Załącznik nr 1 do Zarządzenia Nr 26/2021
Dyrektora Domu Pomocy Społecznej dla Kombatantów w Biłgoraju
z dnia 26 września 2021 r.

POLITYKA OCHRONY DANYCH

w

Domu Pomocy Społecznej dla Kombatantów

w Biłgoraju

Spis treści

ROZDZIAŁ I

WPROWADZENIE

§1

1. Polityka Ochrony Danych jest dokumentem wewnętrznym Domu Pomocy Społecznej dla Kombatantów w Biłgoraju, dlatego też objęta jest obowiązkiem zachowania w poufności przez wszystkie osoby, którym zostanie ujawniona.
2. Wszystkie osoby mające dostęp do danych, zobowiązane są zapoznać się z niniejszym dokumentem oraz powinny podpisać oświadczenie, potwierdzające znajomość jego treści- **zał. nr 1** do niniejszej Polityki.
3. Dokument ten opisuje podstawowe zasady i wymagania organizacyjno-techniczne oraz prawne dla zapewnienia właściwej ochrony danych osobowych przetwarzanych w Domu Pomocy Społecznej dla Kombatantów w Biłgoraju.

§2

Słownik pojęć użytych w Polityce:

1. **DPS**- Domu Pomocy Społecznej dla Kombatantów w Biłgoraju
2. **Polityka**- Polityka ochrony danych w Domu Pomocy Społecznej dla Kombatantów w Biłgoraju.
3. **Administrator Danych Osobowych (Administrator lub ADO)** – Domu Pomocy Społecznej dla Kombatantów w Biłgoraju reprezentowany przez Dyrektora, który decyduje o celach i środkach przetwarzania danych osobowych.
4. **Inspektor Ochrony Danych (Inspektor lub IOD)** – osoba wyznaczona przez Administratora, odpowiedzialna za bieżący nadzór stosowania przepisów dot. ochrony danych.
5. **Administrator Systemów Informatycznych (ASI)** – pracownik DPS, który nadzoruje bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych.
6. **Osoba upoważniona** – osoba posiadająca upoważnienie nadane przez ADO, lub osobę przez niego upoważnioną, dopuszczona do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu.
7. **Użytkownik systemu** – osoba posiadająca upoważnienie wydane przez ADO lub osobę przez niego uprawnioną, dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej, w zakresie wskazanym w upoważnieniu, zwana dalej użytkownikiem.
8. **Organ nadzorczy**- Prezes Urzędu Ochrony Danych Osobowych.
9. **Dane osobowe** - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
10. **Przetwarzanie danych** - operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
11. **Zbiór danych** - oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
12. **Podmiot przetwarzający** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora.
13. **Odbiorca danych** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców. Przetwarzanie tych danych przez organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.
14. **Strona trzecia** - osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, Administrator, Podmiot przetwarzający czy osoby, które z upoważnienia Administratora lub Podmiotu przetwarzającego mogą przetwarzać dane osobowe.

15. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
16. **Bezpieczeństwo informacji** –zachowanie poufności, integralności i dostępności na odpowiednim poziomie.
17. **Bezpieczeństwo systemu informatycznego** – wdrożenie stosowanych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przez zniszczeniem, modyfikacją, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą.
18. **Bezpieczeństwo danych osobowych** – zespół zasad jakimi należy się kierować projektując oraz wykorzystując systemy i aplikacje służące do przetwarzania danych osobowych, by w każdych okolicznościach dostęp do nich był zgodny z założeniami i zapewniał im poufność, integralność oraz dostępność.
19. **Zgoda osoby, której dane dotyczą** - dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.
20. **Usuwanie danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
21. **Państwo trzecie** – państwo nienależące do Europejskiego Obszaru Gospodarczego.
22. **Użytkownik** – osoba, która posiada upoważnienie i polecenie przetwarzania danych osobowych i posiada uprawnienia do uwierzytelnionego dostępu do systemu informatycznego.
23. **Identyfikator użytkownika** - ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
24. **Logowanie** – uwierzytelnienie czyli działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
25. **Hasło** - ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
26. **Nośniki danych** – wszelkie nośniki, na których informacje zapisane są w postaci elektronicznej, w szczególności dyski zewnętrzne, dyski CD/DVD, karty magnetyczne.
27. **Dokumentacja przetwarzania danych** – dokumentacja opisująca sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, określona w przepisach wydanych na podstawie art. 24 ust. 1 i ust. 2 Rozporządzenia.
28. **Rejestr czynności przetwarzania** – zbiór wszystkich związanych z przetwarzaniem danych działań, każda wyodrębniona czynność.
29. **Rejestr kategorii czynności** - zapis aktywności przetwarzania realizowanej przez podmiot przetwarzający dla administratora, ściśle związana z celem przetwarzania danych.
30. **Naruszenie ochrony danych osobowych** – naruszenie bezpieczeństwa prowadzące do przypadkowego i niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
31. **Instrukcja** – rozumie się przez Instrukcję zarządzania systemem informatycznym.
32. **Uwierzytelnianie** - działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

§3

1. Utrzymanie bezpieczeństwa przetwarzanych danych, oznacza to zapewnienie ich:
   a) **poufności**, czyli zapewnienie, że tylko upoważnieni pracownicy mają dostęp do danych,
   b) **integralności** czyli zapewnienie dokładności i kompletności danych oraz metod ich przetwarzania,
   c) **dostępności** czyli zapewnienie, że osoby upoważnione mają dostęp do danych tylko wtedy, gdy są one im potrzebne.

§4

1. Celem wdrożenia Polityki Ochrony Danych jest określenie podstawowych zasad i wymagań organizacyjno-technicznych oraz prawnych dla zapewnienia właściwej ochrony bezpieczeństwa danych będących w posiadaniu DPS.
2. Polityka odnosi się do wszelkich zasobów informacyjnych związanych z realizacją zadań jednostki, a w szczególności do systemów informatycznych, systemów telekomunikacyjnych oraz wszelkich zastosowań informatyki rozpatrywanych w kontekście struktury organizacyjnej i technicznej jednostki oraz wszystkich pracowników.

§5

Zasady określone w Polityce Ochrony Danych mają zastosowanie do całego systemu informacyjnego, a w szczególności do:

1. Wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są informacje podlegające ochronie.
2. Wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie.
3. Wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, stażystów, praktykantów i innych osób mających dostęp do informacji podlegających ochronie.

ROZDZIAŁ II

ZAKRES I ZASADY PRZETWARZANIA DANYCH

§6

1. DPS przetwarza dane osobowe zarówno w postaci papierowej jak i elektronicznej, z poszanowaniem zasad określonych w Rozporządzeniu, czyli:

a) **zgodności z prawem, rzetelności i przejrzystości** – dane są przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane są przetwarzane,

b) **ograniczenia celu** - dane zbierane są w konkretnych, wyraźnych i prawnie uzasadnionym celu i nieprzetwarzane dalej w sposób niezgodny z tymi celami,

c) **minimalizacji danych** - dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane,

d) **prawidłowości** - dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane,

e) **ograniczenia przechowywania** - dane przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane,

f) **integralności i poufności** - dane przetwarzane są w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

2. Administrator jest odpowiedzialny za przestrzeganie w/w zasad przetwarzania danych i musi być w stanie wykazać ich przestrzeganie – **zasada rozliczalności**.

§7

1. Przetwarzanie danych osobowych jest dopuszczalne wyłącznie wtedy, gdy istnieje podstawa prawna przetwarzania.
2. Do przetwarzania danych zwykłych wymagane są:

a) zgoda osoby, której dane dotyczą; może zostać wyrażona w dowolnej formie, ale w razie wątpliwości Administrator powinien wykazać, że została udzielona.

b) przetwarzanie danych jest niezbędne do wykonania umowy z osobą, której dane dotyczą lub do podjęcia działań poprzedzających zawarcie umowy, na żądanie tej osoby,

c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze,

d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi.

W DPS zgodę należy pozyskać w celu publikacji wizerunku mieszkańca lub pracownika na stronie domowej jednostki, w mediach w celu informacji i promocji jednostki. Wzór zgody na wykorzystywanie wizerunku **załącznik nr 2 niniejszej Polityki.** Osobą która w DPS dba o pozyskanie zgody mieszkańca jest pracownik socjalny, od pracownika Inspektor ds. kadr, spraw socjalnych, bhp i p.poż.

Osoba, która wyraziła jakakolwiek zgodę na przetwarzanie danych może ją w każdym czasie odwołać. Wzór odwołania zgody stanowi **załącznik nr 3** do niniejszej Polityki.

3. W przypadku szczególnych kategorii danych, podstawą przetwarzania danych są:

a) wyraźna zgoda osoby, której dane dotyczą,
b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej,
c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody,
d) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy,
e) przetwarzanie jest niezbędne w celu dochodzenia praw przed sądem.

§8

1. Dane osobowe przetwarzane w DPS mogą być uzyskiwane bezpośrednio od osoby, której dane dotyczą lub z innych źródeł, w granicach dozwolonych przepisami prawa.
2. Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są bezpośrednio od niej, Administrator podczas pozyskiwania danych osobowych, podaje jej wszystkie niezbędne informacje zgodnie z art. 13 RODO, w postaci klauzuli informacyjnej.

Klauzula informacyjna dla kandydatów i mieszkańców DPS stanowi **załącznik nr 4** do niniejszej Polityki i jest dołączona do wniosków o przyjęcie do DPS. Klauzula informacyjna dla kandydatów do pracy stanowi **załącznik nr 5** i jest przedstawiona kandydatowi w chwili rozpoczęcia rekrutacji.

Wobec osób zarejestrowanych przez monitoring wizyjny, Administrator również spełnia obowiązek informacyjny, dlatego też wewnątrz budynku przy wejściu umieszczona została skrócona klauzula informacyjna dla osób zarejestrowanych przez monitoring. Pełny obowiązek informacyjny znajduje się w DPS w pokoju nr 405 na stanowisku pracy Inspektora ds. kadr, spraw socjalnych, bhp i poż. Klauzula ta stanowi **załącznik nr 6** do niniejszej Polityki.

5. W przypadku zbierania danych nie bezpośrednio od osoby, której one dotyczą, należy tę osobę dodatkowo poinformować o źródle pochodzenia danych osobowych przy pierwszym kontakcie z tą osobą.

ROZDZIAŁ III

UMOWA POWIERZENIA PRZETWARZANI DANYCH

§9

1. Przetwarzanie danych może zostać powierzone innemu podmiotowi pod warunkiem zawarcia z nim pisemnej umowy zgodnie z przepisami prawa.
2. Umowa powierzenia przetwarzania danych powinna zostać podpisana przez Administratora. Wzór umowy powierzenia przetwarzania danych stanowi **załącznik nr 7** do niniejszej Polityki.
3. Wszystkie umowy powierzenia powinny być zawarte w rejestrze, którego wzór stanowi **załącznik nr 8** do niniejszej Polityki.
4. Rejestr ten prowadzi inspektor ds. kadr, spraw socjalnych, bhp i p.poż.
5. Kierownicy komórek organizacyjnych/samodzielne stanowiska pracy odpowiadają za:
- wybór takiego podmiotu przetwarzającego, który zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.
- za realizację umowy w zakresie powierzenia przetwarzania danych.
6. Należy poinformować IOD o zamiarze powierzenia przetwarzania danych osobowych i przekazać mu niezbędne informacje w tym zakresie, tj. szczegółowy opis, na czym ma polegać przetwarzanie danych osobowych przez podmiot przetwarzający.
7. Każda umowa, porozumienie lub aneks w sprawie powierzenia przetwarzania danych osobowych musi być przedstawione IOD.

ROZDZIAŁ IV

OBOWIĄZKI ADMINISTRATORA DANYCH OSOBOWYCH

§10

Do obowiązków Administratora zaliczamy:

1. Nadzór nad przestrzeganiem przepisów prawa o ochronie danych osobowych i zapewnienie ich przestrzegania.
2. Zapewnienie środków technicznych i organizacyjnych do ochrony przetwarzania danych, a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, przetwarzaniem z naruszeniem przepisów o ochronie danych osobowych oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
3. Wyznaczenie IOD oraz ASI.
4. Zgłoszenie IOD do organu nadzorczego.
5. Włączenie IOD we wszystkie sprawy dotyczące ochrony danych.
6. Wspieranie IOD w wykonywaniu swoich zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych i operacji przetwarzania.
7. Nadawanie upoważnień do przetwarzania danych oraz zawieranie umów powierzenia przetwarzania danych.
8. Organizowanie szkoleń w zakresie przetwarzania danych osobowych i sposobów ich ochrony.
9. Prowadzenie rejestru czynności przetwarzania.
10. Identyfikowanie i analizowanie zagrożeń oraz ryzyka, na które narażone może być przetwarzanie danych w jednostce.
11. Dokonywanie oceny skutków dla ochrony danych.
12. Monitorowanie i zgłaszanie do organu nadzorczego naruszeń ochrony danych.
13. Współpraca z organem nadzorczym.

ROZDZIAŁ V

OBOWIĄZKI INSPEKTORA OCHRONY DANYCH

§11

Do obowiązków Inspektora Ochrony Danych zaliczamy:

1. Informowanie Administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy Rozporządzenia 2016/679 oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie.
2. Monitorowanie przestrzegania Rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty.
3. Udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania.
4. Współpraca z Prezesem Urzędu Ochrony Danych Osobowych.
5. Pełnienie funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.
6. Pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy Rozporządzenia.
7. Wspieranie Administratora w tworzeniu i dostosowywaniu dokumentacji wewnętrznej Szkoły.

ROZDZIAŁ VI

OBOWIĄZKI ADMINISTRATORA SYSTEMU INFORMATYCZNEGO

§12

Administrator Systemu Informatycznego odpowiedzialny jest za:

1. Bieżący monitoring oraz zapewnienie ciągłości działania systemu informatycznego oraz baz danych.
2. Optymalizację systemu informatycznego, baz danych.

3. Instalacje i konfiguracje systemu informatycznego, oprogramowania systemowego, sieciowego.
4. Zabezpieczenie systemu informatycznego przed nieupoważnionym dostępem.
5. Współpracę z dostawcami usług oraz sprzętu sieciowego.
6. Przyznawanie ściśle określonych praw dostępu do informacji w danym systemie.
7. Zarządzanie licencjami oraz procedurami ich dotyczącymi.
8. Prowadzenie polityki antywirusowej.
9. Sprawowanie nadzoru nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych.
10. Sprawowanie nadzoru nad naprawami, konserwacją, likwidacja urządzeń komputerowych, na których zapisane są dane osobowe, zleconymi firmom zewnętrznym.
11. Wdrażanie nowych systemów informatycznych.
12. Nadzorowanie poprawności przetwarzania danych.
13. Sprawowanie nadzoru nad bezpieczeństwem danych zawartych w komputerach przenośnych, dyskach zewnętrznych itd.
14. Przeciwdziałanie próbom naruszenia bezpieczeństwa informacji w jednostce.
15. Identyfikowanie i analizowanie zagrożeń oraz ryzyka, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych.
16. Określanie potrzeb w zakresie zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe.
17. Przeprowadzanie corocznego audytu KRI (Krajowych ram interoperacyjności).
W przypadku nieobecności ASI jego zadania realizuje osoba wyznaczona i upoważniona przez ADO, która składa ASI relacje z działań podejmowanych w czasie jego zastępstwa.

ROZDZIAŁ VII

REJESTRY PRZETWARZANIA

§13

1. Rejestr czynności przetwarzania prowadzi Administrator lub wyznaczona przez niego osoba. Wzór rejestru przetwarzania danych stanowi **załącznik nr 9 do** niniejszej Polityki.
2. Każdy podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego prowadzą rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora. Wzór tego rejestru stanowi **załącznik nr 10** do niniejszej Polityki.
3. Rejestry te w imieniu Administratora prowadzi inspektor ds. kadr, spraw socjalnych, bhp i p.poż.
4. Mają one formę pisemną, w tym elektroniczną.

ROZDZIAŁ VIII

DROGA NADAWANIA UPOWAŻNIEŃ DO PRZTWARZANIA DANYCH OSOBOWYCH

§14

1. Każdy pracownik przed dopuszczeniem do przetwarzania danych osobowych musi mieć pisemne, imienne upoważnienie nadane przez Administratora lub osobę przez niego wyznaczoną. W DPS upoważnienia te nadaje Administrator.
2. Jeśli zachodzi potrzeba nadania nowego upoważnienia lub jego aktualizacja, bezpośredni przełożony składa wniosek do Administratora. Jeżeli bezpośrednim przełożonym pracownika jest ADO, pracownik składa wniosek we własnym imieniu. Wzór wniosku o nadanie/aktualizację upoważnienia stanowi **zał. nr 11** do niniejszej Polityki, zaś wzór upoważnienia stanowi **zał. nr 12** do niniejszej Polityki.
3. Upoważnienia wpisuje się do rejestru upoważnień - zał. **nr 13** do niniejszej Polityki. Rejestr ten prowadzi inspektor ds. kadr, spraw socjalnych, bhp i p.poż.
4. Upoważnienie w każdym czasie może zostać odwołane. Wzór odwołania upoważnienia **stanowi zał. nr 14** do niniejszej Polityki.

6. Pracownicy, którzy nie są zatrudnieni do przetwarzania danych osobowych np. personel sprzątający, a przebywają w pomieszczeniach, gdzie dane osobowe są przetwarzane lub składowane, powinni podpisać oświadczenie-zał. **nr 15 do niniejszej** Polityki). Powinni również zostać przeszkoleni przez IOD.

ROZDZIAŁ IX

PROCEDURA DOPUSZCZENIA NOWEGO RACOWNIKA DO PRACY

§15

1. Do przetwarzania danych osobowych dopuszczone są wyłącznie osoby upoważnione przez Administratora lub osobę wyznaczoną.
2. Wszystkie osoby, których rodzaj wykonywanej pracy będzie wiązał się z dostępem do danych osobowych, przed przystąpieniem do pracy, podlegają szkoleniu w zakresie obowiązujących przepisów prawa dotyczących ochrony danych osobowych oraz obowiązujących w DPS zasad ochrony danych określonych w niniejszej Polityce i innych przepisach szczegółowych.
3. Szkolenie przeprowadza IOD, po zgłoszeniu takiej potrzeby przez ADO.
4. Fakt zapoznania się z w/w dokumentacją, osoba potwierdza poprzez złożenie podpisu według wzoru z załącznika **nr 15 do** niniejszej Polityki.
5. Po szkoleniu IOD przeprowadza test wiedzy i sporządza listę osób uczestniczących w szkoleniu.
6. Następnie Administrator musi nadać upoważnienie i wydać polecenie w zakresie przetwarzania danych osobowych.

§16

1. W przypadku zlecenia osobom lub podmiotom zewnętrznym wykonania usługi na rzecz DPS, z którą wiąże się konieczność upoważnienia do przetwarzania danych, w tym zapewnienia dostępu do systemu informatycznego oraz urządzeń wchodzących w jego skład służących do przetwarzania danych Administrator lub osoba przez niego wyznaczona powinna wydać stosowne upoważnienie.

§17

1. Za bezpieczeństwo informacji, w tym danych osobowych, odpowiedzialni są wszyscy pracownicy i inne osoby upoważnione do przetwarzania danych.
2. Wszyscy pracownicy i inne osoby upoważnione do przetwarzania danych, pod groźbą sankcji dyscyplinarnych i karnych, mają obowiązek zachowania tajemnicy informacji o przetwarzanych w DPS danych osobowych oraz o stosowanych sposobach ich zabezpieczeń. Obowiązek zachowania tajemnicy istnieje również po ustaniu zatrudnienia, innego stosunku prawnego lub współpracy.

ROZDZIAŁ X

OBOWIĄZKI OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH

§18

Osoby upoważnione do przetwarzania danych osobowych zobowiązane są w szczególności do:
- bezwzględnego przestrzegania zasad bezpieczeństwa przetwarzania danych, określonych w niniejszej Polityce oraz innych procedurach dotyczących zarządzania bezpieczeństwem informacji,
- przetwarzania danych osobowych tylko w wyznaczonych do tego celu pomieszczeniach służbowych lub wyznaczonych ich częściach,
- zabezpieczenia zbioru danych osobowych oraz dokumentów zawierających dane osobowe przed dostępem osób nieupoważnionych za pomocą środków określonych w niniejszej Polityce i innych procedurach dotyczących zarządzania bezpieczeństwem informacji,
- niszczenia wszystkich zbędnych nośników zawierających dane osobowe w sposób uniemożliwiający ich odczytanie,
- nieudzielania informacji o danych osobowych przetwarzanych w Szkole innym podmiotom, chyba że obowiązek taki wynika wprost z przepisów prawa i tylko w sytuacji, gdy przesłanki określone w tych przepisach zostały spełnione,

- niezwłocznego zawiadamiania ADO, a gdy dotyczy to danych utrwalonych w zbiorach informatycznych również ASI, o wszelkich zagrożeniach bezpieczeństwa danych osobowych, ewentualnych naruszeń bezpieczeństwa danych osobowych lub uzasadnionych podejrzeniach wystąpienia takiego naruszenia.

ROZDZIAŁ XI

OBSZARY PRZETWARZANIA DANYCH OSOBOWYCH

§19

1. Wykaz budynków i pomieszczeń w których przetwarzane są dane osobowe obejmuje wszystkie pomieszczenia, w których wykonuje się jakiekolwiek operacje na danych osobowych, w szczególności wprowadza się, modyfikuje, archiwizuje, usuwa dane, a także wszystkie miejsca, gdzie przechowuje się nośniki informacji zawierające dane osobowe. W/w wykaz przedstawia Tabela nr 1.

Tabela nr 1. Wykaz budynków Domu Pomocy Społecznej w Biłgoraju.

Lp.	Adres	Pomieszczenie	Rodzaj zabezpieczenia
1.	Ul. Generała Komorowskiego 20	Gabinet dyrektora	Zamek na klucz, kluczami dysponuje Dyrektor DPS
		Administracja pokój: 403, 404, 405, 410	Zamek na klucz, klucze dostępne w gabinecie lekarskim
		Gabinet lekarski 005	Zamek na klucz, klucze dostępne w gabinecie zabiegowym
		Gabinet zabiegowy 006	Zamek na klucz, klucze dostępne w gabinecie lekarskim

ROZDZIAŁ XII

UDOSTĘPNIANIE DANYCH OSOBOWYCH

§20

1. Administrator udostępnia dane osobowe przetwarzane w zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
2. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis prawa stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.
3. Wnioski o udostępnienie danych osobowych przetwarzanych są rozpatrywane przez Administratora DPS.
4. W przypadku konieczności udostępnienia dokumentów i danych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych osobowych.

ROZDZIAŁ XIII

AUDYT W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

§21

1. IOD przeprowadza audyt w zakresie przetwarzania danych osobowych w DPS.
2. Celem audytu jest sprawdzenie przestrzegania Rozporządzenia i innych przepisów o ochronie danych oraz polityk Administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych, w szczególności sprawdzenie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, przestrzegania przez osoby

upoważnione wymagań Polityki Ochrony Danych i innych procedur dotyczących zarządzania bezpieczeństwem informacji oraz stosowanych zabezpieczeń.
3. Do przeprowadzenia audytów, o których mowa w ust. 1 Administrator może upoważnić również ASI.

§22

1. Audyt jest przeprowadzany w trybie:
- planowanym – według planu audytu,
- doraźnym – w przypadku nieprzewidzianym w planie audytów, w szczególności w przypadku zgłoszenia naruszeń ochrony danych.
2. Plan audytów określa przedmiot oraz zakres przeprowadzenia audytu.
3. Plan audytu jest przygotowany przez IOD i przedstawiony Administratorowi nie później niż 7 dni przed planowanym audytem.

§23

1. IOD dokumentuje czynności przeprowadzone w toku audytu, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania sprawozdania.
2. Dokumentowanie czynności z audytu może polegać, w szczególności, na utrwaleniu danych z systemu informatycznego służącego do przetwarzania lub zabezpieczania danych oraz na:
- sporządzeniu notatki z czynności, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych,
- odebraniu wyjaśnień osoby, której czynności objęto sprawdzaniem,
- sporządzeniu kopii otrzymanego dokumentu,
- sporządzenie kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych (printscreen),
- sporządzeniu kopii zapisów rejestrów systemu informatycznego, służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu,
- sporządzaniu dokumentacji fotograficznej.
3. W systemie informatycznym służącym do przetwarzania lub zabezpieczania danych osobowych czynności IOD mogą być wykonywane przy udziale osób upoważnionych do przetwarzania danych, w szczególności osoby zarządzającej tym systemem.
4. Materiały są sporządzone w postaci papierowej lub w postaci elektronicznej.
5. Osoba odpowiedzialna za przetwarzanie danych osobowych, której dotyczy audyt, bierze udział w audycie lub umożliwia IOD przeprowadzenie czynności w toku audytu.

§24

1. Po zakończeniu sprawdzania, IOD przygotowuje sprawozdanie, które w ciągu 30 dni od zakończenia sprawdzenia przedstawia Administratorowi Danych Osobowych. Po sprawdzeniu doraźnym- niezwłocznie (jeśli sprawdzenie jest skutkiem naruszenia - natychmiast po sprawdzeniu).
2. Sprawozdanie jest sporządzone w postaci elektronicznej lub papierowej.
3. Sprawozdanie ze sprawdzenia zawiera co najmniej:
a) termin prowadzonego sprawdzenia,
b) cel, zakres i kryteria prowadzonego sprawdzenia,
c) obszar poddany sprawdzeniu,
d) ustalenia stanu faktycznego.
W/w sprawozdanie może zawierać rekomendacje dotyczące zmian w zakresie środków organizacyjnych i technicznych, których dotyczyło sprawdzenie.
4. Administrator danych jest zobowiązany do zapoznania się z w/w sprawozdaniem.

§25

1. ASI jest zobowiązany do bieżącego monitorowania systemu zabezpieczeń w systemach informatycznych.
2. W ramach monitoringu należy przeprowadzać w szczególności następujące działania:
- okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności do odtworzenia danych,
- sprawdzanie częstotliwości zmiany haseł przez użytkowników oraz stosowania innych zabezpieczeń.

ROZDZIAŁ XI

PROCEDURA POSTĘPOWANIA W PRZYPADKU NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

§26

1. Każdy pracownik lub inna osoba, w szczególności upoważniona do przetwarzania danych zobowiązana jest poinformować ADO i IOD, o każdym przypadku zagrożenia bezpieczeństwa danych osobowych, ewentualnych naruszeniach bezpieczeństwa ochrony danych osobowych lub uzasadnionych podejrzeniach wystąpienia takiego naruszenia.
2. Przez zagrożenie bezpieczeństwa danych osobowych rozumie się każde zdarzenie, zależne jak i niezależne od woli ludzkiej, które może powodować utratę integralności, poufności lub rozliczalności danych osobowych. W razie wątpliwości za zagrożenie bezpieczeństwa danych uważa się w szczególności:
a) niewłaściwe zabezpieczenie pomieszczeń i urządzeń,
b) niewłaściwe zabezpieczenie sprzętu informatycznego lub oprogramowania przed nieupoważnionym dostępem podmiotów trzecich, kradzieżą i utratą danych osobowych,
c) nieprzestrzeganie zasad Polityki Ochrony Danych, czy Instrukcji zarządzania systemem informatycznym lub stosowanych przepisów prawa,
d) naruszenie zabezpieczeń fizycznych przez podmiot trzeci.
3. Typowe sytuacje, gdy użytkownik powinien powiadomić Administratora o naruszeniu:
- ślady na drzwiach, oknach i szafach wskazują na próbę włamania,
- dokumentacja jest niszczona bez użycia niszczarki,
- fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie,
- otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe, stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.,
- nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych,
- ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe,
- wynoszenie danych osobowych w wersji papierowej lub elektronicznej na zewnątrz szkoły bez upoważnienia,
- udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej,
- stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
- telefoniczne próby wyłudzenia danych osobowych,
- kradzież komputerów lub twardych dysków z danymi osobowymi,
- utrata kontroli nad kopią danych osobowych,
- maile zachęcające do ujawnienia identyfikatora i/lub hasła,
- pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
- istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki",
- hasła do systemów przechowywane są w pobliżu komputera.
4. Naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

§27

Zgłoszenie podejrzewania wystąpienia naruszenia

1. Zgłoszenia należy dokonać bezpośrednio do Administratora Danych Osobowych, który zawiadamia IOD.
2. Jeżeli zdarzenie dotyczy podejrzenia naruszenia zabezpieczeń systemu informatycznego służącego do przetwarzania danych osobowych należy dodatkowo zawiadomić o tym ASI lub osobę go zastępującą.
3. Zgłoszenie o którym mowa w ust.1 powinno zawierać:
a)opisanie symptomów zdarzenia dotyczącego zabezpieczeń danych osobowych,

b) określenie sytuacji i czasu w jakim stwierdzono zdarzenie dotyczące zabezpieczeń danych osobowych,
c) określenie wszelkich możliwych informacji mogących wskazywać na przyczynę zdarzenia,
d) określenie wszelkich kroków podjętych po ujawnieniu zdarzenia.
4. W sytuacji wykrycia naruszenia ochrony danych należy:
a) niezwłocznie podjąć czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego zdarzenia, o ile taka możliwość istnieje,
b) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
c) zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym zdarzeniem i mogą utrudnić udokumentowanie i analizę,
d) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących zdarzeniu,
e) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
f) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
g) udokumentować wstępnie zaistniałe zdarzenia,
h) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia upoważnionych osób (ADO, IOD lub ASI).
5. Osoby upoważnione podejmują wszelkie działania mające na celu:
a) powstrzymanie lub ograniczenie dostępu do danych osoby nieuprawnionej,
b) minimalizację negatywnych skutków zdarzenia,
c) wyjaśnienie okoliczności zdarzenia,
d) zabezpieczenie dowodów zdarzenia,
e) umożliwienie dalszego bezpiecznego przetwarzania danych.

§28

Postępowanie wyjaśniające

1. W przypadku podejrzenia wystąpienia naruszenia, ADO w uzgodnieniu z IOD, prowadzi postępowanie wyjaśniające w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych.
2. Jeżeli zdarzenie dotyczy podejrzenia naruszenia zabezpieczeń systemu informatycznego służącego do przetwarzania danych osobowych w postępowaniu wyjaśniającym uczestniczy również ASI.
3. Do uczestniczenia w postępowaniu wyjaśniającym ADO może wyznaczyć również inne osoby.
4. W toku postępowania wyjaśniającego:
a) ustala się wszelkie okoliczności związane z tym zdarzeniem, w szczególności dokładny czas uzyskania informacji o zdarzeniu dotyczącym zabezpieczenia danych osobowych i czas samodzielnego wykrycia tego faktu,
b) niezwłocznie generuje się i drukuje (jeżeli zasoby systemu na to pozwalają) wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatruje się je datą i podpisem, przystępuje się do zidentyfikowania rodzaju zaistniałego zdarzenia, a zwłaszcza do określenia skali naruszeń i metody dostępu do danych osobowych nieuprawnionej osoby,
c) ustala się jakie mogą być skutki zaistniałego zdarzenia,
d) ustala się jakie działania należy podjąć w celu zapobiegnięcia skutkom,
e) ustala się osoby odpowiedzialne za zaistniałą sytuację.
5. W trakcie postępowania wyjaśniającego, należy przeprowadzić szczegółową analizę przyczyny zdarzenia dotyczącego narażenia ochrony danych osobowych oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości. Jeśli przyczyną był:
a) błąd osoby wykonującej jakiekolwiek zadania przy przetwarzaniu danych osobowych w systemie informatycznym, należy przeprowadzić szkolenie osób biorących udział przy przetwarzaniu danych,
b) uaktywnienie wirusa, należy ustalić źródło jego pochodzenia oraz zainstalować zabezpieczenia antywirusowe lub sprawdzić stan istniejących zabezpieczeń,
c) zaniedbanie ze strony osoby wykonującej jakiekolwiek zadania przy przetwarzaniu danych osobowych, należy wyciągnąć odpowiednie konsekwencje,
d) włamanie w celu uzyskania bazy danych osobowych, należy dokonać szczegółowej analizy wdrożonych środków zabezpieczających w celu zapewnienia skutecznej ochrony danych osobowych,

e) zły stan urządzenia, w tym urządzenia do przechowywania danych utrwalonych na papierowych nośnikach lub sposób działania programu, należy niezwłocznie przeprowadzić kontrolne czynności serwisowe.

6. Po przywróceniu normalnego stanu działania systemu przetwarzania danych osobowych, jeżeli nastąpiło uszkodzenie bazy danych lub zbiory tradycyjnego, niezbędne jest odtworzenie jej z dostępnych źródeł, w tym z ostatniej kopii zapasowej, z zachowaniem wszelkich środków ostrożności, mających na celu uniknięcie ponownego dostępu tą samą drogą przez osobę nieuprawnioną.

7. W przypadku naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Zgłoszenia dokonuje się przez stronę internetową Urzędu Ochrony Danych Osobowych.

8. Zawiadomienie, o którym mowa w ust. 7, nie jest wymagane, w następujących przypadkach:

a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,

b) Administrator zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1,

c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

§29

1. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

2. Osoba wyznaczona przez Administratora-inspektor ds. kadr, spraw socjalnych, bhp i p.poż, prowadzi rejestr naruszeń bezpieczeństwa danych osobowych. Wzór rejestru stanowi **załącznik nr 16** do niniejszej Polityki.

3. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Zawiadomienie dokonywane jest zgodnie z art. 34 Rozporządzenia.

4. Administrator Danych Osobowych po każdym wystąpieniu zagrożenia bezpieczeństwa danych osobowych lub naruszenia ochrony danych analizuje możliwość i zasadność podjęcia działań, które zminimalizują ryzyko zaistnienia podobnej sytuacji w przyszłości oraz sporządza raport z naruszenia ochrony danych z **załącznika nr 17** do niniejszej Polityki.

ROZDZIAŁ XII

ODPOWIEDZIALNOŚĆ PRACOWNIKÓW

§30

1. Nieprzestrzeganie zasad postępowania określonych w niniejszej Polityce stanowi naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności dyscyplinarnej określonej w Kodeksie Pracy.

2. Jeżeli skutkiem działania określonego w ust. 1 jest ujawnienie informacji osobie nieupoważnionej, sprawca może zostać pociągnięty do odpowiedzialności karnej wynikającej z przepisów dotyczących ochrony danych osobowych lub Kodeksu Karnego.

3. Jeżeli skutkiem działania określonego w ust. 1 jest szkoda, sprawca może ponieść odpowiedzialność materialną na warunkach określonych w przepisach Kodeksu Pracy oraz Prawa Cywilnego.

ROZDZIAŁ XIII

OKREŚLENIE ŚRODKÓW ORGANIZACYJNYCH I TECHNICZNYCH NIEZBĘDNYCH DO ZAPEWNIENIA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH

§31
Środki organizacyjne

I. Dostęp do danych.

1. Dostęp do danych mogą mieć tylko i wyłącznie osoby posiadające pisemne, imienne upoważnienie nadane przez Administratora Danych Osobowych lub osobę przez niego wyznaczoną.

2. Osoba upoważniona do przetwarzania danych osobowych powinna zachować szczególną ostrożność przy przetwarzaniu danych.

3. Przetwarzać dane osobowe można wyłącznie w zakresie nadanego upoważnienia.

4. Należy chronić dane przed wszelkim dostępem do nich osób nieupoważnionych.

5. Wynoszenie, przekazywanie, kopiowanie, udostępnianie danych osobowych osobom nieupoważnionym grozi sankcjami administracyjnymi i karnymi.

6. W przypadku niszczenia danych osobowych po upływie okresu przechowywania sporządza się protokół ze zniszczenia, którego wzór stanowi załącznik nr 18 do niniejszej Polityki.

II. Polityka czystego biurka.

1. Dane osobowe w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych, a następnie muszą być chowane do szaf.

2. Na biurku nie powinny znajdować się dokumenty zawierające dane osobowe innych osób niż w danej chwili obsługiwanej.

3. Odchodząc od biurka nie wolno pozostawiać dokumentów bez nadzoru.

4. Po zakończeniu pracy akta spraw, dokumenty należy zabezpieczyć w szafach zamykanych na klucz.

5. Nie należy magazynować zbędnych wydruków.

6. Zbędne wydruki i inne dokumenty konwencjonalne (na nośnikach papierowych), zawierające dane osobowe, powinny być zniszczone w niszczarce dokumentów.

7. Za prawidłowe zniszczenie zbędnych dokumentów papierowych, zawierających dane osobowe, odpowiada osoba, która przetwarzała dane.

III. Polityka czystego druku.

Drukując dokumenty z użyciem ogólnodostępnej drukarki należy pamiętać, że drukowane informacje powinny być zabierane z drukarek niezwłocznie po wydrukowaniu. W przypadku nieudanej próby wydrukowania użytkownik powinien skontaktować się z osobą odpowiedzialną za eksploatację urządzenia, jeżeli zachodzi podejrzenie, iż wydruk zostanie wydrukowany bez nadzoru.

VI. Zabezpieczenie pomieszczeń i szaf.

1. Dostęp do pomieszczeń w których są przetwarzane dane osobowe mogą mieć tylko osoby upoważnione.

2. Pracownicy są odpowiedzialni za zabezpieczenie pomieszczeń za każdym razem kiedy opuszczają biuro.

3. Osoby nieupoważnione, mogą przebywać w pomieszczeniach, w których są przetwarzane dane osobowe tylko w obecności osób upoważnionych. Niedopuszczalne jest pozostawienie osób trzecich bez nadzoru.

4. Pomieszczenia, w których są przetwarzane dane osobowe, muszą być zamykane na klucz.

5. Dostęp do kluczy powinni posiadać tylko pracownicy wykonujący pracę w danym pomieszczeniu oraz ich bezpośredni przełożeni.

6. Dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy DPS oraz w przypadkach wykonywania pracy poza godzinami pracy DPS zgodnie z przepisami prawa pracy (w szczególności w przypadkach prowadzenia akcji ratunkowej, wykonywania pracy w godzinach nadliczbowych, odpracowywania wyjąć prywatnych).

7. Szafy w których przechowywane są dokumenty zawierające dane osobowe w formie papierowej muszą być zamykane na klucz, a klucz powinien być chowany w bezpieczne miejsce.

8. Klucze do tych szaf powinni posiadać tylko upoważnieni pracownicy.

9. Szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych, a następnie powinny być zamykane na klucz.

V. Zgłaszanie uszkodzeń.

Uszkodzenia zamków, szaf, drzwi, okien itp. należy zgłaszać do bezpośredniego przełożonego.

VI. Ochrona przeciwpożarowa.

1. Należy przestrzegać zasad przeciwpożarowych.

2. Nie wolno używać otwartego ognia na terenie DPS.
3. W przypadku rozpoczęcia pożaru (o ile to możliwe) należy podjąć próbę zgaszenia pożaru. Należy w tym celu stosować dostępne środki przeciwpożarowe.
4. W przypadku zagrożenia życia osób przebywających na terenie DPS należy niezwłocznie ogłosić ewakuację.
5. Konieczne jest powiadomienie Straży Pożarnej - Tel. 112.
VII. Ochrona przed atakiem bombowym.
1. Źródłem informacji o zagrożeniu bombowym może być list, rozmowa telefoniczna/mail.
2. Pozostawione paczki bez opieki lub rozmowa bezpośrednia.
3. Pracownikom DPS nie wolno lekceważyć informacji o zagrożeniu bombowym.
4. Obowiązkiem jest poinformowanie przełożonego i zgłoszenie tego faktu na Policję - Tel. 112.

§32
Środki techniczne

I. Zasady ogólne.
1. Dostęp do komputerów na których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy DPS.
2. System przetwarzający dane osobowe można wykorzystywać wyłącznie do celów służbowych.
3. Nie należy udostępniać osobom nieupoważnionym komputerów.
II. Zasady wykorzystania haseł.
1. Obowiązkiem każdego pracownika jest tworzenie haseł zgodnie z wymaganiami Ustawy o ochronie danych osobowych.
2. Hasło użytkownika musi składać się z co najmniej 8 znaków. Wskazane jest aby zawierało litery, cyfry i znaki specjalne.
3. Hasło musi być zmieniane przez użytkownika co najmniej raz na 30 dni.
4. Nie wolno udostępniać haseł osobom trzecim.
5. Nie wolno zapisywać haseł na papierze.
6. Nie wolno zapisywać haseł w przeglądarce.
7.Nie wolno wykorzystywać tych samych haseł w wielu miejscach.
III. Polityka czystego ekranu.
1. Ustawienia monitorów muszą zapewniać ograniczenie możliwości podglądania wyświetlanych danych osobom trzecim.
2. W przypadku konieczności czasowego opuszczenia stanowiska pracy, przyłączonego do sieci informatycznej lub służącego przetwarzaniu danych, wiążącego się ze utratą z pola widzenia swojego stanowiska, użytkownik powinien wykonać jedną z następujących czynności:
- wylogować się z programu lub sieci informatycznej lub zablokować stację roboczą odpowiednią kombinacją klawiszy, przy czym odblokowanie może nastąpić dopiero po podaniu hasła,
- aktywować wygaszacz ekranu w ten sposób, aby powrót do normalnej pracy był możliwy dopiero po podaniu hasła.
IV. Bezpieczeństwo sieci elektrycznej.
1. Zabrania się podłączania urządzeń elektrycznych do sieci komputerowej.
2. Ochronę przed awariami zasilania zapewniają zasilacze UPS.
3. System informatyczny służący do przetwarzania danych osobowych zabezpiecza się przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez wydzielenie oddzielnej sieci energetycznej do zasilania urządzeń systemu informatycznego.
V. Zgłaszanie uszkodzeń.
Uszkodzenia urządzeń elektrycznych należy zgłaszać do osoby odpowiedzialnej za bieżące naprawy i konserwacje.
Jeśli dokonuje się zniszczenia nośników komputerowych, sporządza się protokół ze zniszczenia, którego wzór stanowi **załącznik nr 19** do niniejszej Polityki.
VI. Zasady korzystania z sieci Internet.
1. Przeglądanie stron internetowych może być wykorzystywane wyłącznie w zakresie realizacji obowiązków służbowych.
2. Zabronione jest instalowanie aplikacji z sieci Internet.
3. Zabronione jest ściąganie z Internetu oprogramowania, plików muzycznych, zdjęć i filmów.

VII. Zasady korzystania z poczty elektronicznej.
1. Nie wolno wykorzystywać poczty elektronicznej do wysyłania danych osobowych bez odpowiednich zabezpieczeń kryptograficznych.
2. Nie wolno instalować programów załączonych do poczty.
3. Nie wolno korzystać z prywatnej poczty do celów służbowych.
4. Nie wolno korzystać z poczty służbowej do celów prywatnych.
VIII. Komunikatory internetowe.
Nie wolno używać komunikatora do wysyłania i odbierania plików.
IX. Zasady korzystania z nośników wymiennych.
1. Można wykorzystywać wyłącznie służbowe urządzenia wymienne.
2. Na nośnikach wymiennych nie wolno przenosić danych osobowych.
3. Zaleca się korzystanie z szyfrowanych nośników.
X. Zapewnienie legalności oprogramowania.
1. Instalować oprogramowanie może wyłącznie ASI.
2. Szczegółowe zasady zarządzania oprogramowaniem określają odrębne procedury.
XI. Ochrona antywirusowa.
1. Pracownik jest odpowiedzialny za działanie programu antywirusowego.
2. Brak oprogramowania, nieaktualne oprogramowanie i wykryte zagrożenia należy niezwłocznie zgłosić do ASI.
3. O poprawnym działaniu programu antywirusowego informuje odpowiednia ikona.
4. O wykryciu zagrożenia informuje odpowiedni komunikat.
XII. Wynoszenie sprzętu.
1. Niedozwolone jest wynoszenie sprzętu.
2. Laptopy można wynosić poza teren szkoły wyłącznie bez danych osobowych.
XIII. Zabezpieczenia sieci.
1. Sieć komputerowa powinna być zabezpieczona przed wszelkim dostępem z zewnątrz.
2. Zabezpieczenia stacji roboczych poprzez hasła.
XIV. Zabezpieczenia przy przenoszeniu danych.
1. W przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami należy dokonać tego z zachowaniem szczególnej ostrożności.
2. Nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie), aby nie zostały na nich dane osobowe.
3. W wypadku niemożliwości skasowania danych z nośnika (płyta CD-ROM), należy taką płytę zniszczyć fizycznie.
4. W przypadku wykorzystania do przenoszenia dysków, dane należy kasować z tych dysków.
5. Niezabezpieczonych danych osobowych nie wolno przesyłać drogą elektroniczną.
XVI. Monitorowanie.
1. Monitorowanie pomieszczeń szczegółowo opisane jest w Regulaminie funkcjonowania monitoringu DPS.
2. Monitorowanie ruchu sieciowego:
- ASI monitoruje ruch sieciowy w zakresie odwiedzanych stron internetowych i poczty elektronicznej.
- statystyki wykorzystania Internetu.
3. Monitorowanie działania pracy użytkowników:
- monitorowanie w zakresie zmian sprzętu komputerowego i oprogramowania.
- monitorowanie działania pracowników w zakresie przetwarzania danych osobowych oraz dostępu do plików sieciowych.

ROZDZIAŁ XIV

PROCEDURA UŻYTKOWANIA URZĄDZEŃ MOBILNYCH

§33

1. Wszystkie urządzenia mobilne (laptopy, notebooki, tablety) pozostające w zasobach DPS muszą być zinwentaryzowane.
2. Urządzenie, które nie spełnia wymogów bezpieczeństwa, nie powinno być używane do łączenia się z siecią Szkoły.

3. Konieczne jest zainstalowanie rozwiązania zabezpieczającego sieć urządzeń mobilnych. Zapewni to większą przejrzystość pracy i skuteczniejszą identyfikację zagrożeń na poziomie aplikacji, sieci roboczej i systemu operacyjnego.
4. Administrator Systemu Informatycznego dokonuje konfiguracji urządzenia, instaluje wszystkie potrzebne programy zapewniające ochronę antywirusową oraz nadaje użytkownikowi identyfikator i hasło według procedury opisanej w Instrukcji zarządzania systemem informatycznym.
5. Użytkownik nie może wyłączać mechanizmów zabezpieczeń wynikających z konfiguracji dokonywanej przez ASI.
6. Użytkownik nie może instalować żadnego oprogramowania na powierzonym urządzeniu mobilnym.
7. Zabrania się podłączania urządzeń mobilnych do sieci zewnętrznej, bez zgody ASI.
8. Pracownik potwierdza odbiór urządzenia mobilnego.
9. Każdy pracownik, któremu powierzono urządzenie mobilne ma obowiązek należytej pieczy nad powierzonym mu mieniem. Pracownik zobowiązany jest do przechowywania i zabezpieczenia mienia w sposób utrudniający jego uszkodzenie lub kradzież.
10. Dostęp do urządzenia musi być zabezpieczony hasłem.
11. W przypadku przechowywania na urządzeniach danych osobowych, co do których pracownik posiada upoważnienie do ich przetwarzania, jak również informacji objętych tajemnicą służbową, pracownik zobowiązany jest odpowiednio zabezpieczyć dostęp do tych danych.
12. Powierzone mienie należy użytkować zgodnie z jego przeznaczeniem i tylko do celów związanych z wykonaniem obowiązków pracowniczych.
13. Nie należy powierzonego urządzenia wykorzystywać do prywatnych celów oraz udostępniać go osobom nieupoważnionym.
14. Pracownik zobowiązany jest do należytej dbałości o funkcjonowanie urządzenia.
15. Osoba korzystająca z urządzenia mobilnego powinna zachować szczególną ostrożność podczas jego transportu, przechowywania i użytkowania przez co należy rozumieć podejmowanie rozsądnych działań minimalizujących ryzyko utraty lub zniszczenia powierzonego mienia.
16. W przypadku uszkodzenia urządzenia z winy pracownika, to on ponosi koszty naprawy urządzenia.
17. W przypadku kradzieży powierzonego urządzenia mobilnego pracownik jest zobowiązany do natychmiastowego zawiadomienia Administratora, zaś koszty związane z zakupem nowego urządzenia ponosi pracownik.
18. Pracownik jest zobowiązany zdać niezwłocznie powierzone urządzenie, w przypadku ustania stosunku pracy, cofnięcia przyznania pracownikowi urządzenia mobilnego.

ROZDZIAŁ XV

PRZEPISY KOŃCOWE

§34

Polityka Ochrony Danych jest dokumentem wewnętrznym Domu Pomocy Społecznej dla Kombatantów w Biłgoraju i jest objęta obowiązkiem zachowania poufności przez wszystkie osoby, którym zostanie ujawniona.

§35

Do spraw nieuregulowanych w Polityce Ochrony Danych stosuje się przepisy Rozporządzenia i Ustawy o ochronie danych osobowych.

§36

Niniejsza Polityka nie wyłącza stosowania innych instrukcji i procedur dotyczących zabezpieczenia danych.

§37

Integralną część Polityki Ochrony Danych stanowią następujące załączniki:
1. Wzór oświadczenia potwierdzającego znajomość wewnętrznych polityk Administratora.
2. Wzór zgody na wykorzystywanie wizerunku.
3. Wzór odwołania wyrażonej zgody.
4. Klauzula informacyjna dla kandydatów i mieszkańców Domu Pomocy Społecznej dla Kombatantów w Biłgoraju.
5. Klauzula informacyjna dla kandydatów do pracy w Domu Pomocy Społecznej dla Kombatantów w Biłgoraju.

6. Klauzula informacyjna dla osób zarejestrowanych przez monitoring wizyjny.
7. Wzór umowy powierzenia przetwarzania danych.
8. Wzór rejestru umów powierzenia przetwarzania danych.
9. Wzór rejestru czynności przetwarzania.
10. Wzór rejestru kategorii czynności przetwarzania.
11. Wzór wniosku o nadanie/aktualizacje upoważnienia do przetwarzania danych osobowych.
12. Wzór upoważnienia do przetwarzania danych osobowych.
13. Wzór rejestru upoważnień do przetwarzania danych osobowych.
14. Wzór odwołania upoważnienia do przetwarzania danych osobowych.
15. Wzór oświadczenia dla pracowników.
16. Wzór rejestru naruszeń.
17. Wzór raportu z naruszenia ochrony danych osobowych.
18. Wzór protokołu ze zniszczenia danych osobowych.
19. Wzór protokołu ze zniszczenia nośników komputerowych

Opracował Inspektor Ochrony Danych:

INSPEKTOR OCHRONY DANYCH
mgr Ewa Kwiecińska

.....

Zaakceptował Administrator Danych Osobowych -
Dyrektor Domu Pomocy Społecznej
dla Kombatantów w Biłgoraju:

DYREKTOR
mgr Agnieszka Kiesz

.....