REICHMUTH & CO
PRIVATBANKIERS

e-Connect Terms and Conditions and Security Instructions

The present Terms and Conditions and Security Instructions govern the arrangements with regard to access to e-Connect between clients or a person with power of attorney over a client's banking relationships (referred to jointly below as "Contract Partner") and Reichmuth & Co ("the Bank"). The authorized user is the person that actually uses e-Connect, be it the Contract Partner or a user issued with a power of attorney by the Contract Partner (referred to jointly below as the "Authorized User"). The Con-tract Partner bears full responsibility for the Authorized Users they appoint complying with the requirements set out in the present document. **Persons with a power of attorney over the banking relationships of a client are also obliged to obtain the consent of the client to conclude this agreement, and to inform the client in particular of the risks involved (cf. point 4).**

The term "IT System" used below comprises hard-ware and software, including mobile devices, fixed network and mobile telephones, and other technical aids for the use of the personal means of authentication.

1. Personal means of authentication and instructions

The Bank makes the personal means of authentication available to the Authorized User only for use in accordance with the provisions. Access to e-Connect and the services it offers will be granted once the Authorized User has authenticated themselves to the Bank using the personal means of authentication (contract number, password, SMS authentication). The Help/Instructions document, which is available on the Bank's website, sets out how the personal means of authentication are to be used properly to prove authorization for the purpose of gaining access. After the Help/Instructions document has been received, it will be deemed to have been bindingly accepted with the first use of the personal means of authentication (cf. point 2). The Bank may exchange or amend the personal means of authentication at any time.

2. Authentication

Whenever the Authorized User uses a service via e-Connect, the Bank does not identify them by verifying their signature or identity document. The authentication check is carried out solely on the basis of the personal means of authentication provided (point 1) (self-authentication). Any person who successfully gains access to e-Connect using the personal means of authentication and the authentication procedure set out in the "Help/Instructions" document (self-authentication) is deemed by the Bank to be authorized to access e-Connect, regardless of whether this person is in fact the Authorized User or has been authorized accordingly by the Contract Partner.

The Bank is deemed to be instructed and authorized to carry out orders it receives via e-Connect and to follow the instructions and notifications as soon as the authentication check has been passed; they are deemed to have been issued by the Authorized User. The Bank is therefore deemed to have fulfilled its obligations if it complies with the orders, instructions, and notifications it receives within the normal course of business.

3. Duty to exercise due care

a) The Authorized User is obliged to exercise particular care in the safekeeping of the personal means of authentication, and to store them separately from each other. These may not under any circumstances be passed on or made accessible to another person in any way. Passwords must be changed immediately after they are received (10-14 characters in length, with upper and lower case letters as well as numbers and symbols) and kept secret. Passwords must not be written down or saved electronically. Passwords may not be easily determined (no telephone numbers, dates of birth, car registration numbers, easily ascertained sequences of numbers, etc.)

b) E-mails purporting to come from the Bank and requesting the disclosure of the personal means of authentication (e.g. by entering them on a website that is accessed by clicking a link) must not be responded to. The Bank must be informed immediately in such cases. If there are grounds to assume that another person has obtained knowledge of the password, the Authorized User must change it without delay. The Bank must be notified immediately in the event of you losing your mobile telephone, changing your telephone number or terminating your subscription. The Bank recommends locking your mobile telephone to protect against unauthorized access.

c) If a connection is established to e-Connect via the Internet or other electronic networks, to combat errors

and misuse the Authorized User is obliged to verify the correctness of the bank address entered and the authenticity of the corresponding bank server certificate, unless this has already been done automatically with the personal means of authentication used to login (for further details, please see the "Help/Instructions" document). In the event of any irregularities, login must not be carried out, the connection is to be terminated immediately, and the bank is to be contacted. The personal means of authentication are to be disclosed to the Bank only. Login must always take place on the Bank's website only, and never on the website of a third-party provider.

d) It is possible that unauthorized third parties may seek to obtain access to the IT System of the Authorized User undetected (including by means of electronic maintenance tools, etc.). The Authorized User is therefore obliged to take the usual protection precautions to minimize the existing security risks (e.g. the risks inherent in public electronic networks such as the Internet). In particular, operating systems and browsers are to be kept up-to-date, i.e. the Authorized User must install the security patches made available and recommended by the providers concerned. The standard security precautions for public electronic networks are to be taken (e.g. by installing a firewall and using an anti-virus program that are kept up-to-date at all times). The Authorized User is responsible for obtaining exact information about the security precautions required and for implementing them. The Authorized User is also obliged to implement the necessary precautions to ensure the security of any data stored on their IT System.

e) To increase security, when issuing orders the Authorized User may be asked to confirm certain details of the transactions, such as the beneficiary or the entire transaction. In such cases, the Authorized User is obliged to check the correctness of the information presented for confirmation against their original (physical) order instructions, i.e. independently of the information shown in e-Connect, and if correct to confirm this using the personal means of authentication. Responsibility for the correct and diligent execution of the confirmation lies solely with the Authorized User. The Bank may at any time change the existing protection mechanisms or introduce new ones.

f) The Contract Partner bears full responsibility for the Authorized Users they appoint complying with the present requirements.

4. Payment transactions

a) The Bank is instructed by the Contract Partner to execute the orders received via e-Connect and to follow the instructions and notifications provided the system-based authentication check as set out in point 2 has been passed. If orders are issued to the Bank via e-Connect, it is entitled to reject individual orders at its own discretion if there are insufficient free assets or collateral available to cover such orders or if the available credit limit has been exceeded.

b) If several payment orders have been placed, the total amount of which exceeds the free assets or credit granted, these will be executed on the execution date requested, and only to the extent that coverage is available.

c) The Bank may in the client's interests execute a payment order despite a lack of necessary funds.

d) If there is no execution date specified, or if the execution date specified is impossible, too soon or illogical, the Bank is deemed to be authorized to execute the payment order once it has been registered at the Bank, provided the other condition set out under let. a) is met. If the execution date specified by the client or their authorized representative in the payment order is a Saturday, Sunday or public holiday, the next working day thereafter will be deemed the execution date.

e) The correct conduct of electronic payment transactions via e-Connect is a matter for the client or their authorized representative.

5. Risks

The authentication arrangement (point 2) means that the Authorized User bears the risks arising from (i) the manipulation of the Authorized User's IT System by unauthorized persons, (ii) the misuse of the personal means of authentication, (iii) the breach of the duties to exercise due care, or (iv) unauthorized third parties obtaining access to the data transmission.

The Authorized User is aware of the risks relating to the exchange of information and data via public and private data transmission networks. It may not be possible to rule out the targeted manipulation of the Authorized User's IT System by unauthorized parties. The danger of such manipulations falls within the client's sphere of influence, and the client bears the corresponding risks.

6. Blocking

Any Authorized User may have access to e-Connect blocked at one of the offices specified by the Bank during business hours. Additionally, they may block their access (or their means of authentication) them-selves by entering their means of authentication for the service concerned incorrectly enough times for access to be blocked by the system (e.g. by repeatedly entering an incorrect password or code).

The Authorized User bears the risk of any use of their personal means of authentication before the blocking takes effect during the period necessary for this to be done in the normal course of business.

7. Country-specific restrictions, foreign import and export restrictions

The offering of financial services to Authorized Users abroad may be subject to local legal restrictions. If the Bank does not hold the necessary local licenses in a given country, the scope of the services for Authorized Users from that country will have to be restricted. These restrictions are subject to ongoing changes in legislation and the regulatory environment of the country concerned. The Bank is entitled to amend or restrict the scope of the services available at any time and without prior notice.

The personal means of authentication provided by the Bank may be subject to specific import/export restrictions as well as restrictions on use. Furthermore, the import/export and use of the personal means of authentication by Authorized Users in a third country/countries may be subject to additional country-specific laws. Knowledge of and compliance with the above is the responsibility of the Authorized User. The Bank does not accept any liability in this respect.

8. Transmission errors, technical faults, operating failures, and illegal interference

The Bank accepts no liability for any loss or damage caused as a result of transmission errors, misrouting, technical faults, operating failures, and illegal interference in respect of the IT System of the Authorized User or a third party (including publicly accessible systems and transmission networks), except in cases where the Bank has failed to comply with the requirements to exercise the due care customary in the business. Provided it exercises the due care customary in the business, the Bank does not provide any guarantee of error-free uninterrupted access to its services at all times. It thus also accepts no liability whatsoever for loss or damage arising from faults, interruptions (including required system maintenance work) or overloading of the Bank's ATMs or IT Systems.

9. Provisions regarding powers of attorney

For the purposes of this agreement, authorized representatives are persons that have received a written power of attorney using a power of attorney document of the Bank. Access authorizations and personal means of authentication are not automatically invalid, e.g. in the case of death, incapacity, removal of signatory powers or deletion from a register. Irrespectively of this, the blocking of access authorization and the personal means of authentication must always be expressly ordered by the client / their legal successor / the Authorized User.

10. Bank-client confidentiality / data protection, marketing

Swiss law (e.g. on bank-client confidentiality, data protection) applies only to Swiss territory. Any data that is transmitted abroad is therefore no longer protected by Swiss law. The Contract Partner accepts that the data will be transmitted via an open, publicly accessible network. The data may therefore be transmitted across borders without control, even if the sender and recipient are located in Switzerland. The Contract Partner also accepts that information from the Bank that the user has sent to them separately by e-mail, SMS, etc. (authentication procedure, alert functions) is as a rule sent unencrypted, hence bank-client confidentiality is not guaranteed. Even in the case of encrypted transmissions, the sender and recipient remain unencrypted, and it may therefore be possible for third parties to infer the existence of a banking relationship.

11. Amendments to the provisions

In justified cases, the Bank is entitled to amend at any time the present "Terms and Conditions and Security Instructions", the "Help/Instructions" document, any supplementary agreements, and any special provisions relating to the individual services. The Bank is obliged to give prior notice of such amendments in writing, electronically on screen (cf. point 8), by circular or in another suitable manner. Barring any objections in writing within a month of notification, but in any case with the next use of the personal means of authentication, the amendments are deemed to be approved. If they do not consent, clients are free to terminate the service concerned before the amendments take effect, should the client be unable to reach any other agreement with the Bank before such date.

12. Termination

Individual e-Connect services or all e-Connect services taken as a whole may be terminated at any time by the Authorized User and also by the Bank. After the complete termination of e-Connect, the personal means of authentication provided (e.g. contract number, password) are to be rendered unusable/illegible, and returned to the Bank unsolicited and without delay.

Despite the termination, the Bank remains entitled to process all transactions triggered before the return of the personal means of authentication, with such transactions being binding for the Contract Partner. The Bank is also

entitled at any time to terminate individual services immediately and without notifying the Authorized User if that service has not been used for more than two years.

13. Services of the Bank

The Bank will provide the electronic services within the means at its disposal and without guarantee. The Bank will offer technical support during business hours only. Access free from interruption and error cannot be guaranteed. It is also possible at any time for data transmission to be subject to time delays. The Bank is further entitled to interrupt the electronic services at any time for maintenance reasons. The Bank will exercise the care customary in the business in selecting its service providers. However, it bears no responsibility for the service providers it commissions providing it with correct data at all times (e.g. exchange and forex prices) or for the data it makes available being transmitted correctly and in a timely manner to the client's IT access point.

14. Liability of the Bank

The Bank is not liable for loss or damage suffered by the client as a result of breaching its duties in connection with electronic services. Liability is excluded for indirect and consequential loss or damage such as loss of profit, third-party claims or loss/damage arising from the non-performance of contractual obligations of the client.