**CONTRAT D'ACCEPTATION EN PAIEMENT A DISTANCE SECURISE**
**PAR CARTES "CB" OU AGREEES "CB" (VADS)**
**POUR LE 3xCB**

## PREAMBULE

L'Acquéreur « CB », établissement de crédit, a proposé à l'Accepteur« CB », commerçant, la possibilité d'offrir à ses clients le 3xCB pour le paiement de leurs achats sur ses sites marchands.

Le 3xCB permet aux clients de régler sur le site http:///de l'Acquéreur, leurs achats effectués, par carte bancaire en une deux ou trois fois après le paiement d'un acompte, dans un délai maximal de 90 jours.

Par le présent contrat, l'Acquéreur consent à ce que l'Accepteur accepte les cartes bancaires pour le paiement des biens et services par ses clients personnes physiques, agissant pour leurs besoins non professionnels.

**ADHESION AU SYSTEME DE PAIEMENT A DISTANCE SECURISE**
**PAR CARTES "CB" OU AGREEES "CB"**
**POUR LE 3xCB**

... au capital de €, dont le siège social est sis ,
immatriculée au Registre du Commerce et des Sociétés de sous le numéro SIREN , représentée par ,
en sa qualité de ... , dûment habilité(e).
(ci-après "Accepteur « CB »"),

**demande à**
**CA Consumer Finance**, société anonyme au capital de 554 482 422 €, dont le siège social est sis 1 rue Victor Basch – CS 70001 - 91068 Massy Cedex, immatriculée au Registre du Commerce et des Sociétés d'Evry sous le numéro 542 097 522, représentée par Mr Christian FUCHS, en sa qualité de Directeur du Financement des Ventes, dûment habilité.
(ci-après "Acquéreur « CB »")

*agissant tant pour son propre compte qu'en tant que représentant du Groupement des Cartes Bancaires CB (Groupement d'Intérêt Economique régi par l'ordonnance du 23 septembre 1967, ci après "GIE CB") :*

**L'adhésion au système de paiement à distance sécurisé par Cartes "CB" ou agréées "CB" (ci-après "le Système CB") pour le 3xCB selon :**
- les Conditions Générales en annexe 1,
- les Conditions Particulières convenues avec l'Acquéreur CB en annexe 2,
- le Référentiel Sécuritaire Accepteur en annexe 3.

***Reconnaît avoir pris connaissance de l'ensemble de ces Conditions, y compris le Référentiel Sécuritaire Accepteur, dont un exemplaire m'a été remis et déclare les accepter sans réserve.***

Ces Conditions annulent et remplacent celles qui auraient été convenues antérieurement avec le même Acquéreur, pour le(s) même(s) point(s) de ventes, et qui auraient le même objet.
Elles sont applicables à compter du .

Fait en deux exemplaires originaux, à
le

Signature et cachet
de l'Accepteur CB

Signature et cachet
de l'Acquéreur CB

## ANNEXE 1

## CONDITIONS GENERALES D'ADHESION AU SYSTEME DE PAIEMENT A DISTANCE SECURISE PAR CARTES "CB" OU AGREEES "CB"

### PREAMBULE

### Le GIE CB

Pour éviter, dans le commerce électronique et la vente ou la location à distance que tout tiers non autorisé accède aux données liées à la Carte et afin de limiter l'utilisation du seul numéro de Carte pour donner un ordre de paiement, le GIE CB a mis en place des procédures de sécurisation des ordres de paiement donnés à distance par les Titulaires de Cartes CB ou agréées CB tel que le référentiel sécuritaire de protection des données sensibles.

### Article préliminaire

1) L'"Accepteur CB " peut être un commerçant susceptible d'utiliser le Système CB, et d'une manière générale, tout professionnel vendant des biens ou des prestations de services.

   Les remises à l'encaissement sont domiciliées dans un premier dans un premier temps sur un compte de passage ouvert dans les livres de l'Acquéreur "CB". Ensuite, l'Acquéreur "CB" adresse le jour ouvré suivant un virement sur le compte bancaire du choix de l'Accepteur "CB", sauf en cas de compensation de dettes réciproques.

2) Par "Acquéreur CB", il faut entendre tout établissement de crédit ou de paiement Membre du GIE CB ou Entité de Groupe au sens des Statuts du GIE CB, avec lequel l'Accepteur CB a signé un contrat d'acceptation, et cela quel que soit son statut, (banque, etc).

3) Par "Système d'Acceptation", il faut entendre les logiciels, protocoles conformes aux spécifications définies par le GIE CB et nécessaires à l'enregistrement, à la transmission et au traitement sécurisé des ordres de paiement par Cartes CB et agréées CB.

**L'Accepteur CB** déclare connaître les lois et règlements applicables aux ventes et prestations réalisées à distance ainsi que celles applicables au commerce électronique et notamment aux échanges utilisant les réseaux et les différents terminaux de communication (TV, téléphonie mobile, ordinateur…). Il reconnaît qu'il doit se conformer à ces dispositions ou à celles qui pourront intervenir et qu'il doit commercialiser les produits ou prestations de services faisant l'objet d'un paiement à distance sécurisé en respectant les lois et règlements applicables, notamment fiscaux.

### ARTICLE 1 : DEFINITION DU SYSTEME

Le système de paiement à distance sécurisé par Carte CB repose sur l'utilisation de Cartes CB ou agréées CB pour le paiement d'achats de biens ou de prestations de services auprès des Accepteurs adhérant au Système CB et cela dans le cadre des seules dispositions et procédures définies ou homologuées par le GIE CB.
Lorsque l'Acquéreur CB représente le GIE CB, le terme de "représentation" ne concerne que l'ensemble des conditions techniques d'acceptation de la Carte CB ou de Cartes agréées CB et de remise des opérations à l'Acquéreur CB, et non la mise en jeu de la garantie du paiement visée à l'article 5 des présentes Conditions Générales.

### ARTICLE 2 : DISPOSITIONS RELATIVES AUX CARTES

Sont utilisables dans le Système CB :
- les cartes sur lesquelles figure la marque CB
- les cartes agréées CB c'est-à-dire : les cartes portant uniquement la marque Visa ou MasterCard dont l'acceptation dans le Système CB a été agréée par le GIE CB.

L'ensemble de ces cartes précitées est désigné ci-après par le terme générique de "Carte".
Cette liste est précisée dans les conditions particulières.

Les types de cartes acceptées sont susceptibles d'être modifiés par L'Acquéreur "CB" qui en informera l'Accepteur "CB" par tous moyens.

**ARTICLE 3 : OBLIGATIONS DE L'ACCEPTEUR CB**

3.1 L'Accepteur CB s'engage à :

3.1.1 Utiliser les procédures de sécurisation des ordres de paiement donnés à distance par les Titulaires de Cartes dans le respect des dispositions légales, réglementaires et professionnelles applicables, notamment et sans limitation des dispositions relatives aux ventes et prestations réalisées à distance et au commerce électronique (informations des utilisateurs, délais d'exécution des prestations…) ainsi que des bonnes pratiques commerciales telles que définies notamment par les codes de conduite applicables à son activité.

3.1.2 Utiliser le système de paiement à distance sécurisé en s'abstenant de toute activité qui pourrait être pénalement sanctionnée.

3.2 Garantir l'Acquéreur CB et le GIE CB le cas échéant, contre toute conséquence dommageable pouvant résulter pour eux du manquement aux obligations visées à l'article 3.1.

3.3 Afficher visiblement sur son site et sur ses supports de communication :
- les montants minimal et maximal pour lesquels la Carte est acceptée pour le 3xCB afin que le Titulaire de la Carte en soit préalablement informé.
- les différentes marques de Cartes acceptées.

3.4 S'identifier clairement par le numéro SIRET et le code activité (NAF/APE) que l'INSEE lui a attribué.

3.5 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 CB la conformité des informations transmises pour identifier son point de vente en ligne, 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, règlement en présence physique de l'accepteur, etc) dans ce point de vente en ligne.

3.6 Recevoir des paiements à distance sécurisés en contrepartie d'actes de vente ou de prestations de services offerts à sa clientèle et qu'il fournit ou réalise lui-même.

3.7 Accepter les Cartes telles que définies à l'article 2 ci-dessus.

3.8 Faire son affaire personnelle des litiges commerciaux et de leurs conséquences financières pouvant survenir avec des clients notamment lors de l'exercice par ces derniers de leur droit de rétractation, et concernant des biens et services dont l'achat a été réglé par Carte au titre du présent Contrat.

3.9 Utiliser obligatoirement un Système d'Acceptation conforme aux spécifications définies par le GIE CB et les procédures de sécurisation des ordres de paiement donnés à distance par les Titulaires de Cartes, proposées par l'Acquéreur CB.

3.10 Régler, selon les Conditions Particulières convenues avec l'Acquéreur CB, les commissions, frais et d'une manière générale, toute somme due au titre de l'adhésion et du fonctionnement du Système CB.

3.11 Permettre à l'Acquéreur et au GIE de faire procéder aux frais de l'Accepteur CB 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 3. 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 9. L'Accepteur CB autorise la communication du rapport à l'Acquéreur et au GIE CB.

3.12 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 au Titulaire de la Carte utilisée pour l'opération initiale. L'Accepteur CB doit alors utiliser la procédure dite de "transaction crédit", et dans le délai prévu dans les Conditions Particulières convenues avec lui, effectuer la remise correspondante à l'Acquéreur CB à qui il avait remis l'opération initiale. Le montant de la "transaction crédit" ne doit pas dépasser le montant de l'opération initiale.

**ARTICLE 4 : OBLIGATIONS DE L'ACQUEREUR CB**

L'Acquéreur CB s'engage à :

4.1 Inscrire l'Accepteur CB dans la liste des points de vente habilités à recevoir des paiements par Cartes de Titulaires de Cartes dûment authentifiés.

4.2 Indiquer à l'Accepteur CB la liste et les caractéristiques des Cartes pouvant être acceptées (cf article 2).

4.3 Créditer le compte de l'Accepteur CB des sommes qui lui sont dues, selon les Conditions Particulières convenues avec lui (cf article préliminaire).

4.4 Ne pas débiter, au delà du délai maximum de 15 mois à partir de la date du crédit initial porté au compte de l'Accepteur CB, les opérations non garanties et qui n'ont pu être imputées au compte sur lequel fonctionne la Carte.

**ARTICLE 5 : GARANTIE DU PAIEMENT**

5.1 Les opérations de paiement sont garanties sous réserve du respect de l'ensemble des mesures de sécurité visées au présent article ainsi que dans les Conditions Particulières.

Toutes les mesures de sécurité sont indépendantes les unes des autres.

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

5.2 L'Accepteur s'engage à informer immédiatement l'Acquéreur CB en cas de fonctionnement anormal du Système d'Acceptation et de toutes autres anomalies (absence d'application des procédures de sécurisation des ordres de paiement, dysfonctionnement du Système d'Acceptation...).

5.3 <u>Lors du paiement</u>

L'Accepteur CB s'engage à :

5.3.1 Vérifier le montant des achats accepté, tel qu'indiqué aux conditions particulières

5.3.2 Obtenir une autorisation d'un montant identique au montant de l'acompte.

5.4 <u>Après le paiement de l'acompte</u>

L'Accepteur CB s'engage à :

Communiquer, à la demande de l'Acquéreur CB et dans les délais prévus dans les Conditions Particulières convenues avec lui, tout justificatif des opérations de paiement.

**ARTICLE 6 : RECLAMATION ET CONVENTION DE PREUVE**

6.1 Réclamation

Toute réclamation doit être formulée par écrit à l'Acquéreur CB, 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 de paiement non garantie, notamment en cas d'impayé.

6.2 Convention de preuve

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

**ARTICLE 7 : MODIFICATIONS**

7.1 L'Acquéreur CB peut modifier à tout moment les présentes Conditions Générales ainsi que les Conditions Particulières.

L'Acquéreur CB 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 l'état du Système d'Acceptation suite à un dysfonctionnement etc.
- des modifications sécuritaires telles que :
  - la suppression de l'acceptabilité de certaines Cartes
  - la suspension de l'adhésion au Système CB.

7.2 Les nouvelles conditions entrent généralement en vigueur au terme d'un délai minimum fixé à un mois à compter de l'envoi de la lettre d'information ou de notification.

7.3 Ce délai est exceptionnellement réduit à cinq jours calendaires lorsque l'Acquéreur CB ou le GIE CB constate, dans le point vente en ligne, une utilisation anormale de Cartes perdues, volées ou contrefaites.

7.4 Passés les délais visés au présent article, les modifications sont opposables à l'Accepteur CB s'il n'a pas résilié le présent Contrat.

7.5 Le non respect des nouvelles conditions techniques et 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 9 du présent Contrat.

**ARTICLE 8 : DUREE ET RESILIATION DU CONTRAT**

8.1. Le présent Contrat est conclu pour une durée indéterminée, sauf dispositions contraires visées dans les Conditions Particulières.

L'Accepteur « CB » d'une part, l'Acquéreur « CB » d'autre part, peuvent, à tout moment, sans justificatif avec un préavis de 30 jours, 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. L'Accepteur CB garde alors la faculté de continuer à adhérer au Système CB en utilisant des moyens sécurisés d'acceptation avec tout autre Acquéreur CB de son choix.

Lorsque cette résiliation fait suite à un désaccord sur les modifications prévues à l'article 7 ci-dessus, elle ne peut intervenir qu'au-delà du délai prévu dans cet article pour l'entrée en vigueur de ces modifications.

8.2. Le présent contrat sera résilié de plein droit, sous réserve du dénouement des opérations en cours, en cas :
- de cessation d'activité de l'Accepteur "CB", cession ou mutation du fonds de commerce,
- de résiliation de la Convention de d'Agrément 3xCB à distance liant l'Accepteur et l'Acquéreur.

8.3. L'Accepteur CB est tenu de restituer à l'Acquéreur CB les dispositifs techniques et sécuritaires et les documents en sa possession dont l'Acquéreur CB est propriétaire. L'Accepteur CB s'engage à retirer immédiatement de son Système d'Acceptation de son point de vente en ligne et de ses supports de communication tout signe d'acceptation du 3xCB.

**ARTICLE 9 : MESURES DE PREVENTION ET DE SANCTION**

9.1 Mesures de prévention et de sanction mises en œuvre par l'Acquéreur CB :

En cas de manquement de l'Accepteur CB aux dispositions 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 CB peut prendre des mesures de sauvegarde et de sécurité consistant, en premier lieu, en un avertissement à l'Accepteur CB valant mise en demeure précisant les mesures à prendre pour remédier au manquement ou résorber le taux d'impayés anormalement élevé constaté. Si dans un délai de trente jours, l'Accepteur CB 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 CB peut résilier de plein droit avec effet immédiat le présent Contrat par lettre recommandée avec demande d'avis de réception.

De même, si dans un délai de trois mois à compter de l'avertissement, l'Accepteur CB est toujours confronté à un taux d'impayés anormalement élevé, l'Acquéreur CB peut décider la résiliation de plein droit avec effet immédiat du présent Contrat notifiée par lettre recommandée avec demande d'avis de réception.

9.2 Mesures de prévention et de sanction mises en œuvre par le GIE CB :

En cas de manquement de l'Accepteur CB aux dispositions du présent Contrat concernant les mesures de sécurité ou en cas de taux d'impayés constaté anormalement élevé (notamment dans les hypothèses où l'Accepteur CB ventile ses remises en paiement entre plusieurs Acquéreurs CB de sorte qu'aucun de ceux-ci n'est en mesure d'avoir une vision globale de son taux d'impayés), le GIE CB peut prendre des mesures de sauvegarde et de sécurité consistant en :

- la suspension de l'adhésion au Système CB. Cette suspension intervient s'il n'est pas remédié aux problèmes constatés dans un délai de 3 mois suivant la mise en demeure d'y remédier. Ce délai peut être ramené à quelques jours en cas d'urgence et à un mois au cas où l'Accepteur CB aurait déjà fait l'objet d'une mesure de suspension dans les 24 mois précédant l'avertissement.
  La suspension est notifiée par l'envoi d'une lettre recommandée et motivée, avec demande d'avis de réception. Cette suspension prend effet deux jours francs à compter de la réception de la notification.

- La radiation de l'adhésion au Système CB en cas de survenance de manquements d'une exceptionnelle gravité, de comportement dolosif ou frauduleux ou en cas de persistance d'un taux anormalement élevé d'incidents ayant déjà justifié antérieurement une mesure de suspension vis-à-vis de l'Accepteur CB concerné. Cette radiation est notifiée par l'envoi d'une lettre recommandée et motivée, avec demande d'avis de réception.

9.3 En cas de suspension ou de radiation, l'Accepteur CB s'engage alors à restituer à l'Acquéreur CB les dispositifs techniques et sécuritaires et les documents en sa possession dont l'Acquéreur CB est propriétaire et à retirer immédiatement le Système d'Acceptation de son point de vente en ligne et de ses supports de communication tout signe d'acceptation du 3xCB.

9.4 La période de suspension est au minimum de 6 mois.

**ARTICLE 10 : SECRET BANCAIRE ET PROTECTION DES DONNEES A CARACTERE PERSONNEL**

Lors de la signature ou de l'exécution des présentes, chacune des parties peut avoir accès à des données à caractère personnel.
Ainsi, en application des articles 32, 38, 39 et 40 de la loi du 6 janvier 1978 relative à la loi "Informatique et Libertés" modifiée par la loi du 6 août 2004, il est précisé que :

A l'occasion de l'exécution des ordres de paiement donnés par Carte, l'Accepteur CB peut avoir accès à différentes données à caractère personnel concernant notamment les Titulaires de la Carte. L'Accepteur CB ne peut utiliser ces données à caractère personnel que pour l'exécution des ordres de paiement par Carte. Sauf obligations légales et réglementaires, il ne peut ni les céder, ni en faire un quelconque usage qui ne soit pas directement visé par le présent Contrat. Il 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.

Les Titulaires de Cartes sur lesquels des données à caractère personnel ont été recueillies doivent pouvoir disposer des droits d'accès, de rectification et d'opposition auprès de l'Accepteur CB. A cet égard, l'Accepteur CB s'engage d'ores et déjà à leur permettre d'exercer ces droits.

**ARTICLE 11 : NON RENONCIATION**

Le fait pour l'Accepteur CB ou pour l'Acquéreur CB 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 12 : LOI APPLICABLE/TRIBUNAUX COMPETENTS**

**Le présent Contrat et toutes les questions qui s'y rapportent sont régis par le droit français et tout différend relatif à l'interprétation, la validité, et/ou l'exécution du présent Contrat est soumis à la compétence des Tribunaux français, y compris les procédures tendant à obtenir des mesures d'urgence ou conservatoires, en référé ou sur requête.**

## ANNEXE 2
## CONDITIONS PARTICULIERES POUR LE 3xCB

### ARTICLE 1 : DISPOSITIONS RELATIVES AUX CARTES

Sont exclues les cartes à autorisation systématique du type Electron, Nickel, Maestro et les e-cards.

La Carte doit être en cours de validité au moins jusqu'au dernier jour du mois de la présentation du dernier débit carte.

En cas de modification, l'Acquéreur informera l'Accepteur par tous moyens.

### ARTICLE 2 : CONDITIONS LIEES A LA GARANTIE DE PAIEMENT

**1 : Limitation de la Garantie de paiement au paiement de l'acompte**
Par dérogation de l'article 5 de des Conditions générales (Annexe 1), seul le premier débit carte bancaire correspondant à l'acompte bénéficie d'une garantie de paiement, sous réserve des mesures de sécurités visées aux conditions particulières et à l'article 5 des conditions générales.

**2 : Délai de communication des justificatifs**
A compter de la date de la demande dix (10) jours calendaires. Si l'Accepteur "CB" ne communique pas le justificatif, ou le communique au-delà du délai ci-dessus, il s'expose à un impayé.

### ARTICLE 3: TRANSMISSION DES ENREGISTREMENTS D'OPERATIONS

Les enregistrements des opérations de paiement seront collectés par un prestataire de l'Acquéreur.

### ARTICLE 4 : DELAI DE REMBOURSEMENT

La procédure « transaction crédit » peut être utilisée dans un délai de 16 jours à compter de la conclusion du contrat pour les prestations de services et de la livraison pour les contrats de vente de biens.

### ARTICLE 5 : AUTRES CONDITIONS D'UTILISATION

Le montant des achats accepté, les conditions financières et le montant du chiffre d'affaires mensuel maximal avec le 3xCB sont indiquées dans La Convention d'Agrément 3xCB A DISTANCE qui lie l'Acquéreur et l'Accepteur.

Ces conditions pourront être modifiées par l'Acquéreur qui en informera l'Accepteur par tous moyens.

## ANNEXE 3
## REFERENTIEL SECURITAIRE 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, 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 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 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, 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 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 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 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 l'Accepteur CB.
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 CB 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.