POLITYKA BEZPIECZEŃSTWA
PRZETWARZANIA DANYCH OSOBOWYCH
ORAZ
INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM
PRZETWARZAJĄCYM DANE OSOBOWE
W
ZESPOLE SZKÓŁ NR 3
im. KOMBATANTÓW RZECZYPOSPOLITEJ POLSKIEJ
W DZIERŻONIOWIE

Pieczęć firmowa:	Podpis Administratora Danych Osobowych:	Data:
		17 czerwca 2015

Podpis Administratora Bezpieczeństwa Informacji:	Data:	Podpis Administratora Systemu Informatycznego:	Data:
	17 czerwca 2015		**17 czerwca 2015**

WSTĘP

Realizując postanowienia ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2014 poz. 1182 i 1662) oraz wydane w oparciu o delegacje ustawą przepisy rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (Dz.U. 2004 r. Nr 100 poz. 1024 z zm.) w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informacyjne służące do przetwarzania danych osobowych wprowadza się zestaw reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej pozwalający na zapewnienie ochrony danych osobowych.

Rozdział 1
Postanowienia ogólne

Ilekroć w dokumencie jest mowa o:

1. Administratorze Danych Osobowych (ADO) – należy przez to rozumieć Dyrektora Zespołu Szkół nr 3 w Dzierżoniowie
2. Administratorze Bezpieczeństwa Informacji (ABI) – należy przez to rozumieć Kierownika gospodarczego.
3. Administratorze Systemu Informatycznego (ASI) – należy przez to rozumieć pracownika SBS Adam Palus.
4. obszarze przetwarzania należy przez to rozumieć budynki, pomieszczenia lub części pomieszczeń w których przetwarzane są dane osobowe.
5. zbiorze danych osobowych należy przez to rozumieć każdy posiadający strukturę zestaw danych o charakterze osobowym dostępnych według określonych kryteriów niezależnie od jego rozproszenia czy podziału.
6. opisie struktury zbiorów należy przez to rozumieć opis zbiorów danych osobowych wskazujący zawartość poszczególnych pól informacyjnych oraz powiązania miedzy nimi.
7. opisie przepływu danych należy przez to rozumieć opis przepływu danych osobowych pomiędzy zbiorami.
8. środkach technicznych i organizacyjnych należy przez to rozumieć środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.
9. procedurach bezpieczeństwa należy przez to rozumieć procedury mające na celu zabezpieczenie przetwarzanych danych osobowych.
10. 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;

Rozdział 2
Administrator Danych Osobowych

§ 1. Administrator Danych Osobowych w celu zapewnienia ochrony danych osobowych może może:

1. Powołać Administratora Bezpieczeństwa Informacji. (załącznik nr 1)
2. Powołać Administratora Systemu Informatycznego. (załącznik nr 2)

§ 2. Administrator Danych Osobowych ma w szczególności:

1. Opracować i wdrożyć Politykę bezpieczeństwa przetwarzania danych osobowych oraz Instrukcję zarządzania systemem informatycznym przetwarzającym dane osobowe.
2. Wydawać i anulować upoważnienia do przetwarzania danych osobowych osobom, które mają te dane przetwarzać. (załącznik nr 3)
3. Prowadzić ewidencje osób upoważnionych do przetwarzania danych osobowych. (załącznik nr 4)
4. Wykaz zbiorów danych osobowych. (załącznik nr 5)
5. Wykaz budynków, pomieszczeń i stref do przetwarzania danych osobowych. (załącznik nr 6)
6. Dokumentuje zaistniały przypadek naruszenia oraz sporządza raport. (załącznik nr 7)

Środki techniczne i organizacyjne

§ 3. W celu ochrony danych osobowych stosuje się następujące zabezpieczenia organizacyjne:

1. Została opracowana i wdrożona **Polityka bezpieczeństwa przetwarzania danych osobowych** oraz **Instrukcja zarządzania systemem informatycznym przetwarzającym dane osobowe**.
2. Do przetwarzania danych osobowych zostają dopuszczone wyłącznie osoby posiadające ważne upoważnienia do ich przetwarzania.
3. Prowadzona jest ewidencja osób posiadających upoważnienia do przetwarzania danych osobowych.
4. Osoby posiadające upoważnienia zostały przeszkolone w zakresie ochrony danych osobowych i zabezpieczeń systemu informatycznego.
5. Osoby posiadające upoważnienia złożyły oświadczenie o zachowaniu poufności przetwarzanych danych osobowych.
6. Przetwarzanie danych osobowych jest w warunkach zabezpieczających dane osobowe przed dostępem osób nieupoważnionych.
7. Przebywanie osób nieupoważnionych w obszarze przetwarzania jest możliwe tylko w obecności osób upoważnionych oraz w warunkach zapewniających bezpieczeństwo danych osobowych.

§ 4. W celu ochrony danych osobowych stosuje się następujące zabezpieczenia fizyczne:

1. Drzwi do pomieszczeń stanowiących obszar przetwarzania są zamykane na klucz.
2. Dane osobowe w wersji papierowej są przechowywane w meblach zamykanych na klucz.
3. W obszarze przetwarzania są dostępne niszczarki dokumentów i nośników danych.
4. Klucze, kody dostępu lub inne zabezpieczenia do obszarów przetwarzania są wydawane i zdawane za pobraniem przez osoby upoważnione.

§ 5 . W celu ochrony danych osobowych stosuje się następujące zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej:

1. Zastosowano UPS do serwera lub komputerów na których znajdują się przetwarzane dane osobowe.
2. Dostęp do komputerów na których znajdują się dane osobowe odbywa się poprzez podanie loginu i hasła.
3. Dostęp zdalny za pośrednictwem Internetu do danych osobowych odbywa się przez szyfrowane połączenie SSL lub VPN i wymaga podania loginu i hasła.
4. Stosuje się system antywirusowy oraz firewall na komputerach na których znajdują się dane osobowe.

Rozdział 4
Procedury zapewniające bezpieczeństwo danych osobowych

§ 6. Procedura nadawania uprawnień do przetwarzania danych osobowych:

1. Upoważnienia do przetwarzania danych osobowych nadaje ADO lub ABI.
2. Przed nadaniem upoważnienia do przetwarzania danych osobowych osoba zostaje przeszkolona w zakresie ich ochrony oraz zapoznana z zasadami bezpieczeństwa systemu informatycznego.
3. Osoba posiadająca upoważnienie do przetwarzania danych osobowych podpisała oświadczenie o zachowaniu poufności danych osobowych do których ma dostęp.

§ 7. Metody i środki zabezpieczające dostęp do danych osobowych:

1. Hasła dostępu do danych osobowych nie mogą być powszechnie znanymi nazwami własnymi.
2. Osoba upoważniona zobowiązuje się do zachowania w poufności hasła dostępu do danych osobowych oraz jego natychmiastowej zmiany w przypadku ujawnienia.
3. Zabronione jest przechowywanie hasła w sposób jawny lub przekazywania go innym osobom.
4. Hasło jest zmieniane pół-automatycznie lub manualnie co 30 dni przez osoby upoważnione.
5. Hasło składa się z co najmniej 8 znaków, w tym małe i duże litery oraz cyfry lub znaki specjalne.

§ 8. Procedura rozpoczęcia, zawieszenia i zakończenia pracy wymagającej przetwarzania danych osobowych:

1. Osoba upoważniona loguje się do systemu lub programu informatycznego przy użyciu loginu i hasła.
2. Osoba upoważniona jest zobowiązana do informowania ABI o nieautoryzowanych próbach zalogowania do systemu lub programu jeżeli system lub program takie zjawiska monitoruje.

3. Osoba upoważniona jest zobowiązana do uniemożliwienia wglądu w dane osobowe wyświetlane na ekranie monitora lub w wersji papierowej osobom nieupoważnionym.
4. Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana w trakcie czasowego opuszczenia miejsca pracy do uruchomienia wygaszacza ekranu chronionego hasłem lub wylogowania się z systemu oraz usunięcia wydruków z danymi osobowymi z biurka.
5. Po zakończeniu pracy osoba upoważniona jest zobowiązana do wylogowania się lub wyłączenia komputera oraz usunięcia z biurka wszelkich nośników zawierających dane osobowe jak i zabezpieczenia pomieszczenia przed włamaniem, zalanie, pożarem, itd…

§ 9. Procedura tworzenia kopii zapasowych:

1. W zależności od wielkości przyrostu ilościowego i pojemnościowego danych osobowych tworzy się ich kopie zapasowe w odstępach nie częstszych niż 1 dzień i nie rzadszych niż 1 miesiąc.
2. Kopie zapasowe danych osobowych w wersji elektronicznej mogą być przechowywane na zewnętrznym nośniku danych zabezpieczonym zgodnie z zabezpieczeniami organizacyjnymi.
3. Osoba sporządzająca kopie zapasowe jest zobowiązana do ich oznaczenia oraz sprawdzenia spójności danych i możliwości ich ponownego odtworzenia.
4. Kopie zapasowe przechowuje się nie krócej niż 1 rok i nie dłużej niż 5 lat.
5. Po upływie okresu przechowywania kopie zapasowe są trwale niszczone lub anonimizowane.

§ 10. Procedura przechowywania nośników danych osobowych w wersji papierowej i elektronicznej:

1. Nośniki danych osobowych takie jak:
    a. Laptop/Netbook
    b. Telefon komórkowy/Smartfon
    c. Pendrive/Karta pamięci
    d. Zewnętrzny dysk twardy
    e. Płytka CD/DVD/BR
    f. Wydruk papierowy

    są przechowywane w sposób uniemożliwiający dostęp do nich osób nie upoważnionych jak i zabezpieczający je przed uszkodzeniem spowodowanym np.: zalaniem, spaleniem, stopieniem, itd…
2. Osoby upoważnione są zobowiązane do trwałego niszczenia/kasowania danych osobowych po ustaniu celu ich przetwarzania.
3. Zabrania się wynoszenia danych osobowych poza obszar przetwarzania bez zgody ABI lub ADO oraz zapewnienia co najmniej takich samych warunków bezpieczeństwa przetwarzania danych osobowych jakie obowiązują w obszarze przetwarzania.
4. Dane osobowe wysyłane drogą elektroniczną poza obszar przetwarzania muszą być zabezpieczone hasłem.
5. Zabrania się przekazywania nośników danych zawierających dane osobowe podmiotom zewnętrznym w celach naprawczych, darowizny, itd…

§ 11. Procedura wprowadzania i udostępniania danych osobowych podmiotom zewnętrznym:

1. Każde wprowadzenie i udostępnienie danych osobowych musi być dokonane zarówno zgodnie z Ustawą i aktami wykonawczymi jak i niniejszym dokumentem oraz posiadać podstawę prawną.
2. Prowadzi się ewidencje wprowadzanych i udostępnianych danych, określającą w szczególności:
    a. Datę wprowadzenia
    b. Określenie osoby upoważnionej wprowadzającej dane
    c. Datę udostępnienia
    d. Podmiot, któremu udostępniono dane
    e. Zakres udostępnianych lub wprowadzanych danych
    f. Podstawę udostępnienia lub wprowadzenia

§ 12. Procedury kontrolne oraz szkolenia pracowników:

1. Raz do roku przeprowadza się kontrole przestrzegania obowiązujących reguł dotyczących ochrony danych osobowych.
2. Z kontroli sporządza się protokół, który jest podstawą do dokonania aktualizacji procedur oraz niniejszego dokumentu.
3. Raz do roku przeprowadza się szkolenie aktualizacyjne pracowników w zakresie ochrony danych osobowych.
4. Każdy pracownik przed otrzymaniem upoważnienia zostaje przeszkolony indywidualnie.
5. Wszelka naprawa lub konserwacja sprzętu komputerowego zawierającego dane osobowe lub pomieszczeń stanowiących obszar przetwarzania może odbywać się tylko pod nadzorem osób upoważnionych.

§ 13. ADO lub ABI dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru, który powinien zawierać w szczególności:

1) Wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem;

2) Określenie czasu i miejsca naruszenia i powiadomienia.

3) Określenie okoliczności towarzyszących i rodzaju naruszenia.

4) Wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania.

5)Wstępną ocenę przyczyn wystąpienia naruszenia.

6) Ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

§ 13. ADO lub ABI dokonuje zgłoszenia zbioru danych osobowych wymagających zgłoszenia oraz wykreślenia zbioru po ustaniu przetwarzania, do Generalnego Inspektora Ochrony Danych Osobowych (GIODO).

Rozdział 5
Postanowienia końcowe

§ 14. Wszelkie procedury i zasady opisane w niniejszym dokumencie są przestrzegane przez osoby upoważnione do przestrzegania danych osobowych ze szczególnym uwzględnieniem dobra osób, których dane te dotyczą.
§ 15. Powierzenie przetwarzania danych osobowych podmiotowi zewnętrznemu może być dokonanie jedynie w drodze umowy zawartej na piśmie z zastrzeżeniem, iż podmiot ten spełnia co najmniej takie same warunki bezpieczeństwa przetwarzania danych osobowych jak Zespole Szkół Nr 3 w Dzierżoniowie.