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

**Préambule**

**La Banque Acquéreur**

Les présentes Conditions Générales et les Conditions Particulières sont établies par la Banque Acquéreur.

**L'Accepteur**

L'Accepteur utilisant des moyens électroniques ou non pour vendre à distance des biens et des services et notamment souhaite recevoir des paiements à distance en contrepartie d'actes de vente ou de fournitures de prestation de service qu'il réalise lui même.

Par paiement à distance il faut entendre tout paiement par correspondance et assimilé (téléphone, terminal, Internet,..) pour lequel la transaction financière est réalisée au moyen d'un numéro de carte de paiement, de la date de validité de la carte et de son cryptogramme visuel situé au verso de celle-ci.

L'Accepteur déclare connaître les lois et règlements applicables aux ventes et achats à distance et notamment aux échanges utilisant les réseaux électroniques 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 services faisant l'objet d'un paiement à distance en respectant les lois et règlements applicables, notamment fiscaux.

A la lumière de ces éléments l'Accepteur a souhaité être soumis au présent Contrat.

**ARTICLE 1 - OBJET**

Les présentes ont pour objet de déterminer les conditions d'adhésion et de règlement des paiements par cartes bancaires en vente à distance.

**ARTICLE 2 - OBLIGATIONS DE L'ACCEPTEUR**

L'Accepteur s'engage à :

2.1.A respecter les conditions contractuelles proposées par la Banque Acquéreur, les dispositions légales, réglementaires et professionnelles sans limitation des dispositions relatives aux ventes et prestations réalisées à distance, ainsi que les bonnes pratiques commerciales telles que définies notamment par les codes de Conduite.

Dans le cadre du présent Contrat s'abstenir de toute activité qui pourrait être pénalement sanctionnée telle que la mise en péril de mineurs, des actes de pédophilie, des actes de contrefaçon d'œuvres protégées par un droit de propriété intellectuelle et de moyens de paiement, le non-respect de la protection des données personnelles, des atteintes aux systèmes de traitement automatisé de données, des actes de blanchiment, le non respect des dispositions relatives aux jeux de hasard, aux courses de chevaux, aux loteries et des dispositions relatives aux conditions d'exercice de professions réglementées.

2.2 Garantir la Banque Acquéreur contre toute incidence dommageable pouvant résulter pour elle du manquement aux obligations visées à l'article 2.1.

2.3 Indiquer clairement ses coordonnées (dénomination commerciale, RCS, représentant légal...), de telle sorte que le Porteur de Carte n'ait pas de difficulté à vérifier les opérations de paiement qu'il a effectuées,

2.4 Accepter les Cartes pour le paiement d'achats de biens ou de prestations de services offerts à sa clientèle, auquel le porteur a effectivement et expressément consenti, même lorsqu'il s'agit d'articles vendus ou de prestations fournies à titre de promotion ou de soldes. En outre l'Accepteur s'interdit de toute autre activité.

2.5 Appliquer aux Porteurs de Cartes les mêmes prix qu'à l'ensemble de sa clientèle. En tout état de cause, ne faire supporter, directement ou indirectement, aucun frais supplémentaire au Porteur de Carte, du seul fait qu'il utilise sa Carte comme mode de paiement.

2.6 Afficher visiblement, sur le dispositif permettant la transaction et sur ses supports de communication, le montant minimum éventuel à partir duquel la Carte est acceptée afin que le Porteur en soit préalablement informé. Ce montant minimum doit être raisonnable et ne pas être un frein à l'acceptation des Cartes.

2.7 Signaler au public l'acceptation des Cartes de façon apparente par affichage, notamment le dispositif permettant la transaction et sur ses supports de communication, conformément à la charte graphique communiquée par la Banque Acquéreur.

2.8 Afficher visiblement sur tout support de l'offre de vente à distance le prix du produit et/ou du service fourni, ainsi que la devise dans laquelle ce prix est libellé, et ce, notamment de façon à ce que le Porteur de Carte ne soit pas en mesure de croire que le prix était autre.

2.9 Régler, selon les Conditions Particulières, les commissions, frais et d'une manière générale, toute somme due dans le cadre du fonctionnement du mode de paiement à distance objet du présent Contrat.

2.10 Faire son affaire personnelle des litiges commerciaux avec les Porteurs de Carte, notamment lors de l'exercice par le Porteur de son droit de rétractation.

2.11 Utiliser le présent contrat sous la seule référence du SIRET mentionné lors de la signature du présent contrat.

2.12 Informer préalablement et par écrit la Banque Acquéreur de toute modification de son objet social ou de toute extension de la nature des produits ou services vendus à l'aide du présent contrat et, plus généralement, de toutes modifications des conditions d'exercice de l'activité susceptibles d'avoir un impact sur les obligations souscrites par l'Accepteur aux termes des présentes.

2.13 Lutter contre la fraude dont son point d'acceptation pourrait être victime, notamment en mettant en œuvre sans délai les mesures sécuritaires appropriées préconisées par la Banque Acquéreur.

2.14 Prendre à sa charge en cas d'impayés ou de fraude l'intégralité des frais de gestion unitaire tels qu'indiqués dans les Conditions Particulières du présent contrat. A ce titre, l'Accepteur autorise irrévocablement la Banque Acquéreur à débiter à tout moment le compte ouvert en ses livres sous le numéro indiqué dans la « demande d'adhésion » du présent Contrat du montant des frais.

2.15 La Banque Acquéreur se réserve le droit de faire procéder aux frais de
l'Accepteur dans ses locaux ou ceux de ses prestataires, à la vérification par un tiers indépendant du respect des bons usages de la profession (ci-après "l'Audit"), à tout moment lors de la conclusion du présent Contrat et/ou pendant la durée du présent Contrat.

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 aux bons usages de la profession, la Banque Acquéreur peu mettre en Œuvre les mesures prévues à l'article 8.

Adhérer aux bons usages de la profession de la vente à distance correspondant à minima aux principes figurant en annexe du présent Contrat et les mettre en œuvre, comme notamment Paiement Card Industry (PCI), Data Security Standard (DSS).

La Banque Acquéreur se réserve également le droit de subordonner l'adhésion au mode de paiement à distance à la mise en œuvre d'un audit et le cas échéant, à la mise en œuvre des mesures recommandées par l'auditeur.

**ARTICLE 3 - OBLIGATIONS DE LA BANQUE ACQUÉREUR**

La Banque Acquéreur s'engage à :

3.1 Fournir, à l'Accepteur les informations que celui-ci doit obligatoirement utiliser.

3.2 Indiquer à l'Accepteur la liste et les caractéristiques de toutes les cartes bancaires pouvant être acceptées ainsi que les méthodes utilisées pour cette acceptation.

3.3 Créditer le compte de l'Accepteur des sommes qui lui sont dues, selon les modalités prévues dans les Conditions Particulières.

3.4 Ne pas débiter, au delà du délai maximum de 6 mois à partir de la date du crédit initial porté au compte de l'Accepteur les opérations qui ne pourront pas faire l'objet d'un règlement par la Banque Acquéreur et qui n'ont pu être imputées au compte du Porteur.

**ARTICLE 4 - RÈGLEMENT DU PAIEMENT**

4.1 Les opérations de paiement seront réglées sous réserve « d'une bonne fin d'encaissement » impliquant :
- Le respect de l'ensemble des mesures de sécurité énoncées aux présentes.
- L'absence de toute de réclamation écrite du titulaire de la Carte qui conteste la réalité même ou le montant de la transaction.
- L'absence d'opération réalisée au moyen d'une Carte non valide, périmée ou annulée.

4.2 L'Accepteur doit être clairement identifié par le numéro SIRET et le Code NAF que l'INSEE lui a attribués. Le numéro SIRET, identifiant le point de vente, sera celui du siège social de l'Accepteur ou de celui de l'un de ses établissements qui est habilité par les présentes à recevoir les paiements auxquels les clauses du présent Contrat sont opposables.

4.3 Lors du paiement L'Accepteur s'engage à :

4.3.1 Contrôler la longueur (de 13 à 19 caractères) et la vraisemblance mathématique du numéro de la Carte.

4.3.2. S'assurer que la Carte est en cours de validité, suivant les indications communiquées par le Porteur de la Carte.

4.3.3. Contrôler le numéro de Carte par rapport à la dernière liste des Cartes en opposition diffusée par la Banque Acquéreur, pour le point de vente concerné et selon les conditions convenues avec la Banque Acquéreur.

4.3.4. Vérifier, le cas échéant que le bon de commande est bien signé s'il s'agit d'une vente par correspondance.

4.3.5. Obtenir une autorisation pour le montant de la transaction. A défaut, l'opération ne pourra pas faire l'objet d'un règlement. La demande d'autorisation doit indiquer, au minimum, le montant, la date de la transaction, le numéro de Carte du Porteur, la date de fin de validité de la Carte, l'identifiant de l'Accepteur et celui de la Banque Acquéreur. Le numéro de l'autorisation doit être mentionné sur l'enregistrement de l'opération destiné à être remis à l'encaissement. La date de vente doit correspondre à celle de l'autorisation.

4.3.6 L'Accepteur doit informer immédiatement la Banque Acquéreur en cas de fonctionnement anormal de son dispositif d'acceptation et de toutes autres anomalies.

**Après le paiement l'Accepteur s'engage à :**

4.3.7 Transmettre à la Banque Acquéreur après l'envoi du bien ou après la prestation de service, dans les délais et selon les modalités prévus, conformément aux conditions particulières prévues dans le cadre du présent Contrat, les enregistrements des transactions, et s'assurer qu'ils ont bien été portés au crédit du compte conformément aux conditions particulières prévues dans le cadre du présent Contrat.
Toute transaction ayant fait l'objet d'une autorisation doit être remise à la Banque Acquéreur lors de la demande d'autorisation.

4.3.8 Demander, pour les livraisons réalisées à ses comptoirs ou à domicile, la présentation d'une pièce d'identité et de la Carte du Porteur utilisée pour la transaction.

4.3.9 Conserver à titre de justificatif les bons de commande ainsi que les relevés détaillés des commandes reçues par clients Porteurs de Carte.

4.3.10 Communiquer à la demande de la Banque Acquéreur, dans lesdélais prévus aux conditions particulières du présent Contrat, tout justificatif des transactions de paiement.

4.3.11 Adresser, à la demande du porteur de la Carte, une facture précisant notamment, le mode de paiement par Carte.

4.3.12 **L'Accepteur s'engage à ne stocker, sous quelque forme que ce soit, aucune des données Cartes ci-après :**
- **le cryptogramme visuel,**
- **la piste magnétique dans son intégralité,**
- **le code confidentiel**

4.3.13 Les mesures de sécurité énumérées ci-dessus, pourront être modifiées et complétées pendant toute la durée du présent Contrat, selon la procédure prévue à l'article 6.

**ARTICLE 5 - RÉCLAMATION ET CONVENTION DE PREUVE**

5.1. Réclamation
Toute réclamation de l'Accepteur doit être formulée par écrit à la Banque Acquéreur dans un délai maximum de 6 mois à compter de la date de l'opération contestée. Ce délai est réduit à 15 jours calendaires à compter de la date de restitution de l'impayé, dans le cas d'une réclamation relative à un impayé.

5.2.Convention de preuve
De convention expresse entre les parties, les supports électroniques sont réputés constituer au moins des commencements de preuve par écrit. En cas de conflit, les documents électroniques produits par la Banque 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 la Banque Acquéreur.

5.3 Secret bancaire et protection des données à caractère personnel De convention expresse l'Accepteur autorise la Banque Acquéreur à communiquer et stocker le cas échéant des données secrètes ou confidentielles portant sur lui à des entités impliquées dans le fonctionnement du présent Contrat aux seules finalités de traiter les opérations de paiement, de prévenir des fraudes et de traiter les réclamations qu'elles émanent des Porteurs de Cartes ou d'autres entités.

**ARTICLE 6 - MODIFICATIONS DES DISPOSITIONS DU CONTRAT**

6.1 La Banque Acquéreur peut modifier à tout moment le présent Contrat, pour des raisons techniques, commerciales ou juridiques.
Les modifications techniques autres que les travaux d'installation et de maintenance (concernant notamment l'acceptation de nouvelles Cartes, les modifications de logiciel, le changement de certains paramètres, la remise en état du dispositif d'Acceptation suite à un dysfonctionnement) si elles n'ont pas de raisons sécuritaires, doivent être mises en œuvre par l'Accepteur un mois après l'envoi de la lettre de notification par la Banque Acquéreur.

6.2. Les modifications sécuritaires concernent notamment :
- la modification du seuil de demande d'autorisation ;
- la suppression de l'acceptabilité de certaines Cartes ; La Banque Acquéreur peut modifier à tout moment le présent Contrat pour des raisons liées à l'absence de sécurité présentée par le ou les moyens sécuritaires d'acceptation appliquée par l'Accepteur ou pour la mise en œuvre de nouvelles dispositions sécuritaires.

6.3. Le délai dans lequel les modifications sécuritaires doivent être mises en œuvre par l'Accepteur est exceptionnellement réduit à cinq jours calendaires notamment lorsqu'il est constaté une utilisation anormale de Cartes perdues, volées ou contrefaites, exigeant une mesure sécuritaire rapide et motivée telle que notamment la réduction du montant du seuil de demande d'autorisation.

6.4. En cas de suppression de l'acceptabilité de certaines Cartes, les nouvelles dispositions entrent immédiatement en vigueur, à compter de leur date de communication à l'Accepteur, faites par tout moyen par la Banque Acquéreur.

6.5. Passés les délais visés aux articles 6.1. et 6.3, et après diffusion de l'information visée à l'article 6.4, les modifications sont opposables à l'Accepteur. L'Accepteur peut résilier le présent Contrat s'il s'oppose à l'application des nouvelles dispositions.

6.6. Le non-respect des nouvelles conditions techniques ou sécuritaires, dans les délais impartis, peut entraîner outre les conditions de règlement, la résiliation du présent Contrat dans les conditions prévues à l'article 8 du présent Contrat.

**ARTICLE 7 - DURÉE - RÉSILIATION DU CONTRAT**

7.1. Les présentes sont conclues pour une durée indéterminée, sauf dispositions contraires visées dans les Conditions Particulières du présent Contrat.
L'Accepteur d'une part, la Banque Acquéreur d'autre part, peuvent, à tout moment, sans justificatif ni préavis (sauf dérogation particulière convenue entre les deux parties), 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 garde alors la faculté de continuer à adhérer au mode de paiement à distance avec toute autre Banque Acquéreur qui propose le mode de paiement à distance par cartes bancaires objet du présent Contrat.

Lorsque cette résiliation fait suite à un désaccord sur les modifications des conditions contractuelles, elle ne peut intervenir qu'au-delà du délai prévu dans l'article précédent pour l'entrée en vigueur de ces modifications ou immédiatement en cas d'application de l'article 6.4.

7.2. Toute cessation d'activité de l'Accepteur, cession ou mutation du fonds de commerce, entraîne la résiliation immédiate de plein droit du présent Contrat sous réserve du dénouement des opérations en cours.

Dans le cas où, après résiliation du présent Contrat, des impayés apparaîtraient, ils seront à la charge de l'Accepteur.

7.3. En fin du présent Contrat, l'Accepteur est tenu de restituer, le cas échéant à la Banque Acquéreur, les matériels et documents en sa possession dont la Banque Acquéreur est propriétaire. L'Accepteur s'engage à supprimer immédiatement de son serveur et de ses supports de communication tout signe d'acceptation des Cartes.

**ARTICLE 8 - MESURES DE PRÉVENTION ET DE SANCTION**

8.1 Mesures de prévention et de sanction mises en œuvre par la Banque Acquéreur.

En cas de manquement de l'Accepteur aux dispositions du présent Contrat ou aux lois en vigueur ou en cas de constat d'un Taux d'Impayés anormalement élevé au regard de l'activité de l'Accepteur, ou d'utilisation anormalement élevée de Cartes perdues, volées ou contrefaites, la Banque Acquéreur peut prendre des mesures de sauvegarde et de sécurité consistant, en

premier lieu, en un avertissement à l'Accepteur valant mise en demeure précisant les mesures à prendre pour remédier au manquement ou résorber le Taux d'Impayés constaté.

Si dans un délai de trente jours, 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, la Banque Acquéreur 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 est toujours confronté à un Taux d'Impayés anormalement élevé au regard de l'activité de l'Accepteur la Banque Acquéreur peut décider la résiliation de plein droit avec effet immédiat du présent Contrat, notifiée par lettre recommandée avec demande d'avis de réception.

**ARTICLE 9 - PROTECTION DES DONNÉES A CARACTÈRE 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 protection des données à caractère personnel, modifiée par la loi du 6 août 2004, il est précisé que :

a) Les informations collectées par la Banque Acquéreur, nécessaires pour l'établissement et l'exécution des présentes, ne seront utilisées et ne feront l'objet de diffusion auprès d'entités tierces que pour les seules nécessités de la gestion des ordres de paiement par Carte donnés en exécution du présent Contrat, ou pour répondre aux obligations légales et réglementaires.

La Banque Acquéreur étant à cet effet, de convention expresse, déliée du secret bancaire.

L'Accepteur peut avoir accès à différentes données à caractère personnel concernant notamment les Porteurs de Carte lors de l'utilisation du moyen de paiement à distance. L'Accepteur ne peut pas utiliser ces données personnelles 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 contrôle des accès physiques et logiques à ces données.

b) Les personnes sur lesquelles portent les données à caractère personnel ci-dessus recueillies ont le droit d'en obtenir communication, le cas échéant d'en exiger la rectification et de s'opposer, pour des motifs légitimes, à ce qu'elles fassent l'objet d'un traitement ou à leur utilisation à d'autres fins que celles citées ci-dessus.

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

Les Accepteurs, personnes physiques, sur lesquelles des données à caractère personnel ont été recueillies disposeront également desdits droits d'accès, de rectification et d'opposition auprès de la Banque Acquéreur.

**ARTICLE 10 - NON RENONCIATION**

Le fait par l'Accepteur ou par la Banque Acquéreur de ne pas exiger à un moment quelconque l'exécution stricte par l'Accepteur ou par la Banque Acquéreur d'une disposition du présent Contrat n'est en aucun cas réputé constituer une renonciation, quelle qu'elle soit, à l'exécution de celle-ci.

**ARTICLE 11 - LOI APPLICABLE/TRIBUNAUX COMPETENTS**

Le présent Contrat et toutes les questions qui s'y rapportent seront régis par le droit français et tout différend relatif à l'interprétation, la validité, et/ou l'exécution du présent Contrat sera 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.

**REFERENTIEL SECURITAIRE ACCEPTEUR**

Les exigences constituant le référentiel sécuritaire accepteur sont présentées ci-après :

**Exigence 1 (E1)**
**Gérer la sécurité du système commercial et de paiement au sein de l'entreprise**

Pour assurer la sécurité des données des transactions et notamment, des données des porteurs, une organisation, des procédures et des responsabilités doivent être établies.
En particulier, un responsable de la sécurité du système commercial et de paiement doit être désigné. Il est chargé, entre autres, d'appliquer la législation sur la protection des données nominatives et des données bancaires 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 de paiement doit être assuré.
Une organisation chargée du traitement des incidents de sécurité, de leur suivi et de leur historisation doit être établie.

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

Les obligations et les responsabilités du Personnel quant à l'utilisation des données bancaires et confidentielles, à leur stockage et à leur circulation en interne ou à l'extérieur doivent être établies. Il en est de même pour l'utilisation des postes de travail et du réseau interne comme du réseau Internet.
Les obligations et les responsabilités du Personnel quant à la protection des données bancaires et confidentielles doivent être établies. L'ensemble de ces règles doit s'appliquer à tous les personnels impliqués : salariés de l'entreprise et tiers.
Les personnels doivent être sensibilisés aux risques encourus, notamment sur la divulgation d'informations confidentielles, l'accès non autorisé aux informations, aux supports et aux documents.
Les personnels doivent être régulièrement sensibilisés aux risques particuliers liés à l'usage des moyens informatiques (postes de travail en réseau, serveurs, accès depuis ou vers Internet) et notamment, à l'introduction de virus.
Il convient que les personnels reçoivent une formation appropriée sur l'utilisation correcte du système d'exploitation et du système applicatif commercial et de paiement.

**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 transaction et notamment, des données du porteur doit être hébergé dans un local sécurisé et répondre aux exigences édictées par les 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 de paiement**

Les règles de sécurité relatives aux accès et sorties depuis et vers le système commercial et de paiement 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 de paiement 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 de paiement**

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 de paiement.
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 de paiement**

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 de paiement**

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 être le pare-feu, le système supportant la base de données Clients ainsi que celui supportant la base de données Paiements.
Les journaux d'audit doivent être protégées contre des risques de désactivation, modification ou suppression non autorisées. Les responsabilités et rôles quant à l'audit des données enregistrées sont identifiés. Celui-ci doit être effectué quotidiennement.

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

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

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

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

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

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

**Exigence 11 (E11)**
**Maintenir l'intégrité des logiciels applicatifs relatifs au système commercial et de paiement**

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 de paiement**

La protection et l'intégrité des éléments de la transaction 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 de paiement doit décrire les moyens mis en place pour répondre à cette exigence.

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

Les données du porteur ne peuvent être utilisées que pour exécuter l'ordre de paiement et les réclamations. Le cryptogramme visuel d'un porteur ne doit en aucun cas être stocké par le commerçant.
Les données bancaires et nominatives relatives à une transaction, et notamment les données du porteur doivent être protégées lors de leur stockage et lors de leur routage sur les réseaux internes et externes au site d'hébergement conformément aux recommandation de la CNIL. Il en est de même pour l'authentifiant du commerçant et les éléments secrets servant à chiffrer.
Le dossier de sécurité propre au système commercial et de paiement 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.