Załącznik Nr 1
do wydanego przez dyrektora
Publicznego Przedszkola nr 26
Zarządzenia Nr 9/2012
z dnia 17 grudnia2012 roku

POLITYKA BEZPIECZEŃSTWA

PRZETWARZANIA DANYCH OSOBOWYCH

w Publicznym Przedszkolu nr 26

w Jastrzębiu-Zdroju

1. Obszar, w którym przetwarzane są dane osobowe

Budynki, pomieszczenia lub części pomieszczeń

1. Budynek Publicznego Przedszkola nr 26 Jastrzębie-Zdrój, ul. Wiejska 35 „i":
1) Kancelaria dyrektora przedszkola
2) Piętro – składnica akt

2. Wykaz zbiorów danych osobowych

L.p.	Nazwa zbioru (*kadrowy, płacowy, itp.*)	Nazwa programu (*programów*) informatycznego stosowanego do przetwarzania danych osobowych
1	Elektroniczny Obieg Dokumentów	EOD – MADKOM
2	Bankowość Elektroniczna	GBG24 – Getin Bank

3. Opis struktury zbioru danych osobowych

L.p.	Nazwa zbioru	Lista pól informacyjnych
1	Elektroniczny Obieg Dokumentów	Dane adresowe klienta (*nazwisko, imiona, PESEL, kod pocz-towy, miejscowość, ulica, nr domu, nr lokalu, kraj, nr terytorialny, telefon, faks, email, WWW, nazwa banku , numer rachunku bankowego, źródło danych*). Rejestr korespondencji przychodzącej od klienta (*status pisma, stan pisma, kod rejestru, data wpływu, numer kancelaryjny, temat, data pisma, osoba odpowiedzialna, kod nadawcy, nazwa nadawcy, adres nadawcy*) Rejestr korespondencji wychodzącej do klienta (*status pisma, stan pisma, kod rejestru, data wpisu, numer kancelaryjny, temat, data pisma, osoba odpowiedzialna, kod adresata, nazwa adresata, adres adresata, wartość przesyłki, waga przesyłki, opłata, kwota pobrania*) Rejestr spraw klienta (*status sprawy, stan sprawy, komórka organizacyjna, symbol JRWA, hasło JRWA, data rozpoczęcia sprawy, osoba odpowiedzialna, znak sprawy, data pisma, termin załatwienia, sposób załatwienia, temat, treść/przebieg załatwienia sprawy, nazwa strony, adres strony*)

4. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych osobowych

1) Środki techniczne:
   a) zasilanie, urządzenia techniczne wchodzące w skład lokalnej sieci komputerowej podłączone są do gniazd wydzielonej sieci zasilania. Zabrania się podłączania nieautoryzowanych urządzeń (*np. czajników bezprzewodowych, radioodbiorników itp.*) do gniazd zasilających urządzenia komputerowe,
   b) jednostki centralne (*serwery*), urządzenia aktywne lokalnej sieci komputerowej obowiązkowo zabezpieczone są na wypadek zaniku napięcia zasilającego za pomocą wysokiej klasy zasilaczy awaryjnych UPS (*realizowane przez Publiczne Przedszkole nr26 we współpracy z Wydziałem Informatyki Miejskiej w Jastrzębiu-Zdroju*),
   c) stacje robocze zabezpiecza się za pomocą zasilaczy awaryjnych w tych systemach, gdzie zanik napięcia zasilającego mógłby potencjalnie spowodować powstanie zagrożenia dla przetwarzanych informacji.

d) sieć publiczna Internet - dyrektor przedszkola oraz pracownicy mają zapewniony dostęp do sieci publicznej Internet w celu realizacji obowiązków służbowych; dostęp do usług sieci publicznej Internet podlega reglamentacji i kontroli za pomocą specjalistycznych urządzeń technicznych
e) autoryzacja w systemach informatycznych - wszystkie serwery oraz stacje robocze wyposażone są w oprogramowanie systemowe posiadające mechanizmy identyfikacji i autoryzacji operatora oraz związane z nimi mechanizmy przydziału odpowiednich uprawnień do pracy w systemie informatycznym; szczegółowe zasady autoryzacji w systemach informatycznych opisano w „Instrukcji zarządzania systemem informatycznym",
f) oprogramowanie zabezpieczające - serwery oraz stacje robocze chronione są przez zainstalowane na nich programy antywirusowe, które podlega regularnej aktualizacji; serwer poczty elektronicznej wyposażony jest dodatkowo w filtry antyspamowe; obowiązkowo serwery oraz stacje robocze posiadają włączone zapory sieciowe,
g) kopie - regularnie wykonuje się kopie bezpieczeństwa systemów informatycznych, w których przetwarza się dane osobowe; sposób wykonywania i przechowywania kopii bezpieczeństwa opisano w „Instrukcji zarządzania systemem informatycznym".

2) Środki organizacyjne:
a) pomieszczenia tworzące obszar przetwarzania danych osobowych, na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych powinny być zamykane w sposób uniemożliwiający dostęp osób postronnych. Zakazuje się pozostawiania otwartych pomieszczeń podczas nieobecności pracowników,
b) przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osoby zatrudnionej przy przetwarzaniu danych, Administratora Bezpieczeństwa Informacji lub osoby przez niego wyznaczonej,
c) klucze do pomieszczenia posiada dyrektor przedszkola i wicedyrektor, klucze zapasowe do pomieszczenia przechowywane są w gabinecie dyrektora przedszkola w przeznaczonej do tego celu zamykanej szafce, klucze muszą być jednoznacznie i trwale oznaczone numerem pomieszczenia.
d) stanowisko pracy powinno być zorganizowane w taki sposób, aby podczas przebywania w pomieszczeniu osób nieuprawnionych uniemożliwić im nieautoryzowany dostęp do informacji zawartych w dokumentach papierowych, wykonywanych wydrukach komputerowych, czy prezentowanych na monitorach komputerowych,
e) obowiązuje zasada tzw. „czystego biurka"; po zakończeniu pracy wszystkie dokumenty zawierające dane osobowe i wrażliwe informacje należy umieścić w przeznaczonych do tego zamykanych na klucz szafach, szufladach, kasetach; klucze należy zabezpieczyć przed dostępem osób niepowołanych,
f) upoważnienie do przetwarzania danych osobowych nadawane i odbierane jest użytkownikowi przez Administratora Danych,
g) warunkiem upoważnienia użytkownika do przetwarzania danych osobowych jest odbycie przez niego przeszkolenia z zakresu ochrony danych, zapoznanie się z dokumentacją bezpieczeństwa oraz podpisanie oświadczenia o poufności,

h) Administrator Danych prowadzi „Ewidencję osób upoważnionych do przetwarzania danych osobowych administratora w Publicznym Przedszkolu nr26 w Jastrzębiu-Zdroju", w której odnotowuje każdorazowo fakty nadania, zmiany lub cofnięcia uprawnień użytkownika; powyższa ewidencja może być prowadzona w formie elektronicznej,
i) upoważnienie automatycznie traci ważność w momencie ustania zatrudnienia, zmiany stanowiska pracy lub wygaśnięcia umowy,
j) zbędne, przeznaczone do wyrzucenia dokumenty papierowe, wydruki i ich kopie należy niezwłocznie niszczyć w odpowiednich niszczarkach lub zlecać zniszczenie wyspecjalizowanej firmie; w szczególności zabrania się usuwania takich dokumentów przez wyrzucenie ich do kosza na odpadki,
k) stosowane środki ochrony przy przetwarzaniu danych w systemie informatycznych opisuje „Instrukcja zarządzania systemem informatycznym",
l) w przypadku stwierdzenia naruszenia zasad ochrony danych osobowych stosuje się „Instrukcję postępowania w przypadku naruszenia bezpieczeństwa danych osobowych".

Załącznik Nr 3
do wydanego przez dyrektora
Publicznego Przedszkola nr 26
Zarządzenia Nr 9/2012
z dnia 17 grudnia2012 roku

INSTRUKCJA

POSTĘPOWANIA W SYTUACJI NARUSZENIA

BEZPIECZEŃSTWA DANYCH OSOBOWYCH

w Publicznym Przedszkolu nr 26
w
Jastrzębiu-Zdroju

1. Postanowienia ogólne

1) Instrukcja jest dokumentem wewnętrznym, przeznaczonym do stosowania przez pracowników Publicznego Przedszkola nr26 w Jastrzębiu-Zdroju. Ze względów bezpieczeństwa nie stanowi informacji publicznej w rozumieniu ustawy o dostępie do informacji publicznej (*Dz.U. z 2001r., Nr 112, poz. 1198*) i nie podlega publikacji ani udostępnieniu.
2) Instrukcja określa ogólne zasady i tryb postępowania Administratora Danych, Administratora Bezpieczeństwa Informacji oraz pracowników zatrudnionych w Publicznym Przedszkolu nr 26 w Jastrzębiu-Zdroju przy przetwarzaniu danych osobowych w sytuacji stwierdzenia lub powzięcia podejrzenia naruszenia zasad ochrony tych danych.

2. Przypadki naruszeń

1) Za naruszenie bezpieczeństwa uważa się złamanie lub powstanie bezpośredniego zagrożenia dla poufności, integralności, dostępności lub rozliczalności przetwarzanych danych osobowych.
2) Naruszenie bezpieczeństwa danych osobowych może być spowodowane:
   a) umyślnym lub nieumyślnym działaniem lub zaniechaniem działania użytkowników przy przetwarzaniu danych osobowych, nieprzestrzeganiem ustalonych procedur ochrony danych osobowych,
   b) umyślnym lub nieumyślnym działaniem osób trzecich, nieupoważnionych do przetwarzania danych osobowych (*włamania, wirusy komputerowe, kradzież danych*),
   c) błędami w stosowanym oprogramowaniu do przetwarzania danych lub zabezpieczania danych,
   d) awarią sprzętu komputerowego lub sieciowego,

e) nieprzewidzianym oddziaływaniem czynników zewnętrznych takich jak: pożar, powódź, katastrofa budowlana itp.

3. Postępowanie w przypadku stwierdzenia naruszenia lub powzięcia podejrzenia naruszenia ochrony danych osobowych

1) W przypadku stwierdzenia lub powzięcia podejrzenia naruszenia ochrony danych osobowych użytkownik zobowiązany jest niezwłocznie poinformować bezpośredniego przełożonego - ABI .
2) Do momentu przybycia ABI lub osoby przez niego upoważnionej użytkownik:
   a) zabezpiecza dostęp do pomieszczenia lub urządzenia,
   b) zabezpiecza dostępne dowody w zakresie stwierdzonego lub domniemanego naruszenia ochrony (*np. znalezione klucze, dokumenty, nośniki danych*),
   c) powstrzymuje się od działań mogących spowodować zatarcie dowodów (*np. powstrzymuje się od dalszej pracy na komputerze*).
3) W przypadku zgłoszenia podejrzenia naruszenia ochrony danych osobowych, ABI lub osoba przez niego wyznaczona przeprowadza analizę, której celem jest potwierdzenie lub odrzucenie naruszenia zasad ochrony.
4) ABI w przypadku stwierdzenia naruszenia bezpieczeństwa danych niezwłocznie podejmuje działania mające na celu:
   a) zminimalizowanie strat,
   b) doraźnego usunięcia zagrożenia danych (*zmiana haseł, odłączenie urządzeń*),
   c) zgromadzenia i zabezpieczenia dowodów.
5) Po przeprowadzonej analizie incydentu i ustaleniu jego przyczyn, ABI w porozumieniu z użytkownikami ustala działania w zakresie:
   a) naprawy powstałych szkód,
   b) wprowadzenia zmian w zakresie fizycznych, organizacyjnych i technicznych środków ochrony danych,
   c) dodatkowego przeszkolenia pracowników.

4. Dokumentacja zdarzenia

1) W przypadku stwierdzenia wystąpienia naruszenia ochrony danych osobowych, ABI przygotowuje raport zawierający, co najmniej:
   a) datę i miejsce wystąpienia naruszenia,
   b) zakres ujawnionych danych,
   c) przyczynę ujawnienia, osoby odpowiedzialne oraz stosowne dowody winy,
   d) sposób rozwiązania problemu,
   e) przyjęte rozwiązania mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
2) Raport otrzymuje Administrator Danych.

5. Postanowienia końcowe

Do zapoznania się z niniejszym dokumentem oraz stosowania zawartych w nim zasad zobowiązani są wszyscy upoważnieni pracownicy

Załącznik Nr 2
do wydanego przez dyrektora
Publicznego Przedszkola nr 26
Zarządzenia Nr 9/2012
z dnia 17 grudnia2012 roku

INSTRUKCJA

ZARZĄDZANIA SYSTEMEM

INFORMATYCZNYM

w Publicznym Przedszkolu nr26

w Jastrzębiu-Zdroju

1. Nadawanie uprawnień do przetwarzania danych oraz ich rejestrowanie w systemie informatycznym

Dyrekcja Publicznego Przedszkola nr26 w jastrzębiu-Zdroju deklaruje swoje zaangażowanie i odpowiedzialność za wdrożenie, sprawne działanie oraz doskonalenie systemu ochrony informacji przetwarzanych w Publicznym Przedszkolu nr26.
W tym celu:

1) do obsługi systemu informatycznego służącego do przetwarzania danych osobowych, może być dopuszczona wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych, wydane przez dyrektora przedszkola
2) upoważnienia do przetwarzania danych osobowych, o których mowa w pkt. 1.1 przechowywane są w teczkach akt osobowych pracowników,
3) dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po:
   a) podaniu identyfikatora użytkownika i właściwego hasła,
   b) podaniu właściwego hasła dostępu do stanowiska komputerowego,
4) dla każdego użytkownika systemu informatycznego, który przetwarza dane osobowe, dyrektor przedszkola - ASI ustala niepowtarzalny identyfikator i hasło początkowe,
5) identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie,
6) w przypadku utraty przez daną osobę uprawnień do dostępu do danych osobowych
7) w systemie informatycznym, identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych, należy niezwłocznie wyrejestrować z systemu informatycznego, unieważnić jej hasło, oraz podjąć inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych; za realizację procedury

rejestrowania i wyrejestrowywanie użytkowników w systemie informatycznym odpowiedzialny jest dyrektor przedszkola -ASI.

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

Informacje, a w tym dane osobowe przetwarzane są w Publicznym Przedszkolu nr 26 w Jastrzębiu-Zdroju z poszanowaniem przepisów prawa w celu:

1) dane osobowe przetwarzane są z użyciem dedykowanych serwerów, komputerów stacjonarnych,
2) hasło użytkownika powinno mieć minimum 8 znaków i być zmieniane w przypadku:
   a) dostępu do stanowiska komputerowego co 30 dni,
   b) w pozostałych zmiana hasła dostępu co 90 dni.
3) hasło oprócz znaków małych i dużych liter powinno zawierać ciąg znaków alfanumerycznych i specjalnych,
4) hasła wpisywane z klawiatury nie mogą pojawiać się na ekranie monitorów w formie jawnej,
5) hasło nie może zawierać żadnych informacji, które można kojarzyć z użytkownikiem komputera np. osobiste dane użytkownika, tj. nazwisko, inicjały, imiona, marka lub nr rejestracyjny samochodu itp.,
6) hasło nie może być zapisywane w miejscu dostępnym dla osób nieuprawnionych; użytkownik nie może udostępnić swojego identyfikatora oraz hasła jak również dostępu do stanowiska roboczego po uwierzytelnieniu w systemie osobom nieuprawnionym ani żadnej osobie postronnej,
7) hasło użytkownika, umożliwiające dostęp do systemu informatycznego, należy utrzymywać w tajemnicy, również po upływie jego ważności,
8) raz użyty identyfikator nie może być przydzielony innemu użytkownikowi,
9) w przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest do natychmiastowej zmiany hasła, lub w razie problemów powiadomić o tym fakcie dyrektora przedszkola.

3. Procedury rozpoczęcia, zawieszenia i zakończenia pracy

Do stosowania Instrukcji zarządzania systemem informatycznym zobowiązani są wszyscy pracownicy mający jakikolwiek dostęp do danych osobowych, w tym praktykanci, osoby zatrudnione na podstawie umów cywilno-prawnych :

1) dane osobowe, których administratorem jest Publiczne Przedszkole nr 26 mogą być przetwarzane sposobem tradycyjnym lub z użyciem systemu informatycznego tylko na potrzeby realizowania zadań statutowych i organizacyjnych,
2) rozpoczęcie pracy użytkownika w systemie informatycznym następuje po poprawnym uwierzytelnieniu (*zalogowaniu się do systemu*),

3) rozpoczęcie pracy w aplikacji musi być przeprowadzone zgodnie z instrukcją zawartą w dokumentacji aplikacji,
4) zakończenie pracy użytkownika następuje po poprawnym wylogowaniu się z systemu oraz poprzez uruchomienie odpowiedniej dla danego systemu opcji jego zamknięcia zgodnie z instrukcją zawartą w dokumentacji,
5) niedopuszczalne jest zakończenie pracy w systemie bez wykonania pełnej i poprawnej operacji wylogowania z aplikacji i poprawnego zamknięcia systemu,
6) monitory stanowisk komputerowych znajdujące się w pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień do przetwarzania danych osobowych, a na których przetwarzane są dane osobowe należy ustawić w taki sposób, aby uniemożliwić osobom postronnym wgląd w dane,
7) użytkownik ma obowiązek wylogowania się w przypadku zakończenia pracy; stanowisko komputerowe nie może pozostać z uruchomionym i dostępnym systemem bez nadzoru pracującego na nim pracownika,
8) wydruki zawierające dane osobowe należy przechowywać w miejscu uniemożliwiającym ich odczytanie przez osoby postronne; wydruki nieprzydatne należy zniszczyć w stopniu uniemożliwiającym ich odczytanie w niszczarce dokumentów,
9) przebywanie osób nieuprawnionych w pomieszczeniach znajdujących się na obszarze, w którym są przetwarzane dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania,
10) pomieszczenia, w których przetwarzane są dane osobowe, należy zamykać na czas nieobecności osób zatrudnionych w sposób uniemożliwiający dostęp do nich osobom trzecim,
11) użytkownik niezwłocznie powiadamia dyrektora przedszkola w przypadku podejrzenia fizycznej ingerencji w przetwarzane dane osobowe lub użytkowane narzędzia programowe lub sprzętowe; wówczas użytkownik jest zobowiązany do natychmiastowego wyłączenia sprzętu.

4. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi do ich przetwarzania

Administrator Danych sprawuje nadzór nad przestrzeganiem zasad wykonywania kopii zapasowych . Odpowiada on za:

1) zbiory danych osobowych w systemie informatycznym, ich zabezpieczanie przed utratą lub uszkodzeniem za pomocą:

   a) urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej,
   b) sporządzanie kopii zapasowych,

2) tworzenie pełnych kopii zapasowych zbiorów danych 2 razy w roku,
3) w szczególnych sytuacjach, np. przed aktualizacją lub zmianą oprogramowania lub systemu za wykonanie bezwzględnie pełnej kopii zapasowej systemu,
4) kopie zapasowe zbiorów danych, ich okresowe sprawdzanie pod kątem przydatności do odtworzenia w przypadku awarii systemu,

5) pozbawienie danych lub zniszczenie w sposób uniemożliwiający odczyt danych nośników danych po ustaniu ich użyteczności.

5. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi do ich przetwarzania

Administrator Systemu Informatycznego – dyrektor przedszkola odpowiada za poprawne funkcjonowanie systemu informatycznego przedszkola oraz stosowanie technicznych środków ochrony informacji. W szczególności odpowiada za:

1) okresowe kopie zapasowe wykonywane na płytach CD lub innych elektronicznych nośnikach informacji; kopie zapasowe przechowuje się w sposób uniemożliwiający nieuprawnione przejęcie,
2) przechowywanie kopii miesięcznych przez okres roku, wykonywane co pół roku pełne kopie systemu kadrowego i płacowego przechowuje się przez 50 lat; kopie zapasowe należy bezzwłocznie usuwać po ustaniu ich użyteczności,
3) dopilnowanie, aby w przypadku kopii zapasowych sporządzanych indywidualnie przez użytkownika odpowiedzialnością za ich zniszczenie obarczony był użytkownik,
4) w przypadku nośników informacji, przez ich zniszczenie rozumie się ich trwałe i nieodwracalne zniszczenie fizyczne do stanu nie dającego możliwości ich rekonstrukcji i odzyskania danych.

6. Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1. W związku z istnieniem zagrożenia dla zbiorów danych osobowych, ze strony wirusów komputerowych, których celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, konieczna jest ochrona sieci komputerowej i stanowisk komputerowych.
2. Wirusy komputerowe mogą pojawić się w systemach przedszkola poprzez: Internet, nośniki informacji takie jak: dyskietki, płyty CD, dyski przenośne, itp.
3. Przeciwdziałanie zagrożeniom ze strony wirusów komputerowych realizowane jest następująco:
   1) komputer z dostępem do Internetu musi być zabezpieczony za pomocą oprogramowania antywirusowego,
   2) zainstalowany program antywirusowy powinien być tak skonfigurowany, by co najmniej raz w tygodniu dokonywał aktualizacji bazy wirusów oraz co najmniej raz w tygodniu dokonywane było automatycznie sprawdzenie komputera pod kątem obecności wirusów komputerowych,
   3) elektroniczne nośniki informacji takie jak dyskietki, dyski przenośne, należy każdorazowo sprawdzać programem antywirusowym przed użyciem, po zainstalowaniu ich w systemie; czynność powyższą realizuje użytkownik; w przypadku problemów ze sprawdzeniem zewnętrznego nośnika danych użytkownik jest zobowiązany zwrócić się z tym do Administratora Systemu Informatycznego,
   4) komputery i systemy pracujące muszą mieć zainstalowany program antywirusowy, a w przypadku komputerów z dostępem do Internetu, również posiadać

oprogramowanie i mechanizmy zabezpieczające przed nieautoryzowanym dostępem z sieci (*firewall*),

5) w przypadku, gdy użytkownik stanowiska komputerowego zauważy komunikat oprogramowania zabezpieczającego system wskazujący na zaistnienie zagrożenia lub rozpozna tego typu zagrożenie, zobowiązany jest zaprzestać jakichkolwiek czynności w systemie i niezwłocznie skontaktować się z Administratorem Systemu Informatycznego,
6) przy korzystaniu z poczty elektronicznej należy zwrócić szczególną uwagę na otrzymywane załączniki dołączane do treści wiadomości; zabrania się otwierania załączników i wiadomości poczty elektronicznej od „niezaufanych" nadawców,
7) zabrania się użytkownikom komputerów wyłączania, blokowania odinstalowywania programów zabezpieczających komputer (*skaner antywirusowy, firewall*) przed oprogramowaniem złośliwym oraz nieautoryzowanym dostępem.

7. Udostępnianie danych osobowych i sposób odnotowania informacji o udostępnionych danych

Udostępnienie danych osobowych może odbywać się wyłącznie na pisemny uzasadniony wniosek lub zgodnie z przepisami prawa.

8. Wykonywanie przeglądów i konserwacji systemu oraz nośników informacji służących do przetwarzania danych

Za prowadzenie, wykonywanie przeglądów i konserwacji systemu oraz nośników informacji służących do przetwarzania danych odpowiada Administrator Systemu Informatycznego – dyrektor przedszkola, a w szczególności za:

1) przeglądy i konserwacje systemu oraz zbiorów danych wykonywanych na bieżąco,
2) umowy dotyczące instalacji i konserwacji sprzętu zawieranymi na bieżąco z podmiotami, których kompetencje nie budzą wątpliwości, co do wykonania usługi oraz których wiarygodność finansowa zostały sprawdzone na rynku,
3) naprawy sprzętu zlecanym podmiotom, których kompetencje nie budzą wątpliwości, co do wykonania usługi; naprawa sprzętu, na którym mogą znajdować się dane osobowe powinna odbywać się pod nadzorem osób użytkujących sprzęt w miejscu jego użytkowania,
4) w przypadku konieczności naprawy poza miejscem użytkowania, odpowiednie przygotowanie sprzętu komputerowego przed oddaniem do serwisu; dane należy wówczas zarchiwizować na nośniki informacji, a dyski twarde, bezwzględnie, wymontować na czas naprawy,
5) zmiany konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmianę jego lokalizacji, która może być dokonana tylko za wiedzą i zgodą dyrektora przedszkola.

9. Ustalenia końcowe

1. Osobom korzystającym z systemu informatycznego, w którym przetwarzane są dane osobowe w Publicznym Przedszkolu nr26 zabrania się ujawniania loginu i hasła współpracownikom i osobom z zewnątrz.
2. Pozostawiania haseł w miejscach widocznych dla innych osób.
3. Udostępniania stanowisk pracy wraz z danymi osobowymi osobom nieuprawnionym.
4. Udostępniania osobom nieuprawnionym programów komputerowych zainstalowanych w systemie.
5. Używania oprogramowania w innym zakresie niż pozwala na to umowa licencyjna.
6. Przenoszenia programów komputerowych, dysków twardych z jednego stanowiska na inne.
7. Kopiowania danych na nośniki informacji, kopiowania na inne systemy celem wynoszenia ich poza przedszkole.
8. Samowolnego instalowania i używania jakichkolwiek programów komputerowych w tym również programów do użytku prywatnego.
9. Używania nośników danych udostępnionych przez osoby postronne.
10. Przesyłania dokumentów i danych z wykorzystaniem konta pocztowego prywatnego.
11. Otwierania załączników i wiadomości poczty elektronicznej od nieznanych i „niezaufanych" nadawców.
12. Używania nośników danych niesprawdzonych, niewiadomego pochodzenia lub niezwiązanych z wykonywaną pracą; w przypadku konieczności użycia niesprawdzonych przenośnych nośników danych, należy zgłosić te nośniki w celu sprawdzenia - przeskanowania programem antywirusowym.
13. Tworzenia kopii zapasowych niechronionych hasłem i/lub bez odpowiednich zabezpieczeń miejsca ich przechowywania.
14. Ponadto zabrania się:
    1) wyrzucania dokumentów zawierających dane osobowe bez uprzedniego ich trwałego zniszczenia,
    2) pozostawiania dokumentów, kopii dokumentów zawierających dane osobowe w drukarkach, kserokopiarkach,
    3) pozostawiania kluczy w drzwiach, szafach, biurkach, zostawiania otwartych pomieszczeń, w których przetwarza się dane osobowe,
    4) pozostawiania bez nadzoru osób trzecich przebywających w pomieszczeniach przedszkola, w których przetwarzane są dane osobowe,
    5) pozostawiania dokumentów na biurku po zakończonej pracy, pozostawiania otwartych dokumentów na ekranie monitora bez blokady konsoli,
    6) ignorowania nieznanych osób z zewnątrz poruszających się w obszarze przetwarzania danych osobowych,
    7) przekazywania informacji będącymi danymi osobowymi osobom nieupoważnionym,
    8) ignorowania zapisów Polityki Bezpieczeństwa Publicznego Przedszkola nr 26 w Jastrzębiu-Zdroju.
15. Konieczne jest:
    1) posługiwanie się własnym loginem i hasłem w celu uzyskania dostępu do systemów informatycznych,
    2) tworzenie haseł trudnych do odgadnięcia dla innych,
    3) traktowanie konta pocztowego przedszkola jako narzędzia pracy i wykorzystywanie go jedynie w celach służbowych,

4) nie przerywanie procesu skanowania przez program antywirusowy na komputerze,
5) wykonywanie kopii zapasowych danych przetwarzanych na stanowisku komputerowym,
6) zabezpieczenie sprzętu komputerowego przed kradzieżą lub nieuprawnionym dostępem do danych.

16. Wszelkie przypadki naruszenia niniejszej Instrukcji należy zgłaszać dyrektorowi przedszkola lub Administratorowi Systemu Informatycznego.

10. Zalecenia w zakresie przetwarzania danych osobowych sposobem tradycyjnym

1. Miejscem tworzenia, uzupełniania, przechowywania dokumentacji dotyczącej przetwarzania danych osobowych sposobem tradycyjnym jest pomieszczenie w Publicznym Przedszkolu nr26 : gabinet dyrektora,
2. Osoby prowadzące dokumentację zobowiązane są do zachowania tajemnicy służbowej.
3. Dokumentacji, o której mowa w pkt. 10.1 nie można wynosić poza teren przedszkola.
4. Dokumentację, o której mowa w pkt. 10.1 archiwizuje się zgodnie z Instrukcją kancelaryjną.
5. Osoby prowadzące dokumentację zobowiązane są do niezwłocznego poinformowania dyrektora przedszkola, o podejrzeniu dostępu do dokumentacji przez osoby nieupoważnione.

DYREKTOR
Publicznego Przedszkola nr 26
mgr Ewa Radomska-Mura