Załącznik
do Zarządzenia Dyrektora ZSOiZ
w Przeworsku z dnia 30.12.2016r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

Zespołu Szkół Ogólnokształcących i Zawodowych im. Króla Władysława Jagiełły w Przeworsku

Przeworsk 2016

Spis treści

Podstawa prawna

1. Konstytucja Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997r. (Dz. U. Nr 78, poz. 483 z późn. zm.) – art. 47 i 51;
2. Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2016r., poz.922).

Podstawowe pojęcia

Szkoła – w tym dokumencie jest rozumiana jako Zespół Szkół Ogólnokształcących i Zawodowych im. Króla Władysława Jagiełły w Przeworsku, zlokalizowana przy ulicy Szkolnej 6,

Polityka – w tym dokumencie jest rozumiana jako „Polityka Bezpieczeństwa Informacji" obowiązująca w Zespole Szkół Ogólnokształcących i Zawodowych im. Króla Władysława Jagiełły w Przeworsku;

Instrukcja – w tym dokumencie rozumiana jako „Instrukcja Zarządzania Systemem Informatycznym" służącym do przetwarzania danych osobowych w Zespole Szkół Ogólnokształcących i Zawodowych im. Króla Władysława Jagiełły w Przeworsku;

Administrator Danych Osobowych (ADO) – rozumie się przez to Dyrektora Zespołu Szkół Ogólnokształcących i Zawodowych im. Króla Władysława Jagiełły w Przeworsku;

Administrator Systemu Informatycznego (ASI) – pracownik odpowiedzialny za funkcjonowanie systemu teleinformatycznego oraz stosowanie technicznych i organizacyjnych środków ochrony stosowanych w tym systemie;

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;

Identyfikator użytkownika – jest to ciąg znaków jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

Dane osobowe – w rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;

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 systemie informatycznym;

Zbiór danych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów;

System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych w systemie informatycznym;

Wysoki poziom bezpieczeństwa – musi występować wtedy, gdy przynajmniej jedno urządzenie systemu informatycznego służące do przetwarzania danych osobowych połączone jest z siecią publiczną;

Sieć publiczna – sieć telekomunikacyjna wykorzystywana głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych w rozumieniu ustawy z dnia 16 lipa 2004r. – Prawo telekomunikacyjne (Dz. U. 2016r., poz. 1489).

1. POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1.1. Wykaz miejsc, w których przetwarzane są dane osobowe

L.P.	Adres - Budynek	Pomieszczenia	Zabezpieczenie
	37-200 Przeworsk ul. Szkolna 6	gabinet dyrektora	Kluczami dysponuje dyrektor i pracownicy sekretariatu
		gabinet wicedyrektora	Kluczami dysponuje wicedyrektor
		sekretariat	Kluczami dysponuje dyrektor i pracownicy sekretariatu
		księgowość	Kluczami dysponują pracownicy księgowości
		gabinet pedagoga	Kluczami dysponuje pedagog
		gabinet pielęgniarki	Kluczami dysponuje pielęgniarka, klucze dostępne w sekretariacie
		biblioteka	Kluczami dysponuje bibliotekarz, klucze dostępne u pracowników obsługi
		pokój nauczycielski	Kluczami dysponują nauczyciele, klucze dostępne u pracowników obsługi
		sale lekcyjne	Klucze dostępne w pokoju nauczycielskim oraz u pracowników obsługi
		pokój intendenta	Kluczami dysponuje intendent
		archiwum	Klucze dostępne w sekretariacie
		Zaplecze techniczne	Kluczami dysponuje dyrektor i pracownicy sekretariatu

1.2. Wykaz zbiorów danych osobowych

Numer zbioru	Nazwa zbioru - opis	Struktura zbioru	Program
1	Podanie o przyjęcie ucznia do szkoły – informacje dot. ucznia przyjmowanego do szkoły	Imiona i nazwisko, imiona i nazwiska rodziców/prawnych opiekunów, data urodzenia, pesel, adres zamieszkania, wizerunek ucznia, telefon	
2	Księga uczniów – zbiór danych o uczniach	Imiona i nazwisko, imiona i nazwiska rodziców/prawnych opiekunów, data urodzenia, pesel, adres zamieszkania ucznia oraz rodziców/prawnych opiekunów. Przyjęcie do szkoły: data, klasa, zawód. Wypisanie ze szkoły: data, klasa, powód. Data: wydania dokumentów, ukończenia szkoły, numer wydanego świadectwa	Sekretariat UONET+
3	Dziennik lekcyjny, dziennik zajęć rewalidacyjnych, nauczania indywidualnego, pozalekcyjnych – dokumentacja przebiegu nauczania w danym roku szkolnym	Imię i nazwisko, data i miejsce urodzenia, pesel, adres zamieszkania, imiona i nazwiska rodziców i adresy ich zamieszkania, przebieg nauki, wyniki nauki	Dziennik UONET+
4	Arkusz ocen – dokumentacja wyników nauczania ucznia w poszczególnych latach	Imiona i nazwisko, data i miejsce urodzenia, pesel, adres zamieszkania, imiona i nazwiska rodziców i adresy ich zamieszkania, przebieg nauki, wyniki nauki, data przyjęcia do szkoły, nr z księgi uczniów	
5	Księga arkuszy ocen – zbór arkuszy ocen uczniów którzy ukończyli lub opuścili szkołę w danym roku szkolnym	Imiona i nazwisko, data i miejsce urodzenia, pesel, adres zamieszkania, imiona i nazwiska rodziców i adresy ich zamieszkania, przebieg nauki, wyniki nauki, data przyjęcia do szkoły, nr z księgi uczniów	
6	Rejestr wydanych świadectw	Imię i nazwisko ucznia, klasa, pesel, nr świadectwa, data otrzymania świadectwa, podpis	
7	Rejestr wydanych zaświadczeń o wynikach egzaminu gimnazjalnego, maturalnego, z klasyfikacji	Imiona, nazwisko, pesel, nr zaświadczenia, data wydania, podpis	
8	Ewidencja uczniów przystępujących do egzaminów zewnętrznych – Okręgowa Komisja Egzaminacyjna w Krakowie	Imiona i nazwisko, data urodzenia i miejsce, pesel, płeć, mniejszość narodowa, telefon, dostosowanie warunków egzaminu	Obieg - OKE
9	Dziennik pedagoga szkolnego – dziennik zawiera informacje o uczniach zakwalifikowanych do różnych form pomocy	Imię i nazwisko, klasa, forma pomocy	
10	Dokumentacja pedagoga – dokumentacja badań i czynności uzupełniających prowadzonych przez pedagoga w tym orzeczenia i opinie Poradni Psychologiczno-Pedagogicznej	Imię i nazwisko, data urodzenia i miejsce, adres zamieszkania, stan zdrowia	
11	Deklaracje uczęszczania na religię, etykę; sprzeciw od zajęć z	Imię i nazwisko rodzica/prawnego opiekuna, adres zamieszkania, imię i nazwisko ucznia,	

	wychowania w rodzinie	przynależność wyznaniowa	
12	Świadczenia dla uczniów – stypendia, wyprawki szkolne, dożywianie	Imię i nazwisko rodzica, data urodzenia, adres zamieszkania, dochody, nr konta bankowego, imię i nazwisko ucznia, adres zamieszkania	
13	Biblioteka	Imię i nazwisko ucznia, pesel, data i miejsce urodzenia, adres, dane o wypożyczeniach	MOL VULCAN
14	Decyzje dyrektora szkoły – zwolnienie z zajęć w-f, decyzja w sprawie nauczania indywidualnego itp.	Imię i nazwisko rodzica/prawnego opiekuna, adres zamieszkania, imię i nazwisko ucznia	
15	Lista uczestników wycieczek	Imię i nazwisko, pesel, telefon	
16	Ewidencja zasobów szkoły System Informacji Oświatowej – Zbiór zawiera informacje o nauczycielach i uczniach	Pesel, miejsce zatrudnienia, zawód, wykształcenie, wynagrodzenie, imię i nazwisko ucznia, obywatelstwo	SIO
17	Arkusz organizacyjny szkoły	Imię i nazwisko, wykształcenie, pensum	
18	Protokoły Rady Pedagogicznej	Imię i nazwisko nauczycieli, imię i nazwisko uczniów	
19	Awans zawodowy	Imię i nazwisko, data urodzenia, adres zamieszkania, przebieg zatrudnienia, wykształcenie	
20	Książka korespondencyjna	Imię i nazwisko, adres zamieszkania	
21	Akta osobowe pracowników	Imię i nazwisko, nazwisko rodowe, imiona rodziców, data urodzenia, miejsce urodzenia, pesel, NIP, adres zameldowania, obywatelstwo, numer i seria dowodu osobistego, imiona i nazwiska, data urodzenia dzieci pracownika, imię i nazwisko, adres i telefon osoby, którą należy powiadomić o wypadku pracownika, w przypadku mężczyzn dane dotyczące powszechnego obowiązku obrony, wykształcenie, dotychczasowe zatrudnienie	
22	Zakładowy Fundusz Świadczeń Socjalnych	Imię i nazwisko, data urodzenia, pesel, adres zamieszkania, numer i seria dowodu osobistego poręczyciela i pożyczkobiorcy, imiona i nazwiska, data urodzenia dzieci pracownika, nr konta bankowego, oświadczenia o przychodach	
23	Płace pracowników	Imię i nazwisko, data urodzenia, pesel, miejsce zamieszkania, stopień awansu, składniki wynagrodzeń i potrąceń, okresy zwolnienia	Płace VULCAN
24	Skierowania na badania okresowe	Imię i nazwisko, data urodzenia, pesel, miejsce zamieszkania, stanowisko	
25	Ewidencja urlopów, karty czasu pracy	Imię i nazwisko, stanowisko, wymiar urlopu, wykorzystanie urlopów	
26	Kartoteki wydanej odzieży ochronnej	Imię i nazwisko, stanowisko	
27	Ewidencja środków czystości i art. biurowych	Imię i nazwisko, podpis	
28	Deklaracje ubezpieczeniowe pracowników	Imię i nazwisko, nazwisko rodowe, imiona rodziców, data urodzenia, miejsce urodzenia, pesel, adres zamieszkania, obywatelstwo, numer i seria dowodu osobistego, imię i nazwisko, adres i telefon osoby upoważnionej do odbioru świadczenia w razie śmierci pracownika, wysokość składki i ewentualnie otrzymanych świadczeń	

29	Deklaracje i kartoteki ZUS pracowników	Imię i nazwisko, nazwisko rodowe, imiona rodziców, data urodzenia, miejsce urodzenia, pesel, adres zamieszkania, obywatelstwo, imiona i nazwiska, data urodzenia dzieci pracownika. wymiar czasu pracy	e-płatnik
30	Deklaracje podatkowe pracowników	Imiona i nazwisko, imiona rodziców, data i miejsce urodzenia, pesel adres zamieszkania	Płace VULCAN
31	Deklaracje podatkowe uczniów	Imiona i nazwisko, data i miejsce urodzenia, pesel adres zamieszkania	
32	Rejestr zaświadczeń wydanych pracownikom szkoły	Imię i nazwisko, imiona rodziców, dat5a urodzenia, miejsce urodzenia, pesel, adres zamieszkania, wysokość wynagrodzenia, okres zatrudnienia	Płace VULCAN
33	Rejestr zaświadczeń wydanych uczniom	Imię i nazwisko, data urodzenia, klasa	
34	Księga druków ścisłego zarachowania	Imię i nazwisko	
35	Przelewy i faktury	Nazwiska, imiona, adresy zamieszkania, nazwa firmy, nr konta bankowego kontrahentów, NIP, REGON	e-bank
36	Rejestr delegacji służbowych	Imię i nazwisko, stanowisko	
37	Zbiór upoważnień	Imię i nazwisko, stanowisko, zakres upoważnienia	

1.3. System przetwarzania danych osobowych

W skład systemu wchodzą:

- Dokumentacja papierowa (korespondencja, dokumenty pracowników i uczniów);
- Wydruki komputerowe;
- Urządzenia i oprogramowanie komputerowe służące do przetwarzania informacji;
- Procedury przetwarzania danych w tym systemie, w tym procedury awaryjne.

Sposób przepływu danych pomiędzy poszczególnymi systemami:

- Sekretariat UONET+ → Dziennik UONET+
- Płace Vulcan → Księgowość Vulcan
- Płace Vulcan → e-płatnik; platforma oświatowa
- Księgowość Vulcan → Bestia sprawozdania

Sposób przekazywania danych : manualny

Przetwarzanie danych osobowych w systemie informatycznym odbywa się przy zachowaniu wysokiego poziomu bezpieczeństwa.

1.4. Środki techniczne i organizacyjne stosowane w przetwarzaniu danych

1.4.1. Cele i zasady funkcjonowania polityki bezpieczeństwa

Realizujący *Politykę Bezpieczeństwa Informacji* zapewnia ich:

- Poufność – informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, podmiotom i procesom;

- Integralność – dane nie zostają zmienione lub zniszczone w sposób nieautoryzowany;
- Dostępność – istnieje możliwość wykorzystania ich na żądanie w założonym czasie, przez autoryzowany podmiot;
- Rozliczalność – możliwość jednoznacznego przypisania działań poszczególnym osobom;
- Autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest taka jak deklarowana;
- Niezaprzeczalność – uczestnictwo w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne;
- Niezawodność – zamierzone zachowania i skutki są spójne.

Polityka bezpieczeństwa informacji w szkole ma na celu zredukowanie możliwości wystąpienia negatywnych konsekwencji naruszeń w tym zakresie, tj.:

- Naruszeń danych osobowych rozumianych jako prywatne dobro powierzone szkole,
- Naruszeń przepisów prawa oraz innych regulacji,
- Utraty lub obniżenia reputacji szkoły,
- Strat finansowych ponoszonych w wyniku nałożonych kar,
- Zakłóceń organizacji pracy spowodowanych nieprawidłowym działaniem systemów.

Realizując *Politykę bezpieczeństwa informacji* 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:

- Przetwarzane zgodnie z prawem,
- Zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
- Merytorycznie poprawne i adekwatne w stosunku do celu w jakim są przetwarzane,
- Przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

1.4.2. 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.

Administrator danych osobowych (ADO) – Dyrektor szkoły:

- 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,
- Decyduje o zakresie, celach oraz metodach przetwarzania i ochrony danych osobowych,
- Wydaje/odwołuje upoważnienie do przetwarzania i ochrony danych osobowych określając w nich zakres i termin ważności – wzór upoważnienie określa załącznik nr 1 do Polityki Bezpieczeństwa Informacji,
- Odpowiada za zgodne z prawem przetwarzanie danych osobowych w szkole

- Egzekwuje zgodnie z prawem przetwarzanie danych osobowych w szkole,
- Prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych – wzór ewidencji określa Załącznik nr 2 do *Polityki bezpieczeństwa informacji*,
- ewidencjonuje oświadczenia osób upoważnionych, po zaznajomieniu się z zasadami zachowania bezpieczeństwa danych – wzór oświadczenia określa Załącznik nr 3 do *Polityki bezpieczeństwa informacji*, wzór ewidencji oświadczeń określa załącznik nr 4 do *Polityki bezpieczeństwa informacji*, ewidencjonuje oświadczenia o odwołaniu upoważnienia do przetwarzania danych osobowych – wzór odwołania określa załącznik nr 5 do *Polityki bezpieczeństwa informacji*,
- Udziela wyjaśnień i interpretuje zgodność stosowanych rozwiązań w zakresie ochrony danych osobowych z przepisami prawa,
- Bierze udział w podnoszeniu świadomości i kwalifikacji osób przetwarzających dane osobowe w szkole i zapewnia odpowiedni poziom przeszkolenia w tym zakresie.

Administrator systemu informatycznego (ASI) – pracownik szkoły wyznaczony przez dyrektora:

- Zarządza bezpieczeństwem przetwarzania danych osobowych w systemie informatycznym zgodnie z wymogami prawa i wskazówkami ADO
- Doskonali i rozwija metody zabezpieczania danych przed zagrożeniami związanymi z ich przetwarzaniem,
- Nadzoruje prace związane z rozwojem, modyfikacją, serwisowaniem i konserwacją systemu,
- Zapewnia bezpieczeństwo wewnętrznego i zewnętrznego obiegu informacji w sieci i zabezpieczenie łączy zewnętrznych,
- Prowadzi nadzór nad archiwizacją zbiorów danych oraz zabezpiecza elektroniczne nośniki informacji zawierających dane osobowe.

Pracownik przetwarzający dane (PPD) – pracownik upoważniony przez ADO

- Chroni prawo do prywatności osób fizycznych powierzających szkole swoje dane osobowe poprzez przetwarzanie ich zgodnie z przepisami prawa oraz zasadami określonymi w *Polityce bezpieczeństwa informacji* szkoły,
- Zapoznaje się z zasadami określonymi w *Polityce Bezpieczeństwa Informacji* szkoły i składa oświadczenie o znajomości tych przepisów.

1.4.3. Zasady udzielania dostępu do danych osobowych

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.

Dostęp do danych osobowych może mieć wyłącznie osoba posiadająca pisemne oraz imienne upoważnienie wydane przez ADO.

ADO może wyznaczyć upoważnionych do przetwarzania danych osobowych pracowników szkoły nadzoru nad upoważnionymi pracownikami podmiotów zewnętrznych lub innymi upoważnionymi osobami przetwarzającymi dane osobowe w szkole.

1.4.4. Udostępnianie i powierzanie danych osobowych

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.

Udostępnianie danych może nastąpić na pisemny wniosek zawierający następujące elementy:

- Adresat wniosku (administrator danych)
- Wnioskodawca
- Podstawa prawna (wskazanie potrzeby)
- Wskazanie przeznaczenia
- Zakres informacji.

Administrator odmawia udostępnienia danych, jeżeli spowodowałoby to naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.

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 podstawie prawnej powierzenia danych, celu i sposobie ich przetwarzania.

Każda osoba fizyczna, której dane przetwarzane są w szkole, ma prawo zwrócić się z wnioskiem o udzielenie informacji związanych z przetwarzaniem tych danych, ma 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 ma prawo wniesienia umotywowanego żądania zaprzestania przetwarzania danych oraz wniesienia sprzeciwu wobec przekazywania ich innym podmiotom.

Sprawy związane z udzielaniem informacji w tym zakresie prowadzi ADO, udzielając informacji o zawartości zbioru danych na piśmie zgodnie ze wzorem w załączniku nr 6 do *Polityki bezpieczeństwa informacji*.

1.4.5. Bezpieczeństwo w przetwarzaniu danych osobowych w formie tradycyjnej

Pomieszczenia, w których znajdują się przetwarzane zbiory danych osobowych pozostają zawsze pod bezpośrednim nadzorem upoważnionego do ich przetwarzania pracownika. Opuszczenie pomieszczenia, w którym 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.

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 monitoringu.

Korzystanie ze zbiorów danych osobowych przez osoby niezatrudnione w szkole powinno odbywać się po uzyskaniu upoważnienia lub skonsultowane z ADO w przypadku osób upoważnionych do przetwarzania tych danych na podstawie ogólnie obowiązujących przepisów.

1.4.6. 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.

1.5. Analiza ryzyka związanego z przetwarzaniem danych osobowych

1.5.1. Identyfikacja zagrożeń

Forma przetwarzania danych	zagrożenia
Dane przetwarzane w sposób tradycyjny	• oszustwo, kradzież, sabotaż; • zdarzenia losowe (powódź, pożar) • zaniedbania pracowników szkoły (niedyskrecja, udostępnianie 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;

1.5.2. Sposób zabezpieczenia danych

Forma przetwarzania danych	Stosowane środki ochrony
Dane przetwarzane w sposób tradycyjny	• przechowywanie danych w pomieszczeniach zamykanych; • przechowywanie danych osobowych w szafach zamykanych na klucz; • przetwarzanie danych wyłącznie przez osoby posiadające upoważnienie nadane przez ADO; • 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;

1.5.3. 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.

1.5.4. Identyfikacja obszarów wymagających szczególnych zabezpieczeń

Uwzględniając kategorie przetwarzania danych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka dla systemów informatycznych, stosuje się wysoki poziom bezpieczeństwa. Administrator danych osobowych i administrator systemów informatycznych przeprowadzają okresową analizę ryzyka dla poszczególnych systemów i na tej podstawie podejmują decyzje dotyczące zastosowania środków technicznych i organizacyjnych celem zapewnienia właściwej ochrony przetwarzanym danym.

2. INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

2.1. Postanowienia ogólne

Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. 2016r., poz. 922) oraz rozporządzenie ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004r. nr 100, poz. 1024) nakłada na administratora danych osobowych następujące obowiązki:

- Zapewnienie bezpieczeństwa i poufności danych, w tym zabezpieczenie ich przed ujawnieniem,
- Zabezpieczenie danych przed nieuprawnionym dostępem,
- Zabezpieczenie danych przed udostępnieniem osobom nieupoważnionym (nieuprawnionym) pozyskaniem,
- Zabezpieczenie przed utratą danych,
- Zabezpieczenie przed uszkodzeniem lub zniszczeniem danych oraz przed ich nielegalną modyfikacją.

Ochronie podlegają dane osobowe niezależnie od formy przechowywania, sprzęt komputerowy, systemy operacyjne i informatyczne oraz pomieszczenia, w których odbywa się proces przetwarzania. Instrukcja określa ramowe zasady właściwego zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i system informatyczny, odpowiednie do zagrożeń i kategorii danych objętych ochroną.

2.2. Przeznaczenie

Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Zespole Szkół Ogólnokształcących i Zawodowych im. Króla Władysława Jagiełły w Przeworsku, zwana dalej instrukcją, określa sposób zarządzania oraz zasady administrowania systemem informatycznym służącym do przetwarzania danych osobowych.

Niniejsza instrukcja zarządzania systemem informatycznym określa:

- Opisanie poziomu bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym
- Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym
- Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

- Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu
- Metody i częstotliwość tworzenia kopii awaryjnych
- Metody i częstotliwość sprawdzania obecności wirusów komputerowych oraz metody ich usuwania
- Sposób, miejsce i okres przechowywania:
  - elektronicznych nośników informacji zawierających dane osobowe
  - kopii zapasowych
- Sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych
- Sposób postepowania w zakresie komunikacji w sieci komputerowej
- Procedury wykonywania przeglądów i konserwacji systemu oraz nośników informacji służących do przetwarzania danych.

2.3. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

Upoważnienia do przetwarzania danych osobowych nadawane są w związku z wykonywaniem przez upoważnioną osobę obowiązków lub zadań związanych z przetwarzaniem danych osobowych. Upoważnienie nadaje i odwołuje administrator danych. Upoważnienie i jego odwołanie sporządzane są na piśmie, w dwóch jednobrzmiących egzemplarzach – jeden przeznaczony jest dla osoby, której nadano lub odebrano upoważnienie, drugi - dla administratora danych. Wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 1 do *Polityki bezpieczeństwa informacji*. Wzór odwołania upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 5 do *Polityki Bezpieczeństwa Informacji*. Upoważnienia nie sporządza się dla administratora danych. Upoważnienia nadane przed dniem wprowadzenia instrukcji pozostają w mocy.

Upoważnienia do przetwarzania danych osobowych rejestrowane są w ewidencji osób upoważnionych do przetwarzania danych osobowych. Wzór ewidencji stanowi załącznik nr 2 do *Polityki bezpieczeństwa informacji*. Ewidencje prowadzi administrator danych.

2.4. Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

Środki uwierzytelniania dostępu do systemu informatycznego służącego do przetwarzania danych osobowych to identyfikator użytkownika i hasło dostępu. Każdy identyfikator użytkownika zabezpieczony jest hasłem. W Zespole Szkół Ogólnokształcących i Zawodowych im. Króla Władysława Jagiełły w Przeworsku obowiązują następujące zasady tworzenia hasła:

- Hasło nie może składać się z żadnych danych personalnych (imienia, nazwiska, adresu zamieszkania użytkownika lub najbliższych osób) lub ich fragmentów
- Hasło musi składać się z co najmniej 6 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne

- Hasło nie może składać się z identycznych znaków lub ciągu znaków z klawiatury
- Hasło nie może być jednakowe z identyfikatorem użytkownika
- Hasło musi być unikalne, tj. takie, które nie było poprzednio stosowane przez użytkownika.

Hasło, w trakcie wpisywania, nie może być wyświetlane na ekranie. Użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności.

Hasło musi być zmieniane nie rzadziej niż co 30 dni. Jeżeli zmiana hasła nie jest możliwa w wymaganym czasie, należy jej dokonać w najbliższym możliwym terminie.

W przypadku złamania poufności hasła użytkownik zobowiązany jest niezwłocznie zmienić hasło i poinformować o tym fakcie administratora danych.

Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego służącego do przetwarzania danych osobowych nie powinien być przydzielany innej osobie. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych osobowych, należy niezwłocznie zablokować w systemie informatycznym służącym do przetwarzania danych osobowych oraz unieważnić przypisane mu hasło.

2.5. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu informatycznego służącego do przetwarzania danych osobowych

Przed rozpoczęciem przetwarzania danych osobowych użytkownik powinien sprawdzić, czy nie ma oznak fizycznego naruszenia zabezpieczeń. W przypadku wystąpienia jakichkolwiek nieprawidłowości należy powiadomić administratora danych.

Przystępując do pracy w systemie informatycznym, służącym do przetwarzania danych osobowych, użytkownik jest zobowiązany wprowadzić swój identyfikator oraz hasło dostępu.

Zabrania się wykonywania jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych z wykorzystaniem identyfikatora i hasła dostępu innego użytkownika.

W przypadku czasowego opuszczenia stanowiska pracy użytkownik musi wylogować się z systemu informatycznego służącego do przetwarzania danych.

Zakończenie pracy w systemie służącym do przetwarzania danych osobowych powinno być poprzedzone sporządzeniem, w miarę potrzeb, kopii zapasowej danych oraz zabezpieczeniem przed nieuprawnionym dostępem dodatkowych nośników danych, płyty CD, pendrive i innych zawierających dane osobowe. Zakończenie pracy w systemie informatycznym służącym do przetwarzania danych osobowych następuje poprzez wylogowanie się z tego systemu.

2.6. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

Za sporządzanie kopii zapasowych zbiorów danych odpowiedzialny jest użytkownik systemu informatycznego służącego do przetwarzania danych osobowych. Kopie awaryjne może tworzyć jedynie administrator danych. Kopie zapasowe powinny być kontrolowane przez administratora danych, w szczególności pod kątem prawidłowości ich wykonania poprzez częściowe lub całkowite odtworzenie na wydzielonym sprzęcie komputerowym.

Nośniki informatyczne zawierające dane osobowe lub kopie systemów informatycznych służących do przetwarzania danych osobowych są przechowywane w sposób uniemożliwiający ich utratę, uszkodzenie lub dostęp osób nieuprawnionych.

W przypadku likwidacji nośników informatycznych zawierających dane osobowe lub kopie zapasowe systemów informatycznych służących do przetwarzania danych osobowych należy przed ich likwidacją usunąć dane osobowe lub uszkodzić je w sposób uniemożliwiający odczyt danych osobowych.

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

Nie należy przechowywać zbędnych nośników informacji zawierających dane osobowe oraz kopii zapasowych, a także wydruków i innych dokumentów zawierających dane osobowe. Po upływie okresu ich użyteczności lub przechowywania dane osobowe powinny zostać skasowane lub zniszczone tak, aby nie było możliwe ich odczytanie.

Elektroniczne nośniki informacji zawierające dane osobowe oraz kopie zapasowe nie mogą być wynoszone poza pomieszczenia stanowiące obszar przetwarzania danych osobowych, określony w *Polityce bezpieczeństwa informacji*.

Elektroniczne nośniki informacji zawierające dane osobowe oraz kopie zapasowe, a także wydruki i inne dokumenty zawierające dane osobowe przechowywane są w zamykanych szafach w pomieszczeniach stanowiących obszar przetwarzania danych osobowych, określony w *Polityce bezpieczeństwa informacji* w sposób zabezpieczający je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem i zniszczeniem.

W przypadku uszkodzenia lub zużycia nośnika informacji, zawierającego dane osobowe, należy go fizycznie zniszczyć tak, aby nie było możliwe odczytanie danych osobowych.

2.8. Sposób zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych przed działalnością oprogramowani, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych osobowych

Do ochrony przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych osobowych stosowane jest oprogramowanie antywirusowe. Każdy zbiór wczytywany do komputera, w tym także wiadomość e-mail, musi być przetestowany programem antywirusowym. Na każdym stanowisku wyposażonym w dostęp do sieci Internet musi być zainstalowane oprogramowanie antywirusowe. Niedopuszczalne jest stosowanie dostępu do sieci Internet bez aktywnej ochrony antywirusowej oraz zabezpieczenia przed dostępem szkodliwego oprogramowania.

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

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

2.10. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

Przeglądy i konserwacje sprzętu komputerowego oraz nośników informacji służących do przetwarzania danych osobowych, przeprowadzane są w pomieszczeniach stanowiących obszar przetwarzania danych osobowych, określony w *Polityce bezpieczeństwa informacji* przez ASI.

W przypadku przekazywania do naprawy sprzętu komputerowego z zainstalowanym systemem informatycznym służącym do przetwarzania danych osobowych lub nośnikiem informacji służących do przetwarzania danych osobowych, powinien on zostać pozbawiony danych osobowych przez fizyczne wymontowanie dysku lub skasowanie danych lub naprawa powinna zostać przeprowadzona w obecności administratora danych. Przeglądy techniczne wykonywane muszą być nie rzadziej niż raz w roku. Nadzór nad przeprowadzaniem przeglądów technicznych, konserwacji i napraw sprzętu komputerowego, na którym zainstalowano system informatyczny służący do przetwarzania danych osobowych oraz nośników informacji służących do przetwarzania danych osobowych pełni administrator danych.

Zabronione jest wykonywanie przeglądów i konserwacji systemów informatycznych służących do przetwarzania danych osobowych oraz nośników informacji służących do przetwarzania danych osobowych samodzielnie przez pracowników Zespołu Szkół Ogólnokształcących i Zawodowych im. Króla Władysława Jagiełły w Przeworsku z wyłączeniem ASI.

2.11. Pozostałe zasady ochrony systemu informatycznego służącego do przetwarzania danych osobowych

Administrator danych ma prawo do kontroli stanu zabezpieczeń oraz przestrzegania zasad ochrony danych osobowych w dowolnym terminie.

Należy instalować zalecane przez producentów oprogramowania poprawki i uaktualnienia systemu informatycznego służącego do przetwarzania danych osobowych celem wyeliminowania błędów w działaniu lub poprawienia wydajności działania.

3. INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA DANYCH

3.1. Istota naruszenia danych osobowych

Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:

- Nieautoryzowany dostęp do danych,
- Nieautoryzowane modyfikacje lub zniszczenie danych,
- Udostępnienie danych nieautoryzowanym podmiotom,
- Nielegalne ujawnienie danych
- Pozyskiwanie danych z nielegalnych źródeł.

3.2. Postepowanie w przypadku naruszenia danych osobowych

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 do ADO

Każdy pracownik szkoły, który stwierdzi fakt naruszenia bezpieczeństwa danych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz ustalić przyczynę i sprawcę naruszenia ochrony.

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 ADO.

ADO podejmuje następujące kroki:

- Zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postepowania, uwzględniając zagrożenie w prawidłowości pracy szkoły,

- 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,
- Nawiązuje kontakt ze specjalistami spoza urzędu (jeśli zachodzi taka potrzeba).

ADO dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych osobowych, sporządzając raport wg wzoru stanowiącego załącznik nr 7 do *Polityki bezpieczeństwa informacji*. ADO 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).

3.3. Sankcje karne

Wobec osoby, która w przypadku naruszenia danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, wszczyna się postepowanie dyscyplinarne.

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.

Przeworsk, 30.12.2016r. ……..
(podpis Dyrektora)

Załączniki do Polityki bezpieczeństwa informacji

Załącznik Nr 1 – Upoważnienie imienne do przetwarzania danych osobowych

Załącznik nr 2 – ewidencja osób upoważnionych do przetwarzania danych osobowych

Załącznik nr 3 – Oświadczenie osoby odpowiedzialnej do przetwarzania danych osobowych

Załącznik nr 4 – ewidencja oświadczeń osób upoważnionych do przetwarzania danych osobowych

Załącznik nr 5 - Odwołanie upoważnienia do przetwarzania danych osobowych

Załącznik nr 6 – informacja o zawartości zbioru danych osobowych

Załącznik nr 7 – raport z naruszenia bezpieczeństwa danych osobowych

Załącznik nr 8 – wzór umowy powierzenia przetwarzania danych osobowych

Załącznik nr 9 – upoważnienie dla ASI

Załącznik nr 10 – Sprawozdanie – roczny raport z ochrony danych osobowych