

Conditions d'Utilisation IBM – Conditions Spécifiques de l'Offre SaaS

IBM MobileFirst Protect (SaaS)

Les Conditions d'Utilisation regroupent les présentes Conditions d'Utilisation IBM – Conditions Spécifiques de l'Offre SaaS (« Conditions Spécifiques de l'Offre SaaS ») et un document intitulé Conditions d'Utilisation IBM – Conditions Générales (« Conditions Générales ») disponibles à l'adresse URL suivante : <http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/>.

En cas de conflit, les Conditions Spécifiques de l'Offre SaaS prévalent sur les Conditions Générales. En accédant à l'Offre IBM SaaS, en la commandant ou en l'utilisant, le Client de l'Offre IBM SaaS accepte les présentes Conditions d'Utilisation.

Les Conditions d'Utilisation sont régies par le Contrat International IBM Passport Advantage, le Contrat International IBM Passport Advantage Express ou le Contrat International IBM relatif à une Sélection d'Offres IBM SaaS, selon le cas (ci-après le « Contrat ») qui, avec les Conditions d'Utilisation, représentent l'intégralité de l'accord entre les parties.

1. Offres IBM SaaS

Les Conditions Spécifiques de l'Offre SaaS s'appliquent aux Offres IBM SaaS suivantes :

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

- IBM MobileFirst Protect – Productivity Suite (SaaS)
- IBM MobileFirst Protect – Productivity Suite (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Secure Mail (SaaS)
- IBM MobileFirst Protect – Secure Mail (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Gateway Suite (SaaS)
- IBM MobileFirst Protect – Gateway Suite (SaaS) Step up for existing customers
- IBM MobileFirst Protect – Content Suite (SaaS)
- IBM MobileFirst Protect – Content Suite (SaaS) Step up for existing customers
- 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)

2. IBM MaaS360 Professional Bundle Prime (SaaS) Charge Metrics

L'Offre IBM SaaS est vendue en fonction d'une des unités de mesure de redevance suivantes dans le Document de Transaction :

- a. **Utilisateur Autorisé** : unité de mesure par laquelle l'Offre IBM SaaS peut être acquise. Le Client doit se procurer des droits d'utilisation distincts et dédiés pour chaque Utilisateur Autorisé unique ayant reçu l'accès à l'Offre IBM SaaS directement ou indirectement (par exemple, via un logiciel de multiplexage, un périphérique ou un serveur d'applications), par quelque moyen que ce soit. Des droits d'utilisation suffisants sont nécessaires pour couvrir le nombre d'Utilisateurs Autorisés ayant reçu l'accès à l'Offre IBM SaaS pendant la période de mesure indiquée dans l'Autorisation d'Utilisation ou le Document de Transaction du Client.
- b. **Gigaoctet** : unité de mesure par laquelle l'Offre IBM SaaS peut être acquise. Un Gigaoctet représente 2 puissance 30 d'octets de données (soit 1 073 741 824 octets). Des droits d'utilisation suffisants sont nécessaires pour couvrir le nombre total de Gigaoctets traités par l'Offre IBM SaaS pendant la période de mesure indiquée dans l'Autorisation d'Utilisation (ou « PoE ») ou le Document de Transaction du Client.
- c. **Unité Client Gérée** : unité de mesure par laquelle l'Offre IBM SaaS peut être acquise. Une Unité Client est un système informatique utilisateur unique ou un capteur spécial ou une unité de télémétrie demandant l'exécution de, ou recevant à des fins d'exécution, un ensemble de commandes, de procédures ou d'applications à partir de ou fournissant des données à un autre système informatique qui est généralement désigné par serveur ou géré par le serveur. Plusieurs Unités Client peuvent partager l'accès à un serveur commun. Une Unité Client peut être dotée de certaines fonctionnalités de traitement ou peut être programmable afin de permettre à un utilisateur d'effectuer le travail. Le Client doit se procurer des droits d'utilisation pour chaque Unité Client gérée par l'Offre IBM SaaS pendant la période de mesure indiquée dans une Autorisation d'Utilisation ou un Document de Transaction du Client.
- d. **Unité Client** : unité de mesure par laquelle l'Offre IBM SaaS peut être acquise. Une Unité Client est un système informatique utilisateur unique ou un capteur spécial ou une unité de télémétrie demandant l'exécution de, ou recevant à des fins d'exécution, un ensemble de commandes, de procédures ou d'applications à partir de ou fournissant des données à un autre système informatique qui est généralement désigné par serveur ou géré par le serveur. Plusieurs Unités

Client peuvent partager l'accès à un serveur commun. Une Unité Client peut être dotée de certaines fonctionnalités de traitement ou peut être programmable afin de permettre à un utilisateur d'effectuer le travail. Le Client doit se procurer des droits d'utilisation pour chaque Unité Client qui exécute l'Offre IBM SaaS, lui fournit des données, utilise des services fournis par l'Offre IBM SaaS ou autrement accède à l'Offre IBM SaaS pendant la période de mesure indiquée dans l'Autorisation d'Utilisation (PoE) ou le Document de Transaction du Client.

3. Redevances et facturation

Le montant à régler pour l'Offre IBM SaaS est indiqué dans un Document de Transaction.

3.1 Redevances Mensuelles Partielles

Une Redevance Mensuelle Partielle, comme indiqué dans le Document de Transaction, peut être estimée au prorata.

3.2 Redevances de dépassement

Si l'utilisation réelle de l'Offre IBM SaaS par le Client pendant la période de mesure dépasse les droits indiqués dans l'Autorisation d'Utilisation (ou « PoE »), le Client sera facturé pour l'excédent, comme stipulé dans le Document de Transaction.

4. Options de Renouvellement de la Période d'Abonnement à l'Offre IBM SaaS

L'Autorisation d'Utilisation du Client indiquera si l'Offre IBM SaaS sera renouvelée à la fin de la Période d'Abonnement, en désignant l'une des options suivantes :

4.1 Renouvellement automatique

Si l'Autorisation d'Utilisation du Client indique que le renouvellement est automatique, le Client est autorisé, moyennant une demande écrite adressée à l'Ingénieur commercial IBM ou au Partenaire Commercial IBM du Client, à résilier la Période d'Abonnement à l'Offre IBM SaaS arrivant à expiration, au moins quatre-vingt-dix (90) jours avant la date d'expiration, comme indiqué dans l'Autorisation d'Utilisation. Si IBM ou son Partenaire Commercial IBM ne reçoit pas ladite notification de résiliation avant la date d'expiration, la Période d'Abonnement arrivant à expiration sera automatiquement renouvelée pour un an ou pour la même durée que celle de la Période d'Abonnement d'origine, telle qu'elle est stipulée dans l'Autorisation d'Utilisation.

LA QUANTITÉ D'AUTORISATIONS DE RENOUVELLEMENT SERA ÉGALE A LA VALEUR LA PLUS ÉLEVÉE ENTRE LA QUANTITÉ DE COMMANDES D'ORIGINE OU L'UTILISATION MENSUELLE SIGNALÉE POUR LE MOIS AVANT LA GÉNÉRATION DE LA FACTURE DE RENOUVELLEMENT, SAUF SI IBM REÇOIT UNE NOTIFICATION INDIQUANT UNE QUANTITÉ D'AUTORISATIONS DIFFÉRENTE.

LA QUANTITÉ D'AUTORISATIONS DE RENOUVELLEMENT POUR L'OFFRE STEP UP SERA ÉGALE A LA QUANTITÉ DE COMMANDES D'ORIGINE.

4.2 Facturation continue

Lorsque l'Autorisation d'Utilisation indique que le renouvellement du Client est continu, le Client continuera d'avoir accès à l'Offre IBM SaaS et sera facturé pour l'utilisation de l'Offre IBM SaaS en continu. Pour cesser d'utiliser l'Offre IBM SaaS et d'arrêter le processus de facturation continue, le Client doit fournir à IBM ou à son Partenaire Commercial IBM une notification écrite de quatre-vingt-dix (90) jours demandant l'annulation de son Offre IBM SaaS. Une fois l'accès du Client annulé, le Client sera facturé pour toutes les redevances d'accès impayées jusqu'au mois au cours duquel l'annulation a pris effet.

4.3 Renouvellement Requis

Lorsque l'Autorisation d'Utilisation indique que le renouvellement du Client est de type « résiliation », l'Offre IBM SaaS sera résiliée à la fin de la Période d'Abonnement et l'accès du Client à l'Offre IBM SaaS sera supprimé. Pour continuer d'utiliser l'Offre IBM SaaS au-delà de la date de fin, le Client doit passer une commande auprès de l'ingénieur commercial IBM ou du Partenaire Commercial IBM du Client pour acheter une nouvelle Période d'Abonnement.

5. Support Technique

Le support technique de l'Offre IBM SaaS est un support de deuxième niveau structuré destiné à l'équipe des opérations du Client, et non aux Utilisateurs finaux, et est disponible pendant la période d'abonnement.

Le support est fourni par le biais de plusieurs canaux, 24 heures sur 24 et 7 jours sur 7. Des informations relatives au support de la solution IBM SaaS sont disponibles sur le portail du produit.

Objectifs de réactivité prévus :

Niveau de Gravité	Définition de la Gravité	Objectifs de Temps de Réponse	Couverture de Temps de Réponse
1	Impact critique sur les activités/indisponibilité du service : Une fonctionnalité critique est inutilisable ou une interface critique est défaillante. Cela s'applique généralement à un environnement de production et indique l'impossibilité d'accès aux services, ce qui donne lieu à un impact critique sur les opérations. Cette condition nécessite une solution immédiate.	30 minutes	24 heures sur 24 et 7 jours sur 7
2	Impact élevé sur les activités : L'utilisation d'un dispositif ou d'une fonction du service est gravement restreinte ou le Client risque de ne pas respecter des délais.	1 heure ouvrable	24h/24 et 7j/7
3	Impact moyen sur les activités : Indique que le service ou la fonctionnalité est utilisable et qu'il ne s'agit pas d'un impact critique sur les opérations.	2 heures ouvrables	24h/24 et 7j/7
4	Impact faible sur les activités : Une demande d'information ou une demande non technique	3 heures ouvrables	24h/24 et 7j/7

6. Dispositions supplémentaires spécifiques à l'Offre IBM SaaS

6.1 Limitation de l'Offre Step up

Pour les Offres IBM SaaS désignées par « Step up for existing Customers » (« Step up SaaS »), le Client doit avoir acquis au préalable ou simultanément des autorisations de licence appropriées du logiciel IBM associé, comme identifié dans le nom de l'Offre Step up SaaS. Par exemple, le Client qui achète « IBM MobileFirst Protect – Devices (SaaS) Step up for existing customers » doit disposer d'autorisations de licence pour le logiciel IBM associé d'IBM MobileFirst. Les droits d'accès du Client à l'Offre Step up SaaS ne peuvent pas dépasser les droits d'accès du Client au logiciel IBM associé.

Lors de l'acquisition de l'Offre Step up SaaS, le Client n'est pas autorisé à utiliser les mêmes autorisations de licence du logiciel IBM associé dans son environnement installé sur site qu'avec les droits d'accès à l'Offre Step up SaaS. Par exemple, si le Client dispose de 250 droits d'utilisation d'Unité Client Gérée pour le logiciel IBM associé et qu'il choisit d'acquérir 100 droits d'utilisation d'Unité Client Gérée Step up SaaS, le Client peut gérer 100 Unités Client Gérées Step up SaaS à partir de l'environnement de l'Offre IBM SaaS et 150 Unités Client Gérées à partir du logiciel installé sur site.

Le Client déclare qu'il a acquis (1) les autorisations de licence applicables et (2) l'Abonnement et le Support du(es) Logiciel(s) IBM associé(s). Pendant la Période d'Abonnement à l'Offre Step up SaaS, le Client doit tenir à jour l'Abonnement et le Support pour les autorisations d'utilisation de logiciel IBM utilisées conjointement avec les autorisations d'utilisation de l'Offre Step up SaaS. En cas de résiliation de la licence d'utilisation du(es) logiciel(s) IBM associé(s) du Client ou de son Contrat d'Abonnement et de Support pour le(s) logiciel(s) IBM associé(s), son droit d'utilisation de l'Offre Step Up SaaS prend fin.

6.2 Cookies

Le Client accepte qu'IBM puisse utiliser des cookies et des technologies de suivi permettant de rassembler des informations identifiant une personne, dans le cadre de la collecte de statistiques et d'informations d'utilisation conçues pour aider à améliorer l'acquis utilisateur et/ou pour personnaliser les

interactions avec les utilisateurs conformément au site <http://www-01.ibm.com/software/info/product-privacy/index.html>.

6.3 Transferts hors du Territoire

Si le Client communique des Informations Personnelles aux Offres IBM SaaS dans des Etats Membres de l'Union Européenne ou dans les pays suivants : Islande, Liechtenstein, Norvège, Suisse, Turquie et tout autre pays européen disposant d'une législation protégeant la confidentialité des données, le Client accepte qu'IBM traite le Contenu, y compris toutes Informations Personnelles, en vertu des lois et obligations applicables, hors du territoire à destination de sous-traitants ou sous-traitants ultérieurs du traitement des données dans les pays suivants hors de l'Espace Économique Européen et dans les pays considérés par la Commission Européenne comme ayant des niveaux de sécurité adéquats :

Nom du Sous-traitant/Sous-traitant ultérieur du traitement des données	Rôle (Sous-traitant/Sous-traitant ultérieur du traitement des données)	Etablissement
IBM Corporation	Sous-traitant ultérieur du traitement de données	1 New Orchard Rd. Armonk, NY 10504, USA I
IBM India Private Limited	Sous-traitant ultérieur du traitement de données	No. 12, Subramanya Arcade Bannerghatta Road, Bangalore 560029 Inde

Le Client accepte qu'IBM pourra, sur préavis, modifier cette liste de pays d'implantation lorsqu'elle juge cela raisonnablement nécessaire pour la fourniture de l'Offre IBM SaaS.

6.4 Confidentialité des Données dans l'Union Européenne

Si le Client communique des Données à caractère personnel aux Offres IBM SaaS dans les États Membres de l'Union Européenne, en Islande, au Liechtenstein, en Norvège, en Suisse ou en Turquie et tout autre pays européen disposant d'une législation protégeant la confidentialité des données, ou si le Client dispose d'unités ou d'utilisateurs autorisés dans ces pays, le Client, en tant que seul responsable du traitement désigne IBM en tant que sous-traitant du traitement des données pour traiter (ces termes étant définis dans la Directive EU 95/46/EC) les Informations Personnelles. IBM ne traitera ces Informations Personnelles que dans les limites requises pour mettre à disposition l'Offre IBM SaaS conformément aux descriptions publiées d'IBM de l'Offre IBM SaaS et le Client convient que ledit traitement est conforme aux instructions du Client.

6.5 Conformité Safe Harbor

Les Offres IBM SaaS sont incluses dans la certification US - EU Safe Harbor de Fiberlink Communications Corporation (Filiale d'IBM). IBM et Fiberlink se soumettent toutes deux au cadre US - EU Safe Harbor établi par le Département du Commerce des États-Unis d'Amérique concernant la collecte, l'utilisation et la conservation des informations collectées dans l'Union Européenne. Pour plus d'informations sur ces principes de Safe Harbor ou pour accéder à l'attestation de sécurité de Fiberlink, rendez-vous sur le site <http://www.export.gov/safeharbor/>.

Lorsque le principe américano-européen (US-EU) de Safe Harbor ne s'applique pas à un transfert d'Informations Personnelles dans l'EEE (Espace Economique Européen), les parties ou leurs sociétés affiliées concernées pourront conclure les Clauses Contractuelles Types de la Commission européenne non modifiées applicables, conformément à la Décision 2010/87/EU de la Commission européenne, en supprimant les clauses facultatives. Tout différend ou obligation découlant de ces contrats, même s'ils sont conclus par des sociétés affiliées, sera traité comme si le différend ou l'obligation existait entre les parties au titre du présent Contrat.

6.6 Sites bénéficiaires dérivés

Le cas échéant, les taxes sont fonction du(es) site(s) que le Client identifie comme bénéficiant de l'Offre IBM SaaS. IBM appliquera les taxes en fonction de l'adresse indiquée lors de la commande d'une Offre IBM SaaS comme étant le site bénéficiaire principal, sauf si le Client fournit des informations supplémentaires à IBM. Le Client est responsable de la mise à jour de ces informations et est tenu de fournir les éventuelles informations à IBM.

6.7 Données Normatives

Nonobstant toute disposition contraire, uniquement à des fins de recherche normative, d'analyse, de démonstration et de production de rapports, IBM est autorisée à conserver et utiliser au format anonyme agrégé (de sorte que le Client ou les utilisateurs autorisés du Client ne puissent pas être identifiés comme source des données et que les informations personnelles permettant l'identification du Client ou des utilisateurs autorisés du Client soient supprimées) les données reflétant les expériences individuelles des utilisateurs autorisés du Client avec l'Offre IBM SaaS.

6.8 Utilisation et Autorisation Légales

6.8.1 Autorisation de Collecte et de Traitement de Données

L'Offre IBM SaaS est conçue pour mettre à disposition, gérer, sécuriser, surveiller et contrôler des appareils mobiles. L'Offre IBM SaaS collectera des informations auprès des utilisateurs et des unités qui sont autorisés par le Client à interagir avec l'Offre IBM SaaS à laquelle le Client a souscrit. L'Offre IBM SaaS collecte des informations qui, seules ou conjointement, peuvent être considérées comme Informations Personnelles dans certaines juridictions. Les données collectées peuvent inclure le nom, le numéro de téléphone, l'adresse e-mail enregistrée et l'emplacement de l'appareil de l'utilisateur autorisé, l'historique de la navigation sécurisée et des ID utilisateur, des informations relatives au matériel, aux logiciels et aux paramètres de l'appareil de l'utilisateur final, ainsi que des informations générées par l'appareil. Le Client autorise IBM à collecter, traiter et utiliser ces informations conformément aux dispositions des présentes Conditions d'Utilisation.

6.8.2 Consentement en Connaissance de Cause des Personnes Concernées

L'utilisation de l'Offre IBM SaaS peut être soumise à diverses lois et réglementations. L'Offre IBM SaaS ne peut être utilisée qu'à des fins légales et de manière légale. Le Client s'engage à utiliser l'Offre IBM SaaS conformément aux lois, règlements et réglementations applicables et assume toutes les responsabilités relatives au respect desdites lois, règlements et réglementations.

Le Client convient qu'il a obtenu ou qu'il obtiendra tous les consentements, autorisations ou licences en pleine connaissance de cause, nécessaires pour permettre l'utilisation légale de l'Offre IBM SaaS et pour permettre la collecte et le traitement des informations par IBM en tant que sous-traitant du traitement des données du Client par le biais de l'Offre IBM SaaS. Le Client autorise IBM par les présentes à obtenir des consentements en pleine connaissance de cause, nécessaires pour permettre l'utilisation de l'Offre IBM SaaS et pour collecter et traiter les informations décrites dans le contrat de licence d'utilisateur final disponible sur le site <http://www.ibm.com/software/sla/sladb.nsf/>.

6.9 Conservation des Données

IBM supprimera toute information collectée pouvant inclure des Informations Personnelles à l'expiration ou la résiliation des présentes Conditions d'Utilisation, à l'exception des informations devant être conservées pour les raisons citées plus haut ou conformément à une loi, règle ou réglementation applicable. Dans ce cas, IBM conservera les informations collectées pendant la durée requise par ladite cause, loi, règle ou réglementation applicable.

Annexe A

MobileFirst Protect est une plateforme cloud facile à utiliser dotée de toutes les fonctionnalités essentielles permettant la gestion de bout en bout des appareils mobiles actuels, y compris iPhone, iPad, Android, Kindle Fire, Windows Phones et smartphones BlackBerry. Voici une brève description des Offres IBM SaaS :

1. **IBM MobileFirst Protect – Devices (SaaS)**

Les fonctions de gestion d'appareil de mobilité principales (MDM) comprennent l'enregistrement et la configuration des appareils, la gestion de la stratégie de sécurité et les actions d'appareil, telles que l'envoi de message, la localisation, le verrouillage et l'effacement. Les fonctions MDM avancées comprennent les règles de conformité automatisées, les paramètres de confidentialité BYOD (bring your own device) et la génération de rapports et les tableaux de bord Mobility Intelligence.

2. **IBM MobileFirst Protect – Applications (SaaS)**

MobileFirst Protect Applications permet d'ajouter des applications et de les distribuer aux appareils pris en charge gérés par MobileFirst Protect. Il s'agit notamment de MobileFirst Protect App Catalog, une application permettant aux utilisateurs de consulter et d'installer des applications gérées et de recevoir des alertes relatives aux applications gérées mises à jour.

3. **IBM MobileFirst Protect – Application Security (SaaS)**

MobileFirst Protect Application Security permet une protection de données supplémentaire pour les applications d'entreprise utilisant le SDK WorkPlace pendant le développement, ou permet aux applications iOS de télécharger facilement l'application (.ipa), de l'associer à un profil d'application des accès et d'intégrer automatiquement un certificat signataire. Mobile Application Security intègre l'application à Secure Productivity Suite. Cela permet la connexion unique, l'accès Intranet via la passerelle d'entreprise mobile et l'application des paramètres de sécurité de données.

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

MobileFirst Protect Gateway for Apps permet aux utilisateurs situés hors du réseau d'entreprise d'accéder directement et en toute sécurité aux ressources d'application internes sans qu'une connexion VPN de niveau appareil intégral nécessaire.

5. **IBM MobileFirst Protect – Content (SaaS)**

MobileFirst Protect Content permet à l'administrateur d'ajouter et de distribuer des documents aux appareils pris en charge gérés par IBM MobileFirst Protect Devices. Il comprend notamment IBM MobileFirst Protect Doc Catalogue, un conteneur d'appareil protégé par mot de passe qui fournit aux utilisateurs un moyen sécurisé et simple pour consulter et partager des documents et y accéder. Il inclut l'accès direct aux contenus et référentiels distribués tels que SharePoint, Box et Google Drive. L'accès aux partages de fichiers SharePoint et Windows privés est disponible à l'aide de MobileFirst Protect Mobile Enterprise Gateway. Les documents gérés par le biais de MobileFirst Protect peuvent être soumis au contrôle des versions, audités et sécurisés via des options de règle de prévention de perte de données (DLP), notamment l'authentification obligatoire, la fonctionnalité de restriction des fonctions de Copier/Coller et l'interdiction d'ouverture ou de partage dans d'autres applications.

6. **IBM MobileFirst Protect – Document Sync (SaaS)**

MobileFirst Protect Document Sync permet aux utilisateurs de synchroniser aisément et en toute sécurité le contenu d'utilisateur entre les appareils mobiles gérés. Les administrateurs peuvent garantir que les règles telles que la restriction des fonctions Couper/Copier/Coller et l'interdiction d'ouverture ou de partage de contenu dans d'autres applications sont en place pour le contenu utilisateur d'un appareil à l'autre. Le contenu est stocké de manière sécurisée, tant dans le Cloud que sur l'appareil, et n'est accessible que via MobileFirst Protect Doc Catalogue.

7. **IBM MobileFirst Protect – Document Editor (SaaS)**

MobileFirst Protect Document Editor est une puissante suite bureautique qui permet aux utilisateurs de gérer des documents professionnels pendant qu'ils sont en déplacement. MobileFirst Protect Secure Editor permet les fonctions suivantes :

- Création et édition de fichiers .DOC, .PPT et .XLS

- Mode de présentation pour les diapositives
- Gestion simplifiée des pièces jointes d'e-mail et d'autres fichiers issus de MobileFirst Protect pour iOS

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

MobileFirst Protect Gateway for Documents permet aux entreprises d'utiliser MobileFirst Protect Content pour fournir aux appareils situés hors du réseau d'entreprise l'accès direct sécurisé aux sites Connexions internes, aux sites SharePoint, à Windows File Shares et à d'autres magasins de fichiers sans qu'une connexion VPN de niveau appareil intégral soit nécessaire. MobileFirst Protect Gateway for Documents requiert l'achat de MobileFirst Protect Content. Il prend en charge iOS 5.0 et Android 4.0 ou version ultérieure.

9. IBM MobileFirst Protect – Email Management (SaaS)

MobileFirst Protect Email Management comprend des fonctionnalités clés à l'appui de Microsoft Exchange ActiveSync et Lotus Traveler.

- Exchange ActiveSync : permet la prise en charge des appareils mobiles se connectant à Microsoft Exchange via le protocole ActiveSync. Il comprend des fonctionnalités telles que les fonctions principales de gestion d'appareil mobile, par exemple la configuration des appareils, la création, l'application des règles ActiveSync (code d'accès, blocage ou autorisation d'accès à la messagerie électronique), et l'exécution d'actions liées aux appareils, telles que le verrouillage et l'effacement, ainsi que la génération de rapport détaillé sur les attributs des appareils.
- Lotus Traveler : permet la prise en charge des appareils mobiles se connectant à IBM Lotus Notes® via le protocole Lotus Traveler. Il comprend des fonctionnalités telles que la configuration des appareils, le blocage ou l'autorisation d'appareils, l'application des règles de gestion de code d'accès, l'effacement des appareils et la génération de rapport détaillé sur les attributs des appareils.

10. IBM MobileFirst Protect – Browser (SaaS)

MobileFirst Protect Browser est un navigateur Web complet permettant l'accès sécurisé aux sites intranet d'entreprise et mettant en application la conformité des règles de contenu en définissant des stratégies de sécurité et de filtrage de site Web pour garantir que les utilisateurs n'accèdent qu'à du contenu Web approuvé en fonction d'un certain nombre de catégories de contenu, telles que les réseaux sociaux, les sites explicites ou malveillants. Il comprend la fonction de désactivation des navigateurs Web natifs et tiers par le biais de la stratégie d'application ou du placement sur liste noire, lorsqu'il est associé à MobileFirst Protect Devices. Il permet de créer des listes blanches définissant des exceptions aux sites Web, de restreindre les cookies, de copier, de coller et d'imprimer les fonctionnalités et d'activer le mode Kiosk.

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

MobileFirst Protect Gateway for Browser permet aux appareils pris en charge d'accéder aux sites Web internes approuvés sans qu'une connexion VPN de niveau appareil intégral soit nécessaire.

12. IBM MobileFirst Protect for BlackBerry (SaaS)

Permet la prise en charge des appareils mobiles connectés au BlackBerry Enterprise Server (BES) en utilisant des API BlackBerry. Les fonctionnalités incluses sont les actions distantes telles que l'envoi d'un message, la réinitialisation du code d'accès, l'affectation de règle BES et l'effacement, ainsi que la génération de rapport détaillé sur les attributs des appareils. L'installation de MobileFirst Protect Cloud Extender est obligatoire. Disponible uniquement pour les appareils consultés ou gérés avec MobileFirst Protect via BES 5.0.

13. IBM MobileFirst Protect – Expenses (SaaS)

MobileFirst Protect Expenses permet à l'administrateur de créer des politiques d'utilisation de données et de les affecter aux appareils pris en charge gérés par MobileFirst Protect, et d'affecter ces politiques à un niveau d'appareil, de groupe ou global et de configurer des seuils d'alerte et la messagerie pour l'utilisation des données tant dans le réseau qu'en itinérance.

14. IBM MobileFirst Protect – Management Suite (SaaS)

Suite de produits incluant MobileFirst Protect Devices, MobileFirst Protect Applications, MobileFirst Protect Content et MobileFirst Protect Expenses.

15. IBM MobileFirst Protect – Productivity Suite (SaaS)

Suite de produits incluant MobileFirst Protect Secure Mail, MobileFirst Protect Applications, MobileFirst Protect Application Security, MobileFirst Protect Content et MobileFirst Protect Browser.

16. IBM MobileFirst Protect – Secure Mail (SaaS)

MobileFirst Protect Secure Mail fournit une application de productivité bureautique distincte et sécurisée permettant aux utilisateurs d'accéder et de gérer la messagerie, l'agenda et les contacts avec la possibilité de contrôler les e-mails et les pièces jointes pour empêcher la fuite de données en limitant le réacheminement ou le déplacement de contenu vers d'autres applications, d'appliquer l'authentification, de restreindre les fonctions Couper/Copier/Coller et de verrouiller les pièces jointes des e-mail à des fins de consultation uniquement.

17. IBM MobileFirst Protect – Gateway Suite (SaaS)

MobileFirst Protect Gateway Suite permet aux applications prises en charge sur iOS et Android de communiquer de manière sécurisée et transparente avec les ressources du réseau interne de l'entreprise.

18. IBM MobileFirst Protect – Content Suite (SaaS)

Suite de produits incluant MobileFirst Protect Content, MobileFirst Protect Document Editor et MobileFirst Protect Document Sync.

19. IBM MobileFirst Protect – Threat Management (SaaS)

MobileFirst Protect Threat Management permet la sécurité mobile améliorée, à l'aide de la détection de logiciel malveillant mobile et de la détection de jailbreak/root avancée. À l'aide de MobileFirst Protect Threat Management, le Client pourra définir et gérer les règles de conformité relatives aux logiciels malveillants et autres vulnérabilités de sécurité détectés.

20. IBM MobileFirst Protect – Content Service (SaaS)

MobileFirst Protect Content Service (SaaS) permet aux utilisateurs de télécharger des documents et des packages d'application vers le système de distribution de contenu de MobileFirst Protect.

Les clients disposant de MobileFirst Protect Content Service devront également acquérir au moins une autorisation d'utilisation pour MobileFirst Protect Content Service Storage (SaaS) et MobileFirst Protect Content Service Bandwidth (SaaS).

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

MobileFirst Protect Content Service Storage (SaaS) permet aux utilisateurs d'acheter un espace de stockage de données total disponible pour MobileFirst Protect Content Service (SaaS).

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

MobileFirst Protect Content Service Bandwidth (SaaS) permet aux utilisateurs d'acheter la totalité de la largeur de bande disponible pour MobileFirst Protect Content Service (SaaS).

23. IBM MobileFirst Protect – Professional (SaaS)

Dédiée aux PME, cette offre permet de configurer à distance d'une manière rapide et simple des smartphones et des tablettes, de mettre en œuvre des règles de sécurité, de publier des applications et des documents et de protéger les données des appareils personnels et professionnels des employés. Le Client bénéficie de toutes les fonctions de gestion d'appareils mobiles dont son entreprise a besoin rapidement, facilement et à prix raisonnable.

24. IBM MobileFirst Protect – Laptop (SaaS)

Permet d'inscrire, de configurer, de gérer, de sécuriser et de surveiller tous les appareils OS X et Windows du Client ainsi que ses smartphones et tablettes. Le Client peut gérer les profils et les règles de sécurité de manière cohérente entre les unités appartenant à l'entreprise et celles appartenant aux employés à l'aide de la même console de gestion MobileFirst Protect.

24.1 Windows

MobileFirst Protect – Laptop (SaaS) pour PC Windows fournit des informations sur les abonnements et les ressources gérées ainsi que sur le matériel, le système d'exploitation et les logiciels en cours d'utilisation. Le module de génération de rapports sur la sécurité des points d'extrémité fournit des

analyses de données et des rapports interactifs sur les applications fournies par le Client, par exemple les solutions anti-virus, les solutions de restauration/reprise après incident, de chiffrement de données et de pare-feu personnel, ainsi que sur les correctifs de système d'exploitation manquants. Le module de protection des données fournit des analyses de données et des rapports interactifs pour les services de sécurité, notamment le chiffrement de données, la prévention des fuites de données, la restauration/reprise après incident et autres d'applications intégrées. Les systèmes d'exploitation pris en charge sont Windows XP SP3, Windows Vista, Windows 7, Windows 8+ et Windows 8+ Pro (versions 32 et 64 bits).

Les actions réalisables avec les unités sont les suivantes :

- Envoyer un message à l'unité
- Verrouiller l'unité
- Localiser l'unité (requiert MobileFirst Protect Laptop Location)
- Arrêter, démarrer, redémarrer l'unité
- Eteindre et réamorcer l'unité
- Nettoyer le disque dur
- Configurer les paramètres des correctifs
- Distribuer des logiciels

24.2 Mac OS X

MobileFirst Protect – Laptop (SaaS) pour Mac OS X fournit des informations sur les abonnements et les ressources gérées ainsi que sur le matériel, le système d'exploitation et les logiciels en cours d'utilisation. Le module de génération de rapports sur la sécurité des points d'extrémité fournit des analyses de données et des rapports interactifs sur les applications fournies par le Client, par exemple les solutions anti-virus, les solutions de restauration/reprise après incident, de chiffrement de données et de pare-feu personnel, ainsi que sur les correctifs de système d'exploitation manquants. Le module de protection des données fournit des analyses de données et des rapports interactifs pour les services de sécurité, notamment le chiffrement de données. Le module de gestion des configurations permet de gérer à distance un certain nombre de paramètres d'utilisateur et d'unité, notamment pour les mots de passe, le courrier électronique, les réseaux privés virtuels et le Wi-Fi. Les systèmes d'exploitation pris en charge sont Mac OS X version 10.7.3 et les versions ultérieures.

Les actions réalisables avec les unités sont les suivantes :

- Verrouiller l'unité
- Nettoyer le disque dur
- Modifier les règles d'administration des unités

25. IBM MobileFirst Protect – Laptop Location (SaaS)

MobileFirst Protect Laptop Location (SaaS) permet de localiser les tablettes et les ordinateurs portables pris en charge. MobileFirst Protect communique les coordonnées de l'adresse IP ou du réseau Wi-Fi et convertit ces données en une adresse facile à identifier. L'emplacement actuel d'une unité peut être identifié dès lors que cette unité est connectée. MobileFirst Protect consigne les emplacements successivement identifiés et peut fournir un historique de ces emplacements. Requiert IBM MobileFirst Protect Laptop (SaaS) for Windows. Les systèmes d'exploitation pris en charge sont Windows XP SP3, Windows Vista, Windows 7, Windows 8+ et Windows 8+ Pro (versions 32 et 64 bits).

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

Comprend les fonctions de l'offre MobileFirst Protect – Laptop (SaaS) et les fonctionnalités supplémentaires suivantes :

- Permet de télécharger des modules vers la plate-forme MobileFirst Protect Content Service (SaaS) et de planifier la distribution des charges aux unités gérées par le service MobileFirst Protect Laptop (SaaS) pour Microsoft Windows. Le Client peut contrôler tous les aspects de la distribution, dont les instructions d'installation, et le ciblage au niveau d'une unité, d'un groupe d'unités ou d'un ensemble. Il revient au Client de créer tous les fichiers d'installation et de conditionnement. IBM ne fournit pas d'assistance pour créer les modules d'installation.

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

Permet de gérer les profils et les règles de sécurité de manière cohérente entre les unités appartenant à l'entreprise et celles appartenant aux employés à l'aide de la console de gestion.

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

Inclut IBM MobileFirst Protect – Devices (SaaS), IBM MobileFirst Protect – Applications (SaaS), IBM MobileFirst Protect – Content (SaaS) et IBM MobileFirst Protect – Expenses (SaaS).

29. IBM MaaS360 Secure Productivity Suite Prime (SaaS)

Inclut IBM MobileFirst Protect – Secure Mail (SaaS), IBM MobileFirst Protect – Applications (SaaS), IBM MobileFirst Protect – Application Security (SaaS), IBM MobileFirst Protect – Content (SaaS) et IBM MobileFirst Protect – Browser (SaaS).

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

Inclut IBM MobileFirst Protect – Content (SaaS), IBM MobileFirst Protect – Document Editor (SaaS), IBM MobileFirst Protect – Document Sync (SaaS) et IBM MobileFirst Protect – Content (SaaS).

31. IBM MaaS360 Professional Bundle Prime (SaaS)

Dédiée aux PME, cette offre permet de configurer à distance des smartphones et des tablettes, de mettre en œuvre des règles de sécurité, de publier des applications et des documents et de protéger les données des appareils personnels et professionnels des employés.

Annexe B

L'Accord relatif aux Niveaux de Service de disponibilité (ou « SLA ») suivant est fourni pour l'Offre IBM SaaS et s'applique exclusivement s'il est spécifié dans l'Autorisation d'Utilisation (« PoE ») ou le Document de Transaction du Client.

La version du présent Accord relatif aux Niveaux de Service en vigueur à la date de commencement ou de renouvellement de l'abonnement du Client s'appliquera. Le Client reconnaît que l'Accord relatif aux Niveaux de Service ne constitue pas une garantie pour le Client.

1. Définitions

- a. **Contact Agréé** : signifie la personne que le Client a indiquée à IBM, autorisée à soumettre des Réclamations aux termes du présent Accord relatif aux Niveaux de Service.
- b. **Crédit de Disponibilité** : signifie la réparation fournie par IBM pour une Réclamation validée. Le Crédit de Disponibilité sera appliqué sous la forme d'un avoir ou d'une remise sur une future facture des redevances d'abonnement à l'Offre IBM SaaS.
- c. **Réclamation** : signifie une réclamation soumise par le Contact Agréé du Client à IBM, conformément au présent Accord relatif aux Niveaux de Service, selon laquelle un Niveau de Service n'a pas été satisfait pendant un Mois contractuel.
- d. **Mois Contractuel** : signifie chaque mois complet pendant la durée de l'Offre IBM SaaS, mesuré entre le premier jour du mois à minuit (heure GMT) et le dernier jour du mois à 23h59 (heure GMT).
- e. **Client** : signifie une entité souscrivant à l'Offre IBM SaaS directement auprès d'IBM et qui ne manque pas à ses obligations substantielles, y compris ses obligations de paiement, au titre de son contrat avec IBM pour l'Offre IBM SaaS.
- f. **Durée d'Indisponibilité** : signifie Temps d'Arrêt des Applications et/ou Temps d'Arrêt du Traitement Entrant applicable aux Niveaux de Service correspondants indiqués dans le tableau ci-dessous. La Durée d'Indisponibilité ne comprend pas la période pendant laquelle l'Offre IBM SaaS n'est pas disponible pour les raisons suivantes :
 - durée d'Indisponibilité Planifiée du Système ;
 - cas de Force Majeure ;
 - incidents liés aux applications, équipements et données du Client ou d'un tiers ;
 - actes ou omissions du Client ou d'un tiers (y compris toute personne ayant accès à l'Offre IBM SaaS au moyen des mots de passe ou équipements du Client) ;
 - non-respect des configurations système requises et des plateformes prises en charge pour l'accès à l'Offre IBM SaaS ; ou
 - conformité d'IBM à toute conception, spécification ou instruction fournie par le Client ou par un tiers pour le compte du Client.
- g. **Événement** : signifie une circonstance ou un ensemble de circonstances réunies, donnant lieu au non-respect d'un Niveau de Service.
- h. **Force Majeure** : signifie catastrophes naturelles, terrorisme, action sociale, incendie, inondation, tremblement de terre, émeute, guerre, mesures, ordonnances ou restrictions gouvernementales, virus, attaque par saturation et toute autre conduite malveillante, incidents de connectivité des utilitaires ou du réseau ou toute autre cause d'indisponibilité de l'Offre IBM SaaS échappant au contrôle raisonnable d'IBM.
- i. **Durée d'Indisponibilité Planifiée du Système** : signifie une indisponibilité planifiée de l'Offre IBM SaaS pour maintenance.
- j. **Niveau de Service** : signifie la norme exposée ci-dessous permettant à IBM de mesurer le niveau de service qu'elle fournit au titre du présent Accord relatif aux Niveaux de Service.

2. Crédits de Disponibilité

- a. Pour pouvoir soumettre une Réclamation, le Client doit avoir soumis un ticket de support pour chaque Événement auprès du centre de support clients IBM pour l'Offre IBM SaaS concernée,

conformément à la procédure IBM pour la déclaration des incidents relevant du support de Gravité 1. Le Client doit fournir toutes les informations détaillées nécessaires relatives à l'Événement et aider de manière raisonnable IBM à diagnostiquer et résoudre l'Événement dans les limites requises pour les tickets de support de Gravité 1. Ce ticket doit être soumis dans les vingt-quatre (24) heures suivant la première fois où le Client a eu connaissance que l'Événement a eu une incidence sur son utilisation de l'Offre IBM SaaS.

- b. Le Contact Agréé du Client doit soumettre la Réclamation du Client pour un Crédit de Disponibilité au plus tard dans les trois (3) jours ouvrables suivant la fin du Mois Contractuel objet de la Réclamation.
- c. Le Contact Agréé du Client doit fournir à IBM tous les détails raisonnables de la Réclamation, y compris et de façon non limitative, des descriptions détaillées de tous les Événements concernés et du Niveau de Service allégué comme n'ayant pas été satisfait.
- d. IBM mesurera en interne la Durée d'Indisponibilité cumulée au cours de chaque Mois Contractuel applicable au Niveau de Service correspondant dans le tableau ci-dessous. Les crédits de disponibilité seront basés sur la Durée d'Indisponibilité mesurée depuis la première fois que le Client a signalé des problèmes relatifs à la Durée d'Indisponibilité. Si le Client signale simultanément un Événement de Durée d'Indisponibilité d'Application et un Événement de Temps d'Indisponibilité de Traitement des Données Entrantes, IBM traitera les périodes de chevauchement de la Durée d'Indisponibilité comme une seule Durée d'Indisponibilité, et non comme deux périodes distinctes d'indisponibilité. Pour chaque Réclamation valide, IBM appliquera le Crédit de Disponibilité applicable le plus élevé, en fonction du Niveau de Service Obtenu lors de chaque Mois Contractuel, comme indiqué dans les tableaux ci-dessous. IBM décline toute responsabilité en cas de Crédits de Disponibilité multiples pour un ou plusieurs Événement(s) identique(s) ayant lieu dans le même Mois Contractuel.
- e. Pour les Services Regroupés (Services individuels conditionnés et vendus ensemble pour un prix combiné unique), le Crédit de Disponibilité sera calculé en fonction du prix mensuel combiné unique du Service Regroupé, et non de la redevance d'abonnement mensuel pour chaque Offre IBM SaaS prise séparément. Le Client ne pourra soumettre que des Réclamations relatives à une seule Offre IBM SaaS dans une offre groupée au cours de tout Mois Contractuel et IBM ne sera pas redevable des Crédits de Disponibilité concernant plusieurs Offres IBM SaaS dans une offre groupée au cours de tout Mois Contractuel.
- f. Si le Client a acquis l'Offre IBM SaaS auprès d'un revendeur IBM agréé dans le cadre d'une transaction de revente dont la principale responsabilité d'IBM consiste à remplir les obligations relatives aux Offres IBM SaaS et aux Accords relatifs aux Niveaux de Service, le Crédit de Disponibilité sera basé sur le Niveau de Prix Conseillé (Relationship Suggested Value Price ou RSVP) en vigueur à ce moment-là pour l'Offre IBM SaaS concernée pendant le Mois Contractuel qui fait l'objet d'une Réclamation, avec une réduction de cinquante pour cent (50 %).
- g. Le nombre total de Crédits de Disponibilité accordés concernant tout Mois Contractuel ne doit en aucun cas dépasser dix pour cent (10 %) d'un douzième (1/12e) de la redevance annuelle que le Client a payée à IBM pour l'Offre IBM SaaS.
- h. IBM validera les Réclamations, à sa discrétion et en toute bonne foi, en fonction des informations disponibles dans les enregistrements d'IBM, qui prévaudront en cas de conflit avec les données des enregistrements du Client.
- i. **LES CRÉDITS DE DISPONIBILITÉ FOURNIS AU CLIENT CONFORMÉMENT AU PRÉSENT Accord relatif aux Niveaux de Service REPRÉSENTENT LE RECOURS EXCLUSIF DU CLIENT EN CE QUI CONCERNE TOUTE RÉCLAMATION.**

3. Niveaux de Service

Disponibilité de l'Offre IBM SaaS pendant un Mois Contractuel

Niveau de Service Obtenu (pendant un Mois contractuel)	Crédit de Disponibilité (% de Redevance d'Abonnement Mensuel pour le Mois Contractuel objet d'une Réclamation)
Inférieur à 99,8 %	2 %

Niveau de Service Obtenu (pendant un Mois contractuel)	Crédit de Disponibilité (% de Redevance d'Abonnement Mensuel pour le Mois Contractuel objet d'une Réclamation)
Inférieur à 98,8 %	5 %
Inférieur à 95,0 %	10 %

Le « Niveau de Service Obtenu », exprimé en pourcentage, est calculé comme suit : (a) le nombre total de minutes au cours d'un Mois Contractuel moins (b) le nombre total de minutes de la Durée d'Indisponibilité au cours d'un Mois Contractuel, divisé par (c) le nombre total de minutes d'un Mois Contractuel.

Exemple : 50 minutes de Durée d'Indisponibilité totale pendant un Mois Contractuel

Au total 43 200 minutes dans un Mois contractuel de 30 jours - 50 minutes de Durée d'Indisponibilité = 43 150 minutes <hr/> Au total 43 200 minutes	= Crédit de Disponibilité de 2 % pour 99,8 % de Niveau de Service Obtenu au cours du Mois Contractuel
--	---

4. Exclusions

Le présent Accord relatif aux Niveaux de Service n'est disponible que pour les Clients IBM. Il ne s'applique pas :

- aux Services Bêta et d'essai ;
- aux environnements non destinés à la production, y compris et de façon non limitative, aux environnements de test, de Reprise après Incident, d'assurance qualité ou de développement ;
- aux Réclamations déposées par les utilisateurs, participants et invités autorisés de l'Offre IBM SaaS d'un Client IBM ;
- au Logiciel d'Activation.