ZESPÓŁ SZKÓŁ SPECJALNYCH
w Mazowieckim Centrum Rehabilitacji
05-510 Konstancin-Jeziorna, ul. Długa 40/42
Tel/fax: 22 754-74-48, 22 756-29-17
NIP 123-08-29-085, REGON 000195682

Załącznik do Zarządzenia Dyrektora
Zespołu Szkół Specjalnych w Mazowieckim Centrum Rehabilitacji
Nr 7/2023 z dnia 24 kwietnia 2023 r.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

w Zespole Szkół Specjalnych w Mazowieckim Centrum Rehabilitacji w Konstancinie - Jeziornie

Podstawa prawna:

1. *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)*
2. *Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000 z późn. zm.)*

§ 1.

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w Zespole Szkół Specjalnych w Mazowieckim Centrum Rehabilitacji w Konstancinie - Jeziornie, określa zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych. Polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa przetwarzanych danych. Polityka bezpieczeństwa dotyczy danych osobowych przetwarzanych w zbiorach manualnych oraz w systemach informatycznych.

§ 2.

Ilekroć w „Polityce Bezpieczeństwa" jest mowa o:

a) Zespole szkół – rozumie się przez to Zespół Szkół Specjalnych w Mazowieckim Centrum Rehabilitacji w Konstancinie – Jeziornie, ul. Długa 40/42,
b) Rozporządzeniu – rozumie się przez to Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
c) Ustawie – rozumie się przez to Ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych
d) danych osobowych – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
e) zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego,

czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,

f) przetwarzaniu danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,

g) systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych
w celu przetwarzania danych,

h) zabezpieczeniu danych w systemie informatycznym - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,

i) usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,

j) administratorze danych - rozumie się przez to Dyrektora Zespołu Szkół, decydującego o celach i środkach przetwarzania danych osobowych,

k) zgodzie osoby, której te dane dotyczą – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie – zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

§ 3.

1. Każdy z pracowników Zespołu Szkół ma prawo do ochrony dotyczących go danych osobowych.
2. Celem opracowania polityki bezpieczeństwa jest ochrona przed niepowołanym dostępem do:
   a) Systemu informatycznego oraz informacji udostępnianych z jego wykorzystaniem;
   b) Informacji zgromadzonych, przetwarzanych w formie tradycyjnej.
3. Dane osobowe w Zespole szkół są gromadzone, przechowywane, edytowane, archiwizowane w kartotekach, skorowidzach, księgach, wykazach, zestawieniach oraz w innych zestawach i zbiorach ewidencyjnych poszczególnych komórek organizacyjnych na dokumentach papierowych, jak również w systemach informatycznych na elektronicznych nośnikach informacji.
4. Powyższy dokument wprowadza regulacje w zakresie zasad organizacji procesu przetwarzania i odnosi się swoją treścią do informacji:
   a) w formie papierowej – przetwarzanej w ramach systemu tradycyjnego
   b) w formie elektronicznej – przetwarzanej w ramach systemu informatycznego
5. Z zapisami polityki bezpieczeństwa danych osobowych obowiązkowo są zapoznawani wszyscy użytkownicy systemów tradycyjnych i informatycznych.

§ 4.

Bezpośredni nadzór nad przetwarzaniem danych osobowych sprawuje Dyrektor Zespołu Szkół, jako Administrator Danych Osobowych.

§ 5.

1. Administrator Danych wyraża pełne zaangażowanie dla zapewnienia bezpieczeństwa przetwarzanych danych osobowych oraz wsparcie dla przedsięwzięć technicznych i organizacyjnych związanych z ochroną danych osobowych.
2. Polityka dotyczy wszystkich danych osobowych przetwarzanych w podmiocie, niezależnie od formy ich przetwarzania (zbiory ewidencyjne, systemy informatyczne) oraz od tego czy

dane są lub mogą być przetwarzane w zbiorach danych.

3. Polityka ma zastosowanie wobec wszystkich komórek organizacyjnych w tym oddziałów, samodzielnych stanowisk pracy i wszystkich procesów przebiegających w ramach przetwarzania danych osobowych.
4. Celem Polityki jest przetwarzanie zgodnie z przepisami danych osobowych przetwarzanych w podmiocie oraz ich ochrona przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed uszkodzeniem, zniszczeniem lub nieupoważnioną zmianą.
5. Ze względu na nieustannie zmieniające się zagrożenia przetwarzania danych o osobowych i zmiany prawa niniejsza polityka może być dokumentem dynamicznie zmieniającym się w czasie. Uaktualnienia procedur ochrony, oprogramowania i innych parametrów stosowanych przy przetwarzaniu danych osobowych znajdują na bieżąco odzwierciedlenie funkcjonalne w niniejszej Polityce.
6. Cele Polityki realizowane są poprzez zapewnienie danym osobowym następujących cech:
   a) poufności - właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom;
   b) integralności - właściwości zapewniającej, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   c) rozliczalności - właściwości zapewniającej, że działania podmiotu operującego na danych osobowych mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
   d) ciągłości - zdolności do niezakłóconego ich przetwarzania, bez przerw uniemożliwiających ich udostępnianie osobom upoważnionym.
7. Dla skutecznej realizacji Polityki Administrator Danych zapewnia:
   a) odpowiednie do zagrożeń i kategorii danych objętych ochroną, środki techniczne i rozwiązania organizacyjne;
   b) szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony;
   c) kontrolę i nadzór nad przetwarzaniem danych osobowych;
   d) monitorowanie zastosowanych środków ochrony;
   e) ciągłe śledzenie zmieniających się zagrożeń wewnętrznych i zewnętrznych, także uwzględnianie zmieniającego się prawa;
   f) kontrolę i nadzór nad przetwarzaniem danych osobowych przez podmioty trzecie, którym dane zostały udostępnione lub powierzone.
8. Monitorowanie przez Administratora Danych zastosowanych środków ochrony obejmuje m.in. działania użytkowników, naruszanie zasad dostępu do danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.

§ 6.

Dane osobowe przetwarzane są w budynku Mazowieckiego Centrum Rehabilitacji w Konstancinie – Jeziornie, ul. Długa 40/42 w części zajmowanej przez Zespół Szkół, na podstawie umowy użyczenia, w poszczególnych pomieszczeniach wykazanych **w załączniku nr 1.**

§ 7.

1. Dane osobowe są gromadzone, przechowywane i przetwarzane w kartotekach, skorowidzach, księgach, wykazach oraz w innych zbiorach ewidencyjnych poszczególnych komórek organizacyjnych Jednostki w postaci papierowej i elektronicznej.
2. Do przetwarzania zbiorów danych osobowych w systemie informatycznym Jednostki, stosowane są pakiety biurowe lub specjalistyczne programy.

3. Programy służące do przetwarzania danych osobowych w Zespole szkół:
   a) Aplikacja chmurowa FINANSE VULCAN, PŁACE VULCAN, KADRY VULCAN, ARKUSZ ORGANIZACYJNY –,
   b) Dziennik elektroniczny UONET+
   c) Płatnik,
   d) SIO,

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych określa **załącznik nr 2** do „Polityki Bezpieczeństwa".

§ 8.

W podmiocie dba się o to, aby dane osobowe w formie papierowej były niedostępne dla osób nieupoważnionych. Dokumenty znajdują się w pomieszczeniu zamykanym na klucz, do którego dostęp mają tylko osoby posiadające aktualne upoważnienie do przetwarzania danych osobowych.

§ 9.

1. Do przetwarzania danych dopuszczone są wyłącznie osoby posiadające upoważnienie nadane przez Administratora Danych.
2. Administrator Danych stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem zapisów Rozporządzenia oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Administrator Danych nadaje uprawnienia pracownikom, którzy przetwarzają dane poprzez podpisanie upoważnienia, które stanowi **załącznik nr 3** do „Polityki Bezpieczeństwa".
3. Ewidencja osób przetwarzających dane posiadających upoważnienie stanowi **załącznik nr 4** do „Polityki Bezpieczeństwa".

§ 10.

1. Obieg dokumentów zawierających dane osobowe, pomiędzy komórkami organizacyjnymi Jednostki, winien odbywać się w sposób zapewniający pełną ochronę przed ujawnieniem zawartych w tych dokumentach danych (informacji).
2. Administrator Danych zapewnia środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.
3. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych.
4. Środki ochrony, zastosowane przez ADO dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych, obejmują:
   a) środki ochrony fizycznej;
   b) środki techniczne;
   c) środki organizacyjne
5. Zastosowane środki ochrony fizycznej pomieszczeń:
   a) drzwi do pomieszczeń zamykane na klucz,
   b) zasada czystego biurka – należy usuwać z niezabezpieczonego miejsca pracy dane osobowe w wersji papierowej oraz na elektronicznych nośnikach danych osobowych jak również stosować wygaszacze ekranu w przypadku korzystania z urządzeń wyświetlających dane osobowe;
   c) Zasada właściwego ustawienia monitora komputerowego – należy ustawić tak monitor

swojego komputera, aby danych na nim widoczne nie mogła przeczytać osoba postronna;

d) Zasada przechowywania dokumentów w bezpiecznym miejscu – należy dbać o to, aby dokumenty przechowywane były w zamkniętych szafach lub szufladach.
e) Zasada bezpiecznego pomieszczenia – nie należy pozostawiać bez opieki w pokoju osób trzecich.

6. Zastosowane środki techniczne obejmują zastosowanie programu antywirusowego oraz potrzymanie zasilania komputerów przez UPS.
7. Zastosowane środki organizacyjne obejmują utworzenie Instrukcji zarządzania systemem informatycznym.
8. Za niedopełnienie obowiązków wynikających z niniejszego dokumentu pracownik ponosi odpowiedzialność na podstawie Kodeksu pracy oraz Rozporządzenia o ochronie danych osobowych. W odniesieniu do innych osób upoważnionych do przetwarzania danych osobowych, w sytuacji naruszeń obowiązków wynikających z niniejszego dokumentu ponieść mogą odpowiedzialność odszkodowawczą. Wszystkie osoby upoważnione do przetwarzania danych osobowych mogę ponieść odpowiedzialność karną w sytuacji naruszenia zasad określonych w niniejszym dokumencie.

§ 11.

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

§ 12.

Administrator Danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych osobowych w podmiocie. Podmiot ten może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

§ 13.

Sposób zabezpieczenia oraz przetwarzania danych w systemie informatycznym reguluje Instrukcja Zarządzania Systemem Informatycznym - **załącznik nr 5.**

§ 14.

Zapewnienie właściwego korzystania z poczty elektronicznej stanowi obecnie jeden z priorytetów w zakresie odpowiedniej ochrony danych osobowych. Zasady korzystania ze służbowej poczty elektronicznej określa Regulamin poczty elektronicznej stanowiący **załącznik nr 6.**

§ 15.

Administrator Danych lub osoba przez niego upoważniona wdraża wszystkie niezbędne dokumenty wynikające z zapisów Rozporządzenia oraz innych przepisów mających zastosowania przy przetwarzaniu danych osobowych.

§ 16.

W sprawach nieuregulowanych w niniejszej „Polityce Bezpieczeństwa" mają zastosowanie odpowiednie przepisy Rozporządzenia oraz Ustawy.

DYREKTOR
ZESPOŁU SZKÓŁ
A. Malarczyk
mgr Agnieszka Malarczyk

Wykaz załączników:

Załącznik nr 1 – Wykaz pomieszczeń, w których przetwarzane są dane osobowe
Załącznik nr 2 – zbiory danych osobowych
Załącznik nr 3 – wzór upoważnienia do przetwarzania danych osobowych
Załącznik nr 4 – ewidencja osób upoważnionych do przetwarzania danych osobowych
Załącznik nr 5 – Instrukcja Zarządzania Systemem Informatycznym
Załącznik nr 6 – Regulamin korzystania z poczty elektronicznej

ZESPÓŁ SZKÓŁ SPECJALNYCH
w Mazowieckim Centrum Rehabilitacji
05-510 Konstancin-Jeziorna, ul. Długa 40/42
Tel/fax: 22 754-74-48, 22 756 29-17
NIP 123-08-29-085, REGON 000193682

Załącznik nr 1 do Polityki Bezpieczeństwa Danych Osobowych

Wykaz pomieszczeń, w których przetwarzane są dane osobowe

adres	Pomieszczenie	Zastosowane zabezpieczenie
Zespół Szkół Specjalnych w Mazowieckim Centrum Rehabilitacji ul. Długa 40/42, 05-510 Konstancin - Jeziorna	Gabinet dyrektora	Zamknięcie na klucz – kluczami dysponuje dyrektor
	Kancelaria szkoły	Zamknięcie na klucz – kluczami dysponuje dyrektor, sekretarz szkoły,
	Sekretariat uczniowski	Zamknięcie na klucz – kluczami dysponuje sam. referent
	Gabinet pedagoga i kierownika zespołu pozalekcyjnego	Zamknięcie na klucz – kluczami dysponuje pedagog i kierownik zespołu pozalekcyjnego
	Księgowość szkoły	Zamknięcie na klucz – kluczami dysponuje główny księgowy i st. specjalista
	Składnica akt	Zamknięcie na klucz – kluczami dysponuje sekretarz szkoły
	Pokój nauczycielski	Zamknięcie na klucz – kluczami dysponuje dyrektor, nauczyciele Zespołu Szkół
	biblioteka	Zamknięcie na klucz – kluczami dysponuje dyrektor i bibliotekarze
	Sale lekcyjne 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 ,13	Zamknięcie na klucz – klucze znajdują się w pokoju nauczycielskim i w sekretariacie szkoły.

ZESPÓŁ SZKÓŁ SPECJALNYCH
w Mazowieckim Centrum Rehabilitacji
05-510 Konstancin-Jeziorna, ul. Długa 40/42
Tel/fax: 22 754-74-48, 22 756 29-17
NIP 123-08-29-085, REGON 000195682

Załącznik nr 2 **do Polityki Bezpieczeństwa Danych Osobowych**

ZBIORY DANYCH DOSOBOWYCH

Lp.	**Nazwa zbioru danych** *(np. dane klientów, pracowników itd.)*	**Programy zastosowane do przetwarzania danych** *(np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)*	**Struktura zbioru**
1.	**Kartoteki osobowe pracowników, akta osobowe**	Forma papierowa Program komputerowy SIO Aplikacja chmurowa FINANSE VULCAN, PŁACE VULCAN, KADRY VULCAN	Imię i nazwisko, adres zamieszkania i zameldowania, data i miejsce urodzenia, nr NIP, PESEL. Nr i seria dowodu osobistego, nr telefonu, posiadane wykształcenie, stan rodzinny, dane dotyczące przebiegu zatrudnienia, wysokości wynagrodzenia, dane dotyczące przebiegu zatrudnienia u poprzednich pracodawców, oświadczenia o karalności, zaświadczenia o stanie zdrowia
2.	**Ewidencja zwolnień lekarskich**	Forma papierowa Aplikacja chmurowa FINANSE VULCAN, PŁACE VULCAN, KADRY VULCAN Program komputerowy SIO ZUS PUE	Imię, nazwisko, Pesel, data urodzenia, adres zamieszkania, okres niezdolności do pracy
3.	**Ewidencja legitymacji pracowniczych**	Forma papierowa	Imię i nazwisko, stanowisko, wizerunek (zdjęcie)
4.	**Rejestr delegacji służbowych**	Forma papierowa	Imię i nazwisko, stanowisko
5.	**Ewidencja osób zatrudnionych, upoważnionych do przetwarzania danych osobowych**	Forma papierowa	Imię i nazwisko, zakres upoważnienia, okres upoważnienia
6.	**Ewidencja nieobecności w pracy**	Forma papierowa Aplikacja chmurowa FINANSE VULCAN, PŁACE VULCAN, KADRY VULCAN Program komputerowy SIO	Imię i nazwisko, stanowisko, data nieobecności, rodzaj nieobecności

Lp.	**Nazwa zbioru danych** *(np. dane klientów, pracowników itd.)*	**Programy zastosowane do przetwarzania danych** *(np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)*	**Struktura zbioru**
7.	**Zgłoszenia do Ubezpieczenia Społecznego pracowników**	Forma papierowa Program komputerowy „Płatnik”	Imię i nazwisko, nazwisko rodowe, drugie imię, data urodzenia, miejsce zamieszkania i zameldowania, informacja o stopniu niepełnosprawności, prawo do emerytury/renty
8.	**Zgłoszenia do Ubezpieczenia Społecznego członków rodzin**	Forma papierowa Program komputerowy „Płatnik”	Imię i nazwisko, data urodzenia, imię i nazwisko członka rodziny, data urodzenia, adres zamieszkania, informacja o niepełnosprawności
9.	**Pracownicze plany kapitałowe**	Forma papierowa Aplikacja KADRY VULCAN, PŁACE VULCAN	Imię i nazwisko, data urodzenia, PESEL, nr dowodu osobistego
10.	**Ewidencja osób korzystających z Zakładowego Funduszu Świadczeń Socjalnych**	Forma papierowa Forma elektroniczna Excel Aplikacja chmurowa FINANSE VULCAN, PŁACE VULCAN	Imię i nazwisko, adres zamieszkania, numer telefonu, informacja o wysokości dochodu, numer i wysokość przyznanej emerytury, numer konta bankowego
11.	**Listy płac pracowników**	Forma papierowa Aplikacja chmurowa FINANSE VULCAN, PŁACE VULCAN, KADRY VULCAN	Imię i nazwisko, wysokość wynagrodzenia, numer konta bankowego
12.	**Karty zasiłkowe**	Forma papierowa Aplikacja chmurowa PŁACE VULCAN	Imię i nazwisko, Pesel, data i miejsce urodzenia, adres zamieszkania, stanowisko, okresy niezdolności do pracy, wysokość wynagrodzenia
13.	**Karty zarobkowe**	Forma papierowa Aplikacja chmurowa PŁACE VULCAN	Imię i nazwisko, Pesel, data i miejsce urodzenia, stanowisko, wysokość wynagrodzenia, warunki zatrudnienia
14.	**Informacje o zarobkach PIT**	Forma papierowa Aplikacja chmurowa PŁACE VULCAN	Imię i nazwisko, Pesel, data urodzenia, adres zamieszkania, wysokość wynagrodzenia

Lp.	**Nazwa zbioru danych** *(np. dane klientów, pracowników itd.)*	**Programy zastosowane do przetwarzania danych** *(np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)*	**Struktura zbioru**
15.	**Zaświadczenia o wysokości wynagrodzenia**	Forma papierowa Aplikacja chmurowa PŁACE VULCAN	Imię i nazwisko, Pesel, data urodzenia, wysokość wynagrodzenia, warunki pracy
16.	**Rejestr wypadków pracowników**	Forma papierowa	Imię i nazwisko, data i miejsce urodzenia, adres zamieszkania, stanowisko, stan zdrowia
17.	**Umowy cywilno – prawne**	Forma papierowa Aplikacja chmurowa FINANSE VULCAN, PŁACE VULCAN, KADRY VULCAN	Imię i nazwisko, adres zamieszkania i zameldowania, Pesel, Nip, numer konta bankowego, wysokość wynagrodzenia
18.	**Badania lekarskie**	Forma papierowa Aplikacja chmurowa KADRY VULCAN	Imię i nazwisko, Pesel, data urodzenia, miejsce zamieszkania, informacja o stanie zdrowia
19.	**Szkolenia z zakresu BHP pracowników**	Forma papierowa Aplikacja chmurowa KADRY VULCAN	Imię i nazwisko, data i miejsce urodzenia
20.	**Ubezpieczenia grupowe pracowników**	Forma papierowa Forma elektroniczna System „eRU" PZU	Imię i nazwisko, Pesel, data i miejsce urodzenia, adres zamieszkania, stan zdrowia
21.	**Kandydaci do pracy**	Forma papierowa	Imię i nazwisko, imiona rodziców, data urodzenia, obywatelstwo, adres zamieszkania, wykształcenie, przebieg zatrudnienia.
22.	**Praktyki studenckie**	Forma papierowa	Imię i nazwisko, wykształcenie
23.	**Wolontariat**	Forma papierowa	Imię i nazwisko, data urodzenia
24.	**Awans zawodowy nauczycieli**	Forma papierowa Program komputerowy SIO	Imię i nazwisko, data i miejsce urodzenia, stanowisko, wykształcenie
25.	**Księga zastępstw nauczycieli**	Forma papierowa Dziennik elektroniczny UONET+	Imię i nazwisko, okres nieobecności w pracy

Lp.	**Nazwa zbioru danych** *(np. dane klientów, pracowników itd.)*	**Programy zastosowane do przetwarzania danych** *(np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)*	**Struktura zbioru**
26.	**Protokoły Rady pedagogicznej**	Forma papierowa Forma elektroniczna	Imię i nazwisko, zajmowane stanowisko
27.	**Ewidencja osób korzystających z księgozbioru bibliotecznego**	Forma papierowa MOLNET+	Imię i nazwisko, zajmowane stanowisko
28.	**Księga uczniów**	Forma papierowa Dziennik elektroniczny UONET+ Program komputerowy SIO	Nazwisko i imię ucznia, PESEL, data i miejsce urodzenia, Imiona i nazwiska rodziców (opiekunów prawnych), adresy ich zamieszkania.
29.	**Dzienniki lekcyjne i pozalekcyjne**	Forma papierowa Dziennik elektroniczny UONET+	Nazwisko i imię ucznia, PESEL, data i miejsce urodzenia, Imiona i nazwiska rodziców (opiekunów prawnych), adresy ich zamieszkania, numery telefonów
30.	**Arkusze ocen uczniów**	Forma papierowa Dziennik elektroniczny UONET+	Nazwisko i imię ucznia, PESEL, data i miejsce urodzenia, Imiona i nazwiska rodziców (opiekunów prawnych), adresy ich zamieszkania, data przyjęcia do szkoły, nr księgi uczniów, wyniki w nauce.
31.	**Protokoły egzaminów klasyfikacyjnych, poprawkowych, egzaminy kompetencji**	Forma papierowa	Imię i nazwisko ucznia, data i miejsce urodzenia, adres zamieszkania, wyniki z egzaminu
32.	**Ewidencja legitymacji szkolnych**	Forma papierowa	Imię i nazwisko ucznia, numer i data wydania legitymacji
33.	**Ewidencja świadectw szkolnych**	Forma papierowa	Imię i nazwisko, numer i data wydania świadectwa
34.	**Rejestr wypadków uczniów**	Forma papierowa	Imię i nazwisko, data i miejsce urodzenia, data, rodzaj, miejsce wypadku, okoliczności wypadku, rodzaj uszkodzeń
35.	**Składnica akt**	Forma papierowa	Akta osobowe pracowników, listy płac, księgi uczniów, arkusze ocen, dzienniki lekcyjne

Lp.	**Nazwa zbioru danych** *(np. dane klientów, pracowników itd.)*	**Programy zastosowane do przetwarzania danych** *(np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)*	**Struktura zbioru**
36.	**Organizacja roku szkolnego**	Forma papierowa Aplikacja ARKUSZ ORGANIZACYJNY	Imię i nazwisko, pesel, wykształcenie

ZESPÓŁ SZKÓŁ SPECJALNYCH
w Mazowieckim Centrum Rehabilitacji
05-510 Konstancin-Jeziorna, ul. Długa 40/42
Tel/fax: 22 754-74-48, 22 756 29-17
NIP 123-08-29-085, REGON 000193682

Załącznik nr 3 **do Polityki Bezpieczeństwa Danych Osobowych**

Konstancin - Jeziorna dn. ..... r.

UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. UE L 119, s. 1) – dalej **RODO –** nadaję upoważnienie Pani/Panu:

.....
(imię i nazwisko)

.....
(stanowisko)

do przetwarzania danych osobowych w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku.

Upoważnienie obejmuje uprawnienie do przetwarzania danych w: .....
(podać system informatyczny lub inne miejsce przetwarzania danych)

w zakresie: .....
(podać zakres upoważnienia przetwarzania danych)

Identyfikator w systemie informatycznym : .....

Jednocześnie zobowiązuję Panią/Pana do przetwarzania danych osobowych, zgodnie z udzielonym upoważnieniem oraz z przepisami RODO, Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000), innych aktami prawnymi a także z Polityką ochrony danych osobowych.

Okres ważności

od: .....

do: odwołania lub wygaśnięcia, w związku z rozwiązaniem stosunku pracy

.....
podpis osoby uprawnionej do nadania upoważnienia

Data wygaśnięcia upoważnienia* .....
(data rozwiązania stosunku pracy)

Odwołano, dnia .....

.....
podpis osoby uprawnionej do odwołania upoważnienia

ZESPÓŁ SZKÓŁ SPECJALNYCH
w Mazowieckim Centrum Rehabilitacji
05-510 Konstancin-Jeziorna, ul. Długa 40/42
Tel/fax: 22 754-74-48, 22 756 39-17
NIP 123-08-29-085, REGON 000195682

Załącznik nr 4 **do Polityki Bezpieczeństwa Danych Osobowych**

EWIDENCJA UPOWAŻNIEŃ OSÓB PRZETWARZAJACYCH DANE OSOBOWE

Lp.	**Imię i nazwisko**	**Stanowisko służbowe**	**Data nadania upoważnienia**	**Data ustania upoważnienia**	**Identyfikator** *(Jeżeli dane są przetwarzane w systemie informatycznym)*

ZESPÓŁ SZKÓŁ SPECJALNYCH
w Mazowieckim Centrum Rehabilitacji
05-510 Konstancin-Jeziorna, ul. Długa 40/42
Tel/fax: 22 754-74-48, 22 756 39 17
NIP 123-08-29-085, REGON 000195682

Załącznik nr 5 **do Polityki Bezpieczeństwa Danych Osobowych**

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Administrator Danych – dyrektor Zespołu Szkół Specjalnych w Mazowieckim Centrum Rehabilitacji w Konstancinie – Jeziornie, ul. Długa 40/42 05-510 Konstancin – Jeziorna, w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych, wdraża dokument o nazwie „Instrukcja zarządzania systemem informatycznym" zwany dalej „instrukcją", stanowiący załącznik do Polityki Bezpieczeństwa

Ilekroć w „instrukcji" jest mowa o:

1. podmiocie — Zespół Szkół Specjalnych w Mazowieckim Centrum Rehabilitacji w Konstancinie - Jeziornie;
2. ustawie — rozumie się przez to ustawę *z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000 z późn. zm.* , zwaną dalej „ustawą";
3. identyfikatorze użytkownika — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
4. haśle — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
5. sieci telekomunikacyjnej — rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.)
6. sieci publicznej — rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne;
7. teletransmisji – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej
8. rozliczalności — rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
9. integralności danych — rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
10. raporcie — rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
11. poufności danych — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
12. uwierzytelnianiu — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

§ 1.

Za przestrzeganie w Zespole Szkół Specjalnych w Mazowieckim Centrum Rehabilitacji w Konstancinie - Jeziornie zapisów „instrukcji" odpowiedzialny jest Dyrektor Szkoły, jako Administrator Danych Osobowych.

§ 2.

W związku z tym, że w Zespole Szkół Specjalnych w Mazowieckim Centrum Rehabilitacji w Konstancinie - Jeziornie przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną oraz uwzględniając kategorie przetwarzanych danych i zagrożenia wprowadza się poziom bezpieczeństwa przetwarzania

danych osobowych w systemie informatycznym na poziomie wysokim, a w związku z tym wprowadza się poniższe postanowienia:

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

II. W systemie informatycznym służącym do przetwarzania danych osobowych, przetwarzać dane mogą wyłącznie osoby posiadające aktualne upoważnienie nadane przez Administratora Danych Osobowych.

1. Użytkownik przetwarzający dane po otrzymaniu upoważnienia oraz loginu i hasła jest zobowiązany niezwłocznie dokonać zmiany hasła oraz zachować je w tajemnicy. Użytkownik jest zobowiązany do zmiany hasła nie rzadziej niż co 30 dni. Hasło nadane przez użytkownika musi składać się z co najmniej z 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
2. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:
   a) w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator,
   b) dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.
3. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
4. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Kopie wszystkich danych osobowych muszą być tworzone nie rzadziej niż raz na miesiąc.
5. Kopie zapasowe:
   a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem w pomieszczeniu zamkniętym (sekretariat szkoły, księgowość, gabinet dyrektora, archiwum),
   b) usuwa się niezwłocznie po ustaniu ich użyteczności.

III. System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:

1. Działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego poprzez:
   a) zainstalowanie programu antywirusowego o nazwie ESET Endpoint Antivirus
   b) zainstalowanie firewall (zapora sieciowa)
2. utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez zastosowanie zasilacza awaryjnego UPS.

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

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

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

2. przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
3. naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

§ 3.

1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — system ten zapewnia odnotowanie:
   a) daty pierwszego wprowadzenia danych do systemu;
   b) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;
   c) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą.
2. Odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.
3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.
4. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust. 1 pkt 4, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

§ 4.

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

§ 5.

Wyznaczony przez Administratora Ochrony Danych pracownik ma obowiązek dokonywać przeglądów technicznych sprzętu informatycznego w podmiocie oraz dbać o ich dobry stan techniczny. Zaleca się dokonywanie przeglądów okresowych co 60 dni oraz przeglądów generalnych raz na rok. W przypadku stwierdzenia usterek technicznych wyznaczony pracownik ma obowiązek niezwłocznie powiadomić o tym fakcie Administratora Danych.

§ 6.

Każdy użytkownik systemu informatycznego, w przypadku stwierdzenia uchybień dotyczących przetwarzania danych w podmiocie, powinien o tym fakcie niezwłocznie powiadomić Administratora Danych. Administrator Danych wprowadza zabezpieczenia i procedury, które w przyszłości wyeliminują takie zdarzenia.

§ 7.

W sprawach nieuregulowanych w niniejszej Instrukcji mają zastosowanie przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

§ 8.

Instrukcja niniejsza wchodzi w życie z dniem zatwierdzenia jej przez Dyrektora Zespołu Szkół Specjalnych w Mazowieckim Centrum Rehabilitacji w Konstancinie – Jeziornie - administratora danych osobowych.

DYREKTOR
ZESPOŁU SZKÓŁ
A. Malarczyk
mgr Agnieszka Malarczyk

ZESPÓŁ SZKÓŁ SPECJALNYCH
w Mazowieckim Centrum Rehabilitacji
05-510 Konstancin-Jeziorna, ul. Długa 40/42
Tel/fax: 22 754-74-48, 22 756 39-17
NIP 123-00-29-085, REGON 000195682

Załącznik nr 6 **do Polityki Bezpieczeństwa Danych Osobowych**

REGULAMIN KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

Regulamin określa zasady używania służbowej poczty elektronicznej (e-mail). Celem dokumentu jest ustanowienie obowiązujących wymagań w zakresie dozwolonego i poprawnego korzystania z poczty e-mail, a także zminimalizowanie ryzyka dla ochrony danych przekazywanych drogą elektroniczną. Zasady określone w regulaminie obowiązują wszystkich użytkowników poczty służbowej.

§ 1.

1. Korzystanie ze służbowej poczty elektronicznej jest jednym ze sposobów realizowania obowiązków powierzonych użytkownikowi poczty i powinno być realizowane tylko i wyłącznie w celach służbowych, związanych z realizowaniem tych zadań.
2. Użytkownicy poczty elektronicznej są odpowiedzialni za korzystanie z poczty w taki sposób, aby minimalizować ryzyka naruszenia bezpieczeństwa informacji.
3. Użytkownik jest uprawniony do korzystania tylko i wyłącznie z przydzielonego lub przydzielonych mu adresów e-mail. Zakazane jest korzystanie z adresu e-mail innego użytkownika, a także logowanie się do skrzynki pocztowej innego użytkownika.
4. Wszystkie nieprawidłowości w działaniu poczty elektronicznej, a także wątpliwości związane ze sposobem korzystania z poczty elektronicznej, w tym związane z jej bezpieczeństwem, należy niezwłocznie konsultować z wyznaczonym pracownikiem.
5. Dane osobowe przekazywane drogą elektroniczną powinny być przekazywane w załączniku zabezpieczonym hasłem, zgodnie z opisaną w regulaminie procedurą.

§ 2.

1. Przed wysłaniem pierwszej wiadomości użytkownik jest zobligowany do skonfigurowania zasad wysyłania wiadomości, w tym nazwy użytkownika i podpisu pod wiadomością zgodnie z obowiązującymi standardami
2. Ustawienie przekazywania wiadomości na inny adres e-mail, tzn. innego pracownika, wymaga uprzedniej zgody bezpośredniego przełożonego. Zgoda powinna być udokumentowana (na piśmie lub elektronicznie, jako wiadomość e-mail).
3. Jeżeli kilku pracowników korzysta z ogólnego adresu e-mail, np. kontakt@, to każda wiadomość powinna zostać podpisana imieniem i nazwiskiem osoby, która udziela odpowiedzi.
4. Każda wiadomość powinna być wysyłana z zachowaniem należytej staranności w zakresie sprawdzenia poprawności treści, załączników, a także adresatów wiadomości.
5. Zalecane jest okresowe czyszczenie skrzynki pocztowej poprzez usuwanie starych wiadomości, które nie będą już potrzebne oraz przechowywanie wiadomości w strukturze folderów.

§ 3.

Przesyłanie danych osobowych

1. Użytkownik może zastosować szyfrowanie wiadomości wewnętrznych w przypadku przesyłania treści objętych szczególną ochroną, Zasady szyfrowania korespondencji zewnętrznej powinny być uzgadniane z poszczególnymi odbiorcami.

2. Dane osobowe (nawet imiona, nazwiska, czy adresy e-mail) powinny być przekazywane w zabezpieczonym hasłem załączniku do wiadomości e-mail.
3. Użytkownik może także zabezpieczyć plik lub pliki poprzez kompresję z zabezpieczeniem archiwum wynikowego hasłem.
4. Hasło powinno być odpowiednio skomplikowane i niesłownikowe.
5. Hasło powinno zostać przekazane odbiorcy inną drogą korespondencji.
6. Dopuszczalne jest uzgodnienie stałego hasła na korespondencję z jednym odbiorcą.
7. Dopuszczalne jest zastosowanie jako hasła informacji, która jest znana tylko odbiorcy, której nie trzeba będzie przekazywać mu odrębną drogą komunikacji, np. znany mu numer ewidencyjny.

§ 4.

1. Przesłanie wiadomości do konkretnej osoby powinno wynikać z celu komunikacji.
2. Wskazanie adresata w polu DW (Do Wiadomości) powoduje jawne przesłanie do niego kopii wiadomości.
3. Przekazywanie wiadomości w sposób ujawniający dane adresatów (Do / Do wiadomości) jest dozwolone tylko wówczas, gdy adresy e-mail odbiorców są adresami służbowymi, a adresaci znają wzajemnie swoje adresy e-mail i są zaangażowani w sprawę, której dotyczy wysyłana wiadomość.
4. Pole UDW (Ukryte Do Wiadomości) służy do wysyłania wiadomości z dodatkowym ukryciem przed adresatem faktu istnienia (i tożsamości) trzeciej strony wskazanej w tym polu.
5. W przypadku wysyłania wiadomości do kilku odbiorców, którzy nie znają się wzajemnie i/lub korzystają z prywatnych adresów e-mail, należy ich adresy wskazać w polu Ukrytej kopii. W takim wypadku wiadomość należy zaadresować do siebie, wskazując swój adres e-mail w polu Do.

§ 5.

1. Zabrania się używania poczty elektronicznej:
   a) do tworzenia, wysyłania lub przechowywania wiadomości e-mail lub załączników, które mogą być uznane za nielegalne lub są powszechnie uznawane za obraźliwe, nieetyczne, nielegalne lub w inny sposób niestosowne, w tym: obraźliwe komentarze dotyczące rasy, płci, koloru skóry, niepełnosprawności, wieku, orientacji seksualnej, pornografii, terroryzmu, przekonań i praktyk religijnych, przekonań politycznych, narodowości, odnośniki do lub ewidentnie obraźliwych stron WWW i podobnych materiałów; żarty, wiadomości - łańcuszki, ostrzeżenia o wirusach, prośby o pomoc charytatywną, wirusy i inne oprogramowanie złośliwe;
   b) do korespondencji prywatnej lub pracy charytatywnej niepowiązanej z działalnością pracodawcy;
   c) do wysyłania wiadomości e-mail z cudzego konta lub w cudzym imieniu (włączając w to użycie zmienionego pola From:/Od:);
   d) do każdego innego niezgodnego z prawem, nieetycznego celu;
2. Zabrania się korzystania w celach służbowych z innej, w tym prywatnej poczty e-mail.

DYREKTOR
ZESPOŁU SZKÓŁ
A. Malarczyk
mgr Agnieszka Malarczyk