

Zasady funkcjonowania usługi bankowości elektronicznej

Niniejszy dokument stanowi wyciąg z Regulaminu otwierania i prowadzenia rachunków bankowych dla klientów instytucjonalnych w Banku Spółdzielczym w Legionowie i określa zasady korzystania z usługi bankowości elektronicznej świadczonej przez Bank, w szczególności zasady dostępu, autoryzacji, bezpieczeństwa oraz realizacji dyspozycji składanych przez Klienta w kanałach elektronicznych.

Postanowienia wspólne dla kanałów bankowości elektronicznej

1. Bank w ramach systemu bankowości elektronicznej udostępnia:
 - 1) system bankowości internetowej,
 - 2) system bankowości mobilnej
 - 3) usługę SMS,
 - 4) telefoniczną usługę na hasło.
2. Użytkownicy uzyskują dostęp do systemu bankowości elektronicznej po podpisaniu Umowy i złożeniu wniosku o dostęp do systemu bankowości elektronicznej.
3. Umowę i wniosek o dostęp do systemu bankowości elektronicznej określający zakres uprawnień Użytkowników i opcjonalne limity zleceń płatniczych podpisuje Posiadacz rachunku.
4. Posiadacz rachunku może, w każdym czasie, zmienić wysokości limitów określonych we wniosku, jak również wyzerować limity ze względów bezpieczeństwa.
5. W przypadku zmiany danych, takich jak zmiana Użytkowników lub zmiana rachunków bankowych dostępnych w systemie bankowości elektronicznej lub zmiana uprawnień Użytkowników, Posiadacz rachunku składa w placówce Banku zaktualizowany wniosek o dostęp do systemu bankowości elektronicznej lub dyspozycję cofnięcia dostępu do systemu bankowości elektronicznej albo wykonuje zmiany samodzielnie za pomocą systemu bankowości elektronicznej, z zastrzeżeniem ust. 6.
6. W celu zmiany lub nadania uprawnień Użytkownikom w zakresie autoryzowania transakcji płatniczych lub autoryzowania innych dyspozycji związanych z dysponowaniem środkami na rachunku bankowym, Posiadacz rachunku składa w placówce Banku zaktualizowany wniosek o dostęp do systemu bankowości internetowej.
7. Niezłożenie przez Posiadacza rachunku wniosku lub dyspozycji, o których mowa w ust. 5 i 6, niezwłocznie po zaistnieniu zmiany powoduje, że Posiadacz rachunku ponosi pełną odpowiedzialność za dalsze korzystanie z systemu bankowości elektronicznej przez Użytkowników.
8. Bank za pomocą systemu bankowości internetowej oraz bankowości mobilnej udostępnia:
 - 1) informacje o stanie środków pieniężnych zgromadzonych na rachunkach bankowych;
 - 2) wykonywanie transakcji płatniczych;
 - 3) otwieranie i zarządzanie lokatami terminowymi;
 - 4) składanie oświadczeń woli i wniosków o wybrane usługi i produkty bankowe, z zastrzeżeniem ust. 9.
9. Oświadczenia woli i wnioski, o których mowa w ust. 8, wymagają silnego uwierzytelnienia Użytkownika.
10. Opis usług i sposobu uwierzytelnienia usług świadczonych w ramach systemu bankowości internetowej i systemu bankowości mobilnej opublikowany jest na stronie internetowej Banku.
11. Kwoty limitów dla poszczególnych płatności w systemie bankowości mobilnej zamieszczane są w komunikacie dostępnym w placówkach Banku oraz na stronie internetowej.
12. System bankowości internetowej oraz bankowości mobilnej dostępny jest przez 24 godziny na dobę, 7 dni w tygodniu, z zastrzeżeniem ust. 13.

13. Bank zastrzega sobie możliwość wprowadzenia, za uprzednim powiadomieniem Posiadacza rachunku oraz Użytkowników, przerw w funkcjonowaniu systemu bankowości internetowej niezbędnych do wykonania czynności związanych z prawidłowym jego funkcjonowaniem, w tym konserwacją, ulepszeniem lub zabezpieczeniem. Bank zobowiązuje się opublikować powiadomienie na stronie internetowej Banku oraz na stronie logowania do systemu bankowości internetowej, co najmniej dzień przed planowaną przerwą.
14. W celu poprawnego korzystania z systemu bankowości internetowej Użytkownicy powinni korzystać ze sprawnego sprzętu komputerowego z dostępem do sieci Internet oraz przeglądarki internetowej umożliwiającej stosowanie protokołu szyfrującego SSL. Sprzęt komputerowy Użytkowników powinien mieć zainstalowane i działające aktualne wersje systemu operacyjnego, przeglądarki internetowej oraz programów antywirusowych i programów typu „firewall”.
15. Zasady postępowania podczas aktywacji dostępu do systemu bankowości internetowej i uwierzytelniania oraz wszelkich informacji dotyczących działania systemu bankowości internetowej udostępniane są na stronie internetowej Banku.
16. W ramach systemu bankowości mobilnej, Użytkownicy powinni korzystać z aplikacji wskazanej przez Bank i zainstalowanej na urządzeniach mobilnych Użytkowników.
17. Użytkownik zobowiązany jest do zapoznania się z dokumentacją użytkową i ponosi odpowiedzialność za własne straty spowodowane niezajomością jej treści.
18. Posiadacz rachunku ponosi pełną odpowiedzialność za ustalenie zakresu uprawnień poszczególnych Użytkowników oraz za dokonywanie wszelkich czynności za pośrednictwem systemu bankowości elektronicznej.
19. Dla potrzeb silnego uwierzytelnienia w systemie bankowości elektronicznej Użytkownik musi posiadać urządzenie mobilne (np. telefon komórkowy, tablet) z krajowym numerem telefonu.
20. W celu korzystania z usługi bankowości internetowej Bank wydaje Użytkownikom następujące środki dostępu:
 - 1) identyfikator Użytkownika;
 - 2) hasło aktywacyjne w formie elektronicznej lub w postaci wydruku;
 - 3) kod SMS.
21. Korzystanie z systemu bankowości mobilnej po pierwszym zalogowaniu wymaga używania kodu e-PIN, ustanowionego przez Użytkownika w systemie bankowości mobilnej.
22. Blokada dostępu do aplikacji mobilnej następuje w momencie odinstalowania aplikacji z urządzenia mobilnego Użytkownika. Blokada ta nie powoduje blokady SBI.
23. Środki dostępu mogą stanowić uwierzytelnienie lub element silnego uwierzytelnienia Użytkownika oraz element autoryzacji transakcji płatniczych i innych dyspozycji w systemie bankowości elektronicznej.
24. Wszystkie dyspozycje dotyczące dysponowania rachunkiem bankowym składane przez Użytkowników dokonywane są w imieniu i na rzecz Posiadacza rachunku.
25. Informacje o wszystkich czynnościach wykonywanych przez Użytkowników są zabezpieczone przez Bank w sposób trwały i mogą stanowić dowód w przypadku spraw spornych dotyczących wykonania usług za pośrednictwem systemu bankowości elektronicznej.
26. Użytkownicy autoryzują dyspozycje z użyciem silnego uwierzytelnienia za pomocą wydanych im środków dostępu do systemu bankowości elektronicznej poprzez:
 - 1) podanie kodu SMS:
 - a) wraz z kodem uwierzytelnienia, lub
 - b) akceptacji Powiadomienia Push wraz z kodem uwierzytelnienia, w ramach uwierzytelnienia transakcji realizowanych w systemie bankowości elektronicznej, w przypadku transakcji płatniczych i innych dyspozycji, które wymagają silnego uwierzytelnienia;
 - 2) podanie identyfikatora Użytkownika wraz z hasłem oraz kodu SMS w przypadku usługi dostępu do informacji o rachunku, usługi inicjowania transakcji płatniczej i usługi potwierdzenia dostępności środków na rachunku płatniczym.
27. Po aktywacji dostępu do systemu bankowości internetowej, każdy Użytkownik ustala własne hasło Użytkownika, które wraz z identyfikatorem Użytkownika umożliwia jego uwierzytelnianie.
28. Po 90 dniach od ostatniej poprawnej zmiany hasła Użytkownik zobowiązany jest do zmiany obecnie używanego hasła do logowania lub do uwierzytelnienia obecnie używanego hasła. Każde z podjętych przez Użytkownika działań wymaga autoryzacji zgodnie z metodami opisanymi w ust. 26 od dnia wejścia w życie postanowień niniejszego ustępu lub od pierwszego skorzystania z usługi bankowości elektronicznej po tym dniu.

29. Użytkownicy przechowują i skutecznie chronią środki dostępu do systemu bankowości internetowej z zachowaniem należytej staranności – w tym także należyście chronią komputery, z których korzystają z systemu bankowości elektronicznej.
30. Użytkownicy zobowiązani są do niedostępiania środków dostępu osobom nieuprawnionym.
31. Identyfikator Użytkownika może być podany pracownikowi Banku w przypadku, gdy Użytkownik składa w Banku dyspozycję, reklamację lub inne zgłoszenie.
32. W przypadku utraty, kradzieży, wejścia w posiadanie lub podejrzenia wejścia w posiadanie środków dostępu do systemu bankowości elektronicznej przez osobę nieuprawnioną Użytkownik składa dyspozycję zablokowania dostępu do systemu bankowości elektronicznej lub dyspozycję zablokowania wybranych środków dostępu.
33. Dyspozycja może być złożona telefonicznie lub pisemnie w placówce Banku.
34. Jeżeli dyspozycja zablokowania składana jest telefonicznie, warunkiem przyjęcia dyspozycji jest telefoniczna weryfikacja Użytkownika. Dyspozycję uważa się za przyjętą przez Bank w momencie pozytywnego dokonania takiej weryfikacji. Pracownik Banku może oddzwonić do Użytkownika pod znany Bankowi numer telefonu w celu potwierdzenia dyspozycji.
35. Dyspozycja zablokowania wykonywana jest przez pracownika Banku niezwłocznie po otrzymaniu dyspozycji od Użytkownika, z zastrzeżeniem ust. 34 zdanie 3.
36. Dyspozycję zablokowania, o której mowa w ust. 32, każdy Użytkownik składa w odniesieniu do własnego dostępu.
37. Dyspozycję odblokowania dostępu do systemu bankowości elektronicznej każdy Użytkownik składa w odniesieniu do własnego dostępu. Dyspozycja odblokowania może być złożona przez Użytkownika telefonicznie lub pisemnie w placówce Banku.
38. W przypadku zablokowania środków dostępu do systemu z powodu utraty, kradzieży, wejścia w posiadanie lub podejrzenia wejścia w posiadanie przez osobę nieuprawnioną, każdy Użytkownik składa w odniesieniu do własnego dostępu, pisemnie w placówce Banku, dyspozycję wydania nowych środków dostępu.
39. Bank ma prawo zablokować dostęp do poszczególnych Użytkowników do kanałów bankowości elektronicznej w przypadku:
 - 1) naruszenia przez Użytkownika zasad określonych w Regulaminie lub Umowie;
 - 2) celowego wprowadzenia w błąd Banku przez Posiadacza rachunku przy zawieraniu Umowy;
 - 3) podejrzenia popełnienia przestępstwa lub wykroczenia przez Użytkownika lub osobę trzecią w związku z używaniem systemu bankowości elektronicznej.
40. Bank informuje Posiadacza rachunku telefonicznie lub za pomocą poczty elektronicznej o zablokowaniu kanałów bankowości elektronicznej przed ich zablokowaniem, a jeżeli nie jest to możliwe – niezwłocznie po ich zablokowaniu. Nie dotyczy to przypadków, gdy przekazanie informacji o zablokowaniu kanałów bankowości elektronicznej byłoby nieuzasadnione ze względów bezpieczeństwa lub zabronione na mocy odrębnych przepisów.
41. Użytkownicy systemu bankowości elektronicznej zobowiązani są na bieżąco sprawdzać prawidłowość składanych dyspozycji, w szczególności prawidłowość numerów uznawanych i obciążanych rachunków bankowych, a także statusy dyspozycji, a w przypadku wystąpienia nieprawidłowości powinni skontaktować się z Bankiem.

Usługa SMS

1. Usługa SMS polega na automatycznym przesyłaniu na telefon komórkowy Posiadacza rachunku komunikatu SMS informującego o saldzie rachunku i wolnych środkach na rachunku.
2. Informacja przekazywana jest w sposób zapewniający zachowanie poufności.
3. Przekazanie informacji o saldzie i wolnych środkach na rachunku bankowym następuje na numer telefonu komórkowego operatora krajowego, posiadający funkcję odbioru SMS, wskazanego Bankowi przez Posiadacza rachunku.
4. Warunkiem korzystania przez Posiadacza rachunku z usługi SMS jest złożenie w Banku prowadzącym jego rachunek pisemnej dyspozycji uaktywnienia usługi.
5. Dyspozycja podpisana przez Posiadacza rachunku i przyjmującego pracownika Banku traktowana jest jak umowa zawarta pomiędzy Posiadaczem rachunku a Bankiem i stanowi dla Banku dokument, na podstawie którego Bank wprowadza do systemu informatycznego dane stanowiące podstawę do wysyłania komunikatów SMS.
6. Jeżeli rachunek jest rachunkiem wspólnym, dyspozycję może złożyć każdy ze Współposiadaczy rachunku.
7. Bank rozpocznie wysyłanie SMS nie później niż od drugiego dnia roboczego, licząc od daty złożenia dyspozycji, przy czym dnia złożenia dyspozycji nie wlicza się do tego okresu.

8. Bank wysyła SMS informujące o saldzie na rachunku w dniu i o godzinie wskazanej w dyspozycji lub po każdej zmianie salda w sposób określony w dyspozycji.
9. Bank pobiera opłatę za czynności związane z usługą SMS w wysokości określonej w Taryfie opłat.
10. Posiadacz rachunku może zrezygnować z usługi SMS składając w Banku pisemną rezygnację.
11. Bank zaprzestaje wysyłać SMS o stanie salda i wolnych środkach na rachunku w terminie do 2 dni roboczych po dniu złożenia rezygnacji. Dnia złożenia rezygnacji nie wlicza się do tego okresu.
12. Posiadacz rachunku może zmienić dyspozycję SMS w zakresie zmiany numeru telefonu komórkowego.
13. Zmiana numeru telefonu komórkowego wymaga złożenia pisemnego zgłoszenia na druku obowiązującym w Banku.
14. Bank wysyła SMS na nowy numer telefonu, w terminie do 2 dni roboczych po dniu zgłoszenia zmiany, przy czym dnia zgłoszenia zmiany nie wlicza się do tego okresu.
15. Ze względów bezpieczeństwa oraz jakichkolwiek innych przyczyn niezależnych od Banku, Bank ma prawo czasowo zawiesić dostęp do usługi SMS.

Telefoniczna usługa na hasło

1. Usługa umożliwia uzyskanie informacji o saldzie rachunku, dostępnych środkach, odsetkach i obrotach na wszystkich rachunkach posiadanych w Banku, blokowanie/ odblokowywanie hasła do systemu bankowości elektronicznej.
2. Posiadacz rachunku/ składa w Banku pisemną dyspozycję dotyczącą korzystania z telefonicznej usługi na hasło.
3. W celu zmiany hasła lub zablokowania usługi Posiadacz rachunku składa pisemną dyspozycję w placówce Banku.
4. Posiadacz rachunku ponosi pełną odpowiedzialność za skutki ujawnienia hasła osobom trzecim.
5. Bank odmawia udzielenia informacji, jeżeli podane przez Posiadacza rachunku dane są niezgodne z zapisami dyspozycji.
6. Bank zobowiązuje się do zabezpieczenia hasła przed dostępem osób nieuprawnionych.

Płatności mobilne BLIK

1. System płatności mobilnych BLIK umożliwia dokonywanie płatności mobilnych BLIK w PLN w punktach oznaczonych znakiem BLIK.
2. Korzystanie z systemu płatności mobilnych BLIK na danym urządzeniu mobilnym jest możliwe, jeśli Użytkownik BLIK ma aktywny dostęp do aplikacji mobilnej.
3. Użytkownik BLIK może włączać oraz wyłączać dostęp do systemu płatności mobilnych BLIK na danym urządzeniu mobilnym bez rezygnacji z korzystania z aplikacji mobilnej.
4. W celu umożliwienia Użytkownikowi BLIK korzystania z systemu płatności mobilnych BLIK następuje wskazanie rachunku bankowego, jako rachunku, który będzie obciążany kwotą płatności mobilnych BLIK.
5. Płatności mobilne BLIK dzielą się na:
 - 1) transakcje bezgotówkowe BLIK, czyli płatności za towary i usługi w PLN, w tym płatności przez Internet,
 - 2) transakcje gotówkowe BLIK:
 - a) wypłaty gotówki w PLN w bankomatach,
 - b) wypłaty gotówki w PLN u akceptantów BLIK oferujących usługę wypłaty gotówki,
 - c) wypłaty gotówki typu *cash back*, której maksymalna kwota określona jest w Komunikacie.
6. Płatności, o których mowa w ust. 5, Użytkownik BLIK może zrealizować przy użyciu aplikacji mobilnej.
7. Płatności mobilne BLIK realizowane przy użyciu urządzenia mobilnego wymagają podania kodu BLIK wygenerowanego w aplikacji mobilnej.
8. Jeśli na rachunku nie ma wystarczających środków na pokrycie kwoty płatności mobilnej BLIK, wówczas transakcja ta nie dojdzie do skutku.
9. Bank dokonuje rozliczenia płatności mobilnych BLIK o których mowa w ust. 5 w momencie ich autoryzacji.
10. W przypadku braku rozliczenia płatności mobilnej BLIK, na którą została udzielona autoryzacja, blokuje ona dostępne środki na rachunku do czasu jej rozliczenia.
11. Maksymalny czas blokady, o której mowa w ust. 10, nie może być dłuższy niż 7 dni kalendarzowych.
12. W przypadku otrzymania przez Bank rozliczenia po zdjęciu blokady, Bank zastrzega sobie prawo do obciążenia rachunku na kwotę zautoryzowanej przez Użytkownika BLIK i zrealizowanej płatności mobilnej BLIK oraz związanych z nią prowizji i opłat.

13. W przypadku odmowy wykonania płatności mobilnej BLIK, Użytkownik BLIK zostanie poinformowany w momencie próby dokonania transakcji poprzez komunikat w punkcie akceptującym lub w bankomacie, w którym dokonywana jest transakcja.
14. W ramach systemu płatności mobilnych BLIK funkcjonują następujące rodzaje limitów dziennych:
 - 1) limit transakcji gotówkowych oznaczający maksymalną kwotę wypłat gotówki, jaką Użytkownik BLIK może złożyć jednego dnia;
 - 2) limit transakcji bezgotówkowych oznaczający maksymalną kwotę płatności mobilnych BLIK złożonych przez Użytkownika BLIK jednego dnia z tytułu zakupów towarów i usług w stacjonarnych sklepach/ punktach usługowych oraz sklepach internetowych.
15. Użytkownik BLIK może zmieniać wysokość limitów, o których mowa w ust. 14, w placówce Banku lub w systemie bankowości internetowej.
16. Wartości limitów dla poszczególnych płatności mobilnych BLIK dostępne są w Komunikacie zamieszczanym w placówkach Banku oraz na stronie internetowej.

Silne uwierzytelnienie

1. Bank stosuje silne uwierzytelnianie Użytkownika/ Użytkownika karty, w przypadku gdy podmiot ten:
 - 1) uzyskuje dostęp do swojego rachunku w trybie on-line;
 - 2) inicjuje elektroniczną transakcję płatniczą;
 - 3) przeprowadza za pomocą kanału zdalnego czynność, która może wiązać się z ryzykiem oszustwa związanego z wykonywanymi usługami płatniczymi lub innych nadużyć,z zastrzeżeniem postanowień ust. 28 części **Postanowienia wspólne dla kanałów bankowości elektronicznej.**
2. Bank stosuje silne uwierzytelnianie Użytkownika/ Użytkownika karty obejmujące elementy, które dynamicznie łączą transakcję płatniczą z określoną kwotą transakcji oraz określoną odbiorcą.
3. Bank stosuje silne uwierzytelnienie dla usługi dostępu do informacji o rachunku, usługi inicjowania transakcji płatniczej i usługi potwierdzenia dostępności środków na rachunku płatniczym, zgodnie z opisanymi tu zasadami.
4. Zgoda Użytkownika będącego Posiadaczem rachunku płatniczego na wykonanie transakcji płatniczej udzielana jest zgodnie z umową między dostawcą usług a tym Użytkownikiem, z wyjątkiem usługi potwierdzenia dostępności środków na rachunku płatniczym, na którą Użytkownik wyraża zgodę w systemie bankowości internetowej.
5. Wycofanie zgody, o której mowa w ust. 4 dotyczy wszystkich niewykonanych transakcji płatniczych na moment otrzymania przez Bank uwierzytelnienia wycofanej zgody.
6. W przypadku braku realizacji usług określonych w ust. 3, Bank informuje Użytkownika/ Użytkownika karty o odmowie realizacji usługi wraz z podaniem przyczyny odmowy.
7. W przypadku kiedy Bank, pomimo istnienia takiego obowiązku, nie wymaga silnego uwierzytelnienia Użytkownika/ Użytkownika karty, Posiadacz rachunku nie ponosi odpowiedzialności za nieautoryzowane transakcje płatnicze, chyba że Użytkownik/ Użytkownik karty działał umyślnie.
8. Bank zgodnie z ustawą o usługach płatniczych nie stosuje silnego uwierzytelnienia w następujących przypadkach:
 - 1) usług świadczonych przez dostawców usług technicznych, wspierających świadczenie usług płatniczych, jeżeli nie wchodzi on w posiadanie środków pieniężnych będących przedmiotem transakcji płatniczej;
 - 2) transakcji płatniczych przeprowadzanych przez przedsiębiorcę telekomunikacyjnego, dokonywanych obok usług telekomunikacyjnych na rzecz użytkownika końcowego, doliczanych do należności za usługi telekomunikacyjne, zgodnie z wymaganiami ustawy o usługach płatniczych;
 - 3) transakcji zbliżeniowych, zgodnie z limitem transakcji zbliżeniowych oraz z zasadami wskazanymi w Regulaminie otwierania i prowadzenia rachunków bankowych dla klientów instytucjonalnych w Banku Spółdzielczym w Legionowie;
 - 4) inicjowania transakcji płatniczej dla zaufanych odbiorców w systemie bankowości elektronicznej, o ile Użytkownik uzyskał dostęp do swojego rachunku w trybie on-line z użyciem silnego uwierzytelnienia Użytkownika;
 - 5) realizacji zautoryzowanych zleceń stałych;
 - 6) realizacji przelewów między rachunkami własnymi Użytkownika w Banku;
 - 7) inicjowania transakcji płatniczej kartą dla zdefiniowanych w Portalu kartowym zaufanych odbiorców.