Getting started

Access Control Procedures

HSBCnet
www.hsbcnet.com

HSBC

Access Control Procedures

This section (the ACP) sets out the Access Control Procedures referred to in HSBC*net* Customer Agreement.

The main aim of this section is to set out the security duties of Customers ('you') and your nominated Users. The ACP also aims to (1) outline the processes and procedures with which Users must comply when accessing the System and the Services and (2) outline the different authorisations that the Users may be allocated, and the restriction that may be placed on their use of the System and the Services.

This version of the procedures (version 3) has been updated to cover the additional security features that have been introduced to support transactional services on HSBC*net*.

This section is not intended to provide a comprehensive guide to the System and the Services and further information can be found in the customer guides. In the event of any inconsistency between the ACP and the customer guides, the terms of the ACP shall prevail, to the extent of the inconsistency.

All capitalised terms used in this ACP shall have the meanings set out in the HSBC*net* Customer Agreement. Additionally, please note that clause 6.1 of the HSBC*net* Customer Agreement requires customers to comply with this ACP.

Access Control Procedures

1. The System

HSBC*net* is the Bank's internet portal through which you access your selected Services. To access HSBC*net*, you will require browser software and an internet connection – either through a dial-up connection or through your local area network (LAN).

2. The Services

HSBC*net* provides a variety of Services that are accessible using a number of different authentication methods. Generally speaking, these are either password based or involve the use of a physical security token issued to you by the Bank (often referred to as two-factor authentication).

The Bank may vary the nature of these authentication methods and enhance security for any or all of these services from time to time. In addition, all authentication methods may not be available to all Users.

Aunthentication levels of HSBC*net*'s primary Services

SERVICE	IDENTIFIER
Access to account information	Password and Memorable Answer or One-Time-Password Generating Security Device (at logon)
Download reports from system	
Payment of Transaction Preparation	
Payment of Transaction Approval	Password and Memorable Answer and PIN protected Smart card or One-Time-Password Generating Security Device (at logon and service launch)
Set up additional Use profiles	
Upload files to system	

Access Control Procedures

3. Users

Users

Users are all representatives authorised by you to use the System. Users are set up by your nominated System Administrators. Beyond the initial System Administrators who are set up by the Bank, all subsequent Users are set up and controlled by System Administrators directly.

System Administrators

System Administrators are responsible for the setup, authorisation and administration of Users (including other System Administrators). System Administrators set up Users (including other System Administrators) to use the System. They define which Services the Users have access to and, where permitted on the System, set levels of entitlements within the context of each Service. For instance, a System Administrator would be able to entitle a User to the cross-border Account Reporting Service and then define within that Service what accounts the User could actually view. System Administrators administer the use of the System by all Users. They are responsible for ensuring that User profiles are suspended when Users are on leave, for instance, and that they are deleted when appropriate. System Administrators are authorised to reset a User's passwords and maintain their profiles when required. Additional information on how System Administrators set up and entitle Users to Services can be found in the customer guides to HSBC*net*.

Access Control Procedures

User identification

You are responsible for verifying the identity of your Users, particularly those that are entitled to make transactions on your behalf. System Administrators will normally need to be formally identified and have their addresses verified by the Bank for money laundering compliance purposes. Your local Bank contact will advise which documents are required to be presented or whether any exemptions are available for certain types of companies.

4. Registration to System

Registration for HSBC*net* is straightforward and consists of the following simple steps:

Completion of Customer Agreement

This is the standard HSBC*net* Customer Agreement that needs to be signed in accordance with company authorisation. It captures the following information:

- Company details
- Accounts to be reported through HSBC*net*
- Initial System Administrator details

If you wish for one of your subsidiaries to report accounts to you through HSBC*net*, you will also need to ensure that it completes and signs the Customer Associate section of the Customer Agreement which authorises your subsidiary's group office or other bank to report accounts through HSBC*net*.

Access Control Procedures

Initial System Administrator registration

You will be requested to provide the Bank with the names of, and information regarding, up to four Initial System Administrators. The Bank will set up these Initial System Administrators for you. After this, you will be responsible for all aspects of the setup of additional System Administrators and users.

Additional User registration

While the Initial System Administrators are set up by the Bank, additional Users (including additional System Administrators) are set up by System Administrators. The registration process for additional Users is similar to the online System Administrator registration process described above with Users completing an online form, which is subsequently approved by their System Administrator. Please note that additional System Administrators' identities will need to be verified by the Bank as described in the above section entitled 'User Identification'.

When processing a new registration request, System Administrators are advised, in all cases, to cross-check the legitimacy of its source using a channel other than the internet. By their very nature, new registration requests are not submitted over a secure channel.

Access Control Procedures

5. Identifiers

This section describes the various Identifiers used to access HSBC*net* services. Please note that some or all of these methods may be used to authenticate your users when accessing HSBC*net* services and their use may be varied over time at the Bank's discretion if it is necessary to enhance security. In addition, not all authentication methods will necessarily be available to you and where there is a possible choice of authentication method, the Bank reserves the right to determine the security methodology that it believes suitable for your business.

Password

The password is an eight-character-minimum alphanumeric string chosen by the User at registration.

Memorable answer

On registration for HSBC*net*, Users will be prompted to select a memorable question and answer. The memorable answer may be requested at logon, as an additional security measure.

PIN-protected smart card

This is a smart card that contains a pre-loaded digital certificate. To access certain tools as specified in Section 2, Users must insert the smart card into the provided smart card reader and enter their PIN.

PIN-protected Security Device

This is a PIN-protected device that generates unique one-off dynamic passcodes for accessing HSBC*net*. These passcodes can be used only once, expire after a short period of time, and are unique to each device and therefore to each individual account at any particular point in time.

The Security Device is used both to access the site at logon and to re-authenticate identity when accessing certain tools as noted above in Section 2.

The smart card and Security Device are both examples of what is commonly known as two-factor authentication, a form of identification that requires a User not only to know something, the device PIN, but also to physically possess the device itself.

6. Security dos and don’ts

You are responsible for your own systems and for your communications with the Bank and must implement the following to protect yourself, including:

Access Control Procedures

Security credentials

Users must keep their security credentials (password, memorable answer, security answers, smart card PIN, Security Device PIN or any other security credential required to access HSBC*net*) secure and secret at all times and ensure no unauthorised use is made or attempted to be made of these credentials. In particular:

- Never write or otherwise record these credentials or reveal them 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 (eg personal details, simple number combinations)
- Never record passwords, memorable answers, security answers or PINs using any software which can retain it automatically (for example any computer screen prompts or 'save password' feature or the like on an internet browser)
- Ensure that Users are not overlooked by anyone or monitored by closed circuit TV while logging on to the System
- Change PINs as soon as they are received, and both passwords and PINs on a regular basis going forward. Don't alternate between passwords
- Never disclose your security credentials to Bank staff. You should be cautious of any correspondence or communication requesting the disclosure of your passwords or any account details; report to the Bank should you be suspicious of any such correspondence or communication
- If you suspect that your credentials may have been in full or part compromised in any way, ensure that you immediately take appropriate action to protect your account by either changing your details or requesting the account be suspended while action is taken to secure the account. You should also review recent activity on your account to identify unauthorised actions

Access Control Procedures

Physical security tokens; smart cards and Security Devices

- Physical security tokens (and where necessary, PINs) are distributed to you using a variety of forms of delivery. You must inform the Bank promptly if, within a reasonable period of time (normally seven days) of dispatch, you have not received the packages sent
- Where packages containing security materials cannot be delivered directly to the appropriate individuals in your company, (for example where your mail room takes delivery), you are responsible for ensuring that the third party passes the appropriate package directly to the individual
- When using a physical security token to access HSBC*net* services once the User has been authenticated using the device, a secure session is opened that remains open until the User logs off. It is, therefore, vital that you log off from HSBC*net* when leaving your terminal unattended even if the service that was accessed using the physical Security Device is itself closed
- You should never leave physical security tokens unguarded or where they could be misappropriated regardless of the fact that they are PIN-protected. This includes ensuring that devices are stored in a secure place when not in use
- You should never give or lend your physical Security Device to another person
- You must immediately advise the Bank of any loss of a security token, or act in line with the operating procedures established for the management of any physical security tokens

Access Control Procedures

- Physical security tokens must be stored under safe conditions to ensure they remain in an operational condition. Avoid:
  - Extreme temperatures
  - Incorrect voltages
  - High humidity
  - Corrosive or chemical substances
  - Direct sunlight
  - Water, detergent, bleach, alcohol
- You should always follow the usage and security guidance published on the site or in customer guides provided by the Bank

Please note that the Bank reserves the right, if it believes any physical security token is being misused, to demand its return.

Access Control Procedures

Digital certificate management

Digital certificates stored on the smart card device must not be sent to any other party or used for any other purpose than to access HSBC*net*.

System compatibility

You must ensure that you have compatible hardware and software in order to access the System. Minimum technical requirements are detailed in the customer guides to HSBC*net*.

Security standards

You must review your internal security procedures as necessary to ensure protection remains up to date. In particular, you must ensure that:

- The encryption technology used or required to be used by the Bank in relation to the System is compliant with the local law where the System is being accessed
- You establish and maintain system security standards for the components used to access HSBC*net*, in line with recognised industry standards and vendor instructions and adopt all relevant patches, updates and all other measures relating to operation or security issued or recommended by the Bank or suppliers of hardware and software components. This includes the implementation and appropriate maintenance of up-to-date firewall and virus protection, denial of service prevention measures and other security measures such as the use of intrusion detection software commensurate with the size and complexity of your information technology operations
- The Bank will presume that you operate information technology and system controls in line with relevant regulatory standards, for example Sarbanes Oxley, as applicable

Access Control Procedures

System access

To prevent unauthorised access to the system, you must ensure that:

- Users log off from the System after use and do not leave access terminals while logged on
- Users log off from the System properly using the Logout button at the top-right corner of the screen instead of closing the browser window
- You notify the Bank immediately of any unauthorised or suspected access or use of the System (including Identifiers) or any unauthorised, unknown or suspected transaction or instruction
- You remove access rights and notify the Bank immediately of any actual or suspected impropriety on the part of any User in connection with the Services or where a User is no longer authorised to use the System due to leaving employment or otherwise
- You comply with all reasonable requests for assistance from the Bank, the police or other regulatory authorities in identifying actual or potential breaches of security

File Upload

In order to deliver the file containing Customer Instructions to the Bank, you must complete the information required in the File Upload tool covering the file type, format, authorisation level required and country (where appropriate) before selecting the file from the specified location. Once you have selected Go and the Bank has received the file, the Bank will issue a simple on-screen acknowledgement confirming that the file has been received. The Bank will then perform some initial validation before issuing a file acknowledgement report, which should be accessed through the Report and File Download function.

Access Control Procedures

You are responsible for advising the Bank of the receipt of a file acknowledgement report for which no file was sent, any inaccuracy in the file acknowledgement report, or failure to receive a file acknowledgement report within a reasonable period of time. The HSBC*net* file upload tool will take the file of Customer Instructions from the specified location at your site and send it to the Bank. It is therefore important that measures are taken to minimise the chance that the file is tampered with.

These include:

- The file should be kept in a secure location with minimal access to it permitted
- It should only be possible to create the file by an authorised process and read by the HSBC*net* System
- All access to the file is logged in a secure manner to enable investigations to be carried out should these be necessary

In all situations but particularly where pre-authorised files of Customer Instructions are sent to the Bank, it is extremely important that the above measures are adopted. Nothing in this ACP prejudices the terms of Clause 3 of the HSBC*net* Customer Agreement and, in particular, your obligation to ensure that Customer Instructions are correctly transmitted to the Bank.

Access Control Procedures

7. Troubleshooting

Availability of Services

The Services will normally be available at all times, but we may suspend all or part of the System or Services at any time at our discretion.

Please note that a transaction being carried out is not always simultaneous with a Customer Instruction being given. Some matters may take time to process and certain Customer Instructions may only be processed during normal banking hours even though the Services may be available outside such hours.

Technical support

Technical support in relation to the System or the Services is available to all Users from the Bank as follows:

- Online helptext

  Helptext is available on the System that can assist Users to identify and resolve common technical issues.

- System Administrator support

  Most problems Users may experience with HSBC*net* can be resolved by their System Administrators. System Administrators have the ability to perform various tasks including amending User's entitlements and resetting their passwords.

Access Control Procedures

Technical support cont'd…

- Helpdesk support

  Where issues cannot be resolved by System Administrators, telephone support is also available during normal banking hours. At the discretion of the Bank, staff Users may be required to verify their identity.

- Banking support

  In the event that the Customer is unable to use the System, they should contact their helpdesk in order to make contingency arrangements. The Bank may in its discretion require the User to verify their identity.

- User suspension

  The System permits System Administrators to suspend other Users. This feature is intended for use in situations where a User is required to be temporarily disabled from using the System, for example during a holiday absence. It is not intended for use in a situation where material security concerns exist about a User's behaviour. In such a case, the System Administrator should immediately delete the User from the System and revoke the User's smart card (if held). 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 smart card. 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/deletion.