ANNEXE I - CONDITIONS GENERALES DU SERVICE DE BANQUE EN LIGNE

A. UTILISATION DU SERVICE

L'accès au service en ligne Banque Misr s'effectue à partir d'un terminal éligible (ordinateur, mobile ou tablette) connecté au réseau Internet.
L'acquisition ou la location du terminal, son installation et sa maintenance ainsi que les frais d'accès et d'utilisation du réseau ne sont pas à la charge de la banque. Le client déclare être informé que la sécurité du fonctionnement du réseau de télécommunication ne peut être garantie par la banque.
La banque ne peut être tenue pour responsable des conséquences qui résultent d'une erreur de manipulation de la part du client ou d'une anomalie de transmission, ainsi que de l'impossibilité d'accès au service résultant notamment d'un incident technique. La banque s'engage par ailleurs à mettre en œuvre, dans ses systèmes, des moyens techniques et d'organisations appropriés tenant compte de l'état actuel de la technologie pour le fonctionnement du service et la sécurité des opérations. Pour des raisons de sécurité, la banque peut être amené à suspendre l'accès au service.

B. ACCES AU SERVICE ET REGLES DE PREUVE

1. Objet
Les règles d'accès et de preuve du Service ont pour objet de préciser et définir les moyens mis à disposition du client pour effectuer un certain nombre d'opérations via les services de banque en ligne par Internet de la banque. Dans ce cadre et afin de permettre l'utilisation de ses services en ligne, la banque délivre des Authentifiants au client, dans les termes et conditions définies aux présentes.
Ces Authentifiants ont pour objectif de permettre au client de réaliser les opérations telles que décrites ci-dessous dans les termes et conditions définis dans la présente convention :
- accéder au service, notamment pour consulter ses comptes,
- signer des transactions bancaires,
- signer des documents contractuels ou précontractuels (conventions, formulaires,…).

Cette convention relève des conditions générales propres à chaque convention de compte, contrats de produit ou service concernés.

2. Définitions
Les termes mentionnés dans la présente convention comportant une majuscule ou édités en caractères italiques sont définis comme ci-après :
Identification du client : procédure consistant à reconnaître le client dans les systèmes informatiques de la banque à partir d'un identifiant.
Identifiant : élément communiqué au client par la banque lui permettant de reconnaître le client de manière certaine.
Authentification du client : procédure consistant à vérifier par des moyens appropriés, ci-après définis comme des Authentifiants, l'identité déclarée par le client. L'authentification permet d'apporter la preuve de l'identité déclarée par le client lors de l'identification.
Authentifiants : éléments propres au client prenant la forme notamment d'un code personnel d'accès, permettant aux systèmes informatiques de la banque de réaliser l'authentification en ligne dudit client. Cette liste n'est pas exhaustive.
Les Authentifiants peuvent être amenés à évoluer dans le temps en fonction de l'état de l'art et de la technique, considérant que le client sera informé par tout moyen de toute évolution dans un délai de deux (2) mois à compter desdites modifications.
Cachet électronique : forme de signature électronique réalisée automatiquement par un serveur et non une personne physique. Cette forme de signature électronique réalisée au nom d'une entité est comparable à un tampon électronique et permet de garantir la provenance d'un document et d'en sceller électroniquement le contenu.
Code personnel d'accès : code à caractère confidentiel et personnel transmis sous pli sécurisé à une adresse postale du client telle que communiquée par le client à la banque.
Code à usage unique : code à usage unique communiqué par téléphone, non réutilisable à caractère confidentiel et personnel transmis sur un numéro de téléphone communiqué par le client à la banque.
Certificat du client : pièce d'identité électronique dont le contenu est garanti par la banque en tant qu'Autorité de certification. Il permet dans les transactions électroniques d'attester de la correspondance avec l'identité de son titulaire. Il contient donc des informations qui permettent cette identification (nom, prénom, etc.).
Autorité de certification : L'Autorité de certification est une entité qui a en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie et s'appuie pour cela sur une infrastructure technique : une infrastructure de gestion de clés (IGC).
Une Infrastructure de Gestion des Clés (IGC) : est un ensemble de composants et de procédures visant à gérer le cycle de vie des certificats électroniques.

3. Procédure de Délivrance des Authentifiants

3.1. Procédure de Délivrance des différents Authentifiants mis à disposition des Clients
Les Authentifiants délivrés par la banque prennent la forme d'un Code personnel d'accès, et/ou d'un Code à usage unique délivré par téléphone. Ils sont délivrés dans les conditions décrites ci-après :

3.1.1 Délivrance du Code personnel d'accès
Ce code peut être demandé par le client auprès de son conseiller, par téléphone ou par Internet. Il est transmis sous pli sécurisé à une adresse postale du client, telle que communiquée par le client à la banque.

3.1.2 Délivrance d'un Code à usage unique par téléphone
Ce code est demandé au client sur Internet au moment où il a besoin de signer en ligne une demande d'enregistrement d'un compte de tiers dans la liste des destinataires de virements

3.2. Obligations des parties dans le cadre de la délivrance des Authentifiants

3.2.1 Obligations à la charge des clients

Le client s'engage à respecter l'ensemble des règles de sécurité ci-après décrites, à savoir :
- changer son code personnel d'accès lors de la première authentification par code et le changer régulièrement,
- fournir à la banque un numéro de téléphone valide et personnel,
- bloquer ou demander à la banque de bloquer immédiatement (1) l'accès au service en ligne s'il suspecte que son code est connu d'un tiers.
- respecter et mettre en œuvre les conseils de sécurité concernant ses moyens d'authentification communiqués sur le site Sécurité la banque, notamment en mémorisant le code sans l'écrire, en ne le transmettant à personne.
- mettre en œuvre tous les moyens à sa disposition pour s'assurer que son ordinateur est raisonnablement sécurisé

La responsabilité de la banque ne peut être engagée en cas de piratage et/ou utilisation frauduleuse des Authentifiants du client du fait d'une erreur de manipulation de la part du client, de la négligence de celui-ci, ou d'un virus affectant l'ordinateur utilisé. Le client est donc seul responsable du

Date :…….. Signature :……..

matériel informatique qu'il utilise, ainsi que de l'usage et de la conservation de ses Authentifiants qui lui sont personnels et dont il s'interdit de les transmettre à quiconque.
(1) L'accès au Service peut être directement bloqué par le client, notamment en accédant au Service, puis en utilisant la fonction spécifique prévue à cet effet.

3.2.2 Obligations à la charge de la banque
La banque s'engage à :
- s'assurer de l'identité du client demandant l'émission ou la réémission d'un code et selon certaines situations selon nos conditions et le tarif en vigueur.
- s'assurer que les numéros de téléphone utilisés dans le cadre de l'envoi de code à usage unique délivré par téléphone sont bien des numéros qui ont été communiqués par le client,
- permettre, à tout moment, en ligne, le changement du code ou le blocage d'accès au service par le client,
- permettre, pendant les horaires ouvrés, en agence ou par téléphone, de faire bloquer l'accès au service en ligne du client,
- mettre en œuvre des moyens techniques, en termes de sécurité et de disponibilité des systèmes.

4. Utilisation des Authentifiants
Les clients peuvent utiliser les Authentifiants qui leur sont remis dans les termes et conditions ci-après définies pour :
- accéder aux services de banque en ligne de la banque, (article 4.1 des présentes) ;
- signer des transactions dites sensibles (article 4.2 des présentes) ;
- signer des documents précontractuels ou contractuels présentés par la banque dans le cadre des relations liant le client à la banque et signer des documents précontractuels et/ou contractuels présentés par la banque ;
- accepter/valider des formulaires, des instructions, ou des termes et conditions se rapportant au Service.

4.1 Accès aux services de banque en ligne
L'authentification lors de l'accès au service peut se faire, suivant la disponibilité des services proposés par la banque, par la saisie par le Client de son Code personnel d'accès ou par des questions dont les réponses sont de nature à prouver l'identité du client.

4.1.1. Accès au Service par Code personnel d'accès
Pour accéder à son espace personnel, quel que soit le Moyen de communication, le client s'authentifie par l'utilisation des données de sécurité personnalisées composées d'un identifiant et d'un code personnel d'accès. Afin d'assurer la confidentialité de l'accès au Service, l'identification du client en conditionne l'accès. L'identifiant et le code d'accès personnel sont personnels et confidentiels. Le client s'engage donc à en interdire l'utilisation à toute autre personne.
Il est obligatoire que le client modifie son code personnel d'accès lors de la première connexion, puis recommandé qu'il le change ensuite régulièrement. Il peut à tout moment modifier son code personnel d'accès. En cas de perte de son code, le client peut, à tout moment, demander l'attribution d'un nouveau code. S'il pense que son code est volé et connu d'un tiers, il doit immédiatement bloquer son accès et par tous moyens informer la banque qui bloquera l'accès au service.
Le client est entièrement responsable de l'usage et de la conservation de son code personnel d'accès, ainsi que des conséquences d'une divulgation à quiconque. La responsabilité de la banque ne peut être engagée quant aux conséquences qui résulteraient d'un usage frauduleux ou abusif du code dans le cas où le client, du fait d'une négligence grave, n'aurait pas satisfait à ses obligations de protection de la confidentialité des données nécessaires à son authentification.
Aux fins de confirmation de certaines opérations sensibles (virements, ajouts de RIB, souscription par exemple), la banque peut être amené à faire parvenir par téléphone (SMS ou message vocal) au client, un Code à usage unique destiné à valider l'opération en cours. La procédure à suivre permet d'authentifier le client à l'origine de l'opération. Le client doit ainsi récupérer ce Code à usage unique en consultant son téléphone, puis le saisir immédiatement sur le site de banque en ligne Banque Misr. En l'absence de saisie de ce code, l'opération n'est pas validée. Le client doit prendre toutes les mesures propres à assurer la confidentialité du moyen d'authentification qui sera utilisé pour réaliser l'opération et ne pas le communiquer à qui que ce soit. Si le client n'a pas déclaré de numéro de téléphone valide auprès de la banque l'opération sensible ne pourra pas être validée par le client et ne pourra par conséquent pas être exécutée.
Pour valider certaines opérations, il peut être demandé au client de renseigner son code personnel d'accès.
De même, dans le cadre de son obligation de vigilance et en vue de protéger le client contre toute opération frauduleuse, la banque se réserve le droit de suspendre certaines opérations transmises par le biais du Service afin de procéder aux vérifications complémentaires d'usage.
Par mesure de sécurité afin de protéger au mieux les avoirs du client, l'accès au Service est également interrompu après plusieurs essais infructueux d'identification du client, ou bien à l'initiative de la banque en cas de suspicion ou détection de transactions frauduleuses. En outre, les communications avec la banque sont chiffrées. En cas de blocage d'accès au Service, le client doit s'adresser à son agence qui lui communiquera la procédure à suivre pour que la banque débloque son accès.
L'accès au site internet Banque Misr se fait de manière sécurisée afin de garantir un niveau optimal de confidentialité et de protection pour les transactions bancaires. Les systèmes de protection de la banque ne peuvent fonctionner de manière optimale que si le client, de son côté, se protège également contre les risques informatiques.

4.1.2. Administration de la preuve sur l'accès aux services
La banque et le client conviennent de façon expresse que l'utilisation par le client d'un des Authentifiants, tel que décrits à l'article 4.1.1 des présentes, fait preuve de la connexion du client aux services de banque en ligne de la banque ainsi qu'à l'ensemble des autres services proposés par la banque ou pour le compte d'autres entités du groupe.
Il est expressément convenu que toute interrogation ou opération intéressant le ou les comptes du client réalisées conformément à la procédure décrite dans la clause « accès au service » est réputée effectuée, qu'elle qu'en soit l'origine, par le client lui-même.
Il est expressément convenu que les enregistrements des échanges téléphoniques et les enregistrements informatiques ou leur reproduction sur un quelconque support feront foi entre les parties, sauf pour chacune d'elles à apporter la preuve contraire.
Les enregistrements des échanges téléphoniques et les enregistrements informatiques seront conservés dans des conditions de sécurité appropriées.

4.2. Signature électronique / validation électronique de transactions sensibles et convention de preuve

4.2.1. Convention de preuve et description
Après avoir accédé aux services de banque en ligne, le client a la possibilité d'effectuer un certain nombre d'opérations bancaires
Par son acceptation des conditions générales du Service, le client :
- Reconnaît que la saisie de son Identifiant et de son Code personnel d'accès, assorti le cas échéant du Code à usage unique envoyé sur son téléphone, participera de la signature électronique ou de la validation électronique du client, en permettant son identification et en prouvant son consentement aux

opérations effectuées (notamment virement, souscription, prélèvement) et l'imputation de ces dernières au client ou à son mandant ;
- Reconnaît et accepte que la signature électronique (la « Signature Electronique »), ou la validation électronique (la « Validation Electronique ») générée lors du clic par le client sur le bouton « je signe » ou « j'accepte » (précédé ou non de la saisie d'un Code à usage unique) sur l'interface numérique utilisée pour accéder au Service :
    - l'identifiera en tant que signataire ou acceptant des opérations réalisées sur Banque Misr
    - et vaudra expression de son consentement auxdites opérations formalisées par les documents électroniques mis à sa disposition ;
- Reconnaît que les opérations revêtues de sa Signature Electronique ou de sa Validation Electronique lui seront imputables et opposables, et auront force probante, jusqu'à ce que le client en apporte la preuve contraire par tout moyen ;
- Accepte expressément la mise à disposition, sous la forme électronique, des documents revêtus de sa Signature Electronique ou de sa Validation Electronique ;
- Reconnaît être informé que les documents électroniques revêtus de sa Signature Electronique ou de sa Validation Electronique :
    - seront archivés électroniquement par la banque et seront conservés dans des conditions de sécurité et d'intégrité appropriées ;
    - seront mis à sa disposition dans son espace client sur le Service ;

- Reconnaît que l'intégralité des stipulations ci-dessus vaudra convention sur la preuve pour les besoins des opérations réalisées sur l'interface numérique utilisée pour se connecter au Service ;
- Reconnaît qu'en cas d'annulation ou d'abandon au cours de la procédure de Signature Electronique ou de Validation Electronique, l'opération ne sera pas valablement conclue.

Certificat électronique et autres formes de signature électronique :
Confirmation d'opération par Code à usage unique délivré par téléphone :
Le client demande sur la page de confirmation reprenant le récapitulatif de l'opération demandée l'envoi d'un code vers un des numéros de téléphones qu'il a communiqué à la banque. Le récapitulatif de l'opération demandée ainsi que le Code à usage unique sont envoyés sur le téléphone. Le client peut alors saisir le Code à usage unique sur son service de banque en ligne pour valider son opération. Les systèmes informatiques de la banque vérifient le code saisi et prennent en compte ou non l'opération en fonction de cette vérification. En cas d'essais infructueux, au bout de plusieurs tentatives, l'opération est annulée.

4.2.2 Obligations
Le client s'engage, concernant la signature de transactions sensibles, à :
- s'assurer qu'il ne signe une telle transaction sensible qu'après avoir accédé au service dans les conditions décrites à l'article 4.1 des présentes,
- vérifier la bonne prise en compte de l'opération par le système, notamment en consultant les historiques et ses relevés de compte.

En cas de contestation d'opération, le client est tenu de signaler avec diligence toute anomalie à son conseiller.
La banque s'engage à mettre en œuvre les moyens de l'état de l'art permettant d'effectuer les opérations de vérification décrites et refuser de réaliser une opération qui n'aurait pas été validée correctement.

4.2.3. Administration de la preuve sur la signature/validation de transactions
Il est convenu de façon expresse entre la banque et le Client que la validation des transactions dans les conditions décrites dans la clause 4.2 des présentes au moyen des Authentifiants décrits ci-dessus vaut Signature Electronique ou Validation Electronique du client, l'utilisation de l'un des Authentifiants dans les termes et conditions décrits à l'article 4.2.1 des présentes permettant ainsi son authentification, prouvant son consentement aux transactions ainsi effectuées et l'imputation de ces dernières au client ou à son mandant.
Pour les opérations le nécessitant, le client convient également que l'utilisation d'un Code à usage unique, transmis sur un téléphone du client fait également preuve.
Les enregistrements par les appareils de la banque qui sont utilisés pour la réception des instructions ou leur reproduction sur un support informatique ou papier constituent également pour la banque et le client la preuve desdites instructions et la justification de leur imputation au compte du client.
Les informations communiquées par le Service en ligne Banque Misr s'entendent sauf erreur ou omission et sous réserve des opérations en cours. Les écritures auxquelles le client a accès peuvent avoir un caractère provisoire.
Les relevés d'écritures (établis sur) papiers (par la banque) ou sous format PDF mis en ligne par la banque sur le site Banque Misr de gestion de compte en ligne du client, et le cas échéant, les confirmations écrites d'opérations, continueront à faire foi entre les parties dans les conditions habituelles.

4.3. Signature de documents contractuels ou précontractuels

4.3.1. Description
Dans le cadre du Service Internet Banque Misr, il est donné au client la possibilité, après avoir accédé à ce service dans les conditions prévues à l'article 4.1 des présentes, de souscrire à des produits ou services proposés par la banque donnant lieu à signature de documents contractuels dans les conditions prévues à l'article 4.2 des présentes, le client pouvant par ailleurs être amené à accéder à des services nécessitant la signature de documents précontractuels tels que des questionnaires, des fiches conseil ou des formulaires.
Dans les cas de figure précités, les systèmes informatiques de la banque préparent un document à signer (suivant le cas une proposition commerciale, un document contractuel ou bien un formulaire à signer) sur lequel pourra, le cas échéant, être apposé un cachet électronique de la banque. Les systèmes informatiques présentent le document au client. Ce dernier peut alors en prendre connaissance, le compléter si cela est demandé et le cas échéant y consentir en apposant sa signature.
L'acte à signer est présenté sous la forme d'un document électronique, au sein d'une application de signature électronique qui prend en charge techniquement l'opération de présentation du document à signer, puis de signature électronique sur l'ordinateur du client. Le client prend connaissance du document présenté, puis s'il décide de le signer, coche une case pour confirmer son consentement et clique sur le bouton « signer ».
Cette signature peut se faire, dans les conditions prévues à l'article 4.2 des présentes et suivant la disponibilité des services proposés par la banque :
- soit par l'utilisation de son Certificat la banque Certification Client après avoir accédé aux services de banque en ligne dans les conditions prévues à l'article 4.1 des présentes, sans réauthentification supplémentaire,
- soit par l'utilisation de son Certificat la banque Client après avoir accédé aux services de banque en ligne dans les conditions prévues à l'article 4.1 des présentes, complété d'une réauthentification obligatoire à l'aide d'un Code à usage unique délivré par téléphone.

Dans le cas de l'utilisation du certificat la banque Certification Client avec réauthentification, le client doit alors saisir sur l'application de signature électronique le

code à usage unique reçu par téléphone pour réaliser la signature.
Dans le cas de l'utilisation du certificat la banque Client sans réauthentification, le simple fait de cliquer sur le bouton « signer » suffit à réaliser la signature.
Le document est alors signé électroniquement au format PDF puis renvoyé aux systèmes informatiques de la banque.
Les systèmes informatiques de la banque vérifient alors notamment :

- que le document signé n'a pas été modifié depuis sa signature électronique,
- que le certificat du client est valide au moment de la réception du document signé par la banque. Cette vérification est faite par la banque sur le certificat présenté, en contrôlant ses dates de validité et en vérifiant son absence sur la liste des certificats révoqués,
- que le document signé par le client est bien celui qui lui a été présenté, sans modification, ajout ou suppression autre que l'apposition de sa signature.

Si ces conditions sont toutes vérifiées, un exemplaire du document est mis à disposition du client sous forme de document PDF comportant le cachet électronique la banque ainsi que la signature électronique du client. Il peut le stocker sur son ordinateur, et également en réaliser une copie papier. Le client peut également, sous réserve des délais légaux de conservation, accéder à tout moment au document électronique en adressant sa demande à son conseiller Banque Misr.
Si les conditions ne sont pas toutes vérifiées, l'acte est détruit et est considéré comme nul et non avenu.
Le document signé par le client, ainsi que les résultats de cette vérification et les éléments ayant permis d'en réaliser la vérification sont consignés dans des enregistrements techniques horodatés. Ces enregistrements sont techniquement scellés par le système informatique de la banque en charge de la validation de la signature.
La signature électronique du client prend la forme d'un procédé répondant aux conditions définies à la première phrase du second alinéa de l'article 1367 du code civil. Il est convenu entre la banque et le client que la fiabilité de ce procédé est présumée jusqu'à preuve contraire.

4.3.2. Obligations
Le client s'engage à, concernant la signature d'actes :

- S'assurer qu'il ne signe un acte qu'après avoir accédé convenablement au service,
- En cas de contestation, le client est tenu de signaler toute anomalie à son agence avec diligence.

La banque s'engage à :

- Mettre en œuvre les moyens de l'état de l'art permettant d'effectuer les opérations de vérification décrites et refuser de prendre en compte un acte dont la signature électronique n'aurait pas été validée correctement,
- Conserver les éléments de preuve comprenant l'acte signé par le client conformément à la réglementation sur la conservation des actes signés électroniquement pour le compte des clients.

4.3.3. Preuves et enregistrements des ordres passés
Conformément à l'article 4.2 des présentes, il est rappelé que la saisie par le client de son Identifiant et de son Code personnel d'accès, assorti le cas échéant du Code à usage unique envoyé sur son téléphone, participera de la Signature Electronique ou de la Validation Electronique du client, en permettant son identification et en prouvant son consentement aux opérations effectuées (notamment virement, souscription, prélèvement…) et l'imputation de ces dernières au client ou à son mandant.
L'utilisation par le client de son Identifiant et de son du Code personnel d'accès participent chacun de la preuve des ordres transmis par lui sur le Service.

Pour les opérations le nécessitant, le client convient également que l'utilisation d'un Code à usage unique, transmis sur un téléphone du client fait également preuve.
L'utilisation de certificats électroniques par le client emporte les mêmes obligations juridiques à son égard que l'utilisation de l'identifiant associé à son code d'accès personnel pour l'identification ou pour le consentement aux opérations effectuées. La signature d'un document contractuel au moyen d'une signature électronique manifeste le consentement du client aux droits et obligations découlant du contenu dudit document, au même titre qu'une signature manuscrite.
Les enregistrements par les appareils de la banque qui sont utilisés pour la réception des instructions ou leur reproduction sur un support informatique ou papier constituent également pour la banque et le client :

- la preuve desdites instructions et la justification de leur imputation au compte / au crédit du client,
- la preuve de la conclusion et du contenu et modalités des conventions relatives aux produits ou services souscrits en ligne par le biais de Banque Misr.

la banque ne conserve ces enregistrements que pendant un an.
Les reproductions des conventions seront conservées par la banque pendant les durées d'archivage requises par les règles des prescriptions légales et conventionnelles. Les informations communiquées par le Service Banque Misr s'entendent sauf erreur ou omission et sous réserve des opérations en cours. Les écritures auxquelles le client a accès peuvent avoir un caractère provisoire, et, le cas échéant, les confirmations écrites d'opération, continueront à faire foi entre les parties dans les conditions habituelles, telles que déterminées dans les Dispositions Générales de Banque.

C. CONDITIONS DE FONCTIONNEMENT DU SERVICE

1. Conditions générales de fonctionnement
L'ensemble des opérations effectuées dans le cadre du service en ligne Banque Misr est accessible aux conditions réglementaires ou convenues par ailleurs, d'ouverture et de fonctionnement des comptes et sous réserve de provision en compte.
Certaines opérations sont limitées en montant pour des raisons de sécurité. Sont exclues du service les opérations de débit entraînant, en application de la réglementation, la clôture automatique des comptes sur lesquels elles portent.
La banque se réserve à tout moment le droit de demander confirmation sur support papier de tout ordre donné à distance.

2. Consultation des comptes, encours cartes
Le client est autorisé à consulter la situation et les opérations de ses comptes personnels dont il est titulaire ou cotitulaire. Il est également autorisé à consulter l'encours des cartes rattachées à ces comptes.
Les informations sont fournies à la date précisée sur l'écran et sous réserve des opérations en cours de traitement. Ces informations s'entendent sauf erreur ou omission. Le client est tenu de contrôler les relevés pour la souscription du service "relevés et documents en ligne".
Les relevés de comptes périodiques adressés par la banque sous format papier ou sous format électronique PDF, dans le cadre de la souscription au service Relevés et documents en ligne continueront à faire foi entre les parties dans les conditions habituelles, telles que déterminées dans les Dispositions Générales de Banque Clientèle des Particuliers.

3. Virements
Le client a la possibilité de saisir des ordres de virement de compte à compte dont il est titulaire ou cotitulaire et également de ceux pour lesquels il détient une procuration.
Le client a également la possibilité de saisir des ordres de virement en euros vers des comptes de tiers dans la zone

SEPA ou à l'étranger (hors zone SEPA) vers certains pays respectant les normes internationales BIC/IBAN le cas échéant, que le client en soit ou non le titulaire. Pour les virements France et Monaco, il doit enregistrer au préalable les identifiants desdits comptes sur le site.
Tout ordre ne pourra être exécuté que si le compte à débiter présente une situation régulière, une provision disponible et suffisante et pour les virements vers des comptes de tiers, s'il respecte le plafond de virement et la liste des pays vers lesquels les virements sont autorisés par le client.
La liste standard de pays vers lesquels les virements sont autorisés est composée de la France (zone SEPA) et de l'Egypte.
La date de réception de l'ordre de virement est la date à laquelle l'ordre est réputé valablement reçu par la banque.
La banque pourra, le cas échéant, exiger que l'ordre de virement soit donné sous la forme d'un ordre papier manuscrit. Dans le cas où un ordre de virement ne serait pas exécuté, la banque informe le client du refus d'exécuter ainsi que de son motif.
La banque se réserve le droit, pour des raisons de sécurité, de valider le virement en envoyant un code à usage unique par téléphone suivant le procédé décrit à l'article 4.2.1 des présentes conditions. Si le client n'a pas déclaré de téléphone valide auprès de la banque, le virement ne pourra pas être validé par le client.

4. Commande de chéquier - édition RIB
Sur les comptes consultables via le Service Banque Misr, le client a la possibilité d'effectuer des commandes de chéquiers sur ses comptes de dépôt et d'éditer des RIB/IBAN sur ses comptes de dépôt.

5. Comptes de tiers, procuration
Le client pourra consulter et/ou effectuer des transactions sur des comptes de tiers si le client possède une procuration ou un pouvoir de représentation adéquats l'autorisant à consulter et/ou effectuer des transactions sur le ou les comptes concernés. Il est précisé que le client n'aura plus accès auxdits comptes en cas de révocation de son mandat, de perte de la qualité de représentant légal et en cas de décès ou de mise sous un régime de protection du mandant.
Il est par ailleurs précisé que le client agissant en qualité de représentant légal d'un mineur ou d'un incapable majeur doit se conformer aux dispositions légales et/ou décisions judiciaires définissant le régime de protection desdits incapables.

6. Consultation des crédits – réalisation d'opérations en ligne
Le client est autorisé à consulter la situation (principales informations) des prêts et/ou crédits en cours dont il est emprunteur ou co-emprunteur.
Dans le cadre de son obligation de vigilance et en vue de protéger le client contre toute opération frauduleuse, la banque se réserve le droit de suspendre l'exécution de toute utilisation effectuée par le biais des Services en Ligne de la banque afin de procéder aux vérifications complémentaires d'usage.
Dans le cas où une utilisation ne serait pas exécutée, la banque informe du refus d'exécuter ainsi que de son motif par l'affichage d'un message d'information à l'écran.
Les informations sont fournies à la date précisée sur l'écran et sous réserve des opérations en cours de traitement. Ces informations, purement indicatives, s'entendent sauf erreur ou omission. Le contrat de prêt ou de crédit ainsi que le cas échéant, le tableau d'amortissement en vigueur, continueront à faire foi entre les parties.
Enfin, le client peut réaliser des simulations de crédits à la consommation et/ou effectuer des demandes de crédit en ligne ; ainsi que suivre ses demandes.

7. Consultation des contrats signés électroniquement
Le client pourra lorsque le service sera proposé visualiser et télécharger ses contrats et avenants signés dans la rubrique prévue à cet effet.

8. Personnalisation des noms de compte
La banque offre la possibilité à son client de personnaliser le nom de ses comptes et de créer des groupes de comptes. Les intitulés alors choisis par le client ne doivent pas être contraire à la loi française, porter atteinte à l'ordre public, aux bonnes mœurs ou encore aux droits d'un tiers. Le client est seul responsable des intitulés choisis.
Il peut à tout moment revenir à l'intitulé standard.
L'éventuelle personnalisation n'apparaîtra pas sur les relevés de comptes adressés par la banque au client établis sur papier ou sous format PDF le cas échéant.

9. Conditions applicables à l'ensemble des opérations effectuées via les Services en Ligne la banque
L'ensemble des opérations couvertes par les services en ligne de la banque est accessible :
- aux conditions réglementaires, ou convenues par ailleurs, d'ouverture et de fonctionnement des comptes et sous réserve de provision en compte.
- aux conditions et dans les limites réglementaires ou contractuelles de fonctionnement des prêts.

Certaines opérations sont limitées en montant pour des raisons de sécurité. Sont exclues du service les opérations de débit entraînant, en application de la réglementation, la clôture automatique des comptes sur lesquels elles portent. la banque se réserve à tout moment le droit de demander confirmation sur support papier de tout ordre donné à distance.
Les opérations couvertes par le service peuvent également être effectuées en agence aux conditions énoncées dans le document « tarifs et conditions » consultable sur le site.

D. CONDITIONS FINANCIERES - TARIFS

Les conditions financières des produits et services proposés par la banque figurent sur le site Banque Misr.
La banque indique au client les modifications qui peuvent intervenir par tout moyen écrit ou sur support durable (via le relevé de compte du client par exemple). L'absence de manifestation écrite d'un désaccord de la part du client avant l'entrée en vigueur du nouveau tarif vaut acceptation de ce dernier. Il en est de même pour les évolutions d'un service ou des Dispositions Générales de Banque en ligne.
Pour les services entrant dans la gestion du compte de dépôts du Client, le délai de préavis est de 2 (deux) mois.
En ce qui concerne les conditions créditrices de rémunération d'un compte à terme (dans le cas prévu par la réglementation), les variations du taux d'intérêt prennent effet à la date annoncée par la banque sans pouvoir donner lieu à un préavis déterminé, compte tenu de leur dépendance à l'évolution des marchés. Les conditions en vigueur sont disponibles sur le site Banque Misr.
Concernant l'accès au site Banque Misr, les frais d'accès et d'utilisation du réseau de télécommunication sont à la charge du client, selon les modalités fixées par ses fournisseurs d'accès et opérateurs de télécommunications.
La banque demeure étrangère à tout litige pouvant intervenir entre le client et ceux-ci.

E. DUREE, MODIFICATION, SUSPENSION ET RESILIATION

1. Durée et conditions de résiliation
La convention de service Banque Misr est conclue pour une durée indéterminée et peut être dénoncée par l'une ou l'autre des parties, à tout moment, moyennant le respect d'un préavis de 60 jours suivant notification écrite.
La clôture du compte support de la convention, désigné dans les Conditions Particulières du Service de banque en ligne Banque Misr, à l'initiative de l'une ou l'autre des

Date :…….. Signature :……..

parties, entraînera toutefois la résiliation de la convention, sans formalité ni délai.

2. Suspension à l'accès au Service Banque Misr en ligne :

La banque peut suspendre l'utilisation du Service Banque Misr en ligne dans un des cas suivants :

- Impossibilité de prélever pour quelque cause que ce soit ;
- Existence d'un incident bancaire affectant un des comptes du client, notamment blocage ;
- Saisie Administrative à Tiers Détenteur, Saisie Attribution ou toute procédure civile d'exécution ;
- Adresse du titulaire inconnue et par extension pour toutes raisons de conformité tenant au non-respect de la réglementation.

Dans le cas où l'adresse du titulaire est inconnue de la banque, à savoir que les courriers adressés par la banque au titulaire ne sont pas distribués par la Poste et reviennent avec la mention « NPAI » (N'habite pas à l'adresse indiquée) ou « PND » (Pli non distribué), la banque se réserve le droit de bloquer les fonctions du service de banque en ligne à l'issue d'un délai de 2 (deux) mois au cours duquel le Client est invité à régulariser sa situation par des messages SMS dédiés envoyés au numéro de téléphone renseigné par le client. Ces blocages resteront activés jusqu'à ce que le Client régularise sa situation auprès de la banque en communiquant et justifiant sa nouvelle adresse.

3. Modifications

Le client peut demander d'apporter des modifications (notamment liste des comptes, liste des pays vers lesquels les virements sont autorisés). Celles-ci seront effectives sous réserve d'acceptation par la banque.

Le service Banque Misr et ses conditions d'utilisation sont susceptibles d'évoluer.

Tout projet d'évolution des présentes conditions générales est communiqué au client sur support papier ou sur un autre support durable au plus tard deux mois avant la date d'application envisagée. L'absence de contestation de la part du client auprès de l'établissement avant la date d'application des modifications vaut acceptation de celles-ci.

Dans le cas où le client refuse les modifications proposées par l'établissement, il doit faire part de son désaccord avant cette date exclusivement par écrit (lettre recommandée ou remise à votre agence contre récépissé).

Le client pourra, avant cette date, résilier sans frais la convention Banque Misr.

Date :…….. Signature :……..