Obowiązki ostrożnościowe użytkownika	
1.	Logowanie oraz wykonywanie dyspozycji za pośrednictwem elektronicznych kanałów dostępu wyłącznie osobiście, z użyciem indywidualnych instrumentów uwierzytelniających.
2.	Zachowanie w tajemnicy informacji zapewniających bezpieczne korzystanie z usług bankowości elektronicznej, w tym informacji przekazanych bankowi dla celów weryfikacji oraz nieudostępnianie i nieujawnianie innym osobom (w tym osobom bliskim lub pracownikom banku) instrumentów uwierzytelniających.
3.	Nieprzekazywanie danych uwierzytelniających osobom trzecim, zwłaszcza podczas przychodzącej rozmowy telefonicznej, nawet jeżeli rozmówca przedstawia się jako pracownik banku.
4.	Nieprzekazywanie danych uwierzytelniających na stronach internetowych lub w aplikacjach, do których dostęp uzyskiwany jest przez linki przesłane przez nieznane osoby, w tym także na stronach internetowych zawierających znaki graficzne banku.
5.	Nieprzekazywanie danych uwierzytelniających w celu otrzymania płatności przy transakcjach na odległość.
6.	Należyte zabezpieczenie urządzeń i oprogramowania, których klient używa w celu korzystania z usług bankowości elektronicznej, tj. stosowanie legalnego i zaktualizowanego oprogramowania, stosowanie aktualnego oprogramowania antywirusowego, antyspamowego oraz typu *firewall*, najnowszych wersji przeglądarek internetowych oraz niestosowanie aplikacji automatyzujących.
7.	Przechowywanie karty płatniczej oraz kodu PIN z zachowaniem należytej staranności i zasad bezpieczeństwa, np. nieprzechowywanie ich razem, niezapisywanie kodu PIN w telefonie, komputerze lub notatniku.
8.	Przechowywanie indywidualnych danych uwierzytelniających bankowości elektronicznej z zachowaniem należytej staranności, w tym obowiązek nieprzechowywania ich razem.
9.	Nieudostępnianie karty płatniczej lub kodu PIN osobom nieuprawnionym, w tym bliskim lub pracownikom banku.
10.	Nieudostępnianie danych karty w celach innych niż dokonanie transakcji, zgłoszenie reklamacji, czy zgłoszenie zablokowania karty.
11.	Pobieranie aplikacji mobilnej banku wyłącznie z autoryzowanego sklepu z aplikacjami.
12.	Nieotwieranie oraz nieodpowiadanie na wiadomości e-mail od nieznanych nadawców oraz nieotwieranie nieznanych plików z załączników.
13.	Zachowywania fabrycznych zabezpieczeń urządzeń mobilnych.

Dodatkowe klauzule informacyjne	
1.	Informacja, że bank nigdy nie wymaga ujawnienia przez użytkownika haseł do bankowości elektronicznej (poza miejscami do tego przeznaczonymi w ramach bankowości internetowej).
2.	Informacja, że bank nigdy nie wymaga zainstalowania dodatkowego oprogramowania oprócz aplikacji banku pobranej z autoryzowanego sklepu z aplikacjami mobilnymi.
3.	Ostrzeżenie, że w przypadku instalacji aplikacji pozwalającej na zdalny dostęp do urządzenia, narażone zostają dane użytkownika i środki na jego rachunku.
4.	Zalecenie ochrony haseł używanych do logowania w aplikacjach i na stronach internetowych, jeżeli zostały w nich zapisane dane karty.
5.	Zalecenie zachowania ostrożności w przypadku płatności kartą w Internecie, wprowadzania PIN-u w terminalu lub bankomacie.
6.	Zalecenie monitorowania poprawności stanu rachunku.