BANQUE POPULAIRE
RIVES DE PARIS

Société anonyme coopérative de Banque Populaire à capital variable, régie par les articles L. 512-2 et suivants du Code monétaire et financier et l'ensemble des textes relatifs aux Banques Populaires et aux établissements de crédit - 552 002 313 RCS Paris - Société immatriculée au Registre des Intermédiaires en Assurance sous le n° 07 022 545 - 76-78, avenue de France - 75204 Paris Cedex 13 - Téléphone : 01 73 07 48 37 - Télécopie : 01 73 07 78 05. Internet : www.rivesparis.banquepopulaire.fr.
Numéro d'identification intracommunautaire FR 59 552 002 313 Code APE 6419 Z

CONDITIONS GENERALES
DES CONTRATS D'ACCEPTATION DES CARTES BANCAIRES CHINA UNION PAY POUR LES PAIEMENTS DE PROXIMITE

Référencées CACUP_2014001 (pages de 1 à 8)

Les Parties ont convenu et arrêté ce qui suit :

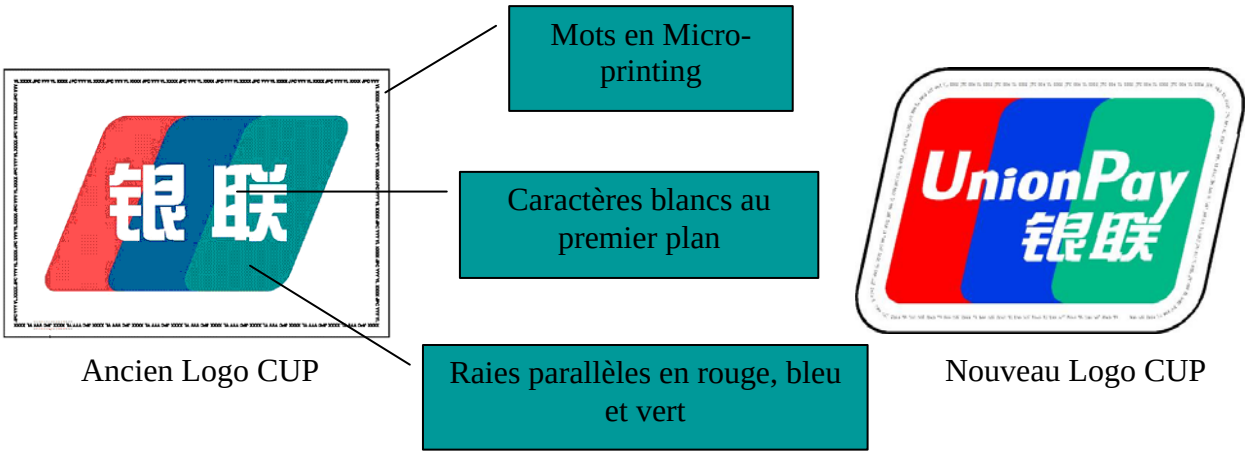
ARTICLE 1 : Définitions

Les termes énoncés dans le présent Contrat et débutant par une majuscule auront la signification qui leur est donnée dans le présent article.

Applicatif CUP : logiciel fourni par la Banque Acquéreur installé sur le TPE permettant la réalisation de transactions au moyen de Carte CUP.

Carte CUP : désigne les cartes émises par les banques adhérentes au réseau CUP.
Le Logo CUP est obligatoirement inséré sur les Cartes CUP, toutefois ces Cartes CUP peuvent être cobadgée avec d'autres logos tel que celui de VISA, de MasterCard. En revanche, la mention du nom du titulaire sur la Carte CUP est facultative..

Logo CUP : Il y a 2 logos en utilisation, les cartes avec ancien logo seront remplacées par CUP au fur et à mesure.



Ancien Logo CUP

Nouveau Logo CUP

CUP : China Union Pay, institution de droit chinois chargée de veiller à l'intégrité du système d'émission et d'acquisition des cartes bancaires chinoises.

Equipement : désigne l'ensemble composé du TPE et de l'Applicatif CUP.

Journée CUP : désigne une journée basée sur les horaires de Beijing transposés en France, soit :
- en hiver lorsque la France a 7 heures de décalage horaire avec Beijing, une Journée CUP commence à 16 heures 00, heure de Paris et finit le lendemain à 16 heures 00, heure de Paris.
- en été lorsque la France a 6 heures de décalage horaire avec Beijing, une Journée CUP commence à 17 heures 00, heure de Paris et finit le lendemain 17 heures 00, heure de Paris.

Titulaire : Personne physique, qui détient une Carte CUP.

Ticket Titulaire : désigne le ticket émis par l'Equipement destiné au Titulaire, sur lequel figure
- le numéro tronqué et la date d'expiration de la Carte CUP ;
- la date et lieu du Paiement ;
- le montant du Paiement en Euros y compris les taxes applicables ;
- les coordonnées et l'identifiant de l'Accepteur (code de la Banque Acquéreur et numéro du commerçant) ;
- le numéro d'Autorisation ;
- le numéro de la transaction.

Ticket Accepteur : désigne le ticket émis par l'Equipement destiné à l'Accepteur, sur lequel figure :
- le numéro de la Carte CUP ;
- la date et lieu du Paiement ;
- le montant du Paiement en Euros y compris les taxes applicables ;
- les coordonnées de l'Accepteur ;
- le numéro d'Autorisation ;
- la signature du Titulaire ;
- le numéro de la transaction.

TPE : terminal de paiement électronique, compatible avec l'applicatif de paiement CUP.

ARTICLE 2 : Objet

Les présentes ont pour objet de définir les conditions dans lesquelles l'Accepteur peut accepter des Cartes CUP pour le paiement de proximité d'achats ou de location de biens ou le paiement de proximité de prestations de services.
Le Contrat est constitué des dispositions du présent document et de ses éventuelles annexes.
Toute modification du Contrat ne pourra intervenir que par voie d'avenant(s) signé(s) entre les représentants des Parties.

ARTICLE 3 : condition d'acceptation de la Carte CUP

3.1 Conditions relatives à l'Equipement

L'Accepteur doit :

- Réserver dans le magasin l'emplacement nécessaire à l'installation de l'Equipement.
- Faire son affaire des travaux préalables à la mise en place de l'Equipement (mise à disposition des prises électriques, téléphoniques, ...).
- S'informer de ses obligations d'utilisation de l'Equipement, et le cas échant concernant l'installation de l'Applicatif CUP sur un TPE qui n'est pas fourni par la Banque Acquéreur.
- Laisser libre accès à la Banque Acquéreur ou tout tiers désigné par elle, pour les différents travaux de mise en oeuvre, de maintenance future et de mise à niveau qui seront effectués.
- Ne pas utiliser l'Equipement à des fins illicites ou non autorisées par le constructeur ou la Banque Acquéreur, et n'y apporter aucune modification.
- Assurer, selon le mode d'emploi, les conditions de bon fonctionnement de l'Equipement dont il a la garde.
- Veiller à ce que sa police d'assurance couvre bien les risques inhérents à la garde de l'Equipement et dont la Banque Acquéreur ne saurait être responsable, ainsi que les dommages directs ou indirects résultant de leur destruction ou de leur altération.
- Assumer toutes les obligations du dépositaire, conformément aux dispositions des articles 1927 et suivants du Code Civil.

3.2 Respect des consignes de signalétique

La Banque Acquéreur fournit, dès la prise d'effet des présentes, des visuels publicitaires (vitrophanies notamment) faisant clairement apparaître l'acceptation des Cartes CUP chez l'Accepteur.

L'Accepteur s'engage à :

- Afficher de manière appropriée les supports publicitaires fournis par la Banque Acquéreur à proximité de l'Equipement;
- Afficher visiblement le montant minimum éventuel à partir duquel le paiement par Carte CUP est accepté afin que les clients en soient préalablement informés.
- Informer clairement le Titulaire des conditions dans lesquelles il peut utiliser sa Carte CUP pour le règlement de ses achats de biens ou de prestations de services conformément aux dispositions des articles 3.3, 4.2 et à l'annexe1.

Les visuels publicitaires doivent être enlevés immédiatement dès la fin des présentes pour quelque raison que ce soit.

3.3 Conditions relatives aux biens ou aux prestations pouvant être payés avec la Carte CUP

La Carte CUP ne peut pas servir au règlement d'une fourniture d'argent liquide ou de tous biens ou services dont l'achat ou la prestation est contraire aux lois en vigueur sur le territoire français. La Banque Acquéreur se réserve la faculté de demander à l'Accepteur le remboursement de tout débit s'il apparaît que celui-ci correspond à un tel règlement.
L'Accepteur s'engage à accepter la Carte CUP pour le paiement d'achats de biens ou de prestations de services offerts à sa clientèle et réellement effectués (à l'exclusion de toutes délivrances d'espèces ou de tous titres convertibles en espèces pour leur valeur faciale), même lorsqu'il s'agit d'articles vendus à titre de promotion ou de soldes.
L'Accepteur s'interdit de collecter des paiements dus à raison de ventes ou de prestations réalisées par d'autres commerçants ou prestataires avec leur propre clientèle.

3.4 Conditions relatives à la neutralité vis-à-vis de l'instrument de paiement

L'Accepteur s'engage à ne pas discriminer ou ne pas encourager un Titulaire, souhaitant régler ses prestations/achats au moyen de la Carte CUP, à utiliser toute autre carte ou un autre instrument de paiement; sauf si l'une quelconque des conditions détaillées dans cet article ne pouvait être remplie.
Aussi, l'Accepteur s'engage à appliquer aux titulaires de la Carte CUP les mêmes prix et tarifs qu'à l'ensemble de sa clientèle. En tout état de cause, l'Accepteur ne doit leur faire supporter, directement ou indirectement, aucun frais supplémentaire ni même imposer aucune restriction ou condition supplémentaire lors de l'utilisation de la Carte CUP.

ARTICLE 4 : Acceptation de la Carte CUP

4.1 Vérification préalable

Lors de la présentation physique de la Carte CUP en paiement l'Accepteur doit vérifier préalablement que :

- le Logo CUP figure sur la Carte CUP ;
- la Carte CUP comporte une signature dans la zone appropriée ;
- la Carte CUP, et en particulier l'espace réservé à la signature, n'est pas altérée ni détériorée, n'a subi aucune modification ou surcharge ;
- la photo si elle figure sur la Carte CUP correspond au Titulaire ;
- aucun avis d'annulation de la Carte CUP n'a été porté à sa connaissance.

Les Cartes CUP non signées doivent être refusées par l'Accepteur.

4.2 Déroulement d'une transaction

Toutes les transactions doivent être réalisées en Euros.
L'Accepteur doit respecter le montant maximum autorisé par CUP pour une transaction. Ce montant maximum est communiqué le cas échéant, par la Banque acquéreur à l'Accepteur. Il est formellement interdit de fractionner le montant des débits.
Dans tous les cas l'Accepteur s'engage à utiliser l'Equipement, respecter les indications affichées sur son écran et suivre les procédures dont les modalités techniques lui ont été indiquées par la Banque Accepteur.
Les transactions peuvent être (i) soit une opération de paiement d'un achat de bien ou de prestation de services immédiat par le client de l'Accepteur, (ii) soit une opération d'annulation d'une opération d'achat (iii) soit un remboursement de l'Accepteur qui se concrétise par une transaction de crédit.
Les conditions d'utilisation et règles de fonctionnement spéciales des opérations de paiement d'achat différé qui nécessitent une pré autorisation sont traitées le cas échéant dans une annexe spécifique à ce Contrat intitulée « opération de paiement différé d'un achat avec pré autorisation ».

4.2.1 Déroulement d'une opération de paiement d'un achat

L'Accepteur saisit le montant de la transaction.
L'Equipement, après la lecture de la piste magnétique de la Carte CUP, demande la saisie d'un code confidentiel. La saisie effective ou non d'un code confidentiel par le Titulaire est fonction des obligations imposées à ce dernier par sa banque émettrice. L'Accepteur doit permettre au Titulaire (i) soit d'appuyer uniquement sur la touche « validation » (ii) soit de composer son code confidentiel, dans les meilleures conditions de confidentialité.
La demande d'autorisation est automatique et systématique. En cas de refus d'autorisation, la transaction est obligatoirement rejetée.
Pour chaque paiement un Ticket Titulaire et un Ticket Accepteur sont émis.
Dans tous les cas, le Ticket Accepteur doit être signé par le Titulaire en présence de l'Accepteur.
L'Accepteur doit alors vérifier sur le Ticket Accepteur (i) la conformité de la signature avec celle qui figure sur la Carte CUP utilisée, (ii) et si le numéro figurant sur la Carte CUP est rigoureusement identique à celui imprimé.
Enfin, l'Accepteur doit remettre au Titulaire le Ticket Titulaire.
Le strict respect du déroulement de l'opération de paiement d'achat tel que décrit dans cet article, est la condition obligatoire pour que l'Accepteur soit garanti du paiement des transactions ayant été autorisées.

4.2.2 Déroulement d'une opération d'annulation

Toutes les transactions d'achat peuvent être annulées, à la condition que l'opération d'achat et l'opération d'annulation soit effectuée au sein de la même Journée CUP telle que définie à l'article 1 des présentes.
Préalablement, l'Accepteur doit impérativement demander au Titulaire, le Ticket Titulaire qu'il a reçu à l'issue d'une opération de paiement.
A partir du numéro de transaction figurant sur le Ticket Titulaire, l'Accepteur peut annuler la transaction en suivant la procédure de l'Equipement.

4.2.3 Déroulement d'une transaction de crédit

Les transactions réglées par Carte CUP ne doivent pas faire l'objet d'un remboursement partiel ou total par un autre moyen de paiement. Tous les remboursements doivent être effectués en respectant les règles de la transaction de crédit telles que décrites dans cet article.
Seules les transactions de paiement lors d'un achat sont susceptibles d'être créditées.
Le montant qui peut être crédité par l'Accepteur peut être égal ou inférieur au montant de la transaction d'achat préalable.
Préalablement, l'Accepteur doit impérativement demander au Titulaire le Ticket Titulaire qu'il a reçu à l'issue d'une opération de paiement. En l'absence de la présentation du ticket l'Accepteur ne pourra pas procéder à l'opération de remboursement
A partir du numéro de transaction figurant sur le Ticket Titulaire, l'Accepteur peut créditer son client en suivant la procédure de l'Equipement.

ARTICLE 5 : Date de transaction

En raison du mode de fonctionnement interne au système CUP, seules les transactions effectuées dans une Journée CUP seront considérées, pour le règlement, avoir été effectuées à la date du jour, soit J. Il en découle que tous les transactions effectuées après 16 heures 00 en hiver heure de Paris et 17 heures 00 en été heure de Paris seront considérées, pour le règlement, avoir été effectuées lors d'une nouvelle Journée CUP.

ARTICLE 6 : Obligation post paiement

L'Accepteur doit pendant une période de un (1) an et un (1) jour à compter de la date de la transaction :

- communiquer, à la demande de la Banque Acquéreur, tous justificatifs des transactions de paiement, notamment un document comportant la signature du porteur, ou tout autre document engageant le titulaire de la Carte CUP, par exemple les Tickets Accepteur ou les tickets de caisse, dans un délai maximum de 8 jours calendaires à compter de la demande,
- répondre à toutes demandes de renseignements adressées par la Banque acquéreur à la suite d'une réclamation formulée par un Titulaire, dans un délai maximum de 8 jours calendaires à compter de la demande.

A défaut, la Banque Acquéreur se réserve le droit de demander le remboursement des sommes si la transaction litigieuse demeurait impayée par le Titulaire, sans préjudice de la résiliation du présent contrat, conformément aux dispositions de l'article 13 ci-dessous.

ARTICLE 7 : Litiges

7.1- Réclamation de l'Accepteur

Toute réclamation doit être formulée par écrit fax ou courrier simple à la Banque Acquéreur, dans un délai maximum de 60 jours calendaires à réception du relevé d'opérations CUP.
A l'issue de ce délai, aucune réclamation ne sera acceptée par la Banque Acquéreur.

7.2- Réclamation du Titulaire

Suite à une contestation de transaction par un Titulaire, la Banque Acquéreur adresse à l'Accepteur une demande d'informations (justificatifs de la transaction), ce dernier dispose d'un délai maximum de 8 jours calendaires à compter de la réception de la demande pour y répondre.
Au delà, le montant de l'impayé sera débité du compte de l'Accepteur.

ARTICLE 8 : Propriété intellectuelle

Ce contrat ne confère aucun droit à une Partie d'utiliser le nom, le logo, les marques, les entités légales, accroches ou toute autre désignation (Marque) de l'autre Partie au présent Contrat.
Aucune utilisation ne peut être faite des Marques de l'une des Parties au présent Contrat sans un accord écrit préalable de cette Partie.
L'Accepteur autorise la Banque Acquéreur à utiliser le nom et l'adresse de son établissement(s), en incluant notamment l'adresse physique, l'adresse du site Internet et/ou URL si nécessaire dans des communications, proposant des listes d'établissements qui acceptent la Carte CUP, publiées périodiquement.
L'Accepteur autorise expressément la Banque Acquéreur à traiter en mémoire informatisée les données à caractère personnel le concernant conformément à la loi « informatique et libertés » du 6 janvier 1978, et à les communiquer à ses fournisseurs de services, à ses sous-traitants, ainsi qu'à des entités de son groupe ou à ses partenaires, à des fins de prospection commerciale. Il peut, pour des motifs légitimes, s'opposer à ce que ces données fassent l'objet d'un traitement, notamment à des fins de prospection commerciale. Pour exercer ses droits d'accès, de rectification ou d'opposition, l'Accepteur doit s'adresser par écrit à : Banque Populaire Rives de Paris – Service Qualité – 76 / 78 Avenue de France – 75 204 Paris Cédex 13.

ARTICLE 9 : Conditions financières

L'Accepteur s'engage à régler les commissions, frais et d'une manière générale, toutes sommes dues au titre de l'acceptation des Cartes CUP du réseau CUP. Les conditions financières sont précisées dans l'annexe « conditions financières ».
L'Accepteur s'engage à payer les frais de location ou de dépôt vente selon les conditions particulières convenues avec la Banque Acquéreur.
La Banque Acquéreur s'engage à créditer le compte de l'Accepteur des sommes qui lui sont dues, selon les modalités décrites dans l'annexe « conditions financières ».

ARTICLE 10 : Dysfonctionnement De L'équipement

L'Accepteur doit informer immédiatement la Banque Acquéreur en cas de fonctionnement anormal de l'Equipement, et pour toutes les autres anomalies.

ARTICLE 11 : Durée

Le présent Contrat entre en vigueur à sa date de signature et est conclu pour une durée indéterminée.

ARTICLE 12 : modification des conditions du contrat

La Banque Acquéreur peut modifier à tout moment le présent Contrat, soit pour des raisons techniques, financières, réglementaires ou relatives à la sécurité du système, soit à la demande de CUP.
Les modifications techniques autres que les travaux d'installation et de maintenance, concernent notamment les modifications de logiciel, le changement de certains paramètres, la remise en état de l'Equipement suite à un dysfonctionnement, etc...
Les nouvelles conditions entrent généralement en vigueur au terme d'un délai minimum fixé à 10 jours calendaires à compter de l'envoi d'une lettre d'information ou de notification ; d'un commun accord les Parties peuvent déroger à ce délai en cas de modifications importantes.
Ce délai est exceptionnellement réduit, pour des raisons de sécurité, à cinq jours calendaires lorsque la Banque Acquéreur constate, dans le point de vente, une utilisation anormale de Cartes CUP perdues, volées ou contrefaites.
Le non respect des nouvelles conditions techniques ou sécuritaires, dans les délais impartis, peut entraîner la résiliation du contrat.

ARTICLE 13 : Résiliation du contrat

13.1. Résiliation de plein droit

L'Accepteur d'une part, la Banque Acquéreur d'autre part, peuvent, à tout moment, sans justificatif, avec un préavis de (1) un mois sous réserve du dénouement des opérations en cours, mettre fin au présent contrat, sans qu'il soit nécessaire d'accomplir aucune formalité que l'envoi d'une lettre recommandée avec demande d'avis de réception. La résiliation prendra effet huit (8) jours après réception par l'autre Partie d'une mise en demeure adressée par lettre recommandée avec demande d'avis de réception.

13.2. Résiliation automatique sans préavis

Une Partie peut également résilier immédiatement de plein droit, sans préavis, le Contrat, par simple lettre recommandée avec demande d'avis de réception, dans les cas limitatifs suivants :

- ♦ cessation d'activité de l'Accepteur pour quelque raison que ce soit, cession ou mutation du fonds de commerce, sous réserve du dénouement des opérations en cours,
- ♦ à la demande de CUP.

En cas de manquement, par l'Accepteur, à l'une quelconque des obligations souscrites au titre des présentes, outre l'éventuelle déchéance du droit à garantie du paiement des transactions (article 4.2.1), la Banque pourra prononcer la résiliation de plein droit sans préavis et sans indemnité du contrat sous réserve du dénouement des opérations en cours.

13.3. Conséquences de la résiliation

Quelque soit le cas de résiliation du contrat, l'Accepteur sera tenu de restituer, sans délai, à la Banque Acquéreur les Equipements, dispositifs de sécurité et documents en sa possession dont la Banque Acquéreur est propriétaire. Dans ce cas, l'Accepteur s'engage à retirer immédiatement de son établissement tout signe d'acceptation des Cartes CUP.
Dans le cas où, après résiliation du Contrat pour cessation d'activité de l'Accepteur, cession ou mutation du fonds de commerce, s'il se révélait des impayés au titre de la période antérieure à la cession ou à la mutation, ceux-ci seront à la charge de l'Accepteur ou pourront faire l'objet d'une déclaration de créances.

ARTICLE 14 : Non Renonciation

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

ARTICLE 15 : Loi applicable et tribunaux compétents

Les présentes et toutes les questions qui s'y rapportent seront régis par le droit français.
En cas de litige, y compris les procédures tendant à obtenir des mesures d'urgence ou conservatoires, en référé ou sur requête, la compétence est attribuée expressément aux Tribunaux du ressort de la Cour d'Appel de Paris.

ANNEXE

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 d'acceptation.

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

Tout dispositif (équipement réseau, serveur, …) qui stocke ou qui traite des données relatives à une transaction et notamment, des données du porteur doit être hébergé dans un local sécurisé et répondre aux exigences édictées par les règles et 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 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 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 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 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.