I Liceum Ogólnokształcące
im. St. Staszica w Pleszewie
ul. Poznańska 38
63-300 Pleszew
tel./fax (0-62) 508-00-44
e-mail: lopleszew@lopleszew.pl
www.lopleszew.pl

Zarządzenie Dyrektora nr 9/K/2011

I Liceum Ogólnokształcącego im. St. Staszica w Pleszewie

z dnia 01 września 2011r.

w sprawie: wprowadzenia polityki bezpieczeństwa danych osobowych i instrukcji w I Liceum Ogólnokształcącego im. St. Staszica w Pleszewie

§ 1

Celem zapewnienia funkcjonowania adekwatnej, skutecznej i efektywnej kontroli zarządczej wprowadza się:

1. Politykę bezpieczeństwa danych osobowych w I Liceum Ogólnokształcącego im. St. Staszica w Pleszewie w brzmieniu stanowiącym załącznik Nr 1 do niniejszego zarządzenia.

2. Instrukcję bezpieczeństwa przetwarzania danych osobowych w I Liceum Ogólnokształcącym im. St. Staszica w Pleszewie w brzmieniu stanowiącym załącznik nr 2 do niniejszego zarządzenia.

§ 2

Zobowiązuję wszystkich pracowników do zapoznania się z treścią niniejszej procedury.

§ 3

Zarządzenie wchodzi w życie w chwili podpisania.

.....
(podpis osoby wydającej zarządzenie)

Załącznik Nr 1
do zarządzenia z dnia 01 września 2011r.

POLITYKA BEZPIECZEŃSTWA

przetwarzania danych osobowych
w I Liceum Ogólnokształcącego im. St. Staszica w Pleszewie

SPIS TREŚCI

Podstawa prawna:

- Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tekst jednolity: Dz. U. 2002 r. Nr 101 poz.926)
- Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 3 listopada 2006 r. w sprawie nadania statutu Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2006, Nr 203, poz. 1494) – art. 13.3 ustawy)
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2004 r. Nr 94, poz.923) – art. 22a ustawy
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 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) – art. 39a ustawy
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. nr 229, poz. 1536) – art. 46a ustawy.

- Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz .U. 2005/196/1631 z późniejszymi zmianami)

ROZDZIAŁ I

Postanowienia ogólne

§1

1. Polityka bezpieczeństwa przetwarzania danych osobowych w I Liceum Ogólnokształcącym im. St. Staszica w Pleszewie zwana dalej „Polityką bezpieczeństwa”, określa podstawowe zasady dotyczące zapewnienia bezpieczeństwa w zakresie danych osobowych przetwarzanych w zbiorach danych:
    a) tradycyjnych, w szczególności kartotekach, księgach, skorowidzach, aktach osobowych, wykazach, w zbiorach ewidencyjnych;

    b) w systemach informatycznych, w szczególności deklaracje ZUS, ewidencje płacowe, stypendialne, informacje skarbowe, ewidencje statystyczne, plany organizacyjne.

2. Ilekroć w Polityce Bezpieczeństwa jest mowa o:
    a) ustawie – rozumie się przez to ustawę z dnia 29 sierpnia 1997r. o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.);

    b) administrator danych osobowych – rozumie się Dyrektora I Liceum Ogólnokształcącego im. St. Staszica w Pleszewie;

    c) lokalny administrator danych osobowych – rozumie się pracowników administracyjnych szkoły, pedagoga, wychowawców, bibliotekarza, nauczycieli;

    d) administrator sieci – rozumie się osobę odpowiedzialną za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych, służących do przetwarzania danych osobowych;

    e) nośniki danych osobowych – dyskietki, płyty CD lub DVD, pamięć flash, dyski twarde, taśmy magnetyczne lub inne urządzenia/ materiały służące do przechowywania plików z danymi;

    f) osoba upoważniona (użytkownik) – osoba posiadająca upoważnienie wydane przez administratora danych osobowych;

g) Administrator Bezpieczeństwa Informacji – osoba powołana przez dyrektora, której zadaniem jest nadzorowanie i koordynowanie w szkole zasad postępowania przy przetwarzaniu danych osobowych;

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

i) przetwarzanie danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;

j) zbiór danych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów;

k) system informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

l) identyfikator użytkownika (login) – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

m) hasło – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

n) uwierzytelnianie – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

o) poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.

§2

1. Dyrektor I Liceum Ogólnokształcącego im. St. Staszica w Pleszewie realizując politykę bezpieczeństwa dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:
    a) przetwarzane zgodnie z prawem;
    b) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane przetwarzaniu niezgodnemu z tymi celami;
    c) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
    d) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą.

2. Dyrektor I Liceum Ogólnokształcącego im. St. Staszica w Pleszewie dąży do systematycznego unowocześniania stosowanych na terenie szkoły 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.

ROZDZIAŁ II

Wykaz zbiorów danych osobowych w I Liceum Ogólnokształcącym im. St. Staszica w Pleszewie

§ 3

1. Dane osobowe gromadzone są w zbiorach:

Nr	Zbiór danych	Nazwa zbioru danych	Systemy informatyczne stosowane do przetwarzania danych osobowych w zbiorze
1	Uczniowie oraz kandydaci do szkoły	**Zbiór 1** – Księga uczniów; **Zbiór 2** – Arkusze ocen; **Zbiór 3** – Karty zgłoszeń uczniów, podania o przyjęcie do szkoły; **Zbiór 4** – Dzienniki zajęć obowiązkowych i dodatkowych; **Zbiór 5** – Zaświadczenia z PPP i inne orzeczenia i opinie; **Zbiór 6** – Ewidencje decyzji administracyjnych dyrektora szkoły – skreślenie z listy; **Zbiór 7** – Deklaracje uczęszczania na religię, sprzeciw od zajęć z wychowania do życia w rodzinie; **Zbiór 8** – Ewidencja decyzji – zwolnienia z obowiązkowych zajęć, odroczenia obowiązku szkolnego; **Zbiór 9**– Pomoc społeczna, stypendia.	Księga papierowa, Word Excel OKE VULCAN
2	Pracownicy oraz kandydaci do pracy	**Zbiór 1** – Akta osobowe pracowników; **Zbiór 2** – Dokumentacja dotycząca polityki kadrowej – opiniowanie awansów, wyróżnień, odznaczeń, nagród, wnioski o odznaczenia, itp.: **Zbiór 3** – Notatki służbowe oraz postępowanie dyscyplinarne; **Zbiór 4** – Zbiory informacji o pracownikach; **Zbiór 5** – Ewidencja zwolnień lekarskich; **Zbiór 6** – Skierowania na badania okresowe, specjalistyczne; **Zbiór 7** – Ewidencja urlopów, karty czasu pracy; **Zbiór 8** – Kartoteki wydanej odzieży ochronnej i środków ochrony indywidualnej; **Zbiór 9** – Rejestr delegacji służbowych; **Zbiór 10** – Ewidencja osób korzystających z funduszu socjalnego i dokumentacja funduszu socjalnego; **Zbiór 11** – Listy płac pracowników; **Zbiór 12**- Rejestr zaświadczeń wydanych pracownikom szkoły; **Zbiór 13** – Rejestr wypadków, ewidencja podejrzeń o chorobę zawodową itp.; **Zbiór 14** – Teczki awansu zawodowego;	Akta osobowe w formie papierowej, Word Excel VULCAN SIO eRU-PZU
3	Płace	**Zbiór 1** – Kartoteki zarobkowe pracowników, nakazy komornicze; **Zbiór 2** – Deklaracje ubezpieczeniowe pracowników; **Zbiór 3** – Deklaracje i kartoteki ZUS pracowników; **Zbiór 4** – Deklaracje podatkowe pracowników; **Zbiór 5** – Umowy zawierane z osobami fizycznymi;	VULCAN PŁATNIK

4	Organizacja	**Zbiór 1** – Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych; **Zbiór 2** – Kontrola wewnętrzna- wyniki, opracowania, protokóły, notatki; **Zbiór 3** – Ewidencja zasobów szkoły – SIO; **Zbiór 4**– Księga druków ścisłego zarachowania; **Zbiór 5** – Zbiór upoważnień; **Zbiór 6** – Ewidencja osób przystępujących do egzaminów zewnętrznych **Zbiór 7** – Protokóły rad pedagogicznych, księga uchwał; **Zbiór 8** – Dokumenty archiwalne; **Zbiór 9** – Arkusz organizacyjny placówki;	SIO Księga w formie papierowej Word Excel VULCAN

§ 4

Zbiory danych osobowych wymienione w § 3 ust. 1 podlegają przetwarzaniu w sposób tradycyjny lub informatyczny.

ROZDZIAŁ III

Wykaz pomieszczeń, w których przetwarzane są dane osobowe.

§5

1. Dane osobowe gromadzone i przetwarzane są w budynku szkolnym, mieszczącym się w Pleszewie przy ul. Poznańskiej 38.

2. Obszarami do przetwarzania danych osobowych z użyciem sprzętu komputerowego oraz sposobem ręcznym są pomieszczenia w budynku I Liceum Ogólnokształcącego im. St. Staszica w Pleszewie.

3. Zabrania się przetwarzania danych poza budynkiem I Liceum Ogólnokształcącego im. St. Staszica w Pleszewie.

4. Przebywanie osób, nieuprawnionym w obszarach przetwarzania danych osobowych w czasie przetwarzania danych osobowych jest dopuszczalne za zgodą Administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych – za jego zgodą.

ROZDZIAŁ IV

Ewidencja osób upoważnionych do przetwarzania danych osobowych

§ 6

1. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne upoważnienie.

2. Zasady wydawania i rejestracji upoważnień w I Liceum Ogólnokształcącym im. St. Staszica w Pleszewie zostały określone odrębnie.

ROZDZIAŁ V

Opis zdarzeń naruszających ochronę danych osobowych

§ 7

Rodzaje zagrożeń naruszających ochronę danych osobowych:

1. Zagrożenia losowe:
    a) 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;
    b) wewnętrzne np. niezamierzone pomyłki operatorów, awarie sprzętowe, błędy oprogramowania – w wyniku ich wystąpienia może dojść do zniszczenia danych, może nastąpić 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:
    a) nieuprawniony dostęp do systemu z zewnątrz;
    b) nieuprawniony dostęp do systemu z wewnątrz;
    c) nieuprawnione przekazanie danych;
    d) 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:
    a) sytuacje losowe lub nieprzewidywalne oddziaływanie czynników zewnętrznych na zasoby systemu np. wybuch gazu, pożar, zalanie pomieszczeń, uszkodzenia wskutek prowadzonych prac remontowych;
    b) niewłaściwe parametry środowiska np. nadmierna wilgotność, temperatura, wstrząsy, oddziaływania pola elektromagnetycznego, przeciążenia napięcia;
    c) awarie sprzętu lub oprogramowania, które są celowym działaniem na potrzeby naruszenia ochrony danych osobowych;
    d) pojawienie się odpowiedniego komunikatu alarmowego od części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;
    e) pogorszenie jakości danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub niepożądaną modyfikację w systemie;

f) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie;
g) modyfikacja danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia;
h) ujawnienie osobom nieuprawnionym danych osobowych lub objętych tajemnicą procedur ochrony ich przetwarzania;
i) podmienienie lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub skasowanie bądź skopiowanie w sposób niedozwolony danych osobowych;
j) 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.);
k) 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. W przypadku stwierdzenia naruszenia zasad bezpieczeństwa danych osobowych sporządza się raport oraz przedstawienia się go Administratorowi danych.

ROZDZIAŁ VI

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

§ 8

1. Formy zabezpieczeń pomieszczeń, w których przetwarzane są dane osobowe:
   a) wszystkie pomieszczenia, w których przetwarzane są dane osobowe zamykane są na klucz, w przypadku opuszczenia przez ostatnią osobę upoważniona do przetwarzania danych osobowych – także w godzinach pracy;
   b) dane osobowe przechowywane w wersji tradycyjnej (papierowej) lub elektronicznej (pamięć flash, płyty CD, DVD, dyskietki) po zakończeniu pracy są przechowywane w zamykanych na klucz meblach biurowych, a tam, gdzie jest to możliwe w szafach pancernych lub metalowych;
   c) nieaktualne lub błędne wydruki zawierające dane osobowe niszczone są w niszczarkach;
   d) budynek, w którym są przetwarzane dane jest chroniony systemem alarmowym z telefonicznym powiadamianiem oraz całodobowym systemem monitoringu na zewnątrz budynku.

§ 9

1. Formy zabezpieczeń przed nieautoryzowanym dostępem do danych osobowych:
   a) podłączenie urządzenia końcowego (komputera, drukarki) do sieci komputerowej I Liceum Ogólnokształcącego im. St. Staszica w Pleszewie dokonywane jest przez administratora sieci;
   b) udostępnianie użytkownikowi zasobów sieci zawierających dane osobowe przez administratora sieci następuje na podstawie upoważnienia do przetwarzania danych osobowych;
   c) identyfikacja użytkownika w systemie następuje poprzez zastosowanie uwierzytelniania (login, hasło; dot. danych przetwarzanych przy użyciu systemu informatycznego);
   d) udostępnianie kluczy do pomieszczeń, w których przetwarzane są dane osobowe tylko osobom upoważnionym;
   e) ustawienie monitorów na stanowiskach pracy w sposób uniemożliwiający wgląd w dane osobowe (dot. danych przetwarzanych przy użyciu systemu informatycznego).
   f) wymuszenie zmiany hasła np. co 30 dni (SIO, Płatnik).

§ 10

1. Formy zabezpieczeń przed utratą danych osobowych w wyniku awarii:
   a) odrębne zasilanie sprzętu komputerowego lub zastosowanie zasilaczy zapasowych UPS – komputer głównej księgowej;
   b) zastosowanie ochrony antywirusowej;
   c) zapewnienie właściwej temperatury i wilgotności w pomieszczeniach.

§ 11

1. Organizację ochrony danych osobowych realizuje się poprzez:
   a) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych przed dopuszczeniem do pracy;
   b) kontrolowanie pomieszczeń budynku;
   c) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
   d) wyznaczenie Administratora Bezpieczeństwa Informacji.

Wzór oświadczenia o zachowaniu poufności i zapoznaniu się z przepisami.

OŚWIADCZENIE

o zachowaniu poufności i zapoznaniu się z przepisami

Ja niżej podpisany (a)…….oświadczam, iż zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miał(a) dostęp w związku z wykonywaniem:

Rodzaj zadań	***)**
zadań i obowiązków służbowych wynikających z umowy o pracę	
zadań wynikających z umowy cywilno-prawnej	
zadań wynikających z umowy – w związku z praktyką studencką	

*) właściwe zaznaczyć X

zarówno **w trakcie wykonywania umowy ,jak i po jej ustaniu.**

Zobowiązuję się przestrzegać polityki, instrukcji i procedur ,obowiązujących w I Liceum Ogólnokształcącym im. St. Staszica w Pleszewie – zwanym dalej Szkołą, a dotyczących ochrony danych osobowych. W szczególności oświadczam, że bez upoważnienia nie będę wykorzystywał(a) danych osobowych ze zbiorów znajdujących się w Szkole. Oświadczam, że zostałem (am) poinformowany(a) o obowiązujących w Szkole zasadach, dotyczących przetwarzania danych osobowych ,określonych w „Polityce Bezpieczeństwa".

Oświadczam, że zostałem(am) zapoznany(a) z przepisami Ustawy o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.) oraz Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne w służące do przetwarzania danych osobowych (Dz. U. Nr 100,poz.1024 ze zm.).

Oświadczam, że zostałem (am) poinformowany (a) o grożącej, stosownie do przepisów rozdziału 8 ustawy o ochronie danych osobowych, odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, że naruszenie zasad ochrony danych osobowych, obowiązujących w Szkole może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

…….

(data i czytelny podpis osoby składającej oświadczenie)

Załącznik Nr 2
do zarządzenia z dnia 01 września 2011r.

INSTRUKCJA BEZPIECZEŃSTWA

przetwarzania danych osobowych
w I Liceum Ogólnokształcącego im. St. Staszica w Pleszewie

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

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

2. Upoważnienia do przetwarzania danych osobowych, przechowywane są w teczkach akt osobowych pracowników oraz prowadzona jest ich ewidencja.

3. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po:
   a) podaniu identyfikatora użytkownika i właściwego hasła w przypadku obsługi SIO, Płatnik;
   b) podaniu właściwego hasła dostępu do stanowiska komputerowego w przypadku obsługi OFFICE, VULCAN.

4. Dla każdego użytkownika systemu informatycznego, który przetwarza dane osobowe, Administrator Bezpieczeństwa ustala niepowtarzalny identyfikator i hasło początkowe.

5. Identyfikator użytkownika nie powinien być zmieniony, a po wyrejestrowaniu użytkownika z systemu informatycznego, nie powinien być przydzielany innej osobie.

6. W przypadku utraty przez daną osobę uprawnień do dostępu do danych osobowych w systemie informatycznym. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie wyrejestrować z sytemu informatycznego, unieważnić jej hasło, oraz podjąć inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych. Za realizację procedury rejestrowania

i wyrejestrowania użytkowników w systemie informatycznym odpowiedzialny Administrator Bezpieczeństwa Informacji.

§ 2.

Metody i środki uwierzytelnienia oraz procedury związane z ich zarządzeniem i użytkownikiem

1. Dane osobowe przetwarzane są z użyciem dedykowanych serwerów, komputerów stacjonarnych.

2. Hasło użytkownika powinno mieć minimum 8 znaków i być zmieniane w przypadku:
   a) systemu SIO, Płatnik – co 30 dni,
   b) zmiana hasła dostępu do stanowiska komputerowego co 90 dni.

3. Hasło oprócz znaków małych i dużych liter winno zwierać ciąg znaków alfanumerycznych i specjalnych;

4. Hasła wpisywane z klawiatury nie mogą pojawiać się na ekranie monitorów w formie jawnej;

5. Hasło nie może zawierać żadnych informacji, które można kojarzyć z użytkownikiem komputera np. osobiste dane użytkownika, tj. nazwisko, inicjały, imiona, marka lub nr rejestracyjny samochodu itp.;

6. Hasło nie może być zapisywane na miejscu dostępnym dla osób nieuprawnionych. Użytkownik nie może udostępniać swojego identyfikatora oraz hasła jak również dostępu do stanowiska roboczego po uwierzytelnieniu w systemie osobom nieuprawnionym ani żadnej osobie postronnej;

7. Hasło użytkownika, umożliwiające dostęp do systemu informatycznego, należy utrzymywać w tajemnicy, również po upływie jego ważności;

8. Raz użyty identyfikator nie może być przydzielony innemu użytkownikowi;

9. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest do natychmiastowej zmiany hasła, lub w razie problemów powiadomić o tym fakcie Administratora Bezpieczeństwa Informacji.

§ 3

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 pełnej i poprawnej operacji wylogowania z aplikacji i poprawnego zamknięcia systemu;

6. Monitory stanowisk komputerowych znajdujące się w pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień do przetwarzania danych osobowych, a na których przetwarzane są dane osobowe należy ustawić w taki sposób, aby uniemożliwić osobom postronnym wgląd w dane;

7. Użytkownik ma obowiązek wylogowania się w przypadku zakończenia pracy. Stanowisko komputerowe nie może pozostać z uruchomionym i dostępnym systemem bez nadzoru pracującego na nim pracownika;

8. Wydruki zawierające dane osobowe należy przechowywać w miejscu uniemożliwiającym ich odczytanie przez osoby postronne. Wydruki nieprzydatne należy zniszczyć w stopniu uniemożliwiającym ich odczytanie w niszczarce dokumentów;

9. Przebywanie osób nieuprawnionych w pomieszczeniach znajdujących się na obszarze, w którym są przetwarzane dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania;

10. Pomieszczenia, w których przetwarzane są dane osobowe, należy zamykać, na czas nieobecności osób zatrudnionych, w sposób uniemożliwiający dostęp do nich osobom trzecim;

11. Użytkownik niezwłocznie powiadamia Administratora Bezpieczeństwa Informacji w przypadku podejrzenia fizycznej ingerencji w przetwarzane dane osobowe lub zobowiązany do natychmiastowego wyłączenia sprzętu.

§ 4

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

1. Zbiory danych osobowych w systemie informatycznym są zabezpieczone przed utratą lub uszkodzeniem za pomocą:
   a) urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej,
   b) sporządzenie kopii zapasowych (kopie pełne).

2. Kopie zapasowe zbiorów danych tworzone są: w przypadku SIO – 3x w ciągu roku, VULCAN KSIĘGOWOŚĆ-PŁACE, Płatnik co miesiąc;

3. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu. Za przeprowadzenie tych czynności odpowiada Administrator Bezpieczeństwa Informacji;

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

§ 5

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

1. Okresowe kopie zapasowe wykonywane są na płytach CD lub innych elektronicznych nośnikach informacji. Kopie zapasowe przechowuje się w sposób uniemożliwiający nieuprawnione przejęcie, modyfikacje, uszkodzenie lub zniszczenie w kasie pancernej pomieszczeniu dyrektora szkoły.
2. Dostęp do nośników z kopami zapasowymi systemu oraz kopiami danych osobowych, ma wyłącznie Administrator Bezpieczeństwa Informacji.

3. Kopie przechowuje się przez okres 2 lat. Kopie zapasowe należy bezzwłocznie usuwać po ustaniu ich użyteczności.

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

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

6. W przypadku nośników informacji, przez ich zniszczenie rozumie się ich trwałe i nieodwracalne zniszczenie fizyczne do stanu nie dającego możliwości ich rekonstrukcji i odzyskania danych.

§6

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

1. W związku z istnieniem zagrożenia dla zbiorów danych osobowych, ze strony wirusów komputerowych, których celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, konieczna jest ochrona sieci komputerowej i stanowisk komputerowych.

2. Wirusy komputerowe mogą pojawić się w systemach szkoły poprzez: Internet, nośniki informacji takie jak: dyskietki, płyty CD, dyski przenośne, itp.

3. Przeciwdziałanie zagrożeniom ze strony wirusów komputerowych realizowane jest następująco:
   a) komputer z dostępem do Internetu musi być zabezpieczony za pomocą oprogramowania antywirusowego,
   b) zainstalowany program antywirusowy powinien być tak skonfigurowany, by co najmniej raz w tygodniu dokonywał aktualizacji bazy wirusów oraz co najmniej raz w tygodniu dokonywane było automatycznie sprawdzenie komputera pod kątem obecności wirusów komputerowych,
   c) 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 Bezpieczeństwa Informacji,
   d) komputery i systemy pracujące muszą mieć zainstalowany program antywirusowy a w przypadku komputerów z dostępem do Internetu, również posiadać oprogramowanie i mechanizmy zabezpieczające przed nieautoryzowanym dostępem z sieci (firewall),
   e) w przypadku, gdy użytkownik stanowiska komputerowego zauważy komunikat oprogramowania zabezpieczającego system wskazujący na zaistnienie zagrożenia lub rozpozna tego typu zagrożenie, zobowiązany jest zaprzestać jakichkolwiek czynności w systemie i niezwłocznie skontaktować się z Administratorem Bezpieczeństwa Informacji,
   f) przy korzystaniu z poczty elektronicznej należy zwrócić szczególną uwagę na otrzymywane załączniki dołączane do treści wiadomości. Zabrania się otwierania załączników i wiadomości poczty elektronicznej od „niezaufanych” nadawców,

g) zabrania się użytkownikom komputerów, wyłączania, blokowania odinstalowywania programów zabezpieczających komputer (skaner antywirusowy, firewall) przed oprogramowaniem złośliwym oraz nieautoryzowanym dostępem.

§7

Udostępnianie danych osobowych i sposób odnotowania informacji o udostępnionych danych

1. Udostępnianie danych instytucjom może odbywać się wyłącznie na pisemny uzasadniony wniosek lub zgodnie z przepisami prawa (OKE, CKE, Starostwo Powiatowe, itp.).
2. Przetwarzanie i udostępnienie danych osobowych uczniów i rodziców wymaga pisemnej zgody, wg wzoru stanowiącego załącznik do niniejszej polityki.

§8

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

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

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

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

4. Naprawy sprzętu należy zlecać podmiotom, których kompetencje nie budzą wątpliwości, co do wykonania usługi. Naprawa sprzętu, na którym mogą znajdować się dane osobowe powinna odbywać się pod nadzorem osób użytkujących sprzęt oraz Administratora Bezpieczeństwa Informacji w miejscu jego użytkowania.

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

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

§9

Ustalenia końcowe

1. Osobom korzystającym z systemu informatycznego, w którym przetwarzane są dane osobowe w szkole zabrania się:
   a) ujawniania loginu i hasła współpracownikom i osobom z zewnątrz,
   b) pozostawiania haseł w miejscach widocznych dla innych osób,
   c) udostępniania stanowisk pracy wraz z danymi osobowymi osobom nieuprawnionym,
   d) udostępniania osobom nieuprawnionym programów komputerowych zainstalowanych w systemie,
   e) używania oprogramowania w innym zakresie niż pozwala na to umowa licencyjna
   f) przenoszenia programów komputerowych, dysków twardych z jednego stanowiska na inne,
   g) kopiowania danych na nośniki informacji, kopiowania na inne systemy celem wynoszenia ich poza szkołę,
   h) samowolnego instalowania i używania jakichkolwiek programów komputerowych w tym również programów do użytku prywatnego; programy komputerowe instalowane są prze Administratora Bezpieczeństwa Informacji,
   i) używania nośników danych udostępnionych przez osoby postronne,
   j) przesyłania dokumentów i danych z wykorzystaniem konta pocztowego prywatnego (niesłużbowego),
   k) otwierania załączników i wiadomości poczty elektronicznej od nieznanych i „niezaufanych” nadawców,
   l) używania nośników danych niesprawdzonych, niewiadomego pochodzenia lub niezwiązanych z wykonywaną pracą; w przypadku konieczności użycia niesprawdzonych przenośnych nośników danych, należy zgłosić te nośniki, w celu sprawdzenia – przeskanowania programem antywirusowym, Administratorowi Bezpieczeństwa Informacji,
   m) tworzenia kopii zapasowych niechronionych hasłem i/lub bez odpowiednich zabezpieczeń miejsca ich przechowywania.

2. Ponadto zabrania się:
   a) wyrzucania dokumentów zawierających dane osobowe bez uprzedniego ich trwałego zniszczenia,
   b) pozostawiania dokumentów, kopii dokumentów zawierających dane osobowe w drukarkach, kserokopiarkach,
   c) pozostawiania kluczy w drzwiach, szafach, biurkach, zostawiania otwartych pomieszczeń, w których przetwarza się dane osobowe,
   d) pozostawiania bez nadzoru osób trzecich przebywających w pomieszczeniach szkoły, w których przetwarzane są dane osobowe,
   e) pozostawiania dokumentów na biurku po zakończonej pracy pozostawiania otwartych dokumentów na ekranie monitora bez blokady konsoli,
   f) ignorowania nieznanych osób z zewnątrz poruszających się w obszarze przetwarzania danych osobowych,
   g) przekazywania informacji będącymi danymi osobowymi osobom nieupoważnionym,
   h) ignorowania zapisów Polityki Bezpieczeństwa szkoły.

3. Konieczne jest:
   a) posługiwanie się własnym loginem i hasłem w celu uzyskania dostępu do systemów informatycznych,
   b) tworzenia haseł trudnych do odgadnięcia dla innych,
   c) traktowanie konta pocztowego szkoły jako narzędzia pracy i wykorzystywanie go jedynie w celach służbowych,
   d) nie przerywanie procesu skanowania przez program antywirusowy na komputerze,
   e) wykonywanie kopii zapasowych danych przetwarzanych na stanowisku komputerowym,
   f) zabezpieczenie sprzętu komputerowego przed kradzieżą lub nieuprawnionym dostępem do danych.

4. Wszelkie przypadki naruszenia niniejszej Instrukcji należy zgłaszać Administratorowi Bezpieczeństwa Informacji lub bezpośredniemu przełożonemu.

§10

Zalecenia w zakresie przetwarzania danych osobowych sposobem tradycyjnym

1. Miejscem tworzenia, uzupełniania, przechowywania dokumentacji dotyczącej przetwarzania danych osobowych sposobem tradycyjnym i przy użyciu systemu informatycznego są pomieszczenia I Liceum Ogólnokształcącego im. St. Staszica w Pleszewie.

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

3. Dokumentacji, o której mowa w punkcie 1 nie można wynosić poza teren szkoły, kopiować, itp.

4. Dokumentację, o której mowa w punkcie 1 archiwizuję się zgodnie z Instrukcją kancelaryjną.

5. Osoby prowadzące dokumentacje zobowiązane są do niezwłocznego poinformowania Administratora Bezpieczeństwa Informacji o podejrzeniu dostępu do dokumentacji przez osoby nieupoważnione.

§11

Obowiązki Administratora Danych

1. Administrator danych zobowiązany jest do zapewnienia, aby dane osobowe były:
   a) przetwarzane zgodnie z prawem,
   b) zbierane dla oznaczonych, zgodnych z prawem celów,
   c) merytorycznie poprawne i adekwatne w stosunku do celów.

2. Wyznacza osobę, zwaną dalej Administratorem Bezpieczeństwa Informacji, odpowiedzialnym za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałania dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.

3. Opracowuje instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych, przeznaczoną dla osób zatrudnionych przy przetwarzaniu tych danych.

4. Określa budynki, pomieszczenia lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego.

5. Prowadzi ewidencję osób uprawnionych do przetwarzania danych osobowych w poszczególnych systemach.

6. Organizuje szkolenia na celu zaznajomienie każdej osoby przetwarzającej dane osobowe z przepisami dotyczącymi ich ochrony.

7. Odpowiada za to by zakres czynności osoby zatrudnionej przy przetwarzaniu danych osobowych określał odpowiedzialność tej osoby za:
    a) ochronę danych przed niepowołanym dostępem,
    b) nieuzasadnioną modyfikację lub zniszczenie danych,
    c) nielegalne ujawnienie danych w stopniu odpowiednim do zadań realizowanych w procesie przetwarzania danych osobowych.

§12

Obowiązki Administratora Bezpieczeństwa Informacji

1. Nadzór nad przestrzeganiem instrukcji określającej sposób zarządzania systemem informatycznym.

2. Nadzór nad właściwym zabezpieczeniem sprzętu oraz pomieszczeń w których przetwarzane są dane osobowe.

3. Nadzór nad wykorzystywanym w szkole oprogramowaniem oraz jego legalnością.

4. Przeciwdziałanie dostępowi osób niepowołanych do systemu, w których przetwarzane są dane osobowe.

5. Podejmowanie odpowiednich działań w celu właściwego zabezpieczenia danych.

6. Badanie ewentualnych naruszeń w systemie zabezpieczeń danych osobowych.

7. Podejmowanie decyzji o instalowaniu nowych urządzeń oraz oprogramowania wykorzystywanego do przetwarzania danych osobowych.

8. Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych zawierających dane osobowe.

9. Definiowanie użytkowników i haseł dostępu.

10. Aktualizowanie oprogramowania antywirusowego i innego, chyba że aktualizacje te wykonywane są automatycznie.

11. Nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności.

12. Sporządzanie raportów z naruszenia bezpieczeństwa systemu informatycznego.

Załącznik

Oświadczenie

Zgoda na przetwarzanie danych osobowych

Dotyczy ucznia ……

Wyrażam zgodę na przetwarzanie i wykorzystywanie:

- Danych osobowych mojego dziecka w zakresie: data i miejsce urodzenia, PESEL, numer telefonu, adres e-mail.[1]
- Danych osobowych moich/naszych, jako rodzica/rodziców/opiekuna prawnego/opiekunów prawnych w zakresie: imiona i nazwiska rodziców bądź prawnych opiekunów, adres zamieszkania rodziców bądź prawnych opiekunów, telefony kontaktowe oraz adresy e-mail rodziców bądź prawnych opiekunów.
- Wizerunku mojego dziecka w gazetkach, biuletynach, materiałach informacyjnych i tablicach oraz na stronach internetowych I Liceum Ogólnokształcącego im. St. Staszica w Pleszewie.

Informuję , że przysługuje Panu/Pani prawo wglądu do zbieranych danych oraz uzupełniania, uaktualniania i sprostowania, jeżeli dane te są niekompletne, nieaktualne lub nieprawdziwe. Jednocześnie informuję, że administrator danych osobowych[2] (Dyrektor I Liceum Ogólnokształcącego im. St. Staszica w Pleszewie) dołoży wszelkich starań, aby dane były zbierane, przetwarzane i chronione zgodnie z prawem.

…… ……

data, miejscowość podpisy rodziców/opiekunów prawnych

[1] Dane ucznia, takie jak: imię i nazwisko, data urodzenia oraz adres zamieszkania nie wymagają zgody rodzica/opiekuna prawnego, gdyż jest to konieczne do spełniania obowiązku szkolnego.

[2] W zakresie działalności dydaktyczno – opiekuńczo – wychowawczej, zgodnie z Ustawą o Ochronie Danych Osobowych (Dz. U. z 1997r. nr 133 poz. 883 z późn. zm.) oraz Rozporządzeniem MENiS z 20 lutego 2004 r. w psprawie warunków i trybu przyjmowania uczniów do szkół publicznych oraz przechodzenia z jednego typu szkół do innych (Dz. U. nr 26 poz. 232 z późn. zm.), rozporządzeniem MEN z dnia 17 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzaju tej dokumentacji (Dz. U. nr 23 poz. 225; z 2003r. nr 107 poz. 1003; z 2009 nr 116 poz. 997 oraz z 2010 nr 156 poz. 1046) administratorem danych osobowych jest Dyrektor I Liceum Ogólnokształcącego im. St. Staszica w Pleszewie.