ZARZĄDZENIE Nr 5/2016

Kierownika Powiatowego Centrum Pomocy Rodzinie

W Aleksandrowie Kujawskim

Z dnia 4 marca 2016 roku

w sprawie wprowadzenia Polityki bezpieczeństwa informacji i Instrukcji zarzadzania Systemem informatycznym, w którym przetwarzane są dane osobowe w Powiatowym Centrum Pomocy Rodzinie w Aleksandrowie Kujawskim

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r. poz. 2135, późn. zm.) oraz § 3 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. Wprowadzam w Powiatowym Centrum Pomocy Rodzinie w Aleksandrowie Kujawskim Politykę bezpieczeństwa informacji, której treść stanowi załącznik nr 1 do Zarządzenia, oraz Instrukcję zarządzania systemem informatycznym , w którym przetwarzane są dane osobowe, która stanowi załącznik nr 2 do Zarządzenia.

§2. Powołuję Panią Karolinę Jargiło do pełnienia funkcji Administratora Bezpieczeństwa Informacji w Powiatowym Centrum Pomocy Rodzinie w Aleksandrowie Kujawskim.

§3. Każdy pracownik przetwarzający dane osobowe w zbiorach Powiatowego Centrum Pomocy Rodzinie w Aleksandrowie Kujawskim, zgodnie z wykazem, jest obowiązany zapoznać się z treścią załącznika nr 1 i nr 2 do niniejszego Zarządzenia.

§4. Oświadczenie o zapoznaniu się z treścią powyższych załączników zaopatrzone w podpis pracownika i datę dołącza się do akt osobowych do części B. Wzór oświadczenia stanowi załącznik nr 3 do niniejszego Zarządzenia.

§5. Pracodawca zobowiązuje wszystkich pracowników do przestrzegania Polityki bezpieczeństwa informacji oraz stosowania w pracy Instrukcji zarządzania systemem informatycznym pod sankcją konsekwencji służbowych, przewidzianych prawem.

§6. Zarządzenie wchodzi w życie z dniem podpisania.

Kierownik
Powiatowe Centrum Pomocy Rodzinie

Załącznik nr 1 do Zarządzenie Kierownika
Powiatowego Centrum Pomocy Rodzinie
w Aleksandrowie Kujawskim
w sprawie wprowadzenia Polityki
bezpieczeństwa informacji i Instrukcji
zarządzania systemem informatycznym,
w którym przetwarzane są dane osobowe
w Powiatowym Centrum Pomocy Rodzinie
w Aleksandrowie Kujawskim

POLITYKA BEZPIECZEŃSTWA INFORMACJI W POWIATOWYM CENTRUM POMOCY RODZINIE W ALEKSANDROWIE KUJAWSKIM

Aleksandrów Kujawski, dnia 04 marca 2016 roku

Spis treści:

§ 1
Wprowadzenie

1. Polityka Bezpieczeństwa Informacji w dalszej części dokumentu zwana Polityką opracowana została w oparciu o następujące przepisy prawa:

- ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2015 poz. 2135, z późn. zm.);
- 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);
- rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz. U. poz. 1934);
- rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. poz. 719);
- rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. poz. 745);
- oraz grupa norm dotyczących bezpieczeństwa informacji (PN-ISO/IEC: 27000:2014-11, 27001:2014-12, 27002:2014-12, 27005:2014-01, 24762:2010), które określają wszystkie istotne aspekty związane z ochroną danych oraz systemów tradycyjnych i informatycznych służących do ich przetwarzania.

2. Polityka określa zbiór zasad przetwarzania danych osobowych w Powiatowym Centrum Pomocy Rodzinie w Aleksandrowie Kujawskim oraz ich zabezpieczania, jako zestaw praw, reguł i zaleceń, regulujących sposób ich zarządzania, ochrony i dystrybucji.

3. Celem Polityki jest wdrożenie i realizacja działań przy wykorzystaniu środków technicznych i organizacyjnych, które zapewnią maksymalny poziom bezpieczeństwa w zakresie przetwarzania danych osobowych, chroniąc je przed nieautoryzowanym dostępem, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed zmianą, uszkodzeniem lub zniszczeniem.

§ 2
Definicje

Określenia użyte w Polityce bezpieczeństwa oznaczają:

1. **Centrum** – Powiatowe Centrum Pomocy Rodzinie w Aleksandrowie Kujawskim mieszczące się przy ul. Sikorskiego 3;
2. **Administrator Danych Osobowych (ADO)** – jednostka organizacyjna w postaci Centrum decydująca o celach i środkach przetwarzania danych osobowych reprezentowana przez Kierownika, który zarządza Polityką bezpieczeństwa za pośrednictwem Administratora Bezpieczeństwa Informacji;
3. **Administrator Bezpieczeństwa Informacji (ABI)** – osoba powołana przez Administratora Danych Osobowych w celu nadzorowania przetwarzania danych osobowych w systemie tradycyjnym i informatycznym, odpowiedzialna w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń systemu zabezpieczeń;
4. **Administrator Systemu Informatycznego (ASI)** – pracownik Starostwa Powiatowego w Aleksandrowie Kujawskim – wyznaczony w drodze delegacji obowiązków do realizacji zadań związanych z eksploatacją sieci i systemów informatycznych na terenie Centrum, w których przetwarzane są dane osobowe;
5. **Zbiór danych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcyjnie, tzn. przetwarzany w sposób taki, że uprawniony użytkownik ma dostęp tylko w ograniczonym zakresie przetwarzania;
6. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, w szczególności poprzez podanie jednego lub kilku specyficznych czynników ją określających;
7. **Przetwarzanie danych osobowych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, które wykonuje się w sposób tradycyjny jak i w systemach informatycznych.
8. **Generalny Inspektor Ochrony Danych Osobowych** - rozumie się przez to organ do spraw ochrony danych osobowych, zwany dalej GIODO;
9. **Hasło** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi, wykorzystywanemu łącznie z identyfikatorem do identyfikowania osoby w systemie informatycznym;

10. **Identyfikator** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
11. **Odbiorca danych** - rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
    1) osoby, której dane dotyczą,
    2) osoby upoważnionej do przetwarzania danych,
    3) przedstawiciela, o którym mowa wart. 31a ustawy,
    4) podmiotu, o którym mowa w art. 31 ustawy,
    5) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;
12. **Osoba upoważniona do przetwarzania danych osobowych** - rozumie się przez to użytkownika zbioru danych osobowych, który otrzymał pisemne upoważnienie do przetwarzania danych osobowych wydane przez ADO na wniosek Właściciela zasobów odpowiadającego merytorycznie za zbiór danych osobowych, zwana dalej osobą upoważnioną;
13. **Przetwarzający** - rozumie się przez to podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawieranej zgodnie z art. 31 ustawy;
14. **Sieć publiczna i sieć telekomunikacyjna** - rozumie się przez to sieć publiczną i sieć telekomunikacyjną w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, z późn. zm.);
15. **System informatyczny** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
16. **Upoważnienie** - rozumie się przez to pisemne imienne upoważnienie do przetwarzania danych osobowych wydane przez ADO;
17. **Ustawa** - rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r. poz. 2132, z późn. zm.);
18. **Rozporządzenie** - 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);
19. **Usuwanie danych** - rozumie się przez to zniszczenie danych lub taka ich modyfikacje, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

20. **Użytkownik** - rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych w formie informatycznej lub tradycyjnej i informatycznej po nadaniu identyfikatora i hasła;
21. **Osoba trzecia** – należy przez to rozumieć, osobę nie będącą osobą upoważnioną przez ADO;
22. **Właściciel zasobów**– osoba odpowiedzialna merytorycznie za gromadzenie i przetwarzanie danych osobowych w komórce organizacyjnej;
23. **Zbiór nieinformatyczny** – zbiór danych osobowych prowadzony poza systemem informatycznym, w szczególności w postaci tradycyjnej.

§ 3
Definicja bezpieczeństwa

1. Utrzymanie bezpieczeństwa przetwarzanych przez ADO danych osobowych rozumiane jest jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z zasobem stanowiącym przedmiot niniejszej Polityki bezpieczeństwa.

2. Poniżej opisane jest rozumienie wyżej wymienionych pojęć w odniesieniu do informacji i aplikacji:
   1) poufność danych – rozumiana jako zapewnienie, że tylko osoby upoważnione mają dostęp do informacji,
   2) integralność danych – rozumiana jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania,
   3) dostępność danych – rozumiane jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,
   4) zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć zbiorów danych przetwarzanych tradycyjnie lub w systemach informatycznych,
   5) zgodności z prawem – właściwości zapewniającej, że gromadzone są wyłącznie dane niezbędne do właściwego funkcjonowania przedsiębiorstwa.

3. Dodatkowo zarządzanie bezpieczeństwem informacji wiąże się z zapewnieniem:
   1) niezaprzeczalności odbioru – rozumianej jako zdolność systemu do udowodnienia, że adresat informacji otrzymał ją w określonym miejscu i czasie;

2) niezaprzeczalności nadania – rozumianej jako zdolność systemu do udowodnienia, że nadawca informacji faktycznie ją nadał lub wprowadził do systemu w określonym miejscu i czasie;
3) rozliczalności działań – rozumianej, jako zapewnienie, że wszystkie działania istotne dla przetwarzania informacji zostały zarejestrowane w systemie i możliwym jest zidentyfikowanie użytkownika, który działania dokonał.

4. Polityka bezpieczeństwa zakłada pełne zaangażowanie kierownictwa oraz wszystkich pracowników Centrum dla zapewnienia bezpieczeństwa danych osobowych przetwarzanych zarówno w sposób tradycyjny, jak i w systemach informatycznych czy innych nośnikach danych.

§ 4
Cel, zakres oraz realizacja Polityki bezpieczeństwa

1. W celu zapewnienia całkowitego bezpieczeństwa danych osobowych, konieczne jest wsparcie ADO. Zgodnie z powyższym ADO deklaruje swoje pełne wsparcie dla wszelkich działań organizacyjnych oraz technicznych, których celem jest zapewnienie pełnego bezpieczeństwa przetwarzania danych osobowych w całym obszarze funkcjonowania ADO.

2. Polityka bezpieczeństwa określa reguły oraz metody postępowania mające na celu zapewnienie integralności, rozliczalności oraz poufności przetwarzanych danych osobowych jak i wskazanie działań, jakie należy wykonać oraz ustanawia zasady i reguły postępowania, które należy stosować w celu zapewnienia pełnego bezpieczeństwa przetwarzania danych osobowych w całym obszarze funkcjonowania ADO, w zakresie zgodnym z obowiązującym aktualnie stanem prawnym.

3. W związku z tym, że w zbiorach przetwarzane są miedzy innymi dane wrażliwe, a system informatyczny posiada szerokopasmowe połączenie z internetem, niniejsza Polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa danych w rozumieniu § 6 rozporządzenia. Niniejszy dokument opisuje niezbędny do uzyskania tego bezpieczeństwa zbiór procedur i zasad dotyczących przetwarzania danych osobowych oraz ich zabezpieczenia.

4. Realizacja funkcji polityki bezpieczeństwa opiera się na:
1) szkoleniu osób upoważnionych w formie tradycyjnej i elektronicznej w zakresie obsługi zbiorów oraz systemów informatycznych;
2) odpowiedzialności osób upoważnionych za wykonywane czynności;

3) odpowiedzialności administratorów za bezpieczeństwo systemów informatycznych oraz egzekwowaniu możliwości wprowadzenia odpowiednich procedur;
4) właściwym wykorzystaniu zasobów systemu informatycznego;
5) podejmowaniu właściwych czynności w razie zaistnienia problemu z utrzymaniem właściwego poziomu bezpieczeństwa przetwarzanych danych osobowych.

5. Powyższe punkty polityki bezpieczeństwa realizuje się za pomocą:
   1) prawidłowego nadania właściwych uprawnień do zbiorów oraz zasobów systemu informatycznego;
   2) ograniczenia dostępu do niektórych komend systemowych;
   3) ograniczenia dostępu do funkcji systemowych: składanie i odtwarzanie danych, przeglądanie i modyfikowanie uprawnień użytkowników w systemie;
   4) uniemożliwienia przekonfigurowania uprawnień swojego konta;
   5) stosowania odpowiednich mechanizmów sprzętowych i programowych w celu uodpornienia na awarie lub zminimalizowania czasu ich trwania;
   6) zastosowania programów monitorujących system informatyczny w celu zabezpieczenia przed wirusami komputerowymi.

6. Zasady określone przez Politykę bezpieczeństwa mają zastosowanie do wszystkich zbiorów danych osobowych przetwarzanych przez ADO, a w szczególności do:
   1) tradycyjnych oraz wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych, w których przetwarzane są dane podległe ochronie,
   2) informacji będących własnością ADO lub klientów ADO, o ile zostały przekazane na podstawie stosownych umów,

7. Do stosowania zasad określonych przez Politykę bezpieczeństwa zobowiązani są wszyscy pracownicy Centrum w rozumieniu ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2014 r. 1502, z późn. zm) stażyści, praktykanci, wolontariusze oraz inne osoby mające zgodny z prawem dostęp do danych podlegających ochronie.

8. Podczas zapewnienia bezpieczeństwa przy przetwarzaniu danych osobowych podlegających ochronie należy uwzględniać możliwe zagrożenia, a w szczególności:
   1) Zagrożenia natury fizycznej:
      a) włamania do pomieszczeń, w których przetwarzane są dane osobowe,
      b) kradzież lub zniszczenie sprzętu lub nośników danych,
      c) nieuprawniony dostęp do systemów przetwarzania i przesyłania danych w wyniku włamania.
   2) Zagrożenia natury losowej:

oddziaływanie czynników zewnętrznych mogących doprowadzić do utraty lub uszkodzenia sprzętu i nośników danych, takich jak: pożar, zalanie wodą, wyładowania elektryczne, awarie zasilania, zakłócenia w sieci energetycznej.

3) Zagrożenia związane z nieprawidłową pracą systemów informatycznych:
   a) niestabilność systemu operacyjnego;
   b) awaria oprogramowania użytkowego;
   c) wirusy komputerowe.
4) Zagrożenia związane z nieuprawnionym dostępem:
   a) niewłaściwe zabezpieczenie i nadzór nad pomieszczeniami, w których przetwarzane są dane osobowe;
   b) niewłaściwe usytuowanie sprzętu, w tym monitorów w sposób umożliwiający dostęp do przetwarzanych danych przez osoby nieuprawnione;
   c) niewłaściwe zabezpieczenie linii i sprzętu teletransmisyjnego;
   d) niewłaściwy nadzór nad naprawami i konserwacją sprzętu oraz nośników danych;
   e) nieprawidłowy nadzór nad kasowaniem danych osobowych oraz niszczeniem nośników.
5) Zagrożenia związane z eksploatacją:
   a) brak właściwego zabezpieczenia systemu w trakcie rozpoczynania i kończenia pracy oraz podczas przerw w pracy;
   b) nielegalne kopiowanie danych osobowych;
   c) kontynuowanie pracy mimo występujących nieprawidłowości w używanym sprzęcie i oprogramowaniu.

§ 5
Administrowanie bezpieczeństwem danych osobowych, osoby przetwarzające dane osobowe

Za bezpieczeństwo danych osobowych u ADO odpowiedzialny jest Kierownik, który zarządza polityką bezpieczeństwa za pośrednictwem powołanego przez siebie Administratora Bezpieczeństwa Informacji.

1. Administrator Danych Osobowych:
   1) odpowiedzialny jest w szczególności za:
      a) powołanie ABI oraz określenie zakresu jego zadań,
      b) nadzór nad ABI w zakresie jego obowiązków, wyrażanie opinii i nadzór nad rozwojem „Polityki bezpieczeństwa informacji w Powiatowym Centrum Pomocy Rodzinie w Aleksandrowie Kujawskim",
      c) podejmowanie właściwych działań mających na celu zabezpieczenie zbiorów danych osobowych zgodnie z ustawą o ochronie danych osobowych,

d) nadzór nad zarządzaniem zbiorami danych osobowych zgodnie z ich przeznaczeniem, czuwanie nad zgodnością procedur przetwarzania z procedurami określonymi w ustawie o ochronie danych osobowych;

2) realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:
   a) podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji administratora danych oraz technik zabezpieczenia danych osobowych;
   b) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi ich obowiązków;
   c) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych.

2. Administrator Bezpieczeństwa Informacji odpowiedzialny jest w szczególności za:
   1) zapewnienie przestrzegania przepisów ustawy o ochronie danych osobowych w zakresie dotyczącym Administratora Bezpieczeństwa Informacji i bezpośrednio w tym zakresie podlega ADO;
   2) realizację innych zadań w komórce, do której jest przyporządkowany i w tym zakresie podlega bezpośrednio kierownikowi jednostki organizacyjnej;
   3) dokonanie sprawozdawczości dla ADO z realizacji poniższych zadań;
   4) nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których dane są przetwarzane oraz kontrolą przebywających w nich osób, który realizowany jest przez prowadzenie wewnętrznych kontroli;
   5) nadzór nad bezawaryjnym funkcjonowaniem sprzętu komputerowego oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych;
   6) nadzór nad naprawami, konserwacją, likwidacją urządzeń komputerowych, na których zapisane są dane osobowe;
   7) przestrzeganie procedur określających częstotliwość zmiany haseł użytkowników systemów informatycznych;
   8) nadzór na wykonywaniem kopii zapasowych ich przechowywaniem oraz zniszczeniem;
   9) nadzór nad bezpieczeństwem danych zawartych w komputerach stacjonarnych, przenośnych, dyskach wymiennych, w których przetwarzane są dane osobowe;
   10) nadzór nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe wytwarzane w sposób tradycyjny lub przez system informatyczny;

11) nadzór nad funkcjonowaniem mechanizmów uwierzytelnienia użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrolą dostępu do danych;
12) prowadzenie ewidencji miejsc w których są przetwarzane dane osobowe;
13) powiadomienie ASI o konieczności utworzenia identyfikatora użytkownika w systemie oraz nadaniu, zmianie lub odebraniu uprawnień dostępu użytkownika do systemu;
14) prowadzenie rejestru zbiorów danych osobowych przetwarzanych przez ADO oraz prowadzenie korespondencji z Generalnym Inspektorem Ochrony Danych Osobowych;
15) nadzór nad prowadzoną dokumentacją przez ASI z zakresu ochrony danych osobowych oraz opracowywanie procedur związanych z ochroną danych osobowych;
16) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych, wzór ewidencji stanowi załącznik nr 6 do niniejszej Polityki;
17) prowadzenie szkolenia użytkowników zbioru danych osobowych w zakresie ochrony danych osobowych;
18) podejmowanie odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia systemu informatycznego lub ochrony danych osobowych w przypadku systemu tradycyjnego;
19) nadzorowanie procesu udostępniania przez ADO danych osobowych odbiorcom danych;
20) określanie na piśmie szczegółowych zasad postępowania z kluczami do pomieszczeń i szaf, w których przetwarzane i przechowywane są dane osobowe;
21) wyznaczenie w porozumieniu z ADO na czas nieobecności powyżej 30 dni roboczych osoby zastępującej.
22) prowadzi rejestr komputerów, w których przetwarzane są dane osobowe;

3. Administrator Systemu Informatycznego realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym ADO, w tym zwłaszcza:
   l) zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji profilu administratora;
   2) przeciwdziała dostępowi osób nieupoważnionych do systemu informatycznego, w którym przetwarzane są dane osobowe, prowadząc profilaktyka antywirusową;
   3) prowadzi rejestr osób (w tym także identyfikatorów) upoważnionych do przetwarzania danych osobowych w systemie informatycznym;

4) przydziela na wniosek ADO, po opinii ABI, ściśle określonych praw dostępu do danych osobowych w danym systemie informatycznym, identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta użytkowników zgodnie z zasadami określonymi w Instrukcji;
5) nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;
6) konfiguruje system informatyczny w oparciu o zasady określone w rozporządzeniu i instrukcji zarządzania, a w szczególności dba o:
   a) konfiguracje systemu operacyjnego oraz programów (jeżeli istnieje taka możliwość) w komputerach, w których przetwarzane są dane osobowe, wymuszającą okresową zmianę haseł użytkownika,
   b) stosowanie i prowadzenie listy haseł do ustawień komputerów (hasło ASI) oraz hasła użytkownika (hasło pierwszego logowania),
   c) konfiguracje dziennika zdarzeń systemu w sposób umożliwiający kontrole czasu pracy poszczególnych użytkowników, a także pracy w programach obsługujących zbiory (jeżeli istnieje taka możliwość),
   d) zakładanie kont użytkownikom komputera w oparciu o minimalne uprawnienia użytkownika,
7) prowadzi szczegółową dokumentacje naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym;
8) informuje ABI o wszelkich stwierdzonych nieprawidłowościach związanych z przetwarzaniem danych osobowych;
9) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje ABI o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia;
10) występuje do ABI z propozycjami zmian w organizacji i zabezpieczeniu przetwarzania danych osobowych zmierzającymi do usprawnienia pracy i bezpieczeństwa danych osobowych;
11) sprawuje nadzór nad:
   a) wykonywaniem napraw i konserwacją urządzeń komputerowych i oprogramowania,
   b) wykonywaniem kopii zapasowych systemów wskazanych przez ADO, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego;
12) podejmuje działania służące zapewnieniu niezawodności zasilania komputerów i innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej;

13) powołuje komisję do niszczenia wycofanych z użycia nośników stosowanych w systemach informatycznych, w których przetwarzano dane osobowe, w skład której, oprócz ASI, wchodzą także ABI oraz wyznaczony przez ADO pracownik;
14) zarządza licencjami, instalacjami i konfiguracją sprzętu sieciowego i określa wymogi techniczne w sprawie zakupu sprzętu komputerowego.
15) ASI uczestniczy w realizacji zadania w zakresie:
    a) dostarczenia sprzętu informatycznego dla ADO (np.: stacje robocze, monitory, komputery przenośne, elementy sieci wewnętrznej, drukarki itp.),
    b) serwisu sprzętu informatycznego,
    c) dostarczenia usług w zakresie utrzymania sprawnego działania sieci,
    d) dostarczenia oprogramowania niezbędnego do poprawnego funkcjonowania ADO.

4. Właściciel zasobów.

Do kompetencji Właścicieli zasobów należy określenie celów w jakich mają być przetwarzane dane osobowe, zakresu oraz sposobu ich przetwarzania danych osobowych.

Do obowiązków Właścicieli zasobów danych osobowych należy:

1) zapewnienie podstaw prawnych do przetwarzania danych osobowych od chwili zebrania danych osobowych do chwili ich usunięcia;
2) zapewnienie aktualności, adekwatności oraz merytorycznej poprawności danych osobowych przetwarzanych w określonym przez nich celu;
3) realizację obowiązku informowania o przetwarzaniu danych osobowych osób, których dane osobowe są pozyskiwane;
4) zapewnienie na żądanie uprawnionych osób, udostępniania informacji o przetwarzanych danych osobowych oraz podmiotach, którym zostały one udostępnione.

5. Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do zapewnienia poufności przetwarzanych danych osobowych oraz stosowania się do obowiązujących w tym zakresie uregulowań. W szczególności zobowiązana jest do:
1) przetwarzania danych osobowych wyłącznie:
    a) w ramach tego zbioru, do którego otrzymała upoważnienie,
    b) w sposób i w zakresie wynikającym z posiadanych uprawnień i obowiązków oraz faktycznych potrzeb służbowych, określonych przez ADO;
2) zachowania w tajemnicy przez cały okres zatrudnienia u ADO, a także po ustaniu stosunku pracy lub odwołaniu z zajmowanego stanowiska:
    a) danych osobowych uzyskanych w trakcie wykonywania czynności służbowych,

b) wszelkich informacji o stosowanych procedurach i zabezpieczeniach danych osobowych i systemów informatycznych;

3) zapoznania się i stosowania do uregulowań wynikających z ustawy oraz polityki bezpieczeństwa i instrukcji zarządzania;
4) udziału w szkoleniach z zakresu ochrony danych osobowych prowadzonych u ADO;
5) właściwego zabezpieczenia danych osobowych przetwarzanych w formie tradycyjnej (papierowej) poprzez uniemożliwienie dostępu do dokumentów osobom nieupoważnionym (w szczególności poprzez zabezpieczenie dokumentów w szafach zamykanych na klucz, a także zabezpieczenie posiadanych pieczątek nagłówkowych i imiennych, zamkniecie pomieszczenia i zdanie kluczy na przechowanie);
6) właściwego zabezpieczenia danych osobowych przetwarzanych w formie elektronicznej, nieudostępniania swojego identyfikatora i hasła oraz posiadanych informacji o zastosowanych zabezpieczeniach, a także do zabezpieczenia oprogramowania, nośników i kart dostępu do systemu;
7) niezwłocznego informowania ADO o stwierdzonych nieprawidłowościach, w szczególności:
   a) dotyczących zabezpieczenia pomieszczeń,
   b) śladach wskazujących na podmianę sprzętu lub jego elementów, włamanie do systemu,
   c) utracie, braku dostępu lub nieautoryzowanej modyfikacji danych,
   d) innych stwierdzonych nieprawidłowościach mających wpływ na bezpieczeństwo danych osobowych przetwarzanych przez ADO;
8) wykorzystywania do pracy w systemie wyłącznie przydzielonego przez ASI profilu z wyłączeniem systemu informatycznego, w którym ze względu na charakter programu wykorzystywanego do obsługi zbioru nie jest to możliwe;
9) niewykonywania we własnym zakresie kopii przetwarzanych danych bez wiedzy i zgody ADO oraz na nośnikach niewydanych przez ADO lub ASI;
10) niepodejmowania jakichkolwiek prób obejścia zastosowanych zabezpieczeń oraz dokonywania zmian w konfiguracji systemu operacyjnego, wyłączania programu antywirusowego i zrywania zabezpieczeń;
11) niedokonywania samodzielnej podmiany elementów lub przenoszenia zestawu komputerowego.

§ 6

Infrastruktura przetwarzania danych osobowych, struktura zbiorów, sposób przepływu danych w systemie, zakres przetwarzania danych i strategia zabezpieczenia danych

Z uwagi na charakter przetwarzanych danych osobowych, a w szczególności z uwagi na konieczność zachowania w tajemnicy informacji, których opublikowanie zagrażałoby poufności przetwarzanych danych osobowych, a także mogłoby narazić system informatyczny ADO na nieuprawniony dostęp poprzez przełamanie lub ominiecie stosowanych zabezpieczeń, informacje w tytułowym zakresie zawarte są w oddzielnych dokumentach, które nie są publikowane i są przeznaczone wyłącznie do użytku służbowego pracowników ADO. ABI i ASI sporządza i prowadzi dodatkowe dokumenty, w których określa szczegółowo dane dotyczące infrastruktury przetwarzania danych osobowych, strukturę zbiorów danych, sposób przepływu danych w systemie, zakres przetwarzania danych oraz strategie zabezpieczenia danych osobowych (działania niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych).

1. Zbiory danych osobowych przetwarzane rzez ADO

   Zbiory danych osobowych przetwarzane są w siedzibie ADO, przy ulicy Sikorskiego 3 w Aleksandrowie Kujawskim. Wykaz pomieszczeń stanowiących obszar przetwarzania danych osobowych stanowi załącznik nr 1 do niniejszej Polityki. Wykaz zbiorów danych osobowych przetwarzanych przez ADO prowadzi i na bieżąco uaktualnia ABI. Wykaz prowadzony jest w oparciu o posiadaną dokumentację zbiorów ADO oraz zbiorów zgłoszonych do rejestracji na podstawie wniosków ADO (dane wrażliwe) do GIODO. Wykaz zbiorów stanowi załącznik nr 2 do niniejszej Polityki.

2. Struktura zbiorów danych i sposób przepływu danych pomiędzy systemami:
   1) dane osobowe przetwarzane mogą być w zbiorach prowadzonych zarówno w formie papierowej jak i w systemach informatycznych. Zasadniczo u ADO dane osobowe przetwarzane są w zbiorach przypisanych do jednej komórki organizacyjnej z uwagi na jej właściwość. Z tego powodu nie ma bezpośredniego przepływu informacji pomiędzy zbiorami przetwarzanymi w tej komórce organizacyjnej;
   2) system informatyczny ADO jest systemem szczelnym, odpowiednio skonfigurowanym, zabezpieczonym i chronionym przez ASI. W ramach tego systemu istnieje sieć, w której pracują wszystkie stanowiska komputerowe ADO, a dostęp do niej mają tylko wskazane przez ADO stanowiska komputerowe i użytkownicy;

3) zbiory zawierają dane wynikające z przepisów, na podstawie których zbiory są zakładane oraz dane do przetwarzania których są wymagane zgody. Poszczególne zbiory różnią się zakresem gromadzonych danych wynikających z ich specyfiki. Zabronione jest przetwarzanie danych wykraczających poza zakres i cel ich przetwarzania.
4) opis struktury zbiorów danych osobowych stanowi załącznik nr 3 do niniejszej Polityki. Zbiór danych osobowych zawiera informacje:
   a) nazwa zbioru danych,
   b) oznaczenie ADO i adres jego siedziby/miejsca zamieszkania oraz numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeśli został mu nadany,
   c) jeśli został wyznaczony przedstawiciel (art. 31a ustawy) – jego oznaczenie, adres siedziby lub miejsca zamieszkania,
   d) jeśli było powierzenie danych (art. 31ustawy) – oznaczenie podmiotu, któremu dane powierzono, adres siedziby lub miejsca zamieszkania,
   e) podstawa prawna upoważniająca do przetwarzania danych osobowych,
   f) cel przetwarzania danych,
   g) opis kategorii osób, których dane są przetwarzane,
   h) zakres przetwarzanych danych,
   i) sposób zbierania danych,
   j) oznaczenie odbiorcy danych,
   k) informacja dotycząca ewentualnego przekazywania danych do państwa trzecich,
   l) w stosunku do zbioru danych w rejestrze podaje się także datę dokonania wpisu informacji oraz ich ostatniej aktualizacji,
   m) w przypadku wykreślenia zbioru danych z rejestru wskazuje się nazwę zbioru danych oraz daty wpisania i wykreślenia,
   n) informacje o zbiorze danych są udostępniane w rejestrze w powszechnie zrozumiałej formie,
   o) ABI dokonuje wpisu zbioru w przypadku rozpoczęcia przetwarzania w nim danych, aktualizacji informacji w przypadku zmiany informacji objętych wpisem, wykreślenia zbioru danych w przypadku zaprzestania,
   p) wpisu do rejestru dokonuje się niezwłocznie po zaistnieniu zdarzenia, powodującego obowiązek dokonania wpisu,
   q) w rejestrze prowadzi się wykaz zmian, który zawiera wskazanie rodzaju zmiany (nowy wpis, aktualizacja, wykreślenia), datę dokonania zmiany, zakres zmiany,
   r) w przypadku prowadzenia rejestru w postaci elektronicznej, ABI udostępnia rejestr do przeglądania przez:

- udostępnienie rejestr na stronie internetowej ADO, przy czym na stronie głównej umieszcza się odwołanie umożliwiające bezpośredni dostęp do rejestru lub;
- udostępnienie każdemu zainteresowanemu rejestru na stanowisku dostępowym w systemie informatycznym ADO znajdującym się w siedzibie lub miejscu zamieszkania ADO;
- w przypadku prowadzenia rejestru w postaci papierowej, ABI udostępnia każdemu zainteresowanemu jego treść w siedzibie lub miejscu zamieszkania ADO;
- ADO zapewnia w systemie informatycznym możliwość realizacji czynności, o których mowa powyżej.

3. Powierzenie przetwarzania danych.
   1) dane osobowe przetwarzane przez ADO mogą być zgodnie z ustawą powierzane w celu przetwarzania innemu podmiotowi (przetwarzającemu), w związku z tym:
      a) przetwarzający występuje z pisemnym wnioskiem do ADO, w którym określa zakres danych i cel ich przetwarzania lub ADO wybiera przetwarzającego, który będzie wspierał ADO w procesie przetwarzania danych;
      b) w przypadku wyboru przetwarzającego przez ADO, ADO opracowuje wytyczne w celu wyboru przetwarzającego;
      c) ADO opracowuje treść umowy powierzenia;
      d) ABI dokonuje analizy polityki bezpieczeństwa i instrukcji zarządzania systemem przetwarzającego pod kątem poziomu bezpieczeństwa (równy lub wyższy niż poziom określony w niniejszej Polityce);
      e) ADO i ABI dokonują kontroli przestrzegania zapisów umowy powierzenia przez przetwarzającego;
   2) przetwarzający, który jest dostawcą systemu informatycznego i przetwarza dane osobowe w ramach obsługi systemu, dostarcza do ADO wykaz osób, którzy mają uzyskać upoważnienia do przetwarzania danych osobowych od ADO.

4. Rejestracja zbiorów danych osobowych / wykaz zbiorów.

   W przypadku zbiorów danych osobowych podlegających obowiązkowi zgłoszeniowemu do GIODO Polityka określa procedury ich zgłoszenia.

   1) Właściciel zasobów jest zobowiązany zgłosić Administratorowi Bezpieczeństwa Informacji zamiar utworzenia nowego zbioru danych osobowych wraz z wskazaniem podstawy przetwarzania danych, uzasadnieniem celowości, zakresu i sposobu zbierania danych osobowych.

2) Administratora Bezpieczeństwa Informacji weryfikuje zbiór pod kątem obowiązku zgłoszeniowego, jeśli obowiązek jest zachowany, przystępuje się do sporządzania wniosku rejestracyjnego
3) Administratora Bezpieczeństwa Informacji weryfikuje wniosek o utworzenie nowego zbioru danych osobowych oraz analizuje nowy zbiór danych pod kątem obowiązku zgłoszenia zasobu, jako zbioru danych do rejestracji w GIODO.
4) Zgłoszenie / zmiana wniosku zgłoszenia zbioru do rejestracji przez GIODO przygotowywane jest wspólnie przez Administratora Bezpieczeństwa Informacji i Właściciela zasobów.
5) Administrator Bezpieczeństwa Informacji sprawdza opisane zgłoszeniu rejestracyjnym warunki techniczne o organizacyjne dotyczące zabezpieczeń w systemie informatycznym, a w przypadku niewystarczającego poziomu zabezpieczeń występuje z wnioskiem do Administratora Danych o podniesienie poziomu tych zabezpieczeń.
6) Sprawdzony przez Administratora Bezpieczeństwa Informacji projekt zgłoszenia zbioru danych osobowych do rejestracji w GIODO jest przedstawiany Administratorowi Danych Osobowych do podpisu.
7) Administrator Bezpieczeństwa Informacji - po akceptacji Administratora Danych Osobowych - zgłasza wniosek o rejestrację zbioru danych osobowych do GIODO i wyznacza Właściciela zasobów danych osobowych dla zarejestrowanego zbioru danych osobowych.
8) Administrator Bezpieczeństwa Informacji uzupełnia Politykę, dokumenty z nią powiązane oraz pozostałe dokumenty obowiązujące w przedsiębiorstwie w zakresie ochrony danych osobowych o informacje na temat nowego zbioru.

5. Opis struktury zbiorów danych osobowych.

1) Dane osobowe mogą być przetwarzane w zbiorach danych, przy zastosowaniu systemów informatycznych oraz zbiorów ewidencyjnych w postaci kartotek, skorowidzów, wydruków, ksiąg i wykazów;
2) Zawartość pól informacyjnych występujących w systemach zastosowanych w celu przetwarzania danych osobowych, musi być zgodna z przepisami prawa, które uprawniają lub zobowiązują Administratora Bezpieczeństwa Informacji do przetwarzania danych osobowych;
3) Administrator Systemów Informatycznych w oparciu o informacje uzyskane od Właścicieli zasobów danych osobowych, prowadzi - Ewidencję stosowanych systemów i programów (w tym licencji oprogramowania), zastosowanych do przetwarzania danych osobowych;

4) Opis struktury zbiorów danych osobowych przetwarzanych w systemach informatycznych prowadzi Administrator Systemów Informatycznych;
5) Na żądanie Administrator Bezpieczeństwa Informacji lub osoby przez niego upoważnionej, Administrator Systemu Informatycznego zobowiązany jest do wskazania powiązań między polami informacyjnymi, które zawierają dane osobowe w systemie;
6) Przepływ danych pomiędzy systemami zastosowanymi w celu przetwarzania danych osobowych może odbywać się w postaci przepływu jednokierunkowego lub przepływu dwukierunkowego;
7) Przepływ jednokierunkowy oznacza, że system informatyczny udostępnia dane ze zbioru (bazy) danych tylko w trybie „do odczytu";
8) Przepływ dwukierunkowy umożliwia upoważnionemu użytkownikowi korzystanie z danych w trybach „do odczytu" i „do zapisu", tj. umożliwia wprowadzanie nowych danych i modyfikację istniejących;
9) Przesyłanie danych pomiędzy systemami może odbywać się w sposób manualny, przy wykorzystaniu nośników zewnętrznych (np. płyta CD, DVD, dysk wymienny, PenDrive itp.) lub w sposób półautomatyczny, przy wykorzystaniu funkcji eksportu/ importu danych za pomocą teletransmisji (np. poprzez szyfrowaną sieć teleinformatyczną).

§ 7

Środki techniczne i organizowanie niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Upoważnienia do przetwarzania danych osobowych udziela ADO.
   l) wydanie upoważnienia:
      a) wniosek o wydanie upoważnienia sporządza ADO zgodnie z przyjętymi procedurami (wniosek pisemny lub ustny),
      b) wniosek należy przekazać do ABI,
      c) we wniosku oprócz danych użytkownika, pełnej nazwy zbioru określa się m.in.:
         - zakres upoważnienia do przetwarzania danych w zbiorze;
         - informacje o potrzebie przeszkolenia użytkownika (obowiązkowo dla osób, które wcześniej nie odbyły stosownego szkolenia w tym zakresie);
      d) wniosek sporządza się przed przystąpieniem pracownika do przetwarzania danych w zbiorze danych osobowych - wniosek należy złożyć z wyprzedzeniem uwzględniającym czas niezbędny do załatwienia formalności związanych z wydaniem upoważnienia oraz przeprowadzeniem szkolenia;

2) cofnięcie upoważnienia:
   a) ADO przekazuje niezwłocznie do ABI wniosek o cofnięcie upoważnienia wydanego podległemu pracownikowi,
   b) w szczególności upoważnienie unieważnia się w przypadkach:
      - rozwiązania lub wygaśnięcia stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniona była osoba upoważniona,
      - odsunięcia od prac związanych z przetwarzaniem danych osobowych, do których wydane było upoważnienie, np. spowodowanych przeniesieniem do innej komórki organizacyjnej lub zmiany zakresu obowiązków,
      - wypowiedzenia umowy o pracę;
3) upoważnienie sporządzane jest w trzech jednobrzmiących egzemplarzach, po jednym dla ADO (kadry) i Administratora Bezpieczeństwa Informacji, który prowadzi ewidencję wydanych upoważnień oraz osoby upoważnionej. Wzór upoważnienia określony jest w załączniku nr 4 do niniejszej Polityki.

2. Zabezpieczenie sprzętu.
   1) ASI udziela wskazówek użytkownikom, jak postępować, aby zapewnić prawidłową eksploatacje systemu informatycznego, zwłaszcza poprzez:
      a) ochronę nośników przenośnych - w tym także nośników danych, na których przechowywane są kopie zapasowe,
      b) właściwe korzystanie z systemu informatycznego,
      c) prawidłową lokalizacje komputerów;
   2) wszystkie urządzenia systemu informatycznego mające zasadnicze znaczenie dla bezpieczeństwa danych są zasilane za pośrednictwem zasilaczy awaryjnych;
   3) okablowanie sieciowe zostało zaprojektowane w ten sposób, że urządzenia aktywne sieci są zabezpieczone w pomieszczeniach, do których dostęp ma wyłącznie ASI, ADO i ABI;
   4) bieżąca konserwacja sprzętu wykorzystywanego w systemie informatycznym do przetwarzania danych prowadzona jest wyłącznie przez ASI. Naprawy wykonywane przez ASI realizowane są pod nadzorem ABI. W czasie naprawy dane osobowe chronione są przed nieuprawnionym dostępem, a nośniki, na których przetwarzano dane osobowej nie podlegają wymianie lub naprawie gwarancyjnej poza siedzibą ADO;
   5) ABI dopuszcza konserwacje i naprawę sprzętu poza siedzibą ADO jedynie po usunięciu nośników danych osobowych. Zużyte nośniki wykorzystywane do przetwarzania danych osobowych mogą być przekazane do użytkowania w innym systemie informatycznym po trwałym usunięciu danych, a nośniki uszkodzone muszą być zniszczone przez ASI w sposób uniemożliwiający odczyt danych;

3. Zabezpieczenia sprzętu i danych osobowych.

Użytkownik systemu jest zobowiązany do niezwłocznego poinformowania ABI o awariach sprzętu wykorzystywanego do przetwarzania danych osobowych. O awariach mających bezpośredni wpływ na bezpieczeństwo danych osobowych ABI informuje ADO i ASI. Istotne dla bezpieczeństwa danych jest wyrobienie i utrwalenie przez każdą osobę upoważnioną do przetwarzania danych lub użytkownika nawyku:

1) ekrany komputerowe powinny być tak ustawione, by osoby niepowołane nie mogły oglądać ich zawartości;
2) nie należy pozostawiać bez kontroli dokumentów, nośników danych i sprzętu;
3) należycie dbać o prawidłową wentylację komputerów (nie można zasłaniać kratek wentylatorów meblami, zasłonami lub stawiać komputerów tuż przy ścianie);
4) nie należy podłączać do listew podtrzymujących napięcie przeznaczonych do zasilania systemu informatycznego innych urządzeń (np. grzejniki, czajniki, wentylatory itp.);
5) należy chronić akta i nośniki informatyczne przed nieuprawnionym dostępem i utratą;
6) należy kasować po wykorzystaniu dane na nośnikach przenośnych;
7) nie należy używać powtórnie dokumentów zadrukowanych jednostronnie;
8) nie należy zapisywać hasła wymaganego do uwierzytelnienia się w systemie;
9) osoby upoważnione do przetwarzania danych osobowych nie powinny ingerować w konfiguracje powierzonego sprzętu i oprogramowanie (szczególnie komputerów przenośnych) nawet wtedy, gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych;
10) należy przestrzegać obowiązujących zasad korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosować się do zaleceń ABI;
11) stanowisko pracy można opuścić dopiero po aktywowaniu się wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób;
12) należy kopiować tylko jednostkowe dane (pojedynczych plików). Obowiązuje zakaz robienia kopii całych zbiorów danych lub takich ich części, które nie są konieczne do wykonywania obowiązków przez pracownika. Jednostkowe dane mogą być kopiowane na nośniki informatyczne po ich zaszyfrowaniu, a przechowywane w zamkniętych na klucz szafach. Po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki;
13) nie należy udostępniać danych osobowych pocztą elektroniczną;
14) pocztę służbową należy wykorzystywać tylko do celów związanych z wykonywaniem zadań zleconych przez ADO;
15) należy wykonywać kopie robocze danych z częstotliwością ustaloną przez ADO oraz właściwego zabezpieczenia nośników w miejscu określonym przez ADO;

16) zakończenie pracy w systemie informatycznym powinno nastąpić po zapisaniu wprowadzonych danych, a następnie prawidłowego wylogowaniu się użytkownika i wyłączeniu komputera oraz wyłączenia zasilania;
17) należy chować do szaf zamykanych na klucz wszelkie dokumenty, wydruki zawierające dane osobowe przed opuszczeniem miejsca pracy albo zniszczyć wydruki wstępne w niszczarce. Jeżeli umieszczenie wszystkich dokumentów zawierających dane osobowe w zamykanych szafach jest niemożliwe, ABI lub osoba upoważniona powiadamia o tym ADO, aby dokonano zakupu nowych mebli biurowych;
18) nie należy pozostawiać osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez nadzoru osoby upoważnionej do przetwarzania danych osobowych;
19) należy zachować w tajemnicy przetwarzane dane osobowe, w tym także wobec osób najbliższych i współpracowników;
20) należy umieścić klucze do szaf w miejscu ustalonym przez ADO;
21) należy zamykać okna w sytuacjach grożących bezpieczeństwu danych lub nośników (np. silne opady deszczu, porywisty wiatr powodujący przeciągi itp.) oraz przed opuszczeniem miejsca pracy;
22) należy zamykać drzwi na klucz po zakończeniu pracy w danym dniu i zabezpieczyć go w wyznaczonym miejscu.

4. Postępowanie z nośnikami.

Osoby upoważnione do przetwarzania danych osobowych powinny pamiętać zwłaszcza o tym, że:

1) dane z nośników przenośnych niebędących kopiami zapasowymi, po wprowadzeniu do systemu informatycznego powinny być trwale usuwane programem trwale usuwającym dane albo przez fizyczne zniszczenie nośnika (czynności te wykonuje ASI). Jeśli istnieje uzasadniona konieczność, dane pojedynczych osób (a nie całe zbiory czy szerokie wypisy ze zbiorów) mogą być przechowywane na specjalnie oznaczonych nośnikach. Nośniki te musza być przechowywane pod nadzorem ABI w zamkniętych na klucz szafach, niedostępnych osobom postronnym. Po ustaniu przydatności tych danych nośniki powinny być trwale kasowane lub niszczone. Czynności, o których mowa wyżej, mogą być wykonywane tylko w uzgodnieniu z ABI;
2) uszkodzone lub wycofane z użycia nośniki należy zniszczyć zgodnie z procedurami określonymi w Instrukcji zarządzania;
3) zabrania się powtórnego używania do sporządzania brudnopisów kart pism jednostronnie zadrukowanych, jeśli zawierają one dane chronione. Zaleca się

natomiast dwustronne drukowanie brudnopisów pism i sporządzanie dwustronnych dokumentów;

4) po wykorzystaniu, wydruki zawierające dane osobowe należy zniszczyć niezwłocznie w niszczarce.

Z czynności, o których mowa powyżej, sporządza się protokół zniszczenia nośników zawierających dane osobowe. Wzór protokołu stanowi załącznik nr 5 do niniejszej Polityki bezpieczeństwa.

5. Wymiana danych i ich bezpieczeństwo.

1) bezpieczeństwo danych, a w szczególności ich integralność i dostępność, w dużym stopniu zależy od zdyscyplinowanego, codziennego umieszczania danych przechowywanych lokalnie;
2) sporządzanie kopii zapasowych następuje w trybie opisanym w § 5 pkt 4 Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
3) inne wymogi bezpieczeństwa systemowego są określane w instrukcjach obsługi producentów sprzętu i używanych programów, wskazówkach ABI oraz Instrukcji zarządzania;
4) przed atakami z sieci zewnętrznej wszystkie komputery ADO (w tym także przenośne) chronione są środkami dobranymi przez ASI w porozumieniu z ABI, ważne jest, by użytkownicy zwracali uwagę na to, czy oprogramowanie, na którym pracują, domaga się aktualizacji tych zabezpieczeń, o wszystkich takich przypadkach należy informować ASI albo zainstalować aktualizacje jeżeli tak skonfigurowano wcześniej oprogramowanie);
5) ASI w porozumieniu z ABI dobiera elektroniczne środki ochrony przed atakami z sieci stosownie do pojawiania się nowych zagrożeń (nowe wirusy, robaki, trojany, inne możliwości wdarcia się do systemu), a także stosownie do rozbudowy systemu informatycznego ADO i powiększania bazy danych. Jednocześnie należy zwracać uwagę, czy rozwijający się system zabezpieczeń sam nie wywołuje nowych zagrożeń;
6) należy stosować ochronę kryptograficzną przy przesyłaniu danych:
   a) za pomocą poczty elektronicznej - stosuje się POP - tunelowanie, szyfrowanie połączenia,
   b) pracowników, niezbędnych do wykonania przelewów wynagrodzeń, używa się bezpiecznych stron "https://" oraz potwierdza przy pomocy środków uwierzytelnienia określonych przez organizatora (np. bank),
   c) ustaloną przez ADO w zbiorach.

6. Kontrola dostępu do systemu.
   1) poszczególnym osobom upoważnionym do przetwarzania danych osobowych przydziela się konta opatrzone niepowtarzalnym identyfikatorem, umożliwiające dostęp do danych, zgodnie z zakresem upoważnienia do ich przetwarzania;
   2) ASI uczestnicząc w procesie opiniowania wniosku ADO przydziela pracownikowi upoważnionemu do przetwarzania danych konto w systemie informatycznym, dostępne po wprowadzeniu prawidłowego identyfikatora i uwierzytelnieniu hasłem (system wymusza zmianę hasła przy pierwszym logowaniu oraz co 30 dni);
   3) w razie potrzeby, po uzyskaniu uprzedniej akceptacji ABI, ASI może przydzielić konto opatrzone identyfikatorem osobie upoważnionej do przetwarzania danych osobowych, nieposiadającej statusu pracownika;
   4) do zagwarantowania poufności i integralności danych osobowych konieczne jest przestrzeganie przez użytkowników swoich uprawnień do pracy w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń ABI i ASI;
   5) zestawy komputerowe i komputery przenośne są ewidencjonowane przez ABI.

7. Kontrola dostępu do sieci.
   1) ASI konfiguruje dostęp do internetu oraz zakres stron internetowych dostępnych w sieci zgodnie z polityką obowiązującą w tej sprawie u ADO;
   2) ASI wykorzystuje centralną zaporę sieciową w celu separacji lokalnej sieci od sieci publicznej;
   3) stacje robocze i komputery przenośne, w których przetwarzane są dane osobowe, skonfigurowane są w sposób zapewniający bezpieczne korzystanie zarówno z zasobów lokalnych jak i sieciowych;
   4) operacje za pośrednictwem rachunku bankowego ADO może wykonywać wyłącznie pracownik do tego upoważniony, po uwierzytelnieniu zgodnie z procedurami określonymi przez bank obsługujący rachunek;
   5) osoby, którym założono konta imienne na poczcie elektronicznej ADO, zobowiązane są do:
      a) wykorzystywania poczty tylko do celów służbowych,
      b) przestrzegania zasady, aby pocztą nie przesyłać plików zawierających dane osobowe podlegające ochronie,
      c) przestrzegania zasady, aby nie otwierać wiadomości od niezaufanych adresatów (spam).

8. Komputery przenośne.
   1) do przetwarzania danych osobowych zasadniczo wykorzystywane są komputery stacjonarne;
   2) wynoszenie komputerów przenośnych poza siedzibę ADO może nastąpić po uzyskaniu zgody ADO oraz po uprzednim uzgodnieniu z ABI;
   3) o ile to możliwe, przy przetwarzaniu danych osobowych na komputerach przenośnych obowiązują procedury określone w Instrukcji zarządzania systemem informatycznym, dotyczące pracy na komputerach stacjonarnych;
   4) użytkownicy, którym zostały powierzone komputery przenośne, powinni chronić je w sposób szczególny przed uszkodzeniem, kradzieżą i dostępem osób postronnych;
   5) obowiązuje zakaz używania komputerów przenośnych służących do przetwarzania danych osobowych przez osoby inne niż użytkownicy, którym zostały one powierzone;
   6) zasady haseł oraz nadawanie uprawnień dostępu do komputera następuje na zasadach określonych dla komputerów stacjonarnych;
   7) obowiązuje zakaz przetwarzania na komputerach przenośnych całych zbiorów danych lub szerokich z nich wypisów, nawet w postaci zaszyfrowanej;
   8) użytkownicy przetwarzający dane osobowe na komputerach przenośnych obowiązani są do systematycznego wprowadzania tych danych w określone miejsca na stacje robocze ADO, a następnie do trwałego usuwania ich z pamięci powierzonych komputerów przenośnych;
   9) szczegółowe zasady postępowania z komputerami przenośnymi zawarto w Instrukcji zarządzania systemem informatycznym.

9. Monitorowanie dostępu do systemu i jego użycia.
   l) w porozumieniu z ABI, ASI jest upoważniony do monitorowania wykorzystania sieci i poszczególnych stacji roboczych pod kątem ich nieuprawnionego wykorzystania - w tym celu może używać specjalistycznego oprogramowania gromadzącego między innymi:
      a) daty wprowadzenia danych do systemu,
      b) identyfikator użytkownika wprowadzającego dane osobowe do systemu,
      c) informacje o odbiorcach w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, o dacie i zakresie tego udostępnienia,
      d) sprzeciwu wobec przetwarzania danych osobowych, o którym mowa w art. 32 ust. l pkt 8 ustawy,
      e) źródła danych - w przypadku zbierania danych nie od osoby, której one dotyczą;

2) w zbiorach umożliwiających monitorowanie działania użytkownika, odnotowanie informacji następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych;
3) dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w pkt 1 lit. a - c, ASI przeprowadza synchronizacje zegarów stacji roboczych, ograniczając dopuszczalność zmian w ustawieniach zegarów. Jakiekolwiek zmiany ustawień zegarów mogą być dokonywane jedynie przez ASI z konta o uprawnieniach administracyjnych;
4) system informatyczny ADO umożliwia zapisywanie zdarzeń systemowych na potrzeby audytu i przechowywanie informacji o nich przez określony czas. Zapisy takie obejmują:
   a) identyfikator użytkownika,
   b) datę i czas zalogowania i wylogowania się z systemu,
   c) tożsamość stacji roboczej,
   d) zapisy udanych i nieudanych prób dostępu do systemu,
   e) zapisy udanych i nieudanych prób dostępu do danych osobowych i innych zasobów systemowych.

10. Przeglądy okresowe zapobiegające naruszeniom obowiązku szczególnej staranności administratora danych.
    1) ADO przeprowadza nie rzadziej niż raz w roku (IV kwartał) przegląd przetwarzanych danych osobowych pod kątem celowości ich dalszego przetwarzania oraz przestrzegania zasad ochrony przetwarzanych danych;
    2) ABI może zarządzić przeprowadzenie dodatkowego przeglądu w wyżej określonym zakresie w razie zmian w obowiązującym prawie, ograniczających dopuszczalny zakres przetwarzanych danych osobowych (dodatkowy przegląd jest możliwy także w sytuacji zmian organizacyjnych ADO);
    3) o zbiorach, w których zaprzestano przetwarzania danych osobowych, należy niezwłocznie poinformować ABI;
    4) wzory dokumentów przewidujących powiadomienie, o którym mowa w art. 24 lub 25 ustawy, mogą być stosowane po zaakceptowaniu przez ABI.

11. Szkolenia z zakresu ochrony danych osobowych.
    1) ABI prowadzi szkolenia:
       a) osób, które mają zostać upoważnione do przetwarzania danych osobowych;

b) dodatkowe dla wszystkich osób upoważnionych do przetwarzania danych osobowych w przypadku zmiany zasad lub procedur ochrony danych osobowych mających istotnych wpływ na bezpieczeństwo danych;
c) osób innych niż upoważnione do przetwarzania danych, jeśli pełnione przez nie funkcje wiążą się z zabezpieczeniem danych osobowych;
d) dodatkowe wynikające z innych potrzeb służbowych.

2) Celem szkolenia, które powinien odbyć każdy użytkownik zbioru danych osobowych, przed otrzymaniem upoważnienia do przetwarzania danych osobowych jest:
a) poznawanie podstaw prawnych dotyczących przetwarzania danych osobowych;
b) poznanie celu, strategii i polityki zabezpieczenia systemu tradycyjnego i informatycznego używanego do przetwarzania danych osobowych;
c) ocena oraz analiza ryzyka związanego z utratą poufności przetwarzanych danych osobowych;
d) określenie środków bezpieczeństwa dla systemów przetwarzania danych osobowych w tym sposoby ochrony danych przed osobami postronnymi oraz procedury udostępniania danych osobom, których dane dotyczą oraz sporządzania i przechowywania nośników zawierających kopie danych, niszczenia wydruków i nośników;
e) omówienie zasad i procedur określonych w Polityce bezpieczeństwa oraz zapoznanie się z „Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" w tym obowiązki osób upoważnionych do przetwarzania danych osobowych;
f) omówienie zagadnień związanych z sytuacją naruszenia ochrony danych osobowych oraz odpowiedzialności za naruszenie obowiązków w zakresie ochrony danych osobowych.

§ 8
Udostępnianie danych osobowych

1. Udostępnianie danych osobowych może nastąpić wyłącznie na podstawie obowiązujących przepisów tylko na podstawie pisemnego, uzasadnionego wniosku.

2. ADO realizując politykę bezpieczeństwa, zapewnia dostęp do przetwarzanych danych osobowych osobom fizycznym będącym dysponentami tych danych, którzy powierzyli swoje dane ADO w związku z pobytem, zatrudnieniem lub występowaniem w roli kontrahenta.

3. Zabrania się udzielania informacji z zakresu danych osobowych interesantom zgłaszającym się telefonicznie, osobom, których tożsamości nie można ustalić oraz osobom nieupoważnionym.

4. Udostępnianie danych osobowych funkcjonariuszom publicznym może nastąpić tylko po przedłożeniu wniosku o przekazanie lub udostępnienie informacji. Wniosek ten powinien mieć formę pisemną i zawierać:
   1) oznaczenie wnioskodawcy;
   2) wskazanie przepisów uprawniających do dostępu do informacji;
   3) określenie rodzaju i zakresu potrzebnych informacji oraz formy ich przekazania lub udostępnienia;
   4) wskazanie imienia, nazwiska i stopnia służbowego funkcjonariusza upoważnionego do pobrania informacji lub zapoznania się z ich treścią.

5. Udostępnianie danych osobowych na podstawie wniosku zawierającego wszystkie cztery elementy wniosku pisemnego może nastąpić w formie ustnej tylko wtedy, gdy zachodzi konieczność niezwłocznego działania, np. w trakcie pościgu za osobą podejrzaną o popełnienie czynu zabronionego albo podczas wykonywania czynności mających na celu ratowanie życia i zdrowia ludzkiego lub mienia.

6. Osoba udostępniająca dane osobowe jest obowiązana zażądać od osoby wymienionej w pkt 4 pokwitowania pobrania dokumentów zawierających informacje przekazane na podstawie pisemnego wniosku albo potwierdzenia faktu uzyskania wglądu w treść informacji.

7. Jeśli informacje są przekazywane na podstawie ustnego wniosku, należy stosownie do okoliczności zwrócić się z prośbą o pokwitowanie albo potwierdzenie. Jeśli pokwitowanie albo potwierdzenie ze względu na okoliczności udostępniania nie są możliwe, osoba udostępniająca informacje sporządza na tę okoliczność notatkę służbową.

§ 9

Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych

1. Osoba przetwarzająca dane osobowe w zbiorze, choć ich przetwarzanie jest niedopuszczalne albo do których przetwarzania osoba nie jest uprawniona, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

2. Jeżeli czyn dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.

3. Niezastosowanie się do prowadzonej przez ADO Polityki bezpieczeństwa przetwarzania danych osobowych, której założenia określa niniejszy dokument, lub naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu pracy.

4. Niezależnie od rozwiązania stosunku pracy osoby popełniające przestępstwo będą pociągane do odpowiedzialności karnej zwłaszcza na podstawie art. 49-54 ustawy oraz art. 266 Kodeksu karnego. Przykładowo przestępstwo można popełnić wskutek:
   1) udostępnienia danych osobowych osobom nieupoważnionym;
   2) stworzenia możliwości dostępu do danych osobowych osobom nieupoważnionym albo osobie nieupoważnionej;
   3) niezabezpieczenia nośnika lub komputera przenośnego służącego do przetwarzania danych osobowych;
   4) podjecie próby obejścia lub złamania zabezpieczeń stosowanych w systemie informatycznym ADO.

5. Administrujący zbiorem danych, który nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub nieprzekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w niniejszej ustawie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

6. Odpowiedzialności za naruszenie zasad przetwarzania danych osobowych podlegają wszystkie osoby przetwarzające dane osobowe u ADO.

§ 10
Archiwizowanie informacji zawierającej dane osobowe

Zasady i tryb postępowania z materiałami archiwalnymi przez ADO określają przepisy wewnętrzne.

§ 11
Przegląd dokumentacji ochrony danych osobowych.

1. Polityka bezpieczeństwa powinna być poddawana przeglądowi raz w roku. W razie istotnych zmian dotyczących przetwarzania danych osobowych ABI może zarządzić przegląd Polityki bezpieczeństwa stosownie do potrzeb. ABI analizuje, czy Polityka bezpieczeństwa i pozostała dokumentacja z zakresu ochrony danych osobowych jest adekwatna do:
   1) zmian w budowie systemu informatycznego;
   2) zmian organizacyjnych ADO mających znaczący wpływ na ochronę danych osobowych;
   3) zmian w obowiązującym prawie.

2. Fakt wystąpienia naruszeń winien skutkować zmianami Polityki i dokumentacji powiązanej.

3. Wszelkie zmiany Polityki – mające wpływ na poziom bezpieczeństwa ochrony danych osobowych – winny być zatwierdzane przez Administratora Danych Osobowych.

§ 12
Inne zalecenia i postanowienia końcowe

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z Polityką bezpieczeństwa informacji i Instrukcją zarządzania oraz złożyć stosowne oświadczenie, potwierdzające znajomość dokumentów oraz przyjęcie do realizacji i stosowania uregulowań tam zawartych. Oświadczenie o zapoznaniu się z dokumentacją dotyczącą ochrony danych osobowych stanowi załącznik nr 3 do Zarządzenia Kierownika Powiatowym Centrum Pomocy Rodzinie w Aleksandrowie Kujawskim w sprawie wprowadzenia Polityki bezpieczeństwa informacji i Instrukcji zarządzania systemem informatycznym, w którym przetwarzane są dane osobowe w Powiatowym Centrum Pomocy Rodzinie w Aleksandrowie Kujawskim

2. Integralną częścią Polityki bezpieczeństwa informacji jest „Instrukcja zarządzania systemem informatycznym, w którym przetwarzane są dane osobowe w Powiatowym Centrum Pomocy Rodzinie w Aleksandrowie Kujawskim" zawierająca szczegółowe zasady postępowania w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym.

3. W sprawach nieokreślonych niniejszą Polityką bezpieczeństwa należy stosować przepisy dotyczące ochrony danych osobowych oraz inne uregulowania dotyczące pracy biurowej i kancelaryjnej, postępowania z dokumentami, o ile nie obniżają zastosowanego poziomu zabezpieczeń.

§ 13
Spis załączników

Załącznik nr 1 – Wykaz budynków i pomieszczeń stanowiących obszar przetwarzania danych osobowych

Załącznik nr 2 – Wykaz zbiorów danych osobowych oraz programów stosowanych do przetwarzania danych osobowych

Załącznik nr 3 – Struktura zbiorów danych osobowych i sposób przepływu danych pomiędzy poszczególnymi systemami

Załącznik nr 4 – Wzór upoważnienia do przetwarzania danych osobowych

Załącznik nr 5 – Wzór protokołu niszczenia nośników

Załącznik nr 6 – Wzór ewidencji osób upoważnionych

Załącznik nr 1 do Polityki

Wykaz budynków oraz pomieszczeń stanowiących obszar przetwarzania danych osobowych

Lp.	Adres budynku	Pomieszczenia, w których przetwarzane są dane osobowe	
		Pokój	Zbiór danych osobowych
(1)	(2)	(3)	(4)
1	ul. Sikorskiego 3 87 – 700 Aleksandrów Kujawski	**Pokój nr 2** Stanowisko ds. pomocy instytucjonalnej Samodzielne stanowisko pracy ds. pomocy środowiskowej i rodzinnej pieczy zastępczej Koordynatorzy rodzinnej pieczy zastępczej	Dane osobowe osób objętych pomocą Powiatowego Centrum Pomocy Rodzinie w Aleksandrowie Kujawskim
			Zbiór kadrowo-płacowy
			Rodziny zastępcze
			Rodzinne domy dziecka
		Pokój nr 3 Referat księgowy	Zlecenie operacji bankowych
		Serwerownia (szafa pancerna)	Zbiór kadrowo-płacowy
			Archiwum zakładowe
			Kandydaci do pracy
		Pokój nr 1 Wieloosobowe stanowisko ds. rehabilitacji społecznej	Rehabilitacja społeczna osób niepełnosprawnych
		Pokój nr 7 Stanowisko pracy ds. obsługi interesanta i monitoringu	Obieg korespondencji
			Monitoring budynku
			Książka kontroli

Załącznik nr 2 do Polityki

Wykaz zbiorów danych osobowych oraz programów stosowanych do przetwarzania danych osobowych

Lp.	Nazwa zbioru	Data rozpoczęcia przetwarzania	Postać Zbioru	Opis sposobu przechowywania	Nazwa systemu informatycznego
(1)	(2)	(3)	(4)	(5)	(6)
1	Zbiór kadrowo-płacowy (nie podlega zgłoszeniu do GIODO)	26.01.1999 rok	forma tradycyjna forma elektroniczna	Akta przechowywane w zamykanych szafach oraz dane zabezpieczone na stacjach roboczych	Kadry i Płace Płatnik GMB Włocławek ZUS Bankowość Elektroniczna KBS Aleks. Kuj.
2	Kandydaci do pracy (nie podlega zgłoszeniu do GIODO)	26.01.1999 rok	forma tradycyjna	Akta przechowywane w zamykanych szafach	Brak
3	Dane osobowe osób objętych pomocą Powiatowego Centrum Pomocy Rodzinie w Aleksandrowie Kujawskim	22.11.1999 rok	forma tradycyjna forma elektroniczna	Akta przechowywane w zamykanych szafach oraz dane zabezpieczone na serwerze	POMOST Sygnity
4	Obieg korespondencji	26.01.1999 rok	forma tradycyjna forma elektroniczna	Akta przechowywane w zamykanych szafach oraz dane zabezpieczone na stacjach roboczych	WORD, Mozilla Firefox, Internet Explorer;
5	Książka kontroli	26.01.1999 rok	forma tradycyjna	Akta przechowywane w zamykanych szafach	WORD, Mozilla Firefox, Internet Explorer;
6.	Rodziny zastępcze	26.01.1999 rok	forma tradycyjna	Akta przechowywane w zamykanych szafach	WORD, Mozilla Firefox, Internet Explorer;

7	Rodzinne domy dziecka	26.01.1999 rok	forma tradycyjna	Akta przechowywane w zamykanych szafach	WORD, Mozilla Firefox, Internet Explorer;
8	Archiwum zakładowe	26.01.1999 rok	forma tradycyjna	Akta przechowywane w zamykanych szafach	Brak
9	Zlecenie operacji bankowych	26.01.1999 rok	forma tradycyjna forma elektroniczna	Akta przechowywane w zamykanych szafach oraz dane zabezpieczone na serwerze	Bankowość Elektroniczna KBS Aleks. Kuj.
10	Rehabilitacja społeczna osób niepełnosprawnych	26.01.1999 rok	forma tradycyjna forma elektroniczna	Akta przechowywane w zamykanych szafach oraz dane zabezpieczone na serwerze	WORD, Mozilla Firefox, Internet Explorer;
11	Monitoring budynku	listopad 2014 r.	forma elektroniczna	Dane zabezpieczone na serwerze	System CCTV

Załącznik nr 3 do Polityki

Opis struktury zbiorów danych osobowych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi

Lp.	Nazwa zbioru	Opis zbioru	Pola informacyjne	Zgoda na przetwarzanie danych osobowych	Opis powiązań pól informacyjnych, przepływ danych
(1)	(2)	(3)	(4)	(5)	(6)
1	Zbiór kadrowo-płacowy	Dane osobowe pracowników Centrum	1. imię i nazwisko 2. imiona rodziców 3. data urodzenia 4. miejsce urodzenia 5. adres zamieszkania lub pobytu 6. numer ewidencyjny PESEL 7. Numer Identyfikacji Podatkowej 8. wykształcenie 9. staż pracy 10. nr konta bankowego 11. imię i nazwisko współmałżonka oraz dzieci 12. zajmowane stanowisko 13. stan cywilny 14. wysokość wynagrodzenia 15. informacje o niekaralności 16. dane o stanie zdrowia – badania w medycynie pracy 17. obciążenia komornicze 18. nr telefonu, adres poczty elektronicznej	Na przetwarzanie danych jest wymagana zgoda osoby, której dane dotyczą oraz bez zgody osoby, której dane dotyczą zezwalają przepisy prawa w celu dopełnienia obowiązków określonych w przepisach prawa	Brak powiązań
2	Kandydaci do pracy	Dane osób, które składają aplikacje dotyczące zatrudnienia w Centrum	1 imię i nazwisko 2 imiona rodziców 3 data urodzenia 4 adres zamieszkania lub pobytu 5 wykształcenie 6 przebieg dotychczasowego zatrudnienia	Na przetwarzanie danych jest wymagana zgoda osoby, której dane dotyczą	Brak powiązań
3	Dane osobowe osób objętych pomocą Powiatowego Centrum Pomocy Rodzinie w Aleksandrowie Kujawskim	Dane osób objętych pomocą Centrum	1. imię i nazwisko 2.nazwisko rodowe i z poprzedniego małżeństwa 3. imiona rodziców 4. data urodzenia 5. miejsce urodzenia 6. akta urodzenia, data i nr USC 7 adres zamieszkania lub	Na przetwarzanie danych jest wymagana zgoda osoby, której dane dotyczą oraz bez zgody osoby, której dane dotyczą	Brak powiązań

			pobytu stałego oraz data zameldowania 8 archiwalne adresy zamieszkania lub pobytu stałego oraz data zameldowania 9 adres czasowy oraz czas pobytu czasowego 10 archiwalne adresy czasowe oraz okresy pobytów czasowych 11 dokument tożsamości rodzaj, seria i nr, wystawca, rysopis 12 numer ewidencyjny PESEL 13 stan cywilny: imię i nazwisko współmałżonka, nazwisko rodowe i nazwisko z poprzedniego małżeństwa, data zawarcia małżeństwa, USC i numer aktu małżeństwa, data wydania i wydający dokument tożsamości 14 data zgonu, USC i numer aktu zgonu, 15 narodowość 16 obywatelstwo (data zmiany, podstawa prawna) 17 adnotacje o rozwodzie 18 dane o dochodach.	zezwalają przepisy prawa w celu dopełnienia obowiązków określonych w przepisach prawa	
4	Obieg korespondencji	Dane osób, które prowadzą korespondencję z Centrum	1 imię i nazwisko 2 adres korespondencji 3 adres poczty elektronicznej 4 numer telefonu	Na przetwarzanie danych jest wymagana zgoda osoby, której dane dotyczą oraz bez zgody osoby, której dane dotyczą zezwalają przepisy prawa w celu dopełnienia obowiązków określonych w przepisach prawa	Brak powiązań
5	Książka kontroli	Dane osób, które prowadzą kontrole w Centrum	1 imię i nazwisko 2 miejsce pracy 3 stanowisko 4 wykształcenie	Na przetwarzanie danych zezwalają	Brak powiązań

				przepisy prawa w celu dopełnienia obowiązków określonych w przepisach prawa	
6	Rodziny zastępcze	Dane osób zakwalifikowanych i pełniących funkcję rodziny zastępczej	1. imię i nazwisko 2.nazwisko rodowe i z poprzedniego małżeństwa 3. imiona rodziców 4. data urodzenia 5. miejsce urodzenia 6. akta urodzenia, data i nr USC 7adres zamieszkania lub pobytu stałego oraz data zameldowania 8 archiwalne adresy zamieszkania lub pobytu stałego oraz data zameldowania 9 adres czasowy oraz czas pobytu czasowego 10 archiwalne adresy czasowe oraz okresy pobytów czasowych 11 dokument tożsamości rodzaj, seria i nr, wystawca, rysopis 12 numer ewidencyjny PESEL 13 stan cywilny: imię i nazwisko współmałżonka, nazwisko rodowe i nazwisko z poprzedniego małżeństwa, data zawarcia małżeństwa, USC i numer aktu małżeństwa, data wydania i wydający dokument tożsamości 14 data zgonu, USC i numer aktu zgonu, 15 Narodowość 16 obywatelstwo (data zmiany, podstawa prawna) 17 adnotacje o rozwodzie 18 dane o dochodach.	Na przetwarzanie danych jest wymagana zgoda osoby, której dane dotyczą oraz bez zgody osoby, której dane dotyczą zezwalają przepisy prawa w celu dopełnienia obowiązków określonych w przepisach prawa	Brak powiązań

7	Rodzinne domy dziecka	Dane osób prowadzących rodzinne domy dziecka	1. imię i nazwisko 2.nazwisko rodowe i z poprzedniego małżeństwa 3. imiona rodziców 4. data urodzenia 5. miejsce urodzenia 6. akta urodzenia, data i nr USC 7adres zamieszkania lub pobytu stałego oraz data zameldowania 8 archiwalne adresy zamieszkania lub pobytu stałego oraz data zameldowania 9 adres czasowy oraz czas pobytu czasowego 10 archiwalne adresy czasowe oraz okresy pobytów czasowych 11 dokument tożsamości rodzaj, seria i nr, wystawca, rysopis 12 numer ewidencyjny PESEL 13 stan cywilny: imię i nazwisko współmałżonka, nazwisko rodowe i nazwisko z poprzedniego małżeństwa, data zawarcia małżeństwa, USC i numer aktu małżeństwa, data wydania i wydający dokument tożsamości 14 data zgonu, USC i numer aktu zgonu, 15 Narodowość 16 obywatelstwo (data zmiany, podstawa prawna) 17 adnotacje o rozwodzie 18 dane o dochodach.	Na przetwarzanie danych jest wymagana zgoda osoby, której dane dotyczą oraz bez zgody osoby, której dane dotyczą zezwalają przepisy prawa w celu dopełnienia obowiązków określonych w przepisach prawa	Brak powiązań
8	Archiwum zakładowe	Dane osób, które były zatrudnione w Centrum	1. imię i nazwisko 2. imiona rodziców 3. data urodzenia 4. miejsce urodzenia 5. adres zamieszkania lub pobytu 6. numer ewidencyjny PESEL 7. Numer Identyfikacji Podatkowej 8. wykształcenie	Na przetwarzanie danych jest wymagana zgoda osoby, której dane dotyczą oraz bez zgody osoby, której dane dotyczą zezwalają	Brak powiązań

			9. staż pracy 10. nr konta bankowego 11. imię i nazwisko współmałżonka oraz dzieci 12. zajmowane stanowisko 13. stan cywilny 14. wysokość wynagrodzenia 15. informacje o niekaralności 16. dane o stanie zdrowia – badania w medycynie pracy 17. obciążenia komornicze nr telefonu, adres poczty elektronicznej	przepisy prawa w celu dopełnienia obowiązków określonych w przepisach prawa	
9	Zlecenie operacji bankowych	Dane osób którym wykonano operację bankową z Centrum	1. imię i nazwisko 2. adres zamieszkania 3. nr konta bankowego	Na przetwarzanie danych jest wymagana zgoda osoby, której dane dotyczą oraz bez zgody osoby, której dane dotyczą zezwalają przepisy prawa w celu dopełnienia obowiązków określonych w przepisach prawa	Brak powiązań
10	Rehabilitacja społeczna osób niepełnosprawnych	Dane osób objętych pomocą Centrum	1. imię i nazwisko 2. data urodzenia 3. adres zamieszkania 4. PESEL 5. NIP 6. Seria i nr dokumentu tożsamości 7. nr telefonu 8. nr konta bankowego 9. wysokości dochodów 10. stopień i rodzaj niepełnosprawności 11. stan zdrowia 12. inne orzeczenia	Na przetwarzanie danych jest wymagana zgoda osoby, której dane dotyczą oraz bez zgody osoby, której dane dotyczą zezwalają przepisy prawa w celu dopełnienia obowiązków określonych w przepisach prawa	Brak powiązań
11	Monitoring budynku	Osoby i pojazdy znajdujące się na nagraniach w budynku Centrum oraz na zewnątrz	1. wizerunek osób i inne szczegóły, pozwalające na identyfikację 2. tablice rejestracyjne pojazdów	Przetwarzanie jest niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych	Brak powiązań

				przez Centrum albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.	

Załącznik nr 4 do Polityki

WZÓR

Aleksandrów Kujawski, dnia ..... r.

...../.....

UPOWAŻNIENIE

Nr ...../.....

Na podstawie art. 37 w związku z art. 39 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r. poz. 2135, z późn. zm.)

Upoważniam

Do przetwarzania danych osobowych w systemie informatycznym i/lub* tradycyjnym

Panią/Pana

Imię i nazwisko .....

Stanowisko .....

Przy obsłudze zbioru danych osobowych .....

W zakresie i systemie informatycznym .....

1) Upoważnienie ważne jest do dnia ...../lub na czas nieokreślony, jednak nie dłużej jak do czasu zakończenia wykonywania pracy związanej z przetwarzaniem danych w wyżej wymienionym zbiorze;
2) Wyżej wymieniona osoba odbyła szkolenie w zakresie ochrony danych osobowych i obsługi wyżej wymienionego zbioru,;
3) Jednocześnie traci moc upoważnienie nr ..... z dnia .....

.....
Administrator Danych Osobowych

Data i podpis osoby upoważnionej:.....

* wpisać właściwe na podstawie zakresu obowiązków lub decyzji ADO.

Załącznik nr 5 do Polityki

WZÓR

Aleksandrów Kujawski, dnia .....

PROTOKÓŁ ZNISZCZENIA

nośników zawierających dane osobowe

Nr .....

Komisja w składzie:

1. .....
2. .....
3. .....

(imię, nazwisko, stanowisko)

Oświadcza, iż nośniki otrzymane .....

zostały w dniu ..... komisyjnie zniszczone .....

.....

(opis procesu zniszczenia)

Rodzaj i oznaczenie nośników: .....

Ilość (szt.): .....

Uwagi: .....

.....

Podpisy komisji:

1. .....
2. .....
3. .....

Załącznik nr 6 do Polityki

WZÓR

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH W POWIATOWYM CENTRUM POMOCY RODZINIE W ALEKSANDROWIE KUJAWSKIM

Lp.	Nazwisko i imię	Numer upoważnienia	Data nadania uprawnień	Data ustania uprawnień	Zakres upoważnienia (zbiór danych osobowych)	Identyfikator w systemie informatycznym	Uwagi (m. in. data rozwiązania umowy o pracę, zmiany upoważnienia)
1.							
2.							
3.							
4.							
5.							
6.							
7.							
8.							
9.							
10.							

Załącznik nr 2 do Zarządzenie Kierownika
Powiatowego Centrum Pomocy Rodzinie
w Aleksandrowie Kujawskim
w sprawie wprowadzenia Polityki
bezpieczeństwa informacji i Instrukcji
zarządzania systemem informatycznym,
w którym przetwarzane są dane osobowe
w Powiatowym Centrum Pomocy Rodzinie
w Aleksandrowie Kujawskim

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE W POWIATOWYM CENTRUM POMOCY RODZINIE W ALEKSANDROWIE KUJAWSKIM

Aleksandrów Kujawski, dnia 04 marca 2016 roku

Spis treści:

§ 1
Wprowadzenie

1. Instrukcja zarządzania systemem informatycznym w Powiatowym Centrum Pomocy Rodzinie w Aleksandrowie Kujawskim, zwana w treści niniejszego dokumentu Instrukcją określa zasady postępowania jakie muszą być stosowane przez osoby przetwarzające dane osobowe w systemach informatycznych.
2. Instrukcja została opracowana w oparciu o unormowania zawarte w § 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).
3. Podstawowym celem zabezpieczeń systemów informatycznych jest zapewnienie jak najwyższego poziomu bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych oraz zabezpieczenia danych osobowych przed zagrożeniami, w tym zwłaszcza przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

§ 2
Definicje

Określenia użyte w Instrukcji oznaczają:

1. **Centrum** – Powiatowe Centrum Pomocy Rodzinie w Aleksandrowie Kujawskim mieszczące się przy ul. Sikorskiego 3;
2. **Administrator Danych Osobowych (ADO)** – jednostka organizacyjna w postaci Centrum decydująca o celach i środkach przetwarzania danych osobowych reprezentowana przez Kierownika, który zarządza Polityką bezpieczeństwa za pośrednictwem Administratora Bezpieczeństwa Informacji;
3. **Administrator Bezpieczeństwa Informacji (ABI)** – osoba powołana przez Administratora Danych Osobowych w celu nadzorowania przetwarzania danych osobowych w systemie tradycyjnym i informatycznym, odpowiedzialna w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń systemu zabezpieczeń;
4. **Administrator Systemu Informatycznego (ASI)** – pracownik Starostwa Powiatowego w Aleksandrowie Kujawskim – wyznaczony w drodze delegacji obowiązków do

realizacji zadań związanych z eksploatacją sieci i systemów informatycznych na terenie Centrum, w których przetwarzane są dane osobowe;

5. **Zbiór danych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcyjnie, tzn. przetwarzany w sposób taki, że uprawniony użytkownik ma dostęp tylko w ograniczonym zakresie przetwarzania;
6. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, w szczególności poprzez podanie jednego lub kilku specyficznych czynników ją określających;
7. **Przetwarzanie danych osobowych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, które wykonuje się w sposób tradycyjny jak i w systemach informatycznych.
8. **Generalny Inspektor Ochrony Danych Osobowych** - rozumie się przez to organ do spraw ochrony danych osobowych, zwany dalej GIODO;
9. **Hasło** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi, wykorzystywanemu łącznie z identyfikatorem do identyfikowania osoby w systemie informatycznym;
10. **Identyfikator** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
11. **Odbiorca danych** - rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
    1) osoby, której dane dotyczą,
    2) osoby upoważnionej do przetwarzania danych,
    3) przedstawiciela, o którym mowa wart. 31a ustawy,
    4) podmiotu, o którym mowa w art. 31 ustawy,
    5) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;
12. **Osoba upoważniona do przetwarzania danych osobowych** - rozumie się przez to użytkownika zbioru danych osobowych, który otrzymał pisemne upoważnienie do przetwarzania danych osobowych wydane przez ADO na wniosek Właściciela zasobów odpowiadającego merytorycznie za zbiór danych osobowych, zwana dalej osobą upoważnioną;
13. **Przetwarzający** - rozumie się przez to podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawieranej zgodnie z art. 31 ustawy;

14. **Sieć publiczna i sieć telekomunikacyjna** - rozumie się przez to sieć publiczną i sieć telekomunikacyjną w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, z późn. zm.);
15. **System informatyczny** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
16. **Upoważnienie** - rozumie się przez to pisemne imienne upoważnienie do przetwarzania danych osobowych wydane przez ADO;
17. **Ustawa** - rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r. poz. 2132, z późn. zm.);
18. **Rozporządzenie** - 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);
19. **Usuwanie danych** - rozumie się przez to zniszczenie danych lub taka ich modyfikacje, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
20. **Użytkownik** - rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych w formie informatycznej lub tradycyjnej i informatycznej po nadaniu identyfikatora i hasła;
21. **Osoba trzecia** – należy przez to rozumieć, osobę nie będącą osobą upoważnioną przez ADO;
22. **Właściciel zasobów**– osoba odpowiedzialna merytorycznie za gromadzenie i przetwarzanie danych osobowych w komórce organizacyjnej;
23. **Zbiór nieinformatyczny** – zbiór danych osobowych prowadzony poza systemem informatycznym, w szczególności w postaci tradycyjnej.

§ 3
Zakres obowiązywania Instrukcji

1. Instrukcja odnosi się do wszystkich systemów informatycznych przetwarzających dane osobowe w Centrum, w tym przetwarzających dane osobowe pracowników ADO, zlokalizowane:
   1) bezpośrednio na komputerach, na których są przetwarzane;
   2) w obrębie sieci lokalnej;
   3) pracujących za pośrednictwem sieci telekomunikacyjnej.

2. Niniejsza instrukcja przeznaczona jest dla użytkowników, którzy przetwarzają dane osobowe i realizują zasady bezpieczeństwa zbiorów ADO.

§ 4
Poziom bezpieczeństwa

1. Uwzględniając kategorie danych osobowych oraz konieczność zachowania bezpieczeństwa ich przetwarzania w systemie informatycznym połączonym z siecią publiczną, wprowadza się "poziom wysoki" bezpieczeństwa w rozumieniu § 6 rozporządzenia w systemach mających połączenie z siecią.

2. Ryzyko nieupoważnionego dostępu do danych osobowych przetwarzanych w systemach informatycznych jest minimalizowane poprzez:
   a) stosowanie sprzętowych programowych zabezpieczeń stacji roboczych i sieci teleinformatycznej;
   b) stosowanie procedur organizacyjnych normujących przetwarzanie zbiorów danych osobowych w systemie informatycznym;
   c) prowadzenie szkoleń użytkowników.

3. Obszary przetwarzania danych osobowych w pomieszczeniach ADO nie mogą być dostępne dla osób nieuprawnionych. Dopuszczalne odstępstwo stanowią pomieszczenia, w których przyjmowani są klienci. Jeżeli pomieszczenia te wyposażone są jednocześnie w urządzenia z dostępem do systemów bazodanowych albo tradycyjne kartoteki, należy w nich stosować szczególne środki ostrożności, w tym:
   1) drukarki i urządzenia peryferyjne powinny być usytuowane tak, aby znajdowały się z dala od przestrzeni, po której poruszają się osoby nieuprawnione;
   2) ADO określi szczegółowe zasady ogłoszenia alarmu i wezwania pomocy przez pracownika w przypadku bezpośredniego zagrożenia jego życia lub zdrowia, albo ujawnienia próby pozyskania danych osobowych.

§ 5
Praca w systemie informatycznym

1. Nadawanie i rejestrowanie uprawnień.
   1) dostęp do systemu informatycznego służącego do przetwarzania danych osobowych może uzyskać wyłącznie osoba upoważniona przez ADO do przetwarzania danych osobowych na podstawie imiennego upoważnienia;

2) upoważnienia wydaje się na podstawie wniosku złożonego przez ADO na zasadach określonych w polityce bezpieczeństwa;
3) po wydaniu przez ADO upoważnienia do przetwarzania danych osobowych, następuje założenie konta użytkownikowi;
4) rejestracja użytkownika w systemie informatycznym polega na nadaniu przez ASI identyfikatora i przydzieleniu hasła oraz wprowadzeniu danych do bazy użytkowników systemu;
5) rejestr przydzielonych identyfikatorów prowadzony jest przez ASI lub ABI;
6) konto w systemie operacyjnym o uprawnieniach "administratora" jest wykorzystywane wyłącznie przez ASI;
7) użytkownik pracuje w systemie operacyjnym komputera w oparciu o najniższy poziom uprawnień o nazwie "użytkownik". W sytuacjach wynikających z wymagań zastosowanego oprogramowania, ASI może podwyższyć poziom uprawnień;
8) ASI konfiguruje system operacyjny w sposób wymuszający określone zachowania użytkownika w sposób określony w rozporządzeniu;
9) wyrejestrowania użytkownika z systemu informatycznego ASI dokonuje na wniosek ADO składany na zasadach opisanych w Polityce, wyrejestrowanie może mieć charakter czasowy lub trwały;
10) wyrejestrowanie następuje poprzez:
    a) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
    b) usuniecie profilu użytkownika z systemu informatycznego oraz naniesienie zmian w stosownych rejestrach (wyrejestrowanie trwale);
11) czasowe wyrejestrowanie użytkownika z systemu informatycznego następuje w razie:
    a) nieobecności użytkownika w pracy trwającej dłużej niż 40 dni kalendarzowych,
    b) zawieszenia w pełnieniu obowiązków służbowych;
12) przyczyną czasowego wyrejestrowania użytkownika może być:
    a) rażące naruszenie zasad przetwarzania danych osobowych,
    b) wszczęcie postępowania dyscyplinarnego, względem osoby upoważnionej do przetwarzania danych osobowych, związanego z rażącym niewywiązywaniem się z obowiązków służbowych mających związek z przetwarzaniem danych osobowych,
    c) długotrwałe zwolnienie lekarskie,
    d) urlop,
    e) inny powód służbowy;
13) przyczyną trwałego wyrejestrowania użytkownika może być:
    a) wypowiedzenie umowy o prace,

b) rozwiązanie lub wygaśniecie stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik,

c) odsuniecie od prac związanych z przetwarzaniem danych osobowych, do których wydane było upoważnienie, np. spowodowane zmianą zakresu obowiązków;

14) użytkownik zbioru danych osobowych ADO, którego stanowisko pracy jest wyposażone w sprzęt komputerowy, posiada uprawnienie do pracy na nim w zakresie określonym w poziomie uprawnień do systemu informatycznego. Założenie, modyfikacja, zablokowanie lub usunięcie poziomu uprawnień, następuje na wniosek ADO.

2. Metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem.

Użytkownicy systemów informatycznych, w których przetwarzane są dane osobowe, zobowiązani są do przestrzegania zasad określonych w Polityce bezpieczeństwa i niniejszej Instrukcji oraz innych dokumentach zapewniających bezpieczeństwo przetwarzanych danych.

1) identyfikator użytkownika:
   a) identyfikator nadaje ASI,
   b) identyfikator składa się z unikalnego zestawu znaków uzgodnionego z użytkownikiem, identyfikator nie może się powtarzać,
   c) ASI lub ABI prowadzi rejestr identyfikatorów wszystkich użytkowników oraz komputerów, na których założono konta;
2) konfiguracja systemu operacyjnego:
   a) za zapewnienie dostosowania wszystkich zestawów komputerowych do zasad określonych w instrukcji odpowiada ADO,
   b) ASI dokonuje odpowiedniej konfiguracji systemu operacyjnego na wniosek ADO,
   c) w celu zapewnienia kontroli dostępu do komputera, ASI konfiguruje podgląd zdarzeń systemu operacyjnego w sposób zapewniający automatyczną rejestrację prób udanych/nieudanych logowania do systemu i rejestracje czasu pracy poszczególnych użytkowników;
   d) użytkownik konfiguruje wygaszacz ekranu w sposób zapewniający kontrolę dostępu do systemu, w szczególności poprzez ustawienie:
      - czas zwłoki wygaszacza ekranu - nie dłużej niż 30 minut,
      - wymaganie podania hasła po wyjściu ze stanu wstrzymania albo po okresie bezczynności;
3) hasło użytkownika i administratora:
   a) ASI prowadzi rejestr haseł do konta "administrator" we wszystkich komputerach ADO, w których przetwarzane są dane osobowe,

b) system informatyczny skonfigurowany jest przez ASI w sposób wymuszający zmianę hasła oraz stosowanie zasad haseł, w uzasadnionych sytuacjach ASI może polecić użytkownikowi dokonanie zmiany hasła przed upływem terminu,

c) w przypadku przewidzianej nieobecności pracownika w okresie zmiany hasła, użytkownik zobowiązany jest do samodzielnej wcześniejszej zmiany hasła,

d) zabrania się udostępniania swojego identyfikatora i hasła innym osobom oraz korzystania przez osoby upoważnione do przetwarzania danych osobowych z identyfikatora lub hasła innego użytkownika,

e) zasady haseł:

- za okresową zmianę oraz ochronę hasła odpowiada użytkownik, hasło musi składać się z unikalnego zestawu znaków zawierającego łącznie małe i wielkie litery, cyfry oraz znaki specjalne (np. spacja, kropka, średnik itp.), hasło nie może być identyczne z identyfikatorem użytkownika ani jego imieniem lub nazwiskiem,
- maksymalny okres ważności hasła: 30 dni,
- minimalna długość hasła administratora: 12 znaków,
- minimalna długość hasła użytkownika: 8 znaków,
- wymuszenie tworzenia historii haseł: 12 haseł,

4) Zasady blokady konta:

a) czas trwania blokady konta: 180 minut,

b) próg blokady konta: 3 nieudane próby logowania,

c) wyzerowanie licznika blokady konta: po 180 minutach;

5) Hasła do serwera, aktywnych urządzeń sieci i istotnych programów konfiguracyjnych, Administrator Systemu Informatycznego umieszcza w zapieczętowanych kopertach i składa w obecności Administratora Bezpieczeństwa Informacji w miejscu zabezpieczonym przed dostępem osób nieuprawnionych. Otwarcie wyżej wymienionych kopert może nastąpić w przypadku:

a) kontroli przez Administratora Bezpieczeństwa Informacji,

b) zamiaru zniszczenia nieaktualnych haseł przez Administratora Systemu Informatycznego,

c) innym określonym niniejszą Instrukcją.

3. Procedury rozpoczęcia, zawieszenia i zakończenia pracy, przeznaczone dla użytkowników systemu.

Korzystając z systemu informatycznego do przetwarzania danych osobowych użytkownik jest zobowiązany do przestrzegania zasad i uregulowań obowiązujących w ADO, o ile nie określają one niższego poziomu zabezpieczeń i nie wpływają ujemnie na bezpieczeństwo przetwarzanych danych osobowych.

l) tryb pracy na poszczególnych stacjach roboczych:
   a) przed rozpoczęciem pracy użytkownik jest zobowiązany do sprawdzenia, czy zestaw komputerowy nie nosi śladów mogących świadczyć o włamaniu do systemu,
   b) w przypadku stwierdzenia nieprawidłowości użytkownik zobowiązany jest do zabezpieczenia zestawu komputerowego i nośników przed nieuprawnionym dostępem oraz niezwłocznego poinformowania ADO o stwierdzonych nieprawidłowościach,
   c) o wszelkich nieprawidłowościach ADO bezzwłocznie informuje ASI i ABI,
   d) rozpoczęcie pracy na stacji roboczej następuje po włączeniu napięcia w listwie podtrzymującej napięcie lub włączeniu zasilacza awaryjnego (UPS) i komputera, wprowadzeniu indywidualnego, znanego tylko użytkownikowi identyfikatora i hasła,
   e) zabrania się wykorzystywania konta innego użytkownika,
   f) zabrania się przydzielania jednego konta kilku osobom, chyba że zachodzi szczególna okoliczność, fakt ten trzeba udokumentować dla ABI,
   g) w systemach, w których administrator zbioru ustala inne zasady kontroli dostępu, np. poprzez zastosowanie indywidualnych kart i kodów PIN, obowiązują zasady łączne albo o wyższym poziomie zabezpieczeń,
   h) w pomieszczeniu, w którym przetwarzane są dane osobowe, interesanci mogą przebywać pod nadzorem użytkownika,
   i) przed osobami postronnymi należy chronić ekrany komputerów (ustawienie monitora powinno uniemożliwiać pogląd), wydruki leżące na biurkach oraz w otwartych szafach,
   j) monitory komputerów chronione są włączającym się automatycznie wygaszaczem ekranu wznowienie wyświetlenia następuje po wprowadzeniu hasła zalogowanego użytkownika (wymuszone przez system),
   k) w przypadku konieczności krótkotrwałego opuszczenia stanowiska użytkownik obowiązany jest aktywować wygaszacz ekranu lub w inny sposób zablokować stację roboczą (kombinacja klawiszy: znak "Windows" oraz litera "L"),
   l) zakończenie pracy na stacji roboczej następuje po wprowadzeniu danych, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w zasilaczu awaryjnym (UPS) lub/i listwie zasilającej,
   m) przed opuszczeniem pokoju (koniec pracy, opuszczenie terenu ADO) należy:
      - schować do zamykanych na klucz szaf przenośne nośniki informatyczne, dokumenty i wykonane wydruki zawierające dane osobowe oraz zniszczyć w niszczarce wydruki wstępne,

- schować do zamykanych na klucz szaf wszelkie akta zawierające dane osobowe, umieścić klucze do szaf w ustalonym, przeznaczonym do tego miejscu,
- zamknąć okna,
- zamknąć pomieszczenie,
- zdać klucze na przechowanie w miejscu określonym przepisami szczególnymi;

2) tryb pracy na komputerach przenośnych:
   a) zasadniczo zbiory danych osobowych przetwarzane są w komputerach stacjonarnych i przenośnych,
   b) przetwarzanie danych osobowych poza terenem ADO przy wykorzystaniu komputerów przenośnych powinno być ograniczone do niezbędnych przypadków,
   c) przetwarzanie danych osobowych przy użyciu komputerów przenośnych może odbywać się wyłącznie na podstawie zgody ADO,
   d) zakres danych przetwarzanych na komputerze przenośnym oraz zakres uprawnień do przetwarzanych danych ADO określa na piśmie,
   e) komputery przenośne podlegają zabezpieczeniom o poziomie nie niższym, niż przewidzianym dla komputerów stacjonarnych,
   f) zabronione jest wynoszenie komputera przenośnego z pomieszczenia służbowego głównego użytkownika, w którym nie zastosowano zasad kont i haseł opisanych w instrukcji zarządzania,
   g) poza obszarem Centrum komputerów przenośnych nie wolno pozostawiać bez nadzoru,
   h) nie należy pozostawiać bez kontroli dokumentów, nośników danych i sprzętu w hotelach, innych miejscach publicznych i w samochodach,
   i) informacje przechowywane na urządzeniach przenośnych lub komputerowych nośnikach danych należy chronić przed uszkodzeniami fizycznymi, a ze względu na działanie silnego pola elektromagnetycznego należy przestrzegać zaleceń producentów dotyczących ochrony sprzętu,
   j) w uzasadnionych przypadkach wykorzystywanie komputerów przenośnych ADO w miejscach publicznych jest dozwolone, o ile otoczenie, w którym znajduje się osoba upoważniona do przetwarzania danych osobowych, stwarza warunki minimalizujące ryzyko zapoznania się z danymi przez osoby nieupoważnione,
   k) w domu osoby upoważnionej niedozwolone jest udostępnianie domownikom komputera przenośnego należącego do ADO - użytkownik powinien zachować w tajemnicy wobec domowników identyfikator i hasło, których podanie jest konieczne do rozpoczęcia pracy na komputerze przenośnym,
   l) ASI w razie potrzeby, wskazuje w dokumencie powierzenia komputera przenośnego osobie upoważnionej do przetwarzania danych osobowych

konieczność i częstotliwość sporządzania kopii zapasowych danych przetwarzanych na komputerze przenośnym oraz określa zasady:

- postępowania w razie nieobecności w pracy dłuższej niż 5 dni. Jeśli komputer przenośny nie może być zwrócony przed okresem nieobecności, to użytkownik tego komputera powinien niezwłocznie powiadomić o tym ADO i uzgodnić z nim zwrot komputera przenośnego,
- zwrotu sprzętu w razie zakończenia pracy u ADO,

m) w zakresie nieuregulowanym w polityce bezpieczeństwa, do pracy z wykorzystaniem komputerów przenośnych, stosuje się postanowienia Instrukcji zarządzania systemem informatycznym.

4. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania, zasady ich przechowywania oraz wykonywania przeglądów i konserwacji nośników.
   1) procedury tworzenia kopii zapasowych danych przechowywanych lokalnie:
      a) ASI decyduje o zasadach, częstotliwości i metodach wykonywania kopii zapasowych danych, które są przetwarzane w systemach informatycznych,
      b) za sporządzanie i zabezpieczenie kopii danych przechowywanych lokalnie odpowiada ABI,
      c) kopie danych powinny być właściwie oznakowane i przechowywane w pomieszczeniu innym, niż system teleinformatyczny, w którym dane są przechowywane,
      d) nośniki informatyczne zawierające kopie danych podlegają ochronie odpowiedniej do nośników i zestawów komputerowych, z których pochodzą,
      e) ABI prowadzi wykaz zawierający m.in. informacje o tym kto, kiedy i na jakim nośniku sporządził kopię, wzór Rejestru kopii zapasowych określa załącznik nr 1 do niniejszej Instrukcji,
      f) ADO określa częstotliwość sporządzania kopii oraz ich testowania i przeglądów, ADO uwzględnia rzeczywiste potrzeby wynikające m.in. z ilości i częstotliwości przetwarzanych danych oraz ich wagi - ADO może uzgodnić dodatkowe zasady sporządzania kopii z ASI;
   2) procedury tworzenia kopii zapasowych danych przechowywanych na serwerze:
      a) za opracowanie harmonogramu sporządzania oraz zabezpieczenie kopii oprogramowania użytkowanego sieciowo odpowiada ASI,
      b) dostęp do kopii bezpieczeństwa mają tylko pracownicy upoważnieni przez ABI – pozostałe kopie tworzy się na oddzielnych nośnikach informatycznych,
      c) nośniki zawierające kopie zapasowe należy oznaczać jako "Kopia zapasowa dzienna/tygodniowa/miesięczna" wraz z podaniem daty sporządzenia,

d) częstotliwość wykonywania kopii (serwer):
   - raz w tygodniu - na koniec tygodnia roboczego, kopie wszystkich aplikacji,

e) testowanie kopii:
   - w celu zapewnienia poprawności wykonywanych kopii ASI opracowuje procedury określające sposób i częstotliwość ich wykonywania,
   - próba polega na odtworzeniu danych w warunkach testowych i sprawdzeniu, czy jest możliwość odczytania danych,

f) przechowywanie kopii zapasowych stacji roboczych:
   - kopie zapasowe przechowuje się w zamykanych szafach, specjalnie do tego przeznaczonych,
   - dostęp do kopii posiada wyłącznie ABI oraz ASI i upoważnieni pracownicy (każde wydanie i przyjęcie kopii jest odnotowywane w rejestrze depozytów),

g) likwidacja nośników zawierających kopie:
   - nośniki zawierające nieaktualne kopie danych lub uszkodzone, będące poza wykazem cyklicznych kopii, podlegają likwidacji,
   - w przypadku nośników jednorazowych, takich jak płyty CD-R i DVD-R, likwidacja polega na ich fizycznym zniszczeniu w taki sposób, by nie można było odczytać ich zawartości,
   - nośniki wielorazowego użytku, takie jak dyski twarde, dyskietki, płyty CD-RW, DVD-RW, można wykorzystać ponownie do celów przechowywania kopii bezpieczeństwa po uprzednim usunięciu ich zawartości,
   - nośniki wielokrotnego użytku nienadające się do ponownego użycia należy zniszczyć fizycznie,

h) przechowywanie komputerowych nośników informacji zawierających dane osobowe:
   - zbiory danych przetwarzanych w oparciu o serwer ADO przechowywane są generalnie na serwerze obsługującym system informatyczny,
   - wszelkie dane przetwarzane w pamięci poszczególnych stacji roboczych oraz komputerów przenośnych przechowywanych lokalnie zabezpieczane są okresowo poprzez sporządzenie kopii zapasowych;

3) kontrola nad wprowadzaniem, dalszym przetwarzaniem i udostępnianiem danych osobowych:

a) system informatyczny ADO, w zależności od możliwości oprogramowania wykorzystywanego do prowadzenia bazy danych osobowych, umożliwia automatycznie:
   - przypisanie wprowadzanych danych użytkownikowi (identyfikatorowi użytkownika), który te dane wprowadza do systemu,

- sygnalizacje wygaśnięcia czasu obowiązywania hasła dostępu do stacji roboczej (dotyczy to także komputerów przenośnych),
- sporządzenie i wydrukowanie dla każdej osoby, której dane są przetwarzane systemie, raportu zawierającego datę pierwszego wprowadzenia danych do systemu ADO, identyfikator użytkownika wprowadzającego te dane, źródła danych - w przypadku zbierania danych nie od osoby, której one dotyczą, informacje o odbiorcach danych, którym dane osobowe zostały udostępnione oraz sprzeciwu, o którym mowa wart. 32 ust. 1 pkt 8 ustawy,

b) odnotowanie powyższych informacji następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych,

c) w przypadku systemów/baz danych/zbiorów, które nie umożliwiają automatycznego monitorowania zakresu działania użytkownika w zbiorze, ADO tworzy procedury rejestracji danych, umożliwiających kontrole nad tym, kto, kiedy i jakie dane wprowadził do zbioru, usunął, modyfikował i przeglądał;

4) przegląd i konserwacja systemu wykonywane przez ASI
   a) ASI prowadzi doraźne przeglądy systemu pod kątem ustalenia przypadków niewłaściwego użytkowania,
   b) ASI dokonuje przeglądu pliku zawierającego raport dotyczący działalności aplikacji bądź systemu na serwerze (log systemowy) wg oddzielnego harmonogramu,
   c) zapisy logów systemowych powinny być przeglądane przez ASI każdorazowo po wykryciu naruszenia zasad bezpieczeństwa,
   d) kontrole i testy przeprowadzane przez ASI powinny obejmować zarówno dostęp do zasobów systemu, jak i profile oraz uprawnienia poszczególnych użytkowników;
5) naprawy urządzeń komputerowych:
   a) wszelkie naprawy urządzeń komputerowych oraz zmiany w systemie informatycznym przeprowadzane są przez ASI,
   b) naprawy i zmiany w systemie informatycznym przeprowadzane przez ASI prowadzone są w siedzibie (jeśli to możliwe) lub poza siedzibą ADO, po uprzednim usunięciu nośników informatycznych, a jeśli wiązałoby się to z nadmiernymi utrudnieniami, to po podpisaniu umów powierzenia przetwarzania danych osobowych (dotyczy to w szczególności serwera);
6) dodawanie, usuwanie i modyfikowanie oprogramowania:
   a) użytkownicy zgłaszają ASI potrzebę instalowania, usuwania lub modyfikowania oprogramowała w wykorzystywanych zestawach komputerowych,

b) zabrania się użytkownikom wykonywania jakichkolwiek czynności dot. zainstalowanego oprogramowania, wykraczającego poza dozwolone dostosowanie ustawień danego programu,

c) zabrania się wykorzystania oprogramowania bez licencji lub innych zezwoleń, np. administratora danej bazy danych;

d) do instalacji i modyfikacji oprogramowania na serwerze uprawniony jest ASI, na serwerze i stacjach roboczych może być instalowane tylko oprogramowanie, na które ADO posiada licencję, instalację lub modyfikację oprogramowania na serwerze lub stacji roboczej odnotowuje się w wykazie oprogramowania instalowanego,

e) ABI prowadzi wykaz oprogramowania dopuszczonego do używania przez ADO, kontroli podlega rodzaj oprogramowania oraz ilość licencji zakupionych przez ADO.

f) zabrania się użytkownikom dokonywania samodzielnej instalacji jakiegokolwiek oprogramowania, instalacji oprogramowania dokonuje wyłącznie ASI;

7) posługiwanie się nośnikami:

a) zabrania się używania prywatnych nośników informatycznych,

b) zakazuje się przetwarzania danych osobowych na zewnętrznych nośnikach bez zezwolenia ADO oraz przesyłania danych pocztą elektroniczną,

c) na nośnikach przenośnych dopuszczalne jest przetwarzanie jedynie jednostkowych danych osobowych,

d) w przypadku posługiwania się nośnikami informatycznymi pochodzącymi od podmiotu zewnętrznego użytkownik jest zobowiązany do sprawdzenia go programem antywirusowym,

e) nośniki informatyczne raz użyte do przetwarzania danych osobowych nie mogą być wykorzystywane poza terenem ADO do innych celów mimo usunięcia danych i podlegają ochronie w trybie niniejszej instrukcji,

f) nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione do przetwarzania danych osobowych oraz w pomieszczeniach innych, niż system, z którego dane pochodzą,

g) za stosowanie ochrony antywirusowej odpowiada ADO,

h) sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie odbywa się przy wykorzystaniu oprogramowania zainstalowanego przez ASI na stacjach roboczych oraz komputerach przenośnych (aktualizacja oprogramowania jest pobierana z serwera),

i) oprogramowanie antywirusowe sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerem i stacjami roboczymi; użytkownik nie może ingerować w ustawienia programu,

j) niezależnie od ciągłego nadzoru, ASI konfiguruje oprogramowanie w sposób wykonujący automatycznie raz na kwartał pełną kontrolę obecności wirusów komputerowych w systemie oraz jego zasobach, jak również w serwerze i stacjach roboczych,

k) aktualizacja oprogramowania antywirusowego oraz określenie częstotliwości automatycznych aktualizacji definicji wirusów, dokonywanych przez to oprogramowanie wykonywana jest automatycznie po odpowiedniej konfiguracji oprogramowania przez ASI,

l) zabrania się innym osobom niż upoważnionym przez ASI dokonywania jakichkolwiek zmian w ustawieniach programu antywirusowego,

m) użytkownik jest obowiązany zawiadomić ASI o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem;

8) wycofanie z użycia i niszczenie nośników informatycznych:

a) dyski twarde, na których były przetwarzane dane osobowe podlegające wycofaniu z użycia niszczone są przez ASI,

b) jeśli nośnik danych (dyskietka, płyta CD/DVD, pendrive) zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, należy go zniszczyć fizycznie w porozumieniu z ASI,

c) ADO powołuje komisję, w skład której, oprócz ABI może wchodzić dodatkowy pracownik - o powołaniu komisji ABI informuje ASI,

d) dyski przeznaczone do ponownego wykorzystania w innym systemie pracującym dla ADO, na wniosek ADO, podlegają procedurze trwałego usunięcia danych przy użyciu specjalistycznego oprogramowania będącego w dyspozycji ASI - termin i miejsce wykonania czynności określa ASI.

5. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji ADO.

1) ADO odpowiada za prowadzenie ewidencji sprzętu komputerowego oraz oprogramowania systemowego i użytkowego służącego do przetwarzania danych osobowych;

2) ewidencje sprzętu komputerowego prowadzi się na zasadach określonych przez ADO;

3) osoba wyznaczona do prowadzenia ewidencji prowadzi okresowe kontrole ukompletowania sprzętu oraz uzgadnia stany na podstawie prowadzonej księgi inwentarzowej;

4) ADO zgłasza ASI potrzebę zainstalowania, modyfikowania lub usunięcia oprogramowania w wykorzystywanym systemie informatycznym;

5) ASI odpowiada za zainstalowanie i właściwe skonfigurowanie oprogramowania systemowego i użytkowego w systemach wykorzystywanych u ADO;

6) ASI dokonuje przeglądów i konserwacji każdorazowo przed wydaniem sprzętu do użytkowania (nowy sprzęt albo przekazanie wewnątrz ADO);

7) przekazanie sprzętu do przetwarzania innego niż dotychczas zbioru, albo przekazania sprzętu poza teren ADO, odbywa się po uprzednim usunięciu przez ASI danych z dysku twardego komputera przy pomocy specjalistycznego oprogramowania do bezpowrotnego usuwania danych;

8) samowolne wykonywanie zmian w oprogramowaniu oraz stosowanych zabezpieczeniach przez użytkowników jest zabronione.

6. Procedura postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego.

l) użytkownik zobowiązany jest zawiadomić niezwłocznie ADO, ABI i ASI o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu, a w szczególności o:

a) naruszeniu hasła dostępu i identyfikatora (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzenia hasła),

b) częściowym lub całkowitym braku danych albo dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień,

c) braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów serwera,

d) wykryciu wirusa komputerowego,

e) zauważeniu elektronicznych śladów próby włamania do systemu informatycznego,

f) znacznym spowolnieniu działania systemu informatycznego,

g) podejrzeniu kradzieży lub podmiany sprzętu komputerowego lub dokumentów zawierających dane osobowe,

h) zmianie połączenia sprzętu komputerowego wskazującego np. na jego wynoszenie z pomieszczenia,

i) zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf,

2) do czasu podjęcia czynności przez ASI użytkownik zobowiązany jest do:

a) niezwłocznego podjęcia czynności niezbędnych dla powstrzymania niepożądanych skutków zaistniałego zdarzenia,

b) zabezpieczenia miejsca zdarzenia,

c) zastosowania się do innych uregulowań, jeśli odnoszą się one do zaistniałego przypadku,

d) przygotowania opisu incydentu, pozostania w miejscu zdarzenia do czasu przybycia ASI lub osoby przez niego wskazanej;

3) ASI przyjmujący zawiadomienie jest obowiązany niezwłocznie poinformować ABI o naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu;

4) ABI po otrzymaniu zawiadomienia, powinien niezwłocznie:
   a) przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia ochrony danych osobowych,
   b) w porozumieniu z ASI ustalić działania chroniące system przed ponownym zagrożeniem,
   c) sporządzić raport z naruszenia bezpieczeństwa danych osobowych ADO, a następnie niezwłocznie przekazać jego kopie ADO, wzór raportu stanowi załącznik nr 3 do niniejszej Instrukcji;
5) ABI w uzgodnieniu z ASI może zarządzić odłączenie (jeżeli to możliwe) części systemu informatycznego dotkniętej incydentem od pozostałej jego części;
6) w razie przywracania danych z kopii zapasowych ASI obowiązany jest upewnić się, że przywracane dane zapisane zostały przed wystąpieniem incydentu (dotyczy to zwłaszcza przypadków infekcji wirusowej);
7) ABI i ASI zobowiązani są do niezwłocznego informowania ADO o stwierdzonych przypadkach naruszenia niniejszej instrukcji przez użytkowników, a zwłaszcza o przypadkach posługiwania się przez użytkowników nieautoryzowanymi programami i nośnikami, nieprzestrzegania zasad używania oprogramowania antywirusowego, niewłaściwego wykorzystania sprzętu komputerowego lub przetwarzania danych w sposób niezgodny z procedurami ochrony danych osobowych;
8) ADO po zapoznaniu się z raportem, podejmuje decyzje o dalszym trybie postępowania, powiadomieniu właściwych organów oraz podjęciu innych szczególnych czynności zapewniających bezpieczeństwo systemu informatycznego bądź zastosowaniu środków ochrony fizycznej,
9) ASI zobowiązany jest prowadzić dziennik pracy dla serwera – wzór dziennika stanowi Załącznik nr 2 do niniejszej Instrukcji. W dzienniku tym opisuje się wszystkie czynności podejmowane w ramach jego administrowania, w szczególności związane z bezpieczeństwem danych.

§ 6
Zabezpieczenie danych przed ich utratą spowodowaną awarią zasilania

1. Serwer pracujący w systemach przetwarzania danych osobowych musi być zasilany poprzez urządzenia filtrujące zakłócenia z sieci zasilającej oraz podtrzymujące zasilanie w przypadku awarii sieci zasilającej.

2. Powyższa zasada dotyczy również stacji roboczych, na których przetwarzane są dane osobowe przetwarzane w systemie informatycznym.

3. W miarę możliwości pożądane jest wyposażenie systemu zasilania w zapasowe źródło energii w postaci agregatu prądotwórczego pozwalającego na pracę w przypadku trwających dłużej wyłączeń źródeł zasilania.

4. Pracownik odpowiedzialny za urządzenie, które jest zasilane poprzez „Urządzenie Podtrzymujące Sieć – UPS" jest obowiązany do sprawdzenia sprawności UPS raz na kwartał. Wszelkie nieprawidłowości należy zgłaszać ASI.

5. Serwer winien być zasilany przez UPS o odpowiednich parametrach, pozwalających na podtrzymanie zasilania przez co najmniej 20 minut oraz na wykonanie bezpiecznego wyłączenia serwera, tak aby przed zanikiem zasilania zostały prawidłowo zakończone operacje rozpoczęte na danych osobowych.

6. Pomieszczenia serwerowni oraz pomieszczenia, w których przetwarzane są dane osobowe winny być odpowiednio chronione przed skutkami pożaru.

7. Infrastruktura techniczna związana z siecią teleinformatyczną i jej zasilaniem (rozdzielnie elektryczne, skrzynki z bezpiecznikami) powinna być zabezpieczona przed dostępem osób nieupoważnionych.

8. Gniazda zasilania sieci teleinformatycznej powinny być odpowiednio oznakowane.

§ 7
Zasady postępowania w sytuacjach szczególnych

1. W przypadku zaistnienia sytuacji szczególnej, takiej jak: pożar, powódź lub zalanie pomieszczeń wodą, zwarcie instalacji elektrycznej, zawalenie stropu, huragan, atak terrorystyczny, sabotaż lub inne, użytkownik natychmiast powiadamia ADO oraz osobę odpowiedzialną za bezpieczeństwo w miejscu pracy, a w zależności od zaistniałej sytuacji odpowiednie służby, czyli policję, straż pożarną, pogotowie ratunkowe, pogotowie energetyczne, pogotowie gazowe, pogotowie wodno-kanalizacyjne, telekomunikację lub inne.

2. Podczas zaistnienia szczególnej sytuacji, wszyscy pracownicy ADO zobowiązani są włączyć się do akcji zabezpieczenia zagrożonego sprzętu i zasobów informatycznych oraz wykonywać ściśle polecenia przełożonych i osób kierujących akcją ratowniczą.

3. Nie czekając na działanie wyspecjalizowanych służb przystępuje się do zabezpieczenia pomieszczeń i sprzętu objętych działaniem sytuacji kryzysowej z zachowaniem przepisów BHP:
   1) wyłącza się zgodnie z instrukcją pracujący serwer,
   2) wyłącza się całkowicie dopływ energii elektrycznej,
   3) uniemożliwia się dostęp do pomieszczeń osób postronnych lub nieupoważnionych,
   4) jeżeli jest to możliwe usuwa się ze strefy zagrożenia sprzęt komputerowy.

4. Po ustąpieniu zagrożenia pracownicy w możliwie najkrótszym czasie, przystępują do likwidacji szkód powstałych w wyniku zaistnienia sytuacji kryzysowej, czyli przywrócenia sprawności sprzętu komputerowego oraz odtworzenia zasobów informatycznych w stanie sprzed sytuacji kryzysowej.

§ 8
Postanowienia końcowe

1. Zgodnie z Kodeksem Pracy, każdy użytkownik sprzętu komputerowego jest zobowiązany do należytego zabezpieczenia przed uszkodzeniem lub zniszczeniem powierzonego mu sprzętu.

2. Instrukcja powinna być poddawana przeglądowi raz w roku. W razie istotnych zmian dotyczących przetwarzania danych osobowych ABI może zarządzić przegląd Instrukcji stosownie do potrzeb. ABI analizuje, czy Instrukcja i pozostała dokumentacja z zakresu ochrony danych osobowych jest adekwatna do:
   1) zmian w budowie systemu informatycznego;
   2) zmian organizacyjnych ADO mających znaczący wpływ na ochronę danych osobowych;
   3) zmian w obowiązującym prawie.

3. Integralną częścią Instrukcji jest „Polityka bezpieczeństwa informacji w Powiatowym Centrum Pomocy Rodzinie w Aleksandrowie Kujawskim" zawierająca szczegółowe zasady postępowania w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych.

4. Niezastosowanie się do procedur określonych w niniejszej instrukcji podlega odpowiedzialności na zasadach określonych w Polityce.

5. W sprawach nieokreślonych niniejszą Instrukcją należy stosować przepisy dotyczące ochrony danych osobowych oraz inne uregulowania dotyczące pracy biurowej i kancelaryjnej, postępowania z dokumentami itp. u ADO, o ile nie obniżają zastosowanego poziomu zabezpieczeń.

§ 9
Spis załączników

Załącznik nr 1 – Wzór rejestru kopii zapasowych
Załącznik nr 2 – Wzór dziennika pracy systemu serwera
Załącznik nr 3 – Wzór raportu z naruszenia bezpieczeństwa danych osobowych

Załącznik nr 1 do Instrukcji
WZÓR

REJESTR KOPII ZAPASOWYCH

Lp.	Data utworzenia kopii	Określenie zakresu kopiowanych danych ze zbioru danych	Nośnik, na którym utworzono kopię	Sporządzający kopię	Data zniszczenia kopii	Niszczący kopię
1	2	3	4	5	6	7

Załącznik nr 2 do Instrukcji

WZÓR

DZIENNIK PRACY SYSTEMU SERWERA
W POWIATOWYM CENTRUM POMOCY RODZINIE W ALEKSANDROWIE KUJAWSKIM

Lp.	Data	Godzina	Opis wykonywanych czynności	Podpis
1	2	3	4	5

Załącznik nr 3 do Instrukcji

WZÓR

Raport
z naruszenia bezpieczeństwa danych osobowych

1. Data stwierdzenia naruszenia: ..... Godzina: .....
(dd.mm.rrrr) (gg:mm)

2. Data zgłoszenia: ..... Godzina: .....
(dd.mm.rrrr) (gg:mm)

3. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....
(imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje)

4. Lokalizacja zdarzenia:

.....
(np. budynek, nr pokoju)

5. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

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

6. Przyczyny wystąpienia zdarzenia:

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

7. Podjęte działania:

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

8. Postępowanie wyjaśniające:

.....
.....

.....
(data, podpis Administratora Bezpieczeństwa Informacji)

Załącznik nr 3 do Zarządzenia Kierownika
Powiatowego Centrum Pomocy Rodzinie
w Aleksandrowie Kujawskim
w sprawie wprowadzenia Polityki bezpieczeństwa
informacji i Instrukcji zarządzania systemem
informatycznym, w którym przetwarzane są dane
osobowe w Powiatowym Centrum Pomocy Rodzinie
w Aleksandrowie Kujawskim

Aleksandrów Kujawski, dnia ..... r.

OŚWIADCZENIE

Ja niżej podpisana/y .....oświadczam, że przed przystąpieniem do pracy przy przetwarzaniu danych osobowych w **Powiatowym Centrum Pomocy Rodzinie w Aleksandrowie Kujawskim** zostałam/em zapoznana/ny z przepisami dotyczącymi ochrony danych osobowych, w tym z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r. poz. 2135, z poźn. zm.) oraz rozporządzeniami wykonawczymi wydanymi na jej podstawie oraz

- Polityką bezpieczeństwa informacji w Powiatowym Centrum Pomocy Rodzinie w Aleksandrowie Kujawskim,
- Instrukcji zarządzania systemem informatycznym, w którym przetwarzane są dane osobowe w Powiatowym Centrum Pomocy Rodzinie w Aleksandrowie Kujawskim,

oraz zobowiązuję się do ich przestrzegania.

Zobowiązuję się także do zachowania w tajemnicy danych osobowych i tajemnicy służbowej, do których mam/będę miał/a dostęp w związku z wykonywaniem przeze mnie zadań służbowych i obowiązków pracowniczych w Powiatowym Centrum Pomocy Rodzinie w Aleksandrowie Kujawskim, zarówno w trakcie obecnie wiążącego mnie stosunku pracy, umowy cywilno-prawnej, aplikacji, stażu, praktyki jak i po ich ustaniu.

Przyjmuję do wiadomości, że postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane za ciężkie naruszenie obowiązków pracowniczych w rozumieniu Kodeksu pracy oraz art. 266 Kodeksu karnego.

.....
(imię i nazwisko składającego oświadczenie)

.....
(data, podpis przyjmującego oświadczenie - ABI)