

# Security Measures

This document (the **Security Measures**) sets out mandatory security requirements (as amended from time to time) relating to any E-Channel Profile.

For the avoidance of doubt, the Security Measures will apply in relation to each E-Channel Profile that the Profile Bank provides to the Profile Owner from time to time.

## Profile Bank Security Measures

The following paragraphs set out the security measures which the Profile Bank will use.

### General

- 1 The Profile Bank may use measures intended to prevent access by unauthorised external parties to the E-Channel infrastructure.
- 2 The Profile Bank can remove or disable any Accessed Service or authentication method at any time without notice if it has any security concerns.
- 3 If the E-Channel Profile has not been accessed by any Users within an 18-month period, the Profile Bank can suspend that E-Channel Profile.
- 4 The Profile Bank may terminate any User's session in the E-Channel Profile for security reasons.

### HSBCnet

- 5 The Profile Bank can suspend any HSBCnet User who has not logged into HSBCnet in a 6-month period.

## Profile Owner Security Measures

The following paragraphs set out the security measures with which the Profile Owner will comply for the E-Channel Profile to which it has access.

### General

- 6 The Profile Owner will, and will ensure that any Third Party will, promptly acquire, maintain, update and install (as relevant) any equipment, software, telecommunications facilities, networks, connections, patches, releases and / or updates which the Profile Bank or relevant provider requires.
- 7 The Profile Owner will, and will ensure that any Third Party will, regularly review its internal security measures and controls to ensure that they are up-to-date, effective, and aligned with regulatory and industry best practice guidance. The internal security measures and controls should include (without limitation) malware protection, network restrictions, hardware and software patching or evergreening, physical and remote access restrictions, computer device settings, monitoring of improper usage, and guidance on acceptable web browsers and email usage, including on how to avoid getting infected by malware.
- 8 The Profile Owner will not, and will ensure that no User or Third Party (as relevant) will, circumvent or attempt to circumvent the Security Measures or any of the Profile Bank's operating systems used in connection with the E-Channel.
- 9 The Profile Owner must promptly notify the Profile Bank if it has any concerns with any activity on the E-Channel Profile.
- 10 The Profile Owner will notify the Profile Bank as soon as possible if it becomes aware of any actual or attempted unauthorised access to or use of the E-Channel Profile or any actual or suspected cyber-incident in relation to the E-Channel Profile.

## Users and Third Parties

- 11 The Profile Owner will, and will ensure that Users and any Third Parties will, only access the E-Channel Profile using the authentication methods prescribed by the Profile Bank.
- 12 The Profile Owner will ensure that Users and any Third Parties do not share any security credentials or access to the E-Channel Profile (as applicable) with any party except as permitted with a Third Party Provider. Except where security credentials are shared with a Third Party Provider, the Profile Owner will ensure that all Users and any Third Parties keep security credentials (including passwords, PINs, encryption keys and security certificates) secret at all times.
- 13 The Profile Owner will review activity and User permissions in relation to the E-Channel Profile on a regular basis, unless it knows or suspects that any User's security credentials have, or an Authentication Device has, been lost, stolen or compromised, in which case it will:
  - (a) carry out an immediate review;
  - (b) promptly notify the Profile Bank; and
  - (c) ensure that (as relevant) the Authentication Device is immediately deactivated, the security credentials are changed and / or the User is suspended.
- 14 The Profile Owner will have commercially reasonable processes in place to prevent Users and any Third Parties being socially engineered or acting on fraudulent communications. These processes should direct Users and any Third Parties, where communications are received seemingly from known senders (including senior management, suppliers and vendors), to ensure that the authenticity of those communications is independently verified using contact details obtained from an independent source (e.g. public website), before continuing with the action.

## Security credentials and authentication

- 15 The Profile Owner will require any User accessing the E-Channel Profile to:
  - (a) take appropriate steps to prevent unauthorised access to any Authentication Device, or to the E-Channel Profile and any device used to access it; and
  - (b) only access the E-Channel Profile using secure devices.
- 16 The Profile Owner will ensure that Users do not share Authentication Devices.

## HSBCnet

### HSBCnet Users

- 17 The Profile Owner will promptly:
  - (a) remove an HSBCnet User from the HSBCnet Profile if they leave the Profile Owner's organisation or should no longer have access for any reason; and
  - (b) suspend an HSBCnet User's access to the HSBCnet Profile if they will not be, or have not been, active on the HSBCnet Profile for a prolonged period of time or if there is any concern about the conduct of that HSBCnet User.

- 18 The Profile Owner will ensure that HSBCnet Users:
- provide and maintain correct, up-to-date, full and unabbreviated details whenever they are required by the Group; and
  - do not register for access to HSBCnet using a shared email address, mobile phone number or under multiple usernames.

## HSBCnet security credentials and authentication

- 19 The Profile Owner will promptly return any security devices supplied by a Group member on request, with a view to aiding any investigations by the Profile Bank into those security devices.

## Reactivation

- 20 When reactivating a suspended HSBCnet Profile, the Profile Bank will use reasonable efforts to reinstate original permissions, limits, HSBCnet Users, accounts and services, unless an exception applies. The Profile Bank may also add additional services, products or permissions to the HSBCnet Profile during the suspension period.

## Definitions

- **Accessed Services** means any account, product and / or service (including without limitation a product or service related to an account) that is accessed or used through the E-Channel Profile.
- **Authentication Device** means any device which can be used for authentication with respect to the E-Channel Profile, including (without limitation) any security device or mobile device registered to the User.
- **E-Channel** means the relevant digital banking system that the Group provides for access and use (e.g. HSBCnet), and any ancillary services and technical tools.
- **E-Channel Profile** means the E-Channel to the extent that it is configured for and provided to the Profile Owner.
- **Group** means HSBC Holdings plc, its subsidiaries, related bodies corporate, associated entities and undertakings and any of their branches from time to time.
- **HSBCnet** means the E-Channel that is the Group's internet banking platform accessed via the portal at [www.hsbcnet.com](http://www.hsbcnet.com) or any other access point or means including the HSBCnet mobile banking app.
- **HSBCnet Profile** is an E-Channel Profile and means HSBCnet to the extent that it is configured for and provided to the Profile Owner.
- **HSBCnet User** means any User who the Profile Owner permits to access or use the HSBCnet Profile.
- **Law** means any applicable local or foreign statute, law, regulation, ordinance, rule, judgment, decree, voluntary code, directive, sanctions regime, court order, agreement between any Group member and an authority, or agreement or treaty between authorities and applicable to the Profile Bank or a Group member.
- **Profile Bank** means the Group member that provides the E-Channel Profile to the Profile Owner.
- **Profile Owner** means any customer that has signed an agreement with the Profile Bank for the access and use of one or more E-Channel Profiles.
- **Third Party** means any party other than a User or a Third Party Provider who acts for the Profile Owner with respect to the E-Channel Profile and / or Accessed Services.
- **Third Party Provider** means a party permitted to provide account information or payment initiation services in accordance with relevant Law or contractual obligations applicable to accounts linked to the E-Channel Profile.
- **User** means any person who the Profile Owner permits to access or use the E-Channel Profile on its behalf and on whose authority and / or identity the Profile Bank can rely in accordance with its agreement with the Profile Owner for the E-Channel Profile.