

Kebijakan Privasi dan Pengamanan – Internet Banking

Kebijakan Privasi ini berlaku untuk semua Nasabah yang mengakses <https://www.okbank.co.id> dan <http://m.okbank.co.id> (“Internet Banking”) (“Pegguna”). Dengan mengakses dan/atau menggunakan layanan-layanan yang tersedia atau melalui Internet Banking ini (“Layanan”), Anda dengan ini mengakui bahwa Anda telah membaca dan setuju dengan ketentuan-ketentuan yang tercantum dalam Kebijakan Privasi ini (berserta dengan Syarat dan Ketentuan, Kebijakan cookie kami, dan setiap dokumen lainnya yang terkait).

1. Kebijakan Privasi

PT Bank Oke Indonesia, Tbk tidak menjual, menukar atau memperlihatkan segala informasi yang berkaitan dengan nasabah atau pengunjung situs dan internet banking PT Bank Oke Indonesia, Tbk. PT Bank Oke Indonesia, Tbk tidak melacak pengunjung situs PT Bank Oke Indonesia, Tbk. Website ini menggunakan cookie.

Semua data perbankan Anda dan informasi rekening lainnya disimpan secara rahasia sesuai dengan ketentuan hukum yang berlaku di Indonesia serta kebijakan perusahaan PT Bank Oke Indonesia, Tbk.

2. Keamanan

1. Sistem Pengaman

PT Bank Oke Indonesia, Tbk menggunakan 3 (tiga) lapis sistem pengamanan untuk melindungi akses dan transaksi Anda di internet banking PT Bank Oke Indonesia, Tbk yaitu :

- Secure Socket Layer ("SSL") SSL adalah teknologi pengamanan yang 'mengacak' jalur komunikasi antar komputer sehingga tidak dapat dibaca oleh pihak lain.
- User ID, Password dan Personal Identification Number ("PIN")
- Response Code yang dihasilkan oleh Sistem token Response Code adalah teknologi pengamanan yang selalu menghasilkan password yang berbeda setiap kali alat/token pengamannya digunakan.

Karena banyaknya variasi browser internet yang ada, sulit untuk menyediakan internet banking yang mengikuti keamanan masing-masing browser. Saat ini PT Bank Oke Indonesia, Tbk hanya menyediakan sarana internet banking yang lebih cocok diakses dengan menggunakan Microsoft Edge, Mozilla Firefox dan Google Chrome.

Proteksi Komunikasi Internet Banking PT Bank Oke Indonesia, Tbk

PT Bank Oke Indonesia, Tbk menggunakan teknologi enkripsi Secure Socket Layer (SSL) 256 bit untuk memproteksi komunikasi antara komputer Anda dan server PT Bank Oke Indonesia, Tbk selama Anda mengakses internet banking PT Bank Oke Indonesia, Tbk.

Untuk memastikan proteksi komunikasi selama Anda mengakses internet banking PT Bank Oke Indonesia, Tbk, Anda dapat melakukan hal-hal sebagai berikut:

- Apabila Anda menerima pesan yang menjelaskan bahwa sertifikat tidak sah, dimohon Anda tidak melanjutkan akses internet banking PT Bank Oke Indonesia, Tbk.
- Pastikan bahwa Anda telah mengetik alamat yang benar yaitu <https://m.okbank.co.id>.
- Pastikan bahwa pada browser Anda terdapat gambar gembok/kunci yang mengindikasikan bahwa halaman yang Anda akses saat ini dienkripsi dengan menggunakan SSL. Jika Anda tidak melihat gambar gembok/kunci, dimohon Anda untuk logout dan kemudian melakukan login kembali.
- Pastikan bahwa Anda telah logout saat meninggalkan komputer Anda meskipun hanya sesaat.
- Sebaiknya Anda tidak mengakses internet banking PT Bank Oke Indonesia, Tbk di jaringan yang tidak pasti keamanannya.

2. Proteksi Akses Internet Banking PT Bank Oke Indonesia, Tbk

PT Bank Oke Indonesia, Tbk, TBK mewajibkan Anda untuk memasukkan User ID dan Login Password sebelum Anda dapat melakukan akses ke internet banking PT Bank Oke Indonesia, Tbk.

Untuk memastikan proteksi bagi Anda dalam melakukan akses ke internet banking PT Bank Oke Indonesia, Tbk, mohon lakukan hal-hal sebagai berikut:

- Jagalah kerahasiaan User ID, login Password dan PIN Anda, jangan diberitahukan kepada orang lain, dan jangan disimpan dalam Browser internet Anda.
- Jangan memberitahukan Password dan PIN Anda kepada orang lain, walaupun orang tersebut mengaku sebagai karyawan PT Bank Oke Indonesia, Tbk.
- PT Bank Oke Indonesia, Tbk tidak pernah menanyakan User ID, Password dan PIN Anda.

- Gantilah Password dan PIN Anda secara periodik di internet banking PT Bank Oke Indonesia, Tbk pada menu Admin. Jangan menggunakan PIN yang mudah diterka. Jangan menuliskan PIN Anda di tempat dimana orang lain dapat membacanya.
- Gunakan Password dan PIN internet banking PT Bank Oke Indonesia, Tbk yang berbeda dengan Password dan PIN yang Anda gunakan untuk mengakses situs lain.

3. Soft token OKBank dan Hard token OKBANK

PT Bank Oke Indonesia, Tbk mewajibkan Anda menggunakan token yang dinamakan soft token Okbank atau Hard token untuk menghasilkan response code yang digunakan untuk mengotentikasi setiap transaksi finansial Anda dan sebagai tanda persetujuan Anda terhadap transaksi yang dilakukan.

Anda harus memasukkan Response Code yang dihasilkan oleh soft token OKBank dan hard token OKBank jika Anda melakukan transaksi finansial seperti : transfer dana, pembelian dan pembayaran.

Transaksi yang dapat dilakukan tanpa menggunakan soft token OKBank dan hard token OKBank adalah : informasi rekening, status transaksi, historis transaksi.

Untuk memastikan proteksi bagi soft token OKBank dan hard token OKBank Anda, mohon lakukan hal-hal sebagai berikut :

- Jangan meminjamkan soft token OKBank dan hard token OKBank Anda kepada orang lain.
- Jagalah kerahasiaan PIN soft token OKBank Anda, jangan diberitahukan kepada orang lain.
- Jangan memberitahukan Response Code dari soft token OKBank dan hard token OKBank Anda kepada orang lain, walaupun orang tersebut mengaku sebagai karyawan PT Bank Oke Indonesia, Tbk.
- PT Bank Oke Indonesia, Tbk tidak pernah menanyakan PIN soft token OKBank dan response code Anda.
- Hubungi OK Customer Care jika soft token OKBank dan hard token OKBank Anda hilang, rusak atau terblokir.

4. Alamat E-mail dan Proteksi Informasi Transaksi

PT Bank Oke Indonesia, Tbk mewajibkan Anda untuk memberikan alamat e-mail Anda kepada PT Bank Oke Indonesia, Tbk. PT Bank Oke Indonesia, Tbk akan menggunakan alamat e-mail Anda untuk mengirimkan informasi reset password yang telah Anda lakukan melalui internet banking PT Bank Oke Indonesia, Tbk, dan lain-lain. Selain itu PT Bank Oke Indonesia, Tbk juga menggunakan alamat e-mail Anda untuk kepentingan promosi, undangan gathering dan informasi-informasi lainnya.

Untuk memastikan proteksi pengiriman informasi ke alamat e-mail Anda, mohon lakukan hal-hal sebagai berikut:

- Berikan kepada PT Bank Oke Indonesia, Tbk alamat e-mail pribadi Anda. Jangan menggunakan alamat e-mail palsu.
- Ubahlah segera alamat e-mail Anda yang terdaftar di PT Bank Oke Indonesia, Tbk jika Anda mengganti alamat e-mail Anda.
- Jika Anda menghubungi PT Bank Oke Indonesia, Tbk melalui e-mail, jangan mengirimkan informasi rekening Anda yang sifatnya rahasia atau sensitif, termasuk PIN Anda.

5. Situs PT Bank Oke Indonesia, Tbk

Di dalam situs PT Bank Oke Indonesia, Tbk, PT Bank Oke Indonesia, Tbk mungkin menyediakan URL link ke situs lain yang tidak dikontrol oleh PT Bank Oke Indonesia, Tbk. PT Bank Oke Indonesia, Tbk tidak bertanggung jawab atas isi dan keamanan dari situs tersebut. Jika Anda mengakses situs tersebut, silakan memeriksa kebijakan privasi dan pengamanan mereka.

Dalam hal Anda mengakses situs atau internet banking PT Bank Oke Indonesia, Tbk melalui URL link dari situs lain, pastikan kebenaran alamat yang Anda akses yaitu <https://www.okbank.co.id> dan <http://m.okbank.co.id>

PT Bank Oke Indonesia, Tbk dapat mengubah kebijakan privasi dan informasi pengamanan ini setiap saat untuk tetap menyesuaikan dengan situasi dan teknologi terbaru. Anda selalu dapat meninjau informasi dan kebijakan privasi PT Bank Oke Indonesia, Tbk yang terbaru di <https://www.okbank.co.id/kebijakanprivasi.html>.