WYMAGANIA DO PRZYŁĄCZENIA JEDNOSTKI TERENOWEJ DO CSIZS

1	Do komunikacji z usługami udostępnianymi przez CSIZS konieczne jest wdrożenie Systemu Dziedzinowego posiadającego świadectwo zgodności lub dopuszczenie do aktualizacji oprogramowania (WAO) wydane przez MRPiPS.
2	Zegar serwera(ów) Systemu Dziedzinowego powinien być zsynchronizowany z publicznym źródłem czasu (np. http://www.gum.gov.pl/pl/zegar/ lub http://www.ntp.org/).
3	Maszyna, na której jest zainstalowana część serwerowa Systemu Dziedzinowego musi mieć możliwość połączenia z serwerem CSIZS za pośrednictwem sieci Internet.
4	Użytkownicy uprawnieni do podpisywania decyzji przekazywanych w formie elektronicznej muszą posiadać osobisty klucz z certyfikatem kwalifikowanym (podpis elektroniczny) oraz niezbędne do jego użycia czytnik i kartę kryptograficzną.
5	W przypadku, gdy funkcje lub usługi Systemu Dziedzinowego są udostępniane przez sieć niezaufaną (np. Internet) komunikacja powinna odbywać się poprzez kanał szyfrowany SSL z uwierzytelnianiem klienta lub obustronnym.
6	Serwer Systemu Dziedzinowego nie może być umieszczony bezpośrednio w sieci Internet. W przypadku, gdy wymagane jest udostępnienie funkcji lub usług za pośrednictwem sieci Internet konieczne jest umieszczenie serwera Systemu Dziedzinowego za zaporą sieciową (firewallem). Zapora powinna być skonfigurowana tak aby przekazywać żądania tylko do udostępnianych funkcji lub usług Systemu Dziedzinowego.
7	Klucz prywatny Systemu Dziedzinowego, do którego został wystawiony certyfikat powinien nie opuszczać serwera, na którym zainstalowano System Dziedzinowy. Magazyn kluczy powinien być zabezpieczony hasłem. Dopuszczalne jest przechowywanie materiału kryptograficznego na specjalizowanych urządzeniach (karty kryptograficzne, HSM).

WYMAGANIA W TRAKCIE UŻYTKOWANIA CSIZS PRZEZ UŻYTKOWNIKÓW I SYSTEMY DZIEDZINOWE JEDNOSTKI TERENOWEJ

1.	Administrator Jednostki Terenowej musi przekazać dane umożliwiające zalogowanie (login i hasło) użytkownikom kont założonych w Module Zarządzania Tożsamością CSIZS w sposób uniemożliwiający ich przechwycenie (np. osobiście etc).
2.	Użytkownik zarejestrowany w Module Zarządzania Tożsamością CSIZS musi powiadomić administratora właściwej jednostki terenowej w przypadku utraty hasła. Administrator jednostki terenowej dokonuje w Module Zarządzania Tożsamością CSIZS zmiany jego hasła. Nowe hasło przekazywane jest do użytkownika w sposób uniemożliwiający przechwycenie.
3.	Użytkownik zarejestrowany w Module Zarządzania Tożsamością CSIZS musi niezwłocznie zmienić swoje hasło w przypadku jego ujawnienia (np. opublikowania hasła do wiadomości innych pracowników)
4.	W przypadku zaginięcia lub ujawnienia klucza prywatnego Systemu Dziedzinowego administrator Jednostki Terenowej musi niezwłocznie pozyskać nowy certyfikat CSIZS.
5.	Dostęp do wrażliwych funkcji Systemu Dziedzinowego oraz danych przez niego przetwarzanych lub przesyłanych musi być możliwy wyłącznie po uwierzytelnieniu.
6.	Użytkownicy Systemu Dziedzinowego muszą posiadać indywidualne konta w Systemie Dziedzinowym. Zasady tworzenia hasła mają być zgodne z ROZPORZĄDZENIEM MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI[1)] z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych
7.	Zdarzenia udostępnienia danych i funkcji Systemu Dziedzinowego użytkownikom powinny być rejestrowane i przechowywane w postaci elektronicznej przez okres 5 lat.
8.	Administrator Jednostki Terenowej nie może zakładać w Module Zarządzania Tożsamością CSIZS kont dla nieuprawnionych osób (niezwiązanych odpowiednią umową z Jednostką Terenową).
9.	Administrator jednostki powinien przypisywać użytkownikom w Module Zarządzania Tożsamością CSIZS najmniejszy zestaw ról wymaganych do realizacji obowiązków.