Conditions Générales du contrat d'acceptation en paiement à distance sécurisé (VADS) par carte bancaire

---

PARTIE I (CG mutualisées)

Avertissement et pré-requis indispensable pour recevoir des paiements à distance sécurisés

Pour éviter, dans le commerce électronique (vente ou location) à distance ou pour le règlement à distance de dons ou cotisations, que tout tiers non autorisé accède aux données liées à la carte (ci-après la/les "Carte(s)") et afin de limiter l'utilisation du seul numéro de Carte pour donner un ordre de paiement, les schémas de paiement par carte ont mis en place des procédures de sécurisation des ordres de paiement donnés à distance par les titulaires de Carte (ci-après le «**Titulaire de la Carte** ») tel que le protocole 3D Secure, ainsi qu'un référentiel sécuritaire de protection des données sensibles (PCI DSS) annexé aux Conditions Particulières et un Référentiel Sécuritaire Accepteur annexé aux présentes Conditions Générales.

La procédure de sécurisation de paiement à distance consiste en l'authentification 3D Secure du Titulaire de la carte conformément aux spécifications établies par les schémas de paiement (« Protocole 3D Secure »).
L'Accepteur qui ne souhaite pas souscrire à l'offre de plateforme technique e-commerce Cyberplus Paiement commercialisée par l'Acquéreur, doit s'assurer auprès du prestataire technique tiers qu'il choisit pour sa solution de paiement à distance que sa plateforme de service technique e-commerce inclut l'authentification 3D Secure du Titulaire de la Carte, et que ce prestataire est en mesure de communiquer à l'Acquéreur et de recevoir de celui-ci toutes les informations nécessaires à la sécurisation des paiements à distance selon le Protocole 3D Secure. Si ledit prestataire ne communique pas les informations précitées à l'Acquéreur et/ou ne traite pas les informations renvoyées par l'Acquéreur, la procédure de sécurisation des paiements ne pourra pas être assurée et l'Accepteur en assumera la responsabilité.

L'Accepteur est également informé que les opérations de paiement sont garanties sous réserve du respect de l'ensemble des mesures de sécurité qu'il doit respecter et en particulier celles visées à l'article 7 des Conditions Générales et celles visées dans le Référentiel Sécuritaire Accepteur en annexe.

Article préliminaire et définitions

Accepteur

L'Accepteur d'un schéma de paiement par carte peut être un commerçant, tout prestataire de services, toute personne exerçant une profession libérale, susceptible d'utiliser ce schéma de paiement par carte tel que défini à l'article 2 du Règlement UE n°2015/751 du 29 avril 2015, et d'une manière générale, tout professionnel vendant ou louant des biens ou des prestations de services ou toute Entité dûment habilitée à recevoir des dons ou percevoir des cotisations utilisant le ou les schéma(s) de paiement par carte convenu(s) entre les Parties.

Les marques des schémas de paiement par carte pouvant être acceptées dans le cadre du présent contrat (ci-après le « **présent Contrat** » ou « **Contrat** ») sont celles indiquées dans les Conditions Particulières des contrats d'acceptation en paiement par carte selon le choix de l'Accepteur.

L'Accepteur dispose de toute liberté pour domicilier ses remises à l'encaissement auprès de l'établissement de crédit ou de paiement de son choix, membre du schéma de paiement par carte avec lequel il a passé un contrat d'acceptation.

Acquéreur

Par "Acquéreur", il faut entendre tout établissement de crédit ou de paiement habilité à organiser l'acceptation des Cartes portant la ou les marques d'un schéma de paiement par carte, avec lequel l'Accepteur a signé un contrat d'acceptation.

Système d'Acceptation

Par "Système d'Acceptation", il faut entendre les logiciels, protocoles conformes aux spécifications définies par les schémas de paiement par cartes et nécessaires à l'enregistrement, à la transmission et au traitement sécurisé des ordres de paiement par carte.

ARTICLE 1 : Définition et rôle du schéma de paiement par carte

Le schéma de paiement par carte est un ensemble unique de règles, pratiques, normes et/ou lignes directrices de mise en œuvre, régissant l'exécution d'opérations de paiement liées à une Carte (ci-après les « **Opérations de Paiement** » ou l' « **Opération de Paiement** »).

Le schéma de paiement par carte fixe ainsi les conditions et procédures pour l'utilisation et l'acceptation des Cartes portant sa ou ses marque(s) en vue du paiement de biens ou de prestations de services ou du règlement de dons ou de cotisations auprès des Accepteurs ayant choisi l'acceptation des Cartes du schéma de paiement par carte concerné, et cela dans le cadre des seules dispositions et procédures définies ou homologuées par celui-ci.

Pour des raisons sécuritaires, le schéma de paiement par carte peut imposer à tout moment et avec effet immédiat des modifications de conditions d'acceptation (seuil de demande d'autorisation, suppression de l'acceptabilité de certaines Cartes, résiliation immédiate du contrat d'acceptation, …).

ARTICLE 2 : Cartes acceptées

L'Accepteur choisit librement les marques des Cartes de paiement qu'il souhaite accepter comme moyen de paiement, sous réserve des Cartes de paiement proposées par l'Acquéreur.

Les Cartes acceptées sont celles listées dans les Conditions Particulières des contrats d'acceptation en paiement par carte (ci-après les « **Conditions Particulières** »).

Les Conditions Spécifiques de fonctionnement relatives au(x)schéma(s)de paiement de ces Cartes (ci-après les « **Conditions Spécifiques** ») figurent en Partie II du présent Contrat, conformément au choix de l'Accepteur.

ARTICLE 3 : Souscription du Contrat et convention de preuve

3.1 Modalités de souscription du contrat d'acceptation

L'Accepteur souscrit le présent Contrat après avoir pris connaissance des *« Conditions Particulières des contrats d'acceptation en paiement par carte bancaire »*, des *« Conditions Générales du contrat d'acceptation en paiement à distance sécurisé par carte bancaire »,* ainsi que des Conditions Spécifiques à chaque schéma de paiement par carte qu'il a sélectionné et du « *Référentiel Sécuritaire Accepteur »* en annexe.

La souscription au Contrat peut être réalisée, soit en agence, en présence d'un conseiller, soit à distance et notamment par internet, au travers de 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 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 ; en cas de réception de dons et règlement de cotisations, il s'engage également à se soumettre à la réglementation applicable.

4.2 - Utiliser le schéma de paiement par carte en s'abstenant de toute activité illicite, et notamment pénalement sanctionnée telle que :

- la mise en péril de mineurs, d'actes de pédophilie ;
- les actes de contrefaçon d'œuvres protégées par un droit de propriété intellectuelle ;
- les actes de contrefaçon de moyens ou d'instruments de paiements ;
- le non-respect de l'utilisation des données personnelles collectées ;
- les atteintes aux systèmes de traitement automatisé des 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 à l'exercice des professions règlementées.

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 - Afficher visiblement et sans ambiguïté chaque catégorie et Marques de Cartes qu'il accepte notamment en apposant de façon apparente sur l'écran du dispositif technique ou /et sur tout autre support de communication utilisé par le Titulaire de la Carte.

- Ne pas collecter au titre du présent contrat une opération de paiement pour laquelle il n'a pas reçu lui-même le consentement du Titulaire de la Carte.
- Garantir l'Acquéreur et le Schéma de paiement par carte le cas échéant, contre toute conséquence dommageable pouvant résulter pour eux du manquement aux obligations visées au présent article.

4.5 - Respecter les montants maximum indiqués par l'Acquéreur pour l'acceptation d'une Opération de Paiement par carte, et précisés dans les Conditions Particulières.

4.6 - S'identifier clairement dans la transmission de ses enregistrements à l'Acquéreur par le numéro d'immatriculation (pour la France le SIRET et le code activité NAF/APE) que l'INSEE lui a 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.

4.7 - 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 de vente en ligne. 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 de vente ou d'acceptation en ligne concerné.

4.8 - Accepter les paiements à distance sécurisés effectués avec les Cartes telles que listées dans les Conditions Particulières du présent Contrat 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.

Il est rappelé à l'Accepteur que, conformément à l'article 8 du règlement UE n°2015/751 du 29 avril 2015, dans le cas d'un paiement effectué par une Carte bancaire co-badgée portant le logo de deux ou plusieurs marques de schéma de paiement par carte (par exemple CB-Visa ou CB-Mastercard), le titulaire de la carte (ci-après le « **Titulaire de la Carte** ») doit pouvoir sélectionner le schéma de paiement par carte par lequel son Opération de Paiement va être opérée. L'Accepteur est dans l'obligation de le permettre et de respecter le choix du Titulaire de la Carte (cf. article 5 ci-après).

4.9 - 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 de paiement par carte.
Le délai de remise de la « transaction crédit » ne peut excéder 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 de paiement par carte.

Au-delà d'un délai maximum indiqué dans les Conditions Spécifiques à chaque schéma de paiement par carte, après la date de l'opération, l'encaissement des Opérations de Paiement n'est plus réalisable.

4.10 - 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 de paiement par Carte concerné.

4.11 - Utiliser obligatoirement un Système d'Acceptation conforme aux spécifications définies par le schéma de paiement concerné par l'Opération de Paiement et les procédures de sécurisation des ordres de paiement donnés à distance par les Titulaires de Carte proposées par l'Acquéreur. A cet effet, l'Accepteur organise la traçabilité adéquate des informations liées au paiement en ligne lorsqu'elles ont été stockées par lui.

4.12 - Prévoir, dans ses relations contractuelles avec les tiers, tels que les prestataires de services techniques ou sous-traitants intervenant dans le traitement et le stockage des données liées à l'utilisation des Cartes, que ces derniers s'engagent à respecter le référentiel de sécurité PCI DSS consultable sur le site pcisecuritystandards.org dont une présentation générale figure en Annexe des Conditions Particulières (« Présentation générale sur les règles PCI-DSS ») ainsi que le Référentiel Sécuritaire Accepteur précité, et acceptent que les audits visés à l'article 4.13 soient

réalisés dans leurs locaux et que les rapports puissent être communiqués comme précisé dans cet article.
- Déclarer annuellement et en cas de changement, à l'Acquéreur, lesdits prestataires techniques ou sous-traitants. A défaut, l'Accepteur s'expose à des pénalités telles qu'indiquées aux Conditions Particulières.

4.13 - Permettre à l'Acquéreur et aux schéma(s) de paiement par carte 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 tant des clauses du présent Contrat et ses annexes, ainsi que des exigences PCI DSS consultables sur le site pcisecuritystandards.org et dont une présentation générale figure en Annexe des Conditions Particulières (« Information sur les règles PCI DSS »). Cette vérification, appelée "procédure d'audit", peut intervenir à tout moment dès la conclusion du présent Contrat et/ou pendant sa durée.

- Autoriser la communication du rapport à l'Acquéreur et au schéma de paiement par carte concerné.

Au cas où le rapport d'audit révélerait un ou plusieurs manquements à ces clauses ou exigences, le schéma de paiement par carte peut demander à l'Acquéreur de procéder à une résiliation du contrat d'acceptation telle que prévue dans les Conditions Spécifiques de ce schéma de paiement.

4.14 - L'Accepteur doit respecter les exigences de sécurité PCI DSS consultables sur le site pcisecuritystandards.org.
En cas de compromission et si la non-conformité aux exigences PCI DSS est confirmée par le schéma de paiement 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 par l'Acquéreur. Ces frais et montants sont indiqués dans les Conditions Particulières.

4.15 - 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.

Les schémas de paiement peuvent appliquer des pénalités aux établissements Acquéreurs, calculées sur des bases identiques quel que soit l'Acquéreur, notamment :

- en cas de dépassement d'un certain nombre et/ou d'un taux d'impayés générés chez l'Accepteur,
- en cas de dépassement d'un certain nombre et/ou d'un certain taux de fraude générés chez l'Accepteur,
- lorsqu'il dépasse un certain nombre de factures crédits,
- en cas de non-respect de ses obligations d'information de l'Acquéreur relatives à son activité (ajout, modification, arrêt),
- en cas d'exercice d'une activité illicite ou non-conforme avec les règles édictées par les schémas de paiement par carte comme précisé à l'article 4.1 du présent Contrat, ou pour toute autre raison du fait des Opérations de Paiement générées chez l'Accepteur.

L'Accepteur accepte expressément et de manière irrévocable de prendre en charge l'intégralité de ces pénalités. Il autorise l'Acquéreur à prélever ces pénalités sur le compte désigné aux présentes Conditions Particulières.

L'attention de l'Accepteur est attirée sur le fait que ces pénalités peuvent atteindre des montants importants, définis par les schémas de paiement en considération des manquements constatés. Il reconnaît avoir été mis en garde par l'Acquéreur et renonce à formuler toute contestation de ce chef auprès de l'Acquéreur.

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

4.16 - 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 contrepassation desdites opérations afin de les inscrire sur le compte d'attente.

4.17 - L'Accepteur s'engage à informer l'Acquéreur de l'acceptation de toute Carte objet d'un accord entre l'Accepteur et un émetteur ou avec un gestionnaire de portefeuille numérique.

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) de paiement par carte visé(s) dans les Conditions Générales et Spécifiques et son (leur) évolution, les catégories de Cartes, les marques et les applications de paiement dont il assure l'acceptation, ainsi que les commissions d'interchange et les commissions de services applicables à chacune des Cartes et marques acceptées par lui ;

- Dans le cas où l'Accepteur a souscrit à l'offre de plateforme technique e-commerce Cyberplus Paiement commercialisée par l'Acquéreur, fournir à l'Accepteur les informations sur les procédures applicables à l'acceptation des paiements à distance sécurisés référencées par les schémas de paiement, que l'Accepteur doit utiliser obligatoirement, ainsi que leurs évolutions éventuelles. Ces informations figurent dans le contrat de service relatif à cette offre.

5.2 - Respecter le choix de la marque et de la catégorie de Carte et de l'application de paiement conformément à l'article 8 du Règlement UE n°2015/751 du 29 avril 2015 retenu par l'Accepteur et le Titulaire de la Carte pour donner l'ordre de paiement au point de vente ou d'acceptation en ligne.

5.3 - Mettre à la disposition de l'Accepteur, selon les Conditions Particulières convenues avec lui les informations relatives à la sécurité des opérations de paiement, notamment l'accès au système Acquéreur d'autorisation.

- Fournir à l'Accepteur toute information lui permettant d'installer un mécanisme automatique de sélection par défaut d'une marque de paiement ou d'une application de paiement spécifique, sous réserve que le Titulaire de la Carte ou de l'application de paiement puisse s'opposer, le cas échéant, à cette sélection et choisir une autre marque ou application de paiement parmi celles affichées par l'Accepteur.

5.4 - Fournir à l'Accepteur la liste et les caractéristiques des Cartes (marques et catégories) ou applications de paiement pouvant être acceptées et lui fournir, à sa demande, le fichier des codes émetteurs (BIN).

5.5 - Fournir à l'Accepteur les informations séparées relatives au montant des commissions de service commerçant, des commissions d'interchange et des frais de schéma de paiement applicables à chaque catégorie et à chaque marque de paiement.

L'Accepteur peut demander que ses Opérations de Paiement soient facturées selon une tarification regroupée quelles que soient les marques, application de paiement, catégories de cartes et quel que soit le taux de commission d'interchange applicable à l'Opération de Paiement, en complétant la demande figurant en Annexe 1 des Conditions Particulières.

- Inscrire l'Accepteur dans la liste des points d'acceptation habilités à recevoir des paiements par Cartes de Titulaires de Cartes dûment authentifiés.

5.6 - Créditer le compte de l'Accepteur des sommes qui lui sont dues, selon les conditions du présent Contrat.

5.7 - 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, les opérations non garanties et qui n'ont pu être imputées au compte sur lequel fonctionne la Carte.

5.8 – Communiquer à l'Accepteur sur support papier ou autre support durable au moins une fois par mois les informations suivantes relatives aux Opérations de Paiement individuelles liées à une carte et exécutées durant 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 ;
- le montant de tous les frais appliqués à l'Opération de Paiement, le montant de la commission de service acquittée par l'Accepteur et le montant de la commission d'interchange.

L'Acquéreur met à disposition, sur support papier ou durable, de l'Accepteur l'information mensuelle relative à la facturation regroupée par marque, application, catégorie de cartes et par taux de commission d'interchange applicable à l'Opération de Paiement dans le relevé mensuel des frais d'encaissement par cartes (RMFEC).

5.9 - 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) de paiement par Carte, les commissions de service payées par l'Accepteur et les commissions d'interchange en vigueur par marque et catégorie de Carte.

ARTICLE 6 : Garantie de paiement

6.1 - Les Opérations de Paiement sont garanties par l'Acquéreur sous réserve du respect de l'ensemble des mesures de sécurité à la charge de l'Accepteur visées à l'article 7 ainsi qu'à l'article relatif à la garantie de paiement figurant dans les Conditions Spécifiques à chacun des schémas de paiement par carte.

6.2 - 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.

6.3 - En cas de non-respect d'une seule de ces mesures, les enregistrements ne sont réglés que sous réserve de bonne fin d'encaissement.

6.4 - L'Accepteur autorise expressément l'Acquéreur à débiter d'office son compte du montant de toute Opération de Paiement non garantie n'ayant pu être imputée au compte auquel la Carte ou l'application de paiement est rattachée.

ARTICLE 7 : Mesures de sécurité

7.1 - La procédure de sécurisation de paiement à distance consiste en l'authentification 3D Secure du Titulaire de la Carte conformément aux spécifications établies par les schémas de paiement (« Protocole 3D Secure »).
L'Accepteur qui ne souhaite pas souscrire à l'offre de plateforme techniques e-commerce Cyberplus Paiement commercialisée par l'Acquéreur, doit s'assurer auprès du prestataire technique tiers qu'il choisit pour sa solution de paiement à distance que son offre de plateforme de services techniques e-commerce inclut l'authentification 3D Secure du Titulaire de la Carte, et que ce prestataire est en mesure de communiquer à l'Acquéreur et de recevoir de celui-ci toutes les informations nécessaires à la sécurisation des paiements à distance selon le Protocole 3D Secure. Si ledit prestataire ne communique pas les informations précitées à l'Acquéreur et/ou ne traite pas les informations renvoyées par l'Acquéreur, la procédure de sécurisation des paiements ne pourra pas être assurée et l'Accepteur en assumera la responsabilité.

7.2 - L'Accepteur doit informer immédiatement l'Acquéreur 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...) ;

- 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.

7.3 - Lors du paiement, l'Accepteur s'engage à :
7.3.1 - Appliquer la procédure de sécurisation des ordres de paiement communiquée par l'Acquéreur, et décrite en en-tête des Conditions Générales du présent contrat, rappelée en avertissement ainsi qu'à l'article 7.1 du Présent contrat.

7.3.2 - Obtenir de l'Acquéreur un justificatif d'acceptation matérialisant les contrôles effectués et la validité de l'ordre de paiement.

7.3.3 – Vérifier électroniquement l'acceptabilité de la Carte c'est-à-dire :

- la période de fin (et éventuellement de début) de validité.
- la marque, la catégorie de Carte ou d'application de paiement du schéma de paiement qui doivent être l'une de celles définies dans les Conditions Particulières.
- le cryptogramme visuel donné par le Titulaire de la carte.

7.3.4 - Contrôler le numéro de Carte par rapport à la dernière liste des Cartes faisant l'objet d'un blocage ou d'une opposition diffusée par l'Acquéreur, selon les Conditions Spécifiques convenues avec l'Acquéreur.

7.3.5 - Obtenir une autorisation d'un montant identique à l'opération :

- il est formellement interdit de fractionner le montant d'un paiement en plusieurs Opérations de Paiement successives,
- 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 en ligne, dépasse celui du seuil de demande d'autorisation fixé dans les Conditions Spécifiques convenues avec l'Acquéreur, et ceci quelle que soit la méthode d'acquisition des informations,

- lorsque le Système d'Acceptation déclenche une demande d'autorisation, indépendamment du seuil de demande d'autorisation fixé dans les Conditions Spécifiques convenues avec l'Acquéreur.

A défaut, l'opération ne sera pas garantie, même pour la fraction autorisée ou correspondant au montant du seuil de demande d'autorisation.
Une opération pour laquelle l'autorisation a été refusée par le système Acquéreur d'autorisation n'est jamais garantie.

7.4 - Après le paiement, l'Accepteur s'engage à :

7.4.1 - Transmettre les enregistrements des Opérations de Paiement à l'Acquéreur dans le délai maximum de 7 jours calendaires à compter de la date de l'Opération de Paiement, sauf dispositions contraires précisées dans les Conditions Spécifiques relatives à chaque schéma de paiement par carte.

Au-delà de ce délai, les Opérations de Paiement ne seront réglées que sous réserve de bonne fin d'encaissement.

L'Accepteur ne doit transmettre que les enregistrements électroniques des opérations pour lesquelles un ordre de paiement a été donné à son profit. Toute opération ayant fait l'objet d'une autorisation transmise par l'Acquéreur signataire du présent Contrat doit être obligatoirement remise à ce dernier.

- 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 convenues avec l'Acquéreur. Toute opération ayant fait l'objet d'une autorisation transmise par l'Acquéreur signataire du présent Contrat doit être obligatoirement remis à ce dernier.

7.4.2 - Envoyer au Titulaire de la Carte, à sa demande, un ticket électronique précisant, entre autres, le mode de paiement par carte utilisé.

7.4.3 - Communiquer, à la demande de l'Acquéreur, tout justificatif des Opérations de Paiement dans les 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.

7.4.4 - L'Accepteur s'engage à :
- ne pas stocker sous quelque forme que ce soit le cryptogramme visuel des Cartes ;
- 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 loi "Informatique et Libertés" du 6 janvier 1978 et notamment de son article 34.

7.4.5 - 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 : Modalités annexe de fonctionnement

8.1 - Réclamation
Toute réclamation doit être justifiée et formulée par écrit à l'Acquéreur, dans un délai maximum de **6 mois** à compter de la date de l'opération contestée, sous peine de forclusion.
Toutefois, ce délai est réduit à **15 jours calendaires** à compter de la date de débit en compte, en cas d'opération non garantie.

8.2 - 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 de paiement par carte 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 de paiement par carte dont les Cartes sont concernées.

8.3 - Remboursement ou Transaction crédit
Le remboursement partiel ou total d'un achat d'un bien ou d'un service réglé par Carte doit, avec l'accord de son Titulaire, être effectué au Titulaire de la Carte utilisée pour l'opération initiale. L'Accepteur doit alors utiliser la procédure dite de "Transaction crédit", et dans le délai prévu par les règles du schéma de paiement concerné et indiqué aux Conditions Spécifiques, effectuer la remise correspondante à l'Acquéreur 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 9 : Modifications du Contrat

9.1 - L'Acquéreur peut modifier à tout moment les présentes Conditions Générales, les Conditions Spécifiques

à chaque schéma de paiement par carte, ainsi que les Conditions Particulières.

9.2 - L'Acquéreur peut notamment apporter :

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

9.3 - Les nouvelles conditions entrent généralement en vigueur au terme d'un délai minimum fixé à un mois à compter de l'envoi d'une lettre d'information ou de notification à l'Accepteur ou par support électronique.

9.4 - En cas de modifications importantes et/ou pour des raisons sécuritaires, notamment lorsque l'Acquéreur constate dans le point d'acceptation en ligne une utilisation anormale de Cartes perdues, volées ou contrefaites, ce délai est exceptionnellement réduit à 5 jours calendaires.

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

9.6 - Le non-respect des nouvelles conditions techniques ou sécuritaires, dans les délais impartis, peut entraîner la résiliation du présent Contrat par l'Acquéreur, voire la suspension de l'acceptation des carte du schéma de paiement par carte concerné selon les dispositions prévues à cet effet dans les Conditions Spécifiques du schéma de paiement concerné figurant en partie II du présent Contrat.

ARTICLE 10 : Durée et résiliation du Contrat

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

L'Accepteur ou l'Acquéreur peuvent chacun et à tout moment, sans justificatif ni préavis, sous réserve du dénouement des opérations en cours, mettre fin au présent Contrat, sans qu'il soit nécessaire d'accomplir aucune autre formalité que l'envoi d'une lettre recommandée avec demande d'avis de réception.

L'Accepteur garde alors la faculté de souscrire un contrat d'acceptation avec tout autre Acquéreur de son choix.
Lorsque cette résiliation fait suite à un désaccord sur les modifications prévues à l'article 8 ci-dessus, elle ne peut intervenir qu'au-delà du délai prévu dans cet article pour l'entrée en vigueur de ces modifications.

10.2 - 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, il se révélerait des impayés, ceux-ci seront à la charge de l'Accepteur ou pourront faire l'objet d'une déclaration de créances.

10.3 - L'Accepteur sera tenu de restituer à l'Acquéreur les dispositifs techniques et sécuritaires, le Système d'Acceptation et les documents en sa possession dont l'Acquéreur 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 de vente en ligne et de ses supports de communication tout signe d'acceptation des Cartes, application de paiement ou marques de schémas de paiement concernés.

ARTICLE 11 : Secret Bancaire et protection des données à caractère personnel

11.1 - Conformément à la loi du 6 janvier 1978 relative à la loi "Informatique et Libertés" modifiée par la loi du 6 août 2004, les informations relatives à l'Accepteur, collectées par l'Acquéreur sont nécessaires pour l'exécution des ordres de paiement transmis et leur sécurisation.

L'Accepteur, personne physique, ou la personne physique le représentant ou sur laquelle portent les données à caractère personnel ci-dessus recueillies, a le droit d'en obtenir communication, et 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, auprès de l'Acquéreur.

11.2 - A 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.
L'Accepteur ne peut utiliser ces données à caractère personnel que pour l'exécution des ordres de paiement par Carte et le traitement des réclamations dont ils peuvent être l'objet.

Sauf obligations légales et réglementaires, il ne peut ni céder, ni faire un quelconque usage qui ne soit pas directement prévu par le présent Contrat des données liées à l'utilisation de la Carte et notamment du numéro de la Carte, de sa date de fin de validité et du cryptogramme visuel dont il doit garantir la sécurité et la confidentialité conformément aux dispositions du 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. A cet égard, l'Accepteur s'engage d'ores et déjà à leur permettre d'exercer ces droits.

11.3 - Les dispositions de la loi pour la confiance dans l'économie numérique du 21 juin 2004 obligent l'Accepteur à recueillir le consentement exprès et préalable du Titulaire de Carte lors de toute utilisation de l'adresse mail et du 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 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.

11.4 - L'Accepteur 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.

ARTICLE 12 : 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 13 : Loi applicable et tribunaux compétents

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 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.

ARTICLE 14 : Langue du présent Contrat

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

ARTICLE 15 : 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 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 règle d'ordre public s'imposant à la partie concernée, ou pour répondre à une demande d'une cour ou d'un tribunal compétent, d'une autorité gouvernementale, bancaire, fiscale ou autre autorité réglementaire ou de toute autre entité similaire, du règlement de tout marché boursier concerné ou conformément à la législation ou à la réglementation applicable.

PARTIE II.1

Conditions spécifiques d'acceptation en paiement à distance sécurisé pour les opérations réalisées selon le schéma de paiement « 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 de paiement par cartes «CB ».

ARTICLE 1 : Conditions spécifiques liées à la garantie de paiement des Opérations de Paiement « CB »

La garantie de paiement est conditionnée par le respect des différentes mesures de sécurité indiquées dans les Conditions Générales et Spécifiques.

Quel que soit le montant de l'Opération de Paiement, une demande d'autorisation doit systématiquement être faite pour une Opération de Paiement à distance sécurisée réalisée selon le schéma de paiement par carte « CB ».

ARTICLE 2 : Délai 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 de paiement CB dans un délai maximum de **6 mois. Au-delà de ce délai, l'encaissement des Opérations de Paiement n'est plus réalisable dans le cadre du schéma de paiement par carte « CB ».**

ARTICLE 3 : 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 4 : Suspension et clôture du contrat pour le schéma de paiement « CB »

4.1 - Le schéma de paiement par carte « 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 de paiement « 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 de paiement « CB »,
- en cas de comportement frauduleux de la part de l'Accepteur responsable du point de vente.

4.2 - L'Accepteur s'engage alors à restituer, le cas échéant, à l'Acquéreur le Système d'Acceptation, les dispositifs techniques et sécuritaires « CB » et les documents en sa possession dont l'Acquéreur est propriétaire et à retirer immédiatement de son point de vente en ligne tout signe d'acceptation des Cartes ou applications de paiement ou marque du schéma de paiement « CB ».

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

4.4 - A l'expiration de ce délai, l'Accepteur peut, sous réserve de l'accord préalable du schéma de paiement « 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.

ARTICLE 5 : Communication des Commissions Interbancaires de Paiement (interchange) de « CB »

Les taux des commissions interbancaires pratiqués par le schéma de paiement par Carte « CB » sont publics et consultables sur son site internet du schéma de paiement par carte« CB », http://www.cartes-bancaires.com.

PARTIE II.2

Conditions spécifiques d'acceptation en paiement à distance sécurisé pour les opérations réalisées selon les schémas de paiement « 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 de paiement par cartes « 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 différentes mesures de sécurité indiquées dans les Conditions Générales et Spécifiques.

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 de paiement par carte « Visa », « Visa Electron » ou « VPAY », que ce soit une carte étrangère ou française, qu'elle soit co-badgée avec le schéma de paiement par carte « CB » ou non.

1.2 – Délai de transmission des Opérations de Paiement à l'Acquéreur

Les délais de transmission à l'Acquéreur des Opérations de Paiement réalisées en Europe (au sens de Visa Europe) sont les suivants :

- Pour les Opérations de Paiement Visa "Prépayé": maximum 2 jours calendaires
- Pour les Opérations de Paiement Visa "Electron" : maximum 5 jours calendaires
- Pour toutes les autres Opérations de Paiement par Carte Visa : maximum 8 jours calendaires.

ARTICLE 2 : Suspension ou clôture du contrat à la demande du schéma de paiement « Visa », « Visa Electron » et « VPAY »

Les schémas de paiement par carte « Visa », « Visa Electron » ou « VPay » peuvent dans certains cas (cf. article 4 des Conditions Générales) se retourner vers l'Acquéreur pour que celui-ci exige de son Accepteur qu'il respecte les règles du schéma de paiement par Carte « 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 de paiement par carte « Visa », « Visa Electron » et « VPay » émises par un émetteur situé hors de l'Union Européenne sont systématiquement acceptées par l'Accepteur si celui-ci accepte au moins un type de Carte du schéma de paiement par carte Visa de l'union Européenne.

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 de paiement par Carte « Visa » , **«** Visa Electron » ou« VPAY » sont publics et consultables sur son site internet : www.visa-europe.fr.

PARTIE II.3

Conditions spécifiques d'acceptation en paiement à distance sécurisé pour les opérations réalisées selon les schémas de paiement « Mastercard » et « 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 de paiement par cartes « Mastercard » et « Maestro ».

ARTICLE 1 : Conditions liées à la garantie de paiement des Opérations de Paiement « Mastercard » et « Maestro »

La garantie de paiement est conditionnée par le respect des différentes mesures de sécurité indiquées dans les Conditions Générales et Spécifiques.

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 le schéma de paiement par carte « Mastercard » ou « Maestro ».

1.2 – Délai de transmission des Opérations de Paiement à l'Acquéreur

Les délais de transmission à l'Acquéreur des Opérations de Paiement réalisées en Europe (au sens de Mastercard) sont les suivants :

- Pour les Opérations de Paiement Mastercard "Prépayé": maximum 2 jours calendaires
- Pour les Opérations de Paiement "Maestro" : maximum 5 jours calendaires
- Pour toutes les autres Opérations de Paiement par Carte Mastercard: maximum 8 jours calendaires.

ARTICLE 2 : Suspension ou résiliation du contrat à la demande du schéma de paiement « Mastercard » et « Maestro »

Les schémas de paiement par carte Mastercard et Maestro peuvent dans certains cas (cf. article 4 des Conditions Générales) se retourner vers l'Acquéreur pour que celui-ci exige de son Accepteur qu'il respecte leurs règles, faute de quoi l'Acquéreur sera dans l'obligation de résilier le présent Contrat.

ARTICLE 3 : Acceptation des cartes « Mastercard » et « Maestro » émises hors Union Européenne

Les Cartes des schémas de paiement par carte « Mastercard » et « Maestro » émises par un émetteur situé hors de l'Union Européenne sont systématiquement acceptées par l'Accepteur si celui-ci accepte au moins un type de Carte de ces schémas de paiement émise dans l'union Européenne.

ARTICLE 4 : Communication des Commissions Interbancaires de Paiement (interchange) de « Mastercard » et « Maestro »

Les taux de commissions d'interchange pratiqués par les schémas de paiement par Carte « Mastercard » et « Maestro » sont publics et consultables sur son site internet : www.mastercard.com.

ANNEXE – Référentiel Sécuritaire 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 Titulaires de Cartes, 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.
Le serveur de base de données client ainsi que le serveur hébergeant le système de paiement ne doivent être accessibles de l'extérieur 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 d'encaissement.
Les droits des utilisateurs et des administrateurs ainsi que 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 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 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 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 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 assurées 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

recommandations 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 préservée 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.