恒生銀行
HANG SENG BANK

Hang Seng HSBCnet Security Features

2023

Hang Seng Bank's approach to Online Security

Our Bank aims to provide you with a robust, reliable and secure online environment in which to do business. We seek to achieve this through the adoption of 'best of breed' technologies, the formulation of best practice IT policies and procedures, and the dedication of expert resources to their implementation and monitoring. We employ industry-standard solutions to authenticate your identity when you log on, to ensure that your data is transmitted securely and reliably, and that the customer data we hold is protected. We have back-up and contingency plans to ensure interruptions to the service, for whatever reason, are minimized. Drawing on our considerable experience as providers of secure electronic banking systems, we also operate a control and support structure designed to ensure that we address all aspects of the risks faced in providing transactional banking online.

Security features

- Robust authentication processes
- Protection against key-logging and "denial-of-service" attacks
- Two-factor authentication using one-time password generating from physical Security Devices or Soft Token
- Encrypted sessions between customer and the Hang Seng Bank (Transport Layer Security -TLS)
- Protection of sensitive information in transmit and storage to ensure confidentiality of customer data
- Industry-standard security mechanisms to protect the infrastructure
- Regular independent reviews of system's security
- Robust and regularly reviewed information security policies covering systems and installation development and management
- Comprehensive contingency and back-up arrangements
- 24/7 security monitoring and centralized incident management team
- Audit trails for administrative and transactional activities

Hang Seng HSBCnet Authentication

Security credentials and two-factor authentication

Hang Seng HSBCnet aims to authenticate users logging onto the system based on a set of the credentials, each designed to combat various aspects of the risks faced when authenticating identity over the Internet. Hang Seng HSBCnet seeks to authenticate a user's identity in a number of ways, each designed to match the risks associated with the service or function being accessed to an appropriate level of security. These methods include traditional usernames and passwords, supplemented by the use of an additional credential we call a Memorable Question that provides added protection against denial-of-service attacks, and two-factor authentication using one-time-password generating from physical Security Devices / Soft Token.

Higher risk services and functions are protected by two-factor authentication (in the case of physical Security Devices / Soft Token at log on level). Two-factor authentication represents a significant enhancement to traditional password-based security as it is based upon not only something you know – in this case a username and physical Security Device / Soft Token PIN – but also something you must physically possess (i.e. Soft Token enabled mobile devices / physical Security Devices) and something that you are inherent (i.e. Biometrics that enabled in your Soft Token (Touch ID/Face ID/ Fingerprint ID – if enabled). A potential attacker, therefore, must obtain the second or third factor – the physical Security Device / Soft Token enabled mobile device and the PIN / Biometrics that protects it before being able to compromise a user's account, eliminating many of the pervasive risks that arise from the distributed nature of the Internet.

Unauthorized access attempts

If someone tries to access your Hang Seng HSBCnet user account without the proper credentials, the System will lock the account after a number of unsuccessful attempts. However, in order to mitigate the risk of someone maliciously locking your Hang Seng HSBCnet user account, our Bank has implemented denial-of-service protection. This aims to ensure that someone who knows only a user's username is unable to lock out that user's account simply by entering incorrect values when challenged.

Encrypted sessions using TLS

Security sensitive data (e.g. password) is masked on-screen when entered. When being transmitted to our Bank from customer's browser, the transmission of data is encrypted (via TLS-Transport Layer Security). On reaching Hang Seng Bank, this data is encrypted within the databases. Even Hang Seng HSBCnet administrators do not have access to this information.

If someone obtained my credentials and was able to access the system, how could I determine whether that had occurred?

There are facilities within the Hang Seng HSBCnet application that you can use to review activities performed by a specific username.

- When you log in, your main landing page will indicate the last time this account logged in
- Any business or administrative activities performed by the user account can be viewed by the Activity log tools

Security of data transmissions

Both the transmission of security details and all online administrative or transactional activities between you and Hang Seng HSBCnet are encrypted using the TLS protocol. Basic encryption involves the transmission of data from one party to another. The sender encodes the data by scrambling it, then sends it on. The receiver must unscramble the data with the correct 'decoder' in order to read and use it. The effectiveness of encryption is measured in terms of how complex the key used is. The more complex the key, the longer it would take for someone without the correct decoder to break the code. TLS is an industry-standard protocol to secure Internet communications between web browsers and Hang Seng Bank. Our Bank currently supports TLS 1.2 and above.

Data confidentiality and integrity

Hang Seng Bank employs security industry best practices to protect customer or personal data. Our data privacy statement is presented to each user for agreement at the time of registration and details the protection that users are afforded.

In addition, no user's information is written to disc or stored on Internet-facing web servers. The web servers are separated physically from the back-office databases that hold the transaction data. Therefore, no customer transaction information is kept on the web servers. Sensitive data such as passwords are stored in encrypted databases using a hardware security module.

Hang Seng HSBCnet Functional Features

Described below are some of the functional features built into Hang Seng HSBCnet to enable you to more easily control the use of the System.

Access levels

Hang Seng HSBCnet provides two access levels for customer staff. System Administrators can perform (under either dual or sole control) general administrative tasks such as the set up and entitlement of users to Hang Seng HSBCnet tools, and the suspension or deletion of users.
End users have no access to administrative functions. Either type of user can be allocated transactional functionality, but the System is flexible enough to allow for the complete segregation of administrative and transactional functions.

User access control

The access control tool allows your designated Hang Seng HSBCnet System Administrators to determine individual user access rights and entitlements, down to account level viewing and payment authorization limits. The number of users required to authorise a payment can be set, as well as the combinations of user levels for differing values of payments. You can establish a system that requires authorization for payments over a certain value from a separate country or at head office. This enables complete control of access and authorization while allowing payments to be processed efficiently.

Dual authorisation control

All critical administrative and business functions in Hang Seng HSBCnet can be controlled on a dual authorisation basis (one user submits a transaction/request; another is required to authorise it). However, the application provides the flexibility for the customer to define whether they require dual authorisation). In normal operating circumstances we would, however, strongly recommend that the dual control option is selected.

Activity log tools (audit trail)

Key administrative and transactional events are logged by Hang Seng HSBCnet and available for viewing online via the activity query log tools. An audit trail is provided allowing for retrospective internal control and financial auditing of System's activity.

Session time-outs

Hang Seng HSBCnet enforces idle (inactivity) session timeouts. If a session remains inactive for a set period of time, the session will be terminated and the user will be required to log back into the application. Moreover, the pages the user has viewed during the session expire to prevent it from being stored in the browser, where they could be accessed later by another user.

Do's and Don'ts

You are responsible for your own systems, connectivity and for the instruction send to the Bank. You must implement the following to protect yourself, including:

Security credentials

Users must keep their security credentials (password, memorable answer, security answers, physical Security Device/Soft Token PIN or any other security credential required to access Hang Seng HSBCnet as applicable) secure and secret at all times and ensure no unauthorized use is made or attempted to be made of these credentials. In particular:

- Never write, record or reveal these credentials to anyone else;
- Promptly destroy any advice of credentials from the Bank or other parties;
- Do not use security credentials that may be easy to guess or deduce (e.g. personal details, simple number combinations);
- Never record passwords, memorable answers, security answers or PINs on any software which can retain it automatically (for example, any computer screen prompts or 'save password' features or the like on a user's Internet browser);
- Ensure users are not overlooked by anyone or monitored by closed circuit TV while logging on to Hang Seng HSBCnet;
- It is highly advisable to have dedicated terminals for users that are only used for accessing Hang Seng HSBCnet in order to reduce the likelihood of malicious code being loaded onto a device. This device should not be used for general web browsing, e-mailing, or social networking;
  Never disclose any security credentials to any of your staff or internally within your organization. You should be cautious of any correspondence or communication purporting to originate from the Bank or from any third party requesting the disclosure of any passwords, security credentials of users, or any account details. You must report any suspicious activity, any possible concern or suspicious correspondence or communication to the Bank as soon as it occurs;
- Ensure that, if you have any suspicious that any credentials may have been in full or part compromised in any way, you immediately take appropriate action to protect your user(s)' profile by either changing them, or by suspending the user while appropriate action is taken. You should also review recent activity on your bank account(s) and user profile(s) as soon as you suspect any credentials may have been compromised to identify any unauthorised actions and you must inform the Bank immediately of any discrepancies; and
- It is your responsibility to regularly review your bank account(s) and user(s)' profile activity to ensure that there are no irregularities and in the event that it does discover any irregularities, you must notify the Bank immediately.

System compatibility

You must ensure that you have compatible hardware and software in order to access the relevant Hang Seng HSBCnet. Minimum technical requirements are detailed in the Hang Seng HSBCnet customer guides.

You agree that you operate information technology and system controls in line with relevant laws and regulations, for example, Sarbanes–Oxley, as applicable.

Security standards

You must review your internal security measures on a regular basis to ensure protection remains up to date and in line with regulatory and industry best practice guidance. In particular, this includes but is not limited to the following:

- Encryption technology you use in relation to the relevant Hang Seng HSBCnet must be compliant with the local law where Hang Seng HSBCnet is being accessed;
- You shall use and maintain spam filters, desktop firewalls, and real-time anti-virus software. These tools should be updated and used to scan your computers at intervals commensurate to the receipt of updates;
- You shall install security updates and application patches to operating systems and all applications as they become available; and
- Not using public Internet access points (e.g. Internet cafes, public Wi-Fi hotspots) to access Hang Seng HSBCnet or your accounts or personal information. If these access points must be used, then a VPN (Virtual Private Network) must be employed

Hang Seng HSBCnet access

To prevent unauthorized access to Hang Seng HSBCnet and/or to minimize your exposure to any potential security threats, you must ensure that:

a) Users log off the Hang Seng HSBCnet after use and do not allow access to these terminals whilst logged on to Hang Seng HSBCnet;
b) Users log off Hang Seng HSBCnet correctly, following the specified logout process (within Hang Seng HSBCnet users should select the 'Logout' button at the top right corner of the screen) instead of just closing the browser window; and
c) You must never provide any information over the phone when the caller's identity has not been confirmed. It is your responsibility to collect the details and verify the caller's identity through an independent means either by contacting the Bank via published lines or through a known contact. You will never be requested by the Bank to provide any password information

You must notify the Bank immediately of any unauthorized or suspected access or use to Hang Seng HSBCnet (including credentials) or any unauthorized, unknown or suspected transaction, communication or instruction.
You must notify the Bank immediately if:

- your browser access to Hang Seng HSBCnet appears unusual and/or unresponsive;
- you notice changes in the way things appear;
- you receive a message that the system is unavailable after security credentials have been provided;
- you receive an unexpected request for a security credential or event e-signature in the middle of an online session;
- you receive unusual pop-up messages; or
- you find new or unexpected toolbars and/or icons

If you detect suspicious activity you must immediately cease all online activity with Hang Seng HSBCnet and remove any computer systems that may be compromised from the network.

When performing electronic signing of events with the signing capable security device, users must validate the accuracy of the data they are being asked to sign (i.e. that the beneficiary account numbers they are asked to sign through Hang Seng HSBCnet are consistent with the data on their internal payment system or documentation). You must immediately notify the Bank if the information presented online deviates from their actual event details.

You must immediately remove access rights of your users and notify the Bank immediately of any actual or suspected impropriety on the part of any user in connection with the use of Hang Seng HSBCnet and/or any of the Products or tools that can be accessed by you, or where a user is no longer authorised to use Hang Seng HSBCnet (due to leaving employment of otherwise).
You must comply with all reasonable requests from the Bank, the police or other regulatory authorities in identifying actual or potential breaches of security. You must perform daily reconciliation of payment instructions executed via Hang Seng HSBCnet.

User suspension

Hang Seng HSBCnet permits System Administrators to suspend other users. This feature should be used in situations where a user is required to be temporarily disabled from using Hang Seng HSBCnet, e.g. during a holiday absence. It is not intended for use in a situation where material security concerns exist about a user's behavior. In such a case, the System Administrators should immediately delete the user from Hang Seng HSBCnet and revoke the user's physical Security Device (if held) / Soft Token .

If suspension is the only option available (for instance, because the user needs to be disabled urgently and no other System Administrator is available to approve the deletion), it should be undertaken in conjunction with other protective measures, such as the retrieval of the user's physical Security Device (if held). If in doubt, please call the Bank for assistance. Users need to be in 'Active' or 'Approved' status before they can be suspended. Once a user has been suspended, it is important that no further maintenance is undertaken on that user's profile or access rights prior to their eventual reactivation or deletion.

Hang Seng HSBCnet Mobile

In addition to your obligation to comply with the general E-Channels Security Measures, you must ensure you also comply with the additional security requirements** relating to Hang Seng HSBCnet Mobile app on your mobile device, including the following:

- Do not store your Hang Seng HSBCnet log on or profile details on your mobile device.
- When connecting to a wireless network using your mobile device, use only trusted networks or service providers and enable additional security protection, such as Wi-Fi Protected Access (WPA), if possible.
- When travelling, use a trusted computer or mobile device whenever possible. Ensure your device has the latest manufacturer software updates and avoid using a 'jailbroken' or 'rooted' device with any unauthorised modifications when using the Hang Seng HSBCnet Mobile app.
- Do not share your mobile device with others. Enable automatic passcode/PIN lock features to prevent other people from using it if stolen.
- Use a strong PIN that a hacker can't easily guess or deduce and change it regularly. You can update your HSBCnet security PIN in the Hang Seng HSBCnet Mobile app settings at any time.
- Do not leave your mobile device unattended after logging on to the Hang Seng HSBCnet Mobile app. When you're finished using Hang Seng HSBCnet, make sure to log off of Hang Seng HSBCnet and close the app.
- Do not install applications on your mobile device from unknown sources.

** For full details of your security obligations in using Hang Seng HSBCnet Mobile app, please refer to the **E-Channels Security Measures** document.