

## ZASADY BEZPIECZEŃSTWA INFORMATYCZNEGO DOTYCZĄCE KORZYSTANIA Z SERWISU ESALIENS24 („SERWIS”)

### 1. Przed zalogowaniem do Serwisu, sprawdź:

- ✓ poprawność adresu internetowego Serwisu – właściwym adresem jest <https://esaliens24.pl>
- ✓ czy połączenie z Serwisem jest szyfrowane – zweryfikuj, czy adres rozpoczyna się od <https://>, a także czy na pasku okna przeglądarki pojawia się ikona z zamkniętą kłódką oraz poprawność certyfikatu bezpieczeństwa oraz datę jego ważności – certyfikat wystawiony jest przez Thawte Inc. dla agenta transferowego, Pekao Financial Services Sp. z o.o.
- ✓ czy wygląd strony nie budzi podejrzania. W przypadku zastrzeżeń zgłoś ten fakt na adres poczty elektronicznej [esaliens24@esaliens.pl](mailto:esaliens24@esaliens.pl)

### 2. Nie wchodź na stronę <https://esaliens24.pl> stosując wyszukiwarkę internetową. Wpisuj adres <https://esaliens24.pl> ręcznie lub wybieraj ten adres z tzw. ulubionych stron. Nie dodawaj do ulubionych stron adresu Serwisu, jeżeli znalazłeś ten adres w wyszukiwarce internetowej.

- 3. Pamiętaj o używaniu złożonego, trudnego do odgadnięcia Hasła dostępu. Hasło do Serwisu składa się z minimum 8 znaków, w tym przynajmniej z: **1 dużej litery, 1 małej litery, 1 cyfry lub znaku specjalnego**. Unikaj zapisywania Hasła w przeglądarkach internetowych lub w formie papierowej. Serwis posiada rozwiązanie umożliwiające odzyskanie Hasła.
- 4. Pamiętaj o cyklicznej zmianie Hasła. Zalecana jest zmiana Hasła nie rzadziej, niż co 30 dni.
- 5. Unikaj logowania do Serwisu z sieci niezaufanych, ogólnodostępnych, w których Twoje dane logowania mogą zostać przejęte a następnie wykorzystane do wykonania operacji bez Twojej wiedzy.
- 6. Pamiętaj o ryzyku wynikającym z korzystania z funkcjonalności zapamiętywania haseł i autouzupełniania formularzy w przeglądarce internetowej.
- 7. Nigdy nie pozostawiaj urządzenia z aktywnym połączeniem z Serwisem **bez swoje opieki**.
- 8. Kończąc wizytę w Serwisie użyj funkcji „Wyloguj”, która zapewni zamknięcie połączenia.
- 9. Sprawdzaj w Serwisie status ostatniego udanego i nieudanego logowania. W przypadku, gdy zauważysz nieprawidłowości w procesie logowania lub w informacjach dotyczących statusów logowania zgłoś ten fakt na adres poczty elektronicznej [esaliens24@esaliens.pl](mailto:esaliens24@esaliens.pl)

10. Pamiętaj, żeby Numer Klienta (Login), Hasło, adres email oraz telefon komórkowy, na który wysyłane są kody SMS do zatwierdzania zleceń zabezpieczyć przed dostępem osób trzecich.
11. Dbaj o bezpieczeństwo urządzenia, z którego następuje połączenie z Serwisem. Każde takie urządzenie powinno:
  - ✓ posiadać system antywirusowy z najnowszą wersją definicji wirusów i uaktualnień
  - ✓ posiadać zaporę bezpieczeństwa (Firewall) skonfigurowaną w sposób uniemożliwiający dostęp do urządzenia z sieci Internet przez osoby trzecie
  - ✓ posiadać zainstalowane wszystkie dostępne poprawki i uaktualnienia dla systemu operacyjnego urządzenia dotyczące bezpieczeństwa
  - ✓ posiadać zainstalowaną przeglądarkę internetową z zainstalowanymi aktualnymi poprawkami bezpieczeństwa dla urządzeń stacjonarnych: Internet Explorer w wersji minimum 11.0 lub Mozilla Firefox wersja minimum 40.0 lub Opera wersja minimum 38.0 lub Google Chrome wersja minimum 43.0
  - ✓ posiadać aktywowaną funkcję akceptacji plików cookie oraz Java Script w przeglądarce internetowej
  - ✓ posiadać aktywowaną funkcję akceptacji wyskakujących okienek w przeglądarce internetowej dla adresu internetowego <https://esaliens24.pl>;
  - ✓ posiadać oprogramowanie umożliwiające odczyt plików PDF Acrobat Reader wersja minimum 11.0.
12. Pamiętaj, że do zatwierdzenia operacji, dla których zgodnie z Regulaminem korzystania z Serwisu konieczny jest kod autoryzacyjny, wymagane jest podanie tylko jednego kodu autoryzacyjnego.
13. Uważaj na podejrzane wiadomości e-mail, zawierające załączniki, pochodzące od nieznanых nadawców. Takie załączniki mogą zawirusować Twoje urządzenie lub pozwolić na przejęcie nad nim kontroli. Dla bezpieczeństwa nie otwieraj takich wiadomości i załączników.
14. Uważaj na wiadomości e-mail, w których proszony jesteś o podanie danych potrzebnych do logowania do Serwisu.
15. Instaluj oprogramowanie z pewnych źródeł jak sklepy z aplikacjami i strony producenta. Używaj tylko legalnego oprogramowania.
16. Zachowaj ostrożność gdy połączenie z serwisem nawiązujesz z niezabezpieczonych sieci bezprzewodowych. Takie sieci nie gwarantują bezpiecznego połączenia.

17. W przypadku chęci korzystania z Serwisu za pośrednictwem Aplikacji na urządzenia mobilne:

- 17.1. przed zainstalowaniem Aplikacji, upewnij się, że pobierasz ją z legalnego źródła tj. sklepów internetowych Google Play - Android lub App Store – Apple;
- 17.2. nie powinieneś udostępniać urządzenia mobilnego osobom trzecim, a w szczególności nie powinieneś umożliwiać dostępu do urządzenia mobilnego osobom trzecim przy użyciu ich danych biometrycznych zdefiniowanych w tym urządzeniu mobilnym;
- 17.3. pamiętaj, że zgadzając się na logowanie przy pomocy danych biometrycznych ponosisz pełną odpowiedzialność za urządzenie i swoje dane biometryczne. Towarzystwo oraz Fundusze nie ponoszą odpowiedzialności za szkodę powstałą w wyniku zalogowania do Serwisu przy pomocy danych biometrycznych;
- 17.4. urządzenie mobilne, z którego następuje połączenie z Serwisem, powinno spełniać następujące wymagania:
  - ✓ posiadać zainstalowane wszystkie dostępne poprawki i uaktualnienia dla systemu operacyjnego urządzenia mobilnego dotyczące bezpieczeństwa
  - ✓ posiadać system antywirusowy z najnowszą wersją definicji wirusów i uaktualnień
  - ✓ posiadać zaporę bezpieczeństwa (Firewall) skonfigurowaną w sposób uniemożliwiający dostęp do urządzenia z sieci Internet przez osoby trzecie.