Condizioni di Utilizzo IBM (TOU) – Condizioni Specifiche dell'Offerta SaaS

IBM MobileFirst Protect (SaaS)

Le Condizioni di Utilizzo (Terms of Use, "ToU") sono costituite dalle presenti Condizioni di Utilizzo IBM – Condizioni Specifiche dell'Offerta SaaS ("Condizioni Specifiche dell'Offerta SaaS") e dalle disposizioni contenute nel documento Condizioni di Utilizzo IBM- Condizioni Generali ("Condizioni Generali") disponibili nel seguente URL: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

In caso di contrasto, le presenti Condizioni Specifiche dell'Offerta SaaS prevalgono sulle Condizioni Generali. Ordinando, accedendo o utilizzando i servizi IBM SaaS, il Cliente accetta le Condizioni di Utilizzo (ToU).

Le presenti Condizioni di Utilizzo (ToU) sono disciplinate dall'Accordo IBM International Passport Advantage, dall'Accordo IBM International Passport Advantage Express, o dall'Accordo Internazionale IBM per le Offerte di servizi IBM SaaS selezionate, quando applicabili, e complessivamente costituiscono l'accordo completo tra le parti ("Accordo").

1. IBM SaaS

Le presenti Condizioni Specifiche dell'Offerta SaaS alle condizioni dell'offerta di servizi IBM SaaS:

- IBM MobileFirst Protect – Devices (SaaS)
- IBM MobileFirst Protect – Devices (SaaS) Step up per Clienti esistenti
- IBM MobileFirst Protect – Applications (SaaS)
- IBM MobileFirst Protect – Applications (SaaS) Step up per Clienti esistenti
- IBM MobileFirst Protect – Application Security (SaaS)
- IBM MobileFirst Protect – Application Security (SaaS) Step up per Clienti esistenti
- IBM MobileFirst Protect – Gateway for Apps (SaaS)
- IBM MobileFirst Protect – Gateway for Apps (SaaS) Step up per Clienti esistenti
- IBM MobileFirst Protect – Content (SaaS)
- IBM MobileFirst Protect – Content (SaaS) Step up per Clienti esistenti
- IBM MobileFirst Protect – Document Sync (SaaS)
- IBM MobileFirst Protect – Document Sync (SaaS) Step up per Clienti esistenti
- IBM MobileFirst Protect – Document Editor (SaaS)
- IBM MobileFirst Protect – Document Editor (SaaS) Step up per Clienti esistenti
- IBM MobileFirst Protect – Gateway for Documents (SaaS)
- IBM MobileFirst Protect – Gateway for Documents (SaaS) Step up per Clienti esistenti
- IBM MobileFirst Protect – Email Management (SaaS)
- IBM MobileFirst Protect – Email Management (SaaS) Step up per Clienti esistenti
- IBM MobileFirst Protect – Browser (SaaS)
- IBM MobileFirst Protect – Browser (SaaS) Step up per Clienti esistenti
- IBM MobileFirst Protect – Gateway for Browser (SaaS)
- IBM MobileFirst Protect – Gateway for Browser (SaaS) Step up per Clienti esistenti
- IBM MobileFirst Protect for Blackberry (SaaS)
- IBM MobileFirst Protect for Blackberry (SaaS) Step up per Clienti esistenti
- IBM MobileFirst Protect – Expenses (SaaS)
- IBM MobileFirst Protect – Expenses (SaaS) Step up per Clienti esistenti
- IBM MobileFirst Protect – Management Suite (SaaS)
- IBM MobileFirst Protect – Management Suite (SaaS) Step up per Clienti esistenti
- IBM MobileFirst Protect – Productivity Suite (SaaS)

- IBM MobileFirst Protect – Productivity Suite (SaaS) Step up per Clienti esistenti
- IBM MobileFirst Protect – Secure Mail (SaaS)
- IBM MobileFirst Protect – Secure Mail (SaaS) Step up per Clienti esistenti
- IBM MobileFirst Protect – Gateway Suite (SaaS)
- IBM MobileFirst Protect – Gateway Suite (SaaS) Step up per Clienti esistenti
- IBM MobileFirst Protect – Content Suite (SaaS)
- IBM MobileFirst Protect – Content Suite (SaaS) Step up per Clienti esistenti
- IBM MobileFirst Protect – Threat Management (SaaS)
- IBM MobileFirst Protect – Content Service (SaaS)
- IBM MobileFirst Protect – Content Service Storage (SaaS)
- IBM MobileFirst Protect – Content Service Bandwidth (SaaS)
- IBM MobileFirst Protect – Professional (SaaS)
- IBM MobileFirst Protect – Laptop (SaaS)
- IBM MobileFirst Protect – Laptop Location (SaaS)
- IBM MobileFirst Protect – Laptop Lifecycle Management (SaaS)
- IBM MobileFirst Protect – Laptop Security and Compliance (SaaS)
- IBM MaaS360 Advanced Mobile Management Suite Prime (SaaS)
- IBM MaaS360 Secure Productivity Suite Prime (SaaS)
- IBM MaaS360 Secure Document Sharing Suite Prime (SaaS)
- IBM MaaS360 Professional Bundle Prime (SaaS)
- IBM MaaS360 Educational Bundle Prime (SaaS)
- IBM MaaS360 Advanced Laptop Management Prime (SaaS)

2. Calcolo dei Corrispettivi

I servizi IBM SaaS sono venduti secondo uno dei seguenti calcoli dei corrispettivi e come specificato nel Documento d'Ordine:

a. **Utente Autorizzato** – è un'unità di misura che consente di ottenere i servizi IBM SaaS. Il Cliente deve ottenere autorizzazioni separate, dedicate, per ciascun Utente Autorizzato che accede ai servizi IBM SaaS in qualsiasi modo, direttamente o indirettamente (ad esempio: mediante un programma multiplexing, dispositivo o server applicativo), con qualsiasi mezzo. È necessario ottenere titolarità sufficienti a coprire il numero di Utenti Autorizzati che accedono ai servizi IBM SaaS durante il periodo di misurazione specificato nella PoE (Proof of Entitlement) del Cliente o nel Documento d'Ordine.

b. **Gigabyte** – è un'unità di misura che consente di ottenere i servizi IBM SaaS. 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 dai servizi IBM SaaS durante il periodo di misurazione specificato nella PoE (Proof of Entitlement) del Cliente o nel Documento d'Ordine.

c. **Dispositivo Client Gestito** – è un'unità di misura che consente di ottenere i servizi IBM SaaS. 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 da IBM SaaS durante il periodo di misurazione specificato nella PoE (Proof of Entitlement) del Cliente o nel Documento d'Ordine.

d. **Dispositivo Client** – è un'unità di misura che consente di ottenere i servizi IBM SaaS. 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 per ciascun Dispositivo Client che esegue, fornisce dati, utilizza i servizi forniti da, o in altro modo acceda ai servizi IBM SaaS durante il periodo di misurazione specificato nella PoE (Proof of Entitlement) del Cliente o nel Documento d'Ordine.

3. Corrispettivi e Fatturazione

L'ammontare da pagare per i servizi IBM SaaS è specificato nel Documento d'Ordine.

3.1 Corrispettivi Mensili Parziali

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

3.2 Corrispettivi di sovraprezzo

Se l'utilizzo effettivo dei servizi IBM SaaS da parte del Cliente durante il periodo di misurazione supera la titolarità per cui è autorizzato nella PoE nella PoE, al Cliente verrà fatturato mensilmente un sovrapprezzo, calcolato applicando la tariffa specificata nel Documento d'Ordine.

4. Opzioni di rinnovo del Periodo di Abbonamento ai servizi IBM SaaS

Nella PoE del Cliente sarà specificato se i servizi IBM SaaS saranno rinnovati alla fine del Periodo di Abbonamento, definendo la durata in base alle seguenti opzioni:

4.1 Rinnovo Automatico

Se nella PoE del Cliente è indicato che il rinnovo del contratto è automatico, il Cliente può non rinnovare il Periodo di Abbonamento ai servizi IBM SaaS in scadenza inoltrando una comunicazione scritta di non voler rinnovare al rappresentante IBM o al Business Partner IBM, almeno novanta (90) giorni prima della data di scadenza del periodo stabilita nella PoE. Se IBM o il relativo Business Partner IBM non riceve alcuna notifica di cancellazione entro la data di scadenza, il Periodo di Abbonamento in scadenza verrà rinnovato automaticamente per la durata di un anno o per la stessa durata di origine come stabilito nella 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.

4.2 Fatturazione Continuativa

Se nella PoE è indicato che il rinnovo del contratto è continuativo, il Cliente continuerà ad aver accesso ai servizi IBM SaaS e gli sarà fatturato senza interruzioni l'utilizzo dei servizi IBM SaaS. Per sospendere l'utilizzo dei servizi IBM SaaS e arrestare il processo di fatturazione continuativa, il Cliente deve fornire ad IBM o al Business Partner IBM un preavviso scritto di novanta (90) giorni, richiedendo la cancellazione dell'accesso ai servizi IBM SaaS. In seguito alla cancellazione dell'accesso del Cliente, saranno fatturati al Cliente tutti i corrispettivi riguardanti l’accesso ancora in sospeso fino al mese in cui è stata effettuata la cancellazione.

4.3 Rinnovo su Richiesta

Se nella PoE è indicato che il tipo di contratto è a tempo determinato, i Servizi di IBM SaaS termineranno alla fine del Periodo di Abbonamento e l'accesso del Cliente ai servizi IBM SaaS verrà rimosso. Per continuare ad utilizzare i servizi IBM SaaS oltre quella data, il Cliente dovrà effettuare un ordine rivolgendosi al rappresentante IBM o al Business Partner IBM e sottoscrivere un nuovo Periodo di Abbonamento.

5. Supporto tecnico

Il supporto tecnico per i servizi IBM SaaS, disponibile durante il periodo di abbonamento, è un supporto strutturato di secondo livello per il team operativo del Cliente e non fornisce supporto per l'Utente Finale.

Il supporto è fornito attraverso molteplici canali; 24 ore al giorno tutti i giorni della settimana. Le informazioni riguardanti il supporto della soluzione IBM SaaS sono disponibili sul portale del prodotto.

Obiettivi della capacità di risposta previsti:

Severità	Definizione di Severità	Iniziale Obiettivi del Tempo di Risposta (Response Time Objectives, RTO)	Copertura del Tempo di Risposta
1	**Inattività di servizio/impatto critico:** La funzionalità aziendale critica non è operativa oppure l'interfaccia critica non funziona. Ciò è di solito applicabile a un ambiente di produzione e indica l'impossibilità di accedere ai servizi determinando un impatto critico sulle operazioni. Questa condizione richiede una soluzione immediata.	30 minuti	24x7
2	**Impatto aziendale alto:** una funzione dei servizi aziendali o una funzione del servizio è gravemente limitata nel suo utilizzo oppure il Cliente rischia di non rispettare le scadenze aziendali.	1 ora lavorativa	24 x 7
3	**Impatto aziendale medio:** Indica che il servizio o la funzionalità è utilizzabile e non ha un impatto critico sulle operazioni.	2 ore lavorative	24 x 7
4	**Impatto aziendale basso:** Una domanda o una richiesta non tecnica	3 ore lavorative	24 x 7

6. Ulteriori Condizioni dell'Offerta IBM SaaS

6.1 Limitazioni per i servizi Step up

Per le offerte IBM SaaS indicate come "Step up per Clienti esistenti" ("Step up SaaS"), è necessario che il Cliente abbia acquistato prima o simultaneamente le titolarità di licenza appropriate per il programma IBM come indicato 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 IBM SaaS 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.

6.2 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.

6.3 Trasferimenti oltre confine

Se il Cliente inserisce Dati Personali per le offerte IBM SaaS 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 trasferire il Contenuto, inclusi i Dati Personali, ai sensi delle leggi e dei requisiti pertinenti, al di fuori dei confini nazionali attraverso i responsabili e incaricati 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, ove lo ritenesse necessario e previa notifica, variare l'elenco delle sedi nazionali per la fornitura dell'offerta IBM SaaS.

6.4 Tutela dei dati personali in conformità alla normativa UE

Se il Cliente rende i dati personali disponibili nei servizi IBM SaaS all'interno degli Stati Membri dell'UE, Islanda, Liechtenstein, Norvegia, Svizzera o Turchia e in 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 per gli scopi richiesti per l'erogazione dell'offerta IBM SaaS, in conformità alle condizioni contenute nella descrizione dei servizi IBM SaaS pubblicate da IBM; il Cliente, inoltre, accetta che tale trattamento venga effettuato in conformità alle istruzioni fornite dal Cliente stesso.

6.5 Conformità Safe Harbor

Le offerte IBM SaaS sono incluse nel certificato Fiberlink Communications Corporation (Filiale IBM) US-EU Safe Harbor. Sia IBM che Fiberlink si attengono al U.S. – EU Safe Harbor Framework come stabilito dal Ministero del Commercio degli Stati Uniti relativamente alla raccolta, all'utilizzo e alla conservazione di informazioni raccolte dall'Unione Europea. http://www.export.gov/safeharbor/.

Qualora la direttiva 'US-EU Safe Harbor Framework' non sia applicabile ad un trasferimento di Dati Personali EEA, le Parti o le relative Consociate possono stipulare separatamente accordi standard non emendati 'EU Model Clause', in conformità alla Decisione della Comunità Europea 2010/87/EU, rimuovendo le clausole facoltative. Qualsiasi controversia o responsabilità derivante da tali accordi, anche se generata da società consociate, sarà considerata dalle Parti come se la controversia o la responsabilità fosse sorta tra le Parti medesime in base alle condizioni del presente Accordo.

6.6 Sedi beneficiarie dei servizi

Ove applicabili, le imposte sono calcolate in base alle sedi che il Cliente identifica come beneficiarie dei servizi IBM SaaS. IBM applicherà le imposte in base all'indirizzo commerciale riportato come sede principale delle attività aziendali durante la compilazione dell'ordine di IBM SaaS, salvo diversamente comunicato dal Cliente a IBM. Il Cliente è responsabile di mantenere tali informazioni aggiornate e di comunicare eventuali variazioni ad IBM.

6.7 Dati normativi

In deroga a qualunque disposizione contraria, e solo a scopo di ricerca normativa, analisi, dimostrazione e reportistica, IBM potrà raccogliere ed utilizzare, in formato aggregato e anonimo (il Cliente o gli utenti autorizzati del Cliente, cioè, non possono essere identificati come fonte dei dati, facendo in modo di rimuovere 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 IBM SaaS.

6.8 Utilizzo consentito dalla legge e consenso

6.8.1 Autorizzazione alla Raccolta ed al Trattamento dei Dati

I servizi IBM SaaS sono progettati per fornire, gestire, proteggere, monitorare e controllare i dispositivi mobili. I servizi IBM SaaS raccoglieranno le informazioni dagli utenti e dai dispositivi autorizzati dal Cliente ad interagire con i suddetti servizi IBM SaaS per i quali il Cliente ha sottoscritto l'abbonamento. I servizi IBM SaaS raccolgono 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 protetta, informazioni sull'hardware, sul software e sulle impostazioni dei dispositivi degli utenti finali nonché informazioni generate dal dispositivo. Il Cliente autorizza IBM a raccogliere, trattare ed utilizzare tali informazioni in conformità con le disposizioni delle Condizioni di Utilizzo.

6.8.2 Consenso Informato degli Interessati

L'utilizzo dei servizi IBM SaaS può implicare varie leggi e normative. I servizi IBM SaaS possono essere utilizzati solo per scopi legali e nei termini consentiti dalla legge. Il Cliente accetta di utilizzare i servizi IBM SaaS in ottemperanza alle leggi, normative e policy applicabili e se ne assume ogni responsabilità ed obbligazione.

Il Cliente dichiara e garantisce di aver ottenuto o che otterrà qualsiasi consenso informato, autorizzazione o licenza completi, necessari per consentire l'utilizzo legale dei servizi IBM SaaS e la raccolta e il trattamento delle informazioni da parte di IBM, quale Responsabile del Trattamento del Cliente, tramite i servizi IBM SaaS. Il Cliente autorizza IBM ad ottenere i consensi informati completi necessari per consentire l'utilizzo legale dei servizi IBM SaaS, 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/.

6.9 Conservazione dei Dati

IBM eliminerà tutte le informazioni raccolte, compresi eventuali Dati Personali, successivamente alla cessazione delle presenti Condizioni di Utilizzo (ToU), 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.

Appendice A

MobileFirst Protect è una piattaforma cloud di facile utilizzo, avente tutte le funzionalità essenziali per la gestione end-to-end dei dispositivi mobili più recenti, che include iPhone, iPad, dispositivi Android, Kindle Fire e gli smartphone Windows Phone e BlackBerry. Di seguito è riportata una breve descrizione delle offerte IBM SaaS:

1. IBM MobileFirst Protect – Devices (SaaS)

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.

2. IBM MobileFirst Protect – Applications (SaaS)

MobileFirst Protect Applications consente di aggiungere le applicazioni e di distribuirle sui dispositivi, supportati gestiti da MobileFirst Protect. Include MobileFirst Protect App Catalog, un'applicazione su dispositivo che consente agli utenti di visualizzare, installare ed essere informati dell'aggiornamento di applicazioni gestite.

3. IBM MobileFirst Protect – Application Security (SaaS)

MobileFirst Protect 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 Secure 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.

4. IBM MobileFirst Protect – Gateway for Apps (SaaS)

MobileFirst Protect Gateway for Apps offre agli utenti esterni alla rete aziendale un accesso sicuro e continuo alle risorse delle applicazioni interne, senza richiedere una connessione VPN completa del dispositivo.

5. IBM MobileFirst Protect – Content (SaaS)

MobileFirst Protect Content consente all'amministratore di aggiungere e distribuire documenti nei dispositivi supportati, gestiti da IBM MobileFirst Protect Devices. Include IBM MobileFirst Protect Doc Catalogue, un contenitore protetto da password, su dispositivo, che offre agli utenti un modo semplice e sicuro 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 SharePoint e Windows privati è disponibile con MobileFirst Protect Mobile Enterprise Gateway. È possibile applicare il controllo, la verifica e la protezione della versione dei documenti gestiti tramite MobileFirst Protect attraverso le opzioni della policy Data Loss Prevention (DLP), come ad esempio l'autenticazione, la limitazione della funzionalità copia e incolla, e il blocco dell'apertura o della condivisione di contenuti in altre applicazioni.

6. IBM MobileFirst Protect – Document Sync (SaaS)

MobileFirst Protect Document Sync fornisce agli utenti la possibilità di sincronizzare, in modo facile e sicuro, il contenuto dell'utente tra 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, con accesso consentito solo tramite MobileFirst Protect Doc Catalogue.

7. IBM MobileFirst Protect – Document Editor (SaaS)

MobileFirst Protect Document Editor è una potente suite per ufficio che consente agli utenti di utilizzare i documenti di business quando sono fuori sede. MobileFirst Protect Secure 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 MobileFirst Protect per iOS.

8. IBM MobileFirst Protect – Gateway for Documents (SaaS)

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

9. IBM MobileFirst Protect – Email Management (SaaS)

MobileFirst Protect Email Management include importanti funzioni 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.

10. IBM MobileFirst Protect – Browser (SaaS)

MobileFirst Protect Browser è un browser web completo che abilita l'accesso sicuro ai siti intranet aziendali e garantisce la conformità delle policy di contenuto, definendo le policy di 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.

11. IBM MobileFirst Protect – Gateway for Browser (SaaS)

MobileFirst Protect Gateway for Browser consente ai dispositivi supportati di accedere ai siti web interni approvati senza richiedere una connessione VPN completa del dispositivo.

12. IBM MobileFirst Protect for Blackberry (SaaS)

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. L'installazione di MobileFirst Protect Cloud Extender è obbligatoria. Disponibile solo per dispositivi visualizzati o gestiti con MobileFirst Protect tramite BES 5.0.

13. IBM MobileFirst Protect – Expenses (SaaS)

MobileFirst Protect Expenses consente all'amministratore di creare le policy di utilizzo dei dati e di assegnarle ai dispositivi supportati, gestiti da MobileFirst Protect, nonché assegnare tali policy a un dispositivo, gruppo o a livello globale, configurando inoltre la messaggistica e le soglie di avviso per l'utilizzo sia dei dati in roaming o che in rete.

14. IBM MobileFirst Protect – Management Suite (SaaS)

Suite o pacchetto di prodotti che include MobileFirst Protect Devices, MobileFirst Protect Applications, MobileFirst Protect Content e MobileFirst Protect Expenses.

15. IBM MobileFirst Protect – Productivity Suite (SaaS)

Suite o pacchetto di prodotti che include MobileFirst Protect Secure Mail, MobileFirst Protect Applications, MobileFirst Protect Application Security, MobileFirst Protect Content e MobileFirst Protect Browser.

16. IBM MobileFirst Protect – Secure Mail (SaaS)

MobileFirst Protect Secure Mail fornisce un'applicazione di produttività separata e sicura per ufficio, che consente agli utenti di accedere e gestire le email, il calendario ed i contatti, con la possibilità di controllare le email e gli allegati e impedire la perdita di dati limitando le operazioni di inoltro o spostamento del contenuto in altre applicazioni, di applicare l'autenticazione, di limitare le attività di taglio, copia ed incolla e di bloccare gli allegati email alla sola consultazione.

17. IBM MobileFirst Protect – Gateway Suite (SaaS)

MobileFirst Protect Gateway Suite consente alle app supportate su sistemi iOS e Android di comunicare in modo sicuro e continuo con le risorse sulla rete interna dell'azienda.

18. IBM MobileFirst Protect – Content Suite (SaaS)

Suite o pacchetto di prodotti che include MobileFirst Protect Content, MobileFirst Protect Document Editor e MobileFirst Protect Document Sync.

19. IBM MobileFirst Protect – Threat Management (SaaS)

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

20. IBM MobileFirst Protect – Content Service (SaaS)

MobileFirst Protect Content Service (SaaS) fornisce agli utenti la capacità di caricare documenti e pacchetti di applicazioni sul sistema MobileFirst Protect Content Distribution.

Con MobileFirst Protect Content Service, i Clienti dovranno anche acquistare almeno una titolarità di MobileFirst Protect Content Service Storage (SaaS) e MobileFirst Protect Content Service Bandwidth (SaaS).

21. IBM MobileFirst Protect – Content Service Storage (SaaS)

MobileFirst Protect Content Service Storage (SaaS) fornisce agli utenti la capacità di acquistare una quantità totale di storage dei dati, disponibile per l'utilizzo con l'offerta MobileFirst Protect Content Service (SaaS)

22. IBM MobileFirst Protect – Content Service Bandwidth (SaaS)

MobileFirst Protect Content Service Bandwidth (SaaS) fornisce agli utenti la capacità di acquistare la quantità totale di larghezza di banda disponibile da utilizzare con l'offerta MobileFirst Protect Content Service (SaaS)

23. IBM MobileFirst Protect – 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. È possibile accedere alle opportune funzionalità di gestione della mobilità per l'azienda del Cliente in modo rapido, semplice e conveniente.

24. IBM MobileFirst Protect – Laptop (SaaS)

Fornisce al Cliente la possibilità di iscriversi, configurare, gestire, proteggere 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 aziendali e di proprietà dei dipendenti all'interno della stessa console di gestione MobileFirst Protect.

24.1 Windows

MobileFirst Protect – Laptop (SaaS) per i PC basati su Windows fornisce la reportistica OTA (Over The Air) sulla gestione dell'inventario e delle iscrizioni riguardante 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 MobileFirst Protect Laptop Location)
- arresto/avvio/riavvio dei Servizi
- chiusura/riavvio
- cancellazione dell'unità disco
- configurazione delle impostazioni delle patch
- distribuzione del software

24.2 Mac OS X

L'offerta MobileFirst Protect – Laptop (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

25. IBM MobileFirst Protect – Laptop Location (SaaS)

MobileFirst Protect Laptop Location (SaaS) ha abilitato la capacità di individuare i computer portatili e i tablet supportati. MobileFirst Protect documenta 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. MobileFirst Protect memorizza le posizioni documentate nel corso del tempo e, pertanto, la cronologia delle posizioni è disponibile per la revisione. Richiede IBM MobileFirst Protect Laptop (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).

26. IBM MobileFirst Protect – Laptop Lifecycle Management (SaaS)

Fornisce le funzionalità dell'offerta MobileFirst Protect – Laptop (SaaS) e aggiunge le seguenti funzionalità:

- caricare i pacchetti sulla piattaforma MobileFirst Protect Content Service (SaaS) e di pianificare la distribuzione dei carichi utili (payload) nei dispositivi gestiti dal servizio MobileFirst Protect Laptop (SaaS) per Microsoft Windows. Il Cliente controlla tutti gli aspetti della distribuzione, incluse le istruzioni di installazione e di destinazione a livello di dispositivo, di 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.

27. IBM MobileFirst Protect – Laptop Security and Compliance (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.

28. IBM MaaS360 Advanced Mobile Management Suite Prime (SaaS)

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.

29. IBM MaaS360 Secure Productivity Suite Prime (SaaS)

Offre la possibilità di accedere in modo sicuro alle email, di archiviare, distribuire e gestire applicazioni e fornire l'accesso al sito intranet utilizzando Secure Browser.

30. IBM MaaS360 Secure Document Sharing Suite Prime (SaaS)

Offre la possibilità di gestire da remoto e configurare smartphone e tablet, applicare policy di sicurezza, distribuire dati, documentare l'uso del Wi-Fi che può essere utilizzato per monitorare l'utilizzo e le spese di dati insieme all'archiviazione e distribuzione di contenuto per applicazioni e documenti.

31. IBM MaaS360 Professional Bundle Prime (SaaS)

Fornisce alle aziende di piccole e medie dimensioni un modo 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.

32. IBM MaaS360 Educational Bundle Prime (SaaS)

Offre agli enti di formazione la possibilità di gestire e configurare da remoto smartphone e tablet, applicare dati di distribuzione delle policy di sicurezza insieme all'archiviazione e distribuzione di contenuto per le applicazioni e la gestione delle applicazioni.

33. IBM MaaS360 Advanced Laptop Management Prime (SaaS)

Offre alle organizzazioni la possibilità di gestire, aggiornare, individuare e distribuire il software ai computer portatili fornendo policy di sicurezza congruenti su tutta la reportistica di laptop/desktop nella console di gestione MaaS360.

Appendice B

IBM fornisce il seguente Service Level Agreement ("SLA") di disponibilità per i servizi IBM SaaS ed è applicabile se specificato nella PoE (Proof of Entitlement) del Cliente o nel Documento d'Ordine.

Verrà applicata la versione aggiornata di questo SLA in vigore all'inizio o al momento del rinnovo delle condizioni dell'abbonamento del Cliente. Il Cliente riconosce che questo SLA non costituisce una garanzia per l'utente.

1. Definizioni

a. **Contatto autorizzato** – indica la persona che il Cliente ha comunicato a IBM come autorizzata ad inoltrare eventuali Pretese ai sensi del presente SLA.

b. **Credito di Disponibilità** – indica il rimedio che IBM riconoscerà per una Richiesta di Rimedio convalidata. Il Credito di Disponibilità sarà applicato sotto forma di credito o sconto rispetto ad una fattura futura per i costi di abbonamento ai servizi IBM SaaS.

c. **Richiesta di Rimedio** – indica una richiesta inoltrata dal Contatto Autorizzato a IBM, ai sensi di questo SLA relativamente al mancato rispetto di un Livello di Servizio in un Mese Contrattuale.

d. **Mese Contrattuale** – indica ciascun mese completo durante il periodo dell'offerta IBM SaaS calcolato dalle 00:00 GMT del primo giorno del mese fino alle 23:59 GMT dell'ultimo giorno del mese.

e. **Cliente** – indica una persona giuridica che si abbona ai servizi IBM SaaS direttamente da IBM eche non sia inadempiente rispetto alle proprie obbligazioni, compresi gli obblighi di pagamentopattuiti nel contratto con IBM per i servizi IBM SaaS.

f. **Tempo di Fermo** – Indica il Tempo di Fermo dell'Applicazione e/o il Tempo di Fermo di Elaborazione In Entrataapplicabile al Livello di Servizio corrispondente mostrato nella seguente tabella. Il Tempo di Fermo non comprende il periodo di tempo in cui l'offerta IBM SaaS non è disponibile in seguito a:

- Tempo di Fermo di sistema pianificato;
- Forza Maggiore;
- Problemi con le applicazioni, attrezzature o dati di un Cliente o di terze parti;
- atti oppure omissioni del Cliente o di terzi (compreso chiunque abbia accesso ai servizi IBM SaaS tramite le password o le apparecchiature del Cliente);
- mancata adesione da parte del Cliente alle configurazioni di sistema richieste e alle piattaforme supportate per accedere all'offerta IBM SaaS; oppure
- La conformità da parte di IBM a qualsiasi progetto, specifiche o istruzioni fornite dal Cliente o da terze parti per conto del Cliente.

g. **Evento** – Indica un avvenimento o una serie di circostanze considerate nel loro complesso, che comportano un mancato rispetto del Livello di Servizio.

h. **Forza Maggiore** – Indica eventi naturali, atti di terrorismo, scioperi, incendi, inondazioni, terremoti, rivolte, guerra, atti, ordini o restrizioni governative, virus ed altri comportamenti dannosi, assenza di connettività di rete e di utilità o qualsiasi altra causa di indisponibilità dell'offerta IBM SaaS fuori dal ragionevole controllo di IBM.

i. **Tempo di Fermo di Sistema Pianificato** – Indica un'interruzione pianificata dell'offerta IBM SaaS a scopo di manutenzione.

j. **Livello di Servizio** – Indica lo standard qui di seguito stabilito con cui IBM valuta il livello di servizio fornito in questo SLA.

2. Crediti di Disponibilità

a. Per avere diritto ad inoltrare una Richiesta di Rimedio, il Cliente deve aver registrato un ticket di assistenza per ciascun Evento con l'help desk dell'IBM Customer Support per l'offerta IBM SaaS applicabile, nel rispetto della procedura IBM relativa alla notifica dei problemi per cui è necessaria un'assistenza di Severità 1. Il Cliente deve fornire nel dettaglio tutte le informazioni necessarie sull'Evento e fornire ragionevole assistenza a IBM nella diagnosi e risoluzione dell'Evento, per

quanto necessario al supporto per i ticket di Severità 1. Tale ticket deve essere registrato entro ventiquattro (24) ore dal momento in cui l'utente si rende conto che l'Evento ha avuto un impatto negativo sull'utilizzo dell'offerta IBM SaaS.

b. Il Contatto Autorizzato del Cliente deve inoltrare la Richiesta di Rimedio per un Credito di Disponibilità non più tardi di tre giorni (3) lavorativi dal termine del Mese Contrattualeoggetto della Richiesta di Rimedio.

c. Il Contatto Autorizzato del Cliente deve fornire a IBM tutti i dettagli che verranno ragionevolmente richiesti per la Richiesta di Rimedio comprese, a titolo esemplificativo e non esaustivo, le descrizioni dettagliate di tutti gli Eventi di interesse e il Livello di servizio che si sostiene non essere stato rispettato.

d. IBM valuterà internamente il tempo di fermo totale combinato durante ciascun Mese Contrattuale applicabile al Livello di Servizio corrispondentemostrato nella seguente tabella. I Crediti di Disponibilità si baseranno sulla durata del Tempo di Fermo misurata dal momento in cui è si è stati interessati dal Tempo di Fermo la prima volta. Qualora il Cliente riferisca che si sono verificati contemporaneamente un Evento di un Tempo di Fermo dell'Applicazione e un Eventodi Tempo di Fermo dell'elaborazione dei dati in entrata, IBM considererà i periodi di sovrapposizione del Tempo di Fermo come un unico periodo di Tempo di Fermo e non come due periodi separati. Per ciascuna Richiesta di Rimedio valida, IBM applicherà il più elevato Credito di disponibilità applicabile sulla base delLivello di Servizio raggiunto durante ciascun Mese Contrattuale, come mostrato nelle tabelle seguenti. IBM non sarà responsabile per più Crediti di Disponibilità inerenti agli stessi Eventi nello stesso Mese Contrattuale.

e. Per il Servizio in bundle (singoli Servizi confezionati e venduti insieme ad un unico prezzo combinato), il Credito di Disponibilità verrà calcolato sulla base del singolo prezzo mensile combinato per il Servizio in bundle e non del costo di abbonamento mensile per ciascuna singola offerta IBM SaaS. Il Cliente può inoltrare soltanto Richieste di Rimedio inerenti ad un singolo Servizio IBM SaaS di un bundle in qualsiasi Mese Contrattuale; e IBM, inoltre, non sarà responsabile per Crediti di Disponibilità relativi a più di un Servizio IBM SaaS di un bundle in qualsiasi Mese Contrattuale.

f. Se il Cliente ha acquistato i servizi IBM SaaS da un rivenditore IBM, in una transazione di rivendita in cui IBM conserva la responsabilità principale per l'adempimento degli impegni dei servizi IBM SaaS e degli SLA, allora il Credito di Disponibilità sarà calcolato sul prezzo RSVP (Relationship Suggested Value Price) per i servizi IBM SaaS, applicato in quel momento, per il Servizio in vigore durante il Mese Contrattuale oggetto della Richiesta di Rimedio, scontato del 50%.

g. I Crediti totali di Disponibilità riconosciuti rispetto ad un Mese Contrattuale non supereranno, in qualsiasi caso, il dieci percento (10%) di un dodicesimo (1/12) del costo annuale pagato dal Cliente a IBM per i servizi IBM SaaS.

h. IBM utilizzerà il proprio ragionevole giudizio per convalidare le Richieste di Rimedio sulla base delle informazioni disponibili registrate da IBM, che prevarranno in caso di eventuali discrepanze con i dati in possesso dell'utente.

i. I CREDITI DI DISPONIBILITÀ FORNITI ALL'UTENTE NEL RISPETTO DEL PRESENTE SLA SONO L'UNICO ED ESCLUSIVO RIMEDIO RISPETTO A QUALSIASI PRETESA RELATIVA AI LIVELLI DI SERVIZI.

3. Livelli di Servizio

Disponibilità dei servizi IBM SaaS in un Mese Contrattuale

Livello di Servizio raggiunto (durante 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%

Il Livello di Servizio raggiunto, espresso come percentuale, è calcolato nel seguente modo: (a) il numero totale di minuti in un Mese Contrattuale, meno (b) il numero totale di minuti di Tempo di Fermo nel Mese Contrattuale, diviso per (c) il numero totale di minuti in un Mese Contrattuale.

Esempio: 50 minuti del Tempo di Fermo totale in un Mese Contrattuale

43.200 minuti totali in un Mese Contrattuale di 30 (trenta) giorni - 50 minuti di Tempo di Fermo = 43,150 minuti _____ 43.200 minuti totali	= 2% Credito di Disponibilità per il 99,8% del Livello di Servizio raggiunto in un Mese Contrattuale

4. Esclusioni dal Servizio

Il presente SLA è stato reso disponibile per i Clienti IBM. Il presente SLA non si applica nei seguenti casi:

- Servizi beta e di prova.
- Gli ambienti di non-produzione, inclusi a titolo esemplificativo ma non esaustivo, gli ambienti di test, disaster recovery, controllo qualità o sviluppo.
- Le richieste di rimedio effettuate dagli utenti, gli ospiti, i partecipanti e gli invitati autorizzati del Cliente IBM relativamente ai servizi IBM SaaS.
- Prerequisiti Software

Accettato da:

_____

Firma e timbro del Cliente

Data:

Ai sensi degli artt. 1341 e 1342 del Codice Civile Italiano, il Cliente accetta espressamente i seguenti articoli del presente documento: “Rinnovo Automatico”; “Fatturazione Continuativa”; “Rinnovo su Richiesta”; “Cookies”; “Crediti di disponibilità”

_____

Firma e timbro del Cliente

Data: