Polityka Bezpieczeństwa Informacji
w Specjalnym Ośrodku Szkolno-Wychowawczym im. Marynarza Polskiego
w Damnicy

Podstawa prawna:

1. Art. 47 i 51 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. 1997 r. nr 78, poz. 483).
2. Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. 2002 r. nr 101 poz. 926 ze zm.).
3. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 2004 r. nr 100 poz. 1024 ze zm.).
4. Ustawa Kodeks Pracy z 26 czerwca 1974 r. (Dz. U. 1974 r. nr 24 poz. 141 ze zm.).

Cz. I. Wstęp

Realizując „Politykę Bezpieczeństwa Informacji ... " zapewnia się ich:

- poufność, tzn. że informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, podmiotom, procesom;
- integralność, tzn. że dane nie zostają zmienione lub zniszczone w sposób nieautoryzowany;
- dostępność, tzn. że istnieje możliwość wykorzystania danych na żądanie, w założonym czasie, przez autoryzowany podmiot;
- rozliczalność, tzn. że istnieje możliwość jednoznacznego przypisania działań poszczególnym osobom;
- autentyczność, tzn. zapewnienie że tożsamość podmiotu lub zasobu jest taka, jak deklarowana;
- niezaprzeczalność, tzn. że uczestnictwo w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne;
- niezawodność, tzn. że zamierzone zachowania i jego skutki są spójne.

„Polityka Bezpieczeństwa Informacji ..." ma na celu zredukowanie wystąpienia negatywnych konsekwencji naruszeń w tym zakresie, tj.:

- naruszeń danych osobowych rozumianych jako prywatne dobro powierzone Ośrodkowi,
- naruszeń przepisów prawa oraz innych regulacji,
- utraty lub obniżenia reputacji placówki,

- strat finansowych ponoszonych w wyniku nałożonych kar,
- zakłóceń organizacji pracy spowodowanych nieprawidłowym działaniem systemu.

Realizując „Politykę Bezpieczeństwa Informacji..." w zakresie ochrony danych osobowych Ośrodek dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia warunki, aby dane te były:

- przetwarzane zgodnie z prawem,
- zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
- merytorycznie poprawne i adekwatne w stosunku do celu, w jakim są przetwarzane,
- przechowywane w postaci umożliwiającej identyfikacje osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

§ 1. Podstawowe pojęcia.

1) Ośrodek – należy rozumieć jako Specjalny Ośrodek Szkolno-Wychowawczy im. Marynarza Polskiego w Damnicy, w skrócie: SOSW im. MP w Damnicy.

2) Polityka - należy rozumieć „Polityka Bezpieczeństwa Informacji w SOSW im. MP w Damnicy" obowiązująca w Ośrodku.

3) Dane osobowe – należy rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

4) Przetwarzanie danych – to jakiekolwiek operacje wykonywane na danych osobowych tj. zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

5) Zbiór danych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny wg określonych kryteriów.

6) Instrukcja – to „Instrukcja zarządzania systemem informatycznym" stanowiąca cz. II dokumentu pn. „Polityka Bezpieczeństwa Informacji ...".

7) Administrator Danych Osobowych (ADO) – należy rozumieć dyrektor Ośrodka.

8) Administrator Bezpieczeństwa Informacji (ABI) – pracownik Ośrodka wyznaczony przez dyrektora (ADO) do nadzorowania przestrzegania zasad ochrony danych osobowych oraz przygotowywania dokumentów wymaganych przez aktualne przepisy o ochronie danych osobowych, powołany zarządzeniem dyrektora SOSW im. MP w Damnicy.

9) Administrator Systemu Informatycznego (ASI) – pracownik odpowiedzialny za funkcjonowanie systemu teleinformatycznego oraz stosowanie technicznych i organizacyjnych środków ochrony stosowanych w systemie.

10) Użytkownik systemu – osoba upoważniona do przetwarzania danych osobowych w systemie; użytkownikiem może być osoba zatrudniona w Ośrodku, osoba wykonująca pracę na podstawie umowy – zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w Ośrodku.

11) Identyfikator użytkownika (login) – ciąg znaków jednoznacznie identyfikujący osobę upoważniona do przetwarzania danych osobowych w systemie informatycznym.

12) System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

13) Zabezpieczanie danych w systemie informatycznym – wdrażanie i wykorzystywanie stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed nieuprawnionym ich przetwarzaniem.

14) Wysoki poziom bezpieczeństwa – musi występować wtedy, gdy przynajmniej jedno urządzenie systemu informatycznego, służące do przetwarzania danych osobowych, połączone jest z siecią publiczną.

15) Uwierzytelnianie – to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

16) Integralność danych - właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

17) Poufność danych osobowych – należy rozumieć jako własność zapewniającą, że dane osobowe nie są udostępniane nieupoważnionym podmiotom.

18) Sieć lokalna – połączenie komputerów pracujących w Ośrodku w celu wymiany danych (informacji) dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych.

19) Sieć publiczna – sieć telekomunikacyjna, nie będąca siecią wewnętrzną, służąca do świadczenia usług telekomunikacyjnych w rozumieniu ustawy - *Prawo telekomunikacyjne* z 21 lipca 2000 r. – (Dz. U. 2000 nr 73 poz.852 ze zm.).

20) Sieć telekomunikacyjna – urządzenia telekomunikacyjne zestawione i połączone w sposób umożliwiający przekaz sygnałów pomiędzy określonymi zakończeniami sieci za pomocą przewodów, fal radiowych, bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną w rozumieniu ustawy - *Prawo komunikacyjne* z dnia 21 lipca 2000 r. (Dz. U. 2000 nr 73 poz.852 ze zm.).

§ 2. Wykaz miejsc w których przetwarzane są dane osobowe.

1) Siedziba główna SOSW im. MP w Damnicy, ul. Korczaka 1.

Lp.	Miejsce przechowywania danych osobowych i ich zabezpieczenie	Zbiory lub opis przechow. danych	Sposób grom. i przetwarzania	Osoba/y odpowiedz.
1.	Gabinet dyrektora Ośrodka *Klucze są wydawane i deponowane w pomieszczeniu technicznym.*	Dokumentacja dotycząca nadzoru pedagogicznego. Protokoły Rad Pedagog. Listy obecności nauczy - cieli na posiedzeniach RP Uchwały Rad Pedagog. Arkusze ocen Arkusze organizacji .. Dokumentacje techniczne Dokumentacja współpracy	tradycyjny	dyrektor Ośrodka
2.	Gabinet wicedyrektora *Klucze są wydawane i deponowane w pomieszczeniu technicznym.*	Dokumentacja dotycząca nadzoru pedagogicznego Zestawienia wyników klasyfikacji Dokumentacja organizacji procesu dydaktycznego Zestawienia rozliczeń godz. pracy nauczycieli	tradycyjny	wicedyrektor Ośrodka

		Plany zajęć szkolnych Dokumentacja dotycząca sprawdzianu i egzaminu gimnazjalnego Dokumentacja wycieczek szkolnych		
3.	Gabinet pedagoga i psycho - loga *Klucze są wydawane i deponowane w pomieszczeniu technicznym.*	Dzienniki zajęć Testy psychologiczne Opinie o uczniach	tradycyjny	pedagog psycholog
4.	Kancelaria Ośrodka *Klucze są wydawane i deponowane w pomieszczeniu technicznym*	Teczki osobowe uczniów i wychowanków Akta osobowe pracown. Rejestr korespondencji Rejestry wypadków ucz - niów i pracowników	tradycyjny elektroniczny *(SIO, Kadry)*	specjalista ds. kancelarii i kadr
5.	Księgowość – pok. biurowy *Klucze są wydawane i deponowane w pomieszczeniu technicznym*	Listy płac Dane dotyczące sytuacji materialnej i socjalnej pracowników	tradycyjny elektroniczny *(SIO, Płatnik, Qwark, Quant)*	główny księgowy specjalista ds. księgo-wych i gospodarczych
6.	Biblioteka *Klucze są wydawane i deponowane w pomieszczeniu technicznym*	Karty wypożyczeń pracow - ników i uczniów	tradycyjny elektroniczny *(MOL*)*	bibliotekarz
7.	Gabinet pielęgniarki *Kluczem dysponuje pielęgniarka, ponadto klucz znajduje się w pomieszczeniu technicznym i wydawany jest z upoważnienia..*	Karty zdrowia uczniów i wychowanków Rejestr porad, wizyt	tradycyjny	pielęgniarka
8.	Pokój nauczycielski *Wejście do pokoju zabezpieczone jest kluczem elektronicznym do którego kod znają nauczyciele*	Dzienniki zajęć Księgi zastępstw Plany zajęć szkolnych	tradycyjny	nauczyciele i wychowawcy grup
9.	Sale zajęć *Klucze są wydawane i deponowane w pomieszczeniu technicznym*	Dzienniki zajęć prowadzo - nych w danym czasie Karty obserwacji uczniów/ wychowanków	tradycyjny	nauczyciele uczący w klasie zgodnie z planem zajęć
10.	Archiwum Ośrodka *Kluczem dysponuje specjalista ds. kadrowych i kancelaryjnych*	Dokumenty archiwalne	tradycyjny	specjalista ds. kancelarii i kadr

* Zainstalowano już program obsługi biblioteki i wprowadzono księgozbiór, jednak pełne jego funkcjonowanie przewiduje się od 1 września 2015 r.

Informacje uzupełniające/dodatkowe:

1) Siedziba główna Ośrodka jest monitorowana: wewnątrz i na zewnątrz obiektu.

2)Do pomieszczeń wymienionych w tabeli dostęp mają pracownicy obsługi wg ustalonego stałego rejonu pracy.

3)Klucze do pomieszczeń obiektu wydawane/zdawane są w pomieszczeniu technicznym Ośrodka.

4)W kancelarii Ośrodka znajdują się w kopertach klucze zapasowe do znacznej większości pomieszczeń.

2) DPS Przytocko

Lp.	Miejsce przechowywania danych osobowych i ich zabezpieczenie	Zbiory lub opis przech. danych	Sposób grom. i przetwarzania	Osoba/y odpowiedz.
1.	Pokój socjalny dla nauczycieli *Kluczem dysponują nauczyciele*	Dzienniki zajęć Karty obserwacji	tradycyjny	N-l odpowiada za przechow. dokum. pracy

3) DPS Machowinko

Lp.	Miejsce przechowywania danych osobowych i ich zabezpieczenie	Zbiory lub opis przech. danych	Sposób grom. i przetwarzania	Osoba/y odpowiedz.
1.	Pokój socjalny dla nauczycieli *Kluczem dysponują nauczyciele*	Dzienniki zajęć Karty obserwacji	tradycyjny	N-l odpowiada za przechow. dokum. pracy

§ 3. Zbiory danych przetwarzanych tradycyjnie:

Lp.	Nazwa zbioru danych – krótki opis	Struktura danych osobowych
1.	Arkusz organizacji	imię i nazwisko n-li, daty i miejsce urodzenia, PESEL, adres zamieszkania, wykształcenie, stopień awansu zawodowego, staż pracy/pedag., pensum, dane płacowe, stanowisko, zadania, plany zajęć,
2.	Księga uczniów	- imię i nazwisko uczniów, daty i miejsce urodzenia, PESEL, adres zamieszkania, nazwiska i imiona rodziców, adres rodziców, - informacje dot. przyjęcia do Ośrodka: data, klasa, świadectwo,
3.	Księga wychowanków	- imię i nazwisko wychowanków, daty i miejsce urodzenia, PESEL, adres zamieszkania, nazwiska i imiona rodziców, adres rodziców,
4.	Ewidencja ubezpieczeń uczniów i wychowanków	- imię i nazwisko uczniów/wychowanków, daty i miejsce urodzenia, PESEL, adres zamieszkania,
5.	Arkusze ocen	imię i nazwisko uczniów, daty i miejsce urodzenia, PESEL, adres zamieszkania, nazwiska i imiona rodziców, adres rodziców,
6.	Księgowość i finanse	imię i nazwisko pracownika oraz członków rodziny zam. we wspólnym gospodarstwie domowym, daty urodzenia, adres, telefon, PESEL, wykształcenie, płace, umowy, pożyczki, ewidencja zwolnień lekarskich, nr kont bankowych,
7.	Kadry	imię i nazwisko, adres, imiona i nazwiska rodziców, dane najbliższej rodziny, telefon, PESEL, seria i nr dowodu tożsamości, stosunek do służby wojskowej, zajmowane stanowisko, przydzielone zadania, dokumentacja doskonalenia zawodowego, nagrody, ubezpieczenie, składniki wynagrodzenia
8.	Dokumentacja osobowa uczniów i wychowanków (tzw. teczki)	imię i nazwisko uczniów, daty i miejsce urodzenia, PESEL, adres zamieszkania, nazwiska i imiona rodziców, adres rodziców, telefon kontaktowe, spostrzeżenia wychowawcze i dydaktyczne, opinie,
9.	Biblioteka	imię i nazwisko ucznia, pracownika
10.	Dokumentacja dotycząca edukacji (dzienniki, zeszyty obserwacji)	imię i nazwisko ucznia, wychowanka, adres zamieszkania, imiona rodziców, dane kontaktowe do rodziców
11.	Dokumentacja zdrowotna (pielęgniarka)	dane dot. stanu zdrowia dziecka udostępnione osobiście pielęgniarce przez rodziców
12.	Dokumentacja badań psychologicznych	imię i nazwisko uczniów, daty i miejsce urodzenia, adres zamieszkania, nazwiska i imiona rodziców, iloraz inteligencji

Informacje uzupełniające/dodatkowe:
1) Siedziba główna Ośrodka jest monitorowana: wewnątrz i na zewnątrz obiektu.
2) Do pomieszczeń wymienionych w tabeli dostęp mają pracownicy obsługi wg ustalonego stałego rejonu pracy.
3) Klucze do pomieszczeń obiektu wydawane/zdawane są w pomieszczeniu technicznym Ośrodka.
4) W kancelarii Ośrodka znajdują się w kopertach klucze zapasowe do znacznej większości pomieszczeń.

§ 4. 1 Miejsce oraz programy informatyczne służące do przetwarzania danych osobowych:

1) kancelaria, księgowość - program do obsługi systemu informacji oświatowej (SIO).

2) kancelaria – program „Sekretariat", „Qadr",

3) księgowość – program „Płatnik" system dwustronnej wymiany informacji do wysłania do ZUS kompletu dokumentów (korekty danych – pobieranych składek na ubezpieczenie emerytalne, rentowe, chorobowe, wypadkowe i zdrowotne) i odbieranie informacji z ZUS.

4) biblioteka – „MOL" - program obsługi biblioteki,

5) księgowość – „Qwant" program obsługi finansowej.

§ 5. Zbiory danych przetwarzanych za pomocą systemów informatycznych

Lp.	Nazwa zbioru danych osob./opis	Struktura danych osobowych
1.	Biblioteka*	imię i nazwisko, data urodzenia, miejsce urodzenia, adres, dane o wypożyczeniach
2.	Kadry	imię i nazwisko, adres, imiona i nazwiska rodziców, dane najbliższej rodziny, telefon, PESEL, seria i nr dowodu tożsamości, stosunek do służby wojskowej, zajmowane stanowisko, przydzielone zadania, dokumentacja

		doskonalenia zawodowego, nagrody, ubezpieczenie, składniki wynagrodzenia, ewidencja zwolnień lekarskich,
3.	Księgowość i finanse	imię i nazwisko pracownika oraz członków rodziny zam. we wspólnym gospodarstwie domowym, daty urodzenia, adres, telefon, PESEL, wykształcenie, płace, umowy, pożyczki, nr kont bankowych,
4.	Gabinet psychologa i pedagoga	imię i nazwisko uczniów, daty i miejsce urodzenia, PESEL, adres zamieszkania, nazwiska i imiona rodziców, adres rodziców, telefon kontaktowe, spostrzeżenia wychowawcze i dydaktyczne, opinie, iloraz inteligencji

* Zainstalowano już program obsługi biblioteki (MOL) i wprowadzono księgozbiór, jednak pełne jego funkcjonowanie przewiduje się od 1 września 2015 r.

§ 6. W skład systemu wchodzą:

1) dokumentacja papierowa (korespondencja, dokumentacja uczniów/wychowanków i pracowników),

2) wydruki komputerowe,

3) urządzenia i oprogramowanie komputerowe służące do przetwarzania informacji,

4) procedury przetwarzania danych w tym systemie, w tym procedury awaryjne.

§ 7. Sposób przepływu danych pomiędzy poszczególnymi systemami jest następujący:

1) programy są niezależne i posiadają samodzielne bazy danych wprowadzane do systemu manualnie,

2) komputery przynależne do poszczególnych stanowisk działają niezależnie,

3) przetwarzanie danych osobowych w systemie informatycznym odbywa się przy zachowaniu wysokiego poziomu bezpieczeństwa.

§ 8. Cele i zasady funkcjonowania polityki bezpieczeństwa:

"Polityka Bezpieczeństwa Informacji w SOSW im. MP w Damnicy" ma na celu zredukowanie wystąpienia negatywnych konsekwencji naruszeń w tym zakresie, tj.:

a) naruszeń danych osobowych rozumianych jako prywatne dobro powierzone Ośrodkowi,

b) naruszeń przepisów prawa oraz innych regulacji,

c) utraty lub obniżenia reputacji Ośrodka,

d) strat finansowych ponoszonych w wyniku nałożonych kar,

e) zakłóceń organizacji pracy spowodowanych nieprawidłowym działaniem systemów.

§ 9. Realizując "Politykę Bezpieczeństwa Informacji.." w zakresie ochrony danych osobowych Ośrodek dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą i zapewnia, że dane te są:

a) przetwarzane zgodnie z prawem,

b) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,

c) merytorycznie poprawne i adekwatne w stosunku do celu, w jakim są przetwarzane,

d) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej nic jest to niezbędne do osiągnięcia celu przetwarzania.

§ 10. Za przetwarzanie danych osobowych niezgodnie z obowiązującym prawem, celami przetwarzania lub przechowywanie ich w sposób nie zapewniający ochrony interesów osób,

których te dane dotyczą grozi odpowiedzialność karna wynikająca z przepisów ustawy o ochronie danych osobowych lub pracownicza na zasadach określonych w kodeksie pracy.

§ 11. Administrator Danych Osobowych (ADO) – Dyrektor Ośrodka:

1) formułuje i wdraża warunki techniczne i organizacyjne służące ochronie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,

2) decyduje o zakresie, celach oraz metodach przetwarzania i ochrony danych osobowych,

3) odpowiada za zgodne z prawem przetwarzanie danych osobowych w Ośrodku.

§ 12. Administrator Bezpieczeństwa Informacji (ABI) – pracownik Ośrodka wyznaczony przez dyrektora:

1) egzekwuje zgodnie z prawem przetwarzanie danych osobowych w Ośrodku w imieniu ADO,

2) wydaje upoważnienie do przetwarzania danych osobowych określając w nich zakres i termin ważności - wg wzoru w ***załączniku nr 1***,

3) odwołuje upoważnienie - wg wzoru w ***załączniku nr 2***,

4) prowadzi ewidencje osób upoważnionych do przetwarzania danych osobowych - wg wzoru rejestru w ***załączniku nr 3***,

5) ewidencjonuje oświadczenia osób upoważnionych o zaznajomieniu się z zasadami zachowania bezpieczeństwa danych – wg wzoru oświadczenia w ***załączniku nr 4***,

6) udziela wyjaśnień i interpretuje zgodność stosowanych rozwiązań zakresie ochrony danych osobowych z przepisami prawa,

7) bierze udział w podnoszeniu świadomości i kwalifikacji osób przetwarzających dane osobowe w Ośrodku i zapewnia odpowiedni poziom przeszkolenia w tym zakresie,

8) określa potrzeby w zakresie stosowanych w Ośrodku zabezpieczeń, wnioskuje do ADO o zatwierdzenie proponowanych rozwiązań i nadzoruje prawidłowość ich wdrożenia.

§ 12. Administrator Systemu Informatycznego (ASI) – pracownik Ośrodka wyznaczony przez dyrektora:

1) zarządza bezpieczeństwem przetwarzania danych osobowych w systemie informatycznym zgodnie z wymogami prawa i wskazówkami ABI lub ADO,

2) doskonali i rozwija metody zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzaniem,

3) przydziela identyfikatory użytkownikom systemu informatycznego oraz zaznajamia ich z procedurami ustalania i zmiany haseł dostępu,

4) nadzoruje prace związane z rozwojem, modyfikacją, serwisowaniem i konserwacją systemu,

5) zapewnia bezpieczeństwo wewnętrznego i zewnętrznego obiegu informacji w sieci i zabezpieczenie łączy zewnętrznych,

6) prowadzi nadzór nad archiwizacją zbiorów danych oraz zabezpiecza elektroniczne nośniki informacji zawierających dane osobowe.

§ 13. Pracownik przetwarzający dane (PPD) – pracownik upoważniony przez ABI:

1) chroni prawo do prywatności osób fizycznych powierzających Ośrodkowi swoje dane osobowe poprzez przetwarzanie ich zgodnie z przepisami prawa oraz zasadami określonymi w „Polityce Bezpieczeństwa Informacji .." i „Instrukcji zarządzania systemem…",

2) zapoznaje się z zasadami określonymi w „Polityce Bezpieczeństwa Informacji.." (cz. I), w tym z „Instrukcją zarządzania systemem…" (cz. II) i składa oświadczenie o znajomości tych przepisów.

§ 14. 1. Dostęp do danych osobowych może mieć wyłącznie osoba zaznajomiona z przepisami ustawy o ochronie danych osobowych oraz zasadami zawartymi w obowiązującej w Ośrodku „Polityce Bezpieczeństwa Informacji ..." i „Instrukcji zarządzania systemem…", przy czym osoba zaznajomiona z zasadami ochrony danych potwierdza to w pisemnym oświadczeniu.

2. Dostęp do danych osobowych może mieć wyłącznie osoba posiadająca pisemne oraz imienne upoważnienie wydane przez ABI.

3. ABI może wyznaczyć upoważnionych do przetwarzania danych pracowników Ośrodka do nadzoru nad upoważnionymi pracownikami podmiotów zewnętrznych lub innymi upoważnionymi osobami przetwarzającymi dane osobowe w Ośrodku.

§ 15. Dane osobowe mogą być udostępniane osobom i podmiotom z mocy przepisów prawa, jeżeli w sposób wiarygodny uzasadnią one potrzebę ich posiadania, a ich udostępnienie nie naruszy praw i wolności osób, których one dotyczą.

§ 16. Udostępnienie danych może nastąpić na pisemny wniosek wg wzoru w ***załączniku nr 5***.

§ 17. Administrator odmawia udostępnienia danych jeśli spowodowałoby to naruszenie dóbr osobistych osób, których te dane dotyczą lub innych osób.

§ 18.1. Powierzenie danych może nastąpić wyłącznie w drodze pisemnej umowy, w której osoba przyjmująca dane zobowiązuje się do przestrzegania obowiązujących przepisów ustawy o ochronie danych osobowych.

2. Umowa powinna zawierać informacje o podstawie prawnej powierzenia danych, celu i sposobie ich przetwarzania.

§ 19. Każda osoba fizyczna, której dane przetwarzane są w Ośrodku, ma prawo zwrócić się z wnioskiem o udzielenie informacji związanej z przetwarzaniem tych danych, prawo do kontroli i poprawiania swoich danych osobowych, a także w przypadkach określonych w art. 32, ust.1, kpt.7 i 8 ustawy o ochronie danych osobowych prawo wniesienia umotywowanego żądania zaprzestania przetwarzania danych oraz sprzeciwu wobec przekazywania ich innym podmiotom.

§ 20. 1. Pomieszczenia, w których znajdują się przetwarzane zbiory danych osobowych pozostają zawsze pod bezpośrednim nadzorem upoważnionego do ich przetwarzania pracownika Ośrodka.

2. Opuszczenie pomieszczenia, w którym znajdują się zbiory danych osobowych musi być poprzedzone przeniesieniem zbioru danych do odpowiednio zabezpieczonego miejsca. Przy planowanej dłuższej nieobecności pracownika pomieszczenie winno być zamknięte na klucz.

3. Klucze do szaf, w których przechowywane są dane osobowe maja jedynie pracownicy upoważnieni do przetwarzania danych w zakresie zgodnym z ich kategorią.

4. Dostęp do pomieszczeń poza godzinami pracy jest kontrolowany za pomocą monitoringu wizyjnego.

5. Korzystanie ze zbiorów danych osobowych przez osoby niezatrudnione w Ośrodku powinno odbywać się po uzyskaniu upoważnienia lub skonsultowane z ABI w przypadku osób upoważnionych do przetwarzania tych danych na podstawie ogólnie obowiązujących przepisów.

6. Dokumentacji, która zawiera zbiory danych osobowych, nie można wynosić poza teren Ośrodka. Wyjątek stanowi dokumentacja związana z realizacją określonych zadań edukacyjno-wychowawczych poza terenem Ośrodka w sytuacja regulowanych przez inne przepisy prawa. Za zabezpieczenia dokumentacji odpowiedzialna jest osoba wskazana przez ADO.

7. Osoby prowadzące dokumentację zobowiązane są do niezwłocznego poinformowania ABI lub ADO o podejrzeniu dostępu do dokumentacji przez osoby nieupoważnione.

8. Zabrania się:

a) wyrzucania dokumentów zawierających dane osobowe bez uprzedniego ich trwałego zniszczenia – anonimizacji,

b) pozostawiania dokumentów, kopii dokumentów zwierających dane osobowe w drukarkach, kserokopiarkach,

c) pozostawiania kluczy w drzwiach, szafach, biurkach, zostawiania otwartych pomieszczeń, w których przetwarza się dane osobowe,

d) pozostawiania bez nadzoru osób trzecich przebywających w pomieszczeniach Ośrodka, w których przetwarzane są dane osobowe,

e) pozostawiania dokumentów na biurku po zakończonej pracy, pozostawiania otwartych dokumentów na ekranie monitora bez blokady konsoli,

f) ignorowania nieznanych osób z zewnątrz poruszających się w obszarze przetwarzania danych osobowych,

g) przekazywania informacji będącymi danymi osobowymi osobom nieupoważnionym.

§ 21. Korzystanie ze zbiorów danych osobowych przez osoby niezatrudnione w Ośrodku powinno odbywać się po uzyskaniu **upoważnienia** lub skonsultowane z ABI w przypadku osób upoważnionych do przetwarzania tych danych na podstawie ogólnie obowiązujących przepisów prawa.

§ 22. Zasady bezpiecznego użytkowania systemu informatycznego zawarte są w cz. II - „Instrukcji zarządzania systemem.." , obligatoryjnej do zapoznania się i stosowania przez wszystkich użytkowników systemu informatycznego Ośrodka.

§ 23. Identyfikacja zagrożeń opiera się o następujące założenia:

Ze względu na formę przetwarzania danych osob.	Rodzaje możliwych zagrożeń
Dane przetwarzane i przechowywane w formie tradycyjnej – papierowej.	- zdarzenia losowe np. pożar, powódź,.. - kradzież danych, oszustwo, celowe działanie na szkodę Ośrodka, -zaniedbania pracowników tj. niedyskrecja, udostępnienie danych osobie nieupoważnionej, - niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania, - pokonanie zabezpieczeń fizycznych, włamania, - podsłuchy, podglądy w celu wyłudzenia danych, - ataki terrorystyczne, - brak rejestrowania udostępnionych danych, niewłaściwe miejsce i sposób przechowywania danych.
Dane przetwarzane i przechowywane za pomocą systemów informatycznych.	- nie przydzielenie użytkownikom systemu informatycznego identyfikatorów, - niewłaściwa administracja systemem, - niewłaściwa konfiguracja systemu, - fałszowanie kont użytkowników, - kradzież danych z kont, - pokonanie zabezpieczeń programowych, - zaniedbania pracowników (niedyskrecja, udostępnienie danych osobie nieupoważnionej), - niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania, - zdarzenia losowe np. pożar, powódź,.. - niekontrolowane wytwarzanie i wypływ danych poza obszar przetwarzania z pomocą nośników informacji i komputerów przenośnych, - naprawy i konserwacje systemu lub sieci teleinformatycznej wykonywane przez osoby nieuprawnione, - przypadkowe bądź celowe uszkodzenie systemów i aplikacji informatycznych lub sieci, - przypadkowe bądź celowe modyfikowanie systemów i aplikacji informatycznych lub sieci, - przypadkowe bądź celowe wprowadzenie zmian do chronionych danych osobowych, - brak rejestrowania zdarzeń tworzenia lub modyfikowania danych.

§ 24. Sposób zabezpieczenia danych:

Ze względu na formę przetwarzania danych osob.	Formy wprowadzonych zabezpieczeń
Dane przetwarzane i przechowywane w formie tradycyjnej – papierowej.	- przechowywanie danych w pomieszczeniach przechowywanych na klucz, - przechowywanie danych osobowych w szafach zamykanych na klucz, - przechowywanie danych wyłącznie przez osoby posiadające upoważnienie nadane przez ABI, - zapoznanie pracowników z zasadami przetwarzania danych osobowych oraz z obsługą systemu służącego do ich przetwarzania.
Dane przetwarzane i przechowywane za pomocą systemów informatycznych.	- kontrola dostępu do systemów, - zastosowanie programów antywirusowych i innych regularnie aktualizowanych narzędzi ochrony, - systematyczne tworzenie kopii zapasowych zbiorów danych przetwarzanych w systemach informatycznych, - składowanie nośników wymiennych i nośników kopii zapasowych w odpowiednio zabezpieczonych szafach, - przydzielenie pracownikom indywidualnych kont

	użytkowników i haseł, - stosowanie indywidualnych haseł logowania do poszczególnych programów, - właściwa budowa hasła, która zawiera litery i cyfry.

§ 25. Poziom ryzyka naruszenia bezpieczeństwa danych jest niski. Zastosowane techniczne i organizacyjne środki ochrony danych są adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych osobowych.

§ 26. Uwzględniając kategorie przetwarzanych danych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka dla systemów informatycznych, stosuje się wysoki poziom bezpieczeństwa. ABI i ASI przeprowadzają okresową analizę ryzyka dla poszczególnych systemów i na tej podstawie przedstawiają ADO propozycje dotyczące zastosowania środków technicznych i organizacyjnych, celem zapewnienia właściwej ochrony przetwarzanym danym.

Cz. II.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

§27. Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych w Ośrodku.

§28. Za tworzenie, modyfikację i nadawanie uprawnień kontom użytkowników odpowiada ASI. ASI nadaje uprawnienia w systemie informatycznym na podstawie upoważnienia nadanego pracownikowi przez ADO lub ABI.

§29. Usuwanie kont stosowane jest wyłącznie w uzasadnionych przypadkach, standardowo, przy ustaniu potrzeby utrzymywania konta danego użytkownika ulega ono dezaktywacji w celu zachowania historii jego aktywności.

§30. Osoby dopuszczone do przetwarzania danych osobowych zobowiązane są do zachowania tajemnicy w zakresie tych danych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje również po ustaniu stosunku pracy, co jest równoznaczne z cofnięciem uprawnień do przetwarzania danych osobowych.

§31.1. Oprogramowanie wykorzystywane do przetwarzania danych posiada własny system kont (zabezpieczonych hasłami) i uprawnień. Zmiana hasła jest wymuszona automatycznie przez system.

2. W przypadku oprogramowania, które nie ma automatycznego wymuszania zmiany hasła, zaleca się dokonywać zmiany hasła co 30 dni.

3. W przypadku utracenia hasła użytkownik ma obowiązek skontaktować się z ASI celem uzyskania nowego hasła.

§32. System informatyczny powinien zapewnić zapis faktu przekazania danych osobowych z uwzględnieniem:

1/ identyfikatora osoby, której dane dotyczą,

2/ osoby przesyłającej dane,

3/ odbiorcy danych,

4/ zakresu przekazanych danych osobowych,

5/ daty operacji,

6/ sposobu przekazania danych.

§33.1. Stosuje się aktywną ochronę antywirusową każdym komputerze, na którym przetwarzane są dane osobowe.

2. Za dokonywanie skanowania systemu w poszukiwaniu złośliwego oprogramowania (w przypadku braku ochrony rezydentnej) i aktualizację bazy wirusów odpowiada użytkownik stacji roboczej.

§34. W celu rozpoczęcia pracy w systemie informatycznym użytkownik:

a/ loguje się do systemu operacyjnego przy pomocy identyfikatora i hasła na komputerach tego wymagających,

b/ loguje się do programów i systemów wymagających dodatkowego wprowadzenia unikalnego identyfikatora i hasła.

§35.1. W sytuacji tymczasowego zaprzestania pracy na skutek nieobecności przy stanowisku komputerowym należy uniemożliwić osobom postronnym korzystanie z systemu informatycznego poprzez wylogowanie się z sytemu lub uruchomienie wygaszacza ekranu chroniony hasłem.

2. W sytuacji gdy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba należy tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor (przymknąć ekran laptopa) w sposób uniemożliwiający wgląd w wyświetlaną treść.

3.Użytkownik wyrejestrowuje się z systemu informatycznego przed wyłączeniem stacji komputerowej poprzez zamknięcie programu przetwarzającego dane oraz wylogowanie się z systemu operacyjnego.

§36. Pracownik korzystający z systemu informatycznego zobowiązany jest do powiadomienia ASI oraz ABI w razie:

1/ podejrzenia naruszenia bezpieczeństwa systemu;

2/ braku możliwości zalogowania się użytkownika na jego konto;

3/ stwierdzenia fizycznej ingerencji w przetwarzana dane;

4/ stwierdzenia użytkowania narzędzia programowego lub sprzętowego.

§37. Na fakt naruszenia zabezpieczeń systemu mogą wskazywać:

1/ nietypowy stan stacji roboczej (np. brak zasilania, problemy z uruchomieniem);

2/ wszelkiego rodzaju różnice w funkcjonowaniu systemu (np. komunikaty informujące o błędach,

3/ brak dostępu do funkcji systemu, nieprawidłowości w wykonywanych operacjach);

4/ różnice w zawartości zbioru danych osobowych (np. brak lub nadmiar danych);

5/ inne nadzwyczajne sytuacje.

§38. 1. Pełne kopie zapasowe zbiorów danych tworzone są 2 razy w ciągu roku - wykonuje ASI

2. Odpowiedzialnym za wykonanie bieżących kopii danych (dziennych) jest pracownik obsługujący dany program przetwarzający dane, w sytuacja gdy wystąpiła zmiana danych.

3. Pełne kopie danych przechowywane są w szafie metalowej w kancelarii Ośrodka.

4. Kopie dzienne danych przechowywane są na nośniku przenośnym np. pendrive.

§39.1. Usuwanie kopii danych następuje poprzez bezpieczne kasowanie. Nośniki danych, na których zapisywane są kopie bezpieczeństwa niszczy się trwale w sposób mechaniczny.

2. Za usuwanie kopii odpowiedzialny jest ABI.

§40.1. Dane osobowe przetwarzane w systemach informatycznych mogą być udostępnione osobom i podmiotom z mocy przepisów prawa.

2. Do podmiotów, dla których dopuszczalne jest udostępnianie danych przez SOSW im. MP w Damnicy należą:

a/ organ nadzorujący (w związku z awansem zawodowym, wyniki badań psychologiczno-pedagogicznych dzieci i młodzieży),

b/ organ prowadzący (wykaz czasu pracy pracowników, udostępnianie dzienników zajęć, wykazy wygenerowane z SIO, wszystkie dane dotyczące pracowników i uczniów/wychowanków),

c/ Centralna Komisja Egzaminacyjna w zakresie umożliwiającym przeprowadzenie sprawdzianu i egzaminów,

d/ dzienniki lekcyjne (dane rodziców w zakresie opisanym w aktualnym rozporządzeniu MEN w sprawie sposobu prowadzenia dokumentacji),

e/ strona www Ośrodka (dane osobowe ucznia/wychowanka i np. jego osiągnięcia, publikowanie list z wynikami, zdjęciem - **tylko za zgodą**, imiona i nazwiska pracowników, tytuły naukowe, plan zajęć, informacje o pracy Ośrodka),

f/ tablica ogłoszeń (informacje o pracy Ośrodka, plany zajęć, dane osobowe ucznia i np. jego osiągnięcia, publikowanie list z wynikami, zdjęciem - **tylko za zgodą**),

g/ formularz rekrutacyjny do szkoły, karta potwierdzenia woli (dane osobowe rodziców/prawnych opiekunów i ucznia: adres zamieszkania, nr telefonu, PESEL ucznia, itp. - **tylko za zgodą**),

h/ podmioty świadczące usługi w zakresie oświaty, np. towarzystwa ubezpieczeniowe (w zależności od celu),

i/ podmioty nadzorujące realizację projektów tj. EFS, ERASMUS,.. (dane osobowe uczestników projektu i ich rodziców, w zależności od celu),

j/ inne podmioty - po określeniu celu i zakresu przekazanych danych, na podstawie wniosku (np. sądy rodzinne)

§41.1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe mogą być wykonywane wyłącznie przez pracowników Ośrodka lub przez upoważnionych przedstawicieli wykonawców.

2. Powyższe prace powinny uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.

3. Wszelkie prace konserwacyjne systemów informatycznych Ośrodka wykonywane są przez ASI lub za jego wiedzą i nadzorem.

4. Przed rozpoczęciem prac przez osoby niebędące pracownikami Ośrodka należy dokonać potwierdzenia tożsamości tychże osób.

§42.1. Wszelkie wydruki z systemów informatycznych zawierające dane osobowe przechowywane są w miejscu uniemożliwiającym ich odczyt przez osoby nieuprawnione, w zamkniętych szafach lub pomieszczeniach i po upływie ich przydatności są niszczone przy użyciu niszczarek /w sposób uniemożliwiający ich odczytanie (pocięte w poprzeczne paski).

2.Niszczenie zapisów na nośnikach danych powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika.

3. Uszkodzone nośniki danych przed ich wyrzuceniem należy fizycznie zniszczyć w niszczarce.

§43. Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:

1/ nieautoryzowany dostęp do danych,

2/ nieautoryzowane modyfikacje lub zniszczenie danych,

3/ udostępnienie danych nieautoryzowanym podmiotom,

4/ nielegalne ujawnienie danych,

5/ pozyskiwanie danych z nielegalnych źródeł.

§44.1. Każdy pracownik Ośrodka, który stwierdzi fakt naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe, bądź posiada informację mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany niezwłocznie zgłosić to ADO lub ABI.

2. Każdy pracownik Ośrodka, który stwierdzi fakt naruszenia bezpieczeństwa danych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenie ochrony oraz ustalić przyczynę i sprawcę naruszenia ochrony.

3. W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ADO lub ABI.

4. Formy naruszeń danych osobowych zawiera ***załącznik nr 6***

§45.1. ABI podejmuje następujące kroki:

1/ zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości pracy Ośrodka,

2/ może zażądać dokładnej relacji z zaistniałego naruszenia bezpieczeństwa danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,

3/ rozważa celowość i potrzebę powiadamiania o zaistniałym naruszeniu ADO,

2. ABI dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych osobowych sporządzając raport wg wzoru stanowiącego ***załącznik nr 7*** i przekazuje go ADO.

3. ABI zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych).

§46.1. Wobec osoby, która w przypadku naruszenia ochrony danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne.

2. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą o ochronie danych osobowych.

DYREKTOR

mgr Władysława Hanuszewicz

Załącznik nr 1
do „Polityki Bezpieczeństwa Informacji ..."

Damnica, 27 sierpnia 2015 r.

(pieczęć placówki)

UPOWAŻNIENIE nr .....

do przetwarzania danych osobowych

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. nr 10 poz. 926 ze zm.) upoważniam Panią/a ..... zatrudnioną/ego w Specjalnym Ośrodku Szkolno-Wychowawczym im. Marynarza Polskiego w Damnicy na stanowisku ..... do przetwarzania danych osobowych zgromadzonych w formie tradycyjnej oraz w systemach informatycznych w zakresie wynikającym z zajmowanego stanowiska pracy, w okresie od dnia ..... 20 .. r. do dnia ..... 20 ... r. / na czas nieokreślony

Wyżej wymieniona osoba została wpisana do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w Ośrodku.

.....
(podpis ABI)

Przyjmuję do wiadomości i stosowania.

.....
(czytelny podpis osoby upoważnionej)

Załącznik nr 2
do „Polityki Bezpieczeństwa Informacji ..."

Damnica, ...20 ...r.

(pieczęć placówki)

ODWOŁANIE UPOWAŻNIENIA nr .....
do przetwarzania danych osobowych

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. nr 10 poz. 926 ze zm.) odwołuję z dniem ..... 20 ... r. upoważnienie do przetwarzania danych osobowych wystawione dla Pani/a.

.....
(podpis ABI)

Załącznik nr 3
do „Polityki Bezpieczeństwa Informacji ..."

Damnica, ...20 ...r.

(pieczęć placówki)

REJESTR OSÓB UPOWAŻNIONYCH
DO PRZETWARZANIA DANYCH OSOBOWYCH

Nr upoważnienia	Imię i nazwisko	Identyfikator użytkownika*	Zakres upoważnienia do przetwarzania danych osobowych	Data nadania uprawnień i podpis ABI	Data odebrania uprawnień i podpis ABI	Uwagi

** Wypełnia się tylko dla osób upoważnionych do przetwarzania danych osobowych, które zostały dopuszczone do przetwarzania danych osobowych w systemie informatycznym.*

Załącznik nr 4
do „Polityki Bezpieczeństwa Informacji ..."

OŚWIADCZENIE
o zachowaniu poufności i zapoznaniu się z przepisami

Ja niżej podpisana/y **oświadczam,** iż
1. **zobowiązuję się** do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miała/ł dostęp w związku z wykonywaniem:
Rodzaj zadań

zadań i obowiązków służbowych wynikających z umowy o pracę	
zadań wynikających z umowy cywilno-prawnej	
zadań wynikających z umowy - w związku z praktyką studencką	

** właściwe zaznaczyć X*

zarówno **w trakcie wykonywania umowy, jak i po jej ustaniu.**

2. **zobowiązuję się** przestrzegać polityki, instrukcji i procedur, obowiązujących w **Specjalnym Ośrodku Szkolno-Wychowawczym im. Marynarza Polskiego w Damnicy przy ul. Korczaka 1** - zwanego dalej Ośrodkiem, dotyczących ochrony danych osobowych.

W szczególności **oświadczam**, że bez upoważnienia nie będę wykorzystywała/ł danych osobowych ze zbiorów znajdujących się w Ośrodku.

Oświadczam, że zostałam/em poinformowana/y o obowiązujących w Ośrodku zasadach, dotyczących przetwarzania danych osobowych, określonych w *„Polityce Bezpieczeństwa Informacji..."*

Oświadczam, że zostałam/em zapoznana/y z przepisami Ustawy o ochronie danych osobowych (tekst jedn.: Dz. U. z 2014, poz. 1182) 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 (Dz. U. Nr 100, poz. 1024 ze zm.).

Oświadczam, że zostałam/em poinformowana/y o grożącej, stosownie do przepisów rozdziału VIII ustawy o ochronie danych osobowych, odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, że naruszenie zasad ochrony danych osobowych, obowiązujących w Ośrodku może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

Damnica, ... r.
(miejsce i data złożenia oświadczenia)

... ...
(czytelny podpis osoby składającej oświadczenie)

Załącznik nr 5
do „Polityki Bezpieczeństwa Informacji ..."

Damnica, ...20 ...r.

.....
(imię i nazwisko)
.....
(adres)
.....

Informacja o zawartości zbioru danych osobowych

W związku z Pana/i wnioskiem z dnia ..... r. o udzielenie informacji związanych z przetwarzaniem danych osobowych w Specjalnym Ośrodku Szkolno-Wychowawczym im. Marynarza Polskiego w Damnicy, działając na podstawie art. 33 ust. 1 Ustawy o ochronie danych osobowych informuję, że zbiór danych zawiera następujące Pani/Pana dane osobowe:
.....

Powyższe dane przetwarzane są w SOSW im. MP w Damnicy w celu .....
.....
z zachowaniem wymaganych zabezpieczeń i zostały uzyskane (podać w jaki sposób)
....

Powyższe dane nie były/były udostępniane* (podać komu) .....
w celu (podać cel przekazania danych).....

Zgodnie z rozdz. IV Ustawy o ochronie danych osobowych przysługuje Pani/Panu prawo do kontroli danych osobowych, prawo ich poprawiania, a także w przypadkach określonych w art. 32 ust. 1 pkt 7 i 8 Ustawy, prawo wniesienia umotywowanego żądania zaprzestania przetwarzania danych oraz prawo sprzeciwu wobec przetwarzania danych w celach marketingowych lub wobec przekazywania danych innemu administratorowi danych osobowych.

.....
(podpis ABI)

**niepotrzebne skreślić*

Załącznik nr 6
do „Polityki Bezpieczeństwa Informacji ..."

Tabela form naruszeń danych osobowych
przez pracownika zatrudnionego przy przetwarzaniu danych.

Nr/kod naruszeń	Formy naruszeń	Sposób postępowania
A		
A.1	**W zakresie wiedzy**	
A.1.1	Ujawnianie sposobu działania aplikacji i systemu jej zabezpie - czeń osobom niepowołanym.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Zawiadomić natychmiast ABI. Sporządzić raport z opisem jaka informacja została ujawniona.
A.1.2	Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Zawiadomić natychmiast ABI. Sporządzić raport z opisem jaka informacja została ujawniona.
A.1.3	Dopuszczanie i stwarzanie warunków, aby ktokolwiek taką wiedzę mógł pozyskać, np. podczas obserwacji lub z dokumentacji.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Zawiadomić natychmiast ABI. Sporządzić raport z opisem jaka informacja została ujawniona.
A.2	**W zakresie sprzętu i oprogramowania.**	
A.2.1	Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych.	Niezwłocznie zakończyć działanie aplikacji. Sporządzić raport.
A.2.2	Bezprawne korzystanie z aplikacji w komputerze.	Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze. Pouczyć osobę, która dopuściła do takiej sytuacji. Sporządzić raport.
A.2.3	Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiekolwiek inne osoby niż osoba, której przydzielono identyfikator.	Natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie. Zawiadomić natychmiast ABI. Sporządzić raport.
A.2.4	Dopuszczenie do użytkowania sprzętu komputerowego i oprogra - mowania umożliwiającego dostęp do bazy danych osobowych przez osoby niebędące pracownikami.	Wezwać osobę nieuprawnioną do opuszczenia stanowiska. ustalić, jakie czynności zostały przez osobę nieuprawnioną wykonane. Przerwać pracę działających programów. Zawiadomić niezwłocznie ABI. Sporządzić raport.
A.2.5	Samodzielne instalowanie jakiegokolwiek oprogramowania.	Pouczyć osobę wykonującą wymienioną obok czyn - ność, aby jej natychmiast zaniechała. Wezwać ASI w celu odinstalowania programu. Sporządzić raport.
A.2.6	Modyfikowanie parametrów systemu i aplikacji.	Wezwać osobę wykonującą wymienioną obok czyn- ność, aby jej zaniechała. Sporządzić raport.
A.2.7	Odczytywanie nośników danych przed sprawdzeniem ich programem antywirusowym.	Pouczyć osobę wykonującą wymienioną obok czyn - ność, aby zaczęła stosować się do wymogów bezpie - czeństwa pracy. Wezwać służby informatyczne w celu wykonania kontroli antywirusowej. Sporządzić raport.

A.3	**W zakresie dokumentów i obrazów zawierających dane osobowe.**	
A.3.1	Pozostawienie dokumentów w otwar -tych pomieszczeniach bez nadzoru.	Zabezpieczyć dokumenty. Sporządzić raport.
A.3.2	Przechowywanie dokumentów zabezpie -czonych w niedostatecznym stopniu przed dostępem osób niepowołanych.	Powiadomić przełożonych. Spowodować poprawienie zabezpieczeń. Sporządzić raport.
A.3.3	Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.	Zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić przełożonych. Sporządzić raport.
A.3.4	Dopuszczanie do kopiowania dokumen -tów i utraty kontroli nad kopią.	Zaprzestać kopiowania. Odzyskać i zabezpieczyć wykona -ną kopię. Powiadomić przełożonych. Sporządzić raport.
A.3.5	Dopuszczanie, aby inne osoby odczyty -wały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.	Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor. Jeżeli ujawnione zostały ważne dane - sporządzić raport
A.3.6	Sporządzanie kopii danych na nośnikach danych w sytuacjach nie przewidzianych procedurą	Spowodować zaprzestanie kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Zawiadomić natychmiast ABI. Sporządzić raport.
A.3.7	Utrata kontroli nad kopią danych osobowych.	Podjąć próbę odzyskania kopii. Zawiadomić natychmiast ABI. Sporządzić raport.
A.4	**W zakresie pomieszczeń i infrastruktury służących do przetwarzania danych osobowych**	
A.4.1	Opuszczanie i pozostawianie bez dozoru nie zamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarza -nia danych osobowych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagraża -jących bezpieczeństwu danych osob.	Zabezpieczyć (zamknąć) pomieszczenie. Powiadomić przełożonych . Sporządzić raport.
A.4.2	Wpuszczanie do pomieszczeń osób nieznanych i dopuszczanie do ich kontaktu ze sprzętem komputerowym.	Wezwać osoby bezprawnie przebywające w pomieszcze-niach do ich opuszczenia, próbować ustalić ich tożsamość. Powiadomić przełożonych i ABI. Sporządzić raport.
A.4.3	Dopuszczanie, aby osoby spoza służb informatycznych i telekomunikacyj -nych podłączały jakikolwiek urządze -nia do sieci komputerowej, demonto -wały elementy obudów gniazd i torów kablowych lub dokonywały jakichkol -wiek manipulacji.	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania. Postarać się ustalić ich tożsamość. Zawiadomić ASI i ABI. Sporządzić raport.
A.5	**W zakresie pomieszczeń, w których znajdują się komputery centralne i urządzenia sieci.**	
A.5.1	Dopuszczenie lub ignorowanie faktu, że osoby spoza służb informatycznych i telekomunikacyjnych dokonują jakichkolwiek manipulacji przy urządzeniach lub okablowaniu sieci komputerowej w miejscach publicznych (hole, korytarze, itp.).	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i ew. opuszczenia pomieszczeń. Postarać się ustalić ich tożsamość. Zawiadomić ASI i ABI. Sporządzić raport
A.5.2	Dopuszczanie do znalezienia się w pomieszczeniach komputerów centralnych.	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i opuszczenia lub węzłów sieci komputerowej osób spoza służb informatycznych i telekomunikacyjnych lub ignorowania takiego faktu,

		chronionych pomieszczeń. Postarać się ustalić ich tożsamość. Zawiadomić ASI i ABI. Sporządzić raport.
B	**Zjawiska świadczące o możliwości naruszenia ochrony danych osobowych.**	
B.1	Ślady manipulacji przy układach sieci komputerowej lub komputerach.	Zawiadomić niezwłocznie ABI oraz ASI. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport
B.2	Obecność nowych kabli o nieznanym przeznaczeniu i pochodzeniu.	Zawiadomić niezwłocznie ASI. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.3	Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych.	Zawiadomić niezwłocznie ASI. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.4	Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych	Zawiadomić niezwłocznie ASI. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.5	Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania.	Zawiadomić niezwłocznie ASI. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.6	Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe.	Postępować zgodnie z właściwymi przepisami. Zawiadomić niezwłocznie ABI. Sporządzić raport.
C	**Formy naruszenia ochrony danych osobowych przez obsługę informatyczną w kontaktach z użytkownikiem.**	
C.1	Próba uzyskania hasła uprawniającego do dostępu do danych osobowych w ramach pomocy technicznej.	Zawiadomić ABI. Sporządzić raport.
C.2	Próba nieuzasadnionego przeglądania (modyfikowania) w ramach pomocy technicznej danych osobowych za pomocą aplikacji w bazie danych identyfikatorem i hasłem użytkownika.	Zawiadomić ABI. Sporządzić raport.

Załącznik nr 7
do „Polityki Bezpieczeństwa Informacji..."

Raport o naruszeniu danych osobowych
zawiera następujące informacje (wzór)

Imię i nazwisko osoby sporządzającej raport:

.....

Stanowisko /funkcja : .....

Kod formy naruszenia danych , zgodny z tabelą: .....

1. Miejsce, dokładny czas i data naruszenia ochrony danych osobowych (nr pokoju, piętro, godzina, itp.)
2. Osoba - z imienia i nazwiska - powodująca naruszenie, która swoim działaniem lub zaniechaniem przyczyniła się do naruszenia ochrony danych osobowych.
3. Osoby, które uczestniczyły w zdarzeniu związanym z naruszeniem ochrony danych osobowych
4. Informacja o danych , które zostały lub mogły zostać ujawnione.
5. Zabezpieczone materiały lub inne dowody związane z wydarzeniem.
6. Krótki opis wydarzenia związanego z naruszeniem ochrony danych osobowych (przebieg zdarzenia , opis zachowania uczestników, podjęte działania)

....., ...20..r. .....
(miejsce, data i podpis osoby sporządzającej raport)