Powiatowe Centrum Usług Wspólnych
w Międzychodzie
ul. 17 Stycznia 14B, 64-400 Międzychód

ZARZĄDZENIE NR PCUW-9/2017

Dyrektora Powiatowego Centrum Usług Wspólnych
w Międzychodzie
z dnia 4 maja 2017 r.

w sprawie wprowadzenia Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Powiatowym Centrum Usług Wspólnych w Międzychodzie

Na podstawie art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.) oraz 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. z 2004 r., Nr 100, poz. 1024), zarządzam, co następuje:

§ 1. Wprowadza się w życie Politykę Bezpieczeństwa oraz Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Powiatowym Centrum Usług Wspólnych w Międzychodzie, stanowiące odpowiednio Załącznik Nr 1 oraz Załącznik Nr 2 do Zarządzenia.

§ 2. Wszystkich pracowników zatrudnionych w Powiatowym Centrum Usług Wspólnych w Międzychodzie zobowiązuje się do zapoznania się i przestrzegania postanowień wynikających z załączników określonych w § 1.

§ 3. Zarządzenie wchodzi w życie z dniem z dniem podpisania.

DYREKTOR
Powiatowego Centrum Usług Wspólnych
w Międzychodzie
mgr Dariusz Nowak

Załącznik nr 1
do Zarządzenia nr .....

z dnia.....

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W POWIATOWYM CENTRUM USŁUG WSPÓLNYCH W MIĘDZYCHODZIE

POSTANOWIENIA OGÓLNE

§ 1.

Polityka bezpieczeństwa, zwana dalej Polityką została opracowana w związku z wymaganiami zawartymi w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101 poz. 926, z późn. zm.) 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 (Dz. U. z 2004 r. Nr 100, poz. 1024) zwanym dalej rozporządzeniem.

§ 2.

Polityka określa tryb i zasady ochrony danych osobowych przetwarzanych w Powiatowym Centrum Usług Wspólnych w Międzychodzie.

§ 3.

Ilekroć w Polityce jest mowa o :

1) **Centrum** - rozumie się przez to Powiatowe Centrum Usług Wspólnych w Międzychodzie;

2) **Jednostce organizacyjnej lub jednostce** – rozumie się przez to Powiatowe Centrum Usług Wspólnych w Międzychodzie lub obsługiwane przez Centrum szkoły lub placówki;

3) **zbiorze 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;

4) **danych osobowych** - rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;

5) **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;

6) **systemie informatycznym** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;

7) **systemie tradycyjnym** - rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji w celu przetwarzania danych osobowych na papierze;

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) **usuwaniu danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

10) **Dyrektorze Centrum** – rozumie się przez to Dyrektora Powiatowego Centrum Usług Wspólnych w Międzychodzie;

11) **Administratorze Danych Osobowych** zwanym też **Administratorem Danych (ADO)** -w świetle art. 3 i 7 pkt 4 ustawy o ochronie danych osobowych rozumie się przez to kierownika jednostki, który decyduje o celach i środkach przetwarzania danych osobowych;

12) **Administratorze Bezpieczeństwa Informacji** zwanym też **Administratorem Bezpieczeństwa (ABI)** - rozumie się przez to osobę wyznaczoną przez kierownika jednostki, 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;

13) **Administratorze Systemu Informatycznego** zwanym też **Administratorem Systemu (ASI)** - rozumie się przez to osobę lub osoby zatrudnione przez kierownika jednostki upoważnione do realizacji zadań związanych z zarządzaniem systemem informatycznym;

14) **użytkowniku systemu** zwanym też **użytkownikiem systemu informatycznego** - rozumie się przez to upoważnionego przez kierownika jednostki, wyznaczonego do przetwarzania danych osobowych w systemie informatycznym pracownika, który został zaznajomiony ze stosownymi przepisami prawa oraz dokumentami wewnętrznymi dotyczącymi ochrony tych danych;

15) **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;

16) **ustawie** - rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101 poz. 926, z późn. zm.);

17) **Polityce** – rozumie się przez to niniejszy dokument;

18) **Instrukcji** – rozumie się przez to „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Powiatowym Centrum Usług Wspólnych w Międzychodzie;" opracowaną na podstawie przepisów ustawy i rozporządzenia.

Rozdział I
CELE

§ 4.

Dane osobowe w Centrum są gromadzone, przechowywane, edytowane, archiwizowane w rejestrach, wykazach, księgach, aktach osobowych, zestawieniach oraz w innych zestawach i zbiorach na dokumentach papierowych, jak również w systemach informatycznych na elektronicznych nośnikach informacji.

§ 5.

Polityka bezpieczeństwa wprowadza regulacje w zakresie zasad organizacji procesu przetwarzania danych osobowych i odnosi się swoją treścią do informacji:

1) **w formie papierowej** - przetwarzanej w ramach systemu tradycyjnego;

2) **w formie elektronicznej** - przetwarzanej w ramach systemu informatycznego.

§ 6.

Celem opracowania Polityki bezpieczeństwa jest ochrona danych osobowych przed niepowołanym dostępem do zgromadzonych i przetwarzanych danych.

§ 7.

Procedury i zasady określone w niniejszej Polityce bezpieczeństwa stosuje się do wszystkich pracowników Centrum, jak i innych osób mających dostęp do danych osobowych przetwarzanych w Centrum (np. osób realizujących zadania na podstawie umów zlecenia lub o dzieło, stażystów, praktykantów, serwisantów).

§ 8.

Przetwarzanie danych osobowych jest zgodne z prawem wyłącznie w celach i na zasadach określonych w Rozdziale 3 (Art. 23-31a) ustawy

§ 9.

Bezpośredni nadzór nad przetwarzaniem danych osobowych sprawuje Dyrektor Centrum.

§ 10.

1. Z zasadami w Polityce bezpieczeństwa obowiązkowo są zapoznawani wszyscy użytkownicy systemów tradycyjnych i informatycznych.
2. Potwierdzeniem zapoznania z Polityką jest złożenie odpowiedniego oświadczenia, którego wzór stanowi załącznik nr 1 do niniejszej Polityki.
3. Oświadczenia przechowywane są w aktach osobowych pracownika.

§ 11.

1. Do informacji przechowywanych w systemach tradycyjnych jak i informatycznych posiadają dostęp jedynie osoby mające imienne zarejestrowane upoważnienie, którego wzór stanowi załącznik nr 2 do niniejszej polityki.
2. Wszyscy pracownicy zobowiązani są do zachowania tych danych w tajemnicy. Dopuszczalny sposób i zakres przetwarzania danych osobowych regulują zapisy ustaw kompetencyjnych, właściwych dla zakresu działania Zespołu.
3. Upoważnienia określone w ust. 1 przechowywane są w aktach osobowych pracownika.
4. Ewidencję osób biorących udział w przetwarzaniu danych osobowych prowadzi stanowisko do spraw kadr.
5. Wzór ewidencji określonej w ust. 4 stanowi załącznik nr 3 do Polityki bezpieczeństwa.

§ 12.

1. Stosowne uprawnienia do przetwarzania danych osobowych nadaje Administrator Bezpieczeństwa Danych, za pośrednictwem stanowiska do spraw kadr.
2. Upoważnienia zawierają listę zbiorów danych osobowych do których dostęp jest niezbędny pracownikowi zgodnie z jego zakresem obowiązków

§ 13.

1. Dane osobowe są chronione zgodnie z polskim prawem oraz procedurami obowiązującymi w Centrum dotyczącymi bezpieczeństwa i poufności przetwarzanych danych.
2. Systemy informatyczne oraz tradycyjne, które przechowują dane osobowe, są chronione środkami technicznymi adekwatnymi do kategorii danych oraz występujących zagrożeń.

Rozdział II
ADMINISTRACJA I ORGANIZACJA BEZPIECZEŃSTWA

§ 14.

1. Za bezpieczeństwo i organizację przetwarzania danych osobowych odpowiada Administrator Danych Osobowych.
2. Pracownicy Centrum obowiązani są zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinni zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

§ 15.

Administrator Danych Osobowych wyznacza Administratora Bezpieczeństwa Informacji, nadzorującego przestrzeganie zasad ochrony. Prowadzi on dokumentację opisującą sposób

przetwarzania danych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

§ 16.

1. Administrator Bezpieczeństwa Informacji wykonuje wszystkie prace niezbędne do efektywnego oraz bezpiecznego zarządzania systemami informatycznymi oraz systemem tradycyjnym.
2. Administrator Bezpieczeństwa Informacji jest zobowiązany do zapewnienia, poprzez zastosowanie odpowiednich środków i metod kontroli dostępu, tak by wyłącznie uprawniony użytkownik miał dostęp do systemów informatycznych oraz systemu tradycyjnego.
3. Administrator Bezpieczeństwa Informacji posiada wgląd do ewidencji osób upoważnionych do przetwarzania danych osobowych.
4. Do zakresu odpowiedzialności i obowiązków Administratora Bezpieczeństwa Informacji należy:
   1) nadzór nad bezpieczeństwem systemów informatycznych i systemu tradycyjnego;
   2) nadzór nad przestrzeganiem przez wszystkich użytkowników stosowania obowiązujących procedur;
   3) weryfikacja ewidencji o której mowa § 11 ust. 4 oraz kont dostępowych użytkowników systemu informatycznego;
   4) doradztwo użytkownikom w zakresie bezpieczeństwa;
   5) dbanie, aby dostęp do systemu posiadali użytkownicy mający stosowne zezwolenia oraz przeszkoleni w zakresie stosowania obowiązujących procedur bezpieczeństwa;
   6) prowadzenie postępowań wyjaśniających w przypadku naruszenia ochrony danych osobowych,

§ 17.

1. Administrator Danych Osobowych wyznacza Administratora Systemu Informatycznego, który posiada najwyższe uprawnienia w systemie informatycznym. Tylko ASI jest osobą uprawnioną do instalowania i usuwania oprogramowania systemowego oraz narzędziowego.
2. Administrator Systemu Informatycznego wykonuje wszystkie prace niezbędne do efektywnego oraz bezpiecznego zarządzania systemem informatycznym. Jest zobowiązany do zapewnienia, poprzez zastosowanie odpowiednich środków i metod kontroli dostępu, że wyłącznie uprawniony użytkownik ma dostęp do systemów informatycznych.
3. Do zakresu odpowiedzialności i obowiązków Administratora Systemu Informatycznego należy:
   1) zapewnianie stałej sprawności urządzeń mających wpływ na bezpieczeństwo danych;
   2) odpowiadanie za bezpieczeństwo systemu informatycznego;

3) zobowiązywanie i bieżąca kontrola stosowania się użytkowników do obowiązujących procedur;

4) utrzymywanie i aktualizowanie kont użytkowników systemu informatycznego;

5) zapewnianie aktualizacji dokumentacji technicznej systemu w tym opis struktur zbiorów i ich zależności;

6) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisywane są dane osobowe;

7) wykonywanie kopii awaryjnych/archiwalnych oraz nadzór nad ich przechowywaniem;

8) wprowadzanie i nadzór nad mechanizmami autoryzacji.

§ 18.

Administrator danych osobowych odpowiada za przestrzeganie ustawy o ochronie danych oraz przepisów wewnętrznych na poszczególnych stanowiskach, a w szczególności:

1) kontroluje sposób zabezpieczenia zbiorów danych osobowych przez pracowników, ze szczególnym uwzględnieniem zbiorów tradycyjnych (papierowych);

2) kontroluje sposób realizacji obowiązku udzielania informacji o jakich mowa w ustawie;

3) zgłasza ABI planowaną rejestrację nowych zbiorów oraz przygotowuje wniosek w tej sprawie, wzór wniosku stanowi załącznik nr 4 do Polityki;

4) nadaje upoważnienia do przetwarzania danych osobowych pracownikom, wzór wniosku stanowi załącznik nr 2 do Polityki;

5) zgłasza potrzeby w zakresie zabezpieczenia danych osobowych w Centrum;

§ 19.

Użytkownik systemu wykonuje wszystkie prace niezbędne do efektywnej oraz bezpiecznej pracy na stanowisku pracy również z wykorzystaniem komputerowej stacji roboczej. Jest odpowiedzialny przed Administratorem Bezpieczeństwa Informacji za implementację i utrzymanie niezbędnych warunków bezpieczeństwa, w szczególności do przestrzegania procedur dostępu do systemu i ochrony danych osobowych.

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

§ 20.

1. Dane osobowe są gromadzone, przechowywane i przetwarzane w rejestrach, wykazach, księgach, aktach osobowych, zestawieniach oraz w innych zestawach i zbiorach na dokumentach papierowych, jak również w systemach informatycznych, w którym stosowane są pakiety biurowe lub wyspecjalizowane aplikacje (programy).

2. Zestawienie zbiorów danych osobowych oraz programów do przetwarzania tych danych stanowi załącznik nr 5 do polityki bezpieczeństwa.

§ 21.

Ze względu na rodzaj i charakter danych osobowych zawartych w zbiorach, w Centrum wyróżnia się dwie kategorie danych:

1) dane osobowe zwykłe - wszelkie dane (informacje) dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, zgromadzone w zbiorach danych osobowych;

2) dane osobowe wrażliwe - zgodnie z katalogiem zawartym w treści ustawy o ochronie danych osobowych (art. 27 ust. 1) wszelkie dane (informacje) ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne, przynależność partyjną lub związkową, jak również informacje o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazania osoby, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

§ 22.

Zgodnie z postanowieniami art. 40 ustawy o ochronie danych osobowych, z uwagi na rodzaj gromadzonych danych osobowych istnieje obowiązek zgłoszenia do rejestracji tych zbiorów Generalnemu Inspektorowi Ochrony Danych Osobowych z wyjątkiem przypadków, o których mowa w art. 43 ust. 1 tejże ustawy.

Rozdział IV
SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

§ 23.

1. Obieg dokumentów zawierających dane osobowe, pomiędzy jednostkami organizacyjnymi obsługiwanymi przez Centrum a pracownikami Centrum, winien się odbywać w sposób zapewniający pełną ochronę przed ujawnieniem zawartych w tych dokumentach danych (informacji).

2. Przekazywanie informacji (danych) w systemie informatycznym poza sieć lokalną Centrum odbywa się w relacji Centrum - jednostka organizacyjna, mieszkańcy, kontrahenci, zakład ubezpieczeń społecznych, urząd skarbowy, banki, urząd wojewódzki i inne jednostki administracji samorządowej i rządowej.

3. Bezwzględnie zabronione jest podłączanie urządzeń (w szczególności komputerów) innych niż służbowe do sieci wewnętrznej Centrum bez zgody i wiedzy ASI.

4. Bezwzględnie zabronione jest podłączanie do komputerów w sieci wewnętrznej urządzeń (takich jak modemy GPRS, 3G, LTE itp.) nawiązujących połączenia do sieci zewnętrznych (np. Plus, Era, Orange, Play, pozostałych sieci komórkowych, WiFi, WiMAX itp.).

Rozdział V
OKREŚLENIE ŚRODKÓW TECHNICZNYCH i ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

§ 24.

1. Dostęp do danych wprowadzonych przez użytkowników systemów informatycznych mają jedynie upoważnione osoby oraz Administratorzy Systemu Informatycznego zapewniający jego prawidłową eksploatację.
2. Pomieszczenia, w których przetwarza się dane osobowe powinny być fizycznie zabezpieczone przed dostępem osób nieuprawnionych, to znaczy posiadać odpowiednie zamki do drzwi, zabezpieczenia w oknach (w szczególności na parterze) oraz być wyposażone w środki ochrony ppoż.
3. W pomieszczeniach gdzie przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób by uniemożliwić tym osobom wgląd w dane osobowe.
4. Dokumenty i nośniki informacji, zawierające dane osobowe powinny być zabezpieczone przed dostępem osób nieupoważnionych do przetwarzania danych. Jeśli nie są aktualnie używane powinny być przechowywane w szafach lub w innych przeznaczonych do tego celu urządzeniach biurowych, posiadających odpowiednie zabezpieczenia.

Rozdział VI
UDOSTĘPNIANIE POSIADANYCH W ZBIORZE DANYCH OSOBOWYCH

§ 25.

1. Na wniosek osoby, której dane dotyczą, ADO 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. Na wniosek osoby, której dane dotyczą, informacji, o których mowa w ust. 1, udziela się na piśmie.

§ 26.

1. Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach Centrum, a zwłaszcza prawo do:

1) uzyskania wyczerpującej informacji, czy taki zbiór istnieje, oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy;

2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze;

3) uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące, oraz podania w powszechnie zrozumiałej formie treści tych danych;

4) uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące;

5) uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane;

6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane;

7) wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację, jeżeli nawet przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą;

8) wniesienia sprzeciwu wobec przetwarzania jej danych, również danych niezbędnych administratorowi do wykonania określonych prawem zadań realizowanych dla dobra publicznego lub niezbędnych dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratora danych albo odbiorców danych, jeśli administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych;

9) wniesienia do administratora danych żądania ponownego, indywidualnego rozpatrzenia sprawy rozstrzygniętej z naruszeniem zakazu ostatecznego rozstrzygnięcia indywidualnej sprawy, gdy treść była wyłącznie wynikiem operacji na danych osobowych prowadzonych w systemie informatycznym.

2. Osoba zainteresowana może skorzystać z prawa do informacji, o których mowa w art.32 ust. 1 pkt 1-5 ustawy, nie częściej niż raz na 6 miesięcy.

§ 27.

1. W razie wykazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, administrator danych jest obowiązany, bez zbędnej zwłoki, do uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, chyba że dotyczy to danych osobowych, w odniesieniu do których tryb ich uzupełnienia, uaktualnienia lub sprostowania określają odrębne ustawy.

2. Każda z osób zatrudnionych przy przetwarzaniu danych w razie powzięcia takiej wiadomości ma obowiązek, o wystąpieniu osoby której dane dotyczą, poinformować administratora danych.

§ 28.

1. Do udostępniania posiadanych w zbiorze danych osobowych upoważniony jest Dyrektor Centrum lub pracownik posiadający wymagane prawem upoważnienie.
2. Administrator danych udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

§ 29.

Powierzenie przetwarzania danych osobowych (to jest wglądu, modyfikacji lub usuwania zgromadzonych danych) innemu podmiotowi może nastąpić wyłącznie w drodze umowy zawartej w formie pisemnej przez Administratora Danych Osobowych.

Rozdział VII
ZACHOWANIE BEZPIECZEŃSTWA PRZEZ UŻYTKOWNIKÓW SYSTEMU

§ 30.

Użytkownicy systemu zobowiązani są stosować odpowiednie środki bezpieczeństwa w pomieszczeniach, w których zainstalowano sprzęt systemu informatycznego by nie spowodować jego uszkodzenia.

§ 31.

1. Wszyscy użytkownicy systemu muszą stosować się do obowiązujących procedur bezpieczeństwa.
2. Hasło użytkownika podlega szczególnej ochronie. Użytkownik ma obowiązek tworzenia haseł. W przypadku, gdy użytkownik zapomni swoje hasło, może on odnowić hasło w porozumieniu z Administratorem Systemu Informatycznego.

Rozdział VIII
BEZPIECZEŃSTWO FIZYCZNE

§ 32.

1. Dane osobowe, które są przedmiotem zainteresowania ustawy o ochronie danych osobowych, gromadzone i przechowywane są w systemie komputerowym oraz w postaci akt.
2. Środki bezpieczeństwa fizycznego są konieczne dla zapobiegania niepowołanemu dostępowi do informacji, nieautoryzowanym operacjom w systemie, kontroli dostępu do zasobów oraz w celu zabezpieczenia sprzętu teleinformatycznego.

§ 33.

1. Obszar przetwarzania danych osobowych w Centrum obejmuje pomieszczenia wymienione w załączniku nr 7 do Polityki.

2. Przetwarzanie danych poza obszarem określonym w ust. 1 jest zabronione.

3. Przenoszenie wydruków komputerowych oraz akt pomiędzy pomieszczeniami wymienionymi w załączniku nr 7 należy wykonywać w sposób uniemożliwiający wgląd do dokumentów.

4. Surowo zabronione jest pozostawianie jakichkolwiek wydruków w pomieszczeniach ogólnodostępnych bez nadzoru (np. „*ksero*", korytarze, pomieszczenia socjalne), niedopełnienie tego obowiązku uważa się za ciężkie naruszenie obowiązków pracowniczych.

§ 34.

Pomieszczenia, w których znajdują się akta lub systemy służące do przetwarzania danych osobowych winny być:

1) wyposażone w szafy zamykane na klucz umożliwiające przechowywanie dokumentów, w sposób zabezpieczający przed dostępem osób nieposiadających stosownych upoważnień,
2) zamknięte, jeśli nikt w nich nie przebywa.

§ 35.

Instalacja urządzeń systemu i sieci teleinformatycznej odbywa się za wiedzą i pod kontrolą Dyrektora Centrum, który jest również odpowiedzialny za warunki wprowadzania do użycia, przechowywania, eksploatacji oraz wycofywania z użycia każdego urządzenia.

Dział IX
BEZPIECZEŃSTWO SPRZĘTU I OPROGRAMOWANIA

§ 36.

Sprzęt i oprogramowanie, indywidualnie lub łącznie mają ścisły związek z bezpieczeństwem systemu i sieci teleinformatycznej. Dlatego, powinny być ściśle przestrzegane procedury bezpieczeństwa odnoszące się do tych elementów.

§ 37.

Sieć teleinformatyczna jest organizacyjnym i technicznym połączeniem systemów teleinformatycznych wraz z łączącymi je urządzeniami i liniami telekomunikacyjnymi. Niedopuszczalne jest samowolne przemieszczanie lub zmiana konfiguracji stacji roboczej bez wiedzy i zgody kierownika komórki organizacyjnej oraz ASI.

§ 38.

Nie zezwala się na korzystanie z jakiegokolwiek nowego oprogramowania bez zgody Administratora Systemu Informatycznego.

§ 39.

1. Dostęp do zbiorów danych osobowych znajdujących się na serwerach następuje po wprowadzeniu hasła, które znane jest tylko osobie przetwarzającej dane.

2. Każdorazowo po dokonaniu przetworzenia aplikacja powinna być zamknięta.

3. W przypadku podejrzenia, iż wiadomości o sposobie dostępu do elektronicznej bazy danych uzyskała osoba do tego niepowołana (podejrzenie ujawnienia hasła), osoba przetwarzającej dane powinna niezwłocznie dokonać zmiany hasła.
4. Komputery za pomocą których uzyskiwany jest dostęp do zbiorów danych osobowych chronione są osobnym hasłem.
5. W przypadku opuszczenia stanowiska pracy użytkownik ma obowiązek zabezpieczyć stanowisko komputerowe przed dostępem (uruchomić wygaszacz ekranu lub wylogować się z systemu).
6. Użytkownik ma obowiązek zmiany haseł nie rzadziej niż co 30 dni, szczegółowe zasady tworzenia haseł określa Instrukcja.

§ 40.

1. Elektroniczne bazy danych osobowych są archiwizowane.
2. Kopie są wykonywane na nośnikach danych lub w magazynach dyskowych do tego przeznaczonych.
3. Szczegółowe zasady tworzenia kopii zapasowych określa Instrukcja.

§ 41.

Używanie oprogramowania prywatnego w sieci jest kategorycznie zabronione. Na stacjach roboczych powinno być zainstalowane jedynie oprogramowanie niezbędne do wykonywania wyznaczonego zakresu obowiązków.

Rozdział X
KONSERWACJE I NAPRAWY

§ 42.

Każde urządzenie użytkowane w systemie informatycznym, powinno podlegać rutynowym czynnościom konserwacyjnym oraz przeglądom wykonywanym przez uprawnione osoby.

§ 43.

Za konserwację oprogramowania systemowego oraz aplikacyjnego systemu informatycznego odpowiedzialny jest Administrator Systemu Informatycznego. Konserwacja oprogramowania obejmuje także jego aktualizację.

§ 44.

Administrator Systemu Informatycznego przed rozpoczęciem naprawy urządzenia przez zewnętrzne firmy sprawdza, czy spełnione są następujące wymagania:

1) w przypadku awarii serwera i konieczności oddania sprzętu do serwisu, nośniki magnetyczne zawierające dane osobowe powinny być wymontowane i do czasu naprawy serwera przechowywane w szafie metalowej znajdującej się w strefie o ograniczonym dostępie lub w sejfie do którego dostęp ma Dyrektor Centrum oraz ASI;

2) w przypadku uszkodzenia nośnika magnetycznego zawierającego dane osobowe należy komisyjnie dokonać jego zniszczenia.

Dział XI
PLANY AWARYJNE I ZAPOBIEGAWCZE

§ 45.

Serwer systemu oraz poszczególne stacje robocze (opcjonalnie) powinny być zabezpieczone urządzeniami podtrzymującymi zasilanie (UPS), znacząco obniży ryzyko awarii systemu w przypadku awarii zasilania.

§ 46.

W celu zabezpieczenia ciągłości pracy, informacja przechowywana i przetwarzana w systemie podlega codziennej, automatycznej archiwizacji oraz pełnej archiwizacji przeprowadzanej nie rzadziej niż raz na tydzień. Kopie archiwalne danych są wykonywane na nośnikach danych lub w magazynach dyskowych. Użycie kopii zapasowych następuje w przypadku odtwarzania systemu po awarii.

§ 47.

Administrator Systemu Informatycznego okresowo kontroluje poprawność kopii zapasowych oraz przydatność do odtworzenia systemu po awarii.

§ 48.

W przypadku wykrycia problemów z odtworzeniem danych z kopi zapasowej ASI niezwłocznie zawiadamia ABI o wykrytym problemie w celu opracowania nowych procedur wykonywania kopii zapasowych, uwzględniających rozwiązanie wykrytego problemu.

Rozdział XII
POLITYKA ANTYWIRUSOWA

§ 49.

1. Wszystkie komputery są sprawdzane przy użyciu oprogramowania do wykrywania i usuwania wirusów komputerowych.
2. W zakresie ochrony antywirusowej wprowadza się następujące zalecenia:
   1) nie należy używać oprogramowania na stacji roboczej innego niż zaleca Administrator Systemu Informatycznego;
   2) zabrania się instalowania oprogramowania typu „freeware" lub „shareware" oraz nieznanego pochodzenia bez zgody i wiedzy Administratora Systemu Informatycznego;
   3) przed użyciem nośnika danych sprawdzić czy nie jest zainfekowany wirusem komputerowym.

3. W przypadku jakichkolwiek wątpliwości odnośnie zagrożenia wirusowego należy sprawdzić zawartość całego dysku twardego programem antywirusowym. W przypadku dalszych niejasności należy kontaktować się z Administratorem Systemu Informatycznego.

Rozdział XIII
PRZEPISY KOŃCOWE

§ 50.

Celowe lub nieumyślne naruszenie obowiązków wynikających z niniejszej Polityki Bezpieczeństwa oraz przepisów ustawy może być uznane za ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym w szczególności wynikającym z przepisów tejże ustawy art.49-54a tj: grzywnie, karze ograniczenia wolności albo pozbawienia wolności od roku do lat trzech w zależności od wagi naruszenia

§ 51.

W sprawach nie uregulowanych w niniejszej Polityce bezpieczeństwa informacji mają zastosowanie przepisy ustawy oraz 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. z 2004 r. Nr 100, poz. 1024)

§ 52.

Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce, w wypadku odrębnych od zawartych w niniejszej Polityce uregulowań występujących w innych procedurach obowiązujących w Jednostce, użytkownicy mają obowiązek stosowania unormowań dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych.

§ 53.

Niniejszy dokument jest dokumentem wewnętrznym i nie może być udostępniany osobom postronnym w żadnej formie.

Załącznik 1
do polityki bezpieczeństwa przetwarzania danych osobowych w PCUW w Międzychodzie

OŚWIADCZENIE PRACOWNIKA

Ja niżej podpisana (*ny*) oświadczam, że:

1. Zostałam (*em*) przeszkolona (*ny*) w zakresie ochrony danych osobowych i znana jest mi treść ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych tj. Dz. U. z 2002 r. nr 101, poz. 926 z późn. zm. oraz **„Polityką bezpieczeństwa przetwarzania danych osobowych w PCUW w Międzychodzie**

2. Zobowiązuję się:
   a. zachować w tajemnicy dane osobowe, z którymi zetknęłam się / zetknąłem się* w trakcie wykonywania swoich obowiązków służbowych, zarówno w czasie trwania stosunku pracy, jak i po jego ustaniu;
   b. chronić dane osobowe przed dostępem do nich osób do tego nieupoważnionych, zabezpieczać je przed zniszczeniem i nielegalnym ujawnieniem.
3. Znana jest mi odpowiedzialność karna za naruszenie ww. ustawy (art. 49-54).
4. Zobowiązuje się do przestrzegania Polityką bezpieczeństwa przetwarzania danych osobowych w PCUW w Międzychodzie

.....
(podpis Pełnomocnika Lokalnego Administratora Danych)

.....
(data, podpis pracownika)

Uwaga:
- niniejsze oświadczenie zostało sporządzone w trzech jednobrzmiących egzemplarzach – każdy na prawach oryginału, które otrzymują:
1. Osoba upoważniona;
2. Kadry a/a
3. Administrator Danych.

*) *niepotrzebne skreślić.*

Załącznik 2
do polityki bezpieczeństwa przetwarzania danych osobowych w PCUW w Międzychodzie

Nr ewidencyjny: .... *(nadaje Pełnomocnik Danych Osobowych)* *(miejscowość) (data)*

UPOWAŻNIENIE
do przetwarzania danych osobowych

I.

Upoważniam Panią/Pana .....
(imię i nazwisko)

zatrudnioną/zatrudnionego w .....
(nazwa komórki organizacyjnej)

.....

do przetwarzania danych osobowych, w celach związanych z wykonywaniem obowiązków na

stanowisku: .....
(zajmowane stanowisko)

oraz do obsługi systemu informatycznego i urządzeń wchodzących w jego skład.

Niniejsze upoważnienie obejmuje przetwarzanie danych osobowych w formie tradycyjnej (kartoteki, ewidencje, rejestry, spisy itp.*) i elektronicznej, wg wykazu zbiorów podanych w pkt. II.

II.

Upoważniam Panią/Pana do przetwarzania danych osobowych zawartych w następujących zbiorach:

1. .....

2. .....

3. .....

4. .....

5. .....

6. .....

7. .....

.....
(podpis Lokalnego Administratora Danych Osobowych)

Załącznik nr 3

do polityki bezpieczeństwa przetwarzania
danych osobowych w PCUW w Międzychodzie

Ewidencja osób upoważnionych do przetwarzania danych osobowych.

L.p.	Imię i nazwisko (1)	Data nadania upoważnienia (2)	Data ustania upoważnienia (3)	Zakres upoważnienia (4)	Login/identyfikator - system	Uwagi/podpis ASI
1	Małgorzata Weimann	03.07.2017 r.				
2	Bogusława Zielonka	03.07.2017 r.				
3	Justyna Plewa	03.07.2017 r.				
4	Beata Zimecka	03.07.2017 r.				
5	Monika Szymanek	03.07.2017 r.				
6	Mikołaj Konopiński	01.09.2017 r.				

Zakres upoważnienia: d - wgląd; w - wprowadzanie; m - modyfikacja; u - usuwanie.

.....
(podpis prowadzącego ewidencję w zakresie kol. 1-4)

ZGŁOSZENIE ZBIORU DANYCH DO REJESTRACJI GENERALNEMU INSPEKTOROWI OCHRONY DANYCH OSOBOWYCH

* ☐ – zgłoszenie zbioru na podstawie art. 40 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 i Nr 153, poz. 1271 oraz z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285),
* ☐ – zgłoszenie zmian na podstawie art. 41 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,
* ☐ – zgłoszenie zbioru, w którym będą przetwarzane dane określone w art. 27 ust. 1 ustawy z dnia 29 sierp–nia 1997 r. o ochronie danych osobowych.

Nr .....
(nadaje urzędnik Biura GIODO)

Część A. Wniosek

Wnoszę o wpisanie zbioru danych osobowych o nazwie:

.....

do Rejestru Zbiorów Danych Osobowych.

Część B. Charakterystyka administratora danych

1. Wnioskodawca (administrator danych):

.....
.....
.....

(nazwa administratora danych i adres jego siedziby lub nazwisko, imię i adres miejsca zamieszkania wnioskodawcy oraz nr REGON)

2. Przedstawiciel Wnioskodawcy, o którym mowa w art. 31a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych:

.....
.....
.....

(nazwa przedstawiciela administratora danych i adres jego siedziby lub nazwisko, imię i adres miejsca zamieszkania)

3. Powierzenie przetwarzania danych osobowych:

* ☐ – administrator danych powierzył w drodze umowy zawartej na piśmie przetwarzanie danych innemu podmiotowi (art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych),
* ☐ – administrator danych przewiduje powierzenie przetwarzania danych innemu podmiotowi.

W przypadku powierzenia przetwarzania danych innemu podmiotowi podaj nazwę i adres siedziby lub nazwisko, imię i adres miejsca zamieszkania podmiotu, któremu powierzono przetwarzanie danych osobowych:

.....
.....
.....
..... * ☐ *ew. cd. w załączniku nr*

4. Podstawa prawna upoważniająca do prowadzenia zbioru danych:

* ☐ – zgoda osoby, której dane dotyczą, na przetwarzanie danych jej dotyczących,
* ☐ – przetwarzanie jest niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa

.....
.....
.....
..... * ☐ *ew. cd. w załączniku nr*

* ☐ – przetwarzanie jest konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,

* ☐ – przetwarzanie jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego – jeśli TAK, to opisz te zadania:

.....
.....
.....
..... * ☐ *ew. cd. w załączniku nr*

* ☐ – przetwarzanie jest niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Część C. Cel przetwarzania danych, opis kategorii osób, których dane dotyczą, oraz zakres przetwarzanych danych

5. Cel przetwarzania danych w zbiorze:

.....
.....
.....
..... * ☐ *ew. cd. w załączniku nr*

6. Opis kategorii osób, których dane dotyczą:

.....
.....
.....

7. Zakres przetwarzanych w zbiorze danych o osobach:

* ☐ – nazwiska i imiona,
* ☐ – imiona rodziców,
* ☐ – data urodzenia,
* ☐ – miejsce urodzenia,
* ☐ – adres zamieszkania lub pobytu,
* ☐ – numer ewidencyjny PESEL,
* ☐ – Numer Identyfikacji Podatkowej,
* ☐ – miejsce pracy,
* ☐ – zawód,
* ☐ – wykształcenie,
* ☐ – seria i numer dowodu osobistego,
* ☐ – numer telefonu.

8. Inne dane osobowe, oprócz wymienionych w pkt 7, przetwarzane w zbiorze – *należy podać jakie*:

.....
.....
.....
..... * ☐ *ew. cd. w załączniku nr*

9. Dane przetwarzane w zbiorze:

a) ujawniają bezpośrednio lub w kontekście:

* ☐ – pochodzenie rasowe,
* ☐ – pochodzenie etniczne,
* ☐ – poglądy polityczne,
* ☐ – przekonania religijne,
* ☐ – przekonania filozoficzne,
* ☐ – przynależność wyznaniową,
* ☐ – przynależność partyjną,
* ☐ – przynależność związkową,
* ☐ – stan zdrowia,
* ☐ – kod genetyczny,
* ☐ – nałogi,
* ☐ – życie seksualne,

b) dotyczą:

* ☐ – skazań,
* ☐ – mandatów karnych,
* ☐ – orzeczeń o ukaraniu,
* ☐ – innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym

Jeśli nie zakreślono żadnej odpowiedzi, należy przejść od razu do pkt 11.

10. Podstawa prawna przetwarzania danych wskazanych w pkt 9:

* ☐ – osoby, których dane dotyczą, będą wyrażać na to zgodę na piśmie,
* ☐ – przepis szczególny innej ustawy zezwala na przetwarzanie bez zgody osoby, której dane dotyczą, jej danych osobowych – jeśli TAK, to podaj odniesienie do przepisu tej ustawy:

.....
.....
.....
..... * ☐ *ew. cd. w załączniku nr*

* ☐ – przetwarzanie danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora,
* ☐ – przetwarzanie jest niezbędne do wykonania statutowych zadań kościoła, innego związku wyznaniowego, stowarzyszenia, fundacji lub innej niezarobkowej organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, a przetwarzanie danych dotyczy wyłącznie członków tej organizacji lub instytucji albo osób utrzymujących z nią stałe kontakty w związku z jej działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych – jeśli TAK, to podaj jakich:

.....
.....
.....
..... * ☐ *ew. cd. w załączniku nr*

* ☐ – przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem,
* ☐ – przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie,
* ☐ – przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych,
* ☐ – przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą,
* ☐ – przetwarzanie jest niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego, a publikowanie wyników badań naukowych uniemożliwia identyfikację osób, których dane zostały przetworzone,
* ☐ – przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

Część D. Sposób zbierania oraz udostępniania danych

11. Sposób zbierania danych do zbioru:

* ☐ – od osób, których dotyczą,

* ☐ – z innych źródeł niż osoba, której dane dotyczą,

12. Sposób udostępniania danych ze zbioru:

* ☐ – podmiotom innym niż upoważniona na podstawie przepisów prawa,

13. Odbiorcy lub kategorie odbiorców, którym dane mogą być przekazywane – należy *podać nazwę i adres siedziby lub nazwisko, imię i adres miejsca zamieszkania podmiotu, któremu dane mogą być przekazywane:*

.....

.....

.....

..... * ☐ *ew. cd. w załączniku nr*

14. Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego – *podaj nazwę państwa:*

.....

.....

.....

..... * ☐ *ew. cd. w załączniku nr*

Część E. Opis środków technicznych i organizacyjnych zastosowanych w celach określonych w art. 36–39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych

(w poniższych odpowiedziach proszę nie ujawniać szczegółów zastosowanych rozwiązań)

15. Zbiór danych osobowych będzie przetwarzany:

a) * ☐ – centralnie

* ☐ – w architekturze rozproszonej

b) * ☐ – wyłącznie w postaci papierowej

* ☐ – z użyciem systemu informatycznego

c) * ☐ – z użyciem co najmniej jednego urządzenia systemu informatycznego służącego do przetwarzania danych osobowych połączonego z siecią publiczną (np. Internetem),

* ☐ – bez użycia żadnego z urządzeń systemu informatycznego służącego do przetwarzania danych osobowych połączonego z siecią publiczną (np. Internetem),

16. Zostały spełnione wymogi określone w art. 36–39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[1)]:

a) * ☐ – został wyznaczony administrator bezpieczeństwa informacji nadzorujący przestrzeganie zasad ochrony przetwarzania danych osobowych,

* ☐ – administrator danych sam wykonuje czynności administratora bezpieczeństwa informacji,

b) * ☐ – do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych,

c) * ☐ – prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych,

d) * ☐ – została opracowana i wdrożona polityka bezpieczeństwa.

e) * ☐ – została opracowana i wdrożona instrukcja zarządzania systemem informatycznym,

f) Inne środki, oprócz wymienionych w pkt. a – e, zastosowane w celu zabezpieczenia danych:

.....

.....

.....

..... * ☐ *ew. cd. w załączniku nr*

Część F. Informacja o sposobie wypełnienia warunków technicznych i organizacyjnych, o których mowa w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie doku–mentacji 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)

17. Zastosowano środki bezpieczeństwa na poziomie:

* ☐ – podstawowym,
* ☐ – podwyższonym,
* ☐ – wysokim.

.....

(data, podpis i pieczęć wnioskodawcy)

Objaśnienia:

* W przypadku odpowiedzi twierdzącej należy zakreślić kwadrat lilerą „X".

1) Administrator danych prowadzący zbiór w systemie tradycyjnym (papierowym) zobowiązany jest do zastosowariia środków określonych w pkt 15 ppkt a – d, a w przypadku prowadzenia zbioru w systemie informatycznym, ponadto środka określonego w pkt 16 ppkt e.

2) Należy wskazać odpowiedni poziom bezpieczeństwa określony w § 6 ww. rozporządzenia (UWAGA! Dotyczy wyłącznie administratorów przetwarzających dane w systemie informatycznym);

– jeżeli wnioskodawca przetwarza dane wymienione w pkt 9 zgłoszenia, należy zastosować środki bezpieczeństwa przynajmniej na poziomie podwyższonym;

– w przypadku gdy przynajmniej jedno urządzenie systemu informatycznego służącego do przetwarzania danych osobowych połączone jest z siecią publiczną należy stosować środki bezpieczeństwa na poziomie wysokim;
– w pozostałych przypadkach wystarczające jest zastosowanie środków bezpieczeństwa na poziomie podstawowym.

Zgłoszenia można dokonać drogą elektroniczną, za pomocą programu komputerowego umożliwiającego jego prawidłowe wypełnienie, dostępnego na stronie Intenetowej Generalnego Inspektora Ochrony Danych Osobowych.

Powiatowe Centrum Usług Wspólnych
w Międzychodzie
ul. 17 Stycznia 143, 64-400 Międzychód

Załącznik 5
do polityki bezpieczeństwa przetwarzania danych osobowych w PCUW w Międzychodzie

Zestawienie zbiorów danych osobowych oraz programów przeznaczonych do przetwarzania danych osobowych w Powiatowym Centrum Usług Wspólnych w Międzychodzie

Nazwa zbioru	Forma prowadzenia rejestru, nazwy systemów/programów **posiadających dostęp do zbioru**
Pracownicy placówek oświatowych	**zbiór elektroniczny** Kadry Płace Sigid, Progmann Arkusz Organizacyjny Wolters Kluwer
Osoby zgłoszone do ubezpieczeń społecznych	**zbiór elektroniczny** Płatnik
Kontrahenci placówek oświatowych	**zbiór elektroniczny** Księgowość

DYREKTOR
Powiatowego Centrum Usług Wspólnych
w Międzychodzie
mgr Dariusz Nowak

(podpis Administratora Danych)

Załącznik 6
do polityki bezpieczeństwa przetwarzania
danych osobowych w PCUW w Międzychodzie

Opis wymiany danych pomiędzy elektronicznymi systemami dziedzinowymi służącymi do przetwarzania danych osobowych w Powiatowym Centrum Usług Wspólnych w Międzychodzie.

Nazwa zbioru udostępniającego dane	Nazwa systemu/programu pobierającego dane oraz sposób wymiany danych
Kadry Płace Sigid	Płatnik – import danych System Bankowości Internetowej - import danych
Kadry Płace Progman	Płatnik – import danych System Bankowości Internetowej – import danych

---

(podpis Administratora Danych)

Załącznik 7
do polityki bezpieczeństwa
przetwarzania danych osobowych
w PCUW w Międzychodzie

Obszar przetwarzania danych osobowych w Powiatowym Centrum Usług Wspólnych w Międzychodzie

Obszar przetwarzania danych osobowych PCUW w Międzychodzie znajduje się w budynku w Międzychodzie, ul. 17 Stycznia 143 i obejmuje poniższy wykaz pomieszczeń:

I PIĘTRO

pok. 105 – pomieszczenie biurowe

pok. 106 – pomieszczenie biurowe,

II PIĘTRO

pok. 221 – pomieszczenie biurowe,

Przetwarzanie danych osobowych jest zabronione jeśli nie są spełnione warunki zdefiniowane w niniejszej Polityce.

(podpis Administratora Danych)

Powiatowe Centrum Usług Wspólnych
w Międzychodzie
ul. 17 Stycznia 143, 64-400 Międzychód

Załącznik 6
do polityki bezpieczeństwa przetwarzania
danych osobowych w PCUW w Międzychodzie

Opis wymiany danych pomiędzy elektronicznymi systemami dziedzinowymi służącymi do przetwarzania danych osobowych w Powiatowym Centrum Usług Wspólnych w Międzychodzie.

Nazwa zbioru udostępniającego dane	Nazwa systemu/programu pobierającego dane oraz sposób wymiany danych
Kadry Płace Sigid	Płatnik – import danych System Bankowości Internetowej - import danych
Kadry Płace Progman	Płatnik – import danych System Bankowości Internetowej – import danych

DYREKTOR
Powiatowego Centrum Usług Wspólnych
w Międzychodzie
mgr Dariusz Nowak
(podpis Administratora Danych)

Powiatowe Centrum Usług Wspólnych
w Międzychodzie
ul. 17 Stycznia 143, 64-400 Międzychód

Załącznik 7
do polityki bezpieczeństwa
przetwarzania danych osobowych
w PCUW w Międzychodzie

Obszar przetwarzania danych osobowych w Powiatowym Centrum Usług Wspólnych w Międzychodzie

Obszar przetwarzania danych osobowych PCUW w Międzychodzie znajduje się w budynku w Międzychodzie, ul. 17 Stycznia 143 i obejmuje poniższy wykaz pomieszczeń:

I PIĘTRO

pok. 105 – pomieszczenie biurowe

pok. 106 – pomieszczenie biurowe,

II PIĘTRO

pok. 221 – pomieszczenie biurowe,

Przetwarzanie danych osobowych jest zabronione jeśli nie są spełnione warunki zdefiniowane w niniejszej Polityce.

DYREKTOR
Powiatowego Centrum Usług Wspólnych
w Międzychodzie
mgr Dariusz Nowak

(podpis Administratora Danych)

Załącznik nr 2
do Zarządzenia nr RCUW-9/2018
z dnia 4 maja 2018 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W POWIATOWYM CENTRUM USŁUG WSPÓLNYCH W MIĘDZYCHODZIE

Niniejsza „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych", zwana dalej Instrukcją została opracowana w związku z wymaganiami zawartymi w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101 poz. 926, z późn. zm.) 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 (Dz. U. z 2004 r. Nr 100, poz. 1024).

§ 1. Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Powiatowym Centrum Usług Wspólnych w Międzychodzie, określa:

1) sposób przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz osoby odpowiedzialne za te czynności,

2) sposób rejestrowania i wyrejestrowywania użytkowników oraz osoby odpowiedzialne za te czynności,

3) zasady i procedury rozpoczynania i kończenia pracy,

4) zasady i częstotliwość tworzenia kopii bezpieczeństwa,

5) zasady i częstotliwość kontroli obecności wirusów komputerowych oraz metodę ich usuwania,

6) zasady i czas przechowywania nośników informacji, w tym kopii informatycznych,

7) zasady dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych,

8) zasady postępowania w zakresie komunikacji w sieci komputerowej.

§ 2. Ilekroć w Instrukcji jest mowa o:

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

2) **rozporządzeniu** - rozumie się przez to 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)

3) **Jednostce** (**Centrum**) - rozumie się przez to Powiatowe Centrum Usług Wspólnych w Międzychodzie;

4) **Pracowniku jednostki** – rozumie się przez to pracownika Powiatowego Centrum Usług Wspólnych w Międzychodzie;

5) **identyfikatorze użytkownika** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

6) **haśle** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

7) **sieci telekomunikacyjnej** - rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.);

8) **sieci publicznej** - rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne;

9) **teletransmisji** - rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;

10) **rozliczalności** - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

11) **integralności danych** - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

12) **raporcie** - rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;

13) **poufności danych** - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;

14) **uwierzytelnianiu** - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,

15) **Administratorze Danych (AD)** - w świetle przepisów ustawy o ochronie danych osobowych , art. 3 i 7 pkt 4 rozumie się przez to Dyrektora Centrum, który decyduje o celach i środkach przetwarzania danych osobowych;

16) **Administratorze Bezpieczeństwa Informacji (ABI)** - rozumie się przez to osobę wyznaczoną przez Administratora Danych (dyrektora Centrum), 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;

17) **Administratorze Systemu Informatycznego (ASI)**, zwanego też Administratorem Systemu - rozumie się przez to osobę lub osoby zatrudnione przez dyrektora Centrum, upoważnione do realizacji zadań związanych z zarządzaniem systemem informatycznym;

18) **użytkowniku systemu informatycznego** - rozumie się przez to upoważnioną przez kierownika jednostki, pracownika do przetwarzania danych osobowych w systemie informatycznym, który odbył stosowne szkolenie w zakresie ochrony danych.

19) **Instrukcji** – rozumie się przez to niniejszy dokument.

20) **Polityce** – rozumie się przez to „Politykę bezpieczeństwa przetwarzania danych osobowych w Powiatowym Centrum Usług Wspólnych w Międzychodzie" opracowaną na podstawie przepisów ustawy i rozporządzenia.

§ 3. 1 Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych, zwanego dalej „systemem" może uzyskać wyłącznie osoba (użytkownik) upoważniona do dostępu do systemu przez Administratora Danych.

2. Rejestracja, o której mowa w ust. 1, polega na nadaniu przez ASI identyfikatora i przydziale hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.

3. Procedurę o którym mowa w ust. 1 nadania upoważnień opisuje Polityka Bezpieczeństwa przetwarzania danych osobowych w Powiatowym Centrum Usług Wspólnych w Międzychodzie, opracowana na podstawie przepisów ustawy i rozporządzenia.

§ 4. 1. Wyrejestrowania użytkownika z systemu informatycznego dokonuje ASI na wniosek Administratora Danych lub stanowiska do spraw kadr.

2. Wyrejestrowanie, o którym mowa w ust. 1, może mieć charakter czasowy lub trwały.

3. Wyrejestrowanie następuje poprzez:

1) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),

2) usunięcie danych dostępowych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

4. Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego jest:

1) nieobecność w pracy trwająca dłużej niż 31 dni kalendarzowych,

2) zawieszenie w pełnieniu obowiązków służbowych,

3) zwolnienie z pełnienia obowiązków służbowych.

5. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy użytkownika.

§ 5. 1. Zgodnie z Rozporządzeniem ustala się następujące zasady postępowania z hasłami dostępu:

1) hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,

2) hasło nie może być identyczne z identyfikatorem użytkownika, ani z jego imieniem lub nazwiskiem,

3) zmiana hasła następuje nie rzadziej niż co 30 dni,

4) zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom.

2. Po otrzymaniu pierwszego hasła, użytkownik zobowiązany jest niezwłocznie zalogować się do systemu i zmienić przydzielone hasło zgodnie z zasadami określonymi w ust. 0

3. Hasło podlega natychmiastowej zmianie w przypadku podejrzenia jego odkrycia przez osobę nieupoważnioną.

4. Hasła nie mogą być nigdzie zapisywane, z wyjątkiem haseł umożliwiających administracyjny dostęp (tj. zapewniających pełne uprawnienia do zarządzania systemem).

5. Tryb przechowywania i udostępniania haseł umożliwiających dostęp administracyjny określa załącznik nr 2 do niniejszej Instrukcji.

§ 6. Rozpoczęcie pracy w systemie odbywa się poprzez:

1) przygotowanie stanowiska pracy,

2) włączenie stacji roboczej,

3) wprowadzenie swojego identyfikatora i hasła, przy czym wprowadzenie hasła odbywa się w sposób uniemożliwiający jego podejrzenie.

§ 7. Opuszczenie stanowiska pracy odbywa się po uprzednim:

1) zabezpieczeniu dokumentacji przed dostępem osób postronnych,

2) wylogowaniem użytkownika z systemu,

3) zablokowaniem dostępu do komputera (przełączenie komputera w tryb wymagający podania hasła).

§ 8. Zakończenie pracy w systemie odbywa się poprzez:

1) zamknięcie aplikacji,

2) zamknięcie systemu operacyjnego,

3) wyłączenie stacji roboczej,

4) zabezpieczeniem stanowiska pracy przed dostępem osób nieupoważnionych.

§ 9. Zabrania się użytkownikom pracującym w systemie:

1) udostępniania stacji roboczej osobom niezarejestrowanym z zastrzeżeniem pkt 2,

2) udostępniania stacji roboczej do konserwacji lub naprawy bez porozumienia z ASI,

3) używania nielicencjonowanego oprogramowania.

§ 10. 1. Każdy przypadek naruszenia ochrony danych osobowych, które mogą wskazywać na naruszenie bezpieczeństwa podlega zgłoszeniu do ABI, a w szczególności:

1) naruszenia bezpieczeństwa systemu informatycznego,

2) stwierdzenia objawów (stanu urządzeń, sposobu działania programu lub jakości komunikacji w sieci).

2. ABI zgłasza się w szczególności przypadki:

1) użytkowania stacji roboczej przez osobę nie będącą użytkownikiem systemu,

2) usiłowania logowania się do systemu (sieci) przez osobę nieuprawnioną,

3) usuwania, dodawania lub modyfikowania bez wiedzy i zgody użytkownika jego dokumentów (rekordów),

4) przebywania osób nieuprawnionych w obszarze, w którym przetwarzane są dane osobowe, w trakcie nieobecności osoby zatrudnionej przy przetwarzaniu tych danych i bez zgody Administratora Danych, pozostawiania bez nadzoru otwartych pomieszczeń, w których przetwarzane są dane osobowe,

5) udostępniania osobom nieuprawnionym stacji roboczej lub komputera przenośnego, służących do przetwarzania danych osobowych,

6) niezabezpieczenia hasłem dostępu do komputera służącego do przetwarzania danych osobowych,

7) przechowywania nośników informacji oraz wydruków z danymi osobowymi, nieprzeznaczonymi do udostępniania, w warunkach umożliwiających do nich dostęp osobom nieuprawnionym.

3. Obowiązek dokonania zgłoszenia, o którym mowa w ust 1, spoczywa na każdym użytkowniku, który powziął wiadomość o naruszeniu ochrony danych osobowych.

4. W przypadku naruszenia integralności bezpieczeństwa sieciowego, obowiązkiem ASI jest natychmiastowe wstrzymanie udostępniania zasobów dla użytkowników i odłączenie serwerów od sieci.

5. Użytkownik sieci i ASI w porozumieniu z ABI ustalają przyczyny naruszenia integralności bezpieczeństwa sieciowego.

6. Przywrócenie udostępniania zasobów użytkownikom może nastąpić dopiero po ustaleniu i usunięciu przyczyny naruszenia integralności bezpieczeństwa sieciowego.

§ 11. Częstotliwość oraz sposób tworzenia kopii awaryjnych reguluje załącznik nr 1 do niniejszej Instrukcji.

§ 12. 1. Sprawdzanie obecności wirusów komputerowych w systemie oraz ich usuwanie odbywa się przy wykorzystaniu licencjonowanego oprogramowania w oparciu o serwer dystrybucji aktualnych sygnatur i wersji oprogramowania.

2. Oprogramowanie, o którym mowa w ust. 1, sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz stacjami roboczymi.

3. Niezależnie od ciągłego nadzoru, o którym mowa w ust. 2, ASI kontroluje nie rzadziej niż raz na kwartał prawidłowość funkcjonowania systemu antywirusowego.

4. Do obowiązków ASI należy zapewnienie prawidłowej aktualizacji oprogramowania służącego do sprawdzania w systemie obecności wirusów komputerowych.

§ 13. 1. System i urządzenia informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, zabezpiecza się przed utratą danych osobowych (np. utratą integralności danych) spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

2. Minimalne zabezpieczenie systemu i urządzeń informatycznych, o których mowa w ust. 1, polega na wyposażeniu serwera (serwerów) oraz stacji roboczych w zasilacze awaryjne (UPS).

§ 14. 1. Urządzenia informatyczne służące do przetwarzania danych osobowych można przekazać do naprawy, lub likwidacji dopiero po uprzednim uzyskaniu zgody ABI.

2. Urządzenia, o których mowa w ust. 1 przed ich przekazaniem pozbawia się zapisanych danych osobowych poprzez wymontowanie dysku twardego z zastrzeżeniem ust. 3.

3. Jeżeli nie jest to możliwe, urządzenie to może być naprawiane wyłącznie pod nadzorem Administratora Systemu.

4. Jeżeli nie jest możliwe pewne pozbawienie urządzenia przekazywanego do likwidacji zapisanych danych osobowych, urządzenie - przed przekazaniem - uszkadza się fizycznie w sposób uniemożliwiający odczytanie tych danych.

§ 15. 1. Przeglądu i konserwacji systemu dokonuje ASI doraźnie.

2. Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje użytkownik doraźnie, o podejrzeniu zaistniałych nieprawidłowości niezwłocznie zawiadamia ASI.

§ 16. 1. Operacje wykonywane w systemach teleinformatycznych Powiatowego Centrum Usług Wspólnych w Międzychodzie zgodnie z § 21 Rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2012. poz.526) podlegają wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach).

2. W dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do:

1) systemu z uprawnieniami administracyjnymi;

2) konfiguracji systemu, w tym konfiguracji zabezpieczeń;

3) przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.

3. Poza informacjami wymienionymi w ust. 2 na podstawie decyzji ASI lub ABI mogą być odnotowywane również inne działania użytkowników lub obiektów systemowych, a także inne zdarzenia związane z eksploatacją systemu w postaci:

1) działań użytkowników nieposiadających uprawnień administracyjnych,

2) zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu,

3) zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny - w zakresie wynikającym z analizy ryzyka.

4. Informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata

5. Zapisy dzienników systemów mogą być składowane na zewnętrznych informatycznych nośnikach danych w warunkach zapewniających bezpieczeństwo informacji.

6. W uzasadnionych przypadkach dzienniki systemów mogą być prowadzone na nośniku papierowym.

§ 17. 1. Bezpieczeństwo komunikacji w obrębie systemów przetwarzających dane osobowe ASI zapewnia przy użyciu narzędzi w obrębie systemu.

2. W systemach działających sieciowo, na zasadzie udostępnienia zasobów na serwerze, ASI powinien uwzględniać dedykowane przyzwolenia dostępu, tj. zapewnić kontrolę nad tym kto i w jaki sposób może uzyskać dostęp do zasobów sieciowych

§ 18. 1. Przesyłanie danych osobowych w komunikacji wewnętrznej (sieć LAN) musi być zorganizowane w sposób dostępny jedynie dla uprawnionych użytkowników przy użyciu narzędzi zabezpieczeń w obrębie systemu informatycznego.

2. W sytuacji, gdy dostępne narzędzia informatyczne nie będą wystarczające do działania w komunikacji wewnętrznej, użytkownik systemu w porozumieniu z ASI wyznacza sposób postępowania, mając w szczególności na uwadze ochronę danych osobowych.

§ 19. 1. Do przesyłania danych w sieci publicznej (Internet), z uwagi na przekazywane dane osobowe, powinny być wykorzystywane wyłącznie kanały transmisji wykorzystywane przez autoryzowane programy lub systemy oraz wyłącznie w oparciu o przepisy prawne regulujące sposób udostępniania (przesyłania) tych danych poza obszar urzędu.

2. W przypadku braku przepisów o których mowa w ust.1 określających sposób przesłania danych użytkownik w porozumieniu z ABI lub ASI powinien zapewnić środki kryptograficzne umożliwiające bezpieczne przesłanie informacji.

§ 20. 1. Nośniki informatyczne zawierające dane osobowe powinny być opisane w sposób czytelny i zrozumiały dla użytkownika, a zarazem nie powinny ułatwiać rozpoznania zawartości przez osoby nieupoważnione.

2. Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione.

§ 21. 1. W pomieszczeniach, gdzie nie jest możliwe ograniczenie dostępu osób postronnych, monitory stanowisk dostępu do danych osobowych ustawia się w taki sposób, aby uniemożliwić tym osobom wgląd w dane.

2. Ekrany monitorów wszystkich stanowisk są zaopatrzone w wygaszacze z ustawioną opcją *„wymagania hasła”*, które po upływie maksymalnie 15 minut nieaktywności użytkownika automatycznie wyłączają możliwość podglądu ekranu, oraz żądają ponownej autoryzacji dostępu do komputera.

§ 22. Osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera poza obszarem ochrony danych w celu zapobieżenia dostępowi do tych danych osobie niepowołanej.

§ 23. 1. Użytkownik sporządzający wydruki, które zawierają dane osobowe jest odpowiedzialny za zachowanie szczególnej ostrożności przy korzystaniu z nich, a zwłaszcza za zabezpieczenie ich przed dostępem osób nie posiadających imiennego upoważnienia oraz nieuprawnionych do wglądu.

2. Wydruki zawierające dane osobowe, które są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.