POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH w

Niepubliczna Placówka Oświatowa Monika Ferenszkiewicz

NIP 6692484430

Obowiązuje od 2018.05.25

I. POSTANOWIENIA OGÓLNE

Celem Polityki Bezpieczeństwa przetwarzania danych osobowych, zwanej dalej Polityką Bezpieczeństwa, jest określenie kierunków działań oraz wsparcia dla zapewnienia bezpieczeństwa przetwarzania zbiorów danych osobowych zarządzanych przez:

Niepubliczna Placówka Oświatowa Monika Ferenszkiewicz zwaną dalej Niepubliczna Placówka Oświatowa lub Firma

NIP 6692484430 reprezentowana przez Monika Ferenszkiewicz

Polityka Bezpieczeństwa ma charakter nadrzędny w stosunku do innych wewnętrznych aktów dotyczących bezpieczeństwa danych osobowych. Ma ona zastosowanie w stosunku do wszystkich pracowników, osób zatrudnionych na innej podstawie niż umowa o pracę, zleceniobiorców, wykonawców, konsultantów, praktykantów, stażystów i innych pracowników, którzy wykonują powierzane im zadania związane z przetwarzaniem danych osobowych.

NIEPUBLICZNA PLACÓWKA OŚWIATOWA zarządza bezpieczeństwem danych osobowych w celu zapewnienia sprawnego i zgodnego z przepisami prawa, wykonywania

swoich zadań oraz zadań wykonywanych na podstawie umów lub powierzonych do wykonania na podstawie porozumień.

Polityka Bezpieczeństwa jest zgodna z obowiązującymi przepisami prawa, w szczególności z rozporządzeniem Parlamentu Europejskiego i Rady 2016/679 z dnia 27 kwietnia 2016 , o ochronie danych osobowych z późniejszymi zmianami oraz z wydanymi na jej podstawie aktami wykonawczymi.

Utrzymanie bezpieczeństwa przetwarzanych przez **NIEPUBLICZNA PLACÓWKA OŚWIATOWA** informacji, rozumiane jest jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z zasobem stanowiącym przedmiot niniejszej Polityki. Poniżej opisane jest rozumienie wyżej wymienionych pojęć w odniesieniu do informacji i aplikacji:

1) poufność informacji – właściwość polegająca na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesorom,

2 integralność informacji – rozumiana jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania,

3) dostępność informacji – rozumiane jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,

4) zarządzanie ryzykiem – rozumiane jako skoordynowane działania kierowania i zarządzania organizacją w procesie identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych.

Dodatkowo zarządzanie bezpieczeństwem informacji wiąże się z zapewnieniem:

1) niezaprzeczalności odbioru – rozumianej jako zdolność systemu do udowodnienia, że adresat informacji otrzymał ją w określonym miejscu i czasie,

2) niezaprzeczalności nadania – rozumianej jako zdolność systemu do udowodnienia, że nadawca informacji faktycznie ją nadał lub wprowadził do systemu w określonym miejscu i czasie,

3) rozliczalności działań – rozumianej, jako zapewnienie, że wszystkie działania istotne dla przetwarzania informacji zostały zarejestrowane w systemie i możliwym jest zidentyfikowanie użytkownika, który działania dokonał.

Określenia użyte w Polityce Bezpieczeństwa oznaczają:

1)komórka organizacyjna – samodzielne stanowiska w Firmie.

2) dane osobowe – oznaczają 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.

3) przetwarzanie danych osobowych – 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;

4) użytkownik – osoba upoważniona do przetwarzania danych osobowych,

5) administrator systemu informatycznego (ASI) – osoba upoważniona do zarządzania systemem informatycznym,

6) system informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur

przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,

7) zabezpieczenie systemu informatycznego – należy przez to rozumieć wdrożenie stosowanych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych a także ich utratą.

II. ZAKRES

Zakres przedmiotowy stosowania niniejszej Polityki Bezpieczeństwa obejmuje wszystkie zbiory danych osobowych przetwarzane w **NIEPUBLICZNA PLACÓWKA OŚWIATOWA**, zarówno w formie elektronicznej, jak i tradycyjnej.

W zakresie podmiotowym Polityka Bezpieczeństwa obowiązuje wszystkich pracowników **NIEPUBLICZNA PLACÓWKA OŚWIATOWA** oraz inne osoby mające dostęp do danych osobowych, w tym stażystów, osoby zatrudnione na umowę zlecenia lub umowę o dzieło itp.

III. STRUKTURA DOKUMENTÓW POLITYKI BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

Dokumenty Polityki Bezpieczeństwa ustanawiają metody zarządzania oraz wymagania niezbędne do zapewnienia skutecznej i spójnej ochrony przetwarzanych informacji.

Zestaw dokumentów Polityki Bezpieczeństwa składa się z:

Polityki Bezpieczeństwa wraz z załącznikami:

Załącznik nr 1 – „Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe”;

Załącznik nr 2 – „Wykaz zbiorów danych osobowych”;

Załącznik nr 3 – „Rejestr czynności przetwarzania”;

Załącznik nr 4 – „Umowa powierzenia danych osobowych”;

Załącznik nr 5 - „Wzór raportu o naruszeniu zasad”;

Załącznik nr 6 - „Schemat postępowania w przypadku naruszenia ochrony danych;

Załącznik nr 7 - „Oświadczenie o przestrzeganiu zasad i przepisów ochrony danych osobowych”;

Załącznik nr 8 – „Wykaz pracowników – zapoznanych z polityką bezpieczeństwa”;

Załącznik nr 9 – „Wzór klauzuli informacyjnej”;

Załącznik nr 10 – „Wzór klauzuli zgodności”;

Załącznik nr 11 – „Wzór upoważnienia imiennego”;

IV. DOSTĘP DO INFORMACJI

1. Wszystkie osoby, których rodzaj wykonywanej pracy będzie wiązał się z dostępem do danych osobowych, przed przystąpieniem do pracy, podlegają przeszkoleniu w zakresie obowiązujących przepisów prawa dotyczących ochrony danych osobowych oraz obowiązujących w **NIEPUBLICZNA PLACÓWKA OŚWIATOWA** zasad ochrony danych osobowych wynikających z Polityki Bezpieczeństwa.
2. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora Danych Osobowych: Aleksandra Domblat
3. Wszystkie osoby dopuszczone do przetwarzania danych muszą zostać wpisane do ewidencji osób dopuszczonych do przetwarzania danych osobowych prowadzonej przez Administratora.
4. Wszystkie osoby, przed dopuszczeniem do przetwarzania danych, muszą otrzymać upoważnienie wskazujące zakres działań przy przetwarzaniu danych, do którego będą uprawnione.
5. Wszystkie osoby dopuszczone do przetwarzania danych zobowiązane są do zapoznania się z treścią przeznaczonych dla nich dokumentów zawierających zasady bezpieczeństwa przetwarzania.
6. Wszystkie osoby dopuszczone do przetwarzania danych podpisują oświadczenie o :

1) znajomości obowiązujących przepisów prawa, Polityki Bezpieczeństwa, oraz innych aktów dotyczących bezpieczeństwa i ochrony informacji obowiązujących w Firmie, i zobowiązaniu się do przestrzegania i stosowania przepisów ww. aktów.

2) zachowaniu tajemnicy treści danych i sposobów ich zabezpieczenia podczas zatrudnienia po jego ustaniu.

7. Zakres czynności dla osoby dopuszczonej do przetwarzania danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę danych osobowych

w stopniu odpowiednim do zadań tej osoby realizowanych przy przetwarzaniu tych danych.

8. Udostępnianie danych osobowych podmiotom upoważnionym do ich otrzymania, na podstawie przepisów prawa, powinno odbywać się wg określonych odrębnymi przepisami procedur postępowania.
9. Prawo do sprostowania danych – przysługuje osobie, której dane dotyczą. Z uwzględnieniem celów przetwarzania. Osoba której dane dotyczą ma prawo żądania, uzupełnienia niekompletnych danych osobowych. W zależności od rodzaju przechowywania danych prawo to jest realizowane poprzez odpowiednią procedurę.
10. Prawo do usunięcia danych – osoba której dane dotyczą ma prawo żądać niezwłocznego usunięcia jej danych osobowych. W zależności od procesu przetwarzania danych osobowych rozwiązania realizujące to prawo zostały w nich opisane.

V. ZARZĄDZANIE DANYMI OSOBOWYMI

Za bezpieczeństwo danych osobowych odpowiadają:

1)Administrator Danych Osobowych – Aleksandra Domblat

2)Inspektor Ochrony Danych Osobowych (IODO) –
……

3)Administrator Systemu Informatycznego (ASI) – MH Kamyk, Łańcucki Spółka Jawna nip: 6692518927, kontakt biuro@mh-informatyka.pl tel 668801391

4)Pracownicy NIEPUBLICZNA PLACÓWKA OŚWIATOWA

Administrator realizując Politykę Bezpieczeństwa ma prawo określać procedury i wydawać instrukcje regulujące kwestie ochrony danych osobowych w Firmie.

W umowach zawieranych przez **NIEPUBLICZNA PLACÓWKA OŚWIATOWA** winny znajdować się postanowienia zobowiązujące podmioty zewnętrzne do ochrony danych udostępnionych przez Firmę.

Obowiązki wynikające z ustawy o ochronie danych osobowych powierza się Inspektorowi Ochrony Danych Osobowych w zakresie podległych im pracowników, którzy odpowiadają za przestrzeganie obowiązujących przepisów prawa, obowiązkiem współdziałania z Administratorem w zakresie swoich właściwości. Kierownicy komórek organizacyjnych **NIEPUBLICZNA PLACÓWKA OŚWIATOWA** zobowiązani są do zapoznania podległych pracowników z treścią Rozporządzenia Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r., Polityką Bezpieczeństwa w zakresie przetwarzania danych osobowych, Instrukcją zarządzania systemem informatycznym, służącymi do przetwarzania danych osobowych oraz Instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych.

Zapoznanie się z dokumentami określonymi powyżej, pracownicy Firmy potwierdzają podpisem na „Oświadczeniu", którego wzór stanowi załącznik 7 do Polityki Bezpieczeństwa i przekazują Administratorowi.

Ochrona zasobów danych osobowych Firmy jako całości przed ich nieuprawnionym użyciem lub zniszczeniem jest jednym z podstawowych obowiązków pracowników.

VI. ZAKRESY ODPOWIEDZIALNOŚCI

Administrator Danych Osobowych.

1) Odpowiada za przestrzeganie ustawy o ochronie danych osobowych w zakresie dotyczącym Administratora Bezpieczeństwa Informacji;

2) W razie zmiany obowiązujących przepisów prawa powodujących niezgodność niniejszego dokumentu z nimi, dostosowuje **Politykę Bezpieczeństwa** do obowiązujących przepisów;

3) Sprawuje nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których dane są przetwarzane oraz kontrolą przebywających w nich osób;

4) Określa strategię zabezpieczania systemów informatycznych;

5) Sprawuje nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych;

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

7) Odpowiada za instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego;

8) Sprawuje nadzór nad bezpieczeństwem danych zawartych w komputerach przenośnych, dyskach wymiennych, pamięciach przenośnych i innych nośnikach, w których przetwarzane są dane osobowe;

9)Monitoruje działanie zabezpieczeń wdrożonych w celu ochrony danych osobowych w systemach informatycznych;

10) Sprawuje nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane oraz kontrolą dostępu do danych;

11) Zatwierdza wniosek kierownika komórki organizacyjnej o przyznaniu danemu użytkownikowi identyfikatora oraz prawa dostępu do informacji chronionych w danym systemie przetwarzania;

12) Prowadzi ewidencję baz danych w systemach informatycznych, w których przetwarzane są dane osobowe;

13) Prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych;

14) Prowadzi ewidencję miejsc przetwarzania danych osobowych w systemach informatycznych;

15) Prowadzi rejestr zbiorów danych osobowych Firmy (przetwarzanych metodą tradycyjną lub w systemach informatycznych);

16) Prowadzi profilaktykę antywirusową;

Inspektor Ochrony Danych Osobowych

1) Określają indywidualne obowiązki i odpowiedzialność osób zatrudnionych przy przetwarzaniu danych osobowych;

2) Zapoznają osoby zatrudnione przy przetwarzaniu danych osobowych z przepisami obowiązującymi w tym zakresie;

3) Wdrażają i nadzorują przestrzeganie **„Polityki Bezpieczeństwa";**

4) Wdrażają i nadzorują przestrzeganie **„Instrukcji Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych**";

5) Działają zgodnie z **„Instrukcją Postępowania w Sytuacji Naruszenia Ochrony Danych Osobowych";**

6) Określają, które osoby i na jakich prawach mają dostęp do danych informacji;

7) Powiadamia Administratora Systemu Informatycznego o konieczności utworzenia identyfikatora użytkownika w systemie oraz zmianie lub nadaniu uprawnień dostępu użytkownika do systemu;

8) Sprawuje nadzór nad obiegiem oraz przechowywaniem dokumentów i wydawnictw zawierających dane osobowe;

9) Identyfikuje i analizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych;

10) Określa potrzeby w zakresie zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe;

Administrator Systemu Informatycznego.

1) Monitoruje i zapewnia ciągłość działania systemu informatycznego oraz baz danych;

2) Optymalizuje wydajność systemu informatycznego baz danych;

3) Zarządza kopiami awaryjnymi danych, w tym danych osobowych oraz zasobów

umożliwiających ich przetwarzanie;

4) Przeciwdziała próbom naruszenia bezpieczeństwa informacji,

5) Przyznaje na wniosek Lokalnego Administratora Danych, za zgodą Administratora Bezpieczeństwa Informacji ściśle określonych praw dostępu do informacji w danym systemie;

6) Wnioskuje do Administratora Bezpieczeństwa Informacji w sprawie procedur bezpieczeństwa i standardów zabezpieczeń;

7) Zarządza licencjami i procedurami ich dotyczącymi;

8) Stwarzają warunki organizacyjno-techniczne umożliwiające spełnienie wymogów wynikających z obowiązywania ustawy o ochronie danych osobowych;

VII. PRZETWARZANIE DANYCH OSOBOWYCH

Systemy informatyczne, służące do przetwarzania danych osobowych, muszą spełniać wymogi obowiązujących aktów prawnych regulujących zasady gromadzenia i przetwarzania danych osobowych.

Do tworzenia kopii bezpieczeństwa danych osobowych w postaci elektronicznej służą indywidualne systemy archiwizowania dla poszczególnych systemów przetwarzania.

Kopie bezpieczeństwa oraz dokumenty papierowe zawierające dane osobowe przechowuje się w warunkach uniemożliwiających dostęp do nich osobom nieuprawnionym.

Pozostałe informacje dotyczące przetwarzania danych osobowych zawarte są w **Instrukcji zarządzania systemami informatycznymi służącym do przetwarzania danych osobowych**, która stanowi załącznik do Polityki Bezpieczeństwa .

VIII. SYSTEM ZABEZPIECZEŃ DANYCH OSOBOWYCH

1. Ochrona zbiorów danych polega na zabezpieczeniu informacji wprowadzonej, przetwarzanej, przesyłanej w systemie informatycznym oraz na nośnikach informacji przed nielegalnym ujawnieniem, kradzieżą oraz nieuprawnioną modyfikacją lub usunięciem.
2. W celu ochrony danych przechowywanych w systemach informatycznych należy wykorzystywać wchodzące w ich skład mechanizmy zarówno sprzętowe jak i programowe oraz inne rozwiązania zwiększające bezpieczeństwo danych.
3. Dane osobowe mogą przetwarzać wyłącznie osoby posiadające upoważnienia do przetwarzania danych osobowych. Osoby upoważnione do przetwarzania danych mają obowiązek zachować w tajemnicy dane, które przetwarzają, oraz sposoby ich zabezpieczenia.
4. Fakt modyfikacji zbioru danych: struktury, lokalizacji, a także utworzenia zbioru **Użytkownik, ASI** ma obowiązek zgłosić **Administratorowi oraz IODO**.
5. Obszary przetwarzania danych osobowych wymienione są w załączniku nr 1 graficznym Polityki Bezpieczeństwa
6. Osoby nieupoważnione do przetwarzania danych osobowych mogą przebywać w obszarach przetwarzania danych osobowych jedynie za zgodą **Administratora** lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

7. Wszystkie pomieszczenia, w których przetwarza się dane osobowe są zamykane na klucz w przypadku opuszczenia pomieszczenia przez ostatniego pracownika upoważnionego do przetwarzania danych osobowych – także w godzinach pracy.

8. Klucze do pomieszczeń służbowych mogą pobierać tylko te osoby, które są umieszczone w „*wykazie osób upoważnionych do pobierania kluczy”*

9. Dane osobowe przechowywane w wersji tradycyjnej (papierowej) są przechowywane po zakończeniu pracy w zamykanych na klucz meblach biurowych, a tam gdzie jest to możliwe – w szafach metalowych lub pancernych. Klucze od szaf należy zabezpieczyć przed dostępem osób nieupoważnionych do przetwarzania danych osobowych.

10. Dokumenty zawierające dane osobowe, w wyjątkowych sytuacjach mogą być wynoszone poza miejsce przetwarzania jedynie w wypadku otrzymania zgody Administratora z jednoczesnym zapewnieniem ochrony fizycznej ich przed niepożądanym dostępem osób nieupoważnionych. Odpowiedzialność za dokumentację ponosi pracownik, który otrzymał zgodę.
11. Po zakończonej pracy klucze do pomieszczeń, w których przetwarza się dane osobowe, oddaje się upoważnionemu pracownikowi obsługi gospodarczej, który zabezpiecza je przed nieuprawnionym dostępem w odpowiednim miejscu do tego wyznaczonym.
12. Dane osobowe w wersji papierowej, wydruki i kopie a także, w wersji elektronicznej na nośnikach typu płyty CD, DVD, dyskach przenośnych należy niszczyć w niszczarkach lub przekazywać do zniszczenia wynajętej do tego celu firmie.
13. Sprzątanie pomieszczeń gdzie przetwarzane są dane osobowe odbywa się po godzinach pracy przez personel sprzątający. Sprzątanie odbywa się tylko z założeniem, że zostaną zachowane przez pracowników przetwarzających dane osobowe zasady „*czystego biurka i ekranu*”.
14. Przy przetwarzaniu danych osobowych w systemach teleinformatycznych stosuje się zasady „*czystego biurka i ekranu*”, realizowane poprzez stosowanie wygaszaczy ekranu, klawiatury odwieszanych za pomocą indywidualnych haseł lub kodów oraz ustawianie monitorów w taki sposób aby nie była widoczna informacja dla osób postronnych. Zasada „*czystego biurka*”, sprowadza się do zabezpieczenia w czasie i po pracy danych osobowych w formie papierowej w taki sposób, aby uniemożliwiało ich odczyt przez osoby nieuprawnione.
15. **Zabrania się** udostępniania indywidualnego kodu dostępu i haseł innym osobom.
16. **Zabronione jest** usuwanie danych przez wyrzucenie ich do kosza na odpadki.
17. **Zabrania się** korzystania z prywatnych nośników informacji w systemach przetwarzających dane osobowe. Służbowe nośniki informacji są zewidencjonowane przez Administratora Systemu Informatycznego (ASI).
18. **Zabrania się** korzystania z sieci publicznej (World Wide Webside) poprzez nieautoryzowane przeglądarki internetowe lub nieznajomego pochodzenia witryny internetowe (domeny zagraniczne tj. com itp), których treść wskazuje na duże ryzyko występowania oprogramowania szpiegowskiego, hakerskiego, spamowego, wirusowego.
19. Przeglądanie sieci publicznej w zakresie tematyki nie związanej z zakresem wykonywanych czynności następuje za zgodą IODO, który to tematykę tych stron ustalił z Administratorem.
20. W przypadku żądania udostępniania danych pracownicy **NIEPUBLICZNA PLACÓWKA OŚWIATOWA** postępują zgodnie z przepisami ustawy o ochronie danych osobowych. Decyzję podejmuje IODO po powiadomieniu Administratora.

21. Udostępnianie danych jest odnotowywane w systemach informatycznych, a w przypadku zbiorów danych w formie tradycyjnej odnotowanie informacji o udostępnianiu przechowuje Administrator.

22. Budynki, w których zlokalizowane są zbiory danych osobowych, obowiązkowo są nadzorowane przez firmę ochroniarską przez 24 godziny na dobę , 7 dni w tygodniu.
23. Szczegółowe procedury zarządzania systemem informatycznym reguluje **„***Instrukcja Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych”.*
24. Dla danych osobowych przetwarzanych w systemach informatycznych stosuje się następujące zasady:

1) kontrola dostępu do zbiorów danych osobowych;

2) indywidualne identyfikatory użytkowników (pracowników przetwarzających dane osobowe);

3) uwierzytelnianie użytkowników (potwierdzanie ich tożsamości);

25.W celu zabezpieczenia danych osobowych przed ich utratą lub uszkodzeniem:

1) dla wszystkich systemów wdrożono procedury tworzenia kopii zapasowych;

2) wszystkie systemy informatyczne wyposażono w awaryjne zasilanie;

3) wdrożono oprogramowanie antywirusowe;

4) dostęp do systemów z sieci publicznej jest kontrolowany za pomocą zapory sieciowej oraz filtrów antyspamowych i oprogramowania antywirusowego;

5) poszczególne lokalizacje są połączone za pomocą sieci LAN;

6) przy przesyłaniu danych osobowych przez sieć publiczną użytkownicy są zobowiązani stosować oprogramowanie szyfrujące;

7) dopuszczalny jest dostęp spoza sieci Firmy przy wykorzystaniu programowej usługi za pomocą protokołu SSL;

8) zastosowano środki fizyczne chroniące urządzenia przed osobami nieupoważnionymi przez *Administratora* do dostępu do danych osobowych oraz zagrożeniami ze strony sił natury;

26.Użytkowników systemów przetwarzających dane osobowe obowiązuje następująca polityka haseł:

1) minimalna długość hasła wynosi 8 (osiem) znaków;

2) zmiana hasła następuje nie rzadziej niż co 30 dni;

3) hasło może się powtórzyć dopiero po 6 zmianie;

4) hasło zawiera małe i wielkie litery oraz cyfry lub znaki specjalne;

27. Jeżeli system informatyczny środkami technicznymi nie wymusza zasad ujętych powyżej, użytkownik zobowiązany jest do przestrzegania powyższych zasad, a tym samym do okresowej zmiany hasła i dobrania odpowiedniej jego długości;
28. Użytkownik, który utracił hasło, zobowiązany jest zgłosić ten fakt bezzwłocznie *Administratorowi Systemu Informatycznego*, który ustali nowe hasło;
29. Zabezpieczanie danych przed ich utratą uszkodzeniem, lub nieupoważnionym przetworzeniem w pozostałych przypadkach:

1) W przypadku naprawy, przekazania, likwidacji nośnika (papier, dysk twardy, płyta kompaktowa, pamięć przenośna, dyskietka, taśma magnetyczna itp.), który zawiera dane osobowe podmiotowi nieupoważnionemu do przetwarzania danych, należy zapewnić trwałe wymazanie informacji stanowiących dane osobowe;

2) W przypadku korzystania z komputerów przenośnych zawierających dane osobowe należy

zachować szczególną ostrożność podczas używania komputera poza obszarem przetwarzania danych wyszczególnionym w załączniku do niniejszej Polityki. W szczególności należy stosować mechanizmy szyfrowania plików lub baz danych, wbudowanych w system operacyjny. Po ustaniu konieczności przetwarzania danych na komputerze przenośnym, należy je trwale usunąć z nośnika danych;

3) Ekrany komputerów, na których przetwarzane są dane osobowe, są chronione wygaszaczami zabezpieczonymi hasłem. Monitory należy ustawić tak, aby ograniczyć dostęp do danych osobom nieupoważnionym do przetwarzania danych;

4) W pomieszczeniach gdzie przetwarzane dane osobowe są szczególnie narażone na ich przetworzenie przez osoby nieuprawnione stosuje się zabezpieczenia fizyczne w postaci odgrodzenia stref przetwarzania danych osobowych poprzez montaż np.:

1. a) przezroczystych szyb, drzwi;
2. b) drewnianych półek, lad, blatów;

Powyższe odgrodzenia mają na celu zabezpieczenie strefy szczególnie narażonych na przetwarzanie danych osobowych przed nieuprawnionym dostępem do strefy więcej niż jednej osoby bez wiedzy upoważnionego pracownika do przetwarzania danych osobowych, w pomieszczeniach gdzie zachowanie zasady „*czystego biurka*" jest ze względów logistycznych , fizycznych (brak miejsca) nie jest możliwe do zrealizowania.

Wstęp do strefy przetwarzania danych osobowych następuje za zgodą upoważnionego Pracownika.

IX.PRZEGLĄDY I AKTUALIZACJE POLITYKI

Polityka Bezpieczeństwa podlega regularnemu przeglądowi pod kątem przydatności, adekwatności i skuteczności. Przeglądu dokonuje *Inspektor Ochrony Danych Osobowych.*

Polityka Bezpieczeństwa podlega aktualizacji każdorazowo w przypadku:

1) likwidacji, utworzenia lub zmiany zawartości informacyjnej zbioru;

2) zmiany lokalizacji zbioru;

3) zmiany opiekuna zbioru lub *Inspektor Ochrony Danych Osobowych;*

4) zmiany przepisów prawa dotyczącego ochrony danych osobowych, wymagającej aktualizacji Polityki Bezpieczeństwa;

5) innych znaczących zmian dotyczących danych osobowych w funkcjonowaniu **NIEPUBLICZNA PLACÓWKA OŚWIATOWA.** Aktualizacji Polityki Bezpieczeństwa dokonuje *Inspektor Ochrony Danych Osobowych***,** wpisując ten fakt w karcie aktualizacyjnej.

X.POSTANOWIENIA KOŃCOWE

1. *Inspektor Ochrony Danych Osobowych* przeprowadzi szkolenie pracowników dotychczas

zatrudnionych w **NIEPUBLICZNA PLACÓWKA OŚWIATOWA** w zakresie przepisów prawa oraz uregulowań wewnętrznych w zakresie bezpieczeństwa danych osobowych w ciągu *2 tygodni* od dnia wejścia w życie niniejszej Polityki Bezpieczeństwa. Dla nowo zatrudnionych pracowników, którzy mają być dopuszczeni do przetwarzania zbiorów danych osobowych szkolenie przeprowadza się najpóźniej w ciągu *1 dnia* od daty zawarcia umowy.

2. Po zakończeniu szkolenia pracownik podpisuje stosowne oświadczenie o zapoznaniu się z zasadami Polityki Bezpieczeństwa lub jej zmianami.
3. W sprawach nieuregulowanych Polityką Bezpieczeństwa mają zastosowanie przepisy ustawy o ochronie danych osobowych, kodeksu pracy.
4. Politykę Bezpieczeństwa oraz zmiany Polityki Bezpieczeństwa wprowadza się w życie w formie zarządzenia właściciela Firmy.
5. Polityka Bezpieczeństwa przechowywana jest przez Administratora

Ramowy plan dnia

- 6.30 – 8.30 – gromadzenie się dzieci w Sali, zabawy swobodne
- 8.30- 9.00 – I śniadanie
- 9.00 – 9.15 – poranna toaleta, mycie ząbków, śpiewanie piosenek
- 9.15 – 9.30 – II śniadanie
- 9.30 – 11.00 – m.in zajęcia tematyczne, spacery, czytanie książeczek, mini teatrzyki, zajęcia sensoryczne, zajęcia plastyczne, zajęcia kulinarne
- 11.00- 11.20 – I część obiadku (zupka)
- 11.20 – 14.00 – czynności opiekuńcze, relaks
- 14.00- 14.30 – II część obiadku (drugie danie) + podwieczorek
- 14.30 – 17.00 – zabawy swobodne, pobyt na świeżym powietrzu, odbiór dzieci

* dodatkowe zajęcia w wybrane dni: jęz. angielski, rytmika, alpakoterapia

Regulamin Organizacyjny Niepublicznego Żłobka „Kamyczek” w Koszalinie

Drodzy Rodzice niniejszy Regulamin powstał przede wszystkim z myślą o bezpieczeństwie Waszych Dzieci. Prosimy Was o jego wnikliwą lekturę i przestrzeganie.

Regulamin Informacje podstawowe

1. Niepubliczny Żłobek „Kamyczek” mieści się przy ul. Powstańców Wlkp. 6a w Koszalinie
2. Niepubliczny Żłobek „Kamyczek” sprawuje funkcję opiekuńczą oraz wychowawczo-dydaktyczną nad dziećmi w wieku od 12 miesiąca do 3 lat
3. Niepubliczny Żłobek „Kamyczek” jest czynny w godzinach od 6.30 do 17.00 przez cały rok kalendarzowy z wyłączeniem świąt i dni ustawowo wolnych od pracy

Bezpieczeństwo Dzieci

4. Do odebrania dziecka upoważnieni są Rodzice oraz wskazani przez nich pisemnie opiekunowie.
5. Osobom w stanie nietrzeźwym dzieci nie będą wydawane
6. Rodzice/opiekunowie zobowiązani są przyprowadzać do żłobka zdrowe dziecko.
7. Dziecko chore lub podejrzane o chorobę nie zostanie przyjęte
8. Ważne sprawy dotyczące dzieci będą przekazywane bezpośrednio Rodzicom przez Opiekunki z poszanowaniem prawa do prywatności.

Organizacja

9. Rodzice oddając dziecko pod naszą opiekę zobowiązani są dostarczyć ubranka i przybory toaletowe (pieluchy jednorazowe, chusteczki nawilżone i krem). Rodzic oddając dziecko udziela wszelkich ważnych informacji dotyczących dziecka.
10. Organizację zajęć i rytmu dnia dla poszczególnych grup określa Ramowy Plan Dnia . Szczegóły planu dostosowywane są do indywidualnych potrzeb dzieci.
11. Dziecko może zostać zapisane do Niepublicznego Żłobka w pełnym wymiarze godzin – maksymalnie do 10 godzin dziennie względem każdego dziecka.

Żywienie

12. Informacje dotyczące żywienia:

• Dziecko korzysta z posiłku oferowanego w żłobku (rodzice ponoszą opłatę dodatkową za posiłki wg cennika.
• Każdego dnia proponujemy dzieciom 5 posiłków:
1 i 2 śniadanie, obiad (dwa dania w przedziale czasowym), podwieczorek oraz napoje
• Żywienie dzieci w żłobku : dzieci spożywają posiłki w sali z podziałem na grupy liczące maksymalnie 8 dzieci z uwagi na bezpieczeństwo i potrzebę dokarmiania indywidualnego.
• Grupa niemowląt spożywa posiłki według indywidualnych potrzeb dzieci.
Szczegóły dotyczące posiłków zostaną omówione z rodzicami, aby uwzględnić indywidualne potrzeby dzieci

Odpoczynek

• Dzieci odpoczywają według rozkładu dnia ustalonego dla żłobka i danej grupy wiekowej w wydzielonej do tego celu sypialni.

• Każde dziecko posiada oznakowany miejsce przeznaczone do odpoczynku (leżak, łóżeczko)

Opłaty za żłobek

13. Opłata (czesne) za pobyt dziecka w Niepublicznym Żłobku „Kamyczek II" wynosi: 750 zł
14. Pełna dzienna stawka żywieniowa wynosi 10 zł. (Stawka może ulec zmianie)
15. Stawka żywieniowa naliczona jest wg obecności dziecka
16. W dniu podpisania umowy Rodzice/opiekunowie zobowiązani są do wniesienia jednorazowej opłaty rezerwującej wynoszącej, 300 zł – gwarantuje ona dziecku miejsce w Niepublicznym Żłobku
17. Rodzice/opiekunowie zobowiązani są wnosić czesne do 5 dnia każdego miesiąca. Brak dokonania opłaty w terminie do 5 dnia miesiąca skutkuje wezwaniem do zapłaty z wyznaczeniem 7 - dniowego terminu zapłaty. Brak zapłaty w wyznaczonym dodatkowym terminie skutkuje skreśleniem dziecka z listy i jest jednoznaczne z rozwiązaniem umowy. Ponowne podpisanie umowy zależne jest od ponownego uiszczenia wpisowego.
18. Nieodebranie Dziecka w godzinach pracy żłobka skutkuje pobieraniem dodatkowej opłaty w wysokości: 50 PLN za każdą rozpoczętą godzinę pobytu dziecka w żłobku.
19. Wszelkie opłaty na poczet Niepublicznego Żłobka „Kamyczek II" wnoszone będą przelewem na rachunek bankowy.
20. Z zastrzeżeniem sytuacji, gdy do rozwiązania umowy dojdzie z przyczyn leżących po stronie Niepublicznego Żłobka Kamyczek II
Wszelkie opłaty wniesione przez Rodziców/opiekunów są bezzwrotne

Postanowienia końcowe

21. Rodzice/opiekunowie podpisując umowę powierzenia Dziecka pod opiekę Niepublicznego Żłobka Kamyczek II zobowiązują się do przestrzegania niniejszego Regulaminu. Pracownicy Niepublicznego Żłobka zobowiązują się do przestrzegania Regulaminu oraz do zapewnienia Państwa Dzieciom bezpieczeństwa oraz optymalnych warunków do ich rozwoju i szczęśliwego dzieciństwa.