BANQUE CALÉDONIENNE D'INVESTISSEMENT
SAEM au capital de 15 milliards F CFP
Siège social : 54, avenue de la Victoire - BP K5 - 98849
Nouméa Cedex
Téléphone (+687) 25 65 65 - Fax (+687) 25 65 57 - Internet :
www.bci.nc
RCS Nouméa 15479 - Ridet n° 0 015 479 001
RIAS NC170007 voir rias.nc

Contrat d'acceptation en paiement de proximité par cartes Conditions Générales

(Mai 2022)

PARTIE I - CONDITIONS GÉNÉRALES communes à tous les schémas

Article 1 – Définition

Accepteur
L'« Accepteur » peut être tout commerçant, tout prestataire de services, toute personne, physique ou morale, exerçant une profession libérale, toute association, toute collectivité publique et, d'une manière générale, tout professionnel vendant ou louant des biens et/ou des prestations de services ou toute entité dûment habilitée à recevoir des dons ou à percevoir des cotisations, susceptible d'utiliser un Système d'Acceptation reconnu par le(s) Schéma(s) dûment convenu(s) avec l'Acquéreur.

Acquéreur
Par « Acquéreur », il faut entendre tout établissement de crédit ou de paiement habilité à organiser l'acceptation des Cartes portant la(les) Marque(s) d'un (des) Schéma(s).

Authentification Forte
Par « Authentification Forte », il faut entendre une authentification basée sur l'utilisation de deux éléments d'authentification, ou plus, qui sont indépendants, de sorte que si un élément est compromis, la fiabilité des autres ne l'est pas, ces éléments faisant partie de deux des catégories suivantes au moins ; (i) un élément connu uniquement du titulaire de la Carte, (ii) un élément détenu uniquement par le titulaire de la Carte, et (iii) un élément inhérent au titulaire de la Carte.

Carte(s)
Par « Carte(s) », on entend un instrument de paiement qui permet à son titulaire d'initier une opération de paiement liée à une Carte. Elle porte une ou plusieurs Marques.
Lorsque la Carte est émise dans l'EEE ou en Nouvelle-Calédonie (à l'exception de la carte privative JADE), elle porte la mention de sa Catégorie, selon la classification indiquée ci-après ou l'équivalent dans une langue étrangère.

Catégories de carte
Par « Catégories de Carte », on entend les catégories de Carte suivantes :
- crédit ou Carte de crédit,
- débit,
- prépayée,
- commerciale (Carte soumise aux règles commerciales du Chapitre III du Règlement [UE] 2015/751 du Parlement européen et du Conseil du 29 avril 2015).

Contrat ou Présent Contrat
Par « Contrat » ou « Présent Contrat », il faut entendre ensemble les Conditions Générales, Particulières et Spécifiques du Contrat d'acceptation en de proximité par Carte, convenues entre l'Acquéreur et l'Accepteur, ainsi que leurs Annexes.

CSB
Par « CSB », il faut entendre le Prestataire qui propose à l'Accepteur les solutions d'Équipement Électronique.

EEE
Par « EEE », il faut entendre l'Espace Économique Européen, soit à la date des présentes, les États membres de l'Union Européenne, l'Islande, le Liechtenstein et la Norvège.

Équipement Électronique
Par « Équipement Électronique », il faut entendre tout dispositif de paiement capable de lire la Carte équipée d'une puce au standard EMV ou d'une piste magnétique permettant l'authentification du titulaire de la Carte, et le cas échéant disposant de la technologie NFC : Near Field Communication (transmission par ondes courtes).

L'Équipement Électronique est soit agréé, soit approuvé par l'entité responsable de chacun des Schémas dont les Cartes sont acceptées sur cet Équipement Électronique.

L'agrément ou l'approbation de l'Équipement Électronique est une attestation de conformité au regard des spécifications techniques et fonctionnelles définies par chaque Schéma concerné, qui dispose de la liste des Equipements Electroniques agréés ou approuvés.

La CSB peut mettre à la disposition de l'Accepteur un Équipement Électronique.

Marque
Par « Marque », il faut entendre tout nom, terme, sigle, symbole matériel ou numérique ou la combinaison de ces éléments susceptibles de désigner le Schéma**.** Les règles spécifiques d'acceptation en paiement propres à chaque Schéma de Carte dont la(les)Marque(s) figure(nt) sur la Carte sont précisées dans les Conditions Spécifiques en Partie II du présent Contrat.

Les Marques pouvant être acceptées dans le cadre du présent Contrat sont celles indiquées en article 2 des présentes.

Paiement par Carte Sans Contact
Par « Paiement par Carte Sans Contact » on entend un paiement par Carte réalisé sur un Équipement Électronique disposant de la technologie NFC : Near Field Communication (transmission par ondes courtes) permettant le règlement rapide d'achats de biens ou de prestations de services par des titulaires de Carte par une lecture à distance de la Carte, avec ou sans frappe du code confidentiel ou identification par apposition de l'empreinte biométrique.

Le Paiement par Carte Sans Contact peut être réalisé soit avec une Carte physique dotée de cette technologie soit de façon dématérialisée, notamment par un dispositif tel qu'un téléphone mobile ou un objet connecté doté de cette technologie et d'une application de paiement ayant permis l'enrôlement préalable de la Carte.

En cas de Paiement par Carte Sans Contact avec utilisation de la Carte physique, les dispositifs d'Authentification Forte du titulaire de la Carte au sens du Règlement délégué UE 2018/389 du 27 novembre 2017 ne sont pas applicables, et ce dans les conditions et selon les modalités prévues par ledit Règlement.

Partie(s)
Par « Partie(s) », il faut entendre l'Acquéreur et l'Accepteur.

Point d'Acceptation
Par « Point d'Acceptation », il faut entendre le lieu physique où est initié l'ordre de paiement.

Prestataires Tiers (Third Services Providers) ou prestataires techniques
Par « Prestataires Tiers », il faut entendre les acteurs qui traient, stockent des données de paiement cartes pour le compte de l'Accepteur.

Réglementation Relative à la Protection des Données à Caractère Personnel
Par « Réglementation Relative à la Protection des Données à Caractère Personnel », il faut entendre les lois et réglementations applicables en Nouvelle-Calédonie en matière de protection des données personnelles et de la vie privée, en particulier loi n° 78-17 du 6 janvier 1978 modifiée et les principes du Règlement (UE) 2016/679 du 27 avril 2016 dit « Règlement Général sur la Protection des Données » (RGPD), reconnus comme applicables en Nouvelle-Calédonie ainsi que toutes les réglementations nationales, délibérations et recommandations de la CNIL ou de toute autorité de contrôle ou de supervision compétente au titre du Contrat ou d'une des Parties, applicables en Nouvelle-Calédonie.

Schéma
Par « Schéma », il faut entendre un schéma de cartes de paiement, soit un ensemble unique de règles et pratiques régissant l'exécution d'opérations de paiement liées à une carte tel que défini à l'article 2 du Règlement (UE) 2015/751 du Parlement européen et du Conseil du 29 avril 2015.

Les Schémas reposent sur l'utilisation de Cartes portant leur Marque auprès des Accepteurs acceptant les Marques desdits Schémas, et cela dans le cadre des seules dispositions et procédures définies ou homologuées par lesdits Schémas.

Système d'Acceptation
Par « Système d'Acceptation », il faut entendre les logiciels, protocoles et équipements conformes aux spécifications définies par chaque Schéma et nécessaires à l'enregistrement, à la transmission et au traitement sécurisé des ordres de paiement par cartes portant l'une des Marques dudit Schéma. L'Accepteur doit s'assurer que le Système d'Acceptation a fait l'objet d'un agrément par l'entité responsable du Schéma, le cas échéant en consultant la liste des Systèmes d'Acceptation reconnus par l'entité responsable du Schéma.

UE
Par « UE », il faut entendre l'Union Européenne, soit les États membres de l'Union Européenne.

Article 2 – Marques et catégories de cartes acceptées

Les Marques acceptées au titre du présent Contrat sont les suivantes : VISA - VISA ELECTRON – VPAY - CB - MASTERCARD – MAESTRO.
Toutes les catégories de Carte sont acceptées.
Dans le cas où l'Accepteur décide de ne pas accepter l'ensemble des Marques et/ou des Catégories de Cartes, ce dernier doit en informer clairement et sans ambiguïté le titulaire de la Carte, selon les modalités précisées à l'article 4.4 des présentes.

Article 3 – Souscription du contrat et convention de preuve

3.1 Modalités de souscription du Contrat

L'Accepteur souscrit le présent Contrat après avoir pris connaissance des Conditions Particulières, des Conditions Générales, des Conditions Spécifiques, de leurs Annexes.
La souscription du Contrat peut être réalisée, soit en agence, en présence d'un conseiller, soit à distance si cette possibilité est offerte, notamment par Internet via l'espace client de la banque en ligne de l'Acquéreur.

3.2 Convention de preuve en cas de souscription au contrat par Internet

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

Article 4 – Obligations de l'Accepteur

L'Accepteur s'engage à :

4.1 Connaître et respecter les lois et règlements, les dispositions professionnelles ainsi que les bonnes pratiques applicables aux ventes et prestations de services, aux prestations réalisées à distance, au commerce électronique et notamment aux échanges utilisant les réseaux et les différents terminaux de communication (TV, téléphonie mobile, ordinateur…) et, le cas échéant, aux jeux d'argent et de hasard et/ou de paris, et aux réceptions de dons et règlements de cotisations.
Lorsque son activité implique des jeux d'argent, de hasard et/ou de paris, il s'engage à obtenir toute autorisation et/ou agrément de l'autorité compétente, à respecter les limites autorisées par la loi, et à refuser d'une personne légalement incapable une prise d'enjeux et/ou de paris et/ou une Carte de crédit.

4.2 Utiliser le(s) système(s) d'acceptation en s'abstenant de toute activité qui pourrait être pénalement sanctionnée, telle que, et sans que cette liste soit limitative :

- la mise en péril de mineurs, des actes de pédophilie,
- les actes de contrefaçon d'œuvres protégées par un droit de propriété intellectuelle,
- les actes de contrefaçon de moyens ou instruments de paiement,
- le non-respect de l'utilisation des données personnelles collectées,
- les atteintes aux systèmes de traitement automatisé de données,
- les actes de blanchiment et de fraude,
- le non-respect des dispositions relatives aux jeux d'argent et de hasard, aux courses de chevaux, aux loteries
- le non-respect des dispositions relatives aux conditions d'exercice de professions réglementées.

4.3 Signaler immédiatement à l'Acquéreur :

- toute modification affectant sa forme juridique ou concernant ses représentants légaux ;
- toute modification de son activité, notamment de l'ajout d'une ou plusieurs branches d'activité, la cessation d'une ou plusieurs branches d'activités et plus généralement de tout événement modifiant les conditions d'exercice de son activité.

4.4 Signaler au public les Marques, Catégories de Cartes qu'il accepte par l'apposition de façon apparente sur l'écran du dispositif technique ou/et sur tout autre support de communication.

Pour la(les) Marque(s) qu'il accepte, l'Accepteur doit accepter toutes les Cartes émises hors de l'UE ou hors Nouvelle-Calédonie sur lesquelles figure(nt) cette(ces) Marque(s), quelle que soit la Catégorie de Carte.

4.5 Accepter les paiements effectués avec les Cartes et les Paiements par Carte Sans Contact 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, à l'exclusion de toute délivrance d'espèces ou de tout titre convertible en espèces pour leur valeur faciale.

Seules les entités dûment habilitées à délivrer des espèces ou des quasi-espèces dans le respect de la législation applicable (casinos, cercles de jeux privés référencés au ministère de l'intérieur, changeurs manuels) acceptent les paiements effectués avec les Cartes et les Paiements par Carte Sans Contact telles que listées dans les Conditions Particulières en contrepartie de la remise d'espèces ou de "quasi-espèces" offertes à leur clientèle et qu'elles fournissent elles-mêmes.

L'Accepteur ne doit pas collecter, au titre du Présent Contrat, une opération de paiement pour laquelle il n'a pas lui-même reçu le consentement du titulaire de Carte.

4.6 Sous réserve de disponibilité du service : dans le cas d'une opération de paiement effectuée avec une Carte cobadgée, c'est-à-dire portant le logo de deux ou plusieurs Marques, permettre au titulaire de la Carte de choisir la Marque. Il est rappelé à l'Accepteur qu'il peut sélectionner prioritairement une des Marques indiquées à l'article 2 des présentes, sous réserve de laisser la possibilité au titulaire de la Carte de passer outre, et de sélectionner une autre Marque.
En cas de Paiement par Carte Sans Contact, le choix par défaut est systématiquement celui de l'Accepteur. Si le titulaire de la Carte souhaite un choix différent, alors, soit il passe en mode « contact », soit l'Accepteur lui propose un autre moyen pour lui offrir le choix.

4.7 Respecter les montants maximums indiqués par l'Acquéreur pour l'acceptation d'une opération de paiement par Carte, et précisés dans les Conditions Particulières et à l'article 7.2.5 des présentes Conditions Générales pour les Paiements par Carte Sans Contact.

4.8 S'identifier clairement dans la transmission de ses enregistrements à l'Acquéreur par le numéro d'immatriculation SIRET et le code activité (NAF/APE) qui lui ont été attribués ou comme Entité dûment habilitée à recevoir des dons ou percevoir des cotisations. Si l'Accepteur n'est pas immatriculable, il doit utiliser un numéro d'identification spécifique, fourni par l'Acquéreur.
L'accepteur s'engage à informer l'Acquéreur en cas de modification ou d'évolution de code d'activité NAF/APE dans les meilleurs délais.

4.9 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 l'Acquéreur la conformité des informations transmises pour identifier son point d'acceptation. Ces informations doivent indiquer une dénomination commerciale ou sociale (pour les dons et cotisations) connue des Titulaires de Carte et permettre d'identifier le point d'acceptation concerné et de dissocier ce type de paiement par rapport aux types modes de paiement (ex. : automate, et règlement en présence physique de la Carte).

4.10 Transmettre les enregistrements des opérations de paiement à l'Acquéreur dans le délai maximum précisé à l'article 7 « Mesures de sécurité », sauf dispositions contraires précisées dans les Conditions Spécifiques relatives à chaque Schéma.
Le délai de remboursement ne peut excéder trente (30) jours calendaires à compter de la date de l'opération de paiement initiale, sauf dispositions contraires précisées dans les Conditions Spécifiques relatives à chaque Schéma.
Au-delà d'un délai maximum indiqué dans les Conditions Spécifiques à chaque Schéma après la date de l'opération, l'encaissement des opérations de paiement n'est plus réalisable.

4.11 Régler, selon les Conditions Particulières convenues avec l'Acquéreur et selon les conditions générales, les commissions, frais, pénalités éventuelles et, d'une manière générale, toute somme due au titre de l'acceptation des Cartes et du fonctionnement du Schéma concerné.

4.12 Utiliser obligatoirement l'Équipement Électronique tel que défini à l'article 1. 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 de l'Acquéreur.

4.13 Prendre toutes les mesures propres à assurer la garde de son Équipement Électronique notamment :
- recenser l'ensemble de ses Équipements Électroniques,
- recenser leur localisation,
- s'assurer de leur identification et de leur conformité aux exigences de sécurité PCI DSS consultables sur le site pcisecuritystandards.org et dont une présentation générale est annexée aux présentes, et notamment les normes PCI PED,
- être vigilant quant à l'utilisation qui en est faite, et notamment ne pas quitter des yeux son Équipement Électronique durant toute l'opération de paiement, sous réserve de la préservation de la confidentialité du code du titulaire de la Carte,
- conserver la carte de domiciliation dans un environnement sécurisé et veiller à une utilisation appropriée de celle-ci par les personnes habilitées,
- s'assurer d'utiliser un Système d'Acceptation certifié par les Schémas et par l'Acquéreur
- Vérifier qu'aucun système frauduleux de capture de données n'a été installé à son insu sur l'automate.

Ces mesures sont applicables pendant toute la durée de vie du présent contrat.

4.14 Respecter le Référentiel Sécuritaire Accepteur figurant en annexe des présentes et le Référentiel Sécuritaire PCI DSS consultable sur le site pcisecuritystandards.org, dont une présentation générale figure également en annexe des présentes. 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 les mêmes exigences et règles sécuritaires et acceptent que les audits visés à l'article 4.15 soient réalisés dans leurs locaux et que les rapports puissent être communiqués comme précisé dans cet article.
Déclarer à l'Acquéreur, annuellement, à compter de la date d'entrée en vigueur du Présent Contrat, et

immédiatement en cas de changements de prestataire technique ou de correspondant au sein d'un prestataire technique, lesdits prestataires techniques ou sous-traitants. À défaut, l'Accepteur s'expose à des pénalités telles qu'indiquées aux présentes.

4.15 Permettre à l'Acquéreur et/ou au(x) Schémas) concerné(s) de faire procéder aux frais de l'Accepteur, dans ses locaux ou ceux de ses prestataires, à la vérification et/ou au contrôle périodique par un tiers indépendant du respect tant des clauses du présent Contrat et ses annexes, que des exigences et règles sécuritaires visées à l'article 4.14. Cette vérification, appelée « procédure d'audit », peut intervenir à tout moment dès la conclusion du présent Contrat et/ou pendant sa durée et s'inscrit dans le respect des procédures de contrôle et d'audit définies par le Schéma concerné.
L'Accepteur autorise la communication du rapport en résultant à l'Acquéreur et au(x) Schéma(s) concerné(s).
Au cas où le rapport d'audit révélerait un ou plusieurs manquements aux Contrat ou exigences et règles sécuritaires, le Schéma peut demander à l'Acquéreur de procéder à une résiliation du contrat d'acceptation.

4.16 En cas de compromission et si la non-conformité aux exigences et règles sécuritaires est confirmée par le schéma ou un tiers indépendant, des frais forfaitaires à l'ouverture du dossier de compromission ainsi qu'un montant par Carte compromise seront applicables à l'Accepteur.

4.17 Mettre en œuvre dans le délai imparti par l'Acquéreur les mesures destinées à résorber un taux d'impayés anormalement élevé ou une utilisation anormale de Cartes perdues, volées ou contrefaites ou pour remédier à tout autre manquement au regard du présent Contrat.
À défaut, l'Acquéreur peut procéder, pour des raisons de sécurité, sans préavis et dans les conditions prévues à l'article 8.2 des présentes, à une suspension de l'acceptation des Cartes portant certaines Marques par l'Accepteur.
En cas de taux de fraude anormalement élevé, notamment au regard du volume d'affaires réalisé par l'Accepteur, de l'augmentation des opérations mises en impayés suite à réclamation du Titulaire de la Carte, d'utilisation anormalement élevée de Cartes perdues, volées ou contrefaites ou dont les données ont été usurpées, l'Acquéreur est fondé à ne créditer le compte de l'Accepteur qu'après l'encaissement définitif des opérations de paiement.
L'Acquéreur est également autorisé à ne créditer le compte de l'Accepteur qu'après encaissement définitif en cas d'opérations présentant un caractère inhabituel ou exceptionnel.
L'Acquéreur en informe l'Accepteur par tout moyen à sa convenance, ladite mesure prenant effet immédiatement. Les opérations de paiement seront alors portées sur un compte d'attente spécialement ouvert à cet effet, distinct et autonome du compte de l'Accepteur, pour n'être portées au crédit de ce dernier qu'après encaissement définitif par l'Acquéreur. Les fonds portés au crédit du compte d'attente demeurent indisponibles.

Dans les mêmes hypothèses, l'Acquéreur peut après avoir dans un premier temps inscrit une ou plusieurs opérations au compte de l'Accepteur, dès lors que le paiement n'est pas encore définitif et selon les mêmes modalités que celles définies aux alinéas précédents, procéder à la contre-passation desdites opérations afin de les inscrire sur le compte d'attente.

4.18 Les Schémas peuvent appliquer des pénalités aux Acquéreurs, calculées sur des bases identiques quel que soit l'Acquéreur, notamment :

- en cas de dépassement d'un certain nombre et/ou taux d'impayés généré(s) chez l'Accepteur, des pénalités mensuelles peuvent être appliquées après mise en demeure restée infructueuse,
- en cas de dépassement d'un certain nombre et/ou taux de fraude généré(s) chez l'Accepteur. A titre d'exemple, des pénalités allant jusqu'à 50% du montant de la fraude cumulée des six (6) derniers mois peuvent être appliquées,
- lorsque l'Accepteur dépasse un certain nombre de factures crédits, ou en cas d'usage inapproprié de la carte de domiciliation comme précisé à l'article 4.13,
- en cas de non-respect des obligations d'information de l'Acquéreur relatives à l'activité de l'Accepteur (ajout, modification, arrêt),
- en cas d'exercice par l'Accepteur d'une activité illicite comme précisé à l'article 4.2 des présentes Conditions Générales ou non-conforme avec les règles édictées par les Schémas,
- en cas d'utilisation d'un Système d'Acceptation non certifié par les Schémas comme précisé à l'article 1 et article 4.13
- en cas de déclaration erronée d'activité ou absence d'information de mise à jour de l'activité »
- en cas d'absence de déclaration de prestataire tiers ou technique ou correspondant au sein d'un prestataire technique en violation de l'article 4.14.

L'Accepteur reconnaît avoir été informé que l'exercice de certaines activités peut être interdit, ou soumis à restrictions ou autorisations par les Schémas.

4.19 Informer dans les meilleurs délais l'Acquéreur en cas de fonctionnement anormal de l'Équipement Électronique et de toutes autres anomalies.

4.20 En cas de survenance d'un incident de sécurité majeur, notamment en cas de collecte et/ou d'utilisation frauduleuse des données liées au paiement, coopérer avec l'Acquéreur et, le cas échéant, les autorités compétentes. Le refus ou l'absence de coopération de la part de l'Accepteur pourra conduire l'Acquéreur à résilier le présent Contrat conformément à l'article 10 des présentes.

4.21 Connaître et mettre en place des systèmes compatibles avec les dispositifs d'Authentification Forte du titulaire de la Carte mis en place par l'émetteur de la Carte lors d'une opération de paiements.

Dans le cas où, lors d'une opération de paiement, l'Accepteur n'appliquerait pas, le cas échéant, un dispositif d'Authentification Forte du titulaire de la Carte dans les conditions et selon les modalités prévues par l'émetteur de la Carte, l'Accepteur accepte expressément de rembourser les sommes relatives à l'opération de paiement litigieuse débitées à l'émetteur de la Carte, l'Acquéreur étant alors déchargé de toute responsabilité en cas de non-respect des dispositifs d'Authentification Forte du titulaire de la Carte mis en place par l'émetteur de la Carte par l'Accepteur.

4.22 L'Accepteur s'engage à respecter l'ensemble de la Règlementation Relative à la Protection des Données à Caractère Personnel, l'Acquéreur étant déchargé de toute responsabilité en cas de non-respect de ses obligations légales et réglementaires par l'Accepteur.

4.23 Garantir l'Acquéreur, et, le cas échéant, les Schémas, contre toute conséquence dommageable pouvant résulter pour eux du manquement aux obligations visées au présent article.

Article 5 – Obligations de l'Acquéreur

L'Acquéreur s'engage à :

5.1 Fournir à l'Accepteur les informations le concernant directement sur le fonctionnement du (des) Schéma(s) et son (leur) évolution.

5.2 Mettre à la disposition de l'Accepteur l'accès à son serveur d'autorisation pour les opérations de paiement.

5.3 Respecter le choix de la Marque et de la Catégorie de Carte utilisés pour le paiement au point d'acceptation.

5.4 Accepter les Paiements par Carte Sans Contact, si le Système d'Acceptation le permet.

5.5 Fournir à l'Accepteur la liste et les caractéristiques des Cartes (Marques et Catégories de Carte) pouvant être acceptées et lui fournir, à sa demande, le fichier des codes émetteurs (BIN).

5.6 Indiquer et facturer à l'Accepteur les commissions à acquitter, séparément pour chaque Catégorie de Carte et chaque Marque selon les différents niveaux d'interchange. L'Accepteur peut demander que les commissions soient regroupées par Marque, application de paiement, Catégorie de Carte et par taux de commission d'interchange applicable à l'opération.

5.7 Créditer le compte de l'Accepteur des sommes qui lui sont dues, selon les Conditions du présent contrat.

5.8 Ne pas débiter, au-delà du délai maximum de vingt-quatre (24) mois à partir de la date du crédit initial porté au compte de l'Accepteur les opérations non garanties et qui n'ont pu être imputées au compte de dépôt auquel la Carte est rattachée.

5.9 Communiquer, à la demande de l'Accepteur, les éléments essentiels des procédures administratives annexes, notamment dans le cadre de la gestion et restitution des Cartes oubliées par leurs titulaires.

5.10 Selon les modalités convenues avec l'Accepteur, communiquer au moins une (1) fois par mois, les informations suivantes pour la période écoulée :
- la référence lui permettant d'identifier l'opération de paiement,
- le montant de l'opération de paiement exprimé dans la devise dans laquelle son compte est crédité.

L'Accepteur peut demander que ces informations relatives aux opérations exécutées soient regroupées par Marque, application de paiement, Catégorie de Carte et par taux de commission d'interchange applicable à l'opération de paiement.

5.11 Communiquer chaque début d'année un relevé dit Relevé Annuel des Frais d'Encaissement par Carte (RAFEC), qui récapitule pour l'année écoulée les frais du (des) Schéma(s), les commissions de service payées par l'Accepteur et les commissions d'interchange par Marque et Catégorie de Carte.

Article 6 – Garantie du paiement

6.1 Les opérations de paiement, que ce soit en mode contact ou en mode "sans contact", sont garanties sous réserve du respect de l'ensemble des mesures de sécurité visées aux articles 4 « obligations de l'Accepteur » et 7 « mesures de sécurité » des présentes, ainsi qu'aux Conditions Spécifiques à chaque Schéma.

6.2 La délivrance additionnelle d'espèces à l'opération de paiement par Carte n'est pas garantie par le Présent Contrat.

6.3 Toutes les mesures de sécurité sont indépendantes les unes des autres. Ainsi, l'autorisation donnée par le système Acquéreur d'autorisation ne vaut garantie que sous réserve du respect des autres mesures de sécurité.

6.4 En cas de non-respect d'une seule de ces mesures, les opérations de paiement ne sont réglées que sous réserve de bonne fin d'encaissement, et ce, en l'absence de contestation.

6.5 L'Accepteur autorise expressément l'Acquéreur à débiter d'office son compte du montant de toute opération de paiement non garantie.

Article 7 – Mesures de sécurité

7.1 L'Accepteur doit informer immédiatement l'Acquéreur en cas de fonctionnement anormal de l'Équipement Électronique et/ou en cas d'autres anomalies (absence de reçu ou de mise à jour des listes d'opposition du Schéma, impossibilité de réparer rapidement, etc).
L'Accepteur doit coopérer avec l'Acquéreur lorsqu'il stocke, traite ou transmet des données de paiement sensibles, en cas d'incident de sécurité de paiement majeur ou de compromission de données.

7.2 Lors du paiement, l'Accepteur s'engage à :

7.2.1 Vérifier l'acceptabilité de la Carte c'est-à-dire :
- la Marque, la Catégorie de Carte du Schéma concerné et qui doivent être l'une de celles définies dans les Conditions Particulières,
- la présence sur la Carte de l'hologramme sauf pour les Cartes portant la marque V Pay,
- la puce sur la Carte lorsqu'elle est prévue par le Schéma concerné,
- le cas échéant, la période de validité (fin et éventuellement de début).

7.2.2 Utiliser l'Équipement Électronique, respecter les indications affichées sur son écran et suivre les procédures dont les modalités techniques lui ont été indiquées, ainsi que respecter et mettre en place, le cas échéant, des systèmes compatibles avec les dispositifs d'Authentification Forte du titulaire de la Carte mis en place par l'émetteur de la Carte. A défaut, l'opération ne sera pas garantie.

L'Équipement Électronique doit notamment :
- après la lecture de la puce des Cartes lorsqu'elle est présente :
  - permettre le contrôle du code confidentiel ou de l'empreinte biométrique apposée lorsque la puce le lui demande,
  - vérifier :
    - le code émetteur de la Carte (BIN),
    - le code service,
    - le cas échéant, la date de fin de validité de la Carte.
- lorsque la puce n'est pas présente, après lecture de la piste ISO 2, vérifier :
  - le code émetteur de la Carte (BIN),
  - le code service,
  - le cas échéant, la date de fin de validité de la Carte.

— lors d'un Paiement par Carte Sans Contact et d'un paiement mobile vérifier :
  - le code émetteur de la Carte (BIN),
  - le code service,
  - le cas échéant, la date de fin de validité de la Carte.

7.2.3 Contrôler le numéro de la Carte par rapport à la dernière liste des Cartes faisant l'objet d'un blocage ou d'une opposition diffusée par l'Acquéreur.

7.2.4 Lorsque la puce le demande à l'Équipement Électronique, faire composer par le titulaire de la Carte, dans les meilleures conditions de confidentialité, son code confidentiel ou procéder à son identification par apposition de son empreinte biométrique. La preuve de la frappe du code confidentiel ou du contrôle de l'empreinte biométrique du titulaire de la Carte est apportée par le certificat qui doit figurer sur le ticket émis par l'Équipement Électronique (ci-après "Ticket").

Lorsque le code confidentiel ou l'empreinte biométrique ne sont pas vérifiés, l'opération n'est réglée que sous réserve de bonne fin d'encaissement, même en cas de réponse positive à la demande d'autorisation.

7.2.5 En cas de Paiement par Carte Sans Contact effectué par une Carte physique dotée de la technologie sans contact et permise par l'Équipement Électronique, pour un montant inférieur à cinquante (50) euros, un montant cumulé ou un nombre de règlements successifs maximums et n'excédant pas ceux indiqués dans les Conditions Spécifiques du Schéma concerné, l'opération de paiement est réalisée sans frappe du code confidentiel ou sans apposition de l'empreinte biométrique. Elle est garantie sous réserve du respect des autres mesures de sécurité à la charge de l'Accepteur. Lorsqu'un certain nombre de règlements successifs ou qu'un certain montant cumulé de Paiement par Carte Sans Contact est atteint, l'Accepteur peut être amené à passer en mode contact même pour une opération de paiement d'un montant inférieur au montant unitaire maximum autorisé pour le Paiement par Carte Sans Contact.

En cas de Paiement par Carte Sans Contact effectué à l'aide d'un téléphone mobile et permis par l'Équipement Électronique, l'opération de paiement est garantie, sans frappe du code confidentiel ou sans contrôle de l'empreinte biométrique, quel que soit son montant, sous réserve du respect de l'ensemble des autres mesures de sécurité à la charge de l'Accepteur.

En toutes circonstances, l'Accepteur doit se conformer aux directives qui apparaissent sur l'Équipement Électronique.

7.2.6 Obtenir une autorisation d'un montant identique à l'opération :
— lorsque le montant de l'opération en cause, ou le montant cumulé des opérations réglées au moyen de la même Carte, dans la même journée et pour le même Point d'Acceptation, dépasse celui du seuil de demande d'autorisation fixé dans les Conditions Particulières, et ceci quelle que soit la méthode d'acquisition des informations,

— lorsque l'Équipement Électronique ou la Carte à puce déclenche une demande d'autorisation, indépendamment du seuil de demande d'autorisation fixé dans les Conditions Particulières.

A défaut, l'opération ne sera pas garantie, même pour la fraction autorisée ou correspondant au montant du seuil de demande d'autorisation.

Lorsque la puce n'est pas présente sur une Carte, l'autorisation doit être demandée en transmettant l'intégralité des données de la piste ISO 2.

Une opération pour laquelle l'autorisation a été refusée par le système Acquéreur d'autorisation n'est jamais garantie.

Une demande de capture de Carte, faite par l'émetteur de la Carte, annule la garantie pour toutes les opérations de paiement faites postérieurement le même jour et avec la même Carte, dans le même Point d'Acceptation.

7.2.7 Faire signer le Ticket dans tous les cas où l'Équipement Électronique le demande.

7.2.8 Mettre à disposition du titulaire de la Carte l'exemplaire du Ticket qui lui est destiné, sous forme papier ou dématérialisée (sous réserve de disponibilité du format).

7.3 Après le paiement, l'Accepteur s'engage à :

7.3.1 Transmettre les enregistrements des opérations de paiement à l'Acquéreur dans le délai maximum de trois (3) jours calendaires à compter de la date de l'opération de paiement. Au-delà de ce délai, les opérations de paiement ne seront réglées que sous réserve de bonne fin d'encaissement.

S'assurer que les opérations de paiement ont bien été imputées au compte dans les délais et selon les modalités prévus dans les Conditions Particulières. Toute opération ayant fait l'objet d'une autorisation transmise par l'Acquéreur doit être obligatoirement remise à ce dernier.

7.3.2 Archiver et conserver dans un environnement sécurisé, à titre de justificatif, pendant vingt-quatre (24) mois après la date de l'opération :
— un exemplaire du Ticket comportant, lorsqu'elle est requise, la signature du titulaire de la Carte,
— l'enregistrement magnétique représentatif de l'opération de paiement ou le journal de fond lui-même.

7.3.3 Communiquer, à la demande de l'Acquéreur, tout justificatif des opérations de paiement dans les huit (8) jours calendaires à compter de la date de la demande présentée par l'Acquéreur. Si l'Accepteur ne communique pas le justificatif, ou le communique au-delà du délai ci-dessus, il s'expose à un impayé.

7.3.4 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 de paiement par Carte ainsi que le contrôle de l'accès à celles-ci et ce, conformément aux prescriptions de la Règlementation Relative à la Protection des Données à Caractère Personnel.

7.3.5 Ne pas stocker, sous quelque forme que ce soit, les données suivantes de la Carte :
— le cryptogramme visuel,
— la piste magnétique dans son intégralité,
— le code confidentiel ou l'empreinte biométrique.

7.3.6 Les mesures de sécurité et de prévention des risques énumérées au présent article pourront être modifiées et complétées pendant toute la durée du Présent Contrat, selon la procédure prévue à l'article 9.

Article 8 – Mesures de prévention et de sanction prises par l'Acquéreur

8.1 Avertissement

8.1.1 En cas de manquement de l'Accepteur aux stipulations du présent Contrat ou aux lois en vigueur, ou en cas de constat d'un taux d'impayés anormalement élevé ou d'utilisation anormale de Cartes perdues, volées ou contrefaites, l'Acquéreur peut prendre des mesures de sauvegarde et de sécurité consistant, en un avertissement valant mise en demeure, précisant les mesures à prendre pour remédier au manquement constaté ou résorber le taux d'impayés anormalement élevé.

8.1.2 Si, l'Accepteur n'a pas remédié au manquement ayant justifié l'avertissement ou n'a pas mis en œuvre les mesures destinées à résorber le taux d'impayés constaté, l'Acquéreur peut soit procéder à une suspension de l'acceptation des Cartes, soit résilier de plein droit, avec effet immédiat, le présent Contrat dans les conditions fixées aux articles 8.2 et 10 des présentes.

8.2 Suspension de l'acceptation - Pénalités

8.2.1 L'Acquéreur peut procéder, pour des raisons de sécurité, sans préavis et sous réserve du dénouement des opérations en cours, à une suspension de l'acceptation des Cartes portant certaines Marques par l'Accepteur. Elle est notifiée par tout moyen et doit être motivée. Son effet est immédiat.
Elle peut s'accompagner d'un avertissement, voire d'une réduction du seuil de demande d'autorisation de l'Accepteur. Son effet est immédiat.
La suspension ne porte pas préjudice à la faculté des Parties de résilier le Contrat conformément à la procédure visée à l'article 10 des présentes. Notamment, l'Accepteur pourra, en cas de suspension, résilier le Contrat avec effet immédiat.

8.2.2 La suspension peut être décidée en raison notamment :

- d'un ou plusieurs manquement(s) aux clauses du Contrat et notamment aux exigences sécuritaires, qui serait (ent) révélé(s) au terme de la procédure d'audit visée à l'article 4 des présentes ;
- du non-respect répété des obligations du présent Contrat et du refus d'y remédier, ou d'un risque de dysfonctionnement important du Système d'Acceptation d'un Schéma,
- d'une participation à des activités frauduleuses, notamment d'une utilisation anormale de Cartes perdues, volées ou contrefaites,
- d'un refus d'acceptation répété et non motivé de la (des) Marque(s) et/ou Catégorie(s) de Carte qu'il a choisi (s) d'accepter ou qu'il doit accepter,
- de plaintes répétées d'autres membres ou partenaires d'un Schéma et qui n'ont pu être résolues dans un délai raisonnable,
- de retard volontaire ou non motivé de transmission des justificatifs,
- d'un risque aggravé en raison des activités de l'Accepteur,
- du non-respect, le cas échéant, des dispositifs d'Authentification Forte du titulaire de la Carte mis en place par l'émetteur de la Carte.

8.2.3 L'Accepteur s'engage alors à restituer à la CSB, le cas échéant, l'Équipement Électronique, les dispositifs techniques et sécuritaires et les documents en sa possession dont l'Acquéreur est propriétaire, et à retirer immédiatement de son Point d'Acceptation tout signe d'acceptation des Cartes concernées.

8.2.4 La période de suspension est au minimum de six (6) mois, renouvelable. À l'expiration de ce délai, l'Accepteur peut, demander la reprise du présent Contrat auprès de l'Acquéreur, ou souscrire un nouveau contrat d'acceptation en paiement de proximité par carte avec un autre acquéreur de son choix.

8.2.5 À tout moment, l'Accepteur peut présenter ses observations sur la suspension.

8.2.6 Si l'Accepteur n'a pas remédié dans un délai raisonnable au manquement ayant justifié l'avertissement ou n'a pas mis en œuvre les mesures destinées à résorber le taux d'impayés constaté ou qu'une suspension de l'acceptation a été décidée, l'Acquéreur peut en outre lui répercuter les pénalités appliquées par les Schémas de paiement en application de l'article 4.18. Dans ce cadre, l'Accepteur accepte expressément de prendre en charge ces pénalités et autorise l'Acquéreur à prélever le montant de la pénalité sur le compte désigné aux Conditions Particulières.

Article 9 – Modifications du contrat

9.1 L'Acquéreur peut modifier à tout moment les dispositions du Contrat, après en avoir informé l'Accepteur avant la date d'entrée en vigueur des nouvelles dispositions.
L'Acquéreur peut notamment apporter :

- des modifications techniques telles que l'acceptabilité de nouvelles Cartes, les modifications de logiciel, le changement de certains paramètres, la remise en l'état du système d'Acceptation si celui-ci est mis à disposition par l'Acquéreur suite à un dysfonctionnement ;
- des modifications sécuritaires telles que :
  - la suppression de l'acceptabilité de certaines Cartes,
  - la suspension de l'acceptabilité de Cartes portant certaines Marques,
  - la modification du seuil d'autorisation.

9.2 Les nouvelles conditions entrent en principe en vigueur au terme d'un délai minimum fixé à un (1) mois à compter de l'envoi de notification sur support papier ou tout autre support durable.

9.3 Ce délai peut exceptionnellement être réduit en cas de modification(s) motivée(s) par des raisons sécuritaires notamment lorsque l'Acquéreur constate, dans le point d'acceptation une utilisation anormale de Cartes perdues, volées ou contrefaites.

9.4 Dans les délais visés au présent article, l'Accepteur peut résilier le présent Contrat s'il refuse les modifications opérées, dans les conditions prévues à l'article 10 des présentes. À défaut de résiliation dans ces délais, les modifications lui seront opposables.

9.5 Le non-respect des nouvelles conditions techniques ou sécuritaires dans les délais impartis peut entraîner la suspension de l'acceptation des cartes du Schéma concerné voire, la résiliation du présent Contrat par l'Acquéreur, selon les dispositions prévues à cet effet aux articles 8.2 et 10 des présentes.

Article 10 – Durée et résiliation du contrat

10.1 Le présent contrat est conclu pour une durée indéterminée, sauf accord contraire des parties.

10.2 L'Accepteur ou l'Acquéreur, peuvent chacun, et à tout moment, sans justificatif sous réserve du dénouement des opérations en cours, mettre fin au présent Contrat, sans qu'il soit nécessaire de

n'accomplir aucune autre formalité que l'envoi à l'autre Partie d'une lettre recommandée avec demande d'avis de réception.
Lorsque cette résiliation fait suite à un désaccord sur les modifications prévues à l'article 9 ci-dessus, elle prend effet à l'issue du délai prévu dans cet article pour l'entrée en vigueur de ces modifications.
Lorsque cette résiliation fait suite à une cessation d'activité de l'Accepteur, cession ou mutation du fonds de commerce, elle prend effet immédiatement.
Lorsque la résiliation intervient à la demande d'un Schéma ou de l'Acquéreur lui-même, pour des raisons de sécurité ou de fraude, notamment pour l'une des raisons visées aux articles 4 « obligations de l'Accepteur » et 7 « mesures de sécurité » des présentes, elle pourra prendre effet immédiatement.
Selon la gravité des faits concernés, cette résiliation immédiate peut intervenir à la suite d'un avertissement et d'une mesure de suspension de l'acceptation prévus à l'article 8 des présentes.

10.3 En cas de résiliation, l'Accepteur garde la faculté d'accepter les Cartes de tout Schéma avec tout autre Acquéreur de son choix.
Dans le cas où, après résiliation du présent Contrat, il se révélerait des impayés, ceux-ci seront à la charge de l'Accepteur ou pourront faire l'objet d'une déclaration de créances.

10.4 L'Accepteur sera tenu de restituer à l'Acquéreur l'Equipement Électronique, les dispositifs techniques et sécuritaires, le Système d'Acceptation et les documents en sa possession dont la CSB est propriétaire.
Sauf dans le cas où il a conclu un ou plusieurs autres contrats d'acceptation, l'Accepteur s'engage à retirer immédiatement de son point d'Acceptation et de ses supports de communication tout signe d'acceptation des Cartes, ou Marques des Schémas concernés.

Article 11 – Modalités annexes de fonctionnement

11.1 Réclamation

11.1.1 Généralités

Toute réclamation de l'Accepteur doit être justifiée et formulée par écrit à l'Acquéreur, dans un délai maximum de six (6) mois à compter de la date de l'opération contestée, sous peine de forclusion. Toutefois, ce délai est réduit à quinze (15) jours calendaires à compter de la date de débit en compte résultant d'une opération de paiement non garantie, notamment en cas d'impayé.

11.1.2 Délai de réponse à une réclamation

Pour toute réclamation liée exclusivement à des services de paiement assurés par l'Acquéreur dans le cadre du Présent Contrat, l'Acquéreur apportera une réponse à l'Accepteur dans les quinze jours ouvrables suivant la réception de la réclamation.
Si, pour des raisons échappant au contrôle de l'Acquéreur, une réponse ne peut être apportée dans les quinze jours ouvrables, l'Acquéreur adressera à l'Accepteur une réponse d'attente motivant le délai requis pour répondre et précisant la date ultime de la réponse définitive à la réclamation. En tout état de cause, l'Accepteur recevra une réponse définitive au plus tard trente-cinq jours ouvrables suivant la réception de la réclamation.

Il n'a pas été prévu d'adhérer à une instance de règlement extrajudiciaire pour les réclamations relatives aux services relevant du Présent Contrat.

11.2 Convention de preuve

De convention expresse entre les Parties, les enregistrements électroniques constituent la preuve des opérations de paiement remises à l'Acquéreur. En cas de conflit, les enregistrements électroniques produits par l'Acquéreur ou le Schéma prévaudront sur ceux produits par l'Accepteur, à moins que ce dernier ne démontre l'absence de fiabilité ou d'authenticité des documents produits par l'Acquéreur ou le Schéma dont les Cartes sont concernées.

11.3 Remboursement

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 avec les données de la Carte utilisée pour l'opération initiale. L'Accepteur doit alors utiliser la procédure dite de remboursement en effectuant, dans le délai prévu par l'article 4.10 des présentes Conditions Générales, le remboursement à l'Acquéreur à qui il avait remis l'opération initiale. Le montant du remboursement ne doit pas dépasser le montant de l'opération initiale. De plus, il est demandé systématiquement une autorisation à l'émetteur pour réaliser une transaction de remboursement et/ou sur le retour de marchandises, dès que le terminal de paiement électronique propose la fonctionnalité.

11.4 Oubli d'une Carte par son titulaire

Une carte capturée ou une carte oubliée doit être déposée par l'accepteur auprès de l'agence de son acquéreur (ou tout autre site sous la responsabilité de l'Acquéreur CB), dans un délai maximum de deux jours ouvrés.

11.5 Carte non signée

En cas de Carte non signée et si le panonceau de signature est présent sur la Carte, l'Accepteur 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, l'Accepteur doit refuser le paiement par Carte.

11.6 Dysfonctionnement

L'Acquéreur et l'Accepteur ne peuvent être tenus pour responsable de l'impossibilité d'effectuer le paiement en cas de dysfonctionnement de la Carte et/ou de son support.

Article 12 – Secret bancaire et protection des données à caractère personnel

12.1 Secret bancaire

De convention expresse, l'Accepteur autorise l'Acquéreur à stocker le cas échéant des données secrètes ou confidentielles portant sur lui, et les communiquer à des entités impliquées dans le fonctionnement du(des) Schéma(s) aux seules finalités de traiter les opérations de paiement, de prévenir des fraudes et de traiter les réclamations, qu'elles émanent des Titulaires de Cartes ou d'autres entités.

12.2 Protection des données à caractère personnel

Lors de la signature ou de l'exécution des présentes, chacune des parties peut avoir accès à des données à caractère personnel.
En application de la Réglementation Relative à la Protection des Données à Caractère Personnel, il est précisé que :

- les informations relatives à l'Accepteur, collectées par l'Acquéreur, nécessaires pour l'exécution des ordres de paiement transmis et leur sécurisation, ne seront utilisées et ne feront l'objet de diffusion auprès d'entités tierces que pour les seules finalités de traitement des opérations de paiement par Carte, données en exécution du présent Contrat, ou pour répondre aux obligations légales et réglementaires, l'Acquéreur étant à cet effet, de convention expresse, délié du secret bancaire.

Dans le cadre de la signature et de l'exécution du présent Contrat, et plus généralement de la relation entre l'Acquéreur et l'Accepteur personne physique, ou la personne physique le représentant, l'Acquéreur recueille
et traite, en tant que responsable de traitement, des données à caractère personnel concernant l'Accepteur et/ou la personne physique le représentant.
Ces traitements ont pour finalités :

- la gestion de la relation commerciale pour l'exécution du Présent Contrat,
- la lutte contre la fraude, le blanchiment de capitaux et le financement du terrorisme.

Ces traitements sont obligatoires. À défaut, l'exécution du Contrat ne pourrait être assurée et l'Acquéreur ne serait en mesure de respecter ses obligations réglementaires.
Certaines informations doivent être collectées afin de répondre aux obligations légales, réglementaires ou contractuelles de l'Acquéreur, ou conditionnent la conclusion du Contrat. L'Accepteur sera informé le cas échéant des conséquences d'un refus de communication de ces informations.
Dans les limites et conditions autorisées par la Réglementation Relative à la Protection des Données à Caractère Personnel, l'Accepteur peut :

- demander à accéder aux données personnelles le concernant et/ou en demander la rectification ou l'effacement ;
- s'opposer au traitement de données personnelles le concernant ;
- retirer son consentement à tout moment ;
- demander des limitations au traitement des données personnelles le concernant ;
- demander la portabilité de ses données personnelles.

Les informations expliquant pourquoi et comment ces données sont utilisées, combien de temps elles seront conservées, ainsi que les droits dont l'Accepteur et/ou son représentant disposent quant à leur usage par l'Acquéreur, figurent dans la notice d'information sur le traitement des données à caractère personnel de l'Acquéreur (la « Notice »).

Cette Notice est portée à la connaissance de l'Accepteur lors de la première collecte de ses données et/ou de celles de son représentant.
L'Accepteur et/ou son représentant peuvent y accéder à tout moment sur le site Internet de l'Acquéreur ou en obtenir un exemplaire auprès d'une agence de l'Acquéreur.
L'Accepteur s'engage à informer son représentant de cette collecte de données et des droits dont il dispose en vertu de la Réglementation Relative à la Protection des Données à Caractère Personnel et du présent article. Il s'engage également à l'informer de l'existence de la Notice et des modalités pour y accéder.

À l'occasion de l'exécution des ordres de paiement donnés par Carte, l'Accepteur peut avoir accès à différentes données à caractère personnel concernant notamment les Titulaires de la Carte, à savoir le numéro de carte, le cryptogramme visuel et le cas échéant, l'identité du titulaire de la carte, sa date de fin de fin de validité, sans que cette liste soit exhaustive, dont il doit garantir la sécurité et la confidentialité conformément aux dispositions du présent Contrat et à la Réglementation Relative à la Protection des Données à Caractère Personnel.

Dans le cadre du présent Contrat, l'Accepteur ne peut utiliser ces données à caractère personnel que pour l'exécution des ordres de paiement par Carte.
En tant que responsable de traitement au sens de la Règlementation Relative à la Protection des Données à Caractère Personnel lorsqu'il traite les données personnelles de ses clients et notamment des titulaires de Carte, l'Accepteur doit respecter les obligations prévues par la Règlementation Relative à la Protection des Données à Caractère Personnel, et notamment les principes de licéité, de loyauté et de transparence des traitements, les droits des personnes et la mise en œuvre de mesures techniques et organisationnelles appropriées pour assurer la confidentialité et l'intégrité des données à caractère personnel qu'il est amené à traiter dans le cadre de son activité et notamment, celles des titulaires de Carte, sous peine d'engager sa seule responsabilité.

12.3 Prospection commerciale

L'Accepteur doit recueillir le consentement exprès et préalable du titulaire de Carte lors de toute utilisation de ses données de contact (notamment, son adresse mail et de son numéro de mobile) à des fins de prospection commerciale.
L'Accepteur s'engage à chaque envoi d'une nouvelle proposition commerciale à informer le titulaire de la Carte de sa possibilité de se désabonner et des modalités y afférentes. L'Accepteur s'engage enfin à respecter ces dispositions et à supprimer de ses propres bases de données, les données personnelles du titulaire de la Carte
relatives à la prospection commerciale si ce dernier en fait la demande auprès de l'Accepteur, l'Acquéreur étant déchargé de toute responsabilité en cas de non-respect de ces obligations légales et réglementaires par l'Accepteur.

Article 13 – Litiges commerciaux

L'Accepteur s'engage à faire son affaire personnelle de tous litiges de nature commerciale ou autre, ou/et de leurs conséquences financières, pouvant survenir avec des clients, adhérents ou donateurs, concernant des biens et services, cotisations ou dons ayant été réglés par Carte au titre du Présent Contrat.

Article 14 – Non-renonciation

Le fait, pour l'Accepteur ou pour l'Acquéreur 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 15 – Loi applicable/tribunaux compétents

Le présent Contrat et toutes les questions qui s'y rapportent seront régis par la loi en vigueur sur le Territoire de la Nouvelle-Calédonie, et tout différend relatif à l'interprétation, la validité, et/ou l'exécution du présent Contrat sera soumis à la compétence des tribunaux de Nouméa, y compris les procédures tendant à obtenir des mesures d'urgence ou conservatoires, en référé ou sur requête.

Article 16 – Langue du présent contrat

Le présent Contrat est le contrat original rédigé en langue française qui est le seul qui fait foi.

Article 17 – Confidentialité

Chacune des deux Parties ne communiquera aucune information et ne publiera aucun communiqué en relation avec l'existence des Conditions Générales, Particulières et Spécifiques, et de leurs annexes ou leur contenu sans l'accord préalable de l'autre Partie, sauf si la communication de l'information ou la publication du communiqué est rendue obligatoire par une disposition légale ou réglementaire s'imposant à la partie concernée, ou pour répondre à une demande d'une autorité judiciaire ou administrative (gouvernementale, bancaire, fiscale ou autre autorité réglementaire similaire).

PARTIE II - CONDITIONS SPÉCIFIQUES - propres à chaque Schéma

SECTION 1
Conditions spécifiques pour les opérations réalisées selon le Schéma « CB »

Article préliminaire

Les règles ci-après s'appliquent lorsque le titulaire de la Carte et l'Accepteur sont d'accord pour réaliser l'opération de paiement par carte selon les règles du Schéma « CB ».

Article 1 – Conditions liées à la garantie de paiement des opérations de paiement « CB »

La garantie de paiement est conditionnée par le respect des conditions prévues au présent Contrat.

Le montant du seuil de demande d'autorisation pour une opération de paiement « CB », par jour et par point d'acceptation, au jour de la signature du Contrat est fixé dans les Conditions Particulières. Ce montant peut être modifié ultérieurement.

Ce montant ne s'applique pas aux Cartes pour lesquelles une autorisation doit être demandée à chaque opération de paiement dès le 1er Franc.

Operations de Paiement par Carte Sans Contact
A des fins de sécurité, le montant unitaire maximum de chaque opération de paiement en mode "sans contact" réalisée dans le Schéma "CB" avec la Carte physique est limité à cinquante (50) euros. De plus, l'émetteur de la Carte peut limiter le nombre (dans la limite d'un nombre maximum de cinq (5) opérations de Paiement par Carte Sans Contact) ou le montant cumulé maximum des règlements successifs en mode "sans contact" à un montant de cent-cinquante (150) euros depuis la dernière utilisation, par le titulaire de la Carte, d'un dispositif d'Authentification Forte mis en place par l'émetteur de la Carte au sens du Règlement délégué UE 2018/389 du 27 novembre 2017.
En conséquence, au-delà de ce nombre maximum d'opérations successives autorisées ou de ce montant cumulé maximum, une opération de paiement avec utilisation du dispositif d'Authentification Forte mis en place par l'émetteur et notamment par frappe du code confidentiel ou de l'apposition de l'empreinte biométrique doit être effectuée par le titulaire de la Carte pour continuer à l'utiliser en mode "sans contact" et réinitialiser le montant cumulé et le nombre cumulé maximum disponibles.

Article 2 – Délai maximum de transmission des opérations de paiement « CB » à l'Acquéreur

L'Accepteur s'engage à transmettre à l'Acquéreur les opérations de paiement réalisées selon les règles du Schéma CB dans un délai maximum de **6 mois**. Au-delà de ce délai maximum, l'encaissement des opérations de paiement n'est plus réalisable dans le cadre du Schéma « CB ».

Ce délai de 6 mois est un délai distinct du délai conditionnant la garantie de paiement prévu à l'article 6 et 7 des présentes.

Article 3 – Suspension et clôture du contrat pour le schéma « CB »

3.1 Le Schéma « CB » peut procéder, pour des raisons de sécurité, sans préavis et sous réserve du dénouement des opérations en cours, à une suspension de l'acceptation des Cartes du Schéma « CB ». Elle est précédée, le cas échéant, d'un avertissement à l'Accepteur, 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'une utilisation d'un Système d'acceptation non agréé,
- d'un risque de dysfonctionnement important du Schéma « CB »,
- en cas de comportement frauduleux de la part de l'Accepteur responsable du Point d'acceptation.

3.2 L'Accepteur s'engage alors à retirer immédiatement de son point d'acceptation tout signe d'acceptation des Cartes « CB » ou de la Marque « CB ».

3.3 La période de suspension est au minimum de 6 mois, éventuellement renouvelable.

3.4 À l'expiration de ce délai, l'Accepteur peut, sous réserve de l'accord préalable du Schéma « CB », demander la reprise d'effet de son contrat auprès de l'Acquéreur, ou souscrire un nouveau contrat d'acceptation avec un autre Acquéreur de son choix.

3.5 En cas de comportement frauduleux de la part de l'Accepteur, il peut être immédiatement radié du Schéma « CB » ou la suspension être convertie en radiation.

Article 4 – Protection des données à caractère personnel

L'Acquéreur, au titre de l'acceptation en paiement par Carte dans le Système « CB », informe que le GIE « CB » traite des données à caractère personnel de l'Accepteur (personne physique ou personne physique le représentant) qui concernent notamment son identité et ses fonctions.
Ces données à caractère personnel font l'objet de traitements afin de permettre :

- la lutte contre la fraude et la gestion des éventuels recours en justice, conformément aux missions définies dans les statuts du GIE « CB » (intérêt légitime) ;
- de répondre aux obligations réglementaires ou légales notamment en matière pénale ou administrative liées à l'utilisation de la Carte (obligation légale).

Le détail des données personnelles traitées par le GIE « CB », de leurs durées de conservation, des destinataires de ces données et des mesures de sécurités mises en œuvre pour les protéger, peut être consulté dans sa politique de protection des données personnelles accessible à :
www.cartes-bancaires.com/protegezvosdonnees.

Pour exercer les droits prévus en application de la Réglementation Relative à la Protection des Données à Caractère Personnel, et notamment les droits d'accès, de rectification et d'effacement des données ainsi que les droits d'opposition et de limitation du traitement, l'Accepteur (personne physique ou personne physique le représentant) peut contacter le Délégué à la protection des données du Schéma « CB » par courriel à protegezvosdonnees@cartes-bancaires.com.
Pour toute question en lien avec la protection des données à caractère personnel traitées par le GIE « CB », l'Accepteur

(personne physique ou personne physique le représentant sur laquelle portent les données à caractère personnel) peut également contacter son Délégué à la protection des données désigné par le GIE « CB » par courriel à : protegezvosdonnees@cartes-bancaires.com.

SECTION 2
Conditions spécifiques d'acceptation en paiement à distance sécurisé pour les opérations réalisées selon les Schémas « Visa », « Visa Electron » ou « VPAY »

Article préliminaire

Les règles ci-après s'appliquent lorsque le titulaire de la Carte et l'Accepteur sont d'accord pour réaliser l'opération de paiement par carte selon les règles des Schémas « VISA », « Visa Electron » ou « VPAY ».

Article 1 – Conditions liées à la garantie de paiement des opérations de paiement « Visa », « Visa Electron ou « VPAY »

La garantie de paiement est conditionnée par le respect des conditions du Présent Contrat.

1.1 **Seuil d'autorisation**
Quel que soit le montant de l'opération de paiement, une demande d'autorisation doit systématiquement être faite pour une opération de paiement réalisée selon les Schémas « Visa », « Visa Electron » ou « VPAY », que ce soit une carte étrangère ou française, qu'elle soit cobadgée avec un autre Schéma ou non.
Il est demandé systématiquement une autorisation pour réaliser une transaction de remboursement et/ou sur le retour de marchandises, lorsque le terminal de paiement électronique propose la fonctionnalité.

1.2 **Mesures de sécurité particulières : opérations de paiement avec Carte sans puce**
Dans le cas où la puce n'est pas présente sur la Carte (cas de certaines Cartes étrangères), l'Accepteur est en droit de vérifier l'identité de son titulaire. L'Accepteur est également en droit de demander l'identité du titulaire si le panonceau de signature est présent sur la Carte et que la Carte n'est pas signée.

1.3 **Operations de Paiement par Carte Sans Contact**
A des fins de sécurité, le montant unitaire maximum de chaque opération de paiement en mode "sans contact" réalisée dans le Schéma "Visa", "Visa Electron" ou "VPAY" avec la Carte physique est limité à cinquante (50) euros. De plus, l'émetteur de la Carte peut limiter le nombre (dans la limite d'un nombre maximum de cinq (5) opérations de Paiement par Carte Sans Contact) ou le montant cumulé maximum des règlements successifs en mode "sans contact" à un montant de cent-cinquante (150) euros depuis la dernière utilisation, par le titulaire de la Carte, d'un dispositif d'Authentification Forte mis en place par l'émetteur de la Carte.
En conséquence, au-delà de ce nombre maximum d'opérations successives autorisées ou de ce montant cumulé maximum, une opération de paiement avec utilisation du dispositif d'Authentification Forte mis en place par l'émetteur et notamment par frappe du code confidentiel ou de l'apposition de l'empreinte biométrique doit être effectuée par le titulaire de la Carte pour continuer à l'utiliser en mode "sans contact" et réinitialiser le montant cumulé et le nombre cumulé maximum disponibles.

Article 2 – Suspension ou clôture du contrat à la demande des schémas « Visa », « Visa Electron ou « VPAY »

Les Schémas Visa, « Visa Electron » ou « VPAY » peuvent dans certains cas (cf. articles 4 « obligations de l'Accepteur » des présentes) se retourner vers l'Acquéreur pour que celui-ci exige de son Accepteur qu'il respecte les règles des Schémas « Visa », « Visa Electron » ou « VPAY », faute de quoi l'Acquéreur sera dans l'obligation de résilier le présent Contrat.

Article 3 – Acceptation des cartes « Visa », « Visa Electron ou « VPAY » émises hors UE

Les Cartes des Schémas « Visa », « Visa Electron » ou « VPAY » émises par un émetteur situé hors de l'UE sont systématiquement acceptées par l'Accepteur si celui-ci accepte au moins un type de Carte des Schémas Visa, « Visa Electron » ou « VPAY ».

Article 4 – Communication des Commissions Interbancaires de Paiement (interchange) de "Visa"," Visa Electron" ou "VPAY"

Les taux de commissions d'interchange pratiqués par les Schémas "Visa"," Visa Electron" ou "VPAY" sont publics et consultables sur le site internet : www.visa.co.uk.

SECTION 3
Conditions spécifiques d'acceptation en paiement à distance sécurisé pour les opérations réalisées selon les Schémas « Mastercard » ou « Maestro »

Article préliminaire

Les règles ci-après s'appliquent lorsque le titulaire de la Carte et l'Accepteur sont d'accord pour réaliser l'opération de paiement par Carte selon les règles des Schémas « Mastercard » ou « Maestro ».

Article 1 – Conditions liées à la garantie de paiement des opérations de paiement « Mastercard » ou « Maestro »

La garantie de paiement est conditionnée par le respect des conditions prévues au présent Contrat.

1.1 **Seuil d'autorisation**
Quel que soit le montant de l'opération de paiement, une demande d'autorisation doit systématiquement être faite pour une opération de paiement réalisée selon les Schémas Mastercard ou Maestro.

1.2 **Mesures de sécurité particulières : opérations de paiement avec Carte sans puce**
Dans le cas où la puce n'est pas présente sur la Carte (cas de certaines Cartes étrangères), l'Accepteur est en droit de vérifier l'identité de son titulaire. L'Accepteur est également en droit de demander l'identité du titulaire de la Carte si la date de validité de sa Carte a expiré.

1.3 **Opérations de Paiement par Carte sans Contact**
A des fins de sécurité, le montant unitaire maximum de chaque opération de paiement en mode "sans contact" réalisée dans le Schéma "Mastercard" ou "Maestro" avec la Carte physique est limité à cinquante (50) euros. De plus, l'émetteur de la Carte peut limiter le nombre (dans la limite d'un nombre maximum de cinq (5) opérations de Paiement par Carte Sans Contact) ou le montant cumulé maximum des règlements successifs en mode "sans contact" à un montant de cent-cinquante (150) euros depuis la dernière utilisation, par le titulaire de la Carte, d'un dispositif d'Authentification Forte mis en place par l'émetteur de la Carte.
En conséquence, au-delà de ce nombre maximum d'opérations successives autorisées ou de ce montant cumulé maximum, une opération de paiement avec utilisation du dispositif d'Authentification Forte mis en place par l'émetteur et notamment par frappe du code confidentiel ou de l'apposition de l'empreinte biométrique doit être effectuée par le titulaire de la Carte pour continuer à l'utiliser en mode "sans contact" et réinitialiser le montant cumulé et le nombre cumulé maximum disponibles.

Article 2 – Suspension ou clôture du contrat à la demande des schémas « Mastercard » ou « Maestro »

Les Schémas Mastercard ou Maestro peuvent dans certains cas (cf. articles 4 « obligations de l'Accepteur » des présentes) se retourner vers l'Acquéreur pour que celui-ci exige de son Accepteur qu'il respecte les règles des Schémas Mastercard ou Maestro, faute de quoi l'Acquéreur sera dans l'obligation de résilier le présent Contrat.

Article 3 – Acceptation des cartes « Mastercard » ou « Maestro » émises hors Union Européenne

Les Cartes des Schémas Mastercard ou Maestro émises par un émetteur situé hors de l'UE sont systématiquement acceptées par l'Accepteur si celui-ci accepte au moins un type de Carte des Schémas Mastercard ou Maestro émis dans l'Union Européenne.

Article 4 – Communication des commissions interbancaires de paiement (interchange) de « Mastercard » ou « Maestro »

Les taux de commissions d'interchange pratiqués par les Schémas Mastercard ou Maestro sont publics et consultables sur le site Internet : www.mastercard.com.

Annexe 1
RÉFÉRENTIEL SÉCURITAIRE ACCEPTEUR

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.
Le Personnel doit être sensibilisé aux risques encourus, notamment sur la divulgation d'informations confidentielles, et l'accès non autorisé aux informations, aux supports et aux documents.
Le Personnel doit être régulièrement sensibilisé 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 le Personnel reçoive 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 Clients 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 corrigibles.
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 de paiement 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 ou 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 protégés 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 antivirus 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 antivirus 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 pour fixer le code 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 assurées 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 l'Accepteur.
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 de l'Accepteur 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.

Annexe 2

PRÉSENTATION GÉNÉRALE SUR LES RÈGLES PCI-DSS

PCI DSS[1] est un standard de sécurité conçu et maintenu par le PCI-SSC, un organisme fondé par Visa, Mastercard, American Express, Discover et Japan Credit Bureau (JCB).

Le numéro de carte, la date de fin de validité, le cryptogramme visuel et les données de la piste magnétique sont des données sensibles. Celles-ci permettent aux fraudeurs de réaliser des paiements sur Internet sans présence physique de la carte. Lorsque les fraudeurs arrivent à s'en emparer, ils peuvent réaliser des paiements sans même détenir la carte.
Ainsi les exigences PCI DSS visent à sécuriser les données des cartes bancaires de vos clients. Le non-respect de ce standard de sécurité expose votre activité commerciale à des risques en termes financiers, d'image et de chiffre d'affaires.

La politique PCI DSS

Elle s'adresse à tous les commerçants ou leurs prestataires de services hébergeurs qui collectent, stockent, transportent et traitent des données de cartes bancaires.

Les 12 exigences PCI DSS

- Installer et gérer une configuration de pare-feu pour protéger les données des titulaires de cartes.
- Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur.
- Restreindre l'accès aux données des titulaires de cartes aux seuls individus qui doivent les connaître.
- Affecter un identifiant unique à chaque utilisateur d'ordinateur.
- Protéger les données des titulaires de cartes stockées.
- Restreindre l'accès physique aux données des titulaires de cartes.
- Crypter la transmission des données des titulaires de cartes sur les réseaux publics ouverts.
- Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données des titulaires de cartes.
- Utiliser des logiciels antivirus et les mettre à jour régulièrement.
- Tester régulièrement les processus et les systèmes de sécurité.
- Développer et gérer des systèmes et des applications sécurisés.
- Gérer une politique de sécurité des informations.

L'évaluation PCI DSS

L'évaluation PCI DSS s'effectue par un audit réalisé par un auditeur agréé ou via un questionnaire d'auto-évaluation. En fonction du nombre de paiement par carte que vous acceptez chaque année, vous pouvez être classé dans l'un des quatre niveaux définis par les réseaux internationaux Visa et Mastercard.

Niveau	Type d'activité	Actions requises pour la conformité
1	• Tout commerçant traitant plus de 6 millions de transactions par an Visa ou MasterCard (toutes transactions confondues) • Tout commerçant ayant subi une compromission	Audit de sécurité sur site (ou SAQ(2) pour Visa Europe) Scan de vulnérabilité trimestriel (si commerce en ligne)
2	Tout commerçant traitant de 1 à 6 millions de transactions par an Visa ou MasterCard (toutes transactions confondues)	Questionnaire d'auto-évaluation annuel Scan de vulnérabilité trimestriel (si commerce en ligne)
3	Tout commerçant traitant de 20 000 à 1 million de transactions e-commerce par an Visa ou MasterCard	Questionnaire d'auto-évaluation annuel Scan de vulnérabilité trimestriel (si commerce en ligne)
4	• Tout commerçant traitant moins de 20 000 transactions e-commerce par an Visa ou MasterCard • Tout commerçant traitant moins de 1 million de transactions par an Visa ou MasterCard (toutes transactions confondues)	Questionnaire d'auto-évaluation annuel Scan de vulnérabilité trimestriel recommandé (si commerce en ligne) : cela dépend si les données sont capturées, stockées ou transmises par l'infrastructure du commerçant ou par un fournisseur de services

[1] PCI DSS est l'acronyme anglais de Payment Card Industry Data Security Standard. Une traduction française serait « Standard de sécurité des données pour l'industrie des cartes de paiement ».

PREREQUIS POUR LA CONNEXION D'UN TPE EN IP VIA L'INTERNET ADSL DU COMMERCANT

Pour connecter un TPE CSB via le réseau INTERNET ADSL commerçant :

1. Le commerçant doit avoir un accès internet via un routeur ADSL

2. Le commerçant doit avoir une prise réseau RJ45 à une distance maximal de 2M du point d'installation du TPE

ATTENTION : Les TPE CSB ne peuvent pas être connectés en WIFI. Une liaison avec un câble RJ45 est impérative.
La CSB fournit avec ces TPE un câble RJ45 de 2M.

entrée

3. En entrée, le routeur ADSL du commerçant a 2 paramétrages possibles :
   - A : Le routeur est en DHCP*. Informer la CSB pour avoir une configuration de la connexion TPE en DHCP
   - B : Le routeur à une configuration en IP FIXE. Informer la CSB des 3 éléments à configurer pour la connexion du TPE (contacter votre prestataire informatique si nécessaire)

     Adresse IP fixe : Passerelle : Masque de sous réseau :

sortie

4. En sortie, le routeur ADSL du commerçant a 2 paramétrages possibles :
   - A : Le routeur n'a pas de restriction de sortie. Informer la CSB
   - B : Le routeur à des restrictions de sortie. Le commerçant doit configurer l'ouverture des adresses IP d'appels CSB suivantes.
     - NOMINAL : IP 202.87.134.13 port 38004 / 38006 / 38007
     - SECOURS : IP 202.87.134.133 port 38004 / 38006 / 38007

DHCP* : Dynamic Host Configuration Protocol est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station ou d'une machine, notamment en lui attribuant automatiquement une adresse IP et un masque de sous-réseau.