

## Security Guidelines for uses of IDEAL™ Services

- a) You should not disclose your IDs or passwords (logon password, token password or any other passwords used to access our Internet service) to any third party. No one at DBS Bank (Hong Kong) Limited will ever ask you for your logon or any other passwords, whether at branches, by telephone, by e-mail or by written request. Please destroy the original printed copy of the password and do not write down or record the IDs/password.
- b) You should choose passwords that are difficult to guess. Do not choose passwords that associate with anything personal such as names, birthdays, telephone numbers or other familiar words. For example, you should set the format of passwords to combinations including both numeric and alphabetic characters. This makes it harder to guess the passwords. Moreover, you should not use the same IDs and password for the access to other internet services;
- c) You should change your initial passwords when you first access the system;
- d) You should change the passwords periodically. Our system will force you to change the logon passwords every three months and you cannot reuse 5 previously used passwords;
- e) You should notify us as soon as practicable if you think that the passwords have been compromised;
- f) You should not leave your computers, token or any terminals, on which you have logged on our Internet service unattended. If you are provided with token for access to our Internet service, please lock your tokens in a safe place;
- g) Once you have finished using our Internet service, please promptly log out from the service;
- h) If the computer used to access our Internet service is likely to be shared with others, you should exercise care. For instance, you should remove the temporary files stored in the memory or in the hard disks of such computer during usage of our Internet service, as the temporary files may contain sensitive information such as account numbers;
- i) You must logon only at our official website for access to our Internet services. Never access our Internet service by using hot-links e.g. from other websites or from e-mails sent to you – these could easily be fake. You may verify that the Internet address is the genuine DBS's website by double clicking the 'lock' icon at the bottom bar of the screen to check the security certificate of DBS.
- j) You should not logon to our Internet service using a publicly available computer e.g. at cyber cafés. Such computers may have hacker programs or otherwise allow other persons to access personal/account information;
- k) You should avoid any unauthorized capturing of your passwords by attackers. For instance, you should exercise extra care in handling doubtful e-mails received or accessing suspicious websites because attackers may make use of these channels to secretly install undetected programs to capture your keystrokes about the passwords;
- l) You should always use the latest recommended Internet browser to ensure that they are using the most updated security features from time to time. You should clear the browser's cache after each session so that the account information is removed, especially if you are using a shared PC;
- m) You should avoid storing PIN/password when using any browser. In Microsoft Internet Explorer 5 or above, the "AutoComplete" function stores and lists possible matches from entries that you have typed previously. You can prevent any passwords (including your PIN) from being stored e.g. in the case of Internet Explorer 5 or above by deactivating the "AutoComplete" function:
  - 1) Launch your Internet Explorer and click on "Tools" >>
  - 2) "Internet Options" >> "Content" Tag.
  - 3) Click on "Settings" under AutoComplete.
  - 4) Uncheck "user names and passwords on forms"
  - 5) Click on "OK" to save the changes.
- n) You should regularly check your account balances and statements to identify unusual transactions.
- o) You should install personal firewall software and anti-virus software. Regularly download updates to your anti-virus software, operating system and internet browser.