



O.K. BANK SPÓŁDZIELCZY

Grupa BPS

Zasady działania i autoryzacji usługi w ramach Systemu bankowości elektronicznej „OK@net” oraz OK@net Mobile w Orzesko – Knurowskim Banku Spółdzielczym z siedzibą w Knurowie

§ 1.

Niniejszy załącznik określa warunki na jakich Bank oferuje do rachunków bankowych za pośrednictwem usługi OK@net i OK@net Mobile zwanego dalej usługą.

§ 2.

1. Udostępnienie usługi następuje po zawarciu z Bankiem Umowy pakietu, sporządzonej na podstawie złożonego w Banku wniosku, pobranego w placówce Banku lub ze strony Internetowej.
2. Bank może zwrócić się o udzielenie dodatkowych informacji lub przedłożenie dodatkowych dokumentów aniżeli dokumenty związane z otwarciem rachunku bankowego.
3. Dostęp do usługi następuje w ciągu 5 dni roboczych od dnia:
 - 1) *zawarcia Umowy ramowej o usługi płatnicze w pakiecie optymalnym* - w przypadku nowozakładanego rachunku w pakiecie lub zawarcia umowy pakietowej stanowiącej kontynuację umowy rachunku rozliczeniowego,
 - 2) *złożenia wniosku o wskazaną usługę* – w przypadku, gdy Posiadacz rachunku podpisał *Umowę ramową o usługi płatnicze w pakiecie*, w której uwzględniono postanowienia dotyczące wskazanego kanału bankowości elektronicznej,
 - 3) *zawarcia aneksu do Umowy pakietu* – w przypadku, gdy Posiadacz podpisał *Umowę ramową o usługi płatnicze w pakiecie*, w którym nie uwzględniono postanowień dotyczących wskazanego kanału bankowości elektronicznej.
4. Bank zastrzega sobie prawo odmowy świadczenia usługi w przypadku naruszenia istotnych warunków Umowy ramowej o usługi płatnicze w pakiecie lub w przypadku braku akceptacji zmian Regulaminu rachunków bankowych dla Klienta instytucjonalnego.

§ 3.

1. Realizacja zleceń płatniczych następuje zgodnie z postanowieniami regulacji dotyczących otwierania i prowadzenia rachunku rozliczeniowego z uwzględnieniem zapisów *Umowy ramowej o usługi płatnicze w pakiecie*.
2. Utworzenie zlecenia przelewu polega na wypełnieniu elektronicznego formularza umieszczonego na stronie Internetowej usługi oraz potwierdzeniu wprowadzenia danych poprzez autoryzację poprzez jeden ze sposobów autoryzacji, o których mowa w §6.
3. Autentyczność zlecenia przelewu autoryzowana w sposób określony w ust. 2 nie może być kwestionowana.
4. Za wszelkie skutki wynikłe z niewłaściwego wypełnienia dyspozycji przelewu, a w szczególności z podania błędnego numeru rachunku odbiorcy, całkowitą odpowiedzialność ponosi Klient.

§ 4.

1. Zlecenie przelewu jest realizowane do wysokości limitów ustalonych przez Posiadacza lub dostępnych środków na rachunku.
2. Zmiana dostępu limitu na rachunku jest możliwa po złożeniu wniosku o zmianę limitów operacji.
3. Dyspozycje zaksięgowane przez Użytkownika są realizowane zgodnie z terminami określonymi w Komunikacie w sprawie godzin granicznych oraz potwierdzane są w Umowie pakietu.

§ 5.

1. Wszystkie dyspozycje złożone przez Klienta są zabezpieczone przez Bank w sposób trwały i stanowią dowody w przypadku sytuacji spornych.
2. Po aktywacji dostępu do systemu bankowości elektronicznej, każdy Użytkownik ustala własne hasło Użytkownika, które wraz z identyfikatorem Użytkownika umożliwia jego uwierzytelnianie.
3. Wszelkie dyspozycje w systemie Użytkownik systemu składa bankowi w postaci elektronicznej, w sposób umożliwiający Bankowi jego identyfikację i zapoznanie się z treścią dyspozycji.
4. Złożenie w postaci elektronicznej i uwierzytelnienie dyspozycji w systemie przy użyciu właściwych dla Użytkownika systemu wydanych mu środków identyfikacji elektronicznej, oznacza zgodę Użytkownika systemu na wykonanie przez Bank danej dyspozycji.
5. Bank wykonuje transakcje płatnicze w oparciu o wskazany w zleceniu płatniczym unikatowy identyfikator płatnika/odbiorcy płatności.
6. Użytkownicy przechowują i skutecznie chronią środki dostępu do systemu bankowości elektronicznej z zachowaniem należytej staranności – w tym także należycie chronią komputery, z których korzystają z systemu bankowości elektronicznej.
7. Użytkownicy zobowiązani są do nieprzechowywania poszczególnych środków dostępu razem w jednym miejscu, niezwłocznego zgłaszania Bankowi utraty lub zniszczenia środków dostępu oraz nieudostępniania środków dostępu osobom nieuprawnionym.
8. Jeżeli podane przez Klienta parametry dyspozycji powodują, że nie może być ona zrealizowana, dyspozycja ta zostanie odrzucona a Klient jest o tym powiadomiony za pośrednictwem usługi. Dotyczy to w szczególności przypadków, gdy:
 - 1) kwota zlecenia przelewu przekracza bieżące saldo dostępne na rachunku bankowym w chwili realizacji zlecenia;
 - 2) podany został nieprawidłowy numer rachunku;
 - 3) tytuł prawny płatności jest niezgodny z obowiązującymi przepisami dewizowymi;

- 4) dyspozycja jest niekompletna, zawiera wewnętrzne sprzeczności.

§ 6.

1. Bank stosuje metody autoryzacji oparte na silnym uwierzytelnieniu, gdy wymagają tego przepisy prawa lub względy bezpieczeństwa. Silne uwierzytelnienie stanowi dodatkowe potwierdzenie tożsamości Klienta lub składanej dyspozycji.
2. Pierwsza autoryzacja dokonywana jest przez system w momencie wejścia na stronę WWW za pomocą:
 - 1) identyfikatora (osobistego kodu nadawanego przez Bank) w chwili uruchomienia usługi, oraz
 - 2) indywidualnego hasła aktywacyjnego, nadanego przez Bank, które Użytkownik jest zobowiązany zmienić z chwili pierwszego logowania Użytkownika do Systemu bankowości internetowej, oraz, w ramach silnego uwierzytelnienia
 - 3) kodu SMS.
3. Wszystkie dyspozycje i oświadczenia Użytkownika składane w formie elektronicznej muszą być autoryzowane w łącznie w co najmniej dwa z poniższych sposobów:
 - 1) Identyfikator Użytkownika;
 - 2) Hasło/ hasło maskowane;
 - 3) kod PIN,
 - 4) kod e-PIN;
 - 5) kod QR;
 - 6) odczyt danych biometrycznych.
4. Użytkownik z chwilą otrzymania kompletu środków dostępu jest zobowiązany podjąć niezbędne środki służące zapobieganiu naruszeniu indywidualnych zabezpieczeń, w szczególności jest zobowiązany do:
 - 1) przechowywania środków dostępu do Systemu bankowości internetowej z zachowaniem należytej staranności - w tym także do należytej ochrony komputera i innych urządzeń, z których Użytkownicy korzystają z Systemu bankowości internetowej,
 - 2) nieprzechowywania łącznie środków dostępu do systemu bankowości elektronicznej,
 - 3) niezwłocznego zgłoszenia Bankowi ich utraty lub zniszczenia oraz do nieudostępniania ich osobom nieuprawnionym.
5. W przypadku utraty, kradzieży przywłaszczenia lub nieuprawnionego użycia środków dostępu do Systemu bankowości elektronicznej, Użytkownik zobowiązany jest do niezwłocznego samodzielnego zablokowania dostępu do usługi poprzez samodzielne trzykrotne wprowadzenie błędnego identyfikatora lub hasła, lub przekazania Bankowi dyspozycji zablokowania możliwości korzystania z Systemu bankowości elektronicznej.
6. Bank nie ponosi odpowiedzialności za skutki wynikłe z użycia podpisu elektronicznego przez osoby nieuprawnione do jego używania.

§ 7.

1. W przypadku wystąpienia podejrzeń co do znajomości hasła lub dostępu do niego przez osoby nieuprawnione, Użytkownik powinien niezwłocznie dokonać zmiany hasła.
2. Jeżeli na skutek działania osób nieuprawnionych Użytkownik nie będzie mógł uzyskać dostępu do usługi, w szczególności na skutek zmiany przez osobę nieuprawnioną hasła, Użytkownik zobowiązany jest niezwłocznie skontaktować się z Bankiem w celu zablokowania dostępu do usługi oraz uzyskania nowego hasła.

§ 8.

1. W przypadku zaniechania wykonywania operacji przez Użytkownika w czasie trwania Sesji, zostanie ona automatycznie zamknięta po przekroczeniu czasu bezczynności określonego przez system bezpieczeństwa. Dalsze korzystanie z usługi będzie wymagać ponownego ustanowienia Sesji.
2. W przypadku zaniechania dokonywania operacji w czasie trwania Sesji, Użytkownik powinien zakończyć korzystanie z usługi we właściwy sposób, tj. poprzez prawidłowe wylogowanie się i zamknięcie systemu.
3. Użytkownik zobowiązuje się do prawidłowej konfiguracji sprzętu i oprogramowania służącego do łączenia się z usługi poprzez stosowanie się do zasad ogólnych korzystania z bankowości elektronicznej, o których mowa w §19.

§ 9.

1. Ze względów bezpieczeństwa operacje dokonywane za pomocą usługi są monitorowane przez Bank. W przypadku wystąpienia podejrzenia działania osoby nieuprawnionej, Bank zastrzega prawo do natychmiastowego zablokowania dostępu do usługi.
2. Bank ma prawo do zablokowania dostępu do usługi w przypadku stwierdzenia korzystania z niej przez Klienta w sposób sprzeczny z Regulaminem, innymi uregulowaniami Banku oraz obowiązującymi przepisami prawa.
3. W przypadku trzech następujących po sobie błędnych próbach autoryzacji, dostęp do usługi zostanie zablokowany.
4. Odblokowanie hasła wymaga telefonicznego kontaktu Klienta z Bankiem oraz pozytywnego zweryfikowania tożsamości Klienta.

§ 10.

1. Posiadacz rachunku ponosi odpowiedzialność za:
 - 1) wyznaczenie Użytkowników posiadających dostęp do Systemu bankowości elektronicznej;

- 2) nadanie poszczególnym Użytkownikom zarejestrowanym przez Bank uprawnień, pozwalających na korzystanie z usługi oraz dostęp do rachunków;
 - 3) wyznaczenie osoby Administratora, który odpowiada za nadanie uprawnień poszczególnym Użytkownikom usługi.
2. Posiadacz rachunku zobowiązany jest zachowywać należytą staranność podczas korzystania z usług bankowości elektronicznej oraz posługiwać się środkami dostępu i autoryzacji w taki sposób, by zapewnić zachowanie ich poufności.
3. W szczególności Posiadacz rachunku i wskazani przez niego Użytkownicy zobowiązani są do:
- 1) należytego zabezpieczenia środków dostępu i autoryzacji przed przypadkowym dostępem osób nieuprawnionych,
 - 2) nieudostępniania środków dostępu i autoryzacji osobom nieuprawnionym.
4. Jeżeli w wyniku naruszenia przez Użytkownika obowiązków wykazanych w pkt. 3 ust. a) i b) osoby nieuprawnione uzyskają dostęp do rachunku i złożą dyspozycje, Bank nie ponosi odpowiedzialności za skutki ich wykonania.
5. Wszelkie dyspozycje złożone w trakcie prawidłowo ustanowionej Sesji oraz autoryzowane w sposób przewidziany procedurami dla danej dyspozycji i/lub kanału obsługi obciążają rachunek Posiadacza rachunku.

§ 11.

1. Bank nie odpowiada za skutki zrealizowania dyspozycji Użytkownika, jeżeli została ona wykonana według jego wskazówek i podanych przez Użytkownika danych.
2. Użytkownik powinien upewnić się, że wszelkie dyspozycje składane w ramach usługi są jednoznaczne i zgodnie z jego intencją określają: numery rachunków, które mają być obciążane i uznawane, posiadacza tych rachunków, kwotę oraz tytuł płatności.

§ 12.

1. Bank nie odpowiada za skutki wadliwego działania lub niezgodnego z prawem wykorzystania łącz telekomunikacyjnych znajdujących się poza dyspozycją Banku i szkody przez nie wywołane.
2. Bank nie odpowiada za skutki związane z zawieszeniem działania usługi na czas konserwacji systemu oraz z jakichkolwiek innych przyczyn niezależnych od Banku.
3. Zasady odpowiedzialności Banku za nieautoryzowane, niewykonane lub nieprawidłowo wykonane dyspozycje szczegółowo określa Regulamin otwierania i prowadzenia rachunków dla Klientów instytucjonalnych.

§ 13.

Zgodnie z ustawą z dnia 29 sierpnia 1997r. - Prawo bankowe i na zasadach w niej określonych, Bank i osoby w nim zatrudnione oraz osoby, za pośrednictwem których Bank wykonuje czynności bankowe, zobowiązane są zachować tajemnicę bankową oraz udzielać informacji w przypadkach przewidzianych Prawem bankowym.

§ 14.

Katalog usług w Systemie OK@net obejmuje w szczególności:

- 1) **uzyskania informacji** dotyczących:
 - a) rachunków Posiadacza tj. :
 - informacji o szczegółach rachunku (np. limicie kwotowym jednorazowej operacji internetowej lub kwotowym limicie dziennym),
 - aktualnych informacji o bieżącym stanie rachunku (np. środkach własnych, limicie kredytowym, zaległych prowizjach, zablokowanych środkach, zleceniach w realizacji),
 - salda i historii rachunków kredytowych oraz udziałowych,
 - wyciągów bankowych z rachunku,
 - oprocentowania rachunków bieżących, depozytowych i kredytowych,
 - tabel kursowych;
 - b) listy banków krajowych i urzędów skarbowych - lista zawiera numery rozliczeniowe, nazwy i adresy banków i urzędów;
- 2) **wykonania operacji** dotyczących:
 - a) rachunków w zakresie:
 - wyszukiwania operacji na wyciągach,
 - zgłoszenia zapytania do Banku;
 - b) kredytów w zakresie podglądu informacji o kredytach,
 - c) przelewów w zakresie:
 - tworzenia i edycji przelewu krajowego,
 - edycji przelewu ZUS,
 - edycji przelewu US
 - importu przelewów,
 - akceptowania przelewu,
 - akceptowania zbiorcze,
 - akceptowania pojedyncze,

- wycofania akceptów,
 - przekazania przelewów do realizacji,
 - usuwania przelewów niezrealizowanych,
- d) lokat w zakresie:
- edycji lokaty (tworzenia nowej lub edycji istniejącej),
 - tworzenia listy lokat (opcja umożliwiająca proste zarządzanie lokatami),
 - akceptowania lokaty,
 - zrywania lokaty
- e) kontrahentów w zakresie.:
- edycji nazw kontrahentów,
 - importu kontrahentów,
- f) konfiguracji systemu w zakresie.:
- nadawania uprawnień użytkowników,
 - nadawanie uprawnienia do rachunków,
- g) administrowania hasła w zakresie zmiany hasła.

§ 15.

Katalog usług w systemie OK@net Mobile obejmuje w szczególności:

- 1) **uzyskania informacji** dotyczących rachunków Posiadacza w zakresie:
 - a) informacji o szczegółach rachunku (np. limicie kwotowym jednorazowej operacji internetowej lub kwotowym limicie dziennym),
 - b) aktualnych informacji o bieżącym stanie rachunku (np. środkach własnych, limicie kredytowym, zaległych prowizjach, zablokowanych środkach, zleceniach w realizacji),
 - c) salda i historii rachunków kredytowych oraz udziałowych,
- 2) **wykonania operacji** dotyczących:
 - a) rachunków w zakresie:
 - b) wyszukiwania operacji na rachunkach,
 - c) kredytów podglądu informacji o kredytach,
 - d) przelewów w zakresie:
 - tworzenia i edycji przelewu krajowego, (tylko w przypadku podpisu jednoosobowego)
 - tworzenie i edycji przelewu ZUS, (tylko w przypadku podpisu jednoosobowego)
 - tworzenie i edycji przelewu US (tylko w przypadku podpisu jednoosobowego)
 - akceptowania przelewu, (tylko w przypadku podpisu jednoosobowego)
 - przekazania przelewów do realizacji,
 - lokat w zakresie przeglądanie listy lokat,
 - kontrahentów w zakresie przeglądania listy kontrahentów.

§ 16.

1. **Usługa płatności masowych** jest usługą rozliczeniową umożliwiającą przypisanie każdemu podmiotowi Klienta lub płatności, odrębnego numeru rachunku identyfikującego tzw. „wirtualny NRB”.
2. **Wirtualne NRB** – przypisany do rachunku płatności masowych Klienta numer rachunku bankowego w standardzie NRB, przynależny każdemu podmiotowi Klienta lub płatności realizowanej na jego rzecz.
3. **Rachunki wirtualne** – przypisane do podmiotów Klienta lub płatności zdefiniowane na potrzeby ich realizacji wirtualne konta posiadające zdefiniowane numery NRB, pozwalające na identyfikację podmiotu lub płatności na rachunku płatności masowych Klienta.

§ 17.

„Wirtualne NRB” ustalane jest w oparciu o rachunek płatności masowych w następującym formacie:

CC 8454 PPPP 8KKK LLLL LLLL LLLL

gdzie:

CC to liczba kontrolna dla danego rachunku, obliczana wg algorytmu opisanego w załącznikach do Zarządzenia nr 5/2002 Prezesa Narodowego Banku Polskiego z dnia 6 maja 2002r w sprawie sposobu numeracji rachunków bankowych prowadzonych w bankach (Dz.Urz.NBP z 2002r nr 8 poz. 26 z późniejszymi zmianami),

8454 – numer Banku,

PPPP – numer Oddziału Banku,

8 – numer wskazujący rachunek wirtualny,

KKK – identyfikator rachunku Posiadacza rachunku płatności masowych - numer specjalny z zakresu <1,999> identyfikujący jednoznacznie rachunek płatności masowych,

LL...L – dwunastocyfrowy kod identyfikujący dłużnika lub płatność do dowolnego wykorzystania przez Posiadacza rachunku płatności masowych.

Bank generuje „wirtualne NRB” dwoma sposobami:

1. Bank generuje wskazaną przez Posiadacza rachunku płatności masowych liczbę „wirtualnych NRB” w następującym formacie:

CC 8454 PPPP 8KKK LLLL LLLL LLL1
CC 8454 PPPP 8KKK LLLL LLLL LLL2
CC 8454 PPPP 8KKK LLLL LLLL LLL3
CC 8454 PPPP 8KKK LLLL LLLL LLL4

gdzie:

1-4 – kolejne numery „wirtualnych NRB” (w tym przypadku zostały wygenerowane 4 rachunki).

Tak wygenerowane rachunki wirtualne Bank przekazuje w formie pliku Klientowi w celu przyporządkowania wygenerowanych NRB poszczególnym podmiotom Klienta lub płatnościom.

2. Bank generuje wirtualne NRB na podstawie pliku otrzymanego od Klienta. Plik musi zawierać numery poszczególnych podmiotów Klienta lub płatności w następującym formacie (numer wpłacającego może mieć maksymalnie 12 znaków):

1
333
55555
7777777

999999999999(koniec linii musi być w tym miejscu, jeżeli koniec linii jest np. w linii 4 to dla linii 5 generuje NRB w postaci 000000000000).

Wygenerowany przez Klienta plik musi mieć nazwę: nrb_lista*.txt

§ 18.

- Posiadacz rachunku przypisuje poszczególnym podmiotom Klienta lub płatnościom „wirtualne NRB”.
- Posiadacz rachunku odpowiada za przekazanie poszczególnym podmiotom Klienta dokumentów (faktury, dowody wpłat, polecenia przelewu) zawierających unikalne „wirtualne NRB” pozwalające na jednoznaczną identyfikację każdego z nich.
- Podmiot Klienta rachunku przekazuje środki na rzecz Klienta na wskazany przez niego w dokumencie rachunek wirtualny w dowolnym miejscu (poczta, bank itp.).
- Płatność dokonana na wskazany rachunek wirtualny w rzeczywistości stanowi uznanie rachunku płatności masowych Posiadacza rachunku - system informatyczny Banku poprzez identyfikację numeru „wirtualnego NRB” zmienia numer z określeniem podmiotu Klienta na rzeczywisty numer rachunku płatności masowych Klienta, zgodnie ze standardem NRB dla rachunku rozliczeniowego.
- Informacje o dokonywanych przez wpłacających wpłatach na rzecz Klienta w formie płatności masowych są dostępne w formie raportów.
- Raporty dostępne za pośrednictwem usługi - dostępne w następujących formatach:
 - plik w formacie XML,
 - plik w formacie MT942,
 - konfigurowalny plik tekstowy.
- Raporty dostępne bezpośrednio w Oddziale Banku – generowane w przypadku braku możliwości uzyskania raportu za pośrednictwem usługi – dostępne w następujących formatach:
 - plik w formacie podstawowym,
 - plik w formacie precyzyjnym.

Zasady bezpieczeństwa przy korzystaniu z bankowości elektronicznej OK@NET

§19.

Posiadacz rachunku oraz wskazani przez niego Użytkownicy zobowiązani są do przestrzegania poniższych zasad bezpiecznego korzystania z bankowości internetowej:

- Należy pamiętać, że żaden bank nigdy nie wysyła do swoich klientów pytań dotyczących haseł lub innych poufnych danych ani próśb o ich aktualizację.** Banki nigdy nie podają w przesyłanych wiadomościach linków do stron transakcyjnych. Listy, wiadomości e-mail lub telefony w takich sprawach należy traktować jako próbę wyłudzenia poufnych informacji. Nie wolno odpowiadać na tego typu wiadomości oraz przekazywać swoich poufnych danych. Bezzwłocznie należy skontaktować się z Bankiem i poinformować o zdarzeniu.
- Należy sprawdzać na stronie internetowej Banku, jakie zabezpieczenia stosowane są w serwisie internetowym.** Przy każdym logowaniu bezwzględnie należy stosować się do zasad bezpieczeństwa tam opublikowanych. W przypadku pojawienia się jakichkolwiek nieprawidłowości natychmiast należy skontaktować się z pracownikiem Banku.
- Komputer lub telefon komórkowy podłączony do Internetu musi mieć zainstalowany program antywirusowy i musi on być na bieżąco aktualizowany.** Niezbędna jest również aktywacja istotnych modułów w pakiecie ochronnym takich jak monitor antywirusowy, skaner poczty czy firewall. Częstym błędem jest wyłączanie wspomnianych modułów w celu redukcji obciążenia systemu.

- 4) **Należy dokonywać płatności internetowych tylko z wykorzystaniem „pewnych komputerów”.** Nie należy dokonywać płatności internetowych z komputerów znajdujących się w miejscach publicznych np. w kawiarenkach internetowych lub na uczelni.
- 5) **W celu upewnienia się, że Dostawca Internetu korzysta on bezpiecznych kanałów dystrybucji tej usługi należy skontaktować się z nim skontaktować.** Należy zwracać szczególną uwagę na jakość i bezpieczeństwo usług internetowych dostarczanych przez Dostawcę. Jeśli istnieją jakieś wątpliwości w tym zakresie, użytkownik ma prawo zapytać się Dostawcy o jakość oferowanego przez niego bezpieczeństwa.
- 6) **Na własnym komputerze należy instalować tylko legalne oprogramowanie.** Programy niewiadomego pochodzenia, w tym ściągane za pośrednictwem programów typu Peer-to-Peer (P2P) mogą być przygotowane przez hakerów i zawierać wirusy lub inne szkodliwe oprogramowanie.
- 7) **Zaleca się okresowe wykonanie skanowania komputera, w szczególności przed wejściem na stronę internetową banku i wykonaniem jakiejkolwiek transakcji.** Większość programów antywirusowych przy włączonym monitorze antywirusowym ma detekcję (wykrywalność) taką samą jak skaner antywirusowy i nie ma konieczności skanowania komputera. Jest jednak część programów, których detekcja monitora antywirusowego jest niższa aniżeli skanera, powoduje to jednak lukę w systemie bezpieczeństwa.
- 8) **Należy aktualizować system operacyjny i istotne dla jego funkcjonowania aplikacje np. przeglądarki internetowe.** Hakerzy stale szukają luk w oprogramowaniu, które są następnie wykorzystywane do przestępstw internetowych. Producenci systemów operacyjnych i aplikacji publikują stosowne „łaty”, których celem jest usuwanie podatności ich produktów na ataki przeprowadzane za pośrednictwem znalezionych luk.
- 9) **Nie należy otwierać wiadomości i dołączonych do nich załączników nieznanego pochodzenia.** Często załączniki takie zawierają wirusy lub inne oprogramowanie, które pozwala na szpiegowanie działań użytkownika.
- 10) **Należy unikać stron zachęcających do obejrzenia bardzo atrakcyjnych treści lub zawierających atrakcyjne okazje.** Szczególnie niebezpieczne mogą być strony internetowe zawierające treści pornograficzne. Ponadto z pozoru niewinne strony zawierające programy typu „freeware” również mogą być bardzo niebezpieczne, ponieważ hakerzy bardzo często dekompilują je uzupełniając o złośliwy kod.
- 11) **Po zalogowaniu do systemu transakcyjnego nie należy odchodzić od komputera, a po zakończeniu pracy należy wylogować się i zamknąć przeglądarkę.**
- 12) **Jeśli przy logowaniu pojawiają się nietypowe komunikaty lub prośby o podanie danych osobowych lub dodatkowe pola z pytaniem o hasła do autoryzacji, natychmiast należy zgłosić problem do Banku.**
- 13) **Nie należy wchodzić na stronę internetową Banku za pośrednictwem linków znajdujących się w przychodzących do użytkownika mailach (Phishing).** Należy używać do tego celu adresu podanego użytkownikowi przez Bank, z którym zawarł umowę o otwarcie i prowadzenia rachunku bankowego. Nie jest również wskazane wykorzystywanie mechanizmu „Zakładek” (Firefox) lub „adresów Ulubionych” (Internet Explorer), gdyż istnieją szkodliwe obiekty, które potrafią modyfikować zachowane tam adresy.
- 14) **Nigdy nie należy używać wyszukiwarek internetowych do znalezienia strony logowania Twojego Banku.** Wyszukane w nich linki mogą prowadzić do fałszywych stron lub stron zawierających wirusy.
- 15) **Przed zalogowaniem należy sprawdzić, czy połączenie z Bankiem jest bezpieczne.** Adres witryny internetowej Twojego Banku powinien rozpoczynać się od skrótu: „https://”, a nie „http://”. Brak litery „s” w skrócie „http” oznacza brak szyfrowania, czyli, że dane użytkownika są transmitowane przez internet tekstem jawnym, co naraża użytkownika na ogromne niebezpieczeństwo.
- 16) **Należy sprawdzać prawidłowość certyfikatu.** Zanim wpisze się identyfikator bądź login i hasło należy sprawdzić, czy połączenie z bankiem odbywa się z wykorzystaniem szyfrowania. Jeżeli odszuka się symbol kłódki, należy kliknąć na niego dwa razy, aby sprawdzić, czy wyświetlony certyfikat jest ważny i czy został wydany dla Banku użytkownika. Jeśli certyfikat utracił ważność lub nie został wystawiony dla Banku użytkownika, albo nie można go zweryfikować należy zrezygnować z połączenia.
- 17) **Nigdy nie należy udostępniać osobom trzecim identyfikatora ani hasła dostępu.** Identyfikator jest poufnym numerem nadawanym przez Bank, użytkownik nie może go zmienić.
- 18) **Nie należy zapisywać nigdzie haseł służących do logowania i należy pamiętać o ich regularnej zmianie.** Idealnym rozwiązaniem jest zmienianie haseł raz w miesiącu, ale o ile system tego nie wymusi należy zmieniać je przynajmniej raz na dwa miesiące używając kombinacji dużych i małych liter oraz cyfr.
- 19) **Należy sprawdzać datę ostatniego poprawnego oraz niepoprawnego logowania do systemu.**
- 20) **Należy korzystać z infolinii udostępnionej przez Bank.** Użytkownik zawsze ma prawo skorzystać z infolinii Banku, jeśli ma wątpliwości w zakresie bezpiecznych transakcji bankowych wykonywanych za pośrednictwem Internetu.
- 21) **Należy regularnie odwiedzać Portal „Bezpieczny Bank” na stronie internetowej ZBP – www.zbp.pl** Jeśli użytkownik chce wiedzieć więcej na temat bezpiecznego posługiwania się bankowością elektroniczną, w tym internetową regularnie powinien odwiedzać ten Portal. Tam fachowcy z zakresu bezpieczeństwa banku wyjaśniają jak uniknąć czyhających w sieci niebezpieczeństw.

Zarząd OK Banku Spółdzielczego