

SKRIPSI

PERLINDUNGAN HUKUM TERHADAP NASABAH PENGGUNA INTERNET BANKING ATAS KEBOCORAN RAHASIA BANK



NURUL KHOIRIYAH

NIM. 030015126

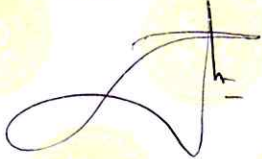
**FAKULTAS HUKUM
UNIVERSITAS AIRLANGGA
SURABAYA
2004**

**PERLINDUNGAN HUKUM TERHADAP
NASABAH PENGGUNA INTERNET BANKING
ATAS KEBOCORAN RAHASIA BANK**

SKRIPSI

**DIAJUKAN UNTUK MELENGKAPI TUGAS DAN
MEMENUHI SYARAT MEMPEROLEH GELAR
SARJANA HUKUM**

Dosen Pembimbing.



Mohammad Sumedi, S.H., M.H.
NIP. 131 653 463

Penyusun



Nurul Khoiriyah
NIM. 030015126

**FAKULTAS HUKUM
UNIVERSITAS AIRLANGGA
SURABAYA
2004**

Skripsi ini telah diuji dan dipertahankan di hadapan Panitia Penguji
Pada tanggal 9 Agustus 2004, pukul 09.00 WIB

Panitia Penguji Skripsi

Ketua : Drs. Abdul Shomad, SH., M.H.



Anggota : 1 Mohammad Sumedi, SH., M.H.

2. Trisadini Prasastinah Usanti, SH., M.H



Cipta Karya
(031) 1041020

**“PERTAMA- TAMA KATAKAN PADA DIRIMU APA YANG AKAN
KAU RAIH; LALU LAKUKAN APA YANG PERLU KAU LAKUKAN”
(EPICTETUS)**

**“RINTANGAN DI HADAPAN KITA TAK PERNAH SEBESAR
KEKUATAN DI BELAKANG KITA, LAGIPULA SETIAP RINTANGAN
MERUPAKAN KESEMPATAN UNTUK MEMPERBAIKI KEADAAN”**

KATA PENGANTAR

Puji syukur saya panjatkan atas kehadiran Tuhan Yang Maha Esa yang telah memberikan tuntunan dan kekuatan-Nya sehingga skripsi yang berjudul “Perlindungan Hukum Terhadap Nasabah Pengguna Internet Banking Atas Kebocoran Rahasia Bank” ini dapat terselesaikan.

Dalam kesempatan ini, saya mengucapkan banyak terima kasih kepada pihak-pihak yang telah membantu penulis guna menyelesaikan skripsi ini, antara lain:

1. Bapak Mohammad Sumedi, S.H., M.H. selaku dosen wali sekaligus dosen pembimbing yang telah bersedia meluangkan waktu untuk membimbing selama saya berada di Fakultas Hukum Universitas Airlangga ini dan memberikan ide dalam penulisan skripsi ini.
2. Tim Dosen Penguji, Bapak Drs. Abdul Shomad, SH., MH., dan ibu Trisadini Prasastinah Usanti, SH.M.H., terima kasih atas petunjuk-petunjuknya.
3. Bapak Machsoen Ali, SH., MS, selaku Dekan Fakultas Hukum Universitas Airlangga.
4. Keluargaku Bapak Achmad Sanusi, Ibu Umu Zumroh, kakak- kakakku mas Didik, mas Herrie, Tobing, dan mas Totok atas segala dukungan, perhatian dan kasih sayang yang selama ini telah diberikan. I guess I'm blessed to have this kind of family.

5. Tedi Heriyanto, my brother, my bestfriend, my teacher, my inspiration, my guard, my uncle and my everything. Thanks for supports, time, patiently, and incredible article.
6. Bapak I Wayan Titib Sulaksana, S.H., M.S., terima kasih telah menjadi dosen dan sekaligus pembimbing.
7. Sahabat- sahabatku Icha, Indra, Endah, Winny, Laily dan Elmy. Thanks girls!!
8. Teman- teman di FHUA (Winda, Wawan, dll), UPKBH(Riesa, Ika, Sumar, dll), DJ (Agung, Dio, Yohanes, dll), KKN-BK ke-29 tahun 2004 Kel. Lidah Wetan, dan teman- teman SMU YWSG (Jira, yuyun, dll)
9. Last but not least, my biggest inspiration in love and life, X'tian. I'm so glad to know you, the best creature God ever made. Du bist ein mirakel.
10. Buat semua yang belum aku sebutkan, blame my head not my heart. Thanks all.

Akhir kata, saya sangat mengharapkan kritik dan saran dari para pembaca sebagai masukan yang berharga untuk lebih menyempurnakan skripsi ini, semoga skripsi ini bermanfaat bagi kita semua.

Surabaya, 09 Agustus 2004

Penulis

DAFTAR ISI

HALAMAN JUDUL	i
LEMBAR PERSETUJUAN	ii
LEMBAR PENGESAHAN	iii
LEMBAR MOTTO	iv
KATA PENGANTAR	v
DAFTAR ISI	vii
BAB I : PENDAHULUAN	
1. Permasalahan : Latar Belakang dan Rumusannya	1
2. Penjelasan Judul	11
3. Alasan Pemilihan Judul	13
4. Tujuan Penelitian	14
5. Metode Penelitian	14
6. Pertanggungjawaban Sistematika	16
BAB II : FAKTOR- FAKTOR PENYEBAB KEBOCORAN RAHASIA BANK AKIBAT PENGGUNAAN INTERNET BANKING	
1. Standard Pengamanan Internet Banking	18
2. Faktor Media	28
3. Faktor Manusia	30

**BAB III : BENTUK PERLINDUNGAN HUKUM BAGI NASABAH
PENGGUNA INTERNET BANKING APABILA TERJADI
KEBOCORAN RAHASIA BANK**

1. Perlindungan Hukum Preventif.....33
2. Perlindungan Hukum Represif.....37

BAB IV : PENUTUP

1. Kesimpulan.....43
2. Saran.....44

DAFTAR BACAAN

LAMPIRAN

BAB I

PENDAHULUAN

Cipta Karya
(031) 5941926

BAB 1

PENDAHULUAN

1. Permasalahan: Latar Belakang dan Rumusannya

Dunia perbankan merupakan salah satu aspek paling utama dalam roda perekonomian nasional. Keberadaan perbankan sangat berpengaruh bagi keberlangsungan perekonomian nasional. Apabila kehidupan perbankan nasional berlangsung dengan baik dan stabil, hal ini akan memberi pengaruh positif terhadap kehidupan perekonomian nasional. Oleh karena itu dunia perbankan dituntut untuk dapat selalu mengembangkan diri dan membuat kemajuan-kemajuan dalam dirinya sendiri. Untuk dapat mencapai hal itu perbankan harus terus berusaha untuk selalu mengikuti perkembangan yang terjadi. Perkembangan ini tidak hanya semata-mata dalam bidang perbankan sendiri melainkan juga di bidang-bidang yang lain, terutama dalam hal teknologi. Hal ini karena teknologi merupakan suatu bidang yang memang paling banyak berkembang, seperti halnya setiap saat teknologi terus berkembang dengan pesatnya.

Perkembangan teknologi yang sangat pesat tersebut dapat dimanfaatkan bank-bank untuk meningkatkan kualitas pelayanan bagi nasabah. Salah satu bentuk perkembangan teknologi yang bisa membantu dunia perbankan meningkatkan kualitas pelayanan tersebut adalah di bidang teknologi informasi khususnya internet. Bentuk konkretnya yaitu dengan diaktifkannya fasilitas *Internet Banking*, yaitu fasilitas atau layanan yang diberikan bank kepada nasabah yang memungkinkan nasabah untuk melakukan transaksi perbankan melalui

internet, dimana dengan adanya fasilitas ini maka nasabah dapat melakukan berbagai transaksi perbankan yang diinginkannya dimana saja dan kapan saja selama 24 jam.

Fasilitas *Internet Banking* ini sudah banyak diterapkan oleh bank- bank di Indonesia, misalnya BCA, BII, Bank Niaga, Lippobank, dan Bank Mandiri. Kelima bank tersebut, melalui situs resminya, telah mengaktifkan fasilitas *Internet Banking* bagi nasabah. Keuntungan yang ditawarkan dari fasilitas *Internet Banking* ini antara lain mengenai kemudahan, kepraktisan, kenyamanan, kelengkapan fitur, dan keamanan.

Kemudahan tersebut antara lain, nasabah bisa melakukan berbagai transaksi tanpa perlu mendatangi langsung bank dan mengantri bersama nasabah- nasabah yang lain; nasabah bisa melakukan transaksi kapan saja, baik ketika jam kerja kantor bank maupun di luar jam kerja kantor bank. Kepraktisannya adalah bahwa nasabah hanya tinggal mengakses ke alamat situs *Internet Banking* dan memasukkan perintah- perintah transaksi yang diinginkan. Kemudahan dan kepraktisan tersebut tentunya memberikan kenyamanan pada nasabah dalam bertransaksi. Selain itu kenyamanan dapat dirasakan karena proses bertransaksi melalui *Internet Banking* relatif lebih cepat.

Kelengkapan fitur juga ditawarkan oleh fasilitas *Internet Banking* karena transaksi yang bisa dilakukan dengan fasilitas *Internet Banking* ini beragam, hampir semua transaksi yang sudah umum dilakukan dengan *face to face* bisa pula dilakukan dengan *Internet Banking*. Akan tetapi macam- macam transaksi perbankan yang dapat dilakukan dengan fasilitas *Internet Banking* ini berbeda-

beda pada tiap- tiap bank, tergantung pada tingkat kecanggihan teknologi komputer dan sumber daya manusia yang dimiliki. Makin canggih teknologi komputer serta makin berkualitas sumber daya manusia yang dimiliki oleh bank, makin bertambah banyak jenis transaksi yang bisa dilakukan dengan fasilitas *Internet Banking* pada bank tersebut. Contoh transaksi perbankan yang disediakan oleh Bank Niaga dengan fasilitas *Internet Banking*-nya yang disebut dengan Niaga Global Access antara lain¹:

- Informasi Saldo
- Informasi Transaksi
- Transaksi Overbooking
- Transaksi Pembayaran (telkom, kartu kredit Bank Niaga, kartu kredit Citibank, kartu kredit GE, sumber kredit, *Citibank Ready Cash*, Telkomsel- *prepaid*, *kidsport*, STIE Perbanas, Bina Sarana Informatika, Kabelvision, Indosatnet)
- Pembelian *voucher* Simpati Telkomsel
- Pembukaan Rekening (tabungan, giro, deposito, kartu kredit)
- Pemesanan buku cek/ BG
- Perubahan alamat rekening atau *E-mail*
- Informasi aktifitas nasabah di *Internet Banking*
- Informasi Biaya
- Informasi Kurs

¹ Niaga Global @ccess Features.
<http://www.bankniaga.com/ProdServ/prodserv.asp?id=PRN0000038>

- Informasi Suku Bunga
- Simulasi Deposito
- Simulasi Pinjaman
- Kirim/ baca Pesan Bank Niaga
- Perubahan *Password*

Issue yang paling utama harus diperhatikan dalam *Internet Banking* adalah faktor keamanan. Setiap bank menjamin bahwa transaksi yang dilakukan melalui *Internet Banking* adalah aman. Keamanan komputer (*computer security*) melingkupi 4 (empat) aspek, yaitu *privacy*, *integrity*, *authentication* dan *availability*². *Privacy* berhubungan dengan kerahasiaan informasi misalnya mengenai data pribadi, keuangan dan transaksi nasabah pengguna yang menjadi kewajiban bank untuk merahasiakannya, sesuai pasal 40 ayat 1 Undang- undang nomor 10 tahun 1998 tentang Perubahan Undang- undang nomor 7 tahun 1992 tentang Perbankan. Harus ada jaminan bahwa informasi tersebut tidak dapat dibuka atau tidak dapat diketahui orang lain yang tidak berhak.

Aspek *integrity* menekankan bahwa informasi yang disimpan tidak boleh diubah tanpa izin dari pemilik informasi. Aspek ini dapat dilindungi dengan *digital signature* (tanda tangan digital) serta enkripsi yaitu metode untuk menyamarkan atau menyembunyikan suatu dokumen yang berbentuk teks (*plaintext*) menjadi kode- kode (*chiphertext*) sehingga isi dokumen tidak dapat dimengerti oleh orang lain.

² Agus Raharjo, *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Cet.I, Citra Aditya Bakti, Bandung, 2002 h. 121.

Aspek *authentication* berhubungan dengan metode untuk menyatakan keaslian informasi, atau bahwa orang yang mengakses atau memberikan data adalah orang yang benar- benar dimaksudkan. Secara umum perlindungan aspek *authentication* dengan menggunakan *digital certificates* atau sertifikat digital, yaitu suatu dokumen pernyataan kebenaran yang berisi informasi yang juga disertai kode tertentu (berupa kunci publik) seseorang dan tanda tangan digital orang tersebut.

Aspek terakhir adalah aspek *availability* yang menjamin pengguna yang sah agar bisa mengakses informasi dan sumber miliknya sendiri. Jadi tujuannya adalah untuk memastikan bahwa orang- orang yang memang berhak tidak ditolak untuk mengakses informasi yang memang menjadi haknya.

Masing- masing bank memiliki prosedur sendiri- sendiri dalam rangka menjaga keamanan fasilitas *Internet Banking* yang mereka terapkan. Misalnya Bank Mandiri³ menerapkan beberapa program yaitu:

1. Program *International Internet Standard Security SSL (Secure Socket layer)* dengan metode 128 bit enkripsi. SSL pada dasarnya adalah merupakan suatu mekanisme yang melindungi koneksi dari usaha penyadapan. Protokol SSL ini akan mengacak data yang dikirimkan menjadi kode- kode rahasia dengan menggunakan 128 bit enkripsi yang artinya terdapat 2 pangkat 128 kombinasi angka kunci, tetapi hanya ada 1 (satu) kombinasi yang dapat membuka kode- kode tersebut;

³ http://www.bankmandiri.co.id/article/254000322846.asp?article_id=245000322846

2. *Security Pluggins* yang dipasang secara otomatis saat nasabah mengakses *Internet Banking* pertama kali. *User ID* dan PIN (*Personal Identification Number*) yang merupakan kode rahasia dan kewenangan penggunaan yang diberikan kepada nasabah. Apabila nasabah salah memasukkan *user ID* dan PIN sebanyak 3 kali maka akses akan diblokir;
3. *Automatic Logout*, yaitu bahwa sistem akan secara otomatis mengakhiri akses apabila tidak terdapat aktifitas selama beberapa waktu tertentu; atau
4. *Firewall*, yaitu suatu sistem yang berfungsi untuk membatasi akses bagi pengguna yang tidak bertanggung jawab dan mencegah keluar masuknya aliran paket yang tidak memenuhi kriteria keamanan yang ditetapkan pemiliknya. *Firewall* merupakan suatu kombinasi dari *software* dan *hardware* yang dirancang untuk memeriksa aliran trafik jaringan dan permintaan servis. *Firewall* yang sederhana mungkin terdiri dari *filtering router*, yang dikonfigurasi untuk menolak paket-paket dengan tujuan *port* yang tidak diizinkan atau datang dari alamat yang tidak mempunyai otorisasi. *Firewall* yang lebih canggih mungkin mencakup *bastion host*, yaitu mekanisme *proxy* yang berjalan untuk servis- servis yang disediakan. Mekanisme ini membutuhkan

otentikasi *user*, memeriksanya, kemudian melakukan *relay* terhadap servis yang diminta kepada *host* yang menyediakan servis⁴.

Internet Banking ini merupakan penerapan dari suatu sistem informasi yang sudah dirancang memiliki perangkat pengamanan yang baik, namun dalam operasi masalah ini harus selalu dimonitor karena resiko, ancaman, dan kelemahan setiap saat akan mengancam dan menyerang apabila pengelola sistem atau administrator lengah. Menjaga kemutakhiran keamanan sistem informasi ini penting karena beberapa hal, yaitu:⁵

1. Telah ditemukan lubang keamanan (*security hole*) yang baru. Perangkat lunak dan perangkat keras biasanya sangat kompleks, sehingga tidak mungkin untuk diuji 100% (seratus persen), kadang-kadang ada lubang keamanan yang ditimbulkan oleh kecerobohan implementasi. Makin kompleks dan saling terhubungnya antar bagian dalam sistem, menjadikan sistem semakin sulit untuk dijamin keamanannya. Lubang keamanan tersebut juga dapat dibuat atau ditembus oleh para kriminal (dikenal dengan istilah *cracker*) dengan keahlian yang mereka miliki.
2. Kesalahan konfigurasi, yaitu kesalahan yang dilakukan ketika membangun bentuk program-program. Hal ini dapat terjadi karena lalai atau alpa. Konfigurasi dari sebuah sistem yang kurang benar dapat menimbulkan lubang keamanan. Misalnya berkas untuk menyimpan *password* yang seharusnya tidak dapat diubah ternyata tidak sengaja

⁴ Onno W. Purbo dan Aang Arif Wahyudi, *Mengenal E-Commerce*, cet. 1, Elex Media Computindo, Jakarta, 2001, h. 90

⁵ Agus Raharjo, *op cit*, h. 124.

dipasang dengan program *writable*. Hal ini menjadi suatu lubang keamanan karena otomatis *password* yang tersimpan bisa dengan mudah diubah oleh siapa saja yang memasuki berkas penyimpanan *password* tersebut.

3. Penambahan perangkat baru (*hardware* dan/atau *software*). Hal ini menyebabkan menurunnya tingkat keamanan atau berubahnya metode untuk mengoperasikan sistem sehingga operator atau administrator sistem harus belajar lagi.

Selain itu, program-program yang ditawarkan oleh bank juga bukan tidak memiliki kelemahan. Program *Secure Socket Layer* (SSL), misalnya, kelemahannya adalah bahwa sistem ini tidak melindungi pengguna dari kemungkinan salah masuk ke *host* yang berbahaya, ataupun tidak melindungi apakah suatu kode yang di-*download* dari suatu situs bisa dipercaya, atau apakah suatu situs itu sendiri bisa dipercaya. Pada model ini pengguna harus dapat memastikan sendiri apakah server yang diajak berkomunikasi benar-benar merupakan server yang ingin dituju.

Risiko lainnya adalah adanya beberapa program yang biasa digunakan untuk menembus suatu sistem, misalnya⁶:

1. *Password cracker*, yaitu sejenis program otomatis yang digunakan untuk memecahkan *password* suatu sistem. Program pemecah password ini akan mengkombinasikan kata-kata dalam daftar hingga mendapatkan kombinasi yang sesuai. Ada juga

⁶ *Ibid*, h. 168.

program pemecah password yang dapat melakukan seluruh karakter kombinasi yang mungkin, baik huruf, angka, maupun karakter yang lain. Metode ini dinamakan *brute forcing cracking*. Beberapa jenis *password cracker* yang terkenal adalah: *crackerjack*, *pacecrack*, *Qrack*, *John the ripper*, serta *viper*.

2. *Trojan*, yaitu program yang mempunyai fungsi yang sepintas terlihat bagus, menarik dan berguna yang menyebabkan orang ingin men-*download* dan menjalankannya, padahal program ini selalu melakukan sesuatu yang tidak disangka oleh pengguna misalnya mencuri berkas *password* atau menyalin berkas. Bahaya dari program *trojan* adalah bahwa yang menjalankan program ini akan mempunyai *user level* yang sama dengan lingkungan yang mengaktifkannya (*administrator system*) sehingga *trojan* bisa melakukan apa saja yang dilakukan oleh *administrator system*.
3. *Decoy*, yaitu suatu program yang dibuat menyerupai program tampilan *login* suatu sistem. Program ini menipu pemakai untuk memasukkan nama dan *password*-nya ke dalam layar *login* tersebut, dan *decoy* akan menyimpan kombinasi tersebut ke dalam sebuah berkas. Kemudian *decoy* akan menampilkan pesan kesalahan yang memaksa pemakai me-*restart* komputernya atau keluar dan mengulangi *login*. Pada saat pemakai mengulang *login*, *decoy* telah mengembalikan pemakai pada halaman *login* yang sebenarnya.

Risiko terutama terjadi apabila mengakses fasilitas *Internet Banking* dari fasilitas milik publik misalnya warung internet (warnet). Umumnya komputer di tempat umum rentan terhadap virus dan program sederhana yang ter-*download*. Bukan mustahil program tersebut sengaja dibuat untuk membaca apapun yang diketikkan (termasuk *user ID*, *password* maupun PIN), untuk kemudian dikirimkan kepada sang pembuat program dan digunakan untuk mengambil manfaat.

Beberapa kelemahan *Internet Banking* di atas menunjukkan bahwa *Internet Banking* tidak selamanya benar-benar aman, bahkan seharusnya kita membiasakan diri dengan pikiran bahwa dunia internet, tidak terkecuali dengan fasilitas *Internet Banking* itu tidak aman. Segala bentuk pengamanan yang dilakukan tidak bisa memberikan keamanan yang mutlak dan dilakukan hanya untuk meminimalisasi terjadinya kejahatan. Sebagai contoh, di Indonesia sudah pernah terjadi kasus yang mengindikasikan kejahatan di bidang *Internet Banking*, yaitu kasus situs klikbca palsu yang dilakukan oleh Steven Haryanto.⁷ Dalam kasus tersebut Steven Haryanto membuat situs yang mirip dengan klikbca misalnya kilkbca, yang dapat dipakai untuk membobol rekening nasabah BCA. Meskipun akhirnya Steven Haryanto membuat surat permintaan maaf tertulis secara terbuka⁸ dan menyatakan tidak melakukan pembobolan rekening BCA bahkan Steven Haryanto memberikan penjelasan bagaimana cara yang ia lakukan sehingga dapat “membuka” rekening-rekening beberapa nasabah BCA⁹.

⁷ Heru Sutadi, www.kompas.com, 8 juli, 2001

⁸ Steven Haryanto, <http://www.master.web.id/tutorial/wawancara/klikbca.htm>, 6 juni, 2001

⁹ Steven Haryanto, <http://groups.yahoo.com/group/berita-it/message/7791>

Kasus tersebut di atas menunjukkan bahwa sistem keamanan *Internet Banking* masih sangat rentan terhadap “serangan” dari luar. Dengan perkataan lain, kebocoran rahasia bank dapat terjadi akibat penggunaan *Internet Banking*. Padahal, menjadi kewajiban bank sebagaimana diamanatkan dalam pasal 40 ayat 1 Undang- undang nomor 10 tahun 1998 tentang Perubahan Undang- undang nomor 7 tahun 1992 tentang Perbankan untuk merahasiakan informasi mengenai nasabah penyimpan dan simpanannya. Oleh karena itu melalui penelitian ini saya tertarik untuk mengetahui aspek perlindungan hukum terhadap nasabah pengguna *Internet Banking* jika terjadi kebocoran rahasia bank.

Berdasarkan uraian latar belakang permasalahan tersebut di atas, maka dapat dirumuskan permasalahan penelitian sebagai berikut:

1. Faktor- faktor apa saja yang menjadi penyebab kebocoran rahasia bank dalam penggunaan *Internet Banking*?
2. Apa bentuk perlindungan hukum terhadap nasabah pengguna *Internet Banking* apabila terjadi kebocoran rahasia bank?

2. Penjelasan Judul

Judul skripsi ini adalah “PERLINDUNGAN HUKUM TERHADAP NASABAH PENGGUNA INTERNET BANKING ATAS KEBOCORAN RAHASIA BANK”. Adapun penjelasan dari judul tersebut adalah sebagai berikut:

Phillipus Mandiri Hadjon¹⁰ membagi perlindungan hukum menjadi dua, yaitu perlindungan hukum preventif dan perlindungan hukum represif. Perlindungan hukum preventif bertujuan untuk mencegah terjadinya sengketa. Sedangkan perlindungan hukum represif bertujuan untuk menyelesaikan sengketa. Berkait dengan penelitian ini, perlindungan hukum preventif seharusnya tertuang dalam perjanjian penggunaan *Internet Banking* antara nasabah dan bank. Sedangkan perlindungan hukum represif selain tertuang dalam perjanjian penggunaan *Internet Banking* antara nasabah dan bank juga tertuang dalam peraturan perundang-undangan.

Nasabah, menurut Kamus Umum Bahasa Indonesia oleh WJS Poerwodarminta, yaitu orang atau badan yang mempunyai rekening simpanan atau pinjaman pada bank. Namun yang dimaksud dengan nasabah dalam skripsi ini hanyalah nasabah penyimpan sebagaimana dimaksud dalam ketentuan pasal 1 angka 17 Undang-undang nomor 10 tahun 1998 tentang Perubahan Undang-undang nomor 7 tahun 1992 tentang Perbankan, yang uraiannya adalah:

Pasal 1 angka 17:

Nasabah Penyimpan adalah nasabah yang menempatkan dananya di bank dalam bentuk simpanan berdasarkan perjanjian bank dengan nasabah yang bersangkutan.

Internet Banking yaitu fasilitas atau layanan yang diberikan bank kepada nasabah yang memungkinkan nasabah untuk melakukan transaksi perbankan melalui internet, dimana dengan adanya fasilitas ini maka nasabah dapat

¹⁰ Philipus M. Hadjon, *Perlindungan Hukum Bagi Rakyat di Indonesia*. Disertasi Fakultas Hukum Universitas Airlangga, Surabaya, 1987.

melakukan berbagai transaksi perbankan yang diinginkannya dimana saja dan kapan saja selama 24 jam.

Rahasia Bank dalam penelitian ini adalah sebagaimana tercantum dalam pasal 1 angka 28 Undang- undang nomor 10 tahun 1998 tentang Perubahan Undang- undang nomor 7 tahun 1992 tentang Perbankan, yang uraiannya adalah:

Pasal 1 angka 28:

Rahasia Bank adalah segala sesuatu yang berhubungan dengan keterangan mengenai nasabah penyimpan dan simpanannya.

Jadi, secara keseluruhan yang dimaksud dengan “PERLINDUNGAN HUKUM TERHADAP NASABAH PENGGUNA INTERNET BANKING ATAS KEBOCORAN RAHASIA BANK” adalah perlindungan hukum preventif dan represif bagi nasabah pengguna fasilitas *Internet Banking* apabila terjadi kebocoran atas data- data nasabah yang seharusnya dirahasiakan oleh bank.

3. Alasan Pemilihan Judul

Alasan pemilihan judul “PERLINDUNGAN HUKUM TERHADAP NASABAH PENGGUNA INTERNET BANKING ATAS KEBOCORAN RAHASIA BANK” karena saat ini fasilitas *Internet Banking* telah banyak digunakan dalam layanan perbankan dan *issue* mengenai kewajiban bank dalam menjaga rahasia bank pada saat bank menyediakan fasilitas *Internet Banking* sangat menarik untuk dikaji, khususnya menyangkut perlindungan hukum terhadap nasabah yang memanfaatkan fasilitas *Internet Banking* tersebut baik perlindungan hukum secara preventif maupun represif.

4. Tujuan Penelitian

Tujuan utama dari penelitian skripsi ini adalah untuk mengetahui bentuk-bentuk perlindungan hukum terhadap nasabah pengguna *Internet Banking* apabila terjadi kebocoran rahasia bank. Sedangkan tujuan khususnya adalah untuk mengetahui faktor-faktor yang menjadi penyebab kebocoran rahasia bank akibat penggunaan *Internet Banking* dan untuk mengetahui bentuk perlindungan hukum preventif dan represif terhadap nasabah pengguna *Internet Banking* apabila terjadi kebocoran rahasia bank

5. Metode Penelitian

a. Pendekatan Masalah.

Penelitian ini merupakan penelitian hukum normatif. Pendekatan masalah yang digunakan adalah *Statute Approach*, *Contractual Approach* dan *Conceptual Approach*. Artinya, jawab atas permasalahan penelitian yang diajukan akan didasarkan pada peraturan perundang-undangan, perjanjian antara nasabah pengguna *Internet Banking* dan bank, dan konsep hukum yang terdapat dalam keduanya.

b. Bahan Hukum

Bahan hukum yang digunakan dalam penelitian ini terdiri atas dua jenis. Pertama, bahan hukum primer yang berupa norma yang terdapat dalam peraturan perundang-undangan dan perjanjian yang mengatur tentang perlindungan hukum terhadap nasabah pengguna *Internet Banking* jika terjadi kebocoran rahasia bank. Di antaranya adalah Undang-undang nomor 10 tahun

1998 tentang Perubahan Undang- undang nomor 7 tahun 1992 tentang Perbankan, SK Direksi Bank Indonesia nomor 27/164/ Kep/ Dir tanggal 31 Maret 1995 tentang Penggunaan Sistem Informasi oleh Bank, SE Direksi Bank Indonesia nomor 27/9/ UPPB tanggal 31 Maret 1995 tentang Penggunaan Teknologi Sistem Informasi oleh Bank, Ketentuan penggunaan *Internet Banking* dari Bank Mandiri.

Kedua, bahan hukum sekunder yaitu pendapat sarjana yang berkaitan dengan pembahasan permasalahan yang ada dalam buku- buku, surat kabar, internet maupun karya- karya lain yang terkait dengan penelitian ini.

c. Prosedur Pengumpulan dan Pengolahan Bahan Hukum

Kegiatan pengumpulan bahan hukum primer yang berupa peraturan perundang- undangan dilakukan dengan cara studi dokumen, sedangkan yang berupa perjanjian dikumpulkan dengan studi lapangan, yaitu mendatangi bank untuk mendapatkan formulir aplikasi *Internet Banking*. Untuk pengumpulan bahan hukum sekunder dilakukan dengan studi kepustakaan dan internet.

d. Analisis Bahan Hukum

Analisis yang digunakan dalam penelitian ini adalah analisis konsep hukum dengan menggunakan metode interpretasi, yaitu dengan menginterpretasikan isi dari norma- norma hukum yang terdapat dalam data primer dengan bantuan data sekunder untuk menemukan jawab dari permasalahan penelitian yang diajukan.

6. Pertanggungjawaban Sistematika

Skripsi ini dibagi menjadi beberapa bab dan masing- masing bab dibagi lagi menjadi beberapa sub bab sesuai dengan pokok bahasan. Masing- masing bab memuat hal- hal yang berbeda namun masih saling terkait antara satu dengan yang lain.

Bab I merupakan pendahuluan, terdiri dari beberapa sub bab yaitu permasalahan: latar belakang dan rumusannya; penjelasan judul; alasan pemilihan judul; tujuan penelitian; metode penelitian; dan yang terakhir sebagai penutup adalah pertanggungjawaban sistematika. Pada bagian uraian metode penelitian, diuraikan mengenai masalah antara lain: pendekatan masalah, bahan hukum, prosedur pengumpulan dan pengolahan bahan hukum, serta analisis bahan hukum.

Bab II merupakan awal pembahasan yaitu mengenai faktor- faktor penyebab kebocoran rahasia bank dalam penggunaan *Internet Banking*. Bab ini terbagi atas beberapa sub bab yaitu standard pengamanan *Internet Banking* yang kemudian dibagi lagi menjadi dua sub sub bab, yaitu standard pengamanan yang diberikan oleh Bank Indonesia dan standard pengamanan yang diberikan oleh para ahli di bidang teknologi informasi. Sub bab berikutnya mengenai faktor media dan yang terakhir mengenai faktor manusia.

Bab III merupakan lanjutan pembahasan, dan yang dibahas pada bab ini yaitu mengenai perlindungan hukum bagi nasabah pengguna *Internet Banking* apabila terjadi kebocoran rahasia bank. Bab ini juga dibagi menjadi beberapa sub bab, yaitu yang pertama yaitu tentang perlindungan hukum yang diberikan secara preventif. Sub bab berikutnya yaitu mengenai perlindungan hukum secara

represif, yang kemudian dibagi lagi menjadi beberapa sub sub bab yaitu perlindungan hukum apabila kebocoran sebagai akibat kelalaian pihak bank, perlindungan hukum atas kebocoran rahasia bank akibat dari kelalaian dari nasabah, dan yang terakhir adalah mengenai perlindungan hukum atas kebocoran rahasia bank akibat pihak ketiga

Bab IV merupakan penutup dan pembahasan tambahan terakhir dari penulisan ini, yang berisi kesimpulan dan saran- saran. Bagian kesimpulan merupakan suatu jawaban singkat terhadap permasalahan yang telah dirumuskan di awal penelitian skripsi. Sedangkan bagian saran merupakan sumbangan pemikiran yang diharapkan dapat menjadi masukan bagi pihak- pihak yang terkait.

BAB II

FAKTOR-FAKTOR PENYEBAB KEBOCORAN RAHASIA BANK AKIBAT PENGUNAAN INTERNET BANKING

Cipta Karya
(031) 5041023

BAB II

FAKTOR- FAKTOR PENYEBAB KEBOCORAN RAHASIA BANK DALAM PENGGUNAAN INTERNET BANKING

1. Standard Pengamanan Internet Banking

Pihak bank tidak boleh menutup mata bahwa fasilitas *internet* sangat rentan terhadap “serangan- serangan” dari luar yang bisa mengakibatkan kebocoran rahasia nasabah. Oleh karena itu pihak bank harus bersifat antisipatif terhadap kemungkinan- kemungkinan kebocoran tersebut, yaitu antara lain dengan mempersiapkan pengamanan sistem baik yang bersifat teknis maupun non teknis.

Yang dimaksud dengan standard pengamanan di sini adalah suatu prosedur baku yang minimal harus dilakukan oleh bank yang menyediakan fasilitas layanan *Internet Banking*. Standard pengamanan ini bisa digunakan untuk mengukur apakah bank lalai dalam melakukan pengamanan, dan menjadi salah satu alat untuk menentukan apakah bank bertanggung gugat saat terjadi kebocoran rahasia bank. Apabila bank telah menerapkan pengamanan sesuai standard maka apabila terjadi kebocoran rahasia bank kemungkinan kelalaian tidak dilakukan oleh pihak bank melainkan pihak lain yang terkait dengan fasilitas *Internet Banking* ini, misalnya nasabah.

Standard pengamanan ini diberikan oleh dua pihak yang berkepentingan dalam hal *Internet Banking* yakni Bank Indonesia dan para ahli dalam dunia Teknologi Informasi (TI). Bank Indonesia memberikan standard pengamanan dalam sistem pengamanan fasilitas *Internet Banking* adalah dalam rangka

menjalankan tugasnya untuk mengatur dan mengawasi bank yang sesuai dengan pasal 8 huruf c juncto pasal 25 ayat 1 Undang- undang nomor 23 tahun 1999 tentang Bank Indonesia. Uraian pasal- pasal tersebut adalah seperti tersebut di bawah ini:

Pasal 8 huruf c :

... Bank Indonesia mempunyai tugas sebagai berikut:

c. mengatur dan mengawasi Bank

Pasal 25 ayat 1:

Dalam rangka melaksanakan tugas mengatur Bank, Bank Indonesia berwenang menetapkan ketentuan- ketentuan perbankan yang memuat prinsip kehati- hatian.

Sedangkan para ahli dalam dunia Teknologi Informasi (TI) memberikan suatu standard pengamanan dalam hal teknologinya sendiri. Hal ini bisa terjadi karena fasilitas *Internet Banking* bersinggungan secara langsung dengan dunia Teknologi Informasi (TI) khususnya internet. Mungkin para ahli tersebut memang tidak secara khusus memberikan standard bagi dunia *Internet Banking* akan tetapi dunia internet secara global akan tetapi standard tersebut dapat diterapkan dalam dunia *Internet Banking*.

1.1. Standard Pengamanan Oleh Bank Indonesia

Standard pengamanan sistem yang diberikan oleh Bank Indonesia tercantum dalam Surat Edaran Direksi Bank Indonesia nomor 27/9/UPPB tanggal 31 Maret 1995 tentang Penggunaan Teknologi Sistem Informasi oleh Bank. Surat Edaran ini memang tidak khusus mengatur mengenai penggunaan *Internet Banking* oleh bank, akan tetapi secara umum tentang semua fasilitas yang menggunakan teknologi informasi misalnya *Automatic Teller Machine* (ATM), *Electronic Fund*

Transfer (EFT) dan *Home Banking Service*. Bahkan dalam Surat Edaran ini tidak menyebut *Internet Banking* secara spesifik, namun dalam praktek, acuan yang paling sering digunakan adalah Surat Edaran ini.

Bank Indonesia dalam Surat Edaran tersebut menyebutkan bahwa dalam rangka penyediaan fasilitas Teknologi Sistem Informasi (TSI), manajemen bank harus memperhatikan pengendalian secara manajerial (Pengendalian Manajer), pengendalian secara umum terhadap sistem dan aplikasi Teknologi Sistem Informasi (TSI), serta kontrol terhadap penggunaan teknologi tersebut. Masing-masing tahapan tersebut perlu dilakukan karena setiap aplikasi Teknologi Sistem Informasi (TSI) harus dilakukan secara detail mulai dari perencanaan sampai pengawasan.

Pengendalian Manajer meliputi aspek perencanaan; kebijaksanaan, standard dan prosedur; pengorganisasian serta fungsi audit intern Teknologi Sistem Informasi (TSI). Dalam hal perencanaan harus diperhatikan mengenai rencana pengembangan, rencana strategis sampai rencana tahunan bank. Juga harus memperhatikan aspek biaya serta manfaat tiap- tiap satuan kerjanya. Kebijaksanaan dibuat dalam mengatur hubungan antar satuan kerja dalam bank maupun bank dengan nasabah pengguna. Standard dalam diri bank yang meliputi segala detail aspek dalam Teknologi Sistem Informasi (TSI). Prosedur juga dibuat untuk mengatur tugas masing- masing satuan kerja. Pengorganisasian dilakukan untuk meningkatkan efektifitas dan efisiensi pemanfaatan sumber daya manusia dan memudahkan penilaian terhadap kinerja masing- masing satuan kerja Sistem

Teknologi Informasi (TSI). Untuk menunjang aspek- aspek pengendalian manajemen ini dibentuk suatu badan audit intern bank.

Pengendalian umum meliputi aspek- aspek yaitu (a) pengadaan, pengembangan, dan pemeliharaan sistem dan aplikasi Teknologi Sistem Informasi (TSI), bank juga harus mampu mengembangkan suatu metode yang mendukung pencapaian tujuan bank dengan adanya kontrol dari sisi ini; (b) pengoperasian Teknologi Sistem Informasi (TSI), harus ada kepastia mengenai keberadaan lingkungan data yang terkontrol dan dapat dipertanggungjawabkan; (c) *disaster and recovery plan* yaitu suatu perencanaan back up yang memadai baik atas perangkat keras, lunak maupun informasi yang dimiliki dalam rangka menghadapi bencana yang tidak terduga yang dapat mengakibatkan terganggunya operasional bank; (d) kontrol aplikasi Teknologi Sistem Informasi (TSI), dilakukan untuk menjamin integritas data.

Sedangkan kontrol terhadap penggunaan teknologi berarti bahwa dalam memanfaatkan Teknologi Sistem Informasi (TSI), bank harus yakin bahwa telah tersedia suatu sistem kontrol intern yang memadai serta tetap menjaga kerahasiaan bank. Sebelum mengaplikasikan fasilitas *Internet Banking* yang rumit dan kompleks maka manajemen bank harus melakukan analisis resiko bersama- sama dengan satuan kerja yang terkait.

1.2. Standard Pengamanan dari para Ahli Teknologi Informasi

Internet Banking sangat erat kaitannya dengan Teknologi Informasi sehingga tidak terasa aneh apabila ada beberapa ahli dalam bidang Teknologi

Informasi yang memberikan standard pengamanan layanan *Internet Banking*, baik ahli dari luar negeri maupun dari dalam negeri. Para ahli ini terutama memberikan standard dari sisi teknis, namun mereka juga memberikan standard operasi dari sisi non teknis.

Pada tahun 1975, Jerome Saltzer dan MD. Schroeder mempublikasikan suatu prinsip disain sistem sekuriti, yaitu¹¹:

1. *Least priviledge*

Setiap pengguna atau proses, harus hanya memiliki hak yang memang benar- benar dibutuhkan. Hal ini akan mencegah kerusakan yang dapat ditimbulkan oleh penyerang. Hak akses atau memasuki sistem harus secara ekspilisit diminta, dan hal ini lebih baik dilakukan daripada diberikan secara *default*.

2. *Economy of mechanism*

Disain sistem sekuriti yang digunakan oleh bank harus dibuat sesederhana mungkin sehingga memudahkan nasabah dalam melakukan verikasi serta dalam mengimplementasikan sistem. Bank juga harus memperhatikan cara- cara verifikasi atas sistem pembangun yang digunakan. Pada beberapa standard sekuriti untuk aplikasi perbankan , keberadaan *source code* menjadi syarat dalam verifikasi.

¹¹ I Made Wiryana dan Tedi Heriyanto. *Resiko Internet Banking Telah Tampak*, www.tedih.com/papers/i-banking.html, 2001

3. *Complete mediation*

Setiap akses atau proses masuk harus diuji untuk otorisasi yang tepat.

4. *Open design*

Disain sistem sekuriti harus dibuat bersifat terbuka, artinya apabila sistem memiliki *source code* maka kode tersebut harus dibuka. Langkah ini dimaksudkan untuk meminimalisasi kemungkinan adanya celah keamanan (*backdoor*) dalam sistem.

5. *Separation of privilege*

Sistem harus membuat suatu pemisahan- pemisahan atau kategorisasi pengguna sehingga pengguna hanya akan dapat memasuki sistem yang sesuai dengan kepentingan mereka. Selain itu, akses ke dalam *resource system* harus dibuat dengan persyaratan yang berlapis (lebih dari satu persyaratan agar mendapatkan akses ke dalam sistem).

6. *Least common mechanism*

Sistem harus memisahkan pengguna sistem yang satu dengan yang lain.

7. *Psychological acceptability*

Sistem harus dibuat mudah untuk digunakan oleh pengguna sehingga pengguna akan menggunakan dan tidak mengabaikan sistem, karena umumnya pengguna malas menggunakan sistem

yang harus mereka pelajari dengan rumit terlebih dahulu karena alasan efektifitas waktu.

Pada tahun 2000 ahli Teknologi Informasi Cybenko dan Jiang mempublikasikan 6 langkah proses proteksi infrastruktur informasi yang bisa diterapkan oleh bank penyedia fasilitas *Internet Banking*. Proses tersebut meliputi¹²:

1. *Intelligence*, dilakukan oleh *Early Warning System* yang terdiri dari :
 - *Incident report analysis*
 - *Human intelligence gathering*
 - *Automated monitoring web and newsgroup*
2. *Threat assesment*, dilakukan dengan simulasi, *cost-benefit analysis* terhadap *threat*.
 - *Infrastructure epidemiology*
 - *Discrete Event simulation*
 - *Industrial and commercial task forces*
 - *Vulnerability analysis*
3. *Interdiction*, dilakukan dengan beragam *toosl* dan *protocol*, *virus scanner*,

¹² *Ibid*

dan lain-lain :

- *Vulnerability detection and repair*
- *Law enforcement alerts and training*
- *Network and protocol design*

4. *Detection*, dengan teknik *data mining*

- *Automated incident report correlation*
- *Distributed intrusion detection*
- *Real time analysis of gigabit networks*

5. *Response*, dengan teknik *forensics, mitigation*

- *Upstream packet tracing*
- *Secure terabyte packet vaults*
- *Out of band networking*
- *Distributed sensing*

6. *Recovery*, dengan *auditing*. Seringkali sekuriti secara teknis digital menjadi segala-galanya dan melupakan audit. Untuk informasi sensitif (misal *log file*, *password file* dan sebagainya), diterapkan mekanisme *two-person rule* yaitu harus minimum 2 orang yang terpisah dan berkualifikasi dapat melakukan perubahan.

- *Incident analysis*
- *Admissible evidence*
- *Non repudiation*
- *Third party privacy*

Sedangkan para ahli Teknologi Informasi dari dalam negeri pada tahun 2001 memberikan panduan pengamanan minimum antara lain¹³, yang pertama yaitu jika sistem menyimpan informasi finansial rahasia, maka harus didisain agar informasi rahasia tersebut dapat digunakan tetapi tanpa dapat dilihat oleh pengguna. Informasi ini harus tersimpan dalam subsistem yang “*trusted*” yang menjamin bahwa informasi tersebut tak bisa terbaca walaupun *host* telah dikuasai oleh pihak lain.

Selanjutnya mengenai subsistem yang menangani database transaksi, *record* akuntansi, audit informasi harus diimplementasikan dalam sistem “*trusted*” yang akan melindungi informasi ini walau *host* dikuasai oleh orang lain.

Yang terakhir adalah apabila seluruh transaksi dan operasi memerlukan pengikatan (*binding*) yang kuat antara *user*, *customer*, identitas proses dan operasi yang dilakukan, maka semua operasi ini harus di-log secara aman untuk kebutuhan audit.

Berbagai standard pengamanan yang diberikan para ahli Teknologi Informasi tersebut adalah langkah- langkah pengamanan dari sisi teknis, dan

¹³ *Ibid*

selain dari sisi teknis, bank harus juga memperhatikan langkah- langkah pengamanan secara non teknis. Pengamanan secara non teknis dilakukan antara lain dengan cara¹⁴, yaitu: penyampaian informasi tentang ancaman potesial pada sistem kepada pengguna, pemeliharaan terhadap kepedulian pengguna, serta pemberian panduan sekuriti system.

Penyampaian informasi tentang ancaman potesial pada sistem kepada pengguna dilakukan dengan cara yaitu bank harus memberikan informasi dalam format yang mudah sehingga nasabah akan lebih memperhatikan setiap langkah yang dia ambil. Karena ada kecenderungan nasabah malas untuk meneliti setiap detail langkahnya, cenderung mudah mengetik “yes” dari setiap penawaran. Kesulitan utama pengguna *Internet Banking* di Indonesia terutama adalah pada bahasa, karena masih banyak bank yang menggunakan Bahasa Inggris sedangkan tidak semua pengguna memahami secara baik Bahasa Inggris sehingga seringkali mereka melewati pesan- pesan atau informasi yang diberikan. Hal ini menuntut bank untuk menggunakan Bahasa Indonesia pada menu maupun aplikasi *Internet Banking*.

Pemeliharaan terhadap kepedulian pengguna berarti bahwa pihak bank harus memberi pertanyaan mengenai masalah sekuriti yang diajukan oleh nasabah, baik yang disampaikan secara langsung maupun tidak. Pelayanan informasi secara berkala mengenai *issue- issue* keamanan juga hendaknya diberikan, misalnya menggunakan fasilitas *newsletter*, *press release* ataupun *white paper*. Pihak bank tidak boleh mengabaikan masukan- masukan yang diberikan oleh nasabah, baik

¹⁴ *Ibid*

yang berupa pertanyaan, pengaduan, usulan ataupun informasi. Selain itu bank juga harus memperhatikan informasi yang mereka berikan, bahwa informasi tersebut seharusnya tidak dibuat hanya sekedar menutupi kelemahan dan juga tidak boleh memberi kesan menakut- nakuti nasabah.

Pemberian panduan sekuriti system mengandung pengertian bahwa bank harus bisa “memaksa” pengguna yang mengakses pertama kali untuk membaca petunjuk terlebih dahulu. Artinya bank melakukan langkah preventif dan tidak menunggu terjadi suatu kasus terlebih dahulu untuk memberi penjelasan kepada pengguna. Dokumentasi dan penjelasan yang diberikan bank dalam situs juga harus lengkap dan detail.

2. Faktor Media

Internet Banking pada dasarnya merupakan suatu fitur tambahan yang diberikan oleh pihak bank untuk meningkatkan pelayanan pada nasabahnya. Sehingga secara umum transaksi yang bisa diaplikasikan oleh *Internet Banking* adalah juga transaksi yang biasa digunakan pada cara konvensional. Faktor pembeda antara transaksi konvensional (*face to face*) dengan transaksi dengan *Internet Banking* adalah medianya. Pada transaksi *Internet Banking* menggunakan suatu media baru yakni *internet*.

Perbedaan media ini seringkali menjadi faktor penyebab terjadinya kebocoran rahasia bank. Kebocoran itu bisa disebabkan antara lain apabila pihak bank kurang memperhatikan faktor keamanan dalam sistem *Internet Banking* yang diterapkannya, atau pihak bank merasa seolah- olah telah memilih sistem

pengamanan yang terbaik dan tidak mengantisipasi adanya kemajuan teknologi yang saat ini memang berkembang sangat pesat. Apabila sistem pengaman yang digunakan oleh pihak bank masih kalah canggih atau kalah maju dari sistem perusak yang digunakan oleh pembobol maka tentu saja sistem pengaman yang digunakan itu menjadi tidak ada artinya. Hal ini tentunya akan berakibat fatal karena pembobol akan dengan mudah memasuki sistem dan “membaca” semua data- data yang seharusnya dijaga dan menjadi rahasia bank.

Faktor media yang menyebabkan kebocoran rahasia bank juga mungkin bisa disebabkan oleh program komputer sendiri misalnya dalam istilah teknis teknologi informasi terdapat apa yang disebut dengan *cockoo egg*, yaitu sejenis kelalaian yang murni dilakukan oleh bank karena pihak bank secara tidak sengaja memberikan nomor identifikasi yang sama kepada dua nasabah pengguna *Internet Banking* yang berbeda sehingga salah satu nasabah bisa menarik dana dari rekening nasabah yang lain yang memiliki nomor identifikasi yang sama. Kelalaian bentuk ini memang terlihat sederhana akan tetapi tentu saja bisa berakibat merugikan pihak nasabah pengguna *Internet Banking*.

Hal yang paling fatal dari faktor media adalah apabila pihak bank dalam menjalankan fasilitas *Internet Banking*-nya tidak menerapkan sistem yang sesuai standard. Standard ini dapat dilihat dari dua sisi yakni dari sisi perbankan dan dari sisi teknologi informasi. Dari sisi perbankan artinya bahwa ada suatu standard sistem keamanan tertentu yang telah diterapkan oleh Bank Indonesia untuk bank-bank yang menyediakan fasilitas *Internet Banking* bagi nasabahnya melalui aturan- aturan yang dibuat oleh Bank Indonesia misalnya dalam Surat Edaran

Bank Indonesia. Dari sisi teknologi artinya bahwa terdapat suatu standard sistem keamanan tertentu yang dibuat oleh para pakar dalam bidang teknologi informasi nasional maupun internasional untuk penggunaan teknologi informasi secara umum, termasuk penerapan *Internet Banking* secara khusus.

Kemungkinan terakhir dari faktor media adalah bahwa internet merupakan suatu media yang tergantung pada sistem sehingga apabila suatu bagian dari sistem tidak berfungsi maka secara keseluruhan sistem juga tidak akan bisa berfungsi atau berfungsi tidak maksimal. Ada satu istilah yang disebut *Server Down Internal*, yakni satu kelalaian dari pihak bank yang terjadi karena mati atau padamnya main server pada bank, sehingga nasabah yang akan menggunakan fasilitas tersebut akan mengalami kesulitan melakukan akses ke dalam situs bank. Kelalaian ini tidak murni dilakukan oleh bank akan tetapi lebih banyak merupakan kelalaian dari pihak *Internet Service Provider* (ISP).

3. Faktor Manusia

Kebocoran rahasia bank juga tidak hanya bisa disebabkan oleh faktor media, akan tetapi juga bisa disebabkan oleh faktor manusia. Hal ini berkait juga dengan unsur kebaruan *internet* itu sendiri sehingga seringkali pengguna fasilitas ini masih belum paham belum mengenai cara kerjanya. Operator atau administrator sistem dari bank seringkali harus belajar lagi apabila ada penambahan perangkat yang baru. Hal ini sangat beresiko bagi keamanan sistem itu sendiri.

Namun seringkali kebocoran rahasia bank akibat faktor manusia datang dari pihak nasabah pengguna *Internet Banking*. Hal ini karena pada umumnya nasabah

pengguna *Internet Banking* adalah orang yang awam terhadap teknologi, khususnya teknologi *internet*. Ketidaktahuan nasabah ini seringkali menimbulkan kelalaian- kelalaian yang beresiko menimbulkan kebocoran rahasia bank. Kelalaian yang paling umum terjadi adalah bahwa nasabah melakukan aktifitas *Internet Banking*-nya dengan menggunakan komputer milik publik atau umum misalnya di warung *internet* (warnet). Hal ini disebabkan karena seringkali komputer bisa mengetik ulang secara otomatis apa yang telah diketik oleh pengguna komputer sebelumnya. Jadi misalnya nasabah pengguna *Internet Banking* mengetikkan nomor rekeningnya, setelah itu ada orang lain yang menggunakan komputer yang sama, apabila orang lain tersebut mengetik satu digit angka pertama yang sama dengan nomor rekening nasabah pengguna *Internet Banking* tersebut maka komputer akan menampilkan nomor rekening secara lengkap, sehingga hal ini dapat dimanfaatkan orang tersebut untuk membaca data dalam rekening nasabah pengguna *Internet Banking*. Selain itu, resiko yang bisa terjadi apabila nasabah pengguna *Internet Banking* menggunakan komputer milik publik adalah karena biasanya komputer milik publik sangat rentan terhadap virus dan program sederhana yang ter-*download*. Bukan mustahil program tersebut sengaja dibuat untuk membaca apapun yang diketikkan (termasuk *user ID*, *password* maupun PIN), untuk kemudian dikirimkan kepada sang pembuat program dan digunakan untuk mengambil manfaat.

Kelalaian yang lain, misalnya nasabah pengguna *Internet Banking* memberitahukan *user ID*, *password* atau nomor PIN miliknya kepada orang lain. Hal ini juga sangat fatal karena seharusnya nasabah tidak boleh memberitahukan

user ID, *password* maupun nomor PIN-nya kepada siapapun bahkan kepada petugas bank tempat *account* nasabah tersebut.

Bentuk kelalaian nasabah yang lain yang kelihatannya sederhana tapi dapat berakibat fatal adalah nasabah tidak membaca dengan teliti petunjuk atau informasi yang diberikan oleh bank sehingga nasabah dengan mudah menjawab “yes” terhadap suatu pertanyaan atau permintaan persetujuan yang muncul di layar. Akibat dari kebiasaan ini adalah apabila ternyata nasabah pengguna *Internet Banking* masuk ke dalam situs yang salah. Masuk ke situs yang salah juga merupakan bentuk kelalaian nasabah karena sebelum melakukan aktifitas perbankannya, nasabah harus memastikan bahwa alamat URL (*Universal Resource Locator*) yang dituju telah benar.

Ada satu lagi aspek yang menjadi penyebab kebocoran rahasia bank dari faktor manusia yakni adanya orang ketiga dalam hal ini *hacker* yang dengan sengaja berusaha masuk ke dalam sistem yang menyimpan data- data yang menjadi rahasia bank. Memang tidak semua *hacker* berniat untuk menyalahgunakan informasi yang ia ketahui dari sistem yang ia masuki tapi kadangkala nasabah bisa merasa dirugikan apabila data- data pribadinya diketahui orang lain yang tidak berkepentingan. Terlebih apabila hacker tersebut kemudian menyalahgunakan informasi yang ia dapatkan, hal ini tentu sangat merugikan nasabah pengguna *Internet Banking*.

BAB III

BENTUK PERLINDUNGAN HUKUM BAGI NASABAH PENGGUNA INTERNET BANKING APABILA TERJADI KEBOCORAN RAHASIA BANK

Cipta Karya
0811 3311025

BAB III

BENTUK PERLINDUNGAN HUKUM TERHADAP NASABAH PENGUNA INTERNET BANKING APABILA TERJADI KEBOCORAN RAHASIA BANK

1. Perlindungan Hukum Preventif

Perlindungan hukum preventif penting diberikan pada nasabah untuk mencegah terjadinya sengketa. Perlindungan ini biasanya dituangkan dalam bentuk perjanjian antara kedua belah pihak yang mengatur mengenai hak dan kewajiban masing-masing pihak. Hak dan kewajiban masing-masing pihak ini harus seimbang dalam arti tidak boleh ada pihak yang dirugikan dan masing-masing pihak harus saling menguntungkan satu sama lain.

Beberapa kewajiban nasabah antara lain yaitu¹⁵:

1. Nasabah harus mengisi semua data yang dibutuhkan untuk setiap transaksi secara benar dan lengkap;
2. Nasabah wajib dan bertanggung jawab untuk memastikan ketepatan dan kelengkapan instruksi transaksi;
3. Nasabah wajib tidak meninggalkan terminal dalam keadaan aktif (log-on) dengan kata lain harus melakukan logout setiap kali meninggalkan terminal;
4. Nasabah wajib mengamankan User ID dan PIN;
5. Nasabah wajib untuk segera memberitahukan kepada Bank apabila User ID

¹⁵ Syarat dan Ketentuan Internet Banking BCA,
http://www.klikbca.com/website/indo/consumer_banking/ib_termandcondition.html

dan atau PIN tersebut telah diketahui oleh orang lain.

Beberapa hak nasabah antara lain¹⁶:

1. Nasabah mempunyai kesempatan untuk membatalkan data yang diinput dengan menekan tombol "Batal";
2. Nasabah diberikan kebebasan untuk membuat PIN-nya sendiri pada saat registrasi.

Sedangkan kewajiban pihak bank antara lain yaitu¹⁷:

1. Melakukan konfirmasi terhadap data yang diinput nasabah;
2. Mengirimkan informasi kepada alamat E-Mail yang telah dikonfirmasi kebenarannya oleh nasabah.

Selain itu Bank juga memiliki hak yaitu¹⁸:

1. Bank berhak untuk memberikan User ID dengan kombinasi huruf dan angka tanpa harus mendapatkan persetujuan terlebih dahulu dari nasabah;
2. Bank berhak untuk mendebet biaya administrasi bulanan dan biaya transaksi yang dibebankan atas penggunaan fasilitas *Internet Banking* dan transaksi yang dilakukan melalui *Internet Banking*;
3. Bank berhak atas pertimbangannya sendiri untuk mengubah, menambah atau menarik biaya-biaya yang dibebankan kepada nasabah atas penggunaan fasilitas *Internet Banking*.

Dalam dunia perbankan, kebiasaan yang paling sering dilakukan adalah apabila nasabah ingin mengaktifasi suatu fasilitas tertentu maka nasabah tersebut

¹⁶ *Ibid*

¹⁷ *Ibid*

¹⁸ *Ibid*

harus mengisi formulir aplikasi tertentu pula. Formulir aplikasi tersebut kemudian dapat dianggap menjadi perjanjian antara nasabah dengan bank.

Demikian juga apabila nasabah ingin menggunakan fasilitas *Internet Banking* maka ia harus mengisi formulir aplikasi pendaftaran layanan *Internet Banking* dari bank. Misalnya seperti yang diterapkan oleh Bank Mandiri¹⁹ yang juga telah menyediakan fasilitas *Internet Banking* bagi nasabahnya. Bank Mandiri mewajibkan nasabah untuk mengisi formulir aplikasi pendaftaran layanan *Internet Banking* Mandiri yang ada di kantor cabang Bank Mandiri atau pada *Automatic Teller Machine* (ATM) Bank Mandiri. Dalam formulir aplikasi *Internet Banking* Mandiri terdapat 2 (dua) lembar halaman. Halaman pertama mengenai data-data nasabah, jenis layanan yang diinginkan, serta pernyataan dari nasabah. Sedangkan halaman kedua berisi tentang syarat dan ketentuan penggunaan *Internet Banking*.

Syarat dan ketentuan ini terdiri atas beberapa bagian, yaitu: daftar istilah, syarat pendaftaran *Internet Banking* Mandiri, Ketentuan Penggunaan *Internet Banking* Mandiri, *User ID* dan *PIN Internet Banking* Mandiri, Penghentian Akses Layanan *Internet Banking* Mandiri, *Force Majeure*, dan lain-lain.

Akan tetapi syarat dan ketentuan yang tercantum dalam formulir aplikasi *Internet Banking* Mandiri tersebut belum dapat dikatakan memberikan perlindungan hukum yang memadai bagi nasabah pengguna *Internet Banking*. Ada beberapa klausula yang dirasa justru memberatkan nasabah, terutama yang berkaitan dengan apabila terjadi kebocoran rahasia bank akibat pelaksanaan *Internet Banking*, misalnya klausula yang menyatakan bahwa Bank menerima dan

¹⁹ Bank Mandiri, *Aplikasi Internet Banking dan SMS Banking Mandiri*

menjalankan setiap perintah dari nasabah pengguna sebagai perintah yang sah berdasarkan penggunaan *user ID* dan PIN dan untuk itu Bank tidak mempunyai kewajiban untuk meneliti atau menyelidiki keaslian maupun keabsahan atau kewenangan pengguna *user ID* dan PIN atau menilai maupun membuktikan ketepatan maupun kelengkapan perintah dimaksud, dan oleh karena itu perintah tersebut sah mengikat nasabah pengguna dengan sebagaimana mestinya, kecuali nasabah pengguna dapat membuktikan sebaliknya.

Klausula lain yang memberatkan nasabah adalah segala penyalahgunaan *access ID/ user ID* dan *access PIN/ PIN Internet Banking Mandiri* merupakan tanggung jawab nasabah pengguna. Nasabah pengguna dengan ini membebaskan bank dari segala tuntutan yang mungkin timbul, baik dari pihak lain maupun nasabah pengguna sendiri sebagai akibat penyalahgunaan *access ID/ user ID* dan *access PIN/ PIN Internet Banking Mandiri*.

Klausula *force majeure* juga dirasa memberatkan nasabah bila dilihat dari komposisi kalimatnya yang berbunyi: "Nasabah pengguna akan membebaskan Bank dari segala tuntutan apapun, dalam hal bank tidak dapat melaksanakan perintah dari nasabah pengguna baik sebagian maupun seluruhnya karena kejadian- kejadian atau sebab- sebab di luar kekuasaan atau kemampuan Bank namun tidak terbatas pada segala gangguan virus komputer atau sistem *trojan horses* atau komponen membahayakan yang dapat mengganggu layanan *Internet Banking Mandiri*, *web browser*, atau komputer sistem Bank, nasabah, atau *Internet Service Provider*, karena bencana alam, perang, huru- hara, keadaan peralatan, sistem atau transmisi yang tidak berfungsi, gangguan listrik, gangguan

telekomunikasi, kebijakan pemerintah, serta kejadian- kejadian atau sebab- sebab lain di luar kekuasaan atau kemampuan Bank”.

Berdasarkan perjanjian antara nasabah pengguna *Internet Banking* dan bank²⁰ dapat diketahui bahwa ternyata nasabah belum diberikan perlindungan hukum secara preventif. Walaupun demikian, bukan berarti tidak ada sama sekali perlindungan hukum bagi nasabah, paling tidak terdapat dua klausula dalam perjanjian itu yang memberikan perlindungan hukum bagi nasabah pengguna *Internet Banking*. Pertama, sebagai bukti bahwa transaksi yang diperintahkan nasabah pengguna telah berhasil dilakukan oleh Bank, nasabah pengguna akan mendapatkan bukti transaksi berupa nomor transaksi pada halaman transaksi layanan *Internet Banking* Mandiri dan bukti tersebut akan tersimpan di dalam menu aktivitas transaksi selama 3 (tiga) bulan sejak tanggal transaksi. Kedua, klausula yang memuat pernyataan bahwa dalam hal nasabah pengguna mengetahui atau menduga *user ID* dan PIN telah diketahui oleh orang lain yang tidak berwenang, nasabah pengguna wajib segera melakukan pengamanan dengan melakukan perubahan PIN. Apabila karena suatu sebab nasabah tidak bisa melakukan perubahan PIN maka nasabah pengguna wajib memberitahukan kepada Bank.

2. Perlindungan Hukum Represif

Kebocoran rahasia bank bisa terjadi akibat kelalaian dari pihak bank maupun dari pihak nasabah *Internet Banking* dan juga dari pihak ketiga yang tidak

²⁰ lihat Syarat dan Ketentuan, Aplikasi *Internet Banking* dan *SMS Banking* Mandiri

berwenang dalam hal ini yaitu *cracker*. Terdapat ketentuan yang berbeda mengenai perlindungan hukum bagi nasabah apabila dilihat dari pihak yang melakukan kesalahan sehingga terjadi kebocoran rahasia bank. Hal ini berkait dengan tanggung jawab masing-masing pihak.

2.1. Perlindungan Hukum Atas Kebocoran Rahasia Bank Akibat Kelalaian Bank

Pada dasarnya hubungan hukum antara bank dengan nasabah pengguna *Internet Banking* adalah hubungan kontraktual dan konsensual²¹. Hubungan kontraktual antara bank dengan nasabah pengguna *Internet Banking* dilandaskan pada kontrak campuran, artinya ada lebih dari satu hubungan kontraktual yang mendasarinya, antara lain: kontrak pemberian kuasa (*lastgeving*) dan kontrak untuk melakukan suatu pekerjaan

Kontrak pemberian kuasa (*lastgeving*), seperti yang diatur dalam pasal 1792 BW:

Pemberian Kuasa adalah suatu perjanjian dengan mana seseorang memberikan kekuasaan pada seorang lain, yang menerimanya, untuk atas namanya menyelenggarakan suatu urusan.

Kontrak untuk melakukan suatu pekerjaan, seperti yang diatur dalam pasal 1601 BW:

Selain perjanjian- perjanjian untuk melakukan sementara jasa- jasa, yang diatur oleh ketentuan- ketentuan yang khusus untuk itu dan oleh syarat- syarat yang diperjanjikan, dan jika itu tidak ada, oleh kebiasaan, maka adalah dua macam perjanjian dengan mana pihak yang satu mengikatkan

²¹ Munir Fuady, *Hukum Perbankan Modern*, buku I, Citra Aditya Bakti, Surabaya, 1999, h.102

dirinya untuk melakukan pekerjaan bagi pihak yang lainnya dengan menerima upah; perjanjian perburuhan dan pemborongan pekerjaan.

Sifat perjanjian antara bank dengan nasabah pengguna *Internet Banking* adalah konsensual yang berarti bahwa perjanjian dan perikatan di antara mereka timbul sejak detik tercapainya kesepakatan, atau dengan kata lain, perjanjian itu sudah sah apabila sudah sepakat mengenai hal-hal yang pokok dan tidaklah diperlukan sesuatu formalitas.²²

Dalam perjanjian pengaktifan fasilitas *Internet Banking* antara bank dengan nasabah pengguna *Internet Banking* tercantum bahwa salah satu kewajiban bank yang pada intinya adalah pihak bank menjamin keamanan serta menjaga kerahasiaan data-data nasabah pengguna *Internet Banking* yang menjadi rahasia bank. Jadi apabila terjadi kebocoran rahasia bank karena kelalaian dari pihak bank maka dapat dikatakan bahwa bank telah melakukan wanprestasi.

Nasabah pengguna *Internet Banking* dapat menjadikan alasan wanprestasi tersebut sebagai dasar untuk melakukan tuntutan ganti rugi. Dasar hukum yang digunakan adalah pasal 1243 BW, yang secara lengkap berbunyi sebagai berikut:

Penggantian biaya, rugi dan bunga karena tak dipenuhinya suatu perikatan, barulah mulai diwajibkan, apabila si berutang, setelah dinyatakan lalai memenuhi perikatannya, tetap melalaikannya, atau jika sesuatu yang harus diberikan atau dibuatnya, hanya dapat diberikan atau dibuat dalam tenggang waktu yang telah dilampaukannya.

2.2. Perlindungan Hukum Atas Kebocoran Rahasia Bank Akibat Kelalaian

Nasabah

Pada dasarnya bank bertanggung gugat membayar kerugian yang dialami

²² Subekti, *Hukum Perjanjian*, cet 18, Intermasa, Jakarta, 2001, h.15

oleh nasabah pengguna *Internet Banking* ketika terjadi kebocoran rahasia bank apabila telah dapat dibuktikan bahwa kebocoran tersebut terjadi akibat kesalahan atau kelalaian dari pihak bank. Akan tetapi apabila ternyata kebocoran rahasia bank tersebut terjadi akibat kesalahan maupun kelalaian dari pihak nasabah sendiri maka nasabah tidak mempunyai hak untuk mengklaim atau menggugat untuk mendapatkan ganti rugi kepada pihak bank.

Namun dalam hal ini tidak berarti bank lepas tangan secara penuh atas kebocoran rahasia yang dialami oleh nasabah pengguna *Internet Banking* -nya, dalam hal ini seharusnya nasabah yang mengetahui bahwa telah terjadi kebocoran atas data- data yang dimilikinya yang seyogyanya menjadi tanggung jawab bank untuk menjaga kerahasiaanya, ia harus segera memberitahukan pihak bank. Notifikasi atau pemberitahuan tersebut dimaksudkan agar bank dapat segera melakukan tindakan penutupan akses terhadap data tersebut dan mencegah terjadinya kebocoran yang lebih parah.

Apabila informasi mengenai kebocoran tersebut dengan cepat masuk ke pihak bank maka kemungkinan bagi pihak bank untuk melacak kepada siapa data itu masuk dapat dilakukan. Dengan diketahuinya pihak ketiga yang membaca data- data nasabah pengguna *Internet Banking* maka dapat dicegah tindakan penyalahgunaan data tersebut. Informasi mengenai kebocoran rahasia bank tersebut juga dapat menjadi peringatan bagi pihak bank bahwa ternyata ada pihak ketiga yang tidak berwenang dapat melakukan akses ke dalam sistem yang dikembangkan oleh bank. Hal ini dapat menjadikan peringatan bank untuk melakukan perbaikan- perbaikan dalam sistemnya. Meskipun ternyata kebocoran

tersebut bukan kesalahan dari pihak bank akan tetapi hal itu seharusnya juga diperhatikan oleh bank bahwa nasabah harus mendapat penjelasan mengenai *Internet Banking* dan sistem pengamanannya.

2.3. Perlindungan Hukum Atas Kebocoran Rahasia Bank Akibat Pihak Ketiga

Apabila ternyata kebocoran rahasia bank sebagai akibat dari masuknya pihak ketiga tanpa izin maka pihak nasabah pengguna *Internet Banking* bisa menuntut ganti kerugian pada pihak ketiga dengan menggunakan dasar Perbuatan Melanggar Hukum seperti yang diatur dalam pasal 1365 BW, yang uraiannya adalah sebagai berikut:

Tiap perbuatan melanggar hukum, yang membawa kerugian kepada seorang lain, mewajibkan orang yang karena salahnya menerbitkan kerugian itu, mengganti kerugian tersebut.

Akan tetapi apabila nasabah menggunakan dasar hukum pasal 1365 BW, maka ada 4 syarat yang harus dipenuhi agar bank dapat dikatakan bertanggung gugat, syarat tersebut yaitu²²: perbuatan yang menimbulkan kerugian itu bersifat melanggar hukum (perbuatan melanggar hukum); kerugian itu timbul sebagai akibat perbuatan tersebut (hubungan kausal); pelaku tersebut bersalah (kesalahan); dan norma yang dilanggar mempunyai "*strekking*" untuk mengelakkan timbulnya

²² J.H. Nieuwenhus, diterjemahkan oleh Djasadin Saragih, *Pokok- Pokok Hukum Perikatan*, Surabaya, 1995, h.118

kerugian (relativitas). Bersifat melanggar hukum artinya adalah bahwa perbuatan tersebut bertentangan dengan kewajiban hukum pelaku, melanggar hak orang lain serta bertentangan dengan asas kesusilaan dan kecermatan.

Hubungan kausal di atas dibuktikan dengan 2 (dua) prosedur yaitu *conditio sine quanon* dan hubungan *adequate*. *Conditio sine quanon* artinya harus diselidiki apakah perbuatan pelaku (dalam hubungannya) dengan kerugian dapat dinilai sebagai syarat yang sedemikian sehingga tanpa perbuatan tersebut kerugian tidak akan timbul. Hubungan *adequate* berarti bahwa kerugian itu dapat dianggap sebagai akibat yang wajar diharapkan dari Perbuatan Melanggar Hukum.

Apabila melihat dari sisi tanggung jawab, maka seharusnya nasabah bisa menuntut pihak ketiga yang telah melakukan pembobolan tersebut, namun pada kenyataannya hal tersebut sangat sulit dilakukan karena faktor sulitnya pembuktian. Pembuktian atas pelaku sulit dilakukan karena dunia *internet* bisa diakses dari mana saja dan oleh siapa saja dan hingga saat ini belum ada alat yang bisa digunakan untuk melacak asal pengguna secara tepat.

Oleh karena itu apabila terjadi kebocoran rahasia bank akibat perbuatan pihak ketiga, maka nasabah yang menanggung resikonya sendiri karena nasabah tidak bisa menuntut pihak bank maupun pihak ketiga yang bersangkutan. Jadi, dalam hal ini nasabah, juga bank, harus berhati- hati agar tidak ada kemungkinan bagi pihak ketiga “menerobos” masuk ke dalam sistem dan menyalahgunakan data- data yang tersimpan.

BAB IV

PENUTUP

Cipta Karya
(1991) 5041924

BAB IV

PENUTUP

1. Kesimpulan

Berdasarkan uraian pada bab- bab sebelumnya maka dapat diambil beberapa kesimpulan sebagai berikut:

1. Dalam penerapan *Internet Banking*, bank harus memperhatikan standard yang telah ditetapkan baik dari Bank Indonesia maupun dari para ahli Teknologi Informasi. Kebocoran rahasia bank terjadi oleh karena faktor media yang tergolong baru dan juga faktor manusia yang umumnya awam terhadap teknologi *Internet Banking* itu sendiri.
2. Perlindungan hukum yang diberikan pada nasabah *Internet Banking* dapat berupa perlindungan hukum preventif dan represif. Perlindungan hukum preventif dituangkan dalam perjanjian antara nasabah pengguna *Internet Banking* dengan bank. Sedangkan perlindungan hukum represif diberikan berdasarkan tanggung jawab atas kebocoran rahasia bank tersebut. Apabila kebocoran disebabkan oleh kelalaian dari pihak bank maka nasabah berhak mengajukan tuntutan ganti rugi. Apabila ternyata kebocoran tersebut sebagai akibat dari kelalaian nasabah sendiri maka nasabah tidak dapat mengajukan ganti rugi pada bank. Sedangkan apabila kebocoran tersebut sebagai akibat dari perbuatan pihak ketiga yang tidak berkepentingan, maka nasabah dapat menuntut pihak ketiga untuk bertanggung jawab dan mengganti kerugian.

2. Saran

Berdasarkan kesimpulan- kesimpulan tersebut di atas, maka penulis dapat menyampaikan beberapa saran sebagai berikut:

1. *Internet Banking* telah menjadi suatu fenomena yang banyak berkembang di dunia perbankan Indonesia saat ini. Bank Indonesia sebagai lembaga yang bertugas mengawasi dan mengatur bank harus tanggap dengan kondisi ini. Bank Indonesia sudah saatnya untuk membuat regulasi yang memadai untuk mengatur *Internet Banking* ini. Sampai saat ini pengaturan mengenai *Internet Banking* masih sangat minim dan hanya bersandar pada regulasi mengenai Penggunaan Sistem Informasi oleh Bank. Standard pengamanan fasilitas *Internet Banking* menjadi sangat mutlak diperlukan sebagai tolok ukur penentuan kesalahan bank. Oleh karena itu Bank Indonesia juga dituntut untuk pro aktif menyikapi hal ini, Bank Indonesia harus menyesuaikan standard agar pengamanan yang dilakukan pun makin maksimal. Bank sendiri juga tidak harus menunggu Bank Indonesia untuk meningkatkan standard pengamanan ini. Bank harus lebih pintar dan menyesuaikan mungkin dengan menggunakan standard yang ditetapkan oleh para ahli Teknologi Informasi utamanya dari luar negeri karena saat inipun standard yang diberlakukan di Indonesia masih sangat tertinggal dari luar negeri misalnya negara- negara Eropa seperti Jerman.
2. Perlindungan hukum secara preventif yang seharusnya diberikan oleh bank melalui perjanjian penggunaan *Internet Banking* antara nasabah dan bank sampai saat ini ternyata belum diwujudkan. Bank seharusnya

mencantumkan klausula- klausula yang memperhatikan kepentingan nasabah pengguna Internet Banking akan rahasia bank. Bank seharusnya secara tegas menempatkan nasabah dalam posisi yang aman. Bank juga tidak boleh melepaskan tanggung jawab begitu saja atas kebocoran rahasia bank. Pada perjanjian juga seharusnya dicantumkan kewajiban- kewajiban bank utamanya kewajiban untuk menjaga rahasia bank. Perlindungan represif utamanya apabila kebocoran rahasia bank diakibatkan oleh pihak ketiga sudah saatnya menjadi perhatian pemerintah. Teknologi pelacakan sudah saatnya ditingkatkan agar lebih mudah mengetahui siapa yang bertanggung jawab atas kerugian nasabah. Bank juga harus makin meneliti apakah transaksi dilakukan oleh orang yang berwenang.

DAFTAR BACAAN

- Fuady, Munir, Hukum Perbankan Modern, Buku I, Citra aditya Bakti, Bandung, 1999.
- Hadjon, Philipus M., Perlindungan Hukum Bagi Rakyat di Indonesia, Disertasi Fakultas Hukum Universitas Airlangga, Surabaya, 1987.
- Nieuwenhus,J.H., diterjemahkan Djasadin Saragih, Pokok- Pokok Hukum Perikatan, Surabaya, 1995.
- Poerwodarminta, WJS, Kamus Umum Bahasa Indonesia, Balai Pustaka, Jakarta, 1976.
- Purbo,Onno W., dan Aang Arif Wahyudi, Mengenal E-Commerce, cet.1, Elex Media Computindo, Jakarta, 2001.
- Raharjo, Agus, Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi, Cet.I, Citra Aditya Bakti, Bandung, 2002.
- Subekti, Hukum Perjanjian, cet 18, Intermasa, Jakarta, 2001.
- Subekti dan Tjitrosudibio, Kitab Undang- undang Hukum Perdata, cet 28, Pradnya Paramita, Jakarta, 1996.

Peraturan Perundang-undangan:

- Undang- undang nomor 10 tahun 1998 tentang Perubahan Undang- undang nomor 7 tahun 1992 tentang Perbankan
- Undang- undang nomor 23 tahun 1999 tentang Bank Indonesia
- SK Direksi Bank Indonesia nomor 27/164/ Kep/ Dir tanggal 31 Maret 1995 tentang Penggunaan Sistem Informasi oleh Bank
- SE Direksi Bank Indonesia nomor 27/9/ UPPB tanggal 31 Maret 1995 tentang Penggunaan Teknologi Sistem Informasi oleh Bank

Internet:

<http://www.bankniaga.com/ProdServ/prodserv.asp?id=PRN0000038>

http://www.bankmandiri.co.id/article/254000322846.asp?article_id=245000322846

<http://groups.yahoo.com/group/berita-it/message/7791>

<http://www.master.web.id/tutorial/wawancara/klikbca.htm>

www.kompas.com

www.tedi-h.com/papers/i-banking.html

LAMPIRAN

Cipta Karya
Jurnal Desain



APLIKASI INTERNET BANKING DAN SMS BANKING
Application for Internet Banking and SMS Banking

CABANG
Branch

TANGGAL
Date

HARAP DITULIS DENGAN HURUF CETAK / Fill in with Block Letter

NAMA LENGKAP
Full Name : _____

NAMA GADIS IBU KANDUNG
Mother's Maiden Name : _____

ALAMAT E-MAIL
E-mail Address : _____

NOMOR TELEPON SELULAR
Cellular Phone Number : _____

ALAMAT SURAT
Mailing Address : _____

Nomor Telepon
Phone Number : _____

Nomor Kartu ATM
ATM Card Number : _____

Kode pos
Postal code : _____

Rumah Kantor
Home Office : _____

Faks
Fax : _____

☐ SMS BANKING ☐ INTERNET BANKING

☐ DAFTAR REKENING SENDIRI
My own account list

No.	Tambah	Kode Cabang	Nomor Rekening
1.	☐	_____	_____
2.	☐	_____	_____
3.	☐	_____	_____
4.	☐	_____	_____
5.	☐	_____	_____
6.	☐	_____	_____
7.	☐	_____	_____
8.	☐	_____	_____

☐ DAFTAR REKENING TUJUAN TRANSFER (KHUSUS SMS BANKING)
Transfer destination account list (SMS Banking service only)

No.	Tambah	Kode Cabang	Nomor Rekening	Nama
1.	☐	_____	_____	_____
2.	☐	_____	_____	_____
3.	☐	_____	_____	_____
4.	☐	_____	_____	_____
5.	☐	_____	_____	_____
6.	☐	_____	_____	_____
7.	☐	_____	_____	_____
8.	☐	_____	_____	_____

PEMBERITAHUAN BANK MELALUI SMS BILA
Bank's notification over sms if

☐ DEPOSITO JATUH TEMPO
Time deposit is mature No. _____ Hari sebelumnya
Days before *)

☐ PENOLAKAN CEK/BG ATAS REKENING SENDIRI
My own check / BG is bounced No. _____

☐ PENGKREDITAN LEBIH DARI
Credited account more than Rp. _____ 1 2 3 4 5 6 7 8 (Harap dilingkari)

☐ PENDEBITAN LEBIH DARI
Debited account more than Rp. _____ 1 2 3 4 5 6 7 8 (Harap dilingkari)

☐ SALDO KURANG DARI
Account balance less than Rp. _____ 1 2 3 4 5 6 7 8 (Harap dilingkari)

☐ BERSEDIA MENERIMA PESAN PROMOSI DARI BANK MELALUI E-MAIL/SMS
Would like to receive bank's promotional messages over e-mail/SMS**)

Saya/kami menyatakan bahwa semua data di atas adalah benar dan menyetujui serta tunduk pada ketentuan dan syarat-syarat layanan internet banking dan atau sms banking yang telah saya baca pada lembar di balik aplikasi ini maupun ketentuan lain yang berlaku dari waktu ke waktu di PT. Bank Mandiri (Persero).
I/we certify that above mentioned data is correct and I/we hereby approve and shall be subject to the terms and conditions internet banking and or sms banking services on the back leaf application, or other terms and conditions from time to time at PT. Bank Mandiri (Persero).

1. Tandatangan
Signature

Nama/Name: _____

2. Tanda tangan (hanya untuk aplikasi rekening gabungan)
Signature (only for joint account application)

Nama/Name: _____

CIF NO. _____

☐ Perorangan ☐ Rekening Gabungan

Diproses Oleh

Disetujui Oleh

Customer Service

*) Maksimum 10 hari sebelum jatuh tempo / Maximum for 10 days before maturity
**) Coret sesuai dengan aplikasi yang diinginkan / Delete where applicable

FFO 057 1/2

istilah

1. Internet Banking Mandiri adalah saluran distribusi Bank untuk mengakses rekening yang dimiliki Nasabah melalui jaringan internet dengan menggunakan perangkat lunak browser pada komputer.
2. Bank adalah PT BANK MANDIRI (PERSERO) yang meliputi Kantor Pusat dan kantor cabang serta kantor lainnya yang merupakan bagian yang tidak terpisahkan dari PT BANK MANDIRI (PERSERO).
3. Nasabah adalah perorangan pemilik rekening simpanan dalam mata uang rupiah berupa Giro Rupiah dan Tabungan Mandiri.
4. Nasabah Pengguna adalah Nasabah yang telah terdaftar sebagai pengguna layanan Internet Banking Mandiri.
5. Daftar Rekening adalah nomor rekening Rupiah di semua cabang yang dimiliki oleh Nasabah di Bank yang telah didaftarkan dan karenanya dapat diakses oleh Nasabah Pengguna.
6. User ID adalah identitas yang dimiliki oleh setiap Nasabah Pengguna yang harus dicantumkan/diinput dalam setiap penggunaan layanan Internet Banking Mandiri.
7. PIN (Personal Identification Number) Internet Banking Mandiri adalah nomor identifikasi pribadi yang bersifat rahasia dan hanya diketahui oleh Nasabah Pengguna serta harus dicantumkan/diinput oleh Nasabah Pengguna pada saat menggunakan layanan Internet Banking Mandiri. Bersama-sama dengan User ID, PIN digunakan untuk membuktikan bahwa nasabah bersangkutan adalah nasabah yang berhak atas layanan Internet Banking Mandiri.

Syarat Pendaftaran Internet Banking Mandiri:

1. Nasabah mengisi dan menandatangani Formulir Aplikasi Internet Banking dan SMS Banking yang dapat diperoleh di cabang atau di situs Internet Bank Mandiri (www.bankmandiri.co.id).
2. Menunjukkan bukti asli identitas diri yang sah (KTP, SIM, Paspor, KITAS) dan bukti kepemilikan pemegang rekening.
3. Setiap perorangan pemegang rekening gabungan masing-masing harus menandatangani Formulir Aplikasi Internet Banking dan SMS Banking.
4. Nasabah harus memiliki alamat E-mail.
5. Nasabah Pengguna telah memperoleh Access ID dan Access PIN dari Bank untuk keperluan aktivasi di situs Internet Banking Mandiri.
6. Telah membaca dan memahami Syarat dan Ketentuan Internet Banking Mandiri.

Ketentuan Penggunaan Internet Banking Mandiri

1. Nasabah Pengguna dapat menggunakan layanan Internet Banking Mandiri untuk mendapatkan informasi dan atau melakukan transaksi Perbankan yang telah ditentukan oleh Bank.
2. Pada saat pertama kali menggunakan layanan Internet Banking Mandiri, Nasabah Pengguna diharuskan melakukan aktivasi di situs Internet Banking Mandiri dengan cara memasukkan Access ID dan Access PIN yang diperoleh dari Bank untuk diubah menjadi User ID dan PIN Internet Banking Mandiri.
3. Untuk setiap pelaksanaan transaksi:
 - a. Nasabah Pengguna wajib memastikan ketepatan dan kelengkapan perintah transaksi (termasuk memastikan bahwa semua data yang diperlukan untuk transaksi telah diisi secara lengkap dan benar). Bank tidak bertanggung jawab terhadap segala dampak apapun yang mungkin timbul yang disebabkan kelalaian, ketidaklengkapan, ketidakjelasan, atau ketidaktepatan perintah/data dari Nasabah Pengguna.
 - b. Nasabah Pengguna memiliki kesempatan untuk memeriksa kembali dan atau membatalkan data yang telah diisi pada saat konfirmasi yang dilakukan secara otomatis oleh sistem sebelum adanya tanda persetujuan sebagaimana diatur di bawah ini.
 - c. Apabila telah diyakini kebenaran dan kelengkapan data yang diisi, sebagai tanda persetujuan pelaksanaan transaksi maka Nasabah Pengguna wajib memasukkan PIN pada kolom yang telah disediakan pada halaman layanan transaksi Internet Banking Mandiri.
4. Segala transaksi yang telah diperintahkan kepada Bank dan disetujui oleh Nasabah Pengguna tidak dapat dibatalkan.
5. Setiap perintah yang telah disetujui dari Nasabah Pengguna yang tersimpan pada pusat data Bank merupakan data yang benar yang diterima sebagai bukti perintah dari Nasabah Pengguna kepada Bank untuk melaksanakan transaksi yang dimaksud.
6. Bank menerima dan menjalankan setiap perintah dari Nasabah Pengguna sebagai perintah yang sah berdasarkan penggunaan User ID dan PIN dan untuk itu Bank tidak mempunyai kewajiban untuk meneliti atau menyelidiki keaslian maupun keabsahan atau kewenangan pengguna User ID dan PIN atau menilai maupun membuktikan ketepatan maupun kelengkapan perintah dimaksud, dan oleh karena itu perintah tersebut sah mengikat Nasabah Pengguna dengan sebagaimana mestinya, kecuali Nasabah Pengguna dapat membuktikan sebaliknya.
7. Bank berhak untuk tidak melaksanakan perintah dari Nasabah Pengguna, apabila:
 - a. Saldo rekening Nasabah Pengguna di Bank tidak cukup.
 - b. Bank mengetahui atau mempunyai alasan untuk mencurigai bahwa penipuan atau aksi kejahatan telah atau akan dilakukan.
- ✓ 8. Sebagai bukti bahwa transaksi yang diperintahkan Nasabah Pengguna telah berhasil dilakukan oleh Bank, Nasabah Pengguna akan mendapatkan bukti transaksi berupa nomor transaksi pada halaman transaksi layanan Internet Banking Mandiri dan bukti tersebut akan tersimpan di dalam menu aktivitas transaksi selama 3 (tiga) bulan sejak tanggal transaksi.
9. Nasabah Pengguna menyetujui dan mengakui bahwa:
 - a. Dengan dilaksanakannya transaksi melalui Internet Banking Mandiri, semua perintah dan komunikasi dari Nasabah Pengguna yang diterima Bank akan diperlakukan sebagai alat bukti yang sah meskipun tidak dibuat dokumen tertulis dan atau dikeluarkan dokumen yang tidak ditandatangani.
 - b. Bukti atas perintah dari Nasabah Pengguna kepada Bank dan segala bentuk komunikasi antara Bank dan Nasabah Pengguna yang dikirim secara elektronik yang tersimpan pada pusat data Bank dan atau tersimpan dalam bentuk penyimpanan informasi dan data lainnya di Bank, baik yang berupa dokumen tertulis, catatan, tape/cartridge, print out komputer dan atau salinan, merupakan alat bukti yang sah yang tidak akan dibantah keabsahan, kebenaran atau keasliannya.
10. Atas pertimbangannya sendiri, Bank berhak untuk mengubah limit transaksi.
11. Semua komunikasi melalui e-mail yang aman dan memenuhi standar serta dianggap sah, otentik, asli dan benar serta memberikan efek yang sama sebagaimana bila hal tersebut dilakukan secara tertulis dan atau melalui dokumen tertulis.
12. Bank tidak diwajibkan untuk melaksanakan setiap perintah baik yang ditandatangani maupun tidak atau menjawab pertanyaan apapun yang diterima melalui e-mail yang tidak aman. Nasabah disarankan untuk tidak mengirim informasi rahasia melalui e-mail yang tidak aman.
13. Bank berhak menghentikan layanan Internet Banking Mandiri untuk sementara waktu maupun untuk jangka waktu tertentu yang ditentukan oleh Bank untuk keperluan pembaharuan, pemeliharaan atau untuk tujuan lain dengan alasan apapun yang dianggap baik oleh Bank, dan untuk itu Bank tidak berkewajiban mempertanggungjawabkannya kepada siapapun.

User ID dan PIN Internet Banking Mandiri

1. User ID dan PIN merupakan kode yang bersifat rahasia dan kewenangan penggunaannya ada pada Nasabah Pengguna. User ID bersifat tetap dan tidak dapat diubah kembali.
2. Nasabah wajib mengamankan User ID dan PIN Internet Banking dengan cara:
 - a. Tidak membentahkan User ID dan PIN Internet Banking kepada orang lain.
 - b. Tidak mencatatkan PIN Internet Banking pada kertas atau menyimpannya secara tertulis atau sarana penyimpanan lainnya yang memungkinkan diketahui orang lain.
 - c. Memusnahkan secepatnya Access ID dan PIN Mailer Internet Banking setelah menerimanya.
 - d. Berhati-hati menggunakan User ID dan PIN Internet Banking Mandiri agar tidak terlihat orang lain.
 - e. Sering mengganti PIN Internet Banking Mandiri secara berkala.
- ✓ 3. Dalam hal Nasabah Pengguna mengetahui atau menduga User ID dan PIN telah diketahui oleh orang lain yang tidak berwenang, maka Nasabah Pengguna wajib segera melakukan pengamanan dengan melakukan perubahan PIN. Apabila karena suatu sebab Nasabah Pengguna tidak dapat melakukan perubahan PIN maka Nasabah Pengguna wajib memberitahukan kepada Bank. Sebelum diterimanya pemberitahuan secara tertulis oleh pejabat Bank yang berwenang, maka segala perintah, transaksi dan komunikasi berdasarkan penggunaan User ID dan PIN oleh pihak yang tidak berwenang sepenuhnya menjadi tanggung jawab Nasabah Pengguna.
4. Penggunaan User ID dan PIN mempunyai kekuatan hukum yang sama dengan perintah tertulis yang ditandatangani oleh Nasabah Pengguna, sehingga karenanya Nasabah Pengguna dengan ini menyatakan bahwa penggunaan User ID dan PIN dalam setiap perintah atas transaksi Internet Banking Mandiri juga merupakan pemberian kuasa dari Nasabah Pengguna kepada Bank untuk melaksanakan transaksi termasuk namun tidak terbatas untuk melakukan pengebetan rekening Nasabah baik dalam rangka pelaksanaan transaksi yang diperintahkan maupun untuk pembayaran biaya transaksi yang telah dan atau akan ditetapkan kemudian oleh Bank.
5. Segala penyalahgunaan Access ID/User ID dan Access PIN/PIN Internet Banking Mandiri merupakan tanggung jawab Nasabah Pengguna. Nasabah Pengguna dengan ini membebaskan Bank dari segala tuntutan yang mungkin timbul, baik dari pihak lain maupun Nasabah Pengguna sendiri sebagai akibat penyalahgunaan Access ID/User ID dan Access PIN/PIN Internet Banking Mandiri.

Penghentian Akses Layanan Internet Banking Mandiri

1. Akses layanan Internet Banking Mandiri akan dihentikan oleh Bank apabila:
 - a. Nasabah Pengguna meminta kepada Bank untuk menghentikan akses layanan Internet Banking Mandiri yang antara lain disebabkan karena Nasabah Pengguna menutup semua rekening yang dapat diakses melalui layanan Internet Banking Mandiri.
 - b. Salah memasukkan Access PIN/PIN Internet Banking Mandiri sebanyak 3 (tiga) kali berturut-turut.
 - c. Diterimanya laporan tertulis dari Nasabah Pengguna mengenai dugaan atau diketahuinya User ID dan PIN oleh pihak lain yang tidak berwenang.
 - d. Bank melaksanakan suatu keharusan sesuai ketentuan perundang-undangan yang berlaku.
2. Untuk melakukan aktivasi kembali karena penghentian akses layanan tersebut di atas, Nasabah Pengguna harus menghubungi Call Centre Bank Mandiri atau melakukan pendaftaran ulang di cabang pengelola rekening.

Force Majeure

Nasabah Pengguna akan membebaskan Bank dari segala tuntutan apapun, dalam hal Bank tidak dapat melaksanakan perintah dari Nasabah Pengguna baik sebagian maupun seluruhnya karena kejadian-kejadian atau sebab-sebab di luar kekuasaan atau kemampuan Bank termasuk namun tidak terbatas pada segala gangguan virus komputer atau sistem Trojan Horses atau komponen membahayakan yang dapat mengganggu layanan Internet Banking Mandiri, web browser atau komputer sistem Bank, Nasabah, atau Internet Service Provider, karena bencana alam, perang, huru-hara, keadaan peralatan, sistem atau transmisi yang tidak berfungsi, gangguan listrik, gangguan telekomunikasi, kebijakan pemerintah, serta kejadian-kejadian atau sebab-sebab lain di luar kekuasaan atau kemampuan Bank.

Lain-lain

1. Bukti perintah Nasabah Pengguna melalui layanan Internet Banking Mandiri adalah mutasi yang tercatat dalam Rekening Koran atau Buku Tabungan Mandiri jika dicetak.
2. Nasabah Pengguna dapat menghubungi Call Centre Bank Mandiri atas setiap permasalahan yang berkaitan dengan transaksi dan perubahan akses layanan Internet Banking Mandiri.
3. Bank dapat mengubah syarat dan ketentuan ini setiap saat dengan pemberitahuan terlebih dahulu kepada Nasabah Pengguna dalam bentuk dan melalui sarana apapun.
4. Nasabah Pengguna tunduk pada ketentuan-ketentuan dan peraturan-peraturan yang berlaku pada Bank serta syarat-syarat pembukaan rekening dan syarat rekening gabungan, termasuk setiap perubahan yang akan diberitahukan terlebih dahulu oleh Bank dalam bentuk dan sarana apapun.
5. Kuasa-kuasa baik yang tersurat dalam Syarat dan Ketentuan ini merupakan kuasa yang sah yang tidak akan berakhir selama Nasabah Pengguna masih memperoleh layanan Internet Banking Mandiri atau masih adanya kewajiban lain dari Nasabah Pengguna kepada Bank.

http://www.bankmandiri.co.id/article/183675062176.asp?article_id=183675062176

Tentang Internet Banking



Bank Mandiri menghadirkan Internet Banking Mandiri

Internet Banking Mandiri memberi Anda akses langsung secara real time kepada rekening Anda di Bank Mandiri melalui internet. Kapan saja, siang ataupun malam, dan di mana saja, Anda bisa memeriksa saldo Anda, melakukan transfer dana, melakukan pembayaran telepon selular, dan masih banyak lagi! Semua itu merupakan layanan yang diberikan Bank Mandiri secara gratis.

Transaksi yang dapat Anda lakukan di Mandiri Internet Banking:

1. Transfer Dana
2. Pembayaran
3. Informasi Rekening
4. Aktivitas Transaksi
5. Fasilitas Cek
6. Update Profil
7. Personalisasi
8. Notifikasi SMS

Mendaftarlah sekarang juga dan dapatkan keuntungan Mandiri Internet Banking. Caranya mudah, Anda tinggal datang ke cabang pengelola rekening dan petugas kami akan membantu Anda. Berbagai pertanyaan dan jawaban tentang Internet Banking dapat Anda lihat pada FAQ Internet Banking atau hubungi kami di nomor (021) 5299 7777 atau email customer.care@bankmandiri.co.id

Kebijakan Kerahasiaan Nasabah

Berikut disampaikan kebijakan yang diterapkan oleh Bank Mandiri untuk menjamin kerahasiaan dan keamanan bagi Nasabah yang mengunjungi Internet Banking Mandiri.

Aplikasi Internet Banking Mandiri dijamin kerahasiaan dan keamanannya, dalam hal ini Bank Mandiri menggunakan teknologi enkripsi Secure Socket Layer (SSL) 128 bit, yang akan melindungi komunikasi antara komputer Nasabah dengan server Bank Mandiri. Untuk menambah keamanan digunakan metode time out session, dimana setelah 10 menit tanpa aktivitas Nasabah, maka akses akan tidak aktif lagi.

Selain itu Bank Mandiri akan menjaga kerahasiaan data pengguna Internet Banking Mandiri, dan hanya orang tertentu yang berhak untuk mengakses informasi tersebut untuk digunakan sebagaimana mestinya (dalam hal ini Bank Mandiri akan selalu mengingatkan karyawan akan pentingnya menjaga kerahasiaan data Nasabah). Bank Mandiri tidak akan memperlihatkan/menjual data tersebut kepada pihak ke tiga.

Bank Mandiri juga tidak secara otomatis mengumpulkan informasi data pengunjung Internet Banking Mandiri, hanya beberapa informasi umum yang akan dikumpulkan dan digunakan antara lain :

- Nama domain yang akan digunakan Nasabah untuk mengakses internet
- Internet address yang digunakan untuk mengakses web site Bank Mandiri
- Browser yang digunakan
- Hari, tanggal & waktu mengakses internet
- Pilihan yang ditentukan oleh Nasabah untuk memberikan informasi kepada Bank, antara lain jenis rekening

Untuk dapat mengakses Internet Banking Mandiri Nasabah harus memasukkan terlebih dahulu User ID dan PIN, dan untuk keamanan Nasabah diharuskan memasukkan kembali PIN untuk setiap transaksi yang bersifat finansial.

Mengingat banyaknya variasi internet browser yang ada, dan internet banking harus mengikuti keamanan masing-masing browser, maka saat ini Bank Mandiri menyediakan sarana internet banking yang lebih cocok diakses dengan menggunakan Netscape Communicator 4.7 atau Microsoft Internet Explorer versi 5.01 atau versi terakhir.

Untuk menjadi pengguna Internet Banking Mandiri, cukup ikuti langkah-langkah petunjuk berikut ini:

Syarat Pendaftaran:

1. Memiliki rekening tabungan, giro rupiah dan atau mata uang lainnya.
2. Untuk pendaftaran di ATM, harus memiliki kartu ATM Mandiri sedangkan untuk pendaftaran di cabang harus menunjukkan bukti identitas diri (KTP, SIM, Passport, KIMS) dan bukti kepemilikan rekening (buku tabungan, kartu ATM MAndiri)

Langkah Pendaftaran:

Langkah 1 : Lakukan pendaftaran Internet Banking Mandiri dengan salah satu cara dibawah ini, untuk mendapatkan nomor Access ID dan Access Code

- Datang ke ATM Bank Mandiri Masuk ke menu utama dan pilih registrasi e-banking serta ikuti petunjuk yang ada di layar ATM untuk membuat Access Code. Sedangkan untuk nomor Access ID gunakan 16 digit nomor kartu ATM Anda.
- Atau datang ke Cabang Bank Mandiri. Isi formulir aplikasi pendaftaran Internet Banking Mandiri yang ada di cabang, selanjutnya bank akan mengirim Access ID ke alamat e-mail Anda serta menyerahkan Access Code dalam amplop tertutup.

Langkah 2 : Lakukan Pendaftaran Token PIN Mandiri

Dapatkan Token PIN Mandiri di cabang Bank Mandiri terdekat dengan mengisi formulir aplikasi Penggunaan Token PIN Mandiri serta ikuti buku petunjuk penggunaan yang terdapat di dalam box.

Note:

- Untuk bisa bertransaksi Anda diharuskan menggunakan Token PIN Mandiri.
- Tanpa Token PIN Mandiri Anda masih bisa log-on kedalam sistem Internet Banking Mandiri untuk mendapatkan Informasi Saldo dan mutasi transaksi.

Langkah 3 : Lakukan Aktivasi Internet Banking Bank Mandiri

- Klik tombol aktivasi pada situs www.bankmandiri.co.id, dan masukkan/input Access ID dan Access Code yang diperoleh dari bank setelah Anda melakukan registrasi di ATM atau cabang Bank Mandiri.
- Selanjutnya buat sendiri User ID dan PIN Internet Banking Mandiri Anda untuk bisa log-in kedalam layanan Internet Banking Mandiri

Langkah 4 : Lakukan Aktivasi Token PIN Mandiri Anda

Login ke Internet Banking Mandiri di www.bankmandiri.co.id , masuk ke menu administrasi dan pilih Aktivasi Token PIN Mandiri.

http://www.bankmandiri.co.id/article/852223880268.asp?article_id=852223880268

My Security

Bank Mandiri menjaga kerahasiaan identitas dan semua informasi keuangan Nasabah Pengguna. Untuk menjaga komitmen jaminan keamanan dan kerahasiaan data pribadi, keuangan dan transaksi Nasabah Pengguna, Internet Banking Mandiri menggunakan beberapa sistem yang melindungi informasi rekening dan data Nasabah :

1. User ID dan PIN (Personal Identification Number), merupakan kode rahasia dan kewenangan penggunaan yang diberikan kepada Nasabah, yaitu setiap kali login ke Internet Banking Mandiri Nasabah harus memasukkan User ID dan PIN, dan untuk transaksi yang bersifat finansial, Nasabah harus memasukkan kembali PIN untuk menghindari penyalahgunaan oleh orang lain saat komputer ditinggalkan dalam keadaan terhubung dengan Internet Banking Mandiri.
2. Automatic log out, jika tidak ada tindakan yang dilakukan lebih dari 10 menit, Internet Banking secara otomatis akan mengakhiri dan kembali ke menu utama.
3. SSL 128-bit encryption, seluruh data di Internet Banking Mandiri dikirimkan melalui protocol Secure Socket Layer (SSL), yaitu suatu standar pengiriman data rahasia melalui internet. Protocol SSL ini akan mengacak data yang dikirimkan menjadi kode-kode rahasia dengan menggunakan 128-bit encryption, yang artinya terdapat 2 pangkat 128 kombinasi angka kunci, tetapi hanya satu kombinasi yang dapat membuka kode-kode tersebut.
4. Firewall, untuk membatasi dan menjamin hanya Nasabah yang mempunyai akses untuk dapat masuk ke sistem Internet Banking Mandiri.

Untuk perlindungan Anda :

- Pastikan Anda telah mengetik situs Internet Banking Mandiri dengan benar, yakni : www.bankmandiri.co.id, dengan hari, tanggal dan jam yang tertera benar. Untuk menghindari kesalahan pengetikan nama situs Bank Mandiri, Anda dapat memasukkan alamat situs tersebut ke dalam menu Favorites (jika Anda menggunakan browser Internet Explorer) atau menu Bookmarks (jika Anda menggunakan browser Netscape Communicator).
- Pastikan bahwa halaman internet banking yang Anda kunjungi merupakan milik Bank Mandiri, pada browser Anda menampilkan tulisan <http://www.bankmandiri.co.id> pada field address dan pada saat Anda telah meng-klik tombol Login field address akan menampilkan tulisan <https://ib.bankmandiri.co.id>.
- Selain itu pastikan bahwa pada saat Anda Login dipojok kanan bawah terdapat gambar gembok yang akan menandai bahwa Anda

memasuki daerah yang aman. Untuk meyakini bahwa Anda Login pada server Internet Banking Mandiri, Anda dapat melihat Certificate Authority milik Bank Mandiri dengan cara meng-klik gambar gembok kunci di kanan bawah. Apabila tidak terlihat gambar gembok segera log out, selanjutnya Anda dapat melakukan Login kembali.

- Untuk keamanan Anda Bank Mandiri akan mengirimkan secara terpisah antara Access ID dengan Access PIN. Access ID akan dikirimkan melalui e-mail Nasabah, sementara Access PIN diambil di cabang tempat Anda mendaftar dalam bentuk PIN mailer.
- Pastikan bahwa komputer yang akan digunakan untuk masuk ke situs Internet Banking Mandiri dalam kondisi tidak terkena virus.

Beberapa tips yang dapat digunakan untuk menjamin keamanan bertransaksi di Internet Banking Mandiri :

- User ID dan PIN merupakan suatu hal yang rahasia, jangan beritahukan PIN sebagian atau seluruhnya kepada orang lain, bahkan karyawan cabang atau petugas customer care Bank Mandiri sekalipun
- Jika Nasabah menduga/mengira adanya orang yang tidak berwenang mengetahui akan PIN Anda, segera ubah PIN dan laporkan hal ini ke cusomer care Bank Mandiri
- Jangan meninggalkan komputer pada saat masih log on, lakukan logout setiap meninggalkan komputer meskipun hanya sebentar, dan setelah selesai seluruh transaksi selalu lakukan log out meskipun komputer tersebut milik Anda pribadi di rumah
- Jangan membuat PIN yang merupakan angka : tanggal lahir, nomor telephone rumah, nomor kendaraan dan lain-lain yang mudah untuk diingat/ditebak orang lain
- Jangan membuat PIN yang merupakan urutan angka, contoh : 123456
- Jangan membuat PIN yang merupakan pengulangan satu angka, contoh : 111111
- Jangan mencatat PIN ditempat yang orang lain bisa membacanya, contoh : agenda, kalender
- Jangan membuat PIN yang merupakan pengulangan dari User ID
- Baca kembali instruksi Anda di layar konfirmasi sebelum PIN dimasukkan, dan instruksi teruskan di klik, hal ini untuk menghindari kesalahan nomor rekening, nomor refrensi dan jumlah yang Anda inginkan
- Catat nomor transaksi atas transaksi yang telah Anda lakukan
- Jika Anda salah memasukkan PIN 3 (tiga) kali berturut-turut, system akan memblokir akses Anda secara otomatis. Untuk mengaktifkan kembali hubungi Customer Care Bank Mandiri di nomor telepon (021) 527-2211 atau melalui e-mail ke customer.care@bankmandiri.co.id, Customer Care akan mengajukan beberapa pertanyaan kepada Anda untuk otentikasi

<https://secure.bank2home.com/appniaga/login.jsp>

Dengan melakukan Login, maka Anda setuju dan tunduk

kepada **SYARAT & KETENTUAN NIAGA GLOBAL@CCESS**

By clicking Login button, you hereby agree and to be bound by

*the **TERMS & CONDITIONS** of **NIAGA GLOBAL@CCESS***

Klik [di sini](#) untuk petunjuk penggunaan **NIAGA GLOBAL@CCESS**

Click [here](#) if you need help in using **NIAGA GLOBAL@CCESS**

"Jangan memberitahukan password Anda kepada siapapun.

Staff kami **TIDAK PERNAH** menanyakan password Anda.

Sebelum Anda mengisi password pada saat login, pastikan alamat halaman login adalah:

<https://secure.bank2home.com/appniaga/login.jsp>

Do not reveal your password to anyone under any circumstances.

*Our staffs **NEVER** ask to reveal your password.*

Before you enter your password when you login,

please make sure that the login page address is:

<https://secure.bank2home.com/appniaga/login.jsp>

Tampilan terbaik dengan Microsoft IE versi 4.0

ke atas atau

dengan Netscape versi 4.08 ke atas, dengan resolusi 800x600

Best viewed with Microsoft IE 4.0 and above or with Netscape 4.08 and above, with 800x600 resolution



NIAGA
GLOBAL@CCESS

User ID

Password

Bahasa / Language



English



Indonesia

Login

Reset



Click to verify

Click VeriSign logo to verify whether your browser supports 128-bit SSL Security Encryption

SYARAT DAN KETENTUAN INTERNET BANKING ("IB") PT BANK NIAGA TBK. ("BN")

NIAGA GLOBAL@CCESS

REGISTRASI INTERNET BANKING BN

Setiap Nasabah perorangan yang mempunyai rekening Tabungan dan/atau Giro di BN berhak untuk menikmati fasilitas IB BN.

Untuk dapat menggunakan fasilitas IB BN, Nasabah harus memiliki identitas pengguna IB BN ("User ID") dan nomor Password IB BN ("Password"). Password akan diberikan pada saat Nasabah melakukan registrasi pada Cabang-Cabang BN, sedangkan User ID akan dikirim melalui alamat e-mail Nasabah.

User ID yang diberikan oleh BN bersifat permanen dan tidak dapat diubah kecuali atas instruksi perubahan oleh Nasabah dan hanya untuk alasan hilang.

Password dapat diubah oleh Nasabah dan jika Password hilang maka BN akan menerbitkan Password baru (sepanjang Nasabah melaporkan kehilangan Password tersebut)

TRANSAKSI MENGGUNAKAN INTERNET BANKING (IB) BN

Nasabah harus mengisi semua data yang dibutuhkan untuk setiap transaksi secara benar dan lengkap.

Nasabah wajib dan bertanggung jawab untuk memastikan ketepatan dan kelengkapan instruksi transaksi. BN tidak bertanggung jawab terhadap segala akibat apapun yang timbul karena ketidaklengkapan, ketidakjelasan data atau ketidaktepatan instruksi dari Nasabah.

Pada setiap transaksi finansial, sistem akan selalu melakukan konfirmasi terhadap data yang diinput Nasabah dan Nasabah mempunyai kesempatan untuk membatalkan data tersebut dengan menekan tombol "Batal".

Sebagai tanda persetujuan, Nasabah wajib menekan tombol "Confirm" setiap melakukan instruksi transaksi finansial.

Setiap informasi yang mendapat konfirmasi "Kirim" dari Nasabah yang tersimpan dalam pusat data BN merupakan data yang benar yang diterima sebagai bukti atas instruksi dari Nasabah kepada BN untuk melakukan transaksi yang dimaksud, kecuali Nasabah dapat membuktikan sebaliknya.

BN menerima dan menjalankan setiap instruksi dari Nasabah sebagai instruksi yang sah berdasarkan penggunaan User ID dan Password dan untuk itu BN tidak mempunyai kewajiban untuk meneliti atau menyelidiki keaslian maupun keabsahan atau kewenangan pengguna User ID dan Password atau menilai maupun membuktikan ketepatan maupun kelengkapan instruksi dimaksud, dan oleh karena itu instruksi tersebut sah mengikat Nasabah dengan sebagaimana mestinya, kecuali Nasabah dapat membuktikan sebaliknya.

Nasabah tidak dapat membatalkan semua transaksi yang diinstruksikan kepada BN yang telah mendapat konfirmasi "Kirim" dari Nasabah, karena dalam waktu yang sama BN langsung memproses instruksi tersebut.

Untuk setiap instruksi dari Nasabah atas transaksi yang berhasil dilakukan oleh BN, Nasabah akan mendapatkan bukti transaksi berupa nomor referensi sebagai bukti transaksi tersebut telah dilakukan oleh BN.

BN berhak untuk tidak melaksanakan instruksi dari Nasabah, jika saldo Nasabah di BN tidak mencukupi dan rekening telah ditutup, rekening dikenai sita atau diblokir atau berdasarkan pertimbangan lain dari Bank yang akan diberitahukan kepada nasabah.

KURS

Informasi nilai tukar valuta asing, suku bunga dan kurs lainnya yang disediakan di IB BN hanya merupakan indikasi dari kurs yang berlaku saat itu, dan dapat diubah sewaktu-waktu oleh BN tanpa pemberitahuan terlebih dahulu.

Transaksi Nasabah dalam mata uang asing menggunakan kurs yang berlaku di BN pada saat transaksi dijalankan.

PEMBUKTIAN

Nasabah setuju bahwa catatan, tape/cartridge, print out komputer, salinan atau bentuk penyimpanan informasi atau data lain sebagai bukti yang sah atas instruksi dari Nasabah, demikian juga sarana komunikasi lain yang diterima atau dikirimkan oleh BN.

Nasabah setuju untuk tidak membantah keabsahan, kebenaran atau keaslian bukti instruksi dan komunikasi yang ditransmisi secara elektronik antara kedua belah pihak, termasuk dokumen dalam bentuk catatan komputer atau bukti transaksi BN, tape/cartridge, print out komputer, salinan atau bentuk penyimpanan informasi yang lain, dan semua alat atau dokumen tersebut merupakan satu-satunya alat bukti yang sah atas transaksi-transaksi perbankan melalui IB BN, kecuali Nasabah dapat membuktikan sebaliknya.

Dengan melakukan transaksi melalui IB BN, Nasabah mengakui semua komunikasi dan instruksi dari Nasabah yang diterima BN akan diperlakukan sebagai alat bukti yang sah meskipun tidak dibuat dokumen tertulis ataupun dikeluarkan dokumen yang ditandatangani.

USER ID, PASSWORD DAN KEWAJIBAN NASABAH

Apabila Nasabah meninggalkan terminal dalam keadaan aktif (log-on), maka secara otomatis dalam waktu 5 menit sistem BN akan mengakhiri akses IB tersebut, untuk mencegah penyalahgunaan oleh pihak yang tidak berwenang.

Nasabah wajib mengamankan User ID dan Password dengan cara :

- Tidak memberitahukan User ID dan Password kepada orang lain.
- Tidak menuliskan User ID dan Password pada meja, terminal atau menyimpannya dalam bentuk tertulis atau pada aplikasi komputer atau sarana penyimpanan lainnya yang memungkinkan untuk diketahui oleh orang lain.
- User ID dan Password harus digunakan dengan hati-hati agar tidak terlihat oleh orang lain.

Nasabah bertanggung jawab sepenuhnya terhadap semua instruksi transaksi yang terjadi berdasarkan penggunaan User ID dan Password yang dimiliki oleh Nasabah, kecuali Nasabah dapat membuktikan sebaliknya.

BN berhak untuk memberikan User ID yang terdiri dari serangkaian angka tanpa harus mendapatkan persetujuan terlebih dahulu dari Nasabah.

Nasabah wajib untuk segera memberitahukan kepada BN apabila User ID dan atau Password tersebut telah diketahui oleh orang lain. Segala instruksi transaksi berdasarkan penggunaan User ID dan Password yang terjadi sebelum pejabat yang berwenang dari BN menerima secara tertulis laporan tersebut merupakan tanggung jawab sepenuhnya dari Nasabah.

LIMIT

Pada saat ini limit transaksi yang dapat dilakukan oleh Nasabah melalui IB BN merupakan satu kesatuan dengan limit produk yang diakses oleh Nasabah, BN atas pertimbangannya sendiri berhak setiap saat untuk mengubah besar limit untuk setiap transaksi.

ELECTRONIC MAIL ("E-MAIL")

Nasabah akan memberikan alamat E-Mail pada saat melakukan pendaftaran IB BN yang mana akan digunakan oleh BN selain untuk mengirimkan User ID Nasabah juga untuk mengirim informasi transaksi yang telah dilakukan oleh Nasabah melalui IB BN.

Nasabah diberikan fasilitas 'E-Mail' di IB yang digunakan untuk berkomunikasi dengan BN.

BN tidak menjamin keamanan informasi atau data yang dikirim kepada BN melalui E-Mail yang tidak terdapat di IB BN, yang tidak dalam format yang aman yang disetujui atau ditentukan oleh BN.

BIAYA & KUASA DEBET REKENING

Dengan ini BN diberi kuasa untuk mendebet rekening Nasabah di BN sebesar :

- a. nilai transaksi yang dilakukan Nasabah kepada BN melalui Internet Banking; dan/atau
- b. biaya administrasi bulanan serta biaya transaksi atas penggunaan fasilitas Internet Banking.

Nasabah sepakat bahwa Bank atas pertimbangannya sendiri diperkenankan untuk mengubah, menambah atau menarik biaya-biaya yang dibebankan kepada Nasabah atas penggunaan fasilitas IB BN.

Kuasa ini akan berakhir apabila Nasabah mengakhiri penggunaan fasilitas IB BN dan segala kewajiban Nasabah kepada BN sudah terpenuhi.

PEMBLOKIRAN USER ID DAN PASSWORD INTERNET BANKING

User ID dan Password Nasabah akan diblokir jika terjadi hal-hal sebagai berikut:

- Apabila Nasabah salah memasukkan Password sebanyak 3 kali dalam atau pada saat login.
- Apabila Nasabah tidak menggunakan fasilitas IB BN selama 45 hari sejak dikirimnya User ID.
- Apabila User ID dan atau Password Nasabah hilang dan atau dilaporkan telah diketahui oleh orang lain.

Apabila Nasabah ingin mengaktifkan kembali User ID dan Password yang diblokir, Nasabah harus menghubungi NIAGA ACCESS (Call Centre) di nomor 14041 atau 62-21-14041 dan melakukan registrasi ulang IB BN pada Cabang-Cabang BN.

FORCE MAJEURE

Nasabah akan membebaskan BN dari segala tuntutan apapun, dalam hal BN tidak dapat melaksanakan instruksi dari Nasabah baik sebagian maupun seluruhnya karena kejadian-kejadian atau sebab-sebab diluar kekuasaan atau kemampuan BN, termasuk namun tidak terbatas pada bencana alam, perang, huru-hara, keadaan peralatan, sistem atau transmisi yang tidak berfungsi, gangguan listrik, gangguan telekomunikasi, kebijaksanaan pemerintah, serta kejadian-kejadian atau sebab-sebab lain diluar kekuasaan atau kemampuan BN.

PENGAKHIRAN LAYANAN

Layanan IB BN akan berakhir jika Nasabah menutup semua rekening yang ada pada BN atau atas permohonan Nasabah sendiri dan atau atas BN dapat mengakhiri layanan IB BN dengan pemberitahuan terlebih dahulu kepada Nasabah, apabila terjadi perselisihan antara BN dan Nasabah.

SETUJU

© 2000 Pacific Communication Networks

<http://www.bankniaga.com/ProdServ/prodserv.asp?id=PRN0000038>

Berdasarkan konsep layanan Bank Niaga yang memberikan kemudahan kepada nasabah untuk bertransaksi dari mana saja dan kapan saja sesuai dengan kebutuhan nasabah, kini kami hadirkan sebuah kemudahan, kenyamanan serta keamanan akses perbankan tanpa batas melalui internet.

Semua urusan perbankan dapat anda selesaikan di meja kerja atau dirumah kapanpun diperlukan. Semuanya cukup dengan masuk ke website Bank Niaga di www.bankniaga.com atau www.bank2home.com.

Keamanan Terjamin

1. Pendaftaran pengguna Niaga Global@ccess hanya dapat dilakukan melalui Cabang Bank Niaga dengan Password diberikan saat pendaftaran dan User ID akan dikirimkan sistem ke email nasabah
2. Untuk akses harus menggunakan User ID dan Password
3. Menggunakan sistem keamanan standard international 3.0 dengan enkripsi SSL 128 bit yang akan mengacak data transaksi di internet banking
4. Seluruh aktifitas nasabah di Niaga Global@ccess akan tercatat oleh sistem
5. Nasabah dapat melihat seluruh aktifitas yang dilakukan pada Niaga Global@ccess selama jangka waktu tertentu
6. Nasabah akan dikirimkan seluruh aktifitas harian yang dilakukan pada Niaga Global@ccess ke alamat email nasabah
7. In Active Timer untuk Log Out otomatis dari Niaga Global@ccess dalam jangka waktu tertentu
8. Limit maksimum kesalahan pengisian Password

Niaga Global @ccess Features

1. Informasi Saldo
2. Informasi Transaksi
3. Transaksi Overbooking
4. Transaksi Pembayaran:
 - o Telkom
 - o Kartu Kredit Bank Niaga
 - o Kartu Kredit Citibank
 - o Kartu Kredit GE
 - o Sumber Kredit
 - o Citibank Ready Cash
 - o Telkomsel (postpaid)
 - o Kidsport
 - o STIE Perbanas
 - o Bina Sarana informatika
 - o Kabelvision
 - o Indosatnet
5. Pembelian Voucher Simpati Telkomsel
6. Pembukaan Rekening :

- o Tabungan
 - o Giro
 - o Deposito
 - o Kartu Kredit
7. Pemesanan Buku Cek/BG
 8. Perubahan Alamat Rekening atau Email
 9. Informasi aktifitas nasabah di internet banking
 10. Informasi Biaya
 11. Informasi Kurs
 12. Informasi Suku Bunga
 13. Simulasi Deposito
 14. Simulasi Pinjaman
 15. Kirim/Baca Pesan Bank Niaga
 16. Perubahan Password

Saatnya anda jelajahi era perbankan tanpa batas. Untuk informasi lebih lanjut silakan kunjungi cabang Bank Niaga terdekat atau hubungi Niaga Access di nomor 14041 dengan pulsa lokal dari seluruh Indonesia .

<http://www.bank2home.com/bankniaga/demo/formulir.html>

Untuk menggunakan Bank **NIAGA Global@ccess** Internet Banking:

1. Anda harus sudah mempunyai rekening Tabungan atau rekening Giro di Bank Niaga, dan juga mempunyai alamat e-mail di internet
2. Datang ke salah satu cabang Bank Niaga yang terdekat untuk mendapatkan formulir aplikasi
3. Isi formulir aplikasi tersebut, dimana anda juga akan diminta untuk menentukan rekening-rekening yang ingin dihubungkan ke Internet Banking
4. Setelah menyerahkan formulir ke customer representative Bank Niaga, anda akan menerima password anda dalam amplop yang tertutup
5. User ID anda akan dikirim ke alamat e-mail yang anda tentukan di formulir aplikasi dalam sekitar dua hari kerja.
6. Jika anda ada pertanyaan lebih lanjut, mohon hubungi **NIAGA Access** di 14041.

Terima kasih.

In order to use the Bank **NIAGA Global@ccess** Internet Banking service:

1. You need to have a Savings account or a Current account at Bank Niaga. You also need to have an internet e-mail address.
2. Please visit the nearest Bank Niaga branch to obtain the application form.
3. Fill-in the application form. In the form, you will be asked to specify the account(s) to be linked to the Internet Banking service.
4. After giving the completed application form to the customer representative at the Bank Niaga branch, you will be given your password in a sealed envelope.
5. Your User ID will be sent to the e-mail address that you specify in the application form in about two business days.
6. If you have any further questions, please contact **NIAGA Access** at 14041.

Thank you.

Home

<https://secure.bank2home.com/appniaga/login.jsp>

1. **Apakah yang dimaksud dengan NIAGA GLOBAL@CCESS ?**

NIAGA GLOBAL@CCESS adalah suatu cara baru untuk melakukan transaksi perbankan dengan menggunakan jaringan internet yang memudahkan anda untuk selalu dapat berinteraksi dengan Bank Niaga dimana pun berada dengan aman dan mudah.

[Kembali ke atas](#)

2. **Amankah menggunakan NIAGA GLOBAL@CCESS ?**

Ya, **NIAGA GLOBAL@CCESS** didisain dengan mengutamakan keamanan informasi pribadi dan keuangan anda.

- **NIAGA GLOBAL@CCESS** menggunakan program Internasional Internet Standard Security SSL 3.0 dengan sistim enkripsi 128-bit, suatu sistim pengacak informasi yang terancang saat ini, sehingga informasi pribadi & keuangan anda tidak dapat terbaca ketika melalui jaringan internet.
- Anda juga akan diberikan User ID & Password yang unik, sehingga tidak ada duplikasi dan hanya anda yang mengetahuinya. Setiap kali Login, anda hanya diperkenankan mengulang User ID & Password yang salah sebanyak 3 kali sebelum akses tersebut diblokir untuk mencegah penyalahgunaan yang tidak bertanggung jawab.
- Setiap transaksi yang diinstruksikan tidak akan diproses tanpa konfirmasi dan persetujuan anda.
- Setiap transaksi akan diberikan nomor referensi yang digunakan apabila ada pertanyaan atau terjadi suatu masalah yang berhubungan dengan transaksi tersebut.
- Jika tidak terdapat aktivitas selama 5 menit, system secara otomatis akan mengakhiri (log-out) akses anda untuk mencegah penyalahgunaan yang tidak berwenang.

[Kembali ke atas](#)

3. **Apakah saya harus mendaftar untuk menggunakan fasilitas NIAGA GLOBAL@CCESS ? Bagaimana caranya ?**

Ya.

- Anda harus memiliki rekening tabungan/giro terlebih dahulu di Bank Niaga.
- Anda harus mengisi aplikasi **NIAGA GLOBAL@CCESS** yang tersedia di semua cabang Bank Niaga.
- Menentukan rekening mana saja yang akan dihubungkan dengan **NIAGA GLOBAL@CCESS**, kecuali rekening bersama & kartu kredit.
- Anda akan langsung diberikan amplop yang berisi password yang digunakan untuk login.
- Dalam waktu 5-10 hari kerja, User ID akan dikirimkan ke alamat email anda yang telah terlebih dahulu dimiliki.

[Kembali ke atas](#)

4. **Apakah yang dimaksud dengan USER ID ?**

- User ID adalah serangkaian angka yang merupakan tanda pengenal anda untuk dapat mengakses **NIAGA GLOBAL@CCESS**

- User ID akan dikirimkan ke email anda dalam waktu 5 sampai 10 hari setelah permohonan anda untuk menggunakan **NIAGA GLOBAL@CCESS** disetujui
- Anda tidak diperkenankan merubah User ID anda
- Jangan memberitahukan User ID anda kepada orang lain, **kecuali kepada petugas NIAGA ACCESS (Call Centre) ketika anda menghubungi call centre tersebut**

Kembali ke atas

5. **Apakah yang dimaksud dengan Password ?**
- Password adalah serangkaian huruf dan angka yang merupakan sandi anda untuk dapat mengakses **NIAGA GLOBAL@CCESS**
 - Password anda akan langsung diberikan ketika permohonan anda untuk menggunakan **NIAGA GLOBAL@CCESS** disetujui
 - Anda diperkenankan merubah Password anda
 - Jangan memberitahukan Password anda ke orang lain, **termasuk petugas NIAGA ACCESS (Call Centre) ketika anda menghubungi Call Centre tersebut.**

Kembali ke atas

6. **Apakah yang dimaksud dengan LOGIN ?**

Login adalah suatu fungsi dimana anda harus memasukkan User ID & Password anda sebelum anda dapat mengakses **NIAGA GLOBAL@CCESS**.

Kembali ke atas

7. **Apakah yang dimaksud dengan LOGOUT ?**

Logout adalah suatu fungsi untuk mengakhiri akses anda dengan **NIAGA GLOBAL@CCESS** dengan sempurna

Kembali ke atas

8. **Bagaimana cara "login" ke NIAGA GLOBAL@CCESS ?**

- Masuk ke :
 - www.bankniaga.com, klik "Login" pada icon **NIAGA GLOBAL@CCESS**
- ATAU
- www.bank2home.com, klik "Login" pada icon **NIAGA GLOBAL@CCESS**
 - Layar selanjutnya adalah layar login **NIAGA GLOBAL@CCESS**. Periksa alamat yang tertera pada kolom Address pada sebelah atas browser Anda. Alamat yang benar adalah <https://secure.bank2home.com/appniaga/login.jsp> Jangan masukkan User ID & Password Anda bila alamat bukan seperti yang tertera di atas.
 - Masukkan [USER ID] dan [PASSWORD].
 - Pilih bahasa yang akan digunakan pada pilihan [BAHASA]
 - Klik [LOGIN] untuk mengakses menu/fasilitas yang tersedia di **NIAGA GLOBAL@CCESS**
 - Sebelum anda menggunakan fasilitas **NIAGA GLOBAL@CCESS**, pastikan anda membaca Syarat & Ketentuan penggunaan **NIAGA GLOBAL@CCESS**.

- Jika ini merupakan login pertama anda, anda diharuskan mengganti password anda.
- Dalam layar perubahan password :
 - Ketik password lama ke dalam kotak **[MASUKKAN PASSWORD LAMA]**.
 - Ketik password baru ke dalam kotak **[MASUKKAN PASSWORD BARU]** Ketentuan Password baru adalah sebagai berikut :
 - Harus terdiri dari minimal 6 karakter, dengan setidaknya 1 huruf besar, 1 huruf kecil, dan 1 angka (Contoh : Bogor1).
 - Tidak boleh sama dengan password lama.
 - Tidak boleh sama dengan USER ID.
 - Tidak boleh mengandung spasi di depan, tengah & belakang.
- Ketik kembali password baru di kotak **[KONFIRMASI PASSWORD BARU]**.
- Klik **[UBAH]** untuk mengkonfirmasi password baru, atau **[HAPUS]** untuk menghapus semua data yang telah diketik sebelumnya.

Kembali ke atas

9. **Bila saya tidak ingat kode USER ID atau Password saya, apa yang harus saya lakukan ?**

- Bila anda tidak ingat User ID anda tapi masih mengingat password anda, silakan menghubungi NIAGA ACCESS (Call Centre) di nomor 14041 atau 62-21-14041 jika anda berada diluar negeri. User ID anda akan dikirimkan melalui email dalam waktu 5-10 hari kerja
- Bila anda tidak ingat Password anda, tapi masih mengingat User ID anda, segera kunjungi cabang Bank Niaga terdekat untuk mendapatkan password yang baru
- Bila anda tidak ingat User ID & Password anda, segera kunjungi cabang Bank Niaga terdekat

Kembali ke atas

10. **Saya kehilangan amplop Password saya. Apa yang harus saya lakukan ?**

Segera laporkan kehilangan tersebut pada NIAGA ACCESS (Call Centre) di nomor 14041 atau 62-21-14041 jika anda berada diluar negeri dengan menyebutkan User ID. Akses anda akan diblokir sementara. Segera kunjungi cabang Bank Niaga terdekat untuk mendapatkan password yang baru

Kembali ke atas

11. **Beberapa waktu yang lalu saya telah mendapatkan User ID & Password untuk mengakses NIAGA GLOBAL@CCESS, tapi saya belum sempat menggunakannya. Mengapa ketika saya memasukkan User ID & Password sistim menolak akses saya ?**

Hal tersebut dapat disebabkan oleh kebijakan pengamanan kami, dimana bila anda tidak menggunakan User ID selama 45 hari sejak User ID dikeluarkan, akses anda tersebut akan diblokir sementara. Untuk dapat mengakses NIAGA GLOBAL@CCESS, silakan anda menghubungi NIAGA ACCESS Call Centre di nomor 14041 atau 62-21-14041 jika anda berada diluar negeri

Kembali ke atas

http://www.bankniaga.com/niagatainment/niagatips_detail.asp?id=TN00000004

Tips Keamanan Niaga Global@ccess

1. Hindari penggunaan Niaga Global@ccess dari komputer-komputer yang diakses secara publik (Warnet, dll)
2. Niaga Global@ccess menggunakan program Internasional Internet Standard Security SSL 3.0 dengan sistem enkripsi 128-bit, suatu sistem pengacak informasi yang terancang saat ini, sehingga informasi pribadi & keuangan anda tidak dapat terbaca ketika melalui jaringan internet. Anda bisa melihat tanda kunci gembok pada bagian bawah menu bar di setiap halaman Niaga Global@ccess. Arahkan mouse Anda pada gambar tersebut, Anda akan menemukan tulisan SSL Secured (128-bit).
3. Situs Niaga Global@ccess dijaga keamanannya oleh Verisign yaitu lembaga sekuriti internet internasional. Hal ini dapat dilihat dari logo Verisign di halaman login Niaga Global@ccess. Bila Anda klik logo Verisign, akan muncul Sertifikat yang menerangkan nama situs dimana logo Verisign tersebut berada, dalam hal ini Secure.Bank2Home.Com, dan masa berlakunya. Situs yang terjamin keamanannya seperti Niaga Global@ccess mempunyai sertifikat yang masih valid masa berlakunya.
4. Pada saat Anda login, sebelum Anda memasukkan User ID dan Password Niaga Global@ccess, pastikan bahwa alamat URL Login Niaga Global@ccess adalah <https://secure.bank2home.com/appniaga/login.jsp>. Alamat ini dapat dilihat di kolom Address atau Location pada sebelah atas browser Anda. Jangan memasukkan User ID dan Password Anda bila alamat login Niaga Global@ccess bukan seperti di atas.

Untuk memudahkan Anda, Anda dapat memasukkan Halaman Login ini sebagai menu Favorites dengan cara berikut ini :
Untuk pengguna Microsoft Internet Explorer
 - Ketika browser Anda berada pada halaman Login Niaga Global@ccess seperti yang tertera di atas, klik Favorites pada sebelah atas menu bar browser Anda.
 - Pilih Add to Favorites
 - Otomatis browser akan menyimpan halaman login ini dengan nama "Welcome to Bank Niaga - Bank2Home Internet Banking"
 - Klik tombol OKUntuk pengguna Netscape Communicator/Navigator
 - Ketika browser Anda berada pada halaman Login Niaga Global@ccess seperti yang tertera di atas, klik Communicator (atau Windows pada Netscape Navigator) pada sebelah atas menu bar browser Anda
 - Klik Bookmarks
 - Pilih Add Bookmarks
 - Otomatis Netscape akan menyimpan halaman login ini dengan nama "Welcome to Bank Niaga - Bank2Home Internet Banking"
6. Untuk selanjutnya bila Anda ingin mengakses situs Niaga Global@ccess, Anda cukup memilih dari menu Favorites/Bookmarks Anda
7. Ingatlah Password Anda, jangan menuliskannya di suatu tempat atau memberitahukannya kepada orang lain, termasuk kepada staff Bank Niaga. Gantilah password anda secara berkala, dengan ketentuan minimal terdiri dari 6 karakter, dengan kombinasi setidaknya 1 huruf besar, 1 huruf kecil dan 1 angka. Password sebaiknya sesuatu yang mudah diingat namun tidak mudah ditebak oleh orang lain (misalnya tanggal lahir Anda dapat dengan mudah diketahui oleh orang lain).

http://www.klikbca.com/website/indo/consumer_banking/internet_banking.html

Klik BCA

BCA menawarkan produk perbankan elektronik berupa KlikBCA, yang memberikan Anda kemudahan untuk melakukan transaksi perbankan melalui komputer dan jaringan internet.

KlikBCA adalah layanan perbankan yang mudah, praktis, aman dan gampang digunakan.

Mudah

Tinggal datang saja ke ATM BCA untuk Registrasi Internet dan mendapatkan user ID serta PIN Internet Banking yang dapat langsung dipakai untuk login (masuk) ke KlikBCA di <http://www.klikbca.com>.

Praktis

Anda dapat langsung melakukan transaksi perbankan melalui internet tanpa mesti repot ke bank atau ATM BCA (kecuali untuk ambil uang tunai).

Aman

KlikBCA dilengkapi dengan security untuk menjamin keamanan dan kerahasiaan data dan transaksi yang Anda lakukan. Untuk menambah keamanan, ia juga dilengkapi dengan **KeyBCA**, yaitu alat pengaman tambahan untuk lebih mengamankan transaksi finansial di KlikBCA. Alat ini berfungsi untuk mengeluarkan password yang selalu berganti setiap kali Anda melakukan transaksi finansial. Dengan demikian, keamanan Anda bertransaksi akan makin terjaga.

Gampang Digunakan

Layar KlikBCA dirancang seperti layar ATM BCA sehingga begitu mudah, dan tidak perlu ketrampilan khusus untuk menggunakannya.

Kegiatan-kegiatan yang dapat Anda lakukan dengan KlikBCA

Transaksi yang Anda dapat lakukan melalui ATM BCA, dapat dilakukan melalui KlikBCA, kecuali penarikan tunai. Dengan begini, Anda seperti memiliki ATM BCA pribadi pada PC Anda.

1. **Pembelian** (Pulsa Isi Ulang, Saham, Tiket)
2. **Pembayaran** (Kartu Kredit, Internet, Telepon, Handphone, Pager, Pendidikan, dan Lain-lain)
3. **Transfer Dana** (Transfer ke Rekening BCA)
4. **Informasi Rekening** (Informasi Saldo, Mutasi Rekening, Tagihan BCA Card)
5. **Transaksi Histori**
6. **Administrasi** (Ganti PIN, Ubah Bahasa, Ganti Alamat Email, Hapus Daftar Pembayaran, Hapus Daftar Transfer, Registrasi KeyBCA, Tambah Koneksi KeyBCA, Hapus Koneksi KeyBCA, Aktivasi KeyBCA, Registrasi Informasi BCA Card, Hapus Informasi BCA Card)

Limit Transfer

Dengan KeyBCA Anda dapat melakukan pemindahan dana rekening di BCA hingga 100 juta setiap hari.

http://www.klikbca.com/website/indo/consumer_banking/ib_termandcondition.html

Klik BCA

Syarat dan Ketentuan Internet Banking (IB) BCA

Registrasi Internet Banking BCA

- Setiap Nasabah yang menyimpan dana di BCA dan mempunyai kartu yang dapat digunakan untuk melakukan transaksi perbankan di ATM BCA ("Nasabah") berhak untuk menikmati fasilitas IB BCA.
- Untuk dapat menggunakan fasilitas IB BCA, Nasabah harus memiliki identitas pengguna IB BCA ("User ID") dan nomor identifikasi pribadi IB BCA ("PIN") yang diperoleh pada saat Nasabah melakukan registrasi di mesin ATM BCA.
- User ID yang diberikan oleh BCA bersifat permanen dan tidak dapat diubah kecuali Nasabah mengganti kartu yang dapat digunakan untuk melakukan transaksi perbankan di ATM BCA ("Kartu ATM BCA") karena rusak/hilang.

Transaksi Menggunakan Internet Banking (IB) BCA

- Untuk melakukan transaksi finansial melalui IB BCA, Nasabah harus memiliki KeyBCA.
- Nasabah harus mengisi semua data yang dibutuhkan untuk setiap transaksi secara benar dan lengkap.
- Pada setiap transaksi finansial, sistem akan selalu melakukan konfirmasi terhadap data yang diinput Nasabah dan Nasabah mempunyai kesempatan untuk membatalkan data tersebut dengan menekan tombol "Batal".
- Nasabah selain menginput User ID dan PIN wajib pula menginput angka yang dihasilkan dari KeyBCA sebagai tanda persetujuan atas instruksi transaksi finansial.
- Setiap informasi yang mendapat konfirmasi 'Submit' atau 'Kirim' dari Nasabah yang tersimpan dalam pusat data BCA merupakan data yang benar yang diterima sebagai bukti atas instruksi dari Nasabah kepada BCA untuk melakukan transaksi yang dimaksud, kecuali Nasabah dapat membuktikan sebaliknya.
- BCA menerima dan menjalankan setiap instruksi dari Nasabah sebagai instruksi yang sah berdasarkan penggunaan User ID, PIN dan KeyBCA dan untuk itu BCA tidak mempunyai kewajiban untuk meneliti atau menyelidiki keaslian maupun keabsahan atau kewenangan pengguna User ID, PIN dan KeyBCA atau menilai maupun membuktikan ketepatan maupun kelengkapan instruksi dimaksud, dan oleh karena itu instruksi tersebut sah mengikat Nasabah dengan sebagaimana mestinya, kecuali Nasabah dapat membuktikan sebaliknya.
- Nasabah tidak dapat membatalkan semua transaksi yang diinstruksikan kepada BCA yang telah mendapat konfirmasi 'Submit' atau 'Kirim' dari Nasabah, karena dalam waktu yang sama BCA langsung memproses instruksi tersebut.
- Untuk setiap instruksi dari Nasabah atas transaksi yang berhasil dilakukan oleh BCA, Nasabah akan mendapatkan bukti transaksi berupa nomor referensi sebagai bukti transaksi tersebut telah dilakukan oleh BCA.
- BCA berhak untuk tidak melaksanakan instruksi dari Nasabah, jika saldo Nasabah di BCA tidak mencukupi.
- Nasabah wajib dan bertanggung jawab untuk memastikan ketepatan dan kelengkapan instruksi transaksi. BCA tidak bertanggung jawab terhadap segala akibat apapun yang timbul karena ketidaklengkapan, ketidakjelasan data atau ketidaktepatan instruksi dari Nasabah.

Kurs

- Penukaran valuta asing, suku bunga dan kurs yang lain termasuk (namun tidak terbatas pada) kutipan bursa yang disediakan di IB BCA hanya merupakan indikasi dari kurs,

kutipan atau informasi yang sebenarnya dan dapat diubah sewaktu-waktu oleh BCA tanpa pemberitahuan terlebih dahulu.

Pembuktian

- Setiap instruksi transaksi finansial dari Nasabah yang tersimpan pada pusat data BCA dalam bentuk apapun, termasuk namun tidak terbatas pada catatan, tape/cartridge, print out komputer, komunikasi yang ditransmisi secara elektronik antara BCA dan Nasabah, merupakan alat bukti yang sah, kecuali Nasabah dapat membuktikan sebaliknya.
- Nasabah menyetujui semua komunikasi dan instruksi dari Nasabah yang diterima oleh BCA merupakan alat bukti yang sah meskipun tidak dibuat dokumen tertulis ataupun dikeluarkan dokumen yang ditandatangani.

User ID, PIN, KeyBCA dan Kewajiban Nasabah

- Nasabah wajib tidak meninggalkan terminal dalam keadaan aktif (log-on) dengan kata lain harus melakukan logout setiap kali meninggalkan terminal.
- Nasabah wajib mengamankan User ID dan PIN dengan cara :
 - Tidak memberitahukan User ID dan PIN kepada orang lain untuk mendapatkan hadiah atau tujuan lainnya termasuk kepada anggota keluarga atau sahabat.
 - Tidak menuliskan User ID dan PIN pada meja, terminal atau menyimpannya dalam bentuk tertulis atau pada aplikasi komputer atau sarana penyimpanan lainnya yang memungkinkan untuk diketahui oleh orang lain.
 - User ID dan PIN harus digunakan dengan hati-hati agar tidak terlihat oleh orang lain.
 - Tidak menggunakan PIN Internet Banking yang diberikan oleh orang lain atau yang mudah diterka seperti tanggal lahir atau kombinasinya, nomor telepon dan lain-lain.
 - Menggunakan komputer pribadi dalam mengakses IB BCA. Tidak menggunakan komputer yang diakses oleh banyak orang.
- User ID yang diberikan oleh BCA bersifat permanen dan tidak dapat diubah kecuali Nasabah mengganti Kartu ATM BCA karena rusak atau hilang.
- Nasabah diberikan kebebasan untuk membuat PIN-nya sendiri pada saat registrasi di mesin ATM BCA.
- Nasabah dapat melakukan inquiry User ID-nya sendiri melalui fasilitas registrasi IB BCA di mesin ATM BCA, apabila Nasabah tidak mengingat User ID-nya.
- Nasabah bertanggung jawab sepenuhnya terhadap semua instruksi transaksi yang terjadi berdasarkan penggunaan User ID dan PIN yang dimiliki oleh Nasabah, kecuali Nasabah dapat membuktikan sebaliknya.
- BCA berhak untuk memberikan User ID dengan kombinasi huruf dan angka tanpa harus mendapatkan persetujuan terlebih dahulu dari Nasabah.
- Nasabah wajib untuk segera memberitahukan kepada BCA apabila User ID dan atau PIN tersebut telah diketahui oleh orang lain. Segala instruksi transaksi berdasarkan penggunaan User ID, PIN dan KeyBCA yang terjadi sebelum pejabat yang berwenang dari BCA menerima secara tertulis laporan tersebut merupakan tanggung jawab sepenuhnya dari Nasabah.

Limit

- Berikut ini adalah Limit transaksi finansial :

Keterangan	Besar
Transfer dari Rupiah ke Rupiah	Rp. 100 juta per hari per User ID.
Transfer dari Rupiah ke Valas	Ekuivalen Rp. 1 juta per hari per User ID (merupakan bagian dari limit Rp. 100 juta)

Transfer dari Valas ke Rupiah	Ekuivalen Rp. 100 juta per hari per User ID
Transfer dari Valas ke Valas yang sama	
Pembayaran	Sesuai dengan tagihan
Pembelian Pulsa Isi Ulang	Rp. 1,1 juta per hari per User ID (termasuk PPN). Limit ini merupakan limit gabungan pembelian pulsa isi ulang di ATM/Mobile Banking/Pulsa Isi Ulang via SMS.

- Limit transaksi tersebut merupakan limit yang terpisah dari limit Kartu ATM BCA yang digunakan untuk melakukan registrasi IB BCA di mesin ATM BCA, BCA atas pertimbangannya sendiri berhak setiap saat untuk mengubah besar limit untuk setiap transaksi.

Electronic Mail ("E-MAIL")

- Alamat E-Mail yang didaftarkan oleh Nasabah pada saat login pertama kali di IB BCA digunakan oleh BCA untuk mengirim informasi transaksi yang telah dilakukan oleh Nasabah melalui IB BCA.
- BCA hanya mengirimkan informasi kepada alamat E-Mail yang telah dikonfirmasi kebenarannya oleh Nasabah kepada BCA dan BCA tidak bertanggung jawab atas kebenaran alamat E-Mail tersebut.
- BCA tidak menjamin keamanan informasi atau data yang dikirim kepada BCA melalui E-Mail yang tidak terdapat di IB BCA, yang tidak dalam format yang aman yang disetujui atau ditentukan oleh BCA.

Biaya & Kuasa Debet Rekening

- BCA berhak untuk mendebet biaya administrasi bulanan dan biaya transaksi yang dibebankan atas penggunaan fasilitas IB BCA dan transaksi yang dilakukan melalui IB BCA.
- Bank berhak atas pertimbangannya sendiri untuk mengubah, menambah atau menarik biaya-biaya yang dibebankan kepada Nasabah atas penggunaan fasilitas IB BCA.
- Nasabah dengan ini memberikan kuasa kepada BCA untuk mendebet rekening Nasabah di BCA atas semua transaksi yang diinstruksikan Nasabah kepada BCA melalui IB BCA dan untuk pembayaran biaya administrasi bulanan serta biaya transaksi atas penggunaan fasilitas IB BCA.
- Kuasa ini akan berakhir apabila segala kewajiban Nasabah kepada BCA sudah terpenuhi.

Pemblokiran User ID dan PIN Internet Banking

- User ID dan PIN Nasabah akan diblokir jika melakukan hal berikut :
 - Salah memasukkan PIN sebanyak 3 kali berturut-turut pada saat login.
 - Salah memasukkan angka dari KeyBCA sebanyak 3 kali berturut-turut pada saat melakukan transaksi finansial.
 - Mengajukan penggantian Kartu ATM BCA dan atau dilaporkan Kartu ATM BCA hilang.
 - User ID dan atau PIN dilaporkan telah diketahui oleh orang lain.
 - Hasil penelitian BCA mengindikasikan adanya kemungkinan User ID dan PIN Nasabah telah diketahui oleh orang lain.
- Apabila terjadi pemblokiran User ID dan PIN, Nasabah harus menghubungi Halo BCA dan melakukan registrasi IB BCA ulang di mesin ATM BCA.
- Pada saat Nasabah mendapat Kartu ATM BCA baru, Nasabah harus melakukan registrasi IB BCA ulang di mesin ATM BCA.

Force Majeure

Nasabah akan membebaskan BCA dari segala tuntutan apapun, dalam hal BCA tidak dapat melaksanakan instruksi dari Nasabah baik sebagian maupun seluruhnya karena kejadian-kejadian atau sebab-sebab diluar kekuasaan atau kemampuan BCA, termasuk namun tidak terbatas pada bencana alam, perang, huru-hara, keadaan peralatan, sistem atau transmisi yang tidak berfungsi, gangguan listrik, gangguan telekomunikasi, kebijaksanaan pemerintah, serta kejadian-kejadian atau sebab-sebab lain diluar kekuasaan atau kemampuan BCA.

Pengakhiran Layanan

Layanan IB BCA akan berakhir jika Nasabah mengakhiri penggunaan Kartu ATM BCA atau menutup semua rekening yang terhubung di Kartu ATM BCA.

Ketentuan KeyBCA

Nasabah dengan ini terikat dan tunduk pada ketentuan-ketentuan KeyBCA yang diatur oleh BCA dan segala perubahannya dalam bentuk apapun yang akan diberitahukan kepada Nasabah melalui sarana apapun.

ONLINE PRIVACY AND SECURITY

Berikut ini adalah kebijakan dan praktek yang dilakukan PT Bank Central Asia, Tbk ("BCA")

untuk menunjukkan komitmen BCA di dalam memelihara *online privacy and security* Anda pada saat Anda mengunjungi website dan internet banking BCA.

BCA menggunakan teknologi enkripsi Secure Socket Layer (SSL) 128 bit untuk memproteksi komunikasi

antara komputer Anda dan serverBCA selama Anda mengakses internet banking BCA.

Untuk memastikan proteksi Anda, silakan lakukan hal-hal sebagai berikut:

- Periksa sertifikat secara teratur untuk memastikan bahwa Anda menerima sertifikat yang sah yang telah terregistrasi untuk IBANK.KLIKBCA.COM.
- Apabila Anda menerima pesan yang menjelaskan bahwa sertifikat tidak sah, dimohon Anda **tidak melanjutkan**. Pastikan bahwa Anda telah mengetik alamat yang benar.
- Pastikan bahwa di sebelah bawah browser Anda terdapat gambar gembok/kunci yang mengindikasikan bahwa halaman yang Anda akses saat ini dienkripsi menggunakan SSL. Jika Anda tidak melihat gambar gembok/kunci, dimohon Anda untuk **logout** dan **login** kembali.

BCA mewajibkan Anda untuk memasukkan user-ID dan PIN sebelum Anda diperbolehkan mengakses

fasilitas internet banking. Anda juga diwajibkan untuk memasukkan PIN Anda pada saat melakukan

transaksi finansial sebagai tanda persetujuan Anda.

Untuk memastikan proteksi Anda, silakan lakukan hal-hal sebagai berikut:

- Jagalah kerahasiaan user-ID dan PIN Anda, jangan diberitahukan kepada orang lain.
- Jangan beritahukan PIN atau sebagian PIN Anda kepada orang lain, walaupun orang tersebut mengaku sebagai karyawan BCA. BCA **tidak pernah** menanyakan PIN Anda.
- Gantilah PIN Anda secara periodik atau jika Anda tidak yakin terhadap kerahasiaan PIN Anda. Jangan gunakan PIN yang mudah diterka seperti: 111111, 222222, 123456, 654321, tanggal lahir, no. mobil, alamat, dll. Jangan menuliskan PIN Anda di tempat dimana orang lain dapat membacanya.
- Hubungi Halo BCA Jakarta di (021) 52-999-888 jika Anda lupa PIN atau PIN Anda terblokir. Ikuti instruksi mereka bagaimana cara untuk mengaktifkan fasilitas internet banking Anda

kembali.

BCA mewajibkan Anda untuk memberikan alamat email Anda kepada BCA. BCA akan menggunakan alamat email Anda untuk mengirimkan kepada Anda informasi atas transaksi finansial yang telah Anda lakukan melalui internet banking.

Untuk memastikan proteksi Anda, silakan lakukan hal-hal sebagai berikut:

- Berikan kepada BCA alamat email **pribadi** Anda. Jangan menggunakan alamat email palsu.
- Ubahlah segera alamat email Anda di internet banking jika Anda mengganti alamat email Anda.
- Jika Anda menghubungi BCA melalui email, jangan kirimkan informasi rekening yang sifatnya rahasia atau sensitif termasuk namun tidak terbatas pada PIN Anda, melalui email Anda tersebut.

BCA tidak menjual, menukar atau memperlihatkan segala informasi yang berkaitan dengan nasabah atau pengunjung website BCA. BCA tidak melacak pengunjung website BCA. Selama Anda login ke internet banking, BCA akan menggunakan *cookie* yang akan berakhir pada saat Anda logout.

Semua transaksi perbankan Anda dan informasi rekening lainnya disimpan secara rahasia sesuai dengan hukum dan peraturan Bank Indonesia dan kebijakan pengamanan internal BCA.

Di dalam website BCA, BCA menyediakan *URL link* ke website lain yang tidak dikontrol oleh BCA.

BCA tidak bertanggung jawab atas isi dan keamanan dari website tersebut. Jika Anda mengakses website tersebut, silakan memeriksa *privacy and security policies* mereka. Dalam hal Anda mengakses website atau internet banking BCA melalui URL link dari website lain, pastikan kebenaran alamat yang Anda akses yaitu <http://www.klikbca.com> atau <https://ibank.klikbca.com>.

Karena banyaknya variasi internet browser yang ada, sulit untuk menyediakan internet banking yang mengikuti keamanan masing-masing browser. Saat ini BCA hanya menyediakan sarana internet banking yang lebih cocok diakses dengan menggunakan Microsoft Internet Explorer versi 5 atau terbaru.

BCA mohon maaf atas ketidaknyamanan ini.

BCA dapat merubah kebijaksanaan ini setiap saat untuk tetap menyesuaikan dengan situasi dan teknologi terbaru.

Anda selalu dapat meninjau kebijakan BCA yang terbaru di <https://ibank.klikbca.com/privacy.html> atau Anda dapat memintanya dengan mengirimkan email ke klikbca@bca.co.id

<https://www.bankbii.com/ibank/registration/registration.asp>

Syarat dan Ketentuan

1. Internet Banking Service merupakan tambahan untuk fasilitas service dan product perbankan lainnya yang diberikan oleh BII kepada Nasabah, dengan membolehkan Nasabah untuk melakukan transaksi perbankan melalui media elektronik Internet. Dengan demikian perintah/ instruksi yang diberikan dengan cara apapun kepada Bank mengenai rekening termasuk (namun tidak terbatas pada) perintah/instruksi pendebitan, pemindah-bukuan/transfer, pengakhiran Internet Bankingmaupun instruksi/perintah lainnya berkenaan dengan rekening yang dimaksud, akan berlaku untuk rekening tersebut.
2. Setiap transaksi yang dilakukan melalui Internet Banking Service, instruksi Nasabah tidak akan diterima/dijalankan oleh Bank sebelum Bank dapat memastikan dengan Nasabah, bahwa instruksi Nasabah telah diterima/dijalankan dengan kode transaksi/atau dengan pesan konfirmasi sebagai penegasan pelaksanaan jika demikian halnya.
3. Instruksi Nasabah tidak dapat diubah, bersifat sah dan mengikat Nasabah pada saat transmisi diterima Bank.
4. Nasabah diharuskan memberitahu Bank dengan segera apabila menerima data/informasi yang tidak lengkap / tidak tepat.
5. Nasabah diharuskan memberitahu Bank dengan segera apabila menerima data/informasi yang tidak ditujukan kepadanya. Nasabah menyetujui bahwa data/informasi tersebut akan dihapuskan dari mesin komputernya.
6. Bank menerima dan menjalankan setiap instruksi Nasabah sebagai instruksi/ perintah yang sah, dan untuk itu Bank tidak diharuskan meneliti/menyelidiki keaslian maupun keabsahan/kewenangan pihak-pihak dimaksud/menilai maupun membuktikan ketepatan maupun kelengkapan instruksi dimaksud dan karenanya instruksi/perintah tersebut sah mengikat Nasabah dengan sebagaimana mestinya. Segala resiko yang timbul sebagai akibat dari kesalahan/kekeliruan, pemalsuan, penipuan, kelalaian, kesalahpahaman/ketidak-jelasan instruksi/perintah tersebut menjadi resiko dan tanggung jawab Nasabah sepenuhnya dan Bank dibebaskan dari segala akibat yang timbul karenanya tanpa kecuali apapun juga.
7. Bank tidak diharuskan menjalankan setiap instruksi Nasabah dan berhak membatalkannya tanpa mempertanggungjawabkannya jika :
 - a. Dana direkening Bank mencukupi atau fasilitas kredit yang diberikan kepada Nasabah tidak memadai.
 - b. Pelaksanaan instruksi Nasabah akan menyebabkan saldo dalam rekening melewati batas kredit.
 - c. Bank mengetahui/mempunyai alasan untuk menyangka bahwa penipuan, aksi atau pelanggaran kriminal telah/akan dilakukan.
8. Bank berhak tanpa memberi peringatan untuk tidak menjalankan atau membatalkan instruksi Nasabah pada setiap saat tanpa memberi alasan dan tanpa mempertanggungjawabkannya.
9. Nasabah bertanggung jawab untuk memastikan ketepatan dan kelengkapan instruksi Nasabah. Bank tidak akan bertanggung jawab terhadap akibat ketidaklengkapan, kecacauan atau ketidaktepatan instruksi Nasabah.
10. Nasabah harus sering memeriksa peringatan untuk tidak menjalankan atau membatalkan instruksi Nasabah-nya yang telah diproses atau sedang diproses oleh Bank.
11. Jika jumlah keseluruhan dana dalam transaksi yang tertera didalam instruksi Nasabah melebihi saldo dalam rekening atau fasilitas kredit yang diberikan kepada Nasabah, Bank berhak memutuskan apakah instruksi Nasabah akan dilaksanakan dan jika begitu bagian dari instruksi mana yang akan dijalankan dengan sepenuhnya atau tidak, dengan mengabaikan tanggal atau waktu pengiriman dan penerimaan instruksi Nasabah. Dalam hal Bank telah menjalankan instruksi tersebut, namun ternyata dana Nasabah tidak mencukupi, maka Nasabah berkewajiban untuk segera menutupi selisih kekurangan dana dimaksud pada saat diberitahukan oleh Bank.
12. Bank tidak berkewajiban untuk membatalkan atau mengubah pembayaran atau instruksi/perintah tersebut telah dikirimkan ke Bank. Bank akan berusaha sedapat mungkin untuk memenuhi permintaan Nasabah untuk dikirimkan pembatalan atau pengubahan sebelum Bank menjalankan instruksi tersebut, tetapi tidak bertanggung jawab atas segala akibat yang timbul jika pembatalan atau pengubahan tersebut tidak

dilaksanakan.

Bank juga tidak bertanggung jawab atas kesalahan/kekeliruan instruksi yang diberikan dan dilaksanakan oleh Bank, segala resiko dan akibat yang timbul menjadi beban dan tanggung jawab Nasabah sepenuhnya.

13. Dalam hal Nasabah memiliki lebih dari satu rekening, Nasabah dengan ini menyatakan menunjuk dan memberi kuasa kepada Bank untuk menghubungi rekening yang akan dipakai di Internet Banking Service.
14. Nasabah harus merahasiakan password dan Login ID dan Kode lainnya yang diberikan untuk memungkinkan Nasabah mengakses Internet Banking Service dan Nasabah harus bertanggung jawab atas semua instruksi Nasabah yang berlaku (yang disahkan atau tidak) melalui pemakaian Password, Login ID dan Kode tersebut.
15. Bank mempunyai wewenang untuk membagikan kombinasi yang terdiri dari huruf dan/atau nomor untuk Password, Login ID dan Kode.
16. Nasabah setuju untuk mengambil tindakan pencegahan untuk menjaga Password, Login ID dan Kode seperti (namun tidak terbatas pada) tidak memberitahunya kepada orang lain, sering mengganti Password, memusnahkan secepatnya kertas Password, Login ID dan Kode setelah menerimanya, mengingat Password dan Kode-kode dan tidak menuliskannya, memberitahukan Bank dengan segera apabila ada kecurigaan tentang Password, Login ID dan Kode diketahui oleh orang lain untuk mencegah penipuan dan pemakaian rekening yang tidak diizinkan. Nasabah bertanggung jawab penuh atas segala resiko atau akibat yang timbul karena penggunaan Password, Login ID dan/atau Kode-kode apapun dan Bank dibebaskan dari segala tuntutan apapun termasuk kerugian yang diderita oleh Nasabah (bila ada) yang timbul sebagai akibat dari kejadian-kejadian diatas.
17. Bank atas kebijaksanaan berhak menonaktifkan atau mencabut pemakaian Password, Login ID dan Kode kapan saja tanpa penjelasan apapun dan tanpa memberi tahu Nasabah dahulu.
18. Nasabah akan tetap terikat terhadap semua tanggung jawab menurut instruksi Nasabah yang sudah diterima Bank setelah Password, Login ID dan Kode diberitahukan kepada orang lain, sampai Bank mengambil langkah-langkah yang perlu sesuai dengan praktek yang berlaku untuk mencegah instruksi Nasabah dari pengaruh melalui pemakaian Password, Login ID dan Kode.
19. Bank berhak mengirim Password, Login ID dan Kode kepada Nasabah dengan cara apapun dan Nasabah tidak berhak untuk menuntut atau meminta pertanggungjawaban Bank, jika Password, Login ID dan Kode tidak sampai ke Nasabah setelah dikirim oleh Bank atau jika dalam perjalanan Password, Login ID dan Kode diketahui dan dimanfaatkan oleh orang-orang yang tidak berhak.
20. Nasabah boleh menginstruksikan pembayara, merencanakan pembayaran cicilan dalam jangka waktu tertentu dan boleh membatalkan atau mengubah pembayaran tersebut jika Nasabah mengikuti semua petunjuk dan syarat yang boleh ditentukan Bank dari waktu ke waktu, termasuk (namun tidak terbatas pada) batas waktu dan periode tertentu untuk pemberitahuan awal sebelum instruksi Nasabah dikirim kepada Bank untuk mempengaruhi sebuah transaksi. Bank berhak mengubah prosedur atau cara pengiriman instruksi Nasabah untuk jasa pembayaran tersebut pada setiap saat tanpa memberikan alasan dan tanpa mempertanggungjawabkannya.
21. Bank berhak untuk membebaskan biaya atas jasa pelayanan pembayaran untuk suatu jumlah/tarif, baik untuk jangka waktu reguler atau per transaksi dan jika ditentukan untuk suatu jangka waktu reguler, maka jangka waktu tersebut akan ditentukan oleh Bank. Dan jumlah tersebut merupakan kewajiban Nasabah untuk membayarnya kepada Bank.
22. Bank tidak bertanggung jawab atas suatu tuntutan, permintaan, cara kerja atau kerugian Nasabah yang mungkin terjadi atau timbul maupun diderita oleh Nasabah yang disebabkan karena :
 - a. Keterlambatan pembayaran yang timbul karena Nasabah tidak mengikuti petunjuk dan syarat Bank dalam melakukan pembayaran melalui Internet Banking Service.
 - b. Kelalaian pihak ketiga melalui pihak manapun pembayaran tersebut ditransmisi untuk yang ditujukan.
 - c. Penolakan atau Kelalaian Bank untuk mengubah pembayaran tersebut dengan alasan adanya perintah pengadilan atau pemberitahuan, permintaan atau perintah yang dikeluarkan menurut Undang-Undang atau Regulasi Hukum (apakah dilindungi oleh Undang-Undang atau tidak, dan jika tidak, penyesuaian dengan

Tata Krama berlaku dengan kelompok orang-orang kepada siapa pemberitahuan, permintaan, instruksi atau perintah ditujukan)

23. Internet Banking Service adalah sebuah jasa/media untuk mengirimkan instruksi Nasabah, yang mensuplemen produk dan fasilitas Bank yang ada. Dengan demikian, pengakhiran Internet Banking Service dimana instruksi Nasabah akan disimpan. Bank berhak untuk terus menjalankan instruksi Nasabah tersebut. Nasabah boleh mengubah atau menarik kembali instruksi Nasabah tersebut hanya jika Nasabah mengikuti semua instruksi dan syarat-syarat yang akan ditetapkan oleh Bank dari waktu ke waktu, termasuk (namun tidak terbatas pada) batas waktu terakhir dan jangka waktu yang telah ditetapkan untuk pemberitahuan terdahulu sebelum instruksi untuk perubahan atau pembatalan tersebut dikirim kepada Bank.
24. Bank berhak setiap saat menetapkan, mengubah atau membatalkan limit setiap transaksi, fasilitas, jasa dan produk yang bisa digunakan melalui Internet Banking Service, meskipun dalam hal keuangan dan untuk mengubah frekuensi dan periode penyediaannya.
25. Bank berhak setiap saat membatasi, membatalkan atau menghentikan seluruh atau sebagian Internet Banking Service tetap memberikan alasan atau mempertanggungjawabkan apapun kepada Nasabah dan Bank juga berhak untuk setiap saat menambah, menarik kembali atau mengubah tipe/bentuk transaksi yang sudah ada atau yang dapat dilakukan melalui Internet Banking Service.
26. Bank tidak menjamin keamanan informasi atau instruksi apapun atau instruksi yang dikirim kepada Bank melalui jasa e-mail yang terdapat di Internet Banking Web Page, yang tidak dalam format yang aman yang disetujui/ditentukan oleh Bank, dari dan karenanya Bank juga tidak bertanggung jawab atas hal-hal tersebut.
27. Bank tidak diwajibkan untuk melaksanakan setiap instruksi (baik yang ditandatangani atau tidak) atau menjawab pertanyaan apapun yang diterima melalui e-mail yang tidak aman. Nasabah disarankan untuk tidak mengirim informasi rahasia melalui e-mail yang tidak aman.
28. Bank tidak bertanggung jawab atas hilangnya keamanan maupun informasi apapun dalam hal rekening atau kerugian apapun yang diderita atau diakibatkan oleh Nasabah karena Nasabah tidak mengikuti instruksi, prosedur dan petunjuk untuk memakai jasa e-mail atau tidak memakai e-mail yang disetujui oleh Bank.
29. Bank tidak menjamin kebenaran atau ketepatan saran/informasi apapun yang dikirim oleh Bank kepada Nasabah melalui Internet Banking Web Page atau jasa e-mail. Nasabah menyetujui bahwa Nasabah bebas untuk menentukan sendiri langkah-langkahnya dengan memeriksa kebenaran atau ketepatan saran/informasi tersebut sebelum bertindak. Bank tidak bertanggung jawab atas kerugian atau resiko apapun yang diderita oleh Nasabah karena Nasabah percaya atas saran dan informasi tersebut, dan dan karenanya Bank dibebaskan dari segala tuntutan mengenai hal itu.
30. Semua pernyataan atas rekening kepada Bank melalui e-mail yang aman dengan cara yang telah ditetapkan oleh Bank.
31. Semua dan seluruh komunikasi melalui e-mail yang aman dan memenuhi standar serta dianggap sah, otentik, asli dan benar serta memberikan efek yang sama sebagaimana hal tersebut dilakukan secara tertulis dan/atau melalui dokumen komunikasi tertulis.
32. Nasabah setuju untuk tidak membantah keabsahan, kebenaran atau keaslian bukti instruksi Nasabah dan komunikasi yang ditransmisi secara elektronik antara kedua pihak termasuk dokumen dalam bentuk catatan komputer atau buku Transaksi Bank, Magnetic Tape, Cartridge, Print-Out Computer, salinan atau bentuk penyimpanan informasi yang lain dan kesemua alat atau dokumen tersebut merupakan satu-satunya bukti yang sah tentang hal tersebut.
33. Nasabah setuju bahwa Catatan, Tape, Cartridge, Print-Out Computer atau bentuk penyimpanan informasi atau data lain sebagai bukti yang sah atas instruksi Nasabah, demikian juga sarana komunikasi lain yang diterima atau dikirimkan oleh Bank.
34. Semua komunikasi dan instruksi Nasabah tersebut yang memenuhi standar operasi dan syarat Bank akan dianggap sebagai dokumen tertulis yang sah dan/atau dokumen komunikasi yang telah ditandatangani.
35. Penukaran Valuta Asing, Suku Bunga dan Rate yang lain termasuk (namun tidak terbatas pada) kutipan bursa yang disediakan di Internet Banking Service hanya merupakan indikasi dan rate, kutipan atau informasi yang sebenarnya dan dapat diubah sewaktu-waktu oleh Bank tanpa pemberitahuan terlebih dahulu.

36. Jangka waktu dimana Internet Banking Service tersedia dapat diubah. Bank akan berusaha selayaknya untuk memastikan keberadaan Internet Banking Service. Bank berhak menghentikan operasi Internet Banking Service untuk sementara waktu maupun untuk jangka waktu yang ditentukan oleh Bank sendiri untuk memperbaharui, memelihara atau untuk tujuan lain dengan alasan apapun yang dianggap baik oleh Bank dan untuk itu Bank tidak berkewajiban untuk mempertanggungjawabkannya kepada siapapun.
37. Nasabah harus membayar kepada Bank, seluruh dan semua biaya langganan dan biaya-biaya lain berkenaan dengan penggunaan Internet Banking Service dengan jumlah/nilai yang akan ditentukan oleh Bank setiap saat dari waktu ke waktu dan akan diberitahukan kepada Nasabah. Bank berhak untuk membebankan seluruh biaya-biaya tersebut dan mengeluarkannya atas nama Nasabah termasuk untuk langsung melakukan pendebitan rekening Nasabah.
38. Bank berhak atas pertimbangannya sendiri untuk mengubah, menambah atau menarik, type-type biaya yang dipergunakan dalam Internet Banking Service.
39. Kesepakatan lain antara Bank dan Nasabah atas pembayaran biaya akan terus berlangsung dan akan menjadi bagian tambahan yang tidak terpengaruhi oleh perjanjian ini khususnya hal-hal yang mengatur mengenai biaya tersebut dengan pemakaian Internet Banking Service.
40. Nasabah setuju untuk bertanggung jawab atas seluruh dan semua biaya untuk mengakses rekening melalui Internet Banking Service.
41. Nasabah berkewajiban untuk membayar seluruh dan semua biaya termasuk pajak-pajak (pajak jasa) yang ditentukan sesuai ketentuan Undang-Undang maupun Peraturan/Ketentuan Pemerintah yang menjadi kewajiban Nasabah. Bank berhak untuk memperhitungkan dan membebankannya kepada Nasabah termasuk untuk melaksanakan pendebitan langsung atas jumlah-jumlah tersebut terhadap rekening Nasabah.
42. Bank setiap saat berhak untuk memperkenalkan/memberitahukan tentang adanya jasa dan produk Bank melalui Internet Banking Service ini. Dengan mempergunakan jasa dan/atau produk baru, pada saat jasa atau produk baru tersedia, maka Nasabah dengan sendirinya terikat pada seluruh syarat dan ketentuan yang berlaku atas penggunaan jasa dan/atau produk yang dimaksud.
43. Bank berhak secara sepihak mengakhiri perjanjian ini atau menon-aktifkan serta membatalkan kesepakatan tentang Internet Banking Service ini, tanpa harus memberitahukan atau meminta persetujuan Nasabah terlebih dahulu, untuk itu Bank berhak untuk mengakhiri perjanjian ini berdasarkan alasan apapun untuk mengakhiri/menutup rekening manapun yang dimiliki oleh Nasabah tidak berhasil mengakses Internet Banking Service dengan nomor-nomor yang ditentukan oleh Bank. Nasabah hanya diperkenankan untuk mengakhiri perjanjian ini terlebih dahulu memberitahukan secara tertulis kepada Bank tentang makdudnya tersebut.
44. Bank meresevir haknya untuk menon-aktifkan atau mengakhiri/membatalkan perjanjian Internet Banking Service ini bilamana Nasabah gagal melakukan akses Internet Banking Service.
45. Nasabah mengikat diri serta tetap berkewajiban untuk membayar seluruh biaya-biaya yang timbul berkenaan dan pada saat berlangsungnya perjanjian ini, meskipun jumlah tersebut baru dapat diperhitungkan setelah perjanjian ini diakhiri oleh sebab atau dengan cara apapun. Pembayaran harus segera dilakukan pada saat diminta/ditagih oleh Bank.
46. Nasabah setuju bahwa semua pertukaran dari valuta ke valuta lain berkenaan dengan Internet Banking Service ini semata-mata berdasarkan pada nilai tukar valuta yang ditentukan oleh Bank pada waktu itu. Di dalam hal timbul kerugian karena nilai tukar tersebut, menjadi beban dan tanggung jawab Nasabah sepenuhnya, untuk itu Bank berhak untuk memperhitungkan dan melakukan pendebitan langsung atas rekening Nasabah untuk jumlah-jumlah tersebut. Didalam hal saldo rekening Nasabah tidak mencukupi, maka Nasabah harus segera membayarnya pada saat ditagih oleh Bank.
47. Jika rekening yang dipilih oleh Nasabah untuk transaksi pertukaran valuta tidak memiliki dana yang cukup, maka Bank berhak untuk melikuidasi Valuta Asing tersebut dan membatalkan transaksi dan seluruh akibat yang timbul termasuk (namun tidak terbatas pada) kerugian menjadi beban dan tanggung jawab Nasabah.
48. Para pihak setuju bahwa Nasabah akan membebaskan Bank dari segala tuntutan apapun, di dalam Bank tidak dapat melaksanakan perjanjian ini baik sebagian maupun seluruhnya karena hal atau sebab-sebab diluar kekuasaan, kemsampuan Bank, termasuk hal-hal yang terjadi karena keadaan peralatan, sistem atau transaksi yang tidak berfungsi atau karena

- terjadinya kebakaran, perang, huru-hara atau karena kebijaksanaan Pemerintah serta kejadian-kejadian lain diluar kekuasaan Bank. Berkenan dengan hal-hal diatas, Bank tidak bertanggung jawab atas segala kelambatan atau kerugian apapun yang timbul karenanya, tanpa kecuali apapun juga.
49. Nasabah setuju bahwa Bank berhak untuk memberikan informasi tentang Nasabah atau Rekening atau Rekening Nasabah yang manapun yang disimpan di Bank untuk keperluan Bank yang dianggap benar atau perlu dan termasuk (namun tidak terbatas pada) keperluan untuk memperbaharui atau memelihara Internet Banking Service, pencetakan dokumen atau untuk mengubah atau menjalankan instruksi Nasabah atau untuk ketetapan Internet Banking Service.
 50. Nasabah setuju bahwa Bank berhak untuk memberikan informasi mengenaiya kepada siapapun untuk keperluan pemasaran produk atau jasa kepada Nasabah dengan cara elektronik atau yang lainnya.
 51. Nasabah setuju jika ada situasi dimana pemakaian, kehilangan atau penyalahgunaan Password dan Login ID Internet Banking, Bank berhak memberitahu kepada orang-orang tertentu yang mengetahui rahasia instruksi Nasabah atau kepada yang berwajib informasi yang berhubungan dengan rekening yang dipegang oleh Nasabah di Bank yang dianggap perlu oleh Bank untuk diselidiki.
 52. Nasabah setuju bahwa Bank tidak bertanggung jawab atas kehilangan maupun kerugian yang diderita oleh Nasabah sebagai akibat dari kelalaian Nasabah atau kejadian-kejadian yang dilakukan oleh pihak ketiga dari dan karenanya Bank dibebaskan dari segala tuntutan maupun akibat yang timbul karenanya.
 53. Nasabah harus memberikan ganti rugi kepada Bank untuk setiap atau segala kehilangan, kerusakan, kerugian, tanggung jawab, tuntutan atau ongkos yang dikeluarkan oleh Bank berhubungan dengan fungsi-fungsi Bank yang bersangkutan dengan Internet Banking Service dan termasuk (namun tidak terbatas pada) :
 - a. Instruksi Nasabah yang tidak sah atau instruksi lainnya yang mungkin dikirim melalui Internet Banking Service atau setiap instruksi Nasabah yang tidak benar atau tidak lengkap.
 - b. Pemulihan atau percobaan pemulihan oleh bank dari nasabah dana yang dihutangi kepada bank atau pelaksanaan ketentuan dalam perjanjian ini oleh bank .
 - c. Perubahan dalam hukum regulasi atau instruksi resmi yang mengakibatkan kerugian materi kepada perjanjian ini atau kepada Bank.
 - d. Pelanggaran kewajiban Nasabah yang tertera dalam perjanjian ini.
 54. Bank tidak akan bertanggung jawab terhadap setiap dan seluruh kehilangan atau kerusakan apapun dan bagaimanapun yang diakibatkan oleh pihak-pihak manapun, baik yang berkaitan atau tidak berkaitan dengan dan termasuk (namun tidak terbatas pada) :
 - a. Segala kehilangan/kerusakan yang diakibatkan perlengkapan, software, penyedia browser internet atau oleh ISP atau agen-agenya.
 - b. Segala gangguan virus komputer atau sistem Trojan Horses atau komponen membahayakan yang dapat mengganggu Internet Banking Service, Web Browser atau komputer sistem Bank, Nasabah atau ISP.
 - c. Pemakaian Internet Banking Service yang tidak resmi.
 - d. Segala tujuan pemakaian Internet Banking Password dan Login ID.
 - e. Pengrusakan atau perubahan Instruksi Nasabah atau Instruksi, Data atau Informasi lainnya yang dikirim oleh Nasabah melalui Internet Banking Service.
 - f. Segala kesalahan dalam transmisi Instruksi Nasabah atau Instruksi Nasabah lainnya yang mungkin ditransmisi melalui Internet banking Service atau transmisi segala data atau informasi lainnya oleh Bank melalui Internet Banking Service.
 - g. Segala Instruksi Nasabah yang tidak tepat atau tidak lengkap dan Instruksi Nasabah lainnya yang ditransmisi melalui Internet Banking Service.
 - h. Segala kelalaian oleh Nasabah mengikuti petunjuk, prosedur dan instruksi yang paling baru untuk memakai Internet Banking Service.
 - i. Segala penundaan pengiriman atau tidak mengirimkan dokumen atau materi apapun dibawah pengujian ini.
 - j. Segala penundaan atau penolakan untuk menjalankan Instruksi Nasabah atau Instruksi lainnya dari Nasabah yang mungkin ditransmisi melalui Internet Banking Service.

- k. Segala kehilangan atau kerugian langsung, tidak langsung atau akibat lain atau berhubungan dengan pemakaian Internet Banking Service.

Tindakan-tindakan yang dilakukan oleh Nasabah berkenaan dengan hal-hal diatas tidak boleh melebihi jangka waktu 1 (satu) tahun sejak tanggal kejadian.

- 55. Pertanggungjawaban Bank karena alasan apapun disetujui untuk dibatasi sampai dengan maksimal 100 (seratus) kali biaya langganan yang berlaku untuk waktu itu.

http://www.lippobank.co.id/cabang_int_lipponet.html

:: Branches & ATMs : Internet Banking : Lippo NetBank

Terima kasih atas kepercayaan Anda telah menggunakan fasilitas Lippo NetBank. Adalah suatu kehormatan bagi kami untuk selalu dapat memberikan pelayanan yang terbaik bagi Anda. Sebagai wujud komitmen kami, mulai 23 September 2003 kami telah meluncurkan Lippo NetBank versi baru dan fasilitas-fasilitasnya yang lebih lengkap. Lippo NetBank versi baru ini akan memberikan kemudahan dan kenyamanan bagi anda dalam bertransaksi kapan dan dimanapun anda berada.

Account Portfolio, terdiri dari :

- *Balance Inquiry* : informasi saldo dari seluruh rekening terdaftar.
- *Transaction Inquiry* : informasi detail transaksi sampai 45 hari terakhir (tampil bertahap maksimal 15 hari).
- *Assets & Liabilities* : informasi nilai total aset dan total liabilitas dari seluruh rekening terdaftar (mulai dari rekening Tahapan, Time Deposit, Kartu Kredit sampai Pinjaman/Loan) yang dapat dilihat pada satu halaman.
- *Funds Transfer* : layanan transfer uang antar rekening di LippoBank, modul ini terdiri dari :
 - *Transfer List Maintenance (Daftar Penerima Dana)* : fasilitas membuat daftar data-data penerima dana dan menggunakan data yang sama berkali-kali untuk melakukan pengiriman uang.
 - *To LippoBank Account* : pengiriman uang antar rekening LippoBank.
 - *To Other Domestic Bank* : pengiriman uang ke bank lain di dalam negeri.
 - *Post-Dated Fund Transfer* : pengiriman uang dijalankan pada waktu atau tanggal (future date) yang ditetapkan Nasabah. Sistem akan otomatis menjalankan permintaan pada hari atau tanggal yang ditetapkan Nasabah tersebut.
 - *Recurring Fund Transfer (Auto Debit)* : menjalankan transaksi pengiriman uang secara berulang untuk frekuensi dan periode yang ditentukan oleh Nasabah, misalnya 1 x seminggu, setiap awal bulan, atau bahkan dalam periode hari.
 - *Mass Fund Transfer* : Menyajikan semua list pengiriman uang yang sudah didaftarkan di Transfer List sehingga Nasabah dapat memilih dan melakukan pengiriman uang sekaligus (dengan sekali eksekusi).
- *Bills Payment* : nasabah dapat membayar tagihannya seperti telepon, kartu kredit (LippoBank, Citibank, HSBC, GE Finance, Mbf), PLN, XL Pasca bayar, dan sebagainya.
 - *Consolidated Bill Presentment* : nasabah dapat membayar beberapa atau seluruh tagihan yang telah didaftarkan dengan sekali klik.
- *Purchase* : nasabah dapat membeli voucher prepaid atau pulsa isi ulang seperti Mentari Satelindo, Simpati Telkomsel, dan sebagainya.
- *Application Module* :

- *Loan* : nasabah dapat mengajukan permohonan pinjaman (home loan).
- *Cheque Function* : nasabah dapat mencocokkan cek *in-house* yang telah dikeluarkannya dan memeriksa laporan atas status ceknya
- *Notification* : menyediakan fasilitas notifikasi kepada nasabah atas transaksi tertentu lewat email
- *ATM Notification* : apabila kartu ATM hilang, dicuri dan sebagainya nasabah dapat dengan segera melakukan pemblokiran terhadap kartu ATM secara online.
- *Help Desk Module* : menyediakan fasilitas kotak surat penyampaian saran, komentar, pertanyaan dan sebagainya yang bersifat interaktif.
- *Personalization* : memungkinkan nasabah untuk mengubah atau mengatur tampilan layar beserta menu yang diinginkan.
- *Utilization Modul*, terdiri dari
 - *Change Password* : fasilitas untuk mengganti password.
 - *Change Email Address* : fasilitas untuk mengganti alamat email.
 - *Transaction Log* : memberikan informasi seluruh aktivitas yang dilakukan di Lippo NetBank.

Perkenalkan kami untuk menguraikan prosedur mendaftar Lippo NetBank

01.Registrasi Online Lippo NetBank

- a. Setiap nasabah LippoBank yang mempunyai kartu ATM yang dapat digunakan untuk melakukan transaksi perbankan di ATM LippoBank berhak untuk menikmati fasilitas Lippo NetBank.
- b. Untuk dapat melakukan registrasi online di Lippo NetBank, nasabah harus memiliki nomor identifikasi pribadi di Lippo NetBank yaitu VPIN. VPIN akan digunakan setiap kali nasabah melakukan transaksi finansial di Lippo Netbank. VPIN diperoleh sendiri di mesin ATM LippoBank.
 - Nasabah datang ke mesin ATM LippoBank .
 - Masukkan kartu ATM, masukkan PIN, tekan "ENTER"
 - Pilih "Registrasi Lippo NetBank"
 - Masukkan VPIN yang diinginkan sebanyak 6 digit dengan format numerik (angka).
 - Masukkan kembali VPIN yang sama dengan sebelumnya, tunggu sistem untuk memproses.
 - Pembuatan VPIN selesai, ambil kartu ATM.
- c. Nasabah masuk ke homepage LippoBank di <http://www.lippobank.co.id>, klik button 'Registrasi Online'. Masukkan :
 - *ATM Card No.* : (16 digit numerik)
 - *User ID* yang diinginkan : (6 s/d 9 karakter alphanumeric)

- Password yang diinginkan : (6 s/d 12 karakter numerik)
 - Confirm Password : (isi dengan password yang sama)
 - Email : (maksimum 70 karakter alphanumerik)
 - Klik submit.
 - VPIN (2 digit dengan posisi digit yang sudah ditentukan sistem).
Catatan :
 - VPIN, User ID dan Password tidak boleh sama.
- d. Setelah mengisi semua data, klik button Submit, silakan tunggu sampai sistem selesai memproses dengan memunculkan screen 'Confirmation Page'.
- e. Registrasi Online sudah selesai, klik login untuk segera menikmati fasilitas Lippo Netbank.

02.Login Internet Banking

Setiap kali login Lippo NetBank, Nasabah cukup memasukkan User ID dan Password yang sudah diperoleh pada saat Registrasi Online.

- Bagi yang memiliki kartu ATM
Mempertimbangkan faktor keamanan atau security, maka *existing user* harus registrasi online lagi. Existing user akan diberi tenggang waktu selama kurang lebih 1 minggu untuk apply VPIN di mesin ATM sebelum Netbank versi baru diluncurkan. Dengan demikian, pada waktu diluncurkan existing user tetap bisa login dengan terlebih dahulu melakukan online registration.
Bagaimana mendaftarkan rekening-rekening terdaftar pada Netbank lama ?
Anda akan dibantu untuk mendaftarkan rekening-rekening tambahan tersebut tanpa perlu ke cabang. Fasilitas yang kami sediakan adalah berupa e-form yang akan anda temukan pada saat anda melakukan Registrasi Online. Silakan mengisi formulir pendaftaran yang disediakan dengan baik dan benar
- Bagi yang tidak atau belum memiliki kartu ATM
Dengan sangat menyesal, user tidak dapat melanjutkan menggunakan Lippo NetBank lagi. User dihimbau agar segera mengajukan aplikasi permohonan kartu ATM di cabang pembuka rekening. Dengan kartu ATM nasabah dapat mendaftar ke Lippo Netbank baru dan menikmati fasilitas yang lebih menjanjikan

Beberapa hal penting yang harus diperhatikan mengenai VPIN dan Password, antara lain :

1. **Penggantian / Perubahan / Lupa VPIN**
Lupa VPIN atau ingin mengganti VPIN merupakan kasus yang sama, artinya mengikuti prosedur yang sama. Apabila lupa VPIN, nasabah harus membuat VPIN lagi di mesin ATM. Secara otomatis VPIN yang lama akan digantikan (over-write) dengan yang baru. Nasabah datang kembali ke ATM terdekat dan mengikuti prosedur Registrasi Lippo Netbank di ATM. VPIN yang sudah diperoleh dapat langsung digunakan di Lippo NetBank dan tidak perlu Online Registration lagi. Kecuali, jika ingin mengganti user id dan passwordnya juga maka harus melakukan online registration lagi
2. **Lupa Password**
Lupa password sehingga salah memasukkan password sebanyak 3 kali, akan menyebabkan user id di-locked. Nasabah dapat mengaktifkan kembali (un-locked) user id di menu 'Forget Password' yang terdapat pada screen login. Di menu ini, Nasabah diminta untuk mengisi kembali nomor kartu ATM, VPIN, User Id, Password, dan Alamat Email

3. Penanganan VPIN dan Password Anda

- o Jangan menggunakan VPIN yang diberikan oleh orang lain atau yang mudah diterka seperti tanggal lahir, no. telepon, dll
- o Jangan pernah memberitahukan VPIN dan password Anda kepada siapapun termasuk kepada anggota keluarga atau sahabat Anda
- o Jika Anda tidak yakin terhadap kerahasiaan VPIN Anda, kami menyarankan Anda segera mengganti VPIN Anda atau mengganti secara periodik melalui mesin ATM LippoBank

Jika Anda membutuhkan informasi lebih lanjut, silakan menghubungi Customer Response Center di (021) 546 0777 atau melalui email erc_nethank@lippobank.co.id atau langsung melalui 'Contact Us' yang tersedia di Website LippoBank, www.lippobank.co.id

http://www.lippobank.co.id/cabang_int_lippolink.html

Bank saya berada di meja kerja saya

Dalam situasi pasar yang dituntut semakin kompetitif, aktifitas perbankan yang semakin rumit tetap menjadi kebutuhan utama dunia bisnis. Tak terhitung usaha dan uang yang telah dikucurkan untuk memecahkan masalah-masalah arus kas, waktu, sumber daya manusia dan tenaga. Terlebih lagi setiap profesional keuangan membutuhkan informasi yang seketika (real time online) untuk mengambil keputusan dalam rangka mencapai tingkat produktivitas dan profitabilitas yang tinggi.

Untuk mengantisipasi kebutuhan tersebut, LippoBank telah memposisikan diri untuk mendukung setiap profesional dalam memecahkan masalah-masalah manajemen keuangannya (cash flow) dengan e-LippoLink, suatu aplikasi Perbankan Elektronik LippoBank untuk Manajemen Keuangan (LippoBank's Electronic Banking for Cash Management). Dengan akses seketika (real time online) aktifitas perbankan dapat dilaksanakan dengan arus kerja yang sederhana, mudah dioperasikan dan keamanan data yang kokoh. Karena aplikasi ini dibangun dengan software berbasis aplikasi web, maka tidak diperlukan lagi software khusus untuk mengakses bank yang dapat dilakukan melalui jaringan internet umum atau sambungan langsung (direct dial up) ke bank.

:: Fitur dan Keuntungan

e-LippoLink menyediakan aktivitas perbankan seketika (real time online) yang memungkinkan nasabah mendapatkan informasi rekeningnya sampai ke detik nasabah mengakses bank.

- Account Inquiry (Pemeriksaan Rekening) menyediakan fasilitas kepada nasabah untuk memeriksa rincian saldo dan transaksi terkini secara seketika (real time). Fasilitas "Save to Text File" (menyimpan file ke dalam format text) disediakan untuk memudahkan nasabah untuk melakukan rekonsiliasi rekeningnya.
- Download Monthly Statement (Menyalin Rekening Koran Bulanan) dengan fasilitas "Save to Text File" disediakan untuk memudahkan nasabah dalam memeriksa dan melakukan rekonsiliasi atas rekeningnya secara offline.
- Funds Transfer (Pengiriman Uang) antar rekening LippoBank dilaksanakan seketika (real time online) untuk mempercepat pengelolaan keuangan dan pembayaran.
- Domestic Bank Funds Transfer (Pengiriman Uang ke bank lain di Dalam Negeri) memungkinkan nasabah untuk mencapai rekanan bisnisnya di manapun di dalam negeri.
- Beneficiary List (Daftar Penerima) memberikan kemudahan kepada nasabah untuk mempersiapkan data-data penerima dana dan menggunakan data yang sama berkali-kali untuk melakukan pengiriman uang.

- **Beneficiary Notification (Pemberitahuan Kepada Penerima Dana)** menyediakan fasilitas kepada nasabah untuk memberitahukan kepada penerima dana atas pembayarannya melalui fax atau e-mail.
- **Bills Payment (Pembayaran Tagihan)** memungkinkan nasabah untuk membayar tagihan bulanan, membayar premi asuransi, melakukan pembelian voucher isi ulang telepon genggam, serta membayar tagihan kartu kredit.
Flexible Funds Transfer Period (Waktu Pengiriman Uang yang Fleksibel) memberikan nasabah keleluasaan untuk melaksanakan pengiriman uang seketika, pengiriman otomatis berulang (recurring) berdasarkan jangka waktu, berdasarkan hari, berdasarkan tanggal serta transaksi pembayaran mundur (post dated).
- **Sweep In Funds Transfer** menyediakan fasilitas kepada nasabah untuk menggabungkan saldo semua rekening LippoBanknya ke dalam satu rekening gabungan (pooling account) dan menjaga saldo minimumnya tanpa harus memeriksa saldo rekening yang digabung (swept account) satu persatu.
Sweep Out Funds Transfer adalah fasilitas yang dapat digunakan nasabah untuk mendistribusikan dananya ke rekening LippoBank manapun dari satu rekening.
Mass Funds Transfer memudahkan nasabah untuk melaksanakan pengiriman uang dari rekeningnya dalam jumlah besar untuk didistribusikan ke rekening manapun di LippoBank atau rekening di Bank Dalam Negeri lainnya. Fitur ini memungkinkan nasabah untuk mengambil data dari aplikasi komputer apapun dan mengimportnya ke e-LippoLink tanpa harus memasukkan data satu per satu.
Cheques Reconciliation (Rekonsiliasi Cek) memungkinkan nasabah untuk mencocokkan cek in-house yang telah dikeluarkannya dan menerima laporan atas status ceknya.
- **Cheque Book Request (permintaan Buku Cek)** memungkinkan nasabah untuk meminta buku cek baru.
- **Personalised and Controlled Access (Kontrol akses yang dipersonalisasi)** memungkinkan nasabah untuk mempersonalisasikan, mengatur dan membatasi akses setiap operator.
- **Secure online Banking (Perbankan online yang aman)** karena e-LippoLink memiliki sistem pemeriksaan Keamanan Berganda (multi level security) dan Arus Kerja Aplikasi (Application Workflow) serta Tingkat Akses Pengguna (User Access Level) yang dapat diatur.

Dua orang Sistem Administrator yang ditunjuk bertindak sebagai administrator aplikasi pengguna (user's application). Tiga tingkat arus kerja transaksi keuangan dari tingkat pengetikan data, sampai sembilan orang pemberi persetujuan, dan sampai sembilan orang yang me-release ditambah dengan kode keamanan Secure Token untuk setiap transaksi keuangan.

Setiap transaksi keuangan yang berhasil akan dibubuhi kode sukses yang khusus sebagai bukti sahnya transaksi. e-LippoLink diamankan dengan enkripsi Secure Socket Layer 128 bits encryption.

- **Enhanced Access (Akses Terpadu)** melalui internet atau sambungan langsung (direct dial up) ke bank menawarkan keleluasaan untuk mengakses rekening bank nasabah.

:: Keuntungan bagi nasabah

e-LippoLink menawarkan kemudahan dan kenyamanan yang dipadu dengan efisiensi operasional yang memberikan keuntungan bagi nasabah dalam mengelola aktivitas perbankannya.

- **Consolidated Data (Data Terpadu)**
Informasi rekening dan laporan bulanan disimpan ke file dan akan tersedia bagi nasabah tanpa harus menyalin ulang data tersebut. Karena file tersebut disimpan ke dalam format text, maka data dapat diakses di berbagai sistem operasi komputer.
- **Cost Effective (Hemat)**
Lebih sedikit waktu yang dihabiskan untuk melaksanakan aktivitas perbankan sehingga meningkatkan produktivitas sumber daya manusia serta meningkatkan keuntungan karena

nasabah tidak perlu lagi datang sendiri ke Bank. Waktu perbankan yang lebih lama memberikan keleluasaan bagi nasabah untuk mengelola rekening banknya.

- **Timely (Tepat Waktu)**
Menyelesaikan pengelolaan dana dalam hitungan menit, tidak ada informasi tertunda karena seluruh aktifitas perbankan dilaksanakan seketika (real time basis).

e-LippoLink mulai beroperasi dari jam 7 pagi sampai jam 9 malam pada hari kerja bank sehingga memberikan waktu perbankan yang lebih panjang, leluasa dan nyaman.

- **Enhanced Accessibility (Akses yang ditingkatkan)**
e-LippoLink menawarkan akses yang leluasa sesuai dengan kebutuhan komunikasi nasabah baik melalui internet atau sambungan langsung (direct dial up) ke bank

Semudah memasuki website bank @ www.lippobank.co.id, pengelolaan dana perusahaan anda dapat diselesaikan dalam hitungan menit. e-LippoLink memberikan kenyamanan yang dipadu dengan efisiensi operasional yang memberikan banyak keuntungan bagi nasabah dalam pengelolaan dana secara seketika dan dapat diakses dari seluruh penjuru dunia.

Untuk keterangan lebih lanjut, harap hubungi cabang-cabang LippoBank atau hubungi Customer Response Center kami.

Telepon: (021) 546-0777, Bebas pulsa: 0-800-18-21-800

Fax (021) 546-0456 atau kunjungi website kami: <http://www.lippobank.co.id>

<http://www.lippobank.co.id/faq.html>

B. FAQ

01. Apakah Lippo NetBank itu?

Lippo NetBank adalah fasilitas yang disediakan bagi nasabah LippoBank untuk melakukan transaksi perbankan melalui jaringan Internet. Nasabah dapat melakukan transaksi kapan saja dan dimana saja, 24 jam sehari 7 hari dalam seminggu.

02. Siapa yang berhak mendaftar ke dalam jaringan Lippo NetBank?

Yang berhak mendaftar ke dalam jaringan Lippo NetBank adalah semua nasabah perorangan yang mempunyai rekening Giro ataupun tabungan bank yang mempunyai kartu ATM ataupun yang tidak mempunyai kartu ATM.

03. Bagaimana saya bisa mendaftar di Lippo NetBank?

Pendaftaran Lippo NetBank dapat dilakukan secara online dan offline.

Bagi anda yang telah mempunyai kartu ATM LippoBank, anda dapat mendaftar secara online (Online Registration) di Internet, sedangkan bagi anda yang belum mempunyai kartu ATM LippoBank dapat mendaftar di cabang LippoBank terdekat.

04. Apakah pelayanan Lippo NetBank berlangsung selama 24 jam?

Ya, pelayanan Lippo NetBank berlangsung selama 24 jam, kecuali pada saat komputer LippoBank dalam pemeliharaan (maintenance).

05. Apakah ada biaya administrasi yang dikenakan untuk penggunaan Lippo NetBank?

Saat ini anda dapat menggunakan fasilitas Internet Banking tanpa dikenakan biaya administrasi.

06. Apa yang harus saya lakukan saat ingin mengakses pertama kali?

Pastikan anda sudah memiliki perangkat lunak dan perangkat keras yang dibutuhkan.

Pastikan anda memiliki User ID dan Password yang diberikan oleh cabang pada saat mendaftar di cabang (Offline Registration) dan bagi anda yang akan mendaftar secara online dapat memilih sendiri User ID dan Password yang akan digunakan di Lippo NetBank.

Kunjungi situs LippoBank di: <http://www.lippobank.co.id>, Klik Login.

Selanjutnya, Anda harus mengisi semua data yang diminta.

07. Apa yang harus disiapkan untuk bisa mengakses Lippo NetBank?

Untuk mengakses Lippo NetBank, Anda paling sedikit harus memiliki perangkat sebagai berikut:

- Perangkat Keras:

1. PC Pentium 133 Mhz, atau lebih tinggi
2. Modem 28.8 kbps (disarankan 56 Kbps)
3. Operating System Windows 95 atau Windows NT/2000 or higher)

- Perangkat Lunak

1. Sistem Operasi Windows 95 atau Windows
2. Internet Account pada salah satu Internet Service Provider (Penyedia Jasa Internet) seperti C.B.N, Indosatnet, Telkomsel dan
3. Browser Microsoft Internet Explorer 5.0

08. Transaksi apa saja yang dapat dilayani oleh Lippo NetBank?

Hampir semua transaksi yang dapat dilakukan melalui ATM LippoBank dapat dilakukan melalui Lippo NetBank kecuali penarikan tunai.

1. Account Summary, terdiri dari:

- o Balance Inquiry : Informasi saldo dari seluruh rekening terdaftar
- o Transaction Inquiry : Informasi detail transaksi hingga 14 hari setelah transaksi (tampil berturut-turut 10 hari)
- o Funds Transfer : Transfer uang yang dilakukan melalui LippoNetBank
- o Bills Payment
- o Telkomsel Internet Banking : Transfer ke Telkomsel
- o Credit Card Billing : Transfer ke kartu kredit

2. Other Services :

- o Reorder Check/Giro : per 30 hari buku Check/Giro
- o Check/Giro Inquiry : Informasi Check/Giro
- o Session Summary : Informasi aktivitas akses yang dilakukan melalui Lippo NetBank
- o Change Password : Fasilitas bagi nasabah yang ingin mengganti password
- o Mail to us : Untuk surat dan informasi saran, komentar, dan pertanyaan dan sebagainya

09. Apakah saya akan mendapatkan bukti transaksi setiap melakukan transaksi finansial?

Ya, setiap kali anda melakukan transaksi finansial melalui Lippo NetBank, anda akan mendapatkan bukti nomor referensi. Bukti nomor referensi terdapat dalam buku keamanan/kepercayaan apabila anda melakukan pengecekan atau menyetor transaksi yang dilakukan melalui Lippo NetBank. Anda dapat mencetak/menyimpan bukti nomor referensi tersebut.

10. Bagaimana cara mencetak bukti transaksi?

Anda cukup menekan tombol 'Control' bersamaan dengan huruf 'p'.

11. Sistem pengamanan apa yang dipakai untuk fasilitas ini?

- Sistem pengamanan yang digunakan adalah International Internet Standard Security SSL 3.0 dengan metode 128 bit enkripsi
- Security plugins yang dipasang secara otomatis saat nasabah mengakses Internet Banking pertama kali. User ID dan PIN Internet Banking yang harus dimasukkan setiap kali melakukan login ke Internet Banking dan dicek oleh sistem

12. Apa yang dimaksud dengan SSL 3.0?

SSL 3.0 adalah sistem pengamanan yang paling aman saat ini dalam mengkodekan data melalui Internet

13. Bagaimana Caranya Mengamankan User ID dan Password Lippo NetBank?

Perhatikan penanganan User ID dan Password anda demi keamanan dalam bertransaksi.

- Tidak memberitahukan User ID dan Password kepada orang lain.

- Tidak menuliskan User ID dan Password pada meja, terminal atau menyimpannya dalam bentuk tertulis atau pada aplikasi komputer atau sarana penyimpan data lainnya yang memungkinkan untuk diketahui oleh orang lain
- User ID dan Password harus digantikan dengan acak tidak terduga secara berkala

14. Apakah aman bertransaksi lewat warnet?

Kami mengundang anda untuk berpartisipasi jika berminat di komputer online yang akan kami sediakan di tempat umum terdapat terdapat di <http://www.scribd.com> dan <http://www.facebook.com> untuk mengikuti program tersebut sengaja dibuat untuk membantu apapun yang anda butuhkan seperti ID dan Password anda, untuk kemudian diikutsertakan kepada siapa pun yang anda inginkan untuk mengambil manfaat.

15. Apa yang harus saya lakukan apabila dalam Online Registration terjadi kesalahan PIN?

Apabila dalam Online Registration terjadi kesalahan PIN, nomor kartu akan dibatalkan. Maka, anda dapat melakukan pencairan uang secara offline melalui mesin ATM Lippo NetBank di cabang.

16. Kemana saya bisa meminta bantuan apabila saya menemukan masalah dalam menggunakan Lippo NetBank?

Jika anda menemui masalah, maka anda bisa menghubungi kami melalui email cs@netbank.co.id sebagai berikut:

2. Strinken eerst beide molaten faciliteiten op een rijtje. Als u Lippobank www.lippobank.co.id bezoekt, ziet u de link www.lippobank.co.id en de link www.lippobank.co.id.

17. Bagaimana Saya dapat mengetahui alamat Kantor Cabang LipppBank tertentu?

Selengkapnya, kunjungi www.lippo.co.id atau hubungi di Homepage Lippo Bank. Untuk informasi Distribusi Channel.

INTERNET BANKING

English Version

Layanan perbankan via internet, yang memungkinkan Anda melakukan transaksi perbankan di tengah kenyamanan rumah ataupun kantor. Anda tinggal memutuskan kapan menginginkan ke bank, apakah jam 3.00 dini hari, siang atau bahkan di tengah malam. Tanpa batas waktu, bebas antri dan macet.

Mengapa memilih BII Internet Banking?

- **Layanan perbankan 24 Jam**
BII Internet Banking beroperasi 24 jam sehari dan 7 hari seminggu*. Anda dapat melakukan transaksi perbankan dengan mudah. Kapan saja dan dimana saja.
- **Tidak ada biaya bulanan**
Setiap nasabah BII berhak mendapatkan fasilitas ini secara gratis. Biaya hanya dikenakan untuk transaksi pengiriman uang dan pembayaran tagihan. Dengan biaya yang sangat ringan. Sama seperti biaya di counter bank.
- **Aman**
Didukung oleh sistem pengamanan dengan 128 bit encryption untuk menjamin keamanan dan kerahasiaan data.
- **Fitur lengkap**
Mulai dari cek saldo sampai dengan pembayaran tagihan bulanan berbagai jasa bisa dilakukan dengan cepat dan mudah.

Fasilitas BII Internet Banking

- Cek saldo
- Melihat ringkasan rekening seperti bunga berjalan, tanggal jatuh tempo PRK atau Deposito
- Melihat rincian rekening
- Melakukan pemindahbukuan secara online antar rekening sendiri maupun rekening orang lain.
- Pembayaran tagihan
- Pembelian voucher isi ulang

- Download mutasi rekening
- Pemindahbukuan RKK
- Pengiriman uang
- Aplikasi pembukaan rekening
- Aplikasi buku cek
- Informasi suku bunga semua produk BII
- Aplikasi buku cek
- Informasi suku bunga semua produk BII
- Informasi nilai tukar berbagai valuta asing
- Mailbox Internet Banking
- Catatan transaksi Internet Banking

Perlengkapan yang dibutuhkan

Untuk mengakses BII Internet Banking, komputer Anda harus memenuhi spesifikasi berikut ini:

Perangkat Keras

- IBM compatible Pentium 133 MHz atau lebih tinggi.
- 16 Mb RAM
- Modem dengan kecepatan 28,8 KBPS atau lebih

Perangkat Lunak:

- Operating system Windows 9x atau Windows NT 4.0
- Microsoft Internet Explorer 4.01 atau Netscape Communicator 4.04 keatas.

Selanjutnya pastikan Internet Service Provider Anda, membuka akses ke secure server (https). Karena dalam beberapa kasus ISP tidak membuka akses ke https. Hal ini menyebabkan pelanggannya tidak dapat mengakses seluruh situs yang menggunakan secure server (https:). Jika Anda mengalami kesulitan ini, hubungi Technical Support dari Internet Service Provider Anda!

Issue Keamanan

Internet adalah suatu media pertukaran informasi antara sistem komputer yang sesungguhnya sangat terbuka. Akses ilegal terhadap data mungkin saja terjadi. Sebagai penyelenggara Internet Banking, BII mengambil berbagai langkah untuk meminimalisasikan resiko akibat pencurian ataupun akses ilegal.

Tindakan pencegahan yang diambil antara lain dengan penggunaan:

- **Digital ID Certificate/128-bit encryption**
Semua informasi yang ditransfer antara komputer Anda dengan sistem BII Internet Banking dienkripsi menggunakan teknologi enkripsi 128-bit.
- **User ID and Password**
Agar userID dan Password tidak diketahui oleh pihak lain. Maka keduanya dikirimkan secara terpisah. Password dikirimkan dalam amplop tertutup (PIN Mailer) yang tidak dapat dibaca

bahkan oleh staff Internal BII. Internet Banking PIN diserahkan oleh staff Customer Service pada saat pengisian formulir aplikasi. Sedangkan userID dikirimkan ke alamat email nasabah. Untuk meningkatkan keamanan, jika melakukan kesalahan pengetikan password sebanyak 3 kali, maka secara otomatis account Internet Banking akan di-blok.

- **Firewall**

Sebagai pagar yang mencegah akses ilegal ke jaringan perbankan, BII Internet Banking dilengkapi firewall yang mengitari sistem.

Antisipasi keamanan menggunakan pendekatan teknologi, tidak akan berjalan sempurna tanpa peran serta nasabah untuk senantiasa menjalankan prinsip kehati-hatian pada waktu bertransaksi:

- Ketika mendaftar, Anda akan menerima password (Internet PIN) dalam sebuah PIN mailer. Jika PIN Mailer rusak ataupun kelihatan seperti telah dibuka, jangan diterima. Mintalah PIN Mailer yang baru.
- Jaga kerahasiaan PIN Anda, sekalipun terhadap staff di bank kami.
- Pastikan bahwa Anda telah melakukan log out setelah selesai menggunakan BII Internet Banking.
- Hindari mengakses Internet Banking melalui komputer milik Publik, terutama di Warnet, karena mungkin saja terdapat program "keyboard tabbing" yang akan membaca dan menyimpan userID dan password Anda.
- Pastikan komputer yang Anda gunakan bebas virus. Hindari mendownload file yang tidak jelas judul dan sumbernya.
- Ketika mengunjungi situs BII, pastikan Anda terhubung ke: <http://www.bii.co.id> Sedangkan ketika melakukan login pastikan Anda terhubung ke <https://www.bankbii.com>. Laporkan ke cs@bii.co.id jika Anda menjumpai keganjilan, dengan alamat URL tersebut.

1. Apakah Internet Banking itu?

Internet Banking adalah fasilitas yang diberikan kepada nasabah BII untuk melakukan transaksi perbankan melalui Internet. Nasabah dapat mengajukan aplikasi dan melakukan transaksi kapan saja dan dimana saja. 24 jam sehari 7 hari dalam seminggu.

Kembali keatas

2. Bagaimana saya bisa mendaftar Internet Banking?

Untuk mendaftar layanan ini, Anda harus memiliki rekening di BII atau memiliki kartu kredit.

Kembali keatas

3. Adakah biaya yang dikenakan?

Layanan ini bebas biaya. Hanya saja untuk beberapa layanan tertentu seperti pembayaran tagihan dan pemindahbukuan ke bank lain, akan dikenakan seperti transaksi perbankan konvensional di counter.

Kembali keatas

Akses pertama kali

4. Apa yang harus saya lakukan saat ingin mengakses pertama kali?
 - a. Pastikan Anda sudah memiliki perangkat lunak dan perangkat keras yang dibutuhkan.
 - b. Pastikan Anda memiliki Registration Number dan Registration PIN yang diberikan pada saat pendaftaran di cabang.
 - c. Kunjungi situs BII di: <http://www.bii.co.id>, Klik Login.
 - d. Jika browser Anda baru pertama kali mengakses IBS, maka secara otomatis security plugins, akan terinstall ke komputer Anda. Ikuti petunjuk pada layar.
 - e. Selanjutnya, lakukan pembuatan User ID dan Password

Kembali keatas

5. Bagaimana cara membuat User ID dan Password?

Caranya:

1. klik 'joint' pada halaman login di Internet Banking, kemudian
2. Pada layar 'Customer Authentication' masukkan Registration Number dan Registration PIN, yang diberikan oleh Customer Service kami pada saat Anda mendaftar layanan Internet banking.

Kembali keatas

Perangkat yang dibutuhkan

6. Apa yang harus disiapkan untuk bisa mengakses BII Internet Banking?

Untuk mengakses BII Internet Banking, Anda paling sedikit harus memiliki perangkat sebagai berikut:

Perangkat Keras:

1. PC Pentium 133 Mhz, atau lebih tinggi
2. Modem 28.8 kbps (disarankan 56 kbps)
3. Operation g System Windows 98 atau Windows NT (V 4.0 or higher)

Perangkat lunak:

1. Sistem Operasi Windows 95 atau Windows
2. Microsoft Internet Explorer 4.01 atau Netscape Communicator 4.04 ke ata

Kembali keatas

7. Apa yang harus saya lakukan jika browser saya lebih rendah dari yang dibutuhkan?

Untuk Microsoft IE, kunjungi pada: <http://www.microsoft.com/msdownload/>
Untuk Nescape, kunjung: <http://home.netscape.com/download/>

Kembali keatas

Transaksi

8. Dapatkah saya memeriksa saldo rekening melalui BII Internet Banking?

Anda dapat memeriksa saldo rekening Superpundi, Superdolar, Supergiro, Giro Valas, Rekening Kartu Kredit dan deposito melalui BII Internet Banking.

Kembali keatas

9. Dapatkah saya melakukan pemindahbukuan ke pihak ketiga?

Anda dapat melakukan pemindahbukuan ke pihak ketiga, baik antar rekening BII dalam mata uang Rupiah atau ke bank lain. Maksimum transaksi untuk pihak ketiga sebesar 30 Juta dalam sehari. Jika transaksi Anda ke pihak ketiga melebihi jumlah tersebut, isilah formulir pendaftaran rekening pihak ketiga:

1. Pada menu utama pilih 'Layanan Pelanggan'.
2. Pada bagian Administrasi pilih 'pendaftaran rekening pihak ketiga'.

Untuk transaksi TT yang diterima setelah pukul 11:45 dana baru diproses keesokan harinya.

Kembali keatas

10. Dapatkah saya membuka rekening baru?

Anda dapat membuka rekening: Superpundi, Superdolar, Supergiro, Giro Valas dan Deposito. Untuk pembukaan rekening deposito transaksi sudah dapat dilakukan secara online, dimana setoran awal akan langsung di debet dari rekening sumber dana.

Kembali keatas

11. Dapatkah saya membayar tagihan kartu kredit melalui Internet Banking?

Anda dapat membayar berbagai jenis tagihan termasuk diantaranya kartu kredit.

Untuk melihat daftar usahawan ataupun BUMN terbaru yang telah bekerja sama untuk menerima pembayaran tagihan, kunjungi: <http://www.bii.co.id>

Kembali keatas

12. Bagaimana cara mencetak bukti transaksi?

Anda cukup menekan tombol 'Control' bersamaan dengan huruf 'p'

Kembali keatas

Keamanan

13. Sistem pengamanan apa yang dipakai untuk fasilitas ini?

Sistem pengamanan yang digunakan adalah:

- a. International Internet Standard Security SSL 3.0 dengan metode 128 bit enkripsi
- b. Security plugins yang dipasang secara otomatis saat nasabah mengakses Internet Banking pertama kali. User ID dan PIN Internet Banking yang harus dimasukkan setiap kali melakukan login ke Internet Banking dan dicek oleh sistem. Apa yang

dimaksud dengan SSL 3.0?

SSL 3.0 adalah sistem pengamanan yang paling aman saat ini dalam mengkodekan data melalui Internet.

Kembali keatas

14. Apakah aman bertransaksi lewat warnet?

Kami menyarankan Anda untuk berhati-hati jika bertransaksi di komputer milik umum. Umumnya komputer di tempat umum rentan terhadap virus dan program sederhana yang terdownload. Bukan mustahil program tersebut sengaja dibuat untuk membaca apapun yang Anda ketikkan (termasuk userID dan Password Anda), untuk kemudian dikirimkan kepada sang pembuat program dan digunakan untuk mengambil manfaat.

Kembali keatas

Bantuan

15. Apa yang harus saya lakukan bila saya lupa PIN?

- a. Bila Anda sama sekali belum pernah menggunakan PIN tersebut, dan belum mengganti UserID dan Password. Anda cukup menghubungi: Customer Service kami (62 21) 318-3888; Bandung (62 22) 421-3188; Surabaya (62 31) 547-3888; Medan (62 61) 537-888.
- b. Bila Anda sudah mengganti User ID dan Password, maka Anda harus datang ke cabang BII tempat Anda mengajukan aplikasi Internet Banking. Untuk meminta PIN baru.
- c. Bila Anda melakukan pendaftaran Internet Banking melalui situs BII, kirimkan email ke cs@bii.co.id, kami akan mengirimkan PIN yang baru ke alamat Anda.

Kembali keatas

16. Dimana saya bisa meminta bantuan apabila saya mengalami masalah dalam menggunakan Internet Banking?

Bila Anda menemui masalah, maka Anda bisa melakukan hal-hal sebagai berikut:

1. Hubungi BII teleBank di Jakarta (62 21) 318-3888; Bandung (62 22) 421-3188; Surabaya (62 31) 547-3888; Medan (62 61) 537-888
2. Kirimkan email Anda melalui fasilitas email pribadi di layanan Internet Banking atau ke cs@bii.co.id

Kembali keatas

Migrasi Sistem Internet Banking Lama (VB) ke Sistem Baru (IBS)

17. Apakah IBS itu ?

- o Merupakan Singkatan dari "Internet Banking System".
- o IBS merupakan sarana layanan perbankan BII melalui Internet, yang merupakan penyempurnaan dari sistem Virtual Banker's (VB ' 98).

Kembali keatas

18. Transaksi apa saja yang dilayani IBS ?

- Pemindahbukuan / Transfer (Intern BII)
- Telegraphic Transfer (PB transfer keluar BII baik bank yang berada didalam negeri maupun di luarnegeri, baik Rupiah maupun Valas).
- Pembayaran Tagihan.
- PU via Western Union.
- Pembelian TC dan Bank Draft.
- Pembukaan rekening.
- Aplikasi kartu ATM baru dan penggantian kartu ATM yang hilang, Kartu Kred'it baik untuk personal maupun corporate.
- Permohonan KPR
- Link/unlink rek ke kartu ATM / ke User ID
- Pendaftaran ke Pihak ketiga dan penambahan limit
- Daftar untuk PB / TT yang dilakukan secara berkala
- Yang utama adalah tersedianya fasilitas TT untuk FUTURE yang pada VB tidak ada.
- Dll

Kembali keatas

19. Apakah nasabah pengguna sistem VB'98 dapat menggunakan IBS ?

Ya, Karena seluruh nasabah Internet Banking VB akan dimigrasikan ke IBS secara bertahap, sehingga semua nasabah BII pengguna Internet Banking pada akhirnya akan dilayani dengan sistem IBS.

Pengguna VB tidak perlu datang ke cabang untuk mendaftarkan diri agar dapat mengakses IBS. Peralihannya dari VB ke IBS dilakukan secara otomatis. Pada saat soft launch IBS, pada tanggal 23 Februari 2001, Nasabah VB akan diminta mengubah UserID dan Password VB ke UserID dan Password yang digunakan untuk mengakses IBS.

Kembali keatas