SBR Bank

Załącznik nr 9 do Instrukcji otwierania i prowadzenia rachunków bankowych dla klientów instytucjonalnych

Oddział w .....

Nazwa Posiadacza rachunku

Modulo/numer Umowy

Wniosek w sprawie korzystania z systemu Internet Banking

☐ nadanie uprawnień ☐ cofnięcie uprawnień ☐ zmiana uprawnień

☐ zablokowanie dostępu ☐ odblokowanie dostępu

Użytkownik, którego dotyczy wniosek

☐ **Posiadacz** ☐ **Pełnomocnik**
Imię i nazwisko
Pesel / **Identyfikator** *(nie dotyczy nadania uprawnień)*

Rachunki bankowe, które objęte usługą

☐ wszystkie rachunki Posiadacza rachunku

☐ rachunki numer (numer rachunku w formie IBAN):

Zakres uprawnień Użytkownika

I. ☐ Przegląd II. ☐ Rejestracja / edycja operacji III. ☐ Akceptacja operacji (bez autoryzacji)

IV. ☐ Pełny dostęp w tym:

Sposób autoryzacji operacji wykonywanych w systemie Internet Banking:

☐ kody SMS nr tel. Komórkowego +48

☐ token USB

Limity transakcji:

☐ **Autoryzacja jednoosobowa**

☐ bez ograniczeń (dostęp bez limitów transakcji)

☐ limit dzienny (do kwoty)

☐ limit transakcji jednorazowej (do kwoty)

☐ **Autoryzacja dwuosobowa**

☐ bez ograniczeń (dostęp bez limitów transakcji)

☐ limit dzienny (do kwoty)

☐ limit transakcji jednorazowej (do kwoty)

Data, pieczęć i podpisy Posiadacza rachunku

(data i podpis Użytkownika)

Data, pieczęć i podpis Pracownika Banku

Potwierdzam odbiór zabezpieczeń do systemu bankowości internetowej w formie nienaruszonej:

☐ tokena o nr seryjnym

☐ identyfikatora do logowania

Token jest własnością Spółdzielczego Banku Rozwoju. Użytkownik jest zobowiązany do zwrotu tokena na żądanie Banku. W przypadku zagubienia lub uszkodzenia tokena pobierana jest opłata wg Taryfy opłat i prowizji za czynności i usługi bankowe w Spółdzielczym Banku Rozwoju.

(data i podpis Użytkownika)

(data, pieczęć i podpis Pracownika Banku)

Informacja dla Użytkownika:

1. *Hasło jest hasłem początkowym. Przy pierwszym logowaniu należy je zmienić. Nowe hasło powinno mieć co najmniej 8 znaków w tym co najmniej jedna duża, jedna mała litera i jedna cyfra np. Szariki4Pancerni.*
2. *Usługa bankowości internetowej jest dostępna pod adresem https://online.sbrbank.pl/*
3. *Instrukcja Użytkownika jest udostępniona do pobrania pod adresem www.sbrbank.pl*

** Zaznaczyć właściwe*

BANKOWOŚĆ ELEKTRONICZNA - PODSTAWOWE ZASADY BEZPIECZEŃSTWA

- należy zweryfikować czy znajdują się Państwo na właściwej witrynie i czy witryna ta ma ważny certyfikat, https://online.sbrbank.pl/
- w momencie wprowadzania poufnych danych należy zachować szczególną ostrożność,
- muszą Państwo pamiętać, iż kod jednorazowy wprowadzamy do systemu tylko i wyłącznie w momencie autoryzacji wykonanego przez Państwa przelewu lub dyspozycji;
- należy pamiętać, iż bank nigdy nie żąda autoryzacji wejścia do systemu bankowości internetowej kodem jednorazowym (wysyłanym sms-em lub z karty kodów jednorazowych);
- należy zwracać uwagę na symbole bezpiecznego połączenia (np. mała kłódka pasku statusu, litera „s" w „https://" przed internetowym adresem banku);
- należy sprawdzać dla kogo został wystawiony certyfikat bezpieczeństwa (kursorem najeżdżamy na symbol kłódki, gdzie po rozwinięciu powinna być widoczna nazwa banku, tj. Spółdzielczy Bank Rozwoju;
- należy instalować programowanie antywirusowe z aktualną bazą wirusów;
- należy instalować aktualizację oprogramowania systemów operacyjnych;
- dane dotyczące konta nie powinny być przechowywane w jawnej postaci w miejscu, z którego mogą być w prosty sposób skradzione bądź ujawnione osobom postronnym;
- nie należy przesyłać danych wykorzystywanych do obsługi kont bankowych przez e-mail, gdyż banki nigdy nie proszą o podanie danych poufnych pocztą elektroniczną, a nadawca takich wiadomości, podszywając się zwykle pod zaufaną firmę lub osobę, ma na celu wyłudzenie poufnych informacji (numery kart kredytowych, hasła do systemów bankowych, hasła portali aukcji internetowych);
- należy korzystać z nowoczesnych narzędzi ostrzegających przed wejściem na strony stworzone w celu wyłudzenia poufnych danych, gdyż w nowych wersjach popularnych przeglądarek dostępne są filtry antyphishingowe;
- należy korzystać z usług bankowości elektronicznej wyłącznie przy użyciu znanego sobie sprzętu, gdyż podstawowym zagrożeniem występującym w ogólnodostępnych systemach jest możliwość instalacji „złośliwego" oprogramowania przez osoby uprzednio korzystające z danego stanowiska;
- każdorazowo podczas logowania należy zwracać uwagę na datę ostatniego logowania do systemu;
- nie należy otwierać ani uruchamiać plików oraz programów nieznanego pochodzenia;
- ze szczególną ostrożnością należy traktować programy pobierane z Internetu;
- należy zwracać uwagę na symptomy zainfekowania komputera, takie jak: spowolnienie działania systemu, spowolnienie transferu, zwiększona liczba reklam, zmiany w działaniu przeglądarki internetowej, problemy z działaniem niektórych programów;
- nie należy klikać na podejrzane odnośniki podawane w e-mailu;
- po każdym wykryciu i usunięciu wirusa lub konia trojańskiego należy zmieniać identyfikator do usługi oraz wszelkie hasła dostępu;
- nie należy uruchamiać programów nieznanego pochodzenia przesyłanych pocztą elektroniczną;
- w przypadku jakichkolwiek wątpliwości dotyczących bezpieczeństwa bankowości internetowej należy jak najszybciej skontaktować się z bankiem.

Oświadczenie o zapoznaniu się z podstawowymi zasadami bezpieczeństwa w bankowości elektronicznej.

……..

Imię i nazwisko

……..

Numer pesel

Niniejszym oświadczam, że otrzymałem/am i zapoznałem/am się z informacją o podstawowych zasadach bezpieczeństwa w bankowości elektronicznej.

…… ……

Podpis Posiadacza rachunku *Miejscowość i data*