

Aktualne wymagania bezpieczeństwa teleinformatycznego dla planowanego systemu elektronicznej obsługi rachunków bankowych zwanego Systemem są następujące:

1. **Wymagania dotyczące aplikacji**, gdzie Zamawiający dopuszcza dostęp do Systemu poprzez przeglądarkę z danymi przechowywanymi poza Urzędem.
2. **Wymagania dotyczące sprzętu i sieci**. Sprzęt lokalny zabezpiecza Zamawiający. Dotyczy to stacji roboczych PC, sieci z możliwością wydzielenia sieci prywatnej/wirtualnej. Zamawiający zapewnia także jednolitą ochronę brzegową na styku Zamawiający Internet, ochronę antywirusową oraz łącze internetowe.

Zarządzanie powyższymi zasobami realizowane jest przez Zamawiającego, w szczególności cały ruch internetowy Zamawiającego jest monitorowany i logowany.

3. **Bezpieczeństwo Systemu** musi być zapewnione poprzez mechanizmy dostępu autoryzowanego. Wymagana jest rejestracja i identyfikacji użytkowników poprzez unikalny identyfikator, autoryzacja poprzez hasła o wysokim stopniu trudności i mechanizm dodatkowej weryfikacji np. SMS. Jako rozwiązanie równoważne przyjmuje się mechanizm jednorazowych tokenów. System musi posiadać mechanizm wielopoziomowego hierarchizowania uprawnień i ich przydzielania/odbierania przez lokalnego administratora. Praca użytkowników musi być kontrolowana przez mechanizm zapewniający automatyczne wylogowanie po określonym czasie braku aktywności. Dostęp do Systemu musi być z zastosowaniem protokołu https lub rozwiązania równoważnego. Zamawiający wyklucza zastosowanie metod biometrycznych do logowania do Systemu.
4. **Dostawca Systemu** obowiązany jest udzielić Zamawiającemu niewyłącznej licencji na System, co najmniej na okres obowiązywania umowy z możliwością przedłużenia na czas nieokreślony.

Wymagana jest zgodność Systemu z obowiązującymi przepisami, w szczególności:

1. Ustawą z 10 maja 2018 o ochronie danych osobowych (tekst jedn. Dz.U. 2019 poz. 1781);
2. Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
3. Ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tekst jedn. Dz.U. 2021 poz. 670);
4. Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tekst jedn. Dz.U. 2017 poz. 2247).