Usage of ABB Online Banking System - preventive measures of internet security

- **Operating System Configuration / Software Installation**
  - Turn off remote access control features to prevent unauthorized access to your PC.
  - Disable file and print option sharing features to prevent the access of your personal information by unauthorized persons. (For Windows 2000 and Windows XP, this option is enabled by default. It is highly recommended to disable the option before using Online Banking system).
  - Never install software from unknown sources
- **Browser Settings**
  - Use the latest recommended internet browser.
  - Do not use a browser which is beta version.
  - Use the browser that supports TLS or above.
  - Clear any "cache" and "history" to prevent unauthorized access to the temporary files stored in your PC/mobile, which may contain your account information.
    - Cache is normally used to store Web page locally in your computer/mobile. Although our system is set to prevent the saving of your personal and account information of customers in cache, the setting may be affected by the type of browsers used and their configuration.
    - To protect against unauthorized access to your personal and account information by opening the last visited page via the cache, you should clear the cache after logoff as follows:
      - NET Banking

For Internet Explorer

1) Select **Tools** ->**Options** from menu bar;

2) Choose**General** tab;

3) Delete **Temporary internet Files** (as well as all offline contents);

4) Clear **History**

For FireFox

1) Select **Tools** ->**Clear Private Data** from menu bar;

2) Select Browsing **History**, **Cache**, and **OfflineWebsite Data**;

3) Click **Clear Private Data Now**;

5) Click OK

4) Click OK

- **Disable the "auto-complete" features**
  - The "auto-complete" feature is a function provided by browser that automatically complete the entries of Web addresses, forms, usernames and passwords with values from previous input.
    - When you use this function during logon, your username and password will be masked and recorded in your PC/Mobile for future auto completion. Unauthorized persons can logon to Online Banking System since this function auto-completes your logon username and password.
    - To eliminate this risk, the auto-complete function should always be disabled.

      - Internet Browser

For Internet Explorer

1) Open **Internet Explorer**.

2) Choose **Tools** ->**internet Options**.

3) Choose **Content** ->**Auto-complete**.

4) Disable **user names and passwords on forms**.

5) Disable the auto-complete.

6) Click OK.

For FireFox

1) Open **FireFox**.

2) Choose **Tools** ->**Option** from menu bar.

3) Choose **Security**.

4) Disable **Always Remember Password**.

5) Click OK.

6) Select Tool->Clear Private Data from menu bar.

7) Select **Saved Password**.

8) Click **Clear Private Data Now**.

- **Caution to ActiveX Controls**

  An ActiveX control is a type of program that can take complete control of your computer. Data in your computer system may be destroyed if you download an ActiveX control from a web site without ensuring its details and source.

  Before downloading an ActiveX control, you should:

    - Read the information provided on the security certificate to ensure that it is the object you want to download;
    - Read any pre-installed document and make sure that you understand the impact of such installation.
    - Never download the ActiveX control if you have doubts about its source, content and impact on your system.
    - Make sure that the source of the program is from a known publisher;

  - **Safety Level Settings**
    - In Internet Explorer, users are allowed to set the safety level for personalizing the security level of domains, such as not executing cookies or prompting alerts before downloading an ActiveX control.

      You are recommended to set your browser safety level to medium to enhance security.

      1. Select **Tools** from menu bar.
      2. Choose **internet Options ->Security** tab.
      3. Click **internet** and then set the **safety level** to medium.
      4. Click **OK.**.

- **Virus / Malicious Programs**
    - Install and always activate anti-virus software, anti-spyware software, update the software regularly with the latest security files and patches.
    - Activate personal firewall to protect your computer/mobile.
    - Do not download files from unknown sources.
    - Clear the infected files once they are discovered.
    - Do not scan portable disks before using them for copying files to or from your computer.
    - Do not use the PC/mobile if a virus is found until the virus is completely cleared.

    - Do not access doubtful web sites
    - Scan your computer/mobile periodically at least once every 30 days (including all local disks and all file types).
    - Keep yourself updated on the latest information of virus and take necessary precaution
- **Others**
    - Disable any wireless network functions (e.g. Wi-Fi, Bluetooth, NFC) not in use. Choose encrypted networks when using Wi-Fi and remove any unnecessary Wi-Fi connection