Załącznik do zarządzenia nr 5/2016 – Polityka bezpieczeństwa danych osobowych

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

§ 1

1. Polityka bezpieczeństwa danych osobowych powstała w oparciu o przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych i rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

2. Dane osobowe to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

3. W Zespole Szkół Budowlanych w Rybniku stosuje się wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych, ponieważ co najmniej jeden komputer, na którym zainstalowane jest oprogramowanie wykorzystywane do przetwarzania danych osobowych, połączony jest z siecią publiczną.

4. Administrator Danych w Zespole Szkół Budowlanych wyznacza Administratora Bezpieczeństwa Informacji w celu nadzorowania i przestrzegania zasad ochrony, o których mowa w Ustawie z dnia 29 sierpnia 1997r. o ochronie danych osobowych chyba, że Administrator Danych sam wykonuje te czynności. Upoważnienie dla Administratora Bezpieczeństwa Informacji oraz zakres obowiązków określa załącznik nr 1

§ 2

Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe

1. Dane osobowe przetwarzane są w budynku Zespołu Szkół Budowlanych w Rybniku przy ul. Świerklańskiej 42, w pomieszczeniach:
    a. Sekretariatu -pokój nr 1 (zamykany na klucz, rolety zewnętrzne, czujniki ruchu połączone z powiadomieniem ochrony),
    b. Dyrektora- pokój nr 2 (zamykany na klucz, rolety zewnętrzne czujniki ruchu połączone z powiadomieniem ochrony),
    c. Wicedyrektorów - pokój nr 3 (zamykany na klucz, rolety zewnętrzne, czujniki ruchu połączone z powiadomieniem ochrony,), pokój nr 49 (zamykany na klucz, czujniki ruchu połączone z powiadomienie ochrony),
    d. Głównego Księgowego- pokój nr 4 (zamykany na klucz, kraty zewnętrzne, czujniki ruchu połączone z powiadomieniem ochrony),
    e. Biblioteki- pokój nr 26 (zamykany na klucz, czujniki ruchu połączone z powiadomienie ochrony),
    f. Pedagoga szkolnego- pokój nr 54 (zamykany na klucz, czujniki ruchu połączone z powiadomieniem ochrony),

g. Pielęgniarki szkolnej- pokój nr 57 (zamykany na klucz, czujniki ruchu połączone z powiadomieniem ochrony),
h. Kierownika gospodarczego- pokój nr 6 (zamykany na klucz, roleta wewnętrzna, czujniki ruchu połączone z powiadomieniem ochrony)
i. Pomieszczenie archiwalne – pokój nr 51(zamykane na klucz),
j. Sale lekcyjne i pracownie- klasa od nr 9,12-25,27, 42-48, 53,59-61

§ 3
Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

1. W Zespole Szkół Budowlanych w Rybniku dane osobowe przetwarzane są w zbiorach papierowych oraz odpowiadających im systemach i programach informatycznych.
2. Wykaz zbiorów danych osobowych i programów zastosowanych do ich przetwarzania:

Zbiór danych osobowych	Program zastosowany do ich przetwarzania	Pomieszczenia
Dane uczniów i związane z nimi dane rodziców (prawnych opiekunów)	Program vEdukacja (nabór)	Sekretariat, Komisji rekrutacyjnej
	Uczniowie Optivum NET+ (dziennik elektroniczny)	Sekretariat, Dyrektor, administrator dziennika, klasy 9,12-25,27, 42-48, 53,59-61
	Uczniowie Optivum NET+ (sekretariat)	Sekretariat, Administratora
	Hermes	Sekretariat, Administratora i osoby odpowiedzialnej
	MOL	Biblioteka
Dane organizacyjne (finansowo – księgowe)	Organizacja Optivum (Arkusz Optivum)	Dyrektor, Wicedyrektor, Kierownik gospodarczy, Administratora
	Organizacja Optivum (plan lekcji, zastępstwa)	Dyrektor, Wicedyrektor, Administratora
	Księgowość Optivum	Główny księgowy
Dane pracowników	Kadry Optivum, Płace Optivum	Dyrektor Wicedyrektor, Kierownik gospodarczy, Główny księgowy
Dane archiwum (składnica akt)	Uczniowie Optivum NET+, Arkusz Optivum, Kadry Optivum, Płace Optivum	Dyrektor Wicedyrektor, Kierownik gospodarczy, Główny księgowy, sekretariat, Administratora (dziennik elektroniczny)
Dane -rejestr korespondencji	Papierowy , Poczta e-mail	Sekretariat
Dane uczniów i pracowników przekazywane do serwisu internetowego szkoły i portalu społecznościowego	Serwis internetowy www.zsbrybnik.pl, facebook	Dyrektor, Biblioteka, Administratora strony
Dane zamówienia publiczne	Serwer nr 1 i nr 2 UZP, BIP	Sekretariat, Kierownik gospodarczy
Dane osobowe ubiegających się o zatrudnienie	Papierowe, Poczta e-mail	Sekretariat
Dane osobowe wypożyczających zbiory biblioteczne	MOL	Biblioteka
Dane- rejestr skarg i wniosków	Papierowe, Poczta e-mail	Sekretariat
Dane - monitoring wizyjny	Program Pillar DVR System CMS (Control Monitoring System)	Wicedyrektor, Kierownik gospodarczy

§ 4
Opis struktury zbiorów danych osobowych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi

1. Zbiór danych **„dane uczniów i związane z nimi dane rodziców (prawnych opiekunów)**" zawiera następujące pola:
    a. nazwisko i imiona,
    b. numer PESEL,
    c. adres zamieszkania,
    d. data i miejsce urodzenia,
    e. imiona i nazwisko rodziców (prawnych opiekunów),
    f. nr telefonu ucznia, rodziców (prawnych opiekunów),
    g. adres e-mail ucznia, rodziców (prawnych opiekunów).

2. Zbiór danych **„dane organizacyjne (finansowo- księgowe)"** zawiera następujące pola:
    a. nazwisko i imiona,
    b. numer PESEL,
    c. płeć,
    d. data urodzenia,
    e. staż pracy,
    f. pełniona funkcja,
    g. stopień awansu zawodowego,
    h. wynagrodzenie.

3. Zbiór danych **„dane pracowników"** zawiera następujące pola:
    a. nazwisko i imiona,
    b. imiona rodziców
    c. data i miejsce urodzenia
    d. numer PESEL,
    e. numer NIP,
    f. seria i numer dowodu osobistego,
    g. nazwisko rodowe,
    h. obywatelstwo,
    i. oddział NFZ,
    j. urząd skarbowy,
    k. adres stałego zameldowania
    l. adres zamieszkania
    m. adres korespondencyjny
    n. wykształcenie,
    o. staż pracy,
    p. ilość godzin,
    q. wynagrodzenie,
    r. stosunek do służby wojskowej,
    s. nr telefonu,
    t. adres e-mail
4. Zbiór danych **„dane archiwum (składnica akt)"** w formie papierowej i elektronicznej z godnie z punktem 1 do 10
5. Zbiór danych „ **dane -rejestr korespondencji**"

6. Zbiór danych „**dane uczniów i pracowników przekazywane do serwisu internetowego szkoły portalu społecznościowego**” zawiera następujące pola (www.zsbrybnik.pl, facebook):
    a. nazwisko i imię,
    b. wizerunek absolwentów,
    c. wyniki konkursu,
    d. udział w wycieczkach,
    e. udział w imprezach szkolnych i prelekcjach.

    Dane przekazywane są do systemu informatycznego www.zsbrybnik.pl.
7. Zbiory danych **„ dane zamówienia publiczne**” zawiera następujące pola:
    a. nazwa firmy,
    b. adres siedziby,
    c. imię i nazwisko właściciela lub pełnomocnika,
    d. NIP,
    e. REGON,
    f. telefon, fax,
    g. adres e-mail
    h. nazwa banku i nr konta bankowego,
8. Zbiory danych ”**dane osobowe ubiegających się o zatrudnienie**” w formie papierowej i elektronicznej zawiera następujące pola:
    a. nazwisko i imię,
    b. wizerunek,
    c. data i miejsce urodzenia
    d. adres stałego zameldowania
    e. adres zamieszkania
    f. adres korespondencyjny
    g. wykształcenie,
    h. staż pracy,
    i. miejsce zatrudnienia,
9. Zbiory danych **„dane osobowe wypożyczających zbiory biblioteczne”** zawiera następujące pola:
    a. nazwisko imię,
    b. wizerunek,
    c. adres zamieszkania,
    d. PESEL,
    e. nr telefonu
    f. adres e-mail.
10. Zbiory danych **„dane- rejestr skarg i wniosków”** zawiera następujące pola:
    a. nazwisko i imię,
    b. adres zamieszkania,
    c. adres korespondencyjny,
    d. numer telefonu
11. Zbiory danych **„dane -monitoring wizyjny”** w formie elektronicznej zawiera następujące pola:
    a. wizerunek
12. Zbiory danych **„dane stażystów i praktykantów”** w formie elektronicznej zawiera następujące pola:
    a. nazwisko i imię,
    b. wizerunek,

c. data i miejsce urodzenia
d. adres stałego zameldowania
e. adres zamieszkania
f. adres korespondencyjny
g. wykształcenie,
h. staż pracy,
i. miejsce zatrudnienia,

13. Zbiory danych **„dane z rekrutacji i związane z nimi dane rodziców (prawnych opiekunów)**"w formie elektronicznej zawiera następujące pola:
    a. nazwisko i imiona,
    b. numer PESEL,
    c. adres zamieszkania,
    d. data i miejsce urodzenia,
    e. imiona i nazwisko rodziców (prawnych opiekunów),
    f. nr telefonu ucznia, rodziców (prawnych opiekunów),
    g. adres e-mail ucznia, rodziców (prawnych opiekunów).

§ 5

Sposób przepływu danych pomiędzy poszczególnymi systemami

1. Program vEdukacja Nabór- szkoły ponadgimnazjalne dostarcza dane kandydatów (i odbiera dane przyjętych uczniów) i przesyła je do programu Uczniowie Optivum NET+. Ponadto Uczniowie Optimum NET + przejmuje plany nauczania oddziałów z Arkusza Optivum.
2. Uczniowie Optimum NET+ oraz Arkusz Optivum eksportują dane do Integratora SIO-Optivum .
3. Uczniowie Optimum NET + eksportują dane do programu Hermes.
4. Program Kadry Optivum dostarcza dane płacowe do programu Płace Optivum.
5. Program MOL importuje dane z programu Uczniowie Optimum NET+.

§ 6

Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. <u>Poufność:</u>

a). upoważnienie do przetwarzania danych osobowych,
b). rejestr osób upoważnionych do przetwarzania danych osobowych,
c). identyfikator użytkownika i hasło dostępu,
d). użytkownik ma obowiązek zablokowania stacji roboczej lub wylogowania się z systemu informatycznego służącego do przetwarzania danych osobowych w przypadku czasowego opuszczenia stanowiska pracy,
e). zakończenie pracy w systemie służącym do przetwarzania danych osobowych poprzedzone jest zabezpieczeniem przed nieuprawnionym dostępem dodatkowych nośników danych, takich jak dyskietki, płyty CD i inne, zawierających dane osobowe,
f). nośniki informatyczne zawierające dane osobowe lub kopie systemów informatycznych służących do przetwarzania danych osobowych są przechowywane w sposób uniemożliwiający ich utratę, uszkodzenie lub dostęp osób nieuprawnionych,

g). przed ich likwidacją nośników informatycznych zawierających dane osobowe lub kopie zapasowe systemów informatycznych służących do przetwarzania danych osobowych dane osobowe zostają usunięte lub uszkodzone w sposób uniemożliwiający ich odczyt,
h). po upływie okresu użyteczności lub przechowywania, dane osobowe zostają skasowane lub zniszczone tak, aby nie było możliwe ich odczytanie,
i). zakaz wynoszenia poza pomieszczenia stanowiące obszar przetwarzania danych osobowych elektronicznych nośników informacji zawierających dane osobowe oraz kopie zapasowe,
j). elektroniczne nośniki informacji zawierających dane osobowe oraz kopie zapasowe, a także wydruki i inne dokumenty zawierające dane osobowe przechowywane są w zamykanych szafach w pomieszczeniach stanowiących obszar przetwarzania danych osobowych, w sposób zabezpieczający je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem i zniszczeniem,
k). uszkodzony lub zużyty nośnik informacji zwierający dane osobowe zostaje fizycznie zniszczony tak, aby nie było możliwe odczytanie danych osobowych,
l). dane osobowe przesyłane poprzez sieć Internet zabezpieczone są poprzez środki kryptograficznej ochrony,
m). przeglądy i konserwacje sprzętu komputerowego oraz nośników informacji służących do przetwarzania danych osobowych, przeprowadzane są w pomieszczeniach stanowiących obszar przetwarzania danych osobowych,
n). w przypadku przekazywania do naprawy sprzętu komputerowego z zainstalowanym systemem informatycznym służącym do przetwarzania danych osobowych lub nośnikiem informacji służących do przetwarzania danych osobowych, powinien on zostać pozbawiony danych osobowych przez fizyczne wymontowanie dysku lub skasowanie danych lub naprawa powinna zostać przeprowadzona w obecności administratora danych,
o). ekrany komputerów umieszczone są w sposób uniemożliwiający obserwację przetwarzania danych przez osoby postronne,
p). dokumenty papierowe i zewnętrze nośniki komputerowe, gdy nie są używane, a szczególnie poza godzinami pracy, przechowywane są w zamykanych szafach lub innego rodzaju zabezpieczanych meblach,
q). fotokopiarki zostają zablokowane lub w inny sposób chronione przed nieuprawnionym użyciem poza normalnymi godzinami pracy,
r). każdy dokument zawierający dane osobowe lub inne dane umożliwiające identyfikację osób, po ustaniu jego użyteczności przenosi się do archiwum lub o ile nie podlega archiwizacji – usuwa się w niszczarce do papieru,
s). elektroniczne archiwa danych osobowych zgromadzone na płytach CD lub DVD są przechowywane w zabezpieczonym miejscu innej strefy pożarowej.

2. <u>Integralność:</u>

a). upoważnienie do przetwarzania danych osobowych,
b). użytkownik musi obowiązek zablokowania stacji roboczej lub wylogowania się z systemu informatycznego służącego do przetwarzania danych osobowych w przypadku czasowego opuszczenia stanowiska pracy,
c). zakończenie pracy w systemie służącym do przetwarzania danych osobowych poprzedzone jest zabezpieczeniem przed nieuprawnionym dostępem dodatkowych nośników danych, takich jak dyskietki, płyty CD i inne, zawierających dane osobowe,

d). uszkodzony lub zużyty nośnik informacji zwierający dane osobowe zostaje fizycznie zniszczony tak, aby nie było możliwe odczytanie danych osobowych,
e). dane osobowe przesyłane poprzez sieć Internet zabezpieczone są poprzez środki kryptograficznej ochrony,
f). w przypadku przekazywania do naprawy sprzętu komputerowego z zainstalowanym systemem informatycznym służącym do przetwarzania danych osobowych lub nośnikiem informacji służących do przetwarzania danych osobowych, powinien on zostać pozbawiony danych osobowych przez fizyczne wymontowanie dysku lub skasowanie danych lub naprawa powinna zostać przeprowadzona w obecności administratora danych.
g). sieć komputerowa skanowana jest dynamicznie pod kątem występowania wirusów komputerowych,
h). kluczowe systemy chronione są przez systemy podtrzymania napięcia UPS,
i). niemożliwe jest zalogowanie się do systemu jako anonimowy użytkownik.

3. Rozliczalność:

a). identyfikator użytkownika i hasło dostępu,
b). zakaz przydzielania identyfikatora danego użytkownika innemu użytkownikowi, nawet po wyrejestrowaniu tego pierwszego z systemu informatycznego służącego do przetwarzania danych osobowych,
c). zakaz wykonywania jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych z wykorzystaniem identyfikatora i hasła dostępu innego użytkownika,
d). w systemie informatycznym służącym do przetwarzania danych osobowych odnotowywane są informacje o odbiorcach danych, a w szczególności imię i nazwisko lub nazwa odbiorcy, data udostępnienia oraz zakres udostępnienia.

§ 7
Procedura alarmowa

1. Administrator danych wprowadza procedurę alarmową stanowiącą załącznik nr 2 do polityki bezpieczeństwa.
2. Administrator danych wprowadza dokument o nazwie: „ Sprawozdanie roczne stanu ochrony danych osobowych” stanowiącą załącznik nr 3 do polityki bezpieczeństwa.

Załącznik nr 1 do „Polityki Bezpieczeństwa" z dnia ……

…….
miejscowość i data

Upoważnienie dla Administratora Bezpieczeństwa Informacji oraz zakres obowiązków

Na podstawie § 1ust.4 Polityki Bezpieczeństwa z dnia ……. zgodnie z założeniami **ROZPORZĄDZENIEM 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**

Na podstawie art. 36.3 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997r. (Dz. U. z 2014 r. poz. 1182, 1662)

Administrator Danych *(imię i nazwisko)*.....powołuje w podmiocie *(nazwa firmy)*.....NIP:.....
Administratora Bezpieczeństwa Informacji *(imię i nazwisko*)…….
PESEL .....

1. Upoważnienie jest ważne od chwili podpisania przez strony do dnia wycofania upoważnienia przez **Administrator Danych.**
2. **Administrator Bezpieczeństwa Informacji** jest zobowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
3. **Administrator Bezpieczeństwa Informacji** jest zobowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1.
4. **Administrator Bezpieczeństwa Informacji** jest odpowiedzialny za przestrzeganie w podmiocie zapisów Instrukcji Zarządzania Systemem Informatycznym. **Administrator Bezpieczeństwa Informacji** prowadzi wszelką dokumentację opisującą sposób przetwarzania danych w podmiocie a w szczególności:
    a. zgodnie z § 2. „Polityki Bezpieczeństwa" Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe,
    b. zgodnie z § 3. „Polityki Bezpieczeństwa" Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
    c. zgodnie z § 4 i 5. „Polityki Bezpieczeństwa" Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami,
    d. zgodnie z § 6. „Polityki Bezpieczeństwa" Ewidencję osób przetwarzających dane w podmiocie posiadających upoważnienie - załącznik nr 4 do „Instrukcji Zarządzania Systemem Informatycznym"
    e. Zestawienie danych osobowych. Kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. – załącznik nr 4 do „Polityki Bezpieczeństwa"

Oświadczam, że zapoznałem się z treścią i obowiązkami wynikającymi z tego upoważnienia oraz, że jako administrator bezpieczeństwa informacji, będę nadzorował przestrzeganie zasad ochrony danych w podmiocie..... zgodnie z obowiązkami wynikającymi z tego upoważnienia oraz ustawy o ochronie danych osobowych.

Administrator Bezpieczeństwa Informacji

…….
Podpis

Administrator Danych

…….
Podpis

Załącznik nr 2 do „Polityki Bezpieczeństwa" z dnia ……

„Procedura Alarmowa"

Administrator Danych: **Dyrektor szkoły - Marek Florczyk** Dnia .....w podmiocie o nazwie: **Zespół Szkół Budowlanych , 44-200 Rybnik, ul. Świerklańska 42**

w celu pełnej kontroli oraz zapobieganiu możliwym zagrożeniom związanym z ochroną danych osobowych na podstawie art. 36.1. ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 i Nr 153, poz. 1271 oraz z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285)

wdraża dokument o nazwie „Procedura Alarmowa".

Zapisy tego dokumentu wchodzą w życie

z dniem.....

§ 1.

1. Ilekroć w „Procedurze alarmowej" jest mowa o:
   a). **Uchybieniu** –rozumie się przez to świadome lub nieświadome działania zmierzające do zagrożenia, wskutek których może dojść do utraty danych osobowych, kradzieży danych osobowych lub uszkodzenia nośników danych.
   b). **Zagrożeniu -** rozumie się przez to świadome lub nieświadome działania, wskutek których doszło do utraty danych osobowych, kradzieży danych osobowych lub uszkodzenia nośników danych.
   c). **ABI** - rozumie się przez to Administrator Bezpieczeństwa Informacji
   d). **ADO** - rozumie się przez to Administrator Danych Osobowych

§ 2.

Procedura alarmowa

1. Procedura alarmowa wskazuje na możliwe zagrożenia oraz definiuje „Dziennik Uchybień i Zagrożeń", związany z niewłaściwym przetwarzaniem danych osobowych lub ich wyciekiem.
2. Celem Procedury Alarmowej jest skatalogowanie możliwych uchybień i zagrożeń oraz opisanie procedur działania w przypadku ich wystąpienia, jak i również ograniczenie ich powstania w przyszłości.
3. Integralną częścią Procedury Alarmowej jest „Dziennik Uchybień i Zagrożeń" - (załącznik nr 1), „Protokół Zagrożenia" - (załącznik nr 2), „Protokół Uchybienia" - (załącznik nr 3), prowadzony przez ABI w przypadku stwierdzenia naruszenia ochrony danych osobowych w podmiocie.

§ 3.

Charakterystyka możliwych „Uchybień i Zagrożeń"

I. Uchybienia i zagrożenia nieświadome wewnętrzne i zewnętrzne

I. Do uchybień i zagrożeń nieświadomych wewnętrznych i zewnętrznych należą działania pracowników podmiotu lub osób nie będących pracownikami podmiotu, w następstwie których może dojść lub doszło do zniszczenia danych, wycieku danych lub naruszenia ich poufności. W szczególności są to działania takie jak:
   a. niewłaściwe zabezpieczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe,

b. niewłaściwe zabezpieczenie sprzętu komputerowego,
c. dopuszczenie do przetwarzania danych przez osoby nie posiadające upoważnienia,
d. pomyłki informatyków,
e. kradzież danych,
f. kradzież sprzętu informatycznego,
g. działanie wirusów i innego szkodliwego oprogramowania oraz inne działania, wskutek których dojdzie do utraty danych osobowych lub uszkodzenia nośników danych.

II. Uchybienia i zagrożenia umyślne wewnętrzne i zewnętrzne

1. Do uchybień i zagrożeń umyślnych wewnętrznych i zewnętrznych należą celowe działania pracowników podmiotu, w następstwie których może dojść lub doszło do zniszczenia danych, wycieku danych lub naruszenia ich poufności. W szczególności są to działania takie jak:
    a. celowe zniszczenie danych osobowych lub nośników danych,
    b. kradzież danych osobowych,
    c. dopuszczenie do przetwarzania danych przez osoby nie posiadające upoważnienia,
    d. kradzież danych,
    e. kradzież sprzętu informatycznego,
    f. działanie wirusów i innego szkodliwego oprogramowania oraz inne działania, wskutek których dojdzie do utraty danych osobowych lub uszkodzenia nośników danych.

III. Uchybienia i zagrożenia losowe

1. Do uchybień i zagrożeń losowych należą sytuacje losowe, w następstwie których może dojść lub doszło do zniszczenia danych, wycieku danych lub naruszenia ich poufności. W szczególności są to sytuacje takie jak:
    a. klęski żywiołowe,
    b. przerwy w zasilaniu,
    c. awarie serwera,
    d. pożar,
    e. zalanie wodą.

§ 4.

Procedura postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych.

1. Każdy pracownik podmiotu posiadający upoważnienie do przetwarzania danych osobowych, w przypadku stwierdzenia uchybienia lub zagrożenia ma obowiązek niezwłocznie powiadomić o tym fakcie Administratora Bezpieczeństwa Informacji lub Administratora Danych.
2. Administrator Bezpieczeństwa Informacji w przypadku stwierdzenia uchybienia ma obowiązek:
    a. odnotować każde uchybienie w „Dzienniku Uchybień i Zagrożeń”
    b. sporządzić „Protokół Uchybienia”
    c. wprowadzić procedury uniemożliwiające ponowne powstanie uchybienia
3. Administrator Bezpieczeństwa Informacji w przypadku stwierdzenia zagrożenia ma obowiązek:
    a. zabezpieczyć dowody, powiadomić policję (w przypadku włamania)
    b. zabezpieczyć dane osobowe oraz nośniki danych

c. odnotować każde zagrożenie w „Dzienniku Uchybień i Zagrożeń”

d. sporządzić „Protokół Zagrożenia”

e. wprowadzić procedury uniemożliwiające ponowne powstanie zagrożenia

f. powiadomić o zaistniałej sytuacji Administratora Danych

g. podjąć próbę przywrócenia stanu sprzed zaistnienia zagrożenia

h. ADO wyciąga konsekwencje dyscyplinarne wobec osób odpowiedzialnych za zagrożenie.

§ 5.

Rejestr Uchybień i Zagrożeń oraz szczegółowa instrukcja postępowania dla osób posiadających upoważnienie do przetwarzania danych osobowych w podmiocie

Kod uchybienia lub zagrożenia	Uchybienia i zagrożenia nieświadome wewnętrzne i zewnętrzne	Postępowanie w przypadku uchybienia lub zagrożenia
1.	Pomieszczenie, w którym przechowywane są dane osobowe pozostaje bez nadzoru.	Należy zabezpieczyć dane osobowe oraz powiadomić ABI. ABI sporządza protokół uchybienia.
2.	Komputer nie jest zabezpieczony hasłem.	Należy zabezpieczyć dane osobowe oraz powiadomić ABI. ABI sporządza protokół uchybienia.
3.	Dostęp do danych osobowych mają osoby nie posiadające upoważnienia.	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić ABI. ABI sporządza protokół uchybienia.
4.	Nieuprawniony dostęp do otwartych aplikacji w systemie informatycznym.	Należy powiadomić ABI, który powinien sprawdzić system uwierzytelniania oraz sprawdzić czy nie doszło do kradzieży lub zniszczenia danych. ABI sporządza protokół uchybienia.
5.	Próba kradzieży danych osobowych poprzez zewnętrzny nośnik danych.	Należy nie dopuścić do kradzieży danych i powiadomić ABI. ABI powinien zabezpieczyć nośnik danych i powiadomić ADO. ABI sporządza protokół zagrożenia.
6.	Próba kradzieży danych osobowych w formie papierowej.	Należy nie dopuścić do kradzieży danych i powiadomić ABI. ABI powinien zabezpieczyć dane i powiadomić ADO. ABI sporządza protokół zagrożenia.
7.	Nieuprawniony dostęp do danych osobowych w formie papierowej.	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić ABI. ABI sporządza protokół uchybienia.
8.	Dane osobowe przechowywane są w niezabezpieczonym pomieszczeniu.	Należy powiadomić ABI. ABI powinien zabezpieczyć pomieszczenie. ABI sporządza protokół uchybienia.
9.	Próba włamania do pomieszczenia/budynku.	Należy zabezpieczyć dowody i powiadomić ABI. ABI sprawdza stan uszkodzeń, zabezpiecza dowody i wzywa policję. ABI sporządza protokół zagrożenia.
10.	Działanie zewnętrznych aplikacji, wirusów, złośliwego oprogramowania.	Należy zrobić audyt systemów zabezpieczeń, a w szczególności systemów antywirusowych, firewall. ABI powinien ocenić, czy nie doszło do utraty danych osobowych i w zależności od tego sporządzić protokół uchybienia lub zagrożenia.
11.	Brak aktywnego oprogramowania antywirusowego.	Należy powiadomić ABI. ABI powinien zaktualizować lub nabyć oprogramowanie antywirusowe. ABI sporządza protokół uchybienia.
12.	Zniszczenie lub modyfikacja danych osobowych w formie papierowej.	Należy zabezpieczyć dowody i powiadomić ABI. ABI sprawdza stan uszkodzeń, zabezpiecza dowody i powiadamia ADO. ABI sporządza protokół zagrożenia.
13.	Zniszczenie lub modyfikacja danych osobowych w systemie	Należy zabezpieczyć dowody i powiadomić ABI. ABI sprawdza stan uszkodzeń, zabezpiecza dowody

	informatycznym.	i powiadamia ADO. ABI sporządza protokół zagrożenia.
14.	Uszkodzenie komputerów, nośników danych.	Należy powiadomić ABI. ABI powinien ocenić w wyniku czego doszło do zniszczenia i przywrócić dane z kopii zapasowej. ABI powiadamia ADO i sporządza protokół zagrożenia.
15.	Próba nieuprawnionej interwencji przy sprzęcie komputerowym.	Należy uniemożliwić dostęp osób do sprzętu komputerowego oraz powiadomić ABI. ABI sporządza protokół uchybienia.
16.	Zdarzenia losowe.	Należy oszacować powstałe starty i sporządzić protokół zagrożenia lub uchybienia.

„Dziennik Uchybień i Zagrożeń”

(załącznik nr 1 do Procedury Alarmowej)

Kod	Data i godzina zdarzenia	Rodzaj zdarzenia *(uchybienie/zagrożenie)*	Opis zdarzenia	Skutki zdarzenia	Działania naprawcze	Podpis ABI

adres podmiotu

.....

Miejscowość i data

.....

„Protokół Zagrożenia”

(załącznik nr 2 do Procedury Alarmowej)

Data i godzina wystąpienia zagrożenia .....

Kod zagrożenia .....

Opis zagrożenia

.....
.....
.....
.....
.....

Przyczyny powstania zagrożenia

.....
.....
.....
.....
.....

Zaistniałe skutki zagrożenia

.....
.....
.....
.....
.....

Podjęte działania naprawczo-zapobiegawcze

.....
.....
.....
.....

Administrator Bezpieczeństwa Informacji	**Administrator Danych Osobowych**
….....	….....
Podpis	Podpis
Nazwa i adres podmiotu	Miejscowość i data
.....….....	.....

„Protokół Uchybienia”

(załącznik nr 3 do Procedury Alarmowej)

Data i godzina wystąpienia uchybienia.....

Kod uchybienia .....

Opis uchybienia

.....
.....
.....
.....
.....

Przyczyny powstania uchybienia

.....
.....
.....
.....
.....

Zaistniałe skutki uchybienia

.....
.....
.....
.....
.....

Podjęte działania naprawczo-zapobiegawcze

.....
.....
.....
.....
.....

Administrator Bezpieczeństwa Informacji

…….
Podpis

Administrator Danych Osobowych

.....
Podpis

Załącznik nr 3 do „Polityki Bezpieczeństwa" z dnia …….

„Sprawozdanie roczne stanu systemu ochrony danych osobowych"

Administrator Danych: **Dyrektor szkoły - Marek Florczyk** Dnia .....w podmiocie o nazwie: **Zespół Szkół Budowlanych , 44-200 Rybnik, ul. Świerklańska 42**

w celu pełnej kontroli oraz zapobieganiu możliwym zagrożeniom związanym z ochroną danych osobowych na podstawie art. 36.1. ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz.926 i Nr 153, poz. 1271 oraz z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285)

wdraża dokument o nazwie

„Sprawozdanie roczne stanu systemu ochrony danych osobowych".

Zapisy tego dokumentu wchodzą w życie

z dniem .....

1. „**Sprawozdanie roczne stanu systemu ochrony danych osobowych"** przeprowadza się raz w roku, z datą rok od chwili wejścia w życie tego dokumentu. Osobą odpowiedzialną za przygotowanie sprawozdania rocznego w podmiocie jest ABI. Sprawozdanie roczne przygotowuje się na podstawie dokumentu o nazwie **„Raport roczny",** który stanowi załącznik nr 1 do „Sprawozdania rocznego stanu systemu ochrony danych osobowych" w podmiocie. Po przeprowadzeniu analizy stanu ochrony danych osobowych w podmiocie oraz uzupełnieniu „Raportu rocznego" ABI zwołuje zebranie, w którym uczestniczą: ABI, ADO i kierownicy działów lub referatów, w których przetwarzane są dane osobowe. Podczas zebrania ABI przedstawia uczestnikom stan zabezpieczeń, stan infrastruktury informatycznej, „Dziennik uchybień i zagrożeń" oraz omawiane są procedury zabezpieczające podmiot przed sytuacjami, w których może dojść do zniszczenia danych, wycieku danych lub naruszenia ich poufności.

„Raport roczny”

(załącznik nr 1 do „Sprawozdania rocznego stanu systemu ochrony danych osobowych”)

Nazwa i adres podmiotu ….....	Miejscowość i data …..
Zagadnienia omawiane na zebraniu	**Uwagi/wnioski**
Podsumowanie realizacji wytycznych z poprzedniego „Sprawozdania rocznego stanu systemu ochrony danych osobowych”	
Omówienie zmian procedur w systemie oraz zmian w systemie informatycznym	
Omówienie Dziennika Uchybień i Zagrożeń	

Wnioski oraz zadania do realizacji	
Uczestnicy zebrania	Podpis uczestnika
Podpis ABI	Podpis ADO

Zestawienie danych osobowych z informacją kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

załącznik nr 4 do „Polityki Bezpieczeństwa” zgodnie z art. 38 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.

Lp.	Rodzaj udostępnionych danych osobowych	Data wprowadzenia danych do zbioru	Data przekazania danych osobowych	Imię i nazwisko osoby która otrzymała dane	Cel przekazania danych osobowych

Data i podpis Administratora Danych

……