BANQUE POPULAIRE GRAND OUEST

DILIZI

CONDITIONS GÉNÉRALES

Référencées PSD01827 CG201902 – pages numérotées de 1 à 8

Banque Populaire Grand Ouest Société Anonyme Coopérative de Banque Populaire à capital variable régie par les articles L512-2 et suivants du code monétaire et financier et l'ensemble des textes relatifs aux Banques Populaires et aux établissements de crédit - 857 500 227 RCS Rennes - Code APE 6419Z – Intermédiaire en assurance immatriculé à l'ORIAS sous le n° 07 004 504 - Siège social : 15 boulevard de la Boutière - CS 26858 - 35768 SAINT GREGOIRE CEDEX - Téléphone : 02 99 29 79 79 -Télécopie : 02 99 29 78 85 - Courriel : bpgo@banquepopulaire.fr - Site : www.bpgo.banquepopulaire.fr. Banque Populaire Grand Ouest exploite la marque Crédit Maritime.

ARTICLE 1 : DEFINITIONS – INTERPRETATION

1.1. Définitions

Les termes utilisés dans les Conditions Générales d'Utilisation dont la première lettre figure en majuscule auront la signification qui leur est conférée dans les Conditions Générales d'Utilisation.

En particulier, les termes ci-après auront la signification suivante :

Application Dilizi : a le sens indiqué à l'Article 2.

Article : désigne un article du Contrat.

Cartes "CB" ou agréées "CB" : désigne les cartes de paiements, telles qu'énumérées sur le site internet du Fournisseur accessible via le lien suivant www.dilizi.fr, reconnues par l'Equipement d'Acceptation.
A titre indicatif, une liste des Cartes "CB" ou agréées "CB" à la date du Contrat figure en ***ANNEXE 1***.

Client Dilizi : Désigne le souscripteur du service Dilizi, personne physique agissant dans le cadre de son activité professionnelle ou personne morale ayant pour objet de vendre ou fournir des biens et/ou services à titre onéreux et disposant d'un compte bancaire dans les livres de la Banque Populaire Grand Ouest.

Client Final / Clients Finaux : Client payeur du Client Dilizi quel que soit le moyen de paiement utilisé

Connexion Compatible : a le sens indiqué à l'Article 8.1

Contrat : désigne l'ensemble formé par les Conditions Générales d'Utilisation et les Conditions Contractuelles et leurs annexes

Données de la Carte : a le sens indiqué à l'Article 2

Données de Transaction : a le sens indiqué à l'Article 2.

Equipement d'Acceptation : désigne le dispositif de paiement constitué du Lecteur sécurisé de Cartes et de l'Application Dilizi permettant le contrôle du code confidentiel. Ce contrôle est opérationnel avec les cartes portant la marque « CB » et certaines cartes portant les marques Visa et MasterCard.
Toute extension de l'application de ce contrôle à d'autres cartes sera notifiée par le Fournisseur au Client, conformément à l'Article 16 du Contrat.

Espace Client Dilizi Désigne l'environnement du service Dilizi propre au Client et accessible par ce dernier par identifiant et mot de passe

Fournisseur désigne la Banque Populaire Grand Ouest proposant les services Dilizi.

GIE « CB » : désigne le Groupement des Cartes Bancaires « CB », groupement d'intérêt économique régi par les articles L. 251-1 à L. 251-23 du Code de commerce

Lecteur sécurisé de Cartes : a le sens indiqué à l'Article 2

Service d'Acceptation : a le sens indiqué à l'Article 2

Smartphone Compatible : a le sens indiqué à l'Article 8.1

Titulaire de la Carte : désigne tout titulaire d'une Carte "CB" ou agréée "CB" effectuant un règlement via l'Equipement d'Acceptation

Territoire : désigne la France métropolitaine

Ticket : a le sens indiqué à l'Article 14.1

Tiers : désigne toute personne qui n'est pas une Partie

Trame de Catalogue Commercial : a le sens indiqué à l'Article 3.2

1.2. Interprétation

Le préambule et les Annexes font partie intégrante des Conditions Générales d'Utilisation et ont la même portée contractuelle.
Les titres attribués à certains Articles et la table des matières sont indiqués à titre informatif pour faciliter la lecture des présentes et ne devront pas être utilisés à des fins d'interprétation et n'affecteront en aucune manière le sens du Contrat.

Les termes employés au pluriel s'appliqueront tant à l'ensemble ainsi défini qu'à un ou plusieurs de ses éléments pris individuellement. Les termes employés au masculin seront également employés au féminin et *vice versa.*

Les définitions données par un substantif s'appliqueront *mutatis mutandis* aux verbes, adjectifs et adverbes ayant la même racine et *vice versa.*

TITRE I – SERVICES FOURNIS PAR DILIZI

ARTICLE 2. SERVICE D'ACCEPTATION

Sous réserve des stipulations du Contrat (notamment, les stipulations du Titre III *« Conditions d'utilisation du Service d'Acceptation »* ci-après), le Fournisseur **(aa)** fournit des services techniques, **(bb)** vend un Lecteur sécurisé de cartes bancaires (ci-après le « **Lecteur sécurisé de Cartes** »), ainsi qu'une licence permettant au Client d'utiliser l'application mobile (ci-après l'« **Application Dilizi** ») et d'approuver ou de procéder à des paiements en utilisant les méthodes de paiements et les cartes de paiements (ci-après le « **Service d'Acceptation** »). Les cartes de paiements reconnues par le Service d'Acceptation sont énumérées sur le site internet du Fournisseur accessible via le lien suivant www.dilizi.fr (ci-après les « **Cartes "CB" ou agréées "CB"** »).
Le Lecteur sécurisé de Cartes traitera les données enregistrées sur les cartes de paiements (ci-après les « **Données de la Carte** »). L'Application générera une transaction ainsi que les données qui y sont associées (ci-après les « **Données de Transaction** »). Les Données de Transaction seront traitées et transmises par l'Application Dilizi au Fournisseur.
Le Fournisseur utilisera les Données de Transaction afin d'engager les opérations de paiement et de transférer les sommes en question sur le compte bancaire spécifié par le Client dans les Conditions Contractuelles
Lorsqu'un paiement est fait pour le compte du Client, le Fournisseur actualisera l'historique des paiements sur l'Espace Client Dilizi ainsi que dans l'Application Dilizi et enverra au Client un courrier électronique confirmant que l'opération de paiement a eu lieu.

ARTICLE 3. AUTRES SERVICES DILIZI

Sous réserve des stipulations du Contrat (en particulier, les stipulations du Titre IV *« Conditions d'utilisation des autres services Dilizi »* ci-après), le Client disposera via l'Application Dilizi des services techniques suivants :

3.1. Historique des opérations effectuées par le Client – Gestion des encaissements

L'Application Dilizi fournit au Client un relevé en temps réel des opérations **(i)** d'encaissement effectuées par le Client au moyen du Lecteur sécurisé de Cartes **(ii)** encaissées par d'autres moyens de paiement (chèques, espèces) et renseignées par le Client dans l'Application Dilizi.
Pour chacune des opérations effectuées via le Lecteur sécurisé de Cartes, l'Application Dilizi indique le statut de chacune de ces opérations

(*« opération encaissée » ; « opération remise en compensation-règlement »*).
Le Client dispose sur l'Application Dilizi d'un accès à l'historique des flux de transactions encaissés et compensés.

3.2. Gestionnaire de l'outil de caisse - Trame de Catalogue Commercial

L'Application Dilizi fournit au Client un assistant permettant de configurer des grilles tarifaires de ses produits ou services.
A cette fin, l'Application Dilizi contient une trame de catalogue commercial (ci-après la « **Trame de Catalogue Commercial** ») dans laquelle le Client peut référencer ses produits ou prestations (avec l'indication des prix hors taxes et toutes taxes comprises ; description desdits produits ou services ; présentation des produits avec des images ou photos).

3.3. Tableau de bord

L'Application Dilizi fournit au Client un tableau de bord présentant l'activité d'acceptation du Client effectué via l'Equipement d'Acceptation.
Les fonctionnalités du tableau de bord sont configurables par le Client sur l'Application Dilizi.

3.4. Constitution et Gestion d'une base de Clients Finaux

L'Application Dilizi permet au Client de se constituer sa base de clients (ci-après « les Clients Finaux ») pour fidéliser et stimuler son activité. Cette base lui permettra de réaliser ses propres actions de prospection commerciale ou de transmettre les données à caractère personnel des Clients Finaux ainsi collectées à ses partenaires commerciaux à des fins de prospection commerciale.
A cet effet, le Client s'engage à respecter les dispositions de la loi n° 78/17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ainsi que les dispositions de la loi pour la confiance dans l'économie numérique du 21 juin 2004. Notamment, le Client s'engage à effectuer toutes les formalités requises et plus particulièrement celles à réaliser auprès de la CNIL, le Fournisseur étant déchargé de toute responsabilité en cas de non-respect de ces dispositions légales et réglementaires.
En cas de résiliation du Contrat et dans un délai de deux mois à compter de la date de résiliation, le Client doit procéder à l'import de l'ensemble des données de la base. A l'issue de ce délai, le Fournisseur procédera à la suppression de ces données.

TITRE II – CONDITIONS D'ACCES AUX SERVICES DILIZI

ARTICLE 4. ENREGISTREMENT DU CLIENT – OUVERTURE DE SON ESPACE CLIENT

Le Client doit s'enregistrer auprès du Fournisseur et créer son Espace Client afin de pouvoir utiliser les services Dilizi.
La procédure d'enregistrement est accessible soit via le site internet www.dilizi.fr, soit via l'Application Dilizi.
Lors du processus d'enregistrement, le Client doit fournir un certain nombre d'informations telles que nom, adresse, adresse e-mail, numéro de téléphone, coordonnées bancaires ainsi que, le cas échéant, le nom de la société et la personnalité juridique de l'organisation, la raison sociale, le type/la catégorie d'entreprise, l'adresse complète de l'entreprise.

En plus des informations demandées lors du processus d'enregistrement, le Fournisseur se réserve le droit de demander au Client des informations complémentaires que le Fournisseur pourrait estimer nécessaires, afin de pouvoir fournir le Service d'Acceptation ou afin de se conformer à des conditions légales ou réglementaires. Dans l'hypothèse où le Client ne fournirait pas de telles informations complémentaires, le Fournisseur se réserve le droit de suspendre ou de résilier le Service Dilizi du Client.

Le Client reconnaît que les informations qu'il fournit lors du processus d'enregistrement ou à tout autre moment sont exactes, complètes, précises et à jour. Le Client s'engage, dans les meilleurs délais, à porter à la connaissance du Fournisseur tout changement relatif à toute information fournie par le Client soit lors du processus d'enregistrement, soit à tout autre moment en application du Contrat. Si toute information fournie lors de l'enregistrement ou par la suite s'avère ou devient inexacte ou incomplète, le Fournisseur se réserve le droit de suspendre ou de résilier le Service Dilizi du Client.

Lors de l'enregistrement, le Client reçoit un identifiant et un mot de passe personnalisé qui sont ensuite requis pour pouvoir accéder à son Espace Client et procéder à des opérations de paiement. Il est de la seule responsabilité du Client de s'assurer que ces identifiant et mot de passe ainsi que toute autre information de connexion sont conservés en sécurité.

Toute information relative à l'Espace Client Dilizi ainsi que l'identifiant et le mot de passe personnalisé sont personnels et ne peuvent être transférés ou utilisés par toute autre personne que le Client.

ARTICLE 5. ADHESION AU CONTRAT ET CONVENTION DE PREUVE

5.1. Modalités d'adhésion

Le Client adhère au Contrat après avoir pris connaissance des présentes *« Conditions Générales d'utilisation»* ainsi que des *« Conditions Contractuelles » et des annexes*.

La souscription au Contrat peut être réalisée soit à distance et notamment par internet, au travers de l'espace Client de la Banque en ligne de la Banque Populaire Grand Ouest, soit en agence, en présence d'un conseiller.

5.2. Convention de preuve en cas d'adhésion au service par internet

De convention expresse entre les Parties, en cas de souscription à distance par internet, les enregistrements électroniques constituent la preuve de l'adhésion au Contrat. En cas de conflit, les enregistrements électroniques produits par le Fournisseur prévaudront sur ceux produits par le Client, à moins que ce dernier ne démontre l'absence de fiabilité ou d'authenticité des documents produits par le Fournisseur.

ARTICLE 6. ACQUISITION DU LECTEUR SECURISE DE CARTES

6.1. Achat du Lecteur sécurisé de Cartes

Le Client reconnait que la fourniture du Service d'Acceptation par le Fournisseur est subordonnée à l'acquisition par le Client du Lecteur sécurisé de Cartes sur le site www.dilizi.fr conformément aux conditions tarifaires indiquées dans les Conditions Contractuelles.

6.2. Installation du Lecteur sécurisé de Cartes

Le Client s'engage à installer le Lecteur sécurisé de Cartes en respectant les instructions figurant dans le Guide utilisateur disponible en téléchargement sur le site www.dilizi.fr.

6.3. Utilisation du Lecteur sécurisé de Cartes

En complément des engagements pris à l'article 16, le Client s'engage à ne pas apporter de modification aux spécifications techniques et logicielles du Lecteur sécurisé de Cartes, de quelque manière que ce soit.
Le Client s'engage à maintenir pendant toute la durée du Contrat un usage approprié du Lecteur sécurisé de Cartes ; en particulier, le Client s'engage à ne pas utiliser le Lecteur sécurisé de Cartes à des fins autres que l'acceptation de Cartes de Paiement.
Le Client s'engage à utiliser le Lecteur sécurisé de Cartes exclusivement sur le Territoire.
Le Client reconnaît que le Lecteur sécurisé de Cartes est uniquement compatible avec le Service d'Acceptation proposé par le Fournisseur dans le cadre du Contrat. Pour l'exécution du Service d'Acceptation dans les conditions du Contrat, le Client s'engage à utiliser exclusivement le Lecteur sécurisé de Cartes référencé sur le site www.dilizi.fr.

Le Fournisseur s'engage à procéder à ses frais – sous réserves des stipulations ci-après – au remplacement de tout Lecteur sécurisé de Cartes du Client reconnu défectueux, pendant un délai de douze (12) mois à compter de l'adhésion au Contrat.
A cette fin, dans l'hypothèse où le Client soupçonne un dysfonctionnement de son Lecteur sécurisé de Cartes, il peut procéder à une demande d'échange auprès du centre d'appel du Fournisseur dont les coordonnées sont disponibles sur l'Espace Client du site Dilizi (www.dilizi.fr) ou sur le guide utilisateur fourni avec le lecteur.
Dans le cas où l'échange est validé par le centre d'appel du Fournisseur, le Client doit retourner à ses frais le Lecteur sécurisé de Carte affecté d'un dysfonctionnement accompagné de ses identifiants client Dilizi.
Après contrôle et expertise et sous réserve de confirmation de la panne ou du dysfonctionnement, un nouveau Lecteur sécurisé de Cartes sera envoyé au Client. Dans l'hypothèse où la panne ou le dysfonctionnement n'est pas confirmé par le Fournisseur, le Lecteur sécurisé de Cartes expertisé non défectueux est retourné au Client.

Les modalités détaillées de la garantie d'utilisation du Lecteur sécurisé de Cartes sont disponibles sur le site www.dilizi.fr.

ARTICLE 7. TELECHARGEMENT ET UTILISATION DE L'APPLICATION DILIZI

7.1. Acquisition et téléchargement de l'Application Dilizi

Le Client reconnait que la fourniture du Service d'Acceptation par le Fournisseur est subordonnée à l'acquisition du Lecteur sécurisé de Cartes et au téléchargement par le Client de l'Application Dilizi.
L'Application Dilizi peut être téléchargée gratuitement sur les plateformes suivantes, selon les termes et conditions prévues par les exploitants desdites plateformes :
- App Store d'Apple ;
- Google Play.

7.2. Utilisation de l'Application Dilizi
Le Client s'engage à maintenir pendant toute la durée du Contrat un usage approprié de l'Application.

Le Client s'engage à ne pas effectuer de copies de l'Application Dilizi. Le Client s'engage à télécharger de manière régulière l'ensemble des mises à jour de l'Application Dilizi. Le Client ne peut apporter aucune modification aux spécifications techniques et logicielles de l'Application Dilizi, de quelque manière que ce soit, sans l'autorisation préalable du Fournisseur.

Le Client s'engage à utiliser l'Application exclusivement sur le Territoire.

7.3. Mesures de sécurité
Le Fournisseur invite le Client à prendre toutes les dispositions utiles pour protéger les données transmises au travers des fonctionnalités de sécurité mise à sa disposition sur sa tablette PC ou son téléphone portable de type « smartphone » notamment en interdisant l'accès aux tiers non autorisés, le Fournisseur ne saurait être tenu pour responsable de tout incident occasionné de ce chef.

ARTICLE 8. COMPATIBILITE DES SYSTEMES – CONFORMITE

8.1. Souscription d'un abonnement téléphonie / internet à la charge du Client
Le Client reconnaît que la fourniture du Service d'Acceptation peut être effectuée exclusivement au moyen d'une tablette PC ou d'un téléphone portable de type *« smartphone »* ayant été agréé par le Fournisseur (ci-après les « **Smartphones Compatibles** ») et dont la liste est disponible auprès de la Banque Populaire Grand Ouest ou sur l'Espace Client Dilizi.

A cette fin, le Client fait son affaire personnelle de la souscription d'un contrat d'abonnement téléphonie et/ou internet permettant une utilisation régulière du Service d'Acceptation (ci-après la « **Connexion Compatible** »).
Le Fournisseur ne saurait être tenu pour responsable des difficultés associées au contrat passé entre le Client et son opérateur de téléphonie mobile.

8.2. Maintien de compatibilité
Pendant toute la durée du Contrat, le Client s'engage à conserver un Smartphone Compatible ou toute version ultérieurement agréée par le Fournisseur et à disposer d'une Connexion Compatible.

Le Fournisseur n'est pas responsable de la qualité et de la disponibilité des réseaux de télécommunication, ni des interruptions pour les interventions de maintenance, par suite de cas fortuits ou de force majeure et, en particulier, celles qui se produisent suite à un mauvais fonctionnement du Smartphone Compatible ou du réseau de télécommunications.
8.3. Respect des exigences sécuritaires
Pendant toute la durée du Contrat, le Client s'engage à respecter les exigences sécuritaires figurant en **ANNEXE 2**.

TITRE III – CONDITIONS D'UTILISATION DU SERVICE D'ACCEPTATION

ARTICLE 9. DEFINITION DU SYSTEME DE PAIEMENT PAR CARTES CB

Le service d'acceptation Dilizi permet l'utilisation de Cartes "CB" ou agréées "CB" pour le paiement d'achats de biens ou de prestations de services et cela dans le cadre des seules dispositions et procédures définies ou homologuées par le GIE "CB".
Le GIE "CB" intervient notamment, pour des raisons sécuritaires, dans les modifications du seuil de demande d'autorisation, la suppression de l'acceptabilité de certaines Cartes "CB" ou de Cartes agréées "CB" et la suspension de l'adhésion au Système "CB".

ARTICLE 10. STIPULATIONS RELATIVES AUX CARTES

Sont utilisables dans Dilizi :
- les cartes sur lesquelles figure la marque "CB"
- les cartes agréées "CB" c'est-à-dire :
- cartes portant uniquement les marques Visa ou MasterCard dont l'acceptation a été agréée par le GIE "CB",
- cartes émises dans le cadre de réseaux étrangers ou internationaux homologuées par le GIE "CB" et dont le Client peut obtenir les signes de reconnaissance auprès du Fournisseur.
L'ensemble des cartes précitées est désigné ci-après par le terme générique de "Carte".

ARTICLE 11. OBLIGATIONS DU CLIENT RELATIVES AU SERVICE D'ACCEPTATION

Le Client s'engage à :
- Signaler au public l'acceptation des Cartes par l'apposition de façon apparente à l'extérieur et à l'intérieur de son établissement des panonceaux, vitrophanies et enseignes qui lui sont fournis par le Fournisseur.
- Afficher visiblement le montant minimum éventuel à partir duquel la Carte est acceptée afin que les Titulaires de la Carte en soient préalablement informés. Ce montant minimum doit être raisonnable et ne pas être un frein à l'acceptation des Cartes.
- S'identifier clairement par le numéro SIRET et le code activité (NAF/APE) que l'INSEE lui a attribués. Si le Client n'est pas immatriculable, il doit utiliser un numéro d'identification spécifique, fourni par le Fournisseur, lui permettant l'accès au Système "CB".
- Afin que le Titulaire de la Carte n'ait pas de difficulté à vérifier et identifier les opérations de paiement qu'il a effectuées, vérifier avec le Fournisseur la conformité des informations transmises pour identifier son point de vente, les informations doivent indiquer une dénomination commerciale connue des Titulaires de Carte et permettre de dissocier ce mode de paiement par rapport aux autres modes de paiement (automate, vente à distance, etc) dans ce point d'acceptation.
- Recevoir des paiements en contrepartie d'actes de vente ou de fournitures de prestations de services offerts à sa clientèle et qu'il fournit ou réalise lui-même.
- Accepter les Cartes telles que définies à l'article 10 ci-dessus, pour le paiement d'achats de biens ou de prestations de services offerts à sa clientèle et réellement effectués (à l'exclusion de toute délivrance d'espèces ou de tout titre convertible en espèces pour leur valeur faciale), même lorsqu'il s'agit d'articles vendus à titre de promotion ou de soldes.
- Faire son affaire personnelle des litiges commerciaux et de leurs conséquences financières pouvant survenir avec des clients et concernant des biens et services dont l'achat a été réglé par Carte.
- Régler, selon les conditions figurant aux Conditions Contractuelles et/ou mentionnées dans la plaquette de tarification des opérations et services bancaires appliqués à la clientèle des professionnels, des entreprises ou des marchés spécialisés disponible sur le site internet de la Banque Populaire Grand Ouest, les commissions, frais et d'une manière générale, toute somme due au titre du Contrat.
- Utiliser obligatoirement l'Equipement d'Acceptation. Ne pas modifier les paramètres de son fonctionnement et ne pas y installer de nouvelles applications notamment en acceptant l'intervention de Tiers, sans avoir au préalable obtenu l'autorisation du Fournisseur.
- Prendre toutes les mesures propres à assurer la garde de son Equipement d'Acceptation et être vigilant quant à l'utilisation qui en est faite.
- Prévoir, dans ses relations contractuelles avec les Tiers, tels que les prestataires de services techniques ou sous-traitants intervenant dans le traitement et le stockage des données liées à l'utilisation des cartes, que ces derniers s'engagent à respecter le référentiel de sécurité PCI DSS et acceptent que les audits visés ci-dessous soient réalisés dans leurs locaux et que les rapports puissent être communiqués comme précisé dans cet article.
- Permettre au Fournisseur et au GIE "CB" de faire procéder aux frais du Client dans ses locaux ou ceux de ses prestataires, à la vérification par un Tiers indépendant du respect tant des clauses du présent Contrat que des exigences figurant en ***ANNEXE 2***. Cette vérification, appelée "procédure d'audit", peut intervenir à tout moment dès la conclusion du présent Contrat et/ou pendant sa durée.
- Au cas où le rapport remis aux Parties par le Tiers indépendant à l'issue de la procédure d'audit révélerait un ou plusieurs manquements à ces clauses ou exigences, le GIE "CB" peut procéder à une suspension de l'adhésion, voire à une radiation du Système "CB" tel que prévu à l'Article 17. Le Client autorise la communication du rapport au Fournisseur et aux réseaux étrangers ou internationaux mentionnés sur les Cartes acceptées par le Client et définies au Contrat.

Le Client doit respecter les exigences du référentiel de sécurité PCI DSS qui lui ont été communiquées par le Fournisseur.

ARTICLE 12. OBLIGATIONS DU FOURNISSEUR RELATIVES AU SERVICE D'ACCEPTATION

Le Fournisseur s'engage à :
- Fournir au Client les informations le concernant directement sur le fonctionnement du Système "CB" et son évolution.
- Indiquer au Client la liste et les caractéristiques des Cartes pouvant être acceptées et lui fournir, à sa demande, le fichier des codes émetteurs (BIN).
- Créditer le compte du Client des sommes qui lui sont dues, selon les Conditions Contractuelles convenues avec lui.
- Ne pas débiter, au-delà du délai maximum de 15 mois à partir de la date du crédit initial porté au compte du Client, les opérations non garanties et qui n'ont pu être imputées au compte sur lequel fonctionne la Carte.
- Communiquer, à la demande du Client, les éléments essentiels des procédures administratives annexes, notamment :
- gestion et renvoi des Cartes capturées par le Client,
- gestion et restitution des Cartes oubliées par leurs Titulaires.

ARTICLE 13. GARANTIE DU PAIEMENT

Les opérations de paiement sont garanties sous réserve du respect de l'ensemble des mesures de sécurité visées aux Articles 14 à 17.
Toutes les mesures de sécurité sont indépendantes les unes des autres.
Ainsi, l'autorisation donnée par le serveur d'autorisation ne vaut garantie que sous réserve du respect des autres mesures de sécurité, et notamment le contrôle du code confidentiel.
En cas de non-respect d'une seule de ces mesures, les enregistrements ne sont réglés que sous réserve de bonne fin d'encaissement. Le Client autorise expressément le Fournisseur à débiter d'office son compte bancaire du montant de toute opération de paiement non garantie n'ayant pu être imputée au compte sur lequel la Carte fonctionne.

ARTICLE 14. MESURES DE SECURITE

Le Client doit informer immédiatement le Fournisseur en cas de fonctionnement anormal de l'Equipement d'Acceptation, et pour toutes autres anomalies (absence de reçu ou de mise à jour de la liste noire, impossibilité de réparer rapidement, etc).

14.1. Lors du paiement
Le Client s'engage à :
- Vérifier l'acceptabilité de la Carte c'est-à-dire :
- la présence de la marque "CB" sur la Carte ou de la marque des cartes acceptées dans le Système "CB",
- la présence de l'hologramme sauf pour les Cartes "CB" portant également la marque V Pay,
- la présence de la puce sur les Cartes "CB" et sur certaines cartes acceptées dans le Système "CB",
- que le type de Carte figure au Contrat,
- la période de validité (fin et éventuellement début).
- Utiliser le Lecteur sécurisé de Cartes, respecter les indications affichées sur son écran et suivre les procédures dont les modalités techniques lui ont été indiquées.

Le Lecteur sécurisé de Cartes doit notamment :
- après la lecture de la puce des Cartes lorsqu'elle est présente :
- permettre le contrôle du code confidentiel lorsque la puce le lui demande,
- vérifier :
- le code émetteur de la Carte (BIN),
- le code service,
- la date de fin de validité de la Carte.
- lorsque la puce n'est pas présente sur une carte agréée "CB" ou qu'elle ne fonctionne pas, après lecture de la piste ISO 2, vérifier :
- le code émetteur de la Carte (BIN),
- le code service,
- la date de fin de validité de la Carte.
- Lorsque la puce le demande à l'Equipement d'Acceptation, faire composer par le Titulaire de la Carte, dans les meilleures conditions de confidentialité, son code confidentiel. La preuve de la frappe du code confidentiel est apportée par le certificat qui doit figurer sur le ticket émis par l'Equipement d'Acceptation (ci-après le « **Ticket** »).Lorsque le code confidentiel n'est pas vérifié, l'opération n'est réglée que sous réserve de bonne fin d'encaissement, même en cas de réponse positive à la demande d'autorisation.

En cas d'opération en mode sans contact permise par l'Equipement d'Acceptation, l'opération de paiement est garantie même si le code confidentiel n'est pas vérifié, sous réserve du respect de l'ensemble des autres mesures de sécurité à la charge du Client.
- Obtenir une autorisation d'un montant identique à l'opération lorsque l'Equipement d'Acceptation ou la Carte à puce déclenche une demande d'autorisation.
A défaut, l'opération ne sera pas garantie.
Une opération pour laquelle l'autorisation a été refusée par le serveur d'autorisation n'est jamais garantie.
Une demande de capture de Carte, faite par le serveur d'autorisation, annule la garantie pour toutes les opérations faites postérieurement le même jour et avec la même Carte, dans le même point de vente.
- Faire signer un Ticket papier manuscrit :
  - lorsque le montant de l'opération est supérieur à 1 500 euros,
  - et, en règle générale, dans tous les cas où l'Equipement d'Acceptation le demande.

Le Ticket doit comporter les mentions obligatoires suivantes :
- Mention « CB »
- Libellé enseigne
- Montant de la transaction en euros
- Date et heure
- 4 derniers chiffres du PAN
- Donnée d'identification du terminal
- Mention « Débit » ou « transaction non aboutie »

Lorsque la signature est requise et que la Carte comporte un panonceau de signature, vérifier attentivement la conformité de celle-ci avec celle qui figure sur ledit panonceau.
Pour une Carte sur laquelle ne figure pas le panonceau de signature, vérifier la conformité de la signature utilisée avec celle qui figure sur la pièce d'identité présentée par le Titulaire de la Carte.
- Remettre au Titulaire de la Carte sous format dématérialisé un exemplaire du Ticket. Si le Titulaire de la Carte ne peut (ou ne veut pas) communiquer un numéro de téléphone mobile ou une adresse mail, le Client lui remet un ticket papier manuscrit. En cas d'interruption au cours de la transaction (refus, abandon), le Client remet un ticket au format papier.

14.2. Après le paiement
Le Client s'engage à ne stocker, sous quelque forme que ce soit, aucune des Données de la Carte ci-après :
- le cryptogramme visuel,
- la piste magnétique dans son intégralité,
- le code confidentiel.

Le Client s'engage à prendre toutes les précautions utiles pour que soient assurés la confidentialité et l'intégrité des données à caractère personnel du Titulaire de la Carte qu'il est amené à recueillir à l'occasion de son activité et notamment lors de la réalisation d'une opération par Carte ainsi que le contrôle de l'accès à celles-ci et ce, conformément aux prescriptions de la loi n°78/17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et notamment de son article 34.

ARTICLE 15. MODALITES ANNEXES DE FONCTIONNEMENT

15.1. Réclamation
Toute réclamation doit être justifiée et formulée par écrit au Fournisseur, dans un délai maximum de 6 mois à compter de la date de l'opération contestée, sous peine de forclusion.
Ce délai est réduit à 15 jours calendaires à compter de la date de débit en compte résultant d'une opération non garantie.

15.2. Convention de preuve
De convention expresse entre les parties, les enregistrements électroniques constituent la preuve des opérations de paiement remises au Fournisseur. En cas de conflit, les enregistrements électroniques produits par le Fournisseur ou le GIE "CB" prévaudront sur ceux produits par le Client, à moins que ce dernier ne démontre l'absence de fiabilité ou d'authenticité des documents produits par le Fournisseur ou le GIE "CB".

15.3. Retrait à son Titulaire d'une Carte faisant l'objet d'un blocage ou en opposition
En cas de retrait à son Titulaire d'une Carte faisant l'objet d'un blocage ou en opposition (le retrait ayant eu lieu notamment sur instruction du serveur d'autorisation en raison de la présence de la Carte sur la liste des Cartes faisant l'objet d'un blocage ou en opposition et/ou contrefaites), le Client utilise la procédure de gestion et de renvoi des Cartes capturées.

15.4. Oubli d'une Carte par son Titulaire
En cas d'oubli de sa Carte par le Titulaire, le Client peut la lui restituer dans un délai maximum de deux jours ouvrés après la date d'oubli de la Carte, sur justification de son identité et après obtention d'un accord demandé selon la procédure communiquée par le Fournisseur. Au-delà de ce délai, le Client utilise la procédure de gestion et de restitution des Cartes oubliées.

15.5. Transaction crédit
Le remboursement partiel ou total d'un achat d'un bien ou d'un service réglé par Carte doit, avec l'accord de son Titulaire, être effectué au Titulaire de la Carte utilisée pour l'opération initiale. Le Client doit alors utiliser la procédure dite de "transaction crédit", et effectuer la remise

correspondante au Fournisseur à qui il avait remis l'opération initiale. Le montant de la "transaction crédit" ne doit pas dépasser le montant de l'opération initiale.

15.6. Carte non signée
En cas de Carte non signée et si le panonceau de signature est présent sur la Carte, le Client doit demander au Titulaire de la Carte de justifier de son identité et d'apposer sa signature sur le panonceau de signature prévu à cet effet au verso de la Carte et enfin vérifier la conformité de cette signature avec celle figurant sur la pièce d'identité présentée par le Titulaire de la Carte. Si le Titulaire de la Carte refuse de signer sa Carte, le Client doit refuser le paiement par Carte.

ARTICLE 16. CONDITIONS RELATIVES A L'UTILISATION DE L'EQUIPEMENT D'ACCEPTATION

Le Client assure l'installation, le fonctionnement, la maintenance et la mise à niveau de l'Equipement d'Acceptation.
Il doit par ailleurs, dans le cadre de l'acceptation des Cartes :
- Veiller à ce que sa police d'assurance couvre bien :
- les risques inhérents à la garde de cet Equipement d'Acceptation dont le Fournisseur ne saurait être responsable, ainsi que les dommages directs ou indirects résultant de leur destruction ou de leur altération,
- les dommages directs ou indirects sur les Cartes utilisées et sur les équipements annexes qui auraient pu lui être confiés.
- Laisser libre accès au constructeur, au Fournisseur ou à toute personne désignée par ce dernier pour les différents travaux à effectuer sur l'Equipement d'Acceptation, notamment lorsque la mise à jour de logiciels s'avère nécessaire et que le Client n'a pas engagé les travaux nécessaires lui incombant.
- Ne pas utiliser l'Equipement d'Acceptation à des fins illicites ou non autorisées par le constructeur ou le Fournisseur et n'y apporter aucune modification de logiciel ayant un impact sur le Système "CB" sans accord préalable du Fournisseur.
- Assurer, selon le mode d'emploi, les conditions de bon fonctionnement de l'Equipement d'Acceptation.

ARTICLE 17. SUSPENSION DE L'ADHESION ET RADIATION DU SYTEME « CB »

Le GIE "CB" peut procéder, pour des raisons de sécurité, sans préavis et sous réserve du dénouement des opérations en cours, à une suspension de l'adhésion au Système "CB". Elle est précédée, le cas échéant, d'un avertissement au Client, voire d'une réduction de son seuil de demande d'autorisation. Cette suspension est notifiée par l'envoi d'une lettre recommandée et motivée, avec demande d'avis de réception. Son effet est immédiat. Elle peut être décidée en raison notamment :
- d'une utilisation anormale de Cartes perdues, volées ou contrefaites,
- d'un risque de dysfonctionnement important du Système "CB".
Le Client s'engage alors à stopper toute utilisation de l'Equipement d'Acceptation et à retirer immédiatement de son établissement tout signe d'acceptation des Cartes.
La période de suspension est au minimum de 6 mois, éventuellement renouvelable.
A l'expiration de ce délai, le Client peut, sous réserve de l'accord préalable du GIE "CB", demander la reprise d'effet de son contrat auprès du Fournisseur.
En cas de comportement frauduleux de la part du Client responsable du point de vente, le Client peut être immédiatement radié ou la suspension être convertie en radiation.

TITRE IV – CONDITIONS D'UTILISATION DES AUTRES SERVICES DILIZI

ARTICLE 18. UTILISATION DES SERVICES DILIZI

Le Client s'engage à utiliser les services Dilizi conformément aux lois et règlement en vigueur.

ARTICLE 19. UTILISATION DE LA TRAME DE CATALOGUE COMMERCIAL

Conformément aux stipulations de l'Article 3, le Client peut charger des textes et des images dans la Trame de Catalogue Commercial.
Dans ce cadre, le Client s'engage à ce que toute image ainsi chargée ne porte pas atteinte de quelque manière que ce soit aux lois et règlements en vigueur, à l'ordre public et aux bonnes mœurs. Ainsi, le Client ne doit notamment pas enfreindre le droit à l'image d'un individu, les droits d'auteur ou tout autre droit de la propriété intellectuelle (dessin, modèle…).
Le Client certifie et atteste au Fournisseur qu'il bénéficie des autorisations nécessaires à la reproduction de l'image.

Le Client s'engage en conséquence à prendre à sa charge toutes les conséquences que pourrait avoir, à l'égard du Fournisseur, l'utilisation d'images sans autorisation et/ ou illicites.

Le Fournisseur interdit expressément, sans que cette énumération ne soit limitative, l'utilisation d'images (photographies, dessins, etc.), représentations, symboles et textes :
- ayant une connotation politique, religieuse ou syndicale ;
- ayant une connotation ou un contenu violent, raciste, xénophobe, subversif, choquant, provoquant, sexuel, obscène, ou contraire à la morale publique ou incitant au suicide, à la violation des dispositions légales ou réglementaires et notamment l'incitation à une violation du droit pénal, à la commission d'un délit, crime ou acte terroriste ;
- qui soit en rapport avec l'alcool, le tabac, la drogue ou tout autre stupéfiant ou produit dont la commercialisation et l'usage sont strictement contrôlés ;
- faisant l'apologie des crimes de guerre ou des crimes contre l'humanité ;
- portant atteinte à la dignité et à l'intégrité de la personne humaine.

TITRE V – SECRET BANCAIRE ET PROTECTION DES DONNEES A CARACTERE PERSONNEL

ARTICLE 20. PROTECTION DES DONNEES A CARACTERE PERSONNEL

Dans le cadre de la signature et de l'exécution du présent contrat, et plus généralement de notre relation, la Banque Populaire Grand Ouest recueille et traite des données à caractère personnel vous concernant et concernant les personnes physiques intervenant dans le cadre de cette relation (mandataire, représentant légal, caution, contact désigné, préposé, bénéficiaire effectif, membre de votre famille...).
Les informations vous expliquant pourquoi et comment ces données sont utilisées, combien de temps elles seront conservées ainsi que les droits dont vous disposez sur vos données figurent dans notre Notice d'information sur le traitement des données à caractère personnel. Cette notice est portée à votre connaissance lors de la première collecte de vos données. Vous pouvez y accéder à tout moment, sur notre site internet https://www.bpgo.banquepopulaire.fr/portailinternet/Editorial/Informations/Pages/protection-donnees-personnelles.aspx ou en obtenir un exemplaire auprès de votre agence. La Banque Populaire Grand Ouest communiquera en temps utile les évolutions apportées à ces informations.

A l'occasion de l'exécution des ordres de paiement donnés par Carte, le Client peut avoir accès à différentes données à caractère personnel concernant les Titulaires de la Carte. Le Client ne peut utiliser ces données à caractère personnel que pour l'exécution des ordres de paiement par Carte et le traitement des réclamations dont ils peuvent être l'objet. Sauf obligations légales et réglementaires, le Client ne peut ni les céder, ni en faire un usage autre que celui directement visé par le présent Contrat.
- Pour l'édition du ticket de caisse et/ou de carte bancaire, le Client peut être amené à collecter des données à caractère personnel (adresse mail, numéro de mobile) des Titulaires de Carte ou des Clients Finaux. Ces données à caractère personnel seront stockées par le Fournisseur, pour le compte du Client ou de ses partenaires commerciaux, le Fournisseur s'engageant à ne faire aucun usage de ces données. En outre, le Client ou ses partenaires commerciaux peut être amené à utiliser ces données à des fins de prospection commerciale, si les Titulaires de la Carte ou les Clients Finaux ont accepté expressément et préalablement de recevoir de la prospection commerciale de la part du Client ou de ses partenaires commerciaux. A ce titre, le Client s'engage à respecter les dispositions de la loi n°78/17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et à effectuer toutes les formalités requises auprès de la CNIL, le Fournisseur étant déchargé de toute responsabilité en cas de non-respect de ces obligations légales et réglementaires par le Client. Notamment, les Titulaires de Carte ou les Clients Finaux sur lesquels des données à caractère personnel ont été recueillies doivent pouvoir disposer des droits d'accès, de rectification et d'opposition auprès du Client ou de ses partenaires commerciaux. A cet égard, le Client s'engage d'ores et déjà à leur permettre d'exercer ces droits tant pour son compte que pour celui de ses partenaires commerciaux.
- Les dispositions de la loi pour la confiance dans l'économie numérique du 21 juin 2004 obligent le Client à recueillir le consentement exprès et préalable du Titulaire de Carte ou des Clients Finaux lors de toute utilisation de l'adresse mail et du numéro de mobile à des fins de

prospection commerciale. Le Client s'engage à chaque envoi d'une nouvelle proposition commerciale à informer le Titulaire de la Carte ou les Clients Finaux de sa possibilité de se désabonner et des modalités y afférentes. Le Client ou ses partenaires commerciaux s'engagent enfin à respecter ces dispositions et à supprimer de leurs propres bases ainsi que dans la base des Clients Finaux de son espace client Dilizi les données personnelles du Titulaire de la Carte ou des Clients Finaux si ce dernier en fait la demande auprès du Client, le Client faisant son affaire personnelle du respect de la loi Informatique et Libertés et de la loi pour la confiance dans l'économie numérique par ses partenaires commerciaux, le Fournisseur étant déchargé de toute responsabilité en cas de non-respect de ces obligations légales et réglementaires par le Client.

- Le Client s'assure également de l'existence et de la mise en œuvre de dispositifs de protection et de contrôle des accès physiques et logiques à ces données.

TITRE VI – CONDITIONS FINANCIERES

ARTICLE 21. TARIFICATION DES SERVICES ET DU LECTEUR SECURISE DE CARTES

La tarification des services et du Lecteur sécurisé de Cartes ainsi que toutes les commissions, frais et d'une manière générale, toute somme due au titre du Contrat sont mentionnées dans les Conditions Contractuelles et/ou dans la plaquette de tarification des opérations et services bancaires appliqués à la clientèle des professionnels, des entreprises ou des marchés spécialisés disponible sur le site internet de la Banque Populaire Grand Ouest.

TITRE VII – STIPULATIONS DIVERSES

ARTICLE 22. DUREE, SUSPENSION ET RESILIATION DU CONTRAT

Le Contrat est conclu pour une durée indéterminée.
Le Fournisseur se réserve le droit de suspendre l'accès ou l'exécution de tout ou partie de l'Application Dilizi, sans aucun préavis ni formalité, s'il devait relever des faits laissant présumer la tentative ou l'utilisation frauduleuse des Services Dilizi, ce dont le client serait immédiatement informé.
Le Fournisseur d'une part, le Client d'autre part, peuvent, à tout moment, sans justificatif ni préavis, sous réserve du dénouement des opérations en cours, mettre fin au présent Contrat, sans qu'il soit nécessaire d'accomplir aucune autre formalité que l'envoi d'une lettre recommandée avec demande d'avis de réception.
La clôture du compte bancaire dans les livres de l'établissement fournisseur des Services Dilizi pour quelque cause que ce soit entraine la résiliation immédiate de plein droit du Contrat sous réserve du dénouement des opérations en cours.
Toute cessation d'activité du Client, cession ou mutation du fonds de commerce, liquidation judiciaire entraîne la résiliation immédiate de plein droit du Contrat sous réserve du dénouement des opérations en cours.
Dans le cas où, après résiliation du présent Contrat, il se révélerait des impayés, ceux-ci seront à la charge du Client et/ou pourront faire l'objet d'une déclaration de créances.

ARTICLE 23. MODIFICATIONS

Le Fournisseur peut modifier à tout moment les Conditions Générales d'Utilisation. Le Fournisseur peut notamment apporter :
- des modifications techniques telles que l'acceptation de nouvelles Cartes, les modifications de logiciel, le changement de certains paramètres, la remise en état de l'Equipement d'Acceptation suite à un dysfonctionnement, etc.
- des modifications sécuritaires telles que :
- la modification du seuil de demande d'autorisation,
- la suppression de l'acceptabilité de certaines Cartes,
- la suspension de l'adhésion au Système "CB"

Les nouvelles conditions entrent généralement en vigueur au terme d'un délai minimum fixé à 1 (un) mois à compter de l'envoi d'une lettre d'information ou de notification au Client.
D'un commun accord, les Parties peuvent déroger à ce délai en cas de modifications importantes.
Ce délai est exceptionnellement réduit à 5 (cinq) jours calendaires lorsque le Fournisseur ou le GIE "CB" constate, dans le point de vente, une utilisation anormale de Cartes perdues, volées ou contrefaites.
Passés les délais visés au présent article, les modifications sont opposables au Client s'il n'a pas résilié le Contrat.
Le non-respect des nouvelles conditions techniques ou sécuritaires, dans les délais impartis, peut entraîner la résiliation du présent Contrat, voire la suspension par le GIE "CB" de l'adhésion au Système "CB" dans les conditions prévues à l'Article 17 du présent Contrat.

ARTICLE 24. CONFIDENTIALITE

Les Parties ne communiqueront aucune information et ne publieront aucun communiqué en relation avec l'existence des Conditions Contractuelles ou son contenu sans l'accord préalable des autres Parties, sauf si la communication de l'information ou la publication du communiqué est rendue obligatoire par une règle d'ordre public s'imposant à la Partie concernée, ou pour répondre aux exigences d'une autorité de régulation. Dans cette hypothèse, la Partie affectée s'engage à en informer les autres Parties rapidement et par écrit.

ARTICLE 25. NON RENONCIATION

Le fait pour le Fournisseur ou pour le Client de ne pas exiger à un moment quelconque l'exécution stricte d'une disposition du présent Contrat ne peut en aucun cas être considéré comme constituant de sa part une renonciation, quelle qu'elle soit, à l'exécution de celle-ci.

ARTICLE 26. INTEGRALITE DE L'ACCORD

Le préambule et son ou ses Annexes font partie intégrante du Contrat et ont la même force obligatoire à l'égard des Parties que les autres stipulations du Contrat. Les Conditions Générales d'Utilisation constituent l'intégralité de l'accord des Parties et remplace en conséquence tout accord ou document antérieur, écrit ou verbal, de quelque nature que ce soit en relation avec son objet.

ARTICLE 27. LOI APPLICABLE – TRIBUNAUX COMPETENTS

Le Contrat est soumis au droit français. Tout désaccord ou litige relatif au Contrat ou aux opérations qui y sont prévues sera soumis aux tribunaux compétents du ressort de la Cour d'Appel de Paris.

ANNEXE 1 : LISTE DES CARTES "CB" OU AGREEES "CB" A LA DATE DU CONTRAT

- Visa ;
- Mastercard ;
- CB.

ANNEXE 2 : EXIGENCES SECURITAIRES DU CLIENT

Les exigences constituant le Référentiel Sécuritaire Accepteur sont présentées ci-après :

Exigence 1 (E1) : Gérer la sécurité du système commercial et d'acceptation au sein de l'entreprise

Pour assurer la sécurité des données des opérations de paiement et notamment, des données des Titulaires de Cartes, une organisation, des procédures et des responsabilités doivent être établies.

En particulier, un responsable de la sécurité du système commercial et d'acceptation doit être désigné. Il est chargé, entre autres, d'appliquer la législation sur la protection des données à caractère personnel et du secret bancaire dans le cadre de leur utilisation et de leur environnement.
Les détenteurs de droits d'usage des informations et du système doivent être identifiés et sont responsables de l'attribution des droits d'accès au système.

Le contrôle du respect des exigences de sécurité relatives au système commercial et d'acceptation doit être assuré.
Une organisation chargée du traitement des incidents de sécurité, de leur suivi et de leur historisation doit être établie.

Exigence 2 (E2) : Gérer l'activité humaine et interne

Les obligations et les responsabilités du Personnel quant à l'utilisation des données bancaires et confidentielles, à leur stockage et à leur circulation en interne ou à l'extérieur doivent être établies. Il en est de même pour l'utilisation des postes de travail et du réseau interne comme du réseau Internet.
Les obligations et les responsabilités du Personnel quant à la protection des données bancaires et confidentielles doivent être établies. L'ensemble de ces règles doit s'appliquer à tous les personnels impliqués : salariés de l'entreprise et Tiers.
Les personnels doivent être sensibilisés aux risques encourus,

notamment sur la divulgation d'informations confidentielles, l'accès non autorisé aux informations, aux supports et aux documents.
Les personnels doivent être régulièrement sensibilisés aux risques particuliers liés à l'usage des moyens informatiques (postes de travail en réseau, serveurs, accès depuis ou vers Internet) et notamment, à l'introduction de virus.
Il convient que les personnels reçoivent une formation appropriée sur l'utilisation correcte du système d'exploitation et du système applicatif commercial et d'acceptation.

Exigence 3 (E3) : Gérer les accès aux locaux et aux informations

Tout dispositif (équipement réseau, serveur, …) qui stocke ou qui traite des données relatives à une opération de paiement et notamment, des données du Titulaire de la Carte doit être hébergé dans un local sécurisé et répondre aux exigences édictées par les règles et recommandations de la CNIL.
Les petits matériels ou supports informatiques sensibles doivent être rendus inaccessibles à des tiers en période de non utilisation. Notamment, les cartouches de sauvegarde doivent être stockées dans un coffre.
Dans le cas où ces petits matériels ou supports informatiques sensibles ne sont plus opérationnels, ils doivent être obligatoirement détruits et la preuve de leur destruction doit être établie.
La politique d'accès aux locaux sensibles doit être formalisée et les procédures doivent être établies et contrôlées.

Exigence 4 (E4) : Assurer la protection logique du système commercial et d'acceptation

Les règles de sécurité relatives aux accès et sorties depuis et vers le système commercial et d'acceptation doivent être établies et leur respect doit être contrôlé.
Seul le serveur supportant l'application commerciale doit être accessible par les internautes. Le serveur de base de données du Client ainsi que le serveur hébergeant le système d'acceptation ne doivent être accessibles que par le serveur commercial front-office et seulement par l'intermédiaire d'un pare-feu.
Les accès internes des utilisateurs comme des administrateurs à ces mêmes serveurs doivent se faire par l'intermédiaire du pare-feu.
L'architecture réseau doit être organisée de manière à ce que les règles de sécurité définies soient mises en œuvre et contrôlées.
Le pare-feu doit être mis à jour systématiquement lorsque des vulnérabilités sont identifiées sur ses logiciels (logiciel pare-feu et logiciel d'exploitation) et corrigeables.
Le serveur supportant le pare-feu doit être doté d'un outil de contrôle de l'intégrité.
Le pare-feu doit assurer l'enregistrement des accès et des tentatives d'accès dans un journal d'audit. Celui-ci doit être analysé quotidiennement.

Exigence 5 (E5) : Contrôler l'accès au système commercial et d'acceptation

Le principe d'autorisation d'utilisation du système doit être défini et reposer sur la notion d'accès des classes d'utilisateurs aux classes de ressources : définition des profils d'utilisateurs et des droits accordés.
Les responsabilités et rôles quant à l'attribution, l'utilisation et le contrôle doivent être identifiés. Notamment, les profils, les droits et les privilèges associés doivent être validés par les propriétaires des informations et du système commercial et d'acceptation.
Les droits des utilisateurs et des administrateurs ainsi que de leurs privilèges, doivent être gérés et mis à jour conformément à la politique de gestion des droits.

Exigence 6 (E6) : Gérer les accès autorisés au système commercial et d'acceptation

Aucune ouverture de droits ne peut se faire en dehors des procédures d'autorisation adéquates. Les autorisations données doivent être archivées et contrôlées régulièrement.
Outre les accès clients, tout accès au système commercial et d'acceptation de Carte doit se faire sur la base d'une identification et d'une authentification.
L'identification doit être nominative y compris pour les administrateurs et les personnels de maintenance. Les droits accordés à ceux-ci doivent être restreints aux opérations qui leur sont autorisées.
L'utilisation de codes d'identification attribués à des groupes ou des fonctions (process techniques comme l'alimentation automatique des signatures antivirales) n'est autorisée que si elle est appropriée au travail effectué.
Les changements de situation (changement de poste, départ, …) des personnels doivent systématiquement entraîner un contrôle des droits d'accès attribués.
La suppression des droits d'accès doit être immédiate en cas de départ d'une personne.
Le contrôle d'accès doit être assuré au niveau réseau par le pare-feu, au niveau système par les systèmes d'exploitation des machines accédées et au niveau applicatif par le logiciel applicatif et par le gestionnaire de base de données.
Les tentatives d'accès doivent être limitées en nombre.
Les mots de passe doivent être changés régulièrement.
Les mots de passe doivent comporter au minimum 8 caractères dont des caractères spéciaux.

Exigence 7 (E7) : Surveiller les accès au système commercial et d'acceptation

Les accès et tentatives d'accès au système doivent être enregistrés dans des journaux d'audit.
L'enregistrement doit comporter au minimum la date et l'heure de l'accès (ou tentative) et l'identification de l'acteur et de la machine.
Les opérations privilégiées comme la modification des configurations, la modification des règles de sécurité, l'utilisation d'un compte administrateur doivent également être enregistrées.
Les systèmes assurant l'enregistrement doivent au minimum avoir la fonction de pare-feu pour le système supportant la base de données Clients ainsi que celui supportant la base de données Paiements.
Les journaux d'audit doivent être protégées contre des risques de désactivation, modification ou suppression non autorisées. Les responsabilités et rôles quant à l'audit des données enregistrées sont identifiés. Celui-ci doit être effectué quotidiennement.

Exigence 8 (E8) : Contrôler l'introduction de logiciels pernicieux

Les procédures et les responsabilités de gestion ayant trait à la protection anti-virus et à la restauration des données et des logiciels en cas d'attaque par virus doivent être définies et formalisées.
L'installation et la mise à jour régulière des logiciels de détection et d'élimination des virus doivent être effectuées sur la totalité des machines ayant accès au système commercial et d'acceptation.
La vérification anti-virus doit être exécutée quotidiennement sur la totalité des machines.

Exigence 9 (E9) : Appliquer les correctifs de sécurité (patches de sécurité) sur les logiciels d'exploitation

Les correctifs de sécurité doivent être systématiquement appliqués sur les équipements de sécurité et les serveurs applicatifs frontaux lorsque des vulnérabilités pourraient permettre des accès non autorisés et non visibles.
Ces correctifs doivent être appliqués sur la base d'une procédure formelle et contrôlée.

Exigence 10 (E10) : Gérer les changements de version des logiciels d'exploitation

Une procédure d'installation d'une nouvelle version doit être établie et contrôlée.
Cette procédure doit prévoir entre autres, des tests de non régression du système et un retour arrière en cas de dysfonctionnement.

Exigence 11 (E11) : Maintenir l'intégrité des logiciels applicatifs relatifs au système commercial et d'acceptation

Il convient d'établir les responsabilités et les procédures concernant les modifications opérationnelles touchant aux applications.
Les modifications apportées aux logiciels applicatifs doivent faire l'objet d'une définition précise.

La demande de modification doit être approuvée par le responsable fonctionnel du système.
Les nouvelles versions de logiciels applicatifs doivent être systématiquement soumises à recette et approuvées par le responsable fonctionnel de l'application concernée avant toute mise en production.

Exigence 12 (E12) : Assurer la traçabilité des opérations techniques (administration et maintenance)
Les opérations techniques effectuées doivent être enregistrées de manière chronologique, dans un cahier de bord pour permettre la reconstruction, la revue et l'analyse en temps voulu des séquences de traitement et des autres activités liées à ces opérations.

Exigence 13 (E13) : Maintenir l'intégrité des informations relatives au système commercial et d'acceptation

La protection et l'intégrité des éléments de l'opération de paiement doivent être assurés ainsi lors de leur stockage et lors de leur routage sur les réseaux (internes ou externes). Il en est de même pour les éléments secrets servant à chiffrer ces éléments.
Le dossier de sécurité propre au système commercial et d'acceptation doit décrire les moyens mis en place pour répondre à cette exigence.

Exigence 14 (E14) : Protéger la confidentialité des données bancaires

Les données du Titulaire de la Carte ne peuvent être utilisées que pour exécuter l'ordre de paiement et pour traiter les réclamations. Le cryptogramme visuel d'un Titulaire de Carte ne doit en aucun cas être stocké par le Client.
Les données bancaires et à caractère personnel relatives à une opération de paiement, et notamment les données du Titulaire de la Carte doivent être protégées lors de leur stockage et lors de leur routage sur les réseaux internes et externes au site d'hébergement conformément aux dispositions de la loi Informatique et Libertés et aux recommandations de la CNIL. Il en est de même pour l'authentifiant du Client et les éléments secrets servant à chiffrer.

Le dossier de sécurité propre au système commercial et d'acceptation doit décrire les moyens mis en place pour répondre à cette exigence.

Exigence 15 (E15) : Protéger la confidentialité des identifiants - authentifiants des utilisateurs et des administrateurs

La confidentialité des identifiants - authentifiants doit être protégée lors de leur stockage et de leur circulation.

Il convient de s'assurer que les données d'authentification des administrateurs ne puissent être réutilisées.
Dans le cadre d'une intervention extérieure pour maintenance, les mots de passe utilisés doivent être systématiquement changés à la suite de l'intervention.