Conditions d'accès et d'utilisation des Services E-Banking (banque en ligne) – Personnes Physiques

Le soussigné (ci-après aussi le « Client ») souhaite avoir un accès via la banque en ligne (ci-après « E-Banking ») sur un ou plusieurs comptes (ci-après « les Comptes Consultables ») auprès de la Banque de Luxembourg (ci-après la « Banque ») sur lesquels il a un pouvoir de signature soit en tant que titulaire soit en tant que représentant ou mandataire.

1. Objet

Les parties conviennent des conditions d'accès et d'utilisation par le Client des services de banque en ligne via le site E-Banking de la Banque et/ou via l'application BL-Mobile Banking (ci-après les « Services E-Banking »), ainsi que des modalités de preuve des échanges et des transactions réalisés. Ces Conditions d'accès et d'utilisation des Services E-Banking ne créent aucune nouvelle obligation d'information ou de conseil, ni aucun nouveau mandat à la charge de la Banque.

Les Services E-Banking de la Banque offrent notamment les fonctionnalités suivantes :

- Présentation de la Banque, de ses produits et services,
- Informations sur les marchés,
- Recherche et analyse financière,
- Consultation des Comptes Consultables,
- Possibilité d'effectuer certaines transactions,
- Communications par voie électronique,
- Consultation et génération de documents,
- Détermination / changement de certaines données personnelles.

Certaines des fonctionnalités mentionnées ci-dessus peuvent être exclusives ou se présenter différemment sur l'espace E-Banking du site internet de la Banque ou dans l'application BL-Mobile Banking

La Banque se réserve le droit de modifier à tout moment ces fonctionnalités.

2. Prix

L'abonnement aux Services E-Banking est facturé selon les tarifs en vigueur auprès de la Banque, que le Client déclare connaître et accepter. Les autres frais tels que l'abonnement Internet (Internet Service Provider), les frais de communication téléphonique ou autres sont à la charge du Client.

3. Sécurité des Services E-Banking

Pour accéder aux Services E-Banking, le Client veillera à disposer d'une connexion au réseau Internet auprès du fournisseur d'accès de son choix. La Banque n'assume aucune responsabilité en relation avec la connexion du Client au réseau Internet, qui se fait aux risques et périls exclusifs du Client.

L'accès aux Services E-Banking s'effectue via l'adresse communiquée au Client avec ses identifiants ou toute autre adresse que la Banque communiquera au Client par tout moyen qu'elle jugera approprié et notamment par voie électronique.

Le Client recevra sous enveloppe de la part de LuxTrust les identifiants correspondant à son choix afin de lui permettre de se connecter aux Services E-Banking, de s'identifier et de signer ses instructions.

Tout support utilisé pour l'authentification lui sera, le cas échéant, remis ou envoyé dans une enveloppe séparée.

Toute transmission des identifiants et, le cas échéant, du support utilisé pour l'authentification se feront aux risques et périls du Client.

Le Client autorise expressément la Banque et LuxTrust à remettre à ses mandataires ou représentants, présents ou futurs, qui ont un pouvoir de signature sur les Comptes Consultables, des identifiants donnant accès aux Services E-Banking, lorsque ces derniers le demandent.

Le Client s'oblige à protéger tous les identifiants et s'engage à prendre toute mesure de sécurité afin de garder le contrôle exclusif sur son mode d'authentification d'accès (identifiant, mot de passe, One Time Password) qu'il est le seul à connaître. Il est de sa responsabilité exclusive de conserver ces codes personnels strictement confidentiels.

La Banque attire plus particulièrement l'attention du Client sur le fait qu'elle ne le sollicitera jamais par courrier électronique pour obtenir des informations confidentielles (son mot de passe, son One Time Password ou son numéro de carte bancaire) ou pour l'inviter à se connecter aux Services E-Banking de la Banque via un lien repris dans l'email.

Le Client peut donc considérer comme suspect tout e-mail non sollicité qui prétendrait provenir de la Banque et qui lui demanderait de communiquer ses coordonnées personnelles et/ou mot de passe. Par ailleurs, la Banque conseille à son Client de saisir lui-même l'adresse www.banquedeluxembourg.com, de vérifier qu'il n'y a pas de faute d'orthographe et de ne pas suivre un lien contenu dans un e-mail.

L'enregistrement par le Client de l'un de ces éléments sur la mémoire d'un ou de plusieurs ordinateurs se fait également à ses risques et périls. Dès l'instant où le Client sait ou soupçonne qu'un tiers puisse accéder aux Services E-Banking grâce à l'un de ces éléments, il en informe immédiatement la Banque afin que celle-ci puisse bloquer un tel accès.

La connexion aux Services E-Banking est protégée par une procédure de chiffrement et d'identification du Client.

Le Client reconnaît avoir reçu de la part de la Banque toutes les précisions utiles sur ce dispositif de sécurité, son efficacité et ses limites. Il l'accepte comme satisfaisant et décharge formellement la Banque de toute responsabilité concernant les conséquences d'une violation du dispositif de sécurité par un tiers non autorisé. Il autorise également la Banque à modifier le fonctionnement pratique et technique des Services E-Banking et, en particulier, le dispositif de sécurité permettant de s'y connecter, notamment pour tenir compte d'une évolution des technologies. Le Client en sera dûment prévenu par les moyens que la Banque jugera adéquats.

Le Client s'engage à respecter strictement les procédures d'accès aux Services E-Banking telles qu'elles lui ont été indiquées par la Banque ainsi que toutes les consignes d'utilisation affichées via les Services E-Banking ou communiquées au Client par tout autre moyen. Il vérifiera à chaque connexion le caractère sécurisé de la communication. En cas de non-respect de cette procédure ou des consignes d'utilisation, comme dans l'hypothèse d'une tentative de connexion aux Services E-Banking au moyen d'un identifiant incorrect, la Banque se réserve le droit de refuser au Client tout nouvel accès aux Services E-Banking.

D'un commun accord entre les parties, tout accès aux Services E-Banking effectué à l'aide de l'un des identifiants du Client est réputé l'être par le Client, le journal des connexions tenu par la Banque faisant foi de celles-ci.

De la même manière, tout accès aux Services E-Banking par un mandataire ou un représentant du Client effectué à l'aide de l'un des identifiants de ce mandataire ou représentant est

réputé être effectué par ce mandataire ou représentant au nom et pour le compte du Client.

La Banque n'encourt aucune responsabilité et ne saurait en particulier se voir reprocher une violation de son obligation au secret au cas où un tiers aurait pu accéder aux Comptes Consultables du Client ou obtenir, grâce au site E-Banking et/ou à l'application BL-Mobile Banking de la Banque ou au réseau Internet, des renseignements sur sa relation avec la Banque.

4. Informations accessibles via les Services E-Banking

Le Client peut consulter via les Services E-Banking diverses informations d'ordre financier ou économique, émanant de la Banque aussi bien que de tiers et portant notamment sur les marchés financiers et les fonds d'investissement.

La Banque indiquera, dans la mesure du possible, la date de parution ou de création des informations publiées via les Services E-Banking et tiendra ces informations à jour aussi rapidement que celles distribuées sur support papier.

L'ensemble des informations publiées via les Services E-Banking l'est à titre purement indicatif et ne saurait être assimilé à un quelconque conseil de la part de la Banque. Le Client s'oblige à utiliser ces informations avec discernement et esprit critique.

Il décharge expressément la Banque de toute responsabilité quant au contenu, à la fiabilité, à l'actualité, à l'intégrité ou à l'exactitude des informations provenant de tiers et signalées comme telles.

Le Client renonce expressément à tout conseil en ligne de la part de la Banque à propos des informations publiées via les Services E-Banking et s'engage à recueillir tout conseil relatif à ses investissements et à la gestion de son portefeuille directement auprès du conseiller de son choix.

Le Client s'engage à respecter la propriété des informations accessibles via les Services E-Banking et s'interdit de les communiquer à des tiers, de les publier ou de les diffuser par quelque moyen et à quelque titre que ce soit ainsi que de reproduire tout ou partie des Services E-Banking. Sauf opposition écrite, il autorise la Banque à lui adresser toute communication y compris de nature commerciale par le biais des Services E-Banking ou par courrier électronique.

5. Consultation des Comptes Consultables

Le Client peut consulter via les Services E-Banking la situation des Comptes Consultables et, le cas échéant, les opérations d'achat et de vente en cours d'exécution sur ces mêmes comptes. Il autorise la Banque à lui communiquer par le réseau Internet toute information sur les Comptes Consultables et les opérations faites sur ces comptes et ce nonobstant un éventuel accord avec la Banque aux termes duquel la correspondance qui lui est destinée doit être tenue à sa disposition dans les locaux de la Banque.

Le Client qui a opté pour une consultation des Comptes Consultables dont il est titulaire ou représentant exclusivement via les Services E-Banking, s'engage à les consulter au moins une fois par trimestre. A défaut, la Banque lui fera parvenir à ses frais un relevé de la situation des Comptes Consultables.

A défaut de consultation des Comptes Consultables pendant une période continue de six mois, la Banque désactivera l'accès aux Services E-Banking et lui fera suivre à ses frais les extraits de compte, les relevés de la situation et la correspondance relative aux Comptes Consultables à l'adresse définie dans la demande d'ouverture de compte ou communiquée ultérieurement par le Client.

La Banque se réserve le droit de refuser l'accès aux Services E-Banking au Client sur un ou plusieurs Comptes Consultables si elle estime de manière discrétionnaire avoir une raison valable de le faire.

6. Ordres électroniques du Client

Le site E-Banking permet au Client de transmettre à la Banque des ordres de virement ainsi que des ordres d'achat ou de vente d'instruments financiers (ci-après « les Ordres Electroniques ») qui seront exécutés dans les mêmes conditions que ses autres ordres.

Les Ordres Electroniques sont présumés être donnés en exécution et/ou en réception et transmission d'ordres en exécution simple visés à l'article 12 des Conditions Générales de la Banque.

Pour chaque Ordre Electronique adressé à la Banque, le Client s'engage à donner les précisions nécessaires à la bonne exécution de l'ordre.

La Banque affichera à l'écran le détail des informations saisies par le Client.

Le Client répond de tous les ordres transmis grâce à ses identifiants jusqu'à ce qu'il ait prévenu la Banque de ne plus s'y fier et que celle-ci ait été en mesure de rejeter de tels ordres.

Les parties reconnaissent aux Ordres Electroniques transmis la valeur probante d'un acte sous seing privé conformément aux articles 1322 et suivants du code civil et leur opposabilité en tant que tels au Client et à la Banque quel qu'en soit le montant.

La Banque s'engage à conserver sur un support durable, pendant une durée de 10 ans, un exemplaire de tous les Ordres Electroniques transmis du Client, en prenant toutes les mesures de sécurité garantissant l'inaltérabilité de ces enregistrements. Le Client accepte expressément que les enregistrements par la Banque de ses Ordres Electroniques transmis fassent foi de leur existence, de leur contenu et de leur date et heure précises et puissent être produits à cette fin en justice. La Banque tient à la disposition du Client une copie de tous ces enregistrements.

7. Traitement et protection des données personnelles

L'accès aux Services E-Banking implique le traitement par la Banque des données à caractère personnel du Client, à des fins d'exécution du présent contrat et de gestion globale de la relation client et des services liés.

Les informations recueillies à l'aide du présent document peuvent ainsi être mises sur tout support et sont enregistrées par la Banque dans un fichier informatisé et traitées aux fins d'identification et de gestion des accès aux Services E-Banking, de la gestion des comptes et des opérations, ainsi que du contrôle de leur régularité.

Afin de répondre à ses obligations réglementaires, notamment au regard de la législation en matière de lutte contre le blanchiment d'argent et contre le financement du terrorisme, la Banque peut être amenée à vérifier l'authenticité des données fournies par le Client et à transférer ces données aux autorités publiques et aux juridictions compétentes.

La Banque pourra conserver les données personnelles pour une durée n'excédant pas celle nécessaire au regard des

finalités poursuivies par la Banque et suivant les modalités reprises dans les Conditions Générales de la Banque.

En vue de l'exécution du présent contrat et de la fourniture des Services E-Banking, la Banque transfère les données personnelles recueillies dans le présent document à la société LuxTrust qui procédera également dans ce contexte au traitement des données. Le Client bénéficie du droit de demander l'accès, la rectification, l'effacement et la portabilité de ses données à caractère personnel, celui de s'opposer à leur traitement ou encore d'en demander une limitation.

Le Client peut consulter et/ou modifier certaines données personnelles via les Services E-Banking. Le Client demande à ce que tout changement ainsi notifié à la Banque soit pris en compte par elle dans les mêmes conditions que toute autre notification de changement.

Le Client s'engage à fournir des données correctes et exactes à la Banque, à informer la Banque dans les meilleurs délais de tout changement de ces données et à communiquer à la Banque sur simple demande tout document ou renseignement complémentaire que celle-ci jugerait utile dans le cadre du maintien des relations bancaires ou qui serait requis par des dispositions légales ou réglementaires.

8. Accessibilité des Services E-Banking

La Banque se réserve le droit de suspendre temporairement l'accès aux Services E-Banking, notamment pour des raisons d'ordre technique.

Lorsque la Banque est en mesure de prévoir l'inaccessibilité temporaire aux Services E-Banking, elle fera de son mieux pour en informer préalablement le Client par tous moyens appropriés, y compris par un message transmis par les Services E-Banking.

Le Client décharge la Banque de toutes les conséquences pouvant résulter d'une inaccessibilité temporaire des Services E-Banking, pour quelque cause que ce soit, ainsi que de toutes les conséquences pouvant résulter d'une panne ou d'un dysfonctionnement des Services E-Banking, de l'infrastructure informatique de la Banque, d'une déconnexion aux Services E-Banking ou de tout autre incident technique même imputable à la Banque.

La Banque se réserve le droit de bloquer ou de retirer définitivement l'accès aux Services E-Banking du Client, si celui-ci ne respecte pas ses obligations ou les recommandations de la Banque ou si celle-ci estime prudent d'interdire l'accès au Client pour toute autre raison.

9. Confidentialité des messages

Les parties reconnaissent aux messages échangés via les Services E-Banking le caractère d'une correspondance privée.

10. Localisation des échanges

Les communications établies entre la Banque et le Client, ainsi que toutes les opérations initiées ou réalisées au travers des Services E-Banking sont réputées être effectuées directement à la Banque, à la date et l'heure indiquées sur le serveur de la Banque, le journal des connexions tenu par la Banque faisant foi de celles-ci.

11. Destruction des identifiants et certificats

Dans l'hypothèse où le Client n'a plus d'accès à ses Comptes Consultables via les Services E-Banking, il s'engage à détruire tous les identifiants lui ayant été remis par la Banque.

12. Responsabilité

Dans le cadre de la mise à disposition des Services E-Banking, la Banque n'assume que des obligations de moyens à l'égard du Client. Conformément à l'article 21 des Conditions Générales de la Banque, la responsabilité de la Banque ne peut être engagée que pour faute grave.

Le Client qui accède aux Services E-Banking à partir de l'étranger s'engage à se conformer au respect des prescriptions légales et réglementaires en vigueur dans le pays à partir duquel cet accès a lieu.

13. Modifications des Conditions d'accès et d'utilisation des Services E-Banking

La Banque peut modifier à tout moment les présentes Conditions d'accès et d'utilisation des Services E-Banking par une notification écrite pour tenir compte notamment des modifications législatives ou réglementaires, ainsi que des usages de la place ou de la politique de la Banque.

La Banque se réserve le droit à tout moment de notifier au Client, par tous moyens y compris par un message transmis ou affiché via les Services E-Banking, les modifications apportées aux présentes Conditions d'accès et d'utilisation des Services E-Banking.

Ces modifications seront considérées comme approuvées si le Client n'y fait pas opposition par écrit.

Cette opposition devra parvenir à la Banque dans un délai de 30 jours à compter de l'envoi de la notification.

La nullité ou l'inapplicabilité de l'une des clauses des présentes Conditions d'accès et d'utilisation des Services E-Banking n'affectera pas la validité des autres clauses qui demeurent applicables en l'absence des dispositions annulées.

14. Acceptation des conditions générales LuxTrust

Le Client ayant opté pour un mode d'accès LuxTrust déclare avoir pris connaissance et approuver les conditions générales et toutes autres conditions le liant et/ou liant la Banque à LuxTrust dans le cadre de ce mode d'accès (disponibles sur le website www.luxtrust.lu.)

Annexe :
Avertissement sur les risques inhérents aux virements effectués via les Services E-Banking (banque en ligne)

Avertissement sur les risques inhérents aux virements effectués via les Services E-Banking (banque en ligne)

Cette note vise à informer le Client des risques non exhaustifs liés à l'exécution des virements électroniques.

Le « phishing »

Le « phishing » est une technique utilisée par les escrocs en ligne, consistant à se faire passer pour la Banque avec l'objectif de collecter des données personnelles de clients.

e-mail phishing :
Par cette technique, **les pirates imitent des messages ou des pages de sites pour recueillir des informations confidentielles.** La victime reçoit un faux e-mail d'une banque ou d'un organisme officiel. Ces messages prétextent une mise à jour technique du portail de la banque ou une prétendue vérification de coordonnées personnelles. En cliquant sur un lien contenu dans le message, la victime est alors redirigée vers un site imitant le site officiel de la banque puis invitée à saisir ses identifiants et mots de passe personnels.

Les e-mails peuvent également consister en des e-mails relatifs à des loteries fictives et qui annoncent à la victime qu'elle a gagné. Pour percevoir le gain, les escrocs demandent la communication des coordonnées personnelles bancaires.

Certains e-mails sollicitent l'assistance de la victime pour procéder à des transferts de fonds. Une personne demande d'utiliser le compte de la victime pour faire transiter une somme très importante en promettant un pourcentage. Ces sollicitations sont des escroqueries auxquelles il ne convient pas de donner suite.

phone phishing :
Une personne reçoit un appel téléphonique d'une personne prétendant être un employé de sa banque. Celui-ci lui annonce que, suite à des problèmes techniques, son compte va être fermé s'il ne lui communique pas ses informations personnelles telles que son numéro de compte et son mot de passe.

L'usurpation d'identité

Une personne mal intentionnée utilise sciemment l'identité d'une autre personne dans le but de réaliser des actions frauduleuses.

Pour pouvoir emprunter cette identité, un fraudeur doit avoir préalablement en sa disposition des renseignements personnels et confidentiels qui concernent la victime d'usurpation.

Une usurpation d'identité peut avoir de graves conséquences comme la constitution de faux papiers, l'utilisation de comptes bancaires et la réalisation d'opérations frauduleuses.

Par exemple, en piratant votre adresse e-mail, le fraudeur a accès à tous vos e-mails et peut s'adresser à vos relations en utilisant votre adresse email et votre manière de communiquer et ainsi abuser de la confiance de vos proches.

Le logiciel malveillant

Le logiciel malveillant, appelé « malware » en anglais, est un logiciel développé pour nuire intentionnellement à un système informatique, ou pour en recueillir des données à l'insu de l'utilisateur.

Il en existe de multiples formes : **les virus, les vers ou encore les chevaux de Troie** en sont les déclinaisons les plus connues (virus qui est installé lorsque vous accédez à un site piraté. Par exemple, le virus collecte alors les touches du clavier qui ont été enfoncées en vue de les transmettre automatiquement aux escrocs). La sophistication de ces logiciels évolue avec l'avancée des technologies.

Que peut-on faire pour réduire les risques ? Revue des bonnes pratiques de sécurité sur Internet

Ne communiquez jamais votre mot de passe ou vos identifiants personnels !

La Banque n'utilise jamais la messagerie électronique pour vous demander de lui fournir vos identifiants personnels, vos mots de passe, vos OTP (One Time Passwords) ou toute autre information confidentielle. La Banque ne demande jamais de codes d'accès (mot de passe, OTP - One Time Passwords, ...) à ses clients, que ce soit par email, téléphone ou tout autre moyen de communication.

Comment protéger votre mot de passe ?

Choisissez un mot de passe sécurisé (composé d'au moins 8 caractères avec des chiffres, des caractères spéciaux, ...) et changez le régulièrement. Utilisez des mots de passe différents pour chaque site que vous consultez (accès à la banque en ligne dans d'autres banques, email, e-commerce, réseaux sociaux, forums, ...).

Comment protéger votre ordinateur ?

Pour protéger votre accès E-Banking, utilisez toujours un ordinateur de confiance dont vous maîtrisez la sécurité et évitez les ordinateurs publics.

A cet effet, nous vous recommandons :

– d'installer sur votre ordinateur un logiciel antivirus et antispyware mis à jour régulièrement et automatiquement
– d'installer les mises à jour des logiciels récentes de votre système d'exploitation et de votre navigateur Internet
– d'installer uniquement des logiciels de confiance
– d'activer le firewall.

Comment vérifier que vous êtes bien sur le site de banque en ligne de la Banque ?

Accédez directement au site de la Banque en saisissant l'adresse http://www.banquedeluxembourg.com dans la barre d'adresse de votre navigateur Internet ou depuis vos favoris après l'avoir enregistrée au préalable.

– Cliquez sur « ACCEDER A MON COMPTE » puis sélectionnez votre mode d'authentification :
– Vérifier que l'adresse commence par « https »
– Vérifier qu'un cadenas est présent en bas et/ou en haut de la page sécurisée et qu'il est fermé
– Double-cliquez sur le cadenas
– Un écran représentant le certificat numérique de la Banque apparaît
– Vérifiez que le nom du certificat comporte bien « BANQUEDELUXEMBOURG.COM ».

Comment vous déconnecter de manière sécurisée et vérifier votre dernière connexion à la banque en ligne ?

Terminez systématiquement toute connexion à votre espace personnel des Services E-Banking en utilisant le bouton « Déconnexion » et fermez la fenêtre de votre navigateur après la consultation de vos comptes en ligne. La date et l'heure de votre dernière connexion réalisée avec vos identifiants sont indiquées sous le bouton DECONNEXION. Pensez également à surveiller les mouvements sur vos comptes.

Comment vous protéger contre le phishing ?

Par cette technique, les pirates informatiques imitent des emails ou des sites institutionnels pour recueillir vos informations confidentielles : numéro de carte de crédit, identifiant, mot de passe, nom, prénom, date de naissance, adresse, numéro de téléphone, etc.

Dans la plupart des cas, cette escroquerie est réalisée par le biais de faux emails des banques ou d'organismes officiels. Ces messages prétextent une mise à jour technique du site correspondant ou une prétendue vérification de vos coordonnées personnelles. En cliquant sur un lien contenu dans l'email, vous êtes alors redirigé vers un site imitant le site institutionnel puis invité à saisir vos informations personnelles. Pour vous prémunir contre le phishing, étudiez le message ou l'appel, son contenu, l'adresse de l'expéditeur. Pour rappel, la Banque et toute institution financière en général ne demandent jamais de mot de passe, identifiant ou OTP (One Time Password) par email ou par téléphone à un client.

Que faire si vous avez perdu vos codes d'accès et qui contacter si vous avez une question ?

Si vous avez perdu vos codes d'accès, contactez au plus vite LuxTrust (www.luxtrust.lu). Pour toute autre question concernant votre compte et l'accès à l'application BL Mobile Banking, téléphonez à BL-Support au (+352) 26 20 26 30 du lundi au vendredi de 09h00 à 18h00.