IBM MaaS360 (SaaS)

Nella presente Descrizione dei Servizi è descritto il Servizio Cloud che IBM fornisce al Cliente. Il termine "Cliente" indica la parte contraente, i relativi utenti autorizzati e i destinatari del Servizio Cloud. Il Preventivo 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 fare in modo che le policy come, ad esempio, la limitazione delle operazioni di taglia-copia-incolla e il blocco dell'apertura e condivisione del contenuto

in altre app 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 email ed altri file di MaaS360 for 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 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.

1.15 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.

1.16 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.

1.17 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.

1.18 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.

1.19 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.

1.20 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).

1.21 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).

1.22 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.

1.23 IBM MaaS360 VPN (SaaS)

IBM MaaS360 VPN è una soluzione VPN (Virtual Private Network) che consente agli utenti di collegarsi senza problemi alla rete del proprio gruppo aziendale dai dispositivi mobili. La soluzione è costituita da un server VPN e da un client per dispositivi mobili e supporta funzionalità come, ad esempio, Device VPN, On-demand VPN, Always on VPN, Per-app VPN e Split tunneling.

1.24 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 una delle Suite MaaS360. Supporta Windows Vista, Windows 7, Windows 8+.

1.25 IBM MaaS360 Suites

IBM MaaS360 Suites consente al Cliente di selezionare le funzionalità più appropriate per gestire i propri casi d'uso. Nella seguente tabella sono descritte le caratteristiche e le funzioni principali incluse in ciascuna Suite MaaS360:

FEATURES	MANAGEMENT (*)	ESSENTIAL	DELUXE	PREMIER	ENTERPRISE
Mobile Device Management (iOS, Android, Windows Mobile, Windows & macOS)	✓	✓	✓	✓	✓
Mobile Application Management (iOS, Android, Windows Mobile, Windows & macOS)	✓	✓	✓	✓	✓
Patch and Update Management (**)	✓	✓	✓	✓	✓
Advisor	✓	✓	✓	✓	✓
Container App	✓	✓	✓	✓	✓
Mobile Expense Management	✓	✓	✓	✓	✓
Identity Management (***)		✓	✓	✓	✓
Secure Mobile Mail			✓	✓	✓
Secure Mobile Chat			✓	✓	✓
VPN				✓	✓
Secure Browser				✓	✓
Gateway for Browser				✓	✓
Content Management				✓	✓
Gateway for Documents				✓	✓
App Security				✓	✓
Gateway for Apps				✓	✓
Mobile Document Editor					✓
Mobile Document Sync					✓
Mobile Threat Management					✓

* IBM MaaS360 Management Suite (SaaS) è disponibile per clienti già esistenti anche come parte di Step Up.

** La funzionalità Patch and Update Management fornisce la possibilità di identificare, documentare, distribuire e installare patch e aggiornamenti nei sistemi operativi e applicazioni in esecuzione sugli endpoint Windows e macOS.

*** La funzionalità Identity Management viene fornita includendo le funzioni dell'offerta IBM Cloud Identity Essentials che fornisce ai Clienti il single sign-on (SSO) per altre applicazioni cloud pubbliche utilizzate dai Clienti.

1.26 IBM MaaS360 Mobility Success Services

IBM MaaS360 Mobility Success Services vengono acquistati come Impegni da utilizzare entro il periodo di abbonamento corrente del Cliente e includono i seguenti servizi specifici. Questi Servizi erogati da remoto utilizzano i consulenti IBM per fornire indicazioni e assistenza per quanto riguarda le best practice, la configurazione e la formazione.

a. **IBM MaaS360 Quick Start Setup Service**

IBM MaaS360 Quick Start Setup Service fornisce competenze e linee guida per l'implementazione di una distribuzione MaaS360 SaaS in un ambiente di destinazione che include fino a 3 (tre) 'extender' cloud, 1 (uno) gateway, fino a 4 (quattro) policy e fino a 10 (dieci) registrazioni dispositivi con l'obiettivo principale del trasferimento della conoscenza. IBM erogherà una serie di web conference e fornirà un massimo di 40 ore di consulenza per assistere il Cliente nella distribuzione. Il consulente si confronterà sulle best practice del programma Bring Your Own Device (BYOD), sulle procedure e le policy aziendali interne che impattano la distribuzione, aiuterà a determinare i prerequisiti hardware, l'architettura della produzione e la strategia di registrazione dispositivi.

Inoltre, il consulente assisterà nel setup e nella configurazione di uno o più Cloud Extender e Enterprise Gateway così come nell'integrazione con l'autorità di certificazione, la directory aziendale ed il sistema di posta elettronica del Cliente. Il consulente fornirà, inoltre, la formazione sulla soluzione e portale MaaS360, inclusa una sessione in cui sarà illustrata una panoramica dettagliata del portale e la relativa attivazione per un massimo di 3 (tre) persone, assistenza nella configurazione di un massimo di 4 (quattro) policy, 1 (uno) contenitore, 1 (una) policy iOS, 1 (una) policy Android e 1 (una) policy per il telefono Windows, inclusa la policy dei dispositivi e le impostazioni della conformità del profilo. Il consulente si confronterà sulle best practice e gli standard di settore per quanto riguarda la gestione utenti e policy, la reportistica, le regole di conformità, la gestione delle applicazioni, nonché la gestione delle app e dei documenti e fornirà la QA sulla soluzione implementata per un massimo di 10 (dieci) dispositivi. Dopo due (2) / quattro (4) settimane dal termine dell'impegno, il consulente effettuerà un controllo dello stato per esaminare l'uso e il successo dell'adozione da parte del Cliente di MaaS360 e identificherà l'eventuale necessità successiva di servizi per la piena adozione.

b. **IBM MaaS360 Health Check Service**

IBM MaaS360 Health Check Service fornisce competenze e linee guida da remoto che consentono di riesaminare l'ambiente MaaS360 del Cliente e l'implementazione e di generare consigli sull'esperienza utente, la sicurezza ed il dimensionamento (scaling) dell'infrastruttura. Il consulente IBM condurrà una serie di web conference fornendo non più di 8 (otto) ore di competenze relative alla consulenza per assistere il Cliente nella distribuzione, riesaminando gli aspetti critici del dimensionamento, dell'integrazione aziendale, dei processi di registrazione ed eseguirà la valutazione di test case per le prestazioni e l'esperienza utente al fine di conoscere e documentare le modifiche dei sistemi e di rete richiesti, necessari per ottenere un'implementazione stabile. Al termine dell'impegno, il consulente IBM fornirà e presenterà una Scheda del Report sul Controllo dello Stato in cui saranno descritti in dettaglio i test case ed i relativi risultati ed i consigli per aumentare l'esperienza utente e l'adozione del dimensionamento della sicurezza e dell'infrastruttura.

c. **IBM MaaS360 Mobility Training Workshop**

IBM MaaS360 Mobility Training Workshop fornisce, per un massimo di 12 (dodici) persone, percorsi di formazione in inglese, erogati da remoto su web e video conference che includono un programma completo di argomenti per fornire al personale amministrativo e del supporto gli strumenti e la conoscenza per supportare la soluzione MaaS360.

Il formatore IBM fornirà un workshop di due giorni al personale amministrativo ed ai team delle operazioni. Il team dell'helpdesk del Cliente (livello 1) imparerà a gestire e rispondere alle richieste degli utenti, gestire il supporto di livello uno, inclusi i concetti di base di IBM MaaS360,

l'amministrazione, l'escalation e gli elementi relativi alla distribuzione del Cliente. Al team delle operazioni mobile del Cliente (livello 2) sarà fornita ulteriore formazione per conoscere il processo e supportare altri team interni nelle aree del contenitore e dell'integrazione aziendale. Ad altro personale relativo all'amministrazione dei dispositivi mobili del Cliente (team addetti all'amministrazione della posta elettronica, della sicurezza, dell'infrastruttura) saranno forniti ulteriori moduli su come gestire il prodotto con efficienza, efficacia e sicurezza, inclusa la modalità multitenant, la protezione dei dispositivi mobili e del contenuto. I materiali sviluppati per la sessione di formazione saranno forniti in formato elettronico a tutti i partecipanti.

d. **IBM MaaS360 Advisor on Demand**

Il servizio IBM MaaS360 Advisor on Demand fornisce fino a 20 (venti) ore del tempo di un consulente IBM di servizi professionale IBM che possono essere utilizzate per attività riguardanti l'ottimizzazione del prodotto IBM MaaS360 e l'attività di distribuzioni. Il consulente IBM presterà la propria assistenza con discussioni tecniche informative al fine di fornire un supporto dedicato a consigliare sulla strategia generale, il progetto tecnico, i processi, i test e la produzione delle best practice operative della produzione durante il processo di implementazione o di migrazione. IBM collaborerà con il Cliente per conoscere e creare una pianificazione del progetto con i requisiti specifici del Cliente inclusi gli obiettivi del progetto, le tecnologie pertinenti, la tempistica desiderata, i materiali da consegnare previsti e il numero stimato di Impegni per il servizio Advisor on Demand. Il Cliente deve fornire l'accesso alle applicazioni, ai sistemi e alla documentazione necessari, richiesti per eseguire i servizi. Il servizio Advisor on Demand sarà considerato completato quando saranno erogate le 20 ore di competenze sulla sicurezza e/o dopo che la pianificazione del progetto e/o i materiali da consegnare documentati definiti nella pianificazione del progetto sono stati consegnati al Cliente.

1.26.1 Responsabilità di IBM inerenti a IBM MaaS360 Mobility Success Services

IBM provvederà a:

- fornire Mobility Success Services acquistati dal Cliente; e
- designare una persona che agisca come IBM Engagement Manager, responsabile di lavorare con il Project Manager del Cliente per pianificare l'impegno e coordinare le risorse.

Il Cliente accetta quanto di seguito specificato:

- essere responsabile di tutti gli oneri associati alle richieste di Impegno effettuate dal Cliente durante il periodo contrattuale;
- e conviene che gli Impegni acquistati devono essere usati entro il periodo contrattuale iniziale e scadono, se non utilizzati, entro la data di fine del periodo contrattuale; e
- presentare una richiesta formale di tutti i Servizi di Setup almeno 30 giorni prima della data di fine dell'abbonamento.

Durante l'erogazione di qualsiasi Mobility Success Service, IBM potrà richiedere informazioni e una ragionevole collaborazione da parte del Cliente. Il mancato adempimento da parte del Cliente nel fornire le informazioni o la collaborazione richieste, potrà, come stabilito da IBM, comportare corrispettivi per gli Impegni, come previsto dai servizi, o ritardi nell'esecuzione del servizio applicabile.

Affinché IBM possa eseguire correttamente il test, il Cliente accetta di attenersi alle istruzioni di IBM nella preparazione e gestione dell'ambiente per il periodo dell'impegno.

2. Descrizione della Sicurezza

Questo Servizio Cloud si attiene ai principi IBM sulla sicurezza e tutela dei dati per i servizi IBM SaaS che sono disponibili alla pagina web http://www.ibm.com/cloud/data-security e ad eventuali condizioni aggiuntive fornite in questo articolo. Eventuali modifiche dei principi IBM sulla sicurezza e tutela dei dati non altereranno la sicurezza del Servizio Cloud.

Questo Servizio Cloud può trattare i dati dei dispositivi, i nomi utente e gli indirizzi email che contengono dati personali, qualora il Cliente, in qualità di titolare del trattamento dei dati, determini che le misure di sicurezza tecniche ed organizzative siano appropriate ai rischi presentati dal trattamento e alla natura dei dati da proteggere. Il Cliente riconosce che questo Servizio Cloud non offre funzionalità per la protezione di contenuto che includa dati sensibili o dati soggetti ad ulteriori requisiti normativi. Il Cliente riconosce che IBM non ha nessuna conoscenza del tipo di dati inclusi nel contenuto del Cliente e non può fare una valutazione riguardo all'idoneità dei Servizi Cloud o alle protezioni di sicurezza in atto.

2.1 Funzionalità per la Sicurezza e Responsabilità

Il Servizio Cloud implementa le seguenti funzionalità di sicurezza:

Il Servizio Cloud esegue la crittografia del contenuto durante la trasmissione dei dati all'esterno della rete IBM. Il Servizio Cloud esegue la crittografia di contenuto 'dormiente' quando in attesa della trasmissione dei dati.

Questo Servizio Cloud è incluso nella certificazione Privacy Shield quando il Cliente sceglie di ospitare il Servizio Cloud in un data center che si trova negli Stati Uniti ed è soggetto alla Policy di IBM su Privacy Shield, disponibile alla pagina web http://www.ibm.com/privacy/details/us/en/privacy_shield.html.

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. 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 inviare 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 un impatto aziendale critico e il Servizio Cloud non è disponibile. Il Cliente deve fornire ad IBM ragionevole assistenza nella diagnosi e risoluzione di qualsiasi problema.

La richiesta di risarcimento per il mancato adempimento di uno SLA dovrà essere inoltrata entro tre (3) giorni lavorativi dal termine del mese contrattuale. Il rimborso per una richiesta di risarcimento 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 (Downtime) 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 il contenuto 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 percento di un dodicesimo (1/12) del corrispettivo annuale per il Servizio Cloud.

Per i Servizi Cloud in bundle (singole offerte confezionate e vendute insieme come unica offerta ad un unico prezzo combinato), il rimborso sarà calcolato sulla base del singolo prezzo mensile combinato per il Servizio Cloud in bundle e non del costo di abbonamento mensile per ciascun singolo Servizio Cloud. Il Cliente può inoltrare soltanto richieste di rimedio inerenti ad un singolo Servizio Cloud all'interno di un bundle in un determinato momento.

3.2 Livelli di Servizio

Disponibilità del Servizio Cloud in un mese contrattuale

Disponibilità in un mese contrattuale	**Rimborso (% del Costo* dell'abbonamento mensile per il mese contrattuale oggetto di una richiesta di risarcimento)**
< 99,8%	2%
< 98,8%	5%
< 95%	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 risarcimento, 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.

4. Supporto tecnico

Il Supporto tecnico per il Servizio Cloud è fornito tramite:

- Email
- Telefono
- Live Chat

IBM renderà disponibile la Guida al Supporto IBM Software as a Service che contiene le informazioni di contatto e le procedure sul supporto tecnico. Il Supporto tecnico è incluso nel Servizio Cloud e non è disponibile come offerta separata.

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'unita 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 d'Ordine 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.

e. Impegno: è un'unità di misura che definisce le titolarità per ottenere i servizi. Un Impegno consiste in servizi professionali e/o di formazione relativi al Servizio Cloud. È necessario ottenere titolarità sufficienti a coprire ciascun Impegno.

5.2 Corrispettivi di Setup

I corrispettivi di setup in un'unica soluzione saranno fatturati in base alla tariffa specificata nel Documento d'Ordine per ciascun servizio di setup ordinato.

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 nella PoE, sarà addebitato un corrispettivo di 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 procede sulla base di un uso continuativo o se termina alla scadenza.

In caso di rinnovo automatico, salvo comunicazione scritta da parte del Cliente di disdetta 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.

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 giorni prima della scadenza. Il Servizio Cloud continuerà ad essere disponibile fino alla fine del mese solare successivo a tale periodo di 90 (novanta) giorni.

7. Ulteriori condizioni

7.1 Prerequisiti Software (Software di Abilitazione)

Il Servizio Cloud richiede l'uso del prerequisito software che il Cliente scaricherà nei propri sistemi per facilitare l'uso del Servizio Cloud. Il Cliente potrà utilizzare il prerequisito software solo in relazione all'utilizzo del Servizio Cloud.

I seguenti programmi software IBM sono inclusi come prerequisito software in base alle condizioni delle relative licenze dei programmi IBM applicabili, in aggiunta alle seguenti limitazioni:

a. IBM MaaS360 Cloud Extender

b. IBM MaaS360 Mobile Enterprise Gateway

c. IBM MaaS360 Mobile Device

d. IBM Security Access Manager

- Limitazioni di Utilizzo: il Cliente può usare IBM Security Access Manager solo per connessioni proxy da dispositivi mobili, gestiti da questo Servizio Cloud, ai server email aziendali.

7.2 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.

7.3 Dati normativi

In deroga a qualunque disposizione contraria, e a solo scopo di ricerca normativa, analisi, dimostrazione e reportistica, 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.

7.4 Autorizzazione alla Raccolta e 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 Dati 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.

7.5 Conservazione dei Dati

IBM eliminerà tutte le informazioni raccolte, compresi eventuali Dati 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.

7.6 Dati sulla Sicurezza

Come parte del Servizio Cloud, che includono le attività di reportistica, IBM preparerà e manterrà i dati anonimi e/o aggregati raccolti dal Servizio Cloud ("Dati sulla Sicurezza"). I Dati sulla Sicurezza non identificheranno il Cliente o le persone, salvo quando diversamente specificato nella seguente lettera (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 sulla 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 dati di terzi confermati inerenti a responsabili di reati.

Accettato da:

_____

Firma e timbro del Cliente

Data:

Ai sensi e per gli effetti degli articoli 1341 e 1342 del Codice Civile Italiano, il Cliente approva specificamente i seguenti articoli del presente documento: “Service Level Agreement (SLA)”, “Crediti di Disponibilità”, “Opzioni di Durata e Rinnovo”, “Prerequisiti Software (Software di Abilitazione)”.

_____

Firma e timbro del Cliente

Data: