Zespół Obsługi Placówek Oświaty
w Okonku, ul. Leśna 46
64-965 OKONEK
NIP 767-15-70-923 REGON 572106468
tel. 067 266 91 45

ZARZĄDZENIE NR 20/2015
Dyrektora Zespołu Obsługi Placówek Oświaty w Okonku
z dnia 29 października 2015 roku

w sprawie „Polityki Bezpieczeństwa w Zespole Obsługi Placówek Oświaty w Okonku" i „Instrukcji Zarządzania Systemem Informatycznym".

Na podstawie art. 36 ust. 1, 2 i 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182 z późn. zm.) oraz § 3, 4 i 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) zarządza się, co następuje:

§ 1. Wprowadza się „Politykę Bezpieczeństwa Informacji w Zespole Obsługi Placówek Oświaty w Okonku" stanowiącą załącznik Nr 1 do niniejszego zarządzenia.

§ 2. Wprowadza się „Instrukcję Zarządzania Systemem Informatycznym w Zespole Obsługi Placówek Oświaty w Okonku" stanowiącą załącznik Nr 2 do niniejszego zarządzenia.

§ 3. Zobowiązuje się wszystkie osoby przetwarzające dane osobowe w Zespole Obsługi Placówek Oświaty w Okonku do przestrzegania zasad i realizacji zadań określonych w załącznikach, o których mowa w § 1 i 2.

§ 4. Wyznacza się Panią Annę Mliczak – inspektora ds. księgowości na Administratora Bezpieczeństwa Informacji w Zespole Obsługi Placówek Oświaty w Okonku.

§ 5. Traci moc zarządzenie nr 27 z dnia 29 grudnia 2011 roku Dyrektora Zespołu Obsługi Placówek Oświaty w Okonku w sprawie ustalenia „Polityki Bezpieczeństwa i instrukcji zarządzania systemów informatycznych służących do przetwarzania danych osobowych w ZOPO".

§ 6. Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
Zespołu Obsługi Placówek Oświaty
w Okonku
Renata Zabrocka

Załącznik nr 1
do Zarządzenie nr 20/2015
z 28.10.2015 r.

DYREKTOR
Zespołu Obsługi Placówek Oświaty
w Okonku

POLITYKA BEZPIECZEŃSTWA

Administrator Danych.....Renata Zabrocka.....

Dnia 28.10.2015 w podmiocie o nazwie .....

Zespół Obsługi Placówek Oświaty
w Okonku, ul. Leśna 46
64-965 OKONEK
NIP 767-15-70-923 REGON 572106468
tel. 067 [illegible]

Zgodnie z **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 (Dz. U. Nr 100, poz. 1024)
wdraża dokument o nazwie „Polityka Bezpieczeństwa". Zapisy tego dokumentu wchodzą w życie
z dniem.....28.10.2015.....

Zespół Obsługi Placówek Oświaty
w Okonku, ul. Leśna 46
64-965 OKONEK
NIP 767-15-70-923 REGON 572106468
tel. [illegible]

§ 1.

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w .....(nazwa podmiotu), określa zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.
Polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa przetwarzanych danych.
Polityka bezpieczeństwa dotyczy danych osobowych przetwarzanych w zbiorach manualnych oraz w systemach informatycznych.

§ 2

Ilekroć w „Polityce Bezpieczeństwa" jest mowa o:

1.zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
2.przetwarzaniu 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,
3.systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
4.zabezpieczeniu danych w systemie informatycznym - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
5.usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
6.administratorze danych - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych,
7.administratorze bezpieczeństwa informacji – rozumie się przez to osobę wyznaczoną przez Administratora Danych w celu nadzorowania i przestrzegania zasad ochrony, o których mowa w ust. 1, chyba, że Administrator Danych sam wykonuje te czynności.
8.podmiocie – rozumie się przez to spółkę prawa handlowego, podmiot gospodarczy nie posiadający osobowości prawnej, jednostkę budżetową;

§ 3.

Administrator Danych w podmiocie.....wyznacza **Administratora Bezpieczeństwa Informacji** w celu nadzorowania i przestrzegania zasad ochrony, o których mowa w USTAWIE z dnia 29 sierpnia 1997 r. o ochronie danych osobowych chyba, że Administrator Danych sam wykonuje te czynności. Upoważnienie dla **Administratora Bezpieczeństwa Informacji** oraz zakres obowiązków określa **załącznik do „Polityki Bezpieczeństwa" nr 1**

§ 4.

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe określa **załącznik do „Polityki Bezpieczeństwa" nr 2**

§ 5.

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych określa **załącznik do „Polityki Bezpieczeństwa" nr 3**

§ 6.

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami określa **załącznik do „Polityki Bezpieczeństwa" nr 4**

§ 7.

Administratora Bezpieczeństwa Informacji dba o to aby dane osobowe w formie papierowej były niedostępne dla osób nieupoważnionych. Dokumenty powinny znajdować się w pomieszczeniu zamykanym na klucz do którego dostęp mają tylko osoby posiadające aktualne upoważnienie do przetwarzania danych osobowych.

§ 8.

Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez **Administratora Danych** lub **Administratora Bezpieczeństwa Informacji**. **Administrator Bezpieczeństwa Informacji** jest obowiązany 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. Administrator Bezpieczeństwa Informacji nadaje uprawnienia pracownikom którzy przetwarzają dane poprzez podpisanie oświadczenia które stanowi **załącznik nr 5 do „Polityki Bezpieczeństwa"**. Administrator Bezpieczeństwa Informacji prowadzi wszelką dokumentację opisującą sposób przetwarzania danych w podmiocie a w szczególności:

1. Ewidencja osób przetwarzających dane w podmiocie posiadających upoważnienie – **załącznik nr 6** do „Polityki Bezpieczeństwa"

2. Zestawienie danych osobowych. Kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. – **załącznik nr 7** do „Polityki Bezpieczeństwa"

§ 9.

Na wniosek osoby, której dane dotyczą, Administrator Bezpieczeństwa Informacji jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić, odnośnie do jej danych osobowych, informacji.

§ 10.

Administrator Bezpieczeństwa Informacji może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych osobowych w podmiocie. Podmiot ten,

może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

§ 11.

Sposób zabezpieczenia oraz przetwarzania danych w systemie informatycznym reguluje Instrukcja Zarządzania Systemem Informatycznym.

§ 12.

W sprawach nieuregulowanych w niniejszej „Polityce Bezpieczeństwa" mają zastosowanie odpowiednie przepisy ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. oraz **ROZPORZĄDZENIA MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI** z dnia 29 kwietnia 2004 r. **w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych**

Podpis Administratora Danych Osobowych

DYREKTOR
Zespołu Obsługi Placówek Oświaty
w Okonku
Renata Żabrocka

.....

Podpis

Podpis Administratora Bezpieczeństwa Informacji

29.10.2015

.....

Podpis

Zespół Obsługi Placówek Oświaty
w Okonku, ul. Leśna 46
64-965 OKONEK
NIP 767-15-70-923 REGON 572106468
tel. 067 266 91 45

ZARZĄDZENIE NR 20/2015
Dyrektora Zespołu Obsługi Placówek Oświaty w Okonku
z dnia 29 października 2015 roku

w sprawie „Polityki Bezpieczeństwa w Zespole Obsługi Placówek Oświaty w Okonku" i „Instrukcji Zarządzania Systemem Informatycznym".

Na podstawie art. 36 ust. 1, 2 i 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182 z późn. zm.) oraz § 3, 4 i 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) zarządza się, co następuje:

§ 1. Wprowadza się „Politykę Bezpieczeństwa Informacji w Zespole Obsługi Placówek Oświaty w Okonku" stanowiącą załącznik Nr 1 do niniejszego zarządzenia.

§ 2. Wprowadza się „Instrukcję Zarządzania Systemem Informatycznym w Zespole Obsługi Placówek Oświaty w Okonku" stanowiącą załącznik Nr 2 do niniejszego zarządzenia.

§ 3. Zobowiązuje się wszystkie osoby przetwarzające dane osobowe w Zespole Obsługi Placówek Oświaty w Okonku do przestrzegania zasad i realizacji zadań określonych w załącznikach, o których mowa w § 1 i 2.

§ 4. Wyznacza się Panią Annę Mliczak – inspektora ds. księgowości na Administratora Bezpieczeństwa Informacji w Zespole Obsługi Placówek Oświaty w Okonku.

§ 5. Traci moc zarządzenie nr 27 z dnia 29 grudnia 2011 roku Dyrektora Zespołu Obsługi Placówek Oświaty w Okonku w sprawie ustalenia „Polityki Bezpieczeństwa i instrukcji zarządzania systemów informatycznych służących do przetwarzania danych osobowych w ZOPO".

§ 6. Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
Zespołu Obsługi Placówek Oświaty
w Okonku
Renata Zabrocka

Załącznik nr 1
do Zarządzenie nr 20/2015
z 28.10.2015 r.

POLITYKA BEZPIECZEŃSTWA

DYREKTOR
Zespołu Obsługi Placówek Oświaty
w Okonku

Administrator Danych.....Renata Zabrocka.....

Dnia 28.10.2015 w podmiocie o nazwie .....

Zespół Obsługi Placówek Oświaty
w Okonku, ul. Leśna 46
64-965 OKONEK
NIP 767-15-70-923 REGON 572106468
tel. 067 [illegible]

Zgodnie z **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 (Dz. U. Nr 100, poz. 1024)
wdraża dokument o nazwie „Polityka Bezpieczeństwa". Zapisy tego dokumentu wchodzą w życie
z dniem.....28.10.2015.....

Zespół Obsługi Placówek Oświaty
w Okonku, ul. Leśna 46
64-965 OKONEK
NIP 767-15-70-923 REGON 572106468
tel. 67 [illegible]

§ 1.

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w ..... (nazwa podmiotu), określa zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.
Polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa przetwarzanych danych.
Polityka bezpieczeństwa dotyczy danych osobowych przetwarzanych w zbiorach manualnych oraz w systemach informatycznych.

§ 2

Ilekroć w „Polityce Bezpieczeństwa" jest mowa o:

1.zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
2.przetwarzaniu 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,
3.systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
4.zabezpieczeniu danych w systemie informatycznym - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
5.usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
6.administratorze danych - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych,
7.administratorze bezpieczeństwa informacji – rozumie się przez to osobę wyznaczoną przez Administratora Danych w celu nadzorowania i przestrzegania zasad ochrony, o których mowa w ust. 1, chyba, że Administrator Danych sam wykonuje te czynności.
8.podmiocie – rozumie się przez to spółkę prawa handlowego, podmiot gospodarczy nie posiadający osobowości prawnej, jednostkę budżetową;

§ 3.

Administrator Danych w podmiocie.....wyznacza **Administratora Bezpieczeństwa Informacji** w celu nadzorowania i przestrzegania zasad ochrony, o których mowa w USTAWIE z dnia 29 sierpnia 1997 r. o ochronie danych osobowych chyba, że Administrator Danych sam wykonuje te czynności. Upoważnienie dla **Administratora Bezpieczeństwa Informacji** oraz zakres obowiązków określa **załącznik do „Polityki Bezpieczeństwa" nr 1**

§ 4.

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe określa **załącznik do „Polityki Bezpieczeństwa" nr 2**

§ 5.

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych określa **załącznik do „Polityki Bezpieczeństwa" nr 3**

§ 6.

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami określa **załącznik do „Polityki Bezpieczeństwa" nr 4**

§ 7.

Administratora Bezpieczeństwa Informacji dba o to aby dane osobowe w formie papierowej były niedostępne dla osób nieupoważnionych. Dokumenty powinny znajdować się w pomieszczeniu zamykanym na klucz do którego dostęp mają tylko osoby posiadające aktualne upoważnienie do przetwarzania danych osobowych.

§ 8.

Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez **Administratora Danych** lub **Administratora Bezpieczeństwa Informacji**. **Administrator Bezpieczeństwa Informacji** jest obowiązany 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. Administrator Bezpieczeństwa Informacji nadaje uprawnienia pracownikom którzy przetwarzają dane poprzez podpisanie oświadczenia które stanowi **załącznik nr 5 do „Polityki Bezpieczeństwa"**. Administrator Bezpieczeństwa Informacji prowadzi wszelką dokumentację opisującą sposób przetwarzania danych w podmiocie a w szczególności:

1. Ewidencja osób przetwarzających dane w podmiocie posiadających upoważnienie – **załącznik nr 6** do „Polityki Bezpieczeństwa"

2. Zestawienie danych osobowych. Kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. – **załącznik nr 7** do „Polityki Bezpieczeństwa"

§ 9.

Na wniosek osoby, której dane dotyczą, Administrator Bezpieczeństwa Informacji jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić, odnośnie do jej danych osobowych, informacji.

§ 10.

Administrator Bezpieczeństwa Informacji może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych osobowych w podmiocie. Podmiot ten,

może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

§ 11.

Sposób zabezpieczenia oraz przetwarzania danych w systemie informatycznym reguluje Instrukcja Zarządzania Systemem Informatycznym.

§ 12.

W sprawach nieuregulowanych w niniejszej „Polityce Bezpieczeństwa" mają zastosowanie odpowiednie przepisy ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. oraz **ROZPORZĄDZENIA MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI** z dnia 29 kwietnia 2004 r. **w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych**

Podpis Administratora Danych Osobowych

DYREKTOR
Zespołu Obsługi Placówek Oświaty
w Okonku

.....Renata Zabrocka.....

Podpis

Podpis Administratora Bezpieczeństwa Informacji

29.10.2015 .....

Podpis

Załącznik Nr 2
do Zarządzenia Nr 20/2015
z 23.10.2015 r.

Zespół Obsługi Placówek Oświatowych
w Okonku, ul. Leśna 46
64-965 OKONEK
15-70-823 REGON

DYREKTOR
Zespołu Obsługi Placówek
w Okonku
Renata Zabrocka

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Administrator Danych .....

Dnia 23.10.2015 ..... w podmiocie o nazwie .....

Zgodnie z **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
wdraża dokument o nazwie „Instrukcja zarządzania systemem informatycznym" zwany dalej „instrukcją".
Zapisy tego dokumentu wchodzą w życie z dniem 23.10.2015 r.

Ilekroć w „instrukcji" jest mowa o:

1) podmiocie — rozumie się przez to spółkę prawa handlowego, podmiot gospodarczy nie posiadający osobowości prawnej, jednostkę budżetową;
2) ustawie — rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, zwaną dalej „ustawą";
3) identyfikatorze użytkownika — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
4) haśle — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
5) sieci telekomunikacyjnej — rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.)
6) sieci publicznej — rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne;
7) teletransmisji – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej
8) rozliczalności — rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
9) integralności danych — rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
10) raporcie — rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
11) poufności danych — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
12) uwierzytelnianiu — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

§ 1

Za przestrzeganie w podmiocie .....64-965 OKONEK..... zapisów „instrukcji" odpowiedzialny jest Administrator danych lub zgodnie z zapisem §2 „Polityki Bezpieczeństwa" wyznaczony **Administrator Bezpieczeństwa Informacji**

§2

W związku z tym, że w podmiocie ..... przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną, oraz uwzględniając kategorie przetwarzanych danych i zagrożenia wprowadza się poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym na poziomie **wysokim,** a w związku z tym wprowadza się poniższe postanowienia:

I

Obszar, w który są przetwarzane dane, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. Przebywanie osób nieuprawnionych w obszarze, w którym są przetwarzane dane, jest dopuszczalne za zgodą Administratora Danych, Administratora Bezpieczeństwa Informacji lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

II

1. W systemie informatycznym służącym do przetwarzania danych osobowych, przetwarzać dane mogą wyłącznie osoby posiadające aktualne upoważnienie nadane przez Administratora Bezpieczeństwa Informacji. Użytkownik przetwarzający dane po otrzymaniu upoważnienia oraz loginu i hasła jest zobowiązany niezwłocznie dokonać zmiany hasła oraz zachować je w tajemnicy. Użytkownik jest zobowiązany do zmiany hasła nie rzadziej niż co 30 dni. Hasło nadane przez użytkownika musi składać się z co najmniej z 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

2. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:

w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator oraz aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

III

System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:
1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

•poprzez zainstalowanie programu antywirusowego o nazwie G DATA INTERNET SECURITY

•poprzez zainstalowanie firewall (zapora sieciowa).

•poprzez zabezpieczenie sieci radiowej odpowiedniej mocy uwierzytelnieniem.

2) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez zastosowanie zasilacza awaryjnego ups.

IV

1. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
2. W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
3. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii

zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Kopie wszystkich danych osobowych muszą być tworzone nie rzadziej niż raz na tydzień.

4. Kopie zapasowe:

a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem w pomieszczeniu zamkniętym (nr pokoju, nazwa działu) ...POKÓJ DYREKTORA - DZIAŁ KSIĘGOWY..... zaopatrzonym w system alarmowy (nazwa systemu, nazwa grupy interwencyjnej) ...EXPERT OBSŁUGA OSÓB I MIENIA - UMOWA NR UM 256/10.....

b) usuwa się niezwłocznie po ustaniu ich użyteczności.

V

Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych w tym stosuje hasła dostępu do komputera przenośnego oraz do plików, w których przetwarzane są dane osobowe.

VI

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

1) likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;

2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;

3) naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

§3

1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — system ten zapewnia odnotowanie:

1) daty pierwszego wprowadzenia danych do systemu;

2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;

3) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;

4) informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;

5) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.

2. Odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.

4. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust. 1 pkt 4, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

§4

Po zakończeniu pracy w systemie informatycznym użytkownik ma obowiązek wylogować się z systemu. W przypadku braku czynności ze strony użytkownika w systemie informatycznym przez 30 min, system samoczynnie wyloguje użytkownika przetwarzającego dane osobowe.

§5

Administrator Bezpieczeństwa Informacji ma obowiązek dokonywać przeglądów technicznych sprzętu informatycznego w podmiocie oraz dbać o ich dobry stan techniczny. Zaleca się dokonywanie przeglądów okresowych co 30 dni oraz przeglądów generalnych raz na rok. W przypadku stwierdzenia usterek technicznych **Administrator Bezpieczeństwa Informacji** ma obowiązek niezwłocznie powiadomić o tym fakcie Administratora Danych.

§6

W przypadku stwierdzenia przez **Administratora Bezpieczeństwa Informacji** uchybień dotyczących przetwarzania danych w podmiocie powinien o tym fakcie niezwłocznie powiadomić Administratora Danych oraz wprowadzić takie zabezpieczenia i procedury, które w przyszłości wyeliminują takie zdarzenia.

§ 7.

W sprawach nieuregulowanych w niniejszej „instrukcji" mają zastosowanie przepisy ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. oraz **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**

Podpis Administratora Danych Osobowych

DYREKTOR
Zespołu Obsługi Placówek Oświaty
w Okonku

.....
Renata Zabrocka

Podpis

Podpis Administratora Bezpieczeństwa Informacji

29.10.2015 .....

Podpis

.....

miejscowość i data

Upoważnienie dla Administratora Bezpieczeństwa Informacji oraz zakres obowiązków

załącznik nr 1 do „Polityki Bezpieczeństwa"

Na podstawie § 3. Polityki Bezpieczeństwa z dnia 29.10.2015 r. 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. 36a 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)

Administrator Danych .....

Administratora Bezpieczeństwa Informacji .....

Pesel .....

Upoważnienie jest ważne od chwili podpisania przez strony do dnia wycofania upoważnienia przez **Administrator Danych.**

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. **Administrator Bezpieczeństwa Informacji** jest zobowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1. **Administrator Bezpieczeństwa Informacji** nadaje uprawnienia pracownikom którzy przetwarzają dane poprzez podpisanie oświadczenia, które stanowi **załącznik nr 5 do „Polityki Bezpieczeństwa".**

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:

zgodnie z § 3. „Polityki Bezpieczeństwa"

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, który określa załącznik do „Polityki Bezpieczeństwa" nr 2

zgodnie z § 4. „Polityki Bezpieczeństwa"

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, który określa załącznik do „Polityki Bezpieczeństwa" nr 3

zgodnie z § 5. „Polityki Bezpieczeństwa"

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami, który określa załącznik do „Polityki Bezpieczeństwa" nr 4

zgodnie z § 7. „Polityki Bezpieczeństwa"

Ewidencję osób przetwarzających dane w podmiocie posiadających upoważnienie - załącznik nr 6 do „Polityki Bezpieczeństwa"

Zestawienie danych osobowych. Kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. – załącznik nr 7 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 Zespole Obsługi Placówek Oświaty w Okonku zgodnie z obowiązkami wynikającymi z tego upoważnienia oraz ustawy o ochronie danych osobowych.

Administrator Bezpieczeństwa Informacji

.....

Podpis

Administrator Danych

.....

Podpis

Zespół Obsługi Placówek Oświaty
w Okonku, ul. Leśna 46
64-965 OKONEK
NIP 767-15-70-923 REGON 572106468
tel. 067 266 31 42

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

załącznik do „Polityki Bezpieczeństwa" nr 2 zgodnie z § 4 pkt 1 Rozporządzenia Ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r.

Lp.	Dokładny adres *(np. adres siedziby firmy gdzie przetwarzane są dane)*	Dział użytkujący pomieszczenie	Nr pokoju lub pomieszczenia	Rodzaj zastosowanego zabezpieczenia pomieszczenia	Uwagi
1	Zespół Obsługi Placówek Oświaty w Okonku Ul. Leśna 46 64-965 Okonek	Gabinet dyrektora	Gabinet dyrektora	Alarm, drzwi zamykane na klucz.	
2	Zespół Obsługi Placówek Oświaty w Okonku Ul. Leśna 46 64-965 Okonek	Dział płacowy	Pokój pierwszy	Alarm, drzwi zamykane na klucz.	
4	Zespół Obsługi Placówek Oświaty w Okonku Ul. Leśna 46 64-965 Okonek	Dział księgowy	Pokój drugi	Alarm, drzwi zamykane na klucz.	
5	Zespół Obsługi Placówek Oświaty w Okonku Ul. Leśna 46 64-965 Okonek	Dział księgowy	Pokój trzeci	Drzwi zamykane na klucz, alarm	
6	Zespół Obsługi Placówek Oświaty w Okonku Ul. Leśna 46 64-965 Okonek	Archiwum	Brak numeru	Drzwi zamykane na klucz, alarm	

Data i podpis Administratora Danych Osobowych

DYREKTOR
Zespołu Obsługi Placówek Oświaty
w Okonku
Renata Zabrocka

.....

Zespół Obsługi Placówek Oświaty
w Okonku, ul. Leśna 46
64-965 OKONEK
NIP 767-15-70-923 REGON 572106468
tel. 067 266 91 45

ZARZĄDZENIE NR 20/2015
Dyrektora Zespołu Obsługi Placówek Oświaty w Okonku
z dnia 29 października 2015 roku

w sprawie „Polityki Bezpieczeństwa w Zespole Obsługi Placówek Oświaty w Okonku" i „Instrukcji Zarządzania Systemem Informatycznym".

Na podstawie art. 36 ust. 1, 2 i 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182 z późn. zm.) oraz § 3, 4 i 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) zarządza się, co następuje:

§ 1. Wprowadza się „Politykę Bezpieczeństwa Informacji w Zespole Obsługi Placówek Oświaty w Okonku" stanowiącą załącznik Nr 1 do niniejszego zarządzenia.

§ 2. Wprowadza się „Instrukcję Zarządzania Systemem Informatycznym w Zespole Obsługi Placówek Oświaty w Okonku" stanowiącą załącznik Nr 2 do niniejszego zarządzenia.

§ 3. Zobowiązuje się wszystkie osoby przetwarzające dane osobowe w Zespole Obsługi Placówek Oświaty w Okonku do przestrzegania zasad i realizacji zadań określonych w załącznikach, o których mowa w § 1 i 2.

§ 4. Wyznacza się Panią Annę Mliczak – inspektora ds. księgowości na Administratora Bezpieczeństwa Informacji w Zespole Obsługi Placówek Oświaty w Okonku.

§ 5. Traci moc zarządzenie nr 27 z dnia 29 grudnia 2011 roku Dyrektora Zespołu Obsługi Placówek Oświaty w Okonku w sprawie ustalenia „Polityki Bezpieczeństwa i instrukcji zarządzania systemów informatycznych służących do przetwarzania danych osobowych w ZOPO".

§ 6. Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
Zespołu Obsługi Placówek Oświaty
w Okonku
Renata Zabrocka

Załącznik nr 1
do Zarządzenie nr 20/2015
z 28.10.2015 r.

DYREKTOR
Zespołu Obsługi Placówek Oświaty
w Okonku

POLITYKA BEZPIECZEŃSTWA

Administrator Danych.....Renata Zabrocka.....

Dnia ....28.10.2015.... w podmiocie o nazwie .....

Zespół Obsługi Placówek Oświaty
w Okonku, ul. Leśna 46
64-965 OKONEK
NIP 767-15-70-923 REGON 572106468
tel. 067 [illegible]

Zgodnie z **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 (Dz. U. Nr 100, poz. 1024)
wdraża dokument o nazwie „Polityka Bezpieczeństwa". Zapisy tego dokumentu wchodzą w życie z dniem....28.10.2015.....

Zespół Obsługi Placówek Oświaty
w Okonku, ul. Leśna 46
64-965 OKONEK
NIP 767-15-70-923 REGON 572106468
tel. [illegible]

§ 1.

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w .....(nazwa podmiotu), określa zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.
Polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa przetwarzanych danych.
Polityka bezpieczeństwa dotyczy danych osobowych przetwarzanych w zbiorach manualnych oraz w systemach informatycznych.

§ 2

Ilekroć w „Polityce Bezpieczeństwa" jest mowa o:

1.zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
2.przetwarzaniu 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,
3.systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
4.zabezpieczeniu danych w systemie informatycznym - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
5.usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
6.administratorze danych - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych,
7.administratorze bezpieczeństwa informacji – rozumie się przez to osobę wyznaczoną przez Administratora Danych w celu nadzorowania i przestrzegania zasad ochrony, o których mowa w ust. 1, chyba, że Administrator Danych sam wykonuje te czynności.
8.podmiocie – rozumie się przez to spółkę prawa handlowego, podmiot gospodarczy nie posiadający osobowości prawnej, jednostkę budżetową;

§ 3.

Administrator Danych w podmiocie.....wyznacza **Administratora Bezpieczeństwa Informacji** w celu nadzorowania i przestrzegania zasad ochrony, o których mowa w USTAWIE z dnia 29 sierpnia 1997 r. o ochronie danych osobowych chyba, że Administrator Danych sam wykonuje te czynności. Upoważnienie dla **Administratora Bezpieczeństwa Informacji** oraz zakres obowiązków określa **załącznik do „Polityki Bezpieczeństwa" nr 1**

§ 4.

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe określa **załącznik do „Polityki Bezpieczeństwa" nr 2**

§ 5.

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych określa **załącznik do „Polityki Bezpieczeństwa" nr 3**

§ 6.

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami określa **załącznik do „Polityki Bezpieczeństwa" nr 4**

§ 7.

Administratora Bezpieczeństwa Informacji dba o to aby dane osobowe w formie papierowej były niedostępne dla osób nieupoważnionych. Dokumenty powinny znajdować się w pomieszczeniu zamykanym na klucz do którego dostęp mają tylko osoby posiadające aktualne upoważnienie do przetwarzania danych osobowych.

§ 8.

Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez **Administratora Danych** lub **Administratora Bezpieczeństwa Informacji**. **Administrator Bezpieczeństwa Informacji** jest obowiązany 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. Administrator Bezpieczeństwa Informacji nadaje uprawnienia pracownikom którzy przetwarzają dane poprzez podpisanie oświadczenia które stanowi **załącznik nr 5 do „Polityki Bezpieczeństwa"**. Administrator Bezpieczeństwa Informacji prowadzi wszelką dokumentację opisującą sposób przetwarzania danych w podmiocie a w szczególności:

1. Ewidencja osób przetwarzających dane w podmiocie posiadających upoważnienie – **załącznik nr 6** do „Polityki Bezpieczeństwa"

2. Zestawienie danych osobowych. Kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. – **załącznik nr 7** do „Polityki Bezpieczeństwa"

§ 9.

Na wniosek osoby, której dane dotyczą, Administrator Bezpieczeństwa Informacji jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić, odnośnie do jej danych osobowych, informacji.

§ 10.

Administrator Bezpieczeństwa Informacji może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych osobowych w podmiocie. Podmiot ten,

może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

§ 11.

Sposób zabezpieczenia oraz przetwarzania danych w systemie informatycznym reguluje Instrukcja Zarządzania Systemem Informatycznym.

§ 12.

W sprawach nieuregulowanych w niniejszej „Polityce Bezpieczeństwa" mają zastosowanie odpowiednie przepisy ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. oraz **ROZPORZĄDZENIA MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI** z dnia 29 kwietnia 2004 r. **w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych**

Podpis Administratora Danych Osobowych

DYREKTOR
Zespołu Obsługi Placówek Oświaty
w Okonku
Renata Zabrocka

.....

Podpis

Podpis Administratora Bezpieczeństwa Informacji

29.10.2015

.....

Podpis

Załącznik Nr 2
do Zarządzenia Nr 20/2015
z 28.10.2015 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Zespół Obsługi Placówek Oświatowych w Okonku, ul. Leśna 46, 64-965 OKONEK, 15-70-823 REGON

DYREKTOR
Zespołu Obsługi Placówek
w Okonku
Renata Zabrocka

Administrator Danych .....

Dnia 28.10.2015 r. w podmiocie o nazwie .....

Zgodnie z **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
wdraża dokument o nazwie „Instrukcja zarządzania systemem informatycznym" zwany dalej „instrukcją".
Zapisy tego dokumentu wchodzą w życie z dniem 28.10.2015 r.

Ilekroć w „instrukcji" jest mowa o:

1) podmiocie — rozumie się przez to spółkę prawa handlowego, podmiot gospodarczy nie posiadający osobowości prawnej, jednostkę budżetową;
2) ustawie — rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, zwaną dalej „ustawą";
3) identyfikatorze użytkownika — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
4) haśle — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
5) sieci telekomunikacyjnej — rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.)
6) sieci publicznej — rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne;
7) teletransmisji – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej
8) rozliczalności — rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
9) integralności danych — rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
10) raporcie — rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
11) poufności danych — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
12) uwierzytelnianiu — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

§ 1

Za przestrzeganie w podmiocie .....64-965 OKONEK..... zapisów „instrukcji" odpowiedzialny jest Administrator danych lub zgodnie z zapisem §2 „Polityki Bezpieczeństwa" wyznaczony **Administrator Bezpieczeństwa Informacji**

§2

W związku z tym, że w podmiocie ..... przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną, oraz uwzględniając kategorie przetwarzanych danych i zagrożenia wprowadza się poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym na poziomie **wysokim,** a w związku z tym wprowadza się poniższe postanowienia:

I

Obszar, w który są przetwarzane dane, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. Przebywanie osób nieuprawnionych w obszarze, w którym są przetwarzane dane, jest dopuszczalne za zgodą Administratora Danych, Administratora Bezpieczeństwa Informacji lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

II

1. W systemie informatycznym służącym do przetwarzania danych osobowych, przetwarzać dane mogą wyłącznie osoby posiadające aktualne upoważnienie nadane przez Administratora Bezpieczeństwa Informacji. Użytkownik przetwarzający dane po otrzymaniu upoważnienia oraz loginu i hasła jest zobowiązany niezwłocznie dokonać zmiany hasła oraz zachować je w tajemnicy. Użytkownik jest zobowiązany do zmiany hasła nie rzadziej niż co 30 dni. Hasło nadane przez użytkownika musi składać się z co najmniej z 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

2. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:

w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator oraz aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

III

System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:
1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

•poprzez zainstalowanie programu antywirusowego o nazwie G DATA INTERNET SECURITY

•poprzez zainstalowanie firewall (zapora sieciowa).

•poprzez zabezpieczenie sieci radiowej odpowiedniej mocy uwierzytelnieniem.

2) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez zastosowanie zasilacza awaryjnego ups.

IV

1. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
2. W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
3. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii

zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Kopie wszystkich danych osobowych muszą być tworzone nie rzadziej niż raz na tydzień.

4. Kopie zapasowe:

a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem w pomieszczeniu zamkniętym (nr pokoju, nazwa działu) ...POKÓJ DRUGI - DZIAŁ KSIĘGOWY...
zaopatrzonym w system alarmowy (nazwa systemu, nazwa grupy interwencyjnej) ...EXPERT OBSŁUGA OSÓB I MIENIA - UMOWA NR UM 256/10...

b) usuwa się niezwłocznie po ustaniu ich użyteczności.

V

Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych w tym stosuje hasła dostępu do komputera przenośnego oraz do plików, w których przetwarzane są dane osobowe.

VI

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

1) likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;

2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;

3) naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

§3

1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — system ten zapewnia odnotowanie:

1) daty pierwszego wprowadzenia danych do systemu;

2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;

3) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;

4) informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;

5) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.

2. Odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.

4. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust. 1 pkt 4, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

§4

Po zakończeniu pracy w systemie informatycznym użytkownik ma obowiązek wylogować się z systemu. W przypadku braku czynności ze strony użytkownika w systemie informatycznym przez 30 min, system samoczynnie wyloguje użytkownika przetwarzającego dane osobowe.

§5

Administrator Bezpieczeństwa Informacji ma obowiązek dokonywać przeglądów technicznych sprzętu informatycznego w podmiocie oraz dbać o ich dobry stan techniczny. Zaleca się dokonywanie przeglądów okresowych co 30 dni oraz przeglądów generalnych raz na rok. W przypadku stwierdzenia usterek technicznych **Administrator Bezpieczeństwa Informacji** ma obowiązek niezwłocznie powiadomić o tym fakcie Administratora Danych.

§6

W przypadku stwierdzenia przez **Administratora Bezpieczeństwa Informacji** uchybień dotyczących przetwarzania danych w podmiocie powinien o tym fakcie niezwłocznie powiadomić Administratora Danych oraz wprowadzić takie zabezpieczenia i procedury, które w przyszłości wyeliminują takie zdarzenia.

§ 7.

W sprawach nieuregulowanych w niniejszej „instrukcji" mają zastosowanie przepisy ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. oraz **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**

Podpis Administratora Danych Osobowych

DYREKTOR
Zespołu Obsługi Placówek Oświaty
w Okonku

.....
Renata Zabrocka

Podpis

Podpis Administratora Bezpieczeństwa Informacji

29.10.2015 .....

Podpis

.....

miejscowość i data

Upoważnienie dla Administratora Bezpieczeństwa Informacji oraz zakres obowiązków

załącznik nr 1 do „Polityki Bezpieczeństwa"

Na podstawie § 3. Polityki Bezpieczeństwa z dnia 29.10.2015 r. 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. 36a 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)

Administrator Danych .....

Administratora Bezpieczeństwa Informacji .....

Pesel .....

Upoważnienie jest ważne od chwili podpisania przez strony do dnia wycofania upoważnienia przez **Administrator Danych.**

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. **Administrator Bezpieczeństwa Informacji** jest zobowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1. **Administrator Bezpieczeństwa Informacji** nadaje uprawnienia pracownikom którzy przetwarzają dane poprzez podpisanie oświadczenia, które stanowi **załącznik nr 5 do „Polityki Bezpieczeństwa".**

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:

zgodnie z § 3. „Polityki Bezpieczeństwa"

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, który określa załącznik do „Polityki Bezpieczeństwa" nr 2

zgodnie z § 4. „Polityki Bezpieczeństwa"

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, który określa załącznik do „Polityki Bezpieczeństwa" nr 3

zgodnie z § 5. „Polityki Bezpieczeństwa"

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami, który określa załącznik do „Polityki Bezpieczeństwa" nr 4

zgodnie z § 7. „Polityki Bezpieczeństwa"

Ewidencję osób przetwarzających dane w podmiocie posiadających upoważnienie - załącznik nr 6 do „Polityki Bezpieczeństwa"

Zestawienie danych osobowych. Kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. – załącznik nr 7 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 Zespole Obsługi Placówek Oświaty w Okonku zgodnie z obowiązkami wynikającymi z tego upoważnienia oraz ustawy o ochronie danych osobowych.

Administrator Bezpieczeństwa Informacji

.....

Podpis

Administrator Danych

.....

Podpis

Zespół Obsługi Placówek Oświaty
w Okonku, ul. Leśna 46
64-965 OKONEK
NIP 767-15-70-923 REGON 572106468
tel. 067 266 41 41

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

załącznik do „Polityki Bezpieczeństwa" nr 2 zgodnie z § 4 pkt 1 Rozporządzenia Ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r.

Lp.	Dokładny adres *(np. adres siedziby firmy gdzie przetwarzane są dane)*	Dział użytkujący pomieszczenie	Nr pokoju lub pomieszczenia	Rodzaj zastosowanego zabezpieczenia pomieszczenia	Uwagi
1	Zespół Obsługi Placówek Oświaty w Okonku Ul. Leśna 46 64-965 Okonek	Gabinet dyrektora	Gabinet dyrektora	Alarm, drzwi zamykane na klucz.	
2	Zespół Obsługi Placówek Oświaty w Okonku Ul. Leśna 46 64-965 Okonek	Dział płacowy	Pokój pierwszy	Alarm, drzwi zamykane na klucz.	
4	Zespół Obsługi Placówek Oświaty w Okonku Ul. Leśna 46 64-965 Okonek	Dział księgowy	Pokój drugi	Alarm, drzwi zamykane na klucz.	
5	Zespół Obsługi Placówek Oświaty w Okonku Ul. Leśna 46 64-965 Okonek	Dział księgowy	Pokój trzeci	Drzwi zamykane na klucz, alarm	
6	Zespół Obsługi Placówek Oświaty w Okonku Ul. Leśna 46 64-965 Okonek	Archiwum	Brak numeru	Drzwi zamykane na klucz, alarm	

Data i podpis Administratora Danych Osobowych

DYREKTOR
Zespołu Obsługi Placówek Oświaty
w Okonku
Renata Zabrocka

.....

Zespół Obsługi Placówek Oświaty
w Okonku, ul. Leśna 46
64-965 OKONEK
757-15-70-923 REGON 572106468
tel. 067 266 91 45

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

załącznik do „Polityki Bezpieczeństwa" nr 3 zgodnie, z § 4 pkt 2 Rozporządzenia Ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r.

Lp.	Nazwa zbioru danych *(np. dane klientów, pracowników itd.)*	Programy zastosowane do przetwarzania danych *(np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)*	Uwagi
1	Akta Osobowe	Wersja papierowa	
2	Dane pracownicze kadrowe	Wersja papierowa	
3	Dane pracownicze kadrowe	Wersja elektroniczna	
4	Dane pracownicze płacowe	Wersja papierowa	
5	Dane pracownicze płacowe	Wersja elektroniczna	
6	Dane pracownicze do ZUS	Wersja papierowa i elektroniczna	
7	Dane pracownicze do projektu organizacyjnego	Wersja papierowa	
8	Dane pracownicze do funduszu socjalnego	Wersja papierowa	
9	Dane pracownicze udostępnione innym podmiotom	Wersja papierowa	
10	Wnioski o nagrody, medale, odznaczenia	Wersja papierowa	
11	Pracownicze książeczki zdrowia	Wersja papierowa	
12	Skierowania na badania	Wersja papierowa	
13	Dane pracownicze do ubezpieczenia	Wersja papierowa	

Data i podpis Administratora Bezpieczeństwa Informacji

29.10.2015 .....

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

załącznik do „Polityki Bezpieczeństwa" nr 3 zgodnie, z § 4 pkt 2 Rozporządzenia Ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r.

Lp.	Nazwa zbioru danych *(np. dane klientów, pracowników itd.)*	Programy zastosowane do przetwarzania danych *(np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)*	Uwagi
14	Dokumentacja wypadkowa pracowników	Wersja papierowa	
15	Dokumentacja emerytalno-rentowa	Wersja papierowa	
16	Dokumentacja związana z organizacją staży zawodowych, praktyk	Wersja papierowa	
17	Umowy cywilno-prawne	Wersja papierowa	
18	Zbiór danych do SIO	Program do SIO	
19	Zbiór danych do SIO	Wersja papierowa	
20	Obowiązek szkolny	Wersja papierowa	
21	Dotacje dla placówek niepublicznych	Wersja papierowa	
22	Zarządzenia dyrektora	Wersja papierowa	
23	Sprawozdania z wykonania budżetu, plany finansowe	Wersja papierowa	
24	Sprawozdania z wykonania budżetu, plany finansowe	Wersja elektroniczna, program BESTIA	
25	Dotacje	Wersja papierowa	
26	Dokumenty dotyczące reorganizacji oświaty	Wersja papierowa	
27	Organizacja dowozu	Wersja papierowa	
28	Dokumenty założycielskie jednostki	Wersja papierowa	
29	Ewidencja placówek niepublicznych	Wersja papierowa	
30	Listy płac pracowników	Wersja papierowa	

Zespół Obsługi Placówek Oświaty
w Okonku, ul. Leśna 46
64-965 OKONEK
NIP 767-15-70-923 REGON 572106468
tel. 067 266 91 45

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

załącznik do „Polityki Bezpieczeństwa" nr 3 zgodnie, z § 4 pkt 2 Rozporządzenia Ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r.

Lp.	Nazwa zbioru danych *(np. dane klientów, pracowników itd.)*	Programy zastosowane do przetwarzania danych *(np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)*	Uwagi
31	Listy płac pracowników	Wersja elektroniczna, program SIGID	
32	Faktury	Wersja papierowa	
33	Polecenia księgowania	Wersja papierowa	
34	Inwentaryzacja	Wersja papierowa	
35	Bilans jednostek	Wersja papierowa	
36	Zaświadczenia o dochodach	Wersja papierowa	
37	Rp 7	Wersja papierowa	
38	Potrącenia z wynagrodzenia	Wersja papierowa	
39	Pracownicy młodociani	Wersja papierowa	
40	Pracownicy młodociani	Wersja elektroniczna, program SHRIMP	
41	Godziny ponadwymiarowe	Wersja papierowa	
42	Rejestr zwolnień lekarskich	Wersja papierowa	
43	Dokumenty rozliczeniowe z ZUS	Wersja papierowa	
44	Dokumenty rozliczeniowe z ZUS	Wersja elektroniczna	

Data i podpis Administratora Bezpieczeństwa Informacji

29.10.2015 .....

Zespół Obsługi Placówek Oświaty
w Okonku, ul. Leśna 46
64-965 OKONEK
NIP 767-15-70-923 REGON 572106468
tel. 067 266 91 45

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami w Zespole Szkół Katolickich im. św. Urszuli Ledóchowskiej w Nowej Soli

- załącznik do „Polityki Bezpieczeństwa" nr 4 zgodnie, z § 4 pkt 3 i 4 Rozporządzenia Ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r.

Lp.	Nazwa zbioru danych *(np. dane klientów, pracowników itd.)*	Struktura zbiorów *(np. imię i nazwisko, e-mail, telefon itd.)*	Przepływ danych (np. wydruk danych z Internetu)	Uwagi
1	Akta osobowe	Awans zawodowy, ocena pracy, imię, nazwisko, numer i seria dowodu osobowego, nip, adres zamieszkania/zameldowania/korespondencja, wykształcenie, orzeczenia lekarskie, świadectwa pracy, umowy, nagrody, zmiany płacowe, numer telefonu, nazwisko rodowe, nazwisko panieńskie matki, imię ojca matki, stan cywilny, dane rodziców, badania BHP, awans zawodowy, dane płacowe, książeczki zdrowia,	brak	
2	Ewidencja czasu pracy	Imię, nazwisko, pesel, data urodzenia, NIP,	Z wersji papierowej na wersje papierową; z wersji papierowej na wersję elektroniczną	
3	Dane pracownicze płacowe	Imię, nazwisko, pesel, data urodzenia, NIP,	Z wersji papierowej na wersje papierową; z wersji papierowej na wersję elektroniczną	
4	Dane pracownicze do ZUS	Imię, nazwisko, pesel, data urodzenia,	Z wersji papierowej na wersje papierową; z wersji papierowej na wersję elektroniczną	
5	Dane pracownicze udostępniane innym podmiotom	Imię, nazwisko, adres, data i miejsce urodzenia, pesel,	Z wersji papierowej na wersje papierową	

Zespół Obsługi Placówek Oświaty
w Okonku, ul. Leśna 46
64-965 OKONEK
NIP 767-15-70-923 REGON 572106468
tel. 067 266 91 45

Lp.	Nazwa zbioru danych *(np. dane klientów, pracowników itd.)*	Struktura zbiorów *(np. imię i nazwisko, e-mail, telefon itd.)*	Przepływ danych (np. wydruk danych z Internetu)	Uwagi
6	Dane pracownicze do ubezpieczenia	Imię, nazwisko, adres, data i miejsce urodzenia, pesel, imiona rodziców , nazwisko rodowe matki, nr i seria dowodu osobistego, imię nazwisko członka rodziny,	Z wersji papierowej na wersje papierową; z wersji papierowej na wersję elektroniczną	
7	Dokumentacja wypadkowa pracowników	Imię, nazwisko, adres, data i miejsce urodzenia, pesel, nr i seria dowodu osobistego, rodzaj uszczerbku na zdrowiu	Z wersji papierowej na wersje papierową	
8	Dokumentacja emerytalno rentowa	Imię, nazwisko, adres, data i miejsce urodzenia, pesel, imiona rodziców , nazwisko rodowe matki, nr i seria dowodu osobistego, przebieg zatrudnienia, RP7	Z wersji papierowej na wersje papierową	
9	Dokumentacja związana z organizacją staży zawodowych, praktyk	Imię, nazwisko, adres, data i miejsce urodzenia, pesel, nr i seria dowodu osobistego	Z wersji papierowej na wersje papierową	
10	Umowy cywilno prawne, prace zlecenia na rzecz szkoły	Imię, nazwisko, adres, numer konta bankowego, imię, nazwisko dziecka, data urodzenia, pesel, dane firmy,	Z wersji papierowej na wersje papierową	
11	Zbiór danych do SIO	Imię, nazwisko, adres, data i miejsce urodzenia, pesel, imiona rodziców, adres zamieszkania/zameldowania nr telefonu	Z wersji papierowej na wersje papierową, z wersji papierowej na wersje elektroniczną	
12	Obowiązek szkolny	Imię, nazwisko, data i miejsce urodzenia, pesel, imiona rodziców, adres zamieszkania/zameldowania	Z wersji papierowej na wersje papierową	
13.	Dotacje dla placówek niepublicznych	Imię, nazwisko, adres, numer konta bankowego, data urodzenia, pesel, dane firmy	Z wersji papierowej na wersje papierową	
14.	Dokumenty finansowe	Imię, nazwisko, adres, pesel	Z wersji papierowej na wersje papierową, z wersji	

Zespół Obsługi Placówek Oświaty
w Okonku, ul. Leśna 46
64-965 OKONEK
NIP 767-15-70-923 REGON 572106468
tel. 067 266 91 45

Lp.	**Nazwa zbioru danych** *(np. dane klientów, pracowników itd.)*	**Struktura zbiorów** *(np. imię i nazwisko, e-mail, telefon itd.)*	**Przepływ danych** (np. wydruk danych z Internetu)	**Uwagi**
			papierowej na wersje elektroniczną	
15.	Organizacja dowozu	Imię, nazwisko, adres, pesel	Z wersji papierowej na wersje papierową	
16.	Dokumentacja rozliczeniowa z ZUS	Imię, nazwisko, adres, data i miejsce urodzenia, pesel, imiona rodziców , nazwisko rodowe matki, nr i seria dowodu osobistego, imię nazwisko członka rodziny	Z wersji papierowej na wersje papierową, z wersji elektronicznej na wersje elektroniczną	
17.	Dziennik korespondencji	Imię, nazwisko, adres, dane firmy, treść wysłanej korespondencji, data	brak	
18.	Zalecenia pokontrolne	Wynik kontroli, nazwa organu kontrolującego, adres, imię i nazwisko, zalecenia pokontrolne	Z wersji papierowej na wersje papierową	

Data i podpis Administratora Bezpieczeństwa Informacji

29.10.2015 .....

Upoważnienie do przetwarzania danych osobowych załącznik nr 5 do „Polityki Bezpieczeństwa" zgodnie z Art 37 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.

..... jako Administrator Bezpieczeństwa Informacji dnia ..... nadaje upoważnienie do przetwarzania danych osobowych w podmiocie ..... dla:

Imię i nazwisko: .....

Adres zamieszkania: .....

Nr PESEL: .....

Stanowisko służbowe: .....

Upoważniony otrzymuje dostęp do poniższych zasobów danych osobowych w celu ich przetwarzania:

.....

.....

.....

.....

.....

.....

.....

Upoważnienie nadaje się do dnia .....

Upoważniony zobowiązuje się do przestrzegania zasad panujących w podmiocie w zakresie ochrony danych osobowych a w szczególności „Polityki Bezpieczeństwa" oraz respektowania zapisów **Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.** Upoważnionego obowiązuje tajemnica dotycząca danych osobowych przetwarzanych w podmiocie oraz sposobów zabezpieczeń.

Administrator Bezpieczeństwa Informacji

.....

Podpis

Użytkownik

.....

Podpis

spół Obsługi Placówek Oświaty
w Okonku, ul. Leśna 46
64-965 OKONEK
767-15-70-923 REGON 572106468
tel. 067 386 91 45

Ewidencja osób przetwarzających dane w podmiocie posiadających upoważnienie

załącznik nr 6 do „Polityki Bezpieczeństwa" zgodnie z Art 39. 1. Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.

Lp.	Imię i nazwisko	Stanowisko służbowe	Data nadania upoważnienia	Data ustania upoważnienia	Wykaz zbiorów danych wynikających z upoważnienia	Identyfikator *(Jeżeli dane są przetwarzane w systemie informatycznym)*
1	Zabrocka Renata	dyrektor			Akta osobowe, dane pracownicze, kadrowe, płacowe oraz księgowość, dane pracownicze udostępnione innym podmiotom, wnioski o nagrody, obowiązek szkolny, dane pracownicze do ZUS, dokumentacja naboru, umowy cywilno prawne, zbiór danych do SIO, sprawozdania, dotacje, ewidencja placówek niepublicznych, organizacja dowozu.	dyrektor
2	Stanasiuk Danuta	Inspektor ds. płac i rozliczeń materiałowych			Akta osobowe, dane pracownicze, kadrowe, płacowe oraz księgowość, dane pracownicze udostępnione innym podmiotom, dane pracownicze do ZUS, umowy cywilno prawne, zbiór danych do SIO, dokumentacja ubezpieczeniowa, dane pracownicze.	
3	Luberda Ewa	Inspektor ds. płac			Akta osobowe, dane pracownicze, kadrowe, płacowe oraz księgowość, dane pracownicze udostępnione innym podmiotom, dane pracownicze do ZUS, umowy cywilno prawne, Płatnik, dokumentacja ubezpieczeniowa, dane pracownicze.	

Lp.	Imię i nazwisko	Stanowisko służbowe	Data nadania upoważnienia	Data ustania upoważnienia	Wykaz zbiorów danych wynikających z upoważnienia	Identyfikator *(Jeżeli dane są przetwarzane w systemie informatycznym)*
4	Mikołajewska Aleksandra	Główna Księgowa			Dane pracownicze, kadrowe, płacowe oraz księgowość, dane pracownicze udostępnione innym podmiotom, dane pracownicze do ZUS, umowy cywilno prawne, faktury, dane nauczycieli, zbiór danych do SIO, dokumentacja oświadczeń ubezpieczeniowych, dane pracownicze do funduszu świadczeń socjalnych, arkusz organizacyjny, listy osób, bilans, sprawozdania, BESTIA.	
5	Mliczak Anna	Inspektor ds. księgowości budżetowej			Dane pracownicze, kadrowe, płacowe oraz księgowość, dane pracownicze udostępnione innym podmiotom, dane pracownicze do ZUS, umowy cywilno prawne, faktury, dane nauczycieli, dokumentacja oświadczeń ubezpieczeniowych, dane pracownicze do funduszu świadczeń socjalnych, listy osób, Home banking – przelewy.	
6	Kowalska Maria	Inspektor ds. kadr			Akta osobowe, dane pracownicze, kadrowe, płacowe, dane pracownicze udostępnione innym podmiotom, dane pracownicze do ZUS, umowy cywilno prawne , dokumentacja emerytalno - rentowa.	

Data i podpis Administratora Bezpieczeństwa Informacji

29.10.2015 Mliczak

Zespół Obsługi Placówek Oświaty
w Okonku, ul. Leśna 46
64-965 OKONEK
NIP 767-15-70-923 REGON 572106468
tel. 067 266 91 45

załącznik nr 7 do „Polityki Bezpieczeństwa" zgodnie z art. 38 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.

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

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
1.	faktury	codziennie	codziennie	księgowość	rozrachunkowy
2.	Dokumenty do ZUS	co miesiąc	co miesiąc	Dział płacowy	Rozrachunkowo - ewidencyjny
3.	Dokumenty (umowy o pracę, umowy zlecenie, nadgodziny, premie, dodatek motywacyjny, wynagrodzenie dodatkowe)	co miesiąc	co miesiąc	Dział płacowy i księgowość	rozrachunkowy
4.	SIO	zgodnie z harmonogramem	zgodnie z harmonogramem		ewidencyjny
5.	Wyprawka szkolna	zgodnie z harmonogramem		Dział płacowy i księgowość	rozrachunkowo-ewidencyjny
6.	Pracownicy młodociani	zgodnie z harmonogramem		Burmistrz Okonka	ewidencyjny
7.	Dotacje	co miesiąc	co miesiąc	Burmistrz Okonka	rozrachunkowo-ewidencyjny
8.	Dane do SIO	zgodnie z harmonogramem		Dyrektorzy placówek	rozrachunkowo-ewidencyjny
9.	Listy wynagrodzeń	co miesiąc	co miesiąc	Dyrektorzy placówek	ewidencyjny
10.	Informacja roczna dla osoby ubezpieczeniowej	raz w roku	raz w roku	Dyrektorzy placówek	ewidencyjny
11.	Informacja roczna o dochodach oraz pobranych zaliczkach na podatek dochodowy	raz w roku	raz w roku	Dyrektorzy placówek	ewidencyjny
12.	Sprawozdania z wykonania budżetu	co miesiąc	co miesiąc	Dyrektorzy placówek	rozrachunkowo-ewidencyjny
13.	Zaświadczenia o dochodach	na potrzebę pracowników	na potrzebę pracowników	Pracownicy poszczególnych placówek	ewidencyjny

14.	Ewidencja placówek niepublicznych	na wniosek	na wniosek	wnioskujący podmiot	ewidencyjny
15.	Upoważnienia do SIO	na wniosek	na wniosek	wnioskujący pracownik	ewidencyjny

Data i podpis Administratora Bezpieczeństwa Informacji

29.10.2015 .....