ZARZĄDZENIE Nr 23/2017
Dyrektora Centrum Usług Wspólnych w Kobylnicy
z dnia 10.05.2017 roku

w sprawie polityki bezpieczeństwa i zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Centrum Usług Wspólnych w Kobylnicy

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2015 r., poz. 2135 z późn. zm.), oraz § 3 w związku z § 4 i § 5 rozporządzenia 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. Nr 100, poz. 1024),

zarządza się co następuje:

§ 1

Ustala się:

1) Politykę bezpieczeństwa przetwarzania danych osobowych w Centrum Usług Wspólnych w Kobylnicy, stanowiącą załącznik nr 1 do zarządzenia;
2) Instrukcję ochrony danych osobowych, stanowiącą załącznik nr 2 do zarządzenia;
3) Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Centrum Usług Wspólnych w Kobylnicy, stanowiącą załącznik nr 3 do zarządzenia;
4) Zasady użytkowania sprzętu komputerowego przez pracowników Centrum Usług Wspólnych w Kobylnicy, stanowiący złącznik nr 4 do zarządzenia;
5) Zasady udzielania pomocy użytkownikom sprzętu komputerowego w Centrum Usług Wspólnych w Kobylnicy, stanowiący złącznik nr 5 do zarządzenia;
6) Wzór wniosku o nadanie upoważnienia użytkownikowi w systemie informatycznym Centrum Usług Wspólnych w Kobylnicy, stanowiący złącznik nr 6 do zarządzenia;
7) Wzór rejestru kopi zapasowych, stanowiący złącznik nr 7 do zarządzenia;
8) Wzór druku zgłoszenia naruszenia bezpieczeństwa w systemach informatycznych Centrum Usług Wspólnych w Kobylnicy, stanowiący złącznik nr 8 do zarządzenia;
9) Wzór „ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych", stanowiący załącznik nr 9 do zarządzenia;
10) Wzór „wykaz zbiorów danych osobowych przetwarzanych w Centrum Usług Wspólnych w Kobylnicy", stanowiący załącznik nr 10 do zarządzenia;
11) Wzór „upoważnienia do przetwarzania danych osobowych", stanowiący załącznik nr 11 do zarządzenia.

§ 2

Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik Nr 1
do Zarządzenia Nr 23/2017
Dyrektora Centrum Usług Wspólnych
w Kobylnicy
z dnia 10.05.2017 r.

Polityka bezpieczeństwa przetwarzania danych osobowych w Centrum Usług Wspólnych w Kobylnicy.

I. Wstęp

§ 1

Celem Polityki Bezpieczeństwa przetwarzania danych osobowych w Centrum Usług Wspólnych w Kobylnicy zwanej dalej Polityką Bezpieczeństwa, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania w Centrum Usług Wspólnych w Kobylnicy informacji zawierających dane osobowe, a przede wszystkim zapewnienie ochrony danych osobowych przetwarzanych w Centrum przed wszelkiego rodzaju zagrożeniami, tak zewnętrznymi jak i wewnętrznymi.

§ 2

Polityka Bezpieczeństwa została utworzona w związku z wymaganiami zawartymi w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz rozporządzeniu 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. Opracowany dokument jest zgodny również z dyrektywą 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osób oraz ochrony prywatności w sektorze komunikacji elektronicznej.

§ 3

Obszarem przetwarzania danych osobowych w Centrum Usług Wspólnych w Kobylnicy są wydzielone pomieszczenia w budynku, w którym mieści się Centrum Usług Wspólnych w Kobylnicy, tj. ul. Wodnej 20/2, 76-251 Kobylnica.

§ 4

Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników.

§ 5

1. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w Centrum Usług Wspólnych w Kobylnicy rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych.
2. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:
   1) poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
   2) integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   3) rozliczalność danych - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
   4) integralność systemu - rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
   5) dostępność informacji - rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;

6) zarządzanie ryzykiem - rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

§ 6

Administratorem Danych Osobowych przetwarzanych w Centrum Usług Wspólnych w Kobylnicy jest Dyrektor Centrum Usług Wspólnych w Kobylnicy.

§ 7

Na Administratora Bezpieczeństwa Informacji w Centrum Usług Wspólnych w Kobylnicy mianowany jest pracownik zatrudniony na stanowisku ds. zaopatrzenia, gospodarowania majątkiem trwałym i prowadzenia archiwum.

II. Definicje

§ 8

Przez użyte w Polityce Bezpieczeństwa określenia należy rozumieć:

1) **Polityka Bezpieczeństwa** – rozumie się przez to Politykę Bezpieczeństwa Ochrony Danych Osobowych w Centrum Usług Wspólnych w Kobylnicy;
2) **Administrator Danych Osobowych –** dalej jako Administrator danych; rozumie się przez to Dyrektora Centrum Usług Wspólnych w Kobylnicy;
3) **Administrator Bezpieczeństwa Informacji (ABI)** - rozumie się przez to osobę wyznaczoną przez Administratora Danych Osobowych, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
4) **Centrum** – Centrum Usług Wspólnych w Kobylnicy;
5) **Ustawa** – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2015 r., poz. 2135 z późn. zm);
6) **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);
7) **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
8) **Zbiór danych osobowych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
9) **Baza danych osobowych** – zbiór uporządkowanych powiązanych ze sobą tematycznie zapisanych np. w pamięci wewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze – rekordów lub obiektów, w których są zapisywane dane osobowe;
10) **Usuwanie danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dotyczą.
11) **Przetwarzane danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
12) **System informatyczny** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
13) **System tradycyjny** - rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;

14) **Zabezpieczenie danych w systemie informatycznym** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
15) **Administrator Systemu Informatycznego (ASI)** – rozumie się przez to osobę lub osoby, upoważnione przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi w Centrum Usług Wspólnych w Kobylnicy (specjalista ds. obsługi i zabezpieczenia informatycznej bazy danych);
16) **Użytkownik** - rozumie się przez to upoważnionego przez Administratora danych lub Administratora Bezpieczeństwa Informacji, wyznaczonego do przetwarzania danych osobowych pracownika lub stażysty, który odbył stosowne szkolenie w zakresie ochrony tych danych.

III. Zakres stosowania

§ 9

1. W Centrum Usług Wspólnych w Kobylnicy przetwarzane są przede wszystkim informacje służące do realizowanych przez Gminę na rzecz społeczności lokalnej zadań własnych i zleconych przez administrację państwową oraz wynikające z stosunku pracy.
2. Informacje te są przetwarzane i składowane zarówno w postaci dokumentacji tradycyjnej jak i elektronicznej.
3. Polityka Bezpieczeństwa zawiera dokumenty dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

§ 10

Politykę Bezpieczeństwa stosuje się przede wszystkim do:
1) Danych osobowych przetwarzanych w systemach (programach) określonych w ***Załączniku C*** do niniejszej polityki bezpieczeństwa.
2) Wszystkich informacji dotyczących danych pracowników i urzędników Centrum Usług Wspólnych w Kobylnicy, w tym danych osobowych i treści zawieranych umów o pracę.
3) Wszystkich danych kandydatów do pracy zbieranych na etapie rekrutacji.
4) Informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych.
5) Rejestru osób dopuszczonych do przetwarzania danych osobowych.
6) Innych dokumentów zawierających dane osobowe.

§ 11

1. Zakresy ochrony danych osobowych określone przez dokumenty Polityki Bezpieczeństwa mają zastosowanie do systemów informatycznych, w których są przetwarzane dane osobowe, a w szczególności do:
   1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie;
   2) wszystkich lokalizacji - budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;
   3) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, stażystów i innych osób mających dostęp do informacji podlegających ochronie.
2. Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa zobowiązani są wszyscy pracownicy w rozumieniu Kodeksu Pracy, stażyści oraz inne osoby mające dostęp do informacji podlegających ochronie Centrum.

§ 12

Informacje niejawne nie są objęte zakresem niniejszej Polityki Bezpieczeństwa.

IV. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe oraz sposobów ich zabezpieczeń.

§ 13

1. Polityka obowiązuje w Centrum Usług Wspólnych w Kobylnicy, w pomieszczeniach lub częściach pomieszczeń, w których przetwarzane są dane osobowe, a których wykaz został określony poniżej oraz w ograniczonym zakresie w pomieszczeniach zajmowanych przez jednostki oświatowe obsługiwane przez Centrum.
2. Centrum mieści się w jednym budynku przy ul. Wodnej 20/2 w Kobylnicy.
3. Wykaz pomieszczeń w budynku tworzących w Centrum obszar, w którym przetwarzane są dane osobowe stanowi ***Załącznik A*** do niniejszego załącznika.

V. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

§ 14

Wykaz zbiorów danych osobowych, gromadzonych i przetwarzanych w Centrum stanowi ***Załącznik B*** do niniejszego załącznika,

VI. Struktura zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych.

§ 15

Struktura zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych dla programów i systemów stosowanych w Centrum adekwatna jest do zakresu przetwarzanych danych i przedstawia się w sposób następujący:

1. **W ramach Działu Finansowo - Księgowego** przetwarzane są dane osobowe pracowników oraz osób, a także kontrahentów świadczących usługi na rzecz administratora danych na innej podstawie niż stosunek pracy. Dane te są niezbędne do dokonywania przelewów wynagrodzeń oraz dokonywania różnego rodzaju płatności bieżących związane z realizacją zadań związanych z polityką fiskalną państwa oraz ściągalnością zobowiązań podatkowych podmiotów wobec Gminy.
   Zbiór **Rejestr umów najmu - p**rzetwarzane są w nim takie dane osobowe jak: nazwisko i imię, nr PESEL lub NIP, adres i miejsce zamieszkania.
   Rejestr umów zleceń - przetwarzane są w nim takie dane osobowe jak: nazwisko i imię, PESEL, adres i miejsce zamieszkania.

2. **Na stanowisku ds. kadr** przetwarzane są dane związane z składaniem skarg Dyrektora Centrum Usług Wspólnych w Kobylnicy w zbiorze **Rejestr skarg i wniosków.** Dane przetwarzane są na podstawie Ustawy z dnia z dnia 16 czerwca 1960 r. Kodeks postępowania administracyjnego. W zbiorze przetwarza się dane: imię i nazwisko, adres zamieszkania.

   W zbiorze **Kadry** przetwarzane są dane byłych i obecnych pracowników Centrum Usług Wspólnych i szkół, dla których organem prowadzącym jest Gmina. W zbiorze przetwarza się dane: imię i nazwisko, adres zamieszkania, numer telefonu, wysokość wynagrodzenia, staż pracy, wykształcenie, urlopy, zwolnienia, numer PESEL, numer dowodu osobistego, numer konta, imiona rodziców, miejsce urodzenia, informacje o odbytach szkoleniach, posiadanych dzieciach i związkach małżeńskich, dane o stanie zdrowia, dane dotyczące zainteresowań.

3. **Na stanowisku ds. obsługi sekretariatu** przetwarzane są dane związane z realizacją na rzecz rożnego rodzaju podmiotów czynności i praw, które pozostają w kompetencjach Centrum Usług Wspólnych w zbiorze: **Książka korespondencji**. Dane przetwarzane są na podstawie art. 6,7 i 8 Ustawy z dnia 8 marca 1990 r. o samorządzie gminnym t.j. Dz. U. z 2015 r. poz. 1515 z późn. zmianami. W zbiorze przetwarza się dane: imię i nazwisko, adres zamieszkania, numer telefonu,

W Centrum Usług Wspólnych w Kobylnicy jako jednostce organizacyjnej Gminy Kobylnica na podstawie art. 68 ust. 2 Ustawy o systemie informacji oświatowej w formie elektronicznej na dostarczonym i administrowanym przez Ministerstwo Edukacji Narodowej w ramach programu rządowego – **System Informacji Oświatowej (SIO)** Na stanowisku ds. obsługi sekretariatu oraz w Dziale Oświaty i Sportu przetwarzane są dane osobowe dzieci do lat 18 podlegających obowiązkowi nauki, wychowaniu przedszkolnemu (od 2,5 roku życia) oraz kadry pedagogicznej i kierowniczej szkoły.
W zbiorze przetwarza się takie dane jak: imiona i nazwisko, datę urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny pesel, adres dla korespondencji, numer dokumentu tożsamości, a w przypadku nauczycieli również posiadane kwalifikacje zawodowe.

4. **W ramach Działu Oświaty i Sporu prowadzone są niżej wymienione zbiory, w ramach których przetwarzane są dane:**

„Pomoc materialna dla uczniów” zbiór prowadzony w celu obsługi stypendiów i zasiłków szkolnych, wypłacanych na podstawie ustawy z dnia 7 września 1991 roku o systemie oświaty, obejmuje dane osobowe uczniów (imię i nazwisko, datę i miejsce urodzenia, PESEL, miejsce zamieszkania, miejsce spełniania obowiązku szkolnego i nauki), dane osobowe członków ich rodzin, (imię i nazwisko, adres zamieszkania, nr telefonu, informację o sytuacji materialnej rodziny – wysokość dochodu, nr konta)**,**

„Obowiązek szkolny i nauki” - zbiór prowadzony do realizacji kontroli spełnienia obowiązku nauki przez młodzież w wieku 16 – 18 lat, zameldowanej na terenie gminy Kobylnica, obejmuje ewidencję uczniów w wieku 16 – 18 lat (podstawowe dane osobowe ucznia: imię i nazwisko, data urodzenia, PESEL, obywatelstwo, imiona rodziców, miejsce zameldowania), wykaz szkół, rejestrację faktów związanych ze spełnieniem obowiązku szkolnego i nauki przez dzieci i młodzież,

„Pomocy zdrowotnej dla nauczycieli” w ramach zbioru przetwarzane są dane Wnioskodawców o przyznanie pomocy zdrowotnej – imię i nazwisko, stan rodzinny, dochód na osobę w rodzinie, zarobki, wydatki na leczenie, choroby i schorzenia.

„Awansu zawodowego na nauczyciela mianowanego”- w ramach zbioru przetwarzane są dane osobowe nauczyciela: imię i nazwisko, data i miejsce urodzenia, miejsce zamieszkania, PESEL.

„Stypendiów: artystycznego, sportowego, naukowego Wójta” w ramach zbioru przetwarzane są dane osobowe ucznia: imię i nazwisko, data i miejsce urodzenia, miejsce zamieszkania, PESEL.

„Ewidencja szkół i placówek niepublicznych” w ramach zbioru przetwarzane są dane osobowe wnioskodawcy (osoby fizycznej): imię i nazwisko, PESEL, NIP.

„Rejestru żłobków i klubów dziecięcych” w ramach zbioru przetwarzane są dane osobowe wnioskodawcy (osoby fizycznej): imię i nazwisko, PESEL, NIP.

„Przyznawania nauczania indywidualnego i rewalidacji” w ramach zbioru przetwarzane są dane osobowe ucznia: imię i nazwisko, dane zawarte w orzeczeniu o potrzebie kształcenia specjalnego, indywidualnego nauczanie tj. imiona rodziców/prawnych opiekunów, adres zamieszkania, wskazanie niepełnosprawności ucznia, stan zdrowia ucznia, diagnoza psychologiczno-pedagogiczna, w tym informacje o możliwościach rozwojowych ucznia i potencjale ucznia, zalecenia .

„Dofinansowania kształcenia młodocianych pracowników” w ramach zbioru przetwarzane są dane osobowe ucznia: imię i nazwisko, data i miejsce urodzenia, miejsce zamieszkania, PESEL.

„Zakwalifikowania dziecka – ucznia szkół z terenu gminy Kobylnica na kolonie” – w ramach zbioru przetwarzane są dane ucznia: imię i nazwisko, szkoła, wyniki w nauce i zachowaniu, stan zdrowia ewentualne choroby i schorzenia nr PESEL, dane rodziców: imię i nazwisko, adres zamieszkania, numery telefonów.

„**Praca wolontariuszy podczas imprez organizowanych przez CUW"** – przetwarzane są dane: imię i nazwisko, data i miejsce urodzenia, pesel, adres zamieszkania.

5. **Na stanowisku ds. zaopatrzenia, gosp. majątkiem i prowadzenia archiwum prowadzone są niżej wymienione zbiory, w ramach których przetwarzane są dane:**

   „Ewidencja dowozu uczniów do szkół" w ramach zbioru przetwarzane są dane osobowe ucznia, rodzica lub prawnego opiekuna: imię i nazwisko, data i miejsce urodzenia, miejsce zamieszkania, PESEL, numer konta.

   „Zakładowy Fundusz Świadczeń Socjalnych" w ramach zbioru przetwarzane są dane osobowe pracowników i ich rodzin: imię i nazwisko, data urodzenia, miejsce zamieszkania.

   „Rejestr umów pozostałych" Przetwarzane są w nim takie dane osobowe jak: nazwisko i imię, nr PESEL lub NIP, telefon kontaktowy, adres i miejsce zamieszkania.

6. **Na stanowisko dyrektora oraz w Dziale Oświaty i Sportu** prowadzone są zbiory związane z realizacją projektów unijnych realizowanych na rzecz Gminy Kobylnica w tym projektu: „Upowszechnianie edukacji przedszkolnej w ramach MOF Słupska" tj. zbiór „**Regionalny Program Operacyjny Województwa Pomorskiego na lata 2014-2020**", „**Regionalny Program Operacyjny Województwa Pomorskiego na lata 2014-2020 – dane uczestników indywidualnych**" oraz **„Centralny system teleinformatyczny wspierający realizację programów operacyjnych.**

   Na podstawie art. 31 ustawy o ochronie danych osobowych, Instytucja Zarządzająca powierzyła Gminie Kobylnica przetwarzanie danych osobowych, w imieniu i na rzecz Instytucji Zarządzającej, na warunkach opisanych w umowie o dofinansowanie, w ramach zbiorów:
   - Regionalny Program Operacyjny Województwa Pomorskiego na lata 2014-2020,
   - Regionalny Program Operacyjny Województwa Pomorskiego na lata 2014-2020 – dane uczestników indywidualnych.

   Na podstawie § 8 ust. 1 Porozumienia w sprawie powierzenia przetwarzania danych osobowych w ramach Centralnego systemu teleinformatycznego wspierającego realizację programów operacyjnych w związku z realizacją Regionalnego Programu Operacyjnego Województwa Pomorskiego na lata 2014-2020 z dnia 9 września 2015 roku, zawartego pomiędzy Ministrem Infrastruktury i Rozwoju a Instytucją Zarządzającą, Instytucja Zarządzającą działając w imieniu i na rzecz Ministra właściwego ds. rozwoju regionalnego powierzyła Gminie Kobylnica przetwarzanie danych osobowych na warunkach opisanych w umowie o dofinansowanie: Centralny system teleinformatyczny wspierający realizację programów operacyjnych.

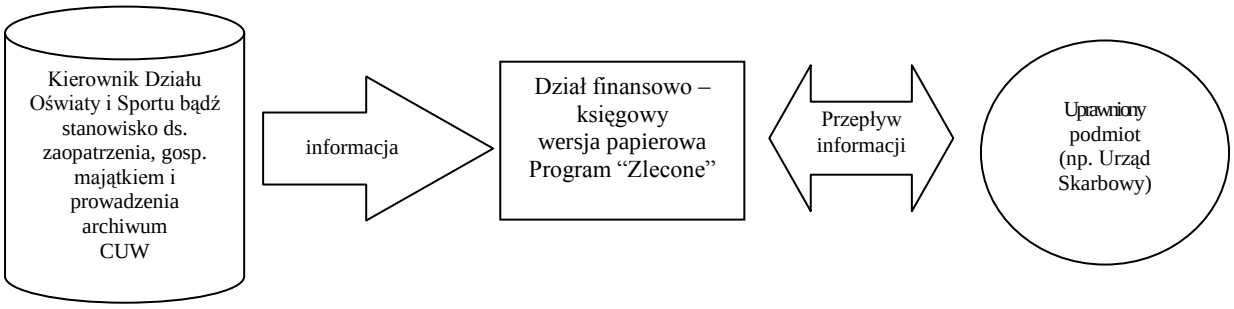
   Powierzone dane osobowe mogą być przetwarzane przez Centrum w zakresie określonym w umowy o dofinansowanie wyłącznie w celu aplikowania o środki unijne i realizacji Projektu:
   - w odniesieniu do zbiorów „Regionalny Program Operacyjny Województwa Pomorskiego na lata 2014-2020" i „Regionalny Program Operacyjny Województwa Pomorskiego na lata 2014-2020 – dane uczestników indywidualnych", w szczególności w zakresie potwierdzania kwalifikowalności wydatków, udzielania wsparcia uczestnikom Projektu, ewaluacji, monitoringu, kontroli, audytu, sprawozdawczości, działań informacyjno-promocyjnych w ramach Programu oraz zapewnienia obowiązku informacyjnego dotyczącego przekazywania do publicznej wiadomości informacji o podmiotach uzyskujących wsparcie z Programu,

   - w odniesieniu do zbioru „Centralny system teleinformatyczny wspierający realizację programów operacyjnych", w szczególności w zakresie 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.

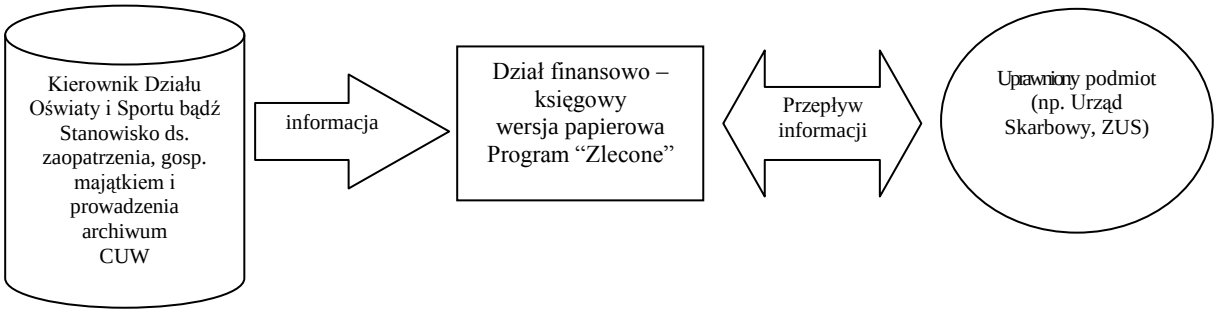
VII. Sposób przepływu danych między poszczególnymi systemami, współpracy systemów informatycznych ze zbiorami danych

1.

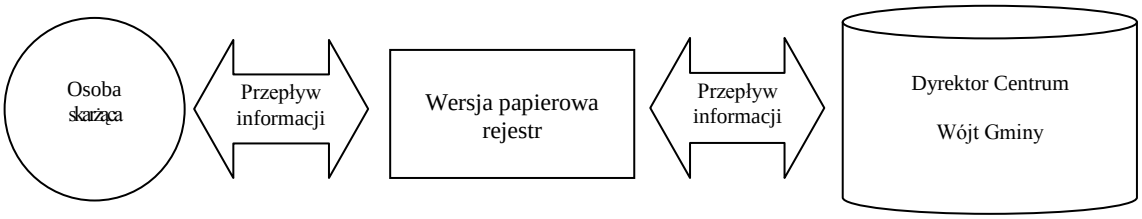
a. zbiór **Rejestr umów najmu**



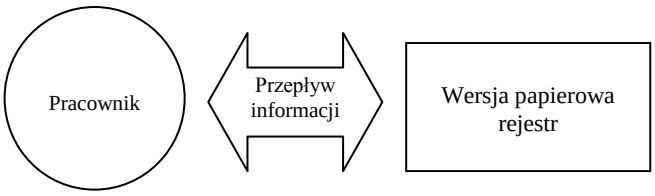
b. zbiór: **Rejestr umów zleceń**



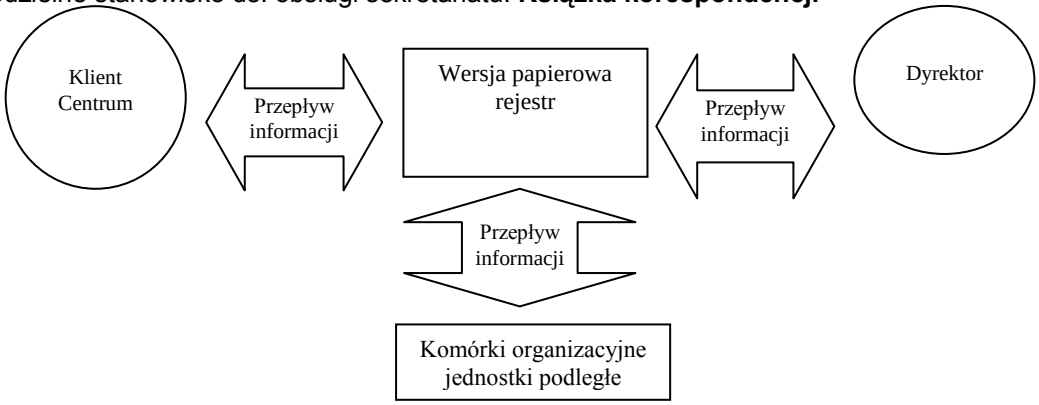
2. Samodzielne stanowisko ds. kadr: **Rejestr skarg i wniosków**



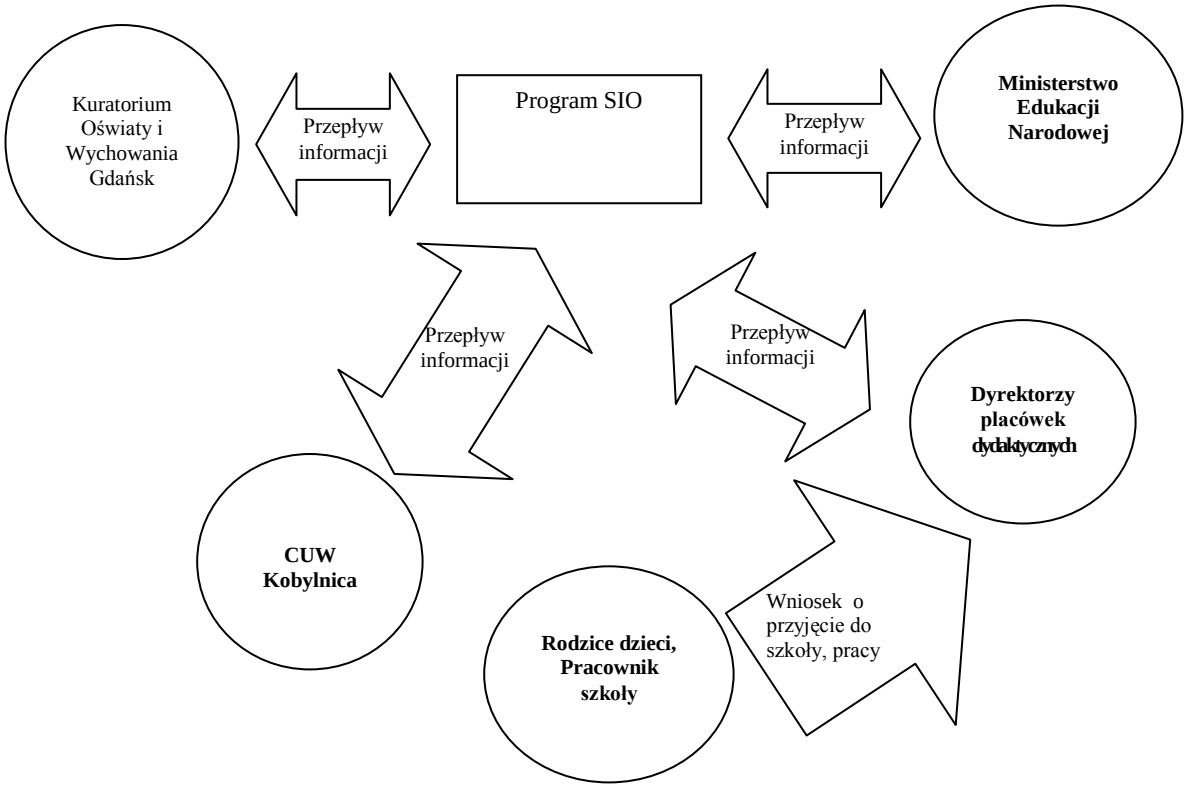
3. Samodzielne stanowisko ds. kadr: **Rejestr Kadry**



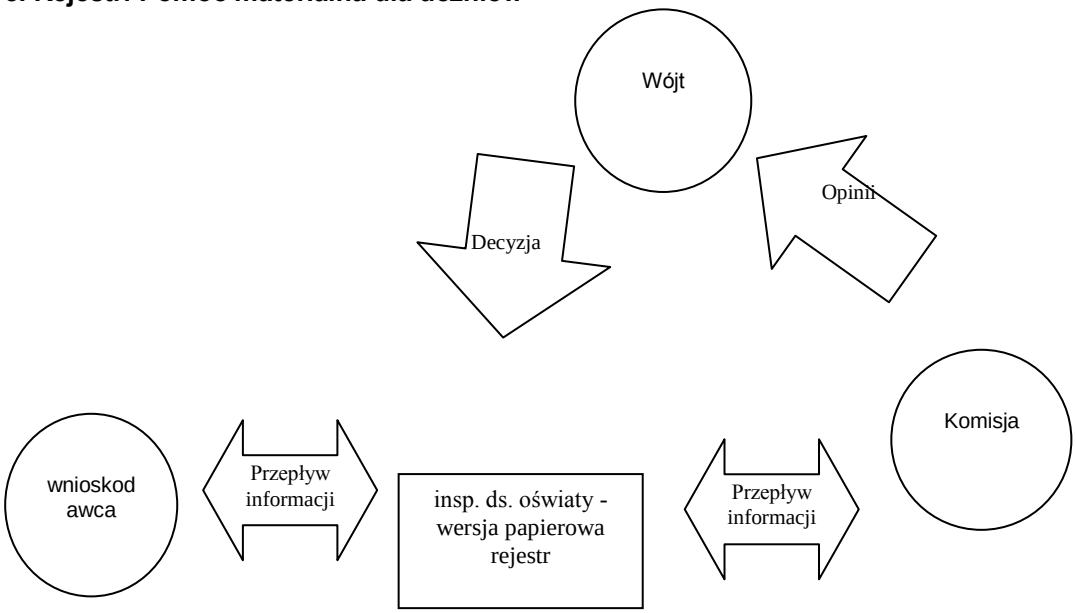
4. Samodzielne stanowisko ds. obsługi sekretariatu: **Książka korespondencji**



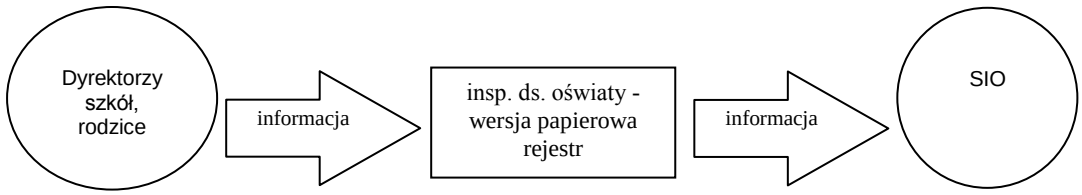
5. Centrum Usług Wspólnych w Kobylnicy: **Zbiór SIO.**



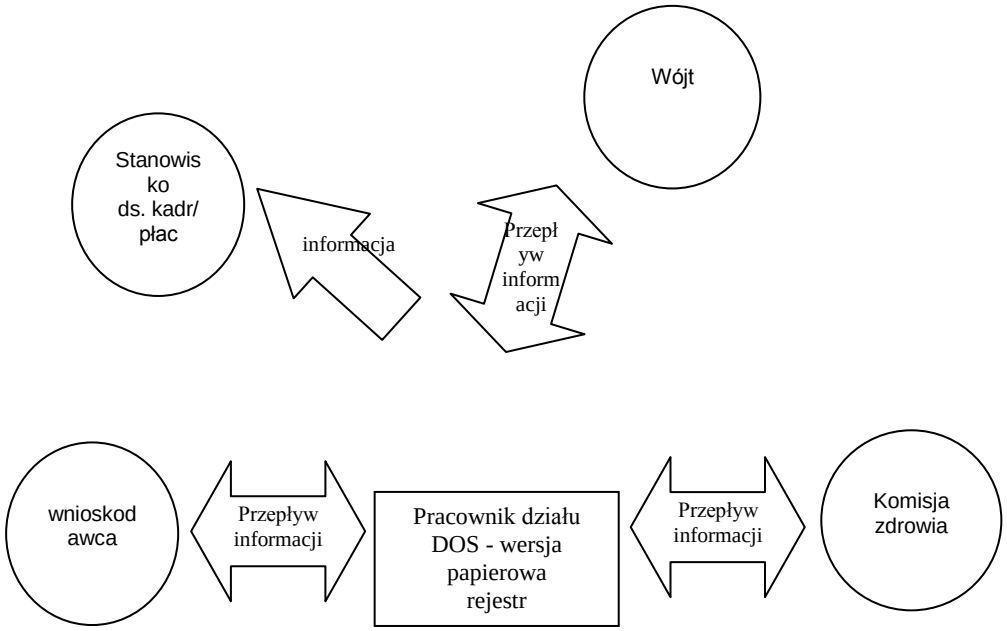
6. Rejestr: Pomoc materialna dla uczniów



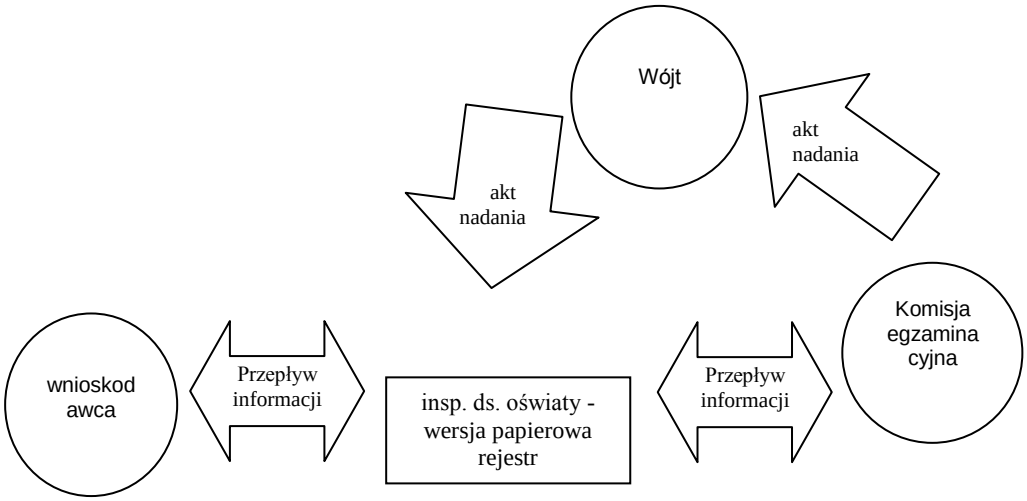
7. Rejestr: Obowiązek szkolny i nauki



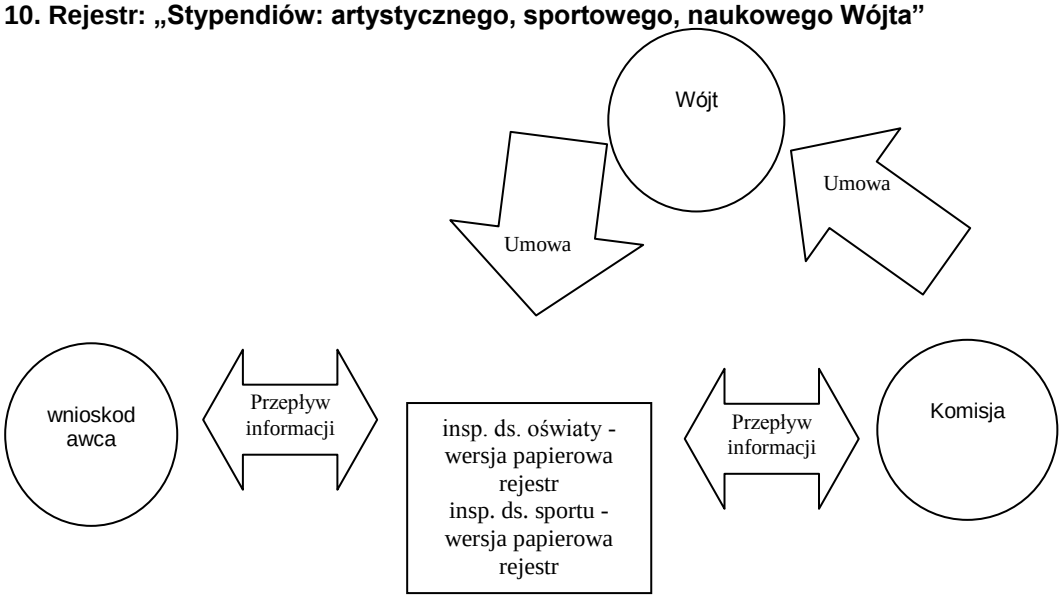
8. Rejestr: Pomoc zdrowotna dla nauczycieli



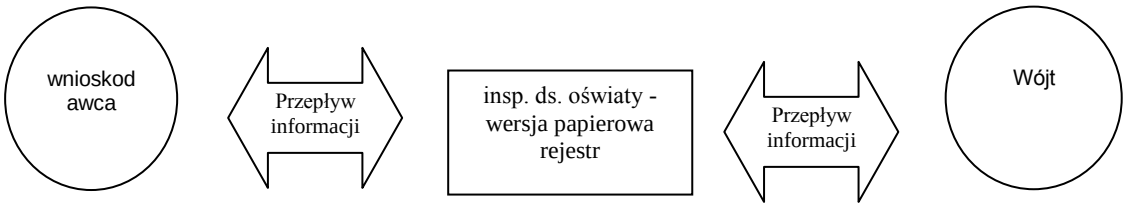
9. Rejestr: „Awansu zawodowego na nauczyciela mianowanego



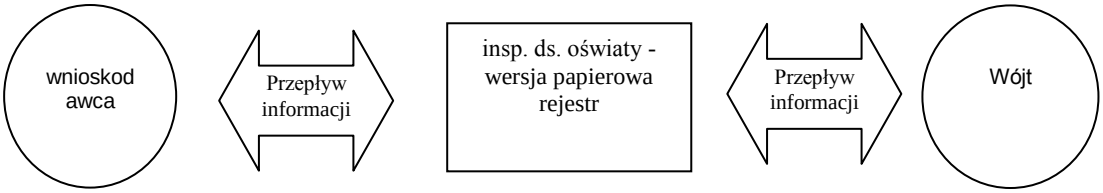
10. Rejestr: „Stypendiów: artystycznego, sportowego, naukowego Wójta”



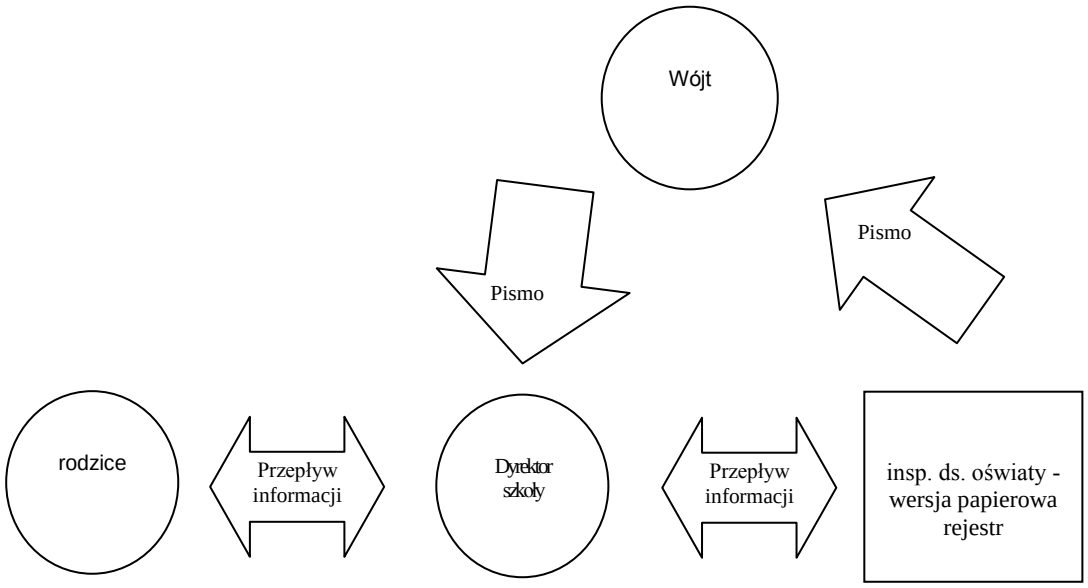
11. Rejestr: „Ewidencja szkół i placówek niepublicznych”



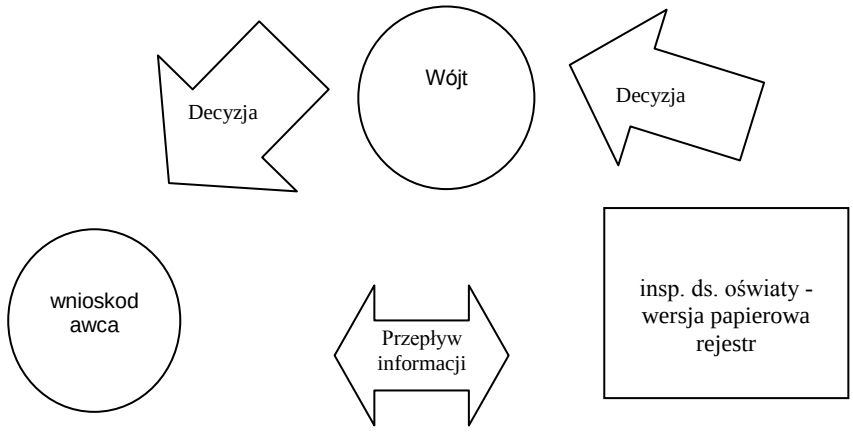
12. „Rejestr żłobków i klubów dziecięcych”



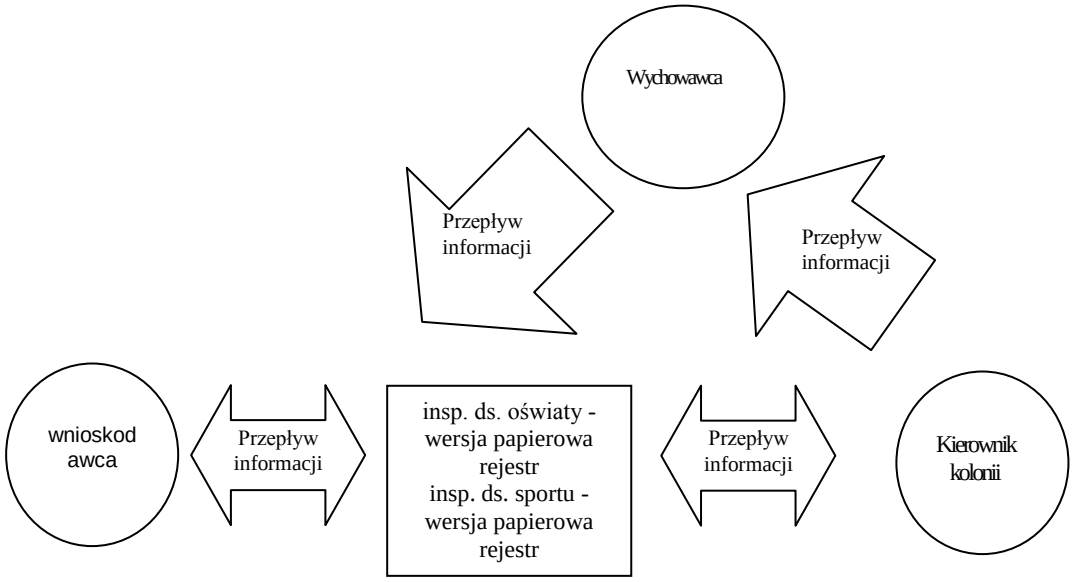
13. Rejestr: „ Przyznawania nauczania indywidualnego i rewalidacji”



14. Rejestr: „Dofinansowania kształcenia młodocianych pracowników”

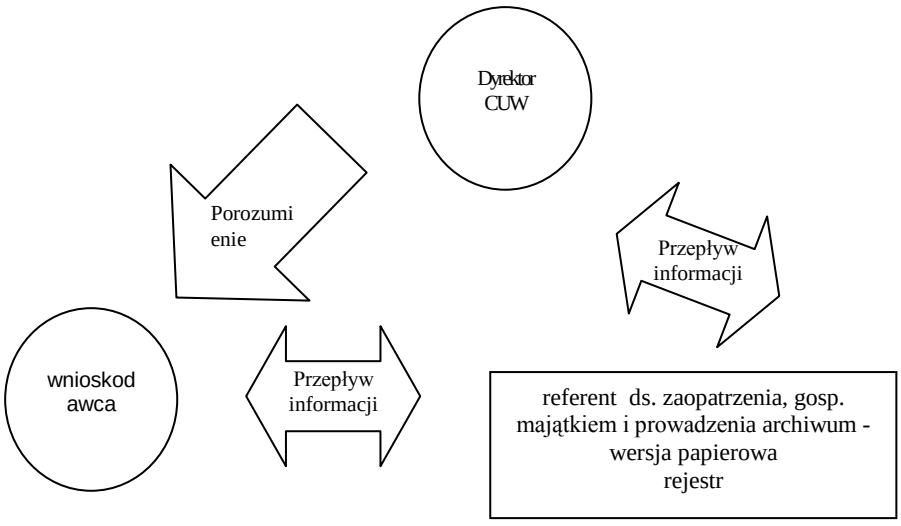


15. Rejestr: „**Zakwalifikowania dziecka – ucznia szkół z terenu gminy Kobylnica na kolonię”**

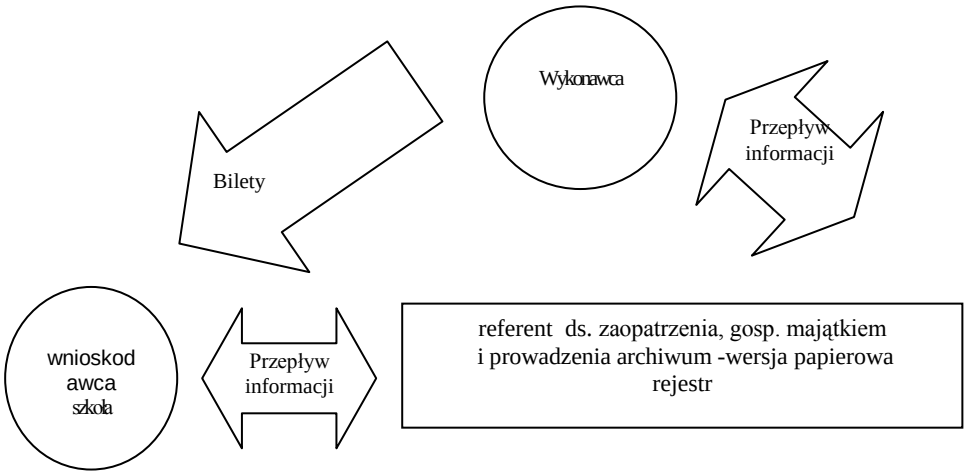


16 „Ewidencja dowozu uczniów do szkół”

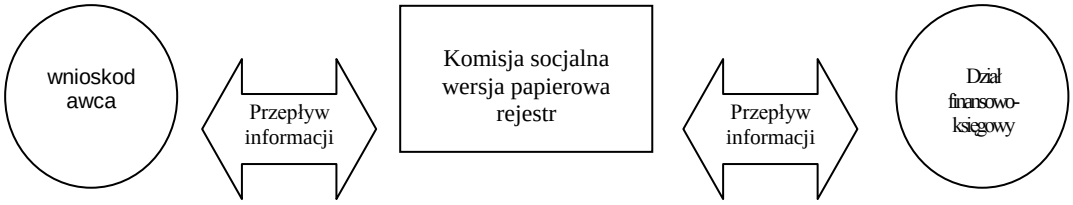
a)Porozumienia –zwrot kosztów dowozu dziecka do szkoły



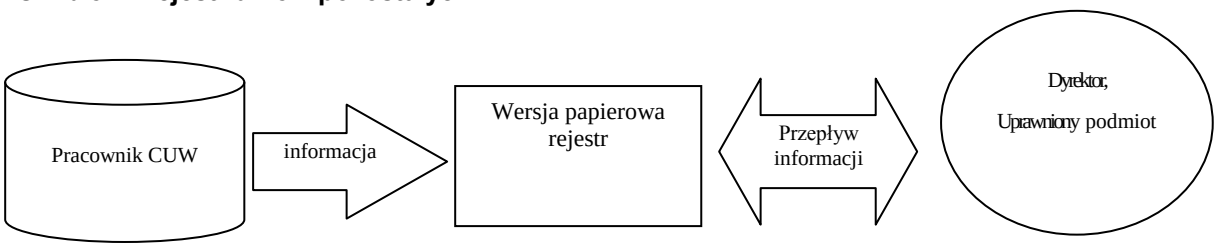
b) Zamówienie biletów miesięcznych dla uczniów i opiekunów



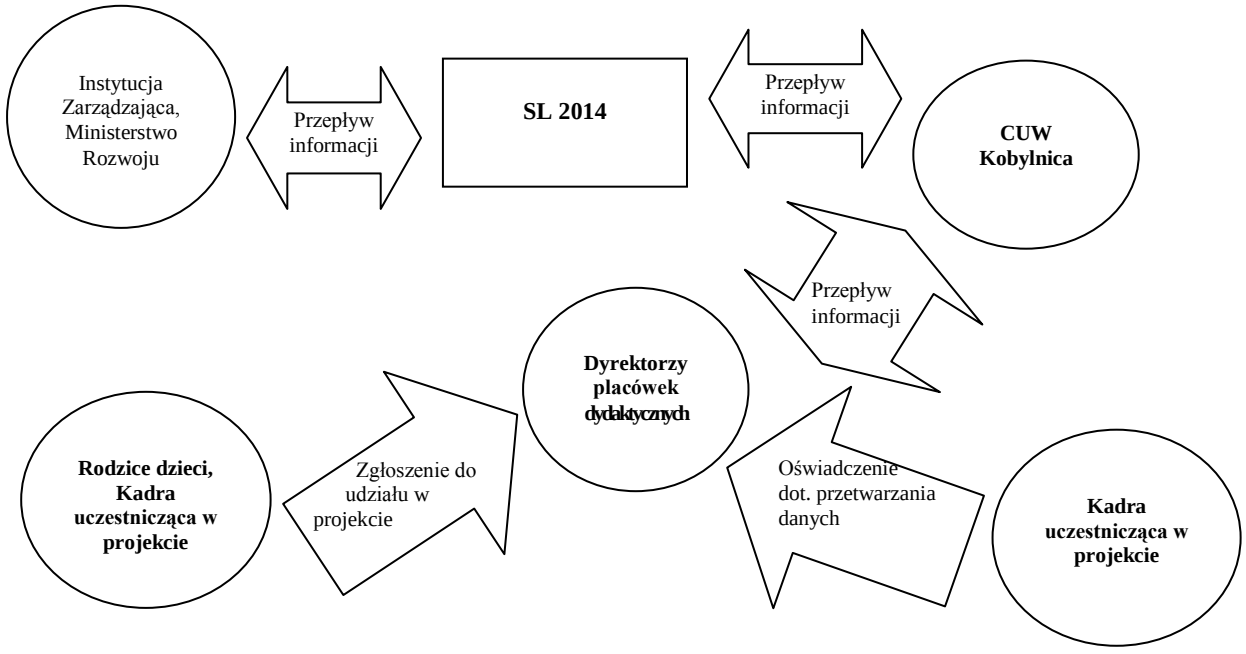
17. Rejestr: „Zakładowy Fundusz Świadczeń Socjalnych”



18. Zbiór: Rejestr umów pozostałych



19. Regionalny Program Operacyjny Województwa Pomorskiego na lata 2014-2020”, „Regionalny Program Operacyjny Województwa Pomorskiego na lata 2014-2020 – dane uczestników indywidualnych” oraz „Centralny system teleinformatyczny wspierający realizację programów operacyjnych



20. Wykaz programów stosowanych w Centrum do przetwarzania danych osobowych określa ***Załącznik C***

VIII. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych

§ 16

1. Zabezpieczenia organizacyjne
   1) sporządzono i wdrożono Politykę Bezpieczeństwa;
   2) wyznaczono ABI i ASI,
   3) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez Administratora danych bądź osobę przez niego upoważnioną;
   4) stworzono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych;
   5) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;
   6) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
   7) przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;
   8) przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych;
   9) dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonując takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści, aby po dokonaniu usunięcia danych niemożliwa była identyfikacja osób.
2. Zabezpieczenia techniczne
   1) stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową,
   2) komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkowania i cykliczne wymuszanie zmiany hasła,
   3) dostęp do systemu informatycznego służącego do przetwarzania danych osobowych, może uzyskać wyłącznie osoba (użytkownik) zarejestrowana w tym systemie przez administratora systemu na wniosek właściwej komórki organizacyjnej i decyzji Dyrektora lub działającego w jego imieniu upoważnionej osoby,
   4) dostęp do systemów operacyjnych serwerów i stacji roboczych powinien być chroniony przez nazwę użytkownika i hasło. Zespół ten tworzy jedną z głównych linii obrony przed intruzami. Dlatego należy uświadamiać użytkownikom rolę, jaką w systemie ochrony odgrywa dobrze wybrane „trudne" hasło o odpowiednio dobranym czasie życia. Jednocześnie należy wdrożyć mechanizmy systemowe kontrolujące składnię i czas życia haseł. System ma wbudowane mechanizmy ograniczające liczbę błędnych prób logowania oraz umożliwia wskazanie stacji roboczych, na których dany użytkownik może pracować. Zalecane jest ustawienie blokady konta użytkownika na ***3 próby logowania***.
   5) identyfikator użytkownika składa się z sześciu znaków z przedrostkiem **CUW** i dalej kolejny numer stacji przypisanej do określonego stanowiska pracy w CUW. Wprowadza się wykaz stacji roboczych, stanowiący ***Załącznik D,***
   6) hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz co najmniej dwie cyfry lub znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika, ani z jego imieniem lub nazwiskiem. Hasła zmienia się nie rzadziej niż ***co 30 dni***,
   7) ***użytkownikom systemu nie wolno udostępniać swojego identyfikatora i hasła innym osobom.***

3. Środki ochrony fizycznej:
   1) obszar, na którym przetwarzane są dane osobowe, poza godzinami pracy, chroniony jest alarmem,
   2) obszar, na którym przetwarzane są dane osobowe objęty jest całodobowym monitoringiem,
   3) urządzenia służące do przetwarzania danych osobowych umieszcza się w zamykanych pomieszczeniach,
   4) dostęp do pomieszczeń posiadają tylko osoby upoważnione, po odebraniu kluczy do pomieszczeń w sekretariacie i pokwitowanie ich odbioru w książce wydawania kluczy,

IX. Instrukcja postępowania w przypadku zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych

§ 17

1. Instrukcja definiuje katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Celem instrukcji jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.
2. Zagrożenia i incydenty zagrażające bezpieczeństwu danych maja postać uchybień i zagrożeń.
   1) Uchybienie – jest świadomym lub nieświadomym działania zmierzające do zagrożenia, wskutek których może dojść do utraty danych osobowych, kradzieży danych osobowych lub uszkodzeń nośników danych.
   2) Zagrożenie – to świadome lub nieświadome działania, wskutek których doszło do utraty danych osobowych lub uszkodzenia nośników danych.
3. Do ***uchybień i zagrożeń <u>nieświadomych</u> wewnętrznych i zewnętrznych*** należą działania pracowników Centrum lub osób nie będących pracownikami Centrum, w następstwie których może dojść lub doszło do zniszczenia danych, wycieku danych lub naruszenia ich poufności. W szczególności są to działania takie jak:
   1) niewłaściwe zabezpieczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe,
   2) niewłaściwe zabezpieczenie sprzętu komputerowego,
   3) dopuszczenie do przetwarzania danych przez osoby nieposiadające upoważnienia,
   4) pomyłki informatyków, ASI,
   5) kradzież danych,
   6) kradzież sprzętu informatycznego,
   7) działanie wirusów i innego szkodliwego oprogramowania oraz inne działania, wskutek których dojdzie do utraty danych osobowych lub uszkodzenia nośników danych.
4. Do ***uchybień i zagrożeń <u>umyślnych</u> wewnętrznych i zewnętrznych*** należą celowe działania pracowników Centrum, lub osób nie będących pracownikami Centrum w następstwie których może dojść lub doszło do zniszczenia danych, wycieku danych lub naruszenia ich poufności. W szczególności są to działania takie jak:
   1) celowe zniszczenie danych osobowych lub nośników danych,
   2) kradzież danych osobowych w wyniku kradzieży z włamaniem do obiektu lub systemu,,
   3) włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania
   4) dopuszczenie do przetwarzania danych przez osoby nieposiadające upoważnienia,
   5) kradzież danych,
   6) kradzież sprzętu informatycznego,
   7) działanie wirusów i innego szkodliwego oprogramowania oraz inne działania, wskutek których dojdzie do utraty danych osobowych lub uszkodzenia nośników danych.
5. Do ***uchybień i zagrożeń losowych należą sytuacje losowe***, w następstwie których może dojść lub doszło do zniszczenia danych, wycieku danych lub naruszenia ich poufności. W szczególności są to sytuacje takie jak:

1) klęski żywiołowe,
2) przerwa lub utrata zasilania,
3) awarie serwera,
4) pożar,
5) zalanie wodą.

6. Każdy pracownik w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować Administratora danych lub ABI o ujawnionych uchybieniach lub zagrożeniach.
7. W przypadku stwierdzenia wystąpienia zagrożenia, Administrator danych lub ABI prowadzi postępowanie wyjaśniające w toku, którego:
   1) ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,
   2) inicjuje ewentualne działania dyscyplinarne,
   3) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości,
   4) dokumentuje prowadzone postępowania, w tym sporządza protokół zagrożenia którego wzór określa ***Załącznik E***,
8. W przypadku stwierdzenia incydentu (naruszenia), Administratora danych lub ABI prowadzi postępowanie wyjaśniające w toku, którego:
   1) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,
   2) zabezpiecza ewentualne dowody,
   3) ustala osoby odpowiedzialne za naruszenie,
   4) podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody),
   5) inicjuje działania dyscyplinarne,
   6) wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości,
   7) dokumentuje prowadzone postępowania, w tym sporządza protokół uchybienia którego wzór określa ***Załącznik E 1***,
9. Wprowadza się Rejestr uchybień i zagrożeń oraz szczegółową instrukcję postępowania osób posiadających upoważnienia do przetwarzania danych w Centrum, którego zakres stosowania określony jest w ***Załączniku F***.

X. Zadania Administratora Bezpieczeństwa Informacji w Centrum

§ 18

Do najważniejszych obowiązków Administratora Danych lub Administratora Bezpieczeństwa Informacji należy:

1. Organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych;
2. Zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki;
3. Wydawanie i anulowanie upoważnień do przetwarzania danych osobowych;
4. Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
5. Prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych, prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
6. Nadzór nad bezpieczeństwem danych osobowych;
7. Kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
8. Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych,
9. Prowadzenie „Dziennika Uchybień i zagrożeń”, którego wzór określa ***Załącznik G***;
10. Opracowanie wspólnie z ASI sprawozdania rocznego zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych na podstawie dokumentu „Raport roczny”, którego wzór określa ***Załącznik H;***

11. Omówienie wspólnie z ASI na zebraniu, zwołanym przez ADO co najmniej raz w roku, procedur obowiązujących w zakresie zabezpieczenia danych oraz ewentualnych uchybieniach i zagrożeniach stwierdzonych w Centrum w okresie sprawozdawczym.

§ 19

Administrator Bezpieczeństwa Informacji ma prawo:

1. Wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych w Centrum;
2. Wstępu do pomieszczeń w których zlokalizowane są zbiory danych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą;
3. Żądania złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego;
4. Żądania okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli;
5. Żądania udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych.

XI. Zadania Administratora Systemu Informatycznego

§ 20

1. Administrator Systemu Informatycznego odpowiedzialny jest za:
   1) Bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych.
   2) Optymalizację wydajności systemu informatycznego, baz danych, instalacje i konfiguracje sprzętu sieciowego i serwerowego.
   3) Instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego.
   4) Konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem.
   5) Nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych.
   6) Współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych.
   7) Zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego.
   8) Zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie.
   9) Przeciwdziałanie próbom naruszenia bezpieczeństwa informacji.
   10) Przyznawanie na wniosek Administratora danych lub Administratora Bezpieczeństwa Informacji ściśle określonych praw dostępu do informacji w danym systemie.
   11) Wnioskowanie do Administratora danych lub Administratora Bezpieczeństwa Informacji w sprawie zmian lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń.
   12) Zarządzanie licencjami, procedurami ich dotyczącymi.
   13) Prowadzenie profilaktyki antywirusowej.
2. Praca Administratora Systemu Informatycznego jest nadzorowana pod względem przestrzegania ustawy o ochronie danych osobowych, Rozporządzenia 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 oraz Polityki Bezpieczeństwa przez Administratora danych lub Administratora Bezpieczeństwa Informacji.

XII. Sprawozdanie roczne stanu systemu ochrony danych osobowych

§ 21

1. Corocznie do końca czerwca, ABI wspólnie z ASI przygotowuje sprawozdanie roczne stanu funkcjonowania systemu ochrony danych osobowych,
2. W spotkaniu sprawozdawczym uczestniczą: Administrator danych oraz ABI i ASI. Na wniosek co najmniej jednego z uczestników w spotkaniu mogą wziąć udział:, kierownicy działów Centrum i jednostek oświatowych.
3. Sprawozdanie przygotowywane jest w formie pisemnej.

XIII. Szkolenia użytkowników

§ 22

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
2. Wniosek o dopuszczenie pracownika do pracy w zbiorach danych zobowiązany jest na piśmie złożyć bezpośredni przełożony przed dopuszczeniem do pracy. Wzór wniosku określony został w ***Załączniku nr 6*** do Zarządzenia Dyrektora w sprawie polityki bezpieczeństwa.
3. Za przeprowadzenie szkolenia odpowiada Administrator danych wspólnie ABI.
4. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u Administratora danych, a także o zobowiązaniu się do ich przestrzegania.
5. Szkolenie zostaje zakończone podpisaniem przez słuchacza oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych.
6. Dokument ten jest przechowywany w aktach osobowych użytkowników i stanowi podstawę do podejmowania działań w celu nadania im uprawnień do korzystania z systemu informatycznego przetwarzającego dane osobowe.

XIV. Postanowienia końcowe

§ 23

1. Polityka jest dokumentem wewnętrznym i nie może być udostępniania osobom postronnym w żadnej formie.
2. Administrator Bezpieczeństwa Informacji ma obowiązek zapoznać z treścią Polityki każdego użytkownika.
3. Wszystkie regulacje dotyczące systemów informatycznych, określone w Polityce dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
4. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce.
5. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
6. Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z ustawą oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
7. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy oraz rozporządzenia.

Załącznik A

Wykaz pomieszczeń budynku przy ul. Wodnej 20/2 w Kobylnicy tworzących w Centrum Usług Wspólnych w Kobylnicy obszar, w którym przetwarzane są dane osobowe∗

1. Dyrektor – pomieszczenie nr 10b
2. Główny Księgowy – pomieszczenie nr 10a
3. Dział Finansowo- Księgowy – pomieszczenie nr 9
4. Dział Oświaty i Sportu – pomieszczenie nr 12
5. Stanowisko ds. obsługi sekretariatu – pomieszczenie nr 10
6. Stanowisko ds. kadr – pomieszczenie nr 11
7. Stanowisko ds. zaopatrzenia, gosp. majątkiem i prowadzenia archiwum – pomieszczenie nr 13

∗ *wykaz jest zbiorem otwartym podlegającym zmianom*

Załącznik B

Wykaz zbiorów*)
danych osobowych gromadzonych i przetwarzanych w Centrum Usług Wspólnych w Kobylnicy

Lp.	Nazwa zbioru	Termin wprowadzenia
1	a) Rejestr umów najmu	w prowadzeniu
	b) Rejestr umów zleceń	w prowadzeniu
2	Rejestr skarg i wniosków	w prowadzeniu
3	Kadry	w prowadzeniu
4	Książka korespondencji	w prowadzeniu
5	Zbiór danych dotyczących nauczycieli, wychowawców i innych pracowników pedagogicznych SIO	w prowadzeniu
6	Pomoc materialna dla uczniów	w prowadzeniu
7	Obowiązek szkolny i nauki	w prowadzeniu
8	Pomoc zdrowotna dla nauczycieli	w prowadzeniu
9	Awans zawodowy na nauczyciela mianowanego	w prowadzeniu
10	Stypendia: artystyczne, sportowe, naukowe Wójta	w prowadzeniu
11	Ewidencja szkół o placówek niepublicznych	w prowadzeniu
12	Rejestr żłobków i klubów dziecięcych	w prowadzeniu
13	Przyznawanie nauczania indywidualnego i rewalidacji	w prowadzeniu
14	Dofinansowanie kształcenia młodocianych i pracowników	w prowadzeniu
15	Zakwalifikowanie dziecka – ucznia szkół z terenu gminy Kobylnica na kolonię	w prowadzeniu
16	a) porozumienia – zwrot kosztów dowozu dziecka do szkoły	w prowadzeniu
	b) zamówienia biletów miesięcznych dla uczniów i opiekunów	w prowadzeniu
17	Zakładowy Fundusz Świadczeń Socjalnych	w prowadzeniu
18	Rejestr umów pozostałych	w prowadzeniu
19a	Regionalny Program Operacyjny Województwa Pomorskiego na lata 2014-2020,	w prowadzeniu
19b	Regionalny Program Operacyjny Województwa Pomorskiego na lata 2014-2020 – dane uczestników indywidualnych	w prowadzeniu
19c	Centralny system teleinformatyczny wspierający realizację programów operacyjnych	w prowadzeniu

***) zbiór jest zbiorem otwartym podlegającym modyfikacji**

Załącznik C

Wykaz programów stosowanych w Centrum Usług Wspólnych w Kobylnicy do przetwarzania danych osobowych∗

1. **Stanowisko ds. kadr**
   PROGMAN – Kadry
2. **Dział finansowo – księgowy**
   Wolters Kluwer – Finanse i księgowość:
   Wolters Kluwer – Płace
   Wolters Kluwer – Kasa
   Wolters Kluwer – Zlecone
   Wolters Kluwer – Przelewy
   PROKOM SOFWARE SA – Płatnik
   TENSOFT - Faktury, e - VAT
3. **Dział Oświaty i Sportu**
   Sputnik Sofware – Pomoc materialna dla uczniów
   Wolters Kluwer – Obowiązek szkolny i nauki
   SIO – **„System Informacji Oświatowej”** program rządowy dostarczony i administrowany przez Ministerstwo Edukacji Narodowej
4. **Stanowisko ds. obsługi sekretariatu**
   SIO – **„System Informacji Oświatowej”** program rządowy dostarczony i administrowany przez Ministerstwo Edukacji Narodowej
5. **Dyrektor, Dział Oświaty i Sportu**
   SL2014 – aplikację główną centralnego systemu teleinformatycznego, o którym mowa w rozdziale 16 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 r. poz. 217), dostępną pod adresem internetowym: https://sl2014.gov.pl;

∗ *wykaz jest zbiorem otwartym podlegającym zmianom*

Załącznik D

Wykaz nazw użytkowników stacji roboczych w Centrum Usług Wspólnych w Kobylnicy∗

Lp.	Nazwa stacji roboczej	Imię i nazwisko stanowisko	Potwierdzenie odbioru hasła
1	**3**	**2**	**4**
1.	CUW001		
2.			
999.	CUW999		

∗ *wykaz jest zbiorem otwartym podlegającym zmianom*

Załącznik E

Protokół Zagrożenia

Data i godzina wystąpienia zagrożenia

.....

Kod zagrożenia

.....

Opis zagrożenia

.....

.....

Przyczyny powstania zagrożenia

.....

.....

Zaistniałe skutki zagrożenia

.....

.....

Podjęte działania naprawczo-zapobiegawcze

.....

.....

Administrator Bezpieczeństwa Informacji	**Administrator Danych Osobowych**
……	……..
Nazwa i adres podmiotu	Miejscowość i data

Załącznik E 1

Protokół Uchybienia

Data i godzina wystąpienia uchybienia.....

Kod uchybienia

.....

Opis uchybienia

.....

.....

Przyczyny powstania uchybienia

.....

.....

Zaistniałe skutki uchybienia

.....

.....

Podjęte działania naprawczo-zapobiegawcze

.....

.....

.....

Administrator Bezpieczeństwa Informacji **Administrator Danych Osobowych**

…… ……..

Nazwa i adres podmiotu Miejscowość i data

Załącznik F

Rejestr Uchybień i Zagrożeń
wraz z szczegółową instrukcję postępowania dla osób posiadających upoważnienie do przetwarzania danych osobowych w Centrum Usług Wspólnych w Kobylnicy

Kod uchybienia lub zagrożenia	**Uchybienia i zagrożenia nie świadome wewnętrzne i zewnętrzne**	**Postępowanie w przypadku uchybienia lub zagrożenia**
1	*2*	*3*
1	Pomieszczenie w którym przechowywane są dane osobowe pozostaje bez nadzoru.	Należy zabezpieczyć dane osobowe oraz powiadomić ABI. ABI sporządza protokół uchybienia.
2	Komputer nie jest zabezpieczony hasłem.	Należy zabezpieczyć dane osobowe oraz powiadomić ABI. ABI sporządza protokół uchybienia.
3	Dostęp do danych osobowych mają osoby nie posiadające upoważnienia.	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić ABI. ABI sporządza protokół uchybienia.
4	Nieuprawniony dostęp do otwartych aplikacji w systemie informatycznym.	Należy powiadomić ABI, który przy pomocy ASI powinien sprawdzić system uwierzytelnienia oraz sprawdzić czy nie doszło do kradzieży lub zniszczenia danych. ABI sporządza protokół uchybienia.
5	Próba kradzieży danych osobowych poprzez zewnętrzny nośnik danych.	Należy nie dopuścić do kradzieży danych i powiadomić ABI. ABI powinien zabezpieczyć nośnik danych i powiadomić ADO. ABI sporządza protokół zagrożenia.
6	Próba kradzieży danych osobowych w firmie papierowej.	Należy nie dopuścić do kradzieży danych i powiadomić ABI. ABI powinien zabezpieczyć dane i powiadomić ADO. ABI sporządza protokół zagrożenia.
7	Nieuprawniony dostęp do danych osobowych w formie papierowej.	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić ABI. ABI sporządza protokół uchybienia.
8	Dane osobowe przechowywane są w nie zabezpieczonym pomieszczeniu.	Należy powiadomić ABI. ABI powinien zabezpieczyć pomieszczenie. ABI sporządza protokół uchybienia.
9	Próba włamania do pomieszczenia/budynku.	Należy zabezpieczyć dowody i powiadomić ABI. ABI sprawdza stan uszkodzeń, zabezpiecza dowody i wzywa policję. ABI sporządza protokół uchybienia.
10	Działanie zewnętrznych aplikacji, wirusów, złośliwego oprogramowania.	Należy zrobić audyt systemów zabezpieczeń a w szczególności systemów antywirusowych, firewall. ABI powinni ocenić, czy nie doszło do utraty danych osobowych i w zależności od tego sporządzić protokół uchybienia lub zagrożenia.
11	Brak aktywnego oprogramowania antywirusowego.	Należy powiadomić ABI. ABI powinien zaktualizować lub nabyć oprogramowanie antywirusowe. ABI sporządza protokół uchybienia.
12	Zniszczenie lub modyfikacja danych osobowych w formie papierowej.	Należy zabezpieczyć dowody i powiadomić ABI. ABI sprawdza stan uszkodzeń, zabezpiecza dowody i powiadamia ADO. ABI sporządza protokół zagrożenia.
13	Zniszczenie lub modyfikacja danych osobowych w systemie informatycznym.	Należy zabezpieczyć dowody i powiadomić ABI. ABI sprawdza stan uszkodzeń, zabezpiecza dowody i powiadamia ADO. ABI sporządza protokół zagrożenia.
14	Uszkodzenie komputerów, nośników danych.	Należy powiadomić ABI. ABI powinien ocenić w wyniku czego doszło do zniszczenia i przywrócić dane z kopii zapasowej. ABI powiadamia ADO i sporządza protokół zagrożenia.
15	Próba nieuprawnionej interwencji przy sprzęcie komputerowym.	Należy uniemożliwić dostęp osób do sprzętu komputerowego oraz powiadomić ABI. ABI sporządza protokół uchybienia.
16	Zdarzenia losowe.	Należy oszacować powstałe straty i sporządzić protokół zagrożenia lub uchybienia.

Załącznik G

Dziennik Uchybień i Zagrożeń

Kod	**Data i godzina zdarzenia**	**Rodzaj zdarzenia *(uchybienie/zagrożenie)***	**Opis zdarzenia**	**Skutki zdarzenia**	**Działania naprawcze**	**Podpis ABI**

Nazwa i adres podmiotu

….....

Miejscowość i data

…….……..

Załącznik H

„Raport roczny”

Nazwa i adres podmiotu ….....	Miejscowość i data ….....

Zagadnienia omawiane na zebraniu	**Uwagi/wnioski**
Podsumowanie realizacji wytycznych z poprzedniego „Sprawozdania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych”	
Omówienie zmian procedur w systemie oraz zmian w systemie informatycznym	
Omówienie Dziennika Uchybień i Zagrożeń	
Wnioski oraz zadania do realizacji	

Podpis ABI	Podpis ADO

Załącznik Nr 2
do Zarządzenia Nr 23/2017
Dyrektora Centrum
Usług Wspólnych w Kobylnicy
z dnia 10.05.2017 r.

Instrukcja ochrony danych osobowych

Rozdział 1
Postanowienia ogólne

§ 1

Podstawę prawną do niniejszej instrukcji stanowią:

1. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2015 r., poz. 2135 z późn. zm.), zwana dalej „ustawą",
2. 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. Nr 100, poz. 1024), zwane dalej „rozporządzeniem".

§ 2

Ilekroć w instrukcji jest mowa o:

1. **Danych osobowych** – uważa się za nie 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 albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne,
2. **Zbiorze danych** - rozumie się przez to każdy posiadający uporządkowaną strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie,
3. **Przetwarzaniu danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
4. **Usuwaniu danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
5. **Administratorze danych** - rozumie się przez to Dyrektora Centrum lub inną upoważnioną przez niego osobę,
6. **Zgodzie osoby, której dane dotyczą** - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści,
7. **Systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
8. **Zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
9. **Administratorze bezpieczeństwa informacji** - rozumie się przez to - pracownika zatrudnionego na stanowisku ds. zaopatrzenia, gospodarowania majątkiem trwałym i prowadzenia archiwum, zwany w dalszej części **ABI**
10. **Administratorze systemów informatycznych –** rozumie się przez to – specjalistę ds. obsługi i zabezpieczenia informatycznej bazy danych, zwany w dalszej części **ASI**

§ 3

Instrukcja określa:

1. Zasady postępowania przy przetwarzaniu danych osobowych,
2. Prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych,
3. Zabezpieczenie zbiorów danych osobowych,
4. Wzór zgody osoby na przetwarzanie jej danych osobowych stanowi ***Załącznik A*** do niniejszej instrukcji,

5. Wzór o zachowaniu w tajemnicy danych osobowych oraz o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych, który stanowi ***Załącznik B*** do niniejszej instrukcji.

§ 4

1. Dane osobowe mogą być przetwarzane:
   1) w systemach informatycznych (mogą być nimi również pojedyncze komputery),
   2) w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych.
2. Przetwarzanie danych osobowych jest dopuszczalne tylko wtedy, gdy spełniony jest, co najmniej jeden z wymienionych poniżej warunków:
   1) osoba, której dane dotyczą, wyrazi zgodę na przetwarzanie danych (chyba, że chodzi o usunięcie dotyczących jej danych), zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści, lecz musi wyraźnie dotyczyć przetwarzania danych,
   2) na przetwarzanie danych zezwalają przepisy prawa,
   3) przetwarzanie danych jest konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia koniecznych działań przed zawarciem umowy,
   4) przetwarzanie danych jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,
   5) przetwarzanie danych jest niezbędne do wypełnienia prawnie usprawiedliwionych celów administratorów danych lub osób trzecich, którym są przekazywane te dane, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą.
3. Jeżeli przetwarzanie danych jest niezbędne dla żywotnych interesów osoby, której dane dotyczą, a spełnienie warunków, o których mowa w ust. 2 pkt 1 jest niemożliwe, administrator danych może przetwarzać dane bez zgody tej osoby, do czasu gdy uzyskanie tej zgody będzie możliwe.
4. Zabrania się przetwarzania danych ujawniających:
   1) pochodzenie rasowe lub etniczne,
   2) poglądy polityczne,
   3) przekonania religijne lub filozoficzne,
   4) przynależność wyznaniową, partyjną lub związkową,
   5) jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym.

Rozdział 2
Zabezpieczenie danych osobowych

§ 5

1. **ABI i ASI są zobowiązani** do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy, zmianą lub utratą, uszkodzeniem lub zniszczeniem.
2. Szczegółowe wymogi w zakresie zastosowania środków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych zawarte zostały w:
   1) Instrukcji zarządzania systemem teleinformatycznym służącym do przetwarzania danych osobowych w Centrum,
   2) Zasadach udzielania pomocy użytkownikom sprzętu komputerowego w Centrum.

§ 6

Każda osoba przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych zostaje zaznajomiona z przepisami dotyczącymi ochrony danych osobowych, a szczególnie z przepisami karnymi zawartymi w rozdziale 8 ustawy.

§ 7

1. Zbiory danych osobowych podlegają ochronie i zabezpieczeniu:
   1) Po zakończeniu pracy dokumenty lub nośniki zawierające dane osobowe winny być zabezpieczone w szafach zamykanych na klucz oraz pomieszczeniach, w sposób uniemożliwiający zapoznanie się z ich treścią osobom trzecim,

2) Pracownicy zatrudnieni przy ich obsłudze nie mogą zezwalać na użytkowanie komputera osobom nieupoważnionym,
3) Przebywanie w pomieszczeniach osób nieupoważnionych jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych,
4) Pomieszczenia powinny być zamykane na czas nieobecności w nich osób zatrudnionych.

2. Monitory komputerów powinny być tak ustawione, aby uniemożliwić osobom postronnym wgląd do danych osobowych.
3. Dokumenty, wydruki itp., które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

§ 8

1. Każdy pracownik posiadający dostęp do danych osobowych składa oświadczenie o zachowaniu w tajemnicy danych osobowych oraz o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych.
2. Zobowiązuje się jest pracownik zatrudniony na stanowisku ds. zaopatrzenia, gospodarowania majątkiem trwałym i prowadzenia archiwum. do pobierania oświadczeń, o których mowa w ust. 1 od nowo zatrudnionych pracowników.
3. Zakresy czynności osób zatrudnionych przy przetwarzaniu danych osobowych, w stopniu odpowiednim do zadań, powinny uwzględniać obowiązki z zakresu odpowiedzialności za bezpieczeństwo danych osobowych.
4. Oświadczenia, o których mowa w ust. 1 sporządza się w dwóch egzemplarzach, z których po jednym egzemplarzu otrzymują:
   1) Stanowisko ds. kadr,
   2) Osoba składająca oświadczenie.

§ 9

1. Oświadczenia, o których mowa w § 8 ust. 1 składają radni Rady Gminy Kobylnica, jeżeli mają oni dostęp do danych osobowych przetwarzanych w Centrum.
2. Niezachowanie tajemnicy dotyczącej danych osobowych skutkuje konsekwencjami przewidzianymi w ustawie.

§ 10

1. Oświadczenia, o których mowa w § 8 ust. 1 składają stażyści i praktykanci, jeżeli w trakcie wykonywania obowiązków mają oni dostęp do danych osobowych.
2. Niezachowanie tajemnicy dotyczącej danych osobowych skutkuje możliwością natychmiastowego rozwiązania umowy o odbycie stażu i praktyki oraz konsekwencjami przewidzianymi w ustawie.

§ 11

Osoby zatrudnione przy przetwarzaniu danych osobowych, mające do nich dostęp, obowiązane są do zachowania ich w tajemnicy zarówno w czasie zatrudnienia, jak też po jego ustaniu.

§ 12

1. Przetwarzanie danych osobowych może być realizowane jedynie w pomieszczeniach wymienionych w Polityce bezpieczeństwa i zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Centrum.
2. Przetwarzanie danych osobowych dopuszczalne jest poza obszarem określonym w ust. 1 tylko w sytuacjach wynikających ze specyfiki realizowanych obowiązków służbowych i musi być określone w upoważnieniu do przetwarzania danych osobowych.

§ 13

1. Dane osobowe mogą być przetwarzane przez uprawnioną osobę w zakresie określonym w upoważnieniu do przetwarzania danych osobowych.
2. Upoważnienie, którym mowa w ust. 1 jest wydawane przez administratora danych na wniosek kierownika komórki organizacyjnej.
3. Wydane upoważnienia podlegają rejestracji w Rejestrze Upoważnień do Przetwarzania Danych Osobowych, który prowadzi pracownik zatrudniony na stanowisku ds. zaopatrzenia, gospodarowania majątkiem trwałym i prowadzenia archiwum.

Rozdział 3
Prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych

§ 15

1. W przypadku zbierania danych osobowych, od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę:
   1) o istnieniu zbioru jej danych osobowych,
   2) o adresie swojej siedziby i pełnej nazwie,
   3) o celu zbierania danych, a w szczególności o znanych mu lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
   4) o prawie wglądu do swoich danych oraz ich poprawiania,
   5) o dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.
2. Obowiązek, o którym mowa w ust. 1 nie istnieje, jeżeli:
   ustawa zezwala na przetwarzanie danych bez ujawnienia faktycznego celu ich zbierania, osoba, której dane dotyczą, posiada informacje, o których mowa w ust. 1.

§ 16

1. W przypadku uzyskania danych osobowych nie od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę bezpośrednio po utrwaleniu zebranych danych:
   1) adresie swojej siedziby i pełnej nazwie,
   2) o celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych,
   3) źródle, z którego uzyskano dane,
   4) prawie wglądu do swoich danych oraz ich poprawiania,
   5) prawie żądania zaprzestania przetwarzania danych oraz o prawie sprzeciwu wobec przetwarzania danych.
2. Obowiązek, o którym mowa w ust. 1 nie istnieje, jeżeli:
   1) przepis prawa przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą,
   2) dane przewidziane do zebrania są ogólnie dostępne,
   3) dane te są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badania opinii publicznej, ich przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą, a poinformowanie osób wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu badania,
   4) administrator danych nie przetwarza dalej zebranych danych po ich jednorazowym wykorzystaniu,
   5) dane są przetwarzane przez administratora danych na podstawie przepisów prawa,
   6) osoba, której dane dotyczą posiada informacje, o których mowa w ust. 1.
3. Zobowiązuje się kierowników komórek organizacyjnych do prowadzenia ewidencji podmiotów, którym udostępniono dane osobowe z zakresu działania komórki organizacyjnej.

§ 17

1. Na administratorze danych i kierowniku komórki organizacyjnej ciąży obowiązek ochrony integralności i poprawności przetwarzanych informacji, szczególnie jest on obowiązany:
   1) przetwarzać je zgodnie z prawem,
   2) zbierać dane dla oznaczonych, zgodnych z prawem celów i nie poddawać dalszemu przetwarzaniu niezgodnemu z tymi celami,
   3) gromadzić dane merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
   4) przechowywać je w postaci umożliwiającej identyfikację osób, których dotyczą nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.
2. Przetwarzanie danych w celach innych niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą oraz następuje w celach badań

naukowych, dydaktycznych, historycznych lub statystycznych, z zachowaniem przepisów art. 23 i 25 ustawy o ochronie danych osobowych.

3. Niedopuszczalne jest ostateczne rozstrzygnięcie indywidualnej sprawy osoby, której dane dotyczą, jeżeli jego treść jest wyłącznie wynikiem operacji na danych osobowych, prowadzonych w systemie informatycznym Nie dotyczy to sytuacji, gdy rozstrzygnięcie zostało podjęte podczas zawierania lub wykonywania umowy i uwzględnia wniosek osoby, której dane dotyczą.

§ 18

1. Administrator danych przetwarzający dane w zbiorach, ma obowiązek udzielania informacji na wniosek osoby, której dane przetwarza i przestrzegania jej praw wynikających z ustawy, takich jak:
   1) prawo do informacji o:
      a) fakcie przetwarzania danych jej dotyczących,
      b) pełnym adresie siedziby i pełnej nazwie administratora danych,
      c) celu, zakresie i sposobie przetwarzania danych,
      d) dacie, od której dane zostały włączone do zbioru,
      e) treści danych,
      f) sposobie udostępniania danych oraz o odbiorcach lub kategorii odbiorców danych,
      g) źródle, z którego pochodzą dane jej dotyczące, chyba że administrator danych jest zobowiązany do zachowania w tym zakresie tajemnicy państwowej, zawodowej lub służbowej,
   2) prawo żądania uzupełnienia, uaktualnienia i sprostowania danych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane,
   3) prawo wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na szczególną sytuację, prawo to nie przysługuje, gdy administrator danych posiada zgodę osoby na wykorzystywanie danych, upoważnia go do tego przepis prawa lub gdy przetwarza dane w celu wykonania umowy,
   4) prawo wniesienia sprzeciwu wobec przetwarzania jej danych w celach marketingowych lub wobec przekazania jej danych osobowych innemu administratorowi danych,
   5) prawo wniesienia do administratora danych żądania ponownego, indywidualnego rozpatrzenia sprawy rozstrzygniętej z naruszeniem art. 26a ust. 1 ustawy.
2. W przypadku wniesienia żądania, o którym mowa w ust. 1 pkt. 5 administrator danych bez zbędnej zwłoki rozpatruje sprawę albo przekazuje ją wraz z uzasadnieniem swojego stanowiska Generalnemu Inspektorowi Ochrony Danych Osobowych, który wydaje stosowną decyzję.

§ 19

1. Na wniosek osoby, której dane dotyczą administrator danych jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach, a zwłaszcza wskazać w formie zrozumiałej odnośnie danych osobowych jej dotyczących:
   1) jakie dane osobowe zawiera zbiór,
   2) w jaki sposób zebrano dane,
   3) w jakim celu i zakresie dane są przetwarzane,
   4) w jakim zakresie oraz komu dane zostały udostępnione.
2. Informacji, o których mowa w ust. 1 udziela się na piśmie.

§ 20

Administrator danych odmawia udostępnienia danych podmiotom i osobom, które nie są uprawnione do ich otrzymania na mocy przepisów prawa, jeżeli spowodowałoby to:

1) ujawnienie wiadomości stanowiącej tajemnicę państwową,
2) zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi, mienia lub bezpieczeństwa i porządku publicznego,
3) zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa,
4) istotne naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.

§ 21

1. Administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi Danych Osobowych.
2. Administrator danych zwolniony jest z obowiązku, o którym mowa w ust.1 w przypadkach określonych w art. 43 ust. 1 i 1a ustawy o ochronie danych osobowych.
3. Zobowiązuje się kierowników komórek organizacyjnych do zgłaszania ABI i ASI wszelkich zmian związanych z aktualizacją zbiorów danych osobowych podlegających rejestracji oraz w przypadku zmian organizacyjno-etatowych przy pracy na zbiorach w formie wniosku.
4. Zmiany, o których mowa w ust. 3 winny być zgłoszone Administratorowi danych w formie pisemnej, celem dokonania zmian w prowadzonych w Centrum Rejestrach i zawiadomieniu Generalnego Inspektora Ochrony Danych Osobowych o zmianach w zbiorze.
5. Wzór wniosku o którym mowa w ust. 4 stanowi ***Załącznik C***.

Rozdział 4
Odpowiedzialność za naruszenie przepisów ustawy o ochronie danych osobowych

§ 22

Zasady odpowiedzialności karnej za naruszenie obowiązków związanych z ochroną danych osobowych określa ustawa o ochronie danych osobowych.

§ 23

Obowiązki i odpowiedzialność poszczególnych pracowników Centrum w zakresie ochrony i zabezpieczania danych osobowych powinien określać indywidualny zakres czynności tej osoby oraz oświadczenie, o którym mowa w § 8 ust. 1.

Załącznik A

……
Imię, nazwisko
……
……
Adres zamieszkania

Oświadczenie

W związku z …….. wyrażam zgodę na przetwarzanie danych osobowych dla celów niezbędnych związanych z realizacji zadań Centrum na podstawie Ustawy o samorządzie i innych przepisów szczegółowych zgodnie z art. 23, 24 i 25 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (t.j. Dz.U. z 2015r. poz. 2135 z późn. zm.).

……. ……
(miejscowość, data) *(czytelny podpis)*

Załącznik B

..... ……
imię i nazwisko miejscowość, data

OŚWIADCZENIE
o zachowaniu w tajemnicy danych osobowych oraz o zapoznaniu się
z przepisami dotyczącymi ochrony danych osobowych

Ja, ...
(imię i nazwisko)

zatrudniony/a na stanowisku .....

w .....
(nazwa komórki organizacyjnej)

Oświadczam, że zapoznałem/am się z treścią Zarządzenia Nr ……/2017 z dnia ……. 17 r. w sprawie wprowadzenia Instrukcji ochrony danych osobowych i zobowiązuję się do zachowania w tajemnicy danych osobowych, do których mam dostęp przy wykonywaniu czynności służbowych, także po ich zakończeniu.
Oświadczam również, że znane mi są konsekwencje przewidziane prawem za ujawnienie tajemnicy dotyczącej danych osobowych, w szczególności przepisy rozdziału 8 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2015 r. poz. 2135 z późn. zm.)

.....
(podpis)

Załącznik C

Administrator
Danych Osobowych

Dyrektor
Centrum Usług Wspólnych
w Kobylnicy

Wniosek
o wydanie/cofnięcie upoważnienia do przetwarzania danych osobowych

Wnoszę o wydanie upoważnienia/cofnięcie* upoważnienia z dnia ……..
Pani/Panu …… zatrudnionej/emu*) w Centrum Usług Wspólnych w Kobylnicy na stanowisku …… do przetwarzania danych osobowych wynikających z zakresu obowiązków pracowniczych z powodu:

a) podjęcia pracy na stanowisku ***związanym z dostępem do*** ……***zbioru***
b) zmiany stanowiska……,
c) zmiany zakresu obowiązków pracowniczych……..,
d) utworzenia nowego zbioru danych osobowych…….....,
e) naruszenia zasad i sposobu przetwarzania danych osobowych…….……,
f) inne …….

1. Nazwa zbioru danych osobowych:
   ……..……
2. Rodzaj uprawnień:
   Z - **pełne prawa do zarządzania bazą danych (**wprowadzanie i dokonywanie zmian),
   P - prawo do przeglądania,*)
3. Sposób i miejsce przetwarzania danych osobowych:
   ……

……..
data i podpis Kierownika Działu/
pracownika na samodzielnym stanowisku pracy

* niepotrzebne skreślić

Załącznik Nr 3
do Zarządzenia Nr 23/2017
Dyrektora Centrum
Usług Wspólnych w Kobylnicy
z dnia 10.05.2017 r.

INSTRUKCJA
zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Centrum Usług Wspólnych w Kobylnicy

ROZDZIAŁ 1
Postanowienia ogólne.

§ 1

Instrukcja Zarządzania Systemami Informatycznymi jest dokumentem eksploatacyjnym, regulującym zasady oraz procedury zarządzania i administrowania Systemami Informatycznymi Centrum. Instrukcja obejmuje swoim zakresem wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w systemach informatycznych, w szczególności zaś osoby pełniące funkcje:

1) administratora bezpieczeństwa informacji w Centrum;
2) administratora systemów informatycznych w Centrum;
3) bezpośrednich przełożonych osób przetwarzających dane osobowe;
4) inne osoby wskazane przez Administratora Danych Osobowych, w tym osoby z podmiotów zewnętrznych współpracujące z Centrum Usług Wspólnych w Kobylnicy współuczestniczące w procesie przetwarzania danych osobowych.

§ 2

Określenia i skróty użyte w Instrukcji oznaczają:

1) **Administrator Danych Osobowych** – Dyrektor Centrum Usług Wspólnych w Kobylnicy, zwany dalej Administratorem.
2) **ABI - Administrator Bezpieczeństwa Informacji** – osoba wyznaczona przez Administratora, w rozumieniu art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2015 r., poz. 2135 z późn. zm.), dalej zwana Ustawą.
3) **ASI - Administrator Systemów Informatycznych** – pracownik wyznaczony przez Administratora odpowiedzialny za wdrożenie i stosowanie zasad bezpieczeństwa systemów informatycznych, zobowiązany do stosowania technicznych i organizacyjnych środków ochrony przewidzianych w systemach informatycznych.
4) **Użytkownik systemu** – osoba posiadająca upoważnienie do wprowadzania i przetwarzania danych w systemie informatycznym w zakresie wskazanym w upoważnieniu.
5) **Przełożony użytkownika, zwany dalej przełożonym** – Dyrektor, Kierownik Działu - osoba odpowiedzialna za przestrzeganie zasad przetwarzania i ochrony danych przez podległych mu pracowników.
6) **Hasło** – ciąg znaków literowych, cyfrowych lub innych specjalnych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
7) **Identyfikator użytkownika** - ciąg znaków literowych, cyfrowych lub innych specjalnych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych w systemie informatycznym.
8) **Sieć LAN** – sieć lokalna umożliwiająca połączenie systemów informatycznych Centrum Usług Wspólnych w Kobylnicy przy wykorzystaniu specjalistycznych dedykowanych urządzeń i sieci telekomunikacyjnych w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (t.j. Dz. U. z 2014 r., poz. 243, z późn. zm.).
9) **Dane sensytywne** - dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także informacje o innych orzeczeniach wydanych w postępowaniu sądowym lub administracyjnym.
10) **Rejestr udostępnionych danych osobowych, zwany dalej Rejestrem** – rejestr, w którym odnotowywane są informacje o odbiorcach danych z systemu/aplikacji, prowadzony dla danego systemu/aplikacji.

ROZDZIAŁ 2
Procedury nadawania, zmiany uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemach informatycznych

§ 3

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych zapoznaje się z:
   1) niniejszą instrukcją,
   2) procedurami określonymi przez Administratora Danych Osobowych.
2. Podstawą nadania uprawnień jest wniosek przełożonego zawarty w **Załączniku nr 6** do Zarządzenia w sprawie wprowadzenia w Centrum Usług Wspólnych w Kobylnicy polityki bezpieczeństwa.

§ 4

1. Opis procedury nadawania/odbierania uprawnień dostępu do lokalnej sieci komputerowej przedstawiony jest poniżej. Stosowany w Centrum Usług Wspólnych w Kobylnicy schemat uprawnień dostępu do sieci LAN zakłada, iż użytkownicy uzyskują dostęp do sieci na z góry zdefiniowanym poziomie użytkownika w zależności od zakresu obowiązków i powierzonych zadań do wykonania na danym stanowisku.
2. Przełożony użytkownika:
   1) wnioskuje o nadanie/odebranie pracownikowi uprawnień do przetwarzania danych w systemach/aplikacjach eksploatowanych w sieci LAN Centrum w związku z wykonywanymi przez niego zadaniami,
   2) zgłasza do ASI potrzebę nadania/odebrania uprawnień w systemie informatycznym na wymaganym poziomie, na formularzu stanowiącym **Załącznik nr 6** do Zarządzania w sprawie wprowadzenia w Centrum polityki bezpieczeństwa.
3. ASI na podstawie otrzymanego formularza, wykonuje:
   1) rejestruje/usuwa użytkownika w systemie i nadaje mu wymagane uprawnienia,
   2) informuje przełożonego użytkownika oraz ABI o fakcie nadania/odebrania uprawnień. W przypadku nadania uprawnień, informuje dodatkowo o założonym koncie wnioskowanym dla użytkownika i nadanych uprawnieniach,
   3) w przypadku, gdy nadanie pracownikowi wymaganych uprawnień może grozić naruszeniem standardów bezpieczeństwa systemów/aplikacji pracujących w sieci, ASI informuje przełożonego użytkownika oraz ABI o tym zagrożeniu i wstrzymuje proces nadawania uprawnień. Przełożony użytkownika ponownie może wnioskować o przyznanie pracownikowi zmodyfikowanych uprawnień, które nie stanowią zagrożenia naruszenia bezpieczeństwa, a jego wniosek musi zostać zaakceptowany przez ABI.
4. Użytkownik, po otrzymaniu od ASI informacji o założonym koncie z wymaganymi uprawnieniami, wykonuje:
   a) loguje się do systemu/aplikacji w celu sprawdzenia poprawności konta i uprawnień,
   b) przy pierwszym logowaniu się do systemu/aplikacji, użytkownik musi zmienić nadane mu przez ASI hasło.
5. Powyższy schemat nadania/odebrania uprawnień dostępu do systemów/aplikacji eksploatowanych w sieci LAN należy stosować również w przypadku wymaganej zmiany w istniejących uprawnieniach użytkownika.

§ 5

1. Powyższe zasady nadawania/odbierania uprawnień dostępu do wszystkich systemów/aplikacji eksploatowanych w Centrum obowiązują wszystkich pracowników.
2. W przypadku gdy system/aplikacja nie posiada wbudowanych mechanizmów kontroli dostępu, wówczas należy niezwłocznie rozbudować taki system/aplikacje o te mechanizmy, a do czasu wdrożenia takich mechanizmów należy zaimplementować ograniczenia dostępu na poziomie systemu operacyjnego, bądź ograniczenia proceduralne.

ROZDZIAŁ 3
Metody i środki uwierzytelnienia w systemach informatycznych

§ 6

Naczelną zasadą bezpieczeństwa systemów/aplikacji i sieci IT jest ochrona informacji przed nieuprawnionym dostępem, ujawnieniem, przypadkowym lub nieautoryzowanym zniszczeniem lub modyfikacją danych. Stosowanie zasad uwierzytelniania użytkowników systemów/aplikacji (w tym sieci LAN) ma bezpośredni wpływ na zachowanie poufności, rozliczalności oraz integralności danych.

§ 7

1. W systemach/aplikacjach informatycznych Centrum stosuje się uwierzytelnienie dwustopniowe, na poziomie:
   a) dostępu do sieci LAN,
   b) dostępu do systemu/aplikacji.
2. Do uwierzytelnienia użytkownika w systemie/aplikacji na obu poziomach używa się identyfikatorów, haseł lub karty inteligentnej.
   a) stosowanie unikalnych identyfikatorów użytkownika zapewnia bezpieczeństwo i realizuje zasady rozliczalności w systemach i sieciach teleinformatycznych Centrum Usług Wspólnych w Kobylnicy,
   b) zasada ta ma na celu przypisanie w sposób jednoznaczny wszelkich działań w systemie konkretnemu użytkownikowi (nie dopuszcza się, aby użytkownik korzystał z kont: administrator, gość, a także z konta innego użytkownika),
   c) ograniczenie dostępu do informacji jedynie do kręgu użytkowników uprawnionych (autoryzowanych) wymaga przyjęcia odpowiednio dobranej polityki stosowania haseł. z
3. W Centrum Usług Wspólnych w Kobylnicy, stosuje się poziom bezpieczeństwa przetwarzania danych adekwatnie do klasyfikacji tych danych w systemach/aplikacjach. W związku z powyższym, obowiązujące są trzy poziomy bezpieczeństwa:
   a) **poziom podstawowy** - dla systemów/aplikacji, w których nie są przetwarzane dane osobowe sensytywne oraz żadne urządzenie systemu informatycznego służące do przetwarzania danych osobowych nie jest połączone z siecią publiczną. Wówczas hasło na poziomie dostępu do systemu/aplikacji musi się składać z co najmniej 8 znaków,
   b) **poziom podwyższony** - dla systemów/aplikacji, w których są przetwarzane dane sensytywne oraz żadne urządzenie systemu informatycznego służące do przetwarzania danych osobowych nie jest połączone z siecią publiczną. Wówczas hasło na poziomie dostępu do systemu/aplikacji musi składać się z co najmniej 8 znaków, i musi zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,
   c) **poziom wysoki** - dla systemów/aplikacji, w których są przetwarzane dane sensytywne oraz co, najmniej jedno urządzenie systemu informatycznego służące do przetwarzania danych osobowych jest połączone z siecią publiczną. Wówczas Administrator danych musi stosować środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelniania.
4. Hasło dostępu do sieci LAN musi składać się z minimum 8 znaków składające się z kombinacji dużych i małych liter i co najmniej dwóch cyfr.
5. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów bądź innych bezpośrednio kojarzących się z użytkownikiem.
6. Hasło nie może być ujawnione innej osobie nawet po utracie ważności hasła.
7. System automatycznie powinien wymuszać zmianę hasła nie rzadziej, niż jeden raz w miesiącu. Hasło musi być zmienione przez użytkownika niezwłocznie w przypadku podejrzenia lub stwierdzenia jego ujawnienia.

§ 8

Procedura zarządzania środkami uwierzytelniania

1) ASI nadaje hasło dostępu do systemu/aplikacji lub sieci LAN dla nowego użytkownika albo dla użytkownika, który zapomniał swojego ostatniego hasła,
2) użytkownik systemu/aplikacji niezwłocznie ustala swoje, znane tylko jemu hasło, po nadaniu hasła przez ASI. System winien automatycznie wymusza na użytkowniku zmianę nadanego przez administratora hasła przy pierwszym logowaniu,

3) w przypadku braku automatycznego wymuszaniu na użytkowniku zmiany nadanego mu przez administratora hasła użytkownik jest zobowiązany zmieniać hasło nie rzadziej niż jeden raz w miesiącu,
4) użytkownik systemu w dowolnym momencie może zmienić swoje hasło dostępu do systemu/aplikacji,
5) obowiązuje bezwzględny zakaz notowania w jakiejkolwiek formie obecnych oraz wygasłych haseł dostępu,
6) ASI zapisuje swój identyfikator oraz hasła dostępu po każdej ich zmianie i umieszcza je w kopercie, a następnie przekazuje zamkniętą kopertę do przechowania w wyznaczonej do tego celu szafie metalowej ulokowanej w pomieszczeniach ABI. Koperta taka może być awaryjnie udostępniona innemu administratorowi za zgodą przełożonego ASI Przełożony ASI odpowiedzialny jest za prowadzenie rejestru udostępnionych awaryjnie haseł. Po awaryjnym użyciu hasła, musi ono zostać jak najszybciej zmienione przez ASI.

ROZDZIAŁ 4
Rozpoczęcie, zawieszenie i zakończenie pracy przez użytkowników systemów

§ 9

1. Procedura rozpoczęcia pracy
   1) uruchomić komputer wchodzący w skład systemu informatycznego, podłączony fizycznie do sieci lokalnej i zalogować się podając własny identyfikator i hasło dostępu,
   2) jeśli użytkownik wprowadzi 3-krotnie błędnie hasło, wówczas jego identyfikator i hasło zostaną zablokowane. W celu odblokowania swojego identyfikatora, użytkownik postępuje według procedury obowiązującej przy nadawaniu/odbieraniu uprawnień dostępu do systemów informatycznych opisanej w Rozdziale 2, § 4,
   3) uruchomić wybrany system/aplikację (w szczególności aplikację bazodanową m.in. przetwarzającą dane),
   4) zalogować się do systemu/aplikacji w sposób analogiczny do przedstawionego powyżej.
1. Procedura zawieszenia pracy w systemie/aplikacji. Przy każdorazowym opuszczeniu stanowiska komputerowego, należy dopilnować, aby na ekranie nie były wyświetlane informacje lub dane, poprzez zablokowanie komputera. Każdy użytkownik ma obowiązek stosowania wygaszacza ekranu zabezpieczonego hasłem lub wylogowania się z systemu.
2. Procedura zakończenia pracy w systemie
   1) zamknąć system/aplikację,
   2) zamknąć system operacyjny komputera i zaczekać na jego wyłączenie,
   3) wyłączyć monitor
   4) sprawdzić, czy elektroniczne nośniki informacji zawierające dane osobowe nie zostały pozostawione bez nadzoru.
4. Użytkownik w pełnym zakresie odpowiada za powierzony mu sprzęt komputerowy i wykonywane czynności aż do momentu rozliczenia ze sprzętu komputerowego.

ROZDZIAŁ 5
Procedury tworzenia kopii zapasowych danych

§ 10

1. W celu zapewnienia optymalnego poziomu ochrony danych gromadzonych w systemach informatycznych Centrum Usług Wspólnych w Kobylnicy, przyjęto do stosowania zasadę przetwarzania informacji zawartych w bazach danych Urzędu w oparciu o architekturę klient – serwer. Wynika stąd praktyka przetwarzania danych w bazach danych na dedykowanych dla systemu/aplikacji serwerach.
2. Jeśli stosowane dotychczas rozwiązania nie są zgodne z architekturą klient – serwer, to należy zapewnić możliwość przechowywania gromadzonych za ich pomocą danych na wyznaczonym serwerze plików.
3. Indywidualne stanowiska komputerowe, do których dostęp posiadają pracownicy Centrum, stanowią jedynie końcówki klienckie systemu komputerowego.
4. Wszelkie informacje (w tym dane osobowe) przetwarzane przy pomocy uruchamianych na poszczególnych stanowiskach aplikacjach bazodanowych są zapisywane bezpośrednio na serwerach.
5. W szczególnych przypadkach, za zgodą ABI, aplikacje oraz dane, w tym dane osobowe, mogą być przechowywane lokalnie na stanowiskach komputerowych niepodłączonych do sieci LAN

Centrum. W takich przypadkach obowiązek wykonania kopii bezpieczeństwa aplikacji oraz codziennego wykonywania kopii bezpieczeństwa bazy danych oraz ich bezpiecznego przechowywania (zgodnie z zasadami opisanymi w poniższym § 11 ust.3), spoczywa bezpośrednio na użytkowniku danej aplikacji.

6. Opisywana tu zasada przetwarzania danych wpływa bezpośrednio na zagadnienia związane z tworzeniem kopii bezpieczeństwa systemów.

§ 11

1. Kopie zapasowe baz danych oraz aplikacji bazodanowych zlokalizowanych na serwerach wykonywane są:
   1) w cyklu dobowym (w godzinach nocnych) za pomocą aplikacji archiwizujących dane do postaci tzw. kopii przyrostowych (zawierających zapis jedynie tych informacji, które podczas ostatniej doby uległy zmianie),
   2) w cyklu tygodniowym, podobnie przy użyciu oprogramowania aplikacji archiwizujących, tworzone są pełne kopie baz danych oraz aplikacji,
   3) w cyklu miesięcznym tworzony jest „ręczny", pełny backup systemu (łącznie z kopią systemu operacyjnego serwera).
2. ASI sprawuje nadzór nad wykonywaniem ww. kopii zapasowych oraz weryfikuje ich poprawność.
3. Zasady przechowywania kopii
   1) kopie zapasowe zbioru danych oraz oprogramowania i narzędzi programistycznych zastosowanych do przetwarzania danych są przechowywane w przeznaczonej do tego celu metalowej szafie, znajdującej się w wyznaczonym pomieszczeniu w Centrum,
   2) dostęp do metalowej szafy mają tylko upoważnieni pracownicy, tj. ASI oraz ABI,
   3) czas przechowywania kopii zapasowych określony został w dokumentacji przetwarzania i ochrony Danych Osobowych (rozdz. 6 Instrukcji Zarządzania Systemami Informatycznymi Służącymi do Przetwarzania Danych Osobowych).

ROZDZIAŁ 6

Przechowywanie nośników informacji zawierające dane oraz kopii zapasowych

§ 12

1. Elektroniczne nośniki informacji
   1) dane w postaci elektronicznej przetwarzane w systemie zapisane na nośnikach materialnych (np. dyskietkach, dyskach magnetooptycznych, taśmach magnetycznych czy dyskach twardych) są własnością Centrum Usług Wspólnych w Kobylnicy,
   2) wyżej wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych,
   3) po zakończeniu pracy przez użytkowników systemu/aplikacji, ww. elektroniczne nośniki informacji są przechowywane w meblach biurowych ze sprawnym zamknięciem lub w kasetkach,
   4) elektroniczne nośniki informacji, o których mowa powyżej, powinny być oznaczone w sposób umożliwiający ich identyfikację.
2. Przekazywanie i niszczenie elektronicznych nośników informacji
   1) elektroniczne nośniki informacji zawierające dane osobowe można przekazywać tylko podmiotom lub osobom uprawnionym na podstawie przepisów prawa, za zgodą osoby do tego upoważnionej przez Administratora Danych Osobowych,
   2) dane osobowe na każdym nośniku zewnętrznym powinny być zabezpieczone przed odczytem (minimum hasłem),
   3) dane osobowe przenoszone za pomocą zewnętrznych nośników informacji powinny być z nich trwale usunięte po poprawnym ich przeniesieniu na docelowy sprzęt komputerowy i do docelowej bazy danych,
   4) przekazanie i niszczenie elektronicznych nośników informacji zawierających dane osobowe, odbywa się na podstawie protokołu podpisanego przez ASI oraz właściwych użytkowników, po ustaniu potrzeby przetwarzania danych w zbiorze.
      Protokół zatwierdzony przez przełożonego użytkownika należy przesłać do ABI.

ROZDZIAŁ 7
Środki ochrony systemów informatycznych

§ 13

1. Poniżej przedstawiono zasady ochrony systemów przetwarzania danych przed tzw. „szkodliwym oprogramowaniem” oraz próbami penetracji przez osoby nieuprawnione.
2. Ochrona antywirusowa
   1) za ochronę antywirusową odpowiada ASI,
   2) czynności związane z ochroną antywirusową systemu informatycznego wykonuje ASI, wykorzystując w trakcie pracy systemu informatycznego moduły programu antywirusowego w aktualnej wersji, sprawdzającego na bieżąco zasoby systemu informatycznego,
   3) oprogramowanie antywirusowe jest instalowane centralnie na serwerze, oraz na wszystkich stanowiskach komputerowych podłączonych do sieci,
   4) aktualizacja oprogramowania antywirusowego odbywa się nie rzadziej niż raz w tygodniu, w sposób automatyczny dla wszystkich komputerów zainstalowanych w sieci,
   5) instalacja oprogramowania antywirusowego oraz jego aktualizacja na komputerach niepodłączonych do sieci, odbywa się nie rzadziej niż raz w tygodniu i jest wykonywana przy zastosowaniu nośników zewnętrznych przez ASI,
   6) użytkownik systemu na stanowisku komputerowym, importujący dane do systemu informatycznego, jest odpowiedzialny za sprawdzenie tych danych pod kątem możliwości występowania wirusów i szkodliwego oprogramowania, a na importowanie plików musi uzyskać zgodę od ASI.

§ 14

1. ASI jest odpowiedzialny za aktywowanie i poprawną konfigurację specjalistycznego oprogramowania monitorującego wymianę danych na styku:
   1) sieci lokalnej (LAN),
   2) stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej.
2. ASI obowiązany jest do utrzymywania stałej aktywności zainstalowanego specjalistycznego oprogramowania monitorującego wymianę danych oraz do jego aktualizacji.
3. Ochrona przed awarią zasilania
   1) system, w którym przetwarzane są dane osobowe powinien posiadać mechanizmy pozwalające zabezpieczyć je przed ich utratą lub nieautoryzowaną zmianą spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej,
   2) dane osobowe przetwarzane w systemie chroni się stosując filtry zabezpieczające przed skutkami spadku napięcia oraz urządzenia podtrzymujące zasilanie do momentu poprawnego zapisania danych i wylogowania się użytkownika z systemu,
   3) dane osobowe przetwarzane z wykorzystaniem serwera w wewnętrznych sieciach teleinformatycznych należy zabezpieczać przed zanikiem napięcia wykorzystując centralny UPS i generator prądu.

ROZDZIAŁ 8
Monitorowanie dostępu do danych

§ 15

1. Dla każdego systemu, w którym przetwarzane są dane osobowe, prowadzony jest Rejestr, w którym odnotowywane są informacje o odbiorcach danych z tego systemu (o ile występuje dla danego systemu proces udostępniania danych osobom wymienionym w § 15 ust.2).
2. Odbiorcą danych jest każdy, komu udostępnia się dane:
   1) osoby, której dane dotyczą,
   2) podmiotu, któremu powierzono przetwarzanie danych,
   3) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
3. Odnotowanie obejmuje informacje o
   1) nazwie jednostki organizacyjnej lub imieniu i nazwisku osoby, której udostępniono dane,
   2) zakresie udostępnianych danych,
   3) dacie udostępnienia.
4. Obowiązek odnotowania ww. informacji w Rejestrze spoczywa na użytkowniku systemu udostępniającemu dane.

5. Odnotowanie informacji w Rejestrze powinno nastąpić niezwłocznie po udostępnieniu danych.
6. Udostępnienie danych osobowych może nastąpić w następujących przypadkach:
   1) w celu innym niż włączenie danych do zbioru - Administrator udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa,
   2) dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.
7. Udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
8. Na żądanie osoby, której dane zostały udostępnione, informacje o udostępnionych danych są zamieszczane w raporcie z Rejestru, a raport przekazywany tej osobie.
9. Nadzór nad prawidłowością odnotowywania w Rejestrze ww. informacji sprawuje ABI.

ROZDZIAŁ 9
Procedury wykonywania przeglądów i konserwacji systemu

§ 16

1. Dla zachowania ciągłości pracy i bezpieczeństwa danych przeprowadza się przegląd i konserwację platformy sprzętowej, na której eksploatowany jest system/aplikacja.
2. Przeglądy i konserwacja urządzeń
   1) przeglądy i konserwacja urządzeń wchodzących w skład platformy sprzętowej dla danego systemu/aplikacji powinny być wykonywane w terminach określonych przez producenta sprzętu,
   2) jeśli producent nie przewidział dla danego urządzenia potrzeby dokonywania przeglądów eksploatacyjnych, lub też nie określił ich częstotliwości, to o dokonaniu przeglądu oraz sposobie jego przeprowadzenia decydują ASI,
   3) przegląd i konserwacja urządzeń, może być wykonana na żądanie przełożonego ASI,
   4) czynności, o których mowa w § 16 ust 2 lit a) i lit b) wykonują ASI co najmniej jeden raz na kwartał,
   5) nieprawidłowości ujawnione w trakcie przeglądów bądź konserwacji, powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie ujawnienia nieprawidłowości ASI informuje ABI,
   6) za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada przełożony ASI.

§ 17

1. Przegląd systemów/aplikacji i narzędzi programistycznych przeprowadzany jest w celu sprawdzenia poprawności działania i wykonywany jest w następujących przypadkach:
   1) zmiany wersji oprogramowania systemu/aplikacji,
   2) zmiany wersji oprogramowania na stanowisku komputerowym użytkownika,
   3) zmiany systemu operacyjnego platformy sprzętowej, na której eksploatowany jest system/aplikacja,
   4) zmiany systemu operacyjnego na stanowisku komputerowym użytkownika,
   5) wykonania zmian w systemie/aplikacji spowodowanych koniecznością naprawy lub modyfikacji systemu.
2. Przed dokonaniem zmian w systemie/aplikacji należy dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych, na testowej bazie danych. Sprawdzenie powinno m.in. obejmować:
   1) poprawność logowania się do systemu w zależności od posiadanych uprawnień (zasymulować pracę wszystkich typów uprawnień użytkownika),
   2) poprawność działania funkcjonalności systemu/aplikacji sprawdzonej na różnego typu danych,
   3) poprawność działania wszystkich elementów aplikacji (menu, zestawienia, formularze, raporty, itp.).
3. Za prawidłowość przeprowadzenia procesu przeglądu i konserwacji systemu/aplikacji odpowiada przełożony ASI.

§ 18

Konserwacja systemów/aplikacji wykorzystywanych przez użytkowników.

1) Konserwację oprogramowania przeprowadza się po zgłoszeniu przez użytkownika systemu/aplikacji potrzeby wprowadzenia zmian pozwalających dostosować funkcjonalność

systemu/aplikacji do obsługi bieżących i planowanych potrzeb Urzędu. Zgłoszenia kierowane jest do ASI.

2) Przed wdrożeniem wymaganych przez użytkownika zmian w systemie/aplikacji informatycznej, należy dokonać sprawdzenia poprawności działania zmodyfikowanego systemu/aplikacji w warunkach testowych na testowej bazie danych na takich samych zasadach jak ma to miejsce w przypadku przeglądu oprogramowania, opisanych w §17 ust.3.
3) Konserwację systemu/aplikacji przeprowadza się w obecności użytkownika.

ROZDZIAŁ 10
Postanowienia końcowe

§ 19

W sprawach nie uregulowanych niniejszą Instrukcją zastosowanie znajdują:

1) Norma PN-I-13335-1 „Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych".
2) Norma PN-ISO/IEC-17799 „Technika informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji.
3) Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2015 r., poz. 2135 z późn. zm.).
4) 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. Nr 100 poz. 1024).

Załącznik Nr 4
do Zarządzenia Nr 23/2017
Dyrektora Centrum
Usług Wspólnych w Kobylnicy
z dnia 10.05.2017 r.

Zasady użytkowania sprzętu komputerowego przez pracowników Centrum Usług Wspólnych w Kobylnicy

§ 1

Zasady użytkowania sprzętu komputerowego przez pracowników Centrum Usług Wspólnych w Kobylnicy, zwane dalej zasadami, określają prawa i obowiązki użytkowników sprzętu komputerowego.

§ 2

Ilekroć w zasadach jest mowa o:

1) **specjalista ds. informatyki** - Specjalista ds. obsługi i zabezpieczenia informatycznej bazy danych Centrum Usług Wspólnych w Kobylnicy przyjmujących i realizujących zgłoszone problemy dotyczące użytkowania sprzętu komputerowego i oprogramowania komputerowego,
2) **sprzęcie komputerowym** - rozumie się przez to komputer oraz urządzenia peryferyjne, w tym: monitor, drukarka, skaner, wymagające do swojego działania połączenia z komputerem,
3) **nośniki informatyczne** - urządzenia umożliwiające zapisywanie i przenoszenie danych (np. dyskietka, twardy dysk, płyta CD, pamięci masowe flash).

§ 3

Użytkownikowi systemu przysługuje prawo:

1) do korzystania ze sprzętu komputerowego wyłącznie w zakresie powierzonych mu zadań,
2) do korzystania z oprogramowania komputerowego zgodnie z umowami i ustawą z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (tj. Dz.U. z 2006 r., nr 90, poz. 631 z poź. zm.).

§ 4

Informacje zapisane na nośnikach informatycznych należą do pracodawcy Centrum Usług Wspólnych w Kobylnicy.

§ 5

O przekazaniu sprzętu komputerowego użytkownikowi decyduje przełożony użytkownika.

§ 6

1. Użytkownik jest materialnie odpowiedzialny za sprzęt komputerowy, który otrzymał do wykonywania obowiązków służbowych.
2. Każdy pracownik Centrum zobowiązany jest w miejscu pracy do użytkowania tylko i wyłącznie legalnego oprogramowania.
3. Przed przystąpieniem do pracy zobowiązany jest do przestrzegania zasad i procedur obowiązujących przy użytkowaniu sprzętu komputerowego w Centrum i podpisania oświadczenia, którego wzór stanowi ***Załącznik nr A***.

§ 7

Specjalista ds. obsługi i zabezpieczenia informatycznej bazy danych prowadzi sprawy w zakresie użytkowania sprzętu komputerowego i oprogramowania komputerowego, a w szczególności:

1) jest jedyna osobą w Centrum uprawnioną do instalowania programów na stanowiskach pracy
2) sprawuje nadzór nad wykonaniem umów, dotyczących zakupu/serwisu sprzętu i oprogramowania,
3) prowadzi ewidencję sprzętu i oprogramowania,
4) zabezpiecza sprawne działanie sprzętu komputerowego i oprogramowania,
5) zapewnia standardy sprzętu komputerowego i oprogramowania spełniające wymagania Centrum,

6) prowadzi dla komputerów użytkowanych w Centrum metryczki z przypisanymi zasobami informatycznymi zgodnymi z wymogami ustalonymi przez pracodawcę, którego wzór stanowi ***Załącznik nr B*** do Zasad użytkowania sprzętu komputerowego przez pracowników Centrum,
7) dokonuje sukcesywnej oceny zasadności zakupów oprogramowania lub instalowania oprogramowania niezbędnego w zasobach Urzędu, a mającego być wykorzystanym na stanowisku pracy,
8) przechowuje w zamkniętej szafie nośniki oprogramowania, do których dostęp maja tylko osoby upoważnione.

§ 8

1. W przypadku zmiany miejsca pracy użytkownika systemu na inną komórkę organizacyjną w Centrum, sprzęt komputerowy pozostaje w dotychczasowej komórce organizacyjnej.
2. Na przeniesienie sprzętu komputerowego wraz z użytkownikiem systemu do nowej komórki organizacyjnej musi wyrazić zgodę dotychczasowy przełożony użytkownika.
3. Użytkownik systemu jest zobowiązany do przekazania informacji specjaliście ds. obsługi i zabezpieczenia informatycznej bazy danych o przeniesieniu pracownika wraz ze sprzętem komputerowym do nowej komórki organizacyjnej.
4. Przełożony użytkownika zobowiązany jest do:
   1) zlecenia specjaliście ds. informatyki zmiany lokalizacji sprzętu komputerowego,
   2) informowania specjalistę ds. informatyki o przekazaniu sprzętu innemu użytkownikowi.

§ 9

Każdy użytkownik systemu posiada identyfikator i hasło, które zabezpieczają dostęp do komputera, baz danych i skrzynki pocztowej użytkownika.

§ 10

Zabronione jest:
1) podłączanie przez użytkownika własnych urządzeń do sprzętu komputerowego**,**
2) podłączania przez użytkowników innych urządzeń niż informatyczne do wydzielonej sieci energetycznej do zasilania komputerów,
3) instalowania oprogramowania na sprzęcie komputerowym**,**
4) przemieszczenia sprzętu komputerowego do innej lokalizacji (pokoju) lub zmiany użytkownika bez uzgodnienia z specjalistą ds. informatyki
5) fizyczne ingerowanie w konfigurację sprzętową urządzeń,
6) udostępnianie swojego identyfikatora i hasła do pracy innym osobom,
7) kopiowanie, wypożyczenie i przekazywanie osobom nieupoważnionym nośników oprogramowania,
8) pozyskiwanie informacji z komputerów innych użytkowników bez ich wiedzy,
9) wynoszenie poza miejsce pracy nośników zawierających dane oraz przesyłanie danych pocztą elektroniczną na zewnątrz.

§ 11

Na stanowiskach pracy, na których używany jest sprzęt komputerowy obowiązują szczegółowe zasady jego użytkowania:
1) zakaz spożywania posiłków przy sprzęcie komputerowym,
2) zapewnienie warunków umożliwiających swobodne działanie układu chłodzenia użytkowanego sprzętu komputerowego,
3) utrzymanie czystości przy stanowiskach komputerowych,
4) zapewnienie odpowiedniego miejsca na lokalizację sprzętu komputerowego,
5) odpowiednie meble,
6) ustawienie z dala od źródeł wilgoci, grzejników lub innych substancji mogących zakłócić prawidłowe działanie sprzętu komputerowego.

§ 12

Wszelkie wątpliwości związane z zasadami użytkowania sprzętu komputerowego i instalowania oprogramowania w Centrum Usług Wspólnych w Kobylnica rozstrzyga ASI w porozumieniu ABI.

§ 13

Naruszenie zasad użytkowania sprzętu komputerowego przez pracowników Centrum Usług Wspólnych w Kobylnicy, ze względu na obowiązujące przepisy prawne stanowi poważne naruszenie podstawowych obowiązków pracowniczych.

Załącznik A

Oświadczenie

Przyjmuję do wiadomości obowiązek korzystania na stanowisku pracy przy obsłudze stacji komputerowych tylko i wyłącznie z legalnego oprogramowania pochodzącego z zasobów Centrum Usług Wspólnych w Kobylnicy, do którego jest on uprawniony.
Jednocześnie zobowiązuje się do przestrzegania zasad określonych Załączniku nr 4 do Zarządzenia Nr ……. z dnia ……. 2017 r. w sprawie Zasad użytkowania sprzętu komputerowego przez pracowników Centrum Usług Wspólnych w Kobylnicy.
Ponadto zobowiązuje się do przestrzegania zakazu kopiowania i rozpowszechniania oprogramowania pozostającego w dyspozycji Centrum Usług Wspólnych w Kobylnicy.

……
(data i podpis pracownika)

Załącznik B

METRYKA KOMPUTERA
stan zainstalowanych programów

Jednostka	***Centrum Usług Wspólnych w Kobylnicy***
Nr inwentarzowy	
Komórka organizacyjna	
Imię i Nazwisko	

Zainstalowane oprogramowanie

Nazwa i producent programu	***Nr wersji***	***Oryginalny nośnik***	***Klucz produktu***

Załącznik Nr 5
do Zarządzenia Nr 23/2017
Dyrektora Centrum
Usług Wspólnych w Kobylnicy
z dnia 10.05.2017 r.

Zasady udzielania pomocy
użytkownikom sprzętu komputerowego w Centrum Usług Wspólnych w Kobylnicy

§ 1.

Zasady udzielania pomocy użytkownikom sprzętu komputerowego w Centrum Usług Wspólnych w Kobylnicy, zwane dalej zasadami, określają zasady postępowania w przypadku wystąpienia problemów w użytkowaniu sprzętu komputerowego lub zainstalowanego oprogramowania

§ 2.

Ilekroć w Zasadach jest mowa o:

4) **Specjalista ds. informatyki** - Specjalista ds. obsługi i zabezpieczenia informatycznej bazy danych Centrum Usług Wspólnych w Kobylnicy,
5) **sprzęcie komputerowym** - rozumie się przez to komputer oraz urządzenia peryferyjne, w tym. monitor, drukarka, skaner, wymagające do swojego działania połączenia z komputerem,

§ 3.

1. Specjalista ds. informatyki przyjmuje od użytkowników systemu zgłoszenia dotyczące problemów związanych z użytkowaniem sprzętu komputerowego i jego oprogramowania.
2. Specjalista ds. informatyki każdy przypadek związany z zgłoszeniem problemów z użytkowaniem sprzętu komputerowego odnotowuje w prowadzonym przez siebie rejestrze z wskazaniem rodzaju podjętych w tym zakresie przedsięwzięć,
3. W przypadku braku możliwości usunięcia problemu ze sprzętem komputerowym, zgłasza sprzęt do serwisu zewnętrznego w celu dokonania naprawy serwisowej z jednoczesnym powiadomieniem użytkownika o braku możliwości naprawy sprzętu we własnym zakresie oraz przekazuje sprzęt komputerowy do serwisu i przedstawia użytkownikowi możliwości udostępnienia sprzętu zastępczego na czas naprawy.

§ 4.

Specjalista ds. informatyki sporządza półroczną analizę interwencji oraz awaryjności sprzętu i przedstawia raport ABI.

§ 5.

W przypadku konieczności oddania sprzętu komputerowego do zewnętrznego serwisu wymontowuje się i zabezpiecza dysk twardy oraz inne nośniki danych zainstalowane w danym sprzęcie.

§ 6.

1. W przypadku konieczności przekazania dysku komputera do naprawy poza miejsce użytkowania komputera:
   1) Specjalista ds. informatyki dokonuje zapisania danych na dysku sieciowym oraz nośniku CD lub DVD, a następnie kasuje dane użytkownika w sposób uniemożliwiający ich odczytanie, ze względu na poufność danych zapisanych na dyskach użytkownika,
   2) w przypadku awarii dysku twardego i konieczności podjęcia próby odtworzenia danych, zadanie to powierzane jest specjalistycznym firmom zewnętrznym, na podstawie zawartych umów.

Załącznik Nr 6
do Zarządzenia Nr 23/2017
Dyrektora Centrum
Usług Wspólnych w Kobylnicy
z dnia 10.05.2017 r.

WNIOSEK PRZEŁOŻONEGO O NADANIE UPRAWNIEŃ DLA UŻYTKOWNIKA W SYSTEMIE INFORMATYCZNYM.

Nowy użytkownik∗	Modyfikacja uprawnień∗	Odebranie uprawnień w systemie∗

DOTYCZY SYSTEMU: ……

(nazwa aplikacji (bazy danych), w której przetwarzane są dane osobowe)

Imię i nazwisko użytkownika:	**Referat / Samodzielne stanowisko∗**	
Pokój nr:	Telefon nr:	
Posiada upoważnienie do przetwarzania danych osobowych:	TAK∗	NIE∗
Opis zakresu uprawnień użytkownika w systemie informatycznym i uzasadnienie:		

Data zagłoszenia:	Przełożony użytkownika systemu:
ASI:	ABI:
	Zatwierdzam Dyrektor

∗ niepotrzebne skreślić.

Załącznik Nr 7
do Zarządzenia Nr 23/2017
Dyrektora Centrum
Usług Wspólnych w Kobylnicy
z dnia 10.05.2017 r.

REJESTR KOPII ZAPASOWYCH

Lp.	Imię nazwisko osoby wykonującej kopię	Opis kopii zapasowej	Nazwa systemu lub konta użytkownika	Numer ewidencyjny pod którym zarejestrowano kopię	Rodzaj kopii (Dzienna/ Tygodniowa/ Miesięczna)	Miejsce przechowywania kopii	Data Podpis	Uwagi

Załącznik Nr 8
do Zarządzenia Nr 23/2017
Dyrektora Centrum
Usług Wspólnych w Kobylnicy
z dnia 10.05.2017 r.

ZGŁOSZENIE NARUSZENIA BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO

DO:	**Administrator Bezpieczeństwa Informacji**				
OD:	Nazwisko i imię	Stanowisko	Komórka organizacyjna	Telefon	Podpis

Data i czas zajścia /zgłoszenia incydentu:	
Opis incydentu:	
Jakie przeciwdziałania zostały podjęte?	
Kto uczestniczył w incydencie?	
Kto został poinformowany o incydencie?	

Proszę podać również poniższe informacje:

Lokalizacja stacji roboczej/serwera	Nazwa stacji roboczej/serwera oraz adres IP	Nazwisko użytkownika stacji roboczej/ administratora serwera	Telefon użytkownika stacji roboczej/ administratora serwera	Uwagi

Informacje o sprzęcie:	Komputer	Monitor	Drukarka (podłączona bezpośrednio)	Inne
Producent				
Nr seryjny				

Załącznik Nr 9
do Zarządzenia Nr 23/2017
Dyrektora Centrum
Usług Wspólnych w Kobylnicy
z dnia 10.05.2017 r.

……
(Sygnatura dokumentu lub inne oznaczenie

EWIDENCJA OSÓB ZATRUDNIONYCH PRZY PRZETWARZANIU DANYCH OSOBOWYCH W CENTRUM USŁUG WSPÓLNYCH W KOBYLNICY

L.p.	Nazwa zbioru	Nazwisko i imię osoby upoważnionej	Identyfikator	Data nadania upoważnienia	Zakres upoważnienia	Data wygaśnięcia/cofnięcia upoważnienia	Uwagi* *Czy elektroniczne nadanie i przez kogo*

** dotyczy osób przetwarzających dane w systemie informatycznym*

Załącznik Nr 10
do Zarządzenia Nr 23/2017
Dyrektora Centrum
Usług Wspólnych w Kobylnicy
z dnia 10.05.2017 r.

.

.....
(Sygnatura dokumentu lub inne oznaczenie

WYKAZU ZBIORÓW DANYCH OSOBOWYCH PRZETWARZANYCH W CENTRUM USŁUG WSPÓLNYCH W KOBYLNICY

Lp.	Nazwa zbioru danych [1]	Nazwa jednostki organizacyjnej	Podstawa prawna utworzenia zbioru danych	Data utworzenia zbioru	Cel przetwarzania danych	Forma funkcjonowania zbioru danych [2]	Program, w którym przetwarzany jest zbiór danych [3]	Tryb uzyskiwania danych	Podmioty, którym dane są udostępniane (przekazywane)	Poziom bezpieczeństwa dla zbioru [4]	Zakres przetwarzanych danych	Klauzula tajności zbioru danych / klasyfikacja [5]
1.												
2.												

Załącznik Nr 11
do Zarządzenia Nr 23/2017
Dyrektora Centrum
Usług Wspólnych w Kobylnicy
z dnia 10.05.2017 r.

……
(Sygnatura dokumentu lub inne oznaczenie)

UPOWAŻNIENIE

DO PRZETWARZANIA DANYCH OSOBOWYCH
CENTRUM USŁUG WSPÓLNYCH W KOBYLNICY

Na podstawie art. 37 Ustawy z dnia 29 sierpnia 1997 o ochronie danych osobowych (tj. Dz. U. z 2015 r., poz. 2281, z późn. zmianami)

U P O W A Ż N I A M

Pana – ***Jana Kowalskiego s. Jana***
PESEL 62051206910

Imię i Nazwisko

do przetwarzania danych osobowych gromadzonych w zbiorach
„rejestr wydanych decyzji nakładających świadczenia osobiste i rzeczowe"
oraz
„***rejestr wniosków o nałożenie świadczeń osobistych i rzeczowych"***

w zakresie ***wprowadzania i dokonywania uaktualnień w zbiorze,***

Upoważnienie nadaje się na okres zatrudnienia ***na stanowisku – ……..***

umowa o pracę na czas nieokreślony

POUCZENIE
zgodnie z treścią art. 39 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2015 r. poz. 2281 ze zm.) zobowiązuje się osobę upoważnioną do przetwarzania danych do zachowania w tajemnicy przetwarzanych danych osobowych oraz sposobów ich zabezpieczenia.

……
(imię i nazwisko administratora danych osobowych)

Centrum Usług Wspólnych w Kobylnicy

Rok-miesiąc-dzień

Data i podpis upoważnionego	Potwierdzam, że zostałam zapoznana z przepisami ustawy o ochronie danych osobowych oraz stosowanymi sposobami ich zabezpieczenia

Data przyjęcia wniosku oraz podpis osoby prowadzącej ewidencję osób upoważnionych do przetwarzania danych	

Upoważnienie cofnięto dnia:

Data i podpis	