Zarządzenie nr 6/2013
Dyrektora Szkoły Podstawowej Nr 2 w Wesołej
z dnia 4 grudnia 2013 roku

w sprawie wdrożenia Polityki Bezpieczeństwa Informacji.

Na podstawie art. 39 ust. 3 pkt 3 ustawy o systemie oświaty i art. 69 ust. 1 pkt 3 w związku z art. 68 ust. 2 pkt 5 ustawy z 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2009 r. Nr 157, poz. 1240) oraz w oparciu o „Standardy kontroli zarządczej dla sektora finansów publicznych", określone w Komunikacie Nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych (Dz. Urz. Min. Fin. Nr 15, poz. 84)

postanawiam:

§ 1

W celu zapewnienia ochrony danych osobowych przetwarzanych w postaci tradycyjnej, jak i cyfrowej oraz przestrzegania przepisów związanych z ochroną danych osobowych wprowadzam do użytku w Szkole Podstawowej Nr 2 w Wesołej "Politykę Bezpieczeństwa Informacji", stanowiącą załącznik do niniejszego Zarządzenia.

§ 2

Każdy pracownik, jest obowiązany zapoznać się z treścią Polityki Bezpieczeństwa Informacji

§ 3

Pracodawca zobowiązuje wszystkich pracowników do przestrzegania Polityki Bezpieczeństwa Informacji pod sankcją konsekwencji służbowych, przewidzianych prawem.

§ 4.

Zarządzenie wchodzi w życie z dniem podjęcia.

Załącznik do Zarządzenia nr 6/2013
Dyrektora Szkoły Podstawowej Nr 2 w Wesołej
z dnia 4 grudnia 2013 r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

Szkoły Podstawowej Nr 2 w Wesołej

§ 1.
Podstawa prawna

1. Konstytucja RP (art. 47 i 51)
2. Konwencja nr 108 Rady Europy – dotycząca ochrony osób w związku z automatycznym przetwarzaniem danych osobowych
3. Dyrektywa PE i RE z dnia 24 października 1995 r. (95/46/EC) w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych
4. Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2002 r. Nr 101 poz. 926 z późn. zm.)-(art. 36)
5. Rozporządzenie MSWiA z dnia 29 kwietnia 2004 r. 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 r. Nr 100 poz. 1024)-(paragraf 3 i 4)
6. Kodeks pracy

§ 2.

Podstawowe pojęcia

2. **Szkoła** – w tym dokumencie jest rozumiana, jako Szkoła Podstawowa Nr 2 w Wesołej, zlokalizowana pod adresem 36-233 Wesoła 607;
1. **Polityka** – w tym dokumencie jest rozumiana jako „Polityka bezpieczeństwa" obowiązująca w Szkole Podstawowej Nr 2 w Wesołej;
2. **Administrator Bezpieczeństwa Informacji (ABI) –** pracownik szkoły wyznaczony przez Administratora Danych Osobowych (Dyrektora) do nadzorowania przestrzegania zasad ochrony danych osobowych, oraz przygotowania dokumentów wymaganych przez przepisy ustawy o ochronie danych osobowych w Szkole Podstawowej Nr 2 w Wesołej. ABI powołany jest zarządzeniem Dyrektora Szkoły Podstawowej Nr 2 w Wesołej.
3. **Administrator Systemu Informatycznego (ASI) –** pracownik odpowiedzialny za funkcjonowanie systemu teleinformatycznego, oraz stosowanie technicznych i organizacyjnych środków ochrony stosowanych w tym systemie;
4. **Użytkownik systemu** – osoba upoważniona do przetwarzania danych osobowych w systemie. Użytkownikiem może być osoba zatrudniona w szkole, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w szkole;
5. **Identyfikator użytkownika** – jest to ciąg znaków jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
6. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

7. **Przetwarzanie danych** – rozumie się to w tym dokumencie, jako jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie;
8. **Zabezpieczenie danych w systemie informatycznym** – wdrożenie i wykorzystywanie stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
9. **Wysoki poziom bezpieczeństwa** – musi występować wtedy, gdy przynajmniej jedno urządzenie systemu informatycznego, służące do przetwarzania danych osobowych, połączone jest z siecią publiczną,
10. **Sieć lokalna** – połączenie komputerów pracujących w szkole w celu wymiany danych (informacji) dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych;
11. **Sieć publiczna** – sieć telekomunikacyjna, niebędąca siecią wewnętrzną służąca do świadczenia usług telekomunikacyjnych w rozumieniu ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z poźn. zm.);
12. **Sieć telekomunikacyjna** – urządzenia telekomunikacyjne zestawione i połączone w sposób umożliwiający przekaz sygnałów pomiędzy określonymi zakończeniami sieci za pomocą przewodów, fal radiowych, bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną w rozumieniu ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne (Dz. U. Nr 73, poz.852 z późń. zm.);

Rozdział I

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

§ 3.

Polityka bezpieczeństwa w zakresie ochrony danych osobowych Szkoły Podstawowej Nr 2 w Wesołej, określa zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

Polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa przetwarzanych danych. Polityka bezpieczeństwa dotyczy danych osobowych przetwarzanych w zbiorach manualnych oraz w systemach informatycznych.

§ 4.

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe określa **załącznik nr 1**.

§ 5.

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów

zastosowanych do przetwarzania tych danych określa **załącznik nr 2**.
Przetwarzanie danych osobowych w systemie informatycznym odbywa się przy zachowaniu wysokiego poziom bezpieczeństwa.

§ 6.

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami określa **załącznik nr 3.**

§ 7

System przetwarzania danych osobowych

1. W skład systemu wchodzą:
   1.1. dokumentacja papierowa (korespondencja, dokumenty pracowników i uczniów);
   1.2. wydruki komputerowe;
   1.3. urządzenia i oprogramowanie komputerowe służące do przetwarzania informacji;
   1.4. procedury przetwarzania danych w tym systemie, w tym procedury awaryjne.
2. Sposób przepływu danych pomiędzy poszczególnymi systemami
   OFFICE - HERMES
   OFFICE – LIBRUS
   OFFICE – SIO
3. Sposób przekazywania danych: manualny.
4. Przetwarzanie danych osobowych w systemie informatycznym odbywa się przy zachowaniu wysokiego poziomu bezpieczeństwa.

§ 8

Środki techniczne i organizacyjne stosowane w przetwarzaniu danych

Cele i zasady funkcjonowania polityki bezpieczeństwa:

1. Szkoła realizując politykę bezpieczeństwa informacji zapewnia ich:
   1.1. poufność – informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, podmiotom i procesom,
   1.2. integralność – dane nie zostają zmienione lub zniszczone w sposób nie autoryzowany,
   1.3. dostępność – istnieje możliwość wykorzystania ich na żądanie, w założonym czasie, przez autoryzowany podmiot,
   1.4. rozliczalność – możliwość jednoznacznego przypisania działań poszczególnym osobom,
   1.5. autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana,
   1.6. niezaprzeczalność – uczestnictwo w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne,
   1.7. niezawodność – zamierzone zachowania i skutki są spójne.

2. Polityka bezpieczeństwa informacji w Szkole ma na celu zredukowanie możliwości wystąpienia negatywnych konsekwencji naruszeń w tym zakresie, tj.:
   2.1. naruszeń danych osobowych rozumianych jako prywatne dobro powierzone Szkole;
   2.2. naruszeń przepisów prawa oraz innych regulacji;
   2.3. utraty lub obniżenia reputacji Szkoły;
   2.4. strat finansowych ponoszonych w wyniku nałożonych kar;
   2.5. zakłóceń organizacji pracy spowodowanych nieprawidłowym działaniem systemów.
3. Realizując Politykę bezpieczeństwa w zakresie ochrony danych osobowych Szkoła dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:
   3.1. przetwarzane zgodnie z prawem,
   3.2. zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
   3.3. merytorycznie poprawne i adekwatne w stosunku do celu, w jakim są przetwarzane,
   3.4. przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

§ 9

Kompetencje i odpowiedzialność w zarządzaniu bezpieczeństwem danych osobowych

Za przetwarzanie danych osobowych niezgodnie z prawem, celami przetwarzania lub przechowywanie ich w sposób niezapewniający ochrony interesów osób, których te dane dotyczą grozi odpowiedzialność karna wynikająca z przepisów ustawy o ochronie danych osobowych lub pracownicza na zasadach określonych w kodeksie pracy.

§ 10

Administrator Danych Osobowych (ADO) – Dyrektor Szkoły:

1. formułuje i wdraża warunki techniczne i organizacyjne służące ochronie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,

2. decyduje o zakresie, celach oraz metodach przetwarzania i ochrony danych osobowych,

3. wydaje upoważnienie do przetwarzania danych osobowych określając w nich zakres i termin ważności – wzór upoważnienia określa **załącznik nr 4,**

4. odwołuje upoważnienie – **załącznik nr 5,**

5. odpowiada za zgodne z prawem przetwarzanie danych osobowych w Szkole.

§ 11

Administrator Bezpieczeństwa Informacji (ABI) – pracownik Szkoły wyznaczony przez Dyrektora **załącznik nr 6**:

1. egzekwuje zgodnie z prawem przetwarzanie danych osobowych w Szkole w imieniu ADO,
2. prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych – wzór rejestru określa **załącznik nr 7,**
3. ewidencjonuje oświadczenia osób upoważnionych o zaznajomieniu się z zasadami zachowania bezpieczeństwa danych – wzór oświadczenia określa **załącznik nr 8**,
4. prowadzi zestawienie danych osobowych. Kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. – **załącznik nr 9,**
5. określa potrzeby w zakresie stosowanych w Szkole zabezpieczeń, wnioskuje do ADO o zatwierdzenie proponowanych rozwiązań i nadzoruje prawidłowość ich wdrożenia,
6. udziela wyjaśnień i interpretuje zgodność stosowanych rozwiązań w zakresie ochrony danych osobowych z przepisami prawa,
7. bierze udział w podnoszeniu świadomości i kwalifikacji osób przetwarzających dane osobowe w Szkole i zapewnia odpowiedni poziom przeszkolenia w tym zakresie.
8. dba o to aby dane osobowe w formie papierowej były niedostępne dla osób nieupoważnionych. Dokumenty powinny znajdować się w pomieszczeniu zamykanym na klucz do którego dostęp mają tylko osoby posiadające aktualne upoważnienie do przetwarzania danych osobowych.

§ 12.

Na wniosek osoby, której dane dotyczą, Administrator Bezpieczeństwa Informacji jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić, odnośnie do jej danych osobowych, informacji.

§ 13.

Administrator Bezpieczeństwa Informacji może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych osobowych w podmiocie. Podmiot ten, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

§ 14

Administrator Systemu Informatycznego (ASI) – pracownik Szkoły wyznaczony przez Dyrektora **załącznik nr 10**:

1. zarządza bezpieczeństwem przetwarzania danych osobowych w systemie informatycznym zgodnie z wymogami prawa i wskazówkami ABI,
2. doskonali i rozwija metody zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzaniem,
3. przydziela identyfikatory użytkownikom systemu informatycznego oraz zaznajamia ich z procedurami ustalania i zmiany haseł dostępu,
4. nadzoruje prace związane z rozwojem, modyfikacją, serwisowaniem i konserwacją systemu,
5. zapewnia bezpieczeństwo wewnętrznego i zewnętrznego obiegu informacji w sieci i zabezpieczenie łączy zewnętrznych,
6. prowadzi nadzór nad archiwizacją zbiorów danych oraz zabezpiecza elektroniczne nośniki informacji zawierających dane osobowe.

§ 15

Pracownik przetwarzający dane (PPD) – pracownik upoważniony przez ABI:
1. chroni prawo do prywatności osób fizycznych powierzających Szkole swoje dane osobowe poprzez przetwarzanie ich zgodnie z przepisami prawa oraz zasadami określonymi w Polityce bezpieczeństwa i Instrukcji zarządzania systemem informatycznym Szkoły,
2. zapoznaje się zasadami określonymi w Polityce bezpieczeństwa i Instrukcji zarządzania systemem informatycznym Szkoły i składa oświadczenie o znajomości tych przepisów.

§ 16

Zasady udzielania dostępu do danych osobowych
1. Dostęp do danych osobowych może mieć wyłącznie **osoba zaznajomiona** z przepisami ustawy o ochronie danych osobowych oraz zasadami zawartymi w obowiązującej w Szkole Polityce bezpieczeństwa Informacji. Osoba zaznajomiona z zasadami ochrony danych potwierdza to w **pisemnym oświadczeniu**.
2. Dostęp do danych osobowych może mieć wyłącznie osoba posiadająca pisemne oraz imienne **upoważnienie** wydane przez ADO.
3. ABI może wyznaczyć upoważnionych do przetwarzania danych osobowych pracowników Szkoły do nadzoru nad upoważnionymi pracownikami podmiotów zewnętrznych lub innymi upoważnionymi osobami przetwarzającymi dane osobowe w Szkole.

§ 17

Udostępnianie i powierzanie danych osobowych
1. Dane osobowe mogą być udostępnione osobom i podmiotom z mocy przepisów prawa lub jeżeli w sposób wiarygodny uzasadnią one potrzebę ich posiadania, a ich udostępnienie nie naruszy praw i wolności osób, których one dotyczą.

2. Udostępnienie danych może nastąpić **na pisemny wniosek** zawierający następujące elementy:
2.1. adresat wniosku (administrator danych),
2.2. wnioskodawca,
2.3. podstawa prawna (wskazanie potrzeby),
2.4. wskazanie przeznaczenia,
2.5. zakres informacji.
3. Administrator odmawia udostępnienia danych jeżeli spowodowałoby to naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.
4. Powierzenie danych może nastąpić wyłącznie w drodze **pisemnej umowy**, w której osoba przyjmująca dane zobowiązuje się do przestrzegania obowiązujących przepisów ustawy o ochronie danych osobowych. Umowa powinna zawierać informacje o podstawia prawnej powierzenia danych, celu i sposobie ich przetwarzania.
5. Każda osoba fizyczna, której dane przetwarzane są w Szkole, ma prawo zwrócić się z **wnioskiem** o udzielenie informacji związanych z przetwarzaniem tych danych, prawo do kontroli i poprawiania swoich danych osobowych, a także w przypadkach określonych w art. 32 ust 1 pkt 7 i 8 ustawy o ochronie danych osobowych prawo wniesienia umotywowanego żądania zaprzestania przetwarzania danych oraz sprzeciwu wobec przekazywania ich innym podmiotom.
6. Sprawy związane z udzielaniem informacji w tym zakresie prowadzi ABI, udzielając informacji o zawartości zbioru danych na piśmie zgodnie ze wzorem w **załączniku nr 11.**

§ 18

Bezpieczeństwo w przetwarzaniu danych osobowych w formie tradycyjnej

1. Pomieszczenia, w których znajdują się przetwarzane zbiory danych osobowych pozostają zawsze pod bezpośrednim nadzorem upoważnionego do ich przetwarzania pracownika. Opuszczenie pomieszczenia, w których znajdują się zbiory danych osobowych musi być poprzedzone przeniesieniem zbioru danych do odpowiednio zabezpieczonego miejsca. Przy planowanej dłuższej nieobecności pracownika pomieszczenie winno być zamknięte na klucz.
2. Klucze do szaf, w których przechowywane są dane osobowe mają jedynie pracownicy upoważnieni do przetwarzania danych osobowych w zakresie zgodnym z kategorią danych. Dostęp do pokoi poza godzinami pracy szkoły jest kontrolowany za pomocą systemu alarmowego.
3. Korzystanie ze zbiorów danych osobowych przez osoby niezatrudnione w Szkole powinno odbywać się po uzyskaniu **upoważnienia** lub skonsultowane z ABI w przypadku osób upoważnionych do przetwarzania tych danych na podstawie ogólnie obowiązujących przepisów.

§ 19

Bezpieczeństwo w przetwarzaniu danych osobowych w systemach informatycznych
Zasady bezpiecznego użytkowania systemu informatycznego zawarte są w **Instrukcji zarządzania systemem informatycznym**, obligatoryjnej do zapoznania się i stosowania przez wszystkich użytkowników systemu informatycznego szkoły.

§ 20

Analiza ryzyka związanego z przetwarzaniem danych osobowych
1. Identyfikacja zagrożeń

FORMA PRZETWARZANIA DANYCH	ZAGROŻENIA
dane przetwarzane w sposób tradycyjny	• oszustwo, kradzież, sabotaż; • zdarzenia losowe (powódź, pożar); • zaniedbania pracowników szkoły (niedyskrecja, udostępnienie danych osobie nieupoważnionej); • niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania; • pokonanie zabezpieczeń fizycznych; • podsłuchy, podglądy; • ataki terrorystyczne; • brak rejestrowania udostępniania danych; • niewłaściwe miejsce i sposób przechowywania dokumentacji;
dane przetwarzane w systemach informatycznych	• nieprzydzielenie użytkownikom systemu informatycznego identyfikatorów; • niewłaściwa administracja systemem; • niewłaściwa konfiguracja systemu; • zniszczenie (sfałszowanie) kont użytkowników; • kradzież danych kont; • pokonanie zabezpieczeń programowych; • zaniedbania pracowników szkoły (niedyskrecja, udostępnienie danych osobie nieupoważnionej); • niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania; • zdarzenia losowe (powódź, pożar); • niekontrolowane wytwarzanie i wypływ danych poza obszar przetwarzania z pomocą nośników informacji i komputerów przenośnych; • naprawy i konserwacje systemu lub sieci teleinformatycznej wykonywane przez osoby nieuprawnione; • przypadkowe bądź celowe uszkodzenie systemów i aplikacji informatycznych lub sieci; • przypadkowe bądź celowe modyfikowanie systemów i aplikacji informatycznych lub sieci;

	• przypadkowe bądź celowe wprowadzenie zmian do chronionych danych osobowych • brak rejestrowania zdarzeń tworzenia lub modyfikowania danych;

2. Sposób zabezpieczenia danych

FORMA PRZETWARZANIA DANYCH	**STOSOWANE ŚRODKI OCHRONY**
dane przetwarzane w sposób tradycyjny	• przechowywanie danych w pomieszczeniach zamykanych na zamki patentowe; • przechowywanie danych osobowych w szafach zamykanych na klucz; • zastosowanie czujników ruchu informujących wyznaczonych pracowników Szkoły o nieautoryzowanym wejściu do budynku; • przetwarzanie danych wyłącznie przez osoby posiadające upoważnienie nadane przez ABI; • zapoznanie pracowników z zasadami przetwarzania danych osobowych oraz obsługą systemu służącego do ich przetwarzania;
dane przetwarzane w systemach informatycznych	• kontrola dostępu do systemów; • zastosowanie programów antywirusowych i innych regularnie aktualizowanych narzędzi ochrony; • systematyczne tworzenie kopii zapasowych zbiorów danych przetwarzanych w systemach informatycznych; • składowanie nośników wymiennych i nośników kopii zapasowych w odpowiednio zabezpieczonych szafach; • przydzielenie pracownikom indywidualnych kont użytkowników i haseł; • stosowanie indywidualnych haseł logowania do poszczególnych programów; • właściwa budowa hasła;

3. Określenie wielkości ryzyka

Poziom ryzyka naruszenia bezpieczeństwa danych jest niski. Zastosowane techniczne i organizacyjne środki ochrony są adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych osobowych.

4. Identyfikacja obszarów wymagających szczególnych zabezpieczeń

Uwzględniając kategorie przetwarzanych danych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka dla systemów informatycznych, stosuje się wysoki poziom bezpieczeństwa. Administrator Bezpieczeństwa Informacji i Administrator Systemów Informatycznych przeprowadzają **okresową analizę ryzyka dla poszczególnych systemów** i na tej podstawie przedstawiają Administratorowi Danych Osobowych

propozycje dotyczące zastosowania środków technicznych i organizacyjnych, celem zapewnienia właściwej ochrony przetwarzanym danym.

Rozdział II

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

§ 21

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. 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:
   3.1. podaniu identyfikatora użytkownika i właściwego hasła w przypadku obsługi programów SIO, HERMES,
   3.2. podaniu właściwego hasła dostępu do stanowiska komputerowego w przypadku obsługi programów Office,
4. Dla każdego użytkownika systemu informatycznego, który przetwarza dane osobowe, Administrator Systemu Informatycznego 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.

5.1. 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 Systemu Informatycznego.

§ 22

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:
   2.1. Systemu– co 30 dni,
   2.2. Office– zmiana hasła dostępu do stanowiska komputerowego co 40 dni.
3. Hasło oprócz znaków małych i dużych liter winno zawierać znaki alfanumeryczne i specjalne.
4. Hasło powinno być tak zbudowane, aby nie można było go kojarzyć z użytkownikiem komputera – przykładowo dane osobiste: nazwisko, inicjały, imiona, data urodzin własna, dziecka lub małżonka, imię domowego zwierzaka itp.
5. Hasło użytkownika, umożliwiające dostęp do systemu informatycznego, należy utrzymywać w tajemnicy, również po upływie jego ważności.
6. Hasło nie może znajdować się w miejscu widocznym oraz nie mogą mieć do niego dostęp osoby nieuprawnione. Użytkownikowi nie wolno udostępnić swojego loginu i hasła, jak również dopuszczać osoby nieuprawnione do stanowiska roboczego po uwierzytelnieniu w systemie.
7. Raz przypisany login nie może być przydzielony innemu użytkownikowi lub po przerwie (przerwa w zatrudnieniu) w pracy temu samemu pracownikowi.
8. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest do natychmiastowej zmiany hasła.
9. Nowo przyjęty pracownik po przydzieleniu loginu i „hasła jednorazowego" zobowiązany jest do jego zmienienia przy pierwszym logowaniu się do systemu.

§ 23

Procedury rozpoczęcia, zawieszenia i zakończenia pracy

1. Dane osobowe, których administratorem jest Szkoła, 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 wylogowania się z aplikacji i zamknięcia systemu.
6. Monitory stanowisk komputerowych znajdujące się w pomieszczeniach, w których 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 monitor komputera.

7. Użytkownik ma obowiązek wylogowania się w przypadku zakończenia pracy. Stanowisko komputerowe nie może pozostać z włączonym i dostępnym systemem bez nadzoru pracującego na nim pracownika.
8. Wydruki zawierające dane osobowe należy przechowywać w miejscu uniemożliwiającym do nich dostęp osobom postronnym. Wydruki niepotrzebne należy zniszczyć 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 Administrator Systemu Informatycznego w przypadku podejrzenia fizycznej ingerencji w przetwarzane dane osobowe lub użytkowane narzędzia programowe lub sprzętowe. Wówczas, użytkownik jest zobowiązany do natychmiastowego wyłączenia sprzętu.

§ 24

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:
   1.1 urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej,
   1.2 sporządzania kopii zapasowych zbiorów danych (kopie pełne).
2. Za tworzenie kopii bezpieczeństwa systemu informatycznego odpowiedzialny jest Administrator Systemu Informatycznego.
3. Pełne kopie zapasowe zbiorów danych są tworzone co najmniej raz w miesiącu.
4. W przypadku aktualizacji lub dokonywania zmian w systemie należy obowiązkowo wykonać kopię zapasową systemu.
5. W przypadku awarii systemu kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia. Za przeprowadzanie tej procedury odpowiedzialny jest Administrator Systemu Informatycznego.
6. Nośniki danych po ustaniu ich użyteczności należy pozbawić danych lub zniszczyć w sposób uniemożliwiający odczyt danych.

§ 25

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

1. Okresowe kopie zapasowe wykonywane są na płytach CD/DVD lub innych elektronicznych nośnikach informacji. Kopie zapasowe przechowuje się w sposób uniemożliwiający nieuprawnione przejęcie, modyfikacje, uszkodzenie lub zniszczenie.
2. Dostęp do nośników z kopiami zapasowymi systemu oraz kopiami danych osobowych ma wyłącznie Administrator Systemu Informatycznego.
3. Kopie miesięczne przechowuje się przez okres 6 miesięcy. 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 – odpowiedzialny za ich zniszczenie jest użytkownik.
6. Przez zniszczenie nośników informacji rozumie się ich trwałe i nieodwracalne zniszczenie do stanu niedającego możliwości ich rekonstrukcji i odzyskania danych.

§ 26

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 złośliwego oprogramowania, którego celem jest m.in. uzyskanie nieuprawnionego dostępu do systemu informatycznego, konieczna jest ochrona sieci komputerowej i stanowisk komputerowych.
2. Wirusy komputerowe mogą rozpowszechniać się w systemach szkoły poprzez: Internet, nośniki informacji takie jak: dyskietki, płyty CD i DVD, pendrive itp.
3. Przeciwdziałanie zagrożeniom ze strony złośliwego oprogramowania realizowane jest następująco:
   3.1. Komputer z dostępem do Internetu musi być zabezpieczony za pomocą oprogramowania antywirusowego i firewall (zapora).
   3.2. Zainstalowany program antywirusowy powinien być tak skonfigurowany, by co najmniej raz dziennie dokonywał aktualizacji bazy wirusów oraz co najmniej raz w tygodniu dokonywane było automatycznie sprawdzenie komputera pod kątem obecności wirusów komputerowych.
   3.3. Elektroniczne nośniki informacji takie jak dyskietki, dyski przenośne, należy każdorazowo sprawdzać programem antywirusowym przed użyciem, po zainstalowaniu ich w systemie. Czynność powyższą realizuje użytkownik systemu. W przypadku problemów ze sprawdzeniem zewnętrznego nośnika danych użytkownik jest zobowiązany zwrócić się z tym do Administratora Systemu Informatycznego.
   3.4. Komputery i systemy 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).

4. W przypadku, gdy użytkownik stanowiska komputerowego zauważy komunikat oprogramowania zabezpieczającego wskazujący na zaistnienie zagrożenia lub rozpoznanie tego typu zagrożenie, zobowiązany jest zaprzestać jakichkolwiek czynności w systemie i niezwłocznie skontaktować się z Administratorem Systemu Informatycznego.
5. 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 nieznanych nadawców.
6. Zabrania się użytkownikom komputerów wyłączania, blokowania, odinstalowywania programów zabezpieczających komputer (skaner antywirusowy, firewall) przed oprogramowaniem złośliwym oraz nieautoryzowanym dostępem.
7. Zabrania się ściągania na komputery i nośniki danych oprogramowania z Internetu.
8. Zabrania się nieautoryzowanego instalowania własnego oprogramowania na służbowych komputerach.

§ 27

Udostępnianie danych osobowych i sposób odnotowania informacji o udostępnionych danych

Udostępnienie danych instytucjom może odbywać się wyłącznie zgodnie z przepisami prawa (np.: OKE, CKE, Urząd Gminy i inne).

§ 28

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

1. Przeglądy i konserwacje systemu oraz zbiorów danych wykonuje na bieżąco Administrator Systemu Informatycznego.
2. Administrator Systemu Informatycznego okresowo sprawdza możliwość odtworzenia danych z kopii zapasowej.
3. Umowy dotyczące instalacji i konserwacji sprzętu należy zawierać z podmiotami, które gwarantują wykonanie prawidłowo usług.
4. Naprawy sprzętu należy zlecać podmiotom, które gwarantują wykonanie prawidłowo usług. Naprawa sprzętu, na którym mogą znajdować się dane osobowe, powinna odbywać się pod nadzorem Administrator Systemu Informatycznego w miejscu jego użytkowania.
5. W przypadku konieczności naprawy w serwisie, sprzęt komputerowy przed oddaniem do serwisu powinien być odpowiednio przygotowany. Dane należy zarchiwizować na nośniki informacji, a dyski twarde,

bezwzględnie wymontować na czas naprawy lub trwale usunąć z nich dane.

6. Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jego lokalizacji może być dokonana tylko za wiedzą i zgodą Administrator Systemu Informatycznego.

§ 29

Niszczenie wydruków i nośników danych

1. Wszelkie wydruki z systemów informatycznych zawierające dane osobowe przechowywane są w miejscu uniemożliwiającym ich odczyt przez osoby nieuprawnione, w zamkniętych szafach lub pomieszczeniach i po upływie ich przydatności są niszczone przy użyciu niszczarek / w sposób uniemożliwiający ich odczytanie (pocięte w poprzeczne paski)
2. Niszczenie zapisów na nośnikach danych powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika.
3. Uszkodzone nośniki danych przed ich wyrzuceniem należy fizycznie zniszczyć w niszczarce.

Rozdział III

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA DANYCH

§ 29

Istota naruszenia danych osobowych

1. Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:
   1.1. nieautoryzowany dostęp do danych,
   1.2. nieautoryzowane modyfikacje lub zniszczenie danych,
   1.3. udostępnienie danych nieautoryzowanym podmiotom,
   1.4. nielegalne ujawnienie danych,
   1.5. pozyskiwanie danych z nielegalnych źródeł.

§ 30

Postępowanie w przypadku naruszenia danych osobowych

1. Każdy pracownik Szkoły, który stwierdzi fakt naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe, bądź posiada informację mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany niezwłocznie zgłosić to ASI, ABI lub ADO.
2. Każdy pracownik Szkoły, który stwierdzi fakt naruszenia bezpieczeństwa danych ma obowiązek podjąć czynności niezbędne do powstrzymania

skutków naruszenie ochrony oraz ustalić przyczynę i sprawcę naruszenia ochrony.

3. W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ABI.
4. ABI podejmuje następujące kroki:
   4.1. zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości pracy Szkoły,
   4.2. może zażądać dokładnej relacji z zaistniałego naruszenia bezpieczeństwa danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,
   4.3. rozważa celowość i potrzebę powiadamiania o zaistniałym naruszeniu ADO,
   4.4. nawiązuje kontakt ze specjalistami spoza urzędu (jeśli zachodzi taka potrzeba).
5. ABI dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych osobowych sporządzając raport wg wzoru stanowiącego **załącznik nr 12** i przekazuje go ADO.
6. ABI zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych).

§ 31

Sankcje karne

1. Wobec osoby, która w przypadku naruszenia ochrony danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne.
2. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą o ochronie danych osobowych.

§ 32

Ustalenia końcowe

1. Osobom korzystającym z systemu informatycznego, w którym przetwarzane są dane osobowe w szkole zabrania się:
   1.1 ujawniania loginu i hasła współpracownikom i osobom z zewnątrz,
   1.2 pozostawiania haseł w miejscach widocznych dla innych osób,
   1.3 udostępniania stanowisk pracy wraz z danymi osobowymi osobom nieuprawnionym,
   1.4 udostępniania osobom nieuprawnionym programów komputerowych zainstalowanych w systemie,

1.5 używania oprogramowania w innym zakresie niż pozwala na to umowa licencyjna,
1.6 przenoszenia programów komputerowych, dysków twardych z jednego stanowiska na inne,
1.7 kopiowania danych na nośniki informacji, kopiowania na inne systemy celem wynoszenia ich poza szkołę,
1.8 samowolnego instalowania i używania jakichkolwiek programów komputerowych, w tym również programów do użytku prywatnego; programy komputerowe instalowane są przez Administratora Bezpieczeństwa Informacji,
1.9 używania nośników danych udostępnionych przez osoby postronne,
1.10 przesyłania dokumentów i danych z wykorzystaniem konta pocztowego prywatnego,
1.11 otwierania załączników i wiadomości poczty elektronicznej od nieznanych i nieznanych nadawców,
1.12 używania nośników danych prywatnych, niesprawdzonych, niewiadomego pochodzenia. W sytuacji, gdy zaistniała konieczności użycia niesprawdzonych przenośnych nośników danych, należy przeskanować je programem antywirusowymi, a w razie jakiś ostrzeżeń wyświetlonych przez program antywirusowy, zgłosić to Administratorowi Bezpieczeństwa Informacji.

2. Użytkownikowi nie wolno:

2.1. wyrzucać dokumentów zawierających dane osobowe (dokumenty zawierające dane osobowe mogą być niszczone tylko w niszczarce),
2.2. pozostawiać dokumentów, kopii dokumentów zawierających dane osobowe w drukarkach, kserokopiarkach,
2.3. pozostawiać kluczy w drzwiach, szafach, biurkach, pozostawiać otwartych pomieszczeń, w których przetwarza się dane osobowe,
2.4. pozostawiać bez nadzoru osoby trzecie przebywające w pomieszczeniach szkoły, w których przetwarzane są dane osobowe,
2.5. pozostawiać dokumentów na biurku po zakończonej pracy, pozostawiać otwartych dokumentów na ekranie monitora bez blokady konsoli,
2.6. ignorować nieznanych osób z zewnątrz, poruszających się w obszarze przetwarzania danych osobowych,
2.7. przekazywać informacji będącymi danymi osobowymi osobom nieupoważnionym.

3. **Użytkownik zobowiązany jest do:**

3.1. posługiwania się własnym loginem i hasłem w celu uzyskania dostępu do systemów informatycznych,
3.2. tworzenia haseł trudnych do odgadnięcia dla innych,
3.3. używanie konta służbowego tylko w celach służbowych,
3.4. niezakańczania procesu skanowania przez program antywirusowy na komputerze,
3.5. wykonywania kopii zapasowych danych przetwarzanych na stanowisku komputerowym (pliki MS Office),
3.6. zabezpieczenia sprzętu komputerowego przenośnego (laptopy) przed kradzieżą lub nieuprawnionym dostępem do danych.

4. Wszelkie przypadki naruszenia niniejszej Instrukcji należy zgłaszać Administratorowi Bezpieczeństwa Informacji, Administrator Systemu Informatycznego lub bezpośredniemu przełożonemu.
5. Zalecenia w zakresie przetwarzania danych osobowych sposobem tradycyjnym
   5.1 Miejscem tworzenia, uzupełniania i przechowywania dokumentacji dotyczącej przetwarzania danych osobowych sposobem tradycyjnym, są pomieszczenia w szkole: sekretariat, pokój nauczycielski, gabinet dyrektora, pomieszczenie intendenta, pedagoga, biblioteka, świetlica.
   5.2 Osoby prowadzące dokumentację zobowiązane są do zachowania tajemnicy służbowej.
   5.3 Dokumentacji, o której mowa w punkcie 5.1. nie można wynosić poza teren szkoły.
   5.4 Dokumentację, o której mowa w punkcie 5.1. archiwizuje się zgodnie z Instrukcją kancelaryjną.
   5.5 Osoby prowadzące dokumentację zobowiązane są do niezwłocznego poinformowania Pełnomocnika dyrektora ds. przetwarzania danych osobowych o podejrzeniu dostępu do dokumentacji przez osoby nieupoważnione.

Załączniki

Załącznik nr 1 – Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe
Załącznik nr 2 - Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych
Załącznik nr 3 - Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami
Załącznik nr 4 - Upoważnienie do przetwarzania danych osobowych
Załącznik nr 5 – Odwołanie upoważnienia do przetwarzania danych osobowych
Załącznik nr 6 – Upoważnienie dla ABI
Załącznik nr 7 – Rejestr osób upoważnionych do przetwarzania danych osobowych
Załącznik nr 8 – Oświadczenie o zachowaniu poufności i zapoznaniu się z przepisami
Załącznik nr 9 – Zestawienie danych osobowych z informacją kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane
Załącznik nr 10 – Upoważnienie dla ASI
Załącznik nr 11 – Informacja o zawartości zbioru danych osobowych
Załącznik nr 12 – Raportu z naruszenia bezpieczeństwa danych osobowych