

POLITYKA
OCHRONY
DANYCH OSOBOWYCH
przetwarzanych
w Zespole Szkół Specjalnych
w Ścinawce Dolnej

Ścinawka Dolna, 03 września 2018

SPIS TREŚCI	str.
--------------------------	-------------

Część I - POLITYKA OCHRONY DANYCH OSOBOWYCH	3
• Upoważnienie do przetwarzania danych osobowych (załącznik nr 1)	12
• Odwołanie upoważnienia do przetwarzania danych osobowych (załącznik nr 2)	13
• Ewidencja osób upoważnionych do przetwarzania danych osobowych (załącznik nr 3)	14
• Oświadczenie o zachowaniu poufności (załącznik nr 4).....	15
• Oświadczenie o zapoznaniu się z przepisami (załącznik nr 5).....	16
• Zgoda na przetwarzanie danych osobowych pracownika (załącznik nr 6).....	17
• Zgoda na przetwarzanie danych osobowych rodzica/opiekuna (załącznik nr 7).....	19
• Zgoda na wykorzystanie wizerunku osób korzystających w imprez/wydarzeń organizowanych przez Szkołę (załącznik nr 8).....	20
• Zgoda na wykorzystanie wizerunku pracownika (załącznik nr 9)	21
• Zgoda na wykorzystanie wizerunku ucznia/rodzica/opiekuna (załącznik nr 10).....	22
• Odwołanie zgody na przetwarzanie danych osobowych (załącznik nr 11).....	23
• Umowa powierzenia przetwarzania danych osobowych (załącznik nr 12).....	24
• Wniosek o udostępnienie danych ze zbioru danych osobowych (załącznik nr 13).....	26
Część II - ANALIZA RYZYKA	27
Część III - INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM.....	37
Część IV- ZASADY POSTĘPOWANIA w przypadku wykrycia naruszenia ochrony danych osobowych.....	41
• Zawiadomienie o naruszeniu danych osobowych (załącznik nr 14)	46
• Raport o naruszeniu danych osobowych (załącznik nr 15)	47
• Karta kontroli wewnętrznej (załącznik nr 16)	48
Część V – REGULAMIN KORZYSTANIA ZE SŁUŻBOWEJ POCZTY ELEKTRONICZNEJ.....	50

POLITYKA OCHRONY DANYCH OSOBOWYCH

przetwarzanych w Zespole Szkół Specjalnych w Ścinawce Dolnej

Podstawa prawna:

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 - dalej RODO)

Działalność jednostek oświatowych w tym zakresie regulują przepisy ustawy dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922), według której szkoły są administratorami danych osobowych, a osobą odpowiedzialną za prawidłowe przetwarzanie chronionych jest dyrektor danego podmiotu.

§ 1

Wstęp

1. W dążeniu do zapewnienia wysokiego poziomu ochrony przetwarzanych danych osobowych, w tym zabezpieczenia danych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych w Zespole Szkół Specjalnych w Ścinawce Dolnej, określa się „Politykę ochrony danych osobowych przetwarzanych w Zespole Szkół Specjalnych w Ścinawce Dolnej”.
2. Administrator czyli Zespół Szkół Specjalnych w Ścinawce Dolnej, reprezentowany przez Dyrektora Zespołu Szkół, zobowiązany jest do zabezpieczenia przetwarzanych danych osobowych, poprzez podjęcie środków technicznych i organizacyjnych odpowiadających ryzyku naruszenia praw lub wolności osób fizycznych, z uwzględnieniem wiedzy technicznej, kosztów wdrożenia oraz charakteru, zakresu, kontekstu i celów przetwarzania.
3. Przetwarzanie danych osobowych, może być realizowane po spełnieniu jednego z warunków określonych w art. 6 RODO.
4. Niniejsza polityka ochrony obejmuje wszystkie procesy i czynności przetwarzania danych osobowych w Szkole i odnosi się do zabezpieczenia danych osobowych przetwarzanych zarówno w formie papierowej jak i przy wykorzystaniu systemów teleinformatycznych. W skład jej wchodzi także wzory pism związanych z RODO oraz Analiza ryzyka, Instrukcja zarządzania systemem informatycznym oraz Zasady postępowania w przypadku naruszenia ochrony danych osobowych w Zespole Szkół Specjalnych w Ścinawce Dolnej.

§ 2

Podstawowe pojęcia

1. Ilekroć w niniejszym dokumencie jest mowa o:
 - a) Szkole – rozumie się przez to Zespół Szkół Specjalnych w Ścinawce Dolnej;
 - b) Administratorze – rozumie się przez to Zespół Szkół Specjalnych w Ścinawce Dolnej reprezentowany przez Dyrektora Szkoły;
 - c) RODO – rozumie się przez to rozporządzenie 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 (Dz. Urz. UE L 119, s. 1);
 - d) Polityce – rozumie się przez to „Politykę ochrony danych osobowych przetwarzanych w Zespole Szkół Specjalnych w Ścinawce Dolnej”;
 - e) IOD w przepisach rozporządzenia – rozumie się przez to inspektora ochrony danych osobowych; (nie obowiązuje w szkole prowadzonej przez podmiot niepubliczny - zob. art 37 RODO i art. 9 ODO).
 - f) ASI – rozumie się przez to Administratora Systemu Informatycznego, czyli pracownika wyznaczonego przez Administratora, odpowiedzialnego za funkcjonowanie systemu teleinformatycznego oraz stosowanie technicznych i organizacyjnych środków ochrony w tym systemie.
 - g) Danych osobowych – rozumie się przez to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
 - h) Przetwarzaniu danych osobowych – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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.

§ 3

Wykaz zbiorów danych osobowych przechowywanych w szkole

1. W szkole prowadzi się następujące zbiory danych osobowych:
 - a) Akta osobowe pracowników.
 - b) Listy płac pracowników.
 - c) Ewidencja legitymacji pracowniczych.
 - d) Rejestr upoważnień.
 - e) Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych,
 - f) Arkusz organizacji roku szkolnego.
 - g) Księga uczniów.
 - h) Arkusze ocen wszystkich uczniów.
 - i) Protokoły zebrań rady pedagogicznej.
 - j) Dzienniki lekcyjne i dzienniki zajęć pozalekcyjnych, dzienniki zajęć specjalistycznych.
 - k) Rejestr orzeczeń poradni PPP.
 - l) Ewidencja wydanych legitymacji szkolnych.

- m) Ewidencja wydanych świadectw ukończenia szkoły.
 - n) Archiwum (akta osobowe pracowników, listy płac, księgi arkuszy ocen, dzienniki lekcyjne).
2. Dane osobowe podlegające ochronie, znajdują się także w następujących dokumentach sporządzanych i przetwarzanych w Zespole Szkół Specjalnych w Ścinawce Dolnej:
- a) Indywidualny program edukacyjno-terapeutyczny.
 - b) Indywidualny program rewalidacyjno-wychowawczy.
 - c) Orzeczenie o potrzebie kształcenia specjalnego.
 - d) Orzeczenie o potrzebie zajęć rewalidacyjno-wychowawczych
 - e) Opinie pedagogiczne o uczniu sporządzane przez wychowawcę lub pedagoga szkolnego.
 - f) Opinie psychologiczne o uczniu sporządzane przez psychologa szkolnego
 - g) Opinie logopedyczne o uczniu sporządzane przez logopedę.
 - h) Wszelkie wyniki badań medycznych uczniów, jeśli organizuje je szkoła za zgodą lub na prośbę rodziców/opiekunów prawnych.
 - i) Arkusze wielospecjalistycznej oceny funkcjonowania ucznia i sporządzana na jej podstawie ocena opisowa ucznia - półroczna i roczna.
 - j) Orzeczenie o niepełnosprawności ucznia udostępnianie przez rodzica, jeśli zachodzi taka potrzeba ze strony szkoły.

§ 4

Identyfikacja zasobów systemu informatycznego oraz programy zastosowane do przetwarzania tych danych.

1. Struktura informatyczna Zespołu Szkół składa się z komputerów stacjonarnych i przenośnych nie połączonych siecią. Komputery stacjonarne i przenośne wykorzystywane do zbierania i wprowadzania danych do systemu są poprzez system firewall dołączone do sieci Internet.
2. W Zespole Szkół funkcjonują następujące systemy informatyczne:
- a) Vulcan:
 - a. księgowość
 - b. płacesłużący do rejestrowania i przetwarzania danych o pracownikach pedagogicznych i niepedagogicznych, wykorzystywany do czynności związanych z przebiegiem zatrudnienia
 - b) Płatnik - system obsługujący przesyłanie danych do ZUS
 - c) SIO - program do obsługi systemu informacji oświatowej.

§ 5

Administrator Danych Osobowych

1. Za bezpieczeństwo danych osobowych przetwarzanych w Szkole odpowiada **ADMINISTRATOR**, który w myśl przepisów RODO, obowiązany jest zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

2. Do zadań Administratora należy:
 - a) wydawanie upoważnień do przetwarzania danych osobowych – wzór upoważnienia określa **załącznik nr 1**;
 - b) odwoływanie upoważnień do przetwarzania danych osobowych – wzór odwołania upoważnienia określa **załącznik nr 2**;
 - c) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych – wzór ewidencji określa **załącznik nr 3**,
 - d) określanie potrzeb w zakresie stosowanych w Szkole zabezpieczeń, zatwierdzanie rozwiązań i nadzorowanie prawidłowości ich wdrożenia,
 - e) podnoszenie świadomości i kwalifikacji osób przetwarzających dane osobowe w Szkole i zapewnienie odpowiedniego poziomu przeszkolenia w tym zakresie,
3. Administrator, może wyznaczyć pracownika administracyjnego, który będzie dbał o dokumentację i będzie podlegał dyrektorowi.

§ 6

Administrator Systemu Informatycznego - ASI

1. Administrator wyznacza pracownika zwanego Administratorem Systemu Informatycznego (ASI), odpowiedzialnego za funkcjonowanie systemu teleinformatycznego oraz stosowanie technicznych i organizacyjnych środków ochrony w tym systemie.
2. Obowiązki ASI może pełnić dyrektor szkoły.
3. Do zadań Administratora Systemu Informatycznego należy:
 - a) zarządzanie bezpieczeństwem przetwarzania danych osobowych w systemie informatycznym zgodnie z wymogami prawa i wskazówkami Administratora,
 - b) doskonalenie metod zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzaniem,
 - c) przydzielanie identyfikatorów użytkownikom systemu informatycznego oraz zaznajamianie ich z procedurami ustalania i zmiany haseł dostępu,
 - d) nadzorowanie prac związanych z rozwojem, modyfikacją, serwisowaniem i konserwacją systemu,
 - e) zapewnienie bezpieczeństwa wewnętrznego i zewnętrznego obiegu informacji w sieci i zabezpieczenie łącz z zewnętrznymi,

§ 7

Pracownicy upoważnieni do gromadzenia i przetwarzania danych osobowych

1. Osobami uprawnionymi do gromadzenia i przetwarzania danych osobowych są:
 - a) główny księgowy
 - b) nauczyciele
 - c) inne osoby upoważnione przez dyrektora szkoły.
2. Osoby te są obowiązane zachować uzyskane informacje w tajemnicy, co potwierdzają własnoręcznym podpisem wraz ze złożeniem stosownego

oświadczenia na odpowiednim formularzu (**oświadczenie o zachowaniu poufności - załącznik nr 4**).

3. Oświadczenie to zostaje włączone do akt osobowych pracownika.
4. Osoba upoważniona:
 - a) chroni prawo do prywatności osób fizycznych powierzających Szkole swoje dane osobowe poprzez przetwarzanie ich zgodnie z przepisami prawa oraz zasadami określonymi w Polityce;
 - b) zapoznaje się zasadami określonymi w Polityce i składa **oświadczenie o znajomości tych przepisów (załącznik nr 5)**
 - c) przetwarza dane osobowe wyłącznie w celu realizacji zadań określonych przepisami prawa;
5. Za przetwarzanie danych osobowych niezgodnie z prawem, celami przetwarzania lub przechowywanie ich w sposób niezapewniający ochrony interesów osób, których te dane dotyczą ponosi odpowiedzialność karną, wynikająca z przepisów ustawy o ochronie danych osobowych lub pracowniczą na zasadach określonych w kodeksie pracy.

§ 8

Realizacja praw i obowiązków osób, których dane są przetwarzane w Szkole

1. W Szkole wprowadza się rozwiązania, które pozwalają na realizowanie praw osób, których dane są przetwarzane. W szczególności dotyczy to:
 - a) umożliwienia osobom, których dane dotyczą wyrażenia zgody na przetwarzanie danych osobowych (gdy brak innej podstawy do przetwarzania danych) (*zgoda pracownika - załącznik nr 6; zgoda rodziców/opiekunów prawnych – załącznik nr 7*)
 - b) informowania osób, których dane dotyczą o zbieraniu i przetwarzaniu tych danych; (*Zgoda na wykorzystanie wizerunku osób korzystających w imprez/wydarzeń organizowanych przez Szkołę - załącznik nr 8*)
 - c) umożliwienia wyrażenia zgody na wykorzystanie wizerunku pracownika (*zgoda na wykonywanie i wykorzystanie wizerunku - załącznik nr 9*)
 - d) umożliwienia wyrażenia zgody na wykorzystanie wizerunku ucznia/rodzica/opiekuna prawnego (*zgoda na wykonywanie i wykorzystanie wizerunku ucznia/rodzica/opiekuna prawnego - załącznik nr 10*)
 - e) umożliwienia osobom, których dane dotyczą wycofania zgody na przetwarzanie danych osobowych (**załącznik nr 11**)
 - f) prawa dostępu do danych przysługującego osobom, których dane dotyczą
 - g) prawa osób, których dane dotyczą, do sprostowania danych,
 - h) prawa osób, których dane dotyczą, do usunięcia swoich danych („prawa do bycia zapomnianym”),
 - i) prawa osób, których dane dotyczą, do ograniczenia przetwarzania danych.
2. Spełnienie obowiązków informacyjnych względem osób, których dane są przetwarzane odbywa się poprzez przekazanie osobom wymaganych prawem informacji przy zbieraniu danych oraz udokumentowanie realizacji tych obowiązków.

3. Warunkiem prawidłowego spełnienia obowiązku informacyjnego wobec osoby, której dane dotyczą, jest przekazanie jej w zwięzłej, przejrzystej i zrozumiałej formie, jasnym i prostym językiem wszelkich informacji, o których mowa w art. 13 i 14 RODO oraz prowadzenie z nią wszelkiej korespondencji, w myśl art. 15-22 i 34 RODO w sprawie przetwarzania danych osobowych.
4. Informacji, o których mowa w pkt. 3 udziela się na piśmie, w tym w stosownych przypadkach – elektronicznie lub w inny sposób (np. ustnie).
5. Informacje podawane na mocy art. 13 i 14 RODO oraz komunikacja i działania podejmowane na mocy art. 15-22 i 34 RODO są wolne od opłat. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nadmierne, w szczególności ze względu na swój ustawiczny charakter, Szkoła może pobrać opłatę uwzględniającą administracyjne koszty udzielenia informacji.
6. Realizacja zadań, o których mowa w pkt. 1 uwzględnia zasady, w tym wyłączenia, które zostały określone w obowiązujących przepisach prawa o ochronie danych osobowych.
7. Dostęp, usunięcie lub ograniczenie przetwarzania danych osobowych musi być zgodne z przepisami prawa, na podstawie których odbywa się przetwarzanie oraz na podstawie przepisów prawa określających zasady przetwarzania dokumentacji archiwalnej.

§ 9

Powierzenie przetwarzania danych osobowych

1. Przetwarzanie powierzonych danych może być realizowane wyłącznie przez podmioty, które gwarantują odpowiednie środki techniczne i organizacyjne dające możliwość spełnienia wymogów RODO, w tym w szczególności skutecznie chronią prawa osób, których dane dotyczą.
2. Przy określaniu minimalnych wymogów, które powinien spełnić podmiot przetwarzający należy brać pod uwagę charakter, skalę i zakres przetwarzania oraz, jeśli to konieczne, uwzględniać wyniki szacowania ryzyka przeprowadzone w Szkole w tym zakresie.
3. Powierzenie przetwarzania danych osobowych odbywa się na podstawie pisemnej umowy lub porozumienia, które wyraźnie określają charakter i cel przetwarzania, przedmiot i czas trwania przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, oraz obowiązki i prawa administratora i podmiotu przetwarzającego. **(wzór - umowa powierzenia - załącznik nr 12)**
4. Dokumentacja, na podstawie której następuje powierzenie danych, musi mieć formę pisemną (dopuszcza się prowadzenie tej dokumentacji w formie elektronicznej).
5. Dokumentacja, na podstawie której następuje powierzenie danych, musi gwarantować Administratorowi realizację zadań wynikających z zapisów art. 28 RODO, w tym w szczególności:
 - a) możliwość egzekwowania wskazanych w dokumentacji obowiązków podmiotu przetwarzającego,
 - b) możliwość przeprowadzanie kontroli/audytów w zakresie realizacji umowy powierzenia,
 - c) możliwości weryfikacji czy powierzone dane nie zostały przekazane innemu podmiotowi przez przetwarzającego bez zgody („podpowierzenie danych”).

§ 10

Udostępnianie danych osobowych

1. Dostęp do danych osobowych i ich przetwarzanie bez odrębnego upoważnienia Administratora danych osobowych może mieć miejsce wyłącznie w przypadku działań osób i podmiotów uprawnionych na mocy odpowiednich przepisów prawa do dostępu i przetwarzania danych określonej kategorii.
2. Udostępnianie danych osobowych odbywa się wyłącznie po złożeniu *wniosku o udostępnienie danych (załącznik nr 13)*
3. Dane osobowe mogą być udostępniane:
 - a) podmiotom i organom publicznym działającym w granicach przyznanych im uprawnień, po okazaniu dokumentów potwierdzających te uprawnienia;
 - b) stronom postępowań administracyjnych prowadzonych w Szkole, na zasadach określonych w kodeksie postępowania administracyjnego lub odrębnych przepisów.
4. Administrator odmawia udostępnienia danych osobowych jeżeli spowodowałoby to naruszenie przepisów prawa.

§ 11

Analiza ryzyka

1. W trakcie procesu zarządzania ryzykiem przeprowadzana jest identyfikacja zagrożeń bezpieczeństwa danych osobowych oraz określane są podatności i skutki wystąpienia tych zagrożeń oraz kategoryzacja danych i czynności przetwarzania pod kątem ryzyka, które przedstawiają **(część II polityki)**
2. W ramach procesu zarządzania ryzykiem przeprowadzana jest:
 - a) analiza ryzyka dla czynności przetwarzania danych lub ich kategorii;
 - b) ocena skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie.
3. Uzyskane, w ramach procesu analizy ryzyka, wyniki są podstawą do dalszego postępowania ze zidentyfikowanymi ryzykami w kontekście wdrożenia rozwiązań technicznych i organizacyjnych, które pozwolą ochronić dane osobowe przed utratą ich podstawowych atrybutów (poufności, integralności, dostępności, rozliczalności) oraz pozwolą zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania tych danych w Szkole.
4. Ocena skutków czynności przetwarzania dla ochrony danych oraz ich wpływu na naruszenia praw lub wolności osób fizycznych obejmuje analizę i rozpatrywanie możliwych sytuacji i scenariuszy naruszenia ochrony danych osobowych przy uwzględnieniu charakteru, zakresu, kontekstu i celów przetwarzania, oraz różnego prawdopodobieństwa wystąpienia i wagi zagrożenia.
5. W ramach przeprowadzanej oceny, o której mowa w pkt. 4, należy brać pod uwagę wskazane przez Prezesa UODO rodzaje procesów i czynności przetwarzania, dla których wymagane jest przeprowadzenie oceny skutków dla ochrony danych.

§ 12

Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych

Szkoła nie przekazuje danych osobowych do państw trzecich lub organizacji międzynarodowych.

§ 13

Bezpieczeństwo w przetwarzaniu danych osobowych w formie tradycyjnej

1. Pomieszczenia, w których przetwarzane są dane osobowe, pozostają zawsze pod bezpośrednim nadzorem upoważnionego do ich przetwarzania pracownika. Opuszczenie pomieszczenia musi być poprzedzone przeniesieniem danych osobowych do odpowiednio zabezpieczonego miejsca. Przy planowanej dłuższej nieobecności pracownika pomieszczenie winno być zamknięte na klucz.
2. Klucze do szaf, w których przechowywane są dane osobowe mają jedynie pracownicy upoważnieni do przetwarzania danych osobowych, w zakresie zgodnym z kategorią danych.
3. Korzystanie ze zbiorów danych osobowych przez osoby niezatrudnione w Szkole powinno odbywać się po uzyskaniu upoważnienia lub skonsultowane z Administratorem, w przypadku pracowników upoważnionych do przetwarzania tych danych na podstawie ogólnie obowiązujących przepisów.

§ 14

Bezpieczeństwo w przetwarzaniu danych osobowych w systemach informatycznych

Zasady bezpiecznego użytkowania systemu informatycznego zawarte są w *Instrukcji zarządzania systemem informatycznym*, obligatoryjnej do zapoznania się i stosowania przez wszystkich użytkowników systemu informatycznego Szkoły, stanowiącej **część III Polityki**.

§ 15

Naruszenie bezpieczeństwa danych osobowych

1. Każda osoba upoważniona do przetwarzania danych osobowych w Szkole jest zobowiązana do natychmiastowego powiadamiania Administratora o wystąpieniu incydentu związanego z naruszeniem ochrony danych osobowych.
2. Szczegółowe *Zasady postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych*, zostały określony w **części IV Polityki**.
3. Zgłaszanie sytuacji naruszenia bezpieczeństwa danych osobowych dokonuje się poprzez: „Zawiadomienia o naruszeniu danych przesyłanego do osób których dane zostały naruszone” (**załącznik nr 14**) oraz „Raportu o naruszeniu danych osobowych” (**załącznik nr 15**).

§ 16

Weryfikacja systemu ochrony danych

1. Weryfikacja systemu ochrony danych odbywa się poprzez prowadzenie kontroli okresowych nie rzadziej niż raz w roku (*Karta kontroli wewnętrznej* - **załącznik nr 16**)

2. W zależności od potrzeb, część prac w ramach weryfikacji systemu ochrony danych, może zostać zlecone podmiotowi zewnętrznemu.

§ 17

Postanowienia końcowe

1. Osoby przetwarzające dane osobowe zobowiązane są do stosowania postanowień zawartych w niniejszym dokumencie oraz pozostałej dokumentacji, która uszczegóławia wymagania i zasady ochrony danych osobowych.
2. Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako naruszenie obowiązków służbowych.
3. Polityka oraz pozostała dokumentacja, która uszczegóławia wymagania i zasady ochrony danych osobowych może być udostępniania osobom trzecim, jeżeli nie zawiera w swojej treści i w załącznikach szczegółowych informacji o wdrożonych w Szkole zabezpieczeniach danych osobowych oraz innych informacji prawnie chronionych.

§ 18

Wykaz załączników

Załącznik nr 1 - Upoważnienie do przetwarzania danych osobowych

Załącznik nr 2 - Odwołanie upoważnienia do przetwarzania danych osobowych

Załącznik nr 3 - Ewidencja osób upoważnionych do przetwarzania danych osobowych

Załącznik nr 4 - Oświadczenie o zachowaniu poufności

Załącznik nr 5 – Oświadczenie o zapoznaniu się z przepisami

Załącznik nr 6 - Zgoda na przetwarzanie danych osobowych pracownika

Załącznik nr 7 - Zgoda na przetwarzanie danych osobowych rodzica/opiekuna

Załącznik nr 8 - Zgoda na wykorzystanie wizerunku osób korzystających w imprez/wydarzeń organizowanych przez Szkołę

Załącznik nr 9 - Zgoda na wykorzystanie wizerunku pracownika /ucznia /rodzica

Załącznik nr 10 - Zgoda na wykorzystanie wizerunku ucznia /rodzica/opiekuna prawnego

Załącznik nr 11 - Odwołanie zgody na przetwarzanie danych osobowych

Załącznik nr 12 - Umowa powierzenia przetwarzania danych osobowych

Załącznik nr 13 - Wniosek o udostępnienie danych ze zbioru danych osobowych

Załącznik nr 14- Zawiadomienie o naruszeniu danych osobowych

Załącznik nr 15- Raport o naruszeniu danych osobowych

Załącznik nr 16 – Karta kontroli wewnętrznej

....., dnia r.

UPOWAŻNIENIE nr /20....

do przetwarzania danych osobowych

Na podstawie art. 29 rozporządzenie 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 (Dz. Urz. UE L 119, s. 1)

- udzielam Pani/Panu:

.....
(imię i nazwisko pracownika)

.....
(stanowisko służbowe)

upoważnienia do przetwarzania danych osobowych, których Administratorem jest Zespół Szkół Specjalnych w Ścinawce Dolnej, zgromadzonych w formie tradycyjnej oraz w systemach informatycznych

.....
(wypisać zbiory danych, programy informatyczne i dokumenty zawierające dane osobowe, do których przetwarzania upoważniony jest pracownik)

Jest Pani/Pan upoważniona do przetwarzania danych osobowych wyłącznie w zakresie wynikającym z Pani zadań oraz polecenia służbowego.

Informuję, że Pani/Pan została wpisana do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w Szkole.

Upoważnienie traci moc z chwilą ustania stosunku pracy.

.....
(podpis Dyrektora)

Przyjmuję do wiadomości i stosowania.

.....
(Data i podpis osoby upoważnionej)

Załącznik Nr 2

....., dnia r.

.....
(pieczęć Szkoły)

ODWOŁANIE UPOWAŻNIENIA nr ...

do przetwarzania danych osobowych

Odwołuję z dniem upoważnienie nr/20.... do przetwarzania
danych osobowych wystawione dla Pani/Pana

.....
(pieczęć i podpis dyrektora)

Przyjmuję do wiadomości

.....

(Data i podpis osoby upoważnionej)

Załącznik Nr 3

....., dnia r.

.....

(pieczęć Szkoły)

**EWIDENCJA OSÓB UPOWAŻNIONYCH
DO PRZETWARZANIA DANYCH OSOBOWYCH**

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

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

Pieczęć szkoły

....., dnia r.

.....

(imię i nazwisko pracownika)

.....

(stanowisko)

OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI

Ja, niżej podpisany/a oświadczam, iż zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań i obowiązków służbowych wynikających ze stosunku pracy, zarówno w czasie trwania umowy, jak i po jej ustaniu.

.....

(Data i czytelny podpis pracownika)

Pieczęć szkoły

Załącznik Nr 5

....., dnia r.

.....

(Imię i nazwisko pracownika)

OŚWIADCZENIE O ZAPOZNANIU SIĘ Z PRZEPISAMI

Oświadczam, iż zostałam/zostałem zapoznana/zapoznany z przepisami dotyczącymi ochrony danych osobowych, w szczególności 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 (Dz. Urz. UE L 119, s. 1) oraz wydanych na jej podstawie aktów wykonawczych ustanowionych przez Administratora Danych - Zespół Szkół Specjalnych w Ścinawce Dolnej czyli: „Polityki ochrony danych osobowych przetwarzanych przez Zespół Szkół Specjalnych w Ścinawce Dolnej” oraz wchodzącej w jego skład: „Instrukcji zarządzania systemem informatycznym” i „Zasad postępowania w przypadku wykrycia naruszenia ochrony danych osobowych”.

Zobowiązuję się przestrzegać zasad ochrony danych osobowych określonych w w/w dokumentach.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane przez Pracodawcę za ciężkie naruszenie obowiązków pracowniczych w rozumieniu art. 52 § 1 pkt 1 Kodeksu Pracy lub za naruszenie przepisów karnych ww. ustawy o ochronie danych osobowych.

.....
Data i czytelny podpis pracownika

....., dnia r.

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH PRACOWNIKA

Ja, niżej podpisany/podpisana, **oświadczam**, że zgodnie z rozporządzeniem 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 RODO - Dz.Urz. UE L 119, s. 1)

wyrażam zgodę ☐ TAK ☐ NIE

na przetwarzanie przez Zespół Szkół Specjalnych w Ścinawce Dolnej, moich danych osobowych w celu i zakresie niezbędnym do nawiązania i przebiegu zatrudnienia w Zespole Szkół Specjalnych w Ścinawce Dolnej.

.....

Data i czytelny podpis pracownika

KLAUZULA INFORMACJA

Jako administrator danych osobowych, informuję Pana/ Panią, iż:

1. Podanie danych jest dobrowolne, ale niezbędne w celu nawiązania i przebiegu zatrudnienia w Zespole Szkół Specjalnych w Ścinawce Dolnej,
2. Podanie przez Panią/Pana danych osobowych jest wymogiem ustawowym zawarcia umowy. Brak podania danych osobowych uniemożliwia zatrudnienie i prowadzenie czynności związanych w przebiegiem zatrudnienia.
3. Posiada Pani/Pan prawo dostępu do treści swoich danych i ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania;
4. Dane mogą być udostępniane przez Zespół Szkół Specjalnych w Ścinawce Dolnej podmiotom upoważnionym do uzyskania informacji, na podstawie odpowiednich przepisów prawa.
5. Informujemy, iż Pani/Pana dane osobowe nie będą przekazywane żadnym odbiorcom danych.
6. Pani/Pana dane osobowe nie będą przetwarzane w sposób zautomatyzowany i nie będą profilowane.
7. Podane dane będą przetwarzane na podstawie art. 6 ust. 1 pkt a) i zgodnie z treścią ogólnego rozporządzenia o ochronie danych (RODO).;
8. Administratorem Ochrony danych jest Zespół Szkół Specjalnych w Ścinawce Dolnej reprezentowany przez Dyrektora Szkoły.

9. Dane osobowe będą przechowywane wg następujących kategorii:

L.p.	Cel przetwarzania	Kategorie danych	Podstawa prawna	Okres przechowywania danych
1.	Prowadzenie ewidencji pracowników zgodnie z Kodeksem pracy	Dane identyfikacyjne, dane adresowe, dane o wykształceniu, przebiegu pracy, absencji (urlopy, zwolnienia lekarskie, rehabilitacyjne, szkoleniowe i inne), dane o zakresie obowiązków, stawce wynagrodzenia, karach i nagrodach oraz inne dane wymagane zgodnie z Kodeksem pracy	Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2018 r., poz. 108 t.j.) - w szczeg. art. 22 z ind. 1 w związku z art. 94 pkt 9a i 9b	50 lat [art. 51u ust. 1 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2018 r., poz. 217 t.j.)]
2.	Zgłoszenia pracownika i członków jego rodziny do ZUS, aktualizacja zgłoszenia oraz przekazywanie informacji o zwolnieniach	Dane identyfikacyjne, dane adresowe oraz inne dane wymagane w formularzu zgłoszenia ZUS ZUA - zgłoszenie, ZUS IUA - zmiana danych, ZUS ZWUA - wyrejestrowanie, ZUS ZCNA - zgłoszenie członka rodziny, ZAS - wniosek o ustalenie okresu zasiłkowego, OL-2 - wniosek o kontrolę zaśw. lekarskiego, Z15a - zgłoszenie opieki nad dzieckiem, Z15B - zgłoszenie opieki nad innym członkiem rodziny	Ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz.U. z 2017 r., poz. 1778 t.j.) - art. 1, 6 oraz 6a	50 lat [art. 125a ust. 4 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz.U.z 2017 r., poz.1383)]

10. Ma Pan/Pani prawo wniesienia skargi do organu nadzorczego, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych (RODO) z dnia 27 kwietnia 2016 r.

.....
Data i podpis dyrektora

Przyjąłem/łam do wiadomości powyższą klauzulę informacyjną

.....
Data i podpis pracownika

....., dnia r.

Pan/Pani

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH**UCZNIA / RODZICA / OPIEKUNA PRAWNEGO** **(właściwe podkreślić)*

Ja, niżej podpisany/podpisana, **oświadczam**, że zgodnie z rozporządzeniem 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 RODO - Dz. Urz. UE L 119, s. 1)

wyrażam zgodę **(zaznaczyć właściwe)* ☐ TAK ☐ NIE

na przetwarzanie przez Zespół Szkół Specjalnych w Ścinawce Dolnej, danych osobowych

mojego dziecka.....(*imię i nazwisko dziecka*) oraz na przetwarzanie moich danych oraz członków rodziny pozostających we wspólnym gospodarstwie domowym, w celu i zakresie niezbędnym do przebiegu nauczania dziecka oraz działalności dydaktycznej, wychowawczej i opiekuńczej szkoły.

.....

Data i czytelny podpis rodzica/opiekuna prawnego

INFORMACJA DLA RODZICÓW/ OPIEKUNÓW PRAWNYCH UCZNIÓW

1. Podanie danych jest dobrowolne, ale niezbędne w celu prawidłowego przebiegu nauczania dziecka w Zespole Szkół Specjalnych w Ścinawce Dolnej,
2. Posiada Pani/Pan prawo dostępu do treści swoich danych i ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania;
3. Dane mogą być udostępniane przez Zespół Szkół Specjalnych w Ścinawce Dolnej podmiotom upoważnionym do uzyskania informacji, na podstawie odpowiednich przepisów prawa.
4. Informujemy, iż dane osobowe nie będą przekazywane żadnym odbiorcom danych.
5. Podane dane będą przetwarzane na podstawie art. 6 ust. 1 pkt a) i zgodnie z treścią ogólnego rozporządzenia o ochronie danych (RODO).;
6. Administratorem Ochrony danych jest Zespół Szkół Specjalnych w Ścinawce Dolnej reprezentowany przez Dyrektora Szkoły.
7. Ma Pan/Pani prawo wniesienia skargi do organu nadzorczego, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących dziecka narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych (RODO) z dnia 27 kwietnia 2016 r.

.....

(Data i podpis dyrektora)

Przyjąłem/łam do wiadomości powyższą klauzulę informacyjną

.....
Data i podpis rodzica/opiekuna prawnego

Zgoda na wykorzystanie wizerunku osób korzystających w imprez/wydarzeń organizowanych przez Zespół Szkół Specjalnych w Ścinawce Dolnej*

Korzystanie osób z imprez/wydarzeń organizowanych przez Zespół Szkół Specjalnych jest równoznaczne z wyrażaniem zgody na przetwarzanie danych osobowych w celu realizacji zadań ustawowych i statutowych Zespół Szkół Specjalnych w Ścinawce Dolnej

Szkoła zastrzega sobie prawo utrwalania przebiegu imprezy (zdjęcia uczestników, zapis filmowy) w celach dokumentacyjnych, edukacyjnych i promocyjnych.

Udział w imprezie oznacza wyrażenie przez Uczestnika zgody na nieodpłatne utrwalenie swojego wizerunku w wyżej wskazanym zakresie, a także na jego rozpowszechnianie bez ograniczeń terytorialnych i czasowych, w szczególności poprzez umieszczanie fotografii, filmów i nagrań dźwiękowych w serwisach internetowych prowadzonych przez Szkołę, a także w publikacjach z zastrzeżeniem, że przedmiotowe fotografie i filmy w publikacjach osób trzecich mogą jedynie ilustrować informacje o działalności prowadzonej przez Szkołę, a ich wykorzystywanie w innym kontekście nie jest dozwolone.

Szkoła zapewnia, że wizerunek Uczestników imprez nie będzie wykorzystywany przez nią w celach zarobkowych, a Uczestnicy przyjmują do wiadomości, że z tytułu jego użycia nie przysługują im jakiegokolwiek roszczenia, w szczególności prawo do wynagrodzenia.

Każdy kto korzysta z imprez organizowanych przez Szkołę i nie wyraża zgody na przetwarzanie jego danych osobowych (w tym wizerunku) w ramach nagrań wizualnych, dźwiękowych, zdjęciowych dokonywanych przez Szkołę w celach promocyjnych i rozpowszechniania działań Szkoły jest obowiązany zgłosić to osobie prowadzącej daną imprezę.

Szkoła nie przekazuje, nie sprzedaje i nie użycza zgromadzonych danych osobowych Uczestników innym osobom lub instytucjom.

*(*Powyższa informacja umieszczona jest na stronie www.szkolascinawka.pl oraz stanowi integralną część regulaminów imprez/wydarzeń organizowanych przez szkołę)*

Pieczęć szkoły

....., dnia

.....

(imię i nazwisko pracownika)

ZGODA NA WYKORZYSTANIE WIZERUNKU PRACOWNIKA

OŚWIADCZAM, ŻE WYRAŻAM ZGODĘ na wykonywanie i przetwarzanie zdjęć i materiałów filmowych zawierających mój wizerunek zarejestrowanych podczas zajęć edukacyjnych i uroczystości szkolnych, podczas uczestnictwa w wycieczkach, konkursach, zawodach itp. organizowanych przez Zespół Szkół Specjalnych w Ścinawce Dolnej w siedzibie szkoły oraz poza siedzibą szkoły.

Jednocześnie **wyrażam zgodę na umieszczanie i publikowanie** zdjęć i filmów na stronie internetowej strony www.szkolascinawka.pl oraz profilu www.facebook.com/specszkola/; na gazecie szkolnej oraz w mediach, w celu informacji i promocji szkoły.

.....

Data i czytelny podpis pracownika

Klauzula informacyjna:

1. Administratorem ochrony danych jest Zespół Szkół Specjalnych w Ścinawce Dolnej reprezentowany przez Dyrektora Szkoły.
2. Wykonane zdjęcia czy filmy będą przetwarzane na podstawie niniejszej zgody przez cały okres trwania zatrudnienia.
3. Posiada Pani/Pan prawo dostępu do swoich danych w postaci zdjęć i filmów, sprostowania, usunięcia, ograniczenia przetwarzania, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania;
4. Zdjęcia i filmy nie będą udostępniane podmiotom innym niż podmioty upoważnione na podstawie stosownych przepisów prawa.
5. Podane dane będą przetwarzane na podstawie art. 6 ust. 1 pkt a) i zgodnie z treścią ogólnego rozporządzenia o ochronie danych (RODO);
6. Przysługuje Panu/Pani prawo do cofnięcia wyrażonej zgody w dowolnym momencie. Powyższe nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie wyrażonej przeze mnie zgody przed jej cofnięciem.
7. Ma Pan/Pani prawo wniesienia skargi do organu nadzorczego, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych dotyczących Pani/Pana czy dziecka narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych (RODO) z dnia 27 kwietnia 2016 r.
8. Szkoła odpowiada jedynie za umieszczanie zdjęć i filmów na zarządzanych przez siebie w/w stronach internetowych.
9. Szkoła nie ponosi odpowiedzialności za umieszczanie zdjęć i materiałów filmowych związanych w życiu szkoły a zawierającym wizerunki w/w osób, na prywatnych stronach i profilach nauczycieli i innych pracowników szkoły oraz innych osób związanych w jakikolwiek sposób ze środowiskiem szkolnym. Wszelkie roszczenia naruszenia danych osobowych w tym względzie, należy kierować do właścicieli tychże stron czy profili internetowych, na których zamieszczone wizerunki osób wyrażających niniejszą zgodę.

.....

Data i podpis dyrektora

Przyjąłem/łam do wiadomości.....

....., dnia.....

**ZGODA NA WYKORZYSTANIE WIZERUNKU:
UCZNIA / RODZICÓW / OPIEKUNA PRAWNEGO**
**(niewłaściwe skreślić)*

OŚWIADCZAM, ŻE WYRAŻAM ZGODĘ na wykonywanie i przetwarzanie zdjęć i materiałów filmowych zawierających wizerunek:

Mój
(Imię i nazwisko rodziców / rodzica / opiekuna prawnego*)

Mojego
(Imię i nazwisko dziecka)*

zarejestrowanych podczas zajęć edukacyjnych i uroczystości szkolnych, podczas uczestnictwa w wycieczkach, konkursach, zawodach itp. organizowanych przez Zespół Szkół Specjalnych w Ścinawce Dolnej w siedzibie szkoły oraz poza siedzibą szkoły.

Jednocześnie **wyrażam zgodę na umieszczanie i publikowanie** zdjęć, filmów i prac wykonanych *przez mnie / przez moje dziecko** na stronie internetowej strony www.szkolascinawka.pl oraz profilu www.facebook.com/specszkola/; gazecie szkolnej oraz w mediach, w celu informacji i promocji szkoły.

.....

.....

Data i podpis rodziców / opiekuna prawnego

Klauzula informacyjna:

1. Administratorem Ochrony danych jest Zespół Szkół Specjalnych w Ścinawce Dolnej reprezentowany przez Dyrektora Szkoły.
2. Podane dane osobowe będą przetwarzane na podstawie niniejszej zgody przez cały okres trwania edukacji szkolnej dziecka.
3. Posiada Pani/Pan prawo dostępu do treści swoich danych i ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania;
4. Dane nie będą udostępniane podmiotom innym niż podmioty upoważnione na podstawie stosownych przepisów prawa.
5. Podane dane będą przetwarzane na podstawie art. 6 ust. 1 pkt a) i zgodnie z treścią ogólnego rozporządzenia o ochronie danych (RODO);
6. Przysługuje Panu/Pani prawo do cofnięcia wyrażonej zgody w dowolnym momencie. Powyższe nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie wyrażonej przez mnie zgody przed jej cofnięciem.
7. Ma Pan/Pani prawo wniesienia skargi do organu nadzorczego, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących dziecka narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych (RODO) z dnia 27 kwietnia 2016 r.
8. Szkoła odpowiada jedynie za umieszczanie zdjęć i filmów na zarządzanych przez siebie w/w stronach internetowych.
9. Szkoła nie ponosi odpowiedzialności za umieszczanie zdjęć i materiałów filmowych związanych z życiem szkoły a zawierającym wizerunki w/w osób, na prywatnych stronach i profilach nauczycieli i innych pracowników szkoły oraz innych osób związanych w jakikolwiek ze środowiskiem szkolnym. Wszelkie roszczenia naruszenie danych osobowych w tym względzie, należy kierować do właścicieli tych stron czy profili, na których zamieszczono wizerunki osób wyrażających niniejszą zgodę.

.....

Data i podpis dyrektora

Przyjąłem/łam do wiadomości.....

.....

Data i podpis rodziców / opiekuna prawnego

Pieczęć szkoły

Załącznik nr 11

....., dnia.....

.....
(Imię i nazwisko wnioskodawcy)

.....
(Adres wnioskodawcy)

.....

.....
(Pełna nazwa administratora danych)

.....
(Adres siedziby administratora danych)

.....

ODWOŁANIE ZGODY NA PRZETWARZANIE DANYCH OSOBOWYCH

Zgodnie z rozporządzeniem 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 RODO - Dz. Urz. UE L 119, s. 1) odwołuję wyrażoną przeze mnie zgodę na przetwarzanie moich danych osobowych w celu

Z poważaniem

.....
(Imię i nazwisko wnioskodawcy)

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Zawarta w dniu r. w pomiędzy:

..... z siedzibą w przy ul.,

reprezentowaną przez:

....., zwaną dalej **Zleceniodawcą**,

a

..... z siedzibą w przy ul., wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego przez Sąd Rejonowy dla w

....., Wydział Krajowego Rejestru Sądowego pod numerem KRS:

....., NIP: Regon:

reprezentowaną przez:

....., zwaną dalej **Wykonawcą**,

zwanymi łącznie „Stronami” o następującej treści:

§ 1. Powierzenie przetwarzania danych osobowych

1. Administratorem, w rozumieniu art. 4 pkt 7 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 (ogólnego rozporządzenia o ochronie danych) zwanego dalej „RODO” jest Zleceniodawca.
2. Wykonawcy, jako podmiotowi przetwarzającemu, stosownie do art. 28 RODO, powierza się przetwarzanie danych osobowych w ramach wykonywanych usług/prac.....
3. Niniejsza umowa nie upoważnia Wykonawcy do dalszego powierzenia przetwarzania danych osobowych w imieniu i na rzecz Zamawiającego innym podmiotom bez wyraźnej szczegółowej pisemnej zgody Zamawiającego.
4. Wykonawca zobowiązuje się przetwarzać powierzone dane osobowe wyłącznie w zakresie i w celu przewidzianym w umowie, przy uwzględnieniu zapisów RODO oraz innych przepisów prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
5. Zakres przetwarzania obejmuje następujące dane osobowe powierzone przez Zamawiającego:

1) *(podać kategorie danych osobowych);*

2)

i dotyczy przetwarzania danych *(wskazać kategorię osób, których dane są przetwarzane)*

6. Przetwarzanie powierzonych danych obejmuje ich *(wybrać odpowiednie czynności)* zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie oraz ich usuwanie

lub niszczenie po osiągnięciu celu przetwarzania danych osobowych, o którym mowa w § 1 ust. 2 umowy.

7. Okres przetwarzania danych osobowych obejmuje okres na jaki została zawarta umowa przy uwzględnieniu okresu gwarancji, przepisów oraz zasad archiwizacji obowiązujących u Wykonawcy oraz rozstrzygania ewentualnych sporów wynikłych z realizacji niniejszej umowy jeśli przetwarzane dane są do tego niezbędne.
8. Po zakończeniu świadczenia przez Wykonawcę oraz upływie okresu gwarancji na wykonane usługi związane z przetwarzaniem powierzonych danych Wykonawca gwarantuje usunięcie wszelkich przetwarzanych danych oraz ich kopii w nieprzekraczalnym terminie do dnia).

§ 2. Obowiązki i prawa administratora

1. Zamawiający jest uprawniony do kontrolowania Wykonawcy w zakresie przetwarzania powierzonych danych osobowych, pod względem zgodności z zapisami umowy.
2. Zamawiający jest uprawniony do egzekwowania od Wykonawcy aby świadczone usługi pozostawały w zgodzie z zasadami określonymi w RODO oraz innych przepisach prawa, dotyczących ochrony danych osobowych, w szczególności w zakresie przywrócenia prawidłowego przetwarzania danych osobowych po wykryciu nieprawidłowości.

§ 3. Obowiązki Wykonawcy

1. Wykonawca zobowiązuje się do zabezpieczenia przetwarzanych danych osobowych poprzez podjęcie środków technicznych i organizacyjnych odpowiadających ryzyku naruszenia praw lub wolności osób fizycznych, z uwzględnieniem wiedzy technicznej, kosztów wdrożenia oraz charakteru, zakresu, kontekstu i celów przetwarzania, o których mowa w art. 32 RODO.
2. Wykonawca, w okresie związania postanowieniami niniejszej umowy, zobowiązuje się bez zbędnej zwłoki zawiadomić Zamawiającego o naruszeniu powierzonych danych osobowych lub ich niewłaściwego użycia.
3. Wykonawca, w okresie związania postanowieniami niniejszej umowy, zobowiązuje się bez zbędnej zwłoki zawiadomić Zamawiającego o wszelkich czynnościach z własnym udziałem w sprawach dotyczących ochrony danych osobowych prowadzonych przez Prezesa Urzędu Ochrony Danych Osobowych, inne urzędy państwowe, policję, prokuraturę lub sąd.
4. Wykonawca zobowiązuje się odpowiedzieć niezwłocznie na każde pytanie Zamawiającego dotyczące przetwarzania powierzonych danych osobowych.
5. Wykonawca odpowiada za wszelkie wyrządzone szkody Zamawiającemu lub osobom trzecim, które powstały w wyniku niezgodnego z umową oraz innymi przepisami prawa powszechnie obowiązującego, przetwarzania powierzonych danych osobowych.

.....
Zleceniodawca

.....
Wykonawca

**WNIOSEK O UDOSTĘPNIENIE DANYCH
ZE ZBIORU DANYCH OSOBOWYCH**

1. Wniosek do.....

.....

(dokładne oznaczenie administratora danych)

2. Wnioskodawca.....

.....

(nazwa firmy i jej siedziba, REFON firmy albo nazwisko, imię i adres zamieszkania wnioskodawcy)

3. Podstawa prawna upoważniająca do pozyskania danych albo wskazanie wiarygodnie uzasadnionej potrzeby posiadania danych w przypadku osób innych niż wymienione w art. ust. 1 o ochronie danych osobowych:

.....

.....

.....

4. Wskazanie przeznaczenia dla udostępnienia danych:

.....

5. Oznaczenie lub nazwa zbioru, z którego mają być udostępnione dane:

.....

6. Zakres żądanych informacji ze zbioru:.....

.....

.....

7. Informacje umożliwiające wyszukanie w zbiorze danych:.....

.....

.....

(data, podpis i ew. pieczęć wnioskodawcy)

ANALIZA RYZYKA

W ZESPOLE SZKÓŁ SPECJALNYCH W ŚCINAWCE DOLNEJ

P-Prawdopodobieństwo incydentu (skala od 1 do 3), S-Skutki wystąpienia incydentu (skala od 1 do 3), R-Ryzyko wystąpienia incydentu (skala od 1 do 9)

L.p.	Zagrożenie	Opis zagrożenia	Prawdopodobieństwo	Skutek zagrożenia w	Wskaźnik Istotność ryzyka	Zabezpieczenie
1.	Podrzucone nośniki danych. Ataki telefoniczne	Atakujący pozostawia w biurze lub w dziale księgowości specjalnie przygotowany pendrive z zainstalowanym samouruchamiającym się szkodliwym programem. W wielu przypadkach z CIEKAWOŚCI pracownicy sprawdzają jego zawartość wkładając go do portu USB. W wyniku tego uruchamiają nieświadomie szkodliwe oprogramowanie (backdoory, exploity, exploitpaki, keyloggers). Intruz podający się za „naszego informatyka” prosi o podanie hasła pod pretekstem sprawdzania lub naprawy naszego systemu informatycznego. Intruz przedstawia się jako „serwisant Orange lub Netii” naprawiający usterkę i prosi o wejście na określoną stronę internetową w ramach testowania łącza internetowego.	1	2	2	<i>Procedura:</i> Szkolenia personelu, Regulamin ODO <i>Zabezpieczenie:</i> Dopuszczenie do użycia wyłącznie zakwalifikowanych pendrive
2.	Instalacja szkodliwego oprogramowania / działanie szkodliwego oprogramowania	Szkodliwe oprogramowanie (backdoory, exploity, exploitpaki, keyloggers). Najczęściej instalowane są poprzez otwarcie „zainfekowanego” załącznika z maila lub poprzez kliknięcie na zarażoną stronę. Maile takie zachęcają do otwarcia załącznika lub kliknięcia na hiperlink (mail z fakturą do opłacenia, mail z DHL o przesyłce, mail z rzekomym pismem urzędowym). W efekcie możemy zarazić nasz komputer lub wiele komputerów w sieci.	1	2	2	<i>Procedura:</i> Szkolenia personelu. Regulamin ODO <i>Zabezpieczenie:</i> Systemy antywirusowy i antyspamowy i blokada dostępu do określonych stron

		Działające szkodliwe oprogramowanie może wywołać różnorodne skutki: Przejęcie konta pocztowego do wysyłki spamu. Użycie przejętych komputerów do kopania kryptowalut. Użycie przejętych komputerów do ataków DOS. Użycie przejętych komputerów do śledzenia haseł użytkowników celem uzyskania dostępu.				
3.	Łamanie haseł Łatwo dostępne, łatwe lub standardowe hasła Ataki na sprzęt - włamania do urządzeń nieaktualizowanych	Intruz przedstawia się jako inżynier Microsoftu lub programista dostawcy oprogramowania. Podsyła „aktualizację” lub prosi o udostępnienie pulpitu Łamanie haseł metodami słownikowymi i siłowymi (brute force) : do baz danych, do serwera, do aplikacji www (np. do wordpressa) do poczty, do windows na stacjach roboczych, do routera, do firewalla. Ujawnianie haseł. Nieprawidłowe przechowywanie (karteczki, pliki) Stosowanie domyślnych haseł producenta Stosowanie słownikowych lub popularnych haseł, np. Grazynka1, qwerty, 12345678 Stosowanie jednego hasła do wielu (często wszystkich) systemów. Ataki na urządzenia sieciowe oraz inne, które działają dzięki umieszczonemu na nich oprogramowaniu (firmware / strowniki) Zagrożenie dla nast. elementów: routery, switchy, access pointy, firewall, macierz.	1	1	1	<i>Procedura:</i> Metody i środki uwierzytelnienia (polityka haseł). Szkolenia personelu, zabezpieczenia systemu informatycznego <i>Zabezpieczenia:</i> Testy penetracyjne długość hasła - 8 znaków. Hasło zawiera duże, małe litery cyfry lub znaki specjalne częstotliwość zmiany hasła – 30 dni, mechanizm wymuszenia zmiany hasła, uwierzytelnianie do aplikacji, stacji roboczych, dysku sieciowego sieci, poczty, smartfona
4.	Ataki na sprzęt - Włamania do urządzeń nieodpowiednio skonfigurowanych	Dysk NAS, drukarki i skanery Brak aktualizacji tego oprogramowania (firmware) skutkuje podatnością na włamania, kradzież danych, zakłócanie pracy. Ataki na błędnie skonfigurowany sprzęt lub sprzęt działający z ustawieniami fabrycznymi. Zagrożenie dla nast. elementów: routery, switchy, access pointy, firewall macierz, dyski NAS, drukarki i skanery Błędy konfiguracyjne popełniane przez administratorów mogą ułatwiać hackerom włamanie się do sieci lub urządzenia. Powodem jest	1	1	1	<i>Procedura:</i> Zabezpieczenia systemu informatycznego <i>Zabezpieczenia:</i> Zmiana domyślnych haseł na urządzeniach Zmiana domyślnej nazwy konta administratora w urządzeniu Testy penetracyjne

		najczęściej brak profesjonalnej wiedzy u osób konfigurujących urządzenia. Przykładem jest np. pozostawienie domyślnych haseł lub dostępu do strony konfiguracyjnej routera z poziomu Internetu.				
5.	Ataki na sprzęt - Włamania z użyciem niezabezpieczonych interfejsów lokalnych	Atakujący wpina się do urządzeń IT przez ich niezabezpieczone porty konfiguracyjne (USB, Ethernet lub COM - szeregowo) Zagrożenie dla nast. elementów: routery, switchy, firewalles, macierze, serwery drukarki i skanery Administratorzy często pozostawiają te porty niezabezpieczone, co powoduje ryzyko wpięcia się do powyższych urządzeń i ich skonfigurowania przez hakera.	1	1	1	<i>Procedura:</i> Zabezpieczenia systemu informatycznego <i>Zabezpieczenia:</i> Kontrola dostępu do pomieszczeń serwerowni i punktów dystrybucyjnych sieci. Testy penetracyjne.
6.	Ataki na sprzęt - Włamania za pośrednictwem niepotrzebnych usług (np. telnet na routerze)	Atakujący wykorzystuje do włamania usługi sieciowe, których działanie w danym środowisku nie jest wymagane Zagrożenie dla nast. Usług: DHCP, DNS, SSH, http, telnet, FTP, SMTP, SNMP. Urządzenia sieciowe posiadają często włączone wszystkie możliwe usługi sieciowe (DHCP, DNS, SSH, HTTP, telnet, FTP), mimo iż nie wszystkie z nich są potrzebne w danym środowisku. Każda z tych usług jest obsługiwana przez oprogramowanie, które może zawierać błędy.	1	1	1	<i>Procedura:</i> Wykonywania przeglądów i konserwacji Zabezpieczenia systemu informatycznego <i>Zabezpieczenia:</i> Wyłączenie niepotrzebnych serwisów (ogranicza ilość dziur i możliwość przechwycenia / podsłuchania ruchu lub haseł.) Włączone tylko te usługi, które są niezbędne do działania danego środowiska. Testy penetracyjne
7.	Ataki na oprogramowanie - Wykorzystanie znanych dziur w nieaktualizowanym oprogramowaniu	Atak z wykorzystaniem znanych dziur w niezaktualizowanym oprogramowaniu Zagrożenie dla programów Systemy operacyjne na stacjach roboczych Systemy serwerowe. Przeglądarki www, Wordpress, Drupal, <inne silniki webowe>, <sklepy internetowe>, Dedykowany CMS, Adobe, Java Istniejące błędy oprogramowania pozwalające na przełamanie zabezpieczeń są upubliczniane po tym, jak producent oprogramowania przygotowuje odpowiednią łatę lub aktualizację. Jeżeli nie	1	2	2	<i>Procedura:</i> Wykonywania przeglądów i konserwacji Procedura zabezpieczenia systemu informatycznego <i>Zabezpieczenia:</i> Wyłączenie niepotrzebnych serwisów (ogranicza ilość dziur i możliwość przechwycenia / podsłuchania ruchu lub haseł.) Włączone tylko te usługi, które są niezbędne do działania danego środowiska. Testy penetracyjne

		zainstalujemy tych aktualizacji, narażamy się na atak, np. zdalny dostęp do systemu lub wykonanie złośliwego kodu (instalacja backdoora, exploita, ransomware).				
8.	Podśluch	Podśluch danych przesłanych drogą mailową podśluch danych podczas korzystania z aplikacji webowych podśluch podczas korzystania z formularzy kontaktowych podśluch podczas zdalnego dostępu do sieci wewnętrznej przez Internet.	1	1	1	<i>Procedura:</i> Zabezpieczenia systemu informatycznego <i>Zabezpieczenia:</i> szyfrowanie poczty wysyłanej (SSL) szyfrowanie połączeń internetowych SSL/VPN szyfrowanie plików (7zip) wysyłanych mailowo Ograniczenie fizycznego dostępu do miejsc, gdzie znajdują się nienadzorowane gniazdka sieciowe. Testy penetracyjne
9.	Ataki na oprogramowanie - Włamanie z wykorzystaniem luk typu zero day"	Zero-day to błędy w oprogramowaniu, do których autor nie przygotował jeszcze poprawek / aktualizacji. Informacje o nich są sprzedawane i wykorzystywane przez intruzów.	1	1	1	<i>Procedura:</i> Zabezpieczenia systemu informatycznego <i>Zabezpieczenia:</i> Oprogramowanie antywirusowe Testy penetracyjne
10.	Ataki na oprogramowanie - Włamanie z wykorzystaniem najczęstszych błędów programistycznych	Programiści pisząc programowanie często popełniają te same, znane błędy. Przykładowo: możliwość wpisania ujemnej liczby sztuk w formularzu zamówienia, możliwość odgadnięcia numeru zamówienia innego klienta i wpisanie go w pasku adresu przeglądarki w celu wyświetlenia szczegółów.	1	1	1	<i>Procedura:</i> Procedura zabezpieczenia systemu informatycznego <i>Zabezpieczenia:</i> Testy penetracyjne
11.	Włamanie z wykorzystaniem API (interfejsów programistycznych)	Niektóre aplikacje pozwalają na zdalne zarządzanie nimi przez specjalnie zaprojektowane funkcje/usługi sieciowe. Np. baza danych może pozwalać na podłączenie się do niej administratorowi w celu wykonania prac naprawczych lub backupu. Dostęp ten odbywa się przy użyciu domyślnych loginów i haseł, co stanowi zagrożenie.	1	1	1	<i>Procedura:</i> Zabezpieczenia systemu informatycznego <i>Zabezpieczenia:</i> Zmiana domyślnych loginów i haseł Wyłączenie zdalnego dostępu, gdy nie jest wymagany Testy penetracyjne"
12.	Ataki na oprogramowanie - Namierzanie wersji testowych (np. strona www) Skanowanie sieci i usług	Niektóre aplikacje posiadają swoje kopie utrzymywane do celów testowych. Są one często gorzej zabezpieczone i łatwiej jest się do nich włamać, a mogą zawierać również krytyczne dane ze środowiska produkcyjnego. Przykładem może być kopia serwera wykonana w celu przetestowania nowej wersji aplikacji. Często udaje się je namierzyć wpisując np. zamiast	0	1	0	<i>Procedura:</i> Zabezpieczenia systemu informatycznego <i>Zabezpieczenia:</i> Zmiana domyślnych loginów i haseł Stosowanie tych samych zasad bezpieczeństwa, co do systemów produkcyjnych. Testy penetracyjne. Firewall, wyłączanie niepotrzebnych usług na urządzeniach sieciowych i serwerach"

		adresu www.strona.pl adres test.strona.pl . Udostępniane w Internecie serwery, urządzenia sieciowe i aplikacje oraz serwisy www mogą być namierzane przez intruzów poprzez skanowanie adresów IP. Polega to na próbach łączenia się z wszystkimi znanymi usługami w celu sprawdzenia, które z nich są dostępne w naszej sieci i w jakiej wersji. Dzięki temu możliwe jest znalezienie usług nieaktualnych i zawierających błędy.				
13.	Włamanie do sieci poprzez WIFI	Uzyskanie dostępu do sieci wewnętrznej poprzez włamanie się do sieci bezprzewodowej	1	1	1	<i>Procedura:</i> Zabezpieczenia systemu informatycznego <i>Zabezpieczenia:</i> Odseparowanie wifi dla gości/klientów od sieci wewnętrznej Stosowanie odpowiednich standardów szyfrowania Stosowanie mocnych haseł dostępowych
14.	Nieuprawniony dostęp do sieci z użyciem hakerskiego urządzenia	Możliwość wpięcia hakerskiego urządzenia do łatwo dostępnych urządzeń sieciowych wewnątrzorganizacyjnych, celem uzyskania dostępu do sieci przez to urządzenie z zewnątrz. Możliwość uruchomienia tzw. wrogiego access pointa w celu przechwycenia klientów sieci bezprzewodowej. Zagrożenie dla nast. elementów: gniazdka sieciowe w korytarzach, w sali konferencyjnej, skanery, drukarki na korytarzach switche w miejscach dostępnych	1	1	1	<i>Procedura:</i> Zabezpieczenia systemu informatycznego <i>Zabezpieczenia:</i> Okablowanie i elementy sieci są fizycznie zabezpieczone przed ingerencją osób postronnych
15.	Nieuprawniony dostęp lub włamanie do pomieszczeń"	Dostęp do: Budynków Pomieszczeń biurowych Archiwów Serwerowni Miejsc przechowywania kopii bezpieczeństwa Może skutkować: dostępem do danych w wersji papierowej dostępem do plików lub aplikacji lub baz danych zainstalowaniem nieautoryzowanych urządzeń do dostępu do sieci wewnętrznej kradzieżą komputerów, nośników				<i>Procedury:</i> Polityka kluczy, Kontrola dostępu <i>Zabezpieczenia:</i> kontrola kluczy zapasowych / kontrola wydawania kluczy / kontrola składowania kluczy, proceduralne ograniczenie dostępu do pomieszczeń osobom nieupoważnionym (zakaz wstępu), praca personelu sprząającego w godzinach pracy i w obecności osób upoważnionych, rozmieszczenie komputerów /drukarek /xero ograniczające dostęp osób nieupoważnionych, dostęp osób nieupoważnionych w obecności osoby upoważnionej, zabezpieczenie dostępu do pomieszczeń (drzwi zamykane na klucz), zabezpieczenie dostępu do

						archiwum (drzwi zamykane na klucz) zabezpieczenie dokumentacji / danych w pomieszczeniach - monitoring wizyjny w obrębie obiektu i otoczeniu
16.	Kradzież / zagubienie sprzętu i nośników poza organizacją"	Kradzież / zagubienie: laptopów smartfonów, pendrive dysków wymiennych	1	2	2	<i>Procedury:</i> Regulamin użytkowania komputerów przenośnych. Zabezpieczenia systemu informatycznego <i>Zabezpieczenia:</i> Szyfrowanie laptopów Stosowanie szyfrowanych dysków przenośnych Stosowanie szyfrowanych pendrive Uwierzytelnianie do urządzeń typu smartfon"
17.	Atak ransomeware	Ransomware - Program do szyfrowania plików. Instaluje się z maili lub z hiperlinków w mailach lub poprzez odwiedziny zainfekowanej strony. Są też znane przypadki infekcji poprzez sieć lokalną. Odszyfrowanie wymaga zapłaty np. 500 USD. Bardzo groźny"	1	1	1	<i>Procedura:</i> Zabezpieczenia systemu informatycznego Procedura tworzenia kopii zapasowych Szkolenia personelu. Regulamin ODO <i>Zabezpieczenia:</i> Systemy antywirusowy i antyspamowy. Kopie bezpieczeństwa kluczowych danych zabezpieczone, blokada dostępu do określonych stron
18.	ATAKI MAN- IN-THE- MIDDLE	Zmuszenie komputerów w sieci lokalnej do komunikowania się za pośrednictwem komputera intruza. Umożliwia przechwytywanie i podśluchiwanie ruchu w sieci.	1	1	1	<i>Procedura:</i> Procedura zabezpieczenia systemu informatycznego <i>Zabezpieczenia:</i> Systemy antywirusowe. Testy penetracyjne
19.	Eskalacja uprawnień	Zwiększenie uprawnień użytkownika przez wykorzystanie błędów programistycznych Przejęcie uprawnień użytkownika" zaawansowanego Przejęcie uprawnień administratora Przejęcie uprawnień systemowych Przejęcie innych poświadczeń (certyfikaty elektroniczne, pliki cookies z identyfikatorami sesji), wykorzystanie błędów programistycznych Przejęcie uprawnień użytkownika"	0	3	0	<i>Procedura:</i> Procedura nadawania uprawnień do przetwarzania danych osobowych Wykonywania przeglądów i konserwacji <i>Zabezpieczenia:</i> Regularny przegląd logów i uprawnień Monitorowanie logowania na konta administracyjne
20.	Atak DOS / DDOS	Atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania. Atak dotyczy głównie stron i aplikacji www. Np. wypełnienie i wysłanie kilka milionów razy formularza kontaktowego (za pomocą skryptu) i spowodowanie zapelnienia dysku. Zmasowany atak pojedynczego atakującego (DOS) lub z wielu komputerów jednocześnie	0	1	0	<i>Procedura:</i> Zabezpieczenia systemu informatycznego <i>Zabezpieczenia:</i> Firewall Mechanizm captcha (kod z obrazka do przepisania w formularzu) - do wdrożenia Testy penetracyjne

		(DDOS) na jakąś stronę www lub na portal, aby ją przeciążyć i „zakorkować”				
21.	Nieuprawniony dostęp do infrastruktury IT oraz do programów	Brak kontroli nad dostępem do serwera, plików, programów, komputerów nadane zbyt wysokie uprawnienia użytkownikom dostęp osób nieupoważnionych do kopii bezpieczeństwa łatwy dostęp osób nieupoważnionych do danych prezentowanych na monitorach, drukarkach, kserokopiarkach niezabezpieczona praca zdalna użytkowników lub serwisu IT	1	1	1	<i>Procedury:</i> Procedura nadawania uprawnień do przetwarzania danych osobowych, Szkolenia personelu Regulamin ODO Zabezpieczenia systemu informatycznego Wykonywanie przeglądów i konserwacji <i>Zabezpieczenia:</i> szyfrowanie baz danych, minimalizacja uprawnień, konta firmowe odseparowane od prywatnych dopuszczenie do użycia wyłącznie zakwalifikowanych pendrive praca terminalowa zabezpieczona VPN. uwierzytelnianie użytkowników z zewnątrz poprzez akceptację wybranych adresów IP, Ochrona przed utratą danych dla zapobiegania przypadkowym i złośliwym wyciekom istotnych danych, takich jak informacje o klientach, dane finansowe, własność intelektualna lub tajemnice handlowe. Identyfikowanie, śledzenie i zabezpieczanie wszystkich poufnych informacji: przechowywanych, używanych, a także przesyłanych . Oświadczenia poufności, zahasłowane wygaszacze ekranu aktywowane po ustalonych przez ADO minutach nieaktywności użytkownika, ustawienie monitorów uniemożliwiających wgląd w dane osób postronnych, polityka czystego ekranu, filtry polaryzacyjne na monitorach (opcjonalnie)
22.	Udostępnianie danych osobom nieupoważnionym z sieci publicznej (przez Internet)	Dostęp do danych osobowych poprzez stronę www bez logowania się dostęp do danych osobowych poprzez stronę www po zalogowaniu się (użytkownik może przeglądać dane osobowe innych użytkowników) dostęp do katalogów udostępnionych pod publicznym adresem IP plików z danymi osobowymi lub kopii bezpieczeństwa (bez logowania się), udostępnianie plików zaindeksowanych przez roboty google na skutek braku komend chroniących katalogi webowe przez taką indeksacją	1	1	1	<i>Procedura</i> Wykonywania przeglądów i konserwacji Regulamin ODO <i>Zabezpieczenia</i> Uwierzytelnianie dostępu do zasobów Testy penetracyjne

		przesłanie lub wydawanie informacji osobie nieupoważnionej				
23.	Awaria / uszkodzenia elementów IT	Awarie: dysków, stacji roboczych, urządzeń sieciowych /routerów, drukarek / skanerów, serwera"	1	2	2	<i>Procedury:</i> Procedura wykonywania przeglądów i konserwacji <i>Zabezpieczenia:</i> polityka kopii, macierz, inwentaryzacji sprzętu zarządzanie licencjami, plan ciągłości działania
24.	Błąd / awaria oprogramowania	Awarie: programu kadrowo-płacowego, poczty aplikacji www (np. wordpressa), bazy danych	1	2	2	<i>Procedury:</i> Wykonywanie przeglądów i konserwacji <i>Zabezpieczenia techniczne</i> <i>Zabezpieczenia:</i> polityka kopii
25.	Pożar / eksplozja	Pożar obiektu Pożar serwerowni Pożar serwera Zniszczenie serwerowni (np. wybuch gazów technicznych)	0	1	0	<i>Procedury:</i> <i>Zabezpieczenia techniczne</i> <i>Zabezpieczenia:</i> gaśnice
26.	Zalanie	Zalanie archiwum (powódź, zalanie z rur)	0	0	0	<i>Procedury:</i> <i>Zabezpieczenia techniczne</i> <i>Zabezpieczenia:</i> składowanie dokumentacji papierowej na podwyższeniu digitalizacja dokumentów archiwalnych
27.	Przegrzanie / zbyt duża wilgotność	wysoka temperatura w serwerowni, wysoka wilgotność w archiwum	0	1	0	<i>Procedury:</i> <i>Zabezpieczenia techniczne</i> <i>Zabezpieczenia:</i> klimatyzacja
28.	Awaria zasilania	skoki napięcia, przerwy w dostawie zasilania	1	2	2	<i>Procedury:</i> <i>Zabezpieczenia techniczne</i> <i>Zabezpieczenia:</i> sieć stabilizowana UPS podtrzymujący zasilanie serwera UPS na kluczowych elementach systemu IT
29.	Nieuprawniona modyfikacja / usunięcie	Niezamierzone lub pomyłkowe zmodyfikowanie / usunięcie danych sfalszowanie danych przez osoby z wewnątrz lub zewnątrz organizacji	1	2	2	<i>Procedury:</i> <i>Zabezpieczenia systemu informatycznego</i> <i>Zabezpieczenia:</i> Rozliczalność operacji kluczowe programy/systemy logują operacje tworzenia, zmiany, usuwania rekordu, wglądu w dane, eksportu danych każdy użytkownik programu/systemu posiada swój indywidualny login

30.	Nieuprawnione kopiowanie danych	Kopiowanie danych z katalogów, dysków, baz, programów kserowanie i robienie zdjęć przez pracownika lub przez osobę obcą	1	1	1	<i>Procedury:</i> Zabezpieczenia systemu informatycznego Regulamin ODO <i>Zabezpieczenia:</i> Rozliczalność operacji kluczowe programy/systemy logują operacje tworzenia, zmiany, usuwania rekordu, wglądu w dane, eksportu danych każdy użytkownik programu/systemu posiada swój indywidualny login Blokada funkcji eksportu danych w kluczowych programach / systemach
31..	Brak / błędy w wykonywaniu kopii bezpieczeństwa	Doraźne lub za rzadkie wykonywanie kopii błędy podczas procesu wykonywania kopi niemożność odtworzenia kopii ze względu na zmiany w oprogramowaniu	1	2	2	<i>Procedury:</i> Procedura tworzenia kopii zapasowych <i>Zabezpieczenia:</i> Wirtualizacja kopii wykonywany jest backup serwerów / aplikacji / plików / konfiguracji / licencji /hasła backup jest zabezpieczony przed ransomware testowanie możliwości odtworzenia kopii niszczenie/czyszczenie nośników przed utylizacją
32.	Nieprawidłowe / brak procedur niszczenia nośników z danymi – Nieprawidłowe / brak procedur napraw w serwisach zewnętrznych	Wyrzucenie uszkodzonych nośników bez ich zniszczenia, wyrzucanie dokumentów papierowych na śmietnik lub pozostawienie dokumentów w miejscu publicznym, wyrzucenie niezniszczonych , HD, pendrive, DVD, naprawa sprzętu z nośnikami bez umowy lub bez standardu bezpiecznej naprawy, wyrzucanie dokumentów papierowych na śmietnik lub pozostawienie dokumentów w miejscu publicznym, wyrzucenie niezniszczonych , HD, pendrive, DVD	0	2	0	<i>Procedury:</i> Utylizacja elektronicznych nośników i wydruków oraz czyszczenie danych <i>Zabezpieczenia:</i> niszczarki paskowe, niszczarki o podwyższonym standardzie niszczenie/czyszczenie nośników przed utylizacją firma niszcząca dokumenty"
33.	Nieprzestrzeganie procedur	Świadome naruszenie pisemnych lub ustnych procedur np. niewylogowywanie się z systemu, przekazywanie haseł osobom nieupoważnionym, naruszenie polityki czystego ekranu lub czystego biurka naruszenia powyżej wskazane na skutek braków w inteligencji lub z powodów niewiedzy	1	2	2	<i>Procedury:</i> Szkolenia personelu Regulamin ODO

34.	Pomyłki i błędy administratorów , użytkowników	Udostępnienia katalogów i dysków, serwerów ftp, aplikacji z danymi do powszechnego dostępu przez sieć publiczną –z powodu „ułatwienia pracy” administratorów systemów łatwe logowanie się do baz i programów „login admin, hasło admin1” dostęp do programów testowych (z prawdziwymi danymi osobowymi) bez logowania pomyłkowe udostępnienie, wysłanie do złego odbiorcy, błędne zabezpieczenia	1	2	2	<i>Procedury:</i> Procedura zabezpieczenia systemu informatycznego Szkolenia personelu Regulamin ODO
35.	Brak aktualnej dokumentacji (instrukcji, opisów, dokumentacji technicznej sprzętu i oprogramowania a)	Brak instrukcji, opisów, dokumentacji technicznej sprzętu i oprogramowania Brak instrukcji instalacyjnych i konfiguracyjnych środowiska lub oprogramowania Zagrożenie związane z możliwymi trudnościami w odtworzeniu środowiska i zarządzania nim, gdy np. odejdzie pracownik IT lub będzie on niedostępny podczas krytycznej awarii	1	2	2	Bieżące monitorowanie aktualnej dokumentacji
36.	Nieprawidłowe / brak umowy o współpracy	Nieprecyzyjnie określone odpowiedzialności we współpracy, co stwarza ryzyko braku zabezpieczeń	1	1	1	<i>Zabezpieczenia:</i> Umowa powierzenia Pisemne upoważnienia dla podmiotu współpracującego z jasnymi warunkami bezpiecznej pracy z danymi powierzonymi
37.	Nieprawidłowe / brak umowy gwarancyjnej lub wsparcia serwisowego	Należy uwzględnić, że umowy wymagają przedłużania, czas reakcji nie oznacza czasu naprawy	1	1	1	<i>Zabezpieczenie</i> stosowane są Umowy powierzenia. W umowach stosuje się kary umowne za niewywiązywanie się z realizacji umów. Stosowana jest Procedura napraw w serwisach zewnętrznych.
38.	Upadek firmy outsourcingowej lub dostawczej	Brak zastępstw, np. dla hostingodawcy poczty, dla wsparcia do zakupionej aplikacji Utrata usługi / aplikacji, którą świadczy pomiot przetwarzający	1	1	1	<i>Zabezpieczenie:</i> Redundancja firmy / osoby"
39.	Awaria łączy telekomunikacyjnych	Krytyczne dla administratora świadczącego usługi wymagające „internetu”, usługi chmurowe, ISP oraz dostawcy platform SaaS	1	1	1	Redundancja łączy

WARTOŚĆ [R = P*S]	
ryzyko pomijalne i akceptowalne (akceptujemy)	1-2
ryzyko jest opcjonalne (akceptujemy albo obniżamy)	3-6
ryzyko jest nieakceptowalne (musimy obniżyć)	9

INSTRUKCJA
ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM
W ZESPOLE SZKOŁ SPECJALNYCH W ŚCINAWCE DOLNEJ

I. Nadawanie i rejestrowanie uprawnień do przetwarzania danych w systemie informatycznym

1. Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych w Szkole.
2. Za tworzenie, modyfikację i nadawanie uprawnień kontom użytkowników odpowiada Administrator.
3. Usuwanie kont stosowane jest wyłącznie w uzasadnionych przypadkach, standardowo, przy ustaniu potrzeby utrzymywania konta danego użytkownika ulega ono dezaktywacji w celu zachowania historii jego aktywności.
4. Osoby dopuszczone do przetwarzania danych osobowych zobowiązane są do zachowania tajemnicy w zakresie tych danych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje również po ustaniu stosunku pracy, co jest równoznaczne z cofnięciem uprawnień do przetwarzania danych osobowych.

II. Zabezpieczenie danych w systemie informatycznym

1. Oprogramowanie wykorzystywane do przetwarzania danych posiada własny system kont (zabezpieczonych hasłami) i uprawnień. Zmiana hasła jest wymuszona automatycznie przez system.
2. W przypadku utracenia hasła użytkownik ma obowiązek skontaktować się z Administratorem celem uzyskania nowego hasła.
3. System informatyczny przetwarzający dane osobowe musi posiadać mechanizmy pozwalające na odnotowanie faktu wykonania operacji na danych. W szczególności zapis ten powinien obejmować:
 - a) rozpoczęcie i zakończenie pracy przez użytkownika systemu,
 - b) operacje wykonywane na przetwarzanych danych,
 - c) przesyłanie za pośrednictwem systemu danych osobowych przetwarzanych w systemie informatycznym innym podmiotom nie będącym właścicielem ani współwłaścicielem systemu,
 - d) nieudane próby dostępu do systemu informatycznego przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych,
 - e) błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.

4. System informatyczny powinien zapewnić zapis faktu przekazania danych osobowych z uwzględnieniem:
 - a) identyfikatora osoby, której dane dotyczą,
 - b) osoby przesyłającej dane,
 - c) odbiorcy danych,
 - d) zakresu przekazanych danych osobowych,
 - e) daty operacji,
 - f) sposobu przekazania danych.
5. Stosuje się aktywną ochronę antywirusową lub w przypadku braku takiej możliwości przynajmniej raz w tygodniu skanowanie całego systemu (w poszukiwaniu „złośliwego oprogramowania”) na każdym komputerze, na którym przetwarzane są dane osobowe.
6. Za dokonywanie skanowania systemu w poszukiwaniu złośliwego oprogramowania (w przypadku braku ochrony rezydentnej) i aktualizację bazy wirusów odpowiada użytkownik stacji roboczej.

III. Zasady bezpieczeństwa podczas pracy w systemie informatycznym

1. W celu rozpoczęcia pracy w systemie informatycznym użytkownik:
 - 1) loguje się do systemu operacyjnego przy pomocy identyfikatora i hasła (autoryzacja użytkownika w bazie usług katalogowych),
 - 2) loguje się do programów i systemów wymagających dodatkowego wprowadzenia unikalnego identyfikatora i hasła.
2. W sytuacji tymczasowego zaprzestania pracy na skutek nieobecności przy stanowisku komputerowym należy uniemożliwić osobom postronnym korzystanie z systemu informatycznego poprzez wylogowanie się z systemu lub uruchomienie wygaszacza ekranu chronionego hasłem.
3. W sytuacji gdy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba należy tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor (przymknąć ekran laptopa) w sposób uniemożliwiający wgląd w wyświetlaną treść.
4. Użytkownik wyrejestrowuje się z systemu informatycznego przed wyłączeniem stacji komputerowej poprzez zamknięcie programu przetwarzającego dane oraz wylogowanie się z systemu operacyjnego.
5. Zawieszenie korzystania z systemu informatycznego może nastąpić losowo wskutek awarii lub planowo (np. w celu konserwacji sprzętu). Planowe zawieszenie prac jest poprzedzone poinformowaniem pracowników Szkoły przez ASI na co najmniej 30 minut przed planowanym zawieszeniem.
6. Pracownik korzystający z systemu informatycznego zobowiązany jest do powiadomienia Administratora w razie:

- a) podejrzenia naruszenia bezpieczeństwa systemu;
 - b) braku możliwości zalogowania się użytkownika na jego konto;
 - c) stwierdzenia fizycznej ingerencji w przetwarzane dane;
 - d) stwierdzenia użytkownika narzędzia programowego lub sprzętowego.
7. Na fakt naruszenia zabezpieczeń systemu mogą wskazywać:
- a) nietypowy stan stacji roboczej (np. brak zasilania, problemy z uruchomieniem);
 - b) wszelkiego rodzaju różnice w funkcjonowaniu systemu (np. komunikaty informujące o błędach, brak dostępu do funkcji systemu, nieprawidłowości w wykonywanych operacjach);
 - c) różnice w zawartości zbioru danych osobowych (np. brak lub nadmiar danych);
 - d) inne nadzwyczajne sytuacje.

IV. Tworzenie kopii zapasowych

1. Pełne kopie zapasowe zbiorów danych tworzone są 4 razy w ciągu roku. W szczególnych sytuacjach, np. przed aktualizacją lub zmianą oprogramowania lub systemu należy wykonać bezwzględnie pełną kopię zapasową systemu.
2. Odpowiedzialnym za wykonanie kopii danych i kopii awaryjnych jest pracownik obsługujący dany program przetwarzający dane.
3. Kopie przechowywane są w szafie metalowej w gabinecie dyrektora Szkoły.
4. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu. Okresową weryfikację kopii bezpieczeństwa pod kątem ich przydatności do odtworzenia danych przeprowadza Administrator.
5. Usuwanie kopii danych następuje poprzez bezpieczne kasowanie. Nośniki danych, na których zapisywane są kopie bezpieczeństwa niszczy się trwale w sposób mechaniczny.

V. Przeglądy i konserwacje systemów

1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe mogą być wykonywane wyłącznie przez pracowników Szkoły lub przez upoważnionych przedstawicieli wykonawców.
2. Prace wymienione w pkt 1 powinny uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.
3. Przed rozpoczęciem prac wymienionych w pkt 1 przez osoby niebędące pracownikami Szkoły należy dokonać potwierdzenia tożsamości tychże osób.

VI. Niszczenie wydruków i nośników danych

1. Wszelkie wydruki z systemów informatycznych zawierające dane osobowe przechowywane są w miejscu uniemożliwiającym ich odczyt przez osoby nieuprawnione, w zamkniętych szafach lub pomieszczeniach i po upływie ich

przydatności są niszczone przy użyciu niszczarek / w sposób uniemożliwiający ich odczytanie (pocięte w poprzeczne paski).

2. Niszczenie zapisów na nośnikach danych powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika.
3. Uszkodzone nośniki danych przed ich wyrzuceniem należy fizycznie zniszczyć w niszczarce.

**ZASADY POSTĘPOWANIA
W PRZYPADKU WYKRYCIA NARUSZENIA OCHRONY DANYCH OSOBOWYCH
PRZETWARZANYCH W ZESPOLE SZKÓŁ SPECJALNYCH W ŚCINAWCE
DOLNEJ**

1. Cel

W niniejszym dokumencie ustalone zostały zasady analizowania przypadków dotyczących naruszenia ochrony danych osobowych oraz sposób postępowania przy zgłaszaniu naruszenia ochrony danych osobowych w myśl przepisów art. 33 i art. 34 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 (Dz. Urz. UE L 119/1, z 4 maja 2016 r.).

2. Definicje

Ileokroć w niniejszej instrukcji zostanie użyte pojęcie:

- 1) Szkołę – należy przez to rozumieć Zespół Szkół Specjalnych w Ścinawce Dolnej;
- 2) Dyrektor – należy przez to rozumieć Dyrektora Szkoły;
- 3) RODO – należy przez to rozumieć 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 (Dz. Urz. UE L 119/1, z 4 maja 2016 r.);
- 4) dane osobowe – należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
- 5) naruszenie ochrony danych osobowych – należy przez to rozumieć, każdą sytuację która jest wynikiem zdarzeń losowych lub działania sił natury bądź nieumyślnego lub celowego działania człowieka i powoduje lub może spowodować zagrożenie bezpieczeństwa danych osobowych przetwarzanych w Szkole;

3. Zakres stosowania

Instrukcja obowiązuje wszystkich pracowników Szkoły i dotyczy zidentyfikowanych przypadków zagrażających bezpieczeństwu danych osobowych przetwarzanych w Szkole, zarówno w formie papierowej, jaki i przy wykorzystaniu systemów teleinformatycznych.

4. Odpowiedzialność

- 1) Każda osoba zatrudniona w Szkole lub wykonująca prace na rzecz Szkoły (stażysta, praktykant, przedstawiciel podmiotu zewnętrznego współpracujący ze Szkołą) jest zobowiązana do niezwłocznego zgłoszenia faktu wykrycia przypadków mających znaczenie dla prawidłowego funkcjonowania Szkoły.
- 2) Obsługę zgłoszonych przypadków związanych z naruszeniem bezpieczeństwa danych osobowych zapewnia dyrektor szkoły.
- 3) Punkt kontaktowy do zgłaszania przypadków związanych z naruszeniem bezpieczeństwa danych osobowych:
 - gabinet dyrektora szkoły
 - tel. 74/ 873 61 06 kom. 505 621 525
 - adres e-mail: zetspec.dyr@gmail.com

5. Tryb postępowania

5.1. Wykrycie sytuacji naruszenia bezpieczeństwa danych osobowych.

- 1) Sytuacje, które będą związane z naruszeniem bezpieczeństwa danych osobowych odnoszą się do:
 - utraty danych (kradzież, zgubienie, zniszczenie danych),
 - przekazania danych osobie lub podmiotowi nieuprawnionemu na skutek działania umyślnego lub w wyniku błędu pracowników lub współpracowników Szkoły.
- 2) W przypadku wykrycia naruszenia bezpieczeństwa danych osobowych należy, o ile istnieje taka możliwość, niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, oraz uwzględnić w działaniu również ustalenie przyczyn lub sprawców. W szczególności należy:
 - rozważyć wstrzymanie bieżącej pracy w celu zabezpieczenia miejsca zdarzenia (wylogować się z systemu, wyłączyć urządzenie);
 - zaniechać, o ile to możliwe, dalszych działań, które wiążą się z zaistniałą sytuacją i mogą utrudnić jej udokumentowanie i późniejszą analizę;
 - w zależności od okoliczności zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałej sytuacji (np. zasady BHP, ewakuacja z budynku, procedury ppoż.),
 - poinformować Dyrektora Szkoły wg zasad określonych w niniejszym dokumencie.

5.2. Zgłaszanie sytuacji naruszenia bezpieczeństwa danych osobowych.

- 1) Z uwagi na wymogi wynikające z RODO, w tym krótki okres na zgłoszenie naruszenia bezpieczeństwa danych osobowych (72 godziny od stwierdzenia/wykrycia naruszenia) informacje w tym zakresie muszą być

przekazywane przez osoby, które zidentyfikowały zagrożenie, bez zbędnej zwłoki.

- 2) Wykrycia naruszenia lub podejrzenie wystąpienia zdarzenia, które może mieć wpływ na bezpieczeństwo przetwarzanych danych należy zgłosić do Dyrektora Szkoły.
- 3) Zgłoszenie musi zawierać miejsce wystąpienia naruszenia bezpieczeństwa danych osobowych oraz, w miarę możliwości, jego krótki opis.

5.3. Analiza przypadków naruszenia bezpieczeństwa danych osobowych.

- 1) Każdy zgłoszony przypadek musi zostać poddany analizie, w zakresie ustalenia czy faktycznie doszło do naruszenia bezpieczeństwa danych osobowych, a w szczególności analiza powinna dać możliwość ustalenia czy doszło do naruszenia bezpieczeństwa danych osobowych, które może skutkować ryzykiem naruszenia praw i wolności osób, np. jeśli naruszenie może prowadzić do kradzieży lub fałszowania tożsamości, straty finansowej, naruszenia dobrego imienia czy też naruszenia tajemnic prawnie chronionych.
- 2) W trakcie analizy należy brać pod uwagę następujące elementy:
 - wdrożone zabezpieczenia i ich funkcjonowanie (potwierdzenie ich skuteczności),
 - zapisy (logi systemowe/rejestry) systemu teleinformatycznego, jeśli zachodzi podejrzenie utraty poufności przetwarzanych danych (np. kradzież danych z bazy),
 - poprawność funkcjonowania systemu – bazy danych jeśli zachodzi podejrzenie utraty integralności przetwarzanych danych (np. uszkodzenie bazy danych),
 - zapisy (logi systemowe/nagrania/rejestry) systemów zabezpieczeń wspomagających ochronę systemów teleinformatycznych oraz przetwarzanych danych, jeśli zachodzi podejrzenie nieautoryzowanego dostępu do danych.
- 3) Analiza przeprowadzana jest przez Dyrektora Szkoły.

5.4. Zawiadomienie organu nadzorczego o sytuacji naruszenia bezpieczeństwa danych osobowych.

- 1) Jeżeli przeprowadzona analiza, o której mowa w podrozdziale 5.3 wskazuje na naruszenie bezpieczeństwa danych osobowych, które może skutkować ryzykiem naruszenia praw i wolności osób, informacja o tym zdarzeniu jest kierowana do Urzędu Ochrony Danych Osobowych.
- 2) Zgłoszenia naruszenia bezpieczeństwa danych osobowych dokonywane jest w sposób określony przez organ nadzorczy nie później niż 72 godziny od stwierdzenia (wykrycia) zdarzenia.
- 3) Jeżeli zgłoszenie naruszenia bezpieczeństwa danych osobowych dokonane zostanie po upływie 72 godzin od stwierdzenia (wykrycia) zdarzenia, musi ono zawierać wyjaśnienie przyczyn opóźnienia.
- 4) Zgłoszenia naruszenia bezpieczeństwa danych osobowych dokonuje Dyrektor Szkoły.

5.5. Zawiadomienie osoby której dane dotyczą o sytuacji naruszenia bezpieczeństwa jej danych osobowych.

- 1) Jeżeli przeprowadzona analiza, o której mowa w podrozdziale 5.3 wskazuje na naruszenie bezpieczeństwa danych osobowych, które może skutkować wysokim ryzykiem naruszenia praw i wolności osób, informacja o tym zdarzeniu jest kierowana bez zbędnej zwłoki do osób których dane dotyczą.
- 2) Zawiadomienia o naruszeniu, powinno zawierać opis jego charakteru naruszenia, możliwe konsekwencje dla osób których dane dotyczą oraz możliwe do zastosowania środki zalecane w celu poradzenia sobie z naruszeniem i zminimalizowania jego negatywnych skutków.
- 3) Zawiadomienia o naruszeniu powinno zostać przekazane zainteresowanym osobom, biorąc pod uwagę dostępne kanały komunikacji z nimi oraz koszty wysyłki korespondencji np. z uwagi na liczbę osób objętych zawiadomieniem:
 - na adres e-mail (jeśli znany),
 - telefonicznie (jeśli znany nr telefonu),
 - listownie (jeśli znany adres).
- 4) Zawiadomienie w formie, o której mowa w pkt 2, nie jest wymagane, jeśli:
 - w celu zabezpieczenia danych wprowadzone zostały w Szkole rozwiązania uniemożliwiające odczyt osobom nieuprawnionym dostępu do tych danych (np. zaszyfrowanie danych),
 - zostały wprowadzone środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw i wolności osób.
- 5) Bezpośrednie zawiadomienie nie jest również wymagane, jeśli podawałoby to poniesienie niewspółmiernie dużych nakładów pracy i środków finansowych ze strony Szkoły.
- 6) W przypadku zaistnienia sytuacji, o której mowa w pkt 5, należy wydać publiczny komunikat (informacja na stronie Biuletynu Informacji Publicznej Szkoły, jednorazowe ogłoszenie w dzienniku o zasięgu regionalnym).

5.6. Usuwanie naruszenia bezpieczeństwa danych osobowych

- 1) W usuwanie naruszenia bezpieczeństwa danych osobowych zaangażowani są pracownicy Szkoły, którzy w ramach powierzonych obowiązków zapewniają i nadzorują funkcjonowanie systemu zabezpieczeń danych osobowych.
- 2) Po wykryciu naruszenia bezpieczeństwa danych osobowych analizowane są okoliczności związane z jego wystąpieniem oraz ustalany jest sposób rozwiązania problemu oraz, jeśli to konieczne, zabezpieczeniu materiału dowodowego.
- 3) W przypadku gdy problem może zostać rozwiązany samodzielnie przez pracowników Szkoły, należy to wykonać bez zbędnej zwłoki.
- 4) W przypadku konieczności wykonania działań przez podmiot zewnętrzny, pracownik zajmujący się rozwiązaniem problemu powinien, używając ustalonych

metod, poinformować o zdarzeniu ten podmiot, oraz razem z jej przedstawicielem uczestniczyć w rozwiązywaniu problemu.

- 5) W przypadku wykrycia działań umyślnych pracownik odpowiedzialny za obsługę naruszenia bezpieczeństwa danych osobowych przekazuje wyniki analizy, wraz z zabezpieczonym materiałem dowodowym, Dyrektorowi w celu wyciągnięcia konsekwencji dyscyplinarnych wobec pracownika Szkoły lub podjęcia kroków prawnych wobec osób trzecich.
- 6) Po przywróceniu prawidłowego stanu bezpieczeństwa danych osobowych należy przeprowadzić analizę w celu określenia przyczyny naruszenia oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
- 7) Jeżeli przyczyną naruszenia bezpieczeństwa danych osobowych:
 - był błąd osoby przetwarzającej dane, w szczególności użytkownika systemu teleinformatycznego, można przeprowadzić dodatkowe szkolenie lub przesłać stosowną informację do wszystkich użytkowników systemu o sposobie postępowania przy przetwarzaniu danych osobowych oraz zapewnieniu ich bezpieczeństwa;
 - było uaktywnienie złośliwego kodu, należy ustalić źródło jego pochodzenia oraz wykonać zabezpieczenia antywirusowe;
 - było zaniedbanie ze strony osoby zatrudnionej przy przetwarzaniu danych osobowych, należy wyciągnąć konsekwencje służbowe;
 - było włamanie lub uszkodzenie systemu zabezpieczeń w celu pozyskania danych osobowych, należy dokonać szczegółowej analizy wdrożonych środków zabezpieczających w celu zapewnienia skuteczniejszej ochrony danych osobowych;
 - był zły stan urządzeń lub sposób działania oprogramowania, należy niezwłocznie przeprowadzić kontrolne czynności serwisowe.
- 8) Do celów dowodowych, naruszenie bezpieczeństwa danych osobowych może zostać dodatkowo szczegółowo udokumentowane.

ZAWIADOMIENIE O NARUSZENIU DANYCH OSOBOWYCH

Informuję, że w wyniku w dniu doszło do naruszenia
Pani/Pana danych osobowych w zakresie ujawnienia (wskazać rodzaj danych osobowych):

-

-

-

Naruszenie zostało spowodowane (włamaniem i kradzieżą danych z bazy/
nieprawidłowym przesłaniem danych przez pracownika/)

W związku z powyższym istnieje duże ryzyko kradzieży lub sfalszowania Pani/Pana tożsamości, co
może spowodować stratę finansową lub utratę dobrego imienia w przypadku wykorzystania tych
danych przez osoby nieuprawnione w sposób niezgodny z prawem.

Informacja dotycząca kradzieży danych została zgłoszona do organów ścigania

W celu zminimalizowania negatywnych skutków tego naruszenia należy zastrzec dowód
tożsamości/zmienić hasło/.....

Dodatkowe informacje w tym zakresie można uzyskać:

- pod nr telefonu

- wysyłając zapytanie na adres e-mail:

.....

podpis Dyrektora

RAPORT O NARUSZENIU DANYCH OSOBOWYCH

1. Opis naruszenia ochrony danych osobowych

W dniu zidentyfikowano naruszenie ochrony danych osobowych w zakresie ujawnienia (wskazać rodzaj danych osobowych):

-

-

-

2. Kategoria i przybliżona liczba osób/wpisów danych których dotyczy naruszenie

.....

.....

.....

3. Możliwe konsekwencje naruszenia ochrony danych osobowych

.....

.....

.....

4. Opis środków zastosowanych lub proponowanych do zastosowania w celu zaradzenia naruszeniu ochrony danych osobowych

.....

.....

.....

.....

Podpis Dyrektora

KARTA KONTROLI WEWNĘTRZNEJ

Nazwa Administratora Danych Osobowych:(nazwa i siedziba szkoły)

Data przeprowadzonej kontroli wewnętrznej:.....

KONTROLA WEWNĘTRZNA – PODSTAWOWE ZAGADNIENIA			
Lp.	Zagadnienie	Tak	Nie
1	Czy wszyscy pracownicy przetwarzający dane osobowe posiadają odpowiednie upoważnienia?		
2	Czy prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych?		
3	Czy wyznaczono Administratora Systemu Informatycznego (o ile nadzór nad przestrzeganiem zasad ochrony danych osobowych nie jest sprawowany przez dyrektora osobiście)?		
4	Czy zawarto umowy powierzenia przetwarzania danych osobowych z podmiotami, którym powierzono przetwarzanie danych osobowych?		
5	Czy wprowadzono zabezpieczenia w zakresie zabezpieczenia danych osobowych odpowiednie do zagrożeń oraz kategorii danych będących przedmiotem ochrony ¹ ?		
6	Czy w każdym przypadku, w którym dane osobowe przekazywane są podmiotom trzecim, istnieje do tego podstawa prawna?		
7	Czy istnieje podstawa prawna do przetwarzania każdej kategorii danych osobowych pobieranych przez szkoły?		
8	Czy dane przetwarzane są zgodnie z celem, dla którego zostały zebrane?		
9	Czy osobom, których dane są przetwarzane, zapewnia się możliwość korzystania z uprawnień (prawo do kontroli, uzupełniania i prostowania przetwarzanych danych)?		
10	Czy sporządzono dokumentację opisującą przetwarzanie danych osobowych, tj.: Polityka Ochrony Danych Osobowych przetwarzanych w Zespole Szkół Specjalnych w Ścinawce Dolnej ?		
11	Czy urządzenia i systemy informatyczne, w których przetwarzane są dane osobowe, spełniają wymagania rozporządzenia, a szczególnie ² : • każdy użytkownik ma swój identyfikator i hasło; • hasło służące do uwierzytelniania użytkowników składa się co najmniej z 8 znaków i zawiera małe i wielkie litery oraz cyfry lub znaki specjalne oraz jego zmiana jest dokonywana nie rzadziej niż co 30 dni; • system chroniony jest przed zagrożeniami pochodzącymi z sieci publicznej (wirusami, tzw. trojanami)?		
12.	Inne:		

¹* Ustalenie, jakie zabezpieczenia należy zastosować i czy spełniają swoją rolę, jest kwestią cenną i wymaga każdorazowej ewaluacji okoliczności i warunków, w których przetwarzane są dane osobowe.

²*Ze względu na obszerność wymagań stawianych przez rozporządzenie wskazano jedynie podstawowe obowiązki. Wskazane jest, by weryfikacja, czy system teleinformatyczny spełnia wszystkie wymagania, została dokonana wspólnie z informatykiem.

Wnioski z przeprowadzonej kontroli wewnętrznej:.....

.....

.....

Zalecenia:.....

.....

.....

.....
Data, podpis, pieczęć osoby przeprowadzającej kontrolę

**REGULAMIN
KORZYSTANIA ZE SŁUŻBOWEJ POCZTY ELEKTRONICZNEJ
Zespołu Szkół Specjalnych w Ścinawce Dolnej**

**ROZDZIAŁ I
Postanowienia ogólne**

§1

1. Regulamin niniejszy ustala zasady korzystania ze służbowej poczty elektronicznej w Zespole Szkół Specjalnych w Ścinawce Dolnej

2. Dyrektor Zespołu Szkół Specjalnych w Ścinawce Dolnej określa w niniejszym regulaminie zasady udostępniania kont pocztowych w ramach systemu służbowej poczty elektronicznej.

3. Regulamin określa:

- 1) procedurę nadania pracownikowi adresu służbowej poczty elektronicznej oraz zasady stosowania hasła;
- 2) zakres czynności, jakie pracownik ma obowiązek wykonywać za pośrednictwem poczty elektronicznej;
- 3) sposób i zakres kontroli pracodawcy nad służbową pocztą pracowników.

§2

1. Nadzór i opiekę techniczną nad systemem służbowej poczty elektronicznej sprawuje Dyrektor Zespołu Szkół Specjalnych w Ścinawce Dolnej, lub wyznaczony przez niego Administrator Systemu Informatycznego.

ROZDZIAŁ II

Zasady korzystania ze służbowej poczty elektronicznej przez pracownika

§3

1. Każdy nauczyciel oraz pracownicy administracyjno-biurowi otrzymują od dyrektora szkoły adres służbowej skrzynki poczty elektronicznej.

2. Adres skrzynki pocztowej zostanie utworzony zgodnie z następującym wzorcem:
zetspec. inicjał imienia i nazwiska lub stanowiska pracy @gmail.com

3. Dyrektor lub osoba upoważniona przez Dyrektora, przekaze pracownikowi szczegóły dotyczące pierwszego logowania oraz tymczasowe hasło do służbowej poczty elektronicznej pracownika.

4. Dostęp do konta pocztowego jest chroniony hasłem i z uwagi na bezpieczeństwo systemu pocztowego oraz danych Użytkownika hasło musi być tajne, to znaczy znane wyłącznie Użytkownikowi. W przypadku odtajnienia hasła należy niezwłocznie zmienić je na nowe.

5. Przy pierwszym logowaniu pracownik zobowiązany jest zmienić hasło. Hasło nie powinno być zbyt proste lub oczywiste do odgadnięcia przez osoby trzecie. Powinno ono spełniać warunki:

- a) zawierać co najmniej 8 znaków,
- b) zawierać wielkie i małe litery,
- c) zawierać co najmniej 1 cyfrę lub znak specjalny, np. ! " # \$ % & ' () * + , - . / : ; < = > ? @

5. Pomocniczy numer telefonu i pomocniczy adres e-mail do odzyskiwania hasła jest nadawany przez dyrektora i nie wolno go zmieniać bez jego wiedzy i zgody.

§ 4

1. Informacja o służbowym adresie e-mail jest jawna i jest dostępna powszechnie, w tym na łamach witryny internetowej szkoły.

2. Pracownik jest zobowiązany do korzystania z przyznanego mu adresu mailowego do wszelkiej korespondencji służbowej z innymi pracownikami placówki.

3. Przy korespondencji pracownik zobowiązany jest do:

- a) sprawdzania skrzynki pocztowej przynajmniej raz dziennie każdego dnia, w którym jest obecny w pracy i wykonuje obowiązki służbowe;
- b) bezzwłocznego odpowiadania na e-mail'e;
- c) podawania tematu e-mail'a oraz umieszczania swojego podpisu.

3. Pracownik zobowiązuje się, że nie będzie działał w sposób naruszający prawa innych użytkowników systemu pocztowego oraz nie będzie przenosił prawa do korzystania ze swojej skrzynki pocztowej na osoby trzecie.

4. Pracownik ma prawo korzystać ze służbowego konta pocztowego w pełnym zakresie jego funkcjonalności pod warunkiem, że będzie to zgodne z obowiązującym prawem, normami społecznymi i obyczajowymi.

5. Pracownik powinien stosować odpowiednie środki ostrożności zapobiegające wprowadzeniu wirusów do systemu poczty elektronicznej.

ROZDZIAŁ

III

Zakres i uprawnienia kontrolne pracodawcy dotyczące służbowej korespondencji elektronicznej pracownika

§ 7

1. Pracodawca zobowiązuje się dołożyć wszelkich starań w celu zapewnienia poprawnego działania systemu poczty elektronicznej oraz zobowiązuje się do udzielania wszelkiej możliwej pomocy w problemach związanych z obsługą służbowych kont pocztowych.

2. E-maile wysyłane z firmowej skrzynki pocztowej stanowią własność pracodawcy i pracodawca może je kontrolować.

3. Z uwagi na konieczność zapewnienia ochrony interesu i bezpieczeństwa Szkoły pracodawca zastrzega sobie prawo do wglądu we wszystkie wiadomości pracownika o charakterze służbowym (zarówno w skrzynce odbiorczej, jak i nadawczej).

4. Kontrola służbowej korespondencji pracowników oraz ich poczty elektronicznej może nastąpić w obecności pracownika.

5. Pracodawca ma prawo kontroli przestrzegania przez pracownika zasad korzystania ze służbowej poczty elektronicznej zgodnie z Regulaminem.

§ 8

1. Szkoła zastrzega sobie prawo do:

- a) zmiany zasad funkcjonowania systemu poczty elektronicznej a informacje o tym fakcie będą podawane do wiadomości pracownikom za pomocą poczty elektronicznej,
- b) zamykania kont pocztowych osób, które przestają być pracownikami szkoły,
- c) zamykania kont pocztowych w przypadkach wykorzystania ich w sposób niezgodny z przeznaczeniem i szeroko rozumianym interesem Szkoły. W szczególności może to dotyczyć: wykorzystania skrzynek pocztowych do prywatnej działalności komercyjnej, zachowań naruszających zasady wymienione w niniejszym dokumencie, zachowań naruszających inne zasady i regulaminy oraz naruszających ogólnie przyjęte zasady współistnienia użytkowników sieci Internet.

§ 9

1. Szkoła nie ponosi odpowiedzialności za:

- a) skutki wejścia przez osoby trzecie w posiadanie hasła umożliwiającego korzystanie z konta pocztowego pracownika,
- b) utratę danych spowodowaną awarią sprzętu, systemu oraz innymi niezależnymi okolicznościami,
- c) przerwy w funkcjonowaniu systemu pocztowego zaistniałe z przyczyn technicznych niezależnych od Szkoły.
- d) sposób wykorzystywania skrzynki pocztowej przez pracownika oraz szkody jakie poniósł na skutek nieprawidłowego zapisu lub nieprawidłowego odczytu wiadomości,
- e) szkody wynikłe z niewłaściwego użytkowania konta pocztowego,
- f) treści przesyłane przez pracownika w systemie poczty elektronicznej.

ROZDZIAŁ

IV

Postanowienia końcowe

§ 10

1. Regulamin korzystania z poczty elektronicznej obowiązuje od 03 września 2018 roku.

2. Zmiany w niniejszym regulaminie mogą być wprowadzane przez dyrektora w trybie właściwym dla jego ustalania.