Elektroniczne kanały dostępu

(dawniej zwany: Zasady udostępniania i funkcjonowania elektronicznych kanałów dostępu)

§ 1

1. W tych zasadach stosujemy następujące pojęcia:

Pojęcie (termin)	Opis pojęcia (terminu)
adres elektroniczny	System teleinformatyczny umożliwiający porozumiewanie się za pomocą środków komunikacji elektronicznej (w szczególności e-mail).
autoryzacja	Zgoda użytkownika na wykonanie dyspozycji. Autoryzujesz dyspozycję, np. zlecenie płatnicze, gdy zgadzasz się na to, aby bank ją wykonał. Twoja autoryzacja następuje w momencie rozpoczęcia uwierzytelnienia lub silnego uwierzytelnienia.
elektroniczny kanał dostępu	Sposób komunikacji między Tobą a nami na odległość, w szczególności poprzez: bankowość elektroniczną, Internet Banking, SMS.
indywidualne dane uwierzytelniające	Dane, które otrzymuje użytkownik od dostawcy usług płatniczych do celów uwierzytelniania – potwierdzania swojej tożsamości podczas operacji w banku.
przewodnik dla klienta	Dokument, w którym opisujemy, jakie oferujemy usługi i jak korzystać z systemu. Mamy następujące przewodniki: • przewodnik po SGB Mobile, • przewodnik użytkownika – aplikacja mobilna Nasz Bank, • przewodnik użytkownika – aplikacja mobilna Nasz bank Junior
klucz zabezpieczający U2F/klucz sprzętowy	Urządzenie zewnętrzne służące do silnego uwierzytelniania wieloskładnikowego przy użyciu pary kluczy – prywatnego i publicznego. Do autoryzacji wymagane jest fizyczne użycie klucza U2F (Universal 2 Factor).
silne uwierzytelnienie	To proces, w którym potwierdzamy, że to użytkownik zleca daną transakcję lub operację do realizacji w banku. Silne uwierzytelnianie chroni Cię przed oszustami, którzy podszywają się pod bank.

Pojęcie (termin)	Opis pojęcia (terminu)
	Jak przebiega proces silnego uwierzytelniania? Potwierdzasz swoją tożsamość **co najmniej dwoma** niezależnymi sposobami, wybranymi spośród **trzech kategorii**: 1. ***Coś, co wiesz tylko Ty:*** • np. hasło, PIN, odpowiedź na pytanie bezpieczeństwa, 2. ***Coś, co tylko Ty posiadasz jako użytkownik:*** • np. telefon, token, karta, aplikacja mobilna generująca kody, 3. ***Coś, co identyfikuje Twoje cechy fizyczne:*** np. odcisk palca, rozpoznanie twarzy, skan tęczówki.
system	System teleinformatyczny, przez który przekazujemy Ci informacje o obsłudze Twoich rachunków oraz tworzenia i wymiany elektronicznych komunikatów, pozwalających na przygotowanie przez Ciebie dyspozycji oraz przesłanie ich do nas.
uwierzytelnianie	Procedura, która umożliwia nam zweryfikować tożsamość użytkownika lub ważność stosowania instrumentu płatniczego, łącznie ze stosowaniem indywidualnych danych uwierzytelniających.
użytkownik systemu	Posiadacz lub współposiadacz rachunku, z którym zawarliśmy umowę lub pełnomocnik, którego umocujesz do dysponowania rachunkiem za pośrednictwem elektronicznych kanałów dostępu, i który otrzyma od nas indywidualne dane uwierzytelniające.

Rozdział 1. Udostępnienie elektronicznych kanałów dostępu i warunki korzystania z nich

§ 2

1. Udostępniamy produkty i świadczymy usługi użytkownikom przez elektroniczne kanały dostępu:

1) w bankowości elektronicznej - zapewniamy dostęp do informacji o produktach i usługach, które oferujemy oraz umożliwiamy Ci składanie dyspozycji:

a) bankowość internetowa (serwis internetowy) – masz dostęp do informacji oraz składasz dyspozycje na komputerze lub urządzeniu mobilnym przez przeglądarkę internetową;

b) bankowość mobilna – masz dostęp do informacji oraz składasz dyspozycje przez zaufane urządzenie mobilnego w aplikacji mobilnej SGB Mobile, Nasz Bank lub Nasz Bank Junior;

2) **powiadamianie SMS** (serwis SMS) – otrzymujesz SMS-y z informacjami o transakcjach na rachunku;

3) **innego kanału oferowanego przez Bank**, jeżeli umowa umożliwia korzystanie z innego kanału.

2. Udostępniamy wszystkim użytkownikom bankowości elektronicznej możliwość stosowania klucza zabezpieczającego U2F/klucza sprzętowego jako formy zabezpieczeń bankowości elektronicznej chroniącej przed phishingiem i wyłudzeniami danych do logowania zgodnie z ***Regulaminem korzystania z funkcji dwuetapowego logowania kluczami U2F w Banku Spółdzielczym w Człuchowie.*** Regulamin udostępniony jest na naszej stronie internetowej *www.bsczluchow.pl* oraz w Internet Bankingu.

3. Metoda zabezpieczeń o której mowa w ust. 2 nie jest obligatoryjna dla Użytkowników bankowości elektronicznej, ale zalecana do stosowania.

4. Wykaz produktów i usług dostępnych w elektronicznych kanałach dostępu oraz warunki korzystania z usług określa Przewodnik dla klienta na naszej stronie internetowej.

5. Informacje o aktualnej ofercie usług dostępnych w aplikacjach mobilnych opisane są w przypadku:

1) aplikacji mobilnej SGB Mobile w Regulaminie korzystania z aplikacji mobilnej SGB Mobile,

2) aplikacji mobilnej Nasz Bank w Przewodniku użytkownika;

3) aplikacji mobilnej Nasz Bank Junior w Przewodniku użytkownika;

ww. dokumenty zamieszczone są na naszej stronie internetowej.

§ 3

1. Aby korzystać z elektronicznych kanałów dostępu, musisz mieć rachunek oszczędnościowo-rozliczeniowy lub podstawowy rachunek płatniczy, chyba, że Regulamin korzystania z aplikacji mobilnej SGB Mobile stanowi inaczej. Możemy udostępnić elektroniczne kanały dostępu bez wymogu posiadania wyżej wymienionych produktów, o czym poinformujemy na naszej stronie internetowej.

2. Aby korzystać z elektronicznych kanałów dostępu, musisz być posiadaczem, współposiadaczem rachunku lub pełnomocnikiem, który ma pełnomocnictwo stałe. Małoletni korzysta z elektronicznych kanałów dostępu na podstawie zgody przedstawiciela ustawowego, w ramach zawartej z nami umowy.

3. Możesz wnioskować o udostępnienie kolejnych produktów lub usług, zmianę warunków świadczenia tych produktów lub usług, zawierać umowy przez elektroniczne kanały dostępu, jeśli udostępniliśmy taki sposób zawierania umów. Informacje o ofercie oraz dostępnych sposobach zawierania umów określa Przewodnik dla klienta.

§ 4

1. Dostęp do bankowości elektronicznej uzyskujesz za pomocą indywidualnych danych uwierzytelniających, z wyjątkiem § 10 tych zasad**.**

2. Możemy umożliwić Ci korzystanie z usługi przy użyciu tych samych indywidualnych danych uwierzytelniających, jeśli jesteś równocześnie posiadaczem innego rachunku lub pełnomocnikiem stałym do rachunku innego klienta. Uwzględniamy przy tym limity transakcji, o których mowa w §§ 21-24.

§ 5

1. Kiedy wykonujesz transakcje:

1) korzystaj z zaufanych komputerów z aktualnym oprogramowanie antywirusowym;

2) sprawdź, czy transmisja jest szyfrowana protokołem SSL (ang. Secure Socket Layer), który zapewnia poufność i integralność transmisji danych;

3) nie korzystaj z otwartych i niezabezpieczonych sieci.

2. W Przewodniku dla klienta oraz na naszej stronie internetowej znajduje się szczegółowy opis środków bezpieczeństwa, jakie powinieneś(-naś) przedsięwziąć, aby bezpiecznie korzystać z elektronicznych kanałów dostępu.

3. Żeby korzystać z usługi, musisz zaakceptować pliki cookies w przeglądarce internetowej. Są one konieczne, aby utrzymać aktywną sesję po zalogowaniu do bankowości elektronicznej. Szczegółowe informacje o wszystkich rodzajach naszych plików *cookies* oraz celu ich wykorzystywania, znajdują się na stronie internetowej.

§ 6

1. Musisz korzystać z elektronicznych kanałów dostępu zgodnie z umową, regulaminem i Przewodnikiem dla klienta. Musisz zabezpieczyć otrzymane indywidualne dane uwierzytelniające przed dostępem osób trzecich i zapewnić ich poufność.

2. Gdy otrzymasz indywidualne dane uwierzytelniające wskazane w ust. 1, chroń je przed naruszeniem. Ze względów bezpieczeństwa nie przechowuj poszczególnych danych razem ze sobą.

3. Zapewniamy Ci należytą ochronę indywidualnych danych uwierzytelniających. Są one dostępne wyłącznie dla użytkownika uprawnionego do korzystania z nich.

§ 7

Zakres usług możemy zmienić tylko zgodnie z warunkami i trybem przewidzianymi dla zmiany regulaminu.

Rozdział 2. Dyspozycje składane przez elektroniczne kanały dostępu

§ 8

Wszelkie oświadczenia woli, w tym dotyczące zawarcia umowy i zmiany jej warunków, które składasz nam w postaci elektronicznej, będą ważne i prawnie wiążące, jeżeli poprawnie zidentyfikujesz się indywidualnymi danymi uwierzytelniającymi i zastosujesz metody uwierzytelnienia, których wymagamy.

§ 9

1. Warunki dysponowania rachunkami przez elektroniczne kanały dostępu określają ogólne zasady dotyczące dysponowania rachunkami zamieszczone w rozdziale 2 regulaminu.

2. Dotyczą one rachunków z rozdziału 4 regulaminu i uwzględniają postanowienia § 10-13 tych zasad. Sposób posługiwania się danym elektronicznym kanałem dostępu opisuje Przewodnik dla klienta.

3. W elektronicznych kanałach dostępu możesz:

1) dokonywać operacji biernych:

a) uzyskiwać ogólnie dostępne informacje o usługach bankowych, zasadach bezpiecznego użytkowania karty, systemu itp.;

b) uzyskiwać informacje o rachunkach bankowych, w tym kredytowych posiadanych w banku oraz operacjach dostępnych dla tych rachunków,

c) uzyskiwać powiadomienia SMS o operacjach przeprowadzonych na rachunku oraz o aktualnym saldzie rachunku, jak również uzyskiwać kody służące do

autoryzacji dyspozycji złożonych za pośrednictwem elektronicznych kanałów dostępu,

d) otrzymywać zawiadomienia o dokonanych zmianach w treści umowy, regulaminu lub Taryfy, a także o zmianach wprowadzonych w systemie, mających wpływ na zmianę dotychczasowego trybu dokonywania operacji biernych lub aktywnych;

2) dokonywać operacji aktywnych:

a) składać, zmieniać dyspozycje płatnicze z rachunków, o których mowa w pkt 1 lit. b, na inne rachunki bankowe w banku lub w innych bankach w kraju i zagranicą, z wyłączeniem rachunków kredytowych,

b) odwoływać niewykonane jeszcze przez nas dyspozycje płatnicze z odroczonym terminem realizacji,

c) tworzyć, zmieniać listy zdefiniowanych odbiorców (baza kontrahentów),

d) składać, zmieniać zlecenia stałe,

e) odwoływać niewykonane jeszcze przez nas zlecenia stałe

f) pobierać wydruki potwierdzenia wykonania operacji,

g) zastrzegać karty,

h) składać oświadczenia woli o otwarciu lub zamknięciu rachunku lokaty w ramach umowy;

i) składać wniosek o wypłatę świadczenia wychowawczego w ramach programu Rodzina 800+ wraz z załącznikami oraz Dobry start – dostępność usługi uzależniona jest od współpracy z Ministerstwem Rodziny i Polityki Społecznej;

j) składać inne wnioski, które udostępniamy;

k) składać inne wnioski, które udostępniamy, dotyczące produktów lub usług podmiotów trzecich współpracujących z nami,

l) uwierzytelniać logowania do Profilu Zaufanego – „***Regulamin świadczenia usług identyfikacji elektronicznej SGB ID dla klientów indywidualnych***”, został opublikowany pod adresem: www.bsczluchow.pl,

m) składać zamówienia na wypłatę środków w bankomacie w ramach sm@rt wypłaty, której limit wynosi 1 000,00 zł zarówno dla transakcji składanej za pośrednictwem elektronicznych kanałów dostępu, jak i w banku. W przypadku złożenia zamówienia o sm@rt wypłatę w banku, pracownik jest zobowiązany wydrukować potwierdzenie zamówienia zawierające kod wypłaty z systemu operacyjnego, na którym klient akceptuje regulamin funkcjonowania usługi. Kod wypłaty ważny jest przez 15 minut;

n) zakładać i administrować skarbonkami dzieci w ramach aplikacji mobilnej Nasz Bank Junior;

o) wysłać prośby o doładowanie telefonu[1]. Zainicjowana przez dziecko transakcja poprzedzona jest wysłaniem do aplikacji rodzica prośby o wygenerowanie i udostępnienie kodu BLIK, a następnie zatwierdzona jest akceptacją rodzica.

p) wysłać prośby o kod Blik[2].
Aplikacja umożliwia dzieciom przesłanie prośby o doładowanie telefonu na kartę w postaci komunikatu widocznego w bankowości internetowej i aplikacji mobilnej rodzica Nasz Bank.

3) dokonywać innych czynności z nami, w tym w szczególności:

a) dokonywać zmiany indywidualnych danych uwierzytelniających (np. zmiana hasła dostępu),

b) składać zamówienia na indywidualne dane uwierzytelniające;

c) zmieniać sposób autoryzacji z mobilnej na hasła SMS w przypadku utraty dostępu do aplikacji mobilnej „Nasz Bank", po udzieleniu odpowiedzi na dodatkowe pytania weryfikacyjne,

d) pobierać pliki udostępnione przez nas;

e) przesyłać komunikaty kierowane do nas zawierające zapytanie lub reklamację;

f) składać wnioski o kredyt gotówkowy;

g) składać wnioski o zmianę limitu pojedynczej transakcji/sumy transakcji dziennych;

h) składać wnioski o instrument płatniczy;

i) składać wnioski o zmianę danych osobowych;

j) składać wnioski o anulowanie przelewu.

4. Aktualny zakres usług dostępnych za pośrednictwem elektronicznych kanałów dostępu określa odpowiedni dla danego kanału przewodnik dla klienta.

5. Świadczymy usługę oferowaną przez integratorów płatności internetowych, którzy inicjują płatności w formie przelewów typu pay by link we współpracy z nami, przy czym:

1) integratorem płatności internetowych jest podmiot, który świadczy usługi sklepom internetowym lub innym podmiotom prowadzącym sprzedaż towarów lub usług; usługi te polegają na umożliwieniu im przyjmowania płatności od ich klientów za pomocą przelewów typu pay by link,

2) przelew typu pay by link realizuje klient, który płaci za zakupy w sklepach internetowych lub u innych podmiotów prowadzących sprzedaż towarów lub usług za pośrednictwem integratorów płatności internetowych.

6. Realizujemy zlecenie płatnicze inicjowane przez innych dostawców świadczących usługę inicjowania transakcji płatniczej.

7. Możesz zgodzić się na transakcję również za pośrednictwem dostawcy, który świadczy

[1] Dotyczy aplikacji Nasz Bank Junior
[2] Dotyczy aplikacji Nasz Bank Junior

usługę inicjowania transakcji płatniczych.

8. Nie możesz odwołać zlecenia płatniczego, jeśli zgodzisz się, aby dostawca świadczący usługę inicjowania transakcji zainicjował transakcję albo ją wykonał. Zasada ta dotyczy inicjowania transakcji przez dostawcę świadczącego usługę inicjowania transakcji przez odbiorcę lub za jego pośrednictwem.

§ 10

1. Aby złożyć elektronicznie dyspozycję lub zlecenie płatnicze, musisz się uwierzytelnić w sposób, który pozwoli nam Cię zidentyfikować i zapoznać się z treścią dyspozycji. Dyspozycje te spełniają wymagania formy pisemnej w zakresie, w jakim mają związek z czynnościami bankowymi. Wybrane dyspozycje, które składa małoletni poniżej 13 roku życia, realizujemy, gdy w bankowości mobilnej zatwierdzi je przedstawiciel ustawowy (będzie to możliwe po wdrożeniu przez nas tej funkcjonalności).

2. Gdy złożysz dyspozycję lub zlecenie płatnicze w bankowości elektronicznej, musisz je autoryzować indywidualnymi danymi uwierzytelniającymi, stosując metody uwierzytelniania, których wymagamy.

3. Stosujemy silne uwierzytelnianie, gdy:

1) uzyskujesz dostęp do swojego rachunku w trybie on-line;

2) inicjujesz transakcję płatniczą;

3) przeprowadzasz w kanale zdalnym czynność, która może wiązać się z ryzykiem oszustwa lub innych nadużyć,

z wyjątkiem sytuacji niewymagających silnego uwierzytelniania, które wskazujemy w ust. 4.

4. Możemy nie stosować silnego uwierzytelniania, gdy:

1) korzystasz z jednej z wymienionych niżej pozycji w trybie on-line lub do obu tych pozycji bez ujawniania szczególnie chronionych danych dotyczących płatności:

a) salda rachunku;

b) transakcji płatniczych przeprowadzonych w ciągu ostatnich 90 dni za pośrednictwem rachunku, z zastrzeżeniem ust. 5;

2) inicjujesz transakcję do odbiorcy z listy zaufanych odbiorców, którą utworzyłeś(-aś) wcześniej, stosując silne uwierzytelnienia;

3) inicjujesz kolejną transakcję z serii transakcji cyklicznych, na tę samą kwotę, dla tego samego odbiorcy pod warunkiem, że pierwszą transakcję cykliczną utworzyłeś(-aś), zmieniłeś(-aś) lub zainicjowałeś(-aś), stosując silne uwierzytelnienie;

4) inicjujesz transakcję płatniczą, w sytuacji, gdy płatnik i odbiorca są tą samą osobą fizyczną lub prawną i prowadzimy oba rachunki płatnicze,

5) inicjujesz transakcję płatniczą, której poziom ryzyka uznajemy za niski, zgodnie z mechanizmem monitorowania naszych transakcji.

5. Stosujemy silne uwierzytelnianie, jeżeli:

1) po raz pierwszy uzyskujesz dostęp do informacji określonych w ust. 4 pkt 1 lit. a w trybie on-line,

2) minęło więcej niż 90 dni odkąd po raz ostatni uzyskałeś(-aś) dostęp do informacji określonych w ust. 4 pkt 1 lit b w trybie on-line oraz odkąd ostatni raz zastosowałeś(-aś) silne uwierzytelnienie.

6. Możemy skontaktować się z Tobą, aby zrealizować zlecenie płatnicze.

6.1. Zlecenia płatnicze zewnętrzne w kwocie ≥ 100 000,00 zł przesłane za pośrednictwem elektronicznych kanałów dostępu (Internet Banking), podlegają autoryzacji w systemie informatycznym. Autoryzacja polega na telefonicznym potwierdzeniu przez Ciebie danych wykonania zlecenia ze swojego rachunku. Akceptacja dokumentu przez osobę autoryzującą oznacza, że potwierdziłeś(-aś) złożenie danego zlecenia.

6.2. Rozmowa, o której mowa w ust. 6.1 jest nagrywana, o czym poinformujemy Cię przed rozpoczęciem potwierdzenia i akceptacji wykonywanego polecenia przelewu.

6.3. Czynność, o której mowa w ust. 6.2 jest możliwa do zrealizowania wyłącznie, gdy wyraziłeś na to zgodę we wniosku o Elektroniczne kanały dostępu.

6.4. Telefonicznej autoryzacji zrealizowanej przez Ciebie, o której mowa w ust. 6.1, dokonujemy przed godzinami granicznymi ustalonymi dla zleceń płatniczych zawartych w Regulaminie kont dla klientów indywidualnych w Banku Spółdzielczym w Człuchowie.

6.5. Za czynność, o której mowa w ust. 6.1. nie pobieramy opłat.

7. Aby uzyskać dostęp do serwisu internetowego, musisz podać:

1) swój identyfikator, hasło stałe lub

2) kod SMS wraz z kodem uwierzytelnienia, z zastrzeżeniem § 19 ust.1 lub,

3) e-PIN przypisany do aplikacji mobilnych oferowanych przez nas, w przypadku operacji zatwierdzanej w aplikacji;

chyba, że udostępnimy inne indywidualne dane uwierzytelniające, opisane w przewodniku dla klienta.

8. Autoryzujesz dyspozycje składane za pośrednictwem elektronicznego kanału dostępu, poprzez podanie, za pośrednictwem telefonu z funkcją wybierania tonowego, identyfikatora oraz hasła dostępu.

9. Autoryzacja, którą wykonujesz, oznacza, że polecasz nam wykonać określoną czynność i jest to podstawą jej wykonania.

10. Przesyłamy kody do autoryzacji na numer telefon komórkowego, który wskażesz w umowie, karcie informacyjnej lub pełnomocnictwie.

11. Możemy wprowadzić, wycofać oraz zmienić rodzaj stosowanych indywidualnych danych uwierzytelniających. W takim przypadku udostępniamy Ci je oraz zawiadamiamy Cię o zmianie. Informację o stosowanych rodzajach indywidualnych danych uwierzytelniających zamieszczamy w Przewodniku dla klienta oraz na naszej stronie internetowej.

§ 11

Moment zarejestrowania odpowiednich danych w bankowości elektronicznej i przyjęcia tego oświadczenia przez nasz serwer uznajemy za chwilę, w której składasz oświadczenie w postaci elektronicznej, w szczególności dyspozycję, lub wykonujesz jakąkolwiek czynność. Od tej zasady mogą obowiązywać wyjątki, które określa umowa, regulamin lub obowiązujące przepisy prawa.

§ 12

1. Dyspozycje, które składasz przez bankowość elektroniczną, realizujemy elektronicznie. Stosujesz zasady autoryzacji obowiązujące dla tego elektronicznego kanału dostępu.
2. Autoryzowanego zlecenia płatniczego nie możesz odwołać, z wyjątkiem sytuacji wskazanych w § 34 ust. 5 regulaminu.

§ 13

1. To, że przyjęliśmy do realizacji dyspozycję, którą złożyłeś(-aś) przez elektroniczne kanały dostępu, potwierdzamy przez ten sam kanał.

2. Jeśli nie przyjęliśmy dyspozycji, którą złożyłeś(-aś) przez elektroniczny kanał dostępu, powiadomimy Cię o tym oraz o przyczynie odmowy przez ten sam kanał lub pracownika naszej placówki. Możliwe powody:

1) niekompletność dyspozycji,
2) złożenie dyspozycji sprzecznych ze sobą,
3) nieprawidłowy numer rachunku odbiorcy,
4) brak środków do realizacji dyspozycji lub
5) inne okoliczności, które uniemożliwiają nam przyjęcie dyspozycji.

Rozdział 3. Korzystanie z elektronicznych kanałów dostępu

§ 14

1. Z elektronicznych kanałów dostępu możesz korzystać 7 dni w tygodniu, 24 godziny na dobę, za wyjątkiem przypadków, w których zachodzą ograniczenia wskazane w § 15.

2. Przez elektroniczne kanały dostępu uzyskujesz dostęp do wszystkich rachunków: zarówno otwartych przed dniem aktywowania usługi, jak i po nim. Możesz jednak zawnioskować o ograniczony dostęp do rachunków w elektronicznych kanałach dostępu.

Rozdział 4. Ograniczenia w korzystaniu z elektronicznych kanałów dostępu

§ 15

1. Zablokujemy Ci dostęp do serwisu internetowego i uniemożliwimy wykonanie transakcji, jeśli:

1) złożysz dyspozycję zablokowania dostępu do serwisu internetowego;

2) zastrzeżenia dokona użytkownik;

3) będziemy podejrzewać, że osoba trzecia mogła uzyskać dostęp do indywidualnych danych uwierzytelniających i może dojść do logowania z adresów IP z czarnej listy lub realizacji przelewów na rachunki z czarnej listy, zgodnie z naszymi procedurami;

4) trzy razy wpiszesz nieprawidłowe hasło dostępu do systemu.

2. Możemy ograniczyć lub zablokować dostęp do serwisu internetowego lub czasowo zablokować wykonanie dyspozycji, jeśli:

1) istnieją uzasadnione przyczyny, które wiążą się z bezpieczeństwem dostępu do serwisu internetowego i indywidualnych danych uwierzytelniających, również gdy podejrzewamy, że ktoś popełnił przestępstwo na Twoją szkodę;

2) umyślnie doprowadziłeś(-aś) do nieautoryzowanej transakcji płatniczej lub mamy uzasadnione podejrzenie, że będziesz posługiwać się dostępem niezgodnie z regulaminem;

3) wystąpią restrykcje geolokalizacyjne lub zrealizujesz przelew na rachunki z szarej listy, zgodnie z obowiązującymi w banku regulacjami;

4) korzystasz z serwisu internetowego niezgodnie z zasadami bezpieczeństwa określonymi w tym załączniku lub zagrażasz bezpieczeństwu korzystania z serwisu internetowego;

5) konserwujemy serwis internetowy lub inne systemy teleinformatyczne związane z wykonywaniem umowy; poinformujemy Cię o tym z wyprzedzeniem na naszej stronie internetowej;

6) usuwamy awarie, usterki lub nieprawidłowości działania w serwisie internetowym lub innych systemach teleinformatycznych związanych z wykonywaniem umowy;

7) wymieniamy stosowane indywidualne dane uwierzytelniające; poinformujemy Cię o tym pisemnie lub na naszej stronie internetowej,

8) mamy uzasadnione podejrzenie, że transakcje na Twoim rachunku mają związek z przestępstwem m.in. związanym z praniem pieniędzy lub finansowaniem terroryzmu,

9) gdy na Twoim rachunku są zamrożone wartości majątkowe lub gdy wobec Ciebie należy stosować sankcje międzynarodowe albo embarga,

10) nie możemy zastosować środków bezpieczeństwa finansowego, do tych sytuacji zaliczamy brak aktualnego dokumentu tożsamości Twojego lub osób upoważnionych do działania w Twoim imieniu.

3. Możemy uchylić ograniczenie albo blokadę dostępu do serwisu internetowego w przypadku, o którym mowa w ust. 2 pkt 1, jeśli odpowiedni wniosek złożysz Ty lub pełnomocnik stały. W takim przypadku albo wydajemy Ci nowe indywidualne dane uwierzytelniające, albo uchylamy ograniczenia lub blokady i zachowujesz dotychczasowe dane uwierzytelniające.

4. W przypadku , o którym mowa w ust. 2 pkt 1, uchylenie:

1) ograniczenia lub blokady dostępu do serwisu internetowego - następuje na podstawie Twojej dyspozycji telefonicznej lub złożonej w naszej siedzibie lub dowolnej placówce,

2) czasowej blokady dyspozycji - następuje po tym, jak nasz pracownik skontaktuje się z Tobą telefonicznie lub pisemnie, a Ty potwierdzisz złożoną dyspozycję.

5. Z wyjątkiem sytuacji wskazanej w ust. 6, informujemy Cię, że zamierzamy zablokować indywidualne dane uwierzytelniające w przypadkach określonych w ust. 2 pkt 1 i 3, zanim je zablokujemy, a jeżeli nie jest to możliwe – telefonicznie, niezwłocznie po zablokowaniu.

6. Nie informujemy o zablokowaniu, jeżeli byłoby to nieuzasadnione ze względów bezpieczeństwa lub zabronione na mocy odrębnych przepisów.

7. W przypadkach, o których mowa w ust. 2 pkt 5 i 6, ograniczenie lub blokada dostępu do serwisu internetowego lub czasowa blokada dyspozycji trwa możliwie krótko - przez okres niezbędny do usunięcia przyczyny ograniczenia lub blokady.

Rozdział 5. Blokowanie i zastrzeganie dostępu do serwisu internetowego

§ 16

1. Dostęp do serwisu internetowego oraz możliwość posługiwania się indywidualnymi danymi uwierzytelniającymi może zostać zablokowana przez:

1) nas – zgodnie z postanowieniami tych zasad;

2) Ciebie;

3) przedstawiciela ustawowego małoletniego.

2. Możesz złożyć wniosek o zablokowanie dostępu do serwisu internetowego i uniemożliwić jednocześnie wykonanie transakcji.

§ 17

1. Jeśli jesteś użytkownikiem serwisu internetowego lub przedstawicielem ustawowym małoletniego, niezwłocznie zastrzeż dostęp do serwisu internetowego, podając swoje dane personalne. Zrób to, jeżeli indywidualne dane uwierzytelniające zostały utracone, skradzione lub przywłaszczone albo ktoś użył ich bez uprawnień.

2. Zastrzeżenie, o którym mowa w ust. 1 możesz dokonać w naszych placówkach lub pod numerami telefonów, które wskazujemy i aktualizujemy w komunikacie w naszych placówkach oraz na naszej stronie internetowej banku, a także za pośrednictwem elektronicznych kanałów dostępu.

3. Możemy zmieniać numery telefonów służące do zastrzegania i blokowania dostępu do serwisu internetowego. Powiadomimy Cię o tym elektronicznie na adres poczty elektronicznej (e-mail), który wskazałeś(-aś), lub komunikatem we właściwym elektronicznym kanale dostępu.

4. Nie możesz odwołać zastrzeżenia, o którym mowa w ust. 1. Powoduje ono, że nie masz dalszego dostępu do serwisu internetowego.

5. Jeśli jesteś posiadaczem rachunku lub działającym w jego imieniu przedstawicielem ustawowym, możesz wystąpić z wnioskiem o nowe indywidualne dane uwierzytelniające, jeśli je wcześniej utracisz oraz zastrzeżesz.

6. Jeśli ktoś ukradnie lub przywłaszczy Twój telefon komórkowy albo stwierdzisz, że został on użyty w nieuprawniony sposób, zmień dane zgodnie z ust. 7. Dotyczy to telefonu oznaczonego jako telefon do autoryzacji lub zmiany numeru telefonu do autoryzacji.

7. Jeśli chcesz zmienić dane niezbędne do otrzymywania kodów SMS na nowe i:

1) masz dotychczasowy numer telefonu do autoryzacji, możesz zmienić numer w serwisie internetowym, jeśli udostępnimy taką funkcjonalność; możemy skontaktować się z Tobą, aby zweryfikować zlecenie zmiany numeru tego telefonu i zmienić numer telefonu,

2) nie masz dotychczasowego telefonu do autoryzacji, musisz złożyć odpowiednią dyspozycję w naszej placówce.

§ 18

1. Możemy zastrzec indywidualne dane uwierzytelniające, jeśli:
   1) umowa wygaśnie lub zostanie rozwiązania,
   2) istnieją uzasadnione przyczyny związane z bezpieczeństwem indywidualnych danych uwierzytelniających, tzn. wiemy, że osoby trzecie weszły w ich posiadanie,
   3) podejrzewamy, że indywidualne dane uwierzytelniające zostały użyte w sposób nieuprawniony lub że umyślnie doprowadziłeś(-aś) do nieautoryzowanej transakcji płatniczej.
2. Z wyjątkiem sytuacji wskazanej w ust. 3, informujemy Cię, że zamierzamy zastrzec indywidualne dane uwierzytelniające w przypadkach wskazanych w ust. 1 pkt 2 i 3, zanim je zastrzeżemy, a jeżeli nie jest to możliwe – telefonicznie, niezwłocznie po zastrzeżeniu.
3. Nie informujemy o zastrzeżeniu, jeżeli byłoby to uzasadnione ze względów bezpieczeństwa lub zabronione zgodnie z odrębnymi przepisami.

Rozdział 6. Urządzenie zaufane

§ 19

1. Podczas logowania się do bankowości internetowej możesz dodać urządzenie, z którego się logujesz, jako urządzenie zaufane. Wtedy kolejne logowania z tego urządzenia do bankowości internetowej w przeglądarce internetowej będziesz przeprowadzać już bez dodatkowego uwierzytelnienia za pomocą kodów SMS. Urządzeniem zaufanym może być np. prywatny komputer, smartfon lub tablet, z którego korzystasz wyłącznie Ty. Podczas logowania weryfikujemy określone cechy tego urządzenia.
2. Dodanie urządzenia wymaga:
   1) autoryzacji za pośrednictwem udostępnionej Tobie metody autoryzacji, o której mowa w § 10 ust. 8,
   2) akceptacji oświadczenia, iż jesteś jedynym użytkownikiem urządzenia i wyrażasz zgodę, na dodanie urządzenia jako zaufanego na potrzeby silnego uwierzytelnienia podczas logowania do systemu bankowości elektronicznej,
   3) akceptacji niniejszych zasad.
3. W dowolnym momencie możesz przez bankowość internetową usunąć swoje urządzenie zaufane. Wtedy każde kolejne logowanie do bankowości internetowej będzie wymagało dodatkowego potwierdzania za pomocą kodów SMS.

Rozdział 7. Udostępnianie informacji na potrzeby świadczenia usług inicjowania transakcji płatniczych i usług dostępu do informacji o rachunku. Potwierdzenie dostępności środków na rachunku

§ 20

1. Jeśli korzystasz z serwisu internetowego i zgodzisz się na udostepnienie informacji o rachunku i transakcjach w nim przeprowadzanych, możemy udostępnić te informacje dostawcy, który świadczy usługi dostępu do informacji o rachunku.

2. Dostęp do informacji o rachunku, wskazanej z ust. 1, mogą mieć także dostawcy, którzy inicjują transakcje płatnicze dla użytkowników korzystających z serwisu internetowego.

3. Niezwłocznie potwierdzamy dostępność na rachunku kwoty niezbędnej do wykonania transakcji realizowanej kartą, jeżeli zawnioskuje o to dostawca wydający instrumenty płatnicze oparte na karcie płatniczej. Dostępność pieniędzy potwierdzamy, jeśli:

1) Twój rachunek płatniczy jest dostępny online w momencie, w którym otrzymamy wniosek,

2) zgodziłeś(-aś) się, abyśmy odpowiadali na tego rodzaju wnioski dostawcy wydającego instrumenty płatnicze oparte na karcie płatniczej,

3) zgody z pkt 2 udzieliłeś(-aś), zanim wpłynął do nas pierwszy wniosek dotyczący potwierdzenia.

4. Dostawca wydający instrumenty płatnicze oparte na karcie płatniczej może wystąpić z wnioskiem, o którym mowa w ust. 3, jeżeli:

1) zgodziłeś(-aś) się, aby występował z wnioskiem wskazanym w ust. 3,

2) zainicjowałeś(-aś) transakcję płatniczą realizowaną kartą płatniczą przy użyciu opartego na tej karcie instrumentu płatniczego, który wydał dany dostawca,

3) dostawca uwierzytelni siebie wobec nas, zanim złoży wniosek wskazany w ust. 3, oraz porozumiewa się z nami w sposób bezpieczny.

5. Potwierdzenie wskazane w ust. 3 polega na tym, że udzielasz tylko odpowiedzi „tak” albo „nie” i nie podajesz salda rachunku. Odpowiedzi nie przechowujemy i wykorzystujemy ją tylko do wykonania transakcji realizowanej kartą płatniczą.

6. Potwierdzenie wskazane w ust. 3 nie umożliwia nam blokady pieniędzy na Twoim rachunku płatniczym.

7. Możesz zwrócić się do nas o przekazanie danych identyfikujących dostawcę, o którym mowa w ust. 4 oraz udzielonej odpowiedzi zgodnie z ust. 5.

8. Możemy odmówić dostępu do rachunku dostawcy świadczącemu usługę dostępu do informacji o rachunku lub dostawcy świadczącemu usługę inicjowania transakcji płatniczej. Mamy do tego prawo z przyczyn, które są obiektywnie uzasadnione i należycie udokumentowane lub mają związek z nielegalnym dostępem do rachunku takiego dostawcy, w tym z nieuprawnionym zainicjowaniem transakcji płatniczej. W takim przypadku w uzgodniony sposób informujemy Cię o odmowie dostępu do rachunku i jej przyczynach. Informujemy Cię, o ile jest to możliwe, zanim odmówimy dostępu, a jeżeli nie jest to możliwe – bezzwłocznie po takiej odmowie, najpóźniej w dniu roboczym następującym po dniu takiej odmowy. Nie informujemy o odmowie, jeżeli byłoby to nieuzasadnione ze względów bezpieczeństwa lub sprzeczne z odrębnymi przepisami. Dostawcy świadczącemu usługę dostępu do informacji o rachunku oraz dostawcy świadczącemu usługę inicjowania transakcji płatniczej umożliwiamy dostęp do rachunku niezwłocznie po tym, gdy ustanie przyczyna odmowy.

Rozdział 8. Standardowe limity pojedynczej operacji oraz limity wszystkich transakcji w ciągu dnia

§ 21

1. Standardowe limity pojedynczej operacji oraz limity wszystkich transakcji w ciągu dnia w serwisie internetowym prezentuje poniższa tabela:

Rodzaj limitu	Standardowy limit obowiązujący w banku	Indywidualny limit ustalony na wniosek posiadacza rachunku[3]
Limit pojedynczej transakcji	3 000,00 zł	do 30 000,00 zł
Limit sumy transakcji dziennych	20 000,00 zł	do 60 000,00 zł

2. Standardowe limity pojedynczej operacji oraz limity wszystkich operacji w ciągu dnia dokonywanych za pośrednictwem serwisu internetowego dla rachunków w walutach wymienialnych prezentuje poniższa tabela:

[3] Przelewy, których wartość przekracza limit indywidualny, można składać w placówkach banku w tradycyjnej formie (papierowej).

Rodzaj limitu	Standardowy limit obowiązujący w banku	Indywidualny limit ustalony na wniosek posiadacza rachunku
Limit pojedynczej transakcji	650 EUR	do 6500 EUR
Limit sumy transakcji dziennych	4300 EUR	do 13 000 EUR

3. Z zastrzeżeniem ust. 4 użytkownik może wnioskować o indywidualne ustalenie limitów, o których mowa w ust. 1 i 2.

4. O wysokości limitów ostatecznie decyduje bank.

§ 22

Standardowe limity pojedynczej operacji oraz limity wszystkich operacji w ciągu dnia dokonywanych za zakupy w sklepach internetowych prezentuje poniższa tabela:

Rodzaj limitu	Standardowy limit obowiązujący w banku
Limit dla pojedynczej transakcji	3 000,00 zł
Limit sum transakcji dziennych	6 000,00 zł

§ 23

Standardowe limity pojedynczej operacji oraz limity wszystkich operacji w ciągu dnia dokonywanych za pośrednictwem aplikacji mobilnej Nasz Bank prezentuje poniższa tabela:

Rodzaj limitu	Standardowy limit obowiązujący w banku
Limit pojedynczej transakcji	300,00 zł
Limit sum transakcji dziennych	1 000,00 zł

§ 24

Standardowe limity pojedynczej operacji oraz limity wszystkich operacji w ciągu dnia dokonywanych za pośrednictwem interfejsu API (PSD2) prezentuje poniższa tabela:

Rodzaj limitu	Standardowy limit obowiązujący w banku
Limit pojedynczej transakcji	300,00 zł
Limit sum transakcji dziennych	1 000,00 zł

§ 25

Standardowy globalny dzienny limit dla transakcji gotówkowych, bezgotówkowych oraz internetowych, realizowanych za pośrednictwem usługi **BLIK** prezentuje poniższa tabela:

Rodzaj limitu	Standardowy limit obowiązujący w banku
Globalny dzienny limit dla transakcji gotówkowych, bezgotówkowych oraz internetowych	5 000,00 zł

Rozdział 9. Inne postanowienia

§ 26

1. Nie wolno Ci przekazywać przez serwis internetowy bezprawnych treści.
2. Nie możesz wykorzystywać serwisu internetowego do popełniania, pomagania w popełnianiu lub podżegania do popełniania czynów zabronionych. w szczególności dotyczy to wprowadzania do obrotu finansowego wartości majątkowych, które pochodzą z nielegalnych lub nieujawnionych źródeł.

Rozdział 10. Usługa biometryczna

§ 27

1. Usługa biometryczna polega na identyfikacji na podstawie danych biometrycznych, tj. elektronicznego zapisu odwzorowania sieci naczyń krwionośnych dłoni.
2. Udostępnimy Ci usługę biometryczną na podstawie wniosku.
3. Usługę biometryczną aktywujemy z chwilą wprowadzenia Twoich danych do systemu informatycznego.
4. Dane wskazane w ust. 1 przetwarzamy wyłącznie w celu identyfikacji użytkownika oraz autoryzacji transakcji z wykorzystaniem czytnika biometrycznego.

5. Dane biometryczne pobieramy za pośrednictwem urządzeń, które spełniają normy bezpieczeństwa oraz zapewniają wierność i dokładność zapisu.
6. Nie ponosimy odpowiedzialności za niewykonanie identyfikacji lub autoryzacji biometrycznej spowodowane siłą wyższą lub następstwem wykonywania obowiązków wynikających z przepisów prawa.