Załącznik Nr 1 do Zarządzenia dyrektora Szkoły Podstawowej w Staniewicach nr 14/2010/2011 z dnia 15 marca 2011 w sprawie zatwierdzenia „Polityki bezpieczeństwa i instrukcji bezpieczeństwa przetwarzania danych osobowych w Szkole Podstawowej w Staniewicach”

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W SZKOLE PODSTAWOWEJ W STANIEWICACH

ROZDZIAŁ I
Postanowienia ogólne

§ 1. 1. Polityka bezpieczeństwa przetwarzania danych osobowych w Szkole Podstawowej w Staniewicach, 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, stypendialne, 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 poźn. zm.);
2) *administrator bezpieczeństwa informatycznego (ABI)* – rozumie się Dyrektora Szkoły Podstawowej w Staniewicach
3) *lokalny administrator danych osobowych* – rozumie się pracowników administracyjnych szkoły, pedagogów, wychowawców, bibliotekarza, nauczycieli;
4) *administrator sieci* – rozumie się osobę odpowiedzialną za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych, służących do przetwarzania danych osobowych;
5) *nośniki danych osobowych* – dyskietki, płyty CD lub DVD, pamięć flash, dyski twarde, taśmy magnetyczne lub inne urządzenia/ materiały służące do przechowywania plików z danymi;
6) *osoba upoważniona (użytkownik)* – osoba posiadająca upoważnienie wydane przez dyrektora szkoły
7) *dane osobowe* - w rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
8) *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;
9) *zbiór danych* - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów;
10) *system informatyczny* - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
11) *identyfikator użytkownika (login*) - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
12) *hasło* - ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
13) *uwierzytelnianie* — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

14) *poufności danych* — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.

§ 2. **1.** Dyrektor Szkoły realizując politykę bezpieczeństwa dokłada 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. Dyrektor Szkoły 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 Szkole Podstawowej w Staniewicach

§ 3. 1 . Dane osobowe gromadzone są w zbiorach:

Zbiór 1 – Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych;
Zbiór 2 – Kontrola wewnętrzna- wyniki, opracowania, protokóły, notatki,;
Zbiór 3 – Akta osobowe pracowników;
Zbiór 4 – Dokumentacja dotycząca polityki kadrowej –opiniowanie awansów, wyróżnień, odznaczeń, nagród, wnioski o odznaczenia, itp;
Zbiór 5 – Notatki służbowe oraz postępowanie dyscyplinarne;
Zbiór 6 – Zbiory informacji o pracownikach
Zbiór 7 – Ewidencja zwolnień lekarskich;
Zbiór 8 – Skierowania na badania okresowe, specjalistyczne;
Zbiór 9 – Ewidencja zasobów szkoły –SIO;
Zbiór 10 – Ewidencja urlopów, karty czasu pracy;
Zbiór 11 – Kartoteki wydanej odzieży ochronnej i środków ochrony indywidualnej;
Zbiór 12 – Rejestr delegacji służbowych;
Zbiór 13 – Ewidencja osób korzystających z funduszu socjalnego i dokumentacja funduszu socjalnego ;
Zbiór 14 – Listy płac pracowników;
Zbiór 15 – Kartoteki zarobkowe pracowników, nakazy komornicze;
Zbiór 16 – Deklaracje ubezpieczeniowe pracowników;
Zbiór 17 – Deklaracje i kartoteki ZUS pracowników;
Zbiór 18 – Deklaracje podatkowe pracowników;
Zbiór 19 – Księga uczniów;
Zbiór 20 – Arkusze ocen;
Zbiór 21 – Karty zgłoszeń uczniów , podania o przyjęcie do szkoły;
Zbiór 22 – Dzienniki zajęć obowiązkowych i dodatkowych;
Zbiór 23 – Zaświadczenia z PPP i inne orzeczenia i opinie;
Zbiór 24 – Ewidencje decyzji administracyjnych dyrektora szkoły- skreślenia z listy;
Zbiór 25 –Deklaracje uczęszczania na religię, sprzeciw od zajęć z wychowania do życia w rodzinie
Zbiór 26 – Ewidencja decyzji – zwolnienia z obowiązkowych zajęć, odroczenia obowiązku szkolnego
Zbiór 27 – Rejestr zaświadczeń wydanych pracownikom szkoły;
Zbiór 28 – Rejestr wypadków, ewidencja podejrzeń o chorobę zawodową, itp;
Zbiór 29 – Księga druków ścisłego zarachowania;
Zbiór 30 – Zbiór upoważnień;
Zbiór 31 – Ewidencja osób przystępujących do egzaminów zewnętrznych
Zbiór 32 – Umowy zawierane z osobami fizycznymi;
Zbiór 33 – Protokóły rad pedagogicznych , księga uchwał;
Zbiór 34 – Dokumenty archiwalne;

Zbiór 35 – Teczki awansu zawodowego;
Zbiór 36 – Arkusz organizacyjny placówki;
Zbiór 37 – Pomoc społeczna, stypendia, wyprawki, obiady

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

ROZDZIAŁ III
Wykaz budynków, pomieszczeń i stref do przetwarzania danych osobowych.

§ 5. 1 . Dane osobowe gromadzone i przetwarzane są w budynku szkolnym, mieszczącym się w Staniewicach 61 , 76-113 Postomino

2. Obszarami do przetwarzania danych osobowych z użyciem sprzętu komputerowego oraz sposobem ręcznym są :
1) sekretariat szkoły
2) gabinet dyrektora
3) biblioteka szkolna
4) gabinet pedagoga
5) pokój nauczycielski
6) składnica – archiwum szkolne.

ROZDZIAŁ IV
Opis zdarzeń naruszających ochronę danych osobowych

§ 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 – 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:
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.

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

§ 7. 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 ostatnia 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, dyskietki) 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 niszczarkach;
4) budynek, w którym są przetwarzane dane chroniony jest całodobowo przez pracowników ochrony firmy Szabel

§ 8. 1. Formy zabezpieczeń przed nieautoryzowanym dostępem do danych osobowych:
1) podłączenie urządzenia końcowego (komputera, drukarki) do sieci komputerowej Szkoły dokonywane jest przez administratora sieci;
2) udostępnianie użytkownikowi zasobów sieci zawierających dane osobowe przez administratora sieci następuje na podstawie upoważnienia do przetwarzania danych osobowych;
3) identyfikacja użytkownika w systemie następuje poprzez zastosowanie uwierzytelniania;
4) przydzielenie indywidualnego identyfikatora każdemu użytkownikowi;
5) udostępnianie kluczy do pomieszczeń, w których przetwarzane są dane osobowe tylko osobom upoważnionym;
6) ustawienie monitorów na stanowiskach pracy w sposób uniemożliwiający wgląd w dane osobowe;
7) wymuszenie zmiany hasła, co 30 dni.

§ 9. 1. 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;

§ 10. 1. Organizację ochrony danych osobowych realizuje się poprzez:
1) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych przed dopuszczeniem do pracy;
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;
5) wyznaczenie administratora bezpieczeństwa informacji.