załącznik nr 1 do zarządzenia nr 9.2015 dyrektora Zespołu Szkół nr 3 w Hajnówce

POLITYKA BEZPIECZEŃSTWA INFORMACJI I OCHRONY DANYCH OSOBOWYCH w Zespole Szkół nr 3 w Hajnówce

Podstawa prawna:

1. *Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. 2014 poz. 1182)*
2. *Rozporządzenie 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 służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024)*
3. *Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (*Dz.U. *2012* poz. 526).

ROZDZIAŁ I
Postanowienia ogólne

§ 1

1. Polityka bezpieczeństwa informacji i ochrony danych osobowych w Zespole Szkół nr 3 w Hajnówce 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. 2014 poz. 1182*);
   2) *Administrator Danych Osobowych (ADO)* – rozumie się Dyrektora Zespołu Szkół nr 3 w Hajnówce
   3) *Administrator Bezpieczeństwa Informacji (ABI)*- rozumie się pracownik Zespołu Szkół nr 3 w Hajnówce, wyznaczony przez Dyrektora Zespołu
   4) *lokalny administrator danych osobowych* – rozumie się pracowników administracyjnych, nauczycieli;
   5) *Administrator Systemów Informatycznych* (ASI)- rozumie się przez to osobę odpowiedzialna za operacyjne zarządzanie systemem informatycznym w sposób zapewniający ochronę danych osobowych w nich przetwarzanych, osobę odpowiedzialną za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych, służących do przetwarzania danych osobowych;

6) *nośniki danych osobowych* – dyskietki, płyty CD lub DVD, pamięć flash, dyski twarde, taśmy magnetyczne lub inne urządzenia/ materiały służące do przechowywania plików z danymi;
7) *osoba upoważniona (użytkownik)* – osoba posiadająca upoważnienie wydane przez administratora danych osobowych ;
8) *dane osobowe* - w rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
9) *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;
10) *zbiór danych* - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów;
11) *system informatyczny* - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
12) *identyfikator użytkownika (login*) - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
13) *hasło* - ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
14) *uwierzytelnianie* — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
15) *poufności danych* — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.

§ 2

2. **1.** Dyrektor Zespołu Szkół nr 3 w Hajnówce 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 nie poddawane 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. 2 Dyrektor Zespołu Szkół nr 3 w Hajnówce 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 Zespołu Szkół nr 3 w Hajnówce

§ 3

1. Dane osobowe gromadzone są w zbiorach:

Lp.	Nazwa zbioru danych	Struktura zbioru	Dokumenty/zbiory
1.	Pracownicy Zespołu Szkół nr 3 w Hajnówce	Imię i nazwisko, data urodzenia, PESEL, miejsce zamieszkania, telefon i inne dane niezbędne do zatrudnienia	-ewidencja zatrudnienia -akta osobowe - ewidencja zwolnień lekarskich - kontrola wewnętrzna -SIO - urlopy, karty czasu pracy -awans zawodowy pracowników - dokumenty archiwalne - ewidencja zaświadczeń -rejestr wypadków, dokumentacja wypadkowa - księga protokołu Rady Pedagogicznej -arkusz organizacyjny zespołu - e-dziennik
2.	Sprawy finansowe	Imię i nazwisko, data urodzenia, PESEL, miejsce zamieszkania, telefon i inne dane niezbędne do wynagrodzenia, oświadczenia o dochodach do ZFŚS,	-listy płac - kartoteki - deklaracje podatkowe, ubezpieczeniowe, ZUS -księgowość Qwant i Qwark - PEFRON, -PZU ERA -płatnik ZUS
3.	Zakładowy Fundusz Świadczeń Socjalnych	Imię i nazwisko, data urodzenia, miejsce zamieszkania, numer telefonu, oświadczenia o dochodach do ZFŚS,	- dokumentacja ZFŚS - decyzje, wnioski, umowy

4.	Uczniowie Zespołu Szkół nr 3 w Hajnówce	Imię i nazwisko, data urodzenia, PESEL, miejsce zamieszkania, numer telefonu rodzica/ opiekuna	- księga ewidencji dzieci - księga uczniów -arkusze ocen - dzienniki zajęć obowiązkowych, dodatkowych - e-dziennik -deklaracje udziału w zajęciach religii, -wniosek nauczania języka mniejszości - SIO, HERMES, ISO - orzeczenia, opinie PPP - decyzje odroczenia i spełniania obowiązku szkolnego - rejestr wypadków, dokumentacja wypadkowa - księga protokołu Rady Pedagogicznej - rejestr wydanych zaświadczeń OKE i świadectw
5.	Rekrutacja uczniów	Imię i nazwisko, data i miejsce urodzenia, PESEL, imię i nazwisko rodziców/ prawnych opiekunów, adres zamieszkania, numer telefonu	- deklaracje pobytu dziecka w świetlicy - wniosek o przyjęcie dziecka do szkoły - świadectwo ukończenia szkoły podstawowej i zaświadczenie OKE
6.	Sprawy socjalne	Imię i nazwisko, data i miejsce urodzenia ucznia, imię i nazwisko rodziców/ prawnych opiekunów, adres zamieszkania, numer telefonu, oświadczenie rodzica o dochodach	- dokumentacja związana z dofinansowaniem zakupu podręczników dla uczniów - protokoły zebrań
7.	Umowy bieżące	Nazwa firmy, organizacji, imię i nazwisko osoby fizycznej, NIP, REGON, numer dokumentu, konto bankowe, wynagrodzenie	- rejestr zawieranych umów
8.	Upoważnienia	Imię i nazwisko, PESEL, data i miejsce urodzenia, numer dokumentu potwierdzającego tożsamość	- powołania, - upoważnienia

9.	Projekty unijne	Imię i nazwisko, PESEL, data i miejsce urodzenia, wykształcenie	- PEFS -deklaracje, oświadczenia o udziale w projekcie - listy obecności - dzienniki zajęć

§ 4

Zbiory danych osobowych wymienione w § 3 ust.1 podlegają przetwarzaniu w sposób tradycyjny oraz przy użyciu systemu informatycznego.

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

§ 5

1. Dane osobowe uczniów gromadzone i przetwarzane są w budynku szkolnym, mieszczącym się w Hajnówce przy ul. Nowowarszawska 20 .

2. Dane osobowe pracowników gromadzone i przetwarzane są w budynku szkolnym, mieszczącym się w Hajnówce przy ul. Nowowarszawska 20.

3. Obszarami do przetwarzania danych osobowych z użyciem sprzętu komputerowego oraz sposobem ręcznym są :
   1) pokój głównej księgowej- obszar za biurkiem ze wszystkimi urządzeniami;
   2) gabinet dyrektora - obszar za biurkiem ze wszystkimi urządzeniami;
   3) sekretariat- obszar za biurkiem ze wszystkimi urządzeniami, szafy w tym szafa pancerna;
   4) biblioteka szkolna – obszar za biurkiem;
   5) pokój nauczycielski;
   6) sale lekcyjne – obszar za biurkiem ze wszystkimi urządzeniami ;
   7) archiwum szkolne;
   8) gabinet pielęgniarki.

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 szczegółowa procedura.

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 ostatnią osobę upoważnioną do przetwarzania danych osobowych – także w godzinach pracy;
2) dane osobowe pracowników szkoły przechowywane są w szafie pancernej;
3) sekretariat, gabinet dyrektora, księgowość, biblioteka, pokój nauczycielski posiadają zakratowane okna;
4) sale informatyczne posiadają zakratowane drzwi;

5) 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;
6) nieaktualne lub błędne wydruki zawierające dane osobowe niszczone są w niszczarkach;

§ 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 w bazie SIO, HERMES, ISO co 30 dni,
8) dostęp do kont bankowych na podstawie hasła i kodu udostępnionego na dany dzień

§ 9

1. Formy zabezpieczeń przed utratą danych osobowych w wyniku awarii:
1) 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 pomieszczeniach lub w ich pobliżu 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, Administratora Systemów Informatycznych
6) Przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji

§ 11

1. ADO zapewnia minimum raz do roku organizuje okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji
2. Kartę kontroli stanowi załącznik nr 8 niniejszego dokumentu

INSTRUKCJA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

W TYM SYSTEMÓW INFORMATYCZNYCH
w Zespole Szkół nr 3 w Hajnówce

§ 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, o których mowa w punkcie 1.1. przechowywane są w teczce ,,Rejestr danych osobowych" 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, HERMES, ISO, e-dziennika, księgowość Qwant i Qwark, płatnik ZUS, PEFRON, PZU ERA
   b) podaniu właściwego hasła dostępu do stanowiska komputerowego w przypadku obsługi wyżej wymienionych programów.
4. Dla każdego użytkownika systemu informatycznego, który przetwarza dane osobowe, Administrator Bezpieczeństwa Informacji ustala niepowtarzalny identyfikator i hasło początkowe.
5. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego, nie powinien być przydzielany innej osobie.
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 systemu informatycznego, unieważnić jej hasło oraz podjąć inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych. Za realizację procedury rejestrowania i wyrejestrowywanie użytkowników w systemie informatycznym odpowiedzialny jest Administrator Bezpieczeństwa Informacji.

§ 2

Metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem.

1. Dane osobowe przetwarzane są z użyciem dedykowanych serwerów, komputerów stacjonarnych.
2. Hasło użytkownika powinno mieć minimum 8 znaków i być zmieniane w przypadku :
   a) Systemu SIO, HERMES, ISO – co 30 dni,
   b) Zmiana hasła dostępu do stanowiska komputerowego co 90 dni.
3. Hasło oprócz znaków małych i dużych liter winno zawierać 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 w miejscu dostępnym dla osób nieuprawnionych. Użytkownik nie może udostępnić 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. Hasła są zdeponowane w kasie pancernej w siedzibie dyrektora szkoły.
10. 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 użytkowane narzędzia programowe lub sprzętowe. Wówczas użytkownik jest 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 zabezpieczane przed utratą lub uszkodzeniem za pomocą:
   a) urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej, o ile jest to możliwe,

b) sporządzanie kopii zapasowych (kopie pełne).

2. Pełne kopie zapasowe zbiorów danych tworzone są 2 razy w ciągu roku;
3. W szczególnych sytuacjach, np. przed aktualizacją lub zmianą oprogramowania lub systemu należy wykonać bezwzględnie pełną kopię zapasową systemu;
4. 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;
5. 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 oraz 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 kopiami zapasowymi systemu oraz kopiami danych osobowych ma wyłącznie administrator bezpieczeństwa informacji.

3. Kopie miesięczne przechowuje się przez okres 6 miesięcy. Wykonywane co pół roku pełne kopie systemu kadrowego przechowuje się przez 50 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 sporządzanych 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 niedającego możliwości ich rekonstrukcji i odzyskania danych.

§ 6

Sp**osób 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 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. Udostępnienie danych instytucjom może odbywać się wyłącznie na pisemny uzasadniony wniosek lub zgodnie z przepisami prawa (MEN,CKE, Urząd Miasta, itp.).

§ 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 wiedzą 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 przez 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) nieprzerywanie 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.

5. Dane kontaktowe

- administrator danych osobowych, administrator bezpieczeństwa informacji – dyrektor szkoły, tel. 85 6832508
- administrator bezpieczeństwa informacji – w-ce dyrektor szkoły, tel. 85 6833388
- administrator systemów informatycznych- informatyk, 85 6832508

§ 10

Zalecenia w zakresie przetwarzania danych osobowych sposobem tradycyjnym

1. Miejscem tworzenia, uzupełniania, przechowywania dokumentacji dotyczącej przetwarzania danych osobowych sposobem tradycyjnym są pomieszczenia w szkole: pokój nauczycielski, gabinet dyrektora, sekretariat, pomieszczenia głównej księgowej, pokój pielęgniarki, biblioteka,
2. Osoby prowadzące dokumentację zobowiązane są do zachowania tajemnicy służbowej.
3. Dokumentacji, o której mowa w punkcie 1. nie można wynosić poza teren szkoły.
4. Dokumentację, o której mowa w punkcie 1 archiwizuje się zgodnie z Instrukcją kancelaryjną.
5. Osoby prowadzące dokumentację zobowiązane są do niezwłocznego poinformowania administratora danych osobowych o podejrzeniu dostępu do dokumentacji przez osoby nieupoważnione.

§ 11

Obowiązki Administratora Danych Osobowych

1. ADO 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. Opracowuje instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych, przeznaczoną dla osób zatrudnionych przy przetwarzaniu tych danych.
3. Określa budynki, pomieszczenia lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego.
4. Opracowuje instrukcję, określającą sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.
5. Prowadzi ewidencję osób uprawnionych do przetwarzania danych osobowych w poszczególnych systemach.
6. Organizuje szkolenia mające na celu zaznajomienie każdej osoby przetwarzającej dane osobowe z przepisami dotyczącymi ich ochrony.
7. Odpowiada za to, by zakres czynności osoby zatrudnionej przy przetwarzania 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 na 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 na 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. Wdrożenie szkoleń z zakresu przepisów dotyczących ochrony danych osobowych oraz środków technicznych i organizacyjnych przy przetwarzaniu danych w systemach informatycznych.
13. Sporządzanie raportów z naruszenia bezpieczeństwa systemu informatycznego.

Obowiązki Administratora Systemów Informatycznych

1. Operacyjne zarządzanie systemami informatycznymi w sposób zapewniający ochronę danych osobowych w nich przetwarzanych.
2. Przestrzeganie opracowanych dla systemu procedur operacyjnych i bezpieczeństwa.
3. Kontrola przepływu informacji pomiędzy systemem informatycznym, a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej a systemem informatycznym.
4. Zarządzanie stosowanymi w systemach informatycznym środkami uwierzytelnienia, w tym rejestrowanie i wyrejestrowywanie użytkowników oraz dokonywanie zmiany uprawnień na podstawie zaakceptowanych wniosków przez osobę do tego upoważnioną.
5. Regularne tworzenie kopii zapasowych zasobów danych osobowych oraz programów służących do ich przetwarzania oraz okresowe sprawdzanie poprawności wykonania kopii zapasowych.

6. Nadzór nad wykonywaniem okresowych przeglądów i konserwacji, zgodnie z odrębnymi procedurami, sprzętu IT, systemów informatycznych, aplikacji oraz elektronicznych nośników informacji, na których zapisane są dane osobowe
7. Utrzymanie systemu w należytej sprawności technicznej.
8. Zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych poprzez aktualizację oprogramowania, minimalizowanie ryzyka utraty informacji w wyniku awarii,
9. Regularne tworzenie kopii zapasowych zasobów danych osobowych oraz programów służących do ich przetwarzania oraz okresowe sprawdzanie poprawności wykonania kopii zapasowych.
10. Wykonywanie lub nadzór nad wykonywaniem okresowych przeglądów i konserwacji, zgodnie z odrębnymi procedurami, sprzętu IT, systemów informatycznych, aplikacji oraz elektronicznych nośników informacji, na których zapisane są dane osobowe.

Załącznik nr 5 do zarządzenia nr 9.2015
Dyrektora Zespołu Szkół nr 3 w Hajnówce z dnia 31.08.2015

PROCEDURY NISZCZENIA NOŚNIKÓW DANYCH
w Zespole Szkół nr 3 w Hajnówce

1. Nośniki danych elektronicznych przekazywanych na zewnątrz powinny być pozbawione zapisów zawierających dane osobowe. Niszczenie poprzednich zapisów powinno odbywać się poprzez nośnika wielokrotnie nadpisanego innych informacji za pomocą specjalistycznego oprogramowania
2. Poprawność przygotowania nośnika danych elektronicznych powinna być sprawdzana przez Administratora Bezpieczeństwa Informacji lub wyznaczonego specjalistę ds. informatyki
3. Uszkodzone nośniki magnetyczne przed ich wyrzuceniem należy fizycznie zniszczyć w sposób uniemożliwiający odzyskanie zapisanych na nich danych
4. Wydruki, kserokopie oraz inne dokumenty w formie papierowej niszczy się przy pomocy niszczarki biurowej

PROCEDURY POSTEPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH W ZESPOLE SZKÓŁ NR 3 W HAJNÓWCE

1. Każdy Upoważniony do przetwarzania danych osobowych, który poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych osobowych przez osobę przetwarzającą dane osobowe bądź posiada informację o mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany niezwłocznie zgłosić ten fakt Administratorowi Danych Osobowych lub Administratorowi Bezpieczeństwa Informacji
2. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych ADO lub upoważnionej przez niego osoby należy:
3. ADO lub osoba go zastępująca :

- niezwłocznie podjąć czynności niezbędne do powstrzymania niepożądanych skutków
  - wstrzymać bieżącą pracę na komputerze
  - podjąć stosowne działania jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej
  - udokumentować wstępnie zaistniałe naruszenie
  - nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia

4. ADO lub osoba lub upoważniony przez niego pracownik dokumentuje zaistniałe zdarzenie w postaci raportu, który stanowi załącznik nr 7 niniejszej instrukcji, jeśli jest taka potrzeba nawiązuje kontakt ze specjalistami z zewnątrz
5. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu ADO zasięga niezbędnych opinii i proponuje postępowanie naprawcze

WZORY DRUKÓW ZWIĄZANYCH Z OCHRONĄ I PRZETWARZANIEM DANYCH OSOBOWYCH

Załącznik Nr 1
do Polityki bezpieczeństwa przetwarzania i ochrony danych osobowych
w Zespole Szkół nr 3 w Hajnówce

UPOWAŻNIENIE nr .....

z dnia .....

Na podstawie ustaw *Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. 2014 poz. 1182).*

upoważniam Panią/Pana ..... zatrudnioną/nego w ….. w ……. na stanowisku ..... do obsługi systemu ręcznego i informatycznego zbiorów Nr .....(wypisać zbiory)

Administrator Danych Osobowych

Załącznik Nr 2
do Polityki bezpieczeństwa przetwarzania i ochrony danych osobowych
w Zespole w Zespole Szkół nr 3 w Hajnówce

ODWOŁANIE
UPOWAŻNIENIA nr .....

z dnia .....

Na podstawie ustaw Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych *(tekst jednolity: Dz.U. 2014 poz. 1182).*

odwołuję upoważnienie Pani/Pana ..... zatrudnioną/nego w ….. w ……. na stanowisku ..... do obsługi systemu ręcznego i informatycznego zbiorów Nr .....(wypisać zbiory)

Administrator Danych Osobowych

Załącznik Nr 3
do Polityki bezpieczeństwa przetwarzania i ochrony danych osobowych
w Zespole w Zespole Szkół nr 3 w Hajnówce

.....
imię i nazwisko

.....
stanowisko

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 (*tekst jednolity: Dz.U. 2014 poz. 1182*.) 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), Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (*Dz.U. *2012* poz. 526).

i zobowiązuję 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 Zespole Szkół nr 3 w Hajnówce

Otrzymałem(łam) dnia:

.....
(oświadczenie odebrał)

.....
(*podpis pracownika)*

Załącznik Nr 4
do Polityki bezpieczeństwa przetwarzania i ochrony danych osobowych
w Zespole w Zespole Szkół nr 3 w Hajnówce

DODATKOWY ZAKRES OBOWIĄZKÓW DLA PRACOWNIKÓW SZKOŁY

2. Pracownik zobowiązany jest dbać o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania danych zgodnie z obowiązującą w szkole polityką bezpieczeństwa, regulaminami i instrukcjami wewnętrznymi, w tym m. in.:

a) chronić dane przed dostępem osób nieupoważnionych,
b) chronić dane przed przypadkowym lub nieumyślnym zniszczeniem, utratą lub modyfikacją,
c) chronić nośniki magnetyczne i optyczne oraz wydruki komputerowe przed dostępem osób nieupoważnionych oraz przed przypadkowym zniszczeniem,
d) utrzymywać w tajemnicy powierzone identyfikatory, hasła, częstotliwość ich zmiany oraz szczegóły technologiczne systemów także po ustaniu zatrudnienia w szkole.
e) archiwizować dane zgodnie z instrukcją technologiczną,
f) prowadzi niezbędną, przewidzianą instrukcją technologiczną dokumentację pracy z systemem, archiwizowania danych itp.

3. Zabrania się pod rygorem odpowiedzialności służbowej i karnej:

a) ujawniać dane – w tym dane osobowe zawarte w obsługiwanych systemach,
b) kopiować bazy danych lub ich części poza przewidzianymi instrukcją technologiczną kopiami bezpieczeństwa,
c) zabrania się przetwarzania danych w sposób inny niż opisany instrukcją technologiczną

Załącznik Nr 5
do Polityki bezpieczeństwa przetwarzania i ochrony danych osobowych
w Zespole w Zespole Szkół nr 3 w Hajnówce

WYKAZ OSÓB I ZAKRES OBOWIĄZKÓW

Lp.	Imię i nazwisko	funkcja	Zakres obowiązków
1.		ADO,	
2.		ABI	
2.		ASI	

Załącznik Nr 6
do Polityki bezpieczeństwa przetwarzania i ochrony danych osobowych
w Zespole w Zespole Szkół nr 3 w Hajnówce

EWIDENCJA OSÓB ZATRUDNIONYCH I UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Imię i nazwisko	Program/dokumenty	Zakres upoważnienia	Data nadania	Data odwołania

Załącznik Nr 7
do Polityki bezpieczeństwa przetwarzania i ochrony danych osobowych
w Zespole w Zespole Szkół nr 3 w Hajnówce

Raport o naruszeniu bezpieczeństwa danych osobowych

Sporządzający raport:…….

Forma naruszenia ochrony danych osobowych

1. miejsce, czas i data zdarzenia
2. osoba powodująca naruszenie
3. informacja o danych, które zostały lub mogły zostać ujawnione
4. zabezpieczone materiały lub inne dowody związane z wydarzeniem
5. krótki opis wydarzenia związanego z naruszeniem ochrony danych osobowych

data…….. podpis……..

Załącznik nr 5 do zarządzenia nr 9.2015
Dyrektora Zespołu Szkół nr 3 w Hajnówce z dnia 31.08.2015

Załącznik Nr 8
do Polityki bezpieczeństwa przetwarzania i ochrony danych osobowych
w Zespole w Zespole Szkół nr 3 w Hajnówce

Karta kontroli okresowej w zakresie stosowania zasad bezpieczeństwa informacji

Data kontroli:
Osoba dokonująca kontroli, pełniona funkcja:
Zakres kontroli

Zagadnienie	Stopień spełniania wymagań		Uzasadnienie
	TAK	NIE	
W szkole prowadzona jest polityka przetwarzania danych osobowych, zgodnie z aktualnymi przepisami			
Wszyscy pracownicy mający dostęp do bazy danych szkoły zostali zapoznani z wewnętrzną polityką przetwarzania danych osobowych			
W szkole prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych			
W szkole prowadzony jest wykaz i zakres obowiązków osób odpowiedzialnych za realizację polityki przetwarzania danych osobowych			
W szkole obowiązuje aktualna instrukcja bezpieczeństwa przetwarzania danych osobowych i systemów informatycznych			
W szkole zapewnione są środki techniczne niezbędne do zapewnienia poufności, integralności i rozliczności przetwarzania danych osobowych			
W szkole każde stanowisko komputerowe jest zabezpieczone aktualnym programem antywirusowym			
W szkole obowiązują procedury niszczenia nośników zawierających bazy danych			
W szkole obowiązuje ścieżka obsługi ,,incydentu naruszenia bezpieczeństwa informacji”			

Wnioski pokontrolne

Zalecenia

Podpisy osób zobowiązanych do wdrożenia zaleceń: