WÓJT GMINY
MARCINOWICE

Zarządzenie nr 60/2015
Wójta Gminy Marcinowice
z dnia 14 maja 2015r.

w sprawie wprowadzenia Polityki bezpieczeństwa informacji i ochrony danych osobowych w Urzędzie Gminy Marcinowice

Na podstawie art. 30 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2013 r. poz. 594 z późn. zm.) oraz art. 36 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014r. poz. 1182 z późn. zm.) i § 1 pkt 1 oraz § 3 i § 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr. 100, poz. 1024)

zarządzam, co następuje:

§ 1.

Dla zapewnienia ochrony przetwarzanych danych osobowych wprowadza się „Politykę bezpieczeństwa informacji i ochrony danych osobowych w Urzędzie Gminy Marcinowice", zwaną dalej Polityką, stanowiącą załącznik do niniejszego Zarządzenia.

§ 2.

Polityka ma zastosowanie na wszystkich stanowiskach pracy, gdzie przetwarzane są dane osobowe lub praca odbywa się w systemie informatycznym Urzędu Gminy Marcinowice.

§ 3.

1. Zobowiązuję wszystkich pracowników Urzędu Gminy Marcinowice do zapoznania się z treścią Polityki w terminie trzech tygodni od dnia wejścia w życie Zarządzenia.
2. Za wykonanie postanowień ust. 1 odpowiadają bezpośredni przełożeni.

§ 4.

Nadzór nad realizacją postanowień Zarządzenia powierzam Sekretarzowi Gminy Marcinowice.

§ 5.

Traci moc Zarządzenie Nr 21/1999 Wójta Gminy Marcinowice z dnia 25 października 1999r. w sprawie ustalenia zasad ochrony danych osobowych w Urzędzie Gminy Marcinowice.

§ 6.

Zarządzenie wchodzi w życie z dniem podpisania.

RADCA PRAWNY
Mariusz Starke

WÓJT
Władysław Gołębiowski

Załącznik
do Zarządzenia nr 60/2015
Wójta Gminy Marcinowice
z dnia 14 maja 2015r.

POLITYKA

bezpieczeństwa informacji i ochrony danych osobowych

URZĘDU GMINY MARCINOWICE

Marcinowice, maj 2015r.

WSTĘP

Niniejszy dokument został opracowany w oparciu o Ustawę z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. Z 2014r., poz. 1182 z późn. zm.).

System Zarządzania Bezpieczeństwem Informacji (SZBI) w Urzędzie Gminy Marcinowice stanowi jeden z elementów mających na celu zapewnienie odpowiednich warunków działalności Urzędu w zakresie prowadzonych spraw, przy jednoczesnym zachowaniu dostępności, poufności i integralności (a także rozliczania) ważnych dla Urzędu informacji oraz przy ochronie wszelkich kluczowych aktywów, w granicach działania Urzędu. SZBI funkcjonuje w integralnym połączeniu z prowadzoną kontrolą zarządczą, przy założeniu wydatkowania posiadanych środków finansowych w sposób celowy, oszczędny i pozwalający na uzyskanie najlepszych efektów i osiągnięcie założonych celów przy optymalnym doborze metod i środków.

Pod używanym w niniejszym dokumencie, pojęciem **Urzędu** rozumiany jest **Urząd Gminy Marcinowice.**

Bezpieczeństwo informacji oraz systemów, w których są one przetwarzane jest jednym z kluczowych elementów zapewniających realizację zadań w Urzędzie, gdyż obejmuje wszystkie sfery działalności Urzędu jako jednostki organizacyjnej Gminy Marcinowice.

Polityka Bezpieczeństwa Informacji Urzędu opisuje m.in. zasady ochrony informacji obowiązujące w tej jednostce, zasady zarządzania incydentem, sposób postępowania z incydentami oraz z naruszeniami bezpieczeństwa informacji, role i zadania osób uczestniczących w procesie przetwarzania informacji, procedury zarządzania bezpieczeństwem informacji.

Z dokumentem Polityki powinny się zapoznać **wszystkie osoby mające dostęp do informacji** - pracownicy Urzędu, kadra kierownicza oraz personel firm zewnętrznych, jeżeli istnieje taka potrzeba. O potrzebie tej decyduje Administrator Bezpieczeństwa Informacji po analizie umowy podpisanej z firmą zewnętrzną.

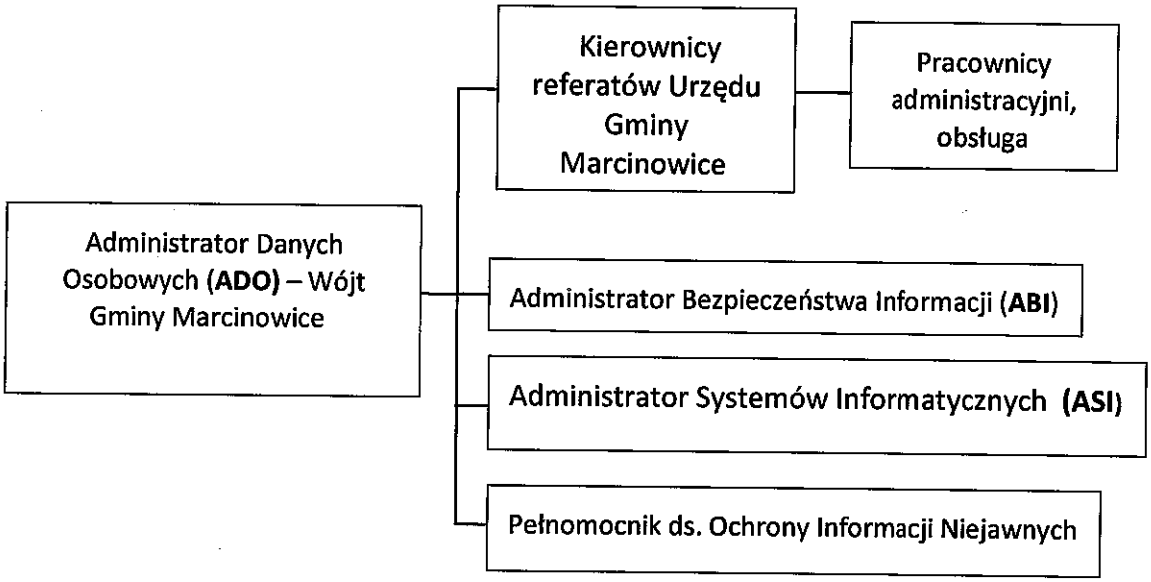
Zasady zawarte w niniejszym dokumencie muszą być przestrzegane przez wszystkie osoby mające dostęp do informacji Urzędu Gminy Marcinowice.

Część procedur SZIB stanowią zarządzenia Wójta Gminy Marcinowice, obowiązujące i zamieszczone w Biuletynie Informacji Publicznej.

ROZDZIAŁ I

SCHEMAT/STRUKTURA ORGANIZACYJNA POLITYKI BEZPIECZEŃSTWA INFORMACJI W URZĘDZIE GMINY MARCINOWICE oraz ZAKRESY ODPOWIEDZIALNOŚCI

Administratorem Danych Osobowych **(ADO)** w stosunku do wszystkich pracowników jest **Wójt Gminy Marcinowice.**



Administrator Danych Osobowych (ADO) - Wójt odpowiada za prawidłowość działania SZBI poprzez:

1. wprowadzenie, zarządzanie i sprawowanie nadzoru nad działaniem SZBI w zakresie dotyczącym kierowników Referatów Urzędu;
2. prowadzenie wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
3. prowadzenie wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
4. sporządzenie opisu struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;

5. określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczania przetwarzanych danych.

W zakresie bezpieczeństwa informacji Wójtowi podlegają kierownicy Referatów Urzędu Gminy Marcinowice.

Kierownicy odpowiadają za:

1. przestrzeganie zasad ochrony informacji przez nich samych jak i przez podległych im pracowników,
2. identyfikowanie i dokumentowanie zagrożeń dla bezpieczeństwa informacji (raport z incydentu), kierownik podejmuje odpowiednie działania w przypadku wykrycia naruszeń bezpieczeństwa (zgłasza fakt ABI, zabezpiecza zdarzenie w taki sposób, by informacje nie dostały się w ręce osób nieupoważnionych),
3. uwrażliwianie pracowników w zakresie obowiązków związanych z ochroną informacji na stanowiskach pracy,
4. odpowiadają za poprawność merytoryczną treści danych gromadzonych w komórce organizacyjnej,
5. odpowiadają za przestrzeganie zasad bezpieczeństwa przetwarzania danych osobowych,
6. merytorycznie wnioskują do ADO o nadanie lub odebranie upoważnień dla swoich pracowników pracujących w systemach teleinformatycznych oraz w zbiorach (kierownik ma obowiązek zgłosić ABI i ASI fakt zatrudnienia lub zwolnienia w jego komórce pracownika),
7. proponują zmiany i rozwiązania w dokumentach Polityki Bezpieczeństwa Informacji,
8. nadzorują zabezpieczenia dla zbiorów własnych (szafy, sejfy, kody dostępu, hasła),
9. wnioskują o zapewnienie użytkownikowi stanowiska pracy zgodnie z powierzonymi obowiązkami,
10. współpracują z osobami pełniącymi rolę odpowiedzialne za bezpieczeństwo informacji w SZBI oraz innymi kierownikami w zakresie realizacji zadań dotyczących bezpieczeństwa informacji.

ADO (Wójtowi) podlegają:

Administrator Bezpieczeństwa Informacji (ABI). Do zadań ABI należy:

1. zapewnienie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
   a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla ADO,
   b) nadzorowanie opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych osobowych oraz przestrzegania zasad w niej określonych,

c) zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,

2. opracowanie Polityki Bezpieczeństwa Informacji Urzędu,
3. sprawuje nadzór nad realizacją zapisów polityki bezpieczeństwa,
4. koordynuje działania związane z ochroną informacji w sądzie,
5. prowadzi we współpracy z zespołem ds. zarządzania ryzykiem wewnętrznym analizę ryzyka i raporty z incydentów,
6. prowadzi rejestry:
   a) nadanych upoważnień,
   b) oświadczeń,
   c) zbiorów danych,
   d) budynków i pomieszczeń, w których przechowuje się dane,
7. przedstawia ADO raz w roku raport o stanie bezpieczeństwa informacji,
8. na polecenie ADO przygotowuje procedury awaryjne związane z incydentami bezpieczeństwa,
9. współpracuje z osobami odpowiedzialnymi za zamówienia publiczne pod kątem przekazywanych firmom zewnętrznych danych osobowych (umowy powierzenia).
10. udzielanie upoważnienia do przetwarzania danych osobowych, określając ich zakres oraz termin ważności,
11. prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
12. identyfikowanie potrzeb w zakresie adekwatności stosowanych zabezpieczeń i nadzorowanie prawidłowości ich wdrożenia i przestrzegania,
13. udzielanie wyjaśnień i interpretowanie zgodności stosowanych rozwiązań w zakresie danych osobowych z przepisami prawa,
14. obsługiwanie kontroli oraz współpracowanie z podmiotami zewnętrznymi uprawnionymi do dostępu do danych osobowych przetwarzanych w Urzędzie,
15. koordynowanie szkoleń dla pracowników w celu podnoszenia świadomości oraz kwalifikacji osób przetwarzających dane osobowe w zakresie problematyki bezpieczeństwa i ochrony danych osobowych,
16. prowadzenie korespondencji z Głównym Inspektorem Ochrony Danych Osobowych (GIODO),
17. nadzorowanie realizacji zadań ASI,
18. szacowanie ryzyka wystąpienia incydentów,
19. uczestniczenie w wyjaśnieniach zaistniałych incydentów.

Administrator Systemów Informatycznych (**ASI**), który:

1. opracowuje Instrukcję zarządzania systemem informatycznym,
2. określa zasady użytkowania stacji roboczej przez pracowników,
3. sprawuje nadzór nad bezpieczeństwem systemów teleinformatycznych,
4. uczestniczy w analizie ryzyka technicznego,
5. opracowuje plany awaryjne dla poszczególnych systemów teleinformatycznych, (patrz: plan ciągłości działania jednostki),
6. opiniuje dokumenty wymagań bezpieczeństwa dla systemów teleinformatycznych,
7. analizuje raporty z wszelkich zdarzeń związanych z bezpieczeństwem systemów teleinformatycznych,
8. udziela, zmienia i odbiera uprawnienia użytkownikom - na wniosek kierowników referatów Urzędu,
9. natychmiastowo odbiera uprawnienia użytkownikom w sytuacji naruszenia bezpieczeństwa informacji (incydent) informując o tym fakcie ADO,
10. szkoli nowo przyjętych pracowników z zakresu bezpieczeństwa informacji w zakresie stanowiska komputerowego na którym będzie pracował,
11. sprawuje kontrole nad procesem przyznawania praw dostępu oraz prowadzi rejestr użytkowników systemów teleinformatycznych,
12. składa ADO raz w roku raport o stanie bezpieczeństwa w systemach teleinformatycznych,
13. monitoruje oraz zapewnia ciągłość działania systemu teleinformatycznego,
14. monitoruje wydajność systemu teleinformatycznego,
15. prowadzi dokumentację systemów teleinformatycznych i aplikacji,
16. instaluje i konfiguruje sprzęt, systemy i aplikacje,
17. odpowiada za administrację oprogramowaniem systemowym w stopniu zapewniającym bezpieczeństwo systemu i danych w nim przetwarzanych przed nieupoważnionym dostępem,
18. współpracuje z dostawcami aplikacji,
19. nadzoruje wdrożone aplikacje,
20. zarządza kopiami awaryjnymi danych, w tym danych osobowych, zgodnie z otrzymanym upoważnieniem,
21. opracowuje dokumentacje dla systemów teleinformatycznych,
22. opracowuje standardy dotyczące systemów teleinformatycznych,
23. opracowuje procedury określające zarządzanie systemem teleinformatycznym,
24. przygotowuje dokumenty Polityk Bezpieczeństwa dla systemów teleinformatycznych, nad którymi sprawuje nadzór,
25. nadzoruje zabezpieczenia dla zasobów, nad którymi sprawuje nadzór.

Odpowiedzialność za bezpieczeństwo informacji w Urzędzie ponoszą

WSZYSCY PRACOWNICY,

zgodnie z posiadanymi zakresami obowiązków oraz wykonywanymi zadaniami.

Każdy pracownik obowiązany jest dbać o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania informacji, zgodnie z obowiązującymi w Urzędzie przepisami wewnętrznymi tj.:

1. stosować zasady opisane w Polityce bezpieczeństwa informacji oraz innych dokumentach wewnętrznych Urzędu,
2. chronić informacje podlegające ochronie przed dostępem do nich osób nieuprawnionych,
3. chronić dane przed przypadkowym lub umyślnym zniszczeniem, utratą lub modyfikacją,
4. chronić sprzęt, wydruki komputerowe i inne nośniki zawierające dane służbowe,
5. utrzymywać w tajemnicy powierzone hasła, częstotliwość ich zmiany oraz szczegóły technologiczne systemów także po ustaniu zatrudnienia w Urzędzie,
6. stosować się do szczegółowych zaleceń ASI w zakresie ochrony antywirusowej,
7. brać udział w szkoleniach z zakresu ochrony danych osobowych i bezpieczeństwa informacji.

Bezzwłocznie należy powiadomić Administratora Bezpieczeństwa Informacji lub Administratora Systemów Informatycznych o:

a. ujawnieniu lub możliwości ujawnienia informacji chronionych osobom nieupoważnionym,
b. nieautoryzowanej zmianie informacji chronionych lub możliwości wprowadzenia nieautoryzowanych zmian,
c. zniszczeniu lub możliwości zniszczenia informacji chronionych,
d. zablokowaniu lub możliwości zablokowania pracy systemu informatycznego przetwarzającego informacje chronione lub uniemożliwienia innego dostępu do informacji chronionych,
e. każdym podejrzeniu próby włamania.

ABI i ASI zastępują się wzajemnie i pełnią swoje obowiązki na czas nieobecności, któregoś z nich.

Pozostałe zastępstwa zgodnie z przyjętymi w Urzędzie zasadami i strukturą.

Deklaracja kierownictwa Urzędu

Kierownictwo Urzędu przywiązuje dużą wagę do ochrony informacji tworzonych, przetwarzanych i składowanych w Urzędzie. Szczególną wagę przywiązuje się do ochrony informacji prawnie chronionych. Zabezpieczenia funkcjonujące w Urzędzie mają na celu zapewnienie

poufności, integralności i **dostępności** informacji a także jej **rozliczania** i ciągłości działania Urzędu.

AKTYWA

Najważniejszymi **aktywami** dla Urzędu są **ludzie, akta spraw i systemy informatyczne** oraz informacje jakie posiadają i zawierają te aktywa.

INFORMACJE w Urzędzie zawarte są w:

a. danych osobowych /kadrowych/ pracowników,
b. danych osobowych zawartych w aktach prowadzonych spraw,
c. merytorycznej treści akt prowadzonych spraw,
d. danych księgowych i płacowych,
e. wszelkich danych statystycznych,
f. innych pismach

i bez względu na to w jakiej formie informacje te się znajdują: papierowej, elektronicznej czy ustnej należy je chronić.

Ochrona informacji w Urzędzie bazuje na czterech kluczowych zasadach:

1. zapewnienia, że informacja jest udostępniana jedynie *osobom upoważnionym* (tzw. zasada **poufności** informacji);
2. zapewnienia *dokładności* i kompletności informacji oraz metod jej przetwarzania (tzw. zasada **integralności** informacji);
3. zapewnienia, że osoby upoważnione mają *dostęp do informacji* i związanych z nią aktywów tylko wtedy, gdy istnieje taka potrzeba (tzw. zasada **dostępności** informacji);
4. zasada **rozliczania,** zapewniająca z jednej strony, możliwość jednoznacznego rejestrowania faktu, *kto dokonał* określonej operacji na informacji, a z drugiej, że działania Urzędu mogą być przypisane w sposób jednoznaczny tylko i wyłącznie Urzędowi.

Powyższe zasady zapewnią właściwą ochronę informacji tylko wówczas, gdy będą one przyjęte za obowiązujące **dla wszystkich** pracowników w ramach stosowania SZIB, gdy zostaną wdrożone i utrzymane niezbędne zabezpieczenia organizacyjne i techniczne, oraz wówczas gdy następował będzie proces ciągłego podnoszenie świadomości i kwalifikacji pracowników w obszarze bezpieczeństwa informacji.

Pozostałe aktywa (meble, sprzęt, urządzenia, budynki, instalacje), jakich posiadaczem jest Urząd, są chronione poprzez zapewnienie całodobowej ochrony i systemów (ppoż, antywłamaniowych i monitoringu).

Dobór zabezpieczeń

Zabezpieczenia dobierane przez Urząd są adekwatne do wymagań prawnych i wyników analizy ryzyka, prowadzonej w ramach kontroli zarządczej.

Zabezpieczenia fizyczne, techniczne i organizacyjne dobierane są tak, aby uzupełniać się wzajemnie, zapewniając wymagany poziom bezpieczeństwa informacji.

Aktywa w postaci akt sprawy zabezpiecza się przed dostępem do nich osób nie upoważnionych w następujący sposób:

Pracownicy w czasie pracy nie pozostawią dokumentów „bez opieki" ani w sekretariacie ani w pomieszczeniu, w którym pracują, ani w żadnym innym pomieszczeniu.

W przypadku konieczności opuszczenia przez pracownika pomieszczenia, w którym znajdują się dokumenty /nośniki/ zawierające informacje, osoby nieuprawnione do przebywania w nim wyprasza się na korytarz.

Po zakończeniu pracy dokumenty zamykane są w szafach. Szafy dwudrzwiowe ,nie przesuwane, zamyka się w sposób uniemożliwiający ich otwarcie, a klucz zabezpiecza się przed dostępem osób nieupoważnionych. Natomiast szafy przesuwne zamyka się i będą plombowane. Jeżeli zamek w szafie dwudrzwiowej, nieprzesuwnej, nie spełnia swojej funkcji taką szafę należy również zaplombować.

Plombowanie i zamykanie szaf daje gwarancję, że po godzinach urzędowania osoby nieupoważnione nie mają dostępu do dokumentów.

W przypadku referatów, w których znajdują się liczne tomy dokumentów i dokumenty te (w wyjątkowych sytuacjach) składowane są na podłodze, po zakończeniu pracy pokój taki należy zamknąć i zaplombować umieszczając na drzwiach widoczny napis „W DNIU DZISIEJSZYM PROSZĘ NIE SPRZĄTAĆ I NIE WCHODZIĆ DO POMIESZCZENIA, podpis i pieczęć kierownika".

Sprzątanie tego pokoju odbędzie się w godzinach urzędowania w innym dniu pod nadzorem upoważnionego pracownika.

Dokumenty wytwarzane przez Urząd przesyłane są do innych podmiotów w bezpieczny sposób tj. pocztą polską lub autem służbowym.

Polityka czystego biurka ma na celu zapobieganie nieautoryzowanemu dostępowi do informacji lub kradzieży informacji.

Ważne dokumenty i nośniki danych absolutnie nie powinny pozostać niezabezpieczone /bez nadzoru użytkownika lub współpracownika/ w czasie nawet chwilowej nieobecności użytkownika w pomieszczeniu. Po opuszczeniu pokoju przez wszystkich pracowników /w tym w godzinach urzędowania/ pokój należy zamknąć w sposób uniemożliwiający dostęp do niego dla osób

nieuprawnionych. Po zakończeniu pracy ważne dokumenty i komputerowe nośniki z danymi powinny być przechowywane w szafach, a pokoje zamyka się na klucz. Klucze przechowuje się w metalowej szafce w sekretariacie Urzędu.

Polityka czystego ekranu ma na celu zabezpieczenie przed nieautoryzowanym dostępem do systemów teleinformatycznych i zabezpieczenie przez ujawnieniem informacji chronionych.

Każdorazowe odejście od stanowiska pracy powinno zostać poprzedzone **wylogowaniem się** lub zablokowaniem dostępu do systemu tak, aby niemożliwe było uzyskanie nieautoryzowanego dostępu do systemu.

Po zakończeniu pracy należy zamknąć aktywne aplikacje oraz wyrejestrować się (wylogować się) z systemu lub też zablokować dostęp do systemu. Szczególną uwagę należy zwrócić na drukarki sieciowe i kserokopiarki dostępne dla większej liczby pracowników. W takim przypadku pracownicy powinni odbierać dokumenty natychmiast po wykonaniu przez urządzenie zleconego zadania. Nie powinny one pozostawać dostępne ani dla obcych osób ani dla pracowników nieposiadających stosownych uprawnień.

Zabezpieczenia kryptograficzne

Wszelkie służbowe nośniki elektroniczne (laptopy, pendrive'y, płyty, dyskietki) używane do przenoszenia informacji, a opuszczające budynek Sądu muszą być szyfrowane. Kierownicy referatów Urzędu sprawują nadzór nad tym, by ich pracownicy posługiwali się właściwymi nośnikami.

Każdy, kto obsługuje w/w nośnik (a nie jest on zaszyfrowany) ma obowiązek zgłosić pisemny wniosek w sprawie otrzymania zaszyfrowanego nośnika lub zaszyfrowania już posiadanego nośnika informacji u Administratora Systemów Informatycznych.

Urząd wykorzystuje zabezpieczenia kryptograficzne wszędzie tam, gdzie istnieje konieczność ich stosowania. O konieczności stosowania decyduje (po otrzymaniu pisemnego wniosku) ASI.

Ze względu na ryzyko utraty dostępności informacji wszystkie zabezpieczenia kryptograficzne muszą być autoryzowane przez ASI.

Szczegółowe wymagania opisane zostały w Instrukcji zarządzania systemem teleinformatycznym.

Nośniki danych lub dokumenty, które są zbędne, a zawierają dane osobowe, należy zniszczyć w sposób uniemożliwiający odczytanie informacji.

Kierownik danego referatu zbiera zbędne/nieużyteczne nośniki informacji (pisma, płyty, pen i inne) we wskazanym przez siebie miejscu w referacie (zabezpiecza je w szafie) i w zależności od potrzeb przekazuje je do ASI celem zniszczenia. Z czynności zniszczenia ASI sporządza notatkę zawierającą datę, rodzaj oraz liczbę niszczonych nośników i przechowuje ją w swoich dokumentach.

Monitorowanie i przegląd Systemu Zarządzania Bezpieczeństwem Informacji

System Zarządzania Bezpieczeństwem Informacji w Urzędzie jest monitorowany i stale usprawniany poprzez podejmowanie następujących działań:

1. wykonywanie audytów wewnętrznych, wg potrzeb i na wniosek ABI, ASI zatwierdzony przez ADO,
2. wykonywanie audytów zewnętrznych wg potrzeb i na wniosek ABI, ASI zatwierdzony przez ADO.
3. weryfikacji dokumentacji na poziomie procedur, instrukcji i regulaminów dokonywanej przez ABI i ASI.

W celu uszczegółowienia zasad opisanych w polityce SZBI w razie potrzeby tworzone będą procedury, instrukcje, regulaminy i inne dokumenty.

Bieżący nadzór nad wypełnianiem zaleceń Polityki bezpieczeństwa Iinformacji pełni ABI i ASI.

Postępowanie niezgodne z niniejszą Polityką wiąże się ze skutkami prawnymi przewidzianymi w Regulaminie Pracy, ustawie o ochronie danych osobowych oraz kodeksie pracy.

Zespół ds. Polityki bezpieczeństwa informacji

W Urzędzie, w zależności od potrzeb, może zostać utworzony **Zespół do spraw Polityki Bezpieczeństwa Informacji.** Zespół do spraw Polityki Bezpieczeństwa Informacji jest powoływany i odwoływany przez Wójta Gminy Marcinowice. Zespół powołuje się na wniosek ABI lub ASI.

Rodzaje informacji przetwarzanych w Urzędzie i sposób ich ochrony

W oparciu o wymagania prawne wszystkie przetwarzane w Urzędzie informacje podzielone zostały na następujące grupy:

Informacje niejawne:

Ochrona informacji niejawnych opiera się o wymagania prawne ustawy o ochronie informacji niejawnych.

Za organizację systemu ochrony informacji niejawnych w Urzędzie odpowiada pełnomocnik ds. Ochrony Informacji Niejawnych, który posiada uprawnienia oraz realizuje zadania określone w przepisach o ochronie informacji niejawnych i w sprawach merytorycznych zgodnie z art. 14 ust 2 ustawy z dnia 5 sierpnia 2010r. o ochronie informacji niejawnych, podlega bezpośrednio Wójtowi Gminy Marcinowice. Informacje niejawne posiadają własny, niezależny od definiowanego przez niniejszą politykę system ochrony zgodny z wymaganiami ustawy o ochronie informacji niejawnych.

Pozostałe tajemnice ustawowo chronione:

Tajemnice pracodawcy na podstawie Kodeksu pracy art. 100.

Tajemnicę skarbową, którą objęte są indywidualne dane zawarte w deklaracji i na podstawie ustawy o kontroli skarbowej art. 34 oraz ordynacji podatkowej Dział VII.

Informacje publiczne to:

informacje, o których mówi ustawa z dnia 6 września 2001 roku o dostępie do informacji publicznej (Dz. U. z 2014r. , poz. 782 z późn. zm.).

Informacja publiczna może być przechowywana na dowolnym nośniku i w dowolnym systemie teleinformatycznym oraz może być przesyłana w sieci pod warunkiem, że zapewniona jest dostępność i integralność informacji.

Informacje w Urzędzie, posiadają odpowiednią klasę i muszą być adekwatnie chronione. Przynależność do odpowiednich klas została opisana poniżej.

Informacje do użytku służbowego:

1. wewnętrzna komunikacja, korespondencja, poczta elektroniczna,
2. wewnętrzne dokumenty takie jak: wytyczne, instrukcje, plany organizacji, zarządzenia,
3. dane wewnętrzne takie jak: oferty, raporty,
4. fragmenty umów zawierające chronione informacje oferenta,
5. dokumentacja projektowa,
7. informacje powierzone przez osoby trzecie,
8. dane osobowe interesantów.

Rozpowszechnianie tych informacji jest dozwolone tylko w ramach wykonywania obowiązków służbowych tj.:

1. rozpowszechnianie ich dozwolone jest tylko wewnątrz Urzędu oraz do instytucji, osób, firm i organizacji współpracujących z Urzędem,
2. nie wolno udostępniać tego typu informacji osobom z zewnątrz bez podpisania odpowiednich umów o poufności,
3. dobór metod zabezpieczeń - transmisji i składowania informacji należy dostosować do rodzaju informacji, wymagań prawnych i treści zobowiązań zawartych w umowach,
4. informacje mogą być przekazywane przez telefon i inne środki komunikacji głosowej, pod warunkiem, że zachowane zostaną zasady bezpieczeństwa tj. dokładna weryfikacja rozmówcy itp.,
5. dokumenty papierowe należy niszczyć w niszczarce o co najmniej 2 stopniu bezpieczeństwa.

Informacje do użytku wewnętrznego:

1. wszelkie informacje związane z dokonywanymi operacjami bankowymi,
2. dane przetargowe przed publikacją,

3. dane kadrowe pracowników.

Rozpowszechniane dozwolone wyłącznie wśród wyznaczonych przez ADO pracowników Urzędu.

1. Kopiowanie jest dozwolone po upoważnieniu przez właściciela informacji.
2. Dokumenty papierowe przekazuje się w zaklejonych kopertach uniemożliwiających podejrzenie,
   z napisem „Do rąk własnych".
3. Transmisja dokumentów zarówno wewnątrz jak i na zewnątrz sieci Urzędu musi być szyfrowana.
4. Do przechowywania informacji w urządzeniach przenośnych należy zastosować mechanizmy szyfrujące.
5. Nie wolno zostawiać dokumentów papierowych w miejscach dostępnych dla osób trzecich.
6. Przechowywanie informacji w sieci wewnętrznej możliwe jest wyłącznie w strefie chronionej.
7. Dokumenty papierowe należy niszczyć w niszczarce o co najmniej 3 stopniu bezpieczeństwa.
8. Informacje w formie elektronicznej można kasować normalnie pod warunkiem, że nie jest możliwy dostęp osób nieuprawnionych do urządzeń przechowujących informacje.
9. Nośniki danych należy kasować w sposób uniemożliwiający odtworzenie lub niszczyć.
10. Przebywając w miejscach publicznych należy unikać przekazywania informacji przez telefon i inne środki komunikacji głosowej.

Informacje Powszechnie Dostępne

Dokument nieopatrzony żadną klauzulą bezpieczeństwa należy traktować jako zawierający informacje powszechnie dostępne.

Powszechna dostępność informacji oznacza możliwość jej ujawnienia pracownikom oraz osobom trzecim, w związku z realizacją spraw czy zadań.

Kontrola dostępu

Urząd zarządza kontrolą dostępu.

Celem takiego postępowania jest zapewnienie, że dostęp do informacji, miejsc, urządzeń lub systemów i ich przetwarzania mają tylko osoby uprawnione.

Pomieszczenia biurowe w Urzędzie zamykane są na klucz.

Każdy pracownik odpowiada za pobrany z tablicy klucz. W przypadku zagubienia klucza należy niezwłocznie pisemnie poinformować o tym fakcie przełożonego.

Zaleca się także stosowanie tzw. barierek ochronnych (lady) wewnątrz sekretariatu, celem ograniczenia dostępu osobie postronnej (petentowi) do informacji.

Kontrola dostępu do obszarów chronionych.

Do budynku prowadzi jedno wejście. Wejście przeznaczone jest dla pracowników oraz petentów.

Na terenie Urzędu znajdują się obszary wydzielone z uwagi na informacje chronione w szczególny sposób i są to: archiwum, serwerownia, pomieszczenie przechowywania akt osobowych, pomieszczenia poddasza, pokój pełnomocnika ds. ochrony informacji niejawnych, pomieszczenie monitoringu, Referat Budżetu i Finansów.

Sprzątanie i konserwacja urządzeń znajdujących się w tych obszarach możliwe jest tylko w obecności upoważnionych pracowników.

Sprzątanie w w/w pomieszczeniach odbywać się będzie w godzinach urzędowania w następujący sposób:

pomieszczenia: serwerownia, - raz na PÓŁ ROKU

pomieszczenia: archiwum – raz w ROKU

pomieszczenia: Referat Budżetu i Finansów , pomieszczenie przechowywania akt osobowych, pokój pełnomocnika ds. ochrony informacji niejawnych, - dwa razy w TYGODNIU

Urząd wyposażony jest w następujące instalacje: alarmową, teleinformatyczną, wodociągową, elektryczną, gazową, CO – wszystkie są sprawne i poddawane regularnym przeglądom.

Zarządzanie incydentami związanymi z bezpieczeństwem informacji

Incydent bezpieczeństwa informacji to jedno lub seria niepożądanych lub niespodziewanych zdarzeń, których wystąpienie może, ze znacznym prawdopodobieństwem, zakłócić działania Urzędu oraz zagrozić bezpieczeństwu informacji.

Każde zdarzenie związane z bezpieczeństwem informacji oraz słabością systemów informacyjnych, musi być zgłoszone w sposób umożliwiający szybkie podjęcie działań korygujących.

Urząd zarządza zdarzeniami i incydentami związanymi z bezpieczeństwem informacji.

Zasady zarządzania incydentem to:

1. każdy zauważony incydent (zerwanie plomby, podejrzenie kradzieży, zainstalowanie niewiadomego oprogramowania, zostawienie bez nadzoru otwartego pomieszczenia, przebywanie w pomieszczeniach osób nieupoważnionych bez nadzoru itp.) powinien zostać zgłoszony, zarejestrowany i załatwiony,
2. w przypadku zauważenia próby włamania, kradzieży dokumentów lub sprzętu oraz wszelkich innych prób niszczenia mienia, powiadamia się ADO, ABI i ASI,

3. w przypadku wystąpienia klęski żywiołowej lub aktu terroru w pierwszej kolejności powiadamiane są właściwe służby, ADO, ABI i ASI,
4. incydenty są rejestrowane przez ABI i ASI.

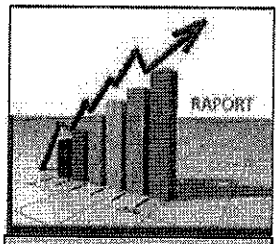
Analiza raptów z incydentów związanych z bezpieczeństwem informacji należy do zadań zespołu ds. zarządzania ryzykiem wewnętrznym, ABI i ASI.

Pracownicy, co do których ustalono, że swoim postępowaniem naruszają procedury bezpieczeństwa informacji, danych osobowych, informacji poufnych w rozumieniu ustawy o obrocie instrumentami finansowymi, poniosą konsekwencje przewidziane prawem.

Wniosek w/w sprawie za pośrednictwem ABI lub ASI kierownicy referatów Urzędu kierują do ADO.

WZÓR:

RAPORT
Z INCYDENTU NARUSZENIA BEZPIECZEŃSTWA INFORMACJI



Osoba zgłaszająca:	
Imię i nazwisko:	
telefon:	
Data zdarzenia:	
Miejsce zdarzenia:	
Krótki opis zdarzenia:	
	Data i podpis osoby zgłaszającej
ABI/ASI	
Data przyjęcia:	
Krótki opis podjętych działań doraźnych:	
Propozycje: Wydane dyspozycje:	

Data i podpis ABI/ASI

Dnia ..... o zaistnieniu incydentu poinformowano zespół ds. zarządzania ryzykiem wewnętrznym.

Zarządzanie ciągłością działania

Na podstawie analizy ryzyka dokonywanej przez zespół ds. zarządzania ryzykiem wewnętrznym, w zależności od wyników przeprowadzonej analizy, w razie konieczności będą tworzone plany postępowania w sytuacjach awaryjnych i kryzysowych.

Celem takiego postępowania będzie przeciwdziałanie przerwom w działalności Urzędu w czasie awarii lub katastrofy.

O konieczności tworzenia planu ciągłości działania dla konkretnego systemu decyduje Wójt Gminy Marcinowice na podstawie wyniku analizy ryzyka.

Za tworzenie, przeglądy i testowanie planów ciągłości działania odpowiadają zespół ds. zarządzania ryzykiem wewnętrznym, ABI, ASI i kierownicy referatów Urzędu.

Odstępstwa od reguł ochrony

W wyjątkowych, uzasadnionych przypadkach, dopuszcza się możliwość odstąpienia od przyjętej Polityki Bezpieczeństwa Informacji.

Aby postępować inaczej niż przewidują przyjęte reguły ochrony należy:

1. postępować zgodnie z wymogami obowiązującego prawa,
2. ustalić osobistą odpowiedzialność osoby, niestosującej się do przyjętych zasad bezpieczeństwa,
3. uzasadnić pisemnie powód odstąpienia od przyjętych zasad bezpieczeństwa.

Odstępując od przyjętych zasad należy zachować możliwie jak najwięcej z obowiązujących reguł.

Zabrania się stosowania precedensu w celu zmiany przyjętych reguł.

O odstąpieniu od przewidzianych zasad bezpieczeństwa decydować może jedynie ADO.

Nadrzędność przepisów prawa i umów nad regułami postępowania

Przepisy prawa i umowy z podmiotami mogą narzucać bardziej restrykcyjne wymagania dla ochrony informacji. W takim przypadku należy zastosować reguły spełniające te wymagania w uzupełnieniu opisanych w niniejszym dokumencie.

ROZDZIAŁ II
BEZPIECZEŃSTWO DANYCH OSOBOWYCH

Dane osobowe - to informacje, które art. 6 ustawy o ochronie danych osobowych definiuje, następująco:

„(...) za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań".

Dane osobowe to informacje na podstawie których można wskazać konkretną osobę niezależnie od tego w jakiej postaci te informacje się znajdują (papierowej, elektronicznej, ustnej).

Za organizację systemu ochrony danych osobowych odpowiada Administrator Danych Osobowych którym, w stosunku do wszystkich zatrudnionych w Urzędzie Gminy Marcinowice jest

WÓJT GMINY MARCINOWICE.

Ochrona danych osobowych w sądzie opiera się na:

1. Ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Z 2014r., poz. 1182 z późn.zm.).
2. Rozporządzeniu MSWiA z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. (Dz. U. Nr 100, poz. 1024).

Pełniąc funkcję Administratora Danych Osobowych - Wójt odpowiada za:

1. właściwy wybór stosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną,
2. zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,

3. prowadzenie dokumentacji opisującej sposób przetwarzania danych,
4. wyznaczenie administratora bezpieczeństwa informacji,
5. zapewnienie kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostają do zbioru wprowadzone oraz komu są przekazywane,
6. prowadzenie ewidencji osób upoważnionych do przetwarzania danych objętych wykazem.

Bezpieczeństwo w obszarze kadr

Urząd dba o zapewnienie kompetentnych pracowników do realizacji zadań.
Celem takiego postępowania jest ograniczenie ryzyka błędu ludzkiego, kradzieży, nadużycia lub niewłaściwego użytkowania aktywów.

Skuteczna realizacja postawionego celu możliwa jest dzięki przestrzeganiu ustanowionych procedur podczas naboru związanego z weryfikacją kandydatów do pracy. Transparentne i rygorystyczne zasady zatrudniania pracowników oraz zgodne z Kodeksem pracy procedury rozwiązywania umów o pracę.

Ludzie i ich ewentualne uchybienia w zakresie pełnionych obowiązków, są jednym z najistotniejszych źródeł zagrożeń dla organizacji.

W celu zapewnienia odpowiedniej ochrony tego obszaru, przyjmuje się następujące okresy w zakresie pracy z kadrą pracowniczą:

1.przed zatrudnieniem. 2.w trakcie zatrudnienia. 3.po zakończeniu zatrudnienia.

1.Przed zatrudnieniem

W zakresie procesu zatrudniania w Urzędzie stosuje się przyjęte zasady naboru kandydatów określone w Zarządzeniach Wójta wydawanych każdorazowo w czasie naboru.

Kandydat przed przystąpieniem do pracy, po podpisaniu umowy o pracę, ma obowiązek:

1. przejść stosowne procedury podczas rozpoczęcia zatrudnienia (uzyskać zaświadczenie wydane przez lekarza medycyny pracy, przejść szkolenie BHP, szkolenie z zakresu bezpieczeństwa informacji i systemów teleinformatycznych, uzyskać upoważnienie do przetwarzania danych osobowych),
2. zapoznać się z obowiązującymi regulacjami wewnętrznymi, a w szczególności z Polityką Bezpieczeństwa Informacji oraz jeśli posiada dostęp do systemów teleinformatycznych, Instrukcją zarządzania systemem informatycznym.

Fakt zapoznania się z dokumentami i ich zrozumieniem powinien zostać potwierdzony własnoręcznym podpisem pracownika na właściwym oświadczeniu.

WZÓR OŚWIADCZENIA,

OŚWIADCZENIE PRACOWNIKA

Ja niżej podpisana/ny oświadczam, iż:

1. znana jest mi treść ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014r., poz. 1182 z późn. zm.).) oraz zasady i dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji Urzędu Gminy Marcinowice.
2. znana jest mi odpowiedzialność karna za naruszenie przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
3. zapoznałam się z treścią Instrukcją Zarządzania Systemem Informatycznym Urzędu Gminy Marcinowice.

zobowiązuję się:

4. zachować w tajemnicy wszelkie informacje objęte ochroną w ramach SZBI Urzędu Gminy Marcinowice, w tym w szczególności, dane osobowe, z którymi zetknęłam się w trakcie wykonywania swoich obowiązków służbowych, zarówno w czasie trwania stosunku pracy, jak i po jego ustaniu,
5. chronić wszelkie informacje objęte ochroną w ramach SZBI Urzędu Gminy Marcinowice, w tym w szczególności, dane osobowe, przed dostępem do nich osób do tego nieupoważnionych,
6. zabezpieczać wszelkie informacje objęte ochroną w ramach SZBI Urzędu Gminy Marcinowice, w tym w szczególności, dane osobowe przed zniszczeniem i nielegalnym ujawnieniem i wykorzystaniem,
7. zachować w tajemnicy informacje o formach i sposobach zabezpieczenia informacji objętych ochroną w ramach SZBI Urzędu Gminy Marcinowice, w tym w szczególności, danych osobowych w Urzędzie Gminy Marcinowice.

....

(Administrator Bezpieczeństwa Informacji) (data, podpis pracownika)

Uwaga:

Niniejsze oświadczenie zostało sporządzone w trzech jednobrzmiących egzemplarzach (każdy na prawach oryginału), które otrzymują:

1 egz. - pracownik.
1 egz. - do akt osobowych pracownika.
1 egz. - Administrator Bezpieczeństwa Informacji.

2.W trakcie zatrudnienia

Zanim kierownik referatu dopuści nowo zatrudnionego pracownika do pracy w zbiorach danych, danej komórki organizacyjnej, obowiązany jest uzyskać dla niego upoważnienie do przetwarzania danych osobowych podpisane przez ADO.

Numer upoważnienia to: kolejny nr łamany przez symbol referatu łamany przez rok np. 001/OR/2015

Upoważnienie wykonywane jest w 3 egzemplarzach (każdy na mocy oryginału) - jeden otrzymuje pracownik, drugi składa się do akt osobowych, trzeci do dokumentacji prowadzonej przez ABI.

Najpóźniej w pierwszym dniu pracy nowo zatrudnionego pracownika kierownik referatu, w którym zatrudniony ma być pracownik, występuje z pisemnym wnioskiem o nadanie uprawnień do systemów teleinformatycznych.

Kierownik danego referatu zwraca się z wnioskiem do ASI o nadanie uprawnień do pracy w systemie.

Nadawanie, modyfikacja lub odbieranie uprawnień w systemach teleinformatycznych realizowane jest poprzez wniosek składany do ADO za pośrednictwem ASI.

Za dopuszczenie pracownika do pracy bez upoważnienia do przetwarzania danych odpowiada właściwy kierownik referatu.

WZÓR UPOWAŻNIENIA

Nr ewidencyjny: **001/OR/2015**

UPOWAŻNIENIE
wydane na podstawie art. 37 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2014r., poz. 1182 z późn. zm.)
DO PRZETWARZANIA DANYCH OSOBOWYCH

w celach związanych z wykonywaniem obowiązków służbowych oraz do obsługi systemu informatycznego i urządzeń wchodzących w jego skład.

Niniejsze upoważnienie obejmuje przetwarzanie danych osobowych, w formie tradycyjnej i elektronicznej, zgromadzonych we właściwych zbiorach danych osobowych prowadzonych przez Urząd Gminy Marcinowice, na podstawie określonych przepisów prawa, w tym w szczególności:

1. Ustawy o samorządzie gminnym.
2. Innych ustaw i rozporządzeń w zakresie przetwarzania danych osobowych.

Część I.

Pan (i): **Olga KOWALSKA**
zatrudniony(a) w: **Urzędzie Gminy Marcinowice**
na stanowisku: .....

Część II.

Proszę o nadanie Upoważnia w/w pracownikowi do przetwarzania danych osobowych zawartych w następujących zbiorach:
.....
.....
.....
<u>oraz do systemu informatycznego:</u>
.....

poprzez nadanie identyfikatora: .....

w zakresie: zbierania, utrwalania, przechowywania, modernizowania, usuwania, drukowania danych osobowych*,
*niepotrzebne skreślić

.....
(pieczęć i podpis Administratora Bezpieczeństwa Informacji)

Część III.

Upoważnienie wydaje się na czas zatrudnienia Pani Olgi Kowalskiej w Urzędzie Gminy Marcinowice.

.....
(pieczęć i podpis Administratora Danych Osobowych)

WYŻEJ NADANE UPOWAŻNIENIE COFAM Z DNIEM .....

.....

(pieczęć i podpis Administratora Danych Osobowych)

Na odwrocie upoważnienia pracownik składa oświadczenie o zapoznaniu się z treścią dokumentu.

WZÓR OŚWIADCZENIA

OŚWIADCZENIE PRACOWNIKA

Oświadczam, że zapoznałem /am się i zrozumiałem /am treść nadanego mi upoważnienia i zobowiązuję się do przetwarzania danych osobowych w oparciu o ustawę z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. Z 2014r., poz. 1182 z późn. zm.) w granicach określonych upoważnieniem.

.....
(data, podpis pracownika)

3.Po zakończeniu zatrudnienia

Po zakończeniu przez pracownika pracy właściwy kierownik referatu odpowiedzialny jest za skierowanie wniosku o cofnięcie upoważnienia. Wniosek kieruje się do ADO.

Po podpisaniu wniosku przez ADO, ABI nanosi odpowiednie adnotacje w rejestrze wydanych upoważnień.

Zakończenie pracy przez pracownika może być związane z ryzykiem kradzieży, przejęcia i wykorzystania informacji chronionej itp. W związku z wymienionymi zagrożeniami należy minimalizować ryzyko z nimi związane.

Odebranie uprawnień do informacji (w systemach i w zbiorach) powinno nastąpić jak najszybciej po podjęciu decyzji o zakończeniu zatrudnienia.

Kierownik kadr oraz kierownik danej komórki /w której zatrudniony jest pracownik/ jest zobowiązany niezwłocznie poinformować ASI o zamiarze rozwiązania bądź nieprzedłużeniu umowy z danym pracownikiem.

Kierownik Kadr odpowiada za pisemne wyznaczenie daty,

w której ASI ma obowiązek odebrać/zablokować uprawnienia do systemu. W tym samym dniu ADO odbiera (poprzez złożenie podpisu) uprawniania wynikające z uzyskanego wcześniej upoważnienia. Przedmiotowe upoważnienie Wójtowi przedstawia Kierownik Referatu Organizacyjnego i Spraw Obywatelskich.

Szkolenia pracowników

Każdy nowo zatrudniony pracownik (stażysta, praktykant) zobowiązany jest do odbycia szkolenia ze stosowania zasad bezpieczeństwa informacji.

Pracownicy będą okresowo szkoleni z zagadnień bezpieczeństwa informacji, ochrony danych osobowych i oceniani ze znajomości tematyki bezpieczeństwa informacji.

Nadto szkolenia dla pracowników z zakresu bezpieczeństwa informacji należy przeprowadzać każdorazowo po:

1. zmianie przepisów dotyczących ochrony danych osobowych,
2. wprowadzeniu istotnych zmian w niniejszej Polityce,
3. na wniosek ABI i ASI.

Szkolenie może zostać przeprowadzone w dowolnej formie, jednak każde powinno się kończyć testem sprawdzającym wiedzę uczestnika.

Szkolenia organizują lub w wyjątkowych sytuacjach przeprowadzają ABI i ASI.

ZBIORY DANYCH OSOBOWYCH/Zarządzanie aktywami

W Urzędzie Gminy Marcinowice kierownicy referatów sporządzają wykazy zbiorów danych, na których pracują i przekazują je ABI.

ABI na tej podstawie sporządza wykaz zbiorów danych, które zarządzeniem Wójta wprowadzone zostaną jako zbiory obowiązujące w jednostce.

Zbiorów obowiązujących nie można likwidować bez uprzedniej pisemnej zgody ADO.
W przypadku konieczność utworzenia nowego zbioru kierownik referatu kieruje uzasadniony wniosek do ADO za pośrednictwem ABI i po uzyskaniu pisemnej zgody ADO, nowy zbiór zostaje wprowadzony do wykazu w Urzędzie jako obowiązujący.

Wszystkie aktywa informacyjne (informacje zawarte w zbiorach danych) w Urzędzie Gminy Marcinowice mają swojego właściciela w postaci danego kierownika referatu.

POSTANOWIENIA KOŃCOWE

Wszystkim pracownikom zatrudnionym przed wejściem w życie zapisów niniejszej Polityki, po zapoznaniu się z jej treścią zostaną na wniosek ABI wydane upoważnienia do przetwarzania danych osobowych.

W związku z dynamicznie zmieniającymi się warunkami pracy przyjmuje się, że niniejsza Polityka w razie konieczności będzie podlegać aktualizacji.

Wszelkie wątpliwości związane z interpretacją zapisów w niniejszym dokumencie wyjaśnia ABI lub ASI.

WÓJT
Władysław Głębiowski
.....
Wójt Gminy Marcinowice
Administrator Danych Osobowych

Przepisy prawne i polskie normy

W Urzędzie Gminy Marcinowice, informacje podlegają ochronie zgodnie z następującymi wymogami prawa:

1. Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz. U. Z 2014r., poz. 1212, z późn. zm.),
2. Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. Nr 88, poz. 553, z późn. zm.),
3. Ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz. U. z 2014 r., poz. 1502, z późn. zm.),
4. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014r., poz. 1182 z późn. zm.),
5. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228, z późn. zm.,).
6. Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r. Nr 153, poz. 1503, z późn. zm.),
7. Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2014 r., poz. 1099, z późn. zm.),
8. Ustawa z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2013 r., poz. 330, z późn. zm.),
9. Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2006 r. Nr 90, poz. 631, z późn. zm.),
10. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. Z 2014r., poz. 782, z późn. zm.),
11. Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Z 2013r, poz. 262, z późn. zm.),
12. Ustawa z dnia 5 lipca 2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub podlegających na dostępie warunkowym (Dz. U. Nr 126, poz. 1068, z późn. zm.),
13. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Z 2014r., poz. 1114, z późn. zm.),
14. Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2015 r., poz. 128, z późn. zm.),
15. Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (Dz. U. Nr 128, poz. 1402, z późn. zm.),
16. Ustawa z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz. U. z 2012 r., poz. 654 z późn, zm.),
17. Ustawa z dnia 6 lipca 1982 r. o Księgach Wieczystych i hipotece (Dz. U. z 2013r., poz. 707),
18. Rozporządzenie Ministra Finansów z dnia 1 lutego 2010 r. w sprawie przeprowadzania i dokumentowania audytu wewnętrznego (Dz. U. Nr 21, poz. 108).
19. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).
20. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr 159, poz. 948).
21. Rozporządzenie Rady Ministrów z dnia z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2012 r., poz. 526 z późn. zm.).
22. Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 1 grudnia 1998 r. w sprawie bezpieczeństwa i higieny pracy na stanowiskach wyposażonych w monitory ekranowe (Dz. U. Nr 148, poz. 973, z późn. zm.).

Niniejszy dokument opracowano wykorzystując częściowo zapisy w n/w normach:

PN ISO/IEC 27001: 2007 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania.

PN ISO/IEC 27005 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji.

PN-ISO/IEC 17799: 2007 Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji.