ZASADY BEZPIECZEŃSTWA INFORMATYCZNEGO DOTYCZĄCE KORZYSTANIA Z SERWISU inPZU

Zasady bezpieczeństwa

1. Użytkownik jest zobligowany do zweryfikowania poprawności adresu internetowego Serwisu przed zalogowaniem do Serwisu. Adres internetowy Serwisu to https://inpzu.pl
2. Użytkownik jest zobligowany do zweryfikowania, czy połączenie z Serwisem 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 Serwisem. Użytkownik powinien sprawdzić, że:
   1) data ważności certyfikatu nie jest przekroczona,
   2) certyfikat został wystawiony dla strony www o adresie https://inpzu.pl
   3) Wystawcą certyfikatu o numerze seryjnym e9cec7e62456f3e88be515764be77fcd7caebc35167c11fd5c7c097aae5a4ad7 jest Certum Extended Validation CA SHA2.
4. Użytkownik nie powinien otwierać strony Serwisu 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 Serwisu zwróconego przez wyszukiwarkę internetową.
5. Po zalogowaniu do Serwisu, Użytkownik jest zobowiązany sprawdzić status ostatniego udanego i nieudanego logowania. W przypadku gdy Użytkownik zauważy nieznane mu logowania, jest zobowiązany zgłosić ten fakt telefonicznie do COK.
6. W odniesieniu do Loginu, Przyjaznego Loginu, Hasła oraz Kodów SMS, Użytkownik zobowiązany jest do:
   1) przechowywania ich w sposób uniemożliwiający ujawnienie osobom trzecim,
   2) nieujawniania ich osobom trzecim,
   3) w przypadku Hasła i Przyjaznego Loginu, natychmiastowej ich zmiany w przypadku ujawnienia osobom trzecim lub zaistnienia możliwości poznania ich przez osoby trzecie,
   4) chronienia dostępu do urządzeń, na których odbiera Kody SMS i przypominany Login.
7. W przypadku zapomnienia lub zgubienia Loginu, Użytkownik zgłasza potrzebę odzyskania Loginu w sposób określony w § 14 Regulaminu. Celem przypomnienia Loginu niezbędne jest podanie przez Użytkownika wybranych danych osobowych lub adresowych Użytkownika. Przesłanie Loginu następuje po pozytywnej weryfikacji danych. Login przesyłany jest Użytkownikowi na dedykowany do operacji wykonywanych w Serwisie numer telefonu oraz adres poczty elektronicznej.
8. Serwis nigdy nie prosi o podanie więcej niż jednego Kodu SMS przy zatwierdzaniu jednego Zlecenia.
9. Użytkownik, który zaobserwuje jakiekolwiek nieprawidłowości w wyglądzie bądź funkcjonowaniu Serwisu powinien zgłosić ten fakt w sposób określony w § 14 Regulaminu.
10. Zalecane jest dokonywanie zmiany Hasła przez Użytkownika nie rzadziej niż co 30 dni. Dla bezpieczeństwa Użytkownika, Towarzystwo może domagać się od Użytkownika okresowej zmiany Hasła, pod rygorem utraty ważności dotychczasowego Hasła. Hasło musi spełniać minimalne wymagania co do złożoności, które narzuca Serwis przy założeniu, że nie będą one słabsze niż: długość hasła co najmniej 8 znaków w tym przynajmniej jedna duża litera, jedna mała litera, jedna cyfra lub znak specjalny.
11. 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 Serwisem. Użytkownik powinien mieć świadomość i pamiętać o istotnym ryzyku wynikającym z korzystania z funkcjonalności zapamiętywania haseł i autouzupełniania formularzy w przeglądarce internetowej.
12. 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, Przyjaznego Loginu, Hasła bądź Kodów SMS, na co nie należy odpowiadać.
13. 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.

Wymagania techniczne

1. Połączenie z Serwisem odbywa się z wykorzystaniem bezpiecznego protokołu, służącego do bezpiecznej transmisji zaszyfrowanej strumienia danych – protokołu TLS w wersji 1.2 opartego o protokół SSL (klucz 2048 bitów).
2. Urządzenie, z którego następuje połączenie z Serwisem (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 dostęp do Internetu nie wolniejszy niż 512 kb/s,
   4) posiadać zaporę bezpieczeństwa (Firewall) skonfigurowaną w sposób uniemożliwiający dostęp do urządzenia z sieci Internet przez osoby trzecie,
   5) posiadać zainstalowane wszystkie dostępne poprawki i uaktualnienia dotyczące bezpieczeństwa dla systemu operacyjnego urządzenia i przeglądarki internetowej,
   6) posiadać zainstalowaną przeglądarkę internetową: Mozilla Firefox wersja minimum 127.0 lub Google Chrome wersja minimum 121.0 lub Microsoft Edge wersja minimum 124.0 lub Safari wersja minimum 15 lub Samsung Internet Browser,
   7) posiadać dozwoloną komunikację z wykorzystaniem protokołu https,
   8) posiadać aktywowaną funkcję akceptacji plików cookie oraz włączony JavaScript w przeglądarce internetowej,
   9) posiadać aktywowaną funkcję akceptacji wyskakujących okienek w przeglądarce internetowej dla adresu internetowego https://inpzu.pl,
   10) posiadać oprogramowanie umożliwiające odczyt plików PDF – Adobe Acrobat Reader wersja minimum 11.0,
   11) komputer/procesor: komputer z procesorem 1 GHz lub szybszym, pamięć: co najmniej 512 MB,
   12) obsługiwać rozdzielczość minimum 1024x768 punktów