Załącznik nr 1 do zarządzenia nr 5a/2018

POLITYKA BEZPIECZEŃSTWA
W ZESPOLE OŚWIATY I WYCHOWANIA W MIEDŹNEJ Z S. W WOLI

§ 1
Podstawowe pojęcia

1. Polityka Ochrony Danych Osobowych służy ustaleniu wymogów, zasad i regulacji dotyczących ochrony danych osobowych w Zespole Oświaty i Wychowania w Miedźnej z s. w Woli.
2. Terminologia:
   1) Polityka – oznacza niniejszą Politykę Bezpieczeństwa;
   2) RODO lub Rozporządzenie – oznacza Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
   1) ZOiW – oznacza Zespoł Oświaty i Wychowania w Miedźnej z s. w Woli;
   2) Administrator Danych – oznacza Zespół Oświaty i Wychowania w Miedźnej z s. w Woli reprezentowaną przez Dyrektora;
   3) Pracownik – oznacza pracownika Zespole Oświaty i Wychowania w Miedźnej z s. w Woli;
   4) Podmiot przetwarzający – oznacza osobę lub podmiot, któremu Zespół Oświaty i Wychowania w Miedźnej z s. w Woli powierzyło przetwarzanie danych osobowych;
   5) Osoba – oznacza osobę, której dane dotyczą, chyba że co innego wynika wyraźnie z kontekstu;
   6) IOD lub Inspektor – oznacza Inspektora Ochrony Danych;
   7) RCPD lub Rejestr – oznacza Rejestr Czynności Przetwarzania Danych Osobowych, o którym mowa w art. 30 ust. 1 RODO;
   8) RKCP – oznacza Rejestr Kategorii Czynności Przetwarzania dokonywanych przez Zespół Oświaty i Wychowania w Miedźnej z s. w Woli w imieniu administratora, o którym mowa w art. 30 ust. 2 RODO;
   9) System informatyczny – oznacza zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
   10) Użytkownik systemu – osoba zatrudniona czasowo (w tym stażyści i praktykanci) lub na czas nieokreślony, której przydzielono osobiste konto, hasło i uprawnienia do dostępu do systemu informatycznego;
   11) administrator systemu informatycznego – pracownik odpowiedzialny za poprawne działanie systemu informatycznego;
   12) autoryzowane oprogramowanie – oprogramowanie dopuszczone do eksploatacji w Zespole Oświaty i Wychowania w Miedźnej z s. w Woli przyjmuje się, że każda aplikacja zainstalowana przez administratora systemu informatycznego jest autoryzowana;
   13) nieautoryzowane oprogramowanie – oprogramowanie, które nie zostało zatwierdzone do eksploatacji przez administratora systemu informatycznego.
3. Administrator we współpracy z IOD dokonuje przeglądu oraz w razie potrzeby aktualizacji Polityki nie rzadziej niż raz w roku.

§ 2
Podstawowe zasady

1. Bezpieczeństwo przetwarzania danych osobowych oraz bezpieczeństwo informacji oznacza, że dane w Zespole Oświaty i Wychowania w Miedźnej z s. w Woli są przetwarzane z zachowaniem poniższych zasad:
   1) legalność – ZOiW dba o ochronę prywatności i przetwarza dane osobowe zgodnie z prawem;
   2) bezpieczeństwo – ZOiW zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stale działania w tym zakresie;

3) prawa jednostki – ZOiW umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje;
4) rozliczalność – ZOiW dokumentuje to, w jaki sposób spełnia obowiązki z zakresie ochrony danych, aby w każdej chwili móc wykazać zgodność z obowiązującymi przepisami.

2. ZOiW przetwarza dane osobowe z poszanowaniem następujących zasad:
   1) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
   2) rzetelnie (rzetelność);
   3) w sposób przejrzysty dla osoby, której danej dotyczą (transparentność);
   4) w konkretnych i wyraźnych celach (ograniczenie celu);
   5) w zakresie nie większym niż niezbędny (minimalizacja);
   6) z dbałością o prawidłowość danych (prawidłowość);
   7) nie dłużej, niż jest to niezbędne (ograniczenie przechowywania);
   8) zapewniając odpowiednie bezpieczeństwo danych (integralność i poufność).

§ 3
Elementy systemu bezpieczeństwa informacji

1. System ochrony danych osobowych w ZOiW składa się z następujących elementów:
   1) Inwentaryzacja danych – ZOiW dokonuje identyfikacji zasobów danych osobowych i sposobów ich wykorzystania;
   2) Rejestr – ZOiW opracowuje, prowadzi i utrzymuje Rejestr Czynności Przetwarzania Danych Osobowych oraz jeśli przetwarza dane osobowe w imieniu innego podmiotu – Rejestr Kategorii Czynności Przetwarzania Danych;
   3) Podstawy prawne – ZOiW zapewnia, identyfikuje i weryfikuje podstawy prawne przetwarzania danych osobowych i rejestruje je w Rejestrze;
   4) Obsługa praw jednostki – ZOiW spełnia obowiązki informacyjne wobec osób, których dane przetwarza oraz zapewnia obsługę ich praw;
   5) Bezpieczeństwo – ZOiW zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:
      a) przeprowadza analizy ryzyka dla czynności przetwarzania lub ich kategorii;
      b) przeprowadza oceny skutków dla ochrony danych;
      c) dostosowuje środki ochrony do ustalonego ryzyka;
      d) posiada system zarządzania bezpieczeństwem informacji;
      e) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych Osobowych;
   6) Przetwarzający – ZOiW posiada zasady doboru podmiotów przetwarzających dane osobowe na rzecz ZOiW, wymogi co do warunków przetwarzania (umowa powierzenia), zasady weryfikacji wykonywania umów powierzenia;
   7) Eksport danych – ZOiW posiada zasady weryfikacji, czy ZOiW nie przekazuje danych do państw trzecich (czyli poza Unię Europejską, Norwegię, Lichtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków takiego przekazywania.

§ 4
Inwentaryzacja danych i Rejestry

1. ZOiW prowadzi Rejestr Czynności Przetwarzania Danych Osobowych, których jest administratorem, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe. Wzór Rejestru, stanowi załącznik nr 1 do Polityki.
2. Administrator oraz wyznaczeni przez niego Pracownicy zobowiązani są do identyfikacji przetwarzanych danych osobowych oraz stałej aktualizacji Rejestru i zapewnienia jego zgodności ze stanem faktycznym oraz stanem prawnym.
3. Jeżeli ZOiW przetwarza dane osobowe w imieniu innego podmiotu, który jest administratorem tych danych, ZOiW zobowiązana jest do prowadzenia Rejestru Kategorii Czynności Przetwarzania dokonywanych w imieniu administratora. Wzór Rejestru, stanowi załącznik nr 2 do Polityki.

4. ZOiW udostępnia RCPD oraz RKCP na żądanie organu nadzorczego.

§ 5
Obsługa praw jednostki

1. ZOiW spełnia obowiązki informacyjne wobec osób, których dane osobowe są przetwarzane, o których mowa w art. 13, art. 14 oraz art. 21 ust. 4 RODO, poprzez zamieszczenie odpowiednich informacji na stronie internetowej oraz poprzez bezpośrednie przekazywanie osobom odpowiednich informacji dotyczących przetwarzania danych.
2. Administrator zamieszcza na stronie internetowej ZOiW ogólną informację o przetwarzaniu danych osobowych oraz Politykę Bezpieczeństwa. Za spełnienie obowiązków informacyjnych wobec osób odpowiedzialni są Pracownicy, którzy pozyskują dane osobowe.
3. ZOiW realizuje prawa osób, których dane są przetwarzane, w szczególności w zakresie:
   1) Dostępu do danych – na żądanie osoby dotyczące dostępu do jej danych, ZOiW informuje tę osobę, czy przetwarza jej dane oraz informuje ją o szczegółach przetwarzania;
   2) Uzyskiwania kopii danych – na żądanie, ZOiW wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych; za wydanie kolejnych kopii danych ZOiW może pobrać opłatę odpowiadającą kosztom obsługi żądania wydania kopii danych; wysokość opłaty ustala Administrator oraz w razie potrzeby opracowuje w tym zakresie cenniki usług;
   3) Sprostowania danych – ZOiW dokonuje sprostowania nieprawidłowych danych na żądanie osoby, której dane dotyczą oraz na jej żądanie informuje ją o odbiorcach, którym ujawniono jej dane osobowe;
   4) Uzupełnienia danych – ZOiW na żądanie osoby, której dane dotyczą, uzupełnia jej dane osobowe; ZOiW ma prawo odmówić uzupełnienia danych, jeżeli byłoby ono niezgodne z celami przetwarzania, w szczególności gdy przetwarzanie tych danych nie jest niezbędne;
   5) Usunięcia danych – osoba, które dane dotyczą ma prawo żądania usunięcia jej danych, a ZOiW, o ile nie zachodzi wyjątek, o którym mowa w art. 17 ust. 3 RODO, jest zobowiązane do ich usunięcia, gdy:
      a) dane nie są niezbędne do celów, do których zostały zebrane ani przetwarzane w innych zgodnych z prawem celach;
      b) zgoda na przetwarzanie danych została cofnięta, a nie ma innej podstawy przetwarzania danych;
      c) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych;
      d) dane były przetwarzane niezgodnie z prawem;
      e) konieczność usunięcia danych wynika z obowiązku prawnego;
      f) ZOiW na żądanie osoby informuje ją o odbiorcach, którym ujawniono jej dane osobowe.
   6) Ograniczenia przetwarzania danych – osoba ma prawo żądania od ZOiW ograniczenia przetwarzania danych, gdy:
      a) kwestionuje prawidłowość danych osobowych – na okres pozwalający sprawdzić ich prawidłowość;
      b) przetwarzanie danych jest niezgodne z prawem, a osoba, której dane dotyczą sprzeciwia się usunięciu tych danych, żądając w zamian ograniczenia ich wykorzystywania;
      c) ZOiW nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
      d) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia czy po stronie ZOiW zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

   W trakcie ograniczenia przetwarzania danych ZOiW przechowuje dane, natomiast nie przetwarza ich w inny sposób (nie przekazuje, nie wykorzystuje) bez zgody osoby, której dane dotyczą, chyba że działa w celu ustalenia, dochodzenia lub obrony roszczeń lub

w celu ochrony praw innej osoby fizycznej lub prawnej, z uwagi na ważne względy interesu publicznego. Przed uchyleniem ograniczenia przetwarzania ZOiW informuje o tym osobę, której dane dotyczą. ZOiW na żądanie osoby informuje ją o odbiorcach, którym ujawniono jej dane osobowe.

7) Przenoszenia danych – jeżeli przetwarzanie danych odbywa się na podstawie zgody osoby lub na podstawie umowy w systemach informatycznych ZOiW, na żądanie tej osoby, wydaje jej w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, a jeżeli jest to techniczne możliwe, przesyła je na żądanie osoby bezpośrednio innemu podmiotowi.
8) Sprzeciwu – osoba może zgłosić umotywowany jej szczególną sytuacją sprzeciw wobec przetwarzania jej danych, jeżeli dane przetwarzane są w oparciu o powierzone SP Frydek zadanie realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej (art. 6 ust. 1 lit. e) RODO). ZOiW uwzględni sprzeciw, o ile nie zachodzą po stronie ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby, zgłaszającej sprzeciw lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

4. Za realizację roszczeń, o których mowa w ust. 3 odpowiedzialny jest Administrator oraz wyznaczeni przez Administratora pracownicy, którzy w tym zakresie współpracują z IOD. W razie zgłoszenia przez osobę roszczeń, o których mowa w ust. 3 bezpośrednio Pracownikowi, jest on zobowiązany niezwłocznie zawiadomić o powyższym Administratora.
5. Administrator bez zbędnej zwłoki, a w każdym razie w terminie miesiąca od otrzymania żądania udziela osobie, której dane dotyczą informacji o działaniach podjętych w związku ze zgłoszonym przez nią żądaniem. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania Administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia.
6. Schemat obsługi żądań powinien wyglądać następująco:
   1) potwierdzenie tożsamości wnioskodawcy,
   2) ustalenie opłaty/decyzja co do odmowy – weryfikacja czy wniosek jest nadmierny lub ewidentnie nieuzasadniony,
   3) ustalenie czy przetwarzamy dane wnioskodawcy – w razie braku danych wnioskodawcy informujemy, że nie przetwarzamy jego danych,
   4) merytoryczna analiza żądania – pod kątem jego zasadności i precyzji żądań;
   5) prośba o uściślenie wniosku – jeśli jest taka potrzeba;
   6) rozpoznanie żądania wnioskodawcy – ewentualnie zawiadomienie go o przedłużeniu terminu,
   7) udzielenie merytorycznej odpowiedzi.
7. Administrator zobowiązany jest poinformować o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał zgodnie z art. 16, art. 17 ust. 1 lub art. 18 RODO każdego obiorcę, któremu ujawniono dane osobowe, chyba, że okaże się to niemożliwe lub wymagać będzie niewspółmiernie dużego wysiłku. Administrator zobowiązany jest udokumentować fakt poinformowania odbiorców lub fakt ustalenia braku możliwości lub niewspółmiernie dużego wysiłku w poinformowaniu odbiorców danych.

§ 6
Bezpieczeństwo informacji

1. W ZOiW stosuje się system identyfikacji zagrożeń - system zabezpieczenia danych nastawiony na likwidację lub ograniczenie zagrożeń, które mogą nastąpić z powodu nieprawidłowości ze strony:
   1) użytkowników systemów:
      a) utrata danych spowodowana brakiem umiejętności obsługi oprogramowania,
      b) nienależyte zabezpieczenie wydruków, raportów i innych dokumentów,
      c) nienależyte zabezpieczenie komputerów przenośnych,

d) wypływ informacji spowodowany nieświadomością użytkowników,
e) wypływ informacji świadomie spowodowany przez użytkowników,
f) nienależyte zabezpieczenie miejsca pracy poprzez:
– niestosowanie wygaszaczy ekranów zabezpieczonych hasłem,
– nienależyte zabezpieczenie pomieszczenia na czas chwilowej nieobecności,
– nienależytą ochronę hasła dostępu do systemu operacyjnego,
– nienależytą ochronę hasła dostępu do aplikacji;

2) oprogramowania pochodzącego z zewnątrz:
a) działanie szkodliwego oprogramowania,
b) nieautoryzowane oprogramowanie instalowane samodzielnie przez użytkowników systemu;

3) wadliwego działania sprzętu lub oprogramowania:
a) używanie nieautoryzowanego sprzętu pracującego w systemie informatycznym,
b) brak poprawnie działających procedur wykonywania i składowania kopii bezpieczeństwa danych,
c) brak zabezpieczenia dostawy energii elektrycznej do serwerów,
d) brak zabezpieczenia przeciwpożarowego.

2. W ZOiW stosuje się proces ciągłego szacowania ryzyka, obejmujący w szczególności:
1) ustalenie danych, jakie są przetwarzane i stosowanych wobec nich zabezpieczeń;
2) ustalenie wymagań odnośnie przetwarzanych danych – celu i podstawy prawnej przetwarzania;
3) zidentyfikowanie zagrożeń dla bezpieczeństwa przetwarzania danych oraz identyfikację podatności na urzeczywistnienie określonych zagrożeń;
4) ocenę potencjalnych skutków urzeczywistnienia się zagrożenia;
5) ustalenie prawdopodobieństwa wystąpienia ryzyka.

3. ZOiW wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający oszacowanemu ryzyku, w tym między innymi w stosownym przypadku:
1) pseudonimizację i szyfrowanie danych osobowych;
2) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
3) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
4) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

§ 7
Środki techniczne i organizacyjne

1. ZOiW stosuje w szczególności następujące środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych:
1) zapewnienie wsparcia kierownictwa dla zabezpieczenia informacji przetwarzanych w ZOiW wyraża się poprzez zapewnienie środków technicznych oraz lokalowych pozwalających na bezpieczne przetwarzanie danych, a także poprzez zapewnienie odpowiedniego przeszkolenia pracowników;
2) zapewnienie znajomości zasad przetwarzania danych wśród pracowników – każda osoba zatrudniona w ZOiW przed rozpoczęciem pracy zobowiązana jest do zapoznania się z przepisami dotyczącymi ochrony danych osobowych, co poświadcza własnoręcznym podpisem. W upoważnieniu powinien zostać określony zakres informacji, do przetwarzania, których została upoważniona oraz data nadania upoważnienia lub okres obowiązywania upoważnienia;
3) zapewnienie znajomości zasad korzystania z systemów informatycznych oraz zabezpieczenia danych w tych systemach - osoba dopuszczająca do pracy w systemie informatycznym nowego pracownika, zobowiązana jest do przeszkolenia go w zakresie korzystania z systemu informatycznego, a także do wystąpienia do administratora

o nadanie nazwy użytkownika (login) oraz odpowiednich uprawnień do systemu informatycznego;

4) zabezpieczenie poufności danych podczas wykonywania prac konserwacyjnych sprzętu, oprogramowania oraz remontów budynków, przez osoby trzecie:
   a) prace konserwacyjne oraz remontowe prowadzone w ZOiW wykonywane przez osoby trzecie, muszą być nadzorowane. W remontowanych pomieszczeniach, w których możliwy jest dostęp do sieci informatycznej należy ją zabezpieczyć tak, aby wyeliminować możliwość nieautoryzowanego skorzystania z sieci, a także w taki sposób, aby jakiekolwiek uszkodzenie sieci nie spowodowało uszkodzenia urządzeń pracujących w sieci,
   b) za zabezpieczenie sieci informatycznej w remontowanych pomieszczeniach odpowiada osoba odpowiedzialna za to pomieszczenie. Prace konserwacyjne oraz remontowe prowadzone w ZOiW, które mogą ingerować w sieć teleinformatyczną, muszą być każdorazowo zgłaszane do dyrektora,
   c) za nadzór nad pracownikami wykonującymi usługi, prace budowlane lub dostawy na terenie ZOiW odpowiada dyrektor. Jeżeli realizacja prac przez firmę zewnętrzną odbywa się poza godzinami urzędowania, firma przekazuje administratorowi danych informację pisemną zawierającą co najmniej: nazwę firmy, nazwę zadania i miejsce jego realizacji, nazwiska pracowników firmy, którzy będą realizować zadania na terenie ZOiW, a jeżeli realizacja zadań wymaga dostępu do pomieszczeń – numery pomieszczeń; informacja musi zawierać również wskazanie pracownika odpowiedzialnego za nadzór nad pracami wraz z kontaktowym numerem telefonu, pod którym pracownik będzie dostępny w godzinach pracy firmy na terenie;
   d) konserwacja oprogramowania może mieć miejsce tylko w obecności pracownika odpowiedzialnego za system operacyjny, na którym przedmiotowe oprogramowanie pracuje;
   e) Nadzór nad zapisami z wykonanych prac konserwacyjnych prowadzi administrator właściwego systemu. O wszelkich pracach, w wyniku których nastąpiła zmiana struktury bazy danych administrator właściwego systemu informatycznego informuje pisemnie Administratora lub wyznaczonego przez niego pracownika, który wprowadza ewentualne zmiany w dokumentacji baz danych;
5) zabezpieczenia danych informatycznych przed ich utratą w przypadku awarii sprzętu lub innych wypadków:
   a) zabezpieczenie ciągłości zasilania systemów informatycznych poprzez zastosowanie niezależnych źródeł zasilania (UPS). Niezależne źródło zasilania zapewnia działanie serwerów systemów informatycznych, przez co najmniej 5 minut oraz odpowiedzialne jest za bezpieczne zakończenie sesji i wyłączenie sprzętu komputerowego. Realizacja tego zadania przebiega w sposób automatyczny przez zastosowanie odpowiedniego oprogramowania oraz sprzętu i odpowiednią konfigurację sprzętowo-programową, za wyjątkiem przypadków, w których UPS nie został wyposażony w odpowiednie oprogramowanie – realizacja tego zadania polega na odpowiedniej organizacji pracy i przeszkolenia pracowników. Działanie tego zabezpieczenia odbywa się bez udziału administratorów,
   b) za wykonanie kopii bezpieczeństwa danych przetwarzanych na serwerach odpowiedzialny jest wyznaczony pracownik. Szczegółową odpowiedzialność za poszczególne systemy informatyczne określa administrator danych poprzez odpowiednie postanowienia w zakresach obowiązków podległych pracowników;
   c) wprowadza się bezwzględny zakaz samodzielnej instalacji nieautoryzowanego oprogramowania,
   d) administratorzy systemów informatycznych zobowiązani są do przygotowania takiej konfiguracji sprzętowo–programowej, która uniemożliwia użytkownikom systemu informatycznego instalowanie nieautoryzowanego oprogramowania,
   e) kontrole przeprowadzane okresowo przez IOD na stanowiskach pracy.

6) bezpieczeństwo obszaru przetwarzania danych osobowych:
   a) obszar przetwarzania danych, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych;
   b) przebywanie osób nieuprawnionych w obszarze przetwarzania danych, jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych;
   c) pracownicy są zobowiązani do natychmiastowego zgłaszania przełożonemu faktu nieautoryzowanego dostępu do pomieszczenia, biurka lub szafy;
   d) do otwierania i zamykania drzwi zewnętrznych uprawnieni są dyrektor oraz upoważnione przez niego osoby. Zasady określone zostały w polityce kluczy będącej załącznikiem nr 10 do Polityki.

2. ZOiW stosuje w szczególności następujące środki techniczne i organizacyjne służące zabezpieczeniu danych przetwarzanych w systemie informatycznym:
   1) w systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby wówczas zapewnia się, aby:
      a) w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator,
      b) dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia,
      c) identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie był przydzielany innej osobie;
   2) system informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:
      a) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,
      b) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej;
   5) do uwierzytelniania użytkowników komputerów używa się haseł. Zasady ich stosowania określa polityka haseł, stanowiąca załącznik nr 8 do niniejszej Polityki.
   6) urządzenia i nośniki zawierające dane osobowe, zabezpiecza się w sposób zapewniający poufność i integralność danych;
   7) system informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem;
   8) zastosowanie logicznych zabezpieczeń, o których mowa w powyższym punkcie obejmuje:
      a) kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną,
      b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych;
   9) administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej;
   10) dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych;
   11) kopie zapasowe:
      a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem,
      b) usuwa się niezwłocznie po ustaniu ich użyteczności;
   12) urządzenia, dyski lub inne nośniki informacji, zawierające dane osobowe, przeznaczone do:
      a) likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,

b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,
c) naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

§ 8
Osoby biorące udział w procesie ochrony danych osobowych

1. W ZOiW powołuje się Inspektora Ochrony Danych Osobowych (IOD).
2. Odpowiedzialność osób biorących udział w procesie ochrony danych osobowych:
   1) za opracowanie, wdrożenie i realizację Polityki Bezpieczeństwa w ZOiW odpowiada administrator danych;
   2) za bezpieczeństwo danych i rejestrów publicznych przetwarzanych w ZOiW odpowiada administrator aanych, w szczególności w zakresie:
      a) upoważniania podległych pracowników do przetwarzania danych osobowych. Upoważnienie takie musi posiadać formę pisemną i może stanowić być zawarte w zakresie czynności pracownika lub w odrębnym dokumencie,
      b) nadzoru nad przydzielaniem uprawnień do baz danych oraz innych zasobów informatycznych,
      c) prowadzenia ewidencji użytkowników upoważnionych do przetwarzania danych w podległych bazach danych,
      d) nadzoru nad wykorzystaniem sprzętu informatycznego przez podległych pracowników;
   3) IOD odpowiada za:
      a) informowanie Administratora oraz Pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii lub prawa krajowego dotyczących ochrony danych i doradzanie im w tej sprawie;
      b) monitorowanie przestrzegania RODO, innych przepisów Unii lub przepisów krajowych o ochronie danych oraz polityk Administratora w dziedzinie ochrony danych osobowych;
      c) działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
      d) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
      e) współpracę z organem nadzorczym;
      f) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.
   4) Pracownicy:
      1. mają dostęp do danych osobowych w zakresie wynikającym z zadań przypisanych im w zakresach czynności,
      2. są zobowiązani do znajomości i przestrzegania zasad polityki bezpieczeństwa przetwarzania danych osobowych,
      3. pracownicy zobowiązani są do zgłaszania wszelkich zmian w strukturze baz danych zawierających dane osobowe oraz celu i trybu ich wykorzystywania.
3. Wzór upoważnienia do przetwarzania danych osobowych oraz oświadczenia o przyjęciu do wiadomości i stosowaniu zasad przetwarzania danych osobowych stanowi załącznik nr 3 do Polityki.
4. Administrator prowadzi rejestr osób upoważnionych do przetwarzania danych osobowych, który stanowi załącznik nr 4 do Polityki.

§ 9
Podmioty przetwarzające

1. ZOiW korzysta z usług wyłącznie takich podmiotów przetwarzających, które zapewniają gwarancje wdrożenia takich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi określone w RODO oraz w przepisach krajowych i chroniło prawa osób, których dane dotyczą.
2. Podmiot przetwarzający może korzystać z usług innego podmiotu przetwarzającego wyłącznie za uprzednią szczegółową pisemną zgodą Administratora, określającą podmiot, któremu zostanie powierzone dalsze przetwarzania danych. Udzielenie przez administratora ogólnej zgody dopuszczalne jest w wypadkach uzasadnionych ważnym interesem Podmiotu Przetwarzającego lub administratora.
3. Powierzenie przetwarzania danych osobowych podmiotom zewnętrznym możliwe jest z zachowaniem następujących wymogów:
    1) powierzenie przetwarzania może nastąpić wyłącznie na podstawie pisemnej umowy spełniającej wymogi określone w art. 28 RODO;
    2) wybór podmiotów przetwarzających następuje z zachowaniem procedur wyboru wykonawców obowiązujących w ZOiW;
    3) na etapie wyboru podmiotu przetwarzającego dokonuje się weryfikacji, czy zapewnia on zastosowanie środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi określone w RODO oraz w przepisach krajowych i chroniło prawa osób, których dane dotyczą;
    4) w umowach na podstawie których wykonawcy świadczą na rzecz ZOiW usługi lub inne świadczenia, należy zastrzec sankcje na wypadek nieprzestrzegania przez wykonawcę wymogów przetwarzania danych osobowych, w szczególności w postaci kar umownych, możliwości odstąpienia od umowy lub jej wypowiedzenia.
4. Wzór umowy powierzenia przetwarzania danych stanowi załącznik nr 7 do Polityki.

.

§ 10
Obszar przetwarzania danych osobowych

1. Obszarem przetwarzania danych osobowych jest Zespół Oświaty i Wychowania w Miedźnej z s. w Woli
2. Nośniki informacji zawierające dane osobowe, uszkodzone informatyczne nośniki danych, kopie zapasowe danych przetwarzanych w systemie informatycznym oraz inne niż informatyczne nośniki zawierające dane osobowe przechowywane są w sejfie oraz w zamykanych szafach.

§ 11
Naruszenie ochrony danych osobowych

1. 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 (art. 4 pkt 12 RODO).
2. W przypadku naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je właściwemu organowi nadzorczemu (Prezesowi Urzędu Ochrony Danych Osobowych), chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Wzór zgłoszenia stanowi załącznik nr 5 do Polityki.
3. Jeżeli ZOiW przetwarza dane osobowe w imieniu innego podmiotu, w razie stwierdzenia naruszenia ochrony danych osobowych ZOiW bez zbędnej zwłoki zgłasza je administratorowi tych danych.
4. Zgłoszenie, o którym mowa w ust. 2 musi co najmniej:

a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
b) zawierać imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

5. Jeżeli informacji, o których mowa w ust. 4 nie da się udzielić w tym samych czasie, można jej udzielać organowi nadzorczemu sukcesywnie bez zbędnej zwłoki.
6. Każdy Pracownik zobowiązany jest do niezwłocznego zawiadomienia administratora o stwierdzeniu lub podejrzeniu naruszenia ochrony danych osobowych.
7. Administrator w porozumieniu z IOD dokonuje oceny czy doszło do naruszenia ochrony danych osobowych i czy naruszenie to podlega zgłoszeniu do organu nadzorczego.
8. Wprowadza się następujące zasady postępowania:
   1) w przypadku stwierdzenia naruszenia ochrony danych pracownik zobowiązany jest do zabezpieczenia miejsca, w którym doszło do naruszenia danych oraz poinformowania przełożonego lub bezpośrednio Administratora. Pracownik lub jego przełożony przygotowuje notatkę służbową i przekazuje ją administratorowi danych, wraz z propozycją rozwiązania problemu. Administrator danych podejmuje decyzję o dalszym przebiegu postępowania;
   2) użytkownik systemu informatycznego jest zobowiązany do poinformowania administratora systemu informatycznego o każdym przypadku niewłaściwego funkcjonowania systemu informatycznego. W przypadku wadliwego działania systemu informatycznego użytkowników obowiązuje całkowity zakaz wykonywania jakichkolwiek napraw. Do diagnozowania usterki lub wadliwego działania systemu informatycznego upoważnieni są tylko administratorzy systemu informatycznego lub inni wyznaczeni pracownicy;
   3) użytkownik systemu informatycznego jest zobowiązany do natychmiastowego zgłaszania swoim przełożonym lub bezpośrednio do administratorowi wszelkich zauważonych elementów systemu zabezpieczeń podatnych na zagrożenia;
   4) administrator systemu informatycznego może na polecenie administratora danych zabezpieczyć komputer pracownika w celu dokonania szczegółowego badania;
   5) wobec pracownika naruszającego postanowienia Polityki Bezpieczeństwa administrator danych wyciąga konsekwencje służbowe;
   6) każde stanowisko pracy jest monitorowane na zasadach określonych w Regulaminie Pracy.
9. Jeżeli naruszenie ochrony danych może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą o takim naruszeniu. Zawiadomienie powinno jasnym i prostym językiem opisywać charakter naruszenia ochrony danych osobowych oraz zawierać przynajmniej informacje i środki, wskazane w zawiadomieniu do organu nadzorczego, o którym mowa w ust. 2 i 4.
10. Zawiadomienie, o którym mowa w ust. 9 nie jest wymagane w przypadkach określonych w art. 34 ust. 3 RODO.
11. Administrator dokumentuje wszystkie przypadki naruszenia ochrony danych osobowych prowadząc rejestr naruszeń ochrony danych osobowych. W rejestrze naruszeń ochrony danych osobowych dokumentuje się w szczególności okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.
12. Wzór rejestru naruszeń ochrony danych osobowych stanowi załącznik nr 6 do Polityki.

§ 12

1. Załączniki do Polityki Bezpieczeństwa podlegają bieżącemu nadzorowi administratora, który w tym zakresie współpracuje z IOD. Zmiany dokonywane w załącznikach nie wymagają zmiany Polityki Bezpieczeństwa:

2. Załączniki do Polityki stanowią:

1) Załącznik nr 1 – Wzór rejestru czynności przetwarzania danych osobowych;
2) Załącznik nr 2 – Wzór rejestru kategorii czynności przetwarzania danych;
3) Załącznik nr 3 – Wzór upoważnienia do przetwarzania danych osobowych i oświadczenia pracownika o przyjęciu do wiadomości i stosowania zasad przetwarzania danych osobowych;
4) Załącznik nr 4 – Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych;
5) Załącznik nr 5 – Wzór zgłoszenia naruszenia ochrony danych osobowych Prezesowi UODO;
6) Załącznik nr 6 – Wzór rejestru naruszeń przetwarzania danych osobowych;
7) Załącznik nr 7 – Wzór umowy powierzenia przetwarzania danych.
8) Załącznik nr 8 – Polityka haseł
9) Załacznik nr 9 – Polityka czystego biurka
10) Załącznik nr 10 – Polityka kluczy