1. Purpose and scope

1.1 The following terms and conditions regulate the e-banking services of bank zweiplus ltd (hereinafter referred to as “Bank”) for the use of e-banking (hereinafter referred to as “client”) as well as any persons that have been authorized by the client by means of e-banking authorization for the use of e-banking services (hereinafter referred to as “authorized representative”).

1.2 The Bank reserves the right to provide the client with bank services of mobile phones such as mobile phones, smartphones, or tablets. The user acknowledges that the Bank provides no advisory support for any services utilized via the e-banking system.

3. Access to e-banking

3.1 Technical access to e-banking is gained via the Internet through the internet service provider (or any other service network accessible by a mobile device or via an access via the mobile device). Access is granted to those who have entered the following authentication details. If the login process is initiated, the e-banking mailbox (see section 7) may be used.

3.2 The user acknowledges that e-banking is only available for retrieval in the e-banking mailbox via the Internet. The Bank accepts no liability for any losses resulting from the unauthorized access.

4. Orders in general

4.1 An order issued via e-banking may not be executed around the clock in each case. Processing such orders is contingent on the technical functionality of the e-banking system, the Bank’s business days / business hours and, under certain circumstances, other processing points as well as on the trading days / hours of the relevant stock exchange.

4.2 The Bank is entitled to reject or cancel orders placed by the user insofar as there are insufficient funds in the corresponding account.

5. Payment orders

5.1 The client acknowledges that a canceling a payment order is possible only in certain circumstances.

5.2 The Bank is entitled to utilize a signature process based on a mobile terminal number (hereinafter referred to as “MIVAN”) as an authorized representative for the authorization of payment orders. Within the scope of the authorization process, the user is not tied to the electronic installation of the e-banking system. To confirm the execution of such an order with a transformed confirmation code (applies to SMS login) when using the application that is available with mobile devices (e.g. via the Bank’s smartphone application), the user may be requested for reasons of security to also approve payment orders via the standard e-banking application (possibly an end device). The user takes note that in this case, payment orders may not be approved via the MIVAN. The Bank reserves the right to process such orders via the mobile transaction number-based signature function is not available for users with ActivaCard as an authentication procedure.

6. Stock exchange orders

6.1 The user acknowledges that the Bank provides no advisory services relating to stock exchange orders executed via the e-banking system.

6.2 The user also acknowledges that the respective valid version of the brochure titled “Special Risks in Securities Trading” issued by the Swiss Banks Association forms an integral part of these terms and conditions, which should be consulted by the user.

6.3 The user hereby confirms awareness of the risks associated with the desired stock exchange orders, that the Bank is not responsible for any losses resulting from the client’s actions (e.g. in connection with changes in regulations by the regulator). The mobile transaction number-based signature function is not as conformable to the applicable form of authentication.

7. Client orders and messages via e-banking mailbox

7.1 Under the navigation point “Messages,” each user within the e-banking system is assigned a mailbox with which messages can be received from, and sent to, the Bank.

7.2 Messages and orders directed to the Bank are not handled with any particular priority. The Bank reviews, replies to, and/or processes such messages and orders within the normal course of business and during business hours as well as during business hours on Saturdays and the first three days of the month. The e-banking mailbox is therefore unsuitable for messages or orders that are time-critical or subject to deadline (for example, time-critical payment orders or stock exchange orders, revocation of orders, blocking of credit cards, etc.).

7.3 The option for an authorized representative to issue orders via the e-banking mailbox depends on the e-banking authorization as well as the relevant power of attorney for the accounts/custody account on file with the Bank.

7.4 In the case of a specially structured account/custody account, the Bank has the right to decline to provide information, reject messages and instructions, as well as to refuse to execute orders at any time and without stating reasons, for the protection of the client. In this regard, the Bank may demand that the user provide another form of authentication (e.g. in written form or attendance in person).

7.5 The client unconditionally accepts all transactions booked to the accounts/custody accounts specified in the Agreement for the Use of e-banking, as far as they have been executed with the respective authentication details (e.g. by means of SMS, or by means of any other procedure relating to authorized representative, commercial register entries, publications or regulations provided in the Bank’s signatory documents to the contract).

7.6 The client unconditionally accepts all transactions booked to the accounts/custody accounts specified in the Agreement for the Use of e-banking as far as they have been executed with the respective authentication details (e.g. by means of SMS, or by means of any other procedure relating to authorized representative, commercial register entries, publications or regulations provided in the Bank’s signatory documents to the contract).

7.7 The user acknowledges that the Bank does not carry out any editorial checks such as subject accuracy. Users bear responsibility for the data they send until such time as they receive confirmation from the Bank’s e-banking system.

9.6 Electronic bank documents are available for retrieval within e-banking for a period of at least 12 months. After this period, if or to security reasons, any passwords or PIN codes should be selected that are easy to determine (e. g. date of birth or telephone number of the user’s close friends or relatives).

10.1 The user is obliged to safeguard the authentication details from any misuse by unauthorized persons. The user should also keep any documentation of the authentication detail and may not reveal or disclose them to other persons. Recording or in-securely storing the authentication details is prohibited.

10.2 The user is obliged to change the initial password as well as ActivaCard PIN code issued by the Bank immediately following receipt and first utilization. In addition, the user should regularly change the personal password and ActivaCard PIN code in the future as well. Due to security reasons, no passwords or PIN codes should be selected that are easy to determine (e. g. date of birth or telephone number of the user’s close friends or relatives).

10.3 The user is obliged to immediately notify the Bank of the loss of the mobile telephone or ActivaCard used for the SMS login.

10.4 If there is any reason to suspect that unauthorized third parties may have gained knowledge of an authentication detail, the relevant authentication detail must be changed; the Bank must be notified immediately and access to e-banking blocked (see section 11).

10.5 The user shall undertake the requisite measures to prevent any unauthorized persons from accessing the client’s device or related programs. The user is obliged to minimize security risks associated with the use of the Internet through utilizing appropriate protective mechanisms (e.g. antivirus updates, a secure firewall, a high-security level for the Internet browser, clearing cache memory and history). The user is responsible for obtaining accurate information regarding the requisite security measures.

10.6 The user must check all the data entered as well as confirmations from the e-banking system to ensure their completeness and accuracy. The user is not responsible for the data sent until such time as they receive confirmation from the Bank’s e-banking system.
11. Blocking access
11.1 By the Bank: The Bank is entitled to block access to the e-banking system at any time without stating reasons and without advance notice, if it regards such blocking as appropriate at its own discretion on objective grounds. The Bank accepts no liability for any losses resulting from such blocking.

12. Scope of liability of the Bank
12.1 The Bank accepts no liability for losses resulting from orders not executed or not executed on time, provided it has exercised proper due diligence. The Bank is only liable in cases of gross negligence for the consequences of malfunctions or disruptions in its e-banking operations (e.g. caused by illegal access into the Bank’s system).

12.2 The Bank is only liable in cases of gross negligence for the consequences of malfunctions or disruptions in its e-banking operations (e.g. caused by illegal access into the Bank’s system).

12.3 The Bank reserves the right to suspend its e-banking services at any time if it uncovers security risks or - within the scope of maintenance work - until such time as the risks have been eliminated or work completed. The Bank accepts no liability for any losses resulting from such disruptions.

12.4 The Bank accepts no liability for any losses resulting from the use of the Internet or the mobile phone network. In particular, the Bank is not liable for losses incurred by the user resulting from transmission errors, technical faults, malfunctions, illegal intu- tion into network equipment, network overload, malicious blocking of e-banking systems, Internet malfunctions, interruptions or other shortcomings on the part of network operators.

12.5 Furthermore, the Bank explicitly accepts no liability for any data transmitted across borders under certain circumstances. Data can be intercepted, viewed and changed. The user hereby confirms that the use of e-banking services is offered through the Internet and telecommuni- cation networks. Hence, the data are transmitted via an open net- work that is publicly accessible. Despite the use of state-of-the-art security technology, absolute security cannot be guaranteed, either on the part of the Bank or on the part of the user. It lies within the Bank’s discretion to introduce additional security systems or authen- tication features for the use of e-banking.

12.6 The Bank accepts no liability for losses incurred by the user re- sulting from the failure to meet contractual obligations toward third parties or for direct, indirect or consequential losses such as loss of earnings or third-party claims.

12.7 The client bears all risks deriving from the disclosure or use (in- cluding misuse and illegal use) of the relevant authentication details. The Bank accepts no liability whatsoever in this regard.

12.8 The Bank accepts no liability for losses incurred by the user re- sulting from the failure to meet contractual obligations toward third parties or for direct, indirect or consequential losses such as loss of earnings or third-party claims.

12.9 The Bank provides no guarantee whatsoever for the accuracy and completeness of the data transmitted via its e-banking system. In particular, details of accounts and custody accounts balances, statements, transactions, etc., as well as any generally accessible information such as stock market and currency prices are regarded as non-binding. e-banking data do not constitute a binding offer unless it is explicit- ly designated as such.

12.10 In the case of slight negligence, the Bank accepts no liabil- ity for losses caused by its auxiliary staff in exercising its duties.

12.11 The Bank is entitled to engage specialists to optimize its e-banking services. In this case, the Bank is obliged only to exercise due diligence in selecting and instructing such specialists.

13. Provisions of authorization
13.1 Authorization for use of e-banking remains in effect in each case until its explicit revocation.

13.2 e-banking authorization does not lapse in the event that the client dies, is declared missing, loses capacity to act or is declared bankrupt, irrespective of otherwise specified commercial register en- try or other published documents. Following the death of the cli- ent, the authorized representative is obliged to protect the interests of the client’s heirs, obtain their instructions and remain accounta- ble to them. In the event of death of the client, the Bank may subject any legal actions taken on the part of the client’s authorized repre- sentative to be contingent on the submission of documentation re- quired under inheritance law and/or the written consent of the client’s heirs.

13.3 e-banking authorization may be revoked at any time by the client, authorized representative or relevant heir. Such revocation should be addressed to the Bank and must be confirmed in writing as well. Revocation of a standard power of attorney does not au- tomatically result in revocation of the authorization to use e-bank- ing services; in fact, such authorization must be explicitly revoked. Vice versa, revocation of the authorization to use e-banking services does not automatically result in revocation of a standard power of attorney. However, the Bank reserves the right to stipulate that the authorization for use of e-banking be contingent on the existence of a standard power of attorney.

14. Information on security and risks relating to transmission of data via the Internet
14.1 Authorization for use of e-banking is offered through the Internet and telecommuni- cation networks. Hence, the data are transmitted via an open net- work that is publicly accessible. Despite the use of state-of-the-art security technology, absolute security cannot be guaranteed, either on the part of the Bank or on the part of the user. It lies within the Bank’s discretion to introduce additional security systems or authen- tication features for the use of e-banking.

14.2 Bank secrecy/data protection: Swiss banking secrecy laws ap- ply only to data stored within Switzerland. Transmission of data via the Internet is carried out regularly and uncontrollably across bor- ders, which may even apply when data are transmitted between senders and recipients located in Switzerland. Although the individ- ual data are transmitted in encrypted form, the respective sender and recipient are always identifiable. The data can also be viewed by third parties. It is therefore possible for a third party to draw conclu- sions about an existing banking relationship. Uplinking banking se- curity and maintaining data protection cannot be guaranteed.

14.3 Profiling of the user’s traffic characteristics by network opera- tors cannot be ruled out i.e. it may be possible for a network oper- ator to track when and with whom the client has made contact.

15. Important information regarding SMS
15.1 The user acknowledges that the transmission of SMS commu- nications is carried out unencrypted, unencrypted and the data may be transmitted across borders under certain circumstances. Data can be intercepted, viewed and changed. The user hereby confirms that the dispatch of SMS is explicitly desired.

15.2 The Bank can provide no guarantee that the information and notifications transmitted by it via SMS reach the user on a timely ba- sis or at all.

15.3 The Bank has no influence on any costs incurred by the user from mobile communications services providers. The Bank accepts no liability whatsoever for such costs.

16. Data collection and data processing
16.1 When using e-banking services, “cookies” will be temporar- ily stored or accessed on the user’s end device. This will enable the Bank to provide navigation short-cuts for the benefit of the user. Only a minimum of information will be input into the cookies, set up by the Bank. By modifying the Internet browser settings, it is possible to prevent cookies from being placed on an end de- vice. Depending on the browser settings selected, it is possible that blocked cookies may reduce the functionality of, or prevent access to, e-banking services. The Bank accepts no liability for such restric- tions.

16.2 The user therefore accepts the fact that the Bank may manip- ulate the relevant data for its own marketing purposes.

17. Foreign laws
17.1 The use of e-banking services in other countries may violate foreign laws under certain circumstances. In this regard, it is the user’s re- sponsibility to obtain the relevant information. The Bank accepts no liability whatsoever in this case.

18. Amendments to the agreement
18.1 The Bank reserves the right to change these terms and conditions as well as the scope of its e-banking services offered and fee struc- ture at any time. The user will be notified of such changes through the appropriate means, which are regarded as being accepted no later than with the subsequent utilization of e-banking services by the user.

19. Cancellation
The client may cancel the Agreement for the Use of e-banking in writing at any time.