

Introduction

These Terms and Conditions for Online Banking (the “**Online Banking T&C**”) govern access by the customer to online banking services (also called “e-banking”) of TradeXBank AG (the “**Bank**”).

Online banking services allow electronic communication of payment orders and various instructions and notifications of the customer to the Bank, and communication of various documents from the Bank to the customer.

These Online Banking T&C are special regulations of the Bank for the purposes of the Bank’s General Terms and Conditions (the “**GTC**”). The matters not specifically governed by these Online Banking T&C are subject to the GTC, other special regulations of the Bank and specific agreements with the customer.

Article 1 E-banking agreement

Online banking services are provided to the customer on the basis of the e-banking agreement constituted by the customer’s application for the use of e-banking, and the Bank’s acceptance thereof. The Online Banking T&C are an integral part of the agreement.

Article 2 Access to online banking services

- (1) Access to online banking services is granted to persons (the “**Users**”), acting on behalf of the customer, having identified themselves with:
 - customer’s e-banking agreement number;
 - personal password; and
 - secret number from a SecurID card of the customer; or
 - alternatively, other forms of identification accepted by TXB.
- (2) The customer shall ensure that each User changes the first password the User

receives from the Bank immediately upon receipt. The Bank recommends the customer to ensure periodic change of passwords by the Users.

- (3) Persons successfully identified in accordance with clause (1) above are authorised to use online banking services on behalf of the customer. The Bank may allow the User, without any further examination of the User’s authority, to access and operate via online banking services the accounts of the customer listed on the application form for use of e-banking, to send binding instructions and notifications to the Bank, and to receive documents from the Bank, regardless of the User’s legal relationship to the customer and regardless of any contradictory entries in commercial registers, public announcements or stipulations on the Bank’s signature documentation. Furthermore, the Bank has the right, at any time and without stating reasons, to refuse to provide information or to accept instructions, orders and communications and to insist that the User is identified by alternative means (by signature or in person).

Article 3 customer’s and Users’ obligations of due diligence

- (1) The customer and each User shall keep the identification elements (clause (1) of Article 2) confidential and protect those elements against disclosure to, and misuse by, unauthorised persons. Without limitation, the passwords may not be stored unprotected, including once changed (clause (2) of Article 2). The customer bears all risks arising from the disclosure of the identification elements.
- (2) If there is any reason to suspect that unauthorised persons may have knowledge of an identification element (clause (1) of Article 2), the customer

shall immediately change that identification element.

- (3) The customer bears full responsibility for all consequences arising from the use or misuse of the identification elements.

Article 4 Limitations of online banking security, waiver of liability for the Bank

- (1) Irrespective of all security precautions neither the Bank nor the customer are guaranteed absolute security. The customer's and Users' devices and network are part of the system but are outside the Bank's control and may become a weak link. The Bank cannot and will not accept responsibility for the customer's and Users' devices.
- (2) The customer acknowledges and accepts, without limitation, the following risks:
 - Insufficient technical knowledge and lack of security precautions can make it easier for unauthorised persons to access the system (e.g. insufficiently protected storage of data on the hard disk, file transfers, information left on the screen, etc.). It is the customer's responsibility to inform the Users of the necessary security precautions, and cause those to be taken.
 - The possibility that the network provider (e.g. Internet provider) may profile the customer and the Users cannot be ruled out, i.e. the provider may be able to identify when and with whom the customer makes contact.
 - There is an inherent risk that third parties gain access to the customer's (a User's) computer during an Internet session (e.g. via a Java or ActiveX application) without being noticed.
 - A virus may enter the customer's (a User's) computer when a network

(such as the Internet) is used.

- It is important that only software from reliable sources is used.
- (3) The Bank does not provide technical access to its services. This is the responsibility of the customer. The customer accepts in particular that the Bank does not provide the software for online banking or security software. The Bank accepts no liability for the network providers or the software.
 - (4) The Bank assumes no responsibility whatsoever for the accuracy and completeness of the data which it transmits. In particular, information regarding accounts (balances, statements, transactions, etc.) and generally available information such as foreign exchange rates is to be regarded as non-binding. Data made available does not constitute a binding offer except where it is explicitly designated as such.
 - (5) In particular, the Bank cannot be held liable for damages which the customer may incur as a result of transmission errors, technical defects, system overloads, interruptions (incl. system related maintenance work) malfunctions, illegal intervention and malicious blocking of telecommunications installations and networks, access by third parties or other deficiencies on the part of the telecommunications equipment and network providers.
 - (6) Provided it has exercised the normal due diligence, the Bank is not liable for the consequences of malfunctions or interruptions, especially in processing, which affect online banking services.
 - (7) The Bank waives all liability for any software or hardware it may have supplied, or for consequences resulting from or occurring during transportation of the software (including via the Internet).
 - (8) If the Bank detects any security risks, it reserves the right to interrupt e-banking

services for the protection of the customer at any time until the risk is removed. The Bank waives all liability for damages incurred as a result of such interruptions.

- (9) The Bank waives all liability for damages which the customer incurs due to non-performance of the contractual obligation vis-à-vis a third party or for indirect and subsequent damages such as missed profits or third-party claims.
- (10) The Bank waives all liability for damages resulting from minor negligence on the part of support staff going about their normal duties.

Article 5 Blocking access

The Bank may at its sole discretion block access of the customer or any Users to specific or all online banking services at any time, without stating reasons and without prior notification.

Article 6 Banking confidentiality

- (1) The customer shall note that Swiss banking confidentiality only applies to data stored in Switzerland, and, in case of information transmission, when both the sender and the recipient are in Switzerland.
- (2) The customer shall also note that data are transported over an open network (i.e. the Internet) which is accessible to third parties. Data are thus transmitted regularly unchecked across international borders. This also applies to data transfers where both the sender and recipient are located in Switzerland. Although individual data packages are transmitted in encrypted form, the identities of the sender and recipient are not encrypted. It is therefore possible for a third party to conclude that a banking relationship exists.

Data processing for security purposes

The customer and all Users agree that the

Bank may process all data for security purposes. The resulting profile will serve to prevent fraudulent transactions.

Article 7 Foreign legal provisions / import and export restrictions

- (1) The customer and the Users shall note that under certain circumstances use of online banking services from outside of Switzerland may constitute breach of the applicable foreign laws. The customer is responsible for finding out whether this is the case. The Bank accepts no responsibility in this regard.
- (2) Further on, use of online banking services from outside of Switzerland may constitute breach of import and export restrictions governing encryption algorithms.

Article 8 Marketing

The customer agrees that the Bank may use customer data from online banking services for its own marketing purposes.

Article 9 Termination

The customer or the Bank may terminate the e-banking agreement at any time by notice in writing.

Article 10 Reservation of certain legislation

- (1) Any legislation which governs the operation and use of telecommunications installations and networks is reserved and applies, once it comes into force, to the online banking services of the Bank.
- (2) The above applies without prejudice to any other legislation.

Article 11 Fees

The Bank reserves the right to charge fees for the online banking services or to adjust

existing charges at any time.

Article 12 Changes to the Online Banking T&C

The Online Banking T&C may be amended at any time in accordance with the GTC.

Article 13 Further provisions

Without prejudice to the application of the GTC in general, the provisions of the GTC on:

- governing law;
- jurisdiction;
- liability and indemnity;
- banking secrecy and confidentiality; and
- data transfer, reporting and disclosure,

shall apply without limitation to the Online Banking T&C.