Załącznik Nr 1 do Zarządzenia nr 021.8.2021
Dyrektora Zespołu Ekonomiczno-Administracyjnego
Szkół Miasta i Gminy Woźniki z dnia 28 października 2021 r.

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W ZESOLE EKONOMICZNO – ADMINISTRACYJNYM SZKÓŁ MIASTA I GMINY WOŹNIKI

Rozdział I. Wprowadzenie

1. Niniejszy dokument stanowi politykę bezpieczeństwa danych osobowych w jednostce, zwany dalej Polityką. Reguluje całościowo dopuszczalny przez prawo sposób zarządzania i ochrony danych osobowych oraz prawa osób, których dane osobowe są przez jednostkę przetwarzane.
2. Celem Polityki jest wskazanie działań, jakie należy podjąć, formy tych działań oraz sposób ich przeprowadzania, aby wykonać ciążące na administratorze danych osobowych obowiązki, o których mowa w art. 24 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz.UE 2016/679). Realizacja postanowień tego dokumentu ma zapewnić ochronę danych osobowych, właściwe udokumentowanie przypadków naruszenia bezpieczeństwa oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych.
3. Postanowienia niniejszej Polityki mają zastosowanie do wszelkich danych osobowych, w rozumieniu art. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781), których administratorem jest **Zespół Ekonomiczno – Administracyjny Szkół Miasta i Gminy Woźniki**, a obowiązek ich przestrzegania spoczywa na każdym, kto przetwarza dane w jednostce.

Rozdział II. Deklaracja Władz

1. Administrator danych osobowych, zwany dalej ADO, świadomy odpowiedzialności za zapewnienie bezpieczeństwa informacji przetwarzanych w jednostce, deklaruje gotowość budowy kompleksowego systemu zarządzania bezpieczeństwem informacji oraz wsparcie wszelkich działań mających na celu ochronę zasobów informacyjnych jednostki.
2. ADO ustanawia politykę bezpieczeństwa informacji i zobowiązuje:
1) osoby zatrudnione w jednostce do podejmowania działań zgodnych z postanowieniami niniejszej Polityki w związku z przetwarzaniem danych osobowych;
2) kierownika jednostki do:
   a) zapewnienia właściwych warunków organizacyjno-technicznych przetwarzania informacji w jednostce,
   b) zapewnienia bieżącego nadzoru nad przestrzeganiem obowiązujących w jednostce zasad bezpieczeństwa przetwarzania informacji.
3. Administrator danych osobowych, świadomy wagi zagrożeń prywatności, w tym zwłaszcza zagrożeń danych osobowych przetwarzanych w związku z udzielaniem świadczeń medycznych, deklaruje podejmowanie wszelkich możliwych działań koniecznych do zapobiegania zagrożeniom, m.in. takim jak:
1) sytuacje losowe lub nieprzewidziane, oddziaływanie czynników zewnętrznych na zasoby systemu, jak np. pożar, zalanie pomieszczeń, katastrofa budowlana, napad, kradzież, włamanie, działania terrorystyczne, niepożądana ingerencja ekipy remontowej;
2) podejmowanie pracy w systemie z przełamaniem lub zaniechaniem stosowania procedur ochrony danych, np. praca osoby, która nie jest upoważniona do przetwarzania danych

osobowych;

3) naruszenia zasad i procedur określonych w dokumentacji z zakresu ochrony danych osobowych przez osoby upoważnione do przetwarzania danych osobowych, związane z nieprzestrzeganiem procedur ochrony danych, w tym zwłaszcza:
   a) niezgodne z procedurami zakończenie pracy lub opuszczenie stanowiska pracy,
   b) naruszenie bezpieczeństwa danych przez nieautoryzowane ich przetwarzanie,
   c) ujawnienie osobom nieupoważnionym procedur ochrony danych stosowanych przez ADO,
   d) ujawnienie osobom nieupoważnionym danych przetwarzanych przez ADO, w tym również nieumyślne ujawnienie danych osobom postronnym, przebywającym bez nadzoru lub w niedostatecznie nadzorowanych pomieszczeniach w siedzibie ADO,
   e) przetwarzanie danych osobowych w celach prywatnych.

Rozdział III. Postanowienia ogólne

A. Słownik pojęć

Użyte w Polityce określenia oznaczają:

1) jednostka - **Zespół Ekonomiczno – Administracyjny Szkół Miasta i Gminy Woźniki,**;
2) administrator danych osobowych (ADO) - **Zespół Ekonomiczno – Administracyjny Szkół Miasta i Gminy Woźniki** decydujący o celach i środkach przetwarzania danych osobowych;
3) analiza ryzyka - proces mający na celu oszacowanie wagi ryzyka rozumianego jako funkcja prawdopodobieństwa wystąpienia skutku i krytyczności jego następstw dla jednostki;
4) autentyczność - właściwość oznaczająca, że zawartość zasobu informatycznego oraz tożsamość osoby mającej dostęp do tego zasobu, jest taka jak deklarowana;
5) baza danych osobowych - zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych w formie papierowej;
6) bezpieczeństwo informacji - stan, w którym informacja jest chroniona przed wieloma różnymi zagrożeniami w taki sposób, aby zapewnić ciągłość prowadzenia działalności, zminimalizować straty i maksymalizować zwrot nakładów na inwestycje. Niezależnie od tego, jaką formę informacja przybiera lub za pomocą jakich środków jest udostępniana lub przechowywana, zawsze powinna być w odpowiedni sposób chroniona, bezpieczeństwo informacji oznacza w szczególności zachowanie: poufności, integralności, dostępności, rozliczalności;
7) dane osobowe (dane) - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
8) dostępność informacji - zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nimi zasobów wtedy, gdy jest to potrzebne;
9) incydent bezpieczeństwa - każde wykryte naruszenie albo wykryta próba naruszenia bezpieczeństwa informacji będące naruszeniem obowiązujących przepisów wewnętrznych lub przepisów prawa, źródłem incydentu bezpieczeństwa może być zarówno przypadkowe, jak i celowe działanie albo jego zaniechanie przez osoby zatrudnione w jednostce;
10) integralność informacji - zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania;
11) ochrona - zespół środków organizacyjno-technicznych i prawnych zapewniających bezpieczeństwo informacji;
12) odbiorcy danych - rozumie się przez to każdego, komu udostępnia się dane osobowe, z

wyłączeniem:
a) osoby, której dane dotyczą,
b) osoby upoważnionej do przetwarzania danych,
c) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;

13) poufność informacji - rozumiana jako zapewnienie, że tylko uprawnieni pracownicy mają dostęp do informacji;
14) przetwarzanie danych - wykonywanie jakichkolwiek operacji na danych osobowych, np. zbieranie, utrwalanie, opracowywanie, udostępnianie, zmienianie, usuwanie i przechowywanie;
15) rozliczalność - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
16) ustawa - ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781);
17) uwierzytelnianie - działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
18) 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.
19) właściwa ochrona - zespół środków organizacyjno-technicznych i prawnych stosowanych w celu zapewnienia bezpieczeństwa informacji;
20) zasada czystego biurka - sposób organizacji na stanowisku pracy, który minimalizuje ryzyko nieuprawnionego wejścia w posiadanie danych osobowych, ważnych informacji lub krytycznych danych;
21) zbiór danych - zestaw danych osobowych posiadający określoną strukturę, prowadzony według określonych kryteriów oraz celów.

B. Podstawy prawne

1. Polityka oraz wynikające z niej dokumenty szczegółowe są wyrazem obowiązujących przepisów prawa, a w szczególności:

1) ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019r. poz. 1781);
2) ustawy z dnia 26 czerwca 1974 r. - Kodeks pracy (tekst jedn.: Dz. U. z 2020 r. poz. 1320, z 2021 r. poz. 1162.);
3) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz.UE 2016/679).

2. Zasady ochrony informacji określa niniejszy dokument wraz z załącznikami.

C. Cel Polityki

1. Celem Polityki jest stworzenie podstaw organizacyjnych dla wdrożenia systemu zarządzania bezpieczeństwem danych osobowych w jednostce oraz określenie podstawowych zasad i wymagań organizacyjno-technicznych oraz prawnych dla zapewnienia właściwej ochrony informacji stanowiących tajemnicę służbową, informacji prawnie chronionych, a w szczególności informacji wytwarzanych, przetwarzanych, przekazywanych i przechowywanych w systemach informatycznych w jednostce. Ponadto Polityka jest zbiorem

spójnych, precyzyjnych reguł i procedur, według których jednostka buduje, zarządza oraz udostępnia zasoby i systemy informacyjne. Określa ona, które zasoby i w jaki sposób mają być chronione.

Zawarte w Polityce regulacje określają kierunki działań oraz wsparcia dla zapewnienia bezpieczeństwa danych osobowych administrowanych przez jednostkę, w szczególności:

1) określają zasady zarządzania, ochrony i dystrybucji danych osobowych;
2) określają standardy zapewniające bezpieczeństwo przetwarzania danych osobowych.

D. Zakres podmiotowy i przedmiotowy Polityki

1. Polityka odnosi się do wszelkich zasobów informacyjnych związanych z realizacją procesów jednostki, infrastruktury technicznej oraz jego pracowników.

2. Niniejsza Polityka dotyczy danych osobowych przetwarzanych w sposób tradycyjny w księgach, wykazach i innych zbiorach ewidencyjnych.

Rozdział IV. Podstawowe zasady przetwarzania danych

A. Zgoda na przetwarzanie danych

1. Przetwarzanie danych osobowych może nastąpić tylko za zgodą osoby, której dane dotyczą. Wyrażenie zgody nie może być domniemane, wymagane jest jej wyraźne udzielenie ustnie lub na piśmie. Zgoda dotyczy wszelkich czynności, które nie są związane z udzielaniem świadczeń leczniczych.

2. Na Administratorze spoczywa obowiązek wykazania zgody osoby, której dane są przetwarzane.

3. Wzór udzielenia zgody na przetwarzanie danych osobowych stanowi **Załącznik nr 1** do niniejszej Polityki.

4. Przetwarzanie danych bez zgody osoby, której dane dotyczą jest bezprawne, chyba że przepis szczególny ustawy stanowi inaczej.

B. Zasada celowości i adekwatności

1. Przetwarzanie danych może nastąpić jedynie dla wyraźnie oznaczonych celów.

2. Celem przetwarzania danych osobowych w jednostce jest w szczególności:

1) prowadzenie, jako jednostka obsługująca, o której mowa w art. 10a pkt 1, art. 10b ust.2 pkt ustawy o samorządzie gminnym (Dz. U z 2021 r. poz. 1372, 1834) wspólnej obsługi na rzecz jednostek obsługiwanych określone w Statucie Zespołu Ekonomiczno – Administracyjnego Szkół Miasta i Gminy Woźniki, będącego załącznikiem do Uchwały Nr 196/XXI/2016 Rady Miejskiej w Woźnikach z dnia 21 listopada 2016 r.
2) przetwarzanie danych osobowych w innych celach, co wymaga odpowiedniej zgody.

3. Przetwarzane dane muszą być adekwatne do celu, w jakim są zbierane, co oznacza, że możliwe jest przetwarzanie tylko takich danych, które są niezbędne dla realizacji określonego celu.

4. Raz w roku należy przeprowadzić przegląd przetwarzanych danych osobowych pod kątem celowości ich dalszego przetwarzania.

5. Dane przetwarzane muszą być merytorycznie poprawne, co oznacza, że dane muszą odzwierciedlać stan faktyczny.

6. Wymagana jest ponowna zgoda na przetwarzanie danych, jeżeli cel przetwarzania uległ zmianie.

7. Przetwarzanie danych dla innych celów niż te, dla których zostały zebrane jest dopuszczalne tylko wtedy, gdy cele te są zgodne.

8. Przetwarzanie danych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą.

D. Obszar przetwarzania danych

1. Przetwarzanie danych dopuszczalne jest wyłącznie na wyznaczonym do tego obszarze.
2. Dane osobowe w jednostce przetwarzane są w budynku Szkoły Podstawowej im. Józefa Lompy w Woźnikach ul. Florianek 18A, 42-289 Woźniki.
3. Wykaz pomieszczeń, w których dopuszczalne jest przetwarzanie danych osobowych, stanowi **załącznik nr 2** do niniejszej Polityki.

E. Upoważnienie do przetwarzania danych

1. Przetwarzać dane osobowe może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych, wydane przez ADO.
2. Do wniosku o wydanie upoważnienia załącza się oświadczenie o zachowaniu poufności przetwarzanych danych.
3. Upoważnioną do przetwarzania danych może być tylko osoba, która uczestniczyła uprzednio w szkoleniu z zakresu ochrony danych osobowych.
4. Osoba posiadająca upoważnienie do przetwarzania danych jest uprawniona do ich przetwarzania w zakresie i czasie wskazanym w upoważnieniu.
5. Dostęp zatrudnionych osób do zasobów informacyjnych ograniczony jest zgodnie z zasadą wiedzy koniecznej.
6. Wniosek o wydanie upoważnienia, o którym mowa w pkt 1 składany jest w formie pisemnej do ADO.
7. Wzór wniosku o wydanie upoważnienia do przetwarzania danych stanowi **załącznik nr 3** do niniejszej Polityki.
8. Wzór upoważnienia do przetwarzania danych stanowi **załącznik nr 4** do niniejszej Polityki.
9. Wzór oświadczenia o zachowaniu poufności przetwarzanych danych stanowi **załącznik nr 5** do niniejszej Polityki.
10. Rejestr osób upoważnionych do przetwarzania danych osobowych stanowi **załącznik nr 6** do niniejszej Polityki.
11. Wykaz zbiorów danych stanowi **załącznik nr 7** do niniejszej Polityki.

Rozdział V. Organizacja przetwarzania danych osobowych

1. Za standard wewnętrzny przyjmuje się poziom ochrony zgodny z kryteriami akceptowalności ryzyka szczątkowego.
2. Każdy pracownik odpowiada za ochronę informacji przetwarzanych zgodnie z indywidualnym zakresem obowiązków, nadanymi uprawnieniami i zakresem odpowiedzialności wynikającym z zajmowanego stanowiska.
3. Obowiązkiem każdego pracownika jest:
1) przestrzeganie przepisów prawa i przepisów wewnętrznych jednostki;
2) dbałość o zachowanie bezpieczeństwa informacji, do których ma dostęp;
3) zgłaszanie do bezpośredniego przełożonego przypadków naruszenia bezpieczeństwa informacji.

A. Administrator danych osobowych (ADO)

1. Administrator danych osobowych realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:
1) wyznacza inspektora ochrony danych oraz określa zakres zadań i czynności;

2) podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji ADO oraz technik zabezpieczenia danych osobowych;
3) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi jej obowiązków;
4) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych.
3. Do podstawowych obowiązków należy:
1) dokonywanie przeglądu dokumentacji bezpieczeństwa, a w szczególności polityk bezpieczeństwa, instrukcji i procedur, nie rzadziej niż 1 raz w roku;
2) dokonywanie bieżącej kontroli nad przestrzeganiem zasad przetwarzania danych. Kontrola polega w szczególności na sprawdzeniu:
a) którzy pracownicy mają dostęp do danych osobowych,
b) czy dane osobowe nie zostały udostępnione nieupoważnionym pracownikom,
c) czy pracownicy i inne osoby mające dostęp do danych osobowych posiadają aktualne upoważnienia do przetwarzania danych osobowych;
3) monitorowanie zagrożeń;
4) dokonywanie przeglądu i monitorowanie naruszeń bezpieczeństwa informacji,
5) nadzór nad przestrzeganiem zasad określonych w Polityce i regulacjach wewnętrznych dotyczących ochrony danych osobowych;
6) zarządzanie dostępem.
4. Każdorazowo należy sporządzić raport w przypadku naruszenia zasad bezpieczeństwa ochrony danych osobowych.

B. Osoba upoważniona do przetwarzania danych osobowych
1. Przed wydaniem upoważnienia do przetwarzania danych konieczny jest udział w szkoleniu z zakresu ochrony danych oraz złożenie oświadczenia o zachowaniu poufności przetwarzanych danych.
2. Do wniosku o upoważnienie do przetwarzania danych załączone zostają odpowiednie dokumenty, o których mowa w ust. 1.
3. Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana przestrzegać następujących zasad:
1) może przetwarzać dane osobowe zgodnie z zakresem opisanym w upoważnieniu i tylko w celu wykonywania nałożonych na nią obowiązków. Ustanie stosunku pracy powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych;
2) musi zachować tajemnicę danych osobowych oraz przestrzegać procedur ich bezpiecznego przetwarzania. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji;
3) zapoznaje się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej Polityki;
4) stosuje określone przez ADO procedury oraz wytyczne mające na celu zgodne z prawem, w tym zwłaszcza adekwatne i celowe, przetwarzanie danych;
5) zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym.

C. Zabezpieczenia we własnym zakresie
1. Niezwykle ważne dla bezpieczeństwa danych jest wyrobienie przez każdą osobę upoważnioną do przetwarzania danych lub użytkownika nawyku:
1) niepozostawiania bez kontroli dokumentów w miejscach publicznych oraz w samochodach;
2) pilnego strzeżenia akt;

3) nieużywania powtórnie dokumentów zadrukowanych jednostronnie;
4) opuszczania stanowiska pracy dopiero po schowaniu dokumentów;
5) udostępniania danych osobowych pocztą elektroniczną tylko w postaci zaszyfrowanej;
6) niszczenia w niszczarce lub chowania do szaf wszelkich dokumentów zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy;
7) niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych;
8) zachowania tajemnicy danych, w tym także wobec najbliższych;
9) chowania do szaf wszelkich akt zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy;
10) zamykania okien w razie opuszczania pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy;
11) zamykania drzwi na klucz po zakończeniu pracy w danym dniu i złożenia klucza w bezpiecznym miejscu. Jeśli niemożliwe jest umieszczenie wszystkich dokumentów zawierających dane osobowe w zamykanych szafach, należy powiadomić o tym pracowników sprzątających, celem uniknięcia zagubienia lub wyrzucenia dokumentów.

D. Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych

1. Niezastosowanie się do prowadzonej przez ADO Polityki, której założenia określa niniejszy dokument, i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 ustawy z dnia 26 czerwca 1974 r. - Kodeks pracy (2020 r. poz. 1320, z 2021 r. poz. 1162).
2. Niezależnie od rozwiązania stosunku pracy osoby popełniające przestępstwo będą pociągane do odpowiedzialności karnej zwłaszcza na podstawie art. 91 i 93 ustawy o ochronie danych osobowych.

E. Postępowanie z kluczami

1. Klucze dostępowe do pomieszczenia wewnętrznego:
- Klucze do pomieszczenia znajdują się u Administratora.
Osoby, które zostały upoważnione do dostępu do kluczy 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.

4. Ewidencja użytkowników / posiadaczy zapasowego klucza do biura ZEASz oraz kluczy do szafek w pomieszczeniach – stanowi **załącznik nr 8 do niniejszej Polityki.**

Rozdział VI. Zabezpieczenia danych osobowych

A. Klasyfikacja informacji

1. Dane przetwarzane w jednostce w formie papierowej.
2. Dane przetwarzane w jednostce dzieli się ze względu na rodzaj danych:
1) dane osobowe,
2) informacje jawne,
3) informacje stanowiące tajemnicę,
4) inne informacje prawnie chronione.

B. Fizyczne środki ochrony danych osobowych

1. Fizyczną ochronę danych i ich przetwarzania realizuje się przez:
1) przetwarzanie danych osobowych w ściśle określonych miejscach do tego przeznaczonych;
2) zabezpieczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe poprzez zastosowanie wysokiej jakości zamków drzwiowych, do których klucze posiadają tylko uprawnione osoby;
3) zamykanie pomieszczeń, w których przetwarzane są dane na czas nieobecności w nich osób upoważnionych do przetwarzania danych;
4) zabezpieczenie wszelkich możliwych dróg dostępu do pomieszczeń, w tym również okien;
5) monitoring pomieszczeń, w których przechowywane są dane, oraz dróg dostępu do tych pomieszczeń (korytarze, klatki schodowe);
6) wyposażenie pomieszczeń w sprzęty oraz meble biurowe dające gwarancję bezpieczeństwa dokumentacji (szafy, biurka zamykane na klucz);
7) zapewnienie odpowiedniej organizacji stanowisk pracy osobom, które przetwarzają dane osobowe;
8) dane osobowe po zakończeniu pracy przechowywane są w zamykanych na klucz meblach biurowych.
2. Niezależnie od niniejszych ustaleń mają zastosowanie wszelkie inne regulaminy i instrukcje dotyczące bezpieczeństwa.

C. Techniczne środki ochrony danych osobowych

1. Techniczną ochronę danych i ich przetwarzania realizuje się poprzez:
1) zastosowanie wykonanych z materiałów nieprzezroczystych teczek oraz segregatorów, w których przechowywane są dane osobowe;
2) oznaczenie teczek oraz segregatorów, w których przechowywane są dane osobowe w sposób utrudniający identyfikację ich zawartości osobom nieupoważnionym;
3) nieprzechowywanie w miarę możliwości danych osobowych w jednym oznaczonym miejscu;
4) wykorzystywanie mechanizmów systemu operacyjnego nadawania uprawnień i praw dostępu;
5) przeprowadzanie testów okresowych systemu ochrony;
6) regularny nadzór oraz przeprowadzanie testów okresowych systemu ochrony danych.

D. Organizacyjne środki ochrony danych osobowych

1. Organizacyjną ochronę danych i ich przetwarzania realizuje się przez:
1) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy ich przetwarzaniu;
2) przeszkolenie osób, o których mowa w pkt 1, w zakresie zabezpieczenia pomieszczeń i budynków;
3) odebranie od osób upoważnionych do przetwarzania danych oświadczeń o zachowaniu poufności przetwarzanych danych;

4) identyfikatory oraz hasła dostępu do poszczególnych baz danych są jedynie w posiadaniu ADO, który jest zobowiązany do przechowywania ich w zamykanych na klucz meblach biurowych, do których nie mają dostępu osoby nieupoważnione.

E. Bezpieczeństwo osobowe

1. Zasady ogólne:

1) w celu ograniczenia ryzyka błędu ludzkiego, kradzieży, oszustwa lub niewłaściwego używania zasobów informatycznych przez pracowników należy przestrzegać procedur w zakresie bezpieczeństwa osobowego;

2) każdy pracownik powinien zostać zapoznany przez bezpośredniego przełożonego z przepisami wewnętrznymi dotyczącymi bezpieczeństwa informacji i podpisać stosowne zobowiązanie;

3) warunki zatrudnienia pracownika na danym stanowisku powinny określać jego zakres dostępu i uprawnień oraz wynikającą z tego odpowiedzialność za bezpieczeństwo informacji;

4) naruszenie przez pracowników zasad ochrony informacji traktowane jest jako ciężkie naruszenie obowiązków pracowniczych.

F. Szkolenia w zakresie ochrony danych osobowych

1. Inspektor ochrony danych po konsultacji z ADO ustala następujące zasady przeprowadzania obowiązkowych szkoleń osób, które są lub będą upoważnione do przetwarzania danych osobowych:

1) szkoli się każdą osobę, która ma zostać upoważniona do przetwarzania danych osobowych;

2) szkolenia wewnętrzne wszystkich osób upoważnionych do przetwarzania danych osobowych przeprowadzane są w przypadku każdej zmiany zasad lub procedur ochrony danych osobowych, oraz innych uzasadnionych okoliczności;

3) przeprowadza się szkolenia dla osób innych niż upoważnione do przetwarzania danych, jeśli pełnione przez nie funkcje wiążą się z zabezpieczeniem danych osobowych;

4) szkolenia przeprowadzane są w siedzibie ADO.

2. Tematyka szkoleń:

1) przepisy i procedury dotyczące ochrony danych osobowych;

2) sposoby ochrony danych przed osobami postronnymi i procedury udostępniania danych osobom, których one dotyczą;

3) obowiązki osób upoważnionych do przetwarzania danych osobowych i innych;

4) odpowiedzialność za naruszenie obowiązków z zakresu ochrony danych osobowych;

5) zasady i procedury określone w polityce bezpieczeństwa.

G. Zarządzanie incydentami

1. Celem zarządzania incydentami bezpieczeństwa jest redukcja ryzyka wystąpienia podobnych incydentów w przyszłości. Jednym z elementów zarządzania ryzykiem jest bieżące monitorowanie zagrożeń oraz okresowa kontrola celowości i adekwatności działań minimalizujących ryzyko.

2. Działania wyjaśniające incydenty bezpieczeństwa mają w szczególności na celu:

1) minimalizację skutków zdarzenia;

2) wyjaśnienie okoliczności zdarzenia;

3) zabezpieczenie dowodów zdarzenia.

3. Skutkiem wystąpienia zagrożenia może być:

1) utrata danych przetwarzanych przez jednostkę;

2) utrata poufności, integralności, dostępności, rozliczalności lub autentyczności danych;

3) utrata wiarygodności i dobrego wizerunku jednostki.

4. System zarządzania ryzykiem jest zbudowany w sposób, który zapewnia prawidłowe działanie na każdym etapie, tj. zapobiegania, monitorowania oraz kontroli.

5. Należy opracować raport z incydentu bezpieczeństwa z uwzględnieniem przyczyn, skutków zdarzenia oraz wniosków ograniczających możliwość wystąpienia zdarzenia w przyszłości.

Rozdział VII. Postępowanie w przypadku naruszenia ochrony danych osobowych

A. Zdarzenie naruszające ochronę danych osobowych

1. Naruszeniem ochrony danych osobowych w rozumieniu Polityki jest każde zdarzenie, zależne jak i niezależne od woli ludzkiej, powodujące zagrożenie bezpieczeństwa danych osobowych, w szczególności:

1) prowadzące do utraty integralności danych (np. pozostawianie dokumentów zawierających dane w miejscach powszechnie dostępnych);
2) zagrażające poufności danych (np. przesyłanie danych drogą elektroniczną bez zabezpieczenia dostępu do plików);
3) zagrażające rozliczalności danych (np. korzystanie przez kilka osób z jednego hasła dostępu).

2. Za naruszenie ochrony danych osobowych uznaje się w szczególności przypadki, gdy:

1) stwierdzono naruszenie obowiązujących przepisów wewnętrznych,
2) stwierdzono naruszenie obowiązujących przepisów prawa,
3) stwierdzono naruszenie zabezpieczeń fizycznych.

B. Zakres przedmiotowy postępowania

1. Postanowienia niniejszego rozdziału stosuje się w przypadku naruszenia oraz uzasadnionego podejrzenia naruszenia ochrony danych osobowych.

C. Tryb postępowania

1. W razie stwierdzenia lub uzyskania informacji stwierdzającej albo uzasadniającej podejrzenie naruszenia ochrony danych osobowych należy niezwłocznie:

1) wysłuchać relacji zawiadamiającego, jak również każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem, w celu oceny zaistniałej sytuacji;
2) poinformować o zaistniałym zdarzeniu ADO;
3) utrwalić wszelkie informacje i okoliczności związane z danym zdarzeniem, a w szczególności:
a) dokładny czas uzyskania informacji stwierdzającej albo uzasadniającej podejrzenie naruszenia ochrony danych osobowych albo samodzielnego wykrycia tego faktu,
b) dane osoby zgłaszającej,
c) stan zabezpieczeń;
4) podjąć niezwłocznie wszelkie działania zmierzające do odzyskania utraconych danych albo zabezpieczenia danych przed utratą;
5) podjąć niezwłocznie wszelkie działania zmierzające do ustalenia przyczyn zdarzenia, jak i okoliczności sprzyjających naruszeniu;
6) podjąć odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby nieuprawnionej do danych osobowych, zminimalizować szkody i zabezpieczyć przed usunięciem ślady naruszenia ochrony danych osobowych.

2. ADO niezwłocznie od momentu ustalenia przyczyn oraz okoliczności sprzyjających naruszeniu, nie później jednak niż w terminie 14 dni od naruszenia, winien sporządzić raport o przyczynach, przebiegu i wnioskach z naruszenia zabezpieczenia.

3. W raporcie winny znaleźć się informacje o:

1) dacie i godzinie powiadomienia,
2) dacie i godzinie naruszenia,
3) środkach podjętych przez zawiadamiającego,
4) podjętych działaniach wraz z ich uzasadnieniem,
5) analizie przyczyn oraz okoliczności sprzyjających naruszeniu.

D. Role i odpowiedzialność

1. Wszyscy pracownicy pełnią w systemie zarządzania bezpieczeństwem informacji określone role i zobowiązani są do zapewnienia właściwej ochrony zasobów informacyjnych.
2. Za bezpieczeństwo informacji przetwarzanych w jednostce odpowiadają wszyscy pracownicy - w zakresie wynikającym z zajmowanego stanowiska, obowiązków, uprawnień i odpowiedzialności z tym związanej.

Rozdział VIII

OCENA RYZYKA I PRZEGLĄDY

1. Ocena ryzyka

a) Systemy informatyczne i aplikacje powinny być poddawane ocenie ryzyka pod kątem identyfikacji zagrożeń dla bezpieczeństwa przetwarzania danych osobowych co najmniej raz na dwa lata. Ocena ryzyka powinna być również przeprowadzana przy dużych zmianach procesów biznesowych, systemów informatycznych i aplikacji.

b) Narzędzia informatyczne służące do oceny ryzyka bezpieczeństwa przetwarzania danych powinny być chronione przed nieautoryzowanym lub nieuprawnionym dostępem a ich użycie odpowiednio kontrolowane.

2. Przeglądy bezpieczeństwa

1. Przeglądy bezpieczeństwa przetwarzania danych osobowych powinny być przeprowadzane okresowo, co najmniej raz na 2 lata w celu określenia wymaganego poziomu zabezpieczeń pozwalającego na ograniczenie ryzyka do poziomu akceptowalnego.
2. Przeglądy zgodności z zasadami bezpieczeństwa przetwarzania danych osobowych urządzeń informatycznych oraz sieci teleinformatycznych należy przeprowadzać okresowo, co najmniej raz na rok.
3. Narzędzia informatyczne służące do przeprowadzania przeglądów bezpieczeństwa przetwarzania danych osobowych powinny być chronione przed nieautoryzowanym lub nieuprawnionym dostępem a ich użycie odpowiednio kontrolowane.

Rozdział IX.

Postanowienia końcowe

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszym dokumentem oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści.
2. Każdej osobie upoważnionej do przetwarzania danych ADO przekazuje wyciąg z polityki bezpieczeństwa, a użytkownikom dodatkowo z IZSI.
3. Polityka wchodzi w życie z dniem podpisania zarządzenia wprowadzającego.

Wykaz załączników

Załącznik nr 1	-	Wzór zgody na przetwarzanie danych osobowych
Załącznik nr 2	-	Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym są przetwarzane dane osobowe
Załącznik nr 3	-	Wzór wniosku o wydanie upoważnienia do przetwarzania danych osobowych
Załącznik nr 4	-	Wzór upoważnienia do przetwarzania danych osobowych
Załącznik nr 5	-	Oświadczenie o zachowaniu poufności
Załącznik nr 6	-	Rejestr osób upoważnionych do przetwarzania danych osobowych
Załącznik nr 7	-	Wykaz zbioru danych
Załącznik nr 8	-	Ewidencja użytkowników/ posiadaczy zapasowego klucza do biura ZEASz oraz kluczy do szafek w pomieszczeniach.
Załącznik nr 9	-	Raport z obowiązujących procedur w zakresie ochrony danych .