Załącznik Nr 1 do Zarządzenia Nr 12/2017/2018
Dyrektora Przedszkola Publicznego Nr 14
z Oddziałem Integracyjnym
z dnia 25.05.2018 r.

POLITYKA BEZPIECZEŃSTWA

PRZETWARZANIA DANYCH OSOBOWYCH

w Przedszkolu Publicznym Nr 14 Z ODDZIAŁEM INTEGRACYJNYM

(nazwa podmiotu)

ul. PUŁASKIEGO 93 A, 33-100 Tarnów

(siedziba: adres pocztowy)

PREAMBUŁA

Przedszkole Publiczne Nr 14 świadome wagi problemów związanych z ochroną prawa do prywatności, w tym w szczególności prawa osób fizycznych powierzających Przedszkolu swoje dane osobowe do właściwej i skutecznej ochrony tych danych przed nieuprawnionym wykorzystywaniem, deklaruje zamiar:

- *podejmowania wszystkich działań niezbędnych dla zapewnienia ochrony praw i usprawiedliwionych interesów każdej jednostki związanych z bezpieczeństwem jej danych osobowych,*

- *traktowania obowiązków zatrudnionych w Przedszkolu pracowników przetwarzających dane osobowe jako należących do kategorii podstawowych obowiązków pracowniczych oraz stanowczego egzekwowania ich prawidłowego wykonywania,*

- *stałego podnoszenia świadomości oraz kwalifikacji osób przetwarzających dane osobowe w Przedszkolu w zakresie konieczności zapewnienia bezpieczeństwa tych danych, w tym istniejących zagrożeń i propagowania świadomości wartości powierzonych danych osobowych jako czynnika wpływającego na jakość i ciągłość działalności oraz wiarygodność Przedszkola,*

- *doskonalenia i rozwijania nowoczesnych metod zabezpieczenia danych osobowych gromadzonych w Przedszkolu przed zagrożeniami związanymi z ich przetwarzaniem, szczególnie w zakresie dotyczącym dynamicznego rozwoju metod i technik przetwarzania tych danych w systemach informatycznych oraz sieciach telekomunikacyjnych.*

ROZDZIAŁ 1
Postanowienia ogólne

§ 1

Celem Polityki Bezpieczeństwa Przetwarzania Danych Osobowych zwana dalej „Polityką bezpieczeństwa", jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających dane osobowe.

§ 2

W związku ze zmianami przepisów niniejszy dokument stanowi wewnętrzną politykę przetwarzania danych w podmiocie na podstawie Rozporządzenia 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) oraz jest zgodny z powszechnie obowiązującymi przepisami prawa.

§ 3

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

ROZDZIAŁ 2
Definicje

§ 4

Przez użyte w Polityce bezpieczeństwa określenia należy rozumieć:

1. **RODO - Rozporządzenie Parlamentu Europejskiego i Rady (UE) General Data Protection Regulation - GDPR** 2016/679 z dnia 27 kwietnia 2016 r. w sprawie osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE;
2. **Ustawa o Ochronie Danych Osobowych** – wewnątrzkrajowy akt prawny mający charakter komplementarny względem Ogólnego Rozporządzenia – ma za zadanie precyzować niektóre zapisy Rozporządzenia;
3. **Administrator (poprzednio ADO – administrator danych osobowych)** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;
4. **dane osobowe** informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną,

genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

5. **zbiór danych osobowych** – „zbiór danych" oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
6. **Inspektor Ochrony Danych (IOD [dawniej administrator bezpieczeństwa informacji (ABI)]** – osoba wyznaczona przez administratora lub podmiot przetwarzający, posiadająca kwalifikacje zawodowe, a w szczególności wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych osobowych oraz umiejętności wypełniania zadań wynikających z zapisów RODO;
7. **Podmiot przetwarzający** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora, czyli działającym na jego zlecenie – instytucja powierzenia przetwarzania danych;
8. **Współadministratorzy** - co najmniej dwóch administratorów, którzy mają wspólny cel przetwarzania i wspólnie ustalają sposoby przetwarzania oraz uzgadniają, w sposób jasny i przejrzysty, zakresy swojej odpowiedzialności – to dwaj równorzędni administratorzy tego samego zbioru danych;
9. **przetwarzanie danych** – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
10. **system informatyczny –** rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
11. **system tradycyjny** – rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;
12. **zabezpieczenie danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
13. **administrator systemu informatycznego** – rozumie się przez to osobę lub osoby, upoważnione przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi;
14. **użytkownik** – rozumie się przez to upoważnionego przez administratora danych osobowych wyznaczonego do przetwarzania danych osobowych pracownika;
15. **identyfikator użytkownika (login)** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
16. **hasło** – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

ROZDZIAŁ 3
Zakres i cel stosowania

§ 5

1. Administrator to: **Przedszkole Publiczne Nr 14 Z Oddziałem Integracyjnym w Tarnowie.** Osobą administrująca w imieniu podmiotu jest: **Danuta Zawadzka Dyrektor Przedszkola**
2. Zgodnie z art. 37 Rozporządzenia Administrator powołuje **Inspektora Ochrony Danych,** którym jest: **Anna Słowik**
   e-mail: dyrpp14@umt.tarnow.pl
3. Do zadań Inspektora Ochrony Danych Osobowych należy:
   a) organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami Rozporządzenia i Ustawy o ochronie danych osobowych,
   b) zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki bezpieczeństwa,
   c) nadzorowanie wydawania i anulowania upoważnień do przetwarzania danych osobowych,
   d) nadzorowanie prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych,
   e) prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
   f) kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
   g) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych.

§ 6

1. Celem Polityki bezpieczeństwa jest przetwarzanie zgodnie z przepisami danych osobowych przetwarzanych w podmiocie oraz ich ochrona przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed uszkodzeniem, zniszczeniem lub nieupoważnioną zmianą.
2. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:
   a) **integralność i poufność** - dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych;
   b) **rozliczalność –** wykazanie, że określone decyzje odnoszące się do procesów przetwarzania danych osobowych zostały przeanalizowane z punktu widzenia zgodności z ogólnymi zasadami przetwarzania danych, a przede wszystkim, że są z nimi zgodne;
   c) **przejrzystość** - wymóg, by wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem tych danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem;
   d) **rzetelność** – wymóg, by osoba, której dane dotyczą, była dokładnie informowana o prowadzeniu operacji przetwarzania i o jej celach z uwzględnieniem konkretnych okoliczności i konkretnego kontekstu przetwarzania danych osobowych. Dotyczy to również faktu profilowania oraz informacji o konsekwencjach takiego profilowania. Jeżeli administrator planuje przetwarzać dane osobowe w celu innym niż cel, w których dane osobowe

zostały zebrane, powinien on przed takim dalszym przetwarzaniem poinformować osobę, której dane dotyczą, o tym innym celu oraz dostarczyć jej innych niezbędnych informacji;

e) **legalność** - dane powinny być przetwarzane zgodnie z prawem, czyli zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach;

f) **ograniczony cel** – dane zebrane wcześniej nie powinny być przetwarzane dalej w sposób niezgodny z celami, dla których zostały zebrane. Dalsze przetwarzanie danych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane za niezgodne z pierwotnymi celami;

g) **minimalizację danych** – przetwarzane dane mają być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;

h) **prawidłowość**– przetwarzane dane mają być prawidłowe i w razie potrzeby uaktualniane. Należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane. Realizacji tej zasady służy legitymowanie osób w celu weryfikacji ich danych oraz umożliwienie aktualizacji i poprawienia danych osobom, których dane się przetwarza;

i) **ograniczone przechowywanie** - dane muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane. Dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne w celu ochrony praw i wolności osób, których dane dotyczą;

3. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych, a **zarządzanie ryzykiem** rozumiane jest jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

§ 7

1. Zapisy polityki bezpieczeństwa zobowiązane są stosować wszystkie osoby, które w podmiocie mają dostęp do danych osobowych.
2. Polityka bezpieczeństwa dotyczy wszystkich danych osobowych przetwarzanych w podmiocie, niezależnie od formy ich przetwarzania (system tradycyjny, systemy informatyczne).
3. Polityka bezpieczeństwa ma zastosowanie wobec wszystkich komórek organizacyjnych w tym oddziałów, samodzielnych stanowisk pracy i wszystkich procesów przebiegających w ramach przetwarzania danych osobowych.

§ 8

Politykę bezpieczeństwa stosuje się w szczególności do:

a) danych osobowych przetwarzanych w systemach informatycznych;

b) wszystkich informacji dotyczących danych osobowych zawartych w przetwarzanych zbiorach;

c) wszystkich lokalizacji – budynków i pomieszczeń, w których są przetwarzane dane (wykaz miejsc przetwarzania danych stanowi **zał. nr 1** do niniejszej Polityki bezpieczeństwa);
d) wszystkich informacji danych zawartych w opisie struktury zbiorów;
e) informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych;
f) rejestru osób dopuszczonych do przetwarzania danych osobowych;
g) innych dokumentów zawierających dane osobowe.

§ 9

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

ROZDZIAŁ 4
Zbiory danych osobowych

§ 10

Dane osobowe gromadzone są w zbiorach danych. Wykaz zbiorów danych wraz ze wskazaniem systemu informatycznego służącego do przetwarzania danych stanowi **zał. nr 2** do niniejszej Polityki bezpieczeństwa.

§ 11

Struktura zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych określona została w **zał. nr 3** do niniejszej Polityki bezpieczeństwa.

§ 12

Przepływ danych pomiędzy poszczególnymi systemami został określony w **zał. nr 4** do niniejszej Polityki bezpieczeństwa.

ROZDZIAŁ 5
Nadawanie upoważnień do przetwarzania danych osobowych

§ 13

1. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające

upoważnienie nadane przez administratora danych osobowych.
Wzór upoważnienia stanowi **zał. nr 5** do niniejszej Polityki bezpieczeństwa.

2. Administrator nadając uprawnienia pracownikom, którzy przetwarzają dane odbiera od pracownika oświadczenie o zachowaniu danych w poufności oraz o zapoznaniu się z dokumentami określającymi zasady zabezpieczania i przetwarzania danych osobowych w podmiocie.
3. Administrator prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, która stanowi **zał. nr 6** do niniejszej Polityki bezpieczeństwa.

ROZDZIAŁ 6
Udostępnienie i powierzanie danych osobowych

§ 14

1. Administrator bądź pracownicy upoważnieni do przetwarzania danych mogą udostępnić dane osobie wnioskującej z zachowaniem zasady, że udostępnienie danych osobowych nie może naruszać praw i wolności osoby, których dane dotyczą. Wzór wniosku o udostępnienie danych stanowi **zał. nr 7** do niniejszej Polityki bezpieczeństwa. Każdorazowe udostępnienie danych musi być odnotowane w rejestrze udostępnienia, który stanowi **zał. nr 8** do niniejszej Polityki bezpieczeństwa.
2. Dopuszczalne jest powierzenie przez administratora danych przetwarzania danych podmiotom zewnętrznym.
3. Powierzenie przetwarzania danych może mieć miejsce na podstawie pisemnej umowy określającej w szczególności zakres i cel przetwarzania danych. Umowa musi określać też zakres odpowiedzialności podmiotu, któremu powierzono przetwarzanie danych z tytułu niewykonania lub nienależytego wykonania umowy oraz sposób rozwiązania umowy. Wzór umowy powierzenia danych stanowi **zał. nr 9** do niniejszej Polityki bezpieczeństwa.
4. Powierzenie przetwarzania danych osobowych musi uwzględniać ponadto wymogi określone w RODO. W szczególności podmiot zewnętrzny, któremu ma zostać powierzone przetwarzanie danych osobowych, jest obowiązany przed rozpoczęciem przetwarzania danych do podjęcia środków zabezpieczających.
5. Powierzenie przetwarzania danych osobowych nie oznacza zwolnienia z odpowiedzialności administratora danych za zgodne z prawem przetwarzanie powierzonych danych, co wymaga w umowach stanowiących podstawę powierzenia przetwarzania danych umieszczenia prawa administratora danych do kontroli wykonania przedmiotu umowy w siedzibie podmiotu zewnętrznego m. in. w zakresie przestrzegania Polityki bezpieczeństwa, Instrukcji zarządzania systemem informatycznym oraz właściwych przepisów prawa.
6. Wykaz podmiotów, którym powierzono przetwarzanie danych stanowi **zał. nr 10** do niniejszej Polityki bezpieczeństwa.
7. Powierzenie przetwarzania danych uregulowane w Polityce bezpieczeństwa nie ma zastosowania do przekazywania danych podmiotom upoważnionym do ich przetwarzania na mocy przepisów prawa, w tym w szczególności ZUS, Prokuraturze, Policji, Sądom, Komornikom, itd.

ROZDZIAŁ 7
Wynoszenie akt i dokumentacji

§ 15

1. Poza miejsca przetwarzania danych wskazanych w zał. nr 1 nie wolno wynosić żadnej dokumentacji ani akt związanych z wykonywaniem czynności służbowych, a zwłaszcza dokumentów zawierających dane osobowe.
2. Przepis powyższy nie dotyczy tych pracowników, których zakres obowiązków wymaga dokonywania czynności służbowych z dokumentacją zawierającą dane osobowe poza obszarem przetwarzania danych, a także czynności związanych z przesyłaniem i transportem korespondencji.
3. Pracownicy, o których mowa w punkcie powyżej, są zobowiązani stosować środki zapewniające ochronę powierzonych danych osobowych podczas ich transportu, przechowywania i użytkowania poza obszarem siedziby pracodawcy, a w szczególności zabezpieczyć te dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
4. Pracownicy tacy ponoszą pełną odpowiedzialność za powierzony im sprzęt oraz dokumentację znajdującą się poza siedzibą administratora.
5. Każdy pracownik, który podejrzewa, iż mogło nastąpić naruszenie bezpieczeństwa ochrony danych osobowych lub próba dokonania takiego naruszenia przez osoby nieupoważnione, jest zobowiązany do niezwłocznego poinformowania o powyższym Administratora, który prowadzi postępowanie kontrolne, pod kątem wyjaśnienia okoliczności ewentualnego naruszenia bezpieczeństwa danych osobowych.
6. Odpowiedzialność za bezpieczeństwo dokumentacji lub akt wynoszonych poza obszar przetwarzania danych ponosi pracownik, który te akta wynosi, z chwilą ich pobrania. Odpowiedzialność ta dotyczy również danych znajdujących się na nośnikach cyfrowych.
7. Po zwrocie akt i dokumentacji (lub przenośnych komputerów) przez pracownika, przełożony zobowiązany jest do jej sprawdzenia pod kątem zgodności ze stanem sprzed wypożyczenia.
8. Pozostawanie w pracy po godzinach pracy może mieć miejsce tylko w związku z pełnionymi obowiązkami i za zgodą administratora danych lub osoby przez niego upoważnionej.
9. Każdy pracownik po zakończeniu pracy zobowiązany jest zamknąć w szafach wszelką dokumentację oraz komputer przenośny (w przypadku jego używania), a następnie osobiście zabezpieczyć klucze z zachowaniem wszelkich zasad bezpieczeństwa.

ROZDZIAŁ 8
Zasady korzystania z komputerów przenośnych

§ 16

1. Przetwarzanie danych osobowych na komputerach przenośnych powinno być ograniczone do niezbędnych przypadków.
2. Przetwarzanie danych osobowych przy użyciu komputerów przenośnych może odbywać się wyłącznie za zgodą administratora danych lub osoby przez niego upoważnionej.
3. Zakres danych przetwarzanych na komputerze przenośnym oraz zakres uprawnień do przetwarzanych danych ustala bezpośredni przełożony pracownika za wiedzą administratora danych.

4. Osoba korzystająca z komputera przenośnego w celu przetwarzania danych osobowych zobowiązana jest do zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych informacji, zwłaszcza przed dostępem do nich osób nieupoważnionych oraz przed zniszczeniem.

§ 17

Użytkownik komputera przenośnego zobowiązany jest do:

a) transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia, a w szczególności: transportowania komputera w bagażu podręcznym, nie pozostawiania komputera w samochodzie, przechowalni bagażu, itp.,
b) przenoszenia komputera w torbie przeznaczonej do przenoszenia komputerów przenośnych,
c) korzystania z komputera w sposób minimalizujący ryzyko podejrzenia danych przez osoby nieupoważnione, w szczególności zabrania się korzystania z komputera w miejscach publicznych i w środkach transportu publicznego,
d) nie zezwalania osobom nieupoważnionym do korzystania z komputera przenośnego, na którym przetwarzane są dane osobowe,
e) zabezpieczania komputera przenośnego hasłem i blokowanie dostępu przed użyciem przez osoby postronne,
f) kopiowania danych osobowych przetwarzanych na komputerze przenośnym do systemu informatycznego w celu umożliwienia wykonania kopii awaryjnej tych danych,
g) umożliwienia, poprzez podłączenie komputera do sieci informatycznej administratora danych w celu aktualizacji wzorców wirusów w programie antywirusowym,
h) utrzymania konfiguracji oprogramowania systemowego w sposób wymuszający korzystanie z haseł,
i) wykorzystywania haseł odpowiedniej jakości zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym przetwarzającym dane osobowe,
j) zmiany haseł zgodnie z wymaganiami dla systemu informatycznego przetwarzającego dane osobowe.

ROZDZIAŁ 9
Środki techniczne i organizacyjne zabezpieczenia danych osobowych

§ 18

1. Zabezpieczenia organizacyjne:
   a) sporządzono i wdrożono Politykę bezpieczeństwa;
   b) sporządzono i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
   c) sporządzono Rejestr czynności przetwarzania, który stanowi **zał. nr 11** do niniejszego dokumentu;
   d) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych, bądź osobę przez niego upoważnioną;
   e) wdrożono instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych, która stanowi **zał. nr 12** do niniejszego dokumentu

f) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;
g) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
h) przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;
i) przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych;
j) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych;
k) wprowadzono zasadę „czystego biurka", która stanowi **zał. nr 13** do niniejszego dokumentu;
l) dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonując takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści, aby po dokonaniu usunięcia danych niemożliwa była identyfikacja osób;
m) informacji telefonicznych nie udziela się, względnie udziela się po zidentyfikowaniu rozmówcy i stwierdzeniu jego upoważnienia do uzyskania danych;
n) wyznaczono inspektora ochrony danych.

2. Zabezpieczenia techniczne:
   a) stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową Eset Endpoint Antivirus;
   b) konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych przechowywanych w systemie informatycznym wyłącznie za pośrednictwem używanych aplikacji;
   c) zastosowano wygaszenie ekranu w przypadku dłuższej nieaktywności użytkownika;
   d) komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkowania, zmiana hasła raz w miesiącu
3. Środki ochrony fizycznej:
   a) drzwi zwykłe (wzmocnione, metalowe, o podwyższonej odporności, zamykane na klucz);
   b) urządzenia służące do przetwarzania danych osobowych i dokumentację zawierającą dane osobowe umieszcza się w zamykanych pomieszczeniach;
   c) obszar, na którym przetwarzane są dane osobowe, chroniony jest poprzez zastosowanie:
      - monitoring
      - alarm.

ROZDZIAŁ 10
Szkolenia użytkowników

§ 19

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej zostaje poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
2. Za zorganizowanie szkolenia odpowiada Administrator.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u administratora danych osobowych.
4. Zgodnie z wymogami pracownicy zostają zapoznani z przepisami z zakresu ochrony danych osobowych w każdym przypadku istotnych zmian w przepisach dotyczących przetwarzania danych.
5. Szkolenie zostaje zakończone podpisaniem przez słuchacza oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych.
6. Dokument ten jest przechowywany w aktach osobowych użytkowników i stanowi podstawę do podejmowania działań w celu nadania im uprawnień do korzystania z systemu informatycznego przetwarzającego dane osobowe.

ROZDZIAŁ 11
Postanowienia końcowe

§ 20

1. Wszyscy pracownicy zobowiązani są do zapoznania się z niniejszym dokumentem oraz do stosowania zawartych w nim reguł.
2. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
3. Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z prawem oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
4. W sprawach nieuregulowanych w polityce mają zastosowanie powszechnie obowiązujące przepisy dotyczące ochrony danych osobowych oraz RODO.
5. Dokumentem powiązanym z niniejszą polityką jest Instrukcja zarządzania systemem informatycznym.
6. Integralną część dokumentacji stanowią załączniki:

Zał. nr 1 - Wykaz budynków i pomieszczeń
Zał. nr 2 - Wykaz zbiorów danych
Zał. nr 3 - Opis struktury zbiorów danych
Zał. nr 4 - Przepływ danych
Zał. nr 5 - Upoważnienie do przetwarzania danych
Zał. nr 6 - Ewidencja osób upoważnionych
Zał. nr 7 - Wniosek o udostępnienie danych
Zał. nr 8 - Zestawienie udostępnianych danych
Zał. nr 9 - Wzór umowy powierzenia danych

Zał. nr 10 - Wykaz podmiotów, którym powierzono dane
Zał. nr 11 - Rejestr czynności przetwarzania
Zał. nr 12 – Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych
Zał. nr 13 – Zasada „czystego biurka"

§ 21

Niniejszy dokument wchodzi w życie z dniem 25 maja 2018 r.

Podpis:

DYREKTOR

mgr Danuta Zawadzka

.....

Administrator