ZARZĄDZENIE NR 8/2017/2018
DYREKTORA ŻŁOBKA MIEJSKIEGO W LUBAWIE „AKADEMIA MALUSZKA"
z dnia 21.05.2018r.

w sprawie: wprowadzenia Polityki Ochrony Danych Osobowych w Żłobku Miejskim w Lubawie „Akademia Maluszka"

Na podstawie:
Art. 29 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) (Dz. Urz. UE L 119, s.1)
zarządzam, co następuje:

§ 1

Wprowadzam w Żłobku Miejskim w Lubawie „Akademia Maluszka" Politykę Ochrony Danych Osobowych, której treść stanowi załącznik nr 1 do zarządzenia, oraz Instrukcję zarządzania RODO, która stanowi załącznik nr 2 do zarządzenia.

§ 2

Każdy pracownik jest obowiązany zapoznać się z treścią załącznika nr 1 i nr 2 do zarządzenia.

§ 3

Pracodawca zobowiązuje wszystkich pracowników do przestrzegania Polityki Ochrony Danych oraz stosowania w pracy Instrukcji pod sankcją konsekwencji służbowych, przewidzianych prawem.

§ 4

1. Zarządzenie wchodzi w życie z dniem podpisania.
2. Z dniem wejścia w życie zarządzenia traci moc Zarządzenie Nr 27/2016/2017 Dyrektora Żłobka Miejskiego w Lubawie „Akademia Maluszka" z dnia 17.08.2017r. w sprawie: wprowadzenia Polityki bezpieczeństwa informatycznego i ochrony danych osobowych obowiązująca w Żłobku Miejskim w Lubawie Akademia Maluszka.

Załączniki:
Załącznik nr 1
do Zarządzenia Nr 8/2017/2018 Dyrektora Żłobka Miejskiego w Lubawie „Akademia Maluszka" z dnia 21.05.2018r. – Polityka Ochrony Danych Osobowych w *Żłobku Miejskim w Lubawie „Akademia Maluszka".*

Załącznik nr 2
do Zarządzenia Nr 8/2017/2018 Dyrektora Żłobka Miejskiego w Lubawie „Akademia Maluszka" z dnia 21.05.2018r. – Instrukcję zarządzania RODO –wykaz zabezpieczeń RODO w Żłobku miejskim w Lubawie „Akademia Maluszka"

Załącznik nr 1 *do Zarządzenia Nr 8/2017/2018 Dyrektora Żłobka Miejskiego w Lubawie „Akademia Maluszka" z dnia 21.05.2018r.* – Polityka Ochrony Danych Osobowych

Polityka Ochrony Danych Osobowych w Żłobku Miejskim w Lubawie „Akademia Maluszka"

Lubawa, 2018

1 Wstęp 3
2 Ocena skutków (analiza ryzyka) 5
2.1 Opis operacji przetwarzania (inwentaryzacja aktywów) 5
2.2 Ocena niezbędności oraz proporcjonalności (zgodność z przepisami RODO) 5
2.3 Analiza ryzyka 6
2.4 Plan postępowania z ryzykiem 8
3 Upoważnienia 8
4 Środki organizacyjne i techniczne zabezpieczające dane osobowe 8
5 Regulamin Ochrony Danych Osobowych 8
6 Szkolenia 8
7 Instrukcja postępowania z incydentami 9

1 WSTĘP

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO).

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

DEFINICJE

Administrator (danych) - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

RODO – rozporządzenie parlamentu europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016)

Dane osobowe - to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną poprzez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej

czynników specyficznych dla fizycznego, fizjologicznego, genetycznego, umysłowego, ekonomicznego, kulturowego lub społecznego.

Przetwarzanie danych osobowych to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych i obejmuje zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych.

Ograniczenie przetwarzania - polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania

Anonimizacja- zmiana danych osobowych w wyniku której dane te tracą charakter danych osobowych

Zgoda osoby, której dane dotyczą - oznacza dowolne, dowolnie określone, konkretne, świadome i jednoznaczne wskazanie osoby, której dane dotyczą, za pomocą oświadczenia lub wyraźnego działania potwierdzającego, wyrażającego zgodę na przetwarzanie danych osobowych z nim związanych. Zgoda musi być udokumentowana we właściwy sposób, aby ją udowodnić.

Ocena skutków w ochronie danych - to proces przeprowadzany przez Administratora, jeśli jest wymagany przez obowiązujące prawo i, jeśli to konieczne, z uczestnictwem inspektora ochrony danych, przed przetwarzaniem, w przypadku, gdy istnieje prawdopodobieństwo wysokiego ryzyka dla praw i wolności osób fizycznych jako rodzaju przetwarzania danych osobowych i zachodzi wraz z wykorzystaniem nowych technologii, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania. Proces ten musi ocenić wpływ planowanych operacji przetwarzania na ochronę danych osobowych.

Podmiotem danych jest każda osoba fizyczna, która jest przedmiotem przetwarzanych danych.

Odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

Podmiot przetwarzający (**Procesor)** to osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu administratora.

Inspektor Ochrony Danych (IOD) - to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi i pracownikom w zakresie obowiązującego prawa o ochronie danych i niniejszej Polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.

Pseudonimizacja - oznacza przetwarzanie danych osobowych w taki sposób (np. poprzez zastępowanie nazw liczbami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. Listy referencyjnej nazwisk i numerów), pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym w celu zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Szczególne kategorie danych osobowych - ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach

zawodowych i obejmują przetwarzanie danych genetycznych, dane biometryczne w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia, dane dotyczące naturalnego życie seksualne osoby lub orientację seksualną. W zależności od obowiązującego prawa, specjalne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych i karnych oraz o sankcjach.

Profilowanie – jest dowolną forma zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Naruszenie ochrony danych osobowych - jest to przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

2 OCENA SKUTKÓW (ANALIZA RYZYKA)

Ocena skutków jest formalną, określoną w art. 35 RODO procedurą przeprowadzenia analizy ryzyka za wykonanie której odpowiada Administrator. Jeżeli Administrator nie jest zobowiązany do przeprowadzenia oceny skutków, może mimo to stosować poniższą procedurę do przeprowadzenia analizy ryzyka na potrzeby wykazania rozliczalności spełnienia wymagań RODO.

W przypadku powołania Inspektora Ochrony Danych – ocena skutków musi być wykonana z jego współudziałem.

2.1 OPIS OPERACJI PRZETWARZANIA (INWENTARYZACJA AKTYWÓW)

1. W celu dokonania analizy ryzyka wymagane jest zidentyfikowanie danych osobowych, które należy zabezpieczyć. Dane te w postaci zbiorów (kategorii osób) zostały wykazane w załączniku: Załącznik nr 1 - Rejestr czynności przetwarzania (wykaz zbiorów danych osobowych).
2. Opis zbiorów (kategorii osób) powinien obejmować takie informacje, jak:
    a. nazwę zbioru (opis kategorii osób)
    b. opis celów przetwarzania
    c. charakter, zakres, kontekst danych osobowych
    d. odbiorcy danych
    e. funkcjonalny opis operacji przetwarzania
    f. aktywa służące do przetwarzania danych osobowych (Informacje, Programy, Systemy operacyjne, Infrastruktura IT, Infrastruktura, Pracownicy i współpracownicy, Outsourcing).

2.2 OCENA NIEZBĘDNOŚCI ORAZ PROPORCJONALNOŚCI (ZGODNOŚĆ Z PRZEPISAMI RODO)

W ramach przeprowadzenia oceny skutków (analizy ryzyka) Administrator zobowiązany jest do spełnienia obowiązków prawnych wobec danych w zbiorach
W szczególności należy zapewnić, że :

1. dane te są legalnie przetwarzane (na podstawie art. 6, 9)
2. dane te są adekwatne w stosunku do celów przetwarzania
3. dane te są przetwarzane przez określony czas (retencja danych)
4. wobec tych osób wykonano tzw. obowiązek informacyjny (art. 12, 13 i 14) wraz ze wskazaniem ich praw (np. prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, odwołania zgody)
5. opracowano klauzule informacyjne dla powyższych osób
6. istnieją umowy powierzenia z podmiotami przetwarzającymi (art. 28) zgodnie z załącznikiem Załącznik nr 2 Umowa powierzenia

2.3 ANALIZA RYZYKA

Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Przyjęto, że analiza ryzyka przeprowadzana jest dla zbioru lub grupy zbiorów (kategorii osób) lub dla procesów przetwarzania.

2.3.1 Definicje

1. Aktywa – środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych
2. Naruszenie (Incydent) ochrony danych osobowych - to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych
3. Zagrożenie - potencjalne naruszenie (potencjalny incydent)
4. Skutki - rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia)
5. Ryzyko - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów

2.3.2 Wyznaczenie zagrożeń

1. Administrator jest odpowiedzialny za określenie listy zagrożeń naruszenia poufności, dostępności i integralności, które mogą wystąpić w przetwarzaniu danych w zbiorze, dla kategorii osób lub w procesie przetwarzania
2. Zagrożenia powinny być identyfikowane w odniesieniu do uprzednio zidentyfikowanych aktywów

2.3.3 Wyliczenie ryzyka dla zagrożeń

1. Administrator określa Prawdopodobieństwo (**P**) wystąpienia poszczególnych zagrożeń w zbiorze (dla kategorii osób) lub w procesie przetwarzania
2. Proponowaną skalę prawdopodobieństwa prezentuje Tabela A
3. Administrator określa Skutki (**S**) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne
4. Proponowaną Skalę skutków prezentuje Tabela B

5. Administrator wylicza Ryzyka (R) dla wszystkich zagrożeń i ich skutków w/g formuły: **R = P * S**

Tabela A PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA	**SKALA (WAGA)**
zagrożenie niskie	1
zagrożenie średnie	2
zagrożenie wysokie	3

Tabela B SKUTKI WYSTĄPIENIA ZAGROŻENIA	**SKALA (WAGA)**
małe (do 10000 PLN, incydent prasowy lokalny)	1
średnie (10000-100000 PLN, incydent prasowy ogólnopolski)	2
duże (od 100000 PLN, naruszenie prawa)	3

2.3.4 Porównanie wyliczonych ryzyk ze skalą i określenie dalszego postępowania z ryzykiem

1. Administrator porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem
2. Proponowaną skalę Ryzyka prezentuje Tabela C

Tabela C POZIOM RYZYKA	**WARTOŚĆ** [**R = P*S**]
ryzyko pomijalne i akceptowalne (akceptujemy)	1-2
ryzyko jest opcjonalne (akceptujemy albo obniżamy)	3-6
ryzyko jest nieakceptowalne (musimy obniżyć)	9

2.3.5 Reakcja na wartość ryzyka

1. Akceptacja ryzyka – zabezpieczenia są właściwe – brak potrzeby stosowania dodatkowych zabezpieczeń
2. Działania obniżające ryzyko, które może zastosować Administrator:
    a. Przeniesienie –przerzucenie ryzyka
    b. Unikanie – eliminacja działań powodujących ryzyko Redukcja – zastosowanie zabezpieczeń w celu obniżenia ryzyka
3. Analizę ryzyka przeprowadza się w specjalnym szablonie Załącznik nr 3 Arkusz analizy ryzyka RODO

2.3.6 Ponowna analiza ryzyka

Ponowna analiza ryzyka przeprowadzana jest cyklicznie lub po znaczących zmianach w przetwarzaniu danych.

2.4 PLAN POSTĘPOWANIA Z RYZYKIEM

1. Wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne, i zobowiązany jest do monitorowania wdrożenia zabezpieczeń

3 UPOWAŻNIENIA

1. Administrator odpowiada za nadawanie / anulowanie upoważnień do przetwarzania danych w zbiorach (dla kategorii osób) w postaci papierowej oraz w systemach informatycznych
2. Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisu prawa
3. Upoważnienia stanowi Załącznik nr 4 - Upoważnienie do przetwarzania danych osobowych

4 ŚRODKI ORGANIZACYJNE I TECHNICZNE ZABEZPIECZAJĄCE DANE OSOBOWE

Administrator jest zobowiązany do stosowania środków technicznych i organizacyjnych (zabezpieczeń) adekwatnych do zagrożeń naruszenia praw i wolności osób.

1. Administrator opracował Instrukcję zarządzania RODO w którym zabezpieczenia są opisane w formie procedur
2. Instrukcja powinien być aktualizowany, jeśli zajdzie taka potrzeba po przeprowadzeniu analizy ryzyka.

5 REGULAMIN OCHRONY DANYCH OSOBOWYCH

Regulamin (rozumiany jako zabezpieczenie) ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania. Patrz załącznik nr 5 Regulamin Ochrony Danych Osobowych

Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania, patrz załącznik nr 6 Oświadczenie poufności

6 SZKOLENIA

1. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi winna być poddana przeszkoleniu lub zapoznana z przepisami RODO
2. Za przeprowadzenie szkolenia odpowiada IOD
3. Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania.

7 INSTRUKCJA POSTĘPOWANIA Z INCYDENTAMI

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu bezpośredniego przełożonego (lub jeśli jest powołany – Inspektora Ochrony Danych)
2. Do typowych podatności bezpieczeństwa danych osobowych należą:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
    b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych
    c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek)
3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
    a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)
    b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych)
    c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania)
4. W przypadku stwierdzenia wystąpienia incydentu, Administrator (lub w przypadku powołania – IOD) prowadzi postępowanie wyjaśniające w toku, którego:
    a. ustala zakres i przyczyny incydentu oraz jego ewentualne skutki
    b. inicjuje ewentualne działania dyscyplinarne
    c. działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu
    d. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia
5. Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze –patrz załącznik nr 7 Formularz rejestracji incydentu
6. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych
7. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – Administrator zgłasza je organowi nadzorczemu.
8. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

Załączniki:

- **Załącznik nr 1** - Rejestr czynności przetwarzania (wykaz zbiorów danych osobowych).
- **Załącznik nr 2** - Umowa powierzenia.
- **Załącznik nr 3** - Arkusz analizy ryzyka RODO.
- **Załącznik nr 4** - Upoważnienie do przetwarzania danych osobowych
- **Załącznik nr 5** - Regulamin Ochrony Danych Osobowych
- **Załącznik nr 6** - Oświadczenie poufności.
- **Załącznik nr 7**- Formularz rejestracji incydentu.

Załącznik nr 1 do Polityki Ochrony Danych Osobowych
Rejestr czynności przetwarzania, jako
Wykaz zbiorów danych osobowych

Administrator: Żłobek Miejski w Lubawie „Akademia Maluszka"

Spis treści:

Kandydaci do pracy 11
Pracownicy etatowi, umowy zlecenia, byli pracownicy 12
Kontrahenci (dostawcy) 12
Rejestr korespondencyjny 13
Monitoring 13
Nabór i rekrutacja do żłobka 14
Dzieci 14

Opis kategorii osób (zbioru) w formie rejestru czynności przetwarzania	Aktywa	Proces przetwarzania / opis funkcjonalny
1. Opis kategorii osób (nazwa zbioru) **8 KANDYDACI DO PRACY** **1.a Opis kategorii danych osobowych** Dane identyfikacyjne, dane adresowe, dane o wykształceniu, stażu pracy, uprawnieniach zawodowych **2. Cele przetwarzania** Rekrutacja pracowników **3. kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **4. planowane terminy usunięcia poszczególnych kategorii danych** w przypadku udzielonej zgody na bieżącą rekrutację – czas przechowywania 2 miesiące w przypadku udzielonej zgody kandydatów na przyszłe rekrutacje – czas przechowywania określono na 2 lata **5. opis technicznych i organizacyjnych środków bezpieczeństwa** Patrz: Instrukcja zarządzania RODO, Regulamin ODO **6. Podstawa prawna przetwarzania** RODO: Art.6, ust 1, lit. a (na podst. zgody osoby)	**1. Informacje (dokumentacja papierowa)** CV **2. Programy i systemy operacyjne** Mail, windows **3. Infrastruktura** Pomieszczenia działu kadr, kierowników **4. Pracownicy i współpracownicy** Pracownicy działu kadr, Informatyk,	1. Przesłanie CV mailem na adres poczty elektronicznej 2. Złożenie CV osobiście 3. Usunięcie CV po wymaganym czasie

1. Opis kategorii osób (nazwa zbioru) **9 PRACOWNICY ETATOWI, UMOWY ZLECENIA, BYLI PRACOWNICY** **1.a Opis kategorii danych osobowych** Dane identyfikacyjne, dane adresowe, dane o Oddziale Kasy Chorych, zgłoszenie członka rodziny, zgłoszenia opieki , wysługa lat pracy, stawka wynagrodzeń, dane o czasie pracy, przyznanych nagrodach, potrąceniach, składki związkowe, zajęcia komornicze, numery kont dla przelewów bankowych pracownika **2. Cele przetwarzania** Zatrudnianie pracowników **3. Kategorie odbiorców** Medycyna pracy, komercyjna opieka medyczna, Pakiety socjalne), biuro rachunkowe (umowa powierzenia), ZUS, US **4. kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. planowane terminy usunięcia poszczególnych kategorii danych** Dane osób zatrudnionych w formie etatów - 50 lat **6. opis technicznych i organizacyjnych środków bezpieczeństwa** Patrz: Instrukcja zarządzania RODO, Regulamin ODO **7. Podstawa prawna przetwarzania** Art.6, ust 1, lit. a - Ubezpieczenie grupowe za zgodą pracowników, upublicznienie wizerunku pracownika za zgodą Art.6, lit. c (na podst. Kodeksu pracy, Ustawa o systemie ubezpieczeń społecznych) Art.6, lit. b (dane niezbędne do umów zleceń i umów o dzieło)	**1. Informacje (dokumentacja papierowa)** Akta osobowe, ZFŚS, Dokumentacja BHP, **2. Programy i systemy operacyjne** Program Kady-Płace, Puma, Płatnik, Windows, pliki z danymi pracowników, email **3. Infrastruktura IT** Serwer, NAS, dyski sieciowe, wewnętrzna sieć, router, switche, stacje robocze **4. Infrastruktura** Pomieszczenia działu kadr, archiwum, system kontroli dostępu do pomieszczeń **5. Pracownicy i współpracownicy** Pracownicy działu kadr, Informatyk,	1. Zaprowadzenie akt osobowych i innej dokumentacji zatrudnieniowej 2. Wprowadzenie danych do systemu kadrowo-płacowego 3. Obsługa Zakładowego Funduszu świadczeń socjalnych 4. Rozliczanie pracowników z ZUS oraz z US, wypłaty wynagrodzenia, organizacja wyjazdów służbowych, ubezpieczenia społecznego, ubezpieczenia chorobowego 5. Archiwizacja byłych pracowników
1. Opis kategorii osób (nazwa zbioru) **10 KONTRAHENCI (DOSTAWCY)** **1.a Opis kategorii danych osobowych** Dane identyfikacyjne, dane adresowe **2. Cele przetwarzania** Realizacja umów na dostawę towarów lub usług świadczonych przez osoby fizyczne prowadzące działalność gospodarczą **3. Kategorie odbiorców** Bank w zakresie przelewów, Biuro rachunkowe **4. kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. planowane terminy usunięcia poszczególnych kategorii danych** dane kontrahenta przechowywane są przez okres 6 lat (art. 86 § 1 Ordynacji podatkowej). LUB	**1. Informacje (dokumentacja papierowa)** Zamówienia, faktury od dostawcy, umowy **2. Programy i systemy operacyjne** Puma, MS Office, Adobe Reader, poczta **3. Infrastruktura IT** Serwer, macierz dyskowa, NAS, dyski sieciowe, wewnętrzna sieć, router, switche, stacje robocze, smartfony **4. Infrastruktura** Pomieszczenia działu zaopatrzenia, serwerownia, księgowość, magazyn **5. Pracownicy i współpracownicy** Informatyk, Księgowe	1. Zbieranie ofert dostawców 2. Umowa z dostawcą / Zamówienie towaru, usługi (przesłanie do dostawcy mailem) 3. Przyjęcie faktury i WZ – mailem lub papierowo 4. Wprowadzenie danych do programu księgowego 6. Realizacja płatności za faktury 7. Archiwizacja faktur

dane kontrahentów przetwarzane są do momentu ustania przetwarzania w celach analityki oraz planowania biznesowego, na podstawie Art.6, ust 1, lit. f (RODO) – prawnie usprawiedliwionego interesu administratora **6. opis technicznych i organizacyjnych środków bezpieczeństwa** Patrz: Instrukcja zarządzania RODO, Regulamin ODO **7. Podstawa prawna przetwarzania** Art.6, ust 1, lit. b – dane niezbędne do realizacji umowy		
1. Opis kategorii osób (nazwa zbioru) **11 REJESTR KORESPONDENCYJNY** **1a. Opis kategorii danych osobowych** Dane identyfikacyjne, dane adresowe **2. Cele przetwarzania** Zarządzanie korespondencją przychodzącą i wychodzącą **3. Kategorie odbiorców** Poczta **4. kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. planowane terminy usunięcia poszczególnych kategorii danych** 2 lata **6. opis technicznych i organizacyjnych środków bezpieczeństwa** Patrz: Instrukcja zarządzania RODO, Regulamin ODO **7. Podstawa prawna przetwarzania** Art.6, ust 1, lit. c – na podstawie przepisów prawa (jeśli rejestr jest prowadzony w podmiocie publicznym) Art.6, ust 1, lit. f – jako prawnie usprawiedliwiony interes administratora (jeśli rejestr jest prowadzony do celów organizacyjnych)	**1. Informacje (dokumentacja papierowa)** Książka korespondencyjna **2. Programy i systemy operacyjne** Rejestr papierowy **3. Infrastruktura IT** Stacja robocza **4. Infrastruktura** Księgowość **5. Pracownicy i współpracownicy** Księgowe, referenci	1. Rejestracja elektroniczna i papierowa korespondencji wysyłanej i otrzymywanej. 2. Archiwizacja.
1. Opis kategorii osób (nazwa zbioru) **12 MONITORING** **1a. Opis kategorii danych osobowych** Wizerunek **2. Cele przetwarzania** <u>Zabezpieczenie obiektu i mienia</u> **3. Kategorie odbiorców** Firma ochroniarska, brokerzy ubezpieczeniowi **4. kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. planowane terminy usunięcia poszczególnych kategorii danych** 10-14 dni. Dane są nadpisywane **6. opis technicznych i organizacyjnych środków bezpieczeństwa** Patrz: Instrukcja zarządzania RODO, Regulamin ODO **7. Podstawa prawna przetwarzania**	**1. Informacje (dokumentacja papierowa)** brak **2. Programy i systemy operacyjne** rejestratory **3. Infrastruktura IT** Serwer, wewnętrzna sieć, stacje robocze, kamery, okablowanie **4. Infrastruktura** serwerownia, stanowiska monitoringu **5. Pracownicy i współpracownicy** Dyrektor	System monitoringu składa się z rejestratorów i kamer. Dostęp do rejestratorów i do zapisów posiada dyrektor. Wydawanie zapisów odbywa się na wniosek policji lub ubezpieczyciela.

Art.6, ust 1, lit. f na podstawie prawnie uzasadnionego interesu administratora		
1. Opis kategorii osób (nazwa zbioru) **13 NABÓR I REKRUTACJA DO ŻŁOBKA** **1.a Opis kategorii danych osobowych** Dane kandydatów, rodziców, opiekunów prawnych: dane identyfikacyjne, kontaktowe, oświadczenia o stanie rodziny, stanie zdrowia, dochodach, wyroki sądu rodzinnego, informacja o pieczy zastępczej **2. Cele przetwarzania** Nabór i rekrutacja do żłobka **3. Kategorie odbiorców** Dostawca oprogramowania do zarządzania rekrutacją **4. kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. planowane terminy usunięcia poszczególnych kategorii danych** 1 rok [art. 160 ust. 2 ustawy z 14 grudnia 2016 r. Prawo oświatowe (Dz.U. z 2017 r., poz. 59)] **6. opis technicznych i organizacyjnych środków bezpieczeństwa** Patrz: Instrukcja zarządzania RODO, Regulamin ODO **7. Podstawa prawna przetwarzania** Art.6, ust 1, lit. c - Przepis prawa. Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe (Dz.U. z 2017 r., poz., 59)	**1. Informacje (dokumentacja papierowa)** Wnioski w formie papierowej **2. Programy i systemy operacyjne** Nie dotyczy **3. Infrastruktura IT** nie dotyczy **4. Infrastruktura** Dyrektor **5. Pracownicy i współpracownicy** Księgowość, Referent, Opiekunowie, Pielęgniarka, Kucharka.	1. Przyjęcie wniosków papierowych 2. Przyjęcie wniosków zgłoszonych elektronicznie 3. Wybór dziecka 4. Archiwizacja
1. Opis kategorii osób (nazwa zbioru) **14 WYCHOWANKOWIE** **1.a Opis kategorii danych osobowych** Dane uczniów, rodziców, opiekunów prawnych: dane identyfikacyjne, kontaktowe, oświadczenia o stanie rodziny, stanie zdrowia, dochodach, wyroki sądu rodzinnego, informacja o pieczy zastępczej, data rozpoczęcia i zakończenia pobytu w żłobku, oddział żłobka, ocena umiejętności dziecka, obserwacje rozwojowe, opinie psychologa i pedagoga, umowy (czesne), wpłaty rodziców, ewidencja wychowanków **2. Cele przetwarzania** Świadczenie usługi opiekuńczo-wychowawczej i edukacyjnej **3. Kategorie odbiorców** Ministerstwo Rodziny Pracy i Polityki Społecznej Zakład opieki zdrowotnej (higieniści) **4. kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. planowane terminy usunięcia poszczególnych kategorii danych** 10 lat	**1. Informacje (dokumentacja papierowa)** Dzienniki zajęć, umowy (czesne), ocena umiejętności dziecka i obserwacje rozwojowe dziecka. **2. Programy i systemy operacyjne** Exel, Word **3. Infrastruktura IT** NAS, serwer, dysk sieciowy, firewall, router, stacje robocze, pendrive **4. Infrastruktura** Księgowość, Referenci, sale, gabinet dyrektora **5. Pracownicy i współpracownicy** Opiekunowie , Pielęgniarka, Psycholog, Pedagog, Higienista	1. Założenie ewidencji wychowanków 2. Prowadzenie dziennika zajęć 3. Rozliczanie 4. Archiwizacja

6. opis technicznych i organizacyjnych środków bezpieczeństwa Patrz: Instrukcja zarządzania RODO, Regulamin ODO **7. Podstawa prawna przetwarzania** Art.6, ust 1, lit. c - Przepis prawa: • Ustawa z dnia 7 września 1991 r. o systemie oświaty (Dz. U. 2017, poz. 2198) • Rozporządzenie Ministra Edukacji Narodowej z dnia 29 sierpnia 2014 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z 2014 r. poz. 1170) Art.6, ust 1, lit. a – Zgoda osoby w przypadku publikacji zdjęć uczniów na stronach www szkoły		

Załącznik nr 2 do Polityki Ochrony Danych Osobowych
Umowa powierzenia przetwarzania
danych osobowych

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH
zwana dalej Umową

zawarta w ..... w dniu ..... r. pomiędzy:

XXX z siedzibą w ....., zarejestrowaną/ym w ..... pod numerem ....., posiadającą/ym numer NIP ..... oraz numer REGON ....., reprezentowaną/ym przez: ....., zwaną/ym dalej Zleceniodawcą,

a

YYY z siedzibą w ....., zarejestrowaną/ym w ..... pod numerem ....., posiadającą/ym numer NIP ..... oraz numer REGON ....., reprezentowaną/ym przez: ....., zwaną/ym dalej Zleceniobiorcą

§ 1

Definicje

1. Podmiot przetwarzający – podmiot, któremu powierzono przetwarzanie danych osobowych na mocy umowy powierzenia ze Zleceniodawcą, zwany dalej Zleceniobiorcą.
2. Administrator - organ, jednostka organizacyjna, podmiot lub osoba, decydujące o celach i środkach przetwarzania danych osobowych, zwany także Zleceniodawcą.
3. Zbiór danych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
4. Przetwarzanie danych - 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. Rozporządzenie- 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).
6. Inny podmiot przetwarzający - podmiot, któremu podmiot przetwarzający w imieniu administratora pod-powierzył w całości lub częściowo przetwarzanie danych osobowych.

§ 2

14.1 PRZEDMIOT UMOWY, CEL, CHARAKTER I ZAKRES

1. Przedmiotem umowy jest powierzenie przez Zleceniodawcę danych osobowych do przetwarzania przez Zleceniobiorcę
2. Celem powierzenia jest:
   - świadczenie usług obsługi kadr, płac, księgowości w zakresie danych osobowych pracowników, współpracowników, podwykonawców, kontrahentów
3. Charakter przewarzania danych dotyczy przetwarzania danych osobowych w formie papierowej, przy wykorzystaniu systemów informatycznych (lub systemach monitoringu wizyjnego / głosowego)

§ 3

Czas trwania

1. Zleceniobiorca uprawniony jest do przetwarzania powierzonych danych do dnia wygaśnięcia lub rozwiązania Umowy.
2. W terminie ….. dni od ustania Umowy, Zleceniobiorca zobowiązany jest do usunięcia powierzonych danych, ze wszystkich nośników, programów i aplikacji w tym również kopii, chyba, że obowiązek ich dalszego przetwarzania wynika z odrębnych przepisów prawa.
3. (warunkowo) Zleceniobiorca w terminie ….. dni od ustania Umowy zobowiązany jest do zwrotu powierzonych danych na nośnikach papierowych lub elektronicznych

§4

Obowiązki i prawa

1. Zleceniobiorca zobowiązuje się współpracować ze Zleceniodawcą w zakresie udzielania odpowiedzi na żądania osoby, której dane dotyczą, opisane w rozdziale III Rozporządzenia (w szczególności w zakresie informowania i przejrzystej komunikacji, dostępu do danych, obowiązku informacyjnego, prawa dostępu, prawa do sprostowania danych, usunięcia danych, ograniczenia przetwarzania, przenoszenia danych, prawa sprzeciwu oraz informowania o zautomatyzowanym podejmowaniu decyzji).
2. Zleceniobiorca zobowiązuje się do pomocy Zleceniodawcy w wywiązaniu się z obowiązków określonych w art. 32-36 Rozporządzenia (w szczególności dla bezpieczeństwa przetwarzania, zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu, zawiadamiania osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, przeprowadzania oceny skutków dla ochrony danych osobowych, konsultacji z organem nadzorczym).
3. Zleceniobiorca zobowiązuje się do udostępnienia Zleceniodawcy wszelkich informacji niezbędnych do wykazania spełnienia obowiązków spoczywających na Zleceniobiorcy oraz umożliwi Zleceniodawcy lub audytorowi upoważnionemu przez Zleceniodawcę przeprowadzanie audytów, w tym inspekcji, współpracując przy działaniach sprawdzających i naprawczych.

§5

Zgłaszanie incydentów

1. Zleceniobiorca zobowiązuje się po stwierdzeniu naruszenia ochrony danych osobowych do zgłoszenia tego Zleceniodawcy bez zbędnej zwłoki.
2. Informacja przekazana Zleceniodawcy powinna zawierać co najmniej:
   a) opis charakteru naruszenia oraz - o ile to możliwe - wskazanie kategorii i przybliżonej liczby osób, których dane zostały naruszone i ilości/rodzaju danych, których naruszenie dotyczy,
   b) opis możliwych konsekwencji naruszenia,
   c) opis zastosowanych lub proponowanych do zastosowania przez Zleceniobiorcę środków w celu zaradzenia naruszeniu, w tym minimalizacji jego negatywnych skutków.

§6

Deklarowane środki techniczne i organizacyjne

1. Zleceniobiorca gwarantuje, że każda osoba realizująca Umowę zobowiązana jest do bezterminowego zapewnienia poufności danych osobowych przetwarzanych w związku z wykonywaniem Umowy, a w szczególności do tego, że nie będzie przekazywać, ujawniać i udostępniać tych danych osobom nieuprawnionym. Jednocześnie każda osoba realizująca Umowę zobowiązana jest do zachowania w tajemnicy sposobów zabezpieczenia danych osobowych
2. Zleceniobiorca deklaruje stosowanie środków technicznych i organizacyjnych określonych w art. 32 Rozporządzenia, jako adekwatnych do zidentyfikowanego ryzyka naruszenia praw lub wolności powierzonych danych osobowych a w szczególności:
   a) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
   b) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
3. Zleceniobiorca zobowiązuje się za pomocą odpowiednich środków technicznych lub organizacyjnych stosować ochronę powierzonych danych przed niedozwolonym lub niezgodnym z prawem przetwarzaniem (zniszczeniem, utraceniem, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych) oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.

§6a

Szczegółowe deklarowane środki techniczne i organizacyjne

1. Zleceniobiorca zobowiązuje się dopuszczać do przetwarzania danych osobowych osoby realizujące Umowę (podać ewentualnie funkcje osób, serwisanci, konsultanci, …..) poinformowane i przeszkolone z zasad bezpieczeństwa pracy z danych osobowymi
2. Każda osoba realizująca Umowę zobowiązana jest do przetwarzania danych osobowych do których uzyskała dostęp wyłącznie w zakresie i celu przewidzianym w Umowie.
3. Każda osoba realizująca Umowę zobowiązana jest do zapewnienia poufności danych osobowych przetwarzanych w związku z wykonywaniem Umowy a w szczególności do tego, że nie będzie przekazywać, ujawniać i udostępniać tych danych osobom nieuprawnionym.
4. Każda osoba realizująca Umowę zobowiązuje się do zachowania w tajemnicy sposobów zabezpieczenia danych osobowych o ile nie są one jawne.
5. Każda osoba realizująca Umowę zobowiązana jest do nie powodowania niezgodnych z Umową zmian danych lub utraty, uszkodzenia lub zniszczenia tych danych.
6. Każda osoba realizująca Umowę zobowiązuje się do niedokonywania jakiegokolwiek kopiowania i utrwalania danych osobowych poza systemami informatycznymi Zleceniodawcy
7. W przypadku wykorzystania sieci publicznej, każda osoba realizująca Umowę zobowiązuje się do stosowania zabezpieczonego przed podsłuchem połączenia zdalnego (VPN, SSL, podać inne).
8. Każda osoba realizująca Umowę zobowiązuje się do pracy w systemach Zleceniodawcy z użyciem uwierzytelnienia.

§7

Postanowienia końcowe

1. Umowa zastępuje wszelkie inne ustalenia dokonane pomiędzy Zleceniobiorcą a Zleceniodawcą dotyczące przetwarzania danych osobowych bez względu na to, czy zostały uregulowane umową czy innym instrumentem prawnym.
2. W zakresie nieuregulowanym Umową mają zastosowanie przepisy prawa obowiązującego na terenie Rzeczypospolitej Polskiej, w tym Rozporządzenia.
3. Wszelkie zmiany Umowy wymagają formy pisemnej pod rygorem nieważności.
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

....

Załącznik nr 3 do Polityki Ochrony Danych Osobowych

Arkusz Analizy ryzyka RODO

……

Załącznik nr 4 do Polityki Ochrony Danych Osobowych
Upoważnienie do przetwarzania
danych osobowych

....., dn. ..... 20..... r.

UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (Dz.Urz. UE L 119, s. 1) – dalej **RODO** – nadaję upoważnienie Pani/Panu:

…….

(imię i nazwisko)

……..

(stanowisko)

do przetwarzania danych osobowych w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku.
Upoważnienie obejmuje uprawnienie do przetwarzania danych: zbiory, do których dostęp wymagany jest, aby realizować obowiązki służbowe.
Jednocześnie zobowiązuję Panią/Pana do przetwarzania danych osobowych, zgodnie z udzielonym upoważnieniem oraz z przepisami RODO, innymi aktami prawnymi a także z Polityką ochrony danych osobowych.
Jednocześnie upoważniam Panią/Pana do posiadania dla potrzeb wykonywanej pracy zestawień, ewidencji oraz rejestrów z danymi osobowymi, z zachowaniem pełnej ich ochrony przy zastosowaniu środków technicznych i organizacyjnych wdrożonych w Żłobku Miejskim w Lubawie „Akademia Maluszka”.
Okres ważności

od: …….

do: wygaśnięcie stosunku pracy

…….
podpis osoby uprawnionej do nadania
upoważnienia

Data wygaśnięcia* ……..……..

Odwołano, dnia …….

.....
podpis osoby uprawnionej do odwołania upoważnienia

* Data rozwiązania stosunku pracy/umowy cywilnoprawnej

***Załącznik nr 5* do Polityki Ochrony Danych Osobowych**
Regulamin Ochrony Danych Osobowych

Regulamin
Ochrony Danych Osobowych
w Żłobku Miejskim w Lubawie
„Akademia Maluszka”

Niniejszy regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych zgodnie z przepisami RODO dla:

- Pracowników
- Współpracowników
- Pracowników podmiotów trzecich, posiadających dostęp do danych osobowych przetwarzanych przez Administratora
- Użytkowników systemów informatycznych z dostępem do danych osobowych przetwarzanych przez Administratora

Każda z w/w osób powinna zapoznać się z poniższym regulaminem oraz zobowiązać się do stosowania zasad w nim zawartych

SPIS TREŚCI

1 Zasady bezpiecznego użytkowania sprzętu IT, dysków, programów 23

2 Zarządzanie uprawnieniami - procedura rozpoczęcia, zawieszenia i zakończenia pracy . 23

3 Polityka haseł 24

4 Zabezpieczenie dokumentacji papierowej z danymi osobowymi 24

5 Zasady wynoszenia nośników z danymi poza firmę/organizację 24

6 Zasady korzystania z internetu 25

7 Zasady korzystania z poczty elektronicznej 25

8 Ochrona antywirusowa 26

9 Skrócona instrukcja postępowania w przypadku naruszenia ochrony danych osobowych 26

10 Obowiązek zachowania poufności i ochrony danych osobowych 27

11 Postępowanie dyscyplinarne 28

1. ZASADY BEZPIECZNEGO UŻYTKOWANIA SPRZĘTU IT, DYSKÓW, PROGRAMÓW

1. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT zobowiązany jest do jego zabezpieczenia przed zniszczeniem lub uszkodzeniem. Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, służbowe tablety i smartfony.
2. Użytkownik jest zobowiązany zgłosić zagubienie, utratę lub zniszczenie powierzonego mu Sprzętu IT.
3. Samowolne instalowanie otwieranie (demontaż) Sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) do lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.
4. Użytkownik jest zobowiązany do usuwania plików z nośników/dysków do których mają dostęp inni użytkownicy nieupoważnieni do dostępu do takich plików (np. podczas współużytkowania komputerów).
5. Użytkownik jest zobowiązany do przekazania informatykowi nośników przeznaczonych do zniszczenia.
6. Użytkownicy komputerów przenośnych na których znajdują się dane osobowe lub z dostępem do danych osobowych przez Internet zobowiązani są do stosowania zasad bezpieczeństwa zawartych w Regulaminie użytkowania komputerów przenośnych.

2. ZARZĄDZANIE UPRAWNIENIAMI - PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

1. Każdy użytkownik musi posiadać swój własny indywidualny identyfikator (login) do logowania się.
2. Tworzenie kont użytkowników wraz z uprawnieniami odbywa się na polecenie przełożonych, a wykonywane przez informatyków-administratorów.
3. Użytkownik nie może samodzielnie zmieniać swoich uprawnień (np. zostać administratorem Windows na swoim komputerze).
4. Każdy użytkownik musi posiadać indywidualny identyfikator. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika.
5. Zabrania się pracy wielu użytkowników na wspólnym koncie.
6. Użytkownik rozpoczyna pracę z użyciem identyfikatora i hasła.
7. Użytkownik jest zobowiązany do powiadomienia informatyków-administratorów o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.

3. W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym informatyków-administratorów.
4. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów) wglądu do danych wyświetlanych na monitorach.
5. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu bądź z programu.
6. Zabrania się uruchamiania jakiejkolwiek aplikacji lub programu na prośbę innej osoby, o ile nie została ona zweryfikowana jako pracownik działu informatyki. Dotyczy to zwłaszcza programów przesłanych za pomocą poczty elektronicznej lub wskazanych w formie odnośnika internetowego.
7. Po zakończeniu pracy, użytkownik zobowiązany jest:
   a) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy
   b) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki elektroniczne, magnetyczne i optyczne, na których znajdują się dane osobowe.

3. POLITYKA HASEŁ

1. Hasła powinny składać się z co najmniej 8 znaków.
2. Hasła powinny zawierać duże litery + małe litery + cyfry (lub znaki specjalne).
3. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów, typowych zestawów: 123456, qwerty.
4. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie.
5. W przypadku ujawnienia hasła – należy natychmiast go zmienić.
6. Hasła muszą być zmieniane co 90 dni.
7. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła.
8. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło.
9. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
10. Zabrania się używania w serwisach internetowych takich samych lub podobnych haseł jak w systemie komputerowym organizacji.
11. Zabrania się stosowania tego samego hasła jako zabezpieczenia w dostępie do różnych systemów.
12. Zabrania się definiowania haseł, w których jeden człon pozostaje niezmienny, a drugi zmienia się według przewidywalnego wzorca (np. Anna001, Anna002, Anna003 itd.). Nie powinno się też stosować haseł, w których któryś z członów stanowi imię, nazwę lub numer miesiąca lub inny możliwy do odgadnięcia klucz.

4. ZABEZPIECZENIE DOKUMENTACJI PAPIEROWEJ Z DANYMI OSOBOWYMI

1. Upoważnieni pracownicy są zobowiązani do stosowania tzw. „**Polityki czystego biurka**". Polega ona na zabezpieczaniu (zamykaniu) dokumentów oraz nośników np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.
2. Upoważnieni pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach lub utylizacji ich w specjalnych bezpiecznych pojemnikach z przeznaczeniem do bezpiecznej utylizacji.
3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych.
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, np., na terenach publicznych miejskich lub w lesie.

5. ZASADY WYNOSZENIA NOŚNIKÓW Z DANYMI POZA FIRMĘ/ORGANIZACJĘ

1. Użytkownicy nie mogą wynosić na zewnątrz organizacji wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Pracodawcy / Zleceniodawcy. Do takich nośników zalicz się: wymienne twarde dyski, pen-drive, płyty CD, DVD, pamięci typu Flash.
2. Dane osobowe wynoszone poza organizację muszą być zaszyfrowane (szyfrowane dyski, zahasłowane pliki).
3. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w plecakach, teczkach.
4. Należy korzystać ze sprawdzonych firm kurierskich.
5. W przypadku, gdy dokumenty przewozi pracownik, zobowiązany jest do zabezpieczenia przewożonych dokumentów przed zagubieniem i kradzieżą.
6. Zabrania się wynoszenia poza obszar organizacji wymiennych nośników informacji a w szczególności twardych dysków z zapisanymi danymi osobowymi i pendrive bez zgody ADO.
7. Dane osobowe wynoszone poza obszar dokumentacji na nośnikach elektronicznych muszą być zaszyfrowane .

8. W sytuacji przekazywania nośników z danymi osobowymi poza obszar organizacji można stosować następujące zasady bezpieczeństwa:
    a. adresat powinien zostać powiadomiony o przesyłce
    b. dane przed wysłaniem powinny zostać zaszyfrowane a hasło podane adresatowi inną drogą
    c. stosować bezpieczne koperty depozytowe
    d. przesyłkę należy przesyłać przez kuriera

6. ZASADY KORZYSTANIA Z INTERNETU

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT (np. ASI) i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).
5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą ”https:”. Dla pewności należy „kliknąć” na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.
7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.
8. Zabrania się samowolnego podłączania do komputerów modemów, telefonów komórkowych i innych urządzeń dostępowych (np.: typu BlueConnect, iPlus, OrangeGo). Zabronione jest też łączenie się przy pomocy takich urządzeń z Internetem w chwili, gdy komputer użytkownika podłączony jest do sieci.

7. ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. Przesyłanie danych osobowych z użyciem maila poza organizację może odbywać się tylko przez osoby do tego upoważnione.
2. W przypadku przesyłania danych osobowych poza organizację należy wysyłać pliki zaszyfrowane/spakowane (np. programem 7 zip, winzipem, winrarem) i zahasłowane, gdzie hasło powinno być przesłane do odbiorcy telefonicznie lub SMS.
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 12 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
6. **WAŻNE:** Nie otwierać załączników (.zip, .xlsm, .pdf, .exe) w mailach!!!!! Są to zwykle „wirusy”, które infekują komputer oraz często pozostałe komputery w sieci.
7. **WAŻNE:** Nie wolno „klikać” na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron z „wirusami”. Użytkownik „klikając” na taki hiperlink infekuje komputer oraz inne komputery w sieci.
8. Należy zgłaszać informatykowi przypadki podejrzanych emaili .

9. Użytkownicy nie powinni rozsyłać „niezawodowych” emaili w formie „łańcuszków szczęścia", np. Życzenia Świąteczne adresowane do 230 osób.
10. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW”. Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości”!
11. Użytkownicy powinni okresowo kasować niepotrzebne maile.
12. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.
13. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.
14. Użytkownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
15. Zabrania się użytkownikom poczty elektronicznej konfigurowania swoich kont pocztowych do automatycznego przekierowywania wiadomości na adres zewnętrzny.
16. Korzystanie z maila dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych.
17. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.
18. Użytkownik bez zgody Pracodawcy / Zleceniodawcy nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Pracodawcy / Zleceniodawcy, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

8. OCHRONA ANTYWIRUSOWA

1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym, jeśli system antywirusowy taką funkcje posiada.
2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.
3. W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów „np.; Twój system jest zainfekowany!, zainstaluj program antywirusowy”, użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Informatyka lub osobę upoważnioną.

9. SKRÓCONA INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia Pracodawcy / Zleceniodawcy w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
2. Do sytuacji wymagających powiadomienia, należą:
   a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
   b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
   c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
3. Do incydentów wymagających powiadomienia, należą:
   a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
   b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych),

c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania),

4. Typowe przykłady incydentów wymagające reakcji:
   a. ślady na drzwiach, oknach i szafach wskazują na próbę włamania,
   b. dokumentacja jest niszczona bez użycia niszczarki,
   c. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie,
   d. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,
   e. ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe,
   f. wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez upoważnienia Pracodawcy / Zleceniodawcy,
   g. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej,
   h. telefoniczne próby wyłudzenia danych osobowych,
   i. kradzież, zagubienie komputerów lub CD, twardych dysków, Pen-drive z danymi osobowymi,
   j. maile zachęcające do ujawnienia identyfikatora i/lub hasła,
   k. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
   l. hasła do systemów przyklejone są w pobliżu komputera.

10. OBOWIĄZEK ZACHOWANIA POUFNOŚCI I OCHRONY DANYCH OSOBOWYCH

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
   a. przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Pracodawcę / Zleceniodawcę zadaniach,
   b. zachowania w tajemnicy danych osobowych do których ma dostęp w związku z wykonywaniem zadań powierzonych przez Pracodawcę / Zleceniodawcę,
   c. niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Pracodawcę / Zleceniodawcę,
   d. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
   e. ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem,
2. Jeśli jest to przewidziane, osoba dopuszczona do przetwarzania odbywa szkolenie z zasad ochrony danych osobowych.
3. Osoby zapoznane z treścią niniejszego Regulaminu ODO lub przeszkolone zobowiązane są podpisać Oświadczenie o poufności.
4. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego.
5. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.
6. Zabrania się ujawniania na grupach dyskusyjnych, forach internetowych, blogach itp. jakichkolwiek szczegółów dotyczących funkcjonowania organizacji, w tym informacji na temat sprzętu i oprogramowania, z jakiego korzysta organizacja, oraz informacji kontaktowych innych, niż ogólnodostępne w materiałach zewnętrznych.

11. POSTĘPOWANIE DYSCYPLINARNE

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez Pracodawcę / Zleceniodawcę za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r.

Załącznik nr 6 do Polityki Ochrony Danych Osobowych
Oświadczenie o ufności

……...
……

(imię i nazwisko) *(miejscowość)*

OŚWIADCZENIE O POUFNOŚCI

Oświadczam, iż zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, w szczególności ogólnego Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r. oraz odnośnymi wymaganiami "Regulaminu Ochrony Danych Osobowych".

W szczególności zobowiązuję się do:

- przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora zadaniach
- zachowania w tajemnicy danych osobowych do których mam lub będę mieć dostęp w związku z wykonywaniem zadań powierzonych przez Administratora
- niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Administratora
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych
- ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez Administratora za naruszenie przepisów Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r.

…….

Data i podpis
oświadczającego

Załącznik nr 2 *do Zarządzenia Nr 8/2017/2018 Dyrektora Żłobka Miejskiego w Lubawie „Akademia Maluszka" z dnia 21.05.2018r. .* – Instrukcję zarządzania RODO –wykaz zabezpieczeń RODO

Instrukcja zarządzania RODO – wykaz zabezpieczeń RODO

w Żłobku Miejskim w Lubawie

„Akademia Maluszka"

1. Wstęp 32
2. Zabezpieczenia fizyczne 32
3. Zabezpieczenia techniczne 32
4. Procedura nadawania uprawnień do przetwarzania danych osobowych. 32
5. Metody i środki uwierzytelnienia (polityka haseł) 33
6. Procedura tworzenia kopii zapasowych 33
7. Utylizacja elektronicznych nośników i wydruków oraz czyszczenie danych 33
8. Procedura zabezpieczenia systemu informatycznego 33
8.1. Bezpieczeństwo przetwarzania danych poza organizacją 33
8.2. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej 34
9. Procedura wykonywania przeglądów i konserwacji 34

1. WSTĘP

Instrukcja stanowi wykaz procedur oraz stosowanych środków technicznych i organizacyjnych mających na celu, zgodnie z Art. 32 RODO, zabezpieczyć przetwarzane dane osobowe przed: przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych oraz nieuprawnionym dostępem do danych osobowych

2. ZABEZPIECZENIA FIZYCZNE

1. zabezpieczono dostęp do kluczowej infrastruktury w postaci budynków / pomieszczeń biurowych, archiwów, serwerowni, miejsc przechowywania kopii bezpieczeństwa
2. rozmieszczenie komputerów i drukarek ogranicza dostęp osób nieupoważnionych
3. rozdzielnie elektryczne zabezpieczono w szafach zamykanych na klucz
4. dostęp do pomieszczeń (w tym biurowych) zabezpieczono drzwiami zamykanymi na klucz
5. dostęp do archiwum zabezpieczono drzwiami zamykanymi na klucz
6. dokumentację / dane na nośnikach zabezpieczono w zamkniętych na klucz niemetalowych szafach

3. ZABEZPIECZENIA TECHNICZNE

1. zastosowano UPS na kluczowych elementów systemu IT
2. zastosowano monitoring wizyjny w obrębie obiektu i w otoczeniu

4. PROCEDURA NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH.

Celem procedury jest minimalizacja ryzyka przetwarzania danych przez osoby nieupoważnione.

1. Dostęp do systemu informatycznego (np. stacji roboczej, dysku sieciowego, programu lub aplikacji, poczty elektronicznej) nadawany jest każdemu użytkownikowi w formie indywidualnego identyfikatora (loginu)
2. Każdemu użytkownikowi uprzywilejowanemu (administratorowi) nadawane jest indywidualne konto administracyjne
3. Nadawanie, zmiana, odbieranie uprawnień użytkownika do zasobów i aplikacji odbywa się na polecenie przełożonych (lub innych osób upoważnionych)
4. Za wykonanie czynności nadawania, zmiany, odbierania uprawnień użytkownikowi odpowiada administrator
5. Użytkowników obowiązuje zasada pracy na własnym koncie. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika. Zasada ta obowiązuje również administratorów systemów
6. W przypadku pracy z uprawnieniami użytkownika uprzywilejowanego, każdy Administrator systemu zobowiązany jest do bieżącej pracy na koncie roboczym. Użycie tzw. konta administracyjnego (np. "root" lub "admin") dopuszczalne jest jedynie w sytuacjach awaryjnych lub podczas poważnych zmian wprowadzanych w administrowanym systemie

5. METODY I ŚRODKI UWIERZYTELNIENIA (POLITYKA HASEŁ)

Celem procedury jest zapewnienie, że do systemów informatycznych przetwarzających dane osobowe mają dostęp jedynie osoby do tego upoważnione.

1. Pierwsze (pierwotne) hasło użytkownika nadawane jest przez administratora i przekazywane mu w poufny sposób
2. Standard hasła: 8 –znakowe, zmieniane co 90 dni. Użytkownicy są zobowiązani do samodzielnej zmiany hasła
3. Administrator nie ma dostępu do haseł użytkowników
4. W sytuacji zapomnienia przez użytkownika swojego hasła, administrator przywraca hasło do ustawień początkowych i przekazuje go użytkownikowi celem niezwłocznej późniejszej zmiany
5. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp

6. PROCEDURA TWORZENIA KOPII ZAPASOWYCH

1. Kopie całościowe sporządzane są raz w miesiącu
2. Przechowywanych jest 6 kopii miesięcznych przez okres roku. Najstarsze kopie są nadpisywane w cyklu rotacyjnym
3. Kopie sporządzane są na pamięci USB
4. Dysk przenośny przechowywany jest w szafie zamykanej na klucz
5. Dostęp do dysku przenośnego mają: Dyrektor.

7. UTYLIZACJA ELEKTRONICZNYCH NOŚNIKÓW I WYDRUKÓW ORAZ CZYSZCZENIE DANYCH

1. Podlegające likwidacji uszkodzone lub przestarzałe nośniki a szczególności twarde dyski z danymi osobowymi ze stacji roboczych i laptopów / pendrive / pamięci flash / dyski SSD / płyty DVD są niszczone w sposób fizyczny w tym również komisyjnie w/g Załącznika Protokół zniszczenia uszkodzonych nośników. Stosowana metoda niszczenia, to fizyczne niszczenie (pocięcie, nawiercenie, młotkowanie) wymontowanych nośników / użycie degaussera / zmielenie w specjalistycznej firmie potwierdzone protokołem zniszczenia lub certyfikatem bezpieczeństwa firmy utylizacyjnej lub nagraniem z procesu transportu i utylizacji
2. Nośniki informacji zamontowane w sprzęcie IT a w szczególności twarde dyski muszą być wyczyszczone specjalistycznym oprogramowaniem zanim zostaną przekazane poza obszar organizacji (np. sprzedaż lub darowizna komputerów stacjonarnych / laptopów / smartfonów)
3. Dokumentacja papierowa niszczona jest w niszczarkach paskowych oraz tam, gdzie to wymagane w niszczarkach o podwyższonym standardzie

8. PROCEDURA ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO

8.1. Bezpieczeństwo przetwarzania danych poza organizacją

1. Użytkownicy komputerów przenośnych wynoszonych poza obszar organizacji, na których są przetwarzane dane osobowe są zobowiązani do przestrzegania zasad bezpieczeństwa
2. Stosuje się szyfrowanie dysków komputerów przenośnych zawierających dane osobowe, jeśli wynoszone są poza obszar organizacji
3. Dane osobowe na komputerach przenośnych wynoszonych poza obszar organizacji muszą być przechowywane na zaszyfrowanych partycjach
4. Dyski przenośne / pendrive wynoszone poza organizację muszą być zaszyfrowane
5. Sprzęt mobilny (smartfony/tablety) zabezpieczono mechanizmem uwierzytelniania

6. W przypadku użycia komputerów przenośnych lub sprzętu mobilnego do zdalnego dostępu do zasobów wewnętrznej sieci przez Internet, stosuje się szyfrowanie tego połączenia z użyciem VPN (np. przez Informatyka / Księgową)

8.2. OCHRONA PRZED NIEAUTORYZOWANYM DOSTĘPEM DO SIECI LOKALNEJ

Stosowane zabezpieczenia mają na celu zabezpieczenie systemów informatycznych przed nieautoryzowanym dostępem do sieci lokalnej np. przez programy szpiegujące, hackerów

1. Dokonuje się aktualizacji oprogramowania (firmware / sterowniki) urządzeń sieciowych
2. Dokonuje się konfiguracji urządzeń sieciowych oraz innych (routery, switche, access pointy, firewalle, macierze, dyski NAS, drukarki, skanery) w celu zabezpieczenia przed nieuprawnionym dostępem do nich (np. zmiana domyślnych haseł na urządzeniach, zmiana domyślnych nazw kont administratora w urządzeniach, konfiguracja portów na routerze)
3. Dokonuje się aktualizacji oprogramowania systemów i aplikacji. Aktualizacja dokonywana jest zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji (np. aktualizacje, service pack-i, łatki)
4. Zastosowano system antywirusowy na stacjach roboczych
5. Sieć bezprzewodową technologią WPA

9. PROCEDURA WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI

1. Administrator odpowiada za sprawdzanie poprawności działania systemu IT, w tym: stacji roboczych, serwerów, drukarek, baz danych, aplikacji, poczty email
2. Administrator odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia
3. W przypadku napraw dokonywanych na zewnątrz z komputerów należy uprzednio wymontować dyski i wszelkie nośniki
4. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest zawarcie specjalnego zapisu w umowie serwisowej, gwarantującego bezpieczną naprawę (należy na to zwrócić uwagę przy zakupach sprzętu)

5. Czynności konserwacyjne i naprawcze wykonywane przez osoby nieposiadające upoważnień do przetwarzania danych (np. specjalistów z firm zewnętrznych) muszą być wykonywane pod nadzorem osób upoważnionych
6. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych

Załącznik - Protokół zniszczenia uszkodzonych nośników komputerowych

.... dnia .....r.

(akcept powołującego komisję)

Protokół nr .....

zniszczenia uszkodzonych nośników komputerowych

.....

(jednostka, komórka organizacyjna XXX)

Dnia ..... komisja powołana przez .....

(data) (imię, nazwisko i stanowisko osoby powołującej komisję)

w składzie:

1. Przewodniczący: .....
2. Członkowie: .....
   .....

dokonała trwałego zniszczenia nośników komputerowych:

L.p.	Nazwa	Nr ewidencyjny	Sposób zniszczenia	Uwagi

Dokonanie w/w czynności zostaje potwierdzone własnoręcznymi podpisami komisji:

.....

.....

.....

ADMINISTRATOR SYSTEMU

.....