ZASADY BEZPIECZEŃSTWA INFORMATYCZNEGO DOTYCZĄCE KORZYSTANIA Z APLIKACJI INTERNETOWEJ PPE PZU ŻYCIE SA

OGÓLNE ZASADY BEZPIECZEŃSTWA

§ 1

1. Urządzenie, z którego następuje połączenie z Aplikacją (m.in. komputer, tablet, telefon komórkowy), powinno spełniać następujące wymagania:
   1) posiadać zainstalowane legalne oprogramowanie systemowe,
   2) posiadać legalny system antywirusowy z najnowszą wersją definicji wirusów i uaktualnień,
   3) posiadać zaporę bezpieczeństwa (Firewall) skonfigurowaną w sposób uniemożliwiający dostęp do urządzenia z sieci Internet przez osoby trzecie,
   4) posiadać zainstalowane wszystkie dostępne poprawki i uaktualnienia dotyczące bezpieczeństwa dla systemu operacyjnego urządzenia i przeglądarki internetowej,
   5) posiadać zainstalowaną i aktualną przeglądarkę internetową,
   6) posiadać dozwoloną komunikację z wykorzystaniem protokołu https, SSL oraz TLS 1.2,
   7) posiadać aktywowaną funkcję akceptacji wyskakujących okienek w przeglądarce internetowej dla adresu internetowego https://ssi.pzu.pl/ssi/zycie,
   8) posiadać włączoną obsługę Javascript oraz zezwolenie na zapisywanie plików cookie w ustawieniach przeglądarki internetowej.
2. Dodatkowo stosowanymi zabezpieczeniami są:
   1) blokowanie kodu PIN/hasła po trzech nieudanych próbach logowania,
   2) automatyczne blokowanie po piętnastominutowej bezczynności ze strony Użytkownika.

SZCZEGÓŁOWE ZASADY KORZYSTANIA Z APLIKACJI

§ 2

1. Użytkownik jest zobligowany do zweryfikowania poprawności adresu internetowego Aplikacji przed zalogowaniem do Aplikacji. Adres internetowy Aplikacji to https://ssi.pzu.pl/ssi/zycie.
2. Użytkownik jest zobligowany do zweryfikowania czy połączenie z Aplikacją jest szyfrowane. Przeglądarka www może sygnalizować to w następujący sposób:
   1) wyświetlając zamkniętą kłódkę obok adresu lub słowo „Bezpieczna”,
   2) wyświetlając https:// na początku adresu,
   3) nie wyświetlając przekreślonego https:// na początku adresu.
3. Użytkownik jest zobligowany do zweryfikowania poprawności certyfikatu, z użyciem którego następuje szyfrowanie połączenia z Aplikacją. Użytkownik powinien sprawdzić, że:
   1) data ważności certyfikatu nie jest przekroczona,
   2) certyfikat został wystawiony dla strony ssi.pzu.pl.
   3) Wystawcą certyfikatu jest Unizeto Technologies S.A.
   4) Numer seryjny certyfikatu to: 19:65:8D:85:6A:A9:DB:38:2F:99:A9:47:0E:46:40:96
4. Użytkownik nie powinien otwierać strony Aplikacji z linku zwróconego przez wyszukiwarkę internetową. Powinien wpisać go ręcznie lub wybrać z tzw. ulubionych stron. Użytkownik nie powinien dodawać do ulubionych stron linku do Aplikacji zwróconego przez wyszukiwarkę internetową.
5. Po zalogowaniu do Aplikacji, Użytkownik jest zobowiązany sprawdzić status ostatniego udanego i nieudanego logowania. W przypadku, gdy Użytkownik zauważy nieznane mu logowania, jest zobowiązany zgłosić ten fakt telefonicznie dzwoniąc na infolinię pod numerem 801 102 102.
6. W odniesieniu do Loginu oraz kodu PIN/hasła, Użytkownik zobowiązany jest do:
   1) przechowywania ich w sposób uniemożliwiający ujawnienie osobom trzecim,
   2) nieujawniania ich osobom trzecim,
   3) natychmiastowej zmiany kodu PIN/hasła w przypadku ujawnienia go osobom trzecim lub zaistnienia możliwości poznania go przez osoby trzecie,
7. W przypadku zapomnienia lub zgubienia kodu PIN/hasła, Użytkownik zgłasza potrzebę odzyskania kodu PIN/hasła poprzez kontakt z PZU Życie. W celu ustawienia nowego kodu PIN/hasła niezbędne jest podanie przez Użytkownika wybranych danych osobowych Użytkownika.
8. Użytkownik, który zaobserwuje jakiekolwiek nieprawidłowości w wyglądzie bądź funkcjonowaniu Aplikacji powinien zgłosić ten fakt na adres kontakt@pzu.pl.
9. Zalecane jest dokonywanie zmiany kodu PIN/hasła przez Użytkownika nie rzadziej niż co 30 dni. Dla bezpieczeństwa Użytkownika, PZU Życie może domagać się od Użytkownika okresowej zmiany kodu PIN/hasła, pod rygorem utraty ważności dotychczasowego kodu PIN/hasła.
10. Użytkownik powinien mieć świadomość i pamiętać o istotnym ryzyku wynikającym z korzystania z niezaufanych sieci Wi-Fi (np. niezabezpieczone hotspoty, sieci Wi-Fi dostępne w centrach handlowych, restauracjach, na lotniskach i w hotelach) przy łączeniu z Aplikacją. Użytkownik powinien mieć świadomość i pamiętać o istotnym ryzyku wynikającym z korzystania z funkcjonalności zapamiętywania haseł i autouzupełniania formularzy w przeglądarce internetowej.
11. Użytkownik powinien zwracać uwagę na podejrzane wiadomości e-mail, zawierające załączniki, pochodzące od nieznanych nadawców. Takie załączniki mogą zawirusować urządzenie Użytkownika lub pozwolić na przejęcie nad nim kontroli. Dla bezpieczeństwa nie należy otwierać takich wiadomości i załączników. Szczególnie podejrzane są wiadomości proszące o podanie Loginu bądź kodu PIN/hasła, na co nie należy odpowiadać. PZU nigdy nie będzie wysyłać korespondencji elektronicznej z prośbą o podanie haseł dostępowych do Aplikacji. W przypadku otrzymania takiej wiadomości pocztowej nie należy na nią odpowiadać oraz powiadomić PZU wysyłając informację na skrzynkę kontakt@pzu.pl.
12. Użytkownik nie powinien instalować na swoim urządzeniu oprogramowania pochodzącego z nieznanych źródeł, ponieważ takie oprogramowanie może zostać wykorzystane do zawirusowania urządzenia Użytkownika lub pozwolić na przejęcie nad nim kontroli.