SZKOŁA PODSTAWOWA
im. Marii Konopnickiej w Mrokowie
05-552 Mroków
ul. Marii Świątkiewicz 2A
tel. 22 756 15 55
REGON: 001147188

Załącznik do zarządzenia nr 7/2021
z dnia 1.09.2021 r.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH
Szkoły Podstawowej im Marii Konopnickiej w Mrokowie

§1
Postanowienia ogólne

1. Niniejszy dokument (dalej: Polityka) jest polityką ochrony danych osobowych w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 **(RODO).**

2. Celem tego dokumentu jest zapewnienie przetwarzania danych osobowych przez Szkołę Podstawową im. Marii Konopnickiej w Mrokowie w sposób zgodny z wymogami prawa. Przy przetwarzaniu danych osobowych, nadrzędnym celem jest ochrona tych danych, poszanowanie prywatności osób, których te dane dotyczą a także możliwie najszersza eliminacja zagrożeń związanych z przetwarzaniem danych.

3. Polityka zawiera opis zasad ochrony danych, wymagania bezpieczeństwa oraz zalecenie szczegółowe, obowiązujących w Szkole Podstawowej in. Marii Konopnickiej w Mrokowie ul. Marii Świątkiewicz 2a 05-552 Mroków, wynikające bezpośrednio z ustawy o ochronie danych osobowych i aktów wykonawczych.

4. Ustanowione w niniejszej polityce zasady muszą być stosowane przez wszystkie osoby posiadające dostęp do danych osobowych.

§2
Podstawowe definicje

a) **Polityka**: oznacza niniejsza Politykę ochrony danych osobowych;
b) **Szkoła**: oznacza Szkołę Podstawową in. Marii Konopnickiej w Mrokowie;
c) **RODO**: oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
d) **Inspektor Ochrony Danych (IOD)**: osoba odpowiedzialna za nadzór nad bezpieczeństwem informacji przetwarzanych w Szkole Podstawowej im Marii Konopnickiej w Mrokowie;
e) **Administrator Danych (ADO)**: podmiot decydujący o celach i środkach przetwarzania danych osobowych tj. Szkoła;
f) **Administrator Systemów Informatycznych(ASI)** - osoba odpowiedzialna za prawidłowe funkcjonowanie systemu informatycznego, oraz wdrożenie zabezpieczeń wymaganych przez przepisy prawa o ochronie danych osobowych.

Osobę powołaną do pełnienia tej funkcji określa Instrukcja zarządzania systemem informatycznym przetwarzającym dane osobowe w Szkole, stanowiąca załącznik nr 1 Polityki Bezpieczeństwa Danych Osobowych.

g) **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;

h) **dane szczególnych kategorii**: oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej;

i) **naruszenie ochrony danych osobowych**: oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

j) **pseudonimizacja**: oznacza przetworzenie danych osobowych w taki sposób, by nie można ich 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;

k) **przetwarzanie**: 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;

§3

Zasady ochrony danych osobowych

1. Dane osobowe przetwarzane w Szkole mogą być uzyskiwane bezpośrednio od osób, których te dane dotyczą, powierzane na podstawie umowy lub gromadzone z innych źródeł, w granicach dozwolonych przepisami prawa;

2. W takcie przyjmowania danych każda osoba upoważniona powinna stworzyć takie warunki, aby ujawniane informacje nie miały możliwości dotrzeć do osób nieuprawnionych, w szczególności do osób postronnych znajdujących się w pomieszczeniu. W miarę możliwości dane należy odbierać w formie pisemnej. Wszelkie sporządzone podczas rozmowy zapiski i notatki, zawierające dane osobowe – o ile nie są potrzebne do dalszego wykorzystania należy zniszczyć.
3. Należy zapewnić, aby dane osobowe były:

   a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (zgodność z prawem, rzetelność i przejrzystość);

   b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami (ograniczenie celu);

c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (minimalizacja danych);

d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane (*prawidłowość);*

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

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

§4

Zadania Administratora Danych

1. Administrator danych realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:
   a) Upoważnia poszczególne osoby do przetwarzania danych osobowych w stosownym, indywidualnie określonym zakresie.
   b) Podejmuje decyzje o powierzeniu danych osobowych podmiotom zewnętrznym;
   c) Wyznacza osoby związane z organizacją przetwarzania danych osobowych i określa ich zadania.
   d) Wyznacza Inspektora Ochrony Danych.
   e) Wdraża dokumentację przetwarzania danych osobowych.
   f) Podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpieczne go przetwarzania danych osobowych.
   g) Podejmuje decyzje o zakresie, celach i środkach przetwarzania i ochrony danych osobowych.
   h) Odpowiada za zgodne z prawem przetwarzanie danych osobowych.
   i) Ocenia ryzyko przetwarzania danych osobowych i podejmuje odpowiednie środki w celu zarządzania nim.

§5

Inspektor Ochrony Danych

1. Inspektor Ochrony Danych (IOD) jest wyznaczany przez Administratora Danych na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wykonywania zadań , o których mowa w art. 39 RODO.
2. Administrator zapewnia, by Inspektor Ochrony Danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
3. Inspektor Ochrony Danych podlega bezpośrednio Dyrektorowi Szkoły, który zapewnia aby nie otrzymywał on instrukcji dotyczących wykonywania przez niego ustawowych zadań.
4. Do zadań Inspektora Ochrony Danych należy:
   a) informowanie administratora, podmioty przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich z

mocy RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

b) monitorowanie przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania

d) współpraca z organem nadzorczym

e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

5. IOD wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.
6. Osoby, których dane dotyczą, mogą kontaktować się z Inspektorem Ochrony Danych we wszystkich sprawach związanych z przetwarzanie ich danych oraz z wykonywaniem praw przysługującym na mocy RODO.
7. Inspektor Ochrony Danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań.

§6

Zapewnienie ochrony danych osobowych w fazie planowania.

1. Administrator Danych Osobowych wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danych osoby niekreślonej liczbie osób fizycznych.
2. Wszelkie plany projektów, które będą opierały się o przetwarzanie danych osobowych wymagają powzięcia uprzedniej opinii IOD:.
   a) IOD sprawdza:
      - przesłanki legalności przetwarzania danych osobowych
      - zatwierdza zakres zbieranych danych
      - zatwierdza czas przetwarzania danych osobowych
      - zatwierdza dostęp i upoważnia pracowników do przetwarzania danych osobowych.
      - Zatwierdza formularze na jakich zbierane będą dane osobowe.
      - Zatwierdza klauzule zgody i informacyjne.
3. Wszelkie procedury funkcjonujące w Szkole Podstawowej w Mrokowie i zakładające przetwarzanie danych osobowych, przed ich wprowadzeniem lub zmianą, wymagają konsultacji z IOD.
4. Wszelkie formularze, na których zbierane są dane osobowe przed ich wprowadzeniem lub zmianą wymagają konsultacji z IOD.
5. Wszelkie systemy komputerowe służące do przetwarzania danych osobowych lub mające wpływ na działanie systemów przetwarzających dane osobowe, przed ich wprowadzeniem/ zakupem wymagają konsultacji z ASI i IOD.

6. Pracownik obowiązany jest zgłaszać IOD zmianę sposobu przetwarzania danych lub zamiar przetwarzania nowych kategorii danych osobowych. IOD sprawdza warunki techniczne i organizacyjne dotyczące zabezpieczeń danych osobowych; w przypadku niewystarczającego poziomu zabezpieczeń występuje z wnioskiem do Administratora o podniesienie poziomu zabezpieczeń.

§7

Środki techniczne i organizacyjne przetwarzanych danych.

Zabezpieczenia organizacyjne:

a) Został wyznaczony Inspektor Ochrony Danych;
b) została opracowana i wdrożona Polityka bezpieczeństwa przetwarzania danych osobowych;
c) została opracowana i wdrożona Instrukcja zarządzania systemem informatycznym;
d) został opracowany Regulamin przetwarzania danych osobowych zawierający praktyczne wskazówki i instrukcje dla pracowników mających dostęp do danych osobowych w Szkole.
e) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające ważne upoważnienia nadane przez Administratora Danych;
f) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz obowiązujących zabezpieczeń systemu informatycznego;
g) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
h) przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych; w szczególności: wszelkie dokumenty zawierające dane osobowe przechowywane są w zamkniętych szafach, do których dostęp mają tylko pracownicy upoważnieni do przetwarzania danych osobowych, dostęp do pomieszczeń, w których są przetwarzane dane osobowe osób nieupoważnionych jest możliwy tylko w obecności pracowników i pod ich kontrolą;
przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych, obszar przetwarzania danych osobowych został określony w załączniku nr 2;
i) stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami przetwarzającymi dane osobowe łącznie z rejestrem kategorii czynności przetwarzania.

Zabezpieczenia ochrony fizycznej danych osobowych:

Szkoła Podstawowa w Mrokowie znajduje się w budynku piętrowym przy ul. Świątkiewicz 2a w Mrokowie. Wejście do budynku jest zabezpieczone dwoma parami drzwi zamykanych. Szkoła objęta jest system alarmowym, oraz nadzorem dozorcy. W szkole zamontowany jest monitoring wizualny, a wejścia i wyjścia z budynku są rejestrowane na portierni. Pokoje nauczycielskie i klasy zamykane są na klucz. W Szkole opracowano zasady stosowania monitoringu obejmującą również regulacje dotyczące monitoringu wizyjnego stanowiące załącznik nr 7. Szczegółowe zabezpieczenia poszczególnych pomieszczeń są ujęte w rejestrze pomieszczeń stanowiącym załącznik nr 2

Zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej:

Zabezpieczenia stosuje się dla fizycznych elementów systemu, ich połączeń oraz systemów operacyjnych. Szczegółowy opis zabezpieczeń zawarty jest w instrukcji zarządzania systemem informatycznym.

Zabezpieczenia narzędzi programowych i baz danych:

Zabezpieczenia (techniczne i programowe) stosuje się dla aplikacji, programów i innych narzędzi programowych przetwarzających dane osobowe.
Szczegółowy opis zabezpieczeń zawarty jest w Instrukcji zarządzania systemem informatycznym stanowiącej załącznik nr 1.
Regulamin korzystania z poczty elektronicznej określa załącznik nr 3

Udzielenia informacji drogą telefoniczną

Przy udzielaniu informacji drogą telefoniczną, należy zachować szczególną ostrożność. Przed udzieleniem informacji należy upewnić się, że mamy do czynienia z osobą uprawnioną do odbioru danych. W przypadku jakichkolwiek wątpliwości, należy powstrzymać się od udzielania informacji.

Przechowywanie dokumentacji roboczej w trakcie pracy

1. Każdy pracownik zobowiązany jest do przechowywania na biurku tylko tych dokumentów, które są mu niezbędne do pracy w danym momencie. W trakcie pracy dokumenty należy tak przechowywać, aby osoby postronne nie miały do nich wglądu. W szczególności nie należy wykładać na widok dokumentów zawierających dane osobowe, w sytuacji gdy przy stanowisku znajdują się lub mogą się znaleźć osoby postronne.
2. Po zakończeniu pracy z dokumentami zawierającymi dane osobowe należy odłożyć je do szuflady lub szafy zamykanej na klucz.
3. Na biurku nie powinny znajdować się napoje w pojemnikach grożących rozlaniem.

Ustawienia monitorów

Monitory, na których wyświetlane są dane osobowe należy ustawić w taki sposób aby osoby postronne nie miały możliwości wglądu. Przed opuszczeniem stanowiska pracy należy zablokować ekran.

§8

Klauzula informacyjna i zgoda na przetwarzanie danych.

1. Dane osobowe mogę być przetwarzane w oparciu o:
   a) zgodę osoby, której dane dotyczę wraz z określeniem celu przetwarzania tych danych lub
   b) dane niezbędne są do wykonania umowy, której stroną jest osoba, której dane dotyczą lub
   c) dane te są niezbędne do podjęcia działań przed zawarciem umowy, z osobą której dane dotyczą,
   d) przetwarzanie jest niezbędne dla wykonania obowiązku prawnego ciążącego na administratorze,
   e) przetwarzanie jest niezbędne do ochrony żywotnych interesów, której te dane dotyczą lub innej osoby fizycznej,
   f) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
   g) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

2. Każdej osobie fizycznej, której dane są przetwarzane należy udzielić informacji w sposób jasny, czytelny i zrozumiały o:
   a) podstawie przetwarzania danych osobowych
   b) administratorze danych osobowych,
   c) IOD,
   d) celu przetwarzania danych,
   e) okresie przechowywania danych,
   f) prawie dostępu do treści tych danych,
   g) prawie wniesienia skargi do Prezesa UODO,
   h) czy przetwarzanie wynika z obowiązku ustawowego czy umowy.
3. Informacja, o której mowa powyżej powinna również znajdować się w ogólnodostępnym miejscu w budynku szkoły lub na stronie internetowej Szkoły.
4. W przypadku przetwarzania danych, wymagającego zgody na ich przetwarzanie, w klauzuli informacyjnej należy umieścić oświadczenie o zgodzie na przetwarzanie danych.

§9

Upoważnienie i zmiana uprawnień do przetwarzania danych osobowych

1. Do przetwarzania danych osobowych może mieć dostęp wyłącznie pracownik lub zleceniobiorca, który został upoważniony do przetwarzania danych przez Administratora Danych.
2. Dyrektor szkoły, jako Administrator Danych, podejmuje decyzję o nadaniu upoważnia do przetwarzania danych osobowych. Określa on zakres danych do jakich nadaje upoważnienie oraz zakres czynności jakie upoważniony może wykonywać w ramach wykonywanych przez niego obowiązków służbowych oraz czas na jaki nadawane jest upoważnienie.
3. Każdy pracownik przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z następującymi dokumentami:
   - Rozporządzeniem 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.
   - Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych
   - Regulaminem przetwarzania danych osobowych w Szkole, a także jeśli zajmowane stanowisko tego wymaga z niniejszą Polityką bezpieczeństwa informacji i Instrukcją zarządzania systemem informatycznym.
   - Wewnętrznymi procedurami i instrukcjami wymaganymi wobec zajmowanego stanowiska.
4. Zapoznanie się z powyższymi dokumentami użytkownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi załącznik nr 4.
5. Dyrektor szkoły może w każdej chwili cofnąć pracownikowi upoważnienie do przetwarzania danych osobowych w całości lub w części.
6. Wzór dokumentu znajdują się w Załącznikach nr 4.
7. Przyznanie uprawnień do przetwarzania danych osobowych w systemach informatycznych określa Instrukcja zarządzania systemem informatycznym.

§10

Instrukcja alarmowa

1. Instrukcja alarmowa określa zasady postępowania w sytuacji zaistnienia zagrożenia naruszenia zasad ochrony danych osobowych. Instrukcja alarmowa sanowi załącznik nr 5

§11

Rejestr czynności przetwarzania danych osobowych

1. W placówce prowadzi się rejestr czynności przetwarzania danych osobowych w formie elektronicznej lub papierowej.
2. Rejestr, o którym mowa w ust. 1. zawiera co najmniej:
   a) informacje o administratorze danych,
   b) informacje o Inspektorze Ochrony Danych Osobowych,
   c) cel przetwarzania danych,
   d) kategorię osób, których dane te dotyczą,
   e) kategorię danych osobowych,
   f) informację o odbiorcach danych,
   g) planowany termin usunięcia danych,
   h) podjęte środki bezpieczeństwa.
3. Ustalając termin usunięcia danych można wskazać konkretną datę, czasookres lub też odwołać się do innych przyszłych zdarzeń, jak np. do czasu zakończenia obowiązywania umowy i pełnego rozliczenia.

§12

Kontrola przetwarzania danych

Uprawnionym do przeprowadzania kontroli sposobu zabezpieczeń danych osobowych jest IOD. Okresowe sprawdzenia i weryfikacje przeprowadzane mogą być również samodzielnie przez Administratora lub na jego zlecenie przez podmiot zewnętrzny. Mają one na celu stały nadzór nad poziomem zabezpieczeń danych osobowych w Szkole, weryfikację aktualności procedur i ich stosowania. Pozwala także na zgodność z obowiązującymi na dany czas standardami przetwarzania i ochrony danych osobowych jak i obowiązującymi przepisami prawa.

1. Sprawdzenie przeprowadzane w trybie:
   a. sprawdzenia planowanego poszczególnych zbiorów danych osobowych – minimum raz w roku;
   b. sprawdzenia doraźnego - w przypadku zaistnienia lub podejrzenia zaistnienia naruszenia ochrony danych osobowych;
   c. sprawdzenia dla organów nadzorczych, w przypadku kiedy się o po to zwróci.

Czynności sprawdzające.

1. Sprawdzeniu podlegają w szczególności:
   - Stan zabezpieczeń danych przetwarzanych w kartotekach papierowych;
   - Stan zabezpieczeń systemów informatycznych przetwarzających dane osobowe;

- Wypełnienie obowiązku informacyjnego o którym mowa w art. 13 i 14 RODO
- Sprawdzenie przesłanek legalizujących przetwarzanie danych osobowych;
- Weryfikacja czasu retencji danych osobowych.
- Sprawdzenie prawidłowości umów powierzenia danych osobowych;

Czynności pokontrolne.

1. Po dokonaniu kontroli IOD przygotowuje dla Administratora raport zawierający wnioski pokontrolne.
2. W przypadku wykrycia nieprawidłowości Administrator Danych lub IOD:
   a) Uzupełnia braki w dokumentacji lub jej elementach oraz podejmuje działania w celu doprowadzenia dokumentacji do wymaganego stanu.
   b) Poucza lub instruuje osobę nieprzestrzegającą zasad określonych w dokumentacji przetwarzania danych o prawidłowym sposobie ich realizacji, wskazując osobę odpowiedzialną za naruszenie tych zasad oraz jego zakres.
3. Pouczenia lub instrukcje zawierane są w odrębnym dokumencie skierowanym do osoby nieprzestrzegającej zasad określonych w dokumentacji przetwarzania danych.
4. O pouczeniu i zakresie pouczenia zostaje poinformowany bezpośredni przełożony osoby nieprzestrzegającej zasad.
5. Administrator Danych lub IOD może przeprowadzić weryfikację wyrywkowo, na podstawie zgłoszenia osoby trzeciej lub powzięcia z innych źródeł informacji o możliwych nieprawidłowościach.
6. Na podstawie obserwacji i spostrzeżeń poczynionych w trakcie sprawdzenia dokonywana jest weryfikacja opracowania i kompletności dokumentacji przetwarzania danych osobowych, oraz jej zgodności z obowiązującymi przepisami, a także zgodności ze stanem faktycznym i przestrzegania zasad i obowiązków określonych w dokumentacji.

§13

Realizacja praw osób, których dane dotyczą.

1. Szkoła dba o czytelność i sposób przekazywania informacji i komunikowania się z osobami, których dane przetwarza.
   a) Każdy z pracowników ma obowiązek zadbać aby każda czynność mająca na celu zbieranie danych była powiązana z przekazaniem, osobom których dane są zbierane, odpowiedniej klauzuli informacyjnej o której mowa w art. 13 i 14 RODO.
   b) Treść klauzul informacyjnych jest konsultowana z IOD.
   c) Na stronie internetowej Szkoły podawane są: imię i nazwisko oraz jego dane kontaktowe do IOD, w celu umożliwienia sprawnej komunikacji i realizacji praw o których mowa w art. 15- 22 RODO.
   d) Na stronie internetowej Szkoły udostępniana jest klauzula informacyjna opisująca sposób przetwarzania danych osobowych przez Administratora.
   2. Żądanie prawa dostępu do danych
   a) Żądanie sprostowania lub usunięcia danych
   b) Żądanie prawa do ograniczenia przetwarzania danych
   c) Żądanie przeniesienia danych
   d) Wniesienie sprzeciwu do przetwarzania danych osobowych lub cofnięcie zgody na przetwarzanie danych osobowych,
3. Po wpłynięciu żądania w formie pisemnej lub elektronicznej wyszczególnionego w pkt. 2, pracownik ma obowiązek potwierdzić przyjęcie takiego żądania zgodnie z instrukcją kancelaryjną.
4. W przypadku żądania wyrażonego telefonicznie, pracownik sporządza notatkę służbową wskazując dokładnie którego z praw wyszczególnionych w pkt. 2 domaga się osoba, oraz ustala tożsamość tej osoby i sposób kontaktu.
5. Po przyjęciu żądania pracownik przekazuje je niezwłocznie do Inspektora Ochrony Danych.

6. Inspektor Ochrony Danych ustala, czy żądanie jest zasadne i identyfikuje osobę, której dane dotyczą.
7. Pracownicy mają obowiązek współpracować z Inspektorem Ochrony Danych w kwestii spełnienia żądania osoby wyszczególnionego w pkt. 2
8. Osobą uprawnioną do odpowiadania na żądania wyszczególnione w pkt. 2 jest Inspektor Ochrony Danych.

§14

Rejestr pomieszczeń

1. Administrator danych prowadzi rejestr pomieszczeń, w których przetwarzane są dane osobowe. Rejestr ten zawiera co najmniej następujące informacje:
   a) lokalizacja
   b) przeznaczenie pomieszczenia (pomieszczeń),
   c) piętro,
   d) nazwa wydziału użytkującego pomieszczenia,
   e) osoby pracujące w pomieszczeniu (z pominięciem imion i nazwisk),
   f) rodzaj zabezpieczeń.
2. Rejestr, o którym mowa w ust. 1 stanowi Załącznik nr 2 do polityki.

§15

Analiza ryzyka

W Szkole prowadzi się analizę ryzyka dla procesów związanych z pozyskiwaniem danych. Analiza ryzyka prowadzona jest w sposób ciągły, zgodnie z procedurą stanowiącą **Załącznik nr 6** do Polityki i stanowi ona podstawę podejmowania działań zapobiegawczych, w celu wzmocnienia procesu ochrony danych osobowych.

§16

Postanowienia końcowe.

1. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce, Instrukcji zarządzania systemem informatycznym i Regulaminem przetwarzania danych osobowych.
2. Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.
3. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
4. Kara dyscyplinarna, orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

5. W sprawach nieuregulowanych w niniejszej Polityce bezpieczeństwa mają zastosowanie przepisy RODO oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych

Załącznik nr 1
do Polityki Bezpieczeństwa Danych Osobowych
w Szkole Podstawowej im. Marii Konopnickiej w Mrokowie

INSTRUKACJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH w Szkole Podstawowej im. Marii Konopnickiej w Mrokowie

Niniejsza Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej Instrukcją, przyjęta została w celu wykazania, że dane osobowe w systemach informatycznych Szkoły Podstawowej w Mrokowie przetwarzane są w sposób zgodny z przepisami prawa mającymi zastosowanie do takiej czynności, zgodnie z zasadą art. 5 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (dalej RODO).

Definicje:

1. **Administrator Danych** – Szkoła Podstawowa im Marii Konopnickiej w Mrokowie ul. Marii Świątkiewicz 2a 05-552 Mroków, reprezentowana przez Dyrektora Szkoły.
2. **Dane osobowe** – wszelkie informacje, dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
3. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu przetwarzania danych.
4. **Użytkownik** – osoba upoważniona przez Administratora Danych do Przetwarzania danych osobowych w Szkole Podstawowej w Mrokowie.
5. **Sieć lokalna** – połączenie Systemów informatycznych Administratora Danych wyłącznie dla własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych.
6. **Zbiór danych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
7. **Przetwarzanie danych** – jakiekolwiek operacje wykonywane na Danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
8. **Zabezpieczenie danych w systemie informatycznym** – wdrożenie i eksploatacja stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
9. **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym (użytkownika) w razie przetwarzania danych osobowych w takim systemie instrukcja zarządzania systemem informatycznym.
10. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym (użytkownikowi).
11. **Administrator Systemów Informatycznych (ASI)** – osoba odpowiedzialna za zapewnienie bezpieczeństwa danych przetwarzanych w systemach informatycznych.

I. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym

Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych wydane przez Administratora.

1. **Nadawanie i rejestracja uprawnień administratorów.**

a) Administratora Systemu Informatycznego powołuje Administrator.
b) Administrator Systemu Informatycznego odpowiedzialny jest za sprawne funkcjonowanie systemu informatycznego, a także za jego konfigurację zapewniającą ochronę danych osobowych w nim przetwarzanych.
c) Administrator Systemu Informatycznego zobowiązany jest do bieżącej pracy na koncie roboczym. Użycie tzw. konta administratora dopuszczalne jest jedynie w sytuacjach awaryjnych lub podczas poważnych zmian wprowadzanych w administrowanym systemie.
d) W przypadkach awaryjnych (np. nieobecność ASI) hasło może być przekazane decyzją Administratora osobie zastępującej ASI.
e) Po ustaniu sytuacji awaryjnej, ASI jest zobowiązany do zmiany hasła

2. **Nadawanie i rejestracja uprawnień użytkowników.**

a) Do obsługi Systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do Przetwarzania danych, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie wydane przez Administratora Danych,
b) Po upoważnieniu osoby do dostępu do przetwarzania danych osobowych w systemie informatycznym Administrator Systemów Informatycznych nadaje Identyfikator użytkownika. Z chwilą nadania Identyfikatora osoba może uzyskać dostęp do systemów informatycznych w zakresie odpowiednim do danego upoważnienia.
c) Dla każdego Użytkownika Systemu informatycznego ustalony jest odrębny Identyfikator i Hasło.
d) Identyfikator użytkownika nie może być zmieniany, a po wyrejestrowaniu Użytkownika z Systemu informatycznego nie może być przydzielony innej osobie.
e) Identyfikator osoby, która utraciła uprawnienia do dostępu do Danych osobowych, zostaje niezwłocznie wyrejestrowany z Systemu informatycznego, w którym są przetwarzane, zaś Hasło dostępu zostaje unieważnione oraz zostają podjęte inne działania niezbędne w celu zapobieżenia dalszemu dostępowi tej osoby do danych. Instrukcja zarządzania systemem informatycznym.
f) Wyrejestrowanie użytkownika z systemu informatycznego może nastąpić na wniosek Administratora, na rzecz którego były wykonywane czynności związane z przetwarzaniem danych osobowych. Wyrejestrowanie użytkownika z systemu realizuje Administrator Systemu Informatycznego.
g) Administrator lub wskazana przez niego osoba nadzoruje aktualizację wszystkich upoważnień.

3. **Zasady postępowania z hasłami.**

a) ASI informuje użytkownika o nadaniu pierwszego hasła do systemu.
b) Użytkownik systemu zobowiązany jest do niezwłocznej zmiany tego hasła.
c) Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
d) Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.

e) Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.
f) Zabronione jest zapisywanie haseł i umieszczanie ich w widocznym miejscu.

4. **Hasła do sieci.**
   a) Hasło dostępu do sieci składa się co najmniej z 8 znaków.
   b) Hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych.
   c) ASI zobowiązany jest do skonfigurowania systemu informatycznego w taki sposób aby wymuszał on zmianę hasła po upływie 30 dni od dnia ostatniej zmiany hasła.
   d) ASI zobowiązany jest do skonfigurowania dwóch odrębnych punktów dostępu do sieci, dla uczniów i pracowników, w ten sposób aby uczniowie nie mieli dostępu do sieci pracowników.
   e) Hasło do sieci dla uczniów zmieniane jest nie rzadziej niż raz w miesiącu.

5. **Hasła do programów przetwarzających dane osobowe.**
   a) Hasło dostępu do programów składa się co najmniej z 8 znaków.
   b) Hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych.
   c) Zmiana hasła odbywa się raz na 30 dni.
   d) Zmiana hasła jest wymuszana automatycznie.

6. **Hasła administratora.**
   a) Hasło administratora składa się co najmniej z 8 znaków.
   b) Hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych.
   c) Administrator Systemu Informatycznego zobowiązany jest zmieniać swoje hasło nie rzadziej niż co 30 dni.
   d) Administrator Systemu Informatycznego zobowiązany jest do prowadzenia metryk haseł administratora i umieszczenie ich w zamkniętych kopertach, odrębnych dla każdego systemu i umieszczania ich w kasie pancernej.
   e) Metryka hasła powinna zawierać: treść hasła, datę jego wprowadzenia do systemu, datę i powód awaryjnego udostępnienia hasła oraz być przechowywane przez okres 5 lat.
   f) W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp.

II. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przez Użytkowników systemu

1. Pracownik po przyjściu do pracy uruchamia stację roboczą.
2. Przed uruchomieniem komputera należy sprawdzić, czy nie zostały do niego podłączone żadne niezidentyfikowane urządzenia.
3. Po uruchomieniu pracownik loguje się przy pomocy identyfikatora Użytkownika oraz hasła do systemu informatycznego.
4. Użytkownik jest zobowiązany do powiadomienia ASI / IOD o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.
5. Maksymalna ilość prób wprowadzenia hasła przy logowaniu się do systemu przetwarzającego dane osobowe wynosi trzy. Po przekroczeniu tej liczby prób logowania system lokuje dostęp do zbioru danych na poziomie danego użytkownika. Odblokowania konta może dokonać ASI.
6. W trakcie pracy przy każdorazowym opuszczeniu stanowiska komputerowego należy dopilnować, aby na ekranie nie były wyświetlane Dane osobowe.

7. W przypadku bezczynności użytkownika na stacji roboczej przez okres dłuższy niż 1 minuta, automatycznie włączany jest wygaszacz ekranu. Wygaszacze ekranu powinny być zaopatrzone w hasła zbudowane analogicznie do haseł używanych przez użytkownika przy logowaniu. Hasło powinno składać się z co najmniej 8 znaków i zawierać małe i wielkie litery oraz cyfry lub znaki specjalne oraz być zmieniane nie rzadziej niż co 30 dni.
8. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. uczniom, innym pracownikom) wgląd do danych wyświetlanych na monitorach komputerowych - tzw. „Polityka czystego ekranu."
9. Po zakończeniu pracy, użytkownik zobowiązany jest:
    - wylogować się z systemu informatycznego
    - zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.

III. Tworzenie kopii zapasowych.

1. Dla zabezpieczenia integralności danych dokonuje się archiwizacji danych w systemach Szkoły Podstawowej w Mrokowie.
2. Do archiwizacji służą płyty DVD z zapisem danych z systemu.
3. Wszystkie dane archiwizowane winny być identyfikowane, tj. zawierać takie informacje jak datę dokonania zapisu oraz identyfikator zapisanych w kopii danych.

IV. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających Dane osobowe oraz kopii zapasowych.

1. Kopie sporządzane są na dyskach wymiennych typu pendrive lub na innych nośnikach adekwatnych do oprogramowania.
2. Kopie zapasowe przechowywane są w zamkniętych szafach, do których dostęp jest kontrolowany.
3. Dostęp do kopii mają jedynie użytkownicy upoważnieni do ich wykonywania.
4. ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.
5. 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 na nich danych.
6. Tworzenie kopii bezpieczeństwa dokumentacji serwera:
    - Kopie bezpieczeństwa sporządzane są także dla dokumentacji gromadzonej na dyskach stacji roboczych użytkowników w wybranym katalogu.
    - Kopie całościowe przechowywane są przez okres 5 lat, a kopie przyrostowe przez 1 miesiąc.
    - Kopie przechowywane są w szafie pancernej.
    - ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.
1. Procedury tworzenia kopii zapasowych do programu Vulcan Optivum opisuje *Załącznik nr 3.*

V. Przechowywanie nośników informacji zawierających Dane osobowe.

1. Nośniki danych są przechowywane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych).
2. Zabrania się wynoszenia poza obszar organizacji wymiennych nośników informacji a w szczególności twardych dysków z zapisanymi danymi osobowymi bez zgody kierownika działu lub ADO.
3. W sytuacji przekazywania nośników z danymi osobowymi poza obszar organizacji należy stosować następujące zasady bezpieczeństwa:
   - adresat powinien zostać powiadomiony o przesyłce,
   - nadawca powinien sporządzić kopię przesyłanych danych,
   - dane przed wysłaniem powinny zostać zaszyfrowane, a hasło podane adresatowi inną drogą,
   - nośniki pamięci np. typu pendrive, płyty CD wynoszone poza obszar organizacji powinny być szyfrowane,
   - stosować bezpieczne koperty depozytowe,
   - adresat powinien powiadomić nadawcę o otrzymaniu przesyłki.
4. Użytkownicy są zobowiązani do niezwłocznego i trwałego usuwania/kasowania danych osobowych z nośników informacji po ustaniu powodu ich przechowywania (chyba, że z powodu odrębnych przepisów należy je zachować na dłużej).
5. Podlegające likwidacji uszkodzone lub przestarzałe nośniki, a w szczególności twarde dyski z danymi osobowymi są komisyjnie niszczone w sposób fizyczny. Wzór protokołu zniszczenia zawiera *Załącznik nr 4.*
6. Nośniki informacji zamontowane w sprzęcie IT, a w szczególności twarde dyski z danymi osobowymi powinny być wymontowane lub wyczyszczone specjalistycznym oprogramowaniem, zanim zostaną przekazane poza obszar organizacji (np. sprzedaż lub darowizna komputerów stacjonarnych / laptopów)

VI. Sposób zabezpieczenia Systemu informatycznego przed działalnością szkodliwego oprogramowania.

Celem procedury jest zabezpieczenie systemów informatycznych przed szkodliwym oprogramowaniem (np. typu robaki, wirusy, konie trojańskie, rootkity) oraz nieautoryzowanym dostępem do systemów przetwarzających dane osobowe.

1. Ochrona antywirusowa.

1. Osobą upoważnioną do instalowania oprogramowania i aplikacji na jednostkach komputerowych należących do Szkoły Podstawowej w Mrokowie jest wyłącznie ASI. Zobowiązany jest on do takiej konfiguracji systemu aby uniemożliwić instalowanie oprogramowania samodzielnie przez użytkowników.
2. Ochronę przed szkodliwym oprogramowaniem w Szkole Podstawowej w Mrokowie zapewnia program antywirusowy NOD.
3. Za zaplanowanie i zapewnienie ochrony antywirusowej odpowiada ASI, w tym za zapewnienie odpowiedniej ilości licencji dla użytkowników.
4. System antywirusowy ASI instaluje na wszystkich stacjach roboczych i laptopach używanych przez pracowników Szkoły Podstawowej w Mrokowie.
5. Użytkownicy zobowiązani są do skanowania plików przychodzących programem antywirusowym, chyba że program antywirusowy robi to automatycznie.
6. ASI zapewnia stałą aktywność programu antywirusowego tzn. program antywirusowy musi być aktywny podczas pracy systemu informatycznego przetwarzającego dane osobowe.

7. Aktualizacja definicji wirusów odbywa się automatycznie przez system.
8. W przypadku stwierdzenia pojawienia się wirusa, każdy użytkownik winien powiadomić ASI.

2. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej.

1. Za zaplanowanie, konfigurowanie, aktywowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku sieci lokalnej i sieci rozległej odpowiada ASI.
2. Z uwagi na udostępnianie sieci WiFi dla uczniów, ASI konfiguruje i zabezpiecza sieć w ten sposób aby uniemożliwić dostęp do danych przetwarzanych w Szkole Podstawowej w Mrokowie na komputerach używanych przez uczniów.
3. Zastosowano mechanizmy monitorujące przeglądanie Internetu przez użytkowników. Uwzględniają one:
   - blokowanie stron internetowych określonego typu,
   - blokowanie określonych stron internetowych,
   - analizę przesyłanych informacji pod kątem niebezpiecznego oprogramowania.

3. Sposób zabezpieczenia systemu informacji publicznej przed działaniem szkodliwego oprogramowania.

Do zabezpieczenia poufności przekazania danych do bazy danych SIO i pozyskiwania danych z bazy SIO wykorzystuje się mechanizmy szyfrowania danych, zgodnie z Rozporządzeniem MEN z dnia 8 marca 2012 r. w sprawie minimalnych wymagań technicznych dla sprzętu przeznaczonego do obsługi oprogramowania służącego prowadzeniu lokalnych baz danych SIO, udostępnionego przez ministra właściwego do spraw oświaty i wychowania, warunków technicznych, jakie powinno spełniać inne niż udostępnione przez ministra właściwego do spraw oświaty i wychowania oprogramowanie służące prowadzeniu lokalnych baz danych SIO, wydawaniu certyfikaty zgodności z SIO, a także warunków technicznych przekazywanych i pozyskiwania danych z bazy danych SIO.

4. Sposób zabezpieczenia danych w Systemie Vulcan Optivum.

Informację o zabezpieczeniach danych w systemie Vulcan Optivum, obejmującą zabezpieczenia fizyczne, zabezpieczenia integralności danych oraz dostępu do nich i ciągłości działania zawiera *Załącznik nr 5*.

VII. Procedury wykonywania przeglądów i konserwacji systemu oraz nośników informacji służących do Przetwarzania danych

1. ASI odpowiada za bezawaryjną pracę systemu IT, w szczególności: stacji roboczych, oprogramowania, baz danych, poczty email.
2. Przegląd i konserwacja systemu informatycznego powinny być wykonywane w terminach określonych przez producentów systemu lub zgodnie z harmonogramem ASI, jednak nie rzadziej niż raz w roku.
3. Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ASI.
4. ASI odpowiada za sprawdzanie poprawności działania systemu IT, w szczególności: stacji roboczych, serwerów, dysków, drukarek, baz danych, poczty e-mail.

5. ASI odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia.
6. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego, wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych.
7. Czynności konserwacyjne i naprawcze wykonywane doraźnie przez osoby nie posiadające upoważnień do przetwarzania danych (np. specjalistów z firm zewnętrznych), muszą być wykonywane pod nadzorem osób upoważnionych.
8. Przy dokonywaniu serwisu należy przestrzegać następujących zasad:
    a) czynności serwisowe powinny być wykonywane w obecności osoby upoważnionej do Przetwarzania danych, Instrukcja zarządzania systemem informatycznym
    b) przed rozpoczęciem tych czynności dane i programy znajdujące się w systemie powinny zostać zabezpieczone przed ich zniszczeniem, skopiowaniem lub niewłaściwą zmianą,
    c) prace serwisowe należy ewidencjonować w książce zawierającej rodzaj wykonywanych czynności serwisowych, daty rozpoczęcia i zakończenia usługi, odnotowanie osób dokonujących czynności serwisowych, tj. imienia i nazwiska, a także osób uczestniczących w pracach serwisowych,
    d) w przypadku prac serwisowych dokonywanych przez podmiot zewnętrzny, wymagających dostępu do Danych osobowych, z podmiotem takim powinny zostać zawarte stosowne umowy powierzenia danych osobowych lub podpisane upoważnienie do przetwarzania danych osobowych.