GENERAL TERMS AND CONDITIONS, ACCESS CONTROL PROCEDURES OF HSBC*net* ONLINE BANKING SERVICE

Information booklet for Legal Entities

Publication date: March 2023.
Terms stipulated in the booklet may be changed.
For up-to-date and detailed information
please refer to www.business.hsbc.am
or call us at +374 60 655 200.
HSBC Bank Armenia is regulated
by the Central Bank of Armenia.

HSBC

Contents

E-Channels Terms and Conditions (E-Terms) General E-Terms

1. Introduction

1.1 The E-Channels shall be governed by these terms and conditions and the terms and conditions which apply to the Services (the "Service Terms") and which shall replace all previous agreements between the Parties relating to the E-Channels. In the event of any conflict between any applicable terms, the following order of priority shall apply:

(a) the applicable Country Conditions;

(b) any Supplementary E-Terms;

(c) the General E-Terms; and

(d) any Service Terms.

1.2 The E-Terms may be entered into by the execution of any number of copies of the relevant Application Form, all of which taken together shall form one document.

1.3 References to the singular include the plural and vice versa. Clause headings are included for convenience only and do not affect interpretation.

2. Definitions

- **Account Holder** means the party agreeing to have their accounts and/or Services included on the Profile Owner's E-Channels.
- **Application Form** means any form in which the Profile Owner agrees to the provision of an E-Channels by the Profile Bank.
- **Authorised Person** means a person that the Profile Owner has authorised (either alone or in combination with others) to give Instructions and/or otherwise perform acts on the Profile Owner's behalf.
- **Country Conditions** means, for each relevant jurisdiction, the specific terms which supplement and/or amend any E-Terms.

- **E-Channels** means the Group's electronic banking systems.
- **E-Terms** means the General E-Terms, any applicable Supplementary E-Terms and any applicable Country Conditions.
- **General E-Terms** means these terms and conditions.
- **Group** means HSBC Holdings plc, its subsidiaries, related bodies corporate, associated entities and undertakings and any of their branches.
- **Infrastructure Provider** means any third party providing shared market infrastructure necessary for a Party to perform its obligations under the E-Terms including any communications, clearing, settlement or payment system, or intermediary or correspondent bank.
- **Instruction** means any communication which is received by the Profile Bank via an E-Channels which has or appears to have been provided by an Authorised Person.
- **Loss** means any loss, damages, liability, costs, claims, demands and expenses of any kind whether or not foreseeable.
- **Party** means the Profile Owner or the Profile Bank.
- **Profile Bank** means the member of the Group that provides the Profile Owner with an E-Channels.
- **Profile Owner** means the party provided with access to the E-Channels by the Profile Bank.
- **Security Measures** means the measures required to ensure the security of an E-Channels as may be provided to the Profile Owner by the Profile Bank from time to time.
- **Services** means any banking or related service provided and accessed via an E-Channels.
- **Supplementary E-Terms** means any terms and conditions which relate to a particular E-Channels service and incorporates these terms and conditions.

3. Instructions

3.1 The Profile Owner agrees to provide Instructions in the form which the Profile Bank has advised it to use from time to time, and the Profile Bank shall not be obliged to act on an Instruction provided in any other form.

3.2 Provided it followed its Security Measures, the Profile Bank is entitled to rely on any Instruction and the Profile Bank may treat all Instructions received as authorised and valid. The Profile Owner is responsible for setting up its profile

on E-Channels to be in accordance with its own mandates and internal controls. Neither the Profile Bank nor any other member of the Group is under any obligation to review whether an Instruction conflicts with any other instruction or mandate of the Profile Owner or Account Holder. The Profile Bank may decline or delay to act on an Instruction where it doubts its legality, origination or authorisation.

3.3 The Parties agree to comply with the Security Measures. The Profile Owner shall establish, maintain and review its own appropriate internal security measures for its use of and access to the E-Channels, including the installation and ongoing update of anti-virus software. The Profile Owner is responsible for ensuring the appropriate application of the Security Measures when submitting Instructions.

3.4 The Profile Owner shall promptly acquire, maintain, update and install (where relevant) any equipment, software, telecommunications facilities, networks, connections, patches, releases and/or updates which the Profile Bank requires it to obtain and use, or that the Profile Bank provides to the Profile Owner in connection with its access to the E-Channels. The Profile Owner is responsible for obtaining and maintaining the computer software and equipment necessary to access and use the E-Channels.

3.5 The Profile Owner shall not alter, reverse engineer, copy (other than to the extent necessary for the permitted use), publish or impart to any third party any products or services provided by the Profile Bank, including the E-Channels or any software or materials provided as part of its products or services.

4. Warranties, Representations and Undertakings

4.1 The Profile Owner undertakes to:

(a) provide to the Profile Bank all documents and other information reasonably requested by it from time to time in relation to the E-Channels; and

(b) notify the Profile Bank as soon as possible if it becomes aware of any theft, fraud, illegal activity, loss, damage or other misuse in relation to the E-Channels.

4.2 If the Profile Owner uses or accesses an E-Channels in relation to an account of a third party, it represents and warrants that it has appropriate authorisation from that third party to do so.

4.3 Neither the Profile Bank nor any other member of the Group shall be liable for any Loss suffered as a result of the acts or omissions of an Infrastructure Provider, but will cooperate with the Profile Owner in the recovery of any such Loss.

4.4 The Profile Bank may suspend the E-Channels for maintenance or for any other reason where it reasonably considers it necessary to do so. The Profile Bank will provide the Profile Owner with reasonable prior notice of the suspension where it is practical to do so.

5. Fees and charges

The Profile Owner shall pay to the Profile Bank such fees, costs, charges, interest and expenses in connection with the E-Channels as stipulated by or agreed with the Profile Bank in accordance with the terms and conditions applicable to the Services.

6. Amendments

The Profile Bank may make amendments to the E-Terms which will become effective on the expiry of 45 days' notice to the Profile Owner. Any such notice may be given to the Profile Owner in writing or by publishing such amendments on www.hsbcnet.com. However, the Profile Bank may, in exceptional circumstances, make amendments to the E-Terms at any time in order to comply with any law or regulation, which will become effective immediately on notice to the Profile Owner.

7. Termination

7.1 Either Party can terminate any or all E-Terms and/or E-Channels by giving 30 days prior written notice to the other. Any liabilities owing to the Profile Bank thereunder will become immediately due and payable on termination of the E-Terms.

7.2 Subject to any applicable legal or regulatory restriction, either Party can terminate any or all E-Terms and/or E-Channels immediately if:

(a) the other Party commits a material breach of the E-Terms which is incapable of remedy or not remedied within a reasonable time period;

(b) the other Party becomes insolvent; or

(c) it is or may become unlawful for that Party to perform its obligations under any of the E-Terms.

7.3 Clauses 7.3 and 3.5 shall survive termination of the E-Terms.

7.4 In the event that any Services are terminated, the Service Terms shall survive the termination of such Services to the extent necessary to give effect to the E-Terms.

Security Measures

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

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 HSBC*net* E-Channels may be subject to automatic suspension when they have not logged into HSBC*net* within a 6 month period. If a HSBC*net* profile is not accessed by any Users within an 18 month period, the HSBC*net* profile may also be suspended.

4. If biometric authentication methods (for example, fingerprint scan or facial recognition) are used to access an E-Channels 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-Channels with any third party other than to 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-Channels 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 authorised.

7. The Profile Owner shall ensure that its users provide correct, full and unabbreviated details whenever they are required by the HSBC Group. 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-Channels and seeking to change an address or 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-Channels is accessed by a User via a mobile device, the Profile Owner shall require that the User:

(d) does not leave the mobile device unattended after logging on to any E-Channels;

(e) clicks the 'Logout' button when the User is finished accessing any E-Channels;

(f) enables the mobile device's automatic pass code lock feature;

(g) does not share mobile devices being used to access E-Channels with others;

(h) is the only person registered for biometrics (for example, face, fingerprint, voice, retina) etc.) on the device;

(i) takes steps to de-register devices that should no longer be used as an authentication method as envisaged in clause 15; and

(j) does not access the E-Channels 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-Channels is suspended for any reason, any subsequent reactivation of that E-Channels 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-Channels 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-Channels 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).

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.

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.

Aunthenticationlevels 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	

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*.

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 subsidiar's group office or other bank to report accounts through HSBC*net*.

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.

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:

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

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
- 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.

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

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.

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.

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.

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.

Notes:

- Description, advantages and tariff of charges of “HSBC*net* Online Banking service” are presented in the respective brochure and in our website at business.hsbc.am.
- General terms and conditions applicable to Products and Services for Legal Entities are presented in our website at business.hsbc.am and in “General Terms and Conditions for the Operation of Customer Bank Accounts, Bank Deposits, Electronic Banking and Other Banking Services for Legal Entities” information bulletin.

NOTE: In case of discrepancies between Armenian and English versions of the brochure, the Armenian version shall prevail.

Issued by "HSBC Bank Armenia" CJSC
"HSBC Bank Armenia" CJSC is a member of HSBC Group, one of the largest banking and financial services organizations in the world.
HSBC Group international network covers 63 countries and territories.

www.business.hsbc.am
+374 60 655 200

Legal sign off
66 Teryan Street, Yerevan 0009, Republic of Armenia
Registration number 67