Regulamin bezpieczeństwa informacji przetwarzanych w centralnym systemie teleinformatycznym

(§ 9. INFORMACJE W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH)

wersja 1.5

§ 1.

POSTANOWIENIA OGÓLNE

1. Regulamin bezpieczeństwa informacji przetwarzanych w centralnym systemie teleinformatycznym, zwany dalej „Regulaminem", określa prawa i obowiązki Użytkowników Systemu w zakresie bezpieczeństwa informacji, w tym ochrony danych osobowych przetwarzanych w tym Systemie oraz zasady, zakres i warunki korzystania przez Użytkowników z Systemu.

   Regulamin nie obejmuje aplikacji centralnego systemu teleinformatycznego wspierającej obsługę projektów pomocy technicznej (SL2014-PT).

2. Ilekroć w Regulaminie jest mowa o:

   1) Systemie – należy przez to rozumieć centralny system teleinformatyczny, 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. z 2017 r. poz. 1460, 1475 i 2433), w którego skład wchodzą:

      a) aplikacja główna, zwana dalej „SL2014";

      b) aplikacja raportująca Systemu, zwana dalej „SRHD";

      c) system zarządzania tożsamością, zwany dalej „SZT";

   2) Operatorze – należy przez to rozumieć urząd obsługujący ministra właściwego do spraw rozwoju regionalnego;

   3) Użytkowniku - należy przez to rozumieć osobę mającą dostęp do Systemu, wyznaczoną przez Właściwą instytucję do wykonywania w jej imieniu czynności związanych z realizacją programu operacyjnego;

   4) 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;

   5) 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;

   6) 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

   7) Administratorze Merytorycznym – należy przez to rozumieć wyznaczonego pracownika Właściwej instytucji realizującego zadania określone w rozdziale 7 Wytycznych;

   8) Wytycznych - należy przez to rozumieć Wytyczne Ministra Rozwoju i Finansów w zakresie warunków gromadzenia i przekazywania danych w postaci elektronicznej na lata 2014-2020;

   9) Właściwej instytucji – należy przez to rozumieć Instytucję Zarządzającą, Instytucję Pośredniczącą, Instytucję Wdrażającą lub inną instytucję zaangażowaną w realizację

programów operacyjnych w perspektywie finansowej 2014-2020;

10) Bazie Wiedzy - należy przez to rozumieć system, o którym mowa w Wytycznych w zakresie informacji i promocji programów operacyjnych polityki spójności na lata 2014-2020.

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, awariami łącza sieci Internet lub nieprzestrzeganiem postanowień Regulaminu.
2. Operator nie ponosi odpowiedzialności za brak dostępu do Systemu z przyczyn niezależnych od Operatora.
3. SL2014 i SZT działają w trybie ciągłym przez 24 godziny na dobę - za wyjątkiem okresu przeznaczonego na przerwę konserwacyjną przypadającą w godzinach od 0:30 do 5:00 czasu polskiego.
4. SRHD działa w trybie ciągłym przez 24 godziny na dobę - za wyjątkiem okresu przeznaczonego na przerwę konserwacyjną przypadającą w godzinach od 0:30 do 7:00 czasu polskiego.
5. 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 i 4 na okres niezbędny do wykonania planowanych prac lub wyeliminowania niepożądanych zdarzeń. O planowanych przerwach związanych z prowadzeniem prac konserwacyjnych w Systemie Operator poinformuje Właściwą instytucję z wyprzedzeniem.
6. Zabrania się Użytkownikowi podejmowania wszelkich prób mających na celu naruszenie bezpieczeństwa danych przetwarzanych w Systemie, w tym prób przełamania zabezpieczeń Systemu.
7. Użytkownik może pracować w danej sesji wykorzystując wyłącznie jeden posiadany profil - zabrania się jednoczesnego uruchamiania kilku sesji przeglądarki/przeglądarek i równoległej pracy w Systemie na więcej niż jednym posiadanym profilu.
8. Operator ze względów bezpieczeństwa oraz z powodu innych ważnych przyczyn niezależnych od Operatora ma prawo czasowo zawiesić dostęp Użytkowników do Systemu na okres niezbędny do wyeliminowania niepożądanych dla Operatora skutków zaistniałych okoliczności.

9. Operator zastrzega sobie prawo do zawieszenia konta Użytkownika, który narusza prawo lub postanowienia Regulaminu.
10. Operator może trwale zablokować konto Użytkownika jeśli Użytkownik nie zaprzestanie działań sprzecznych z prawem lub postanowieniami Regulaminu.
11. Operator jest zobowiązany do poinformowania Właściwej instytucji Użytkownika o zawieszeniu bądź zablokowaniu konta Użytkownika.
12. W celu prawidłowego korzystania z Systemu niezbędne są:
    1) połączenie z siecią Internet;
    2) zainstalowana przeglądarka internetowa: Internet Explorer, 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.
13. Operator gromadzi informacje o adresie IP, z którego Użytkownik uwierzytelnia się w Systemie. Operator gromadzi adresy IP wyłącznie w celu wykrywania prób naruszenia zabezpieczeń Systemu oraz prowadzenia audytu zabezpieczeń Systemu.

§ 3.

DOSTĘP DO SYSTEMU

1. Korzystanie z funkcjonalności Systemu jest możliwe pod warunkiem złożenia wniosku o nadanie/zmianę uprawnień w ramach Właściwej instytucji i założenia konta w Systemie zgodnie z procedurą określoną w Wytycznych.
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 jest realizowana na podstawie wniosku o nadanie/zmianę uprawnień lub wniosku o wycofanie/czasowe wycofanie uprawnień, przekazanego do Właściwej instytucji zgodnie z procedurą określoną w Wytycznych.
4. W celu korzystania z SL2014 lub SRHD konieczne jest wcześniejsze uwierzytelnienie Użytkownika w SZT.
5. Uwierzytelnienie Użytkownika w SZT następuje przy wykorzystaniu loginu i hasła.
6. Aktywacja konta w SZT następuje po kliknięciu Użytkownika w link aktywacyjny przesłany w wiadomości mailowej na podany przez Użytkownika w SZT adres e-mail.
7. Z chwilą utworzenia i aktywacji konta w Systemie Użytkownik akceptuje możliwość otrzymywania drogą elektroniczną informacji dotyczących Systemu.
8. Operator udostępnia Użytkownikom *Instrukcję użytkownika Systemu*.
9. Użytkownik jest odpowiedzialny za wszystkie czynności wykonane przez siebie przy użyciu loginu i hasła, którymi się posługuje.

§ 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 SZT.
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 rozporządzenia 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 (Dz. U. UE. L. 2016.119.1), ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych oraz prawa powszechnie obowiązującego dotyczącego ochrony danych osobowych , 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 zatrudnienia we Właściwej instytucji, jak i po jego ustaniu.
5. Użytkownicy, którzy posiadają dostęp do Systemu, są zobowiązani do przestrzegania Regulaminu.
6. W SZT są używane hasła skonfigurowane zgodnie z następującymi zasadami bezpieczeństwa:
    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 w SZT (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 wygenerowanego przez SZT, służącego Użytkownikowi do pierwszego logowania odbywa się drogą mailową na adres podany w SZT. System SZT wymusza zmianę hasła podczas pierwszego logowania.
11. W celu zapobieżenia nieautoryzowanemu dostępowi do Systemu Użytkownik:
    1) nie może przechowywać loginu i hasła do SZT w miejscach dostępnych dla innych osób;
    2) nie może ujawniać danych dostępowych do SZT 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.
14. Komputery powinny zostać ustawione również w taki sposób, aby osoby postronne miały utrudniony dostęp do portów zewnętrznych lub przynajmniej dostęp do portów zewnętrznych był pod kontrolą wizualną Użytkowników.
15. Użytkownik zobowiązany jest do przestrzegania zasady czystego biurka. W szczególności przed opuszczeniem swego stanowiska pracy Użytkownik powinien schować wszelkie dokumenty związane z używanym Systemem oraz informatyczne nośniki danych (dyskietki, płyty CD, DVD, BD, pendrive itp.).

§ 5.

KONFIGURACJA SPRZĘTU KOMPUTEROWEGO UŻYTKOWNIKA

1. Podczas pracy z Systemem na komputerze Użytkownika nie powinien być uruchomiony żaden serwer, w szczególności nie powinien być uruchomiony serwer WWW oraz FTP (TFTP).
2. Komputer powinien posiadać oprogramowanie antywirusowe, którego sygnatury wirusów powinny być aktualizowane nie rzadziej niż raz na tydzień. Oprogramowanie antywirusowe powinno być stale aktywne.
3. Użytkownik jest zobowiązany do stałego monitorowania komunikatów pochodzących z oprogramowania antywirusowego zainstalowanego na stacji roboczej i reagowania na nie.
4. Komputer Użytkownika powinien być chroniony zaporą sieciową (firewall).
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: *.sl.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://sl.gov.pl -> strona aplikacji Systemu Zarządzania Tożsamością .
2. Połączenie do Systemu jest szyfrowane.

3. Po poprawnym zalogowaniu Użytkownik otrzymuje w przeglądarce ekran startowy SZT zawierający aktywne przyciski wyboru aplikacji, do których Użytkownik ma nadany dostęp.
4. W celu chwilowego zawieszenia pracy w Systemie, Użytkownik musi zablokować ekran stacji roboczej (zablokować pulpit lub włączyć wygaszacz ekranu zabezpieczony hasłem). Jeśli komputer Użytkownika nie pozwala na zabezpieczenie ekranu hasłem, to należy bezwzględnie wylogować się z Systemu.
5. Po zakończeniu pracy należy wylogować się z każdej używanej aplikacji Systemu poprzez kliknięcie w prawym górnym rogu ekranu funkcji „Wyloguj". Nie należy kończyć pracy poprzez zamknięcie okna przeglądarki znakiem „x".

§ 7.

POCZTA ELEKTRONICZNA, INTERNET

1. W SZT wykorzystano funkcjonalność wysyłania powiadomień na adres e-mail podany w SZT. 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

1. Użytkownik jest zobowiązany do niezwłocznego powiadomienia o podatności, zdarzeniu związanym z bezpieczeństwem informacji lub incydencie.
2. Każdy Użytkownik, w przypadku podejrzenia wystąpienia podatności lub incydentu związanego z bezpieczeństwem informacji lub zauważenia, że stan sprzętu komputerowego, zawartość zbioru danych osobowych w Systemie, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie bezpieczeństwa danych osobowych przetwarzanych w Systemie, jest zobowiązany do niezwłocznego poinformowania o tym fakcie Administratora Merytorycznego Właściwej instytucji.
3. Administrator Merytoryczny Właściwej instytucji powinien postępować zgodnie z Procedurą obsługi zgłoszeń w Service Desk centralnego systemu teleinformatycznego.
4. Aktualna Procedura obsługi zgłoszeń w Service Desk centralnego systemu teleinformatycznego jest udostępniana dla Administratorów Merytorycznych w Bazie Wiedzy.

§ 9.

INFORMACJE W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Administratorem danych osobowych w rozumieniu przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 jest minister właściwy do spraw rozwoju regionalnego z siedzibą w Warszawie przy ul. Wspólnej 2/4, 00-926 Warszawa.
2. Inspektorem ochrony danych, o którym mowa w art. 8 ustawy o ochronie danych osobowych jest Pan Jacek Orzeł, adres poczty elektronicznej: Jacek.Orzel@miir.gov.pl
3. Zakres przetwarzanych w Systemie przez Użytkownika danych osobowych nie może być szerszy niż określony w umowie/porozumieniu dot. powierzenia przetwarzania danych osobowych zawartej/tym przez Administratora, o którym mowa w ust. 1 lub w jego imieniu.
4. Przetwarzanie danych osobowych jest zgodne z prawem i spełnia warunki, o których mowa art. 6 ust. 1 pkt. c) oraz art. 9 ust. 2 pkt. g) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679. Dane są przetwarzane wyłącznie w celu określonym w umowie/porozumieniu dot. powierzenia przetwarzania danych osobowych zawartej/tym przez Administratora, o którym mowa w ust. 1 lub w jego imieniu, na podstawie:
    1) 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 Rady (WE) nr 1083/2006 (Dz.U.UE.L.2013.347.320).
    2) Rozporządzenia Parlamentu Europejskiego I Rady (UE) NR 1304/2013 z dnia 17 grudnia 2013 r. w sprawie Europejskiego Funduszu Społecznego i uchylającego rozporządzenie Rady (WE) nr 1081/2006 (Dz.U.UE.L.2013.347.470).
    3) Rozporządzenia Wykonawczego Komisji (UE) nr 1011/2014 z dnia 22 września 2014 r. ustanawiającego szczegółowe przepisy wykonawcze do Rozporządzenia Parlamentu europejskiego i Rady (UE) nr 1303/2013 w odniesieniu do wzorów służących do przekazywania Komisji określonych informacji oraz szczegółowe przepisy dotyczące wymiany informacji między beneficjentami a instytucjami zarządzającymi, certyfikującymi, audytowymi i pośredniczącymi.
    4) Ustawy z dnia 11 lipca 2014 r. o zasadach realizacji programów w zakresie polityki spójności finansowanych w perspektywie finansowej 2014-2020 (Dz. U. z 2017 r. poz. 1460, 1475 i 2433).
    5) Rozporządzenia Wykonawczego Komisji (UE) nr 897/2014 z dnia 18 sierpnia 2014 r. ustanawiającego przepisy szczegółowe dotyczące wdrażania programów współpracy transgranicznej finansowanych na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 232/2014 ustanawiającego Europejski Instrument Sąsiedztwa.
5. Użytkownik odpowiada za zgodność z dokumentami źródłowymi, danych osobowych wprowadzonych przez siebie do Systemu.
6. Dane osobowe będą przechowywane do czasu rozliczenia programów operacyjnych współfinansowanych z funduszy Unii Europejskiej na lata 2014 -2020.
7. Każdy Użytkownik ma prawo dostępu do treści swoich danych i ich uzupełnienia, uaktualnienia lub sprostowania.
8. Każdy Użytkownik ma prawo do wniesienia skargi do organu nadzorczego, którym jest Prezes Urzędu Ochrony Danych Osobowych.

Warszawa, 25.05.2018 r.