POLITYKA BEZPIECZEŃSTWA
PRZETWARZANIA DANYCH OSOBOWYCH
W PRZEDSZKOLU NR 1 IM. CZESŁAWA JANCZARSKIEGO
W WĘGROWIE

Przedszkole nr 1 im. Czesława Janczarskiego
ul. Klonowa 4
07-100 Węgrów

POSTANOWIENIA OGÓLNE

§ 1. **Polityka bezpieczeństwa** została opracowana w związku z dobrymi praktykami mającymi na celu uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania w Przedszkolu nr 1 im. Czesława Janczarskiego w Węgrowie informacji zawierających dane osobowe.

§ 2. Polityka określa tryb i zasady ochrony danych osobowych przetwarzanych w Przedszkolu nr 1 im. Czesława Janczarskiego przy ulicy Klonowej 4 w Węgrowie (zwanym w dalszej części dokumentu „Przedszkolem")

§ 3. Ilekroć w Polityce jest mowa o :

1) **Jednostka organizacyjna** – rozumie się przez to Przedszkole;
2) **zbiorze danych osobowych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
3) **danych osobowych** - rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
4) **przetwarzaniu danych -** rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
5) **systemie informatycznym** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
6) **systemie tradycyjnym** - rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;
7) **zabezpieczeniu danych w systemie informatycznym** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
8) **usuwaniu danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

9) **Administratorze Danych Osobowych (ADO)** - w świetle art. 24 RODO rozumie się przez to kierownika jednostki który decyduje o celach i środkach przetwarzania danych osobowych;
10) **Inspektor ochrony danych** zwanym też **Inspektorem (IOD)** - rozumie się przez to osobę wyznaczoną przez Dyrektora Przedszkola, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
11) **Kierownik jednostki –** rozumie się przez to Dyrektora Przedszkola;
12) **użytkowniku systemu** zwanym też **użytkownikiem systemu informatycznego** - rozumie się przez to upoważnionego przez kierownika jednostki, wyznaczonego do przetwarzania danych osobowych w systemie informatycznym pracownika, który odbył szkolenie prowadzone przez IOD w zakresie ochrony tych danych;
13) **zgodzie osoby, której te dane dotyczą** - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie - zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

PODSTAWA PRAWNA

Polityka Bezpieczeństwa została utworzona w związku z wymaganiami zawartymi w:

1. Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 r. poz. 1000).
2. Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych - RODO) – art.24.
3. Ustawa z dnia 14 grudnia 2016 r. – Prawo Oświatowe (Dz.U. 2017 r. poz. 60),
4. Ustawa z dnia 7 września 1991 r. o systemie oświaty (Dz.U.2018 r. poz. 1457),
5. Rozporządzenie MEN z 14 luty 2017 r. w sprawie podstawy programowej wychowania przedszkolnego oraz kształcenia ogólnego w poszczególnych typach szkół. (Dz.U. 2017 r. poz. 356).

6. Rozporządzenie MEN z 9 sierpnia 2017 r. w sprawie indywidualnego obowiązkowego rocznego przygotowania przedszkolnego dzieci (Dz.U. 2017 r. poz. 1616).

7. Rozporządzenie MENiS z 31 grudnia 2002 r. w sprawie bezpieczeństwa i higieny w publicznych i niepublicznych szkołach i placówkach (Dz.U. 2003. poz. 69).

8. Rozporządzenie MEN z dnia 22 lipca 2011 r. zmieniające rozporządzenie w sprawie bezpieczeństwa i higieny w publicznych i niepublicznych szkołach i placówkach (Dz.U. 2011 r. nr. 161 poz. 968)

Rozdział I

CELE

§ 4. Dane osobowe w Przedszkolu są gromadzone, przechowywane, edytowane, archiwizowane w kartotekach, skorowidzach, księgach, wykazach, zestawieniach oraz w innych zestawach i zbiorach ewidencyjnych na dokumentach papierowych, jak również w systemach informatycznych na elektronicznych nośnikach informacji.

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

1) w formie papierowej - przetwarzanej w ramach systemu tradycyjnego;
2) w formie elektronicznej - przetwarzanej w ramach systemu informatycznego.

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

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

§ 8.1. Przetwarzanie danych osobowych do celów związanych z działalnością Administratora Danych jest zgodne z prawem w sytuacji, gdy dane te zostały uzyskane od osoby, której dotyczą i wyraziła ona na ich przetwarzanie zgodę.

2. W sytuacji, gdy dane osobowe nie zostały uzyskane od osoby, której dotyczą, to ich przetwarzanie jest zgodne z prawem, gdy przepis szczególny tak stanowi.

3. Usunięcie danych nie wymaga zgody osoby, której dotyczą.

4. Ocena niezbędności przetwarzania danych do wypełnienia usprawiedliwionych celów Administratora Danych powinna być dokonywana indywidualnie w każdej sytuacji .

§ 9.1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, w wypadkach przewidzianych ustawą należy poinformować tę osobę o:

1) adresie swojej siedziby i pełnej nazwie,
2) celu zbierania danych, a w szczególności o znanych w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
3) prawie dostępu do treści swoich danych oraz ich poprawiania,

4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.
5) prawie do przenoszenia danych.
6) prawie do wzniesienia sprzeciwu wobec przetwarzania danych osobowych.
7) prawie do wniesienia skargi do Urzędu Ochrony Danych Osobowych.
8) prawie do bycia zapomnianym.

2. Powyższy obowiązek Administrator Danych nakłada na osoby zatrudnione przy przetwarzaniu danych osobowych.

§ 10.1. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, Administrator Danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o:

1) adresie swojej siedziby i pełnej nazwie,
2) celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych,
3) źródle danych,
4) prawie dostępu do treści swoich danych oraz ich poprawiania,
5) prawie wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację, jeżeli nawet przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą,
6) prawie wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, gdy przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.

2. Powyższy obowiązek Administrator Danych nakłada na osoby zatrudnione przy przetwarzaniu danych osobowych.

§ 11. Z zasadami w Polityce bezpieczeństwa obowiązkowo są zapoznawani wszyscy użytkownicy systemów tradycyjnych i informatycznych, składając odpowiednie oświadczenie, którego wzór stanowi załącznik Nr 1 do Polityki.

2. Oświadczenie przechowywane jest w aktach osobowych pracownika.

§ 12.1. Do informacji przechowywanych w systemach tradycyjnych jak i informatycznych mają dostęp jedynie upoważnieni pracownicy Przedszkola oraz osoby mające imienne zarejestrowane upoważnienie, którego wzór stanowi załącznik Nr 2 do niniejszej polityki. Wszyscy pracownicy zobowiązani są do zachowania tych danych w tajemnicy. Dopuszczalny sposób i zakres przetwarzania danych osobowych regulują zapisy ustaw kompetencyjnych, właściwych dla komórek organizacyjnych Przedszkola;

2. Upoważnienie określone w ust. 1 przechowywane jest w aktach osobowych pracownika;

2. Ewidencję osób uprawnionych do przetwarzania danych osobowych prowadzi Dyrektora Przedszkola oraz Inspektor Ochrony Danych;

3. Wzór ewidencji określonej w ust. 2 stanowi załącznik Nr 3 do Polityki bezpieczeństwa.

§ 13.1. Dane osobowe są chronione zgodnie z polskim prawem oraz procedurami obowiązującymi w jednostce organizacyjnej dotyczącymi bezpieczeństwa i poufności przetwarzanych danych.

2. Systemy informatyczne oraz tradycyjne, które przechowują dane osobowe, są chronione odpowiednimi środkami technicznymi.

Rozdział II

ADMINISTRACJA I ORGANIZACJA BEZPIECZEŃSTWA

§ 14. Za bezpieczeństwo danych osobowych przetwarzanych w systemach przetwarzania danych osobowych odpowiada Administrator Danych Osobowych (ADO).

§ 15.1 Administrator Danych Osobowych może powołać Inspektora Ochrony Danych, nadzorującego przestrzeganie zasad ochrony. Prowadzi on dokumentację opisującą sposób przetwarzania danych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

2. Administrator Danych Osobowych może powołać zastępców Inspektora Ochrony Danych, którzy spełniają warunki określone w art. 37-39 RODO oraz w art. 1. pkt 1) i art. 8 Ustawy o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000).

§ 16.1. Inspektor Ochrony Danych wykonuje wszystkie prace niezbędne do efektywnego oraz bezpiecznego zarządzania systemami informatycznymi i tradycyjnymi.

2. Inspektor Ochrony Danych jest zobowiązany do zapewnienia, poprzez zastosowanie odpowiednich środków i metod kontroli dostępu, tak by wyłącznie uprawniony użytkownik miał dostęp do systemów informatycznych i tradycyjnych.

3. Inspektor Ochrony Danych posiada bieżącą listę osób upoważnionych do przetwarzania danych osobowych.

4. Do zakresu odpowiedzialności i obowiązków Inspektor Ochrony Danych w szczególności:

1) zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,
b) nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 39 RODO.
c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych (szkolenia);

§ 17. Kierownik jednostki odpowiada za przestrzeganie ustawy o ochronie danych oraz przepisów wewnętrznych na poszczególnych stanowiskach, a w szczególności:

1) kontroluje sposób zabezpieczenia zbiorów danych osobowych przez pracowników,

2) kontroluje sposób realizacji obowiązku udzielania informacji o jakich mowa w ustawie,
3) zgłasza IOD planowaną rejestrację nowych zbiorów oraz przygotowuje wniosek w tej sprawie,
4) wnioskuje o nadanie upoważnień do przetwarzania danych osobowych pracownikom,
5) zgłasza potrzeby w zakresie zabezpieczenia danych osobowych w Przedszkolu.

§ 18. Użytkownik systemu wykonuje wszystkie prace niezbędne do efektywnej oraz bezpiecznej pracy na stanowisku pracy również z wykorzystaniem stacji roboczej. Jest odpowiedzialny przed ADO oraz IOD za realizację i utrzymanie niezbędnych warunków bezpieczeństwa, w szczególności do przestrzegania procedur dostępu do systemu i ochrony danych osobowych.

§ 19. Ze względu na rodzaj i charakter danych osobowych zawartych w zbiorach, w Przedszkolu wyróżnia się dwie kategorie danych:

1) **dane osobowe zwykłe** - wszelkie dane (informacje) dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, zgromadzone w zbiorach danych osobowych.
2) **dane osobowe szczególnej kategorii** – zgodnie z art. 4 pkt. 13-15 oraz art. 9 RODO - wszelkie dane (informacje) ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne, przynależność partyjną lub związkową, jak również informacje o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazania osoby, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Rozdział V

SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

§ 20.1. Obieg dokumentów zawierających dane osobowe, pomiędzy komórkami organizacyjnymi jednostki , winien się odbywać w sposób zapewniający pełną ochronę przed ujawnieniem zawartych w tych dokumentach danych (informacji).

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

3. Zabronione jest jednoczesne podłączanie komputerów do sieci wewnętrznej Przedszkola i sieci zewnętrznych (Plus , Era , Orange , Play, pozostałe sieci komórkowe, WiFi , WiMAX itp.).

Rozdział VI

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

§ 21.1. Dostęp do danych wprowadzonych przez użytkowników systemów informatycznych mają jedynie upoważnione osoby.

2. Pomieszczenia, w których przetwarza się dane osobowe powinny być fizycznie zabezpieczone przed dostępem osób nieuprawnionych, to znaczy posiadać odpowiednie zamki do drzwi.

3. Dokumenty i nośniki informacji, zawierające dane osobowe powinny być zabezpieczone przed dostępem osób nieupoważnionych do przetwarzania danych. Jeśli nie są aktualnie używane powinny być przechowywane w szafach lub w innych przeznaczonych do tego celu urządzeniach biurowych, posiadających odpowiednie zabezpieczenia.

Rozdział VII

UDOSTĘPNIANIE POSIADANYCH W ZBIORZE DANYCH OSOBOWYCH

§ 22.1. Na wniosek osoby, której dane dotyczą, ADO jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach, a zwłaszcza wskazać w formie zrozumiałej odnośnie danych osobowych jej dotyczących:

1) jakie dane osobowe zawiera zbiór,
2) w jaki sposób zebrano dane,
3) w jakim celu i zakresie dane są przetwarzane,
4) w jakim zakresie oraz komu dane zostały udostępnione.

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

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

1) uzyskania wyczerpującej informacji, czy taki zbiór istnieje, oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy,
2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze,
3) uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące, oraz podania w powszechnie zrozumiałej formie treści tych danych,
4) uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące,
5) uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane,
6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem RODO albo są już zbędne do realizacji celu, dla którego zostały zebrane
7) prawie wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację, jeżeli nawet przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą,

8) wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, gdy przetwarzanie jest niezbędne do wypełnienia usprawiedliwionych celów administratora danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych
9) wniesienia do administratora danych żądania ponownego, indywidualnego rozpatrzenia sprawy rozstrzygniętej z naruszeniem zakazu ostatecznego rozstrzygnięcia indywidualnej sprawy, gdy treść była wyłącznie wynikiem operacji na danych osobowych prowadzonych w systemie informatycznym.

2. Osoba zainteresowana może skorzystać z prawa do informacji, o których mowa w RODO, nie częściej niż raz na 6 miesięcy.

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

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

§ 25.1. Do udostępniania posiadanych w zbiorze danych osobowych upoważniony jest kierownik jednostki lub pracownik posiadający wymagane prawem upoważnienie.

2. W przypadku udostępniania danych osobowych w celach innych niż wyłączenie do zbioru, administrator danych udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

§ 26.1. Powierzenie przetwarzania danych osobowych innemu podmiotowi może nastąpić wyłącznie w drodze umowy zawartej w formie pisemnej przez ADO z uwzględnieniem wymagań określonych w art. 28 RODO.

Rozdział VIII

ZACHOWANIE BEZPIECZEŃSTWA PRZEZ UŻYTKOWNIKÓW SYSTEMU

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

§ 28.1. Wszyscy użytkownicy systemu muszą stosować się do obowiązujących procedur bezpieczeństwa.

2. Hasło podlega szczególnej ochronie. Użytkownik ma obowiązek tworzenia haseł.

Rozdział IX

BEZPIECZEŃSTWO FIZYCZNE

§ 29.1 Dane osobowe, które są przedmiotem przetwarzania zgodnie z przepisami ustawy o ochronie danych osobowych, gromadzone i przechowywane są w komputerach i w postaci tradycyjnej .

2. Środki bezpieczeństwa fizycznego są konieczne dla zapobiegania niepowołanemu dostępowi do informacji, nieautoryzowanym operacjom w systemie, kontroli dostępu do zasobów oraz w celu zabezpieczenia sprzętu teleinformatycznego.

§ 30.1. Obszar systemów informatycznych w Przedszkolu obejmuje wszystkie pomieszczenia znajdujące się w budynku przy ul. Klonowej 4 w Węgrowie.

§ 31. Pomieszczenia, w których znajdują się systemy informacji winny być:

wyposażone w szafy, meble biurowe zamykane na klucz umożliwiające przechowywanie dokumentów,

1) zamknięte, jeśli nikt w nich nie przebywa.

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

Rozdział X

BEZPIECZEŃSTWO SPRZĘTU I OPROGRAMOWANIA

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

§ 34. Sieć teleinformatyczna jest organizacyjnym i technicznym połączeniem systemów teleinformatycznych wraz z łączącymi je urządzeniami i liniami telekomunikacyjnymi. Niedopuszczalne jest samowolne przemieszczanie lub zmiana konfiguracji stacji roboczej bez wiedzy kierownika jednostki.

§ 35.1. Dostęp do zbiorów danych osobowych znajdujących się w komputerze następuje po wprowadzeniu hasła, które znane jest tylko osobie przetwarzającej dane.

2. Każdorazowo po dokonaniu przetworzenia aplikacja powinna być zamknięta.

3. W przypadku podejrzenia, iż wiadomości o sposobie dostępu do elektronicznej bazy danych uzyskała osoba do tego niepowołana, osoba przetwarzająca dane w porozumieniu z ADO powinna dokonać zmiany hasła.

§ 36.1. Elektroniczne bazy danych osobowych są archiwizowane.

§ 37. Używanie oprogramowania prywatnego w sieci jest zabronione. Na stacjach roboczych powinno być zainstalowane jedynie niezbędne oprogramowanie.

§ 38. W przypadku wynoszenia danych osobowych poza obszar przetwarzania na dyskach przenośnych typu pendrive, należy zadbać aby dyski te zabezpieczone hasłem lub szyfrem.

Rozdział XI

KONSERWACJE I NAPRAWY

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

§ 39. Za konserwację oprogramowania systemowego odpowiedzialny jest kierownik jednostki. Konserwacja oprogramowania obejmuje także jego aktualizację.

Rozdział XII

POLITYKA ANTYWIRUSOWA

§ 40. 1. Wszystkie komputery są sprawdzane przy użyciu oprogramowania do wykrywania i usuwania wirusów komputerowych.

2. W zakresie ochrony antywirusowej wprowadza się następujące zalecenia:

1) nie należy używać oprogramowania na stacji roboczej innego niż zaleca Administrator Danych Osobowych;
2) przed użyciem nośnika danych sprawdzić czy nie jest zainfekowany wirusem komputerowym.

2. W przypadku jakichkolwiek wątpliwości odnośnie zagrożenia wirusowego należy sprawdzić zawartość całego dysku twardego programem antywirusowym. W przypadku dalszych niejasności należy kontaktować się z administratorem sieci lokalnej.

Rozdział XIII

PRZEPISY KOŃCOWE

§ 41. Za naruszenie obowiązków wynikających z niniejszej Polityki Bezpieczeństwa oraz przepisów ustawy o ochronie danych osobowych może być uznane za ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym w szczególności wynikającym z przepisów RODO.

§ 42. W sprawach nie uregulowanych w niniejszej Polityce bezpieczeństwa informacji mają zastosowanie przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U.

2018 r. poz. 1000) oraz Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Rozdział XIV

ZAŁĄCZNIKI

1. Dokumenty Polityki Bezpieczeństwa ustanawiają metody zarządzania oraz wymagania niezbędne do zapewnienia skutecznej i spójnej ochrony przetwarzanych informacji.
2. Zestaw dokumentów Polityki Bezpieczeństwa składa się z:
    - 2.1. Niniejszego dokumentu Polityki Bezpieczeństwa.
    - 2.2. Wzoru oświadczenia pracownika do przetwarzania danych osobowych – Załącznik nr 1 Polityki.
    - 2.3. Wzoru upoważnienia dla pracownika do przetwarzania danych osobowych – Załącznik nr 2 Polityki.
    - 2.4. Wzoru ewidencji osób upoważnionych do przetwarzania danych osobowych – Załącznik nr 3 Polityki.
    - 2.5. Wzoru procedury postępowania na wypadek zaistnienia incydentu związanego z przetwarzaniem danych osobowych – Załącznik nr 4 Polityki.
    - 2.6. Wzoru rejestru naruszeń ochrony danych osobowych – Załącznik nr 5 Polityki.
    - 2.7. Wzoru raportu z naruszenia danych osobowych – Załącznik nr 6 Polityki.
    - 2.8. Wzoru rejestru realizacji żądań podmiotu danych – Załącznik nr 7 Polityki.
    - 2.9. Wzoru umowy powierzenia przetwarzania danych osobowych – Załącznik nr 8 Polityki.
    - 2.10. Wzoru analizy ryzyka – Załącznik nr 9 Polityki.
    - 2.11. Polityki monitoringu wizyjnego – Załącznik nr 10 Polityki