Terms and conditions for accessing and using the E-Banking (online banking) Services – individuals

The undersigned (hereinafter the "Client") requests E-Banking (online banking) access to one or more of their account(s) (hereinafter "Accounts Available Online") held at Banque de Luxembourg (hereinafter the "Bank") on which they have individual signatory power either as account holder, representative or attorney.

1. Scope

In accordance with this agreement, the parties hereby agree on the terms and conditions of accessing and using the services offered via the Bank's E-Banking (online banking) website and/or the BL-Mobile Banking app (hereinafter the "E-Banking Services"), as well as the conditions governing the provision of proof of trading and transactions carried out. These Terms and Conditions for accessing and using the E-Banking Services shall not create any new information or advisory obligation, nor do they constitute a new mandate under the responsibility of the Bank.

The Bank's E-Banking Services offer the following features in particular:

- Presentation of the Bank, its products and services,
- Market information,
- Financial research and analysis,
- Consulting Accounts Available Online,
- Online trading,
- Electronic communication,
- Viewing and generating documents,
- Entering/modifying personal data.

Some of the functionalities mentioned above may be exclusive or may appear different on the E-Banking space or in the BL-Mobile Banking app

The Bank reserves the right to modify these services at any time.

2. Fees and charges

Access to the E-Banking Services is invoiced according to the Bank's applicable charges. The Client hereby confirms that they have been informed of and accept such charges. Other charges, such as internet subscription (via an internet service provider), telephone communications or any other charges shall be borne by the Client.

3. Security of the E-Banking Services

In order to access the E-Banking Services, the Client shall ensure that they have internet access through the internet service provider of their choice. The Bank accepts no liability with regard to the Client's internet connection, which shall be exclusively at the Client's own risk.

Access to the E-Banking Services shall be arranged by communicating an address to the Client together with their identifiers and any other address that the Bank provides to the Client by whatever means it deems appropriate, including electronically.

The Client shall receive an envelope from LuxTrust containing the identifiers that correspond to their choice of access in order to enable them to connect to the E-Banking Services, to identify themselves and sign instructions.

Where applicable, any device to be used for authentication purposes shall be provided or sent in a separate envelope.

Any sharing of identifiers and, where applicable, the device used for authentication purposes shall be at the Client's own risk.

The Client expressly authorises the Bank and LuxTrust to supply identifiers for access to the E-Banking Services to current or future attorneys and representatives who have signatory authority on the Accounts Available Online when such persons request access.

The Client undertakes to protect all identifiers and to take security measures to maintain sole control over their access authentication modes (identifier, password, one-time password) which shall be known only to them. The Client shall be solely responsible for ensuring that their personal codes are kept strictly confidential.

The Bank particularly draws the Client's attention to the fact that it will never ask them by email for confidential information (password, one-time password or bank card number) or to invite them to connect to the E-Banking Services via a link in an email.

The Client should therefore consider as suspect any unsolicited email that claims to come from the Bank asking them to communicate bank details and/or their password. In addition, the Bank recommends that the Client manually enters the address www.banquedeluxembourg.com and checks that there are no spelling mistakes when they have finished instead of clicking on a link contained in an email.

The Client acknowledges that saving any of this information on one or more computers shall also be at their own risk. Should the Client become aware or suspect that a third party is trying to gain access to the E-Banking Services using any of these codes, they shall immediately inform the Bank, which shall block such access.

Access to the E-Banking Services is protected by a ciphering and identification process.

The Client acknowledges that the Bank has provided all the necessary information concerning the security, efficiency and restrictions of this process. They accept as satisfying and formally discharges the Bank from any liability concerning the consequences of any breach of the security system by an unauthorised third party. They also authorise the Bank to modify the practical and technical workings of the E-Banking Services, and, in particular, the security system that offers access to the E-Banking Services, particularly in the event of any upgrades or technological improvements. The Client shall be informed of such improvements by any means deemed appropriate by the Bank.

The Client undertakes to strictly comply with the procedures for connecting to the E-Banking Services, as explained by the Bank, as well as any instructions for use displayed via the E-Banking Services or communicated to the Client by any other means. They undertake to check the secure character of the communication at each connection. In the event of this procedure not being observed and/or of any other instruction for use being ignored, e.g. attempts to connect to the E-Banking Services using an incorrect identifier, the Bank reserves the right to prevent the Client from further attempts to access the E-Banking Services.

The parties mutually agree that access to the E-Banking Services using one of the Client's identifiers shall be deemed to be made by the Client, with the Bank's connection log serving as proof thereof.

In addition, each connection to the E-Banking Services by an attorney or a representative of the Client using their identifier shall be deemed to have been made by that attorney or representative in the name of and on behalf of the Client.

The Bank accepts no liability and will not be blamed for any breach of secrecy should a third party access the

Client's Accounts Available Online or gain any other kind of information as to their relationship with the Bank via the E-Banking Services and/or the BL Mobile Banking application or the internet.

4. Information accessible via the E-Banking Services

The Client may use the E-Banking Services to consult financial and economic information offered by the Bank as well as other parties, notably about the financial markets and investment funds.

In so far as possible the Bank shall display the date of publication or creation of the information on the E-Banking Services and undertakes to keep this information as up-to-date as its paper-based information.

All information published via the E-Banking Services is provided for information purposes only and should not be interpreted as advice or guidance from the Bank. The Client undertakes to use the information with proper judgement and a critical eye.

The Client expressly releases the Bank from any liability relating to the content, reliability, timeliness, integrity or accuracy of information from a third party and indicated as such.

The Client expressly acknowledges that no advice shall be given online by the Bank with regard to information published via the E-Banking Services, and undertakes to obtain advice relating to their investments and portfolio management directly from an adviser of their choice at the Bank.

The Client undertakes to respect the confidential nature of the information available via the E-Banking Services and to refrain from passing this information to a third party, from publishing or disseminating it by any means or for whatever reason, and from reproducing the E-Banking Services in part or in full. Notwithstanding any written information to the contrary, the Client authorises the Bank to send them any promotional material via the E-Banking Services or by email.

5. Consulting Accounts Available Online

The Client may consult the Accounts Available Online via the E-Banking Services as well as pending trades on these accounts, where applicable. The Client authorises the Bank to send them information online about the Accounts Available Online as well as operations on these accounts. This does not affect any agreements that the Client may have with the Bank pertaining to correspondence to be held at the Bank's premises on behalf of the Client.

If the Client has opted to consult their Accounts Available Online (of which they are the account holder or representative) solely via the E-Banking Services, they shall undertake to consult these accounts at least once per quarter. Failing this, the Bank shall forward them a bank statement for the Accounts Available Online. In such a case, the Client shall be liable for any costs relating to this.

If the Client has not consulted their Accounts Available Online for a continuous period of six months, the Bank shall revoke their access to the E-Banking Services and shall forward to the Client any account statements and correspondence relating to the Accounts Available Online to the address provided in the account-opening application form or other address provided by the Client. In such a case, the Client shall be liable for any costs relating to this.

The Bank reserves the right to deny the Client access to one or more of their Accounts Available Online via the E-Banking Services if it deems it has valid reason to do so.

6. Electronic Orders

The Client may use the E-Banking Services to submit to the Bank orders for credit transfers and trades on financial instruments (hereinafter "Electronic Orders") that will be executed according to the same conditions applied to their other orders.

Electronic Orders are presumed to be instructed for execution and/or for reception and transmission as execution-only, referred to in Article 12 of the General Terms and Conditions of the Bank.

With regard to Electronic Orders submitted to the Bank, the Client undertakes to provide the specific information required for the proper execution of that order.

The Bank will display the information that the Client has entered on screen.

The Client shall be responsible for all orders signed off using their identifiers until the Bank receives notice from the Client not to trust such orders and the Bank is in a position to refuse such orders.

The parties acknowledge that Electronic Orders shall have the probative value of a private agreement in accordance with articles 1322 et seq. of the Civil Code, and that opposition may be made to the Client or the Bank regardless of the amount.

The Bank undertakes to keep a log of all the Electronic Orders signed by the Client on a durable medium and for a period of 10 years, while ensuring that the records remain unchanged. The Client expressly agrees that the records of their Electronic Orders kept by the Bank shall be proof of their existence, content, and precise date and time, and that these details be valid before a court of law. The Bank shall keep a copy of all these records at the Client's disposal.

7. Processing and protection of personal data

In order to grant access to the E-Banking Services, the Bank will need to process the personal data of the Client for the purposes of executing this contract and managing the client relationship and any related services.

The information collected by means of this document may be stored on any medium and saved by the Bank in a computer file, and processed for the purposes of authenticating and managing access to the E-Banking Services, managing accounts and transactions, and ensuring that they are authorised.

In order to meet its regulatory obligations, particularly with regard to anti-money laundering and anti-terrorist financing legislation, the Bank may have to verify the authenticity of the data provided by the Client and transfer this data to the public authorities and competent courts.

The Bank may store personal data for a period not to exceed that necessary for its purposes, and in accordance with its General Terms and Conditions.

Within the framework of executing this contract and the provision of the E-Banking Services, the Bank transfers the personal data collected in this document to LuxTrust, which will also process the data in this framework. The Client has the right to request access to, rectify or delete their personal

data, the right to data portability, and the right to object to or restrict its processing.

The Client may consult and/or modify their personal data via the E-Banking Services. The Client requests that any changes notified accordingly to the Bank be considered in the same way as any other notification of a change in personal data.

The Client undertakes to provide correct and accurate information to the Bank, to inform the Bank as soon as possible of any change in their personal information, and to communicate on request any document or additional information that the Bank deems necessary within the framework of the banking relationship or that may be required by legal or regulatory provisions.

8. Accessibility of the E-Banking Services

The Bank shall reserve the right to temporarily suspend access to the E-Banking Services, particularly for technical reasons.

Should the Bank expect that access to the E-Banking Services may become temporarily unavailable, it will make every effort to give the Client advance notice, using all appropriate means, including a message displayed via the E-Banking Services.

The Client discharges the Bank from any liability arising from the temporary inability to access the E-Banking Services, for whatever reason, and from consequences arising from a breakdown or malfunction of the E-Banking Services, from the Bank's IT infrastructure, from the E-Banking Services being disconnected or from any other technical incident, even in case this is through the fault of the Bank.

The Bank reserves the right to block or permanently withdraw the Client's access rights to the E-Banking Services, should the Client fail to comply with their obligations or the Bank's recommendations, or in the event that the Bank considers it prudent to prevent the Client from gaining access for any other reason.

9. Message confidentiality

The parties acknowledge that messages sent using the E-Banking Services shall be confidential in nature.

10. Place of communication

Communications between the Bank and the Client, as well as any operations initiated or completed using the E-Banking Services shall be considered as having been conducted at the Bank, at the date and time indicated on the Bank server and confirmed by the Bank's connection log.

11. Destruction of identifiers and certificates

In the event that the Client no longer has access to their Accounts Available Online via the E-Banking Services, they undertake to destroy all identifiers provided by the Bank.

12. Liability

In its role as E-Banking Services provider, the Bank's responsibility shall only extend to due diligence and best efforts with regards to the Client. In accordance with article 21 of the Bank's General Terms and Conditions, the Bank shall only be liable for gross negligence.

Should the Client access the E-Banking Services in another country, they undertake to abide by the legal regulations and requirements in force in the country in which the access takes place.

13. Amendment to Terms and Conditions of accessing and using the E-Banking Services

The Bank may amend these Terms and Conditions at any time by means of a written notification informing the Client of regulatory changes or changes in legislation, market practices, the market situation and the Bank's policy.

The Bank reserves the right to notify the Client of amendments to these Terms and Conditions at any time and by any means, including via a message sent by or displayed on the E-Banking Services.

Such amendments shall be considered approved if the Client raises no objection in writing.

Any objection must be received by the Bank within 30 days of the notification being received.

Should any of the clauses of these Terms and Conditions of accessing and using the E-Banking Services become inapplicable or void, this shall not affect the validity of the other clauses which shall remain in force unless any of their provisions are rescinded.

14. Acceptance of the LuxTrust general terms and conditions.

Clients having opted for the LuxTrust access mode state that they are aware and approve of the LuxTrust general terms and conditions and any other terms and conditions binding them or the Bank to LuxTrust, with regards to the access mode. Please check www.luxtrust.lu for more information.

Appendix: Notice concerning the risks inherent to credit transfers made via the E-Banking (online banking) Services

Notice concerning the risks inherent to credit transfers made via online banking on the E-Banking website

This notice is intended to provide a non-exhaustive list of some of the risks involved in electronic credit transfers.

"Phishing"

"Phishing" is a technique used by online fraudsters (scammers), pretending to represent the Bank in a bid to collect personal details about clients.

email phishing:

This is a technique that **computer hackers use to mimic emails or institutional websites to collect confidential data.** The victim receives a scam email from a bank or official organisation. The messages pretend that a technical upgrade of the bank's website is needed or that your personal details need to be verified. By clicking on a link in the message, the victim is redirected to a site mimicking the bank's official website and then invited to enter their ID and personal passwords.

The emails may also consist of emails about fictitious lotteries, informing the victim that they have won. In order to pay out the winnings, the scammers request the victims' personal banking details.

Some emails seek the victim's assistance in order to transfer funds. The sender will ask to use the victim's account for the transmission of a very large sum, promising a percentage. The requests are scams and should be ignored.

phone phishing :

The victim receives a phone call from someone pretending to represent the bank. This person explains that, due to technical problems, the victim's account will have to be closed if they do not communicate certain personal details such as their bank account number and password.

Identity theft

A malevolent person knowingly uses the identity of another person in order to carry out fraudulent actions.

To use someone else's identity, a scammer needs to have obtained in advance the personal and confidential information of the scam victim.

Identity theft can have serious consequences including the constitution of false papers, use of bank accounts and execution of fraudulent transactions.

For example, by stealing your email address, the fraudster has access to all your emails and can write to your contacts using your email address and your style of communicating and betray the trust of those close to you.

Malware

Malware is a computer program developed to intentionally harm a computer system, or collect data without the user's knowledge.

It comes in many forms: **viruses, worms or Trojan horses** are the most widely known examples (a virus is installed when you access a hacked website and, for example, it collects details of the keys that are pressed and then automatically transfers these to the fraudsters). Such programs are becoming increasingly sophisticated with advances in technology.

What can you do to reduce risk?
Review of best security practices on the internet

Never tell anyone your password or your personal ID!

The Bank will never contact you by email to ask you for your usernames, passwords, OTPs (one-time passwords) or any other form of confidential information.
The Bank never asks its clients for their access codes (passwords, OTPs, etc.) by email, phone or any other means of communication.

How can I protect my password?

Choose a secure password (composed of at least 8 characters, including numbers and special characters) and change it regularly. Use different passwords for every website you visit (online banking access to other banks' online banking, email, online shopping, social networks, forums, etc.).

How can I protect my computer?

To protect your E-Banking (online banking) access, always use a computer you trust and know is secure; avoid public computers.

We recommend that you:
– install antivirus and antispyware software on your computer which update automatically on a regular basis
– install recent updates of your operating system and internet browser
– only install trustworthy programs
– activate the firewall.

How can I check that I really am on the Bank's online banking website?

Go to the Bank's website by entering http://www.banquedeluxembourg.com in the address bar of your internet browser, or from your Favourites if you have previously
saved it there.

– Click on "MY ACCOUNT ONLINE" then select your authentication mode:
– Check that the address starts with "https"
– Check that there is a padlock symbol at the bottom and/or top of the secure page and that the padlock is closed
– Double-click on the padlock
– A screen representing the Bank's digital certificate appears
– Check that the name on the certificate actually says "BANQUEDELUXEMBOURG.COM"

How can I log off securely and check when I last connected to the online banking site?

After checking your accounts online, always terminate the connection on your personal area of the E-Banking Services using the "Logout" button and close the window of your browser. The date and time of your last connection using your ID are shown under the log out button. Remember to check movements on your accounts.

How can I protect against phishing?

This is a technique that computer hackers use to mimic emails or institutional websites to collect confidential data such as your credit card number, ID, password, name, first name, date of birth, address, phone number, etc.

In most cases, this scam uses fake emails from banks or official organisations. The messages use the pretext of a technical upgrade of the site in question or say that your personal details need to be verified. By clicking on a link contained in the email, you are redirected to a site that mimics the institutional site and invited to enter your personal data. To protect against phishing, be vigilant concerning any such message or call, its content, and the address of the sender. Remember that the Bank and other financial institutions in general will never ask a client for their password, ID or OTP by email or phone.

What can I do if I've lost my access codes and who can I contact if I have a question?

If you have lost your access codes, please contact LuxTrust as soon as possible (www.luxtrust.lu). For any other questions regarding your account or problems the BL Mobile Banking application, please telephone BL-Support (+352) 26 20 26 30, open Monday to Friday from 9am to 6pm.