Uchwała Nr 100/274/2017
Zarządu Powiatu w Wałczu
z dnia 12 grudnia 2017 r.

w sprawie przyjęcia „Polityki Bezpieczeństwa Powiatu Wałeckiego przy realizacji projektów RPO WZ 2014-2020" oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych przy realizacji projektów RPO WZ 2014-2020".

Na podstawie art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922),

Zarząd Powiatu w Wałczu uchwala, co następuje:

§ 1. Uchwala się „Politykę Bezpieczeństwa Powiatu Wałeckiego przy realizacji Projektów RPO WZ 2014-2020", w brzmieniu jak w załączniku nr 1 do niniejszej uchwały.

§ 2. Uchwala się „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych przy realizacji Projektów RPO WZ 2014-2020", w brzmieniu jak w załączniku nr 2 do niniejszej uchwały.

§ 3. Zobowiązuje się osoby realizujące projekty w ramach Regionalnego Programu Operacyjnego Województwa Zachodniopomorskiego 2014-2020 do stosowania „Polityki Bezpieczeństwa Powiatu Wałeckiego przy realizacji Projektów RPO WZ 2014-2020" oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych przy realizacji Projektów RPO WZ 2014-2020".

§ 4. Wykonanie uchwały powierza się Naczelnikowi Wydziału Inwestycji, Zamówień Publicznych i Funduszy Pomocowych oraz koordynatorom projektów.

§ 5. Uchwała wchodzi w życie z dniem podjęcia.

Zarząd Powiatu:

1. Starosta Wałecki – Bogdan Wankiewicz .....
2. Wicestarosta Wałecki – Jolanta Wegner .....
3. Członek Zarządu – Danuta Kęsek .....

RADCA PRAWNY
Michał Merefenko

Polityka Bezpieczeństwa Powiatu Wałeckiego przy realizacji Projektów RPO WZ 2014-2020

Zatwierdzam:

STAROSTA
dr Bogdan Wankiewicz

WICESTAROSTA
Jolanta Wegner

1.WPROWADZENIE

1.1. Cel opracowania dokumentu pt. "Polityka Bezpieczeństwa Powiatu Wałeckiego przy realizacji Projektów RPO WZ 2014-2020"

Powiatowi Wałeckiemu jako Beneficjentowi umów na realizacje Projektów RPO WZ 2014-2020 zgodnie z podpisanymi umowami z Zarządem Województwa Zachodniopomorskiego na podstawie Porozumienia w sprawie powierzenia przetwarzania danych osobowych w związku z realizacją Regionalnego Programu Operacyjnego Województwa Zachodniopomorskiego 2014-2020 z dnia 17.09.2015 r. zawartego pomiędzy Instytucją Zarządzającą a Instytucja Pośredniczącą oraz w związku z art. 31 ustawy o ochronie danych osobowych (Dz. U. z 2016 r. 922) powierzono przetwarzanie danych osobowych, w imieniu i na rzecz Właściwego Administratora danych osobowych.

Beneficjent przed rozpoczęciem przetwarzania danych osobowych przygotowuje dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, w tym w szczególności politykę bezpieczeństwa oraz instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

1.2. Podstawa prawna

Dokument **Polityka Bezpieczeństwa Powiatu Wałeckiego przy realizacji Projektów RPO WZ 2014-2020, zwana dalej „Polityka bezpieczeństwa"** oparta jest na podstawie następujących aktów prawnych:

1)ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. 922);

2)Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024.

3)w odniesieniu do zbioru Projekty RPO WZ 2014-2020:

- rozporządzenia Parlamentu Europejskiego i Rady Europu (UE) nr 1303/2013 z dnia 17 grudnia 2013 r.;
- rozporządzenia Parlamentu Europejskiego i Rady Europu (UE) nr 1304/2013 z dnia 17 grudnia 2013 r.;
- ustawy z dnia 11 lipca 2014 r. o zasadach realizacji programów w zakresie polityki spójności finansowanych w perspektywie finansowej 2014-2020 (Dz. U. z 2016 poz. 217).

1.3. Słownik pojęć

1)ustawa – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101 poz. 926 z późn. zm.), zwana dalej "ustawą";

2)dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny, jeden lub kilka specyficznych czynników określających jej cechy. Do danych osobowych zalicza się więc nie tylko imię, nazwisko i adres osoby, ale również przypisane jej numery, dane o cechach fizjologicznych, umysłowych, ekonomicznych, kulturowych i społecznych;

3)dane szczególnie chronione – informacje o pochodzeniu rasowym lub etnicznym, poglądach politycznych, przekonaniach religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, dane o stanie zdrowia, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu, mandatach karnych i innych orzeczeniach wydanych w postępowaniu sądowym lub administracyjnym. Przetwarzanie niniejszych danych jest dopuszczalne, jeżeli osoba, której dotyczą wyrazi zgodę na piśmie lub przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dotyczą.

4)zbiór danych osobowych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw jest rozproszony (jego części znajdują się w różnych miejscach) czy podzielony funkcjonalnie (przetwarzany za pomocą programów realizujących różne funkcje);

5)**przetwarzanie danych** – to operacje wykonywane na danych osobowych, tj. : zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie;

6)system informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

7)zabezpieczenie danych w systemie informatycznym – wdrożenie i eksploatacja stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przez ich nieuprawnioną modyfikacją, zniszczeniem, dostępem i ujawnieniem lub utratą;

8)usuwanie danych osobowych – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,

9)osoba upoważniona – osoba posiadająca wydane przez Zarząd Powiatu w Wałczu upoważnienie do przetwarzania danych osobowych;

10)identyfikator użytkownika (LOGIN) – ciąg znaków literowych i cyfrowych lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

11)**hasło (password)** – ciąg znaków literowych, cyfrowych lub innych, znany wyłącznie osobie uprawnionej do pracy w systemie informatycznym.

2. Rejestracja zbiorów danych

Administratorem Danych Osobowych przy realizacji Projektów RPO WZ 2014-2020 jest Ministerstwo Rozwoju oraz Zarząd Województwa Zachodniopomorskiego.

3. Upoważnienia do przetwarzania danych osobowych

Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Zarząd Powiatu w Wałczu, który jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 7 do Polityki bezpieczeństwa.

4. Środki techniczne i organizacyjne zastosowane do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Określone środki techniczne i organizacyjne niezbędne dla zapewnienia poufności i integralności przetwarzanych danych. Środki te mają na celu zapewnić jednocześnie rozliczalność wszelkich działań powodujących przetwarzanie danych osobowych. Niniejsze środki ochrony zostały określone po uprzedniej wnikliwej analizie zagrożeń i ryzyka związanych z przetwarzaniem danych osobowych.

Środki ochrony fizycznej

a. zbiory danych osobowych przetwarzane w formie papierowej przechowywane są w szafach zamykanych na klucz,
b. urządzenia, służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zamykanych na klucz,
c. przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osoby zatrudnionej przy przetwarzaniu danych,
d. na czas nieobecości pracownika zatrudnionego przy przetwarzaniu danych, pomieszczenia zamykane są na klucz, w sposób uniemożliwiający dostęp do nich osób trzecich,

e. każdy dokument papierowy, zawierający dane osobowe, przeznaczony do wyrzucenia, powinien zostać zniszczony w sposób uniemożliwiający jego odczytanie treści, przy pomocy niszczarki,

f. kontrola przetwarzanych danych prowadzona jest na bieżąco na każdym stanowisku merytorycznym, nadzór prowadzą koordynatorzy projektów,

g. o udostępnianiu danych osobowych innym podmiotom decyduje Zarząd Powiatu w Wałczu,

h. budynki, po zakończeniu pracy są zamykane na klucz, ponadto zabezpieczane systemem alarmowym oraz nadzorem służb ochrony.

Środki organizacyjne

a. została opracowana i wdrożona Polityka Bezpieczeństwa przetwarzanych danych osobowych oraz Instrukcja Zarządzania Systemem Informatycznym do przetwarzania danych w Projektach,

b. osoby zatrudnione przy przetwarzaniu danych przed rozpoczęciem pracy zostają przeszkolone w zakresie obowiązujących przepisów o ochronie danych osobowych (chyba, że posiadają aktualne zaświadczenie o odbytym szkoleniu z zakresu ochrony danych osobowych) , procedur przetwarzania danych, Polityką bezpieczeństwa oraz Instrukcją Zarządzania Systemem Informatycznym do przetwarzania danych osobowych obowiązujących w Projektach;

c. do przetwarzania danych osobowych są dopuszczone wyłącznie osoby, posiadające upoważnienie nadane przed Zarząd Powiatu w Wałczu,

d. osoby posiadające upoważnienie do przetwarzania danych, składają pisemne oświadczenie o zapoznaniu się z przepisami ustawy, Polityką bezpieczeństwa oraz pisemne zobowiązanie do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczania,

e. Koordynator projektu prowadzi ewidencje osób upoważnionych do przetwarzania danych osobowych (wzór ewidencji stanowi załącznik nr 6);

f. niedopuszczalne jest wykorzystywanie danych osobowych pozyskiwanych w trakcie wykonywania obowiązków służbowych do celów prywatnych,

g. w przypadku przebywania interesantów bądź innych osób postronnych w pomieszczeniach, monitory komputerów powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.

Zabronione jest:

- przechowywanie danych osobowych w szafach na korytarzach,
- pozostawienie otwartych pomieszczeń, w których przetwarzane są dane osobowe, pod nieobecność osób upoważnionych,
- pozostawienie dokumentów na biurku po zakończeniu pracy,
- przechowywanie dokumentów na parapetach, podłodze.

Ochrona obiektów oraz system alarmowy

Ochraniane są następujące obiekty:

a. budynek siedziby Starostwa Powiatowego w Wałczu (ul. Dąbrowskiego 17)
b. budynek Zespołu Szkół nr 1 w Wałczu (ul. Kilińszczaków 54)
c. budynek Zespołu Szkół Nr 4 RCKU w Wałczu (ul. Południowa 10A)
d. budynek Powiatowego Centrum Kształcenia Zawodowego i Ustawicznego (ul. Bankowa 13).

Ochrona ww. budynków prowadzona jest na zasadach określonych przez poszczególnych administratorów budynków.

Polityka kluczy

Polityka kluczy realizowana jest zgodnie z politykami bezpieczeństwa w poszczególnych instytucjach.

5. Opis zdarzeń naruszających ochronę danych osobowych

Podział zagrożeń

1) **Zagrożenia losowe zewnętrzne-** (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych.

2) **Zagrożenia losowe wewnętrzne** - (np. niezamierzone pomyłki administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.

3) **Zagrożenia zamierzone, świadome i celowe** - najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na :

- nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
- nieuprawniony dostęp do systemu z jego wnętrza,
- nieuprawniony przekaz danych,
- pogorszenie jakości sprzętu i oprogramowania,
- bezpośrednie zagrożenie materialnych składników systemu.

6 Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych

Niniejsza instrukcja określa tryb postępowania w sytuacji naruszenia ochrony danych osobowych gromadzonych i przetwarzanych zarówno w zbiorach tradycyjnych jak i informatycznych. Instrukcję stosuje się w przypadku, gdy stwierdzono naruszenie zabezpieczeń sprzętu informatycznego, sieci komputerowej, systemu alarmowego i zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe.

Przez naruszenie ochrony danych osobowych rozumie się niezgodne z przepisami ustawy o ochronie danych i rozporządzeń wykonawczych przetwarzanie danych oraz usuwanie danych osobowych.

Osobami bezpośrednio odpowiedzialnymi za zgodną z prawem ochronę danych osobowych i ich zabezpieczenie są koordynatorzy projektów.

1. Każda osoba biorąca udział w przetwarzaniu danych osobowych w systemie informatycznym jest odpowiedzialny za bezpieczeństwo tych danych. W szczególności osoba, która zauważyła zdarzenie, mogące być przyczyną naruszenia ochrony danych osobowych lub mogących spowodować naruszenie bezpieczeństwa danych, zobowiązana jest do natychmiastowego poinformowania Koordynatora projektu.

2. Każda osoba, która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych w systemie informatycznym (lub przetwarzanych w inny sposób), powinna niezwłocznie poinformować o tym fakcie Koordynatora projektu.

3. Do czasu przybycia Koordynatora projektu należy:

a)niezwłocznie podjąć czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,

b)zabezpieczyć dostęp do miejsca lub urządzenia przez osoby trzecie,

c)wstrzymać pracę na komputerze na którym zaistniało naruszenie ochrony oraz nie uruchamiać bez koniecznej potrzeby komputerów i innych urządzeń, których funkcjonowanie w związku naruszeniem ochrony zostało wstrzymane,

d)zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę zdarzenia,

e)nie zmieniać położenia przedmiotów, które pozwalają stwierdzić naruszenie ochrony lub odtworzyć jej okoliczności,

f)podjąć stosownie do zaistniałej sytuacji, inne niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych,

g)podjąć inne działania przewidziane w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,

h)wstępnie udokumentować zaistniałe naruszenie,

4. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych Koordynator projektu lub osoba zastępująca powinna :

a)zapoznać się z zaistniałą sytuacją i dokonać wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Starostwa,

b)zaprotokołować wszelkie informacje związane ze zdarzeniem,

c)wygenerować i wydrukować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia,

d)przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby niepowołanej,

e)dokonać fizycznego odłączenia urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nie uprawnionej,

f)wylogować użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych.

g)dokonać zmiany hasła użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania,

h)zażądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem.

POSTANOWIENIA KOŃCOWE

1. Wobec osoby, która w przypadku naruszenia ochrony danych osobowych lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zadaniami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.
2. Koordynatorzy projektu prowadzą ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych.
3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia ochrony danych osobowych lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym Koordynatora projektu.
4. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia Administratora Bezpieczeństwa Informacji nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
5. W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych , 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
6. Wykaz Załączników:
   1) Załącznik Nr 1 – **WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE**
   2) Załącznik Nr 2 – **WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH**
   3) Załącznik Nr 3 - **OPIS STRUKTURY ZBIORÓW DANYCH WSKAZUJĄCYCH ZAWARTOŚĆ POSZCZEGÓLNYCH PÓL INFORMACYJNYCH**
   4) Załącznik Nr 4 – **EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA ZBIORÓW DANYCH OSOBOWYCH**

5) Załącznik Nr 5 – **RAPORT Z NARUSZENIA OCHRONY DANYCH OSOBOWYCH**

6) Załącznik Nr 6 – **WYKAZ OSÓB, KTÓRE ZOSTAŁY ZAPOZNANE Z POLITYKĄ BEZPIECZEŃSTWA ORAZ INSTRUKCJĄ ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W PROJEKTACH**

7) Załącznik Nr 7 – **WZÓR UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH**

Załącznik Nr 1
do Polityki Bezpieczeństwa

WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

Nr pokoju	Komórka organizacyjna
Pomieszczenia Starostwa Powiatowego w Wałczu, ul. Dąbrowskiego 17	
202	Sekretariat
301	Wydział Inwestycji, Zamówień Publicznych i Funduszy Pomocowych
102	Wydział Inwestycji, Zamówień Publicznych i Funduszy Pomocowych
309	Wydział Inwestycji, Zamówień Publicznych i Funduszy Pomocowych
Pomieszczenia ZS Nr 1 w Wałczu, ul. Kilińszczaków 54	
1	Gabinet dyrektora
1	Sekretariat
Pomieszczenia ZS Nr 4 w Wałczu, ul. Południowa 10A	
105	Gabinet dyrektora
104	Gabinet wicedyrektorów
103	Sekretariat
Pomieszczenia Powiatowego Centrum Kształcenia Zawodowego i Ustawicznego w Wałczu, ul. Bankowa 13	
	Gabinet dyrektora
	Sekretariat

Załącznik Nr 2
do Polityki Bezpieczeństwa

WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

Lp.	NAZWA ZBIORU DANYCH OSOBOWYCH	PROGRAM ZASTOSOWANY DO PRZETWARZANIA DANYCH
1.	Zabiór danych uczestników projektu „NASZE RÓWNE SZANSE W SZKOLENIU I ZATRUDNIENIU - aktywna integracja Mieszkanek i Mieszkańców Powiatu Wałeckiego prowadząca do zatrudnienia w Zakładzie Aktywności Zawodowej"	**SL2014**
2.	Zabiór danych uczestników projektu „Moje kompetencje - otwarte wrota do kariery - podniesienie jakości i efektywności kształcenia w zakresie kompetencji kluczowych uczniów liceów ogólnokształcących w powiecie wałeckim”	
3.	Zabiór danych uczestników projektu „Wiedza oparta na praktyce - modernizacja kształcenia zawodowego w powiecie wałeckim”	

Załącznik Nr 3
do Polityki Bezpieczeństwa

Opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych

Lp.	NAZWA ZBIORU DANYCH OSOBOWYCH
1.	Zbiór danych uczestników projektu „NASZE RÓWNE SZANSE W SZKOLENIU I ZATRUDNIENIU - aktywna integracja Mieszkanek i Mieszkańców Powiatu Wałeckiego prowadząca do zatrudnienia w Zakładzie Aktywności Zawodowej”
2.	Zbiór danych uczestników projektu „Moje kompetencje - otwarte wrota do kariery - podniesienie jakości i efektywności kształcenia w zakresie kompetencji kluczowych uczniów liceów ogólnokształcących w powiecie wałeckim”
3.	Zbiór danych uczestników projektu „Wiedza oparta na praktyce - modernizacja kształcenia zawodowego w powiecie wałeckim”

Lp.	Nazwa
1.	Imię I nazwisko
2.	Adres
3.	Nr telefonu
4.	Nr faksu
5.	Adres e-mail
6.	Adres strony www
7.	Data rozpoczęcia udziału w projekcie
8.	Data zakończenia udziału w projekcie
9.	Rodzaj przyznanego wsparcia
10	Data rozpoczęcia udziału we wsparciu
11	Data zakończenia udziału we wsparciu
12	Rodzaj uczestnika
13	PESEL
14	Płeć
15	Wiek w chwili przystępowania do projektu
16	Wykształcenie
17	Status osoby na rynku pracy w chwili przystąpienia do projektu
18	Wykonywany zawód
19	Zatrudniony w(miejsce zatrudnienia)
20	Sytuacja osoby w momencie zakończenia udziału w projekcie
21	Zakończenie udziału osoby w projekcie zgodnie z zaplanowaną ścieżką uczestnictwa
22	Data założenia działalności gospodarczej
23	Kwota przyznanych środków na założenie działalności gospodarczej
24	PKD założonej działalności gospodarczej
25	Osoba bezdomna lub dotknięta wykluczeniem z dostępu do mieszkań
26	Osoba z niepełnosprawnościami
27	Osoba przebywająca w gospodarstwie domowym bez osób pracujących
28	W tym: w gospodarstwie domowych z dziećmi pozostającymi na utrzymaniu
29	Osoba żyjąca w gospodarstwie składającym się z jednej osoby dorosłej i dzieci pozostających na utrzymaniu
30	Osoba w innej niekorzystnej sytuacji społecznej (innej niż wymienione powyżej)
31	Przynależność do grupy docelowej zgodnie ze Szczegółowym Opisem Osi Priorytetowych Regionalnego Programu Operacyjnego Województwa Zachodniopomorskiego 2014-2020/zatwierdzonym do realizacji Rocznym Planem Działania/ zatwierdzonym do realizacji wnioskiem o dofinansowanie projektu
32	Rodzaj użytkownika
33	Forma zaangażowania
34	Miejsce pracy
35	Okres zaangażowania w projekcie
36	Wymiar czasu pracy
37	Godziny czasu pracy
38	Stanowisko
39	Data zaangażowania w projekcie
40	Specjalne potrzeby
41	Numer rachunku beneficjenta odbiorcy

Załącznik Nr 4
do Polityki Bezpieczeństwa

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA ZBIORÓW DANYCH OSOBOWYCH

Lp	Imię Nazwisko	Nr upoważnienia	Data wydania upoważnienia	Okres upoważnienia	Data ustania upoważnienia	Zakres upoważnienia
1	**2**	**3**	**4**	**5**	**6**	**7**

Załącznik Nr 5
do Polityki Bezpieczeństwa

Raport z naruszenia ochrony danych osobowych

1. Data:..... Godzina:.....
(dd-mm-rrrr)

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....
(Imię, nazwisko, stanowisko służbowe)

3. Lokalizacja zdarzenia:

.....
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....

.....

5. Podjęte działania:

.....

.....

6. Przyczyny wystąpienia zdarzenia:

.....

.....

7. Postępowanie wyjaśniające:

.....

.....

.....
data, podpis Koordynatora projektu

Załącznik Nr 6
do Polityki Bezpieczeństwa

WYKAZ OSÓB, KTÓRE ZOSTAŁY ZAPOZNANE Z POLITYKĄ BEZPIECZEŃSTWA ORAZ INSTRUKCJĄ ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W PROJEKTACH RPO WZ 2014-2020

Imię i nazwisko	Komórka organizacyjna	Data, podpis
1	2	3

Załącznik nr 7

do Polityki bezpieczeństwa

UPOWAŻNIENIE Nr_____
DO PRZETWARZANIA DANYCH OSOBOWYCH

Z dniem [_____] r., na podstawie art. 37 w związku z art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 t.j.), upoważniam [_____] do przetwarzania danych osobowych w zbiorze Projekty RPO WZ 2014-2020. Upoważnienie wygasa z chwilą ustania Pana/Pani* zatrudnienia w [_____] lub z chwilą jego odwołania.

_____
Czytelny podpis osoby upoważnionej do wydawania i odwoływania upoważnień

Upoważnienie otrzymałem

_____
(miejscowość, data, podpis)

Oświadczam, że zapoznałem/am się z przepisami dotyczącymi ochrony danych osobowych, w tym z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 t.j.), a także z obowiązującymi w _____ Polityką bezpieczeństwa ochrony danych osobowych oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych i zobowiązuję się do przestrzegania zasad przetwarzania danych osobowych określonych w tych dokumentach.

Zobowiązuję się do zachowania w tajemnicy przetwarzanych danych osobowych, z którymi zapoznałem/am się oraz sposobów ich zabezpieczania, zarówno w okresie zatrudnienia w _____/ wykonywania zadań na podstawie stosunku cywilnoprawnego*, jak też po jego ustaniu/po zrealizowaniu zadań wykonywanych na podstawie stosunku cywilnoprawnego*.

_____
Czytelny podpis osoby składającej oświadczenie

*niepotrzebne skreślić

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych przy realizacji Projektów RPOWZ 2014-2020

Zatwierdzam:

STAROSTA
dr Bogdan Wankiewicz

WICESTAROSTA
Jolanta Wegner

1. Podstawa prawna

Dokument „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych przy realizacji Projektów RPOWZ 2014-2020", zwana dalej „Instrukcją" oparta jest na podstawie następujących aktów prawnych:

1)ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. 922);

2)rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024.

3)w odniesieniu do zbioru „Centralny system teleinformatyczny wspierający realizację programów operacyjnych":

- rozporządzenia Parlamentu Europejskiego i Rady Europu (UE) nr 1303/2013 z dnia 17 grudnia 2013 r.;
- rozporządzenia Parlamentu Europejskiego i Rady Europu (UE) nr 1304/2013 z dnia 17 grudnia 2013 r.;
- ustawy z dnia 11 lipca 2014 r. o zasadach realizacji programów w zakresie polityki spójności finansowanych w perspektywie finansowej 2014-2020 (Dz. U. z 2016 poz. 217).
- 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 miedzy beneficjentami a instytucjami zarządzającymi, certyfikującymi, audytowymi i pośredniczącymi (Dz. Urz. UE L 286 z 30.09.2014, str. 1).

2. Przetwarzanie danych osobowych w Centralnym systemie teleinformatycznym (SL2014)

Przetwarzanie danych osobowych na potrzeby realizacji Projektów RPO WZ 2014-2020 w systemach teleinformatycznych odbywa się wyłącznie przy wykorzystaniu Aplikacji głównej centralnego systemu teleinformatycznego (SL2014), którego administratorem jest Ministerstwo Rozwoju.

3. Upoważnienia do przetwarzania danych osobowych

Do przetwarzania danych osobowych w systemie teleinformatycznym mogą być dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych nadane przez Zarząd Powiatu w Wałczu,

zgodnie z **Polityką Bezpieczeństwa Powiatu Wałeckiego przy realizacji Projektów RPO WZ 2014-2020**.

Zarząd Powiatu w Wałczu wyznacza osoby uprawnione do wykonywania w jego imieniu czynności związanych z realizacją projektów i zgłasza je do Instytucji Pośredniczącej do pracy w SL2014. Zgłoszenie ww. osób, zmiana ich uprawnień lub wycofanie dostępu jest dokonywane na podstawie wniosku o nadanie/zmianę/wycofanie dostępu dla osoby uprawnionej.

Wzór wniosku o nadanie/zmianę/wycofanie dostępu dla osoby uprawnionej w ramach SL2014, stanowi załącznik nr 1 do Instrukcji.

Każdy użytkownik systemu SL2014 przed przystąpieniem do przetwarzania danych osobowych zostaje zapoznany z regulaminem bezpieczeństwa informacji przetwarzanych w aplikacji głównej centralnego systemu teleinformatycznego, stanowiącym załącznik nr 2 do Instrukcji, i zobowiązuje się do jego przestrzegania.

Zapoznanie się z powyższymi dokumentami pracownik potwierdza własnoręcznym na wniosku nadanie/zmianę/wycofanie dostępu dla osoby uprawnionej w ramach SL 2014.

Załącznik nr 1 do Instrukcji

a) Wniosek o nadanie/zmianę[1] dostępu dla osoby uprawnionej w ramach SL2014[2]

Dane Beneficjenta:	
Kraj	
Nazwa Beneficjenta	
NIP Beneficjenta	
Nr projektu	

Dane osoby uprawnionej:	
Kraj	
PESEL[3]	
Nazwisko	
Imię	
Adres e-mail	

[1] Niepotrzebne skreślić, jedna z dwóch opcji jest obsługiwana danym wnioskiem dla osoby uprawnionej.
[2] Bez podania wymaganych danych nie będzie możliwe nadanie praw dostępu do SL2014.
[3] Dotyczy osób, dla których w polu „Kraj" wskazano „Polska".

Oświadczenie osoby uprawnionej[4]:
Ja, niżej podpisany/a .....*(imię i nazwisko)* oświadczam, że zapoznałem/am się z Regulaminem bezpieczeństwa informacji przetwarzanych w aplikacji głównej centralnego systemu teleinformatycznego i zobowiązuję się do jego przestrzegania. ..... *Data, podpis osoby uprawnionej*

Wnioskowany zakres uprawnień w SL2014:

Aplikacja obsługi wniosków o płatność, w tym:
· Wnioski o płatność
· Korespondencja
· Harmonogram płatności
· Monitorowanie uczestników projektu
· Zamówienia publiczne
· Personel projektu

[4] Należy wypełnić tylko w przypadku wniosku o nadanie dostępu dla osoby uprawnionej.

Oświadczenie Beneficjenta:	
Oświadczam, że wszystkie działania w SL2014, podejmowane przez osoby uprawnione zgodnie z niniejszym załącznikiem będą działaniami podejmowanymi w imieniu i na rzecz ..... *(nazwa beneficjenta).*	
Data sporządzenia wniosku	
Podpis Beneficjenta*	

*** Osoba/Osoby uprawnione do reprezentowania Beneficjenta (np. prokurent, członek zarządu, itd.)**

b) Wniosek o wycofanie dostępu dla osoby uprawnionej w ramach SL2014

Dane Beneficjenta:	
Kraj	
Nazwa Beneficjenta	
NIP Beneficjenta	
Nr projektu	

Dane osoby uprawnionej:	
Kraj	
PESEL[5]	
Nazwisko	
Imię	
Adres e-mail	

Data sporządzenia wniosku	
Podpis Beneficjenta*	

*** Osoba/Osoby uprawnione do reprezentowania Beneficjenta (np. prokurent, członek zarządu, itd.)**

[5] Dotyczy osób, dla których w polu „Kraj" wskazano „Polska".

Regulamin bezpieczeństwa informacji przetwarzanych w aplikacji głównej centralnego systemu teleinformatycznego

wersja 1.2

§ 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. z 2014 r. poz. 1146, z 2015 r. poz. 378, 1130), 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 Właściwą instytucję 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.
6. 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 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 wniosku o nadanie/zmianę dostępu dla osoby uprawionej lub wniosku o wycofanie dostępu dla osoby uprawnionej.
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. Właściwa instytucja udostępnia Użytkownikom *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 Właściwą instytucję 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.
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 oraz informatyczne nośniki danych (dyskietki, płyty CD, DVD, BD, pendrive itp.).

§ 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, 20 października 2015 r.

ZATWIERDZAM:

.....