Regulamin bezpieczeństwa informacji przetwarzanych w aplikacji głównej centralnego systemu teleinformatycznego

wersja 1.1

§ 1.
POSTANOWIENIA OGÓLNE

1. Regulamin bezpieczeństwa informacji przetwarzanych w aplikacji głównej centralnego systemu teleinformatycznego, zwany dalej „Regulaminem", określa prawa i obowiązki Użytkowników aplikacji głównej centralnego systemu teleinformatycznego w zakresie bezpieczeństwa informacji, w tym ochrony danych osobowych przetwarzanych w tym Systemie oraz zasady, zakres i warunki korzystania przez Użytkowników z Systemu.
2. Ilekroć w Regulaminie jest mowa o:
   1) Systemie – należy przez to rozumieć aplikację główną centralnego systemu teleinformatycznego, o którym mowa w art. 69 ust. 1 ustawy z 11 lipca 2014 r. o zasadach realizacji programów w zakresie polityki spójności finansowanych w perspektywie finansowej 2014-2020 (Dz. U. poz. 1146), wspierającą procesy dotyczące obsługi projektu od momentu podpisania umowy o dofinansowanie;
   2) Operatorze– należy przez to rozumieć urząd obsługujący ministra właściwego do spraw rozwoju regionalnego;
   3) Beneficjencie – należy przez to rozumieć podmiot, o którym mowa w art. 2 pkt 10 lub w art. 63 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1303/2013 z dnia 17 grudnia 2013 r. ustanawiającego wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności, Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich oraz Europejskiego Funduszu Morskiego i Rybackiego oraz ustanawiającego przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności i Europejskiego Funduszu Morskiego i Rybackiego oraz uchylającego rozporządzenie (WE) nr 1083/2006 (Dz. Urz. UE L 347 z 20.12.2013, str. 320);
   4) Użytkowniku – należy przez to rozumieć osobę mającą dostęp do Systemu, wyznaczoną przez Beneficjenta do wykonywania w jego imieniu czynności związanych z realizacją projektu/projektów;
   5) Administratorze Merytorycznym – należy przez to rozumieć wyznaczonego pracownika Właściwej instytucji;
   6) podatności - należy przez to rozumieć lukę (słabość) aktywu lub grupy aktywów, która może być wykorzystana przez co najmniej jedno zagrożenie, rozumiane jako potencjalna przyczyna niepożądanego incydentu, który może wywołać szkodę w Systemie;
   7) zdarzeniu związanym z bezpieczeństwem informacji - należy przez to rozumieć stan Systemu, usługi lub sieci, wskazujący na możliwe naruszenie Regulaminu, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem;
   8) incydencie – należy przez to rozumieć pojedyncze zdarzenie lub serię niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji lub zmniejszeniem poziomu usług systemowych, które stwarzają znaczne prawdopodobieństwo zakłócenia działania Systemu i zagrażają bezpieczeństwu informacji, w tym danych osobowych przetwarzanych w Systemie;

9) Właściwej instytucji – należy przez to rozumieć instytucję zaangażowaną w realizację programów operacyjnych w perspektywie finansowej 2014-2020, z którą Beneficjent zawarł umowę o dofinansowanie projektu.

3. Regulamin wskazuje prawa i obowiązki Użytkowników w obszarach:
   1) korzystania z Systemu;
   2) konfiguracji sprzętu komputerowego Użytkownika;
   3) rozpoczynania, zawieszania i kończenia pracy Użytkowników w Systemie;
   4) korzystania z poczty elektronicznej i Internetu;
   5) zgłaszania incydentów, usterek, awarii Systemu, uszkodzeń i podatności Systemu;
   6) przetwarzania danych osobowych w Systemie.

§ 2.
WARUNKI KORZYSTANIA Z SYSTEMU

1. Operator nie odpowiada za szkody powstałe w związku z korzystaniem z Systemu, bądź w związku z niewłaściwym działaniem Systemu spowodowanym błędami, brakami, zakłóceniami, defektami, opóźnieniami w transmisji danych, wirusami komputerowymi, awarią łączy sieci Internet lub nieprzestrzeganiem postanowień Regulaminu.
2. Operator nie ponosi odpowiedzialności za brak dostępu do Systemu z przyczyn niezależnych od Operatora.
3. System działa w trybie ciągłym przez 24 godziny na dobę - za wyjątkiem okresu przeznaczonego na przerwę konserwacyjną przypadającą w godzinach od 2:00 do 4:00 czasu polskiego.
4. Operator, w związku z realizacją prac dotyczących administrowania lub modyfikacji funkcjonalności Systemu, ze względów bezpieczeństwa lub innych przyczyn niezależnych od Operatora, ma prawo czasowo zawiesić dostęp Użytkowników do Systemu w innych godzinach niż podane w ust. 3 na okres niezbędny do wykonania planowanych prac lub wyeliminowania niepożądanych zdarzeń. O planowanych przerwach związanych z prowadzeniem prac konserwacyjnych w Systemie Operator poinformuje Użytkowników z wyprzedzeniem.
5. W celu prawidłowego korzystania z Systemu niezbędne są:
   1) połączenie z siecią Internet;
   2) zainstalowana przeglądarka internetowa: Internet Explorer (lub inna wbudowana w system Windows), Mozilla Firefox lub Google Chrome w najnowszej stabilnej wersji (nie starszej niż dwie wersje wstecz);
   3) włączenie obsługi technologii Java Script, tzw. "cookie" oraz wyłączenie blokowania wyskakujących okien w przeglądarce internetowej;
   4) zainstalowanie i włączenie najnowszej wersji wtyczki Flash Media Player pobranej ze strony Adobe dla przeglądarek wymienionych w pkt 2.

§ 3.
DOSTĘP DO SYSTEMU

1. Korzystanie z funkcjonalności Systemu przez Użytkownika jest możliwe pod warunkiem złożenia przez Beneficjenta wniosku o nadanie/zmianę/wycofanie dostępu dla osoby uprawnionej.
2. Po weryfikacji wniosku, Użytkownikowi zostaje wydane upoważnienie do przetwarzania danych osobowych w zbiorze „Centralny system teleinformatyczny wspierający realizację programów operacyjnych".
3. Zmiana dotychczasowych uprawnień Użytkownika w Systemie, jest realizowana po przekazaniu przez Beneficjenta zgłoszenia aktualizacji listy osób uprawnionych.
4. Uwierzytelnianie Użytkownika w Systemie następuje poprzez wykorzystanie profilu zaufanego ePUAP w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114) albo bezpiecznego podpisu elektronicznego weryfikowanego za pomocą ważnego kwalifikowanego certyfikatu, na zasadach określonych w ustawie z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. z 2013 r. poz. 262), z zastrzeżeniem ust. 5.
5. W przypadku gdy z powodów technicznych wykorzystanie profilu zaufanego ePUAP nie jest możliwe, uwierzytelnianie w Systemie następuje przez wykorzystanie loginu użytkownika oraz hasła wygenerowanego przez System.
6. Aktywacja hasła dostępowego do Systemu następuje po kliknięciu przez Użytkownika w link aktywacyjny, przesłany w wiadomości mailowej, na podany w Systemie adres e-mail.
7. Z chwilą poprawnego zalogowania w Systemie Użytkownik akceptuje możliwość otrzymywania drogą elektroniczną informacji dotyczących Systemu.
8. Operator, na dedykowanej Systemowi stronie WWW, udostępnia dla Użytkowników *Instrukcję użytkownika Systemu*.

§ 4.
ZASADY BEZPIECZEŃSTWA

1. Użytkownik jest zobowiązany do zapoznania się i zaakceptowania Regulaminu, co potwierdza (przez złożenie oświadczenia na formularzu elektronicznym) podczas pierwszego logowania w Systemie.
2. Złożenie oświadczenia, o którym mowa w ust. 1, jest warunkiem uzyskania dostępu do Systemu. Informacja o dacie i godzinie złożenia przez Użytkownika oświadczenia jest przechowywana w Systemie.
3. Użytkownik ma obowiązek przestrzegania przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 z późn. zm.) oraz przepisów wykonawczych do tej ustawy, co potwierdza (przez złożenie oświadczenia na formularzu elektronicznym) w Systemie.
4. Użytkownik ma obowiązek zachować w tajemnicy przetwarzane dane osobowe oraz informacje o sposobach ich zabezpieczenia, zarówno w okresie trwania umowy, o której mowa w § 1 ust. 2 pkt 9, jak też po jej zakończeniu.
5. Użytkownicy, którzy posiadają dostęp do Systemu, są zobowiązani do przestrzegania Regulaminu.

6. System jest skonfigurowany zgodnie z następującymi zasadami bezpiecznych haseł:
    1) hasło składa się z minimum 8 znaków (maksymalny rozmiar hasła wynosi 16 znaków);
    2) hasło zawiera wielkie i małe litery oraz cyfry lub znaki specjalne;
    3) hasło jest zmieniane nie rzadziej niż co 30 dni;
    4) hasło musi zaczynać się od litery;
    5) nowe hasło musi różnić się od 12 haseł ostatnio wykorzystywanych przez Użytkownika.
7. Czas trwania nieaktywnej sesji (czas bezczynności) po jakim następuje automatyczne wylogowanie Użytkownika wynosi 20 minut.
8. W przypadku nieumyślnego ujawnienia hasła osobie nieuprawnionej lub podejrzenia ujawnienia, należy bezzwłocznie dokonać zmiany hasła na nowe.
9. W przypadku braku możliwości dokonania przez Użytkownika zmiany hasła (braku działania funkcjonalności „Wyślij hasło"), należy powiadomić Administratora Merytorycznego Właściwej instytucji w celu zmiany hasła.
10. Przekazywanie hasła, o którym mowa w § 3 ust. 5 odbywa się drogą mailową na adres podany w Systemie. Użytkownik jest zobowiązany do niezwłocznej zmiany tego hasła.
11. W celu zapobieżenia nieautoryzowanemu dostępowi do Systemu Użytkownik:
    1) nie może przechowywać danych służących do logowania do Systemu w miejscach dostępnych dla innych osób;
    2) nie może ujawniać danych służących do logowania innym osobom.
12. Zabronione jest korzystanie z Systemu z użyciem danych dostępowych innego Użytkownika.
13. Użytkownicy są zobowiązani do ustawienia ekranów monitorów w taki sposób, aby uniemożliwić osobom postronnym wgląd lub spisanie informacji aktualnie wyświetlanej na ekranie monitora.

§ 5.
KONFIGURACJA SPRZĘTU KOMPUTEROWEGO UŻYTKOWNIKA

1. Komputer Użytkownika powinien posiadać oprogramowanie antywirusowe, którego sygnatury wirusów powinny być aktualizowane nie rzadziej niż raz na tydzień. Oprogramowanie antywirusowe powinno być stale aktywne.
2. Użytkownik jest zobowiązany do stałego monitorowania komunikatów pochodzących z oprogramowania antywirusowego zainstalowanego na stacji roboczej i reagowania na nie.
3. Komputer Użytkownika powinien być chroniony zaporą sieciową (firewall).
4. Podczas pracy z Systemem na komputerze Użytkownika nie powinien być uruchomiony żaden serwer, w szczególności nie powinien być uruchomiony serwer WWW oraz FTP (TFTP).
5. Oprogramowanie komputera powinno być regularnie aktualizowane, w szczególności dotyczy to systemu operacyjnego oraz przeglądarki internetowej.
6. Przeglądarkę internetową należy skonfigurować, aby miała włączoną obsługę protokołu OCSP (Online Certificate Status Protocol), umożliwiającego przeprowadzenie weryfikacji ważności certyfikatu Systemu.
7. Użytkownik podczas logowania się do Systemu jest zobowiązany sprawdzić:
    1) czy w pasku adresowym przeglądarki adres zaczyna się od https?;

2) czy w obrębie okna przeglądarki znajduje się mała kłódka informująca o bezpieczeństwie?;

3) czy po kliknięciu na kłódkę pojawia się informacja o tym, że certyfikat został wydany dla: *.sl2014.gov.pl i jest on ważny?

§ 6.

ROZPOCZYNANIE, ZAWIESZANIE I KOŃCZENIE PRACY UŻYTKOWNIKÓW W SYSTEMIE

1. Rozpoczęcie pracy Użytkownika w Systemie następuje po uruchomieniu przeglądarki oraz wprowadzeniu adresu:

   https://www.sl2014.gov.pl.

2. Połączenie z Systemem jest szyfrowane, odbywa się, po wybraniu przez Użytkownika odpowiedniego sposobu uwierzytelniania (spośród dostępnych na ekranie powitalnym).

3. W celu chwilowego zawieszenia pracy w Systemie, należy zablokować ekran (zablokować pulpit lub włączyć wygaszacz ekranu zabezpieczony hasłem). Jeśli komputer Użytkownika nie pozwala na zabezpieczenie ekranu hasłem, należy wylogować się z Systemu.

4. Po zakończeniu pracy należy wylogować się z Systemu poprzez wybranie funkcji „Wyloguj" zlokalizowanej nad menu w prawym górnym rogu ekranu. Nie należy kończyć pracy poprzez zamknięcie okna przeglądarki znakiem „x".

§ 7.

POCZTA ELEKTRONICZNA, INTERNET

1. W Systemie wykorzystano funkcjonalność wysyłania powiadomień na adres e-mail podany w Systemie. Użytkownik jest zobowiązany do dbania o bezpieczeństwo konta mailowego, o którym mowa powyżej, w szczególności do:

   1) używania silnego hasła dostępu;

   2) nieotwierania załączników do poczty i linków pochodzących z nieznanych źródeł;

   3) zachowania ostrożności podczas otwierania nieoczekiwanych załączników w korespondencji pochodzącej od znanych nadawców.

2. Użytkownik powinien korzystać z sieci Internet w sposób, który nie zagraża bezpieczeństwu Systemu.

§ 8.

ZGŁASZANIE ZAGROŻEŃ BEZPIECZEŃSTWA

Użytkownicy są zobowiązani do niezwłocznego powiadomienia Właściwej instytucji o zauważonej podatności, zdarzeniu związanym z bezpieczeństwem informacji lub incydencie.

§ 9.

DODATKOWE POSTANOWIENIA W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Administratorem Danych w zrozumieniu ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych gromadzonych w Systemie, w tym również danych osobowych użytkowników jest minister właściwy do spraw rozwoju regionalnego z siedzibą w Warszawie przy ulicy Wspólnej 2/4, 00-926 Warszawa.
2. Zakres danych osobowych przetwarzanych przez Użytkownika w Systemie nie może być większy niż powierzony do przetwarzania przez Właściwą instytucję.
3. Dane osobowe są przetwarzane wyłącznie w celu realizacji umowy, o której mowa w § 1 ust. 2 pkt 9.
4. Użytkownik odpowiada za zgodność z dokumentami źródłowymi, danych osobowych wprowadzonych przez siebie do Systemu.
5. Każdy Użytkownik ma prawo dostępu do treści swoich danych osobowych oraz prawo żądania ich uzupełnienia, uaktualnienia lub sprostowania.

Warszawa, 26 czerwca 2015 r.

ZATWIERDZAM:

DYREKTOR
Departamentu Informatyki
.....
Małgorzata Kozyra