Millennium bank
Biuro maklerskie

**Informacja**
**o zasadach uzyskiwania dostępu do usług internetowych oraz telefonicznych świadczonych przez Biuro Maklerskie Banku Millennium S.A. oraz zasadach zachowania bezpieczeństwa podczas korzystania z tych usług**
(zawiera informacje dodatkowe dla klientów Biura Maklerskiego Banku Millennium S.A. wg stanu na dzień 30 lipca 2022r.)

## I. Dostęp do usług świadczonych przez Internet oraz telefonicznie

- **umowy zawierane od 25 lipca 2006 r.**

Jeśli Inwestor zawiera z Biurem Maklerskim Banku Millennium S.A. (zwanym dalej Biurem Maklerskim) „Umowę o wykonywanie zleceń nabycia lub zbycia instrumentów finansowych oraz prowadzenie rachunków" (zwaną dalej Umową) – na podstawie tej Umowy Inwestor otrzymuje dostęp do usług świadczonych z wykorzystaniem Internetu oraz telefonicznie.

W przypadku usług internetowych - nie ma konieczności składania odrębnych wniosków o nadanie uprawnień do tych usług, o ile dostęp do tych usług uzyskuje właściciel rachunku inwestycyjnego. Wymagane jest natomiast złożenie odrębnego wniosku o nadanie uprawnień internetowych pełnomocnikowi do rachunku inwestycyjnego. Usługi internetowe świadczone są z wykorzystaniem:

- aplikacji ePromakPlus (w dokumentach oficjalnych zwanej Serwisem maklerskim) służącej do składania zleceń, dyspozycji i wniosków,
- Serwisu informacyjnego stanowiącego część strony millenniumbm.pl i zawierającego informacje dedykowane wyłącznie klientom Biura Maklerskiego,
- programu Statica - dodatkowego programu dedykowanego do obserwacji notowań w Internecie lub na urządzeniach mobilnych, np. telefony komórkowe i tablety.

Na podstawie Umowy Inwestor otrzyma dostęp do wszelkich informacji udostępnianych przez Biuro Maklerskie bezpłatnie. Dostęp do informacji płatnych wymaga złożenia odpowiedniego wniosku, który może zostać złożony w Punkcie Obsługi Klienta (zwanym dalej POK), telefonicznie lub w aplikacji ePromakPlus.

Szczegółowy sposób korzystania z usług internetowych opisany jest w „Instrukcji korzystania z Serwisu maklerskiego oraz Serwisu informacyjnego Biura Maklerskiego Banku Millennium S.A." dostępnej w Serwisie informacyjnym pod linkiem Instrukcja internetowa oraz w Komunikacie Obsługa dyspozycji zdalnych wdrażającym aktualną treść instrukcji dostępnym na stronie millenniumbm.pl w zakładce „Regulacje i opłaty" – „Komunikaty".

Szczegółowy sposób korzystania z usług telefonicznych opisany jest w Serwisie informacyjnym pod linkiem Instrukcja telefoniczna oraz w Komunikacie Obsługa dyspozycji zdalnych dostępnym na stronie millenniumbm.pl w zakładce „Regulacje i opłaty" – „Komunikaty".

- **umowy zawarte przed 25 lipca 2006 r. oraz umowy, na których nie zostały uruchomione usługi internetowe lub telefoniczne**

Inwestor może otrzymać dostęp do usługi internetowej oraz telefonicznej pod warunkiem zaktualizowania Umowy (zawarcia nowej wersji Umowy). W przypadku zawarcia nowej Umowy obowiązują identyczne zasady uzyskiwania dostępu do usługi internetowej i telefonicznej jak opisane powyżej. Sposób aktualizowania Umowy opisany jest na ogólnodostępnej stronie internetowej w opcji pod nazwą „Aktualizacja umowy".

## II. Odbiór loginów i haseł w POK

Jeśli Inwestor zawiera Umowę bezpośrednio w POK - łącznie z Umową otrzyma:

- **w przypadku usług internetowych:**
  1. Kopertę z hasłem do aplikacji ePromakPlus,
  2. Kartę informacyjną zawierającą login do aplikacji ePromakPlus oraz login i hasło do Serwisu informacyjnego.

  Dostęp do programu Statica nadawany jest na podstawie odrębnego wniosku, który może zostać złożony w POK, telefonicznie lub w aplikacji ePromakPlus. Login i hasło do programu Statica przesyłane są za pośrednictwem aplikacji ePromakPlus

- **w przypadku usługi telefonicznej:**
  1. Formularz z hasłem telefonicznym (w POK Inwestor może samodzielnie ustalić hasło, którym będzie się identyfikować składając zlecenia, dyspozycje i wnioski telefoniczne).

Hasła do usług internetowych oraz usługi telefonicznej odebrane w POK są aktywne (można w pełni korzystać z tych usług).

## III. Odbiór loginów i haseł poza POK

Jeśli Inwestor zawiera z Biurem Maklerskim Umowę w PUM (czyli Punkcie Usług Maklerskich - oddziale Banku Millennium prowadzącym obsługę klientów Biura Maklerskiego) lub aktualizuje Umowę drogą korespondencyjną (zawiera kolejną Umowę w aktualnej wersji) nie otrzymuje loginów i haseł w momencie zawarcia Umowy. Dane identyfikacyjne przekazywane są Inwestorowi w następujący sposób:

- **w przypadku usług internetowych:**
  - w przypadku, gdy Inwestor podał numer telefonu komórkowego:
    1. login do aplikacji ePromakPlus – w zaszyfrowanym pliku przesłanym na adres e-mail,
    2. hasło do aplikacji ePromakPlus – w wiadomości SMS. Otrzymane hasło nie jest aktywne – przed próbą logowania do aplikacji ePromakPlus należy je aktywować zgodnie z zasadami zawartymi w części IV niniejszej informacji,
    3. login i hasło do Serwisu informacyjnego – w zaszyfrowanym pliku przesłanym na adres e-mail. Otrzymane hasło jest aktywne;
  - w przypadku, gdy Inwestor nie podał numeru telefonu komórkowego:
    1. login do aplikacji ePromakPlus – w zaszyfrowanym pliku przesłanym na adres e-mail,
    2. hasło do aplikacji ePromakPlus – listem poleconym na adres korespondencyjny. Otrzymane hasło nie jest aktywne – przed próbą logowania do aplikacji ePromakPlus należy je aktywować zgodnie z zasadami zawartymi w części IV niniejszej informacji,
    3. login i hasło do Serwisu informacyjnego – w zaszyfrowanym pliku przesłanym na adres e-mail. Otrzymane hasło jest aktywne;

- login i hasło do programu Statica przesyłane są za pośrednictwem aplikacji ePromakPlus;

○ **w przypadku usługi telefonicznej:**

- hasło telefoniczne przesyłane jest za pośrednictwem aplikacji ePromakPlus. Otrzymane hasło jest aktywne.

## IV. Aktywacja haseł.

W przypadku konieczności aktywacji hasła internetowego do aplikacji ePromakPlus lub hasła telefonicznego Inwestor powinien zadzwonić pod jeden z poniższych numerów telefonów:

- **Gdańsk:** **58 323 79 41, 58 323 79 42; 58 323 79 43**
- **Warszawa:** **801 601 601; 22 598 26 87;**

Podczas procesu aktywacji hasła internetowego lub telefonicznego Inwestor powinien mieć dostęp do zawartej z Biurem Maklerskim Umowy.

Aktywacja haseł wykonywana jest przez pracownika Biura Maklerskiego po udzieleniu przez Inwestora poprawnych odpowiedzi na zadane pytania. Pytania mogą dotyczyć danych personalnych Inwestora, numeru rachunku inwestycyjnego oraz rodzaju i szczegółów usług, z których Inwestor korzysta.

## V. Zmiana haseł

○ **zmiana hasła do aplikacji ePromakPlus**

Aplikacja ePromakPlus wymusza zmianę hasła podczas pierwszego logowania.

Z uwagi na możliwość składania zleceń oraz innych dyspozycji na rachunek Inwestora - zaleca się regularną samodzielną zmianę hasła internetowego do aplikacji ePromakPlus. Hasło internetowe do aplikacji ePromakPlus można zmienić klikając w tej aplikacji w ikonę zmiany hasła (ikona zawiera rysunek kłódki).

W przypadku utraty hasła do aplikacji ePromakPlus – o zmianę hasła można się zwrócić w nastepujący sposób:

(1) w POK (hasło zostanie przekazane w POK);

(2) korespondencyjnie - poprzez przesłanie wniosku o ustalenie i przesłanie nowego hasła (wymagane jest notarialne potwierdzenie podpisu Inwestora) (sposób przekazania hasła określa wniosek);

(3) składając wniosek o zmianę hasła drogą telefoniczną (wymagane jest w takim przypadku posiadanie hasła telefonicznego) (pracownik Biura Maklerskiego poinformuje o dostępnym sposobie przekazania hasła);

(4) poprzez podpisanie w PUM Umowy w zakresie ustalania warunków obsługi dyspozycji telefonicznych i internetowych zawierającej wniosek o nadanie uprawnień do usługi internetowej;

○ **zmiana hasła do Serwisu informacyjnego**

Serwis informacyjny nie posiada mechanizmów wymuszających zmianę hasła.

Mimo iż Serwis informacyjny nie przechowuje indywidualnych informacji o Inwestorze oraz nie ma w nim możliwości składania zleceń - zaleca się regularną zmianę hasła internetowego do Serwisu informacyjnego.

Hasło do Serwisu informacyjnego można zmienić w Serwisie informacyjnym w zakładce „Narzędzia” - „Zmiana hasła”.

W przypadku utraty hasła do Serwisu informacyjnego – o zmianę hasła można się zwrócić w nastepujący sposób:

(1) w POK;

(2) korespondencyjnie - poprzez przesłanie wniosku o ustalenie nowego hasła (z adresu e-mail podanego wcześniej Biuru Maklerskiemu);

(3) składając wniosek o przywrócenie hasła startowego drogą telefoniczną (wymagane jest w takim przypadku posiadanie hasła telefonicznego);

(4) poprzez złożenie wniosku w aplikacji ePromakPlus.

W przypadkach (1) – (4) zostanie przywrócone hasło startowe, czyli hasło, które zostało ustalone w momencie uzyskiwania dostępu do Serwisu informacyjnego po raz pierwszy;

○ **zmiana hasła do programu Statica**

Inwestor nie ma możliwości samodzielnej zmiany hasła do programu Statica.

W celu wymiany hasła do programu Statica Inwestor powinien złożyć odpowiedni wniosek telefoniczny lub internetowy w aplikacji ePromakPlus, lub przesłać wniosek o zmianę hasła drogą korespondencyjną (z adresu e-mail podanego wcześniej Biuru Maklerskiemu).

Nowe hasło do programu Statica przesyłane jest zawsze za pośrednictwem aplikacji ePromakPlus;

○ **zmiana hasła telefonicznego**

Inwestor nie ma możliwości samodzielnej zmiany hasła telefonicznego.

O zmianę hasła telefonicznego można się zwrócić w nastepujący sposób:

(1) bezpośrednio w POK (w takim przypadku Inwestor ustala hasło telefoniczne na zasadach określonych w części II niniejszej instrukcji);

(2) korespondencyjnie - poprzez przesłanie formularza z nowym hasłem (wymagane jest notarialne potwierdzenie podpisu Inwestora);

(3) korespondencyjnie - poprzez przesłanie wniosku o ustalenie i przesłanie nowego hasła telefonicznego (wymagane jest notarialne potwierdzenie podpisu Inwestora) (sposób przesłania hasła określa wniosek);

(4) poprzez złożenie wniosku w aplikacji ePromakPlus (sposób przesłania hasła określa wniosek);

(5) poprzez podpisanie w PUM Umowy w zakresie ustalania warunków obsługi dyspozycji telefonicznych i internetowych zawierających wniosek o nadanie uprawnień do usługi telefonicznej-.

W przypadkach (3) – (5) nowe hasło telefoniczne ustala Biuro Maklerskie.

## VI. Podstawowe zasady bezpieczeństwa podczas korzystania z usług internetowych

Znaczna część kanału umożliwiającego świadczenie internetowych usług maklerskich znajduje się poza bezpośrednią kontrolą Biura Maklerskiego. W związku z tym Biuro Maklerskie nie może ponosić odpowiedzialności za czynności wynikające z faktu ingerencji osób trzecich w komputer osobisty klienta. Istotnym elementem wpływającym na bezpieczeństwo transakcyjnych systemów elektronicznych jest indywidualne zachowanie użytkowników tych systemów. Dlatego w celu zwiększenia własnego bezpieczeństwa zaleca się korzystanie z poniżej przedstawionych dobrych praktyk:

**1. Dbaj o bezpieczeństwo systemu operacyjnego i oprogramowania użytkowego.**

Krytyczne błędy bezpieczeństwa systemów operacyjnych i przeglądarek internetowych mogą być przyczyną wykorzystania komputera bez wiedzy użytkownika. Dlatego regularnie aktualizuj system oraz aplikacje służące do przeglądania stron internetowych. Korzystaj z funkcji powiadamiania o dostępnych aktualizacjach. Poprawki pobieraj tylko ze stron producentów oprogramowania lub wykorzystuj automatyczne mechanizmy wykonujące aktualizację. Szczególną uwagę zwracaj na krytyczne aktualizacje dotyczące bezpieczeństwa. W ten sposób zwiększysz szansę wyeliminowania podatności swojego komputera na ataki oszustów komputerowych.

**2. Zwracaj uwagę na instalowane i uruchamiane oprogramowanie. Użytkuj tylko legalne oprogramowanie.**

Prawdopodobieństwo instalacji aplikacji szpiegujących podczas użytkowania oprogramowania pochodzącego z niewiadomego źródła jest realne. Nigdy nie instaluj i nie uruchamiaj oprogramowania, którego pochodzenia nie jesteś pewny. Szczególną uwagę zwróć na programy przesyłane na e-maila lub przez internetowe komunikatory. Pod żadnym pozorem nie uruchamiaj niepewnych aplikacji.
Korzystaj tylko z legalnego oprogramowania .

**3. Zabezpiecz komputer oprogramowaniem antywirusowym oraz zaporą sieciową (firewall).**

W celu zabezpieczenia swojego systemu oraz danych osobistych korzystaj z programu antywirusowego, który zabezpiecza Twój komputer przed szkodliwym oprogramowaniem. Ponadto korzystaj z zapory internetowej, która kontroluje i chroni przesyłanie informacji pomiędzy Twoim komputerem a Internetem. Pamiętaj o regularnej aktualizacji oprogramowania zabezpieczającego. W przypadku tego typu aplikacji staraj się unikać wersji testowych.

**4. Stosuj bezpieczne hasła i dbaj o ich poufność.**

Autoryzacja w aplikacji transakcyjnej została oparta na weryfikacji unikatowego identyfikatora (login) oraz hasła. Biuro Maklerskie udostępnia również możliwość logowania z wykorzystaniem sprzętowego tokena generującego hasła dynamicznie. Środki te mają zapewnić poufność dostępu do systemu transakcyjnego. Dlatego loguj się osobiście, pod żadnym pozorem nikomu nie ujawniaj danych umożliwiających dostęp do aplikacji transakcyjnej. Przekazanie loginu, hasła oraz tokena osobom trzecim stanowi naruszenie regulaminu świadczenia usług maklerskich. Odpowiednio zabezpiecz dane umożliwiające dostęp do aplikacji transakcyjnej.
Biuro Maklerskie nigdy nie kontaktuje się z klientami za pośrednictwem e-maila w celu zmiany lub potwierdzenia hasła. Pracownicy Biura Maklerskiego nigdy sami nie dzwonią z prośbą o podanie hasła lub innych danych wrażliwych. Podanie hasła jest konieczne jedynie, gdy Inwestor z własnej inicjatywy zadzwoni do HelpDesk w celu złożenia telefonicznej Dyspozycji:
- aktywowania Tokena przesłanego pocztą,
- synchronizacji Tokena,
- odblokowania Tokena.

Pamiętaj, o regularnej zmianie hasła. Informacje dotyczące sposobu zmiany hasła znajdują się w pkt. V. 'Zmiana haseł'. Definiując nowe hasło wykorzystuj wielkie i małe litery, cyfry oraz znaki specjalne. W przypadku korzystania z różnych internetowych aplikacji finansowych nie stosuj do autoryzacji identycznych haseł. Nie korzystaj z funkcji zapamiętywania haseł, które udostępniają przeglądarki internetowe.

**5. Dbaj o bezpieczeństwo fizyczne komputera osobistego.**

Bezpieczeństwo Twoich danych to nie tylko świadome użytkowanie oprogramowania czy też stosowanie się do dobrych praktyk dotyczących bezpieczeństwa hasła. Szczególnie w przypadku korzystania z komputera przenośnego zachowaj najwyższą ostrożność i nie zostawiaj go w miejscach publicznych bez opieki. Pozostawienie komputera wiąże się nie tylko z ryzykiem utraty urządzenia ale daje również możliwość bezpośredniej ingerencji w użytkowane oprogramowanie. Dlatego odchodząc od komputera pamiętaj aby wylogować się z aplikacji transakcyjnej oraz zablokować dostęp do systemu operacyjnego. W celu zabezpieczenia swojego laptopa przed kradzieżą używaj specjalnych linek zabezpieczających.

**6. Sprawdzaj czy logujesz się do systemu transakcyjnego Biura Maklerskiego.**

Nie sugeruj się wyglądem strony umożliwiającej zalogowanie się do aplikacji transakcyjnej. Zwracaj szczególną uwagę czy zostało ustanowione połączenie z witryną: https://epp.millenniumbm.pl. Połączenie z Biurem Maklerskim odbywa się przy użyciu protokołu SSL z odpowiedniej długości kluczem szyfrującym. Technologia ta daje gwarancje poufności przy korzystaniu z usług Biura Maklerskiego. Zastosowanie certyfikatu bezpieczeństwa umożliwia sprawdzenie czy osoby nieuprawnione nie próbują podszyć się pod dany serwis. Dlatego zalecamy, sprawdzanie szczegółów certyfikatu dotyczących właściciela witryny oraz ważności certyfikatu.
Pamiętaj, że Biuro Maklerskie nigdy nie wysyła e-maili do klientów z treścią sugerującą zalogowanie się do aplikacji poprzez linki zawarte w treści e-maila. Takie działanie należy potraktować jako potencjalną próbę wyłudzenia danych i jak najszybciej zgłosić pracownikom Biura Maklerskiego.

**7. Bądź świadomym użytkownikiem internetowych aplikacji transakcyjnych.**

Dość istotnym faktem wpływającym na bezpieczeństwo transakcyjnych systemów elektronicznych jest poprawne postępowanie użytkowników tych systemów. Świadomość mechanizmów potencjalnych zagrożeń wynikających z wykorzystywania internetowych systemów transakcyjnych może ograniczyć ryzyko wyłudzenia przez osoby trzecie danych i uzyskania nieautoryzowanego dostępu do rachunku inwestycyjnego. Prosimy o zapoznanie się z informacją dotyczącą prawidłowego ustawienia przeglądarki internetowej opisane w pomocy technicznej dla użytkowników systemu transakcyjnego dostępnej w tym systemie pod ikoną ze znakiem zapytania. Zalecamy zapoznanie się dodatkowymi informacjami, o których mowa na końcu niniejszego działu oraz informacjami dotyczącymi kwestii bezpieczeństwa aplikacji transakcyjnych prezentowanymi przez Komisję Nadzoru Finansowego czy Związek Banków Polskich zamieszczanych na stronach internetowych.

**8. Reaguj w przypadku wystąpienia lub podejrzenia wystąpienia nadużycia.**

Jeśli zostałeś ofiarą przestępców i Twoje środki są zagrożone zgłoś niezwłocznie ten fakt do HelpDesk-u Biura Maklerskiego. Informuj również jeśli masz wątpliwości w zakresie bezpieczeństwa, zauważyłeś niestandardowe działanie aplikacji transakcyjnej lub zostałeś poproszony o przesłanie pocztą elektroniczną swoich danych do logowania lub wykonania innych czynności związanych z koniecznością podania loginu i hasła, bądź otrzymałeś „od Biura Maklerskiego" wiadomość dotyczącą konieczności instalacji aplikacji lub certyfikatu.

Bardziej szczegółowe informacje dotyczące zagrożeń oraz zasad weryfikacji i zachowania bezpieczeństwa udostępniane są w Serwisie informacyjnym Biura Maklerskiego (zakładka „Bezpieczeństwo") oraz na formatce do logowania do aplikacji ePromakPlus (link „Biuro Maklerskie przypomina o podstawowych zasadach bezpieczeństwa").

## VII. Podstawowe zasady bezpieczeństwa podczas korzystania z usług telefonicznych

Działając w dobrze pojętym interesie własnym, ale przede wszystkim w interesie Inwestora, w ramach świadczonych usług telefonicznych, Biuro Maklerskie stosuje odpowiednie zabezpieczenia dostępu do danych wrażliwych związanych z właściwą identyfikacją, uwierzytelnieniem tożsamości i autoryzacją transakcji zlecanych telefonicznie. Poniżej przedstawiono najistotniejsze zasady bezpiecznego korzystania z usług telefonicznych. Ich znajomość minimalizuje potencjalne ryzyka związane z telefonicznymi kontaktami Inwestora z Biurem Maklerskim oraz Biura Maklerskiego z Inwestorem.

1. **Biuro Maklerskie musi zidentyfikować i uwierzytelnić tożsamość Inwestora.**

Przed ujawnieniem jakiejkolwiek informacji związanej z usługami świadczonymi w ramach podpisanej umowy, Biuro Maklerskie musi przeprowadzić proces identyfikacji i uwierzytelnienia osoby dzwoniącej (czyli zweryfikować, że ma do czynienia z osobą uprawnioną do otrzymania informacji, której wymaga).

2. **Opis metod identyfikacji i autoryzacji.**

Stosowane przez Biuro Maklerskie mechanizmy identyfikacji i uwierzytelniania Inwestorów, mają odzwierciedlenie w zapisach umowy i regulaminu świadczenia usług maklerskich. Dodatkowe wyjaśnienia znajdują się w niniejszym dokumencie powyżej.

3. **Informacje o aktualnych numerach telefonów Biura Maklerskiego.**

Biuro Maklerskie publikuje informacje dotyczące oficjalnych numerów telefonów na stronie internetowej millenniumbm.pl oraz wywiesza w POK. Aktualne informacje dotyczące numerów telefonów umieszczane są także na wyciągach kwartalnych przesyłanych na oficjalny adres Inwestora. Należy korzystać tylko z tych oficjalnych numerów telefonów.

Nie należy korzystać z numerów telefonów odnalezionych w wyszukiwarkach internetowych.

4. **Inwestor zawsze ma prawo sprawdzić, czy telefonuje do niego pracownik Biura Maklerskiego.**

Dzwoniąc do Inwestora pracownik Biura Maklerskiego powinien dawać możliwość sprawdzenia – poprzez oddzwonienie na znany Inwestorowi numer – czy połączenie jest faktycznie wykonane przez pracownika Biura Maklerskiego. Ponieważ obecne technologie umożliwiają przekierowanie połączenia na inny numer telefonu niż wybrany przez użytkownika, dlatego, w przypadku podejrzenia co do tego, czy połączenie nastąpiło z Biurem Maklerskim można to zweryfikować np. pytając pracownika o stan rachunku. Należy jednak pamiętać, że Biuro Maklerskie nie udzieli takiej informacji bez identyfikacji Inwestora.

5. **Biuro Maklerskie nigdy nie pyta telefonicznie o dane wrażliwe nie służące do bezpośredniej identyfikacji tożsamości.**

W ramach wykonywanych do Inwestorów telefonów wychodzących w procesach identyfikacji pracownik Biura Maklerskiego nie zadaje pytań o dane umożliwiające dokonanie transakcji, w przypadku, gdy Inwestor nie zamierza jej wykonać w ramach trwającego połączenia, w szczególności pracownik Biura Maklerskiego nie pyta o numery PIN, numery rachunków bankowych, hasła dostępu do systemu internetowego.

6. **Podczas rozmowy Biuro Maklerskie może posługiwać się danymi osobowymi Inwestora.**

W trakcie rozmów z Inwestorami w procesach identyfikacji Biuro Maklerskie może wykorzystywać dane osobowe, jednak ze względu na ryzyko ujawnienia tych danych osobom nieuprawnionym (potencjalnie podszywającym się pod pracownika Biura Maklerskiego, szczególnie podczas rozmów, gdzie stroną inicjującą jest Biuro Maklerskie) pracownik Biura Maklerskiego nie powinien zwracać się z prośbą o ich podanie w całości (pytania powinny być ograniczone do wybranych znaków z numerów PESEL, numerów dokumentów tożsamości, wybrane dane z adresu etc.).

7. **Nie należy dzwonić na numery, których autentyczność nie jest pewna.**

Biuro Maklerskie nie wysyła do Inwestorów wiadomości e-mail, sms oraz nie wykonuje rozmów wychodzących zmuszających do zwrotnego kontaktu telefonicznego na nieznane numery telefonów. W przypadku odebrania takiego żądania, Klient powinien zweryfikować jego autentyczność poprzez kontakt z infolinią Biura Maklerskiego zlokalizowaną pod znanym i właściwym numerem telefonu.

8. **Nie każda rozmowa z Biurem Maklerskim wymaga uwierzytelnienia.**

Nie wszystkie telefoniczne kontakty z Biurem Maklerskim wymagają identyfikacji i uwierzytelnienia Inwestora. Zapytanie o informacje ogólnodostępne, w tym o ofertę Biura Maklerskiego lub jej przedstawienie przez pracownika Biura Maklerskiego nie niosą ze sobą konieczności identyfikacji.

9. **Każda rozmowa z Biurem Maklerskim może zostać nagrana.**

W celach udokumentowania swojej działalności oraz kontroli jakości świadczonych usług Biuro Maklerskie rejestruje rozmowy z Inwestorami. Inwestor ma prawo odmówić prowadzenia rozmowy nagrywanej przez Biuro Maklerskie, jednak może to uniemożliwić skorzystanie z usługi.

10. **Telefonu z Biura Maklerskiego należy spodziewać się tylko w dni robocze w godzinach pracy POK.**

Biuro Maklerskie dąży do tego, aby rozmowy wykonywane do Inwestorów nie były realizowane w godzinach wieczornych i nocnych oraz w niedziele i święta, chyba że postanowienia umów z Inwestorami lub ustalenia indywidualne stanowią inaczej.

11. **Nie należy udostępniać swoich danych identyfikacyjnych osobom nieuprawnionym.**

Nie należy podawać osobom trzecim danych osobowych, a w szczególności hasła służącego do składania dyspozycji telefonicznych oraz numeru rachunku inwestycyjnego prowadzonego przez Biuro Maklerskie.

12. **Należy starannie przechowywać swoje dane identyfikacyjne i uwierzytelniające.**

Inwestor powinien zachować szczególną ostrożność w przechowywaniu identyfikatorów, haseł i innych danych wykorzystywanych w procesach identyfikacji i uwierzytelnienia tożsamości oraz autoryzacji. W przypadku ich utraty powinien bezzwłocznie skontaktować się z Biurem Maklerskim. Nie należy podawać osobom trzecim danych osobowych, a w szczególności hasła służącego do składania dyspozycji telefonicznych oraz numeru rachunku inwestycyjnego prowadzonego przez Biuro Maklerskie.

13. **Należy dbać o poufność danych w trakcie kontaktu z Biurem Maklerskim.**

Kontakt wymagający identyfikacji i uwierzytelnienia tożsamości powinien być przeprowadzony w warunkach umożliwiających Inwestorowi zachowanie poufności identyfikatorów, haseł i innych kodów dostępowych do usług telefonicznych. Nie należy nawiązywać połączenia telefonicznego z Biurem Maklerskim w miejscach publicznych, pomieszczeniach, gdzie przebywa dużo osób, zatłoczonych środkach komunikacji itp.

14. **Należy wprowadzić do swojego telefonu komórkowego telefony do kontaktu z Biurem Maklerskim.**

W sytuacjach „kryzysowych" Inwestor powinien mieć możliwość szybkiego nawiązania kontaktu z Biurem Maklerskim np. w celu blokady usług telefonicznych i internetowych w przypadku podejrzenia poznania danych identyfikacyjnych przez osoby nieupoważnione, zgubienia tokena, etc.