E-Banking Terms of Use

1. Services and definitions

Union Bank AG ("Bank") offers its contracting partners ("Client" or "Accountholder") use of E-Banking. E-Banking includes various electronic bank services described in the "E-Banking Agreement". The Bank may change this range of services at any time. It will so notify the Client in the form agreed with the Client.

The E-Banking Agreement and these E-Banking Terms of Use ("Terms of Use") as well as the E-Banking security guidelines published on the Internet in the most recent form in effect shall collectively constitute the agreement between the Bank and the Client governing the use of E-Banking.

The data exchange by E-Banking specified in the following relates to banking transactions that are specified in separate form. In the event of any inconsistencies between the following regulations governing the use of E-Banking and those in separate form, the regulations contained herein shall have priority.

The "E-Banking User" ("User") shall be any individual acting for the Client, whether the Accountholder personally or any authorised agent of the Accountholder. One E-Banking Agreement must be signed for each User. An "authorised agent" shall be any party who has been duly authorised in relation to the Bank by the Accountholder by means of a "Signature and Power of Attorney Card" or by another form acceptable to the Bank.

2. Access to E-Banking

Technically, E-Banking is accessed via the Internet through an Internet provider selected by the User and a standard Internet browser. Information on the individual steps for logging in can be found in the E-Banking Security Guidelines below.

Any person who logs in in the manner provided for, and who has thus completed self-authentication, shall be deemed by the Bank as authorised to use the contractually agreed E-Banking services. All instructions, orders and communications transmitted to the Bank via E-Banking shall be deemed to have been drawn up and authorised by the Client. The Bank may allow any E-Banking User to make enquiries within the framework and scope of the agreed authorisations without any further check. The Bank will accept orders, instructions and legally-binding communications transmitted using the E-Banking mailbox function (secure mail), provided that a corresponding agreement with respect to is-suing orders by e-mail is available and the relevant User is authorised to issue instructions to the Bank. This shall apply regardless of the legal relationship between the User and the Client, and irrespective of any commercial register extracts or equivalent documents specifying otherwise.

The Bank shall have the right to decline the provision of information or the receipt of instructions, orders and communications by Internet at any time without having to provide reasons, and to insist that Users identify themselves in another manner, such as by way of signature.

The Client shall ensure that all Users are informed about the use of E-Banking and that they receive proper instructions. If necessary, the Client shall ensure that such Users are bound by the relevant contractual obligations and shall monitor the Users as far as the Client believes necessary. The Client shall be exclusively liable for any damage or loss incurred as a result of any failure to comply with these obligations.

3. Duty of care on the part of the User

The User shall be required to change the first password provided to him by the Bank immediately following receipt. Authentication information such as password shall be kept confidential and protected against misuse by unauthorised persons. This duty shall apply to each User individually. The Bank shall have no liability for the misuse by any User of the authentication information of another User.

If there is any risk that an unauthorised third party has gained knowledge of the password of a User, the password must be changed immediately. In the event of any danger of misuse of a password, the User shall immediately block his E-Banking access by the Bank.

The Client shall be solely liable for all consequences arising from any regular use or any misuse of his own authentication information or that of other authorised Users.

LI 9440 Vaduz Austrasse 46 P.O.Box 1535 T +423 239 35 35 F +423 239 35 37 info@unionbankag.com
HR FL-0002.303.567-3 MwSt.-Nummer 57173 IBAN: CH3208710035330142001 SWIFT: UNIVLI22

4. Blocking access

Any User may have his own access to E-Banking blocked at any time. In addition, the Accountholder or any authorised signatory or authorised person may have access by any of the others to E-Banking blocked. The latter shall not apply to Users who only hold a limited power of attorney to deal with the Bank.

The User may request a block from his Client advisor by telephone during normal business hours. Any such request must be promptly confirmed to the Bank in writing.

Any written revocation of a power of attorney or signing authority provided to the Bank in writing will also result in a block of the relevant E-Banking access.

5. Issuing orders

The issue of payment orders within E-Banking is subject to the agreements concluded between the Bank and the Client.

The transmission of orders by way of the E-Banking mailbox function shall be subject to the agreements made between the Client and the Bank and shall require, in particular, execution of the form specifically created for the issuing orders by way of electronic communication (email). Additionally, any time-critical orders must be communicated to the Client advisor by telephone in good time. The Bank assumes no liability for any orders, communicated by way of E-Banking mailbox only, not being executed on time, nor does it accept liability for any damage or loss arising as a result.

6. Order execution

Payment orders will be executed by the Bank in case of the sufficient balance of the account. Payment orders which are placed within the E-Banking after 1 pm CET, will be executed on the next banking day.

The Bank reserves the right to clarify the purpose of the received payment order with the Client / Authorised agent prior to the execution of the payment order and to request appropriate documentation and to reject the execution, if necessary.

7. Electronic bank statements

For information purposes, all banking statements will be available to the Client in electronic form through E-Banking. The existing correspondence instructions given by the Client to the Bank shall remain unchanged.

Delivery of the bank statements in accordance with correspondence instructions, i.e. by post or in accordance with the provisions governing the retention of correspondence (hold mail), shall apply in respect of legally-effective delivery and the commencement of any deadline periods. In the event of any conflict, the bank statements delivered to the Client in accordance with the Client's instructions respecting correspondence shall take precedence.

8. Security

Security shall be governed by the E-Banking Security Guidelines below.

9. Exclusion of liability on the part of the Bank

The Bank accepts no responsibility for the accuracy or completeness of any information rendered accessible through E-Banking, or for whether such information is up-to-date. In particular, information on accounts and custody accounts, as well as market data, shall not be binding. Only the information contained in the documents physically produced by the Bank and sent to the Client in accordance with the Client's instructions regarding correspondence will be legally binding.

Users shall be responsible for their secure technical access to the services provided by the Bank. The Bank accepts no responsibility for Internet providers.

E-Banking communication occurs through the Internet, a network of telecommunications facilities that is accessible to anyone and not in receipt of any special protection. The Bank accepts no liability for any damage or loss incurred by the User as a result of transmission errors, technical defects, disruptions, illegal interference with network installations, network overload, malicious blockage of electronic access by third parties, any Internet malfunction, interruptions or the like or other shortcomings on the part of network providers.

In spite of all security measures, the Bank cannot accept any responsibility for the User's computer as this is not possible from a technical perspective. The Client agrees and accepts that the computer of each User may present a security risk.

When exercising the customary level of care, the Bank shall not be liable for any consequences incurred as a result of malfunctions and interruptions in the operation of E-Banking.

In order to identify and eliminate security risks, the Bank reserves the right to interrupt E-Banking services at any time without notice for the protection of the Client. The Bank accepts no liability for any damage or loss resulting from any such interruption.

The Bank accepts no liability for any loss or damage incurred by the Client as a result of non-performance of contractual obligations, nor for any indirect or consequential losses such as lost profits or claims by third parties.

The Bank assumes no liability for any loss or damage caused by slight negligence on the part of auxiliary staff in the performance of their duties.

10. Bank-client confidentiality

Information, in particular client data, as well as information on transactions conducted by the Client, will be transferred via public and private transmission media. Transmission often occurs through several countries.

Data transmitted via E-Banking is encrypted in accordance with the currently applicable standards. You can find more information on this in the E-Banking Security Guidelines below.

The Client expressly acknowledges and accepts that the application of Liechtenstein bank-client confidentiality and the Liechtenstein data protection provisions is limited to data located in Liechtenstein. Even if the sender and recipient of transmitted data are domiciled in Liechtenstein, data are transmit-ted through third countries, as a rule, and are then no longer governed by these provisions.

11. E-Banking restrictions for certain persons

The range of financial services for Users of E-Banking may be subject to local restrictions. If the Bank does not hold the required local licences, the scope of E-Banking services may be adapted or restricted for such Users at any time and without notice.

The use of E-Banking for accountholders with the status of a "US person" or some Users with domicile in the USA is currently excluded.

12. Proviso in respect of legal regulations

Legal provisions as well as the requirements of the Liechtenstein financial market regulatory authority FMA that govern the use of the Internet and services offered by the Bank within the framework of E-Banking shall have priority over any contractual agreements between the Bank and the Client and shall apply from the date of entry into force.

13. Amendments to the Terms of Use

The Bank may amend these Terms of Use at any time. The Bank will notify the Client of any such amendment in the manner agreed with the Bank by the Client, and any amendment shall be deemed to have been accepted within one month of such notice unless contested in writing.

14. Termination

The E-Banking Agreement including the Terms of Use and the E-Banking Security Requirements in their respective forms shall apply for an unlimited period. The E-Banking Agreement may be terminated by the Bank or the Client at any time in writing and with immediate effect, without the Bank or the Client having to provide reasons.

15. Severability

The invalidity, illegality or unenforceability of one of more provisions of this Agreement shall not affect the validity of the other parts of the E-Banking Agreement.

16. Applicable law and place of jurisdiction

All legal relations with the Bank shall be governed by Liechtenstein law. The exclusive place of jurisdiction for all proceedings, as well as exclusive place of performance, shall be Vaduz. The Bank shall also be entitled to take legal action against the Client before any other competent court.

ANNEX: E-BANKING SECURITY GUIDELINES

In connection with the use of E-Banking, the E-Banking services of the Bank, the Bank expressly points out the following risks:

- inadequate security precautions and a lack of knowledge about the system used may facilitate unauthorised access. It shall be the responsibility of Clients to inform themselves as to exactly which safety precautions are required in their case;
- evaluation of data by Internet providers cannot be ruled out. This means that Internet providers, domestic and foreign, are able to trace who had contact with whom and when, and
- there is the latent risk of a third party gaining access, unnoticed, to the computer of a Client while the User is connected to the Internet.

In order to reduce these risks, the Client should observe the following security guidelines.

1. Login

The following rules of conduct shall apply when logging in to the E-Banking services of the Bank:

- always start E-Banking via the link published on www.unionbankag.com;
- check the certificate (see point 7) prior to each login. If there is any doubt as to the authenticity of the login page displayed, please contact us immediately;
- do not store any login information (e.g. agreement number, password, etc.) on your computer.

The login takes place via a multi-level security system. The following is the procedure to be followed:

- Step 1: enter E-Banking agreement number (see point 2)
- Step 2: enter personal password (see point 3)
- Step 3: enter authorisation code (see point 4)

The individual steps are described below in greater detail. If your login was unsuccessful, please contact your client advisor.

2. E-Banking agreement number (the "Agreement Number")

Each User will be sent an individual E-Banking Agreement Number by way of the form of correspondence agreed with the Client. The Agreement Number is required to log in. Please protect it carefully against access by third parties.

3. Personal password ("Password")

The Bank sends each User an initial Password together with the Agreement Number. The password is a part of the Bank's multi-level security concept. The initial password must be changed to a personal password after the first login. When selecting a password, we recommend that you observe the following rules:

- the password must be at least 6 characters long;
- use lower and upper case letters;
- use at least one number;
- use special characters such as *%&;
- do not use any personal information such as names, dates of birth or telephone numbers;
- change your password on a regular basis; and

– use a password for the E-Banking services that you have not already used elsewhere.

Please note further that you should not disclose your password to anyone, write it down or store it on your computer or other storage media. The Bank will only ask you to enter your password on its homepage (www.unionbankag.com) when you log in.

4. Authorisation code

Login or releasing a transaction in E-Banking is done by entering an authorisation code. This authorisation code is encrypted by a coloured mosaic that is generated and displayed directly in E-Banking. The activation code contained in the mosaic can only be decrypted by a special software and the use of a camera-capable device.

5. Blocking access

If you suspect that someone has access to your E-Banking access or your identification information (password), please contact your client advisor immediately to block your access. The E-Banking services will also be blocked if you try to log in with incorrect information. After 5 failed attempts the E-Banking access will be blocked. If your access has been blocked and you wish to unblock it, please contact your client advisor. The client advisor will tell you how to proceed so that access can be unblocked.

6. Security when using the E-Banking services

When you are using the E-Banking services, we would ask you to observe the following points:

– carefully read all messages and warnings;

– contact your client advisor in the event of any suspicious messages or changes of which you were not notified in advance by the Bank;

– end every E-Banking session by logging out properly (using the logout button) to ensure that the E-Banking session has really been ended.

7. Certificate

A security certificate ("Certificate") is automatically generated each time you log in. This will ensure that you are really connected with the bank's secure server. You can review the authenticity of this Certificate by selecting it in the status bar of your browser and examining whether the Certificate contains the following information:

– Applicant: Union Bank AG

– Registration authority: SwissSign AG, Glattbrugg

8. Software

The software which you use, and in particular your Internet browser, may contain bugs which represent a security issue and can be exploited by viruses and similar programs. We therefore ask you to update your software on a regular basis;

– use only software from trusted sources;

– use current browser versions with installed security updates, and

– update your operating system on a periodic basis.

9. Viruses

Viruses and Trojan horses constitute a risk to the security of your data. You can protect yourself against this by

– installing virus protection software on your computer;

- using a personal firewall in addition;
- never opening any email attachment
  - if you are not exactly sure what is contained within it, even if you believe you know the sender or
  - any attachments that are sent by a unknown sender;
- and not using software from untrustworthy providers.

Under no circumstances will the Bank ask you by email, telephone or SMS to disclose personal information, including the Agreement Number or password, without having been requested by you to do so.

10. Encryption

So that not only access to your data but also transmission is as secure as possible, the data between your computer and the Bank's server is encrypted using 128-bit technology. Encryption is automatic and does not require any additional encryption software on your computer.

11. Data retention

Your computer continually files data in your browser's cache. Clear the cache after every E-Banking session. Otherwise, confidential information will be stored unprotected on your computer.

12. Additional links on security

Reporting and Analysis Center for Information Assurance MELANI

Datenschutzstelle der Liechtensteinischen Landesverwaltung (in German)