

Załącznik Zarządzenia Nr 55/2017
Wójta Gminy Sławatycze
z dnia 31 grudnia 2017 r.



**INSTRUKCJA ZARZĄDZANIA SYSTEMEM
INFORMATYCZNYM**

SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

DLA ZBIORÓW:

„UCZESTNICY PROJEKTÓW DOFINANSOWANYCH Z EUROPEJSKIEGO FUNDUSZU SPOŁECZNEGO W RAMACH REGIONALNEGO PROGRAMU OPERACYJNEGO WOJEWÓDZTWA LUBELSKIEGO 2014-2020” ORAZ CENTRALNY SYSTEM TELEINFORMATYCZNY WSPIERAJĄCY REALIZACJĘ PROGRAMÓW OPERACYJNYCH

Rozdział 1

Postanowienia ogólne

§1.

Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych dla zbiorów: „Uczestnicy projektów dofinansowanych z Europejskiego Funduszu Społecznego w ramach Regionalnego Programu Operacyjnego Województwa Lubelskiego 2014-2020” oraz Centralny system teleinformatyczny wspierający realizację programów operacyjnych zwana dalej „Instrukcją”, określa zasady i tryb postępowania przy przetwarzaniu danych osobowych w centralnym systemie teleinformatycznym służącym do przetwarzania danych osobowych beneficjentów i uczestników projektów w ramach Regionalnego Programu Operacyjnego Województwa Lubelskiego na lata 2014-2020 zwanym dalej „SL2014” w Urzędzie Gminy w Sławatyczach, zwanym dalej „Beneficjentem” w zakresie bezpieczeństwa informacji w tym ochrony danych osobowych przetwarzanych w Systemie SL2014 oraz zakres i warunki korzystania przez Użytkowników z Systemu SL2014.

§2.

Użyte w Instrukcji określenia oznaczają:

Ustawa - ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922)

Rozporządzenie - rozporządzenie Ministra Spraw Wewnętrznych i Administracji 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 (Dz. U. z 2004 r. nr 100. poz. 1024);

Instytucja Zarządzająca - należy przez to rozumieć instytucję zaangażowaną w realizację programów operacyjnych w perspektywie finansowej 2014-2020 z którą Beneficjent zawarł umowę o dofinansowanie projektu - Zarząd Województwa Lubelskiego;

System SL2014 - należy przez to rozumieć aplikację główną centralnego systemu teleinformatycznego, wykorzystywany w procesie rozliczania Projektu oraz komunikowania się z Instytucją Zarządzającą, o którym mowa w Wytycznych Ministra Infrastruktury i Rozwoju w zakresie warunków gromadzenia i przechowywania danych w postaci elektronicznej na lata 2014-2020;

SZT - System zarządzania tożsamością — aplikacja wspierająca zarządzanie procesami logowania w ramach centralnego systemu teleinformatycznego. Umożliwia zalogowanie się do systemu SL2014;

Operator - należy przez to rozumieć urząd obsługujący ministra właściwego do spraw rozwoju regionalnego;

Beneficjent - Gmina Sławatycze;

Użytkownik - należy przez to rozumieć osobę mającą dostęp do Systemu SL2014, wyznaczoną przez Beneficjenta do wykonywania w jego imieniu czynności związanych z realizacją projektów;

Dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej dane osobowe, w rozumieniu ustawy, dotyczące:

- a) pracowników Beneficjenta.
- b) uczestników projektów realizowanych ze środków EFS w ramach Regionalnego Programu Operacyjnego Województwa Lubelskiego 2014-2020,
- c) osób, których dane są przetwarzane w związku z badaniem kwalifikowalności wydatków w projekcie, w tym w szczególności personelu projektu, a także oferentów, uczestników komisji przetargowych i wykonawców przetwarzanie przez Beneficjenta w celu realizacji projektu;

Administrator danych osobowych - Zarząd Województwa Lubelskiego - Instytucja Zarządzająca (IZ) dla zbiorów „Uczestnicy projektów dofinansowanych z Europejskiego Funduszu Społecznego w ramach Regionalnego Programu Operacyjnego Województwa Lubelskiego 2014-2020” Minister Rozwoju dla zbioru Centralny system teleinformatyczny wspierający realizację programów operacyjnych;

Przetwarzanie danych osobowych - jakiegokolwiek operacje wykonywane na danych osobowych polegające na: zbieraniu, utrwalaniu, przechowywaniu, opracowywaniu, zmienianiu, udostępnianiu i usuwaniu danych osobowych, zwłaszcza te, które wykonuje się w systemie informatycznym;

Usuwanie danych osobowych - zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

Zbiór danych osobowych - posiadający strukturę zestaw danych o charakterze danych osobowych, które są dostępne według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

Zabezpieczenie danych osobowych w systemie informatycznym - środki administracyjne, techniczne i fizyczne wdrożone w celu zabezpieczenia zasobów technicznych oraz ochrony przed zniszczeniem, nieuprawnionym dostępem i modyfikacją, ujawnieniem lub pozyskaniem danych osobowych bądź ich utratą;

Naruszenie zabezpieczenia - jakiegokolwiek zdarzenie lub działanie, które może stanowić przyczynę utraty zasobów, niezawodności, integralności lub poufności;

Administrator Bezpieczeństwa Informacji - ABI - osobę odpowiedzialną za nadzór nad zapewnieniem bezpieczeństwa danych osobowych w instytucji zarządzającej;

Administrator Danych u Beneficjenta - Wójt Gminy Sławatycze;

Administrator Systemu Informatycznego u Beneficjenta - ASI - osoba odpowiedzialna za sprawność, konserwację, oraz wdrażanie technicznych zabezpieczeń systemu informatycznego u Beneficjenta.

§3.

1. Instytucja Zarządzająca powierza Beneficjentowi przetwarzanie danych osobowych.
2. Zakres danych osobowych przetwarzanych przez Użytkownika w Systemie nie może być większy niż powierzony do przetwarzania przez Instytucję Zarządzającą.
3. Dane osobowe są przetwarzane wyłącznie w celu realizacji umowy na realizację projektu współfinansowanego z Unii Europejskiej w ramach Regionalnego Programu Operacyjnego Województwa Lubelskiego na lata 2014-2020

4. Powierzone dane osobowe mogą być wykorzystywane przez Beneficjenta wyłącznie w celu:
 - 1) udzielania wsparcia uczestnikom Projektu, z uwzględnieniem rekrutacji, działań informacyjnych, monitorowania, sprawozdawczości, ewaluacji, kontroli i audytu prowadzonych w zakresie projektu dotyczy zbioru „Uczestnicy projektów dofinansowanych z Europejskiego Funduszu Społecznego w ramach Regionalnego Programu Operacyjnego Województwa Lubelskiego 2014-2020”
 - 2) zarządzania, kontroli, audytu, ewaluacji, sprawozdawczości i raportowania w ramach Programu oraz zapewnienia realizacji obowiązku informacyjnego dotyczącego przekazywania do publicznej wiadomości informacji o podmiotach uzyskujących wsparcie z funduszy polityki spójności w ramach Programu dotyczy zbioru „Centralny system teleinformatyczny wspierający realizację programów operacyjnych”.
5. Do przetwarzania danych osobowych mogą być dopuszczone jedynie osoby upoważnione przez Beneficjenta, posiadające imienne upoważnienie do przetwarzania danych osobowych.
6. Użytkownik odpowiada za zgodność z dokumentami źródłowymi, danych osobowych wprowadzonych przez siebie do Systemu SL2014.
7. Obszar, w którym przetwarzane są dane osobowe, zabezpieczone są przed dostępem osób nieuprawnionych .
8. Przetwarzanie danych osobowych w formie elektronicznej odbywa się wyłącznie na komputerach służbowych i obsługiwanych przez uprawnione osoby.
9. Administratorem danych dla zbioru:
 - a) „Uczestnicy projektów dofinansowanych z Europejskiego Funduszu Społecznego w ramach Regionalnego Programu Operacyjnego Województwa Lubelskiego 2014-2020” jest Województwo Lubelskie z siedzibą przy ul. Grottgera 4, 20-029 Lublin
 - b) Centralny system teleinformatyczny wspierający realizację programów operacyjnych” jest Minister Rozwoju

Rozdział 2

Warunki korzystania z systemu SL2014

§4.

Beneficjent, w przypadku przetwarzania powierzonych danych osobowych w systemie informatycznym, zobowiązuje się do przetwarzania ich w systemie SL 2014 oraz systemie informatycznym wskazanym przez Instytucję Zarządzającą.

§5.

System SL2014 działa w trybie ciągłym przez 24 godziny na dobę - za wyjątkiem okresu przeznaczonego na przerwę konserwacyjną.

§6.

W celu prawidłowego korzystania z Systemu SL2014 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.

§7.

Operator gromadzi informacje o adresie IP, z którego Użytkownik uwierzytelnia się w Systemie SL2014. Operator gromadzi adresy IP wyłącznie w celu wykrywania prób naruszenia zabezpieczeń Systemu SL2014 oraz prowadzenia audytu zabezpieczeń Systemu SL2014

Rozdział 3

Procedury nadawania uprawnień do przetwarzania danych osobowych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności Rejestrowanie i wyrejestrowywanie użytkowników Dostęp do Systemu SL2014

§8.

1. Korzystanie z funkcjonalności Systemu SL2014 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 przez Ministra Rozwoju do przetwarzania danych osobowych w zbiorze "Centralny system teleinformatyczny wspierający realizację programów operacyjnych".
3. Zmiana dotychczasowych uprawnień Użytkownika w Systemie SL2014, jest realizowana po przekazaniu przez Beneficjenta wniosku o nadanie/zmianę dostępu dla osoby uprawnionej lub wniosku o wycofanie dostępu dla osoby uprawnionej.
4. Uwierzytelnianie Użytkownika w Systemie SL2014 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 SL2014 następuje przez wykorzystanie loginu użytkownika oraz hasła wygenerowanego przez System SL2014
6. Aktywacja hasła dostępowego do Systemu następuje po kliknięciu przez Użytkownika w link aktywacyjny, przesłany w wiadomości mailowej, na podany w Systemie SL2014 adres e mail.
7. Z chwilą poprawnego zalogowania w Systemie SL2014 Użytkownik akceptuje możliwość otrzymywania drogą elektroniczną informacji dotyczących Systemu SL2014.
8. Użytkownik musi się zapoznać z Instrukcją użytkownika Systemu SL2014.
9. Użytkownik jest wyrejestrowywany z systemu SL2014 w każdym przypadku utraty przez niego uprawnień do przetwarzania danych w zbiorze „Centralny system teleinformatyczny wspierający realizację programów operacyjnych”, co ma miejsce szczególnie w przypadku:
 - 1) ustania zatrudnienia tego użytkownika u Beneficjenta lub zakończeniu przez tego użytkownika współpracy z Beneficjentem na podstawie umowy cywilno-prawnej;
 - 2) zmiany zakresu obowiązków użytkownika powodujących utratę uprawnień do przetwarzania danych osobowych.
10. Wydane przez Ministra Rozwoju upoważnienie wygasa z chwilą wycofania dostępu do aplikacji głównej centralnego systemu teleinformatycznego.
11. Dla każdego użytkownika jest ustalany odrębny identyfikator i hasło dostępu do Systemu SL2014.
12. Identyfikator użytkownika:
 - 1) jest niepowtarzalny, a po wyrejestrowaniu użytkownika z SL2014 nie jest przydzielany innej osobie;

- 2) jest wpisywany do rejestru osób upoważnionych do przetwarzania danych osobowych, wraz z imieniem i nazwiskiem użytkownika.
13. Na potrzeby ewidencji osób upoważnionych do przetwarzania danych osobowych nadawany jest Użytkownikowi identyfikator w systemie informatycznym.
 14. Użytkownik jest odpowiedzialny za wszystkie czynności wykonane przy użyciu identyfikatora, który został mu przyznany.
 15. Użytkownik jest zobowiązany utrzymywać hasło, którym się posługuje lub posługiwał, w ścisłej tajemnicy, w szczególności dołożyć wszelkich starań w celu uniemożliwienia zapoznania się przez osoby trzecie z hasłem, nawet po ustaniu jego ważności.
 16. Identyfikator nie jest wykorzystywany do logowania się lub pracy w aplikacji głównej centralnego systemu teleinformatycznego.
 17. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.

§9.

1. Upoważnienia do przetwarzania danych osobowych w „Uczestnicy projektów dofinansowanych z Europejskiego Funduszu Społecznego w ramach Regionalnego Programu Operacyjnego Województwa Lubelskiego 2014-2020” dokonuje osoba upoważniona do wydawania i odwoływania upoważnień u Beneficjenta. Wzór upoważnienia do przetwarzania danych osobowych oraz wzór odwołania upoważnienia do przetwarzania danych osobowych stanowią załączniki do umowy o dofinansowanie projektu. Upoważnienia są przechowywane w siedzibie Beneficjenta.
2. Imienne upoważnienia są ważne do dnia odwołania. Upoważnienie wygasa z chwilą ustania stosunku prawnego łączącego Beneficjenta z osobą której wydano upoważnienie. Beneficjent powinien posiadać przynajmniej jedną osobę legitymującą się imiennym upoważnieniem do przetwarzania danych osobowych odpowiedzialną za nadzór nad zarchiwizowaną dokumentacją.
3. Administrator Danych u Beneficjenta prowadzi rejestr - ewidencję osób upoważnionych do przetwarzania danych osobowych użytkowników, który stanowi załącznik nr 1 do Polityki Bezpieczeństwa.
4. Jakakolwiek zmiana informacji ujawnionych w rejestrze podlega natychmiastowemu odnotowaniu i uaktualnieniu.

Rozdział 4

Metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem Zasady bezpieczeństwa

§10.

1. Użytkownik jest zobowiązany do zapoznania się i zaakceptowania „Regulaminu bezpieczeństwa informacji przetwarzanych w aplikacji głównej centralnego systemu teleinformatycznego”, co potwierdza (przez złożenie oświadczenia na formularzu elektronicznym) podczas pierwszego logowania w Systemie SL2014.
2. Złożenie oświadczenia, o którym mowa w ust. 1, jest warunkiem uzyskania dostępu do Systemu SL2014. Informacja o dacie i godzinie złożenia przez Użytkownika oświadczenia jest przechowywana w Systemie SL2014.
3. Użytkownik ma obowiązek przestrzegania przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922) oraz przepisów wykonawczych do tej ustawy, co potwierdza (przez złożenie oświadczenia na formularzu elektronicznym) w Systemie SL2014.

4. Użytkownik ma obowiązek zachować w tajemnicy przetwarzane dane osobowe oraz informacje o sposobach ich zabezpieczenia, zarówno w okresie trwania umowy o dofinansowanie projektu, jak też po jej zakończeniu.
5. Dostęp do danych osobowych przetwarzanych w SL2014 jest dozwolony jedynie po właściwym zalogowaniu się i podaniu własnego hasła użytkownika.
6. System SL2014 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 musi zaczynać się od litery;
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. Użytkownik jest zobowiązany do niezwłocznej zmiany tego hasła.
10. W celu zapobiegania 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.
11. Zabronione jest korzystanie z Systemu SL2014 z użyciem danych dostępowych innego Użytkownika.
12. Użytkownicy są zobowiązani do ustawienia ekranów monitorów w taki sposób, aby uniemożliwić osobom postronnym wgląd lub spisanie informacji aktualnie wyświetlanej na ekranie monitora.
13. Komputery powinny zostać ustawione w taki sposób, aby osoby postronne miały utrudniony dostęp do portów zewnętrznych lub przynajmniej dostęp do portów zewnętrznych był pod kontrolą wizualną użytkowników.
14. Użytkownik zobowiązany jest do przestrzegania zasady czystego biurka. W szczególności przed opuszczeniem swego stanowiska pracy Użytkownik powinien schować wszelkie dokumenty związane z używanym Systemem SL2014 oraz informatyczne nośniki danych (dyskietki, płyty CD, DVD, pendrive itp.).
15. Osoby nieuprawnione do dostępu do danych osobowych w SL2014 mogą przebywać w pomieszczeniach, w których są przetwarzane dane osobowe w SL2014 wyłącznie w obecności co najmniej jednego użytkownika odpowiedzialnego za te osoby.
16. Beneficjent niezwłocznie informuje Instytucję Zarządzającą o:
 - 1) wszelkich przypadkach naruszenia tajemnicy danych osobowych lub o ich niewłaściwym użyciu;
 - 2) wszystkich czynnościach z własnym udziałem w sprawach dotyczących ochrony danych osobowych;
 - 3) wynikach kontroli prowadzonych przez podmioty uprawnione w zakresie przetwarzania danych osobowych wraz z informacją na temat zastosowania się do wydanych zaleceń.

Rozdział 5

Rozpoczęcie, zawieszenie i zakończenie pracy w Systemie SL2014

§ 11.

1. Rozpoczęcie pracy Użytkownika w Systemie SL2014 następuje po uruchomieniu przeglądarki oraz wprowadzeniu adresu: <https://www.sl2014.gov.pl>
2. Połączenie z Systemem SL2014 jest szyfrowane, odbywa się, po wybraniu przez Użytkownika odpowiedniego sposobu uwierzytelniania. Uwierzytelnianie Użytkownika następuje w procesie logowania przez wprowadzenie loginu i hasła.

3. Osoby upoważnione przez Beneficjenta zobowiązane są do wykorzystywania profilu zaufanego ePUAP lub bezpiecznego podpisu elektronicznego weryfikowanego za pomocą ważnego kwalifikowalnego certyfikatu w ramach uwierzytelnienia czynności dokonywanych w ramach SL2014.
4. Jeśli z powodów technicznych wykorzystanie profilu zaufanego ePUAP nie jest możliwe - w takich przypadkach uwierzytelnienie następuje przez wykorzystanie loginu i hasła wygenerowanego przez SL2014, gdzie jako login stosuje się PESEL danej osoby uprawnionej a hasło zostanie wygenerowane i przesłane na adres e-mail.
5. 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.
6. 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".

§12.

1. W przypadku stwierdzenia przez użytkownika naruszenia zabezpieczenia SL2014 lub zauważenia, że stan sprzętu komputerowego, zawartość zbioru danych osobowych w SL2014, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie bezpieczeństwa danych osobowych w SL2014, użytkownik jest zobowiązany niezwłocznie poinformować o tym Administratora Danych u Beneficjenta oraz Administratora Systemu Informatycznego u Beneficjenta.
2. O każdym przypadku naruszenia zabezpieczenia SL2014 Administrator Danych jest zobowiązany poinformować w formie pisemnej Administratora Danych w IZ.
3. Rozpoczynając pracę użytkownik powinien zwrócić szczególną uwagę na okoliczności, o których mowa w ust. 1.

Rozdział 6

Tworzenie oraz przechowywanie kopii zapasowych

§13.

1. Dane osobowe są wprowadzane do systemu SL2014 i są przechowywane w tym systemie.
2. Dane osobowe przetwarzane w systemie SL2014 zabezpieczone są przed wykonaniem kopii zapasowych zbiorów danych.
3. W przypadku utworzenia kopii zapasowych w celu sprawdzenia danych osobowych z systemu SL2014 przez Użytkownika zbiór jest przechowywany w sposób zgodny z przepisami i odpowiedzialny za prawidłowe przechowywanie jest AD.
4. Kopie o których mowa w ust.3 przechowuje się w sposób zabezpieczony przed dostępem osób nieuprawnionych.
5. Kopie zapasowe są bezzwłocznie usuwane po ustaniu ich użyteczności.
6. Urządzenia, dyski lub inne elektroniczne nośniki informacji zawierające dane osobowe przeznaczone do likwidacji, naprawy pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie.

Rozdział 7

Sposób zabezpieczania systemu informatycznego. Ochrona Systemu SL2014 przed wrogim oprogramowaniem

§14.

Bieżące i bezpośrednie sprawdzanie obecności wirusów komputerowych, koni trojańskich, robaków komputerowych, oprogramowania szpiegującego i kradnącego hasła odbywa się przy zastosowaniu zainstalowanego na każdej stacji roboczej aktualizowanego na bieżąco programu antywirusowego automatycznie monitorującego występowanie wirusów, koni trojańskich, robaków komputerowych, oprogramowania szpiegującego, oprogramowania kradnącego hasła podczas operacji na plikach;

§15.

1. Nadzór nad instalowaniem oprogramowania antywirusowego oraz nad bieżącą jego aktualizacją sprawuje Administrator Danych u Beneficjenta,
2. Czynności opisane w ust. 1 wykonuje Administrator Systemu Informatycznego u Beneficjenta.

§ 16.

1. O każdorazowym wykryciu wirusa lub konia trojańskiego przez oprogramowanie monitorujące użytkownik jest zobowiązany niezwłocznie powiadomić Administratora Danych u Beneficjenta. Po usunięciu wirusa lub innego niebezpiecznego oprogramowania Administrator Danych u Beneficjenta, sprawdza oraz przywraca go do pełnej funkcjonalności i sprawności.
2. Czynności opisane w ust. 1 wykonuje Administrator Systemu Informatycznego u Beneficjenta.

§ 17.

1. W ramach ochrony przed wrogim oprogramowaniem u Beneficjenta stosuje logiczne lub fizyczne urządzenia firewall.
2. Czynności opisane w ust. 1 wykonuje Administrator Systemu Informatycznego u Beneficjenta.

§ 18

Żadne nośniki informacji zawierające dane osobowe nie są udostępniane poza obszar, w którym są przetwarzane dane osobowe.

Zapis w ust. 1 nie dotyczy sytuacji, tzn. udostępnienia posiadanych w zbiorze danych osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa, w szczególności przekazania przez Beneficjenta danych z SL2014 właściwej Instytucji Zarządzającej.

Rozdział 8

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji Konfiguracja sprzętu komputerowego użytkownika

§ 19.

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 (fircwall).

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 SL2014.
7. Użytkownik podczas logowania się do Systemu SL2014 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?

§20.

1. Administrator Systemu Informatycznego ma obowiązek dokonywać przeglądów technicznych sprzętu informatycznego u Beneficjenta oraz dbać o ich dobry stan. W przypadku stwierdzenia usterek technicznych ASI ma obowiązek niezwłocznie powiadomić AD.
2. Przeglądy i konserwacje sprzętu komputerowego wynikające ze zużycia sprzętu oraz warunków zewnętrznych i eksploatacji, z uwzględnieniem ważności sprzętu dla funkcjonowania SL2014, są nadzorowane przez Administratora Danych u Beneficjenta.
3. Czynności opisane w ust. 2 wykonuje Administrator Systemu Informatycznego u Beneficjenta.

§21.

1. Dyski lub inne informatyczne nośniki informacji umieszczone w urządzeniach przeznaczonych do napraw, gdzie jest wymagane zaangażowanie zewnętrznych firm serwisowych, usuwa się z tych urządzeń lub pozbawia się przed naprawą zapisu danych osobowych przetwarzanych w SL2014.
2. W przypadku niemożliwości usunięcia nośnika lub pozbawienia go zapisu tych danych osobowych naprawy dokonuje się pod nadzorem Administratora Danych u Beneficjenta. Nadzór opisany w ust. 2 sprawuje Administrator Systemu Informatycznego u Beneficjenta.

§22

1. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przetwarzane w SL2014, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.
2. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przetwarzane w SL2014, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania tych danych osobowych, pozbawia się wcześniej ich zapisu.

Rozdział 9

Postępowanie w zakresie komunikacji w sieci komputerowej

§23.

1. W Systemie SL2014 wykorzystano funkcjonalność wysyłania powiadomień na adres e-mail podany w Systemie SL2014 . 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 nieznanymi 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 SL2014.

§24.

1. Decyzję o instalacji na stacji roboczej obsługującej przetwarzanie danych osobowych w SL2014 jakiegokolwiek oprogramowania systemowego lub użytkowego podejmuje Administrator Danych u Beneficjenta.
2. Czynności opisane w ust. 1 wykonuje Administrator Systemu Informatycznego u Beneficjenta.

Rozdział 10

Postanowienia końcowe

§25.

Do spraw nieuregulowanych w Instrukcji stosuje się przepisy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. oraz Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.

§26.

Instrukcja nie wyłącza stosowania innych instrukcji dotyczących zabezpieczenia SL2014.

§27.

Tekst Instrukcji jest udostępniany Użytkownikom w taki sposób, aby mogli się z nim zapoznać i wdrożyć w życie jej postanowienia.

WÓJT

Grzegorz Kier