CCB 中国建设银行(马来西亚)
China Construction Bank (Malaysia) Berhad
Company No. 201601032761 (1203702-U)

Security Statement

China Construction Bank (Malaysia) Berhad (“CCBM”) commits to ensure all data and information transacted at CCBM are secured and confidential. CCBM has put in place policies, procedures and mechanisms to meet the required security requirements.

The security mechanisms that CCBM implements includes but are not limited to the following:

1. Anti-Virus Software;
2. Firewalls;
3. Secure Sockets Layer (SSL)/ Transport Layer Security (TLS);
4. Username and password protection;
5. Encryption; and
6. Account locking.

What can you do to Protect Yourself?

1. Password/PIN is the key to your account information. User ID and password/PIN allow you to access to your account via CCBM’s internet banking services. A strong and unique password is an important protection to help you conduct safer and more secured online transactions. You must ensure ONLY you know the password/PIN and ONLY you have access to the account. Below are some suggested ways on how you can protect your passwords/PIN.

    - Do not share your password with your spouse, friends, relatives or anyone. Your password and PIN are designed to protect the safety and privacy of your banking information. This will only be effective if you keep them private. Change your password frequently.

    - Create strong and unique passwords that are hard to guess. Don't use personal information e.g. your name, birthday, names of your children, etc.

    - Use a combination of letters, numbers and symbols. Passwords with upper and lower case letters, numbers and symbols are harder to guess.

    - Use different passwords for different websites.

    - Never write down your passwords anywhere or record them in your computer, hand phone or smart phone.

    - Always be suspicious when receiving e-mail/SMS/telephone calls requesting you to conduct any form of banking transaction which requires you to use your password/PIN.

    - Do not click on any links or open any attached files found in spam emails/SMS, delete them.

    - Contact CCBM immediately if you feel the security of your password has been compromised.

    - Ensure your computer or mobile devices are protected with effective anti-viruses software.

2. Protecting your computer

   Never leave your computer unattended when you are performing any internet transactions.

   Log off properly after completing your online banking transactions. Follow the secure exit instructions and do not just close your internet browser.

   Lock your computer by activating the screensavers/password protection feature. This is an effective way to prevent others from using your computer when you are away from your computer.

3. Anti-Virus Protection

   Run an anti-virus program on your computer on a regular, frequent basis to prevent computer viruses and worms from entering your computer system. Purchase programs that automatically upgrade your virus protection on a regular basis.

   Learn about computer infections and be aware of the latest computer threats and other malicious programs designed to damage your computer or steal your personal information.

   Do not open e-mail or e-mail attachments from unknown sources. Scan e-mail through your anti-virus software first.

   Never double-click on an e-mail attachment that contains an executable file (such as '.exe' '.com' or '.vbs', etc.) unless you have run anti-virus software first. If a file is infected and opened, the virus can damage your hard drive, program files, and e-mail files.

4. Securing your internet browser

   Clear your cache (information stored in your computer memory) each time you log out. The cache is a temporary storage that keeps all your browsing history. By clearing your cache, it enhances the security of your online experience. The steps for clearing cache in different browser are as below:

   Internet Explorer

   1) Launch Internet Explorer
   2) Click “Tools”
   3) Select “Internet Options”
   4) Go to “Temporary Internet Files” and click “Delete Files”
   5) Followed by “OK”
   6) Click OK again to close the Internet Options window

   Mozilla Firefox

   1) Launch Firefox browser
   2) Click “Tool”
   3) Select “Options”
   4) Click “Privacy”
   5) Go to Clear your recent history and tick all except Site Preferences
   6) Click “Clear Now”
   7) Click “OK” again to close the Options window

Google Chrome

1) Launch Google Chrome
2) Click on the tab next to the URL bar and a drop-down menu will appear
3) Select "Settings" from the menu and a new Chrome browser will appear
4) Go to "Privacy" and click on "Clear Browsing Data…"
5) Tick on the tabs (the first four tabs have been ticked as default). You can tick all the tabs.
6) Then click "Clear Browsing Data"
7) Close the Chrome tab