



Conditions for the use of E-Services

These Conditions for the use of E-Services govern the modalities relating to the access to E-Services between the Client (the “**Client**”)¹ and/or his Authorised Representative (as defined in clause 12.1 below) and Bank J. Safra Sarasin (Gibraltar) Ltd, (the “**Bank**”). For the purpose of these conditions, the Client and/or the Authorised Representative (the “**Authorised User**”)¹ is the actual user of the E-Services system. The access authorisation of the Authorised User is detailed in either the “**Agreement for the use of E-Services**” or its supplement “**Authorisation to use E-Services**”, as applicable. In addition, the Bank’s “**General Terms and Conditions**” form an integral part of the aforementioned agreements. In case of any inconsistency between the provisions of the aforementioned General Terms and Conditions and those contained herein, the provisions of these Conditions for the use of E-Services shall prevail.

The Client bears complete responsibility that any Authorised User appointed by him complies fully with the obligations specified herein as well as those in the aforementioned agreements and terms.

1. Services offering

- 1.1 The term E-Services refers to the online services which the Bank may now or in the future agree to make available to the Client through electronic means. These E-Services may include basic services (such as account or portfolio overviews and movements, market information (time delayed) performance data, asset allocation and the use of messages and notifications) as well as payment and financial instrument transactions. The Bank reserves the right to adjust or amend its E-Services offering at any time without prior notice.
- 1.2 The current service offering and fee schedule for E-Services as well as the valid “**Conditions for the use of E-Services**” will be brought to the Client’s attention in an appropriate manner. In addition, a Client can contact his Relationship Manager for any additional information or question.

2. Access to E-Services and authorisation

- 2.1 Technical access by the Authorised User to E-Services is via the Internet (incl. via mobile end devices such as mobile phones or tablets) through an Internet service provider selected by the Authorised User and special browser software that the Authorised User acquires independently from third parties or via a mobile end device application. Access to E-Services and the services contained therein shall only be granted once the Authorised User has legitimised himself via one of the available authentication procedures.
- 2.2 Access to E-Services is protected by four security levels via self-legitimation, either with a token (e.g. ActivCard) or by SMS log-in. To access the Bank’s E-Services, the Authorised User must identify himself as follows:

a) Access with a token (e.g. ActivCard):

- user ID assigned by the Bank to the Authorised User (1st security level);
- password assigned by the Bank to the Authorised User (2nd security level);
- PIN code on the token (3rd security level); and
- token transaction number regenerated by the token every minute (4th security level).

b) Access by SMS log-in:

- user ID assigned by the Bank to the Authorised User (1st security level);
- password assigned by the Bank to the Authorised User (2nd security level);
- PIN code of the mobile end device of the Authorised User (3rd security level); and
- transaction number (log-in) generated by the E-Services system and sent to the mobile end device of the Authorised User by SMS (4th security level).

For mobile end device applications, the authentication procedures to access E-Services may vary. Furthermore, the Bank has full discretion at any time to add additional authentication procedures or change or cancel existing authentication procedures. The Bank specifically reserves the right to switch the authentication procedure for Authorised Users with tokens to SMS log-in and vice-versa. Any changes to the authentication procedures shall be communicated to the Authorised User in an appropriate manner.

- 2.3 The Authorised User is required to change the password issued by the Bank immediately upon receipt and subsequently to change his password on a regular basis.
- 2.4 Any Authorised User identifying himself correctly as described in clause 2.2 above (self-legitimation) is entitled to use

¹ To facilitate readability, the masculine form is used for both genders. To the extent justified by the context, the singular form includes the plural and vice versa.

the Bank's E-Services. Consequently, the Bank may then allow the Authorised User to access the services as defined by the Client for each Authorised User. This is possible without further authentication of the Authorised User's entitlement and irrespective of the internal legal relationship between the Client and an Authorised User, if different from the Client, and irrespective of any different commercial register entries, publications or arrangements made in other Bank documents. The Bank does not check the matter of internal user entitlement for companies with several sets of authentication features. In principle, no agreement is possible with the Bank to provide access to or the use of E-Services exclusively through authentication of two or more Authorised Users (e.g. "dual signature"). However, the Bank reserves the right to allow transactions to be executed by means of collective authorisation for certain services.

- 2.5 In order to protect the Client, the Bank is entitled at any time, and without giving reasons, to refuse to issue information and to refuse to accept or execute instructions, orders and messages submitted through E-Services and to insist that the Authorised User provides a different form of authentication (by signature or by personal visit).
- 2.6 The Client unconditionally accepts all transactions booked to the accounts, safe custody and metal accounts specified in the agreement(s) relating to the use of E-Services, provided they have been executed with the authentication features of the Authorised User. This applies in particular also to transactions effected via the improper use of an Authorised User's authentication features. Likewise, all instructions, orders and messages received by the Bank through use of E-Services by an Authorised User are deemed to have been composed and authorised by the Client.
- 2.7 The Bank may use its discretion in introducing additional technical security systems related to the use of E-Services or individual services contained therein.

3. Financial instrument transactions

- 3.1 The Authorised User acknowledges that in some cases the financial instrument orders placed via E-Services may not be executed immediately or on a twenty-four hour basis, but may depend on, amongst other things, the relevant stock exchange hours/days of trading and on holiday arrangements/working hours of the Bank as set out in the Bank's "**General Terms and Conditions**". The Authorised User also acknowledges that if problems occur, the Bank's trading department will only be available to offer support during normal business opening hours and on days on which the relevant stock exchange is open for trading.
- 3.2 It is at the sole discretion of the Bank which stock exchanges and which financial instruments are offered to the Authorised User within the E-Services trading functionality.
- 3.3 The Bank does not accept any liability for financial instrument orders not being executed or which are not executed on time or for any damages (especially losses resulting from share price fluctuations) provided it has exercised due care. It is only liable in cases of gross negligence.
- 3.4 When the Authorised User places financial instrument orders, he acknowledges the applicable laws and regulations (stock market laws, ordinances, regulations, practices, etc.) as binding and undertakes to comply with them. In the case of stock exchanges, equity markets or products with special rules and requirements, the Authorised User may only be able to place financial instrument orders after complying with the necessary requirements and formalities. In some instances, it may be necessary for the Client himself to meet these requirements and formalities.
- 3.5 By entering into a financial instrument transaction via E-Services, the Authorised User confirms that he has taken note of, understands and adheres to any applicable Client restrictions (e.g. eligibility requirements) for a particular financial instrument pursuant to the respective product documentation. With respect to collective investment schemes, the Authorised User particularly confirms to only invest in shares/units for which the Client is eligible for pursuant to the collective investment scheme documentation in question.
- 3.6 The Bank is entitled to reject or cancel financial instrument orders placed by the Authorised User if they fail to comply with the applicable law and regulations (stock market laws, ordinances, regulations, practices, etc.). The Bank is further entitled to reject or cancel financial instrument orders placed by the Authorised User if there are insufficient funds in the Client's corresponding settlement account, or if the execution of the financial instrument order runs counter to the letter and spirit of an existing pledge or a block on assets.
- 3.7 Before entering into a financial instrument transaction, the Authorised User is obliged to consult the Risk Warnings in the Bank's "**General Terms and Conditions**" and any risk information provided within E-Services, which provide information about the particular features and risks of financial instruments. By entering into financial instrument transactions via E-Services, the Authorised User confirms that he is familiar with the customs and practices of financial instrument transactions, in particular the structures and risks of the individual types of financial instrument transactions.
- 3.8 For financial instrument transactions effected via E-Services, the Bank has no responsibility or liability whatsoever for determining the suitability of any such transaction. This particularly applies to financial instrument transactions which are effected without individual advice and upon the Authorised User's own initiative, which are executed by the Bank on an "execution-only dealing" basis. For "execution-only dealing" transactions, the Client explicitly waives any specific information or risk assessment by the Bank.
- 3.9 In the case of a partial execution of financial instrument orders, increased stock exchange fees and commissions may accrue (e.g. because of minimum tariffs).
- 3.10 The Authorised User may receive an acknowledgement of his financial instrument order through the E-Services platform. In case of any conflict between the order acknowledgement received through the E-Services platform and the standard confirmation received from the Bank after the execution of the financial instrument transaction, the terms of the Bank's confirmation will prevail.

4. Payment transactions

4.1 Payment transactions

The Bank reserves the right to decline at its sole discretion payment transactions submitted via E-Services. Such discretion may be utilised, but not limited to, circumstances where the Client's account has insufficient funds or if the credit limit would be exceeded. The Bank accepts no responsibility for the delayed execution or non-execution of payment transactions and losses, provided it has exercised due care. The Bank assumes responsibility only in cases of gross negligence.

The Authorised User acknowledges that the value and execution date of a payment transaction submitted via E-Services may vary from one given to the Bank via other means of communication (e.g. telephone). The Authorised User furthermore acknowledges that authorised payment orders in E-Services can only be cancelled on a limited basis.

The Bank may charge a separate fee for the payment transaction services provided via E-Services.

The Bank reserves the right to not provide payment transaction services in E-Services to external asset managers for accounts of their asset management customers.

4.2 In providing payment transactions services as part of E-Services, the Bank offers the additional functionality "confidential payments" in order to process these payments in line with conditions determined specially by the Bank. The following regulations apply in particular:

- Confidential payments can only be entered and/or authorised by Authorised User who have the relevant additional authorisation;
- Confidential payments will be listed on the Client's physical contract notes without details of the payment entered; and
- Details on the executed confidential payments can only be viewed in E-Services by Authorised Users who have the relevant additional authorisation.

The special processing conditions for confidential payments only apply to payment transactions processed via E-Services. Any right of an Authorised User with a standard authorisation to request information on confidential payments remains unrestricted.

4.3 Transaction signature

The Bank may require payment orders to be authorised by means of a transaction signature as an additional security measure for payment transactions. As part of the authorisation process, the Authorised User will in such cases be informed of the content of a payment order interactively by SMS and be requested to confirm the execution of payment order in question by using an authorisation code.

It is at the sole discretion of the Bank to decide when and under which conditions the transaction signature may apply. The Bank may also use its discretion in determining the regulations governing the use of the transaction signature. In particular, it reserves the right to require the transaction signature for certain payment orders and may authorise the Authorised User to make changes to the regulations governing the use of the transaction signature, either individually or in their entirety. The Client assumes any liability and losses resulting from changes to the regulations made by the Authorised User. The Bank may also use its discretion in introducing additional technical security systems when providing payment transactions via E-Services.

The Bank may charge a separate fee for the transaction signature provided via E-Services.

4.4 Collective authorisation for execution of payment transactions (any two Authorised Users)

If the Client has declared that payment transactions may only be processed with collective authorisation, then a payment order entered may only be executed with the electronic approval of any two Authorised Users. If this authorisation is not in place, the entered payment orders will not be executed. An Authorised User must ensure that the second authorisation is promptly obtained for electronic collective authorisations. The Bank accepts no responsibility for payment transactions that are delayed as a result of a missing second authorisation. The Bank reserves the right to delete from its E-Services system those payment orders for which a second authorisation is still missing after a period of time determined by the Bank. The Client understands that it is possible for only one Authorised User to enter (but not to authorise) payment orders for collective authorisations.

5. Electronic delivery of bank documents

5.1 The Bank reserves the right to provide the Client or any other Authorised User at its sole discretion with bank documents by electronic means, either exclusively or in addition to normal dispatch by post. In case of an electronic delivery of bank documents, the conditions contained in this clause 5 shall apply.

5.2 Within the framework of the service of electronic provision of bank documents, the Bank shall send to the Authorised User certain bank documents for all accounts, safe custody and metal accounts included in the "Agreement for the use of E-Services" by sending them in electronic form, instead of paper form, to the E-Services mailbox of the Authorised User. The Client notes that all Authorised Users who have entitlement relating to the above accounts, safe custody and metal accounts are able to access the electronic bank documents. The Client acknowledges that certain bank documents may not be available in electronic form and that the Bank will therefore continue to send such bank documents to the Client and/or third parties in paper form in accordance with the so far existing correspondence instructions (incl. hold retained mail where applicable). In consequence, any agreed provisions in regard to such

correspondence instructions continue to apply. A list of the categories of bank documents provided by the Bank electronically via E-Services can be requested from the Client's Relationship Manager. The Bank expressly reserves the right, at its sole discretion, to switch further documents that are currently sent in paper form to electronic service.

- 5.3** The Client hereby expressly acknowledges that the Bank fulfils in particular its duties of notification and accountability by electronic service of bank documents in the E-Services mailbox of an Authorised User and that the Client deems the relevant bank documents to have been delivered and accepted to the same extent and with the same force and effect as if such bank documents had been delivered in hard copy form through other means. The Client further acknowledges that the Bank may qualify any electronic access of bank documents by an Authorised User as a contact in the sense of the legal and regulatory requirements.
- 5.4** Electronic dispatch of bank documents will be in PDF format (or other file formats that the Bank deems appropriate). The Authorised User is responsible for installing the corresponding software required to display the documents.
- 5.5** The bank documents provided electronically are deemed to have been delivered to the Client, irrespective of any subsequent additional dispatch by post, within the meaning of the Bank's "**General Terms and Conditions**" at the time when they are made available within the E-Services environment and can be accessed by an Authorised User. This applies even if the Client himself has no E-Services access and consequently has no knowledge of the bank documents sent electronically or if an Authorised User does not or cannot access the bank documents that are provided electronically. The period for making complaints in accordance with the Bank's "**General Terms and Conditions**" also commences at the time of availability of the electronic documents.
- 5.6** It is deemed service when the documents are provided electronically and the Bank is not liable if the Authorised User did not access his mailbox at the right time. Notwithstanding and in addition to the provisions in clause 11.2 below, the Client acknowledges that it is the responsibility of the Authorised User to ensure that he accesses the relevant bank documents which will be deemed received by the Client on the date delivered to the Authorised User's E-Services mailbox and that the Bank does not need to review the Authorised User's E-Services mailbox regularly to ensure that the Authorised User has reviewed any bank documents or information. This applies in particular for notification of direct debit charges with the right of objection.
- 5.7** Electronic bank documents are available for downloading within E-Services for at least 12 months. They are then deleted. The deletion is carried out irrespective of the aforementioned period in the case of termination of the account, safe custody and/or metal account for which the electronic service of documents is effected or upon termination of the "**Agreement for the use of E-Services**". It is the responsibility of the Authorised User to access the documents beforehand if necessary and to save them. The Bank accepts no liability for losses caused by the deletion of documents.
- 5.8** If necessary bank documents provided electronically may subsequently be requested in paper form against payment of a fee.
- 5.9** The Bank is entitled to send the bank documents scheduled for exclusive electronic service either additionally or exclusively in paper form by post to the Client's domicile address last notified to the Bank, if the Bank considers this, at its sole discretion, appropriate for justified exceptional cases (particularly where it is deemed to be in the interest of the Client). The Bank accepts no liability for loss resulting from postal dispatch. Furthermore, the Client expressly releases the Bank from its confidentiality duty and expressly acknowledges that he bears any and all damages resulting from the use by the Bank of such postal dispatch.
- 5.10** The electronic bank documents have the same periodicity as bank documents hitherto dispatched by postal service. Modification of this periodicity within E-Services is not possible. The Authorised User may, however, generate ad-hoc and customised bank documents within E-Services based on specific parameters set by the Authorised User himself (e.g. account statements for a specified time period). The Authorised User takes note that such ad-hoc and customised bank documents may not contain the same information and/or meet the same standards as bank documents which are periodically issued by the Bank.
- 5.11** The Bank can provide no guarantee that bank documents accessed electronically and subsequently printed out meet the standards of proof required in court or other administrative proceedings (e.g. tax assessment procedure). This particularly applies to ad-hoc and customised bank documents which are generated by the Authorised User himself based on specific parameters.
- 5.12** With the issue of the order for exclusive electronic dispatch of bank documents, the existing other instructions for dispatch or retention are not cancelled with regard to the bank documents in question and continue to apply. This especially applies for dispatch or retention instructions relating to third parties.
- 5.13** The electronic service of bank documents (exclusive or in addition to normal dispatch by post) may be cancelled by the Client or by the Bank in writing at any time without stating reasons. The cancellation then also applies for service to all Authorised Users. In the case of cancellation of the exclusively electronic service, and in the absence of any instructions to the contrary, all documents shall be sent only to the Client at his recorded permanent address notified to the Bank as of the time of the cancellation.
- 5.14** In the event that the signature or acknowledgement of the Client or any Authorised User other than the Client is required or requested with respect to any bank document, the Client or any Authorised User other than the Client agree that, by "clicking" in the appropriate space, or by taking such other action as may be indicated on the E-Services platform the Client or any Authorised User other than the Client will be deemed to have signed or acknowledged such bank document to the same extent, and with the same force and effect, as if they had signed such bank document manually.

6. Duty of care of the Authorised User

- 6.1** The Authorised User is obliged to keep secret all the personal identification details (see clause 2.2 above) and to prevent them from being misused by unauthorised persons. In particular, after changing the password, the Authorised

User must not write down the password or store it in an unprotected form on the Authorised User's computer or mobile end device. Furthermore, the password and user ID should not be codes that are easy to guess (e.g. dates of birth, phone numbers etc.). Individual identification details must be kept separate from each other. The Client bears all risks deriving from the disclosure or use (including misuse and illegal use) of an Authorised User's identification details. The Bank does not accept any liability in this respect.

- 6.2 The duty to keep identification details secret applies to each individual Authorised User. The Client is therefore also liable for any losses resulting from Authorised Users misusing the identification details of other Authorised Users.
- 6.3 If there is any reason to suspect that unauthorised third parties may have discovered an identification detail of an Authorised User, the relevant identification detail must be changed, the Bank must be informed immediately and if necessary the Client or any Authorised User must block access to E-Services or request the Bank to block access (see clause 9 below).
- 6.4 The Authorised User must notify any token loss (e.g. ActivCard) to the Bank immediately, and must also arrange for E-Services access to be blocked as soon as possible in accordance with clause 9 below. Requests to issue replacement tokens, including replacements for Authorised Users, to the Bank's branch where the business relationship is maintained may only be submitted by the Client, not by an Authorised User other than the Client.
- 6.5 Authorised Users who access E-Services via SMS log-in and who lose their mobile end device must inform the Bank promptly and arrange for their service provider to block its use immediately.
- 6.6 The Authorised User must check all data they enter and the confirmations from the E-Services system to ensure they are complete and accurate. Responsibility for data sent by the Authorised User remains with the Client until confirmation is received from the Bank's E-Services system.
- 6.7 The Authorised User must minimise security risks associated with the use of the Internet or mobile end device network (e.g. viruses, unauthorised access by third parties, etc.) by use of suitable protection mechanisms (in particular anti-virus programs with active updates, a secure firewall, a high security level on the used internet browser and an operating system with current service packs applied).
- 6.8 If the Authorised User has issued an order relating to a payment or financial instrument transactions to the Bank by electronic means and after issuing the order the Authorised User is able to ascertain that the order has not been executed or has not been executed correctly by the Bank, the Authorised User is required to raise a corresponding query with the Bank immediately.

7. Scope of the liability of the Bank and its employees (hereinafter jointly referred to as the "Bank")

- 7.1 The Bank does not guarantee in any way the accuracy, completeness or relevance of the data displayed or transmitted via E-Services, including ad-hoc and customised bank documents generated by the Authorised User based on specific parameters. In particular, details of accounts, safe custody and metal accounts (balances, statements, transactions, etc.) as well as any generally available information such as financial instrument prices are not legally binding unless certain information is explicitly stipulated as such within the framework of a specific service. For investment services, E-Services data does not constitute a recommendation, an offer or invitation to buy or sell any financial instruments, effect transactions, or to enter into any legal transaction of any kind whatsoever, unless it is explicitly stipulated as such.
- 7.2 The Bank accepts no liability for orders that it fails to carry out or does not carry out in time and for any losses as a consequence thereof except in the case of gross negligence.
- 7.3 The Bank accepts no liability for losses suffered by Clients or any other Authorised User as a result of their failure to meet their contractual obligations towards third parties or for direct, indirect or consequential losses such as loss of earnings or third-party claims.
- 7.4 E-Services traffic runs via an open network, the Internet, which uses public telecommunication channels without any special protection. The Bank accepts no liability for losses resulting from the use of the Internet (incl. via mobile end devices). In particular the Bank accepts no liability for losses suffered by the Client or any other Authorised User as a result of transmission errors, technical faults, malfunctions, illegal intrusion into network equipment, network overload, malicious blocking of electronic access by third parties, Internet malfunctions, interruptions or other shortcomings on the part of network operators.
- 7.5 The Bank accepts no liability for the consequences of malfunctions or interruptions, in particular in processing, in the Bank's E-Services operation (e.g. caused by illegal hacking into the Bank's system), except in the case of gross negligence.
- 7.6 The Bank accepts no liability for any software or mobile end device application supplied by it (e.g. on CD or via download) or for any consequences that result from or during the transportation of the software via the network (e.g. Internet).
- 7.7 If the Bank discovers security risks, it reserves the right to suspend its E-Services without prior notice to the Authorised User temporarily at any time in order to protect the Client until these risks are eliminated. The Bank is likewise entitled to interrupt the relevant services for maintenance works without prior notice to the Authorised User. The Bank does not accept liability for any losses arising from such interruptions.
- 7.8 In the case of slight negligence the Bank does not accept liability for losses caused by its auxiliary staff in the performance of their work.
- 7.9 The Bank is entitled to engage third party specialists to optimise the E-Services it offers as set out in the Bank's

“**General Terms and Conditions**”. In this case it undertakes only to exercise due care in selecting and instructing third parties who are otherwise bound by applicable UK confidentiality provisions.

- 7.10** The Bank does not accept any responsibility for the computer or mobile end device of the Authorised User, technical access to the E-Services or for the software required for it.

8. Security

- 8.1** In order to protect the Client, a multi-level security system has been developed which uses amongst other things an encryption procedure. However, absolute security cannot be guaranteed: the Authorised User's computer or mobile end device, the third party provider's computers and the public networks which form part of the E-Services system as a whole may be subject to security breaches or other risks which are outside the Bank's direct or indirect control.
- 8.2** The Client or any other Authorised User acknowledges the following additional risks, for which the Bank cannot accept any liability:
- Insufficient knowledge of the system on the part of the Authorised User and inadequate security measures on the computer or mobile end device of the Authorised User may make it easier for unauthorised parties to enter the system (e.g. inadequately protected storage of data on the hard disk, file transfers, display insight by unauthorised third parties etc.). It is the responsibility of the Authorised User to obtain information about the necessary security measures.
 - It is impossible to exclude the possibility of traffic monitoring by network operators (e.g. Internet service providers); this means a network operator may be able to track when the Authorised User has made contact with whom.
 - There is a latent risk that a third party may gain access to the computer or mobile end device of the Authorised User without being detected while they are using E-Services (e.g. via Java or ActiveX application).
 - When using a public network (e.g. the Internet) there is a danger that viruses or other harmful programs (e.g. trojans or spyware) may infect the end user's computer or mobile end device if the computer or mobile end device is connected to the Internet. Virus-scanning programs with active updates, a secure firewall, a high security level on the used internet browser and an operating system with current service packs applied may support the Authorised User in their security measures.
 - It is important that the Authorised User only work with software from trustworthy sources.
 - The availability of the Internet or mobile end device network cannot be guaranteed. In particular it is possible that transmission errors, technical faults, malfunctions, illegal intrusion into network equipment, network overload, malicious blocking of electronic access by third parties, interruptions or other shortcomings on the part of network operators may occur.
 - Data downloaded by the Authorised User while using E-Services (e.g. Client data such as overviews of accounts, safe custody and metal accounts) are automatically placed in temporary storage by the Authorised User's browser software on the Authorised User's computer or mobile end device (temporary Internet files/cache). At the same time the Authorised User's browser software stores all the Internet addresses (history) accessed by the Authorised User. This can enable a third party who gains access to the Authorised User's computer or mobile end device to access Client data and draw conclusions about an existing banking relationship. The Bank therefore recommends that the cache and history be cleared at the end of every use of E-services and to restart the Internet browser or other E-Services access software before every E-Services session.
 - Client data exported from E-Services into other programs (e.g. Excel, Word etc.) by the Authorised User or filed electronic bank documents will be filed unprotected on the computer or the mobile end device if the Authorised User fails to take any further precautions. This may enable a third party gaining access to the computer or the mobile end device of the Authorised User to access Client data and draw conclusions about an existing banking relationship.
- 8.3** When using E-Services, cookies (strings of information sent by a website and stored on the Authorised User's computer or mobile end device) will be temporarily stored or accessed on the Authorised User's computer or mobile end device. In this way the Bank is able to provide navigation shortcuts for the benefit of the Authorised User. Only a minimum of information will be stored in the cookies created by the Bank. By modifying the Internet browser or other E-Services access software settings it is possible to prevent cookies being placed on a computer or mobile end device. Depending on the browser or other access software settings selected, it is possible that blocked cookies may reduce the functionality of E-Services or prevent access to them. The Bank accepts no liability for such restriction.

9. E-Services block

- 9.1** The Client can block his own access and that of any Authorised User to the Bank's E-Services, while an Authorised User other than the Client can only block his own access. A request for access to be blocked can only be made during normal business hours on bank working days of the Bank. A request to the Bank for access to be blocked should be confirmed to the Bank in writing immediately thereafter.
- 9.2** In addition, the Authorised User may block his own access within the E-Services system.
- 9.3** Any blocks can be cancelled upon request by the Client to the Bank. The request should be submitted or confirmed by the Client to the Bank in writing. Authorised Users other than the Client can only remove blocks they have placed themselves on their own access.
- 9.4** The Bank is entitled to block Authorised Users from accessing individual services or all services at any time without

stating reasons or giving prior notice if, in the Bank's sole discretion, this is appropriate under the circumstances (primarily to protect the Client). The Bank accepts no liability for losses resulting from such a block.

10. Data Protection/Confidentiality and service providers

10.1 Information about how the Bank treats Client data under applicable data protection law can also be found in the Bank's "**General Terms and Conditions**". The Client should in particular be aware, and ensure that any Authorised User other than the Client is aware, that personal data regarding the Client or any Authorised User other than the Client may be transmitted to jurisdictions which do not have data protection laws as strict as those in the European Union.

10.2 Data may be transported amongst other things via an open network that is accessible to the public (e.g the Internet and/or mobile end device networks). This also applies to data sent by e-mail or SMS. Consequently, data is frequently transmitted across borders without controls. This can even happen with a data transfer where the sender and recipient are situated in UK.

With the exception of e-mail and SMS, individual data is transmitted in encrypted format within the E-Services system. However, the sender and recipient are identifiable. They can be seen by third parties. It is therefore possible for a third party to draw conclusions about an existing business relationship.

10.3 In accordance with the Bank's "**General Terms and Conditions**" governing the Client's business relationship with the Bank, the Client understands and accepts that the Bank may, at its sole discretion, use the services of affiliated companies and third parties for the provision of E-Services, and to this end may send anonymised and/or non-anonymised data relating to the Client and his business relationship with the Bank to such parties. The Bank will ensure that these service providers are bound by appropriate confidentiality and data protection obligations and non-disclosure agreements.

11. E-mail and SMS/Messages

11.1 E-mails and SMS

The transmission of e-mails and SMS via public networks (e.g. the Internet) are unencrypted and they may be intercepted, read and altered by third parties. This also applies for e-mails and SMS which are deployed in the use of E-Services of the Bank (including SMS for log-in and transaction signing). Subject to any separate agreements, messages and orders by e-mail and SMS are not binding for the Bank for reasons of security. The Bank never accepts liability for losses incurred from the use of e-mail and SMS. Although the SMS services are provided by the Bank free of charge, costs for provision of SMS may be charged to the Authorised User by their mobile end device provider for SMS service. The Bank excludes any liability for these costs.

The Bank is authorised but not obliged to reply by e-mail to e-mails from the Authorised User.

The Bank cannot provide any guarantee that the information and notifications sent by e-mail or SMS at the request of the Authorised User will be received by the Authorised User or that they will arrive without delay.

Subject to any separate agreements, payment orders may not be submitted by e-mail and SMS. The Bank does not accept liability for any losses resulting from the non-execution of such payment orders.

11.2 Messages via the E-Services mailbox

In addition to the e-mail message channel, every Authorised User is provided with a mailbox within E-Services in which messages can be received from the Bank and sent to the Bank. These messages are encrypted. Sending or accessing these messages requires a successful identification check of the Authorised User with the Authorised User's personal E-Services authentication features.

A message from the Bank to the Authorised User is deemed to have been received when it is available for downloading from his E-Services mailbox. The Authorised User is responsible for taking note in good time of the message addressed to him. The Authorised User has the option of being notified by e-mail or SMS of the arrival of a new message. Such information is sent unencrypted via public networks and therefore provides no protection of confidentiality. Furthermore, the Bank cannot accept responsibility for notifications reaching the Authorised User or for them arriving in time.

Messages or instructions sent to the Bank via the E-Services mailbox are checked, replied to or processed within the framework of the existing business processes during normal business hours on bank working days. They do not have priority for processing. On the basis of the self-legitimation which takes place, the Bank may assume that instructions which it receives via the E-Services mailbox have come from the Authorised User and may execute the instructions. However, no messages or instructions that are critical in terms of time or associated with a deadline (e.g. payment transactions, financial instrument transactions, cancellations of orders, credit card blocks etc.) must be sent to the Bank via the E-Services mailbox. Subject to any separate agreements, Authorised Users may only give instructions on the basis of their actual authorisation on the account, safe custody and metal account.

The Bank is entitled, without prior announcement, to delete from the E-Services mailbox of the Authorised User messages that are older than 12 months or if a maximum storage space per user is exceeded. The deletion is carried out without regard to the aforementioned period in the case of termination of an account, safe custody and/or metal account for which the messages are sent or if the "**Agreement for the use of E-Services**" is terminated. It is the responsibility of the Authorised User to download and save the messages beforehand. The Bank accepts no liability for losses caused by the deletion of messages.

12. Conditions governing Authorised Representatives

- 12.1** In this agreement, an Authorised Representative refers to someone who has been granted access to use E-Services by the Client as an Authorised User via form “**Authorisation to use E-Services**” Any such Authorised Representative’s E-Services access remains in place unless the aforementioned underlying authorisation is expressly revoked.
- 12.2** The Authorised Representative shall maintain his E-Services access even in the event of death, incapacity to act or bankruptcy of the Client and any E-Services access authorisation shall remain in force until the Bank receives a notice of cancellation in writing by the Client or any of the Client’s duly authorised heirs, executors or personal representatives. All actions by the Bank pursuant to an existing E-Services access authorisation prior to receipt of such notice of cancellation shall be binding on the Client and any of the Client’s duly authorised heirs, executors or personal representatives. The Authorised Representative is aware that he must protect the interests of the Client’s duly authorised heirs, executors or personal representatives after the Client’s death, incapacity to act or bankruptcy. The Authorised Representative must obtain instructions from the Client’s duly authorised heirs, executors or personal representatives and is accountable to them. The Bank reserves the right to make any dealings on the part of the Client’s Authorised Representative dependent on the submission of documents required under applicable inheritance or other laws and/or the written consent of the Client’s duly authorised heirs, executors or personal representatives.
- 12.3** The cancellation of a standard authorisation (e.g. power of attorney or authorised signatory right) does not automatically result in the revocation of an Authorised Representative’s E-Services access; the Authorised Representative’s E-Services access must be explicitly revoked as specified in clause 12.1 above. Similarly, the revocation of the Authorised Representative’s E-Services access does not automatically result in the revocation of a standard authorisation. However, the Bank reserves the right to make an Authorised Representative’s E-Services access dependent on the existence of a standard authorisation.
- 12.4** It is at the Bank’s sole discretion whether it requires separate authorisations for additional functionalities made available via E-Services. In such a case, the provisions of clauses 12.1 – 12.3 above apply as well.

13. Foreign laws/import and export restrictions

- 13.1** The use of the Bank’s E-Services abroad may contravene the laws of a foreign country under certain circumstances. The Authorised User shall be responsible for finding out about and complying with all relevant restrictions and laws. At the same time, the Bank may at any time and without prior notice restrict its service offering to Authorised Users abroad via E-Services due to local restrictions. The Bank does not accept any liability in this regard.
- 13.2** Authentication features or procedures (e.g. via encryption algorithms) to access E-Services may be subject to specific import/export restrictions as well as restrictions of use abroad. Furthermore, country-specific restrictions in regard to authentication features may exist if the Authorised User is travelling to third countries. The Authorised User shall be responsible for finding out about and complying with all relevant restrictions and laws. The Bank does not accept any liability in this regard.

14. Amendments to these conditions

The Bank reserves the right to amend these conditions, its E-Services offering and its fee schedule at any time. Any such amendment will be notified to the Client and any Authorised User other than the Client via E-Services or in another appropriate manner. Any additional provisions or amendments or modifications to existing provisions, agreements and services shall be regarded as accepted with binding effect by the Client and any Authorised User other than the Client upon the next E-Services access by an Authorised User by using the personal means of authorisation, but in any event when the relevant service is first used by an Authorised User.

15. Termination

Either the Client, his duly authorised heirs, executors or personal representatives as well as the Bank can terminate the “**Agreement for the use of E-Services**” and any associated supplementary agreements at any time. Any termination must be confirmed in writing and must be forwarded to the Bank as set out in the Bank’s “**General Terms and Conditions**”.

16. Validity of other legal regulations

The validity of other provisions of law, in particular those governing the operation and use of telecommunications equipment and networks, is not affected by these conditions and they apply to the Bank’s E-Services as soon as they come into effect.

17. Severability

The invalidity, illegality or unenforceability of one or more clauses of these conditions does not affect the validity of the rest of the agreement.

18. Applicable law and jurisdiction

These conditions shall be governed by and construed in accordance with Gibraltar law. The laws of Gibraltar will govern the Bank and the Client's relations prior to the conclusion of these conditions. The Client irrevocably agrees that the courts of Gibraltar are to have exclusive jurisdiction to settle any disputes which may arise out of or in connection with these conditions and the Client agrees to submit to the jurisdiction of those courts. Nothing in this clause limits the Bank's right to take proceedings against the Client in any court of competent jurisdiction nor will the taking of proceedings in one or more jurisdictions preclude the taking proceedings in any other jurisdiction, whether concurrently or not.