

IBM Payments Gateway

Le présent Descriptif de Service détaille le Service Cloud qu'IBM fournit au Client. Le terme « Client » signifie et inclut la société, ses utilisateurs autorisés et les destinataires du Service Cloud.

1. Service Cloud

L'offre de Service Cloud fournie par IBM est décrite ci-après. Le Devis et l'Autorisation d'Utilisation (ou « PoE ») sont fournis séparément sous la forme de Documents de Transaction.

IBM Payments Gateway

IBM Payments Gateway permet la connectivité aux environnements de développement, de pré-production et de production. Ses fonctionnalités sont les suivantes :

- Coffre PCI (Payment Card Industry), correspondant à une unité de stockage conçue pour assurer la sécurité des informations de paiement sensibles
- Passerelle de paiement, réalisant le routage, la commutation et le traitement des transactions de paiement avec des sous-traitants tiers
- Terminal virtuel, correspondant à un outil Web conçu pour le recouvrement des paiements dans les centres d'appels, la gestion des crédits et les opérations de paiement back-office
- Authentification conçue à l'aide de dispositifs de sécurité
- Outils de prévention des fraudes
- Fonctionnalités de génération de rapports
- Documentation

1.1 Services Supplémentaires

Le Client doit acheter IBM Payments Gateway conjointement avec moins une (1) des offres Cloud Service Payment suivantes :

a. IBM Payments Gateway API Payment

Ces fonctionnalités sont les suivantes :

- Les transactions sont transmises via une API comprenant un ensemble de services Web conçus pour faciliter l'intégration aux systèmes client. Cette API fournit une interface globale aux paiements globaux entre les banques et les sous-traitants du traitement dans un grand nombre de pays et de devises.

b. IBM Payments Gateway Hosted-Page Payment

Ces fonctionnalités sont les suivantes :

- Les transactions sont transmises par le biais de HPP (Hosted Payment Page), une interface graphique de recouvrement des paiements et de gestion de portefeuille, qui est conçue pour être intégrée aux sites Web, aux sites de commerce mobile, aux applications SmartPhone, aux applications de centre d'appels et aux systèmes de recouvrement back-office. L'interface Hosted Payment Page est conçue pour être livrée dans un cadre en ligne (iframe) HTML.

c. IBM Payments Gateway Advanced API Payment

Ces fonctionnalités sont les suivantes :

- Les transactions sont transmises par le biais de l'interface JSON (JavaScript Object Notation) qui est conçue pour faciliter le développement des fonctions de paiement dans les applications smartphone natives.
- L'interface JSON offre un ensemble d'API de paiement exécutées à l'aide de méthodes HTTP sur l'URL associée, avec des données distribuées au format JSON.

L'offre IBM Payments Gateway suivante peut être achetée en option :

d. IBM Payments Gateway Settlement

Ces fonctionnalités sont les suivantes :

- Les transactions sont transmises par un vendeur à l'établissement financier d'un acheteur et contiennent des informations de paiement permettant le règlement des transactions.

2. Description de la sécurité

2.1 Règles de sécurité

IBM a établi une équipe d'informations de sécurité et applique des règles de confidentialité et de sécurité qui sont communiquées aux employés d'IBM. IBM fournit chaque année une formation à la confidentialité et la sécurité des données destinée au personnel. Les règles de sécurité IBM sont revalidées annuellement en fonction des pratiques du secteur et des exigences métier IBM. Les incidents de sécurité sont traités dans le cadre de procédures de réponse après incident complètes. IBM applique des normes de sécurité physique strictes conçues pour limiter l'accès seulement au personnel autorisé aux centres de données IBM, et dispose notamment de points d'accès contrôlés et en nombre limité. Les visiteurs sont enregistrés dès leur arrivée et sont accompagnés lorsqu'ils se trouvent dans les locaux.

2.2 Contrôle d'accès

Le personnel autorisé d'IBM utilise l'authentification à deux facteurs auprès d'un hôte de gestion de « passerelle » intermédiaire. Le blocage IP peut être utilisé pour empêcher l'accès par des utilisateurs et sites Internet compromis connus dans les pays soumis à l'embargo des États-Unis. L'accès aux données Client et le transfert des données vers ou hors de l'environnement d'hébergement sont consignés. L'utilisation du WIFI est interdite dans les centres de données IBM qui prennent en charge ce Service Cloud.

Le Service Cloud nécessite le chiffrement du contenu pendant la transmission de données entre le réseau IBM et le point d'accès réseau du Client. Les méthodes de chiffrement spécifiques sont définies par entente contractuelle avec le Client et le chiffrement requiert l'installation de certificats SSL sur le site d'IBM et sur le site du Client. Seules les informations personnelles requises pour le traitement des paiements sont collectées. Le Service Cloud chiffre ce contenu stocké attendant la transmission de données.

2.3 Intégrité et Disponibilité des Services

Les modifications des systèmes d'exploitation, logiciels d'application et règles de firewall sont traitées dans le cadre de la procédure de gestion des modifications d'IBM. Les modifications des règles de firewall sont examinées par le personnel de sécurité IBM avant d'être mises en œuvre. IBM surveille le centre de données 24 heures sur 24 et 7 jours sur 7. Des scannages de vulnérabilité internes et externes sont régulièrement effectués par des administrateurs autorisés et des fournisseurs tiers pour aider à détecter et résoudre les risques potentiels liés à la sécurité des systèmes. Les systèmes de détection de logiciel malveillant (antivirus, détection d'intrusion, scannage de vulnérabilité et prévention contre les intrusions) sont utilisés dans tous les centres de données IBM. Les services de centre de données d'IBM prennent en charge de nombreux protocoles de distribution d'informations pour la transmission de données sur les réseaux publics. Exemples : HTTPS/SFTP/FTPS/S/MIME et VPN de site à site. Les données de sauvegarde destinées au stockage hors site sont chiffrées avant le transport.

2.4 Consignation des activités

IBM gère des journaux de ses activités pour les systèmes, applications, référentiels de données, middleware et unités d'infrastructure de réseau qui sont capables de et configurés pour consigner l'activité. Pour minimiser la possibilité de falsification et pour permettre l'analyse centralisée, la gestion d'alertes et la génération de rapports, l'activité est consignée en temps réel dans des référentiels de journaux centralisés. Les données sont signées pour empêcher la falsification. Les journaux sont analysés en temps réel et via des rapports d'analyse périodiques pour détecter les comportements anormaux. Le personnel des opérations est averti des anomalies et contacté, si nécessaire, un spécialiste de sécurité joignable 24 heures sur 24 et 7 jours sur 7.

2.5 Conformité

IBM effectue annuellement des audits de norme ISAE3402 (ou équivalents) dans les centres de données de production IBM Payments Gateway aux fins de contrôler le respect de ses règles de sécurité informatique. La certification PCI DSS annuelle d'IBM comprend des audits sur site menés par un

évaluateur de sécurité qualifié externe (Trustwave) dans tous les centres de données IBM Payments Gateway. L'attestation de conformité ou la lettre de conformité peut être communiquée au Client et à ses vérificateurs sur demande.

2.6 Déclaration de Pratiques de Sécurité

La sécurité des systèmes informatiques implique la protection des systèmes et des informations par le biais de la prévention, la détection et la résolution des accès non autorisés tant de l'intérieur que de l'extérieur de l'entreprise du Client. Tout accès non autorisé peut entraîner l'altération, la destruction ou le détournement des informations ou l'utilisation abusive des systèmes du Client pour attaquer d'autres systèmes. Sans une approche globale de la sécurité, aucun système ou produit informatique ne doit être totalement sécurisé et aucun produit ou mesure de sécurité ne peut être entièrement efficace pour empêcher tout accès non autorisé. Les systèmes et produits IBM sont conçus pour faire partie d'une approche de sécurité globale qui impliquera nécessairement des procédures opérationnelles supplémentaires et pourra exiger l'efficacité optimale d'autres systèmes, produits ou services. IBM ne garantit pas que les systèmes et produits jouissent d'une immunité contre tout comportement malveillant ou illicite d'un tiers quel qu'il soit.

2.7 Confidentialité des Données

IBM et le Client sont chacun responsables du respect de leurs obligations respectives en vertu des lois en vigueur relatives à la protection des données personnelles (telles qu'elles sont définies dans les lois en vigueur relatives à la protection des données) qui sont stockées et traitées par IBM pour le Client au titre du présent Contrat (les « Données Client »). En signant le présent Contrat, le Client désigne IBM comme Sous-traitant du Traitement des Données Client. Le Client est seul responsable d'identifier la finalité et les moyens de traitement par IBM des Données Client dans le cadre du présent Contrat, et ce traitement, qui suit les instructions du Client, ne doit pas faire déroger IBM aux lois en vigueur relatives à la protection des données. IBM et le Client reconnaissent qu'ils ne mènent pas d'enquêtes sur les mesures que l'autre partie prend pour le respect des lois en vigueur relatives à la protection des données. Aucune disposition du présent Contrat n'empêche IBM ou le Client de prendre les mesures jugées nécessaires pour le respect des lois en vigueur relatives à la protection des données. Si le Client demande des services additionnels ou différents afin de se conformer aux lois en vigueur relatives à la protection des données, le Client devra demander que ces services soit livrés avec les conditions d'un contrat séparé. Le Client reconnaît qu'il est seul responsable de déterminer que les mesures de sécurité stipulées dans le présent Contrat constituent des mesures techniques et organisationnelles appropriées pour protéger les Données Client, comme requis par les lois en vigueur relatives à la protection des données. IBM n'est pas tenue d'exécuter ou de respecter les mesures de sécurité concernant les Données Client autres que celles stipulées dans le présent Contrat et, en tant que Sous-traitant du Traitement des Données Client, IBM traitera les Données Client comme indiqué dans le présent Contrat et comme jugé raisonnablement nécessaire ou approprié pour réaliser les Services. Le Client est uniquement tenu de déterminer si tout transfert de Données Client effectué par IBM ou le Client hors du territoire au titre du présent Contrat est conforme aux lois en vigueur sur la protection des données.

3. Accord relatif aux Niveaux de Service

IBM fournit l'Accord relatif aux Niveaux de Service (ci-après dénommé « Accord relatif aux Niveaux de Service » ou « SLA ») ci-dessous pour le Service Cloud, comme indiqué dans le Document de Transaction. Le SLA ne constitue pas une garantie.

3.1 Définitions

- a. **Crédit de Service** : signifie le dédommagement fourni par IBM pour une Réclamation validée. Le Crédit de Service sera appliqué sous la forme d'un avoir sur une future facture du Service Cloud si ce dernier est acquis directement auprès d'IBM. Si le Service Cloud est acquis auprès d'un Partenaire Commercial IBM, IBM accordera une remise directement au Client.
- b. **Réclamation** : signifie une réclamation que le Client soumet à IBM selon laquelle un Niveau de Service n'a pas été satisfait pendant un Mois Contractuel.
- c. **Mois Contractuel** : signifie chaque mois calendaire complet pendant la durée du Service Cloud, mesuré entre le premier jour du mois à minuit (heure de l'Est des États-Unis) et le dernier jour du mois à 23h59 (heure de l'Est des États-Unis).

- d. **Durée d'Indisponibilité** : signifie une période de temps pendant laquelle le traitement du système de production pour le Service Cloud que le Client est autorisé à utiliser n'est pas disponible. La Durée d'Indisponibilité ne comprend pas la période pendant laquelle le Service Cloud n'est pas disponible pour les raisons suivantes :
- (1) indisponibilité de maintenance programmée ou annoncée ;
 - (2) événements ou causes échappant au contrôle d'IBM (par exemple, catastrophes naturelles, pannes Internet, maintenance d'urgence, etc.) ;
 - (3) problèmes au niveau du contenu, des équipements ou des applications que le Client utilise avec le Service Cloud ou tout logiciel ou équipement tiers ou autre technologie ;
 - (4) non-respect par le Client des configurations système requises et des plateformes prises en charge ou problèmes liés à l'administration de système, aux commandes ou à des erreurs de programmation du Client ;
 - (5) atteinte à la sécurité du fait du Client ou tout test de sécurité mené par le Client ; ou
 - (6) conformité d'IBM à toute conception, spécification ou instruction fournie à IBM par le Client ou par un tiers pour le compte du Client.
- e. **Événement** : signifie une circonstance ou un ensemble de circonstances réunies, donnant lieu au non-respect d'un Niveau de Service.
- f. **Délai de Réponse** : signifie le temps écoulé depuis le moment où les Services Web CheckoutStartSession et/ou CardAuthorize reçoivent une demande au point d'entrée des systèmes d'IBM jusqu'à ce que la réponse de services Web d'IBM soit renvoyée au Client.

3.2 Crédits de Service

Pour pouvoir soumettre une Réclamation, le Client doit consigner un ticket de support de Gravité 1 (comme défini ci-dessous dans la section Support Technique) pour chaque Événement auprès du centre d'assistance technique IBM, dans les vingt-quatre (24) heures suivant la première fois où le Client a eu connaissance que l'Événement a eu une incidence sur l'utilisation du Service. Le Client doit fournir toutes les informations nécessaires relatives à l'Événement et collaborer de manière raisonnable avec IBM lors du diagnostic et de la résolution.

La Réclamation pour un Crédit de Service doit être soumise dans les trois jours ouvrables suivant la fin du Mois Contractuel au cours duquel la Réclamation a eu lieu.

IBM mesurera en interne la Durée d'Indisponibilité cumulée au cours de chaque Mois Contractuel applicable aux niveaux de service correspondants dans les tableaux ci-dessous. Les crédits 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.

- a. Si le Client signale simultanément des Événements de Durée d'indisponibilité de Web Services, Hosted Payment Page et Virtual Terminal, 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.
- b. Si le Client signale simultanément des Événements de Durée d'Indisponibilité de Délai de Réponse des Services Web CheckoutStartSession et CardAuthorize, IBM traitera les périodes de chevauchement de la Durée d'Indisponibilité de Délai de Réponse comme une seule Durée d'Indisponibilité de Délai de Réponse, et non comme deux périodes distinctes d'indisponibilité de Délai de Réponse.

Pour chaque Réclamation valide, IBM appliquera le Crédit de Service 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 multiples pour un ou plusieurs Événements identiques ayant lieu dans le même Mois Contractuel.

Si le Service Cloud a été acquis auprès d'un Partenaire Commercial IBM, le Crédit de Service sera calculé sur la redevance d'abonnement mensuelle correspondant pour le prix en vigueur à ce moment-là du Service Cloud concerné pendant le Mois Contractuel qui fait l'objet d'une Réclamation, avec une réduction de cinquante pour cent (50 %).

Le nombre total de Crédits de Service accordés pour tout Mois Contractuel ne pourra pas dépasser dix pour-cent (10 %) d'un douzième (1/12ème) de la redevance annuelle du Service Cloud.

3.3 Niveaux de Service

Les interfaces Web Services, Hosted Payment Page et Virtual Terminal d'IBM seront accessibles au Client au moins 99,95 % du temps pendant un Mois Contractuel.

Pourcentage de Disponibilité (pendant un Mois Contractuel)	Crédit de Service (% de Redevance d'Abonnement Mensuelle pour le Mois Contractuel objet d'une Réclamation)
< 99,95 %	2 %
< 99,80 %	4 %
< 99,60 %	6 %
< 99,30 %	8 %
< 99,00 %	10 %

La disponibilité, exprimée en pourcentage, est calculée comme suit : le nombre total de minutes d'un Mois Contractuel pendant lequel les interfaces Web Services, Hosted Payment Page et Virtual Terminal d'IBM sont disponibles et répondent aux demandes du Client, divisé par le nombre total de minutes d'un Mois Contractuel multiplié par 100.

3.4 Délai de Réponse de Service Web IBM pendant un Mois Contractuel

IBM offre les deux SLA de Délai de Réponse suivants :

3.4.1 Délai de Réponse de Service Web IBM Moyen

Le Délai de Réponse IBM moyen pour les Services Web CheckoutStartSession et CardAuthorize sera moins de 100 millisecondes.

Le Délai de Réponse IBM pour un Service Web donné est mesuré sous la forme du temps écoulé depuis le moment où la demande de Service Web est reçue au point d'entrée du système d'IBM jusqu'à ce que la réponse du service Web d'IBM soit renvoyée au Client, moins le temps passé par le système d'IBM à attendre des réponses des Sous-traitants Tiers en aval.

L'objectif de niveau de service est calculé comme le Délai de Réponse IBM moyen pour les Services Web CheckoutStartSession et CardAuthorize respectivement, au niveau de toutes ces demandes de Service Web au cours d'un Mois Contractuel donné.

Délai de Réponse Moyen (pendant un Mois Contractuel)	Crédit de Service (% de Redevance d'Abonnement Mensuelle pour le Mois Contractuel objet d'une Réclamation)
> 100 ms	2 %
> 500 ms	6 %
> 1 seconde	10 %

3.4.2 Délai de réponse de Service Web IBM à 99 %

99 % des Services Web CheckoutStartSession et CardAuthorize auront un délai de réponse IBM de moins de 1 seconde.

Le Délai de Réponse IBM est calculé comme défini ci-dessus pour le Délai de Réponse de Service Web IBM Moyen.

L'objectif de niveau de service est calculé comme le Délai de Réponse IBM à 99 % pour les Services Web CheckoutStartSession et CardAuthorize respectivement, au niveau de toutes ces demandes de Service Web au cours d'un mois donné.

Délai de Réponse à 99 % (pendant un Mois Contractuel)	Crédit de Service (% de Redevance d'Abonnement Mensuelle pour le Mois Contractuel objet d'une Réclamation)
> 1 seconde	2 %
> 5 secondes	6 %
> 10 secondes	10 %

3.5 Autres Informations relatives à ce SLA

Ce SLA n'est disponible que pour la société du Client et ne s'applique pas aux réclamations des utilisateurs du Service Cloud ou à tout service bêta ou d'essai. Le SLA ne s'applique qu'aux Services Cloud destinés à la production. Il ne s'applique pas aux environnements hors production, y compris et de façon non limitative, aux environnements de test, de reprise après incident, d'assurance qualité ou de développement. IBM ne traitera pas les Réclamations de Crédit de Service de Délai de Réponse lorsqu'une interruption de niveau de service de disponibilité a été enregistrée pour la même période.

4. Objectifs de Niveau de Service

Les objectifs de niveau de service ci-dessous sont indiqués à titre informatif et ne constituent pas une garantie pour le Client. Aucun remboursement, avoir ou recours n'est mis à la disposition du Client au cas où IBM ne respecterait pas les objectifs de niveau de service.

Service	Objectif
Délai de réponse du Traitement par Lots	90 % de tous les lots de transactions seront traités intégralement en moins de 60 minutes suivant la réception.
Délai de réponse aux e-mails	La réponse à 95 % des e-mails envoyés à la boîte aux lettres de support partagée d'IBM se fera sous 24 heures ouvrables.
Délai de réponse aux appels émis au centre d'assistance disponible 24 heures sur 24 et 7 jours sur 7	Le centre d'assistance d'IBM disponible 24 heures sur 24 et 7 jours sur 7 répondra aux appels téléphoniques en moins de 60 secondes.
Gestion de la sécurité	<ul style="list-style-type: none">• La Certification PCI-DSS de niveau 1 d'IBM sera renouvelée au moins une fois par an.• IBM résoudra les vulnérabilités en matière de sécurité de haute gravité sous 10 jours.• IBM résoudra les vulnérabilités en matière de sécurité de faible gravité sous 30 jours.
Disponibilité du système Pré-Production	<ul style="list-style-type: none">• Disponible pour les tests client 24 heures sur 24 et 7 jours sur 7• Le système Pré-Production est en mode non surveillé hors des heures de travail normales de l'Europe centrale.• Les incidents du système Pré-Production seront par défaut traités sous forme d'incidents de gravité 3.

5. Support Technique

Le support technique destiné au Service Cloud est disponible par e-mail et par téléphone. Les améliorations, mises à jour et autres éléments fournis par IBM dans le cadre dudit support technique sont considérés comme faisant partie intégrante du Service Cloud et sont donc soumis au présent Descriptif de Service. Le support technique est inclus dans le Service Cloud et n'est pas disponible en tant qu'offre distincte.

Pour plus d'informations sur les heures de disponibilité, les adresses e-mail, les systèmes de notification de problème en ligne ainsi que d'autres moyens et procédures de communication de support technique, voir le manuel IBM Software as a Service Support Handbook.

Niveau de gravité	Définition de la gravité	Objectifs de temps de réponse	Couverture de temps de réponse
1	Impact critique sur les activités/indisponibilités 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.	Notification du Client sous 15 minutes	24 heures sur 24 et 7 jours sur 7

Niveau de gravité	Définition de la gravité	Objectifs de temps de réponse	Couverture de temps de réponse
2	Impact significatif 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.	Notification du Client sous 15 minutes	Heures ouvrables locales du lundi au vendredi
3	Impact mineur sur les activités : Indique que le service ou la fonctionnalité est utilisable et qu'il n'a pas d'impact critique sur les opérations.	Aucune notification requise	Heures ouvrables locales du lundi au vendredi
4	Impact minime sur les activités : Une demande d'information ou une demande non technique	Aucune notification requise	Heures ouvrables locales du lundi au vendredi

6. Autorisation d'Utilisation et Informations de Facturation

6.1 Unités de Mesure des Prix

Le Service Cloud est disponible en fonction de l'unité de mesure indiquée dans le Document de Transaction :

- a. **Instance** : unité de mesure par laquelle le Service Cloud peut être acquis. Une Instance est l'accès à une configuration spécifique du Service Cloud. Des Droits d'Utilisation suffisants doivent être obtenus pour chaque Instance du Service Cloud mise à disposition à des fins d'accès et d'utilisation pendant la période de mesure indiquée dans l'Autorisation d'Utilisation (« PoE ») ou le Document de Transaction du Client.
- b. **Événements en Millier** : unité de mesure par laquelle le Service Cloud peut être acquis. Les droits d'Événements en Millier se basent sur le nombre d'occurrences d'un événement caractéristique relatif à l'utilisation du Service Cloud, mesurées par lots de mille. Les droits d'Événements en Millier sont caractéristiques du Service Cloud et le type d'événement ne peut pas être modifié, échangé ou cumulé avec d'autres droits d'Événements en Millier d'un autre Service Cloud ou d'un autre type d'événement. Des Droits d'Utilisation doivent nécessairement être obtenus pour couvrir chaque événement qui a lieu durant la période de mesure spécifiée dans une Autorisation d'Utilisation (« PoE ») ou un Document de Transaction.
- c. **Événement** : pour ce Service Cloud, un Événement est défini comme étant une Transaction Maître, calculée par lots de mille. Une Transaction Maître est un ensemble d'instructions lancées à partir d'une application externe au logiciel (par exemple, canal Web de services bancaires pour entreprises ou canal d'entrée de message manuel) ou déclenchées par un événement dans le logiciel (par exemple, paiement récurrent ou heure du jour de démarrage du traitement en vrac). La Transaction Maître gère l'activité métier et l'unité de travail logique associées comprenant l'ensemble des mises à jour et événements associés aux diverses étapes de traitement et se terminant lorsque l'instruction finale est envoyée à une application externe ou que le cycle de traitement est terminé. Une Transaction Maître déclenche des transactions sous-jacentes pendant son cycle de traitement.

6.2 Redevances Mensuelles Partielles

Une redevance mensuelle partielle, comme indiqué dans le Document de Transaction, peut être estimée au prorata.

6.3 Redevances de Dépassement

Si l'utilisation réelle du Service Cloud pendant la période de mesure dépasse les droits indiqués dans l'Autorisation d'Utilisation (« PoE »), le Client sera facturé pour l'excédent, comme indiqué dans le Document de Transaction.

7. Durée et options de renouvellement

7.1 Durée

La durée du Service Cloud commence à la date à laquelle IBM notifie au Client que ce dernier a accès au Service Cloud, comme décrit dans l'Autorisation d'Utilisation. Le Client est autorisé à augmenter son niveau d'utilisation du Service Cloud pendant la durée en contactant IBM ou le Partenaire Commercial IBM du Client. Cette augmentation sera confirmée dans un Document de Transaction.

7.2 Options de renouvellement

Le Document de Transaction indiquera laquelle des options suivantes s'applique au renouvellement de la durée du Service Cloud :

7.2.1 Renouvellement Automatique

Lorsque le renouvellement est automatique, le Service Cloud sera automatiquement renouvelé pour une durée indiquée dans le Document de Transaction (soit pour une durée d'un an, soit pour la même durée que celle arrivant à expiration), sauf si le Client a demandé la résiliation par écrit au moins 90 jours avant la date d'expiration de la durée.

7.2.2 Facturation Continue

Lorsque la facturation est continue, le Client continuera à avoir accès au Service Cloud à l'issue de la durée et sera facturé en continu pour l'utilisation du Service Cloud. Pour cesser d'utiliser le Service Cloud et arrêter le processus de facturation continue, le Client doit faire parvenir à IBM une notification écrite de quatre-vingt-dix (90) jours demandant l'annulation. Le Client sera facturé pour toutes les redevances d'accès impayées jusqu'à la fin du mois d'annulation.

7.2.3 Renouvellement requis

Lorsque le renouvellement du Client est de type « résiliation », le Service Cloud sera résilié à la fin de la durée et l'accès du Client prendra fin. Pour continuer d'utiliser le Service Cloud au-delà de la date de fin de la durée, le Client doit commander une nouvelle période d'abonnement.

8. Dispositions Générales

Le cas échéant, les taxes pourront varier selon le ou les sites bénéficiant du Service Cloud. IBM appliquera les taxes en fonction de l'adresse indiquée lors de la commande du Client, 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.