLA FATTURA DI RINNOVO, SALVO CHE SIA DIVERSAMENTE SPECIFICATO AD IBM MEDIANTE COMUNICAZIONE.

LA QUANTITÀ DELLE TITOLARITÀ DI RINNOVO PER L'OFFERTA STEP UP SARÀ UGUALE ALLA QUANTITÀ DELL'ORDINE ORIGINALE.

6.2 Fatturazione Continuativa

In caso di utilizzo continuativo, il Servizio Cloud continuerà ad essere disponibile con cadenza mensile fino a quando il Cliente non fornirà una comunicazione scritta di non voler rinnovare almeno 90 (novanta) giorni prima della scadenza. Il Servizio Cloud continuerà ad essere disponibile fino alla fine del mese di calendario successivo a tale periodo di 90 (novanta) giorni.

7. Software di Abilitazione (Prerequisiti Software)

Il presente Servizio Cloud comprende il software di abilitazione che potrà essere utilizzato solo in associazione con l'utilizzo da parte del Cliente del Servizio Cloud e solo per la durata del periodo di abbonamento.

8. Ulteriori Informazioni

8.1 Limitazioni per i servizi Step up

Per le offerte del Servizio Cloud indicate come "Step up per Clienti esistenti" ("Step up SaaS"), è necessario che il Cliente abbia prima o simultaneamente acquistato le titolarità di licenza appropriate per il programma IBM associato, identificato nel nome dell'offerta Step up SaaS. Ad esempio, il Cliente che acquista i servizi "IBM MobileFirst Protect – Devices (SaaS) Step up per Clienti esistenti" deve avere le titolarità di licenza per il programma IBM associato IBM MobileFirst Protect. Le titolarità del Cliente per i servizi Step up SaaS non possono superare le titolarità del Cliente per il programma IBM associato.

Quando si acquistano i servizi Step up SaaS, il Cliente non può utilizzare le stesse titolarità della licenza per il programma IBM associato all'interno dell'ambiente installato presso la sede del Cliente, così come avviene con le titolarità per i servizi Step up SaaS. Ad esempio, se il Cliente ha 250 titolarità 'Dispositivo Client Gestito' per il programma IBM associato e decide di acquistare 100 titolarità 'Dispositivo Client Gestito' per i Servizi Step up SaaS, il Cliente potrà gestire 100 Dispositivi Client Gestiti dei Servizi Step up SaaS dall'ambiente del Servizio Cloud e 150 Dispositivi Client Gestiti dal software installato presso la sede.

Il Cliente dichiara di aver acquistato (1) le titolarità di licenza applicabili e (2) l'Abbonamento e il Supporto per uno o più programmi IBM associati. Durante il Periodo di Abbonamento dei servizi Step up SaaS, il Cliente deve mantenere aggiornati l'Abbonamento e il Supporto per le titolarità del programma IBM utilizzato, oltre alle titolarità per i servizi Step up SaaS. Qualora la licenza del Cliente per l'utilizzo di uno o più programmi IBM associati, o l'Abbonamento e il Supporto del Cliente per uno o più programmi IBM associati, siano terminati, cesserà anche il diritto all'utilizzo dei servizi Step up SaaS da parte del Cliente.

8.2 Cookies

Il Cliente accetta che IBM possa utilizzare i cookies e le tecnologie di traccia per riunire informazioni idonee ad identificare persone fisiche nella raccolta di statistiche di utilizzo e informazioni progettate per migliorare l'esperienza utente e/o adattare le interazioni con gli utenti in base a <http://www-01.ibm.com/software/info/product-privacy/index.html>.

8.3 Esclusione di informazioni concernenti dati sanitari personali

Il Servizio Cloud non è progettato per conformarsi alle disposizioni HIPAA e non può essere utilizzato per la trasmissione o la memorizzazione di informazioni concernenti i dati personali sanitari.

8.4 Dati normativi

In deroga a qualunque disposizione contraria, e a solo scopo di ricerca normativa, analisi, dimostrazione e reporting, IBM può raccogliere ed utilizzare, in formato aggregato e anonimo (ossia il Cliente e gli utenti autorizzati del Cliente non possono essere identificati come fonte dei dati, rimuovendo pertanto tutte le informazioni di carattere personale che potrebbero consentire la loro identificazione), i dati che rispecchiano le singole esperienze degli utenti autorizzati del Cliente con i Servizi Cloud.

8.5 Utilizzo consentito dalla legge e consenso

8.5.1 Autorizzazione alla Raccolta ed al Trattamento dei Dati

Il Servizio Cloud è progettato per fornire, gestire, monitorare e controllare i dispositivi mobili. Il Servizio Cloud raccoglierà le informazioni dagli utenti e dai dispositivi autorizzati dal Cliente ad interagire con il Servizio Cloud per cui il Cliente ha sottoscritto l'abbonamento. Il Servizio Cloud raccoglie informazioni che, singolarmente o insieme, possono essere considerate da alcuni ordinamenti Informazioni Personali.

I dati raccolti possono includere il nome utente autorizzato, il numero di telefono, l'indirizzo email registrato e l'ubicazione del dispositivo, l'ID utente e la cronologia di navigazione dalle informazioni del browser MaaS360 riguardanti l'hardware, il software e le impostazioni dei dispositivi degli utenti finali, nonché le informazioni generate dal dispositivo. Il Cliente autorizza IBM a raccogliere, trattare ed utilizzare tali informazioni in conformità con le condizioni di questa Descrizione dei Servizi.

8.5.2 Consenso informato degli Interessati

L'utilizzo del Servizio Cloud può implicare varie leggi e normative. Il Servizio Cloud può essere utilizzato solo per scopi legali e nei termini consentiti dalla legge. Il Cliente accetta di utilizzare il Servizio Cloud in ottemperanza alle leggi, normative e politiche applicabili e se ne assume ogni responsabilità ed obbligazione.

Il Cliente riconosce di aver ottenuto o si impegna ad ottenere qualsiasi consenso informato, autorizzazione o licenza completi, necessari per consentire l'utilizzo legale dei Servizi Cloud e la raccolta e il trattamento delle informazioni da parte di IBM, quale Responsabile del Trattamento del Cliente, tramite il Servizio Cloud. Il Cliente autorizza IBM ad ottenere i consensi informati completi necessari per consentire l'utilizzo legale del Servizio Cloud, la raccolta e il trattamento delle informazioni come descritto nell'Accordo di Licenza per l'Utente Finale disponibile alla pagina web

<http://www.ibm.com/software/sla/sladb.nsf/>.

8.6 Conservazione dei Dati

IBM eliminerà tutte le informazioni raccolte, comprese eventuali Informazioni Personali, successivamente alla scadenza o cessazione della presente Descrizione dei Servizi, ad eccezione dei dati che saranno conservati per gli scopi definiti in precedenza, oppure in conformità alle leggi, regole o normative applicabili. In questo caso, IBM conserverà le informazioni raccolte per la durata richiesta da tali finalità, leggi, regole o normative applicabili.

8.7 Riservatezza dei Dati

8.7.1 Trasferimenti oltre confine

Se il Cliente inserisce Informazioni Personali per i Servizi IBM Cloud negli Stati Membri dell'UE, Islanda, Liechtenstein, Norvegia, Svizzera, Turchia e in qualsiasi altro paese europeo che abbia adottato delle norme legislative locali sulla protezione e sulla tutela dei dati personali, il Cliente accetta che IBM possa trattare il Contenuto, incluse le Informazioni Personali, ai sensi delle leggi e dei requisiti pertinenti, al di fuori dei confini nazionali attraverso i responsabili e subincaricati del trattamento, nei seguenti paesi al di fuori dell'Area Economica Europea e nei paesi che la Commissione Europea ritiene abbiano livelli di sicurezza adeguati:

Nome del Responsabile del Trattamento/Subincaricato	Ruolo (Responsabile del Trattamento dei dati o Subincaricato)	Sede
IBM Corporation	Subincaricato	1 New Orchard Rd. Armonk, NY 10504, USA I
IBM India Private Limited	Subincaricato	No. 12, Subramanya Arcade Bannerghatta Road, Bangalore 560029 India

Il Cliente accetta che IBM possa variare, ove lo ritenesse necessario e previa notifica, l'elenco delle sedi nazionali per la fornitura dei Servizi Cloud.

8.7.2 Tutela dei dati personali in conformità alla normativa UE

Se il Cliente rende i dati personali disponibili nei Servizi Cloud IBM all'interno degli Stati Membri dell'UE, Islanda, Liechtenstein, Norvegia, Svizzera o Turchia e qualsiasi altro paese europeo che abbia adottato delle norme legislative locali sulla protezione e sulla privacy dei dati personali oppure se il Cliente ha utenti autorizzati o dispositivi in tali paesi, il Cliente, quale unico Titolare del trattamento, nomina IBM quale responsabile esterno del trattamento di tali informazioni ai sensi dell'articolo 29 del D.Lgs 196/2003 e ss.mm.. IBM tratterà tali Informazioni Personali esclusivamente nella misura necessaria per rendere l'offerta dei Servizi IBM Cloud disponibile in conformità alle condizioni contenute nella descrizione dei Servizi IBM Cloud pubblicate da IBM; il Cliente, inoltre, accetta che tale trattamento venga effettuato in conformità alle istruzioni fornite dal Cliente stesso.

8.8 Dati sulla Sicurezza

Come parte del Servizio Cloud, che includono le attività di reportistica, IBM preparerà e manterrà le informazioni disidentificate e/o aggregate raccolte dal Servizio Cloud ("Dati della Sicurezza"). I Dati sulla Sicurezza non identificheranno il Cliente o una persona, salvo quando diversamente specificato nel seguente comma (d). Il Cliente, inoltre, nel presente documento accetta che IBM possa utilizzare e/o copiare i Dati sulla Sicurezza solo per i seguenti scopi:

- a. pubblicazione e/o distribuzione dei Dati della Sicurezza (ad es., nelle compilazioni e/o analisi relative alla sicurezza informatica);
- b. sviluppo o miglioramento di prodotti o servizi;
- c. conduzione interna della ricerca o con terzi; e
- d. condivisione legale di informazioni confermate di terzi inerenti a responsabili di reati.

Accettato da:

Firma e timbro del Cliente

Data:

Ai sensi ed agli effetti degli artt. 1341 e 1342 del Codice Civile italiano, il Cliente approva espressamente i seguenti articoli del presente documento: "Service Level Agreement ("SLA")"; "Crediti di Disponibilità"; "Opzioni di Durata e Rinnovo"; "Cookies"; "Autorizzazione alla Raccolta ed al Trattamento dei Dati Personali".

Firma e timbro del Cliente

Data: