ZASADY BEZPIECZEŃSTWA INFORMATYCZNEGO DOTYCZĄCE KORZYSTANIA Z SERWISU eRU

Zasady bezpieczeństwa

1. Użytkownik jest zobligowany do zweryfikowania poprawności adresu internetowego serwisu eRU przed zalogowaniem do serwisu eRU. Adres internetowy serwisu eRU to https://eru.pzu.pl.
2. Użytkownik jest zobligowany do zweryfikowania, czy połączenie z serwisem eRU 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 eRU. Użytkownik powinien sprawdzić, że:
   1. data ważności certyfikatu nie jest przekroczona;
   2. certyfikat został wystawiony dla strony www o adresie https://eru.pzu.pl:
   3. Wystawcą certyfikatu jest Certum Extended Validation CA SHA2.
4. Użytkownik nie powinien otwierać strony serwisu eRU 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 eRU zwróconego przez wyszukiwarkę internetową.
5. W odniesieniu do loginu, hasła oraz kodów jednorazowych, użytkownik zobowiązany jest do:
   1. przechowywania ich w sposób uniemożliwiający ujawnienie osobom trzecim;
   2. nieujawniania ich osobom trzecim;
   3. w przypadku hasła, natychmiastowej ich zmiany w przypadku ujawnienia osobom trzecim lub zaistnienia możliwości poznania ich przez osoby trzecie;
   4. chronienia dostępu do urządzeń, na których odbiera korespondencję e-mail, sms zawierającą kody jednorazowe.
6. W przypadku zapomnienia hasła, użytkownik ma możliwość samodzielnego zresetowania hasła do swojego konta w serwisie eRU. Jednorazowe hasło przesyłane jest użytkownikowi na dedykowany do operacji wykonywanych w serwisie eRU adres poczty elektronicznej lub numer telefonu.
7. Użytkownik, który zaobserwuje jakiekolwiek nieprawidłowości w wyglądzie bądź funkcjonowaniu serwisu eRU powinien zgłosić ten fakt poprzez kontakt z infolinią eRU pod numerem telefonu 22 566 55 66.
8. Zalecane jest dokonywanie zmiany hasła przez użytkownika nie rzadziej niż co 30 dni. Dla bezpieczeństwa użytkownika, PZU może domagać się od użytkownika okresowej zmiany hasła, pod rygorem utraty ważności dotychczasowego hasła. Hasło musi spełniać minimalne wymagania co do złożoności i zawierać minimum 8 znaków, w tym małą i wielka literę, cyfrę i znak specjalny, oraz nie może być takie samo jak pięć poprzednich haseł.
9. 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 eRU. Użytkownik powinien mieć świadomość i pamiętać o istotnym ryzyku wynikającym z korzystania z funkcjonalności zapamiętywania haseł i autouzupełniania formularzy w przeglądarce internetowej.
10. Użytkownik powinien zwracać uwagę na podejrzane wiadomości email, 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 które nie należy odpowiadać.
11. Użytkownik powinien dbać o bezpieczeństwo swoich urządzeń, które służą dostępowi do sieci Internet. Takie urządzenie powinno posiadać program antywirusowy z aktualną bazą definicji wirusów, aktualną i bezpieczną wersję przeglądarki internetowej. Użytkownik powinien ponadto cyklicznie sprawdzać, czy system operacyjny i programy zainstalowane na nim posiadają najnowsze aktualizacje.
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.

Wymagania techniczne

1. Połączenie z serwisem eRU odbywa się z wykorzystaniem bezpiecznego protokołu, służącego do bezpiecznej transmisji zaszyfrowanej strumienia danych – protokołu TLS w wersji 1.2 (klucz 2048 bitów).
2. Urządzenie (komputer), z którego następuje połączenie z serwisem eRU 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 jedną z następujących przeglądarek internetowych:
      – dla komputerów stacjonarnych:
         1. Google Chrome (MS Windows, macOS): wersja aktualna oraz 10 wcześniejszych wersji (głównych wydań).
         2. Mozilla FireFox (MS Windows, macOS): wersja aktualna oraz 10 wcześniejszych wersji (głównych wydań).
         3.
         4. Edge Chromium (MS Windows, macOS): obsługiwany od wersji 81.0, brak wsparcia dla wersji niższych.
   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://eru.pzu.pl;
   10. posiadać oprogramowanie umożliwiające odczyt plików PDF Adobe Acrobat Reader wersja minimum 11.0;
   11. obsługiwać rozdzielczość minimum 1280x768 punktów w minimum 256 kolorach.