EFG Bank AG, Hong Kong Branch
Incorporated in Switzerland with limited liability

EFG HONG KONG EBANKING PRIVACY STATEMENT

EFG Bank AG Hong Kong are committed to offering you a secure and private online banking experience, protecting your information, including, but not limited to, your personal and transaction data and any unique online identifiers (collectively the "data"), in a secure and managed environment.

Our protection strategies as well as continuous evolution enforce our security measures, in response to technological changes and emerging threats. We work in partnership with you to protect your online activities through this eBanking website (the "site").

This Statement should be read in conjunction with our Statement of Practice to the Personal Data (Privacy) Ordinance (Chapter 486) in the Hong Kong SAR.

We will only collect your data for the purpose of providing service (s) to you.

Your data will only be accessed by our authorised staff and/or agents whom are governed by our confidentiality policies.

Both you and EFG have an important role in protecting your data as well as preventing any fraud.

All your communications with this site over the public internet is encrypted using 128-bit Secure Socket Layer (SSL) encryption technology – an industry standard for encryption over internet to protect data.

This site uses an extended validity (EV) digital certificate to prove its identity. The certification process has undergone extensive verification and is intended to provide the highest level of confidence of the authenticity of this site.

For security, this site applies two-level authentication for user logon, namely:

- logon credentials, i.e. username and password;
- a one-time-passcode generated by an electronic token assigned exclusively for you.

To help protect your account from password guessing, an intrusion lock will be applied to block access to this site upon three consecutive incorrect password and/or one-time-passcode attempts. In that event, please contact your CRO/relationship manager to reinstate your service accordingly.

In addition, an online session will be terminated after 20 minutes of inactivity to prevent unauthorised access in case, for example, you leave your device unattended or you do not log off at the end of your session.

This site may use cookies, spotlight tags, web beacons and the like (collectively the "cookies") to record your visit behavior and use patterns, but no personal or transaction data, for our analysis and to improve our service (s). Cookies are small bits of information that are stored on the web browser in your computer or other device and which can be retrieved by this site. Most browsers allow "cookies" by default, but you may disable them, at your discretion, in the browser settings. Nevertheless, by turning off cookies you may not be able to take full advantage of the functionality of this site.

This site provides a secure messaging function to facilitate communication with us. This is subject to availability from time to time but when you utilize this function all your messages to us will be saved and transmitted within our secure environment. However, you should note that secure messaging is for general communications with us and may not be used to communicate any Instructions or effect order placement.

To enhance data security, you can help protect your information and improve your online banking experience by doing the following:

- Validate website authenticity by checking the relative certificates;
- Install a Firewall and Antivirus software and apply up-to-date rules and updates on your computer;
- Do not open any suspicious emails and attachments;
- Do not click on any hyperlinks embedded in emails without any validation;
- Promptly apply patches and security updates for your operating system, applications, plug-ins, and other software;
- Secure your wireless network by enabling a robust encryption algorithm;
- Clean up your browsing history regularly;
- Erase the cache regularly;
- Erase any confidential downloads;
- Close the browser window after ending an online session;
- Do not enable 'AutoComplete' function of your browser or plug-ins which may store confidential information on your computer;
- Safeguard your logon credentials (username and password) and token
- do not share your credentials with anyone, including Bank staff, Police or other authorities. EFG staff will never ask for your password;
- change your password regularly;
- do not create your password with easily guessed codes, such as date of birth, telephone number, and other personal identifiers for yourself or family members;
- keep your token safely;
- Do not use any administrator mode or privileged accounts for day-to-day use;
- Never write down your password on the token or keep it with it;
- Do not write down or record the password without disguising it;
- Do not disclose personal identity information, such as identity card, passport, address, bank accounts or similar identifiers to any persons failing to prove their identity or on any doubtful websites;
- Do not attempt to access internet banking services through public or shared computers (such as cyber cafes, public libraries and the like);
- Refer to any further security advice issued by EFG from time to time;
- Do not connect to third party intermediary account aggregation service and not managed by EFG;
- Remove file, printer and other resource sharing on your device connecting to the internet;
- If in doubt, contact EFG immediately.

EFG reserves the right to revise this Statement in accordance with any changes to applicable laws and regulations and also to reflect the continuous development of best market practice.

Should you have any queries, concerns or complaints in relation to data privacy, please contact

The Data Protection Officer
EFG Bank AG, Hong Kong
18/F, International Commerce Centre
1 Austin Road West, Kowloon, Hong Kong
Tel: +852 2298 3152
Fax: +852 2298 3400

EFG Bank AG, 瑞士盈丰银行股份有限公司