ZASADY BEZPIECZEŃSTWA I WYMOGI TECHNICZNE

I. WYMOGI TECHNICZNE

1. Bankowość Internetowa („BI") działa poprawnie gdy masz jedną przeglądarek tj. Internet Explorer (wersja min. 9.0) lub Mozilla FireFox (wersja min. 12.0) lub Google Chrome (wersja min. 15.0) lub Safari (wersja min. 5.0) lub Opera (wersja min. 10.0).
2. Aby korzystać z internetowego kanału dostępu GB24 („GB24") muszą być spełnione wymagania: system operacyjny (MS Windows Vista/Win7/Win8), Internet Explorer 8 lub wyższy – przeglądarka z 128-bitowym protokołem szyfrowania transmisji danych, zainstalowane oprogramowanie – Java JRE Update 1.7 lub wyższe, wolny port USB (zalecany) lub szeregowy RS232 (dot. tylko stacji z zainstalowanym czytnikiem kart mikroprocesorowych), łącze internetowe min. 64 kb/s.
3. W celu skorzystania z Bankowości Mobilnej („BM") należy pobrać aplikację ze sklepu internetowego: Google Play - platforma Android od wersji 2.2, App Store – platforma iOS od wersji 5.0, Windows Phone Marketplace dla wersji systemu 7.5 lub wyższej.
4. Informacje na temat zmian w zasadach bezpieczeństwa i wymogach technicznych zamieszczane są na www.getinbank.pl w zakładce „bankowość elektroniczna" lub pod adresem https://korporacja.gb24.pl/ (dot. GB24).

II. ZASADY BEZPIECZEŃSTWA

Wytyczne w zakresie danych uwierzytelniających

PAMIĘTAJ

1. Dane służące do identyfikacji i weryfikacji tożsamości oraz autoryzacji powinny być chronione i zabezpieczone.
2. Danych uwierzytelniających nie należy przekazywać nikomu i Klient ponosi pełną odpowiedzialność za ich udostępnienie.
3. Należy ze szczególną uwagą zabezpieczyć login, hasło, numery PIN, Getin Token. Klienta obciążają wszystkie dyspozycje złożone przez osoby, którym udostępnił powyższe dane.
4. Należy zapewnić , aby hasło było wystarczająco silne tj. min 8 znaków, kombinacja dużych i małych liter oraz cyfr, znaki specjalne. PIN nie powinien zawierać kolejnych cyfr czy dat urodzenia.
5. Hasło powinno być zmieniane nie rzadziej niż co kilka miesięcy.
6. Należy się logować wyłącznie ze strony www.getinbank.pl, a przed wpisaniem loginu, PIN oraz hasła sprawdzać czy w adresie strony jest oznaczenie https oraz czy na dolnym pasku przeglądarki widnieje rysunek kłódki (oznaczenie certyfikatu bezpieczeństwa).
7. Prosimy o używanie do komunikacji z Bankiem bezpiecznych kanałów – wiadomości w BI i GB24, kontakt telefoniczny po ustanowieniu hasła.

Procedura przesyłania i autoryzowania transakcji płatniczej

1. Zaloguj się do właściwej bankowości internetowej tj. BI, GB24, BM przy użyciu loginu i hasła.
2. Następnie wprowadź wszystkie dane wskazane w formularzu wybranej przez Ciebie transakcji płatniczej.
3. Dokonaj autoryzacji transakcji przy użyciu: karty mikroprocesorowej lub Getin Token (GB24), hasła jednorazowego SMS (BI) oraz kodu PIN (BM).

Wytyczne w zakresie bezpiecznego korzystania z internetowych i mobilnych kanałów dostępu oraz kart płatniczych

Zaleca się:	Nie należy:
– przed skorzystaniem sprawdzić czy środowisko komputerowe jest bezpieczne; – używanie karty mikroprocesorowej tylko w momencie podpisu zleceń, po dokonaniu autoryzacji/wylogowaniu przechowywanie karty w bezpiecznym miejscu; – korzystanie z aktualnego oprogramowania antywirusowego oraz zapory sieciowej (firewall); – sprawdzanie numeru rachunku odbiorcy, zwłaszcza w przypadku kopiowania danych do przelewu oraz ; – regularne sprawdzanie historii przeprowadzonych transakcji, w tym transakcji wysyłanych w „paczkach"; – instalowanie najnowszych wersji przeglądarki internetowej oraz wszystkich zalecanych poprawek do systemu operacyjnego; – używanie komputera przeznaczonego wyłącznie do korzystania z bankowości internetowej ze stałym adresem IP oraz nie instalowanie oprogramowania nieznanego pochodzenia.	– logować się, podczas korzystania z nieznanych urządzeń (np.w kawiarniach internetowych, kioskach multimedialnych); – logować się przez linki przesłane w wiadomościach e-mail, zawsze należy wybierać stronę do logowania www.getinbank.pl; – otwierać plików nieznanego pochodzenia z rozszerzeniem np. exe, pdf, doc przesłanych na pocztę elektroniczną; – podawać informacji o karcie płatniczej na stronach, które nie są bezpieczne; – podawać numeru karty przez telefon; – odpowiadać na maile, które zapraszają do podania danych, w tym o kartach w celu weryfikacji (phishing); – zapisywać numeru PIN na karcie i przechowywać go razem z kartą; – udostępniać nikomu numeru PIN; – przechowywać karty w sposób umożliwiający pozyskanie jej numeru oraz cyfr umieszczonych na odwrocie karty np. poprzez wykonanie zdjęcia.

Dodatkowe zalecenia, ostrzeżenia i komunikaty Bank zamieszcza na stronach do logowania https://secure.getinbank.pl/ dla BI oraz https://korporacja.gb24.pl/ dla GB24. Warto także śledzić komunikaty Związku Banków Polskich na stronach (http://zbp.pl/dla-konsumentow).

Sposób postępowania na wypadek utraty lub kradzieży danych uwierzytelniających

W wypadku utraty lub podejrzenia utraty wyłącznej kontroli lub kradzieży danych służących do logowania i autoryzacji oraz ich nieuprawnionego użycia zablokuj niezwłocznie dostęp lub anuluj dane do logowania poprzez kontakt z infolinią lub zgłoś ten fakt w placówce Banku.
Odblokowanie i wydanie nowych instrumentów uwierzytelniających następuje po kontakcie z infolinią Banku lub wizycie w placówce, i jest poprzedzone weryfikacją klienta.

Odpowiedzialność i zobowiązanie Banku

1. Bank nie ponosi odpowiedzialności za skutki zrealizowanej dyspozycji zgodnie z jej treścią określoną przez Posiadacza lub Użytkownika.
2. Bank, zobowiązuje się do zapewnienia bezpieczeństwa wykonywania dyspozycji, z zachowaniem należytej staranności oraz przy wykorzystaniu właściwych rozwiązań technicznych.

Limity transakcji i weryfikacja telefoniczna dyspozycji

Bank, jest uprawniony do dodatkowej telefonicznej weryfikacji faktu złożenia w BI dyspozycji kwocie od 50.000 zł (lub równowartości tej kwoty w innej walucie), wielu dyspozycji na łączną kwotę od 50.000 zł (lub jej równowartości w innej walucie) złożonych w tym samym dniu przez jednego Klienta lub więcej niż trzech dyspozycji złożonych w tym samym dniu przez jednego Klienta na rzecz tego samego odbiorcy. Weryfikacja jest prowadzona w dniach roboczych w godz. od 8:00 do 20:00, w ciągu 5 godzin roboczych od momentu złożenia dyspozycji. Bank podejmuje minimum 3 próby kontaktu na numer telefonu Klienta wskazany do obsługi BI. W przypadku braku kontaktu lub niepotwierdzenia faktu złożenia dyspozycji nie zostanie ona zrealizowana. Informacja, dotycząca telefonicznej weryfikacji dyspozycji zostanie przekazana bezpośrednio po jej złożeniu w formie komunikatu w BI.
W celu zwiększenia bezpieczeństwa możesz ustanowić limity transakcji:

– dzienne oraz pojedynczej operacji dla operacji wykonywanych w BI, BM i GB24
– gotówkowych i bezgotówkowych – dla kart płatniczych.

Getin Noble Bank Spółka Akcyjna z siedzibą przy ulicy Przyokopowej 33, 01-208 Warszawa, wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod numerem 0000304735 przez Sąd Rejonowy dla m.st. Warszawy, XII Wydział Gospodarczy Krajowego Rejestru Sądowego, NIP 1080004850, REGON 141334039, wysokość kapitału zakładowego wynosi 2.461.630.421,25 złotych (wpłacony w całości). Opłata jak za połączenie lokalne wg taryfy operatora.