ZESPÓŁ
SZKOLNO-PRZEDSZKOLNY Nr 1
ul. Jordana 6
47-400 RACIBÓRZ
tel./fax 032 415-61-95
NIP 639-17-75-954

Załącznik nr 2 do Zarządzenia Dyrektora nr 23 2010/ 2011 z dnia 10.06.2011

Polityka bezpieczeństwa
i
Instrukcja zarządzania systemem przetwarzania danych osobowych
w sposób tradycyjny oraz przy użyciu
systemu informatycznego
w Zespole Szkolno - Przedszkolnym nr 1 w Raciborzu

CEL PROWADZENIA I GROMADZENIA DANYCH OSOBOWYCH

Cele, dla których Zespół Szkolno - Przedszkolny nr 1 w Raciborzu zbiera dane osobowe to:

1. Przebieg zatrudnienia i wynagradzania w odniesieniu do pracowników i ich rodzin.

2. Realizacja zadań dydaktyczno - wychowawczo - opiekuńczych w stosunku do wychowanków Przedszkola nr 17 i uczniów Szkoły Podstawowej nr 14 im. Arki Bożka w Raciborzu.

3. Gromadzenie ofert pracy.

Podstawa prawna:

1. Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997r. (tekst jednolity: Dz. U.2002, Nr 101,poz.926)

2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004, Nr 100, poz. 1024)

3. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008r w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. z 2009, Nr 229, poz.1536)

4. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych wydane do art. 39 a ustawy.

Spis treści

1. Pojęcia

1) Ustawa — rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych z dnia 29 sierpnia 1997r. (tekst jedn. Dz. U. z 2002 r. Nr 101, poz. 926 z poźn. zm.).
2) Administrator danych osobowych – rozumie się przez to Dyrektora Zespołu Szkolno-Przedszkolnego nr 1 w Raciborzu.
3) Pełnomocnik dyrektora ds. Ochrony Danych Osobowych – osoba powołana zarządzeniem dyrektora, której zadaniem jest nadzorowanie i koordynowanie w szkole zasad postępowania przy przetwarzaniu danych osobowych.
4) Administrator Bezpieczeństwa Informacji – osoba powołana zarządzeniem dyrektora, która odpowiada za bezpieczeństwo danych osobowych w systemie informatycznym szkoły, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w których przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.
5) Dane osobowe - w rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
6) Przetwarzanie danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
7) Zbiór danych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów.
8) System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
9) Identyfikator użytkownika (login) - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
10) Hasło - ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
11) Uwierzytelnianie — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
12) Integralność danych — rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
13) Poufności danych — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.

2. Polityka bezpieczeństwa

1) Wykaz budynków, pomieszczeń tworzących obszar , w którym przetwarzane są dane osobowe:

Lp.	Budynek	Rodzaj danych/ miejsce przechowywania	Zabezpieczenie
1.	ul. Jordana 6	Dzienniki lekcyjne	Szafa metalowa – sekretariat
		Dzienniki zajęć specjalistycznych	Szafa metalowa – sekretariat
		Dzienniki nauczania indywidualnego	Szafa metalowa – sekretariat
		Dzienniki zajęć pozalekcyjnych	Szafa metalowa – sekretariat
		Opłaty Optimum-VULKAN	Hasło
		Płatnik ZUS	Hasło
		Dokumenty zarchiwizowane	Archiwum szkolne

2) W placówce znajdują się bazy danych:

a) arkusz organizacyjny szkoły,

b) kadry,

c) ewidencja dzieci i uczniów (rodzice/ prawni opiekunowie, opinie i orzeczenia dotyczące pomocy psychologiczno – pedagogicznej, pomoc specjalistyczna, pomoc społeczna itp.)

3) W szkole znajdują się zbiory danych :

a) organizacja pracy szkoły,

b) teczki akt osobowych,

c) teczki nadzoru pedagogicznego, awansu zawodowego,

d) księgi dzieci,

e) księgi uczniów,

f) arkusze ocen,

g) dzienniki lekcyjne, nauczania indywidualnego,

h) dzienniki zajęć pozalekcyjnych, specjalistycznych,

i) dzienniki pedagoga, świetlicy, biblioteki

j) dokumentacja pedagoga szkolnego, wychowawców klas.

4) Przekazanie informacji osobom, których dane będą zbierane

a) Obowiązek informowania, a także uzyskania oświadczeń woli traktowany jest łącznie w stosunku do grup, których dane zespół zbiera i przetwarza.

b) W przypadku pracowników obowiązek, o którym mowa w pkt. „a" uważa się za spełniony po podpisaniu druku stanowiącego załącznik nr 1.

c) Obsługę finansowo-księgową placówki prowadzi Zespół Obsługi Placówek Oświatowych w Raciborzu, ul. Środkowa.

d) W przypadku wychowanków, uczniów i rodziców obowiązek, o którym mowa w pkt. 1 uważa się za spełniony po podpisaniu przez rodziców (prawnych opiekunów) druku zgłoszenia dziecka do przedszkola oraz do szkoły.

5) Sposoby przetwarzania danych .

Lp.	Rodzaj danych/ miejsce przechowywania	Sposób przetwarzania	Osoba odpowiedzialna	Zabezpieczenie
1.	Dzienniki lekcyjne	tradycyjny	wychowawcy	Szafa metalowa - sekretariat
2.	Dzienniki zajęć przedszkolnych	tradycyjny	wychowawcy	Biurka w salach przedszkolnych
3.	Dzienniki zajęć specjalistycznych	tradycyjny	Nauczyciele prowadzący zajęcia specjalistyczne	Szafa metalowa – sekretariat

6) Przepływ danych pomiędzy poszczególnymi systemami :

a) OFFICE – HERMES – brak
b) OFFICE – SIO – brak
c) OFFICE – VULCAN – brak
d) SIO – HERMES –brak
e) SIO – VULCAN – brak
f) HERMES – VULCAN – brak
g) PŁATNIK (ZUS)- HERMES - brak
h) PŁATNIK (ZUS)- OFFICCE- brak
i) PŁATNIK (ZUS)- SIO- brak
j) PŁATNIK (ZUS)- VULKAN- brak
k) PŁATNIK (ZUS)- ŚWIADECTWA- brak
l) OPŁATY- HERMES- brak
m) OPŁATY- SIO- brak
n) OPŁATY- VULKAN- brak
o) OPŁATY- OFFICE- brak
p) ŚWIADECTWA- OFFICCE- brak
q) ŚWIADECTWA- HERMES- brak
r) ŚWIADECTWA- SIO- brak
s) ŚWIADECTWA- VULKAN- brak
t) ŚWIADECTWA- ZUS- brak
u) ŚWIADECTWA- OPŁATY- brak

7) **Zadaniem Pełnomocnika dyrektora ds. Ochrony Danych Osobowych** jest nadzorowanie pracy Administratora Bezpieczeństwa Informacji.

8) **Zadania „Administratora Bezpieczeństwa Informacji" :**

a) ochrona i bezpieczeństwo danych osobowych zawartych w zbiorach prowadzonych sposobem tradycyjnym oraz poprzez system informatyczny,

b) podejmowanie stosownych działań zgodnie z niniejszą „Polityką bezpieczeństwa" w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym,

c) niezwłoczne informowanie dyrektora - Administratora Danych lub Pełnomocnika dyrektora ds. Ochrony Danych Osobowych o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,

d) nadzór i kontrola systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych,

e) nadzór i kontrola systemu przetwarzania danych osobowych sposobem tradycyjnym.

3. Instrukcja

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

1) Do obsługi systemu informatycznego służącego do przetwarzania danych osobowych, może być dopuszczona wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych, wydane przez Administratora danych osobowych.

2) Upoważnienia do przetwarzania danych osobowych, o których mowa w punkcie 1.1. przechowywane są w teczkach akt osobowych pracowników oraz prowadzona jest ich ewidencja.

3) Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po:

   a) podaniu identyfikatora użytkownika i właściwego hasła w przypadku obsługi SIO, HERMES, PŁATNIK

   b) podaniu właściwego hasła dostępu do stanowiska komputerowego w przypadku obsługi OFFICE, VULCAN, OPŁATY

4) Dla każdego użytkownika systemu informatycznego, który przetwarza dane osobowe, Administrator Bezpieczeństwa Informacji 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 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 Administrator Bezpieczeństwa Informacji.

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

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) Systemu SIO, HERMES, PŁATNIK – co 30 dni,
   b) OFFICE, VULCAN, OPŁATY- zmiana hasła dostępu do stanowiska komputerowego co 90 dni.
3) Hasło oprócz znaków małych i dużych liter winno 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) Hasła są zdeponowane w szafie metalowej w sekretariacie.
10) 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 Administratora Bezpieczeństwa Informacji.

3. Procedury rozpoczęcia, zawieszenia i zakończenia pracy

1) Dane osobowe, których administratorem jest Zespół Szkolno- Przedszkolny nr 1 w Raciborzu mogą być przetwarzane sposobem tradycyjnym lub z użyciem systemu informatycznego tylko na potrzeby realizowania zadań statutowych i organizacyjnych szkoły.
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 Administratora Bezpieczeństwa Informacji 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 służących do ich przetwarzania

1) Zbiory danych w systemie informatycznym są zabezpieczane przed utratą lub uszkodzeniem za pomocą: sporządzania kopii zapasowych zbiorów danych (kopie pełne).

2) Za tworzenie kopii bezpieczeństwa systemu informatycznego odpowiedzialny jest Administrator Bezpieczeństwa Informacji.

3) Pełne kopie zapasowe zbiorów danych są tworzone co najmniej 2 razy w roku.

4) W szczególnych przypadkach – przed aktualizacją lub zmianą w systemie należy bezwarunkowo wykonać pełną kopię zapasową systemu.

5) Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu. Za przeprowadzanie tej procedury odpowiedzialny jest Administrator Bezpieczeństwa Informacji.

6) Nośniki danych po ustaniu ich użyteczności należy pozbawić danych lub zniszczyć w sposób uniemożliwiający odczyt danych.

5. **Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych**

1) Okresowe kopie zapasowe wykonywane są na płytach CD lub innych elektronicznych nośnikach informacji. Kopie zapasowe przechowuje się w sposób uniemożliwiający nieuprawnione przejęcie, modyfikacje, uszkodzenie lub zniszczenie w szafie metalowej w sekretariacie.

2) Dostęp do nośników z kopiami zapasowymi systemu oraz kopiami danych osobowych, ma wyłącznie Administrator Bezpieczeństwa Informacji .

3) Kopie miesięczne przechowuje się przez okres 6 miesięcy. Wykonywane co pół roku pełne kopie systemu kadrowego przechowuje się przez 50 lat. Kopie zapasowe należy bezzwłocznie usuwać po ustaniu ich użyteczności.

4) Usunięcie danych z systemu powinno zostać zrealizowane przy pomocy oprogramowania przeznaczonego do bezpiecznego usuwania danych z nośnika informacji.

5) W przypadku kopii zapasowych sporządzanych indywidualnie przez użytkownika odpowiedzialnością za ich zniszczenie obarczony jest użytkownik.

6) W przypadku nośników informacji, przez ich zniszczenie rozumie się ich trwałe i nieodwracalne zniszczenie fizyczne do stanu niedającego 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 systemach szkoły poprzez: Internet, nośniki informacji takie jak: płyty CD, dyski przenośne, itp.

3) Przeciwdziałanie zagrożeniom ze strony wirusów komputerowych realizowane jest następująco:

   a) komputer z dostępem do Internetu musi być zabezpieczony za pomocą oprogramowania antywirusowego,

   b) 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.

4) Elektroniczne nośniki informacji takie jak dyski przenośne, należy każdorazowo sprawdzać programem antywirusowym przed użyciem, po zainstalowaniu ich w systemie. Czynność powyższą realizuje użytkownik systemu. W przypadku problemów ze sprawdzeniem zewnętrznego nośnika danych użytkownik jest zobowiązany zwrócić się z tym do Administratora Bezpieczeństwa Informacji.

5) 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).

6) 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 Bezpieczeństwa Informacji.

7) 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.

8) Zabrania się użytkownikom komputerów, wyłączania, blokowania odinstalowania programów zabezpieczających komputer (skaner antywirusowy, firewall) przed oprogramowaniem złośliwym oraz nieautoryzowanym dostępem.

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

1) Udostępnienie danych instytucjom może odbywać się wyłącznie na pisemny uzasadniony wniosek lub zgodnie z przepisami prawa (OKE, CKE, Urząd Miasta, ZUS itp.).

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

1) Przeglądy i konserwacje systemu oraz zbiorów danych wykonuje Administrator Bezpieczeństwa Informacji na bieżąco.

2) Administrator Bezpieczeństwa Informacji okresowo sprawdza możliwość odtworzenia danych z kopii zapasowej.

3) Umowy dotyczące instalacji i konserwacji sprzętu należy zawierać z podmiotami, których kompetencje nie budzą wątpliwości, co do wykonania usługi oraz których wiarygodność finansowa zostały sprawdzone na rynku.

4) Naprawy sprzętu należy zlecać 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 oraz Administratora Bezpieczeństwa Informacji w miejscu jego użytkowania.

5) W przypadku konieczności naprawy poza miejscem użytkowania, sprzęt komputerowy, przed oddaniem do serwisu, powinien być odpowiednio przygotowany. Dane należy zarchiwizować na nośniki informacji, a dyski twarde, bezwzględnie, wymontować na czas naprawy.

6) Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jego lokalizacji, może być dokonana tylko za wiedzą i zgodą Administratora Bezpieczeństwa Informacji.

9. Ustalenia końcowe

1) Osobom korzystającym z systemu informatycznego, w którym przetwarzane są dane osobowe w szkole zabrania się:

   a) ujawniania loginu i hasła współpracownikom i osobom z zewnątrz,

   b) pozostawiania haseł w miejscach widocznych dla innych osób,

   c) udostępniania stanowisk pracy wraz z danymi osobowymi osobom nieuprawnionym,

   d) udostępniania osobom nieuprawnionym programów komputerowych zainstalowanych w systemie,

   e) używania oprogramowania w innym zakresie niż pozwala na to umowa licencyjna,

   f) przenoszenia programów komputerowych, dysków twardych z jednego stanowiska na inne,

   g) kopiowania danych na nośniki informacji, kopiowania na inne systemy celem wynoszenia ich poza szkołę,

   h) samowolnego instalowania i używania jakichkolwiek programów komputerowych w tym również programów do użytku prywatnego; programy komputerowe instalowane są przez Administratora Bezpieczeństwa Informacji,

   i) używania nośników danych udostępnionych przez osoby postronne,

   j) przesyłania dokumentów i danych z wykorzystaniem konta pocztowego prywatnego (niesłużbowego),

   k) otwierania załączników i wiadomości poczty elektronicznej od nieznanych i „niezaufanych" nadawców,

   l) 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, Administratorowi Bezpieczeństwa Informacji,

   m) tworzenia kopii zapasowych niechronionych hasłem i/lub bez odpowiednich zabezpieczeń miejsca ich przechowywania.

2) Ponadto zabrania się:

a) wyrzucania dokumentów zawierających dane osobowe bez uprzedniego ich trwałego zniszczenia,

b) pozostawiania dokumentów, kopii dokumentów zawierających dane osobowe w drukarkach, kserokopiarkach,

c) pozostawiania kluczy w drzwiach, szafach, biurkach, zostawiania otwartych pomieszczeń, w których przetwarza się dane osobowe,

d) pozostawiania bez nadzoru osób trzecich przebywających w pomieszczeniach szkoły, w których przetwarzane są dane osobowe,

e) pozostawiania dokumentów na biurku po zakończonej pracy, pozostawiania otwartych dokumentów na ekranie monitora bez blokady konsoli,

f) ignorowania nieznanych osób z zewnątrz poruszających się w obszarze przetwarzania danych osobowych,

g) przekazywania informacji będącymi danymi osobowymi osobom nieupoważnionym,

h) ignorowania zapisów Polityki Bezpieczeństwa szkoły.

3) Konieczne jest:

a) posługiwanie się własnym loginem i hasłem w celu uzyskania dostępu do systemów informatycznych,

b) tworzenia haseł trudnych do odgadnięcia dla innych,

c) traktowanie konta pocztowego zespołu jako narzędzia pracy i wykorzystywanie go jedynie w celach służbowych,

d) nieprzerywanie procesu skanowania przez program antywirusowy na komputerze,

e) wykonywanie kopii zapasowych danych przetwarzanych na stanowisku komputerowym,

f) zabezpieczenie sprzętu komputerowego przed kradzieżą lub nieuprawnionym dostępem do danych.

4) Wszelkie **przypadki naruszenia** niniejszej Instrukcji należy zgłaszać przełożonemu.

4. Zalecenia w zakresie przetwarzania danych osobowych sposobem tradycyjnym

1) Miejscem tworzenia, uzupełniania, przechowywania dokumentacji dotyczącej przetwarzania danych osobowych sposobem tradycyjnym są pomieszczenia:

a) w szkole: sekretariat, pokój nauczycielski, gabinet dyrektora, pedagoga, biblioteka, świetlica, sale lekcyjne, boiska i teren zielony wokół placówki,

b) w przedszkolu: gabinet wicedyrektora, sale zajęć, pomieszczenie intendenta.

2) Osoby prowadzące dokumentację zobowiązane są do zachowania tajemnicy służbowej.

3) Dokumentacji, o której mowa w punkcie 1.1. nie można wynosić poza teren szkoły.

4) Dokumentację, o której mowa w punkcie 1.1. archiwizuje się zgodnie z Instrukcją kancelaryjną.

5) Osoby prowadzące dokumentację zobowiązane są do niezwłocznego poinformowania Pełnomocnika dyrektora ds. przetwarzania danych osobowych o podejrzeniu dostępu do dokumentacji przez osoby nieupoważnione.

DYREKTOR
ZESPOŁU SZKOLNO-PRZEDSZKOLNEGO
mgr Daniel Siedlok