

Załącznik nr 1
do Zarządzenia nr 1/13/14
Dyrektora
Liceum Ogólnokształcącego dla Dorosłych w Poświętnem
z dnia 02 grudnia 2013r.

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH w Liceum Ogólnokształcącym dla Dorosłych w Poświętnem

§ 1 Postanowienia ogólne

1. Polityka bezpieczeństwa przetwarzania danych osobowych w Liceum Ogólnokształcącym dla Dorosłych w Poświętnem, zwana dalej „Polityką bezpieczeństwa”, określa podstawowe zasady dotyczące zapewnienia bezpieczeństwa w zakresie danych osobowych przetwarzanych w zbiorach danych:
 - 1) tradycyjnych, w szczególności kartotekach, księgach, skorowidzach, aktach osobowych, wykazach, w zbiorach ewidencyjnych;
 - 2) w systemach informatycznych, w szczególności deklaracje ZUS, ewidencje płacowe, informacje skarbowe, ewidencje statystyczne, plany organizacyjne.
2. Ilekroć w Polityce Bezpieczeństwa jest mowa o:
 - 1) *ustawie* – 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 późn. zm.);
 - 2) *Szkole* – należy przez to rozumieć Liceum Ogólnokształcące dla Dorosłych w Poświętnem;
 - 3) *Księgowość* – należy przez to rozumieć **Biuro Rachunkowe W&P ENTERTAX Spółka z Ograniczoną Odpowiedzialnością**, któremu na podstawie odrębnej umowy powierza się obsługę księgową Szkoły;
 - 4) *administratorze bezpieczeństwa informatycznego (ABI)* – rozumie przez to się Organ Prowadzący – NNH Spółka z Ograniczoną Odpowiedzialnością i Dyrektora Szkoły;
 - 5) *lokalnym administratorze danych osobowych* – rozumie się przez to nauczycieli zatrudnionych w Szkole oraz pracowników księgowości;
 - 6) *administrator sieci* – rozumie się osobę odpowiedzialną za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych, służących do przetwarzania danych osobowych;
 - 7) *nośniki danych osobowych* – dyskiety, płyty CD lub DVD, pamięć flash, dyski twarde, taśmy magnetyczne lub inne urządzenia/ materiały służące do przechowywania plików z danymi;
 - 8) *osoba upoważniona (użytkownik)* – osoba posiadająca upoważnienie wydane przez Dyrektora Szkoły;
 - 9) *dane osobowe* - w rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
 - 10) *przetwarzanie danych* - rozumie się przez to jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;

- 11) *zbiór danych* - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów;
- 12) *system informatyczny* - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
- 13) *identyfikator użytkownika (login)* - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
- 14) *hasło* - ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
- 15) *uwierzytelnianie* — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
- 16) *poufności danych* — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.

§ 2

1. Organ Prowadzący i Dyrektor Szkoły realizując politykę bezpieczeństwa dokładają szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:
 - 1) przetwarzane zgodnie z prawem;
 - 2) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane przetwarzaniu niezgodnemu z tymi celami;
 - 3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
 - 4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą.
2. Organ Prowadzący i Dyrektor Szkoły dążą do systematycznego unowocześniania stosowanych informatycznych, technicznych i organizacyjnych środków ochrony tych danych w celu zabezpieczenia danych osobowych przed ich udostępnianiem osobom nieupoważnionym, przetwarzaniem z naruszeniem przepisów o ochronie danych osobowych, nieautoryzowaną zmianą, uszkodzeniem lub zniszczeniem.

§ 3

Wykaz zbiorów danych osobowych w Szkole

Dane osobowe gromadzone są w zbiorach:

Zbiór 1	Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych.
Zbiór 2	Kontrola wewnętrzna- wyniki, opracowania, protokoły, notatki.
Zbiór 3	Akta osobowe pracowników.
Zbiór 4	Dokumentacja dotycząca polityki kadrowej; zbiory informacji o pracownikach.
Zbiór 5	Ewidencja zasobów szkoły –SIO.
Zbiór 6	Rejestr delegacji służbowych.
Zbiór 7	Listy płac pracowników.
Zbiór 8	Deklaracje ubezpieczeniowe pracowników.
Zbiór 9	Deklaracje i kartoteki ZUS pracowników.
Zbiór 10	Deklaracje podatkowe pracowników.
Zbiór 11	Księga słuchaczy.
Zbiór 12	Arkusze ocen.
Zbiór 13	Podania o przyjęcie do szkoły.
Zbiór 14	Dzienniki zajęć obowiązkowych i dodatkowych.
Zbiór 15	Zaświadczenia z PPP i inne orzeczenia i opinie.

Zbiór 16	Rejestr zaświadczeń wydanych słuchaczom.
Zbiór 17	Rejestr zaświadczeń wydanych pracownikom szkoły.
Zbiór 18	Rejestr wypadków.
Zbiór 19	Księga druków ścisłego zarachowania.
Zbiór 20	Zbiór upoważnień.
Zbiór 21	Ewidencja osób przystępujących do egzaminów zewnętrznych.
Zbiór 22	Umowy zawierane z osobami fizycznymi.
Zbiór 23	Protokoły i uchwały rad pedagogicznych
Zbiór 24	Ewidencja decyzji administracyjnych dyrektora szkoły.
Zbiór 25	Zarządzenia dyrektora.
Zbiór 26	Arkusz organizacyjny placówki.
Zbiór 27	Dokumenty archiwalne.

§ 4

Zbiory danych osobowych wymienione w § 3 podlegają przetwarzaniu w sposób tradycyjny lub informatyczny.

§ 5

Wykaz budynków, pomieszczeń i stref do przetwarzania danych osobowych

1. Dane osobowe gromadzone i przetwarzane są w siedzibie Liceum Ogólnokształcącym dla Dorosłych w Poświętnem: Jadwiniew 10, 05-326 Poświętne oraz w siedzibie Biura Rachunkowego **W&P ENTERTAX Spółka z Ograniczoną Odpowiedzialnością ul. Mińska 33, 05-326 Cygów**.
2. Obszarami do przetwarzania danych osobowych z użyciem sprzętu komputerowego oraz sposobem ręcznym są:
 - 1) siedziba Liceum;
 - 2) klasy lekcyjne mieszczące się w budynku Szkoły Podstawowej im. Porucznika Stanisława Lecha; ul. Szkolna 1, 05-326 Poświętne;
 - 3) pomieszczenia księgowości.

§ 6

Rodzaje zagrożeń naruszających ochronę danych osobowych

1. Zagrożenia losowe:
 - 1) zewnętrzne np. klęski żywiołowe, przerwy w zasilaniu – ich wystąpienie może prowadzić do utraty integralności danych lub ich zniszczenia lub uszkodzenia infrastruktury technicznej systemu: ciągłość zostaje naruszona , jednak nie dochodzi do naruszenia danych osobowych;
 - 2) wewnętrzne np. niezamierzone pomyłki operatorów, awarie sprzętowe, błędy oprogramowania, które mogą spowodować zniszczenie danych lub nastąpić może zakłócenie ciągłości pracy systemu i naruszenia poufności danych.
2. Zagrożenia zamierzone (świadome i celowe naruszenia poufności danych) – w wyniku ich wystąpienia zazwyczaj nie występuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy. W ramach tej kategorii zagrożeń wystąpić mogą:
 - 1) nieuprawniony dostęp do systemu z zewnątrz;
 - 2) nieuprawniony dostęp do systemu z wewnątrz;
 - 3) nieuprawnione przekazanie danych;
 - 4) bezpośrednie zagrożenie materialnych składników np. kradzież, zniszczenie.

3. Okoliczności zakwalifikowane, jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to w szczególności:
- 1) sytuacje losowe lub nieprzewidywalne oddziaływanie czynników zewnętrznych na zasoby systemu np. wybuch gazu, pożar, zalanie pomieszczeń, uszkodzenia wskutek prowadzonych prac remontowych;
 - 2) niewłaściwe parametry środowiska np. nadmierna wilgotność, temperatura, wstrząsy, oddziaływania pola elektromagnetycznego, przeciążenia napięcia;
 - 3) awarie sprzętu lub oprogramowania, które są celowym działaniem na potrzeby naruszenia ochrony danych osobowych;
 - 4) pojawienie się odpowiedniego komunikatu alarmowego od części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;
 - 5) pogorszenie, jakości danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub niepożądaną modyfikację w systemie;
 - 6) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie;
 - 7) modyfikacja danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia;
 - 8) ujawnienie osobom nieuprawnionym danych osobowych lub objętych tajemnicą procedur ochrony ich przetwarzania;
 - 9) podmienienie lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub skasowanie bądź skopiowanie w sposób niedozwolony danych osobowych;
 - 10) rażące naruszenie obowiązków w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowywanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce lub kserokopiarce, niewykonanie kopii zapasowych, prace na danych osobowych w celach prywatnych itp.);
 - 11) nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych, znajdujących się na dyskach, płytach CD, kartach pamięci oraz wydrukach komputerowych w formie niezabezpieczonej (otwarte szafy, biurka, regały, archiwum).
4. Szczegółowe zasady postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych reguluje Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

§ 7

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

1. Formy zabezpieczeń pomieszczeń, w których przetwarzane są dane osobowe:
 - 1) wszystkie pomieszczenia, w których przetwarzane są dane osobowe zamykane są na klucz, w przypadku opuszczenia przez ostatnią osobę upoważnioną do przetwarzania danych osobowych – także w godzinach pracy;
 - 2) dane osobowe przechowywane w wersji tradycyjnej (papierowej) lub elektronicznej (pamięć flash, płyty CD, DVD) po zakończeniu pracy są przechowywane w zamykanych na klucz meblach biurowych, a tam, gdzie jest to możliwe w sejfach;
 - 3) nieaktualne lub błędne wydruki zawierające dane osobowe niszczone są w niszcarkach.
2. Formy zabezpieczeń przed nieautoryzowanym dostępem do danych osobowych:
 - 1) udostępnianie użytkownikowi zasobów zawierających dane osobowe przez administratora komputera następuje na podstawie upoważnienia do przetwarzania danych osobowych (wzór nr 1);
 - 2) identyfikacja użytkownika w systemie następuje poprzez zastosowanie uwierzytelniania;
 - 3) przydzielenie indywidualnego identyfikatora każdemu użytkownikowi;
 - 4) udostępnianie kluczy do pomieszczeń, w których przetwarzane są dane osobowe tylko osobom upoważnionym;

- 5) ustawienie monitora na stanowisku pracy w sposób uniemożliwiający wgląd w dane osobowe;
 - 6) wymuszenie zmiany hasła, co 30 dni.
3. Formy zabezpieczeń przed utratą danych osobowych w wyniku awarii:
- 1) odrębne zasilanie sprzętu komputerowego lub zastosowanie zasilaczy zapasowych UPS;
 - 2) ochrona przed utratą danych poprzez cykliczne wykonywanie kopii zapasowych;
 - 3) zapewnienie właściwej temperatury i wilgotności w pomieszczeniach;
 - 4) zastosowanie ochrony przeciwpożarowej poprzez umieszczenie w dostępnej odległości gaśnic.
4. Organizację ochrony danych osobowych realizuje się poprzez:
- 1) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych przed dopuszczeniem do pracy (wzór nr 2);
 - 2) przeszkolenie osób w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem danych i programów;
 - 3) kontrolowanie pomieszczeń budynku;
 - 4) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych (wzór nr 3);
 - 5) wyznaczenie administratora bezpieczeństwa informacji.

§ 8

1. Za organizację ochrony danych osobowych dotyczących Liceum w księgowości odpowiada pani **Wioletta Kuczyńska** reprezentująca **Biuro Rachunkowe**.
2. W przypadkach nieuregulowanych niniejszym dokumentem stosuje się odpowiednie przepisy prawa.

UPOWAŻNIENIE nr
z dnia

Na podstawie Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)

upoważniam Panią/Pana

zatrudnioną/zatrudnionego w Liceum Ogólnokształcącym dla Dorosłych w Poświętnem,

na stanowisku

do obsługi systemu ręcznego i informatycznego następujących zbiorów:

Nr zbioru	Nazwa zbioru	Zakres
Zbiór 1	Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych.	
Zbiór 2	Kontrola wewnętrzna- wyniki, opracowania, protokoły, notatki.	
Zbiór 3	Akta osobowe pracowników.	
Zbiór 4	Dokumentacja dotycząca polityki kadrowej; zbiory informacji o pracownikach.	
Zbiór 5	Ewidencja zasobów szkoły –SIO.	
Zbiór 6	Rejestr delegacji służbowych.	
Zbiór 7	Listy płac pracowników.	
Zbiór 8	Deklaracje ubezpieczeniowe pracowników.	
Zbiór 9	Deklaracje i kartoteki ZUS pracowników.	
Zbiór 10	Deklaracje podatkowe pracowników.	
Zbiór 11	Księga słuchaczy.	
Zbiór 12	Arkusze ocen.	
Zbiór 13	Podania o przyjęcie do szkoły.	
Zbiór 14	Dzienniki zajęć obowiązkowych.	
Zbiór 15	Zaświadczenia z PPP i inne orzeczenia i opinie.	
Zbiór 16	Rejestr zaświadczeń wydanych słuchaczom.	
Zbiór 17	Rejestr zaświadczeń wydanych pracownikom szkoły.	
Zbiór 18	Rejestr wypadków.	
Zbiór 19	Księga druków ścisłego zarachowania.	
Zbiór 20	Zbiór upoważnień.	
Zbiór 21	Ewidencja osób przystępujących do egzaminów zewnętrznych.	
Zbiór 22	Umowy zawierane z osobami fizycznymi.	
Zbiór 23	Protokoły i uchwały rad pedagogicznych	
Zbiór 24	Ewidencja decyzji administracyjnych dyrektora szkoły.	
Zbiór 25	Zarządzenia dyrektora.	
Zbiór 26	Arkusze organizacyjny placówki.	
Zbiór 27	Dokumenty archiwalne.	

OŚWIADCZENIE

Oświadczam, że zapoznałem(łam) się z przepisami prawa dotyczącymi ochrony danych osobowych, a w szczególności z ustawą z 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U z 2002 r., Nr 101 poz. 926 ze zm.) oraz Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. *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) i zobowiązuje się do ich przestrzegania.

Oświadczam ponadto, że zapoznałem(łam) się z wewnętrzną Instrukcją określającą sposób zarządzania systemem informatycznym i ręcznym, służącym przetwarzaniu danych osobowych i instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych.

Świadomy(a) odpowiedzialności porządkowej i karnej oświadczam, że znane mi dane osobowe będę przetwarzać zgodnie z prawem i nie dopuszczę do bezprawnego naruszenia tajemnicy również w sytuacji, gdy ustanie moje zatrudnienie w Liceum Ogólnokształcącym dla Dorosłych w Poświętnem.

Otrzymałem(łam) dnia:

.....
(podpis pracownika)

.....
(oświadczenie odebrał)

**Rejestr osób upoważnionych do przetwarzania danych osobowych
w Liceum Ogólnokształcącym dla Dorosłych w Poświętnem**

Nr upoważnienia	Imię i nazwisko użytkownika	Zakres przydzielonych uprawnień (nr zbioru)	Data nadania uprawnień	Data odebrania uprawnień