Załącznik 2 *do Zarządzenia Nr 5/2022*
Dyrektora Zespołu Szkolno – Przedszkolnego nr 1 we Włocławku
z dnia 11.02.2022 roku

Instrukcja Zarządzania Systemem Informatycznym Ochrony Danych Osobowych

w Zespole Szkolno – Przedszkolnym nr 1

we Włocławku

ul. Gałczyńskiego 9

87 – 800 Włocławek

1 CELE WPROWADZENIA I ZAKRES ZASTOSOWANIA INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

1. Instrukcja jest dokumentem powiązanym z *Polityką Bezpieczeństwa* w zakresie *Zarządzania Systemem Informatycznym,* służącym do przetwarzania danych osobowych **w Zespole Szkolno – Przedszkolnym nr 1 we Włocławku.** Stanowi wykaz procedur oraz stosowanych środków technicznych i organizacyjnych mających na celu, zgodnie z Art. 32 RODO, zabezpieczyć przetwarzane dane osobowe przed: przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych oraz nieuprawnionym dostępem do danych osobowych.

2. Niniejsza *Instrukcja* znajduje zastosowanie do systemów informatycznych, stosowanych w Zespole, w których są przetwarzane dane osobowe.

3. *Instrukcja* podlega monitorowaniu i w razie potrzeby uaktualnianiu co roku, do końca stycznia, przez administratora danych osobowych lub upoważnioną przez niego osobę, w ramach sprawowania kontroli zarządczej.

4. Dokument instrukcji przechowywany jest w wersji papierowej i elektronicznej.

2 DEFINICJE

Przez użyte w Instrukcji określenia należy rozumieć:

1) **instrukcja** – to *Zarządzania Systemem Informatycznym,* służącym do przetwarzania danych osobowych **w Zespole Szkolno – Przedszkolnym nr 1 we Włocławku.**
2) **administrator danych osobowych** – to osoba, decydującą o celach i środkach przetwarzania danych; w **Zespole Szkolno – Przedszkolnym nr 1 we Włocławku** funkcję administratora danych pełni dyrektor szkoły;
3) **inspektor ochrony danych** – to osoba formalnie wyznaczona przez *Administratora* w celu informowania i doradzania *Administratorowi,* pracownikom w zakresie obowiązującego prawa o ochronie danych i niniejszej *Polityki* oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego;
4) **administrator systemu informatycznego** – to osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagane specjalnych uprawnień;
5) **dane osobowe** – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
6) **zbiór danych** – to zestaw danych osobowych posiadający określoną strukturę, prowadzony wg określonych kryteriów oraz celów;

7) **przetwarzanie danych** – oznacza 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.
   W skład systemu wchodzą:
   • dokumentacja papierowa (korespondencja, dokumenty pracowników i uczniów);
   • wydruki komputerowe;
   • urządzenia i oprogramowanie komputerowe służące do przetwarzania informacji;
   • procedury przetwarzania danych w systemie, w tym procedury awaryjne.
   Sposób przepływu danych pomiędzy poszczególnymi systemami:
   • przenoszenie,
   • eksport/import danych,
   • kopiowanie,
   • usuwanie,
   • generowanie w postaci list do wydruków MS Office VULCAN → PDF (Acrobat Reader lub inny) MS Office – SIO
8) **ograniczenie przetwarzania** - polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
9) **hasło** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
10) **identyfikator użytkownika** – to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych; osobowych w systemie informatycznym;
11) **odbiorca danych** – to każdy, komu udostępnia się dane osobowe, z wyłączeniem: osoby, której dane dotyczą; osobę upoważnioną do przetwarzania danych; osobę, której powierzono przetwarzanie danych; organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;
12) **osoba upoważniona do przetwarzania danych osobowych** – to pracownik szkoły, który upoważniony został do przetwarzania danych osobowych przez dyrektora szkoły na piśmie;
13) **poufność danych** – to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
14) **raport** – to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
15) **serwis** – to firma lub pracownik firmy, zajmującej się instalacją, naprawą i konserwacją sprzętu komputerowego;
16) **sieć publiczna** –to sieć telekomunikacyjna, wykorzystywana głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych;
17) **system informatyczny** – to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
18) **szkoła/zespół** – to **Zespół Szkolno – Przedszkolny nr 1 we Włocławku;**
19) **teletransmisja** – to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;

20) **RODO** – to Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016);
21) **ustawa** – to Ustawa z dnia 10 maja 2018r. o ochronie danych osobowych (Dz. U. z 2018r. poz. 1000) oraz ustawa z dnia 14 grudnia 2018r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. 2019r., poz. 125);
22) **uwierzytelnianie** – to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
23) **użytkownik** – to pracownik szkoły upoważniony do przetwarzania danych osobowych, zgodnie z zakresem obowiązków, któremu nadano identyfikator i przyznano hasło w przypadku korzystania z systemu informatycznego;
24) **zgoda osoby, której dane dotyczą** - oznacza dowolne, dowolnie określone, konkretne, świadome i jednoznaczne wskazanie osoby, której dane dotyczą, za pomocą oświadczenia lub wyraźnego działania potwierdzającego, wyrażającego zgodę na przetwarzanie danych osobowych z nim związanych. Zgoda musi być udokumentowana we właściwy sposób, aby ją udowodnić;
25) **ocena skutków w ochronie danych -** to proces przeprowadzany przez *Administratora,* jeśli jest wymagany przez obowiązujące prawo i, jeśli to konieczne, z uczestnictwem inspektora ochrony danych, przed przetwarzaniem, w przypadku, gdy istnieje prawdopodobieństwo wysokiego ryzyka dla praw i wolności osób fizycznych jako rodzaju przetwarzania danych osobowych i zachodzi wraz z wykorzystaniem nowych technologii, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania. Proces ten musi ocenić wpływ planowanych operacji przetwarzania na ochronę danych osobowych;
26) **podmiotem danych** jest każda osoba fizyczna, która jest przedmiotem przetwarzanych danych;
27) **podmiot przetwarzający** (**Procesor)** - to osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu administratora;
28) **anonimizacja** – to zmiana danych osobowych w wyniku której dane te tracą charakter danych osobowych;
29) **pseudonimizacja -** oznacza przetwarzanie danych osobowych w taki sposób (np. poprzez zastępowanie nazw liczbami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. Listy referencyjnej nazwisk i numerów), pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym w celu zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
30) **szczególne kategorie danych osobowych** - ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach zawodowych i obejmują przetwarzanie danych genetycznych, dane biometryczne w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia, dane dotyczące naturalnego życie seksualne osoby lub orientację seksualną. W zależności od obowiązującego prawa, specjalne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych i karnych oraz o sankcjach;

31) **profilowanie** – jest dowolną forma zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
32) **naruszenie ochrony danych osobowych** - jest to przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

3 NADAWANIE I REJESTROWANIE (WYREJESTROWANIE) UPRAWNIEŃ DO PRZETWARZANIA DANYCH W SYSTEMIE INFORMATYCZNYM

1. Nadawanie i rejestrowanie uprawnień

1) Dostęp do systemu informatycznego, służącego do przetwarzania danych osobowych, może uzyskać wyłącznie osoba upoważniona do przetwarzania danych osobowych, zarejestrowana jako użytkownik w tym systemie przez dyrektora szkoły lub uprawnioną przez niego osobę.

2) Rejestracja użytkownika, o którym jest mowa w pkt. 1., polega na nadaniu identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.

2. Wyrejestrowanie uprawnień

1) Wyrejestrowanie użytkownika systemu informatycznego dokonuje dyrektor szkoły lub upoważniona przez niego osoba.

2) Wyrejestrowanie, o którym jest mowa w pkt. 1., może mieć charakter czasowy lub trwały.

3) Wyrejestrowanie następuje przez:
   a) zablokowanie konta użytkownika do czasu ustania przyczyny, uzasadniającej blokadę (wyrejestrowanie czasowe),
   b) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

4) Czasowe wyrejestrowanie użytkownika z systemu musi nastąpić w razie:
   a) nieobecności użytkownika w pracy, trwającej dłużej niż 21 dni kalendarzowych,
   b) zawieszenia w pełnieniu obowiązków służbowych.

5) Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego może być:
   a) wypowiedzenie umowy o pracę,
   b) wszczęcie postępowania dyscyplinarnego.

6) Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik.

4 METODY I ŚRODKI UWIERZYTELNIENIA

1. Celem zastosowania poniższych metod i środków uwierzytelniania jest zapewnienie, że do systemu informatycznego mają dostęp jedynie osoby do tego upoważnione. W systemie informatycznym stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do sieci lokalnej oraz dostępu do aplikacji.
2. Procedura haseł:
   1) ogólne zasady postępowania z hasłami, zarówno do systemu jak i poszczególnych aplikacji:
   a) zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom,
   b) użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności,
   c) użytkownik systemu zobowiązany jest do niezwłocznej zmiany hasła, gdy zostało ono ujawnione,
   d) użytkownik zobowiązany jest zapamiętać hasło i przestrzegać powyższych zasad.
   2) Restrykcje dla haseł stosowanych w systemie informatycznym:
   a) hasło dostępu musi składać się z co najmniej 8 znaków, z dużych i małych liter oraz cyfr lub znaków specjalnych,
   b) hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów,
   c) hasło do systemu informatycznego nie może pokrywać się z żadnym z ostatnich 10 haseł stosowanych przez użytkownika,
   d) zmiana hasła odbywa się co najmniej raz na 30 dni i jest wymuszana przez system informatyczny, w przypadku braku automatycznego wymuszania hasła ze względów technicznych, użytkownik powinien we własnym zakresie zmienić hasło zgodnie z podanym okresem czasu,
   e) każdy użytkownik systemu informatycznego otrzymuje od Administratora Systemu Informatycznego identyfikator i hasło tymczasowe (służące do pierwszego logowania) lub instrukcję aktywacji konta oraz utworzenia do niego hasła.
   f) użytkownik informowany jest ustnie o przydzielonym mu haśle dostępowym, pozwalającym na zdefiniowanie własnego hasła spełniającego wszystkie wyżej wymienione wymogi. Hasło dostępowe musi zostać zmienione przez użytkownika przy pierwszym jego użyciu w systemie informatycznym.
3. Identyfikator (login) składa się imienia i nazwiska użytkownika oddzielonych kropką oraz końcówki @zsp1.pl W identyfikatorze pomija się polskie znaki diakrytyczne. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika systemu *Administrator Systemu Informatycznego* nadaje inny identyfikator, odstępując od wyżej opisanej. W uzgodnieniu z ASI użytkownik może korzystać z innego identyfikatora, niż opisany powyżej.

5 PROCEDURY ZWIĄZANE Z GROMADZENIEM, PRZECHOWYWANIEM, PRZETWARZANIEM I USUWANIEM DANYCH OSOBOWYCH

1. **Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informacyjnym oraz wskazanie osoby odpowiedzialnej za te czynności**

1) Przetwarzać dane osobowe w systemie informatycznym może wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych (wzór upoważnienia stanowi załącznik nr 13 do *Polityki*). Wydanie upoważnienia oraz rejestracja użytkownika systemu informatycznego, przetwarzającego dane osobowe, następuje na wniosek dyrektora szkoły.

2) Oryginał upoważnienia zostaje przekazany pracownikowi za potwierdzeniem odbioru, kopia upoważnienia zostaje dołączona do akt osobowych pracownika.

3) Identyfikator i hasło do systemu informatycznego, przetwarzającego dane osobowe, są przydzielone użytkownikowi tylko w przypadku, gdy posiada on pisemne upoważnienie do przetwarzania danych osobowych. Za przydzielenie i wygenerowanie identyfikatora i hasła użytkownikowi, który pierwszy raz będzie korzystał z systemu informatycznego, odpowiada *Administrator Systemu Informatycznego.* Wyrejestrowanie użytkownika z systemu informatycznego następuje na wniosek administratora danych osobowych.

4) *Administrator Danych Osobowych* jest zobowiązany do prowadzenia **ewidencji pracowników upoważnionych do przetwarzania danych osobowych** w Zespole Szkolno – Przedszkolnym nr 1 we Włocławku – załącznik nr 17 do *Polityki*.

2. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1) Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła, oraz uzyskaniu zaświadczenia do przetwarzania danych osobowych, zaświadczenie jest także niezbędne do przetwarzania danych osobowych w systemie tradycyjnym.

2) Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiada za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje.

3) Identyfikator i hasło użytkownika powinny odpowiadać wymaganiom, określonym w rozdziale IV.

4) Nazwy i hasła użytkowników, posiadających uprawnienia do informatycznego przetwarzania danych osobowych, powinny być przechowywane w zamkniętej szafie lub sejfie, do której dostęp jest w pełni kontrolowany, przy czym dostęp do nich mają wyłącznie osoby uprawnione (***Dziennik haseł*** załącznik nr 18 do *Polityki),*

5) W przypadku konieczności użycia nazw i haseł tych użytkowników konieczny jest wpis, ilustrujący zaistniałą sytuację w ***Dzienniku Administratora*** (załącznik nr 19 do *Polityki).* Wpis powinien zawierać następujące informacje:

a) imię i nazwisko oraz stanowisko osoby upoważnionej, udostępniającej dostęp do szafy, w której znajdują się hasła,
b) imię i nazwisko oraz stanowisko osoby, która pobiera nazwy użytkowników i hasła,
c) krótki opis sytuacji, która zmusiła do awaryjnego wykorzystania haseł.

6) O konieczności i okolicznościach awaryjnego użycia nazw i haseł musi niezwłocznie zostać powiadomiony *Inspektor Ochrony Danych* oraz *Administrator Danych.*

3. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

1) Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym oraz w trakcie pracy każdy pracownik jest obowiązany do zwrócenia bacznej uwagi, czy nie wystąpiły symptomy, mogące świadczyć o naruszeniu ochrony danych osobowych.

2) Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.

3) W przypadku bezczynności użytkownika na stacji roboczej przez okres dłuższy niż 30 minut automatycznie włączony jest wygaszasz ekranu. Wygaszacze ekranu powinny być zaopatrzone w hasła zbudowane analogicznie do haseł używanych przez użytkownika przy logowaniu.

4) Zmianę użytkownika stacji roboczej każdorazowo musi poprzedzać wylogowanie się poprzedniego użytkownika. Niedopuszczalne jest, aby dwóch lub większa liczba użytkowników wykorzystywała wspólne konto użytkownika.

5) W przypadku, gdy przerwa w pracy na stacji roboczej trwa dłużej niż 60 minut, użytkownik obowiązany jest wylogować się z aplikacji i systemu stacji roboczej, na której pracuje, oraz sprawdzić, czy nie zostały pozostawione bez zamknięcia nośniki informacji, zawierające dane osobowe. W pomieszczeniach, w których przetwarzane są dane i w których jednocześnie mogą przebywać osoby postronne, monitory stanowisk dostępu do danych powinny być ustawione w taki sposób, żeby uniemożliwić tym osobom wgląd w dane.

6) Zakończenie pracy użytkownika w systemie informatycznym obejmuje wylogowanie się użytkownika z aplikacji.

4. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych, służących do ich przetwarzania

1) Dane osobowe, przetwarzane w systemie informatycznym, podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych.

2) Kopie zapasowe danych tworzone są przez użytkownika.
3) Kopie sporządzane są na pendrive lub dysku zewnętrznym.
4) Kopie zapasowe sporządzane są w miarę potrzeb, nie rzadziej niż raz na 2 miesiące. Po tym terminie stare kopie są niszczone poprzez nadpisywanie ich przez bardziej aktualne.
5) Każdy nośnik jest opisany datą jej sporządzenia i zaewidencjonowany w ***Rejestrze nośników komputerowych zawierających dane osobowe*** (załącznik nr 20 do *Polityki).*
6) Kopie zapasowe przechowywane są do momentu utworzenia nowych kopi.
7) Dostęp do kopii mają: dyrektor, czyli ADO, ASI i pracownik, który je utworzył.
8) Kopie przechowywane są w zamkniętej szafie w sekretariacie.
9) W przypadku przechowywania kopii zapasowych przez okres dłuższy niż pół roku, wszystkie kopie zapasowe zbiorów danych osobowych, aplikacji przetwarzających dane osobowe oraz danych konfiguracyjnych systemu informatycznego, przetwarzającego dane osobowe, których to dotyczy, muszą być okresowo (co najmniej raz na pół roku) sprawdzane pod względem ich dalszej przydatności. Czynności te wykonuje *Administrator Systemu Informatycznego* lub osoba przez niego upoważniona.
10) Nośniki kopii zapasowych, które zostały wycofane z użycia, jeżeli jest to możliwe, należy pozbawić zapisanych danych za pomocą specjalnego oprogramowania do bezpiecznego usuwania zapisanych danych. W przeciwnym wypadku podlegają fizycznemu zniszczeniu z wykorzystaniem metod adekwatnych do typu nośnika, w sposób uniemożliwiający odczytanie zapisanych danych.

5. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

1) Nośniki danych zarówno w postaci elektronicznej, jak i papierowej powinny być zabezpieczone przed dostępem osób nieuprawnionych, nieautoryzowaną modyfikacją i zniszczeniem. Dane osobowe mogą być zapisywane na nośnikach przenośnych w przypadku tworzenia kopii zapasowych lub gdy istnieje konieczność przeniesienia tych danych w postaci elektronicznej, a wykorzystanie do tego celu sieci informatycznej jest nieuzasadnione, niemożliwe lub zbyt niebezpieczne.

2) Nośniki danych osobowych oraz wydruki powinny być przechowywane w zamkniętych szafach i nie powinny być bez uzasadnionej przyczyny wynoszone poza ten obszar. Przekazywanie nośników danych osobowych i wydruków poza budynek szkoły powinno odbywać się za wiedzą *Administratora Danych Osobowych*.

3) W przypadku, gdy nośnik danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie nośnika lub usunięcie danych z nośnika zgodnie ze wskazówkami umieszczonymi w punkcie 4. Jeżeli wydruk danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie wydruku przy użyciu niszczarki dokumentów.

4) W przypadku, gdy kopia zapasowa nie jest dłużej potrzebna, należy przeprowadzić jej zniszczenie lub usunięcie danych z nośnika, na którym się ona znajduje.

6. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1) W związku z tym, że system informatyczny narażony jest na działanie oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do tego systemu, konieczne jest podjęcie odpowiednich środków ochronnych.

2) Można wyróżnić następujące rodzaje występujących tu zagrożeń:

- nieuprawniony dostęp bezpośrednio do bazy danych,
- uszkodzenie kodu aplikacji, umożliwiającej dostęp do bazy danych w taki sposób, że przetwarzane dane osobowe ulegną zafałszowaniu lub zniszczeniu,
- przechwycenie danych podczas transmisji w przypadku rozproszonego przetwarzania danych z wykorzystaniem ogólnodostępnej sieci Internet,
- przechwycenie danych z aplikacji, umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych przez wyspecjalizowany program szpiegowski i nielegalne przesłanie tych danych poza miejsce przetwarzania danych,
- uszkodzenie lub zafałszowanie danych osobowych przez wirus komputerowy, zakłócający pracę aplikacji, umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych.

3) W celu przeciwdziałania wymienionym zagrożeniom system informatyczny musi posiadać następujące zabezpieczenia:

- autoryzację użytkowników przy zachowaniu odpowiedniego poziomu komplikacji haseł dostępu,
- stosowanie szyfrowanej transmisji danych przy zastosowaniu odpowiedniej długości klucza szyfrującego,
- stosowanie odpowiedniej ochrony antywirusowej na stacjach roboczych wykorzystywanych do przetwarzania danych osobowych.

  Ponieważ systemy informatyczne, działające w szkole, nie są połączone z serwerem, nie ma konieczności stosowania rygorystycznego systemu autoryzacji dostępu do nich oraz stosowania aplikacji i nieumieszczania kodu źródłowego aplikacji na serwerach.

4) Potencjalnymi źródłami przedostawania się programów szpiegowskich oraz wirusów komputerowych na stacje robocze są:

- załączniki do poczty elektronicznej,
- przeglądane strony internetowe,
- pliki i aplikacje, pochodzące z nośników wymiennych, uruchamiane i odczytywane na stacji roboczej.

5) W celu zapewnienia ochrony antywirusowej *Administrator Systemu Informatycznego,* przetwarzający dane osobowe, lub osoba specjalnie do tego celu wyznaczona, jest odpowiedzialny za zarządzanie systemem, wykrywającym i usuwającym wirusy. System antywirusowy powinien być skonfigurowany w następujący sposób:

- rezydentny monitor antywirusowy (uruchomiony w pamięci operacyjnej stacji roboczej) powinien być stale włączony,

- antywirusowy skaner ruchu internetowego powinien być stale włączony,
- monitor, zapewniający ochronę przed wirusami w dokumentach MS Office, powinien być stale włączony,
- skaner poczty elektronicznej powinien być stale włączony.

6) Systemy antywirusowe, zainstalowane na stacjach roboczych, powinny być skonfigurowane w sposób następujący:

- zablokowanie możliwości ingerencji użytkownika w ustawienia oprogramowania antywirusowego,
- możliwość centralnego uaktualnienia wzorców wirusów.

7) System antywirusowy powinien być aktualizowany na podstawie materiałów publikowanych przez producenta oprogramowania.

8) Użytkownicy systemu informatycznego zobowiązani są do następujących działań:

- skanowania zawartości dysków stacji roboczej, pracującej w systemie informatycznym pod względem potencjalnie niebezpiecznych kodów przynajmniej 2 razy w tygodniu,
- skanowania zawartości nośników wymiennych odczytywanych na stacji roboczej, pracującej w systemie informatycznym, pod względem potencjalnie niebezpiecznych kodów – przy każdym odczycie,
- skanowanie informacji przesyłanych do systemu informatycznego pod kątem pojawienia się niebezpiecznych kodów – na bieżąco.

9) W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy administrator systemu informatycznego lub inny wyznaczony pracownik powinien podjąć działania, zmierzające do usunięcia zagrożenia.

W szczególności działania te mogą obejmować:

- usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego,
- odtworzenie plików z kopii zapasowych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane,
- samodzielną ingerencję w zawartość pliku – w zależności od posiadanych kwalifikacji lub skonsultowanie się z zewnętrznymi ekspertami.

10) System informatyczny, przetwarzający dane osobowe, powinien posiadać mechanizmy pozwalające na zabezpieczenie ich przed utratą lub wystąpieniem zafałszowania w wyniku awarii zasilania lub zakłóceń w sieci zasilającej. W związku z tym system informatyczny powinien być wyposażony w co najmniej filtry zabezpieczające stacje robocze przed skutkami przepięcia.

11) W celu zapewnienia bezpieczeństwa technicznego przetwarzanych danych osobowych za pomocą sposobów szybkiego przywrócenia dostępności danych osobowych w razie incydentu fizycznego lub technicznego, wprowadzono w Zespole Szkolno-Przedszkolnym nr 1 we Włocławku opisane poniżej zabezpieczenia:

a) tworzenie kopii zapasowych przetwarzania danych osobowych, w celu przywrócenia dostępności do zapisanych w nich danych osobowych, kopia zapasowa jest niczym

innym jak formą przechowywania informacji. Przechowywanie zaś jest postacią przetwarzania danych osobowych,

b) szyfrowanie pliku hasłem, na którym są zapisywane dane,

a) wdrożone zostały mechanizmy podnoszące poziom bezpieczeństwa teleinformatycznego tj. stosuje się oprogramowanie antywirusowe na stacjach roboczych z automatyczną aktualizacją w celu ochrony systemu przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,

b) kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych
i optycznych, służących zarówno do przetwarzania danych osobowych w systemie jak i do celów instalacyjnych,

c) przegląd techniczny komputerów poddawany jest okresowemu testowaniu i odtwarzaniu,

d) prowadzona regularnie analiza ryzyka pozwala na ocenę skuteczności stosowanych środków technicznych i organizacyjnych zapewniających bezpieczeństwo,

e) zachowanie poufności przetwarzanych informacji oraz kopii danych.

Zabezpieczenia te w razie awarii pozwalają na szybsze przełączenie i zachowanie ciągłości działania i dostępu do danych.

Administrator Danych Osobowych zapewnia, iż dane osobowe w kopiach zapasowych:

a) pozyskane są zgodnie z prawem,

b) przechowywane jedynie na potrzeby celu przetwarzania oraz wyłącznie w okresie, w którym ów cel istnieje – jeżeli cel przetwarzania wygasł i nie można dysponować inną przesłanką legalnego przetwarzania danych osobowych, to dane są usuwane, w tym również kopie zapasowe tychże danych,

c) w przypadku zaktualizowania plików z danymi osobowymi aktualizuje się również ich kopię,

12) Zespół Szkolno-Przedszkolny nr 1 we Włocławku dba o zapewnienie ciągłości funkcjonowania usług związanych z przetwarzaniem danych. Celem takiego postępowania jest przeciwdziałanie przerwom w działalności Zespołu oraz ochrona krytycznych procesów przed rozległymi awariami lub katastrofami. Skuteczna realizacja postawionego celu Zespołu jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z zarządzeniem ciągłością działania tak, aby ograniczać do akceptowalnego poziomu skutków wypadków i awarii. W sposób systemowy tworzone są plany postępowania w sytuacjach kryzysowych. Zespół Szkolno-Przedszkolny nr 1 we Włocławku dba o ich aktualność i testuje je pod względem przydatności w sytuacji realnego zagrożenia. Powyższe zasady zapewniają, że Zespół Szkolno-Przedszkolny nr 1 we Włocławku jest przygotowany na działanie w przypadkach wystąpienia katastrofalnej szkody.

7. Sposób realizacji wymogów dotyczących systemów służących do przetwarzania danych osobowych – art. 39, 40, 41 ustawy

1) Administrator i podmiot przetwarzający stosują środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, które w szczególności mają na celu:

- uniemożliwienie osobom nieuprawnionym dostępu do sprzętu używanego do przetwarzania (kontrola dostępu do sprzętu);
- zapobiegnięcie nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu nośników danych (kontrola nośników danych);
- zapobiegnięcie nieuprawnionemu wprowadzaniu danych osobowych oraz nieuprawnionemu oglądaniu, zmienianiu lub usuwaniu przechowywanych danych osobowych (kontrola przechowywania);
- zapobiegnięcie korzystaniu z systemów zautomatyzowanego przetwarzania przez osoby nieuprawnione, używające sprzętu do przesyłu danych (kontrola użytkowników);
- zapewnienie osobom, uprawnionym do korzystania z systemu zautomatyzowanego przetwarzania, dostępu wyłącznie do danych osobowych objętych posiadanym przez siebie uprawnieniem (kontrola dostępu do danych);
- umożliwienie zweryfikowania i ustalenia podmiotów, którym dane osobowe zostały lub mogą zostać przesłane lub udostępnione, za pomocą sprzętu do przesyłu danych (kontrola przesyłu danych);
- umożliwienie następczej weryfikacji i ustalenia, które dane osobowe zostały wprowadzone do systemów zautomatyzowanego przetwarzania, kiedy i przez kogo (kontrola wprowadzania danych);
- zapobieżenie nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu danych osobowych podczas ich przekazywania lub podczas przenoszenia nośników danych (kontrola transportu);
- zapewnienie przywrócenia zainstalowanych systemów w razie awarii (odzyskiwanie);
- zapewnienie działania funkcji systemu, zgłaszania występujących w nich błędów (niezawodność) oraz odporności przechowywanych danych na uszkodzenia powodowane błędnym działaniem systemu (integralność).

2) Administrator i podmiot przetwarzający niszczą w sposób trwały niepodlegające archiwizacji informatyczne nośniki danych wykorzystywane do przetwarzania danych osobowych wycofane z eksploatacji przy użyciu odpowiednich narzędzi i środków technicznych. Nośniki wycofane z eksploatacji nie mogą być zbywane. Ze zniszczenia nośników sporządza się protokół, w którym uwzględnia się wskazanie sposobu ich zniszczenia.

3) Do przetwarzania danych osobowych może być dopuszczona wyłącznie osoba zapewniająca bezpieczeństwo przetwarzanych danych osobowych oraz posiadająca upoważnienie do przetwarzania danych osobowych w ramach danej kategorii czynności przetwarzania, nadane przez administratora lub podmiot przetwarzający. Zatwierdzony

przez administratora lub podmiot przetwarzający wniosek o nadanie uprawnień do dostępu do danych osobowych w ramach danej kategorii czynności przetwarzania uznaje się za nadanie takiego upoważnienia.

4) Wniosek o nadanie uprawnień dostępu do danych osobowych powinien zawierać:
- imię i nazwisko, stanowisko, miejsce zatrudnienia osoby, której wniosek dotyczy;
- zakres i czasookres dostępu do danych osobowych;
- rodzaj danych osobowych i sposób ich przetwarzania.

5) Do wniosku należy dołączyć oświadczenie osoby, której wniosek dotyczy, o zobowiązaniu się do zapewnienia bezpieczeństwa danych osobowych, w tym ochrony przed niedozwolonym lub niezgodnym z prawem przetwarzaniem danych osobowych oraz ich przypadkową utratą, zniszczeniem lub uszkodzeniem.

6) Wniosek oraz oświadczenie, o których mowa odpowiednio w ust. 2 i 3, mogą być sporządzone w formie elektronicznej.

Rejestr systemów teleinformatycznych funkcjonujących w Zespole Szkolno-Przedszkolnym nr 1 stanowi załącznik 20a do *Polityki.*
Wykaz urządzeń funkcjonujących w Zespole Szkolno-Przedszkolnym nr 1 wykorzystywanych do przetwarzania danych osobowych stanowi załącznik 20b do *Polityki.*

8. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

1) Wszelkie prace związane z naprawami i konserwacją systemu informatycznego, przetwarzającego dane osobowe, muszą uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych (***Oświadczenie o zachowaniu danych w poufności*** – załącznik nr 1 do *Instrukcji Zarządzania Systemem Informatycznym).*

2) Prace serwisowe na terenie szkoły, prowadzone w tym zakresie, mogą być wykonywane wyłącznie przez jego pracowników lub przez upoważnionych przedstawicieli wykonawców zewnętrznych, znajdujących się w towarzystwie pracowników szkoły (***Rejestr zgłoszeń dotyczący napraw, przeglądów i konserwacji sprzętu komputerowego i systemu informatycznego*** – załącznik nr 2 do *Instrukcji Zarządzania Systemem Informatycznym).*

3) Przed rozpoczęciem prac serwisowych przez osoby spoza szkoły konieczne jest potwierdzenie tożsamości serwisantów.

4) Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
- likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
- przekazania podmiotowi nieuprawnionemu do przetwarzania danych - pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
- naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

6 POZIOM BEZPIECZEŃSTWA

Uwzględniając kategorie danych osobowych oraz konieczność zachowania bezpieczeństwa ich przetwarzania w systemie informatycznym, połączonym z siecią publiczną, wprowadza się „poziom wysoki”.

7 STOSOWANE ŚRODKI BEZPIECZEŃSTWA

1. W Zespole Szkolno – Przedszkolnym nr 1 we Włocławku stosuje się środki bezpieczeństwa na poziomie wysokim.

2. W szkole stosuje się następujące środki bezpieczeństwa:

1) Zabezpieczenie obszaru, w którym przetwarzane są dane osobowe, przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.

2) Przebywanie osób nieuprawnionych, jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

3) Stosowane są mechanizmy kontroli dostępu do danych.

4) Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie jest przydzielany innej osobie.

5) W przypadku, gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 6 znaków.

6) Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów, służących do przetwarzania danych osobowych.

7) Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem oraz usuwa się niezwłocznie po ustaniu ich użyteczności.

8) *Administrator Danych Osobowych* monitoruje wdrożone zabezpieczenia systemu informatycznego.

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

a) likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,
c) naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

10) W przypadku, gdy do uwierzytelnienia użytkowników używa się haseł, hasło to składa się co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry i znaki specjalne.

11) Urządzenia i nośniki, zawierające dane osobowe, zabezpiecza się w sposób zapewniający poufność i integralność tych danych.

12) *Administrator Danych* stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

8 POSTANOWIENIA KOŃCOWE

1. Osobą odpowiedzialną za przegląd przestrzegania instrukcji, przegląd jej aktualności oraz aktualizację, a także nadawanie praw dostępu do systemu informatycznego jest *Administrator Systemu Informatycznego* lub inna osoba upoważniona przez *Administratora Danych.*
2. W sprawach nieokreślonych niniejszą instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.
3. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszą instrukcją oraz złożyć stosowne oświadczenie, potwierdzające znajomość jej treści.
4. Niezastosowanie się do procedur określonych w niniejszej instrukcji przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52. *Kodeksu Pracy.*

5. Niniejsza instrukcja wchodzi w życie z dniem 14.02.2022r.

Włocławek ……..
data

Dyrektor
Zespołu Szkolno –Przedszkolnego nr 1
(Administrator Danych Osobowych)

……

…….. ……
(podmiot) *(miejscowość, data)*

Oświadczenie o zachowaniu danych w poufności

Oświadczam, że w związku z przeprowadzaniem napraw/konserwacji sprzętu komputerowego (np. kserokopiarki) ……
w Zespole Szkolno-Przedszkolnym nr 1 we Włocławku, zobowiązuję się zgodnie z przepisami rozporządzenia Paramentu 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 informacji oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) do zachowania w tajemnicy wszelkich informacji i danych osobowych, w tym danych szczególnej kategorii otrzymanych w związku z realizacją świadczeń / usług ……
w Zespole Szkolno-przedszkolnym nr 1 reprezentowany przez Dyrektora z siedzibą we Włocławku, ul. Gałczyńskiego 9, 87-800 Włocławek 9 (e-mail: sekretariat@zsp1.pl, tel. 54 234 96 94).

Jednocześnie oświadczam, że w związku ze zobowiązaniem do zachowania w tajemnicy danych osobowych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora Danych.

……..
podpis osoby upoważnionej

Przyjmuję do wiadomości:

……
podpis Administratora Danych Osobowych

Rejestr zgłoszeń dotyczący napraw, przeglądów i konserwacji sprzętu komputerowego i systemu informatycznego Zespól Szkolno-Przedszkolny nr 1 we Włocławku

L.p.	Data zgłoszenia	Opis zgłoszenia	Podpis osoby zgłaszającej	Osoba/podmiot dokonujący naprawy/przeglądu/ konserwacji Podpis	Zakres czynności wykonywanych podczas naprawy/przeglądu/ konserwacji
1					
2					
3					