E-Channels Security Measures

English | En français (European) | En français (Canadian) | En español | 繁體中文 | 简体中文 | Bahasa Indonesia | العربية

January 2019

PUBLIC

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

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 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.

7 The Profile Owner shall ensure that individuals do not maintain more than one username or set of security credentials.

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 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).

Mesures de sécurité des Canaux électroniques

Ce document énonce les mesures de sécurité (susceptibles d'être révisées ou mises à jour ponctuellement par le Groupe HSBC) pour tout système bancaire électronique (« **Canal électronique** ») fourni par un membre du Groupe HSBC (« **Banque liée au profil** ») à son client (« **Propriétaire du profil** »).

Mesures de sécurité de la Banque liée au profil

1 La Banque liée au profil doit mettre en œuvre des mesures visant à interdire l'accès non autorisé des parties externes à l'environnement dans lequel son service Internet fonctionne.

2 La Banque liée au profil doit s'assurer que ses systèmes sont strictement contrôlés, notamment en élaborant des plans de continuité des activités.

3 Dans le cadre des mesures de sécurité de la Banque liée au profil, tout utilisateur autorisé par le Propriétaire du profil (« **Utilisateur** ») qui accède au canal électronique HSBCnet peut faire l'objet d'une suspension automatique s'il ne se connecte pas à HSBCnet pendant 6 mois. Si aucun Utilisateur n'accède à un profil HSBCnet, pendant 18 mois, le profil HSBCnet peut également être suspendu.

4 Si une méthode d'authentification biométrique (empreintes digitales, reconnaissance faciale, etc.) est utilisée pour accéder à un canal électronique à partir d'un périphérique mobile, la Banque liée au profil et l'entité HSBC associée qui fournit les applications à l'appareil mobile se réservent le droit de supprimer la fonction d'authentification biométrique à tout moment et, si nécessaire, sans préavis en cas de préoccupations relatives à la sécurité d'un appareil. Dans des circonstances normales, il sera toujours possible de s'authentifier par le biais du périphérique mobile à l'aide d'autres méthodes existantes.

Mesures de sécurité du Propriétaire du profil

1 Le Propriétaire du profil doit accéder aux canaux électroniques en utilisant uniquement les méthodes d'authentification prescrites par la Banque liée au profil.

2 Le Propriétaire du profil doit s'assurer que tous les Utilisateurs sécurisent leurs informations de sécurité (mot de passe, réponse mémorable, réponses de sécurité, code PIN du dispositif de sécurité, code PIN/mot de passe de l'appareil mobile ou tout autre identifiant requis pour accéder aux canaux électroniques, le cas échéant), les gardent secrètes à tout moment et ne facilitent pas l'utilisation non autorisée de ces informations de sécurité. En particulier, le Propriétaire du profil ne doit partager ni ses informations de sécurité, ni l'accès à un canal électronique avec un tiers.

3 Le Propriétaire du profil est responsable de la sélection rigoureuse de ses Utilisateurs, en gardant à l'esprit que ces Utilisateurs pourront accéder à un large éventail de capacités, notamment l'attribution d'autorisations à des comptes ou à des services et l'envoi d'instructions relatives à ces comptes ou services.

4 Le Propriétaire du profil doit signaler à la Banque liée au profil toute perte ou vol d'un dispositif de sécurité dans les plus brefs délais.

5 Le Propriétaire du profil doit :

(a) prendre immédiatement les mesures nécessaires pour protéger un profil d'Utilisateur s'il soupçonne que les informations d'authentification de cet Utilisateur ont été intégralement ou en partie compromises de quelque façon que ce soit ;

(b) passer en revue l'activité récente sur ses comptes et ses profils Utilisateur s'il soupçonne que des informations d'authentification ont été compromises et informer sans délai la Banque liée au profil de tout écart ; et

(c) passer régulièrement en revue l'activité de son compte et de ses profils Utilisateur et informer sans délai la Banque liée au profil s'il constate un écart ou une irrégularité.

6 Le Propriétaire du profil doit immédiatement supprimer de son profil de canal électronique tout Utilisateur quittant l'organisation du Propriétaire du profil. Le Propriétaire du profil doit immédiatement suspendre l'accès d'un Utilisateur aux canaux électroniques en cas de doute concernant sa conduite ou ses autorisations. Le Propriétaire du profil doit s'assurer que les informations et les dispositifs de sécurité sont utilisés uniquement par l'Utilisateur auxquels ils sont assignés.

7 Le Propriétaire du profil doit s'assurer qu'aucun individu ne possède plus d'un nom d'utilisateur ou plus d'un ensemble d'informations de sécurité.

8 Le Propriétaire du profil doit informer la Banque liée au profil, dans un délai de sept jours à compter de l'expédition d'un dispositif de sécurité par la Banque liée au profil, qu'il n'a pas reçu le colis envoyé, à condition d'avoir lui-même été informé de l'envoi.

9 Le Propriétaire du profil doit immédiatement renvoyer tout dispositif de sécurité demandé par la Banque liée au profil.

10 Le Propriétaire du profil doit adopter et réviser régulièrement ses mesures de sécurité interne pour s'assurer que la protection dont il bénéficie reste à jour et conforme aux orientations réglementaires et aux meilleures pratiques du secteur. Ces mesures doivent inclure, mais sans s'y limiter, une protection contre les programmes malveillants, des restrictions (réseau, accès physique, accès à distance), des paramètres de sécurité informatique, une surveillance des utilisations inappropriées et des conseils relatifs à la fois aux navigateurs Web acceptables et à l'utilisation de la messagerie électronique, en particulier pour apprendre à éviter les programmes malveillants.

11 Le Propriétaire du profil doit mettre en place des mesures pour empêcher les Utilisateurs d'être victimes d'ingénierie sociale ou de communications frauduleuses. Il s'agit par ces mesures d'empêcher les stratagèmes d'usurpation d'adresse électronique professionnelle, dans lesquels un fraudeur usurpe par e-mail l'identité d'une personne connue d'un Utilisateur autorisé à accéder à un canal électronique en lui demandant de modifier l'adresse ou le numéro de compte bancaire où les paiements doivent être envoyés. De telles mesures doivent notamment inclure, les communications reçues par les Utilisateurs provenant d'expéditeurs apparemment connus (y compris, mais sans s'y limiter, les cadres supérieurs et les fournisseurs), afin de vérifier l'authenticité de ces communications de façon indépendante (par un moyen autre que le courrier électronique).

12 Si un Utilisateur accède à un canal électronique par le biais d'un appareil mobile, le Propriétaire du profil peut exiger que l'Utilisateur :

(a) ne laisse pas l'appareil mobile sans surveillance lorsqu'il est connecté au canal électronique ;

(b) clique sur le bouton « Déconnexion » lorsqu'il a terminé d'accéder au canal électronique ;

(c) active la fonction de verrouillage automatique par mot de passe de l'appareil mobile ;

(d) ne partage jamais avec d'autres individus un appareil mobile utilisé pour accéder aux canaux électroniques ;

(e) soit la seule personne enregistrée pour l'authentification par biométrie (visage, empreintes digitales, voix, rétine, etc.) sur l'appareil ;

(f) annule l'enregistrement des appareils ne devant plus servir à l'authentification, comme stipulé à l'article 15 ; et

(g) cesse d'accéder aux canaux électroniques par le biais d'un appareil mobile débridé, routé ou autrement compromis.

13 Le Propriétaire du profil reconnaît et accepte que, dans l'éventualité d'une suspension d'un canal électronique pour quelque raison que ce soit, toute réactivation ultérieure de ce canal électronique rétablira automatiquement les autorisations, les limites, les accès Utilisateur et les accès comptes et services existant avant la suspension.

14 Le Propriétaire du profil doit garder à l'esprit qu'un Utilisateur accédant à un canal électronique par le biais d'un appareil mobile peut effectuer un grand nombre d'activités avec cet appareil. Ces activités incluent notamment l'utilisation de l'appareil mobile (à la place d'un dispositif de sécurité, par exemple) pour authentifier les activités menées sur une autre session de canal électronique ouverte sur un ordinateur de bureau.

15 Si un Utilisateur accède aux canaux électroniques en utilisant les méthodes d'authentification biométrique disponibles sur certains appareils mobiles (empreintes digitales, reconnaissance faciale, etc.), le Propriétaire du profil reconnaît que de telles méthodes d'authentification risquent d'être compromises ou de permettre un accès non autorisé (notamment à des membres de la famille, par exemple).

Mesures de sécurité pour les canaux électroniques

Le présent document établit les mesures de sécurité (qui peuvent être révisées ou mises à jour par le groupe HSBC à l'occasion) pour tous les systèmes bancaires électroniques (les «**canaux électroniques**») fournis par tout membre du groupe HSBC (la «**banque du profil**») à ses clients (le «**responsable du profil**»).

Mesures de sécurité de la banque du profil

1 La banque du profil doit utiliser des mesures pour refuser les accès non autorisés des parties externes à l'environnement où son service Internet est exploité.

2 La banque du profil doit s'assurer que ses systèmes sont strictement contrôlés, et avoir des plans de continuité des opérations.

3 Dans le cadre des mesures de sécurité de la banque du profil, l'accès des utilisateurs autorisés par le responsable du profil (les «**utilisateurs**») au canal électronique HSBC*net* peut être suspendu automatiquement lorsqu'ils ne se connectent pas au système HSBC*net* pendant six mois. Si aucun utilisateur n'a accédé à un profil HSBC*net* pendant 18 mois, le profil peut également être suspendu.

4 Si des méthodes d'authentification biométriques (par exemple, numérisation des empreintes digitales ou reconnaissance faciale) sont utilisées pour accéder à un canal électronique à partir d'un appareil mobile, la banque du profil et l'entité HSBC associée fournissant les applications à l'appareil mobile se réservent le droit de retirer la fonctionnalité d'authentification biométrique, au besoin et sans préavis, dans le cas où la sécurité de l'appareil risquerait d'être compromise. Dans les circonstances normales, il sera tout de même possible de procéder à une authentification en utilisant d'autres méthodes existantes.

Mesures de sécurité du responsable du profil

1 Le responsable du profil doit uniquement accéder aux canaux électroniques en utilisant les méthodes d'authentification prescrites par la banque du profil.

2 Le responsable du profil doit s'assurer que tous les utilisateurs conservent leurs identifiants de sécurité (mots de passe, réponses secrètes, réponses aux questions de sécurité, NIP de dispositif d'accès sécurisé, NIP et mot de passe d'appareil mobile et tout autre identifiant de sécurité requis pour accéder aux canaux électroniques, le cas échéant) en sécurité et secrets en tout temps, et n'en facilitent pas l'utilisation non autorisée. En particulier, le responsable du profil ne doit pas partager les identifiants de sécurité et les accès aux canaux électroniques avec une tierce partie.

3 Le responsable du profil est chargé de la sélection rigoureuse de ses utilisateurs, car ceux-ci ont accès à un grand nombre de fonctionnalités, y compris l'attribution de droits d'accès à des comptes ou à d'autres services et l'envoi de directives concernant ces comptes et ces services.

4 Le responsable du profil doit aviser la banque du profil rapidement en cas de perte ou de vol d'un dispositif d'accès sécurisé.

5 Le responsable du profil doit :

(a) prendre rapidement les mesures nécessaires pour protéger tout profil d'utilisateur s'il soupçonne que les identifiants de cet utilisateur ont été compromis en tout ou en partie d'une quelconque façon;

(b) vérifier les activités récentes dans ses comptes et ses profils d'utilisateur s'il soupçonne que les identifiants d'un utilisateur ont été compromis, et signaler sans tarder toute anomalie à la banque du profil;

(c) vérifier de manière périodique ses comptes et les profils de ses utilisateurs afin de s'assurer qu'il n'y a pas d'irrégularité et signaler sans tarder toute anomalie à la banque du profil.

6 Le responsable du profil doit retirer rapidement du profil du canal électronique un utilisateur si celui-ci quitte l'entreprise du responsable du profil. Le responsable du profil doit suspendre rapidement l'accès aux canaux électroniques à un utilisateur en cas de doute sur le comportement de l'utilisateur ou ses droits d'accès. Le responsable du profil doit s'assurer que les identifiants de sécurité ou les dispositifs ne sont utilisés que par l'utilisateur à qui les droits d'accès ont été accordés.

7 Le responsable du profil doit s'assurer que les utilisateurs ne disposent pas de plusieurs noms d'utilisateurs ni de plusieurs identifiants de sécurité.

8 S'il n'a pas reçu le dispositif d'accès sécurisé de la banque du profil, le responsable du profil doit en aviser la banque du profil dans les sept jours, dans la mesure où le responsable du profil a été avisé de cet envoi.

9 Le responsable du profil doit retourner rapidement tout dispositif d'accès sécurisé à la banque du profil si celle-ci en fait la demande.

10 Le responsable du profil doit adopter des mesures de sécurité interne et les vérifier sur une base périodique afin de s'assurer que la protection est à jour et conforme aux directives et aux meilleures pratiques des autorités réglementaires et de l'industrie. Ces mesures devraient inclure, sans s'y limiter, une protection contre les logiciels malveillants, des restrictions relatives au réseau, des restrictions d'accès physique, des restrictions d'accès à distance, des paramètres de sécurité informatique, une surveillance des utilisations inappropriées, des directives sur l'utilisation acceptable des navigateurs et du courriel, dont des directives pour éviter d'acquérir des programmes malveillants.

11 Le responsable du profil doit mettre en place des processus pour éviter que les utilisateurs soient victimes de fraude ou agissent par suite de communications frauduleuses. Ces processus doivent permettre d'éviter qu'un fraudeur envoie un courriel dans lequel il se fait passer pour une personne connue de l'utilisateur afin de lui faire modifier une adresse ou un numéro de compte bancaire pour l'envoi d'un paiement. De tels processus doivent inclure, par exemple, la vérification indépendante (autrement que par courriel) de l'authenticité de la communication lorsqu'on reçoit une communication semblant provenir d'un expéditeur connu (y compris, un membre de la haute direction ou un fournisseur).

12 Si un utilisateur accède à un canal électronique à partir d'un appareil mobile, le responsable du profil doit demander à l'utilisateur de respecter ce qui suit :

(a) ne pas laisser l'appareil mobile sans surveillance après avoir ouvert une session dans un canal électronique;

(b) cliquer sur le bouton de fermeture de session lorsqu'il a fini d'utiliser un canal électronique;

(c) activer la fonctionnalité de verrouillage par code et mot de passe automatique de l'appareil mobile;

(d) ne pas partager des appareils mobiles servant à accéder aux canaux électroniques avec d'autres;

(e) être la seule personne enregistrée pour l'authentification biométrique de l'appareil (par exemple, numérisation des empreintes digitales ou reconnaissance faciale, rétinienne ou vocale);

(f) suivre les étapes pour annuler l'enregistrement des appareils ne devant plus utiliser les méthodes d'authentification, comme décrit au paragraphe 15;

(g) ne pas accéder aux canaux électroniques à partir d'un appareil mobile ayant été débridé ou compromis d'une quelconque façon.

13 Le responsable du profil reconnaît et accepte que dans l'éventualité où l'accès au canal électronique est suspendu pour une quelconque raison, toute réactivation rétablira automatiquement tous les droits initiaux, toutes les limites, tous les accès des utilisateurs et tous les accès aux comptes et services d'avant la suspension.

14 Le responsable du profil doit savoir qu'un utilisateur qui accède à un canal électronique à partir d'un appareil mobile a accès à un grand nombre de fonctionnalités; il peut par exemple utiliser l'appareil mobile (à la place d'un dispositif d'accès sécurisé) pour authentifier des activités menées dans une session d'un canal électronique distincte d'une session à partir d'un ordinateur de bureau.

15 Dans le cas où les utilisateurs accèdent aux canaux électroniques à partir de certains appareils mobiles munis de systèmes d'authentification biométrique (par exemple, numérisation des empreintes digitales ou reconnaissance faciale), le responsable du profil reconnaît que de telles méthodes d'authentification peuvent être compromises ou utilisées pour obtenir un accès non autorisé (par exemple, par des membres proches de la famille).

Medidas de seguridad de los Canales Electrónicos

En este documento, se establecen las medidas de seguridad (que el Grupo HSBC puede revisar o actualizar de vez en cuando) para cualquier sistema de banca electrónica ("**Canales Electrónicos**") proporcionado por cualquier miembro del Grupo HSBC ("**Grupo HSBC**") a sus clientes **("Dueño del Portafolio").**

Medidas de seguridad del Grupo HSBC

1 El Grupo HSBC empleará medidas para denegar el acceso a partes externas no autorizadas al entorno en el que opera su servicio de Internet.

2 El Grupo HSBC garantizará que sus sistemas estén estrictamente controlados, lo que incluye tener planes de continuidad del negocio.

3 Como parte de las medidas de seguridad del Grupo HSBC, los usuarios autorizados por el Dueño del Portafolio ("Usuarios") que acceden al canal electrónico HSBCnet estarán sujetos a suspensión automática cuando no hayan iniciado sesión en HSBCnet en un período de 6 meses. Si un perfil de HSBCnet no es visitado por los Usuarios en un período de 18 meses, también se podrá suspender el perfil de HSBCnet.

4 Si se utilizan los métodos de autenticación biométrica (por ejemplo, la lectura de huellas dactilares o el reconocimiento facial) para acceder a un canal electrónico desde un dispositivo móvil, el Grupo HSBC y la entidad de HSBC asociada que proporciona las aplicaciones para el dispositivo móvil se reservan el derecho de eliminar la función de autenticación biométrica en cualquier momento y, si es necesario, sin previo aviso si existen problemas relacionados con la seguridad de un dispositivo. En circunstancias normales, seguirá siendo posible realizar la autenticación mediante el dispositivo móvil a través de otros métodos existentes.

Medidas de seguridad del Dueño del Portafolio

1 El Dueño del Portafolio solo podrá acceder a los canales electrónicos mediante los métodos de autenticación establecidos por el Grupo HSBC

2 El Dueño del Portafolio deberá garantizar que todos los Usuarios mantengan sus credenciales de seguridad (contraseña, respuesta fácil de recordar, respuestas de seguridad, PIN de dispositivo de seguridad, contraseña o PIN de dispositivo móvil, o cualquier otra credencial de seguridad necesaria para acceder a los canales electrónicos, según corresponda) resguardadas y secretas en todo momento y que no faciliten ningún tipo de uso no autorizado de dichas credenciales. En particular, el Dueño del Portafolio no compartirá ninguna de las credenciales de seguridad de un canal electrónico, ni el acceso a él, con ningún tercero.

3 El Dueño del Portafolio es responsable de seleccionar cuidadosamente a sus Usuarios y de comprobar que obtengan acceso a una amplia variedad de capacidades, lo que incluye la asignación de derechos a cuentas u otros servicios y el envío de instrucciones relacionadas con esas cuentas o servicios.

4 El Dueño del Portafolio deberá notificar al Grupo HSBC con prontitud en caso de perder alguno de sus dispositivos de seguridad o ser víctima de robo de ellos.

5 El Dueño del Portafolio deberá:

(a) adoptar medidas apropiadas con prontitud para proteger el perfil del Usuario en caso de tener alguna sospecha de que tales credenciales puedan haberse visto en peligro en su totalidad o en parte en cualquier forma;

(b) revisar la actividad reciente en sus cuentas y perfiles de Usuario en caso de que sospeche que haya credenciales que se han visto comprometidas e informar al Grupo HSBC con prontitud sobre cualquier discrepancia; y

(c) revisar periódicamente la actividad de su cuenta y perfil del Usuario para asegurarse de que no haya irregularidades y reportar cualquier discrepancia con prontitud al Grupo HSBC.

6 El Dueño del Portafolio deberá eliminar con prontitud a un Usuario de su perfil de Canal electrónico en caso de que cualquier Usuario abandone la organización del Dueño del Portafolio. El Dueño del Portafolio deberá suspender con prontitud el uso de los Canales electrónicos por parte de cualquier Usuario en caso de que exista alguna inquietud con respecto a la conducta de dicho Usuario o sus derechos. El Dueño del Portafolio se debe asegurar de que las credenciales o los dispositivos de seguridad solo sean utilizados por el Usuario individual específico al que están asignados.

7 El Dueño del Portafolio se debe asegurar de que los individuos no posean más de un nombre de usuario o conjunto de credenciales de seguridad.

8 El Dueño del Portafolio debe informar al Grupo HSBC, en un período de siete días a partir del envío de un dispositivo de seguridad por parte del Grupo HSBC, que no ha recibido el paquete enviado, siempre y cuando el Dueño del Portafolio haya sido informado del envío.

9 El Dueño del Portafolio deberá devolver con prontitud al Grupo HSBC cualquier dispositivo de seguridad que este le solicite.

10 El Dueño del Portafolio debe adoptar y revisar sus medidas internas de seguridad regularmente para garantizar que la protección esté actualizada y concuerde con las pautas normativas y de mejores prácticas de la industria. Estas deberían incluir, entre otros aspectos, protección contra malware, restricciones de red, restricciones de acceso físico, restricciones de acceso remoto, ajustes de seguridad del equipo, monitoreo de usos inadecuados, orientación acerca del uso aceptable de navegadores web y correos electrónicos, además de cómo evitar la obtención de malware.

11 El Dueño del Portafolio debe establecer procesos para evitar que los Usuarios sean víctimas de la ingeniería social o participen en comunicaciones fraudulentas. Esto, con el fin de evitar una intervención del correo electrónico corporativo y esquemas similares en los que un estafador envía un correo electrónico suplantando a alguien que el Usuario autorizado de un Canal electrónico conoce e intenta cambiar la dirección o el número de la cuenta bancaria a la que se enviarán los pagos. Tales procesos deberían incluir, por ejemplo, que cuando los Usuarios reciban comunicaciones de parte de remitentes aparentemente conocidos (que incluye, entre otros, a la Alta Dirección y los proveedores) se verifique la autenticidad de dichas comunicaciones de forma independiente (a través de un medio distinto del correo electrónico).

12 Si un Usuario accede a cualquier Canal electrónico a través de un dispositivo móvil, el Dueño del Portafolio debe solicitar al Usuario que:

(a) no deje el dispositivo móvil desatendido después de iniciar sesión en alguno de los Canales electrónicos;

(b) haga clic en el botón "Cerrar sesión" cuando termine de acceder a cualquier Canal electrónico;

(c) habilite la función de bloqueo automático con contraseña en su dispositivo móvil;

(d) no comparta con otros los dispositivos móviles que utiliza para acceder a los Canales electrónicos;

(e) sea la única persona registrada para la biometría (por ejemplo, cara, voz, huellas dactilares, retina, etc.) en el dispositivo;

(f) realice las acciones para anular el registro de dispositivos que ya no se utilizarán como un método de autenticación como se prevé en la cláusula 15; y

(g) no acceda al Canal electrónico mediante un dispositivo móvil liberado, con acceso al directorio raíz o que se someta a cualquier otro riesgo de seguridad.

13 El Dueño del Portafolio reconoce y acepta que, en el caso de que su Canal electrónico se suspenda por cualquier motivo, su posterior reactivación restablecerá automáticamente todos los derechos, límites, accesos del Usuario y accesos a las mismas cuentas y servicios originales con los que contaba antes de dicha suspensión.

14 El Dueño del Portafolio debe tener en cuenta que los Usuarios que acceden a un Canal electrónico mediante un dispositivo móvil pueden llevar a cabo una amplia gama de actividades con el dispositivo. Esto incluye el uso del dispositivo móvil (por ejemplo, en lugar de un dispositivo de seguridad) para autenticar las actividades realizadas en una sesión de Canal electrónico diferente con una computadora de escritorio.

15 Si los Usuarios acceden a los Canales electrónicos a través de medidas de autenticación biométricas disponibles en ciertos dispositivos móviles (por ejemplo, lectura de huellas dactilares o reconocimiento facial), el Dueño del Portafolio reconoce que dichos métodos de autenticación también representan un riesgo de seguridad o que pueden permitir el acceso a personas no autorizadas (por ejemplo, cuando hay familiares cercanos involucrados).

電子管道安全性措施

本文件將說明電子銀行業務系統 (下稱「**電子管道**」) 的安全性措施 (HSBC 集團可能會不定期修訂或更新)，適用範圍為 HSBC 集團旗下任何成員 (下稱「**設定檔銀行**」) 向客戶 (下稱「**設定檔所有人**」) 提供的任何電子銀行業務系統。

設定檔銀行安全性措施

1 設定檔銀行應採取相關措施，拒絕未經授權的外部人士存取其網際網路服務營運的環境。

2 設定檔銀行應確保自家系統受到嚴格控管，包括設立營運持續方案。

3 在設定檔銀行的安全性措施中，由設定檔所有人授權存取滙豐財資網電子管道的使用者 (下稱「**使用者**」) 若長達 6 個月未登入滙豐財資網，系統可能會根據設定檔銀行的安全性措施自動將其停權。如有匯豐財資網之設定檔在長達 18 個月的時間中沒有任何使用者存取，該匯豐財資網設定檔可能也會暫停使用。

4 如果使用生物特徵驗證方式 (如指紋掃描或臉部辨識) 從行動裝置存取電子管道，設定檔銀行及其提供應用程式至行動裝置的關聯 HSBC 實體，保留任何時間視需要移除生物特徵驗證功能的權力，若裝置有安全性相關疑慮則不另行通知。在正常情況下，仍然可以使用其他現有方法透過行動裝置進行驗證。

設定檔所有人安全性措施

1 設定檔所有人只能透過設定檔銀行指定的驗證方式存取電子管道。

2 設定檔所有人應確保所有使用者均能妥善保管其安全性認證 (密碼、提示問題答案、安全性答案、安全性裝置 PIN、行動裝置密碼/PIN 或任何需要存取電子管道的安全性認證 (如適用)) 並維持此類資訊的機密性，同時不幫助對這些認證進行任何未經授權的使用。特別是設定檔所有人不得與任何第三方分享任何安全性認證或存取電子管道。

3 謹慎挑選使用者是設定檔所有人的責任，設定檔所有人須考量到這些使用者將能存取多種功能，包括向帳戶或其他服務指派權限，以及傳送與這些帳戶或服務有關的指示。

4 若任何安全裝置遺失或遭竊，設定檔所有人應立即通知設定檔銀行。

5 設定檔所有人應：

(a) 在懷疑任何使用者的認證透過任何方式遭到部分或完全盜用時，立即採取適當動作保護該使用者的設定檔；

(b) 在懷疑任何使用者的認證遭盜用時，審查其帳戶和使用者設定檔的近期活動，並在有任何異常情形時，立即通知設定檔銀行；以及

(c) 定期審查其帳戶和使用者設定檔的活動，藉此確保沒有異常情形，並在有任何異常情形時，立即通報設定檔銀行。

6 如有任何此類使用者離開設定檔所有人的組織，設定檔所有人應立即從電子管道設定檔中移除該使用者。若對使用者的行為或權限有任何疑慮，設定檔所有人應立即暫停該使用者對電子管道的使用。設定檔所有人應確保安全性認證或裝置僅由指派的特定個人使用者使用。

7 設定檔所有人應確保每個人只維護一個使用者名稱或一組安全性認證。

8 設定檔所有人若得知設定檔銀行已寄送安全性裝置，卻未收到寄送的包裹，則應在寄送後的七天內通知設定檔銀行。

9 若經設定檔銀行要求，設定檔所有人應立即將任何安全裝置歸還給設定檔銀行。

10 設定檔所有人應定期採用及審查其內部安全性措施，藉此確保所有保護措施保持在最新狀態，並符合法規及產業的最佳實務指示。這包括但不限於惡意軟體防護、網路限制、實體存取限制、遠端存取限制、電腦安全性設定、不當使用情況的監控、可接受的網路瀏覽器與電子郵件使用方式 (包括如何避免收取惡意軟體) 的指引。

11 設定檔所有人應設立相關流程，避免使用者遭受社交工程攻擊或聽從詐騙通訊的指示行動。這是為了防止企業電子郵件遭盜用和其他類似的攻擊手法，避免詐騙者冒充為電子管道之授權使用者已知的對象，並寄送電子郵件給授權使用者，企圖變更收款對象的地址或銀行帳號。此類流程應包括如使用者收到看似來自已知寄件者 (包括但不限於高階管理階層、供應商和廠商) 的通訊內容時，如何確保獨立驗證 (透過電子郵件以外的方式) 此類通訊內容的真實性。

12 若使用者透過行動裝置存取任何電子管道，設定檔所有人應要求該使用者：

(a) 登入任何電子管道後，切勿讓行動裝置處於無人看管的情況下；

(b) 存取完任何電子管道後，按一下「登出」按鈕；

(c) 啟用行動裝置的自動密碼鎖定功能；

(d) 不與他人分享用於存取電子管道的行動裝置；

(e) 為裝置中唯一註冊了生物驗證 (臉部辨識、指紋、聲音、視網膜) 的人；

(f) 採取行動以取消註冊不應再作為第 15 條的條款中所認定之驗證方法的裝置；以及

(g) 不經由任何已越獄、取得最高使用權限或其他修改的行動裝置存取電子管道。

13 設定檔所有人瞭解並同意，其電子管道若因任何原因遭停用，該電子管道後續的任何重新啟用作業，都會將所有權限、限制、使用者存取權以及對相同帳戶和服務的存取權，恢復至停用前的原始狀態。

14 設定檔所有人應瞭解使用行動裝置存取電子管道的使用者可以使用該裝置執行廣泛的活動。這包括使用行動裝置 (如代替安全性裝置) 驗證在獨立電子管道工作階段經由桌上型電腦執行的活動。

15 當使用者經由某些行動裝置上可用的生物特徵驗證方式存取電子管道時 (如指紋掃描或臉部辨識)，設定檔所有人瞭解此種驗證方式依舊存在被侵害或允許未經授權的存取風險 (例如親近的家庭成員涉入)。

电子渠道安全措施

本文件阐述了汇丰集团成员（以下简称“业务关系行”）向其客户（以下简称“业务关系所有人”）提供任何电子银行系统（以下简称“电子渠道”）的安全措施（经汇丰集团不时的修订或更新）。

业务关系行安全措施

1 业务关系行应采取措施不让未经授权的外部人士对其互联网服务运行环境进行访问。

2 业务关系行应确保其系统受到严格控制，包括制定业务连续性计划。

3 作为业务关系行安全措施的一部分，由业务关系所有人授权可访问汇丰财资网电子渠道的用户（“用户”），如在 6 个月内未登录汇丰财资网，其登录权限将自动暂停生效。如果某汇丰财资网客户资料在 18 个月内未被任何用户访问，则该客户资料也会被暂停访问。

4 如果使用生物识别认证方法（例如指纹扫描或面部识别）从移动设备访问电子渠道，则向移动设备提供应用程序的业务关系行和相关汇丰实体保留在必要情况下（如出现与设备安全相关的问题）无需通知即可随时删除生物识别认证功能的权利。在正常情况下，使用其他现有方法通过移动设备进行身份验证仍可行。

业务关系所有人安全措施

1 业务关系所有人应只采用业务关系行规定的认证方法访问电子渠道。

2 业务关系所有人应确保所有用户始终保证安全证书（密码、提示答案、安全问题答案、安全设备PIN码、移动设备密码/PIN或访问电子渠道所需的任何其他安全证书（如果适用））安全且处于保密状态，且不支持在未经授权的情况下使用这些证书。尤其是，业务关系所有人不得与任何第三方分享安全证书或电子渠道的访问权。

3 业务关系所有人应谨慎选择其用户，因该等用户有权进行广泛的活动，包括赋予有关账户或其它服务的授权并代表业务关系所有人和/或开户人发出指令。

4 当任何安全设备丢失或被盗时，业务关系所有人应立即通知业务关系行。

5 业务关系所有人应：

(a) 在怀疑用户证书已经以任何方式全部或部分受损时，立即采取适当行动来保护该用户的个人资料；

(b) 在怀疑用户证书已经被受损时，对其账户上的近期活动及用户资料进行审核，并且立即将发现的任何差异通知业务关系行；且

(c) 定期审核其账户以及用户的资料活动，以确保不存在任何异常，并且及时向业务关系行汇报发现的任何差异。

6 如果任何用户离开业务关系所有人的机构，业务关系所有人应立即禁止该用户使用电子渠道。业务关系所有人如果对任何用户的行为或其权限有任何疑虑，则应立即暂停该用户的电子渠道使用权。业务关系所有人应确保，安全凭据或安全设备仅被获得该等凭据或设备的特定个人用户使用。

7 业务关系所有人应确保，个人不能持有多个用户名或多套安全证书。

8 业务关系所有人应在业务关系行发出安全设备后七天之内，通知业务关系行其尚未收到发送的包裹，但前提是业务关系所有人收到了派件提示。

9 一旦业务关系行提出要求，业务关系所有人应立即将安全设备归还业务关系行。

10 业务关系所有人应采取并定期审查内部安全措施，以确保保护措施及时且符合法规和行业最佳实践指导。此等保护措施应当包括（但不限于）恶意软件防护、网络限制、物理访问限制、远程访问限制、电脑安全设置、监控不当使用、关于如何选择可接受的网页浏览器和使用电子邮件（包括如何避免沾染恶意软件）的指导。

11 业务关系所有人应有措施防止用户陷入社交工程陷阱或根据欺诈指令行事。此项是为防止商业邮件欺诈或类似骗局，即行骗者发送邮件假扮为电子渠道的授权用户所认识的某人，从而试图修改接收款项的地址或银行账号。例如，该等措施应包括：若从看似认识的发送人（包括但不限于高级管理层、卖方或供应商）处收到通讯信息，应确保对该等通讯信息的真实性（以非电子邮件形式）进行独立验证。

12 当用户通过移动设备访问任何电子渠道时，业务关系所有人应要求该用户：

(a) 不要在登录到任何电子渠道之后，使移动设备处于无人看管状态；

(b) 在用户结束电子渠道访问后，点击`退出'按钮；

(c) 启用移动设备的自动密码锁功能；

(d) 不与他人共享用于访问电子渠道的移动设备；

(e) 是唯一在设备上注册生物识别（例如面部、指纹、语音、视网膜识别等）的人士；

(f) 根据第 15 条的规定，注销不应再用作身份验证的设备；以及

(g) 不通过已被破解、取得根权限或以其他方式被破坏的移动设备访问电子渠道。

13 业务关系所有人确认并同意，如果其电子渠道由于任何原因被暂停使用，该电子渠道在被重新激活后，将自动恢复与暂停之前相同的原权限、限额、用户访问以及可访问的账户和服务。

14 业务关系所有人应注意，通过移动设备访问电子渠道的用户可以使用设备开展各种活动。这包括利用移动设备（例如代替安全设备）对通过台式计算机执行的单独电子渠道会话中开展的活动进行身份验证。

15 如果用户通过可在某些移动设备上使用的生物识别身份验证方式（例如指纹扫描或面部识别）访问电子渠道，则业务关系所有人承认此类认证方式仍然存在被破坏或允许未经授权人士（例如在涉及亲密的家庭成员的情况）访问的风险。

Tindakan Keamanan E-Channel

Dokumen ini mengatur tindakan keamanan (yang isinya dapat direvisi atau diubah oleh HSBC Group dari waktu ke waktu) untuk sistem perbankan elektronik ("**E-Channel**") yang disediakan oleh anggota grup HSBC ("**Bank Profil**") kepada nasabahnya ("**Pemilik Profil**").

Tindakan Keamanan Bank Profil

1 Bank Profil harus menggunakan upaya untuk menolak akses oleh pihak eksternal yang tidak sah ke dalam lingkungan tempat di mana layanan internetnya beroperasi.

2 Bank Profil harus memastikan bahwa sistemnya dikontrol dengan ketat termasuk memiliki rencana keberlangsungan bisnis.

3 Sebagai bagian dari langkah keamanan Bank Profil, pengguna yang diotorisasi oleh Pemilik Profil ("**Pengguna**") yang mengakses HSBCnet E-Channel dapat ditangguhkan secara otomatis apabila tidak login ke HSBCnet dalam jangka waktu 6 bulan. Jika profil HSBCnet tidak diakses oleh Pengguna dalam jangka waktu 18 bulan, profil HSBCnet juga dapat ditangguhkan.

4 Jika metode autentikasi biometrik (contohnya, pemindaian sidik jari atau pengenalan wajah) digunakan untuk mengakses E-Channel dari perangkat seluler, Bank Profil dan entitas HSBC terkait yang menyediakan aplikasi ke perangkat seluler, memiliki hak untuk menghapus fitur autentikasi biometrik kapan saja dan, jika perlu, tanpa pemberitahuan jika terdapat masalah keamanan perangkat. Dalam keadaan normal, autentikasi melalui perangkat seluler masih dapat dilakukan menggunakan metode lainnya yang tersedia.

Tindakan Keamanan Pemilik Profil

1 Pemilik Profil hanya boleh mengakses E-Channel menggunakan metode autentikasi yang ditentukan oleh Bank Profil.

2 Pemilik Profil harus memastikan bahwa semua Pengguna menyimpan kredensial keamanan (kata sandi, jawaban yang mudah diingat, jawaban keamanan, PIN Perangkat Keamanan, kata sandi/PIN perangkat seluler, atau kredensial keamanan lainnya yang diperlukan untuk mengakses E-Channel, sebagaimana berlaku) dengan aman dan rahasia sepanjang waktu dan tidak memfasilitasi penggunaan kredensial ini secara tidak sah. Secara khusus, Pemilik Profil tidak boleh berbagi kredensial keamanan atau akses E-Channel dengan pihak ketiga mana pun.

3 Pemilik Profil bertanggung jawab untuk memilih Penggunanya secara cermat, dengan mempertimbangkan bahwa Pengguna tersebut akan diberikan akses ke berbagai kemampuan, termasuk memberikan hak atas rekening atau layanan lain dan mengirimkan perintah terkait dengan rekening atau layanan tersebut.

4 Pemilik Profil harus segera memberi tahu Bank Profil jika Perangkat Keamanan hilang atau dicuri.

5 Pemilik Profil harus:

(a) segera mengambil tindakan yang sesuai untuk melindungi profil Pengguna jika dicurigai kredensial Pengguna telah disalahgunakan secara sebagian atau sepenuhnya dengan cara apa pun;

(b) meninjau aktivitas terbaru pada akun dan profil Pengguna jika dicurigai kredensial telah disalahgunakan dan segera memberi tahu Bank Profil jika ada ketidaksesuaian; dan

(c) secara teratur meninjau aktivitas rekening dan profil Pengguna untuk memastikan tidak ada penyimpangan dan segera melaporkan ketidaksesuaian ke Bank Profil.

6 Pemilik Profil harus segera menghapus Pengguna dan profil E-Channel jika Pengguna tersebut keluar dari organisasi Pemilik Profil. Pemilik Profil harus segera menangguhkan penggunaan E-Channel oleh Pengguna jika ada masalah terkait tindakan pengguna tersebut atau hak yang dimilikinya. Pemilik Profil harus memastikan bahwa kredensial atau perangkat hanya digunakan oleh Pengguna yang telah ditetapkan.

7 Pemilik Profil harus memastikan bahwa individu tidak memiliki lebih dari satu nama pengguna atau set kredensial keamanan.

8 Pemilik Profil harus memberi tahu Bank Profil dalam 7 hari pengiriman Perangkat Keamanan oleh Bank Profil bahwa ia belum menerima paket yang dikirim, asalkan Pemilik Profil diberi tahu tentang pengiriman tersebut.

9 Pemilik Profil harus segera mengembalikan Perangkat Keamanan ke Bank Profl jika diminta oleh Bank Profil.

10 Pemilik Profil harus menerapkan dan meninjau tindakan keamanan internalnya secara berkala guna memastikan perlindungan tetap terbaru dan sesuai dengan perundang-undangan dan pedoman praktik terbaik industri. Perlindungan tersebut harus mencakup, tetapi tidak terbatas pada, perlindungan malware, pembatasan jaringan, pembatasan akses fisik, pembatasan akses jarak jauh, pengaturan keamanan

komputer, pemantauan penggunaan yang tidak tepat, panduan tentang browser web, dan penggunaan email yang layak termasuk cara menghindari malware.

11 Pemilik Profil harus memiliki proses yang sudah disiapkan untuk mencegah Pengguna direkayasa secara sosial atau terlibat dalam komunikasi yang menipu. Ini untuk mencegah email bisnis disalahgunakan dan skema yang serupa di mana penipu mengirimkan email seolah-olah berasal dari seseorang yang dikenal oleh Pengguna E-Channel yang diotorisasi dan ingin mengubah alamat atau nomor rekening tempat pembayaran dikirimkan. Proses semacam ini harus menyertakan, misalnya, saat komunikasi diterima oleh Pengguna yang seolah-olah berasal dari pengirim yang dikenal (termasuk, tapi tidak terbatas pada, manajemen senior, pemasok dan vendor) guna memastikan keaslian komunikasi semacam itu harus diverifikasi secara mandiri (melalui sarana lain selain email).

12 Jika E-Channel diakses oleh Pengguna melalui perangkat seluler, Pemilik Profil harus meminta Pengguna:

(a) tidak meninggalkan perangkat seluler tanpa pengawasan setelah login ke E-Channel;

(b) mengklik tombol ‘Logout’ ketika Pengguna selesai mengakses E-Channel;

(c) mengaktifkan fitur kunci kode sandi otomatis pada perangkat seluler;

(d) tidak berbagi perangkat seluler yang digunakan untuk mengakses E-Channel dengan orang lain;

(e) adalah satu-satunya orang yang terdaftar untuk akses biometrik (contohnya, wajah, sidik jari, suara, retina, dll.) pada perangkat;

(f) mengambil langkah-langkah untuk menghapus pendaftaran perangkat yang tidak lagi digunakan sebagai metode autentikasi seperti yang telah dijelaskan dalam klausul 15; dan

(g) tidak mengakses E-Channel melalui perangkat seluler yang telah di-jailbreak, di-root, atau diotak-atik.

13 Pemilik Profil mengakui dan menyetujui bahwa apabila E-Channel-nya ditangguhkan karena alasan apa pun, setiap aktivasi ulang E-Channel berikutnya akan secara otomatis mengembalikan semua hak, batas, akses Pengguna, dan akses ke rekening dan layanan seperti semula sebelum penangguhan.

14 Pemilik Profil harus mengetahui bahwa Pengguna yang mengakses E-Channel melalui perangkat seluler dapat melakukan berbagai aktivitas menggunakan perangkat tersebut. Ini termasuk memanfaatkan perangkat seluler (misalnya sebagai pengganti Perangkat Keamanan) untuk mengautentikasi aktivitas yang dilakukan pada sesi E-Channel terpisah yang dilakukan melalui komputer desktop.

15 Apabila Pengguna mengakses E-Channels melalui tindakan autentikasi biometrik yang tersedia pada perangkat seluler tertentu (misalnya, pemindaian sidik jari atau pengenalan wajah), maka Pemilik Profil menyadari bahwa metode autentikasi masih menimbulkan risiko pembobolan atau mengizinkan akses yang tidak sah (misalnya saat ada anggota keluarga dekat yang terlibat).

5 على صاحب المعلومات التعريفية القيام بما يلي:

(a) اتخاذ الإجراءات الملائمة بسرعة لحماية المعلومات التعريفية للمستخدم في حال ساورته الشكوك باحتمال تعرّض بيانات اعتماد المستخدم للخطر، بشكل كامل أو جزئي، بأي طريقة من الطرق؛

(b) ومراجعة الأنشطة الأخيرة على حساباته وتلك المتعلقة بالمعلومات التعريفية للمستخدم في حال ساورته الشكوك بتعرّض أي بيانات اعتماد تابعة للمستخدم للخطر وإعلام بنك المعلومات التعريفية بسرعة بأي اختلافات؛

(c) ومراجعة حسابه ونشاط المستخدمين في ما يتعلق بالمعلومات التعريفية بانتظام لضمان عدم وجود أي اختلافات، وإبلاغ بنك المعلومات التعريفية بسرعة بأي اختلافات.

6 يزيل صاحب المعلومات التعريفية مستخدم ما من المعلومات التعريفية لقناته الإلكترونية بسرعة في حال ترك هذا المستخدم شركته .يعلّق صاحب المعلومات التعريفية استخدام القنوات الإلكترونية من أي مستخدم بسرعة في حال برزت أي مخاوف حول سلوك ذلك المستخدم أو تخويلاته. يضمن صاحب المعلومات التعريفية أنه لا يتم استخدام بيانات اعتماد الأمان أو الأجهزة إلّا من قبل المستخدم الفردي المحدد المُعينة له .

7 يضمن صاحب المعلومات التعريفية عدم احتفاظ الأفراد بأكثر من اسم مستخدم واحد أو مجموعة واحدة من بيانات اعتماد الأمان.

8 يُعلم صاحب المعلومات التعريفية بنك المعلومات التعريفية، خلال سبعة أيام من إرسال بنك المعلومات التعريفية جهاز أمان، بعدم استلامه الحزمة المرسلة بعد، شرط أن يكون صاحب المعلومات التعريفية على علم بعملية الإرسال.

9 يُعيد صاحب المعلومات التعريفية أي أجهزة أمان إلى بنك المعلومات التعريفية بسرعة بعد أن يطلب منه هذا الأخير ذلك.

10 يعتمد صاحب المعلومات التعريفية التدابير الأمنية الداخلية ويراجعها بشكل منتظم لضمان المحافظة على حداثة طرق الحماية وتوافقها مع توجيهات أفضل الممارسات التنظيمية وأفضل الممارسات في المجال. ينبغي أن يشمل ذلك، على سبيل المثال لا الحصر، الحماية من البرامج الضارة، وقيود الشبكة، وقيود الوصول المادي، وقيود الوصول عن بُعد، وإعدادات أمان الكمبيوتر، ومراقبة الاستخدام غير السليم، والتوجيهات حول الاستخدام المقبول لمستعرضات الويب والبريد الإلكتروني بالإضافة إلى الطريقة التي يمكن اتّباعها لتجنب التعرض للبرامج الضارة.

11 يتبع صاحب المعلومات التعريفية إجراءات لمنع تعرض المستخدمين لانتحال الشخصية عبر الهندسة الاجتماعية أو للحؤول دون أن يتخذوا قراراتهم بالاستناد إلى بلاغات احتيالية .ويهدف ذلك إلى منع تعريض البريد الإلكتروني الخاص بالشركة للخطر ومنع أي مخططات مماثلة يعمد المحتال من خلالها إلى إرسال بريد إلكتروني إلى مستخدم مفوّض استخدام القناة الإلكترونية منتحلاً فيها شخصية معروفة لديه ليطلب من هذا المستخدم تغيير عنوان ما أو رقم حساب مصرفي يتم تحويل الدفعات إليه. ويجب أن تشمل هذه الإجراءات، على سبيل المثال، عندما يتلقى المستخدمون بلاغات تبدو وكأنها مُرسلة من مُرسلين معروفين (بما في ذلك، على سبيل المثال لا الحصر، الإدارة العليا والموردين والبائعين) لضمان التحقق من صحة هذه البيانات بشكل مستقل (عبر طرق مغايرة للبريد الإلكتروني.)

لتدابير الأمنية للقنوات الإلكترونية

يحدد هذا المستند التدابير الأمنية (حسبما قد تتم مراجعتها أو يتم تحديثها من قبل مجموعة HSBC من وقت لآخر) لأي أنظمة مصرفية إلكترونية") **القنوات الإلكترونية** ("يوفّرها أي عضو في مجموعة ") HSBC**بنك المعلومات التعريفية** ("إلى عملائه") **صاحب المعلومات التعريفية** ").

التدابير الأمنية الخاصة ببنك المعلومات التعريفية

1 يستخدم بنك المعلومات التعريفية تدابير لرفض وصول الجهات الخارجية غير المفوضة إلى البيئة حيث تعمل خدمة الإنترنت الخاصة به.

2 يضمن بنك المعلومات التعريفية مراقبة أنظمته مراقبة صارمة، بما في ذلك وضع خطط لاستمرارية الأعمال.

3 كجزء من تدابير بنك المعلومات التعريفية الأمنية، قد يخضع المستخدمون المفوّضون من صاحب المعلومات التعريفية ")**المستخدمون** ("والذين يصلون إلى القناة الإلكترونية HSBCnet E-Channelإلى التعليق التلقائي في حال لم يكونوا قد سجلوا دخولهم إلى HSBCnet خلال 6 أشهر. في حال لم يصل أي مستخدم إلى معلومات تعريفية ما على HSBCnetفي غضون 18 شهراً، قد يتم تعليق المعلومات التعريفية على HSBCnet أيضاً.

4 في حال استُخدمت طرق المصادقة الحيوية) كميزة مسح البصمة أو التعرف إلى الوجه) للوصول إلى القناة الإلكترونية من جهاز محمول ما، يحتفظ بنك المعلومات التعريفية وكيان HSBCالمرتبط الذي يوفّر التطبيقات الخاصة بالأجهزة المحمولة بالحق في إزالة ميزة المصادقة الحيوية في أي وقت كان، ومن دون إرسال أي إشعار، إن دعت الحاجة، إذا ما برزت أي مخاوف ذات صلة بأمان جهاز ما. في الظروف العادية، ستبقى إمكانية المصادقة، عن طريق الجهاز المحمول باستخدام طرق أخرى قائمة، متاحة .

التدابير الأمنية الخاصة بصاحب المعلومات التعريفية

1 لا يمكن لصاحب المعلومات التعريفية الوصول إلى القنوات الإلكترونية إلّا باستخدام طرق المصادقة المذكورة بواسطة بنك المعلومات التعريفية .

2 يضمن صاحب المعلومات التعريفية محافظة جميع المستخدمين على أمان بيانات اعتماد الأمان الخاصة بهم وسريّتها دائماً (ككلمة المرور، أو الإجابة التي يمكن تذكّرها، أو إجابات الأمان، أو رمز PIN الخاص بجهاز الأمان، أو كلمة مرور الجهاز المحمول أو رمز PIN الخاص به، أو أي بيانات اعتماد أمان أخرى مطلوبة للوصول إلى القنوات الإلكترونية بحسب الاقتضاء)، وألّا يعمدوا إلى تسهيل أي استخدام غير مفوّض لبيانات الاعتماد هذه. وبشكل خاص، يمتنع صاحب المعلومات التعريفية عن مشاركة أي من بيانات اعتماد الأمان وعن الوصول إلى قناة إلكترونية مع أي جهة خارجية.

3 إنّ صاحب المعلومات التعريفية مسؤول عن اختيار المستخدمين بدقة، آخذاً بعين الاعتبار أنه يتم تزويد المستخدمين بحق الوصول إلى مجموعة واسعة من الإمكانيات، بما في ذلك تعيين تخويلات للحسابات أو أي خدمات أخرى بالإضافة إلى إرسال تعليمات تتعلّق بهذه الحسابات أو الخدمات .

4 على صاحب المعلومات التعريفية إعلام بنك المعلومات التعريفية بسرعة في حال تم فقدان أي أجهزة أمان أو تمت سرقتها.

12 إذا وصل المستخدم إلى القناة الإلكترونية من خلال جهاز محمول، فيطلب مالك المعلومات التعريفية من المستخدم ما يلي:

(a) عدم ترك الجهاز المحمول من دون مراقبة بعد تسجيل الدخول إلى أي قنوات إلكترونية؛

(b) والنقر فوق الزر" تسجيل الخروج "عندما ينتهي المستخدم من تواجده في أي قنوات إلكترونية؛

(c) وتمكين ميزة تأمين رمز المرور التلقائي على الجهاز المحمول؛

(d) وعدم مشاركة الأجهزة المحمولة التي يتم استخدامها للوصول إلى القنوات الإلكترونية مع الآخرين؛

(e) وبقاؤه هو وحده مسجّلاً على الجهاز لاستخدام الميزات المرتبطة بالمقاييس الحيوية (كالوجه وبصمة الاصبع والصوت وشبكية العين وغيرها)؛

(f) واتخاذ الخطوات اللازمة لإلغاء تسجيل الأجهزة التي لا ينبغي أن يتم استخدامها كطريقة مصادقة بعد الآن وفقاً لما هو منصوص عليه في البند 15؛

(g) والامتناع عن الوصول إلى القناة الإلكترونية من خلال جهاز محمول مكسور الحماية أو محدد الجذر أو بخلاف ذلك معرض للخطر.

13 يقر صاحب المعلومات التعريفية بأنه في حال تم تعليق القناة الإلكترونية التابعة له لأي سبب من الأسباب، فستؤدي تلقائيًا أي إعادة تنشيط لاحقة للقناة الإلكترونية هذه إلى إعادة كل التخويلات الأصلية والحدود وإمكانية وصول المستخدم إلى الحسابات والخدمات نفسها والوصول إليها إلى الحالة التي كانت عليها قبل هذا التعليق، ويوافق على ذلك.

14 ينبغي أن يكون صاحب المعلومات التعريفية على علم بأنه بإمكان المستخدمين الذين يصلون إلى قناة إلكترونية عن طريق الجهاز المحمول إجراء مجموعة واسعة من الأنشطة باستخدام الجهاز. ويشمل ذلك استخدام الجهاز المحمول (بدلاً من جهاز أمان على سبيل المثال (للمصادقة على أنشطة التي تتم في جلسة قناة إلكترونية منفصلة يتم إجراؤها عن طريق كمبيوتر مكتبي .

15 عندما يصل المستخدمون إلى القنوات الإلكترونية عن طريق تدابير المصادقة الحيوية المتوفرة في بعض الأجهزة المحمولة (كميزة مسح البصمة أو التعرف إلى الوجه)، يقر صاحب المعلومات التعريفية بأن طرق المصادقة هذه لا تزال تشكل خطر التعرض للاختراق أو السماح بالوصول غير المفوّض (على سبيل المثال عندما يتم إشراك أفراد العائلة المقرّبين.)