Zarządzenie Nr 1/2021
Dyrektora Zespołu Szkolno-Przedszkolnego w Reńskiej Wsi
z 29 marca 2021 r.

w sprawie wdrożenia dokumentacji dotyczącej ochrony danych osobowych w Zespole Szkolno-Przedszkolnym w Reńskiej Wsi

Na podstawie 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, wprowadza się dokumentację ochrony danych osobowych dla Zespołu Szkolno-Przedszkolnego w Reńskiej Wsi

Zasady organizacji ochrony danych osobowych

§ 1

Ustala się Politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym służącą do przetwarzania danych osobowych w Zespole Szkolno-Przedszkolnym w Reńskiej Wsi zwaną dalej dokumentacją ochrony danych osobowych.

§2

Zobowiązuje się pracowników oraz osoby współpracujące z Zespołem Szkolno-Przedszkolnym w Reńskiej Wsi do stosowania zasad określonych w dokumentacji ochrony danych osobowych.

§3

1. Celem niniejszego dokumentu jest opisanie zasad ochrony danych osobowych oraz dostarczenie podstawowej wiedzy z zakresu ich ochrony w Zespole Szkolno-Przedszkolnym w Reńskiej Wsi z siedzibą przy ul. Raciborskiej 27, 47-208 Reńska Wieś zwanej dalej placówką oświatową.

2. W celu zwiększenia świadomości obowiązków i odpowiedzialności pracowników, a tym samym skuteczności ochrony przetwarzanych zasobów, w dokumencie opisano podstawy prawne przetwarzania danych osobowych oraz scharakteryzowano zagrożenia bezpieczeństwa, podając jednocześnie schematy postępowań na wypadek wystąpienia naruszenia bezpieczeństwa.

3. Dokument szczegółowo opisuje podstawowe zasady organizacji pracy przy zbiorach osobowych przetwarzanych metodami tradycyjnymi oraz w systemie informatycznym wyrażone w Polityce bezpieczeństwa oraz w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

4. Wszelkie zestawienia uzupełniające treść dokumentu zebrano w postaci załączników. Do najważniejszych należy ewidencja:

- zbiorów danych osobowych,

- miejsc ich przetwarzania,

- osób upoważnionych do przetwarzania danych,

a także lista środków organizacyjnych i technicznych służących bezpieczeństwu danych.

Podstawe definicje

§ 4

1. W dokumencie przyjmuje się następującą terminologię:

- Organ nadzorczy – oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51 rozporządzenia.
- Dane osobowe – oznaczają informacje z 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.
- Przetwarzanie – oznacza operacje 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.
- Ograniczone przetwarzanie – oznacza oznaczenie przechowywanych danych w celu ograniczenia ich przyszłego przetwarzania.
- Profilowanie – oznacza dowolna formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystywaniu 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.
- Pseudonimizacja - oznacza przetwarzanie danych osobowych w taki sposób, by nie można było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
- Zbiór danych – oznacza uporządkowany zestaw danych osobowych, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
- Dane wrażliwe - dane o pochodzeniu rasowym lub etnicznym, poglądach politycznych, przekonaniach religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.
- Dane genetyczne- oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej.
- Dane biometryczne- oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczna identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.

- Dane dotyczące zdrowia- oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej- w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia.
- Administrator- oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państw członkowskich, to również w prawie Unii lub w prawie państw członkowskich może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.
- Podmiot przetwarzający – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.
- Odbiorca- oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców. Przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mających zastosowanie stosownie do celów przetwarzania.
- Strona trzecia- oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia lub podmiotu przetwarzającego- mogą przetwarzać dane osobowe.
- Zgoda osoby, – której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.
- Naruszenie ochrony danych osobowych – oznacza naruszenie bezpieczeństwa prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesłanych, przechowywanych lub w inny sposób przetwarzanych.
- Inspektor ochrony danych (IOD)– osoba realizująca zadania określone w art. 39 rozporządzenia, w tym nadzorująca stosowanie środków technicznych i organizacyjnych przetwarzanych danych osobowych, odpowiednich do zagrożeń oraz kategorii danych objętych ochroną. IOD jest powoływany przez Administratora lub organ prowadzący.
- Administrator systemu informatycznego (ASI) – osoba lub osoby odpowiedzialna/e za prawidłowe funkcjonowanie systemu informatycznego. ASI pełni funkcję pomocnika IOD i jest powoływany przez Administratora..
- System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
- Zabezpieczenie danych w systemie informatycznym - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
- Identyfikator użytkownika – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
- Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

- Uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
- Rozliczalność - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
- Integralność danych – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
- Poufność danych – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.
- Dokumentacja przetwarzania danych – dokumentacja opisująca sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.
- Zagrożenia danych – polega z jednej strony na możliwości ich utraty, zniszczenia lub zafałszowania, z drugiej strony zaś na możliwości ich nieuprawnionego rozpowszechnienia.
- Zabezpieczenia – praktyki, procedury i mechanizmy zmniejszające ryzyko, chroniące przed zagrożeniami, ograniczające następstwa wykrywające niepożądane incydenty i ułatwiające odtworzenie prawidłowego stanu systemu.
- Pracownik – osoba zatrudniona na umowę o pracę, umowę cywilno-prawną, stażysta lub praktykant świadczący pracę dla Zespołu Szkolno-Przedszkolnego w Reńskiej Wsi.
- Placówka oświatowa – Zespół Szkolno-Przedszkolny w Reńskiej Wsi.
- Instrukcja – instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Zespole Szkolno-Przedszkolnym w Reńskiej Wsi.
- Sprawdzenie – czynności mające na celu zweryfikowanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, w szczególności w wyniku zwrócenia się o dokonanie sprawdzenia przez organ nadzorczy.
- Sprawozdanie – dokument opracowany przez IOD po dokonaniu sprawdzenia, którego celem jest zweryfikowanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
- Państwa trzecie – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego.

Rozdział I

Polityka

§ 5

Polityka bezpieczeństwa rozumiana jest, jako wykaz praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych wewnątrz instytucji. Obejmuje całokształt zagadnień związanych z problemem zabezpieczenia danych osobowych przetwarzanych zarówno tradycyjnie jak i w systemach informatycznych. Wskazuje działania przewidziane do wykonania oraz sposób ustanowienia zasad i reguł postępowania koniecznych do zapewnienia właściwej ochrony przetwarzanych danych osobowych.

Deklaracja

§ 6

1. Administrator danych mając świadomość, iż przetwarza dane zwykłe i szczególne pracowników oraz dane zwykłe i szczególne osób fizycznych, którym instytucja świadczy usługi, deklaruje dołożyć wszelkich starań, aby przetwarzanie odbywało się w zgodności z przepisami prawa.

2. W celu zabezpieczenia danych osobowych przed nieuprawnionym udostępnieniem Administrator danych wprowadza określone niniejszym dokumentem zasady przetwarzania danych. Zasady te określa w szczególności Polityka bezpieczeństwa oraz Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Dokumenty te są uzupełniane załącznikami do dokumentacji, na które składają się m.in.: rejestr czynności przetwarzania danych osobowych, wykaz miejsc ich przetwarzania oraz osób upoważnionych do przetwarzania danych.

3. W celu zapewnienia prawidłowego monitorowania przetwarzania danych wprowadza się liczne ewidencje, które szczegółowo charakteryzują obszary objęte monitoringiem, umożliwiając pełną kontrolę nad tym, jakie dane i przez kogo są przetwarzane oraz komu udostępniane.

4. Mając świadomość, iż żadne zabezpieczenie techniczne nie gwarantuje 100%-towej szczelności systemu, konieczne jest, aby każdy pracownik upoważniony do przetwarzania danych pełen świadomej odpowiedzialności, postępował zgodnie z przyjętymi zasadami i minimalizował zagrożenia wynikające z błędów ludzkich.

5. W trosce o czytelny i uporządkowany stan materii, wprowadza się stosowne środki organizacyjne i techniczne zapewniające właściwą ochronę danych oraz nakazuje ich bezwzględne stosowanie, zwłaszcza przez osoby dopuszczone do przetwarzania danych.

Charakterystyka instytucji

§ 7

Zespół Szkolno-Przedszkolny w Reńskiej Wsi realizuje zadania głównie na mocy przepisów prawa zawartych w ustawie Prawo Oświatowe, systemie informacji oświatowej oraz Karcie Nauczyciela, a także innych aktach wykonawczych uprawniających Dyrektora szkoły do podejmowania stosownych działań, w tym do przetwarzania danych osobowych. Podstawowym obszarem działania są zadania związane z bezpłatną opieką, wychowaniem oraz nauczaniem.

Rejestr kategorii oraz czynności przetwarzania danych osobowych

§ 8

1. Na podstawie art. 30 i 32 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 tworzy się:
   - Rejestr kategorii oraz czynności przetwarzania danych osobowych" – formularz nr 1,
   - Wykaz pomieszczeń tworzących obszar fizyczny przetwarzania danych" – formularz nr 2,
   - Rejestr osób upoważnionych do przetwarzania danych osobowych – formularz nr 3.

Środki organizacyjne ochrony danych osobowych

§ 9

1. W celu stworzenia właściwych zabezpieczeń, które powinny bezpośrednio oddziaływać na procesy przetwarzania danych, wprowadza się następujące środki organizacyjne:
   - Przetwarzanie danych osobowych w instytucji może odbywać się wyłącznie w ramach wykonywania zadań służbowych. Zakres uprawnień wynika z zakresu tych zadań,

- Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne upoważnienie. Wzór upoważnienia stanowi - formularz nr 4,
- Administrator prowadzi ewidencję osób upoważnionych oraz na jej podstawie przygotowuje upoważnienia do przetwarzania danych,
- Unieważnienie upoważnienia następuje na piśmie, wg wzoru - formularz nr 5,
- Zabrania się przetwarzania danych poza obszarem określonym w formularzu nr 2, za wyj. przypadków dopuszczonych przez Administratora,
- Każdy pracownik instytucji, co najmniej raz na rok musi odbyć szkolenie z zakresu ochrony danych osobowych. Za organizację szkoleń odpowiedzialny jest IOD, który prowadzi w tym celu odpowiednią dokumentację. Nowo przyjęty pracownik odbywa szkolenie przed przystąpieniem do przetwarzania danych. Za przeprowadzenie szkolenia wstępnego odpowiada IOD.
- Każdy upoważniony do przetwarzania danych potwierdza pisemnie fakt zapoznania się z niniejszą dokumentacją i zrozumieniem wszystkich zasad bezpieczeństwa. Wzór oświadczenia stanowi formularz nr 6. Podpisany dokument jest dołączany do przedmiotowej dokumentacji.
- Obszar przetwarzania danych osobowych określony w formularzu nr 2, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych poprzez zamknięcie pomieszczenia na klucz.
- Przebywanie osób, nieuprawnionych w w/w obszarze jest dopuszczalne za zgodą Administratora lub w obecności osoby upoważnionej do przetwarzania danych osobowych. Wzory zgody na przebywanie w pomieszczeniach dla osób nieposiadających upoważnienia, a także odwołania tej zgody, stanowią odpowiednio formularz nr 7 oraz formularz nr 8.
- Pomieszczenia stanowiące obszar przetwarzania danych powinny być zamykane na klucz.
- Monitory komputerów/laptopów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
- Przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna oraz usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w odpowiednich zamykanych szafach lub biurkach.
- Przetwarzanie danych podawanych dobrowolnie może odbywać się tylko na podstawie pisemnej zgody podającego te dane wg. wzoru określonego w formularzu nr 9.
- Dokumenty zawierające dane osobowe należ niszczyć w specjalistycznych niszczarkach.
- Każdorazowe zbieranie danych od osoby właściciela tych danych lub o osobach trzecich, rodzi obowiązek informacyjny. Obowiązek należy realizować umieszczając odpowiednią treść informacyjną pod formularzem z danymi.
- Dokumenty w wersji elektronicznej, które zapisywane są na nośniki zewnętrzne, przenoszone poza obszar przetwarzania lub przesyłane pocztą elektroniczną, należy zabezpieczyć poprzez nadanie im haseł odczytu.
- Zbiory osobowe przetwarzane elektronicznie należy zabezpieczyć poprzez wykonywanie kopii bezpieczeństwa, zapisywanych na zewnętrznych nośnikach i przechowywanych pod zamknięciem.
- Komputery/laptopy, które przetwarzają zbiory osobowe wyszczególnione na formularzu nr 1 do dokumentacji, za wyjątkiem komputerów służących jedynie do edycji tekstu, należy wyposażyć w urządzenia podtrzymujące napięcie na wypadek braku zasilania.
- Pliki edytorów tekstu lub arkuszy kalkulacyjnych należy traktować, jako kopie zbiorów, z których pochodzą przetwarzane w nich dane i odpowiednio zabezpieczyć stosując wytyczne zawarte w Instrukcji zarządzania systemem informatycznym będącej częścią niniejszego dokumentu.
- W celu zapewnienia ochrony danych przetwarzanych elektronicznie należy zapewnić logowanie do systemu operacyjnego oraz bezpośrednio do specjalistycznych programów przetwarzających dane.

- Szczegółowe zasady postępowanie ze zbiorami przetwarzanymi elektronicznie określa Instrukcja zarządzania systemem informatycznym będąca częścią niniejszej dokumentacji.
- IOD do 31 stycznia każdego roku budżetowego sporządza na formularzu nr 10 Planu sprawdzeń z zakresu przestrzegania zasad ochrony danych osobowych. Plan sprawdzeń jest zatwierdzany przez Administratora.
- W oparciu o Plan sprawdzeń IOD dokonuje sprawdzeń stanu zabezpieczenia danych osobowych prowadzonych zarówno w zbiorach tradycyjnych jak i w zbiorach elektronicznych. Fakt przeprowadzenia sprawdzenia IOD dokumentuje na formularzu nr 11 – Sprawozdanie ze sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
- IOD do 31 grudnia każdego roku budżetowego sporządza na formularzu nr 12 – Sprawozdanie roczne ze stanu zabezpieczenia danych osobowych. Sprawozdanie roczne ze stanu zabezpieczenia danych osobowych zatwierdzane jest przez ADO.
- IOD raz w roku do 31 grudnia przeprowadzana formularzu nr 20 audyt KRI. Wnioski z audytu KRI zawarte w rekomendacjach są podstawą do opracowania Sprawozdania rocznego z funkcjonowania ochrony danych osobowych w Zespole Szkolno-Przedszkolnym w Reńskiej Wsi.

Środki techniczne ochrony danych osobowych

§ 10

1. Zbiory danych przetwarzane w instytucji zabezpiecza się poprzez:

a. Środki ochrony fizycznej.

- Zbiory danych osobowych przechowywane są w pomieszczeniu zabezpieczonym drzwiami zwykłymi.
- Zbiory danych osobowych przechowywane są w pomieszczeniach, w których okna nie są zabezpieczone kratami.
- Zbiory danych osobowych w formie papierowej przechowywane są w zamkniętej nie metalowej szafie.
- Zbiory danych osobowych (akta osobowe) w formie papierowej przechowywane są w zamkniętej nie metalowej szafie.
- Kopie zapasowe/archiwalne zbiorów danych osobowych przechowywane są na dysku zewnętrznym.
- Pomieszczenia, w którym przetwarzane są zbiory danych osobowych zabezpieczone są przed skutkami pożaru wolno stojącymi gaśnicami.
- Dokumenty kat. „B” zawierające dane osobowe po upływie okresu przechowywania i utracie przydatności, w tym do celów dowodowych są za zgodą Archiwum Państwowego niszczone poprzez spalenie lub zniszczenie w niszczarce. Natomiast dokumenty kat. „Bc” zawierające dane osobowe, które nie podlegają archiwizacji, po ich wykorzystaniu na stanowisku pracy, w porozumieniu z archiwistą i za zgodą Archiwum Państwowego są niszczone w niszczarce.

b. Środki sprzętowe, infrastruktury informatycznej i telekomunikacyjnej.

- Zbiory danych osobowych przetwarzane są przy użyciu komputerów stacjonarnych i na laptopach.
- Komputery służące do przetwarzania danych osobowych są połączone z lokalną siecią komputerową.
- Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
- Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.

- Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.
- Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.
- Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.
- Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
- Użyto system Firewall do ochrony dostępu do sieci komputerowej.

c. Środki ochrony w ramach systemowych narzędzi programowych i baz danych.

- Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbiorów danych osobowych.
- Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanych zbiorów danych osobowych.
- Dostęp do zbiorów danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
- Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
- Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbiorów danych osobowych.
- Zastosowano kryptograficzne środki ochrony danych osobowych.
- Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
- Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.
- Dodatkowe środki ochrony technicznej systemu informatycznego, jak również wszystkie niezbędne informacje dotyczące jego pracy oraz zasad użytkowania, określa Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

d. Procedura bezpieczeństwa sprzętu poza siedzibą Instytucji.

- Użytkownik komputera przenośnego poza siedzibą instytucji ma obowiązek jego ochrony.
- Zabrania się pozostawiania komputerów przenośnych bez opieki w miejscach, gdzie użytkownik nie ma możliwości sprawowania nad nim skutecznego nadzoru.
- Osoba używająca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania, przestrzegając jednocześnie zaleceń producentów dotyczących ochrony sprzętu
- Korzystanie z komputera przenośnego w miejscach publicznych i innych niechronionych miejscach poza siedzibą instytucji wymaga ostrożności, by nie ujawnić danych osobom nieupoważnionym.
- Użytkowanie komputera przenośnego/dysku zewnętrznego/pendrive poza siedzibą instytucji dopuszczanie jest tylko za zgodą Administratora. Wzór zgody na użytkowanie komputera poza siedzibą instytucji stanowi formularz nr 13.

- Użytkownik komputera przenośnego/dysku zewnętrznego/pendrive jest zobowiązany złożyć oświadczenie, którego wzór stanowi formularz nr 14,
- W przypadku utraty komputera przenośnego/dysku zewnętrznego/pendrive użytkownik niezwłocznie powiadamia o tym fakcie swojego bezpośredniego przełożonego, a w przypadku kradzieży dokonuje również niezwłocznego zgłoszenia faktu popełnienia przestępstwa na Policji. W zawiadomieniu użytkownik, poza danymi ogólnymi, podaje okoliczności utraty komputera oraz opis charakteru utraconych danych wraz z podaniem ich znaczenia. W szczególności w zawiadomieniu należy określić, czy utracone dane miały charakter danych osobowych.

e. Szkolenie pracowników.

IDO na polecenie Administratora, osobiście lub przy wykorzystaniu podmiotu zewnętrznego, przeprowadza okresowe szkolenia pracowników w zakresie przepisów prawa oraz uregulowań wewnętrznych.

Szkolenia:

- Okresowe odbywają się nie rzadziej niż raz w roku.
- Pracownicy nowozatrudnieni przed przystąpieniem do pracy podlegają szkoleniu przez IOD z zakresu ochrony danych osobowych.
- Ze szkoleń grupowych sporządza się listę obecności pracowników biorących udział, którą przechowuje IOD.

f. Zasady aktualizacji Polityki bezpieczeństwa.

1. Aktualizację Polityki bezpieczeństwa przeprowadza się na wniosek IOD lub ASI.

2. Przyczynami prowadzącymi do aktualizacji Polityki bezpieczeństwa są następujące czynniki:

- Zgłoszenie ASI lub IOD przez pracownika ważnego problemu lub trudności w przestrzeganiu zasad zwartych w aktualnie obowiązującej Polityce bezpieczeństwa.
- Wykrycie przez ASI lub IOD nieprawidłowości w obowiązującej Polityce bezpieczeństwa,
- Wystąpienie zmian w obowiązujących przepisach związanych z Polityką bezpieczeństwa.
- Wejście w życie nowych przepisów, które mogą mieć wpływ na treść Polityki bezpieczeństwa.
- Likwidacja, utworzenie lub zmiany zawartości informacyjnej zbioru danych.

g. Następstwa grożące za nieprzestrzeganie Polityki bezpieczeństwa

1. Pracownicy zobowiązani są do zapoznania i bezwzględnego stosowania wszystkich obowiązujących w instytucji przepisów i zarządzeń wewnętrznych dotyczących ochrony danych.

2. Za nieprzestrzeganie zasad Polityki bezpieczeństwa pracownik ponosi odpowiedzialność na zasadach określonych w Kodeksie Pracy, Kodeksie Karnym oraz ustawie o ochronie danych osobowych.

3. Nieprzestrzeganie Polityki bezpieczeństwa stanowi ciężkie naruszenie obowiązków pracowniczych.

h. Postepowanie z kluczami.

1. Klucze główne:

- Administrator wyznacza osoby, które są upoważnione do otwierania i zamykania głównych drzwi wejściowych przed rozpoczęciem i po zakończeniu pracy.
- Osoby upoważnione, którym zostały powierzone klucze do głównych drzwi są zobowiązane do wykorzystywania ich zgodnie z przeznaczeniem oraz nie kopiowania bez zgody Administratora oraz nie udostępniania osobom trzecim.

2. Klucze dostępowe do pomieszczeń wewnętrznych:

- Klucze do poszczególnych pomieszczeń znajdują się w skrzynce zlokalizowanej w pomieszczeniu Biura.
- Osoby, które zostały upoważnione do dostępu do skrzynki zlokalizowanej w pomieszczeniu Biura są zobowiązane do zabezpieczenia kluczy i wykorzystywania ich zgodnie z przeznaczeniem oraz nie kopiowania ich bez zgody Administratora oraz nie udostępniania osobom trzecim.

3. Klucze do biurek stanowiskowych i szaf:

- Do kluczy od biurek stanowiskowych, szaf biurowych, dostęp mają upoważnione przez Administratora osoby, które zobowiązane są do ich zabezpieczenia w indywidualny, właściwy do każdej sytuacji sposób, poprzez stosowanie odpowiednich środków technicznych i organizacyjnych.
- Osoby, które zostały upoważnione do kluczy od biurek stanowiskowych, szaf biurowych, są zobowiązane do wykorzystywania ich zgodnie z przeznaczeniem oraz nie kopiowania bez zgody Administratora oraz nie udostępniania osobom trzecim.

Rozdział II
Instrukcja zarzadzania systemem informatycznym

Charakterystyka systemu informatycznego

§ 11

1. Sieć informatyczna, w której przetwarzane są dane osobowe stanowią wszystkie pracujące obecnie i przyszłe planowane serwery, komputery stacjonarne i przenośne, a także urządzenia peryferyjne i sieciowe.

2. Sygnał internetowy dostarczany jest przez usługodawcę internetowego i odpowiednio zabezpieczony.

3. System zabezpieczony jest oprogramowaniem antywirusowym zainstalowanym, na każdym stanowisku.

4. Serwera posiada zasilanie awaryjne utrzymujące stałe zasilanie oraz posiada oprogramowanie antywirusowe.

Ogólne zasady pracy w systemie informatycznym

§ 12

1. IOD lub ASI odpowiada za korygowanie niniejszej instrukcji w przypadku uzasadnionych zmian w przepisach prawnych dotyczących przetwarzania danych osobowych w systemach informatycznych, jak również zmian organizacyjno-funkcjonalnych.

2. Przetwarzanie danych w systemie informatycznym może być realizowane wyłącznie poprzez dopuszczone przez ASI do eksploatacji licencjonowane oprogramowanie.

3. ASI prowadzi ewidencję oprogramowania.

4. Do eksploatacji dopuszcza się systemy informatyczne wyposażone w:

- Mechanizmy kontroli dostępu umożliwiające autoryzację użytkownika, z pominięciem narzędzi do edycji tekstu.
- Mechanizmy ochrony poufności, dostępności i integralności informacji, z uwzględnieniem potrzeby ochrony kryptograficznej.

- Mechanizmy umożliwiające wykonanie kopii bezpieczeństwa oraz archiwizację danych, niezbędne do przywrócenia prawidłowego działania systemu po awarii.
- Urządzenia niwelujące zakłócenia i podtrzymujące zasilanie.
- Mechanizmy monitorowania w celu identyfikacji i zapobiegania zagrożeniom, w szczególności pozwalające na wykrycie prób nieautoryzowanego dostępu do informacji lub przekroczenia przyznanych uprawnień w systemie.
- Mechanizmy zarządzania zmianami.

5. Użytkownikom zabrania się:

- Korzystania ze stanowisk komputerowych podłączonych do sieci informatycznej poza godzinami i dniami pracy bez pisemnej zgody Administratora.
- Udostępniania stanowisk roboczych osobom nieuprawnionym.
- Wykorzystywania sieci komputerowej w celach innych niż wyznaczone przez Administratora.
- Samowolnego instalowania i używania programów komputerowych.
- Korzystania z nielicencjonowanego oprogramowania oraz wykonywania jakichkolwiek działań niezgodnych z ustawą o ochronie praw autorskich.
- Umożliwiania dostępu do zasobów wewnętrznej sieci informatycznej oraz sieci Internetowej osobom nieuprawnionym.
- Używania komputera bez zainstalowanego oprogramowania antywirusowego.

Procedura nadawania uprawnień do przetwarzania danych osobowych

§ 13

1. Użytkowników systemu informatycznego tworzy oraz usuwa ASI na podstawie zgody IOD.

2. Do przetwarzania danych osobowych zgromadzonych w systemie informatycznym jak również w rejestrach tradycyjnych wymagane jest upoważnienie.

3. Wprowadza się rejestr osób upoważnionych do przetwarzania danych osobowych, który stanowi formularz nr 3.

4. Uprawnienia do pracy w systemie informatycznym odbierane są czasowo, poprzez zablokowanie konta w przypadku:

- Nieobecności pracownika w pracy trwającej dłużej niż 30 dni kalendarzowych.
- Zawieszenia w pełnieniu obowiązków służbowych.

5. Uprawnienia do przetwarzania danych osobowych odbierane są trwale w przypadku ustania stosunku pracy.

6. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia nawet w przypadku ustania stosunku pracy.

Metody i środki uwierzytelniania

§ 14

1. System informatyczny przetwarzający dane osobowe wykorzystuje mechanizm identyfikatora i hasła, jako narzędzi umożliwiających bezpieczne uwierzytelnienie.

2. Użytkownik posiadający upoważnienie do przetwarzania danych osobowych powinien posiadać hasło do systemu operacyjnego oraz osobne do baz danych osobowych i aplikacji.

3. Każdy użytkownik systemu informatycznego powinien posiadać odrębny identyfikator, którego nazwa składa się z imienia lub nazwy stanowiska pracy.

4. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika IOD, nadaje inny identyfikator odstępując od ogólnej zasady.

5. W identyfikatorze stosuje się polskie znaki diakrytyczne.

6. Hasło składa się, z co najmniej ośmiu znaków, zawiera, co najmniej jedną literę wielką, jedną cyfrę i jeden znak specjalny.

7. Hasło nie powinno zawierać żadnych informacji, które można skojarzyć z użytkownikiem komputera (imiona najbliższych, daty urodzenia, inicjały itp.) i nie może być sekwencją kolejnych znaków klawiatury.

8. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieupoważniona, użytkownik zobowiązany jest do zgłoszenia tego faktu ASI i do natychmiastowej zmiany hasła.

9. Zmianę hasła należy dokonywać nie rzadziej, niż co 30 dni.

10. Po zapoznaniu się z loginem i hasłem użytkownik zobowiązany jest do ich zniszczenia w odpowiednim urządzeniu niszczącym.

11. Hasło nie może być zapisywane i przechowywane.

12. Użytkownik nie może udostępniać identyfikatora oraz haseł osobom nieupoważnionym.

Procedury rozpoczecia, zawieszenia i zakończenia pracy

§ 15

1. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione.

2. Użytkownik systemu jest odpowiedzialny za zabezpieczenie danych wyświetlanych przez system przed osobami niemającymi uprawnień.

3. Zawieszenie pracy polega na opuszczeniu stanowiska pracy bez wylogowania się i jest dopuszczalne tylko w przypadku pozostania w pomieszczeniu. Użytkownik jest zobowiązany w takiej sytuacji do włączenia wygaszacza ekranu odblokowywanego hasłem.

4. Zabrania się opuszczania stanowiska pracy bez wcześniejszego wylogowania z systemu z zastrzeżeniem pkt 3.

5. Zakończenie pracy polega na wylogowaniu się z systemu i wyłączeniu komputera.

6. Czas rozpoczęcia i kończenia pracy w systemach sieciowych, w tym w systemach przetwarzania danych osobowych, określa Regulamin Pracy.

7. Konieczność pracy w aplikacjach sieciowych w godzinach innych, niż określone w Regulaminie Pracy, powinno być zgłoszone IOD.

8. ASI monitoruje logowanie oraz wylogowanie się użytkowników oraz nadzoruje zakres przetwarzanych przez nich zbiorów danych.

Procedury tworzenia kopii awaryjnych

§ 16

1. Dane osobowe zabezpiecza się poprzez wykonywanie kopii zapasowych.

2. Ochronie poprzez wykonanie kopii podlegają także programy i narzędzia programowe służące przetwarzaniu danych. Kopie programów i narzędzi wykonywane są zaraz po instalacji oraz po każdej aktualizacji na zewnętrznych nośnikach informacji – na serwerze.

3. Zabezpieczeniu poprzez wykonywanie kopii zapasowych podlegają także dane konfiguracyjne systemu informatycznego przetwarzającego dane osobowe, w tym uprawnienia użytkowników systemu.

4. Za proces tworzenia kopii programów i narzędzi programowych oraz danych konfigurujących system odpowiedzialna jest ASI. Kopie przechowywane są przez ASI.

5. Kopie zapasowe mogą być sporządzane automatycznie lub manualnie z wykorzystaniem specjalistycznych urządzeń do wykonywania kopii lub standardowych narzędzi oferowanych przez stacje robocze.

6. Pliki edytorów tekstu lub arkuszy kalkulacyjnych traktowane są, jako kopie zbiorów, z których pochodzą przetwarzane w nich dane i nie są objęte procedurami wykonywania kopii zapasowych.

7. Nośniki, na których są przechowywane kopie danych osobowych powinny być wyraźnie oznaczone.

8. Za bezpieczeństwo kopii awaryjnych przetwarzanych lokalnie odpowiadają poszczególni użytkownicy systemu, którzy je wykonali. Kopie usuwa się niezwłocznie po ustaniu ich użyteczności w sposób uniemożliwiający odtworzenie danych.

9. ASI zobowiązany jest do okresowego wykonywania testów odtworzenia kopii zapasowych.

10. Zewnętrzne nośniki kopii zapasowych, które zostały wycofane z użycia, podlegają zniszczeniu po usunięciu danych osobowych, w odpowiednim urządzeniu niszczącym.

11. Użytkownik tworzy wydruki związane z przetwarzaniem danych osobowych wyłącznie w zakresie i ilości niezbędnej dla celów służbowych w uzgodnieniu z przełożonym.

12. Wszystkie dokumenty, zestawienia i wydruki zawierające dane osobowe powinny być chronione przed dostępem osób nieupoważnionych. Użytkownik przechowuje je w zamkniętej szafie w pomieszczeniu zabezpieczonym przed nieuprawnionym dostępem.

Przechowywanie elektronicznych nośników informacji

§ 17

1. Nośniki danych oraz programów służących do przetwarzania danych osobowych, a także danych konfiguracyjnych systemu informatycznego, przechowuje ASI w odpowiednio zabezpieczonym pomieszczeniu.

2. Dane osobowe mogą być przetwarzane na serwerach, a także na dyskach lokalnych komputerów w lokalizacji ustalonej z IOD. Zabrania się gromadzenia danych osobowych na innych, nieautoryzowanych przez IOD nośnikach danych.

3. W uzasadnionych przypadkach, za zgodą IOD, dane osobowe można przetwarzać na zewnętrznych nośnikach informacji, autoryzowanych przez ASI.

4. Serwery oraz komputery, na których odbywa się przetwarzanie danych osobowych, powinny być zabezpieczone przed utratą danych spowodowaną awarią zasilania poprzez stosowanie specjalnych urządzeń podtrzymujących zasilanie i eliminujących zakłócenia sieci zasilającej.

5. Komputery przenośne oraz inne mobilne nośnik danych osobowych powinny być zabezpieczone ochroną kryptograficzną – powinny być zaszyfrowane.

6. 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 IOD.

7. Nośniki kopii awaryjnych, które zostały wycofane z użycia, podlegają zniszczeniu po usunięciu danych osobowych, w odpowiednim urządzeniu niszczącym przez IOD.

Zabezpieczenie systemu informatycznego przed złośliwym oprogramowaniem

§ 18

1. ASI zapewnia ochronę antywirusową oraz zarządza systemem wykrywającym i usuwającym wirusy i inne niebezpieczne kody.

2. System antywirusowy jest skonfigurowany w następujący sposób:

- Skanowanie dysków zawierających potencjalnie niebezpieczne dane następuje automatycznie po włączeniu komputera.
- Skanowanie wszystkich informacji przetwarzanych w systemie, a zwłaszcza poczty elektronicznej jest realizowane na bieżąco.
- Automatycznej aktualizacji wzorców wirusów.

3. W przypadkach wystąpienia infekcji użytkownik powinien niezwłocznie powiadomić o tym fakcie ASI.

4. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, ASI podejmuje 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 awaryjnych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane.
- Samodzielną ingerencję w zawartość pliku - w zależności od posiadanych narzędzi i oprogramowania.

5. Użytkownicy systemu mają również obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, który chcą wykorzystać.

Informacje o odbiorcach, których dane zostały udostępnione, dacie i zakresie tego udostępnienia

§ 19

1. Dla każdej osoby, której dane są przetwarzane w systemie informatycznym powinny być automatycznie odnotowane następujące dane:

- Dane o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba, że dane te traktuje się, jako dane jawne.
- Sprzeciwu osoby, której dane dotyczą w przypadku zamierzenia przetwarzania jej danych w celach marketingowych lub zamierzenia przekazania jej danych innemu administratorowi.

2. Zapis pkt. 1 nie dotyczy systemów służących do przetwarzania danych ograniczonych do edycji teksu w celu udostępnienia go na piśmie i niezwłocznym usunięciu z systemu.

3. Dla każdej osoby, której dane są przetwarzane w systemie informatycznym, system powinien zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnym rozumieniu formę informacji, o którym mowa w pkt. 1.

4. W uzasadnionych przypadkach uniemożliwiających automatyczne odnotowywanie, o którym mowa w pkt. 1, prowadzi się odrębny Rejestr udostępnień- formularz nr 15.

5. Za udostępnianie danych zgodnie z przepisami prawa odpowiedzialny jest Administrator.

Przesyłanie danych poza obszar przetwarzania

§ 20

1. Urządzenia i nośniki zawierające dane osobowe, przekazywane poza obszar przetwarzania zabezpiecza się w sposób zapewniający poufność i integralność tych danych, w szczególności poprzez zastosowanie ochrony kryptograficznej.

2. W wypadku przesyłania danych osobowych przez sieć internetową pocztą elektroniczną należy każdy z załączników zabezpieczyć ochroną kryptologiczną poprzez nadanie hasła odczytu. Hasło należy przesłać lub podać odbiorcy w innej przesyłce, a najlepiej z wykorzystaniem innych metod komunikacji (telefon, fax, w bezpośredniej rozmowie).

3. Umożliwienie wysyłania danych osobowych tylko z wykorzystaniem określonej aplikacji i tylko przez określonych użytkowników.

4. Zabrania się przekazywania danych przez aplikacje internetowe niewykorzystujące odpowiedniego protokołu szyfrowania (adres internetowy musi być poprzedzony zapisem „https”.

Wykonywanie przeglądów i konserwacji systemów oraz nosników informacji

§ 21

1. Przeglądy i konserwacje systemu oraz nośników informacji służących do przetwarzania danych mogą być wykonywane jedynie przez osoby posiadające upoważnienie wydane przez Administratora lub posiadające umowy na powierzenie przetwarzania danych osobowych w zakresie konserwacji i napraw.

2. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wymaganego poziomu zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych, w szczególności poprzez bezpośredni nadzór prowadzony przez IOD.

3. W przypadku uszkodzenia zestawu komputerowego, laptopa lub nośniki danych, na których są przechowywane dane osobowe powinny zostać zabezpieczone przez ASI.

4. W przypadku konieczności przeprowadzenia prac serwisowych poza instytucję dane osobowe znajdujące się w naprawianym urządzeniu muszą zostać w sposób trwały usunięte.

5. Jeżeli nie ma możliwości usunięcia danych z nośnika na czas naprawy komputera, należy zapewnić stały nadzór nad tym nośnikiem przez osobę upoważnioną do przetwarzania danych osobowych na nim zgromadzonych.

6. ASI wykonuje okresowy przegląd nośników danych osobowych eliminując te, które nie zapewniają odpowiedniego poziomu bezpieczeństwa oraz niezawodności.

ROZDZIAŁ III

Analiza zagrożeń i ryzyka przy przetwarzaniu danych osobowych

§ 22

1. Analiza zagrożeń i ryzyka w instytucji określa środki zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych. Analiza ryzyka jest kluczowym elementem procesu bezpieczeństwa teleinformatycznego.
2. Ilekroć w analizie zagrożeń i ryzyka jest mowa o:
a. dostępności – należy przez to rozumieć właściwość określającą, że zasób systemu informatycznego jest możliwy do wykorzystania na żądanie, w określonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym,
b. incydencie bezpieczeństwa teleinformatycznego – należy przez to rozumieć pojedyńcze zdarzenie lub serię zdarzeń, związanych z bezpieczeństwem informacji, które zagrażają ich poufności, dostępności lub integralności,
c. informatycznym nośniku danych – należy przez to rozumieć materiał służący do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej,
d. integralność – należy przez to rozumieć właściwość określającą, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony,
e. oprogramowanie złośliwe – należy przez to rozumieć oprogramowanie , którego celem jest przeprowadzenie nieuprawnionych lub szkodliwych działań w systemie teleinformatycznym,
f. podatność- należy przez to rozumieć słabość zasobów lub zabezpieczenia systemu teleinformatycznego, która może zostać wykorzystana przez zagrożenie,
g. połączeniu miedzysystemowym – należy przez to zrozumieć techniczne lub organizacyjne połaczenie dwóch lub więcej systemów teleinformatycznych, umożliwiajace ich współpracę, a w szczególności wymianę danych,
h. poufność – należy przez to rozumieć właściwość określającą, że informacja nie jest ujawniana podmioto do tego nieuprawnionym,
i. przekazywanie informacji – należy przez to rozumieć zarówno transmisję informacji, jak i przekazywanie informacji na informatycznych nośnikach danych, na których zostały utrwalone,
j. test bezpieczeństwa – należy przez to rozumieć testy poprawności i skuteczności funkcjonowania zabezpieczeń w systemie teleinformatycznym,
k. zabezpieczeniu – należy przez to rozumieć środki o charakterze fizycznym, technicznym lub organizacyjnym zmniejszające ryzyko,
l. zagrożeniu – należy przez to rozumieć potencjalną przyczynę niepożądanego zdarzenia, które może wywołać szkodę w zasobach systemu teleinformatycznego,
m. zasobach systemu teleinformatycznego – należy przez to rozumieć informacje przetwarzane w systemie teleinformatycznym, jak również osoby, usługi, oprogramowanie, dane i sprzęt oraz inne elementy mające wpływ na bezpieczeństwo tych danych.
3. W czasie przetwarzania danych osobowych w instytucji informacje występują w postaci :
a. plików lub informacji przechowywanych na dysku twardym komputera stacjonarnego/laptopa,
b. plików lub informacji przechowywanych w pamięci operacyjnej komputera stacjonarnego/laptopa,
c. plików lub informacji zapisanych w nośnikach komputerowych,
d. wersji roboczych lub gotowych dokumentów wydrukowanych na papierze.
4. Bezpieczeństwo przetwarzanych i przechowywanych informacji zawierajacych dane osobowe wymaga:
a. zapewnienia ochrony fizycznej stanowiska komputerowego przed nieuprawnionym dostępem,
b. ochrony nośników technicznych i wydruków dokumentów wytworzonych przy pomocy sprzętu komputerowego, w tym określenia zasad postępowania z nimi w celu zabezpieczenia przez

nieuprawnionym dostępem,
c. zabezpieczenia przed nieupoważnionym dostępem do danych osobowych znajdujacych się w zasobach systemu informatycznego,
d. zapewnienia dostępności do danych osobowych znajdujących się na technicznych nośnikach informacji oraz pamięci systemu informatycznego dla upoważnionych użytkowników,
e. zapewnienia możliwości kontroli dostępu do zasobów systemu informatycznego oraz wykonywania na nich czynności,
f. zapewnienia możliwości kontroli nośników, na których przetworzono lub przechowywano dane osobowe.

Zagrożenia dla systemu (poufność)

§ 23

1. Poufność to zapewnienie, że dane osobowe nie są udostępniane nieupoważnionym podmiotom.
2. Czynniki zagrażające poufności :
a. nieuprawniony dostęp do pomieszczeń, w których przetwarzane są dane osobowe,
b. ujawnienie haseł dostępu do stanowiska komputerowego, na którym przetwarzane są dane osobowe,
c. nieuprawnione przeniesienie informacji zawierającej dane osobowe na inny nośnik komputerowy,
d. utrata nośnika komputerowego zawierajacego dane osobowe,
e. klęska żywiołowa, w wyniku której utracono poufność danych osobowych,
f. nieuprawnione wynisienie danych osobowych zawartych na nosniku elektronicznym.
3.Ocena ryzyka utraty poufności przetwarzanych danych osobowych polega na zwartościowaniu (przy pomocy skali punktowej) skutku i prawdopodobieństwa wystąpienia ryzyka.
4. Zasady określania skutku oraz prawdopodobieństwa wystąpienia ryzyka określa formularz nr 16.
5. Zidentyfikowane ryzyka utraty poufności przetwarzanych danych osobowych podlegają analizie pod kątem prawdopodobieństwa wystąpienia oraz jego wpływu (skutku) na przebieg procesów i wykonywanych zadań przez instytucję.
6. W ramach analizy, dokonuje się punktowej oceny ryzyka podejmowanego w związku z realizowanym zadaniem zarówno przed, jak i po wprowadzeniu mechanizmów kontrolnych tj. Polityki bezpieczeństwa, instrukcji, czy też innych obowiązujących regulacji normatywnych.
7.Istotność ryzyka jest iloczynem wartości prawdopodobieństwa wystąpienia ryzyka oraz wartości skutku zaistnienia ryzyka.
8.Ocenę prawdopodobieństwa wystąpienia czynników zagrażających poufności dokonuje się w skali punktowej od 1 o 5, gdzie:
a. Bardzo małe – 1,
b. Małe prawdopodobne – 2,
c. Średnie – 3,
d. Prawdopodobne – 4,
e) Prawie pewne – 5.
9. Ocenę skutków zaistnienia ryzyka utraty poufności dokonywana jest w skali od 1 do 5, gdzie:
a. Oddziaływanie nieznaczne - 1,
b. Oddziaływanie małe - 2,
c. Oddziaływanie średnie -3,
d. Oddziaływanie poważne - 4,
e. Oddziaływanie katastrofalne - 5.
10. W celu określenia poziomu istotności ryzyka i reakcji na ryzyko, wyniki analizy ryzyka należy porównać z mapą ryzyka – formularz nr 16.
11. W zależności od poziomu istotności zidentyfikowanego ryzyka dla poufności danych osobowych, IOD rekomenduje działania mające na celu ograniczenie negatywnego wpływu ryzyka na poufność

przetwarzanych danych osobowych.
12. Przyjmuje się następujące zasady akceptowalności ryzyka utraty poufności przetwarzania danych osobowych:
a. Ryzyko niskie - to ryzyko akceptowalne, należy je monitorować oraz poddawać systematycznej ocenie zgodnie z obowiązującymi zasadami (skala od 0,00 – 4,99),
b. Ryzyko średnie - to ryzyko akceptowalne, jeżeli podlega stałemu monitorowaniu, ale należy ograniczać jego wpływ na działalność instytucji, poprzez wprowadzenie dodatkowych mechanizmów kontrolnych (skala od 5,00 – 12,99),
c. Ryzyko wysokie – stanowi realne zagrożenie dla poufności przetwarzanych danych osobowych przez instytucję, w żadnym wypadku nie podlega akceptacji i wymaga natychmiastowej interwencji ADO (skala od 13,00 – 25,00).

Zagrożenia dla systemu (rozliczalność)

§ 24

1. Rozliczalność to właściwość zapewniająca, że działania podmiotu przetwarzającego dane osobowe mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
2. Czynniki zagrażające rozliczalności:
a. brak kontroli nad dokumentami wykonywanymi na stanowisku komputerowym w zakresie ich kopiowania i drukowania,
b. wyparcie się pracy na stanowisku komputerowym, gdzie przetwarzane są dane osobowe,
c. wprowadzenie zmian w treści dokumentu zawierającego dane osobowe,
d. błędy oprogramowania lub sprzętu.
3.Ocena ryzyka utraty rozliczalności przetwarzanych danych osobowych polega na zwartościowaniu (przy pomocy skali punktowej) skutku i prawdopodobieństwa wystąpienia ryzyka.
4. Zasady określania skutku oraz prawdopodobieństwa wystąpienia ryzyka określa formularz nr 16.
5. Zidentyfikowane ryzyka utraty rozliczalności przetwarzanych danych osobowych podlegają analizie pod kątem prawdopodobieństwa wystąpienia oraz jego wpływu (skutku) na przebieg procesów i wykonywanych zadań przez instytucję.
6. W ramach analizy, dokonuje się punktowej oceny ryzyka podejmowanego w związku z realizowanym zadaniem zarówno przed, jak i po wprowadzeniu mechanizmów kontrolnych tj. Polityki bezpieczeństwa, instrukcji, czy też innych obowiązujących regulacji normatywnych.
7.Istotność ryzyka jest iloczynem wartości prawdopodobieństwa wystąpienia ryzyka oraz wartości skutku zaistnienia ryzyka.
8.Ocenę prawdopodobieństwa wystąpienia czynników zagrażających rozliczalności przetwarzanych danych osobowych dokonuje się w skali punktowej od 1 o 5, gdzie:
a. Bardzo małe – 1,
b. Małe prawdopodobne – 2,
c. Średnie – 3,
d. Prawdopodobne – 4,
e) Prawie pewne – 5.
9. Ocenę skutków zaistnienia ryzyka utraty rozliczalności przetwarzanych danych osobowych dokonywana jest w skali od 1 do 5, gdzie:
a. Oddziaływanie nieznaczne - 1,
b. Oddziaływanie małe - 2,
c. Oddziaływanie średnie -3,
d. Oddziaływanie poważne - 4,
e. Oddziaływanie katastrofalne - 5.
10. W celu określenia poziomu istotności ryzyka i reakcji na ryzyko, wyniki analizy ryzyka należy porównać z mapą ryzyka – formularz nr 16.
11. W zależności od poziomu istotności zidentyfikowanego ryzyka dla rozliczalności przetwarzanych danych osobowych, IOD rekomenduje działania mające na celu ograniczenie negatywnego wpływu

ryzyka na rozliczalność przetwarzanych danych osobowych.
12. Przyjmuje się następujące zasady akceptowalności ryzyka utraty rozliczalności przetwarzania danych osobowych:
a. Ryzyko niskie - to ryzyko akceptowalne, należy je monitorować oraz poddawać systematycznej ocenie zgodnie z obowiązującymi zasadami (skala od 0 – 4,99),
b. Ryzyko średnie - to ryzyko akceptowalne, jeżeli podlega stałemu monitorowaniu, ale należy ograniczać jego wpływ na działalność instytucji, poprzez wprowadzenie dodatkowych mechanizmów kontrolnych (skala od 5,00 – 12,99),
c. Ryzyko wysokie – stanowi realne zagrożenie dla rozliczalności przetwarzanych danych osobowych przez instytucję, w żadnym wypadku nie podlega akceptacji i wymaga natychmiastowej interwencji ADO (skala od 13,00 – 25,00).

Zagrożenia dla systemu (integralność)

§ 25

1. Integralność to zapewnienie, aby wszelkie zmiany wykonywane w systemie informatycznym, w systemie jego katalogów oraz poszczególnych plikach zawierających dane osobowe były skutkiem zaplanowanych działań użytkowników systemu. Integralność to właściwość zawierajaca zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
2. Czynniki zagrażające integralności:
a. nielegalny dostęp do danych osobowych, w tym do stanowiska komputerowego,
b. błędy, pomyłki,
c. brak mechanizmów uniemożliwiających skasowanie lub zmianę logów przez administratora lub innego uzytkownika,
d. wadliwe działanie systemu operacyjnego,
e. wirus,
f. brak w wykorzystywanych aplikacjach mechanizmów zapewniajacych integralność danych.
3.Ocena ryzyka utraty integralności przetwarzanych danych osobowych polega na zwartościowaniu (przy pomocy skali punktowej) skutku i prawdopodobieństwa wystąpienia ryzyka.
4. Zasady określania skutku oraz prawdopodobieństwa wystąpienia ryzyka określa formularz nr 16.
5. Zidentyfikowane ryzyka utraty integralności przetwarzanych danych osobowych podlegają analizie pod kątem prawdopodobieństwa wystąpienia oraz jego wpływu (skutku) na przebieg procesów i wykonywanych zadań przez instytucję.
6. W ramach analizy, dokonuje się punktowej oceny ryzyka podejmowanego w związku z realizowanym zadaniem zarówno przed, jak i po wprowadzeniu mechanizmów kontrolnych tj. Polityki bezpieczeństwa, instrukcji, czy też innych obowiązujących regulacji normatywnych.
7.Istotność ryzyka jest iloczynem wartości prawdopodobieństwa wystąpienia ryzyka oraz wartości skutku zaistnienia ryzyka.
8.Ocenę prawdopodobieństwa wystąpienia czynników zagrażających integralności przetwarzanych danych osobowych dokonuje się w skali punktowej od 1 o 5, gdzie:
a. Bardzo małe – 1,
b. Małe prawdopodobne – 2,
c. Średnie – 3,
d. Prawdopodobne – 4,
e) Prawie pewne – 5.
9. Ocenę skutków zaistnienia ryzyka utraty integralności przetwarzanych danych osobowych dokonywana jest w skali od 1 do 5, gdzie:
a. Oddziaływanie nieznaczne - 1,
b. Oddziaływanie małe - 2,
c. Oddziaływanie średnie -3,
d. Oddziaływanie poważne - 4,

e. Oddziaływanie katastrofalne - 5.
10. W celu określenia poziomu istotności ryzyka i reakcji na ryzyko, wyniki analizy ryzyka należy porównać z mapą ryzyka – formularz nr 16.
11. W zależności od poziomu istotności zidentyfikowanego ryzyka dla integralności przetwarzanych danych osobowych, IOD rekomenduje działania mające na celu ograniczenie negatywnego wpływu ryzyka na integralność przetwarzanych danych osobowych.
12. Przyjmuje się następujące zasady akceptowalności ryzyka utraty integralności przetwarzania danych osobowych:
a. Ryzyko niskie - to ryzyko akceptowalne, należy je monitorować oraz poddawać systematycznej ocenie zgodnie z obowiązującymi zasadami (skala od 0 – 4,99),
b. Ryzyko średnie - to ryzyko akceptowalne, jeżeli podlega stałemu monitorowaniu, ale należy ograniczać jego wpływ na działalność instytucji, poprzez wprowadzenie dodatkowych mechanizmów kontrolnych (skala od 5,00 – 12,99),
c. Ryzyko wysokie – stanowi realne zagrożenie dla integralności przetwarzanych danych osobowych przez instytucję, w żadnym wypadku nie podlega akceptacji i wymaga natychmiastowej interwencji ADO (skala od 13,00 – 25,00).

Zagrożenia dla stanowisk komputerowych

§ 26

1. Źródłami zagrożeń dla stanowisk komputerowych, gdzie przetwarza się dane osobowe, mogą być :
a. siły natury (zdarzenia, które nie wynikają z działalności człowieka):
- uderzenia pioruna,
- pożar będacy konsekwencja uderzenia pioruna,
- starzenie się sprzętu,
- starzenie się nośników pamięci,
- smog, kurz,
- katastrofa budowlana,
- ulewny daszcz,
- huragan,
- ekstremalne temperatury, wilgotność,
- epidemia.

b. ludzie (mogą to być pracownicy lub osoby z zewnątrz, które działają w sposób celowy lub przypadkowy):
- błedy i pomyłki uzytkowników,
- błedy i pomyłki administratorów,
- błędy utrzymania systemu w poufności, integralności i rozliczalności,
- zaniedbania użytkowników przy przesyłaniu, udostępnianiu lub kopiowaniu,
- zagubienie nośników zawierających dane osobowe,
- niewłaściwe zniszczenie nośnika,
- nielegalne użycie oprogramowania,
- choroba ważnych osób i nieuprawnione zastępstwo,
- epidemia kadry i brak osób upoważnionych do dostępu,
- podpalenie obiektu,
- zalanie wodą,
- katastrofa budowlana będaca konsekwencją przypadkowego działania człowieka,
- zakłócenia elektromagnetyczne, radiotechniczne,
- podłożenie i wybuch bomby, ładunku wybuchowego,
- użycie broni,
- zmiany napiecia w sieci,

- utrata pradu,
- zbieranie się ładunków elektrostatycznych,
- utrata kluczowych pracowników,
- niedobór pracowników,
- defekty oprogramowania,
- szpiegostwo,
- terroryzm,
- wandalizm,
- destrukcja zbiorów i programów impulsem elektromagnetycznym,
- kradzież,
- włamanie do systemu,
- wyłudzenie, fałszowanie dokumentów,
- podszycie się pod uprawnionego użytkownika,
- podsłuch,
- użycie złośliwego oprogramowania,
- wykorzystanie promieniowania ujawniajacego.

2. Każde z wyżej wymienionych zagrożeń wynikających z działalności człowieka może być ograniczone poprzez :
a. rygorystyczne przestrzeganie zasad postępowania z danymi osobowymi,
b. fizyczne zabezpieczenie obiektu, w którym działa system,
c. wdrożenie systemu kontroli użytkowników,
d. brak połączenia stanowisk komputerowych systemu z siecią internetową.
3. Zagrożenia wynikajace z działania sił natury można ograniczyć poprzez właściwe zabezpieczenie budynków i pomieszczeń, w których znajdują się stanowiska komputerowe, na których przetwarza się dane osobowe.
4. Potencjalne ataki mogą być wyponywne poprzez:
a. podsłuch,
b. wyłudzenie,
c. falszowanie dokumentów,
d. wykorzystywanie promieniowania ujawniającego.

Zagrożenia dla systemu

§ 27

1. Zagrożenia dla systemu to wszystkie niekorzystne czynniki mogące przyczynić się w trakcie pracy z danymi osobowymi do wystąpienia incydentów, mogacych mieć wpływ na ich ujawnienie bądź utratę tzn.:
a. poufność – właściwość polegajaca na tym,że informacja nie jest dostępna lub wyjawiona nieuprawnionym osobom, podmiotom lub procesorom.
b. rozliczalność – właściwość pozwalajaca na rozliczenie osoby pracującej na stanowisku komputerowym systemu przetwarzającego dane osobowe w zakresie dostępu do pomieszczenia, w którym ono jest zainstalowane oraz rozliczenie czynności wykonywanych przy pomocy tego stanowiska komputerowego, w systemie katalogów oraz pojedyńczych zbiorów,
c. integralność – właściwość polegajaca na zapewnieniu dokładności , kompletności aktywów.

Stopień ważności informacji

§ 28

1. Stopień ważności informacji zawierajacych dane osobowe określa poziom ochrony oraz zastosowanie właściwych środków bezpieczeństwa.
2. W instytucji przetwarza się dane osobowe zwykłe i wrażliwe – merytorycznie związane z zakresem zadań realizowanych przez instytucję oraz zakresami obowiązków użytkowników.
3. Ponieważ przeważająca część danych osobowych w instytucji przetwarzana jest w sposób tradycyjny, a tylko nieznaczna część danych przetwarzana jest za pomocą komputerów, wielkość potencjalnych skutów ujawnienia lub utraty informacji w nich zawartych jest stosunkowo mała, dlatego też należy oszacować poziom utraty poufności, jako obarczone ryzykiem niskim (poziom -1,332) Dotyczy to każdej kategorii w/w przetwarzanych zasobów danych osobowych.
4. Wytwarzane dokumenty zawierajace dane osobowe są rejestrowane, przechowywane do wglądu, a następnie niszczone lub archiwizowane przez osoby posiadajace stosowne uprawnienia.
5. Kopie zapasowe tworzone są na pendrive. Można zatem określić wymgania zawiązane z zachowaniem rozliczalności jako obarczone
ryzykiem niskim (poziom – 1,000).
6. Dokładność i kompletność realizowanych czynności w zakresie realizowanych zadań statutowych przez instytucje są zapewnione poprzez odpowiednie usytuowanie stanowisk komputerowych, na których przetwarza się dane osobowe (stanowiska jednoosobowe).
7. Według oceny osób odpowiedzialnych za ochronę danych osobowych, wymagania związane z potrzebą zachowaniem integralności informacji zawierających dane osobowe w systemie są obarczone ryzykiem niskim (wartość -1,000). Dotyczy to każdej kategorii w/w przetwarzanych zasobów danych osobowych.

Podatność systemu na zagrożenia

§ 29

1. Podatność systemu na zagrożenia może wynikać z:
   - dostępności systemu wynikającego np. z braku ochrony fizycznej budynku lub znacznej liczby pracowników mających potencjalny dostęp do systemu oraz wiedzę jak obsługiwać system,
   - dostępność informacji znajdujacych się w systemie za posrednictwem połączeń zewnętrznych,
   - możliwość celowego wprowadzenia luk w sprzęcie i oprogramowaniu lub wprowadzenia wirusów komputerowych,
   - możliwość awarii sprzętu lub oprogramowania ze względu na uszkodzenia, błędy projektowe lub umyślna interwencję,
   - przesłanie informacji przez niezabezpieczone łacze telekomunikacyjne.
2. Podatność systemu na zagrożenia została ograniczona poprzez:
   - ochronę fizyczną stanowisk komputerowych,
   - kontrolę dostępu do pomieszczeń, gdzie przetwarzane są dane osobowe,
   - wydzielenie stref ochronnych,
   - ograniczenie liczby pracowników, mających potencjalnie dostęp do stanowisk komputerowych oraz wiedzę jak je obsługiwać,
   - zbudowanie stabilnej sieci zasilającej,
   - przeglądy okresowe nośników,
   - kontrole zmian konfiguracji,
   - testowanie oprogramowania,
   - audyt teleinformatyczny,
   - zabezpieczenie haseł,

- użycie oprogramowania komputerowego,
- backupy – kopie zapasowe.

3. W celu oszacowania potencjalnych strat wynikajacych z utraty lub ujawnienia danych osobowych przetwarzanych na stanowiskach komputerowych wykonano analizę ryzyka na podstawie przewidywanych zagrożeń dla zasobów.
4. Analiza ryzyka wykonywana jest nie rzadziej niż raz w roku przez IOD przy udziale ASI z wykorzystaniem formularza nr 17.
5. Analiza ryzyka wykonywana jest każdorazowo po zaistnieniu incydenty związanego z naruszeniem zasad ochrony danych osobowych. Analizą objęty jest obszar, w którym doszło do naruszenia zasad przetwarzania danych osobowych. Incydent związany z naruszeniem zasad ochrony danych osobowych jest dokumentowany przez IOD z wykorzystaniem formularza nr 18 na formularzu nr 19.

Analiza zagrożeń i ryzyka

§ 30

1. Analiza zagrożeń i ryzyka polega na identyfikacji ryzyka wystapienia niepożądanego czynnika, określenie jego wielkosci, zidentyfikowania obszarów wymagajacych zabezpieczeń tak, abyto ryzyko zminimalizować lub całkowice je zlikwidować.
2. Aby przeprowadzić poprawna analizę ryzyka na poczatku należy określić:
   - zasoby, które będziemy chronić,
   - zagrożenia – czynnik, który może powodować wystapienie incydentów,
   - skutki – jaki wpływ będzie miał zaistniały incydent na system informatyczny.
3. Zasobami systemu są wszystkie elementy służace do przetwarzania, przechowywania lub przekazywania informacji oraz do zapewnienia im właściwego pozimou bezpieczeństwa , tzn.:
   - sprzet komputerowy przechowujacy dane – dysk twardy,
   - pracownicy przetwarzajacy dane osobowe,
   - aplikacje, w których przetwarzane są dane osobowe,
   - pomieszczenia, w których pracuja osoby przetwarzające dane osobowe,
   - koszty dodatkowych zabezpieczeń oraz odbudowy systemu po incydencie.
4. Podatność systemu to słabości zasobów, które mogą być wykorzystane do ujawnienia informacji lub ich utraty.
5. Skutki określają wysokość strat w systemie informatycznym po zistnieniu incydentu.

ROZDZIAŁ VI

Postanowienia końcowe

§ 31

Traci moc Zarządzenie Nr 3/2018 Dyrektora Zespołu Szkolno-Przedszkolnego w Reńskiej Wsi z dnia 12 stycznia 2018 r. w sprawie wdrożenia dokumentacji ochrony danych osobowych w Zespole Szkolno-Przedszkolnym w Reńskiej Wsi.

§ 32

Wykonanie zarządzenia powierza się Inspektorowi ochrony danych.

§ 33

Zarządzenie wchodzi w życie z dniem podpisania.

.....

(data, podpis Dyrektora)