

ADDITIONAL CONDITIONS REGARDING THE USE OF EFG EBANKING

The eBanking facility called “EFG eBanking” is made available to clients of EFG Bank (“EFG”) worldwide, and in the case of Clients of EFG Bank AG, Singapore Branch (“the Bank”), subject to the following Additional Conditions which are supplemental to its General Conditions. To the extent varied and amended by the terms of these Additional Conditions, the General Conditions of the Bank shall continue to apply and be in full force and effect. Words and expressions defined in the General Conditions have the same meaning in these Additional Conditions unless separately defined below:

Access to the EFG eBanking Services

1. All persons identified as users according to the “logon procedure” are authorised to have access to the EFG eBanking services. The elements necessary for successful logon are:
 - The Username
 - The Password
 - The Authentication Code
2. The password is determined by the Client and/or by the person with authorised access, and indicated in the enrolment form for EFG eBanking and/or in the Third Party Authorisation. The password must be modified by the authorised user when using the service for the first time (see “Security and Liability” below).
3. By signing the enrolment form, the Client confirms that he/she is fully aware of the risks involved in the logon procedure (for example: fraudulent use or user blockage following errors), and that he/she assumes these risks. At the same time, the Client confirms that he/she is familiar with and fully aware of the risks involved with the use of public networks such as the Internet.
4. Whoever has been duly identified according to the logon procedure described in point 1 shall be an “authorised user” for the purposes of these Additional Conditions and EFG shall be under no duty to further verify the identity or authorisation of any such person. Within the limits of the conditions stipulated in the enrolment form and/or in the Third Party Authorisation form, and without any additional monitoring procedure by EFG, each user and/or the third party authorised user may have access to the EFG eBanking services.
5. EFG reserves the right to deny, at its discretion, the use of EFG eBanking or to request that the authorised user provides additional identification to the satisfaction of EFG. EFG is under no obligation to justify any such action, nor shall the acceptance of an authorised user in good faith without further identification give rise to any liability on the part of EFG.
6. The Client represents and warrants to the Bank that he is an accredited investor for the purposes of the Securities and Futures Act (Cap. 289) and hereby requests the Bank not to provide him with periodic statements of account (as referred to in regulation 40 of the Securities and Futures (Licensing and Conduct of Business) Regulations).
7. The Client further consents to the Bank making available to him, via the eBanking services, information, statements, contract notes/advice and communications from the Bank relating to the Client’s Transactions and balances in the Client’s Account (s), as well as correspondence or notifications received from third parties relating to the Client’s Accounts (s), including any demand of payment, margin calls or other documents of any nature which may have legal consequences to the Client (collectively, the “Correspondence”). Such Correspondence shall be deemed to have been validly transmitted to and received by the Client on the date they bear and with the same positive force as those sent by postal mail. The Bank will send email and/or SMS notification to the Client’s email address and/or telephone number in the Bank’s records when the Correspondence are available for viewing in eBanking. Please see points 35 to 41 below for the terms and conditions relating to SMS/Email notifications.

Due Diligence

8. The Client and persons authorised by the Client are under the obligation to keep secret the means of identification associated with the logon procedure in order to prevent fraudulent, unauthorised or abusive use. In particular, the different means of identification (e.g. password and User ID) must be kept separately and should never be stored electronically. The client bears all responsibility for loss or damage resulting from the abusive use of EFG eBanking by persons authorised by the Client (see further “Security and Liability” below).
9. The Client is equally responsible for ensuring that all persons authorised by him/her to have access to EFG eBanking observe the General and Additional Conditions of the Bank.
10. The Client confirms that he/she is fully aware of the inherent risks involved with online services (such as computer viruses and unauthorised third party access). The Client commits to take all necessary security measures and assumes all risks connected to unauthorised or fraudulent use of EFG eBanking.
11. Should there be any doubt as to the confidentiality of the means of identification, it is the responsibility of the Client and/or all authorised users to immediately remedy the situation by informing EFG by telephone followed by a written confirmation.
12. The Client or authorised user is under the obligation to inform EFG without delay of the loss, theft or disappearance of the Entrust Hard Token so that EFG may take adequate measures (see further “Security and Liability” below).
13. If for any reason the Client is unable to notify EFG in a timely manner of an impending risk or potential abuse of EFG eBanking, it is his/her responsibility to immediately block the access to the services (see below point 18).

Exclusion of EFG’s Responsibility

14. EFG provides access to the EFG eBanking as a convenience to the Client only. EFG assumes no responsibility for the accuracy and completeness of the data and information accessible to the Client through EFG eBanking (account and deposit information, transactions, market rates, exchange rates, etc.) and in the event of any discrepancy, the account statements and records of EFG shall prevail. Furthermore, EFG cannot guarantee that the information available reflects the reality of the situation at the moment of consultation, in particular taking into account the time necessary for the execution of transactions.
15. Except when otherwise stipulated, the information accessible to the Client through EFG eBanking does not constitute binding offers on the part of EFG, and any proposed transaction is subject to acceptance by EFG.
16. EFG shall have no responsibility for financial loss or physical damage incurred by the Client as a result of technical deficiencies (transmission errors, network overload, interference, interruption

of service, maintenance, unauthorised third party access, etc.). Furthermore, EFG assumes no responsibility for financial loss or physical damage caused to the Client's or authorised user's equipment or the data stored therein. The Client fully understands and accepts the risks associated with this service and will hold harmless and indemnify EFG against all claims, losses, damages, costs and expenses (including legal costs on a full indemnity basis) which may be incurred in connection with this service unless the same arises directly from gross negligence, willful misconduct or fraud of EFG.

17. EFG is not responsible for providing any material or equipment required for the use of the service, nor is EFG responsible for ensuring the proper installation or functionality of any such material and equipment. EFG assumes no responsibility arising in connection with the downloading or use of software by the Client or authorised user.
18. If EFG has any doubt as to the reliability of the security measures, EFG has the liberty to interrupt the services of EFG eBanking without notice and for so long as EFG may consider necessary. EFG will not bear any responsibility for direct or indirect damages that may result from such interruption.
19. The servers for EFG eBanking are located in Switzerland. The use of EFG eBanking services outside Swiss territory may be subject to foreign legislation (encryption methods, import and export restrictions etc.). It is the user's duty to obtain the necessary information and EFG assumes no responsibility for losses or damages caused by the use of EFG eBanking services from other countries.
20. Without prejudice to the generality of clause 2 of the General Conditions, where the Client has requested the Bank to permit the Client to give Instructions to the Bank via the use of the eBanking services, and the Bank has agreed to do so, all risks attaching to the same, and in particular (but without limitation) risks of forgery or abuse, shall be borne solely by the Client. Any such Instructions shall only be regarded as having been received by the Bank upon the Bank providing written acknowledgement of receipt (via the e-Banking services) to the Client. Notwithstanding the foregoing, the Bank's receipt or acknowledgement of any such Instructions shall not (unless otherwise expressly stated by the Bank) be regarded as the Bank's acceptance or agreement to act on any such Instruction and the Bank shall always retain the sole discretion whether to act or to refrain from acting on any Instructions of the Client or part thereof. The Bank shall have no liability to the Client for any refusal to act on all or part of any such Instruction. The Bank shall also not be liable for any failure, delay or inability to process or to act on any Instructions.

Blockage of Access to EFG eBanking Services

21. If necessary, a user may block his/her access to EFG eBanking services by inputting the wrong password 3 times. The access may only be reinstated through written request of the Client.
22. EFG may also block the access to EFG eBanking services without providing any reason or warning, in the event that EFG considers it to be necessary in its absolute discretion. EFG assumes no responsibility for any loss or damage incurred, including (but not limited to) loss of profit.

Portfolio Validation for Hold Mail Clients

23. EFG eBanking provides validation of portfolio balance for Clients who subscribed to Hold Mail service provided by the Bank. The Client and/or appointed authorised signatories with general authority to deal with the accounts may validate Client's portfolio balance via EFG eBanking if mail held by the Bank ("hold mail") at Client's request is not collected within the required period. The Client acknowledges that hold mail shall be deemed to have thereupon been duly delivered to the Client or destroyed on the date of validation of portfolio balance via EFG eBanking.

Banking Secrecy

24. All Client information maintained on the servers for EFG eBanking is protected by the current local legislation on banking secrecy, which applies only to Singapore. The Client is aware of the fact that the Internet network is an open one and that any data transmitted may migrate beyond the borders of Singapore.

Fees

25. EFG may charge fees for certain EFG eBanking services according to a rate variable at any time. The respective services and fees shall be communicated to the Client in advance. EFG is authorised to debit the said fees from the Client's account.

Amendment to the Services

26. EFG may freely amend or update the present conditions as well as the services provided.

Cancellation

27. Both the Client and EFG have the right to cancel in writing the use of EFG eBanking at any time and without prior notice.

Security and Liability

28. The Client will be liable for all losses if the Client or any other authorised user has acted fraudulently in the conduct of EFG eBanking. The Client may also be held liable by EFG for all losses if the Client or any authorised user has acted with gross negligence. This may include cases where the Client knowingly allows the use by others (whether or not an authorised user) of their Entrust Hard Token, or if the Client fails to follow the safeguards set out in points 26 to 28 below if such failure has caused the losses.
29. In selecting passwords, it is not suitable to use easily accessible personal information such as telephone numbers or date of birth or a recognisable part of the Client's name.
30. The Client must take reasonable steps to keep the Entrust Hard Token safe and the password secret and to access EFG eBanking in a secure manner to prevent fraud or abuse. In particular, the Client (and any other authorised user):
 - (a) Should not allow anyone else to use the password or disclose their passwords to anyone including EFG staff or the Police. EFG staff will never ask for the Client's password. If in doubt, the Client should immediately contact EFG;
 - (b) Should never write down the password on the Entrust Hard Token or on anything usually kept with or near it;
 - (c) Should not write down or record the password without disguising it;
 - (d) Should not disclose their personal information such as information on their identity card or passport, addresses or bank accounts to any persons failing to prove their identities or any doubtful websites;
 - (e) Should not attempt to access EFG eBanking services through public or shared computers (e.g. at cyber cafes or public libraries), or through hyperlinks embedded in e-mails unless the Client or authorised user has verified the genuineness of the website such as the validity of the digital certificate of the website.
31. The Client and any other authorized user must inform EFG as soon as reasonably practicable after they discover or have reason to believe that their password or Entrust Hard Token has been compromised, lost or stolen, or that unauthorised transactions have been conducted over their accounts.

32. The Client and any other authorised user should also:

- (a) Ensure that their PCs are securely configured and that they are adequately protected from computer viruses and malicious programs, for example, by installing a personal firewall and regularly updating their anti-virus software; and
- (b) Refer to any further security advice provided by EFG from time to time.

Reporting Security Incidents or Complaints

33. The Client should report any actual or suspected loss of the Entrust Hard Token or possible security breach in respect of any password or any complaint in regard to the operation of EFG eBanking to his/her Client Relationship Officer.

Data Privacy

34. The Client confirms that any data in regard to the Client or any other authorised user collected by or in the possession of the Bank in connection with EFG eBanking may be transferred to EFG in Switzerland and stored on its servers in that jurisdiction in order to provide EFG eBanking services and acknowledges that it will not be possible to provide such services without transferring the relative data out of Singapore.

SMS / Email Notifications

35. At its sole discretion the Bank may (but shall not be obliged to) send the Client notifications of Transactions, funds transfers or other information which the Bank believes may be relevant, by SMS to the mobile telephone number and/or electronic mail to the Email address provided by the Client to the Bank for the purpose either in the Account and Trading Mandate or in any other written request to the Bank from time to time.
36. The Client acknowledges and accepts that each notification may be sent to the Client without being encrypted and may include the Client's name and information pertaining to the Account (s).
37. The Client may receive notifications through a SMS-enabled mobile phone, an Email account that is accessed via a personal computer, or both. The Client is responsible to ensure the security of the designated mobile phone and/or Email account and any relevant passwords. Accordingly, the Client shall hold the Bank free and harmless and indemnify the Bank against any and all loss, damages, costs and expenses (including legal costs on a full indemnity basis), liability, administrative, civil or criminal, including but not limited to those relating to secrecy laws or regulations, should any notification which may include the Client's name and information pertaining to the Account (s) be viewed or accessed by persons other than the Client.
38. The Client is also responsible to determine if the mobile phone service provider supports text messaging and the mobile phone is capable of receiving SMS messages. The SMS and/or Email notification service is subject to the terms and conditions of the Client's agreement (s) with the Client's mobile phone carrier and/or Internet service provider. The Client is responsible for any fees imposed by the Client's mobile phone service and Internet service provider of any kind whatsoever.
39. The Client acknowledges and agrees that the receipt of any SMS and/or Email notifications may be delayed or prevented by factor (s) affecting the mobile phone service provider (s) or Internet service provider (s) and other factors outside the Bank's control. The Bank neither guarantees the delivery nor the accuracy of the contents of each notification. The Client agrees to hold the Bank, its directors, officers, employees and agents free and harmless and to indemnify the Bank from any and all losses, damages, costs and expenses (including costs on a full indemnity basis), that may arise, directly or indirectly, in whole or in part, from:

- (a) a non-delivery, delayed delivery, or the misdirected delivery of an SMS and/or Email notification;
- (b) inaccurate or incomplete content in an SMS and/or Email notification;
- (c) the Client's reliance on or use of the information provided in an SMS and/or Email notification for any purpose;
- (d) any third party, whether authorized or not, obtaining information on the Client's Account (s) disclosed in the SMS and/or Email notifications by accessing the Client's mobile phone or Email account.

40. Any SMS and/or Email notifications will be given in addition to and not in place of any formal confirmations which the Bank is required to send to the Client and will be sent for information purposes only. The Bank shall not be liable to the Client for any loss of any nature arising from use of, or failure to use, the SMS and/or Email notifications. In the event of any conflict or discrepancy between an SMS and/or Email notification and a Transaction Confirmation, the latter shall prevail but the Client should separately notify the Bank promptly upon receipt of any SMS and/or Email notification which appear to be irregular or not to reflect the Client's understanding of the Transaction to which it relates. However, SMS and/or E-mail notifications are one-way communications from the Bank to the Client only and the Client should not reply to such messages by SMS and/or Email. Any reply purporting to come from a Client in response to an SMS and/or Email notifications may not be received by the Bank, and if received will not be acted upon.
41. The Bank reserves the right to terminate the SMS and/or Email notifications at any time without prior notice to the Client.