

## Règlement E-Banking

Le soussigné (ci-après le « Souscripteur ») souhaite avoir un accès via le réseau Internet à un ou plusieurs comptes (ci-après les « Comptes liés »).

### ARTICLE I : DEFINITIONS

Dans le présent Règlement et dans les documents auxquels ils se réfèrent, les termes suivants sont utilisés et applicables ; ceux-ci pouvant être utilisés au pluriel ou au singulier :

- Appareil mobile : l'appareil informatique portatif du Souscripteur, tel un smartphone, une tablette ou instrument de même nature, disposant d'un accès à Internet, et, le cas échéant, sur lequel l'Application LuxTrust Mobile et l'Application E-Banking ont été téléchargées et qui permet au Souscripteur de bénéficier du Service mis à sa disposition par la Banque. Les exigences techniques auxquelles cet appareil doit satisfaire figurent sur la plateforme de téléchargement d'applications en ligne (telle que l'Apple Store ou Google Play) ;
- Application E-Banking : l'application mobile de banque à distance de la Banque, appelée « Mobile Banking BT Belgium » que le Souscripteur peut télécharger et installer sur un Appareil mobile et qui lui permet de bénéficier du Service ;
- Application LuxTrust Mobile : l'application utilisée pour générer un code à usage unique sur base de données contextualisées ;
- Authentification : une procédure permettant à la Banque, en sa qualité de prestataire de services de paiement, de vérifier l'identité d'un utilisateur de services de paiement ou la validité de l'utilisation d'un instrument de paiement spécifique, y compris l'utilisation des données de sécurité personnalisées de l'utilisateur de services de paiement ;
- Authentification forte du Souscripteur : une authentification reposant sur l'utilisation de deux éléments ou plus appartenant aux catégories « connaissance » (quelque chose que seul l'utilisateur connaît), « possession » (quelque chose que seul l'utilisateur possède) et « inhérence » (quelque chose que l'utilisateur est) et indépendants en ce sens que la compromission de l'un ne remet pas en question la fiabilité des autres, et qui est conçue de manière à protéger la confidentialité des données d'authentification ;
- Banque : Banque Transatlantique Belgium SA, ayant son siège social à B-1000 Bruxelles, rue de Crayer 9, RPM Bruxelles, TVA BE 0872.743.345, agréée comme établissement de crédit de droit belge et soumise en cette qualité au contrôle prudentiel de la Banque centrale européenne et de la Banque Nationale de Belgique (BNB) ainsi qu'au contrôle en matière de protection des investisseurs et des consommateurs de l'Autorité des Services et Marchés Financiers (FSMA) ;
- Certificat du Souscripteur : le certificat LuxTrust 'Signing Server' (LuxTrust Mobile) ou d'un autre moyen d'authentification reconnu par LuxTrust ;
- Comptes liés : les comptes tenus auprès de la Banque, dont le Souscripteur est titulaire et/ou co-titulaire et/ou ceux sur lesquels il est mandataire et/ou ceux ouverts au nom d'une personne dont il est le représentant légal, et/ou ceux sur lesquels le Tiers autorisé a été autorisé par le Titulaire à consulter et à recevoir des informations et qui sont renseignés par le Souscripteur dans la Demande d'accès E-Banking.
- Demande d'accès E-Banking : la demande/modification d'accès E-Banking complétée et signée par le Souscripteur et acceptée par la Banque ;
- Dispositif de sécurité personnalisé : tout moyen technique affecté par un prestataire de services de paiement à un utilisateur donné pour l'utilisation d'un instrument de paiement. Ce dispositif propre à l'utilisateur de services de paiement et placé sous sa garde, permet de vérifier l'utilisation d'un instrument de paiement donné et vise à authentifier l'utilisateur ;
- Données de sécurité personnalisées : des caractéristiques personnalisées fournies à un utilisateur de services de paiement par le prestataire de services de paiement à des fins d'authentification ;
- LuxTrust : LuxTrust SA, ayant son siège social à L-8308 Capellen (Luxembourg), 13-15, Parc d'activités, TVA LU 20976985, RCS BI 12233 ;
- Manuel : manuel mis à la disposition du Souscripteur, sur un support durable, définissant les conditions et modalités auxquelles le Service peut être activé et utilisé ;
- Password personnel : code choisi par le Souscripteur lors de l'activation du Certificat du Souscripteur ;
- Passcode : code d'identification personnel et confidentiel choisi par le Souscripteur ;
- Règlement : le présent règlement ;
- Relevés : les relevés d'opérations et/ou les relevés estimatifs relatifs aux Comptes liés ;
- Service : le service de banque par Internet que la Banque propose via son Site E-Banking et/ou via son Application E-Banking et ses systèmes informatiques, tel que décrit dans le présent Règlement ;
- Site E-Banking : l'espace sécurisé E-Banking du site Internet de la Banque ;
- Souscripteur : la personne physique, majeure et capable, à qui le Service a été mis à disposition suite à l'acceptation par la Banque de la Demande d'accès E-Banking et qui l'utilise soit en son nom et pour son compte en tant que titulaire ou co-titulaire du ou des Comptes liés au Service, soit en qualité de mandataire ou de représentant légal du Titulaire du ou des Comptes liés, soit en qualité de personne habilitée à représenter le tiers autorisé par le Titulaire à consulter et à recevoir des informations, notamment, sur le fonctionnement du ou des Comptes liés ;
- Titulaire : la personne physique ou morale titulaire ou co-titulaire d'un ou des Comptes liés et lorsque le Souscripteur agit comme mandataire ou représentant légal du titulaire du compte, la personne au nom et pour compte de laquelle le Service est utilisé. En cas de pluralité

de titulaires, sauf mention contraire, le terme « titulaire » vise l'ensemble des co-titulaires ;

- Web-User : nom d'utilisateur du Souscripteur dans les systèmes de la Banque.
- User-ID : nom d'utilisateur du Souscripteur dans les systèmes de LuxTrust, reçu par le Souscripteur, par SMS, lors de la commande du certificat LuxTrust 'Signing Server' (LuxTrust Mobile).

#### ARTICLE 2 : OBJET

- 2.1 Le présent Règlement détermine les droits et obligations du Souscripteur et de la Banque relativement à la mise à disposition, à l'accès et à l'utilisation du Service. Ce Règlement constitue un complément aux conditions générales de la Banque, en précisant les conditions et modalités propres au Service. Pour autant qu'il n'y soit pas explicitement dérogé par le présent Règlement, les conditions générales de la Banque demeurent d'application. Les conditions générales de la Banque, la Demande d'accès E-Banking signée par le Souscripteur, le présent Règlement et le Manuel forment le cadre contractuel du Service. Le Souscripteur reconnaît avoir reçu et pris connaissance de ces documents avant la signature de la Demande d'accès E-Banking. En signant la Demande d'accès E-Banking et en utilisant le Site E-Banking de la Banque et/ou l'Application E-Banking, le Souscripteur y adhère sans réserve.
- 2.2 Le Règlement, les conditions générales de la Banque ainsi que le Manuel sont disponibles gratuitement à tout moment sur le site Internet de la Banque. Le Souscripteur peut également recevoir, sur demande adressée à la Banque, un exemplaire des documents précités sur support papier ou sur tout autre support durable.

#### ARTICLE 3 : OCTROI DU SERVICE

- 3.1 Le Service peut être octroyé à toute personne physique qui le demande en tant que titulaire et/ou co-titulaire ou mandataire ou représentant légal du Titulaire, d'au moins un compte ouvert dans les livres de la Banque, ou en tant que personne habilitée à représenter le tiers autorisé par le Titulaire à consulter et à recevoir des informations, notamment, sur le fonctionnement du ou des Comptes liés, dans les limites fixées par les dispositions du cadre contractuel du Service.
- 3.2 Seuls les comptes tenus auprès de la Banque et dont le Souscripteur est titulaire, et/ou co-titulaire, ceux sur lesquels il est mandataire, ceux ouverts au nom d'une personne dont il est le représentant légal, ceux sur lesquels il est repris en tant que personne habilitée à représenter le tiers autorisé par le Titulaire à consulter et à recevoir des informations, notamment, sur le fonctionnement desdits comptes, et qui sont renseignés dans la Demande d'accès E-Banking sont, dès l'octroi du Service, des Comptes liés. Le Souscripteur peut consulter, via le Service, la liste des Comptes liés accessibles. La liste est mise à jour en fonction des événements qui modifient la situation

de ces comptes ou la relation du Souscripteur à ces comptes.

- 3.3 La Banque se réserve le droit de refuser l'octroi du Service, sans devoir motiver ce refus, ou après l'avoir octroyé, de l'interrompre ou d'y mettre fin dans les conditions prévues dans le présent Règlement.

#### ARTICLE 4 : ACCES AU SERVICE

- 4.1 L'accès au Service E-Banking s'effectue soit via l'Application E-Banking, soit via le Site E-Banking de la Banque dont l'adresse est communiquée au Souscripteur par la Banque.
- 4.2 Le Service n'est accessible soit via l'Application E-Banking, soit via le site Internet de la Banque qu'après que le Souscripteur se soit identifié et authentifié, via LuxTrust Mobile App ou via un autre moyen d'identification et d'authentification reconnu par LuxTrust. Si le moyen d'accès au Service est un Signing Server LuxTrust (LuxTrust Mobile App), le Souscripteur recevra par SMS de la part de LuxTrust les identifiants correspondant à son choix afin de lui permettre de se connecter au Service, de s'identifier et de signer ses instructions. Dès mémorisation des identifiants, le SMS doit être détruit. Si le moyen d'accès au Service E-Banking est un autre moyen d'authentification reconnu par LuxTrust, le Souscripteur recevra les modalités et les conditions d'utilisation par le fournisseur de sa solution d'authentification. Le Titulaire autorise expressément la Banque et LuxTrust à remettre à ses mandataires, qui ont pouvoir de signature ou un droit de regard sur les Comptes liés, des identifiants et moyens d'authentification donnant accès au Service, lorsque ces derniers le demandent.
- 4.3 Le Manuel décrit précisément les étapes à suivre, en fonction du moyen d'accès au Service sélectionné par le Souscripteur, pour activer l'accès au Service (par ex. activation du certificat LuxTrust 'Signing Server', configuration de l'Application E-Banking, etc.). Le Manuel constitue par ailleurs une documentation technique relative à l'utilisation du Service (y compris les procédures de communication et de signature électronique). L'accès au Service et son utilisation exigent que le Souscripteur dispose d'un ordinateur ou d'un Appareil mobile ayant un accès et une connexion à Internet et qui remplit les exigences techniques de l'équipement minimum décrit dans le Manuel.
- 4.4 Tout accès au Service effectué au moyen des identifiants du Souscripteur est réputé l'être par le Souscripteur, le journal des connexions tenu par la Banque faisant foi de celles-ci. La Banque conserve un historique des connexions au Site E-Banking et à l'Application E-Banking. Le contenu de ce journal peut être conservé sur tout support (y compris électronique). Le Souscripteur reconnaît que ces modes de conservation ont la même force probante qu'un document original.
- 4.5 La Banque se réserve le droit de modifier la procédure d'accès et/ou d'identification et/ou d'authentification

- et/ou les mesures de sécurité, en fonction, notamment, de l'évolution technique, des systèmes de sécurité et/ou de la réglementation applicable. La Banque préviendra le Souscripteur de ces modifications en respectant les délais prévus à l'article 15 du présent Règlement, sauf en cas d'urgence.
- 4.6 Le Souscripteur a accès au Service 24 heures sur 24 et 7 jours sur 7. Cependant, la Banque se réserve le droit de procéder, à tout moment et sans indemnité, à des interruptions du Service, notamment, pour l'entretien et la maintenance du système, pour l'installation de nouvelles versions ou de mises à jour des systèmes et dispositifs informatiques. Lorsque la Banque est en mesure de prévoir l'inaccessibilité temporaire du Service, elle en avertira le Souscripteur au préalable, dans la mesure du possible, par tous moyens appropriés (y compris par un message sur le Site E-Banking et/ou l'Application E-Banking de la Banque). Des interruptions et des incidents dans le fonctionnement du Service peuvent toutefois également se produire sans que la Banque soit en mesure de prévenir préalablement le Souscripteur, notamment à la suite d'un incident ou d'un problème technique, de surcharge du réseau, de coupure de ligne téléphonique, d'erreur, de négligence ou de faute d'un tiers ou du Souscripteur ainsi que dans toutes autres circonstances indépendantes de la volonté de la Banque ou en cas de force majeure. Le Souscripteur dégage la Banque de toute responsabilité à cet égard. La Banque fera tout son possible pour informer le Souscripteur, dans un délai raisonnable, de la nature et de la durée probable de l'interruption, par tous moyens appropriés.
- 4.7 De nouvelles versions de l'Application E-Banking sont mises à la disposition du Souscripteur à travers les plateformes de téléchargement d'applications en ligne (telles que l'Apple Store ou Google Play). Le Souscripteur en sera averti par tous moyens appropriés (y compris par un message sur l'Application E-Banking de la Banque). En téléchargeant ces mises à jour, le Souscripteur accepte les modifications apportées au présent règlement qui résultent de celles-ci. Le Souscripteur s'engage à télécharger régulièrement les mises à jour et, sauf exception prévoyant une période plus courte, au plus tard dans le mois de leur mise à disposition. Le Souscripteur est informé que s'il n'installe pas certaines mises à jour, la Banque peut suspendre l'accès à l'Application E-Banking.
- 4.8 La Banque se réserve le droit, à l'égard d'un Souscripteur déterminé, de restreindre ou d'interrompre, sans mise en demeure préalable, en tout ou en partie, temporairement ou définitivement, l'accès au Service et dans ce dernier cas de mettre fin à la convention E-Banking, notamment, dans les cas suivants :
- pour des raisons objectivement motivées ayant trait à la sécurité du Service, de l'Application E-Banking ;

- en cas de présomption d'une utilisation non autorisée ou frauduleuse du Service, de l'Application E-Banking ;
- en cas d'usage abusif ou frauduleux du Service et/ou des identifiants ;
- en cas de non-respect par le Souscripteur des procédures d'accès et d'utilisation du Service et/ou des consignes de sécurité ;
- en cas d'inexécution par le Souscripteur de ses obligations légales, réglementaires ou contractuelles en rapport avec les services proposés par la Banque ;
- si le Souscripteur ne s'est pas connecté au Site E-Banking et/ou à l'Application E-Banking pendant une période ininterrompue de 6 mois et/ou s'il a négligé d'installer deux mises à jour consécutives de l'Application E-Banking ;
- en cas de clôture ou de blocage des Comptes liés ;
- en cas de suppression, pour quelle cause que ce soit, de son mandat ou de sa qualité de représentant légal sur les Comptes liés lorsque le Souscripteur agit en qualité de mandataire ou de représentant légal du Titulaire ;
- en cas de suppression, pour quelle cause que ce soit, de l'autorisation conférée au Tiers autorisé, lorsque le Souscripteur agit en qualité de personne habilitées à représenter un Tiers autorisé ;
- sur demande d'une autorité judiciaire ;
- en cas de décès d'un des Titulaires.

La Banque informe le Souscripteur et/ou le Titulaire du blocage ou de l'interruption du Service par téléphone, par courrier ou par courrier électronique et ce, si possible, avant que le blocage ou l'interruption ne soit effectif et au plus tard immédiatement après, excepté si des raisons objectives de sécurité, une décision de justice ou la réglementation s'y oppose. La Banque débloque l'accès au Service dès lors que les raisons justifiant le blocage n'existent plus.

#### ARTICLE 5 : DESCRIPTION DU SERVICE – FONCTIONNALITES

- 5.1 Le Service permet au Souscripteur de se connecter aux systèmes informatiques de la Banque, par le biais d'un réseau de télécommunication, pour notamment :
- consulter l'état et la situation des Comptes liés, l'historique des mouvements effectués sur les Comptes liés ainsi que les opérations d'achat et de vente en cours d'exécution sur ces mêmes Comptes liés ;
  - télécharger, consulter, sauvegarder et/ou imprimer les Relevés relatifs aux Comptes liés, disponibles dans l'espace documentaire ;
  - initier et transmettre des ordres de virements au départ d'un compte de paiement, entre comptes propres et vers comptes de tiers ;
  - communiquer par voie électronique avec la Banque ;
  - signer électroniquement des documents et des instructions ;
  - déterminer / changer des données personnelles ;

- avoir accès aux numéros utiles d'aide et d'assistance.
- Certaines des fonctionnalités mentionnées ci-dessus peuvent être exclusives ou se présenter différemment sur le Site E-Banking de la Banque et/ou dans l'Application Mobile.
- 5.2 Les informations relatives aux Comptes liés sont arrêtées au dernier traitement informatique précédant leur consultation par le Souscripteur via le Service et sont fournies sous réserve des opérations en cours qui ne sont pas encore traitées au moment de la consultation.
- 5.3 La Banque se réserve le droit de modifier à tout moment le Service (afin d'ajouter de nouvelles fonctionnalités au Service ou de modifier ou de supprimer des fonctionnalités existantes). Toute évolution du Service sera portée à la connaissance du Souscripteur conformément aux dispositions de l'article 15 du présent Règlement.
- 5.4 La Banque enregistre les données essentielles de toute opération effectuée dans le cadre du Service. Ces enregistrements sont conservés par la Banque au moins pendant 10 ans à compter de l'exécution des opérations et peuvent être reproduits sous forme lisible sur n'importe quel support standard. L'enregistrement des communications dans le journal des connexions de la Banque a valeur de preuve pour déterminer précisément les données envoyées ou transmises. Le Souscripteur et le Titulaire acceptent ces enregistrements comme preuve.
- 5.5 La Banque se réserve le droit, pour l'exécution du Service, de faire appel à des sous-traitants.

#### ARTICLE 6 : ORDRES DE VIREMENT

- 6.1 Le Service E-Banking permet au Souscripteur d'initier et de transmettre des ordres de virement, entre comptes propres et vers comptes de tiers, au départ d'un compte de paiement accessible en ligne :
- des virements nationaux en euro ;
  - des virements transfrontaliers en euro vers certains pays qui font partie de la zone SEPA (« *Single Euro Payments Area* ») (à savoir l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Irlande, l'Italie, le Luxembourg, les Pays-Bas et le Portugal).
- Si un ordre de virement n'est pas autorisé pour un compte déterminé, ce compte ne pourra pas être sélectionné pour l'ordre concerné. Les comptes bloqués sont toujours exclus pour tous les ordres.
- 6.2 Tous les ordres donnés à la Banque sont régis par les conditions générales de la Banque dans la mesure où le présent Règlement n'y déroge pas explicitement. Un ordre de paiement transmis dans le cadre du Service est exécuté par la Banque à condition que l'état du compte, ainsi que les conventions et règlements qui le régissent le permettent. Le Souscripteur autorise irrévocablement la Banque à débiter son compte du montant de l'ordre de paiement transmis dans le cadre du Service.
- 6.3 Les champs obligatoires pour un ordre de virement introduit via l'Application E-Banking ou via le Site E-

Banking, au départ d'un compte de paiement accessible en ligne, sont :

- le montant ;
- la devise ;
- le numéro de compte à créditer (IBAN – *International Bank Account Number*) ;
- le nom du bénéficiaire ;
- la date d'exécution souhaitée. Si le Souscripteur souhaite mentionner une date mémo pour un ordre de virement, cette date doit répondre aux conditions suivantes :
  - au minimum le jour de l'envoi de l'ordre de virement + 1 jour bancaire ouvrable ;
  - au maximum le jour de l'envoi de l'ordre de virement + 365 jours calendriers.

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

- 6.4 Le Souscripteur signe un ordre de virement au moyen :

- soit de son Passcode ;
- soit de son empreinte digitale (si son Appareil mobile prévoit cette fonctionnalité et qu'elle a été activée).

Le Souscripteur reconnaît que les Dispositif et Données de sécurité personnalisées constituent une signature électronique. Ils constituent une preuve valable et suffisante de son accord quant à l'existence et au contenu de l'ordre de paiement. Le Souscripteur renonce explicitement au droit de contester la validité ou la preuve des engagements qui découlent des ordres de paiement signés au moyen de son Passcode ou de son empreinte digitale (si l'Appareil mobile prévoit cette fonctionnalité et qu'elle a été activée).

- 6.5 Pour les ordres de paiement électroniques via l'Application E-Banking ou le Site E-Banking de la Banque :

- concernant des ordres de paiements nationaux et transfrontaliers en euro qui sont enregistrés avant 13 heures un jour ouvrable bancaire, l'ordre de paiement est réputé avoir été reçu ce même jour ouvrable bancaire ;
- concernant des ordres de paiements nationaux et transfrontaliers en euro qui sont enregistrés après 13 heures un jour ouvrable bancaire, ou qui sont enregistrés un jour qui n'est pas un jour ouvrable bancaire, l'ordre de paiement est réputé avoir été reçu le premier jour ouvrable bancaire suivant.

- 6.6 Le Souscripteur ne peut ni modifier, ni révoquer, via l'Application E-Banking ou via le Site E-Banking de la Banque, un ordre de virement reçu par la Banque. Pour révoquer un ordre de virement, il est tenu de s'adresser à la Banque. Ce paragraphe ne porte pas préjudice aux dispositions en matière de révocation reprises dans les conditions générales de la Banque.

- 6.7 **Le traitement des ordres de virement transmis à la Banque via l'Application E-Banking ou via le Site E-Banking de la Banque ne s'effectue pas en temps réel et nécessite une validation par les services de la Banque.** Le Souscripteur en est averti par un message sur l'Application E-Banking ou le Site E-Banking de la Banque de la Banque.

- 6.8 La Banque se réserve le droit de refuser d'exécuter un ordre conformément à ce qui est prévu par ses conditions générales.  
Si la Banque refuse d'exécuter un ordre de virement, elle en informe le Souscripteur dans les meilleurs délais et lui communique, le cas échéant, les motifs du refus ainsi que la procédure à suivre pour corriger toute erreur factuelle ayant entraîné le refus, sans préjudice de l'application de la réglementation anti-blanchiment et/ou d'une autre interdiction légale. Cette notification est effectuée par courrier ou courrier électronique. Un ordre de paiement dont l'exécution a été refusée est réputé non reçu.
- 6.9 Lorsqu'il transmet un ordre de virement, le Souscripteur tient compte des limites minimales et maximales fixées par la Banque, pour l'instrument de paiement considéré. Les limites sont précisées sur la feuille des tarifs.
- 6.10 Seuls les virements qui ont été validés par le système interne de la Banque apparaissent dans l'historique du compte de paiement concerné, accessible en ligne via l'Application E-Banking ou le Site E-Banking de la Banque. Les transactions futures ou les transactions en suspens n'y figurent pas.

#### ARTICLE 7 : RELEVES

- 7.1 Les Relevés sont disponibles via le Service au format PDF.
- 7.2 Le Souscripteur peut opter pour une mise à disposition de ses Relevés via le Service (en plus d'un envoi par courrier postal et/ou par courrier électronique).  
Le Souscripteur peut, au choix, consulter les Relevés, les télécharger et les enregistrer et/ou les imprimer.
- 7.3 Les Relevés imprimés via le Service n'ont pas valeur de relevés originaux. En cas de différence entre les Relevés imprimés par le Titulaire ou le Souscripteur et ceux imprimés par la Banque, ces derniers, basés sur la situation du compte telle qu'elle apparaît dans les livres de la Banque, priment et constituent la preuve formelle des opérations effectuées.

#### ARTICLE 8 : SIGNATURE ELECTRONIQUE DE DOCUMENTS

- 8.1 Le Service E-Banking permet au Souscripteur de signer électroniquement des documents qui lui sont transmis par la Banque.
- 8.2 L'utilisation de tout procédé de signature électronique mis à disposition par la Banque a valeur de signature au sens de la loi. Pour le surplus, les conditions générales (notamment l'article 19.6) sont d'application.

#### ARTICLE 9 : DETERMINATION / CHANGEMENT DE DONNEES

- 9.1 Le Service permet au Souscripteur de consulter et dans certains cas, de modifier certaines données personnelles du Titulaire.
- 9.2 Certaines modifications demandent un examen plus approfondi et/ou une décision de la part des services de la Banque. Le Souscripteur en est averti par un message sur l'Application E-Banking ou le Site E-Banking de la Banque.

#### ARTICLE 10 : SERVICES D'ASSISTANCE TECHNIQUE

- 10.1 Pour toute question ou problème technique en lien avec l'Application LuxTrust Mobile et le certificat LuxTrust 'Signing Server', le Souscripteur peut contacter le Service Desk de LuxTrust par téléphone au +352 24 550 550 ou par e-mail sur [helpdesk@luxtrust.lu](mailto:helpdesk@luxtrust.lu). Les agents de LuxTrust sont disponibles du lundi au vendredi de 8h à 18h (service révocation, suspension et déblocage disponible 24/7). Pour toute question ou problème technique en lien avec tout Certificat autre que le certificat LuxTrust 'Signing Server', le Souscripteur peut contacter le service d'assistance technique du fournisseur de ce Certificat et/ou de cette solution d'authentification.
- 10.2 Pour toute autre question, la Banque met à la disposition du Souscripteur un service d'assistance technique, dont les coordonnées ainsi que les jours et heures d'accessibilité figurent sur l'Application E-Banking de la Banque et sur le Site E-Banking de la Banque, afin d'assister le Souscripteur lors de la survenance de problèmes techniques liés à l'utilisation de l'Application E-Banking ou le Site E-Banking de la Banque.

La Banque procurera toute l'assistance raisonnable par téléphone, sur la base d'une obligation de moyens, afin d'identifier et si possible, de corriger les éventuels problèmes techniques rencontrés dans le fonctionnement du Service ou encore de fournir au Souscripteur des informations supplémentaires sur les fonctionnalités et le fonctionnement du Service.

La Banque ne peut être tenue pour responsable de la non-résolution partielle ou totale d'un problème technique qui lui a été soumis par le biais de ce service d'assistance technique compte tenu des limitations techniques liées à un tel service d'assistance.

#### ARTICLE 11 : OBLIGATIONS ET RESPONSABILITES DU SOUSCRIPTEUR

- 11.1 Le Souscripteur est tenu d'utiliser le Service conformément aux conditions qui en régissent l'accès et l'utilisation. Il doit notamment respecter strictement toutes les instructions relatives à la procédure de connexion ainsi que toutes les conditions et modalités d'utilisation et les consignes de sécurité, décrites notamment dans le présent Règlement et dans le Manuel ou communiquées par la Banque par tout autre moyen. Le non-respect de celles-ci est à considérer comme une négligence grave et mettra le Souscripteur dans l'obligation de supporter l'entière perte pouvant, le cas échéant, résulter d'un accès frauduleux au Service.  
La connexion au Service est protégée par une solution de chiffrement et d'identification du Souscripteur. L'accès à et l'utilisation du Service ainsi que les mesures de sécurité et les mesures de compatibilité sont conformes aux exigences légales en matière d'Authentification forte du Souscripteur.  
Le Souscripteur 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.
- 11.2 Le Souscripteur est tenu de sauvegarder le caractère confidentiel et personnel de ses identifiants, Données et Dispositifs de sécurité personnalisés (support d'authentification et identifiant reçu par LuxTrust ou par un autre fournisseur de sa solution d'authentification reconnue, Passcode, mot de passe, Password, etc.) et de prévenir tout risque d'utilisation non autorisée. Il s'engage notamment à ne les communiquer et à ne pas les mettre à portée ou à disposition de tiers quels qu'ils soient. Il lui incombe de prendre les mesures raisonnables en vue de les protéger, tout en suivant les conseils de sécurité de la Banque, tels qu'ils figurent notamment en annexe et dans le Manuel et qui sont pleinement applicables. En particulier et sans que cette liste soit exhaustive, le Souscripteur doit veiller à ne pas communiquer ces Données et Dispositifs de sécurité personnalisés à des tiers. Il doit également faire preuve de discrétion en introduisant son Passcode pour accéder à l'Application E-Banking et/ou au Site E-Banking de la Banque. Le Passcode doit être choisi avec soin, en évitant les combinaisons trop évidentes (date de naissance, par exemple).
- 11.3 Le Souscripteur ne peut conserver son Passcode sur le même Appareil mobile qui sert d'instrument d'Authentification, ni enregistrer sur la mémoire d'un ou de plusieurs autres appareils.
- 11.3 Le Souscripteur est tenu d'avertir la Banque et LuxTrust ou tout autre fournisseur de sa solution d'authentification, dès qu'il en a connaissance et par tous moyens :
- de la perte, du vol, du détournement, de l'utilisation non autorisée ou de tout risque d'abus de ses identifiants, Données et/ou Dispositifs de sécurité personnalisés permettant d'accéder à l'Application E-Banking et/ou au Service et/ou de tout appareil utilisé pour accéder au Service ;
  - de tout problème rencontré alors qu'il essaie d'accéder au Service ou qu'il utilise le Service et ce, sans préjudice des dispositions du présent Règlement.
- A cet effet, le Souscripteur peut contacter chacun des services d'assistance technique mis à sa disposition par la Banque et par LuxTrust, dont les coordonnées ainsi que les jours et heures d'accessibilité sont repris à l'article 10.1 du présent Règlement et dans le Manuel. Dès l'instant où la Banque et LuxTrust en sont averties pendant les jours et heures d'accessibilité du service d'assistance technique, l'accès au Service sera immédiatement interrompu. En dehors des jours et heures d'accessibilité des services d'assistance technique susmentionnés, le Souscripteur procédera au blocage de son dispositif LuxTrust, depuis de site Internet de LuxTrust (<https://www.luxtrust.com>). En cas d'accès au Service par un autre moyen d'authentification, le Souscripteur consultera le site Internet du fournisseur de cette autre solution d'authentification.
- En cas de perte, de vol, de détournement ou d'utilisation non autorisée de ses identifiants, Données et/ou Dispositifs de sécurité personnalisés permettant d'accéder à l'Application E-Banking et/ou au Site E-Banking et/ou au Service et/ou de tout appareil utilisé pour accéder au Service, le Souscripteur doit également faire une déclaration de ces faits ou déposer une plainte auprès des autorités officielles locales, belges ou étrangères compétentes dans les 24 heures de leur constatation et faire parvenir la preuve et les références de cette déclaration ou plainte à la Banque.
- 11.4 Le Souscripteur n'acquiert qu'un droit d'utilisation, non-exclusif et non cessible sur les logiciels, programmes, applications, le Manuel et autres modes d'emploi et plus généralement sur tous les documents mis à sa disposition par la Banque, dans le cadre du Service. Il est tenu de les utiliser dans le respect des prescriptions de la Banque. Il ne peut, sous quelque forme ou manière que ce soit, les mettre à disposition de tiers ou les copier, les décompiler, les adapter ou les altérer. Le Souscripteur est en outre tenu de respecter tous les droits de propriété, notamment intellectuelle, de la Banque, de son(ses) sous-traitant(s) et/ou fournisseur(s) éventuel(s) et de toute(s) autre(s) personne(s) concernée(s). L'Application E-Banking et le Site E-Banking de la Banque restent la propriété de la Banque ou de tiers qui ont accordé à la Banque une licence d'utilisation pour celle-ci.
- 11.5 Le Souscripteur est seul responsable de l'équipement informatique, y compris l'Appareil mobile, l'ordinateur, du matériel, des logiciels, du navigateur, des systèmes informatiques et de leurs extensions, qu'il utilise pour avoir accès au Service ainsi que de leur fonctionnement, de leur maintenance et de leur mise à jour. Le Souscripteur supporte seul les conséquences de leur non-fonctionnement ou de leur mauvais fonctionnement. Le Souscripteur choisit son fournisseur d'accès à Internet et de communication et supporte seul toutes les conséquences de ce choix. La Banque ne peut en aucun cas être tenue pour responsable d'un quelconque dommage causé par les services de ce fournisseur ou d'un dommage causé par d'éventuels problèmes de connexion du Souscripteur aux services fournis par ce tiers.
- 11.6 Le Souscripteur qui accède au Service 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. La Banque ne peut encourir aucune responsabilité en cas de défaillance des solutions d'authentification fournies par le fournisseur de la solution d'authentification choisie par le Souscripteur.

## ARTICLE 12 : OBLIGATIONS ET RESPONSABILITES DE LA BANQUE

- 12.1 La Banque :
- s'assure que les données de sécurité personnalisées ne sont pas accessibles à d'autres parties que le Souscripteur, sans préjudice des

- obligations de ce dernier à l'article 11 du présent Règlement ;
- s'engage à fournir au Souscripteur les moyens nécessaires à l'exécution, à tout moment, de la notification visée à l'article 11.3 du présent Règlement ou de demander le déblocage, par l'intermédiaire de LuxTrust dont les services peuvent être contactés conformément à ce qu'il est prévu à l'article 10.1, et à lui fournir, sur demande, pendant dix-huit mois à compter de la notification, les moyens lui permettant de prouver que celle-ci a été faite ;
  - à empêcher, dans la mesure des possibilités techniques, tout nouvel usage de l'Application E-Banking/du Site E-Banking/du Service aussitôt que le Souscripteur lui en a signalé la perte, le vol ou l'utilisation abusive ;
  - s'engage à assumer le risque lié à l'envoi au Souscripteur des Dispositifs et Données de sécurité personnalisée ou de tout moyen qui permet l'utilisation de l'Application E-Banking/du Site E-Banking/du Service.
- Pour le surplus, le régime de responsabilité décrit à l'article 78 des conditions générales est d'application.
- 12.2 S'agissant du Service, la Banque veille à maintenir des systèmes et programmes conformes aux développements technologiques récents. Elle met en œuvre des mesures appropriées pour assurer la sauvegarde de leur sécurité.
- Après plusieurs tentatives infructueuses de connexion à l'Application E-Banking/au Site E-Banking, l'accès au Service est bloqué pour des raisons de sécurité.
- 12.3 Sauf dol ou faute grave, la Banque ne peut pas être tenue pour responsable des dommages, directs ou indirects, que le Souscripteur ou un tiers pourraient subir, suite, notamment mais non limitativement :
- au non-respect par le Souscripteur de ses obligations en vertu du présent Règlement ou d'une quelconque législation ou disposition réglementaire ou contractuelle qui lui est applicable ;
  - à l'impossibilité de créer une connexion nécessaire à l'installation ou à l'utilisation du Service, aux interruptions de cette connexion, de quelque manière que ce soit, dans la mesure où elles sont dus à des tiers ;
  - au téléchargement, à l'utilisation ou à la suppression de l'Application E-Banking sur un Appareil mobile ;
  - de l'utilisation de l'Application E-Banking, du Site E-Banking, du Service, en dehors du territoire belge, notamment si cette utilisation s'avérait être incompatible, en tout ou en partie, avec la réglementation en vigueur sur le territoire où l'Application E-Banking et/ou le Site E-Banking et/ou le Service serait utilisé(e) par le Souscripteur ;
  - au mauvais fonctionnement de l'équipement du Souscripteur ou du service de télécommunications offert par un tiers ;
  - à une interruption du Service, à l'arrêt de celui-ci ou à son dysfonctionnement, pour quelque cause

- que ce soit ou si la régularité du Service était compromise en raison d'actes, d'erreurs ou de problèmes techniques, quelle que soit leur nature, leur origine ou leur cause, sur lesquelles la Banque n'a aucun contrôle direct.
- 12.4 L'adaptation par la Banque des caractéristiques ou des exigences techniques du Service ou encore des conditions et tarifs en vigueur ne peut en aucun cas donner lieu à une responsabilité dans le chef de la Banque à l'égard du Souscripteur.
- 12.5 Au vu des différents types de systèmes d'exploitation, browsers, logiciels de sécurisation et matériels informatiques disposant de configurations spécifiques, la Banque ne peut garantir que l'Application E-Banking et/ou le Site E-Banking pourra(ont) être utilisé(e)s ou fonctionnera(ont) de manière optimale sur tout appareil même doté d'un browser en principe compatible. La Banque ne peut par conséquent pas être tenue responsable si la configuration matérielle ou logicielle de l'Appareil mobile et/ou de tout autre appareil utilisé par le Souscripteur ne permet pas l'utilisation ou une utilisation optimale de l'Application E-Banking et/ou du Service.

#### ARTICLE 13 : TARIF ET FRAIS

- 13.1 L'accès au et l'usage du Service sont gratuits, tandis que la délivrance d'un nouveau certificat LuxTrust 'Signing Server' peut impliquer des frais, conformément à la liste des tarifs de la Banque. Dans le respect de la procédure décrite à l'article 15 du présent Règlement, la Banque peut à l'avenir soumettre l'accès et/ou l'usage du Service au paiement de frais. La Banque en informera le Souscripteur au moins deux mois avant l'entrée en vigueur de la modification, par écrit ou sur un support durable et approprié mis à la disposition du Souscripteur.
- 13.2 Tous les frais relatifs à l'équipement et au matériel informatique, au fonctionnement de ceux-ci, à l'accès Internet, ainsi que tous les coûts des télécommunications liés aux connexions effectuées dans le cadre du Service sont à charge du Souscripteur.

#### ARTICLE 14 : DUREE ET RESILIATION

- 14.1 La convention E-Banking relatif au Service est conclue pour une durée indéterminée.
- 14.2 Le Souscripteur peut mettre fin au contrat, à tout moment, sous réserve de ce qui est prévu à l'article 15 en cas de modification, en adressant une demande écrite à la Banque.
- La résiliation de l'accès au Service par le Souscripteur Titulaire de compte n'emporte pas de plein droit résiliation des accès conclus avec ses mandataires ou représentants.
- La résiliation de l'accès au Service par un mandataire ou représentant n'emporte pas résiliation de l'accès conclu avec le Souscripteur Titulaire de compte ni, le cas échéant, avec les autres mandataires ou représentants. Le Souscripteur Titulaire de compte a le droit de résilier l'accès d'un de ses mandataires ou représentants. Dans ces cas, le Souscripteur Titulaire de compte reste responsable solidairement et indivisiblement pour les opérations effectuées par ce

mandataire ou représentant jusqu'à la résiliation de cet accès.

- 14.3 La Banque peut mettre fin au contrat, à tout moment et moyennant le respect d'un préavis de deux mois donné par écrit.

Sans préjudice des dispositions légales impératives ou d'ordre public éventuellement applicables, la Banque peut également mettre fin à la convention, à tout moment et sans préavis, dans les cas repris à l'article 4.7 du présent Règlement, sans préjudice du droit de la Banque de prétendre à des dommages et intérêts.

- 14.4 La clôture de tous les Comptes liés met fin automatiquement à la convention E-Banking.

- 14.5 Dans l'hypothèse où le contrat a pris fin et où le Souscripteur n'a plus accès au Service, il s'engage à détruire tous les moyens d'authentification lui ayant été remis par la Banque.

#### ARTICLE 15 : MODIFICATIONS

La Banque se réserve le droit de modifier unilatéralement, à tout moment, le présent Règlement ainsi que les fonctionnalités du Service ou encore les frais comptés dans le cadre du Service.

La Banque en informera le Souscripteur au moins deux mois avant l'entrée en vigueur de la modification, par écrit ou sur un autre support durable et approprié mis à la disposition du Souscripteur.

Pendant ce délai, le Souscripteur a la faculté, en cas de désaccord sur les modifications proposées, de le notifier, par écrit, à la Banque avant l'entrée en vigueur de ladite modification. La notification de ce désaccord entraînera la résiliation de la convention. Cette résiliation a lieu sans frais pour le Souscripteur. A défaut de notification de son désaccord avant l'entrée en vigueur de ladite modification, le Souscripteur est réputé l'avoir acceptée.

#### ARTICLE 16 : TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

- 16.1 L'accès au Service implique le traitement par la Banque de données à caractère personnel du Souscripteur, à des fins d'exécution de la convention E-Banking et de gestion globale de la relation client et des services liés. Les informations recueillies à l'aide de la Demande d'accès aux Services E-Banking 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 au Service E-Banking, de la gestion des comptes et des opérations, ainsi que du contrôle de leur régularité.

En vue de l'exécution de la convention E-Banking ou du Règlement et de la fourniture du Service, la Banque transfère les données personnelles du Souscripteur à LuxTrust et/ou à tout autre fournisseur de la solution d'authentification choisie par celui-ci et reconnue par LuxTrust, qui procédera également dans ces contextes au traitement des données, auquel le Souscripteur donne son accord explicite. Le Souscripteur 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.

Pour le surplus, les informations relatives au traitement par la Banque des données à caractère personnel sont décrites dans la « Déclaration en matière de protection des données et de respect de la vie privée » (ci-après dénommée « Déclaration Vie Privée ») de la Banque. La Déclaration Vie Privée est disponible gratuitement, à tout moment, en français, sur le site Internet de la Banque ou auprès du siège social de la Banque. Le Souscripteur peut également en recevoir un exemplaire, gratuitement, à tout moment, sur simple demande.

- 16.2 La Banque n'utilise pas de cookies ou autres techniques similaires.

#### ARTICLE 17 : DISPOSITIONS DIVERSES

- 17.1 La nullité d'une ou de plusieurs dispositions de la convention E-Banking ou du Règlement n'affecte pas la validité des autres dispositions qui demeurent applicables.

- 17.2 Le Souscripteur ne peut céder à des tiers les droits et obligations décrits dans le présent Règlement ou dans la convention E-Banking. De telles cessions sont nulles.

#### ARTICLE 18 : RECLAMATIONS – PLAINTES

Les réclamations et plaintes peuvent être introduites conformément à ce qui est prévu dans les conditions générales de la Banque.

#### ARTICLE 19 : LIEU D'EXECUTION – LOCALISATION DES ECHANGES – DROIT APPLICABLE – TRIBUNAUX COMPETENTS

- 19.1 Le siège social de la Banque est le lieu d'exécution des obligations de la Banque envers le Souscripteur et du Souscripteur envers la Banque. Les communications établies entre la Banque et le Souscripteur ainsi que toutes les opérations initiées au travers du Service 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.

- 19.2 La convention E-Banking et le présent Règlement sont régis par le droit belge.

- 19.3 Le Souscripteur accepte la compétence exclusive des tribunaux belges.

#### ARTICLE 20 : ACCEPTATION DES CONDITIONS GENERALES LUXTRUST

- 20.1 Le Souscripteur 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 site [www.luxtrust.com](http://www.luxtrust.com)).

- 20.2 Le Souscripteur ayant opté pour un autre mode d'accès reconnu par LuxTrust, déclare avoir pris connaissance et approuver les conditions générales et toutes autres conditions de son fournisseur le liant et/ou liant la Banque à ce fournisseur dans le cadre de ce mode d'accès.



## Annexe – Internet et sécurité

La Banque met en œuvre toutes les mesures appropriées afin que son Application E-Banking et son Site E-Banking répondent à des normes de sécurité strictes.

Vous êtes également tenu, en tant qu'utilisateur du service E-Banking, de contribuer à sécuriser votre utilisation d'Internet. Vous trouverez ci-après quelques règles de base et bonnes pratiques à mettre en œuvre à cette fin.

### ► Que fait la Banque ?

L'Application E-Banking et le Site E-Banking de la Banque de la Banque répondent à des normes de sécurité strictes.

#### Connexion sécurisée

- > Lorsque vous vous connectez à l'Application E-Banking de la Banque ou au Site E-Banking de la Banque, la connexion est automatiquement sécurisée par LuxTrust ou tout autre fournisseur d'un moyen d'authentification reconnu par LuxTrust.

#### Blocage automatique

- > Après plusieurs essais infructueux pour vous connecter à l'Application E-Banking ou au Site E-Banking de la Banque via l'outil d'authentification, l'accès au service E-Banking est réinitialisé et vous devrez vous réenroller.

#### Déconnexion automatique

- > Vous êtes déconnecté automatiquement de votre session E-Banking après 15 minutes.
- > Si vous souhaitez vous reconnecter, il vous suffit de vous identifier à nouveau.

### ► Que pouvez-vous faire ?

#### Protégez votre Appareil mobile et votre ordinateur

- > Installez un **code de verrouillage** pour bloquer votre appareil lorsque vous ne l'utilisez pas et activez le verrouillage automatique de vos appareils lorsque ceux-ci sont inactifs (après 1 minute maximum). Si cela est possible activez un verrouillage temporaire de l'appareil après un certain nombre de tentatives échoués et prévoyez l'effacement automatique des données après un nombre excessif de tentatives d'accès.
- > Téléchargez uniquement nos applications via les sites officiels de votre système d'exploitation et utilisez uniquement des applications et des programmes sûrs. N'installez que des applications qui proviennent de plateformes de téléchargement fiable (telle que Google Play Store, Apple Store) ou d'un fournisseur officiel. Utilisez des sites intermédiaires augmente le risque d'être touché par un virus.
- > Limitez les accès autorisés à vos applications au strict nécessaire et activez l'accès au Wi-Fi, au Bluetooth, aux données mobiles, etc. uniquement lorsque cela est nécessaire. N'optez pas pour les fonctions d'activation automatique.
- > Veillez à supprimer les applications que vous n'utilisez pas et vérifiez régulièrement les données exploitées par vos applications.
- > Gardez les logiciels et les applications de votre Appareil mobile et de votre ordinateur toujours à jour.
- > Installez un programme **anti-virus**, un programme **anti-spyware** ainsi qu'un filtre **anti-spam** fiables. Après l'installation de ces programmes, veillez à ce qu'ils soient actifs lorsque vous utilisez votre Appareil mobile et votre ordinateur. Procédez régulièrement à une mise à jour de ces programmes et effectuez régulièrement un scan complet de votre Appareil mobile et de votre ordinateur.
- > Installez et activez un **pare-feu (firewall)** sur votre Appareil mobile et sur votre ordinateur afin de contrôler les flux d'informations entrants et sortants. Après l'installation de ce programme, veillez à ce qu'il soit actif lorsque vous utilisez votre Appareil mobile et votre ordinateur. Procédez régulièrement à une mise à jour de ce programme.
- > Si vous utilisez un réseau local (plusieurs Appareils mobiles, ordinateurs sur une même connexion Internet), veillez à sécuriser celui-ci de manière suffisante, de façon à contrôler l'échange d'informations entre tous les appareils (ordinateurs, imprimantes, etc.) qui sont connectés à votre réseau. Protégez chaque appareil séparément.

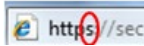

- > Installez les dernières mises à jour de votre système d'exploitation (IOS, Android, etc.) sur votre Appareil mobile et sur votre ordinateur.
- > Utilisez toujours la version la plus récente de votre navigateur (Internet Explorer, Firefox, etc.). Procédez systématiquement à toutes les mises à jour de sécurité.
- > Si vous utilisez une connexion sans fil (WiFi), veillez à sécuriser votre connexion pour empêcher les personnes se trouvant à proximité de l'utiliser à votre insu. Modifiez les mots de passe fournis avec le matériel et le nom du réseau (SSID). Utilisez un système de cryptage des données WPA2.
- > Assurez-vous de l'origine d'un programme avant de l'installer sur votre Appareil mobile et sur votre ordinateur. Soyez particulièrement attentif si vous partagez votre Appareil mobile et votre ordinateur avec vos proches.
- > Réinitialisez votre Appareil mobile et votre ordinateur si vous le vendez.

## Utilisez E-Banking de manière vigilante et responsable

### Préservez la confidentialité de vos données d'identification

- > Lorsque vous choisissez votre nouveau mot de passe, évitez les combinaisons trop évidentes (par exemple, une partie de votre date de naissance, celle de votre conjoint ou de vos enfants, une partie de votre numéro de téléphone, votre code postal, etc.) et modifiez régulièrement votre mot de passe.
- > L'accès et l'utilisation du service E-Banking sont strictement personnels. Vos données d'identification doivent rester confidentielles. Ne les communiquez à personne (même s'il s'agit de votre conjoint, d'un membre de votre famille ou d'une connaissance en qui vous avez confiance). Ni la Banque, ni LuxTrust ne vous demandera jamais de communiquer vos données d'identification (User-ID, identifiant, mot de passe, etc.), par courrier, par téléphone, par courriel, par SMS, par un message pop-up ou par tout autre moyen de communication. Toutefois, si vous prenez contact avec le service d'assistance technique de la Banque (au +32 (0)2 626 02 70) ou de LuxTrust (au +352 24 550 550), il est probable que l'on vous demande le User-ID. Veillez à ne communiquer cette information que lorsque vous avez-vous-même contacté la Banque. Ne communiquez jamais, d'identifiant, de code, mot de passe ou vos données d'identification si quelqu'un vous appelle, vous contacte par courriel, par courrier, par SMS ou par tout autre moyen de communication. Ne répondez en aucun cas à ce type de demande et avertissez le plus vite possible notre service d'assistance technique.
- > Lorsque vous vous connectez à l'application E-Banking ou au site E-Banking, composez votre mot de passe à l'abri des regards indiscrets.

### Vérifiez l'authenticité du site Internet auquel vous vous connectez

- > Lorsque vous souhaitez vous connecter au site sécurisé de Banque Transatlantique Belgium, veillez à saisir vous-même l'adresse du site et à vérifier que celle-ci ne comporte pas d'erreur dans votre browser ou cliquez sur le bouton « Login » / « Espace client » du site public <http://www.banquetransatlantique.be>. Ne cliquez pas directement sur un lien contenu dans un courrier électronique ou un SMS ou tout autre moyen de communication pour accéder au site sécurisé de Banque Transatlantique Belgium.
- > Lorsque vous vous connectez au site sécurisé de Banque Transatlantique Belgium, vous pouvez aisément vérifier que vous êtes en connexion avec le véritable site sécurisé de la banque de la manière suivante :
  - vérifiez si l'URL est correct et commence par « https:// »  et non « http:// » (<https://secure.banquetransatlantique.be/signin>).
  - vérifiez la présence de l'icône représentant un cadenas  (= connexion sécurisée) dans votre navigateur en bas à droite de la page Internet ou en haut de la page si votre navigateur est récent. Cela signifie qu'un certificat de sécurité a été envoyé à votre ordinateur et que vous êtes seul à avoir accès aux informations que vous envoyez ou que vous recevez. En cliquant sur le cadenas, vous pouvez visualiser les données du certificat.
  - vérifiez que la procédure de login se déroule normalement.

Si vous rencontrez des problèmes ou des irrégularités durant votre connexion ou votre session ou si votre session se déroule de manière inhabituelle (un écran d'attente apparaît subitement, une demande, prétendument pour des raisons de sécurité, de vous identifier une seconde fois, des écrans rédigés dans une autre langue que celle de vos sessions habituelles, ...), fermez immédiatement votre session et prenez contact le plus rapidement possible avec notre service d'assistance technique au +32 (0)2 626 02 70, tous les jours ouvrables de 9h00 à 17h00.

### Soyez également attentif à

- > vérifier dès réception vos relevés d'opérations ainsi que vos relevés estimatifs et signalez immédiatement à la Banque toute transaction suspecte.
- > ne pas laisser pas votre Appareil mobile et votre ordinateur sans surveillance alors que vous êtes connecté sur l'Application E-Banking de la Banque ou sur son Site E-Banking.
- > vous assurer de mettre fin à la connexion au service E-Banking après avoir effectué les opérations souhaitées ; il doit être mis fin à la connexion par l'utilisation de l'onglet de déconnexion prévu à cet effet.
- > clôturer votre session en vous déconnectant.
- > éviter les logiciels inconnus. La Banque ne vous demandera jamais de télécharger un logiciel par courriel ou par SMS.

### **Soyez un utilisateur vigilant et responsable d'Internet**

- > Ne communiquez pas d'informations personnelles et confidentielles sur un site marchand ou sur un site bancaire sans avoir préalablement vérifié que le site est sécurisé.
- > Ne divulguez pas d'informations personnelles sur des forums ou sur les réseaux sociaux, pour éviter spam et usurpation d'identité.
- > Ne surfez que sur des sites Internet fiables et ne téléchargez pas de fichiers ni de programmes sur des sites Internet inconnus ou suspects. Faites aussi toujours attention lors de l'ouverture d'un fichier ou d'un programme inconnu ou lorsque vous cliquez sur certains liens.
- > N'ouvrez pas les e-mails provenant d'expéditeurs inconnus. En cas de doute quant à l'origine d'un e-mail, supprimez le message sans l'avoir lu.
- > Ne répondez jamais aux messages non sollicités ni aux courriels suspects dans lesquels on vous promet que vous allez recevoir de l'argent sur votre compte ou qui vous promettent des gains, ou encore que vous devez conserver une somme pour des inconnus.

### **Que faire en cas de perte ou de vol, de détournement, d'utilisation abusive ou non autorisée de vos moyens d'accès, dispositifs et données de sécurité personnalisés au service E-Banking ou si vous soupçonnez une fraude ou un abus ?**

- > Prenez contact le plus rapidement possible avec le Service Desk de LuxTrust par téléphone au +352 24 550 550 ou par e-mail sur [helpdesk@luxtrust.lu](mailto:helpdesk@luxtrust.lu). Les agents de LuxTrust sont disponibles du lundi au vendredi de 8h à 18h (service révocation et déblocage des cartes disponible 24/7) ou le service d'assistance technique de la Banque, par téléphone, au +32 (0)2 626 02 70, tous les jours ouvrables de 9h00 à 17h00.
- > Déclarez la perte ou le vol dans les 24 heures aux services de police compétents.

### **Que faire si vous avez reçu un avis de phishing ?**

Vous avez reçu un mail suspect dans lequel on vous demande de communiquer ou de confirmer vos données d'identification prenez contact le plus rapidement possible, avec le Service Desk de LuxTrust par téléphone au +352 24 550 550 ou par e-mail sur [helpdesk@luxtrust.lu](mailto:helpdesk@luxtrust.lu). Les agents de LuxTrust sont disponibles du lundi au vendredi de 8h à 18h (service révocation et déblocage disponible 24/7) ou le le service d'assistance technique de la Banque, par téléphone, au +32 (0)2 626 02 70, tous les jours ouvrables de 9h00 à 17h00. Conservez soigneusement le message de phishing et transmettez-le à la Banque.

D'autres conseils et informations sont disponibles sur :

- > le site Internet Safeonweb : <https://safeonweb.be> et sur l'application Safeonweb (disponible sur les plateformes de téléchargement d'applications en ligne, Apple Store ou Google Play)  
  
Le portail Safeonweb du gouvernement pour objectif d'informer rapidement et efficacement les citoyens belges en matière de sécurité informatique, des plus récentes et plus importantes menaces numériques et de sécurité sur Internet.  
  
L'application Safeonweb, entièrement gratuite, vous avertit des cybermenaces et escroqueries en ligne.
- > le site Internet de Febelfin dédié à la sécurité de la banque par Internet : [www.safeinternetbanking.be](http://www.safeinternetbanking.be).

**Pour toute question, n'hésitez pas à contacter notre service d'assistance technique, par téléphone, au numéro suivant +32 (0)2 626 02 70, tous les jours ouvrables de 9h00 à 17h00.**