恒生銀行
HANG SENG BANK

E-Channels Security Measures

This document sets out the security measures (as may be revised or updated by Hang Seng Bank or HSBC Group from time to time) for any electronic Profile Banking systems ("**E-Channels**") provided by Hang Seng Bank or any member of the HSBC group (the "**Profile Bank**") to its Profile Owners (the "**Profile Owner**").

The Profile Bank Security Measures

1. The Profile Bank shall employ measures to deny access by unauthorised external parties to the environment in which its internet service operates.
2. The Profile Bank shall ensure that its systems are strictly controlled including having business continuity plans.
3. As part of the Profile Bank's security measures, users authorised by the Profile Owner ("Users") who access the Hang Seng HSBCnet E-Channel may be subject to automatic suspension when they have not logged into Hang Seng HSBCnet within a 6-month period. If a Hang Seng HSBCnet profile is not accessed by any Users within an 18-month period, the Hang Seng HSBCnet profile may also be suspended.
4. If biometric authentication methods (for example fingerprint scan or facial recognition) are used to access an E-Channel from a mobile device, the Profile Bank and associated HSBC entity that provides applications to the mobile device, reserve the right to remove the biometric authentication feature at any time and, if necessary, without notice if there are concerns relating to the security of a device. In normal circumstances it will still be possible to authenticate via the mobile device using other existing methods.

Profile Owner Security Measures

1. The Profile Owner shall only access E-Channels using the authentication methods prescribed by the Profile Bank.
2. The Profile Owner shall ensure that all Users keep their security credentials (password, memorable answer, security answers, Security Device PIN, mobile device password/PIN or any other security credential required to access E-Channels, as applicable) secure and secret at all times and not facilitate any unauthorised use of these credentials. In particular, the Profile Owner shall not share any security credentials or access of an E-Channel with any third party other than a regulated third party service provider that the Profile Owner has authorised.
3. The Profile Owner is responsible for the careful selection of its Users, noting such Users are provided with access to a wide range of capabilities including assigning entitlements to accounts or other services and sending instructions in relation to those accounts or services.
4. The Profile Owner shall notify the Profile Bank promptly if any Security Devices are lost or stolen.
5. The Profile Owner shall:
   (a) promptly take appropriate action to protect any User's profile if it has any suspicion that such User's credentials have been in full or part compromised in any way;
   (b) review recent activity on its accounts and User profiles if it suspects any User's credentials have been compromised and inform the Profile Bank promptly of any discrepancies; and
   (c) regularly review its account and Users' profile activity and entitlements to ensure that there are no irregularities and report any discrepancies promptly to the Profile Bank.
6. The Profile Owner shall promptly remove a User from its E-Channel profile in the event that any such User leaves the Profile Owner's organisation. The Profile Owner shall promptly suspend the use of the E-Channels by any User where there is any concern about the conduct of that User or their entitlements. The Profile Owner shall ensure that security credentials or devices are only used by the specific individual User that they are assigned to other than to a regulated third party service provider that the Profile Owner has authorized.
7. The Profile Owner shall ensure that its Users provide correct, full and unabbreviated details whenever they are required by the Profile Bank. The Profile Owner shall further ensure that their Users regularly review such information and update their details whenever there is a change to their details and do not maintain more than one username or set of security credentials at any time.
8. The Profile Owner shall inform the Profile Bank within seven days of dispatch of a Security Device by the Profile Bank that it has not received the package sent, provided that the Profile Owner is made aware of the dispatch.
9. The Profile Owner shall return any Security Devices to the Profile Bank promptly if requested by the Profile Bank.
10. The Profile Owner shall adopt and review its internal security measures on a regular basis to ensure protection remains up to date and in line with regulatory and industry best practice guidance. These should include, but not be limited to, malware protection, network restrictions, physical access restrictions, remote access restrictions, computer security settings, monitoring of improper usage, guidance on acceptable web browsers and email usage including how to avoid acquiring malware.
11. The Profile Owner shall have processes in place to prevent Users being socially engineered or acting on fraudulent communications. This is to prevent business email compromise and similar schemes where a fraudster sends an email impersonating someone known to the authorised User for an E-Channel and seeking to change an address or Profile Bank account number where payments are to be sent. Such processes should include, for example, where communications are received by Users seemingly from known senders (including, but not limited to, senior management, suppliers and vendors) to ensure the authenticity of those communications are independently verified (through a means other than email).
12. If any E-Channel is accessed by a User via a mobile device, the Profile Owner shall require that the User:
   (a) does not leave the mobile device unattended after logging on to any E-Channels;
   (b) clicks the 'Logout' button when the User is finished accessing any E-Channels;
   (c) enables the mobile device's automatic pass code lock feature;
   (d) does not share mobile devices being used to access E-Channels with others;
   (e) is the only person registered for biometrics (for example, face, fingerprint, voice, retina etc.) on the device;
   (f) takes steps to de-register devices that should no longer be used as an authentication method as envisaged in clause 15; and
   (g) does not access the E-Channel via a mobile device that has been 'jailbroken', 'rooted' or otherwise compromised).
13. The Profile Owner acknowledges and agrees that in the event that its E-Channel is suspended for any reason, any subsequent reactivation of that E-Channel will automatically reinstate all original entitlements, limits, User access and access to the same accounts and services as prior to such suspension.
14. The Profile Owner should be aware that Users accessing an E-Channel via a mobile device can carry out a wide range of activities using the device. This includes utilising the mobile device (for instance in place of a Security Device) to authenticate activities carried out on a separate E-Channel session conducted via a desktop computer.
15. Where Users access E-Channels via biometric authentication measures available on certain mobile devices (for example, fingerprint scan or facial recognition), the Profile Owner acknowledges that such methods of authentication still pose a risk of being compromised or permitting unauthorised access (for instance where close family members are involved).