# Security Guidelines for Uses of IDEAL™ Services

## Important tips: Safeguard your login information

a) Do not disclose your IDEAL™ login information such as organisation ID, user ID, PIN or any other pins used to any third party. No one at DBS will ever ask you for your login or any other pins. Destroy the original pin mailer and do not write down or record the IDs/pin.

b) Do not choose login information or pins that associate with anything personal such as names, birthdays, telephone numbers or other familiar words to make it difficult to guess. For example, set the format to combinations including both numeric and alphabetic characters. Moreover, you should not use the same IDs and pin for the access to other internet services.

c) Change your login pin periodically.

d) Never access IDEAL™ by using hot-links e.g. from other websites or e-mails – these could easily be fake. Access IDEAL™ via DBS official website through typing the authentic website address on the address bar of the browser or by bookmarking IDEAL™ website and using that for subsequent access. 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.

e) Exercise care if the computer used to access IDEAL™ is likely to be shared with others. For instance, remove the temporary files stored in the memory or in the hard disks of such computer during usage of IDEAL™, as the temporary files may contain sensitive information such as account numbers.

f) Do not enter your User ID, PIN and token One-Time-Password to the website or mobile app of the bank suspicious such as unusual screens pop up and/or your computer or mobile device responds unusually slow, log out from that website or app immediately, scan your computer or device and report to us.

g) Promptly log out from IDEAL™ once finished using the service.

h) Do not logon to IDEAL™ 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.

i) Make sure your personal firewall software and / or anti-virus software is in good state. Regularly download updates to your anti-virus software, operating system and internet browser.

j) Avoid any unauthorized capturing of your pins 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 pins.

k) 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.

l) Do not forward your one time registration code (OTRC) or one time password (OTP) to another device.

m) Avoid storing PIN/pin when using any browser. In Microsoft Internet Explorer, the "AutoComplete" function stores and lists possible matches from entries that you have typed previously. You can prevent any pins (including your PIN) from being stored e.g. (in the case of Internet Explorer by de-activating the "AutoComplete" function:
    1. Launch your Internet Explorer and click on "Tools" >> "Internet Options" >> "Content".
    2. Under "Personal Information", click on "AutoComplete".
    3. Uncheck "User names and password on forms", and click on "Clear Passwords", check “Passwords” and click on “Delete”.
    4. Click on "OK" to save the changes.)

## Important tips: Safeguard your IDEAL™ Security Device

a) If you would leave your computers unattended, please log out IDEAL™ and lock your tokens in a safe place.

b) Change your token PIN regularly by pressing and holding the red button for more than two seconds.

c) Notify DBS on loss of token immediately.

## Important tips: Access IDEAL™ Mobile

a) Do not root or jailbreak your mobile device and install latest security updates.

b) Do not download and install apps from unsecured sources.

c) Ensure that no one is watching you while you enter user ID, PIN or any other sensitive information.

d) Set strong password and screen lock for your mobile device. This can avoid unauthorised use of your device in case it is lost or stolen.

e) Log off IDEAL™ Mobile app after using it, do not just close the app or press the "Home" button because the app still runs in background.

f) Do not share your mobile device with others.

g) Do not save sensitive information such as your account numbers, user ID and PIN in your mobile device.

h) Delete sensitive data such as SMS and Email if they are no longer required.

i) Notify DBS immediately if you change your contact particulars.

j) Check your last IDEAL™ login and notify DBS if there is any dubious login.

k) Disable any wireless network functions (e.g. Wi-Fi, Bluetooth, NFC) not in use. Choose known and encrypted networks when using Wi-Fi and remove any unnecessary Wi-Fi connection settings.

## Notes:

a) Notify us as soon as practicable if you think that the pins have been compromised.

b) Do not enter challenge code into your token if you did not authorise any transaction(s) in IDEAL™. Please note that during the log in process, you will never be asked to input a Challenge/Response.

c) To facilitate your timely detection of unauthorized transactions that may arise as a result of fraudulent activities, system generated post authorisation notification via IDEAL™ Messages, SMS and Email within few minutes upon transactions are approved. Please contact us immediately if your registered mobile phone number or Email address is invalid.

d) Check the relevant notifications and your account balances and statements/advices regularly to identify unusual transactions.

e) Review your IDEAL™ authorisation policies regularly such as adopting dual management control.

f) Always follow our website login instructions and security tips published by us when conducting any financial transactions.

g) If you have not logged in IDEAL™ for a pre-defined period (e.g. 180 days), for security reason, the bank has sole discretion to inactivate or delete your IDEAL™ account without notice and liability to you.

# 使用 IDEAL™ 服務的安全指引

## 重要提示: 保護您的登入資訊

a) 切勿向第三方披露您的 IDEAL™ 登入資訊 (例如: 公司編號，用戶編號，登入密碼或其他用戶密碼)。本行員工不會向您索取您的登入資訊或任何密碼。不要寫下您的用戶編號/密碼並將本行寄給您的密碼通函銷毀。

b) 切勿選用姓名，生日日期，電話號碼等令其他人容易猜到的登入資訊或密碼。例如，登入資訊的格式應以英文字母與數字的組合。並且不要將相同的用戶編號及密碼用在其他網路服務上。

c) 定期變更您的登入密碼。

d) 不要經其他網站或電郵中的超連結登入 IDEAL™ ，這會很大機會進入假冒網站。您必須直接輸入星展的官方網站網址以登入 IDEAL™ 或將 IDEAL™ 網址儲存至瀏覽器書簽留待下次使用。您可以透過雙擊瀏覽器中的 址鎖"“小圖示以查看星展的安全認證。

e) 若於一台與其他人共用的電腦上使用 IDEAL™ 應該特別小心。例如在使用 IDEAL™ 前後清除儲存在您電腦上的暫存檔案，因為暫存檔案可能包含一些敏感資料，例如戶口號碼。

f) 切勿在一些懷疑是假冒銀行的網站或流動應用程式上輸入您的用戶編號，登入密碼或保安編碼機編碼，假如發現一些彈出視窗或您的電腦或流動裝置反應異常地變慢，請立即登出該網站或應用程式，掃描電腦或流動裝置是否有病毒並向本行報告。

g) 當使用完 IDEAL™ ，請立即登出。

h) 切勿使用網吧等公用電腦登入 IDEAL™ ，那些電腦可能已感染黑客軟件，而其他人也可能會取得您的個人/戶口資訊。

i) 確保您的個人防火牆及/或防毒軟件在最佳狀態。定期下載更新到您的防毒軟件，操作系統及瀏覽器。

j) 避免黑客任何非法存取您的登入密碼，例如當您收到一些可疑電郵或訪問可疑網站時要特別小心，因為黑客可能利用這些渠道安裝黑客軟件以套取您的密碼。

k) 必須確保您的瀏覽器更新至本行建議的最新版本，以確保其安裝了最新的安全功能。每次使用完 IDEAL™ 後清除瀏灠器的暫存檔，尤其是當您正在使用共用的電腦。

l) 切勿轉發您的一次專用登記編碼或一次專用密碼至令一台裝置。

m) 避免使用任何瀏覽器的儲存密碼功能。在微軟 Internet Explorer 中， “自動完成” 功能會儲存及顯示您曾經輸入的文字，您可以跟著以下步驟去取消 Internet Explorer 的 “自動完成” 功能以防止您的密碼被自動輸入。

1. 開啟 Internet Explorer ，點擊 “工具” >> “網際網路選項” >> “內容”。
2. 在 “個人資訊” 部份點擊 “自動完成"。
3. 反點選 “表單上的使用者名稱和密碼” ，然後點擊 “清除密碼”，再點選 “密碼” 然後點擊 “刪除”。
4. 點擊 “確定” 以儲存變更。

## 重要提示: 保護您的 IDEAL™ 保安編碼機

a) 如要離開您的電腦，請登出 IDEAL™ 並將您的保安編碼機收藏在安全及已上鎖的地方。

b) 定期更保安編碼機密碼，長按保安編碼機上的紅色鍵。

c) 如遺失保安編碼機, 請立即通知本行。

## 重要提示: 使用 IDEAL™ 流動理財

a) 切勿 root 或 jailbreak 您的流動裝置，並且安裝最新的安全更新。

b) 切勿由不明的來源下載或安裝應用程式。

c) 確保在不被監視下輸入用戶編號，登入密碼或任何敏感資料。

d) 設定嚴謹的密碼和屏幕鎖定功能，這能夠防止非法使用您的流動裝置。

e) 使用完 IDEAL™ Mobile 應用程式後請立即登出，切勿只關閉應用程式或按 “主畫面” 鍵因為應用程式還在背景運行。

f) 切勿把流動裝置借予其他人。

g) 切勿儲存敏感資料例如您的戶口號碼、用戶編號或登入密碼到您的流動裝置。

h) 如無必要保留，請刪除載有敏感資料的短訊及電郵。

i) 如變更了聯絡資料，請立即通知本行。

j) 檢查您的 IDEAL™ 上次登入時間，如發現可疑登入，請立即通知本行。

k) 關閉無需使用的無線網絡功能(如Wi-Fi、藍芽、NFC)。如需使用Wi-Fi，應選用已知及加密的網絡，並移除不必要的Wi-Fi連線設定。

## 備註:

a) 若懷疑您的密碼被盜用，請立即通知本行。

b) 如在 IDEAL™ 不是在進行交易授權，切勿在保安編碼機上輸入密碼提示。請注意，登入 IDEAL™ 過程中。本行不會要求您輸入密碼提示 / 交易編碼。

c) 為了讓您能及時偵測到有可能因詐騙活動所產生的未經授權交易, 當您進行交易，系統會透過 IDEAL™ 訊息, 短訊及電郵在數分鐘內向您發送交易授權後的通知。如發現您的登記手機號碼或電郵地址不正確，請立即通知本行。

d) 定期查看您的戶口結餘及月結單及相關的通知，留意有否異常的交易。

e) 定期檢討您的授權政策，例如採用雙重管理監控。

f) 當進行任何付款交易，必須按照本行網頁的上載有的登入指示及安全指引。

g) 如您超過一段預設的期間 (例如180日) 沒有登入IDEAL™，基於安全考慮，本行可根據本行的獨立判斷權在不通知您及不向您承擔任何責任的情況下將您的 IDEAL™ 賬戶指定為不活動賬戶或將其刪除。