Langkah-Langkah Pengamanan 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**").

1 Langkah-langkah Pengamanan Bank Profil

1.1 Bank Profil harus menerapkan sejumlah tindakan untuk menolak akses oleh pihak luar yang tidak sah ke lingkungan tempat layanan Internet miliknya beroperasi.

1.2 Bank Profil harus memastikan sistemnya dikontrol secara ketat, termasuk memiliki program keberlanjutan bisnis.

1.3 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.

1.4 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.

2 Langkah-langkah Pengamanan Pemilik Profil

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

2.2 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 (selain dari penyedia layanan pihak ketiga teregulasi yang telah di otorisasi oleh Pemilik Profil).

2.3 Pemilik Profil bertanggung jawab atas pemilihan Pengguna dengan hati-hati, mengingat bahwa Pengguna tersebut diberi akses ke berbagai kemampuan termasuk memberikan hak kepada rekening atau layanan lainnya dan mengirimkan instruksi terkait dengan rekening atau layanan tersebut.

2.4 Pemilik Profil harus segera memberi tahu Bank Profil jika perangkat keamanan hilang atau dicuri.

2.5 Pemilik Profil harus:

(a) segera mengambil tindakan yang sesuai untuk melindungi profil Pengguna jika menduga kredensial Pengguna tersebut telah terungkap sepenuhnya atau sebagian dengan cara apa pun;

(b) memeriksa aktivitas terakhir di rekeningnya dan profil Pengguna jika menduga kredensial Pengguna telah terungkap dan segera memberi tahu Bank Profil tentang perbedaan apa pun; dan

(c) secara rutin memeriksa rekeningnya dan aktivitas profil Pengguna dan hak untuk memastikan tidak ada penyimpangan dan segera melaporkan perbedaan apa pun kepada Bank Profil.

2.6 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 selain dari penyedia layanan pihak ketiga teregulasi yang telah di otorisasi oleh Pemilik Profil.

2.7 Pemilik Profil harus memastikan bahwa para penggunanya memberikan informasi yang benar, penuh dan tidak disingkat kapan pun diminta oleh Grup HSBC. Pemilik Profil selanjutnya akan memastikan bahwa para pengguna profilnya meninjau secara teratur informasi tersebut dan memperbarui rinciannya setiap kali ada perubahan pada detil mereka dan tidak memelihara lebih dari satu nama pengguna atau lebih dari satu set pengenal keamanan pada satu waktu.

2.8 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.

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

2.10 Pemilik Profil harus menerapkan dan meninjau tindakan keamanan internalnya secara berkala guna memastikan perlindungan tetap terbaru dan sesuai dengan perundangundangan 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.

2.11 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).

2.12 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.

2.13 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.

2.14 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.

2.15 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).