ZARZĄDZENIE NR 306/17
Burmistrza Michałowa
z dnia 24 października 2017 roku
w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji (PBI)

Na podstawie art. 31 Ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (Dz. U. z 2017 r. poz. 1875 ze zm.), rozporządzenia MSWiA z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące przetwarzaniu danych osobowych (Dz. U. z 2004 roku, Nr 100, poz. 1024 ze zm.) oraz ustawy z dnia 29 sierpnia 1997roku o ochronie danych osobowych (Dz. U. z 2016 roku, poz. 922 ze zm.) zarządza się, co następuje:

1. Wprowadza się Politykę Bezpieczeństwa Informacji w zakresie przetwarzania danych osobowych w Urzędzie Miejskim w Michałowie stanowiącą załącznik nr 1 do niniejszego zarządzenia oraz Instrukcję Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych stanowiącą załącznik nr 1 do Polityki Bezpieczeństwa Informacji.
2. Polityka Bezpieczeństwa Informacji i Regulamin Zarządzania Systemami Informatycznymi będą stosowane na wszystkich stanowiskach, na których przetwarzane są dane osobowe.
3. Zobowiązuje się urzędników, pracowników etatowych, osób zatrudnionych na podstawie umowy - zlecenia oraz stażystów i praktykantów Urzędu Miejskiego w Michałowie do stosowania zasad określonych w Polityce Bezpieczeństwa Informacji.
4. Tracą moc:
   1) Zarządzenie nr 243/09 Burmistrza Michałowa z dnia 14 września 2009 r.
5. Zarządzenie wchodzi w życie z dniem 24 października 2017 roku.

Burmistrz Michałowa

Załącznik nr 1 do
Zarządzenia nr 306/17 Burmistrza Michałowa
z dnia 24 października 2017 roku

Polityka Bezpieczeństwa Informacji Urzędu Miejskiego w Michałowie

I. Cel przygotowania polityki bezpieczeństwa informacji

Polityka została stworzona w celu uczynienia zadość wymogom ustawowym dotyczącym ochrony danych osobowych. Konieczność stworzenia polityki bezpieczeństwa wynika wprost z art. 39a Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 roku, poz. 922 ze zm.) oraz § 3-4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 roku, Nr 100, poz. 1024 ze zm.).
Niniejszy dokument opisuje sposoby przetwarzania danych osobowych oraz całokształt środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych odpowiednią do zagrożeń możliwych do występowania w Urzędzie Miejskim w Michałowie. Zadaniem Polityki jest także określenie wymagań w zakresie odnotowywania udostępniania danych osobowych. Polityka określa zasady dotyczące bezpieczeństwa w zakresie danych osobowych przetwarzanych w zbiorach danych.

Definicje, zawarte w Polityce Bezpieczeństwa Informacji oznaczają:

Ustawa - ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 roku, poz. 922 ze zm.)
Administrator Danych Osobowych (ADO) – należy przez to rozumieć Burmistrza Michałowa;
Administrator Bezpieczeństwa Informacji(ABI) – jest to osoba, nadzorująca przestrzeganie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych w sposób odpowiedni do zagrożeń oraz kategorii danych objętych ochroną. Osoba ta może być powołana przez ADO.
Administrator Systemu Informatycznego (ASI) – jest to zewnętrzna firma informatyczna lub osoba zatrudniona u ADO, odpowiedzialna za prawidłowe funkcjonowanie systemów informatycznych, sprzętu, oprogramowania i jego konserwację w Urzędzie Miejskim w

Michałowie.
Osoba upoważniona (użytkownik) – osoba posiadająca upoważnienie nadane przez Administratora Danych Osobowych lub osoba wyznaczona przez niego i uprawniona do przetwarzania danych osobowych, w zakresie wskazanym w upoważnieniu.
System informatyczny, zwany dalej systemem, - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
Zbiór danych – jest to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
Nośniki danych osobowych – dyski twarde, płyty CD lub DVD, pamięci przenośne (pendrive) i inne urządzenia/ materiały służące do przechowywania plików z danymi;
Przetwarzanie danych - każda czynność dokonywana na informacjach mających charakter osobowy;
Zabezpieczenie danych w systemie (zabezpieczeniem) – wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
Wewnętrzna sieć teleinformatyczna – sieć ADO, łącząca co najmniej dwa indywidualne stanowiska komputerowe, umożliwiająca użytkownikom określony dostęp do danych.
Urząd - należy przez to rozumieć Urząd Miejski w Michałowie;
PBI – Polityka Bezpieczeństwa Informacji.

2. Postanowienia ogólne

ADO, należycie zdający sobie sprawę z wagi problemu ochrony danych osobowych, w tym w szczególności osób fizycznych powierzających urzędowi swoje dane osobowe, wyraża pełne zaangażowanie dla zapewnienia bezpieczeństwa przetwarzanych danych osobowych oraz wsparcie dla przedsięwzięć technicznych i organizacyjnych związanych z ochroną danych osobowych i w związku z powyższym w celu właściwej ochrony tych danych deklaruje zamiar:

1. Podejmowania działań skierowanych na stałe podnoszenie bezpieczeństwa przetwarzania danych osobowych, podwyższenia kwalifikacji osób przetwarzających te dane oraz ich świadomości co do występujących zagrożeń.
2. Podnoszenia świadomości wartości danych osobowych występujących w Urzędzie gdyż w głównym stopniu dane te są przetwarzane w sytuacji, gdy obowiązujące przepisy prawa obligują podmiot do udostępnienia określonych informacji na swój temat.

3. Doskonalenia i rozwijania nowoczesnych technik zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzaniem w sytuacji przetwarzania tych danych w systemach informatycznych i sieciach telekomunikacyjnych.

W trakcie realizacji Polityki Bezpieczeństwa Informacji w zakresie ochrony danych osobowych Urząd dokłada wszelkich starań w celu ochrony interesów osób, których dane dotyczą, zapewniając, żeby:

a) przetwarzanie danych odbywało się zgodnie z przepisami prawa;
b) zbieranie danych dokonywane było dla osiągniecia konkretnych, dozwolonych przez prawo celów, przy równoczesnym zakazie dalszego przetwarzania pozyskanych danych niezgodnemu z tymi celami; jednakże dalsze przetwarzanie jest dozwolone, o ile nie narusza ono praw i wolności osób, do których dane się odnoszą oraz dokonywane jest dla celów prowadzonych badań naukowych, historycznych, dydaktycznych bądź też statystycznych;
c) dane były merytorycznie poprawne oraz odpowiednie do celów, dla osiągnięcia których dokonuje się ich przetwarzania;
d) dane były przechowywane w formie pozwalającej na dokonanie identyfikacji osób, do których się odnoszą przez okres nie dłuższy niż jest to uzasadnione dla osiągnięcia celów przetwarzania.

W celu zabezpieczenia danych osobowych przed nieuprawnionym udostępnieniem ADO wprowadza określone zasady przetwarzania danych. Zasady te określone zostaną w Polityce Bezpieczeństwa Informacji oraz załącznik nr 1 do PBI – Regulamin zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Każda osoba, upoważniona do przetwarzania w Urzędzie danych osobowych powinna zwracać szczególną uwagę żeby jej postępowanie było zgodne z przyjętymi zasadami i minimalizować błędy wynikające z tzw. "czynnika ludzkiego".

Ponadto wprowadzone zostały w Urzędzie stosowne środki organizacyjne i techniczne zapewniające właściwą ochronę danych osobowych. PBI nakazuje ich bezwzględne stosowanie przez osoby dopuszczone do przetwarzania danych osobowych. Polityka Bezpieczeństwa Informacji podlega aktualizacji w celu zapewnienia coraz wyższego poziomu ochrony danych. Przegląd i weryfikacja obowiązującej PBI odbywa się raz w roku.

III. Charakterystyka instytucji (Urzędu)

Urząd Miejski w Michałowie przyjmuje i obsługuje interesantów w siedzibie Urzędu, dokonuje wymiaru oraz poboru należnych kwot podatku rolnego, leśnego i od nieruchomości, jak również umożliwia zainteresowanym dostęp do informacji odnoszących się do szeroko rozumianej działalności Urzędu i załatwianych w nim spraw. Ponadto na podstawie odrębnych przepisów Urząd prowadzi ewidencję mieszkańców, wyborców, jak również ewidencjonuje i wydaje akty stanu cywilnego itd.
Obszar przetwarzania danych osobowych w ujęciu przestrzennym obejmuje siedzibę Urzędu.
Wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe w Urzędzie zawiera załącznik nr 2 do PBI.

4. Cele bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych

Jako bezpieczeństwo funkcjonowania systemów informatycznych przeznaczonych do przetwarzania danych osobowych rozumie się zdolność urzędu do zapewnienia dostatecznego stopnia ochrony danym osobowym, których przetwarzania dokonuje się w wymienionych systemach.
Zwraca się uwagę na konieczność zabezpieczenia danych osobowych przed potencjalnymi zagrożeniami, jakie mogą pojawić się wskutek wystąpienia luk, błędów oraz innych wad technicznych, a w dalszym ciągu doprowadzić do zaistnienia sytuacji nieuprawnionego wyjawienia bądź udostępnienia danych osobowych podmiotom nieupoważnionym oraz do niepowołanej modyfikacji lub zniszczenia danych.
Generalnym celem wdrażanej w Urzędzie polityki bezpieczeństwa systemów informatycznych przeznaczonych do przetwarzania danych osobowych jest szczegółowe określenie poziomu bezpieczeństwa danych osobowych wprowadzanych do systemów informatycznych, które wykorzystuje się na obszarze Urzędu oraz ustanowienie wymogów bezpieczeństwa jeśli chodzi o stosowane środki techniczno-organizacyjne. Wymogi te powinny być adekwatne do możliwych zagrożeń oraz charakteru danych podlegających ochronie.

1. Wykaz zbiorów

1. Dane osobowe gromadzone są w zbiorach.
2. Wykaz zbiorów danych osobowych stanowi załącznik nr 3 do PBI.

VI. Środki organizacyjne ochrony zbiorów danych osobowych

Procesy przetwarzania danych osobowych powinny posiadać właściwe zabezpieczenia. Niniejszym dokumentem wprowadza się następujące środki organizacyjne:

1. Przetwarzanie danych osobowych w Urzędzie może być dokonywane jedynie w związku z wykonywaniem obowiązków służbowych. Zakres posiadanych uprawnień oraz zakres w jakim dane osobowe będą udostępniane wynika z zakresu tychże obowiązków.
2. Dopuszczenie do przetwarzania danych osobowych możliwe jest wyłącznie w odniesieniu do osób, którym przyznano stosowne upoważnienie. Wzór upoważnienia zawiera załącznik nr 4 do PBI.
3. Każdy pracownik (urzędnik, osoba zatrudniona na podstawie umowy cywilnoprawnej, stażysta, praktykant), który w związku z zakresem swoich zadań służbowych jest lub może być dopuszczony do wglądu bądź do przetwarzania danych osobowych zobowiązany jest do podpisania oświadczenia o zachowaniu poufności i zapoznaniu się z przepisami. Wzór oświadczenia zawiera załącznik nr 5 do niniejszej Polityki.
4. Ewidencję osób którym przyznano dostęp do zbiorów danych osobowych zawiera załącznik nr 6 do PBI.
5. Dla osób, zajmujących się w ramach swoich obowiązków służbowych przetwarzaniem danych osobowych, co najmniej raz w roku ADO organizuje szkolenia odnośnie tematyki ochrony danych osobowych.
6. Każda nowo zatrudniona osoba (pracownik, urzędnik, osoba zatrudniona na podstawie umowy cywilnoprawnej, stażysta, praktykant) przed przystąpieniem do przetwarzania danych zapoznaje się z Polityką Bezpieczeństwa Informacji.
7. Każda osoba, której przyznano upoważnienie do przetwarzania danych osobowych poświadcza w sposób pisemny zapoznanie się z niniejszą dokumentacją oraz potwierdza, że rozumie i przyjmuje do wiadomości wszystkie zasady bezpieczeństwa. Wzór poświadczenia zawiera załącznik nr 7 do PBI.
8. Pomieszczenia, w których dokonuje się przetwarzania danych podczas nieobecności osób wymienionych w pkt. 3 zamykane są na klucz. Klucze przechowuje się w zamkniętej szafce.
9. Monitory komputerów, które wykorzystuje się do przetwarzania danych osobowych ustawiane są w sposób uniemożliwiający uzyskanie wglądu w te dane przez osoby postronne.
10. Przed opuszczeniem pomieszczenia, w którym dokonywane jest przetwarzanie danych osobowych należy usunąć z biurka wszelkie dokumenty, pieczątki oraz nośniki informacji, a następnie umieścić je w odpowiednich zamykanych szafach bądź biurkach, jak również zamknąć okna.

11. Na czas nieobecności osób posiadających stosowne upoważnienie, pomieszczenie, w którym dokonuje się przetwarzania danych osobowych zabezpieczane jest przed dostępem osób nieuprawnionych. Zabronione jest korzystanie z dokumentacji służbowej, nośników pamięci itp. oraz komputerów służbowych (zarówno stacjonarnych, jak i przenośnych) poza pomieszczeniami przeznaczonymi do przetwarzania danych osobowych.

7. Odpowiedzialność za realizację Polityki Bezpieczeństwa Informacji

Wszyscy pracownicy, urzędnicy, osoby zatrudnione na podstawie umowy - zlecenia oraz stażyści i praktykanci ponoszą odpowiedzialność za ochronę danych osobowych w Urzędzie stosownie do nałożonych na nich obowiązków oraz posiadanych kompetencji.

ADO ponosi odpowiedzialność za stworzenie odpowiednich warunków prawnych, organizacyjnych i finansowych do wdrożenia i ciągłego doskonalenia systemu ochrony danych osobowych przetwarzanych manualnie i w systemach informatycznych, a w szczególności odpowiada za:

1. Stworzenie w Urzędzie odpowiedniej struktury organizacyjnej ze wskazaniem osób i/lub firm zewnętrznych odpowiedzialnych za zarządzanie bezpieczeństwem informacji.
2. Zgłoszenie do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbiorów danych osobowych przetwarzanych w Urzędzie zgodnie z art. 41 Ustawy o ochronie danych osobowych.
3. Wprowadzenia do użytku w Urzędzie:
    a) Polityki Bezpieczeństwa Informacji ;
    b) Instrukcji zarządzania system informatycznym służącym do przetwarzania danych osobowych.

Zatwierdził:

.....

Administrator Danych Osobowych

REGULAMIN ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

I. Postanowienia ogólne

1. Regulamin zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwany dalej "Regulaminem", określa procedury odnoszące się do zasad bezpieczeństwa przetwarzania danych osobowych oraz reguły postępowania ADO, osób i/lub firm zewnętrznych przez niego wyznaczonych oraz użytkowników przetwarzających dane osobowe w Urzędzie Miejskim w Michałowie.
2. W systemach informatycznych przeznaczonych do przetwarzania danych osobowych stosowane są środki bezpieczeństwa na poziomie wysokim.

2. Rejestracja w systemie informatycznym

1. Wyłącznie osoby posiadające wydane przez Administratora Danych Osobowych upoważnienie do przetwarzania danych osobowych mogą zostać dopuszczone do obsługi systemu informatycznego oraz innych urządzeń wchodzących w jego skład, które służą do przetwarzania danych osobowych.
2. Administrator Systemów Informatycznych zakłada identyfikator sieciowy/konto w systemach informatycznych, a następnie podaje login i hasło tymczasowe użytkownikowi. Podczas swojego pierwszego logowania użytkownik zobowiązany jest do zmiany hasła tymczasowego na własne, zgodnie z zasadami nadawania haseł opisanymi w Rozdziale III niniejszego Regulaminu.
3. Dokument przyznania bądź cofnięcia uprawnień musi być ponownie wypełniony w przypadku zmiany zakresu uprawnień.
4. Karty uprawnień przechowuje ADO.
5. ASI jest odpowiedzialny za przydzielenie i wygenerowanie identyfikatora i hasła użytkownikowi, który pierwszy raz korzysta z systemu informatycznego.
6. Identyfikator użytkownika nie może być zmieniany ani modyfikowany, a po wyrejestrowaniu użytkownika nie może być już więcej przydzielany innym osobom.

3. Metody i środki uwierzytelniania użytkownika oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Użytkownik może uzyskać dostęp do danych osobowych przetwarzanych w systemie informatycznym jedynie po podaniu identyfikatora i hasła.
2. Identyfikator jest przypisany użytkownikowi w sposób jednoznaczny i niebudzący wątpliwości. Użytkownik odpowiada za wszelkie czynności wykonane przy użyciu przypisanego mu identyfikatora.
3. Identyfikator składa się z przynajmniej 4 znaków, które nie mogą być rozdzielone spacjami ani znakami interpunkcyjnymi. Identyfikator tworzy się przy użyciu małych liter z wyłączeniem polskich znaków.
4. Hasło składa się z przynajmniej 8 znaków. Hasło powinno zawierać małe i wielkie litery oraz cyfry bądź znaki specjalne.
5. Jeżeli system informatyczny nie jest wyposażony w mechanizm wymuszający zmianę hasła po upływie 30 dni od dnia ostatniej zmiany, użytkownik zobowiązany jest do dokonywania cyklicznych zmian hasła. Zmiany te powinny odbywać się w odstępie czasowym 30 dni. Hasło nie może być zapisane w miejscu dostępnym dla osób nieuprawnionych i powinno być zachowane w tajemnicy również po upływie jego ważności.
6. Użytkownik nie może przekazywać osobom nieuprawnionym swojego identyfikatora oraz hasła. Po dokonanym uwierzytelnieniu w systemie, użytkownik nie może udostępniać swojego stanowiska pracy osobom nieuprawnionym.
7. W przypadku istnienia podejrzenia, że dostęp do hasła mogła uzyskać nieuprawniona, użytkownik zmienia swoje hasło oraz powiadamia o tej sytuacji ASI oraz ABI.

4. Rozpoczęcie, zawieszenie oraz zakończenie pracy przez użytkownika

1. Rozpoczynając pracę na komputerze, użytkownik loguje się do systemu informatycznego.
2. Jedynie po wcześniejszym dokonaniu uwierzytelnienia użytkownika możliwy jest dostęp do danych osobowych.
3. Maksymalna ilość prób wprowadzenia hasła przy logowaniu do systemu informatycznego wynosi 3. W przypadku przekroczenia tej liczby system blokuje dostęp do zbioru danych na poziomie danego użytkownika. Odblokowania dostępu może dokonać ASI w porozumieniu z ABI.
4. Jeżeli użytkownik nie wykazuje żadnej aktywności przez czas dłuższy niż 10 minut powinien automatycznie włączać się wygaszacz ekranu.
5. Monitory stanowisk komputerowych, na których dokonuje się przetwarzania

danych osobowych, i które umiejscowione są w pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnienia do przetwarzania danych osobowych, należy ustawić w taki sposób, aby uniemożliwić tym osobom wgląd w dane osobowe bądź stosować blokowanie ekranu uniemożliwiające odczyt danych.

6. Obecność osób nieuprawnionych w pomieszczeniach, w którym przetwarzane są dane osobowe, dopuszczalna jest tylko w obecności osoby upoważnionej do ich przetwarzania.
7. Pomieszczenia, w których przetwarzane są dane osobowe, muszą być zamykane na czas nieobecności osób upoważnionych.
8. Przed opuszczeniem stanowiska użytkownik jest zobowiązany do:
   a) wylogowania się z systemu informatycznego;
   b) uruchomienia wygaszacza ekranu blokowanego hasłem.
9. Ukończywszy pracę użytkownik zobowiązany jest do:
   a) wylogowania się z systemu informatycznego, a następnie wyłączenia sprzętu komputerowego;
   b) zabezpieczenia stanowiska pracy w taki sposób, aby okna w pomieszczeniu były zamknięte, wszystkie dokumenty, pieczątki i nośniki informacji zostały usunięte z blatu biurka oraz umieszczone w odpowiednich zamykanych szafach lub biurkach.

5. Kopie zapasowe zbiorów danych oraz programy i narzędzia służące do ich przetwarzania

1. Dane osobowe, których przetwarzania dokonuje się w systemie informatycznym zabezpieczone są poprzez tworzenie kopii zapasowych.
2. ASI lub inna osoba przez niego wyznaczona odpowiada za tworzenie kopii zapasowych zbiorów danych osobowych.
3. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich użyteczności i możliwości odtworzenia w sytuacji usterki bądź awarii systemu informatycznego. Przeprowadzanie tej procedury należy do obowiązków ASI.
4. Kopie zapasowe wykonuje się wedle następującego harmonogramu:
   a) kopia zapasowa aplikacji przeznaczonej do przetwarzania danych osobowych – pełna kopia wykonywana jest co miesiąc;
   b) kopia zapasowa danych osobowych przetwarzanych przez aplikację – pełną kopia wykonywana jest raz w tygodniu, a w sytuacji wprowadzenia istotnych zmian danych osobowych, może być również wykonywana częściej;
   c) kopia zapasowa danych konfiguracyjnych systemu informatycznego przetwarzającego dane osobowe, w tym uprawnień użytkowników systemu – pełna kopia wykonywana jest raz do roku.

5. Kopie zapasowe przechowuje się w sejfie, która obowiązkowo musi być zamykany na klucz.

6. Sposoby, miejsce i okres przechowywania nośników danych zawierających dane osobowe oraz kopii zapasowych

1. Użytkownicy nie mogą wynosić z Urzędu nośników danych z zapisanymi danymi osobowymi, bez uprzedniej zgody ADO.
2. Okresowe kopie zapasowe wykonuje się na pamięciach przenośnych, płytach CD, DVD, taśmach bądź też innych nośnikach danych. Kopie przechowywane są w innych pomieszczeniach aniżeli te, w których przechowywane są na bieżąco wykorzystywane zbiory danych. Kopie zapasowe przechowuje się w sposób, który uniemożliwia nieuprawnione przejęcie, uszkodzenie, modyfikację lub zniszczenie.
3. Wyłącznie ADO oraz ASI mają dostęp do nośników z kopiami zapasowymi danych osobowych.
4. Usuwanie danych z systemu powinno się odbywać przy pomocy oprogramowania służącego do bezpiecznego usuwania danych z nośnika danych.
5. Użytkownik odpowiada za zniszczenie kopii zapasowych indywidualnie sporządzanych przez siebie danych.
6. Nie później niż po upływie 5 dni po ich wykorzystaniu, dane osobowe w postaci elektronicznej należy usuwać z nośnika danych w sposób uniemożliwiający ich ponowne odtworzenie, chyba że z odrębnych przepisów wynika obowiązek ich przechowywania.
7. W przypadku wycofania z eksploatacji sprzętu komputerowego, na którym przetwarzane były dane osobowe oraz po przeniesieniu danych osobowych do zbiorów danych w systemie informatycznym z nośników, których ponowne wykorzystanie nie jest możliwe, nośniki danych podlegają komisyjnemu zniszczeniu. Komisja sporządza protokół z przeprowadzonych czynności.
8. Przez zniszczenie nośników danych należy rozumieć ich trwałe i nieodwracalne zniszczenie fizyczne do stanu, w którym ich rekonstrukcja oraz odzyskanie danych jest niemożliwe.

7. Zabezpieczenie systemu informatycznego przed działaniem oprogramowania służącego uzyskaniu nieuprawnionego dostępu do systemu informatycznego.

1. ASI odpowiada za ochronę antywirusową systemu informatycznego.
2. W każdym komputerze z dostępem do danych osobowych należy zainstalować

system antywirusowy. Wysyłanie aktualizacji bazy sygnatur wirusów i ustawienie poziomu bezpieczeństwa podlega centralnemu zarządzaniu.

3. Programy antywirusowe muszą być aktywne przez cały czas pracy każdego komputera w systemie informatycznym.
4. Wszystkie pliki otrzymywane z zewnątrz, a także wysyłane na zewnątrz, podlegają automatycznemu sprawdzeniu przez system antywirusowy pod kątem występowania wirusów, przy zastosowaniu najnowszej dostępnej wersji programu antywirusowego.
5. W przypadku ujawnienia się wirusa, użytkownik zobowiązany jest do zaniechania wykonywania jakichkolwiek czynności i niezwłocznego powiadomienia ASI.
6. Otwieranie poczty elektronicznej pochodzącej od nieznanych nadawców jest surowo zabronione.
7. Zabronione jest wyłączanie, blokowanie i odinstalowywanie programów zabezpieczających komputer przed oprogramowaniem złośliwym oraz nieautoryzowanym dostępem (skaner antywirusowy, firewall).
8. Do obowiązków ASI należy jest aktywowanie i prawidłowe konfigurowanie oprogramowania monitorującego wymianę danych na styku:
   a) sieci lokalnej oraz rozległej;
   b) stanowiska komputerowego użytkownika systemu, a także pozostałych urządzeń, które wchodzą w skład sieci lokalnej.

8. Udostępnianie danych oraz metody odnotowywania informacji o udostępnianiu danych.

1. Dane osobowe przetwarzane w jednostce można udostępniać osobom lub podmiotom uprawnionym do ich otrzymania, na mocy ustawy o ochronie danych osobowych oraz innych przepisów powszechnie obowiązujących.
2. Udostępnianie danych osobowych odbywa się w oparciu o pisemny, umotywowany wniosek, chyba że przepisy odrębne stanowią inaczej.
3. Dane, które zostały udostępnione jednostce przez inny podmiot mogą być wykorzystywane wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
4. Ewidencja udostępnionych danych prowadzona jest przez ADO. Ewidencja ta zawiera:
   a) numer ewidencyjny wydruku;
   b) adresata udostępnionych danych;
   b) zakres udostępnionych danych;
   d) datę udostępnienia.
5. Odnotowanie informacji następuje niezwłocznie po udostępnieniu danych.

9. Przegląd i konserwacja systemu oraz nośników danych służących do przetwarzania danych.

1. Wszelkie prace z zakresu naprawy i konserwacji systemu informatycznego przetwarzającego dane osobowe mogą być dokonywane przez firmy zewnętrzne. Nadzór nad wykonywaniem tych prac prowadzi ASI.
2. Do ASI należy sprawdzanie możliwości odtworzenia danych z kopii zapasowej. ASI ustala w porozumieniu z ADO częstotliwość wykonywania procedury odtwarzania danych.
3. Aktualizację oprogramowania przeprowadza się zgodnie z zaleceniami producentów oraz opinią rynkową, odnośnie bezpieczeństwa i stabilności nowych wersji.
4. ASI odpowiada za terminowość przeprowadzania przeglądów i konserwacji oraz ich prawidłowy przebieg.
5. Ewentualne nieprawidłowości w działaniu systemu informatycznego oraz oprogramowania są bezzwłocznie naprawiane przez ASI bądź firmę zewnętrzną pod nadzorem ASI, a ich przyczyny badane i analizowane.
6. Zmiana konfiguracji sprzętu komputerowego na którym przechowywane są dane osobowe lub zmiana jego lokalizacji może być dokonana tylko za wiedzą i wyraźną zgodą ADO.

10. Naruszenie ochrony danych osobowych.

1. Każdy użytkownik, który stwierdza bądź podejrzewa naruszenie ochrony danych osobowych w systemie informatycznym, niezwłocznie powiadamia o tym ASI.
2. Do momentu przybycia ASI na miejsce naruszenia lub ujawnienia naruszenia ochrony danych osobowych należy:
   a) bezzwłocznie podjąć wszelkie możliwe działania niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, a następnie w miarę możliwości dokonać ustalenia przyczyn lub sprawców naruszenia;
   b) wstrzymać bieżącą pracę na komputerze w celu zabezpieczenia miejsca zdarzenia, jeśli jest to stosowne w zaistniałych okolicznościach;
   c) w miarę możliwości zaniechać dalszych przedsięwzięć, które wiążą się z powstałym naruszeniem i mogą utrudnić jego udokumentowanie oraz analizę;
   d) dokonać wstępnej dokumentacji zaistniałego naruszenia;
   e) bez uzasadnionej potrzeby nie opuszczać miejsca zdarzenia do czasu zjawienia się ASI;
3. Po przybyciu na miejsce naruszenia lub ujawnienia naruszenia ochrony danych osobowych ASI:
   a) analizuje zaistniałą sytuację i wybiera metodę dalszego postępowania;

b) może zażądać wyjaśnień dotyczących zaistniałego zdarzenia od osoby powiadamiającej, a także od każdej innej osoby, która może posiadać informacje dotyczące zaistniałego naruszenia;

c) zabezpiecza system informatyczny przed rozprzestrzenianiem się skutków naruszenia;

d) podejmuje kroki w celu powstrzymania lub ograniczenia dostępu osoby nieuprawnionej, minimalizacji szkód i zabezpieczenia przed usunięciem śladów naruszenia;

e) rozważa potrzebę zawiadomienia o powstałym naruszeniu ADO.

4. Wyczerpawszy niezbędne środki doraźne, ASI zasięga niezbędnych opinii i wskazuje działania mające na celu usunięcie naruszenia i jego skutków oraz opiniuje kwestię ewentualnego odtworzenia danych z kopii zapasowej i terminu wznowienia przetwarzania danych.
5. ADO dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, który zawiera w szczególności:

   a) wskazanie osoby zawiadamiającej o naruszeniu oraz innych osób, które złożyły wyjaśnienia w związku ze zdarzeniem;

   b) określenie miejsca i czasu naruszenia oraz powiadomienia o naruszeniu;

   c) określenie rodzaju naruszenia oraz okoliczności w jakich do niego doszło;

   d) wskazanie wziętych pod uwagę przesłanek wyboru metody postępowania i opis powziętego działania;

   e) wstępną ocenę przyczyn nastąpienia naruszenia;

   f) ocenę przeprowadzonego postępowania wyjaśniającego i działań podjętych w celu usunięcia naruszenia i jego skutków.
6. Po przywróceniu poprawnego funkcjonowania systemu informatycznego ASI dokonuje szczegółowej analizy celem określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia oraz podejmuje kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

Zatwierdził:
Burmistrz Michałowa

Załącznik nr 2 Polityki Bezpieczeństwa Informacji

Wykaz pomieszczeń w których odbywa się przetwarzanie danych osobowych:

Obszar w którym są przetwarzane dane osobowe ogranicza się do budynku zlokalizowanego w Michałowie przy ulicy Białostockiej 11, wymienione w poniższej tabeli oraz wszystkie w archiwum zakładowym.

L.P.	Zbiór danych osobowych	Sposób przetwarzania	Pomieszczenie nr

Załącznik nr 3 Polityki Bezpieczeństwa Informacji

Wykaz zbiorów danych oraz systemów informatycznych stosowanych do przetwarzania tych zbiorów w Urzędzie Miejskim w Michałowie wraz z opisem struktury:

L.p.	Nazwa zbioru	Rodzaj rejestru	Zawartość poszczególnych pól informacyjnych i powiązania między nimi	Podlega zgłoszeniu do GIODO Tak/Nie

Załącznik nr 4 Polityki Bezpieczeństwa Informacji

UPOWAŻNIENIE NR .... / ....
do przetwarzania danych osobowych

Działając na podstawie uprawnień nadanych mi w Urzędzie Miejskim w Michałowie – w sprawie ochrony danych osobowych upoważniam
Panią / Pana ..... do przetwarzania danych osobowych w systemach informatycznych / nieinformatycznych funkcjonujących w Urzędzie Miejskim w Michałowie służących do przetwarzania danych osobowych.

Data nadania .....
Data ustania .....

Wyżej wymieniona osoba została zapoznana z obecnie obowiązującymi przepisami dotyczącymi ochrony danych osobowych i dopuszczona jest do ich przetwarzania jedynie w zakresie określonym w obowiązkach służbowych i zgodnie z Ustawą z dnia 29.08.1997 roku o ochronie danych osobowych i wydanych do niej przepisach wykonawczych.

Wymieniona osoba została wpisana do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w Urzędzie Miejskim w Michałowie.

.....
Podpis osoby wystawiającej upoważnienie

.....
Data i czytelny podpis osoby upoważnionej

Załącznik nr 5 Polityki Bezpieczeństwa Informacji

OŚWIADCZENIE NR .... / ....
o zachowaniu poufności i zapoznaniu się z przepisami

Ja niżej podpisany(a) ..... oświadczam, iż zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia do których mam lub będę miał(a) dostęp w związku z wykonywaniem:
a) zadań i obowiązków służbowych wynikających z umowy o pracę,
b) zadań wynikających z umowy cywilno-prawnej,
c) zadań wynikających z umowy – w związku z praktyką studencką,
d) porozumieniem dotyczącym odbycia stażu.

zarówno w trakcie wykonywania umowy, jak i po jej ustaniu:

Zobowiązuję się przestrzegać polityki, instrukcji i procedur obowiązujących w Urzędzie Miejskim w Michałowie. W szczególności oświadczam, że bez upoważnienia nie będę wykorzystywał(a) danych osobowych ze zbiorów znajdujących się w Urzędzie Miejskim w Michałowie. Oświadczam, że zostałem(am) poinformowany(a) o obowiązujących w Urzędzie Miejskim w Michałowie zasadach dotyczących przetwarzania danych osobowych określonych w "Polityce Bezpieczeństwa Informacji".

Oświadczam, że zostałem(am) zapoznany(a) z przepisami ustawy o ochronie danych osobowych (Dz. U. z 2016 roku, poz. 922 ze zm.) oraz 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 ze zm.).

Oświadczam, że zostałem(am) poinformowany o grożącej, stosownie do przepisów rozdziału VIII Ustawy o ochronie danych osobowych, odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, że naruszenie zasad ochrony danych osobowych obowiązujących w Urzędzie Miejskim w Michałowie, może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

....
Miejscowość i data *Czytelny podpis osoby składającej upoważnienie*

Załącznik nr 6 Polityki Bezpieczeństwa Informacji

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Imię i nazwisko osoby upoważnionej	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważ.	Identyfikator w systemie informatycznym
1					
2					
3					
4					
5					

Załącznik nr 7 Polityki Bezpieczeństwa Informacji

Michałowo, dnia .....

OŚWIADCZENIE PRACOWNIKA O ZAPOZNANIU SIĘ Z TREŚCIĄ POLITYKI BEZPIECZEŃSTWA INFORMACJI

Niżej podpisany/a ....., zam..... ....., zatrudniony/a w Urzędzie Miejskim w Michałowie na stanowisku ..... potwierdzam, że zostałem/am zapoznany/a z Polityką Bezpieczeństwa Informacji Urzędu Miejskiego w Michałowie, co potwierdzam własnoręcznym podpisem.

.....
(Czytelny podpis pracownika)