PR

B U R M I S T R Z
Drawska Pomorskiego
ul.Gen.Wł.Sikorskiego 41
78-500 Drawsko Pomorskie
tel. 094-3633485; fax. 094-3633113

ZARZĄDZENIE NR 46/2014
BURMISTRZA DRAWSKA POMORSKIEGO
z dnia 10 marca 2014 r.

zmieniające Zarządzenie Nr 78/2011 Burmistrza Drawska Pomorskiego z dnia 25 maja 2011r. w sprawie wyznaczenia administratora bezpieczeństwa informacji oraz wprowadzenia polityki bezpieczeństwa przetwarzania danych osobowych i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Drawsku Pomorskim

Na podstawie art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101 poz. 926, Nr 153, poz. 1271, z 2004 r. Nr 25, poz. 219, Nr 33, poz. 285, z 2006 r. Nr 104, poz. 708 i poz. 711, z 2007 r. Nr 165, poz. 1170, Nr 176, poz. 1238, z 2010 r. Nr 41, poz. 233, Nr 182, poz. 1228, Nr 229, poz. 1497, z 2011r. Nr 230, poz. 1371) oraz §3 ust. 1 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), zarządza się, co następuje:

§1. W Zarządzeniu Nr 78/2011 Burmistrza Drawska Pomorskiego z dnia 25 maja 2011r. w sprawie wyznaczenia administratora bezpieczeństwa informacji oraz wprowadzenia polityki bezpieczeństwa przetwarzania danych osobowych i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Drawsku Pomorskim zmienia się treść załączników nr 2 i 3, które otrzymują brzmienie zgodne z załącznikami nr 1 i 2 do niniejszego Zarządzenia.

§2. Zarządzenie wchodzi w życie z dniem podjęcia.

z up. BURMISTRZA
mgr inż. Marek Tobiszewski
Z-ca Burmistrza

Pod względem formalno-prawnym
bez zastrzeżeń
Piotr Matlon
RADCA PRAWNY

Załącznik Nr 2 do zarządzenia Nr 78/2011
Burmistrza Drawska Pomorskiego
z dnia 25 maja 2011r.

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE MIEJSKIM W DRAWSKU POMORSKIM

Podstawa prawna:

1) Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. jedn. Dz. U. z 2002 r. Nr 101 poz. 926, ze zm.).
2) § 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).

Spis treści

1. Deklaracja kierownictwa urzędu 3
2. Definicje podstawowe 3
3. Zagadnienia organizacyjne. 6
4. Wykaz budynków i pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe. 7
5. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych. 7
6. Opisy struktury zbiorów danych osobowych wskazujące zawartość poszczególnych pól informacyjnych i powiązania między nimi. 7
7. Sposób przepływu danych pomiędzy poszczególnymi systemami. 7
8. Środki techniczne i organizacyjne, niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych 8
9. Lokalizacja sprzętu komputerowego 11
10. Instrukcja alarmowa w przypadku naruszenia ochrony danych osobowych 11
11. Plan ciągłości działania 13
12. Konsekwencje naruszenia Polityki Bezpieczeństwa Danych 14
13. Lista załączników 14

1. Deklaracja kierownictwa urzędu

Burmistrz Drawska Pomorskiego (Administrator Danych Osobowych) jest świadomy wagi i znaczenia zagadnienia ochrony danych osobowych, dlatego też bezpieczeństwo danych uznaje jako jeden z priorytetów działania oraz zapewnia wszelkie możliwe środki techniczne i organizacyjne, jakie są niezbędne dla bezpiecznego przetwarzania danych.

2. Definicje podstawowe

1) **Dane osobowe.** Zgodnie z art. 6 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 1, poz. 926 ze zm.) 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 (art. 6 ust. 2 ustawy).
   Stosownie do ust. 3 przywołanego przepisu, informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu i działań.
   Ustawowa definicja danych osobowych odpowiada standardom międzynarodowym wyrażonym w Dyrektywie 95/46/EC, w której dane osobowe to wszystkie informacje odnoszące się do oznaczonej lub możliwej do oznaczenia osoby fizycznej. Do dokonania oznaczenia, bez względu czy następuje ono wprost czy pośrednio, wystarcza w szczególności znajomość identyfikujących ją numerów (PESEL, NIP, etc.) albo jednego lub większej liczby czynników specyficznych dla jej psychicznej, psychologicznej, emocjonalnej, ekonomicznej, kulturowej lub społecznej tożsamości. Danymi osobowymi będą zatem zarówno takie dane, które pozwalają na określenie tożsamości konkretnej osoby, jak i takie, które nie pozwalają na jej natychmiastową identyfikację, ale są, przy pewnym nakładzie kosztów, czasu i działań, wystarczające do jej ustalenia. Daną osobową będzie taka informacja, która pozwala na ustalenie tożsamości danej osoby, bez nadzwyczajnego wysiłku i nakładów, zwłaszcza przy wykorzystaniu łatwo osiągalnych i powszechnie dostępnych źródeł. Poza zakresem przedmiotowej definicji znajdzie się, zatem taka informacja, na podstawie której identyfikacja osoby wymagać będzie nieracjonalnych, nieproporcjonalnie dużych nakładów kosztów, czasu lub działań. W świetle powyższej definicji należy przyjąć, że danymi osobowymi nie będą pojedyncze informacje o dużym stopniu ogólności, np. nazwa ulicy i numer domu czy wysokość wynagrodzenia. Informacja ta będzie jednak stanowić daną osobową wówczas, gdy zostanie zestawiona z innymi dodatkowymi informacjami, które w konsekwencji można odnieść do konkretnej osoby. Przykładem pojedynczej informacji stanowiącej daną osobową jest natomiast numer PESEL, który jest 11-cyfrowym, stałym symbolem numerycznym, jednoznacznie identyfikującym osobę fizyczną, w którym sześć pierwszych cyfr oznacza datę urodzenia (rok, miesiąc, dzień), kolejne cztery – liczbę porządkową i płeć osoby, a ostatnia jest cyfrą

kontrolną służącą do komputerowej kontroli poprawności nadanego numeru ewidencyjnego.

2) **Ochrona danych osobowych.** Przez pojęcie ochrony danych osobowych rozumiemy wdrożenie i eksploatowanie wszelkich środków organizacyjno – technicznych mających na celu zabezpieczenie tychże danych przed ich nieuprawnionym przetwarzaniem, oraz ewentualną utratą bądź uszkodzeniem.
3) **Przetwarzanie danych osobowych.** Przetwarzanie danych to dokonywanie jakiejkolwiek operacji na danych osobowych, w szczególności ich zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie i usuwanie, zwłaszcza jeśli operacji dokonuje się w systemie informatycznym. Mieści się w tym zatem także przeglądanie i przekształcanie danych. Do przetwarzania danych zalicza się usuwanie danych, polegające na zniszczeniu bądź modyfikacji danych w sposób, który nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.

Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.

Osoby, które zostały upoważnione do przetwarzania danych, są zobowiązane zachować w tajemnicy nie tylko dane osobowe, do których mają dostęp, ale także sposoby zabezpieczenia tych danych.

4) **Polityka Bezpieczeństwa Danych.** „Polityka Bezpieczeństwa Danych" jest częścią dokumentacji opisującej zasady przetwarzania danych osobowych w Urzędzie Miejskim w Drawsku Pomorskim umożliwiającą ich skuteczną ochronę. Zgodnie z art. 36 ust. 2 oraz art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.), Polityka Bezpieczeństwa Danych odnosi się zarówno do danych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemach informatycznych, przy czym (odnośnie drugiego sposobu przetwarzania danych) istnieje także dodatkowa „Instrukcja zarządzania systemem informatycznym".

Polityka Bezpieczeństwa Danych wskazuje na działania, ustanawia zasady i reguły postępowania, które należy stosować, aby właściwie wykonać obowiązki administratora danych w zakresie zabezpieczenia danych osobowych.

5) **Administrator danych osobowych (ADO).** Przez Administratora danych osobowych rozumie się organ, jednostkę organizacyjną, podmiot lub osobę, wobec których ustawa znajduje swoje zastosowanie zgodnie z dyspozycją art. 3 Ustawy, a które decydują o celach i środkach przetwarzania danych. Administratorem danych są więc wszystkie podmioty realizujące zadania publiczne, jeżeli przetwarzają dane osobowe. Szczególne kompetencje administratora danych, jako decydującego o środkach i celach przetwarzania danych, konkretyzują się w formie nałożonych na niego obowiązków i przyznanych uprawnieniach.

W świetle powyższej definicji za Administratora Danych Osobowych (ADO) należy uważać Urząd Miejski w Drawsku Pomorskim, który reprezentuje Kierownik Urzędu – Burmistrz Drawska Pomorskiego.

Administrator danych zobowiązuje podwładnych do przestrzegania postanowień niniejszego dokumentu.

6) **Urząd** – w tym dokumencie jest rozumiany, jako Urząd Miejski w Drawsku Pomorskim, z siedzibą w Drawsku Pomorskim, ul. Gen. Wł. Sikorskiego 41.
7) **Administrator Bezpieczeństwa Informacji (ABI)** – pracownik urzędu wyznaczony przez Administratora Danych Osobowych (Burmistrza) do nadzorowania i przestrzegania zasad ochrony danych osobowych oraz przygotowania dokumentów wymaganych przez przepisy Ustawy o Ochronie Danych Osobowych w Urzędzie Miejskim w Drawsku Pomorskim, powołany zarządzeniem Burmistrza Drawska Pomorskiego.
8) **Użytkownik systemu** – osoba upoważniona do przetwarzania danych osobowych w systemie. Użytkownikiem może być osoba zatrudniona w Urzędzie, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej czy osoba odbywająca staż.
9) **Identyfikator użytkownika** – jest to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
10) **Hasło** – jest to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
11) **Uwierzytelnianie** – jest to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
12) **Administrator Systemu Informatycznego (ASI)** – pracownik odpowiedzialny za funkcjonowanie systemu teleinformatycznego oraz stosowanie technicznych i organizacyjnych środków ochrony stosowanych w tym systemie.
13) **Sieć lokalna** – połączenie komputerów pracujących w urzędzie w celu wymiany danych (informacji) dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych.
14) **Sieć publiczna** – sieć telekomunikacyjna, niebędąca siecią wewnętrzną służąca do świadczenia usług telekomunikacyjnych w rozumieniu Ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z poźn. zm.).
15) **Sieć telekomunikacyjna** – urządzenia telekomunikacyjne zestawione i połączone w sposób umożliwiający przekaz sygnałów pomiędzy określonymi zakończeniami sieci za pomocą przewodów, fal radiowych, bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną w rozumieniu Ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne (Dz. U. Nr 73, poz.852, z późń. zm.).
16) **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

17) **Przetwarzanie danych** – rozumie się to w tym dokumencie, jako jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.
18) **Zabezpieczenie danych w systemie informatycznym** – wdrożenie i wykorzystywanie stosownych środków technicznych i organizacyjnych, zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
19) **Teletransmisja** – przesyłanie informacji za pomocą sieci telekomunikacyjnej.
20) **Poufność danych** – jest to właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.
21) **Integralność danych** – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
22) **Rozliczalność** – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
23) **Aplikacja** – program komputerowy wykonujący konkretne zadanie.
24) **Wysoki poziom bezpieczeństwa** – musi występować wtedy, gdy przynajmniej jedno urządzenie systemu informatycznego, służące do przetwarzania danych osobowych, połączone jest z siecią publiczną.
25) **Komórka organizacyjna** – rozumie się przez to referat, samodzielne stanowisko pracy.

3. Zagadnienia organizacyjne.

1) **Administrator Danych Osobowych (ADO)** wyznacza **Administratora Bezpieczeństwa Informacji (ABI).**
2) **Administratorem Bezpieczeństwa Informacji (ABI)** w Urzędzie jest Paweł Górzyński.
3) Do obowiązków **Administratora Bezpieczeństwa Informacji (ABI)** należy zapewnienie odpowiednich pomieszczeń, stosownie zabezpieczonych i wyposażonych do przetwarzania i przechowywania danych osobowych, zaznajomienie pracowników z prawnymi oraz pracowniczymi konsekwencjami naruszenia bezpieczeństwa danych osobowych, sporządzenie listy pracowników mających dostęp do danych i je przetwarzających - wraz z zakresem ich uprawnień i odpowiedzialności, reagowanie na zgłaszane incydenty związane z naruszeniem ochrony danych osobowych oraz analizowanie ich przyczyn i kierowanie wniosków dotyczących ukarania winnych naruszeń, niezwłoczne informowanie Administratora Danych Osobowych o przypadkach naruszenia przepisów Ustawy o Ochronie Danych Osobowych.

   Administrator Bezpieczeństwa Informacji (ABI) jest obowiązany również zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. Prowadzi także ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać:
   - imię i nazwisko osoby upoważnionej,
   - datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,

- identyfikator, jeśli dane są przetwarzane w systemie informatycznym.

Szczegółowy zakres obowiązków Administratora Bezpieczeństwa Informacji określony został w Załączniku nr 1 do Zarządzenia nr 78/2011 Burmistrza Drawska Pomorskiego z dnia 25 maja 2011r.

4) **Administrator Danych Osobowych,** w przypadku udostępniania danych osobowych w celach innych, niż włączanie do zbioru, udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba, że przepisy ustaw innych niż Ustawa o Ochronie Danych Osobowych (Dz. U. Nr 101, poz. 926) stanowią inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.
5) **Administrator Bezpieczeństwa Informacji** ma nadzorować przestrzeganie zasad ochrony i przetwarzania danych.
6) **Administrator Systemu Informatycznego** zajmuje się techniczną stroną zabezpieczenia danych w systemie informatycznym.
   Szczegółowy zakres obowiązków Administratora Systemu Informatycznego określony został w Załączniku nr 1 do Zarządzenia nr 79/2011 Burmistrza Drawska Pomorskiego z dnia 25 maja 2011r.
7) Do obowiązków wszystkich administratorów należy zapoznanie pracowników z nowymi zasadami pracy. Odpowiedzialność w tym zakresie spoczywa na każdej z tych osób, odpowiednio do zakresu i poziomu jej zadań.

4. Wykaz budynków i pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe.

Wykaz budynków i pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe znajduje się w Załączniku nr 1 do niniejszego dokumentu.

5. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

Wykaz zbiorów danych osobowych znajduje się w Załączniku nr 2 do niniejszego dokumentu.

6. Opisy struktury zbiorów danych osobowych wskazujące zawartość poszczególnych pól informacyjnych i powiązania między nimi.

Opisy struktur zbiorów danych wskazujące na zawartość poszczególnych pól informacyjnych i powiązania między nimi i znajduje się w Załączniku nr 3 do niniejszej dokumentacji.

7. Sposób przepływu danych pomiędzy poszczególnymi systemami.

Sposób przepływu danych pomiędzy poszczególnymi systemami przedstawia Załącznik nr 4 do niniejszego dokumentu.

8. Środki techniczne i organizacyjne, niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

1) Środki ochrony fizycznej.
   - Wejście do budynku Urzędu zabezpieczone jest zamkami drzwiowymi oraz systemem alarmowym.
   - Pomieszczenia w Urzędzie chronione są systemem alarmowym (czujniki dymu oraz ruchu), za poprawne funkcjonowanie którego odpowiada Kierownik Referatu Ogólnoorganizacyjnego.
   - System alarmowy połączony jest z centralą agencji ochrony.
   - Urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych zamkami patentowymi.
   - Dostęp do pokoi jest kontrolowany za pomocą wydawania kluczy tylko osobom uprawnionym.
   - Poszczególne pokoje, w których odbywa się przetwarzanie danych i ich składowanie, są wyposażone w niezależne zamki i muszą być zamykane podczas nieobecności pracownika. Klucze pobierane są przez pracowników przed rozpoczęciem pracy oraz oddawane po jej zakończeniu do zamykanej gabloty znajdującej się w pomieszczeniu (tzw. „dyżurce").
   - Przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osoby zatrudnionej przy przetwarzaniu danych lub w obecności Administratora Bezpieczeństwa Informacji.
   - Dostęp do pomieszczenia, w którym znajdują się urządzenia serwerowe ma tylko Administrator Danych Osobowych (ADO), Administrator Bezpieczeństwa Informacji (ABI), Administrator Systemu Informatycznego (ASI).
   - Lokalizacja urządzeń komputerowych (komputerów typu PC, laptopów, drukarek) uniemożliwia osobom niepowołanym dostęp do nich oraz wgląd do danych wyświetlanych na monitorach komputerowych.
   - Komputery przenośne, wykorzystywane do przetwarzania danych osobowych, po zakończonej pracy są przechowywane w warunkach zapewniających ich bezpieczeństwo.
   - Dopuszcza się możliwość wynoszenia komputerów przenośnych poza siedzibę Urzędu w celu realizacji zadań służbowych, po uprzednim uzyskaniu zgody Administratora Danych Osobowych (ADO) i zgłoszeniu tego faktu Administratorowi Bezpieczeństwa Informacji (ABI). Uzyskanie takiej zgody odbywa się na podstawie pisemnego wniosku, w którym podaje się miejsce użytkowania wynoszonego sprzętu, w jakim okresie będzie on tam użytkowany oraz w jakim celu. Za bezpieczeństwo danych znajdujących się na komputerze przenośnym odpowiada osoba wynosząca go poza teren Urzędu.
2) Środki sprzętowe, informatyczne i telekomunikacyjne.
   - Dokumenty zawierające dane osobowe, po ustaniu przydatności, są niszczone przez pocięcie w niszczarce.

- Urządzenia wchodzące w skład systemu informatycznego podłączone są do odrębnego obwodu elektrycznego, zabezpieczonego na wypadek zaniku napięcia albo awarii w sieci zasilanej urządzeniem UPS.
- Akumulatory w zasilaczach awaryjnych UPS wymieniane są na nowe co 3 lata.
- Kopie awaryjne wykonywane są w cyklach: dzienna na dysku twardym, tygodniowa na macierzy dyskowej.
- Sieć lokalna skonfigurowana jest w topologii gwiazdy.
- Sieć lokalna podłączona jest do Internetu poprzez serwer spełniający funkcję sprzętowego, zewnętrznego firewalla, filtrującego dane przechodzące pomiędzy siecią lokalną i siecią publiczną.
- Dostęp fizyczny do sieci lokalnej jest ograniczony, centralny punkt dystrybucyjny sieci umieszczony jest w serwerowni – pokój nr 209,
- Zastosowano ochronę przeciwpożarową poprzez zlokalizowanie w pomieszczeniach oraz na korytarzach gaśnic oraz węży gaśniczych, a także czujników dymu połączonych z systemem alarmowym.
- W pomieszczeniu serwerowni utrzymywana jest stała, niska temperatura (dzięki zastosowaniu klimatyzatorów).

3) Środki ochrony w ramach oprogramowania urządzeń teletransmisji.
   - Na stacjach roboczych systemu działa oprogramowanie antywirusowe.
   - Na komputerach użytkowników systemu działa programowy firewall.
   - Dostęp do serwera zawierającego dane osobowe zabezpieczony jest hasłem.
   - W razie wystąpienia konieczności wymiany danych pomiędzy Urzędem a jednostkami współpracującymi, zestawiany jest tunel, zapewniający poufność i integralność przesyłanych danych (szyfrowanie, sumy kontrolne), oparty o protokół IPSEC.
   - Do połączenia z serwerem poczty wykorzystywane jest połączenie z wykorzystaniem algorytmu SSL, zapewniające poufność danych używanych do autoryzacji i uwierzytelniania.
   - Dostęp do Internetu realizowany jest za pomocą urządzeń technicznych, zapewniających ochronę przed nieautoryzowanym dostępem z zewnątrz.
4) Środki ochrony w ramach oprogramowania systemu.
   - Dostęp do baz danych osobowych zastrzeżony jest wyłącznie dla uprawnionych pracowników.
   - Konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych przechowywanych w systemie informatycznym, wyłącznie za pośrednictwem aplikacji wymienionych w punkcie 4.
   - System informatyczny pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu, odrębnie dla każdego pracownika.
   - Zastosowano działający w tle program antywirusowy na komputerach użytkowników.
   - W systemie sieciowym stosuje się mechanizm wymuszający okresową zmianę haseł dostępu.
5) Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych.

- Zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji.
- Dla każdego użytkownika systemu wyznaczony jest odrębny identyfikator.
- Użytkownicy mają dostęp do aplikacji umożliwiający dostęp tylko do tych danych osobowych, do których mają uprawnienia.

6) Zabezpieczenie zbiorów przetwarzanych tradycyjnie.
   - Zbiory danych przetwarzane tradycyjnie (ręcznie) po godzinach pracy przechowywane winny być w szafkach zamykanych (zamki, kłódki). W przypadku przetwarzania takich danych w pomieszczeniu, w którym przebywać mogą osoby nieupoważnione do przetwarzania takich danych (np. interesanci albo inni pracownicy) powinno być ono przeprowadzane w taki sposób, aby osoby nieupoważnione nie miały wglądu do tych danych.
7) Środki ochrony w ramach systemu użytkowego.
   - Komputer, z którego możliwy jest dostęp do danych osobowych, zabezpieczony jest hasłem uruchomieniowym.
   - Zastosowano wygaszenie ekranu w przypadku dłuższej nieaktywności użytkownika.
   - Zastosowano blokadę hasłem podczas dłuższej nieaktywności użytkownika.
8) Środki organizacyjne.
   - Wyznaczono Administratora Bezpieczeństwa Informacji.
   - Wyznaczono Administratora Systemów Informatycznych.
   - Opracowano i wdrożono Politykę Bezpieczeństwa Danych i Instrukcję Zarządzania Systemem Informatycznym.
   - Tymczasowe wydruki z danymi osobowymi są, po ustaleniu ich przydatności, niszczone.
   - Do przetwarzania danych osobowych przy użyciu systemu informatycznego dopuszczane są osoby na podstawie indywidualnego pozwolenia na dostęp do przetwarzania danych osobowych wydawanego przez Administratora Danych Osobowych.
   - Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane są do zachowania ich w tajemnicy.
   - Osoby przetwarzające dane osobowe są przed dopuszczeniem ich do tych danych szkolone w zakresie obowiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych osobowych w systemie informatycznym.
   - Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.
   - Zdefiniowano procedury postępowania w sytuacji naruszenia ochrony danych osobowych.
   - Administrator systemu informatycznego usuwa wszystkie przypadki awarii systemu oraz dokonuje bieżącej konserwacji systemu.
   - W przypadku, gdy zachodzi konieczność naprawy sprzętu poza siedzibą urzędu, należy wymontować z niego nośniki informacji zawierające dane osobowe.

- W przypadku, gdy uszkodzenie sprzętu zawierającego nośnik danych, na którym zapisane są dane osobowe wymusza konieczność przekazania go poza siedzibę urzędu, nośnik ten należy wymontować.
- Pracownikom wolno przebywać na terenie Urzędu tylko w wyznaczonych godzinach pracy, a później - po zawiadomieniu i uzyskaniu zgody bezpośredniego przełożonego.
- Przebywanie w Urzędzie w dni wolne od pracy możliwe jest jedynie po uzyskaniu zgody Administratora Danych Osobowych.
- Wszyscy pracownicy przebywający na terenie Urzędu zobowiązaniu są do noszenia identyfikatorów.

9. Lokalizacja sprzętu komputerowego

Szczegółowy opis fizycznego rozmieszczenia elementów infrastruktury informatycznej (np. rozmieszczenie gniazdek, elementów sieciowych, komputerów) w Urzędzie przedstawia Załącznik nr 6.

10. Instrukcja alarmowa w przypadku naruszenia ochrony danych osobowych

Opis zdarzeń naruszających ochronę danych osobowych.

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:

1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
2) niewłaściwe parametry środowiska, np. niewłaściwa wilgotność, temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje,
3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub sabotaż,
4) niewłaściwe działanie serwisu zewnętrznego, w tym także pozostawienie serwisantów bez nadzoru,
5) pojawienie się komunikatu alarmowego, pochodzącego od części systemu informatycznego zapewniającej ochronę zasobów lub innego komunikatu o podobnym znaczeniu,
6) zła jakość danych w systemie informatycznym lub inne odstępstwo od stanu oczekiwanego, wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
7) naruszenie lub próba naruszenia integralności systemu informatycznego lub bazy danych w tym systemie,
8) stwierdzenie modyfikacji danych, próby ich modyfikacji lub zmiany w strukturze danych bez upoważnienia,

9) stwierdzenie niedopuszczalnej manipulacji danymi osobowymi w systemie informatycznym,
10) ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania lub innych chronionych elementów systemu zabezpieczeń,
11) funkcjonowanie systemu lub jego sieci komputerowej, wykazujące odstępstwa od założonego rytmu pracy, uprawdopodobniające przełamanie lub zaniechanie ochrony danych osobowych, np. praca przy komputerze lub w sieci osoby, która nie jest dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
12) obecność w obszarze bezpieczeństwa osób postronnych bez dozoru pracowników zatrudnionych przy przetwarzaniu danych osobowych,
13) ujawnienie istnienia nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki", itp.,
14) naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (np. niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie wydrukowanych danych osobowych w drukarce czy w kserografie, niewykonanie w określonym terminie kopii bezpieczeństwa, itp.),
15) za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia fizycznego miejsc przetwarzania danych osobowych, np. pozostawienie otwartego pomieszczenia w obszarze bezpieczeństwa, umożliwienie nieautoryzowanego dostępu do urządzeń archiwizujących, itp.

Postępowanie w przypadku naruszenia ochrony danych osobowych.

W przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego, stanu urządzeń, zawartości zbioru danych osobowych, wynikającego z ujawnienia metody pracy lub sposobu działania programu, jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych, innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. pożar, itp.) każdy pracownik zatrudniony przy przetwarzaniu danych osobowych jest obowiązany niezwłocznie powiadomić o tym fakcie Administratora Systemu Informatycznego oraz Administratora Bezpieczeństwa Informacji.

Pracownicy, którzy stwierdzili naruszenie ochrony danych osobowych, w oczekiwaniu na przybycie Administratora Bezpieczeństwa są zobligowani, by:

1) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
2) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
3) wstrzymać bieżącą pracę w celu zabezpieczenia miejsca zdarzenia,
4) zaniechać, dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,

5) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych, stosownie do objawów i komunikatów towarzyszących naruszeniu,
8) udokumentować wstępnie zaistniałe naruszenie,
6) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa Informacji lub osoby upoważnionej.

Działania Administratora Bezpieczeństwa Informacji.

1) Po przybyciu na miejsce naruszenia ochrony danych osobowych Administrator Bezpieczeństwa Informacji zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania, mając na uwadze Politykę Bezpieczeństwa Danych w tym zakresie, żąda dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem.
2) Administrator Bezpieczeństwa Informacji dokumentuje zaistniały przypadek naruszenia w rejestrze incydentów, którego wzór stanowi Załącznik nr 5 do niniejszego dokumentu oraz sporządza raport, który powinien w szczególności zawierać:
   a) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
   b) określenie czasu i miejsca naruszenia i powiadomienia,
   c) określenie rodzaju naruszenia i okoliczności towarzyszących,
   d) opis podjętego działania i metody postępowania,
   e) wstępną ocenę przyczyn wystąpienia naruszenia,
   f) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.
3) Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu, Administrator Bezpieczeństwa Informacji zasięga niezbędnych opinii i proponuje postępowanie naprawcze, w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.
4) Zaistniałe naruszenie powinno stać się przedmiotem szczegółowej, zespołowej analizy z udziałem Administratora Bezpieczeństwa Informacji, Administratora Danych Osobowych i Administratora Systemu Informatycznego.

Postanowienia końcowe.

Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszej Instrukcji, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne, przewidziane przepisami prawa pracy.

11. Plan ciągłości działania

1) Awaria systemów komputerowych:

W razie wystąpienia awarii systemów komputerowych należy powiadomić Administratora Systemów Informatycznych:
Informatyk, tel.: 94 363 34 85wew. 843.
Jeśli to niemożliwe, to osobę upoważnioną przez Administratora Systemów Informatycznych.

2) Awaria sieci internetowej:
W pierwszej kolejności - kontakt do osoby podanej w pkt. 1.
W innych przypadkach - kontakt z operatorem sieci – firma Orange Polska
3) Awaria systemu alarmowego:
W razie wystąpienia awarii systemu alarmowego należy powiadomić osobę odpowiedzialną za jego poprawne funkcjonowanie:
Kierownik Referatu Ogólnoorganizacyjnego, tel.: 94 363 34 85 wew. 826.
Jeśli to niemożliwe to osobę serwis zewnętrzny:
Przedsiębiorstwo „Monitor", tel.: 94 34 66 632.
4) Zdarzenia losowe (pożar, powódź, itp.):
Wznowienie działania Urzędu koordynuje:
Sekretarz Gminy, tel.: 94 363 34 85 wew. 833.
Zgłoszenie szkody następuje do firmy ubezpieczeniowej – Towarzystwo Ubezpieczeń Wzajemnych Koszalin, tel. 94 34 20 390.
5) Instrukcja Bezpieczeństwa Pożarowego.
Opracowana i zatwierdzona przez Burmistrza Drawska Pomorskiego w 2011r.

12. Konsekwencje naruszenia Polityki Bezpieczeństwa Danych

1) Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane, jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym Administratora Bezpieczeństwa Informacji.
2) W sprawach nieuregulowanych niniejszym dokumentem mają zastosowanie przepisy Ustawy z dnia 29 sierpnia 1997 r. o Ochronie Danych Osobowych z późniejszymi zmianami oraz możliwość wniesienia wobec tej osoby sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

13. Lista załączników

Załącznik Nr 1 – Wykaz budynków i pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe.
Załącznik Nr 2 – Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.
Załącznik Nr 3 – Opis struktury zbiorów danych osobowych, wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.
Załącznik Nr 4 – Sposoby przepływu danych.
Załącznik Nr 5 – Rejestr incydentów.
Załącznik Nr 6 – Mapa sieci.

Załącznik Nr 1 do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Miejskim w Drawsku Pomorskim

WYKAZ BUDYNKÓW I POMIESZCZEŃ TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE.

Lp.	Adres - budynek	Nr pokoju	Nazwa jednostki organizacyjnej
1.	Budynek Urzędu Miejskiego w Drawsku Pomorskim, ul. Gen. Wł. Sikorskiego 41	102 (parter)	Referat podatków i opłat oraz windykacji: 1) stanowisko ds. windykacji i opłat lokalnych 2) stanowisko ds. wymiaru podatków 3) stanowisko ds. wymiaru podatków
		103 (parter)	Referat planowania budżetu i finansów: 1) kierownik referatu
		104 (parter)	Referat planowania budżetu i finansów: 1) stanowisko ds. księgowości budżetowej 2) stanowisko ds. księgowości budżetowej
		105 (parter)	Referat planowania budżetu i finansów: 1) stanowisko ds. księgowości budżetowej 2) stanowisko ds. księgowości budżetowej
		106 (parter)	Skarbnik Gminy
		107 (parter)	Referat planowania budżetu i finansów: 1) stanowisko ds. księgowości podatkowej 2) stanowisko ds. płac i rozliczeń podatku dochodowego
		108 (parter)	Referat planowania budżetu i finansów: 1) stanowisko ds. obsługi kasowej
		110 (parter)	Referat urbanistyki, rozwoju lokalnego i gospodarki nieruchomościami: 1) stanowisko ds. planowania przestrzennego i budownictwa
		111 (parter)	Referat urbanistyki, rozwoju lokalnego i gospodarki nieruchomościami: 1) stanowisko ds. gospodarki nieruchomościami 2) stanowisko ds. gospodarki nieruchomościami

		113 (parter)	Biuro spraw obywatelskich: 1) stanowisko ds. ewidencji ludności 2) stanowisko ds. ewidencji ludności i dowodów osobistych
		114 (parter)	Referat podatków i opłat oraz windykacji: 1) stanowisko ds. windykacji, podatków i opłat 2) poborca
		115 (parter)	Biuro spraw obywatelskich: 1) stanowisko ds. wojskowych 2) pełnomocnik ds. ochrony informacji niejawnych i obrony cywilnej
		116 (parter)	Referat podatków i opłat oraz windykacji: 1) kierownik referatu
		117 (parter)	Referat ogólno-organizacyjny: 1) stanowisko ds. obsługi obywateli
		201 (I piętro)	Obsługa prawna: 1) radca prawny 2) radca prawny
		203 (I piętro)	Pełnomocnik ds. kontroli zarządczej
		204 (I piętro)	Referat ogólno-organizacyjny 1) kierownik referatu 2) stanowisko ds. organizacyjnych 3) stanowisko ds. organizacyjnych i gospodarczych
		205 (I piętro)	Referat pozyskiwania funduszy: 1) kierownik referatu 2) stanowisko ds. pozyskiwania funduszy 3) stanowisko ds. pozyskiwania funduszy i zrównoważonego rozwoju
		206 (I piętro)	Referat promocji 1) kierownik referatu 2) stanowisko ds. promocji gminy 3) stanowisko ds. kultury, sportu i rekreacji
		207 (I piętro)	Sekretarz Gminy

		208 (I piętro)	Serwerownia
		210 (I piętro)	Burmistrz Z-ca Burmistrza Referat ogólno-organizacyjny: 1) stanowisko ds. sekretariatu urzędu
		212 (I piętro)	Referat urbanistyki, rozwoju lokalnego i gospodarki nieruchomościami: 1) stanowisko ds. rozwoju lokalnego i zamówień publicznych 2) stanowisko ds. inwestycji i funduszy pomocowych
		213 (I piętro)	Referat urbanistyki, rozwoju lokalnego i gospodarki nieruchomościami: 1) stanowisko ds. gospodarki komunalnej i rozwoju lokalnego 2) stanowisko ds. inwestycji, remontów i drogownictwa
		214 (I piętro)	Referat urbanistyki, rozwoju lokalnego i gospodarki nieruchomościami: 1) kierownik referatu
		215 (I piętro)	Referat urbanistyki, rozwoju lokalnego i gospodarki nieruchomościami: 1) stanowisko ds. drogownictwa 2) stanowisko ds. gospodarki nieruchomościami
		306 (II piętro)	Referat ogólno-organizacyjny: 1) stanowisko ds. obsługi rady miejskiej i organów pomocniczych
		307 (II piętro)	Referat ogólno-organizacyjny): 1) informatyk 2) stanowisko ds. obsługi informatycznej urzędu
		308 (II piętro)	Biuro obsługi finansowej szkół i przedszkoli: 1) stanowisko ds. płac
		309 (II piętro)	Biuro obsługi finansowej szkół i przedszkoli: 1) stanowisko ds. księgowości budżetowej 2) stanowisko ds. księgowości budżetowej 3) stanowisko ds. finansowo-księgowych

		310 (II piętro)	Archiwum
		311 (II piętro)	Archiwum
2.	Budynek Urzędu Miejskiego w Drawsku Pomorskim, Park Chopina 2	parter	Referat rolnictwa i ochrony środowiska: 1) kierownik referatu 2) stanowisko ds. ochrony środowiska, z-ca kierownika 3) stanowisko ds. edukacji ekologicznej 4) stanowisko ds. gospodarki odpadami 5) stanowisko ds. rolnictwa, melioracji i urządzeń wodnych
		I piętro	Referat spraw społecznych: 1) kierownik referatu 2) stanowisko ds. działalności gospodarczej 3) stanowisko ds. administracyjno-oświatowych
3.	Budynek Urzędu Miejskiego w Drawsku Pomorskim, ul. Kolejowa 1	8	Straż Miejska: 1) komendant 2) strażnik miejski
		4	Straż Miejska 1) z-ca komendanta 2) strażnik miejski
		5	Straż Miejska 1) strażnik miejski 2) strażnik miejski
		1	Straż Miejska 1) strażnik miejski 2) strażnik miejski
		15	Referat promocji 1) stanowisko ds. turystyki i ochrony dziedzictwa kulturowego 2) stanowisko ds. obsługi informacji turystycznej
		7	Serwerownia
4.	Siedziba Urzędu Stanu Cywilnego w Drawsku Pomorskim, Plac Orzeszkowej 3	parter	Urząd Stanu Cywilnego: 1) kierownik urzędu stanu cywilnego 2) z-ca kierownika urzędu stanu cywilnego

Załącznik Nr 2 do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Miejskim w Drawsku Pomorskim

WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH.

Lp.	Nazwa zbioru	Program obsługujący
1.	Ewidencja podatników	Gmina 2 (ZETO Koszalin)
2.	Ewidencja upomnień i tytułów wykonawczych	Gmina 2 (ZETO Koszalin)
3.	Zwrot akcyzy dla rolników	ZWROTY Piotr Zielonka, Piotrków Trybunalski
4.	Płatnik UM (bez rejestracji w GIODO)	Płatnik Asseco Poland S.A.
5.	Płace i Kadry UM (bez rejestracji w GIODO)	Qrezus Kadry i Płace QNT Systemy Informatyczne Sp. z o.o. Gliwice
6.	Rejestr decyzji o ustaleniu warunków zabudowy	Wyłącznie w postaci papierowej
7.	Rejestr decyzji o ustaleniu lokalizacji inwestycji celu publicznego	Wyłącznie w postaci papierowej
8.	Ewidencja gruntów	SWDE (m6 Soft Plus Opole)
9.	Rejestr dzierżawców gruntów oraz opłat za użytkowanie wieczyste	Wyłącznie w postaci papierowej
10.	Rejestr nabywców nieruchomości	Wyłącznie w postaci papierowej
11.	Dowody osobiste	SWDO (Wasko S.A.)
12.	Ewidencja ludności	SELWIN (ARAM Warszawa)
13.	Baza danych osobowych w postępowaniu o wykroczenia	Wyłącznie w postaci papierowej
14.	Rejestr świadczeń na rzecz obrony	Wyłącznie w postaci papierowej
15.	Rejestracja i pobór do odbycia zasadniczej służby wojskowej	Wyłącznie w postaci papierowej
16.	Rejestracja i kwalifikacja wojskowa	Wyłącznie w postaci papierowej
17.	Ochrona ludności i sprawy obronne	Wyłącznie w postaci papierowej
18.	Ochrona przeciwpożarowa	Wyłącznie w postaci papierowej
19.	Zarządzanie kryzysowe	Wyłącznie w postaci papierowej
20.	Dłużnik alimentacyjny	Krajowy Rejestr Długów (przez przeglądarkę internetową)
21.	Stypendia szkolne	Microsoft Office Excel

22.	Zasiłki szkolne	Wyłącznie w postaci papierowej
23.	Oświadczenia majątkowe	BIP
24.	Ewidencja obiektów w których świadczone są usługi hotelarskie (bez rejestracji w GIODO)	Wyłącznie w postaci papierowej
25.	Rejestr decyzji zezwalających na usunięcie drzew i krzewów	Wyłącznie w postaci papierowej
26.	Ewidencja właścicieli psów na posiadanie których wymagane jest zezwolenie	Wyłącznie w postaci papierowej
27.	Rejestr skarg i wniosków	Wyłącznie w postaci papierowej
28.	Ewidencja działalności gospodarczej (bez rejestracji w GIODO)	EDG Sputnik Software Poznań
29.	Ewidencja osób posiadających zezwolenie na sprzedaż alkoholu	Koncesje Alkoholowe Sputnik Software Poznań
30.	Zezwolenie na prowadzenie krajowego, drogowego przewozu osób	Wyłącznie w postaci papierowej
31.	Ewidencja osób ubiegających się o przydział mieszkania	Wyłącznie w postaci papierowej
32.	Rejestr zezwoleń na lokalizację zjazdów	Wyłącznie w postaci papierowej
33.	Rejestr zezwoleń na zajęcie pasa drogowego	Wyłącznie w postaci papierowej
34.	Płace BOFKSIP (bez rejestracji w GIODO)	Qrezus Płace QNT Systemy Informatyczne Sp. z o.o. Gliwice
35.	Płatnik BOFKSIP (bez rejestracji w GIODO)	Płatnik Asseco Poland S.A.
36.	Rejestr radnych i sołtysów	Wyłącznie w postaci papierowej
37.	Awans zawodowy nauczycieli	Wyłącznie w postaci papierowej
38.	Urząd Stanu Cywilnego w Drawsku Pomorskim	PB_USC (PTH „Technika" Gliwice)
39.	Ewidencja zbiorników bezodpływowych	Wyłącznie w postaci papierowej
40.	Rejestr działalności regulowanej w zakresie odbierania odpadów komunalnych (bez rejestracji w GIODO)	GOMiG Odpady (Arisco)
41.	Rejestr właścicieli nieruchomości składających deklaracje o wysokości opłaty za gospodarowanie odpadami komunalnymi	GOMiG Odpady (Arisco)

Załącznik Nr 3 do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Miejskim w Drawsku Pomorskim

OPISY STRUKTURY ZBIORÓW DANYCH OSOBOWYCH WSKAZUJĄCY ZAWARTOŚĆ POSZCZEGÓLNYCH PÓL INFORMACYJNYCH I POWIĄZANIA MIĘDZY NIMI.

Lp.	Nazwa zbioru	Struktura zbioru
1.	Ewidencja podatników	- nazwiska i imiona - imiona rodziców - data urodzenia - adres zam. lub pobytu - nr ewidencyjny PESEL - NIP - seria i nr DO - nr telefonu
2.	Ewidencja upomnień i tytułów wykonawczych	- nazwiska i imiona - imiona rodziców - data urodzenia - NIP - adres zam. lub pobytu - nr ewidencyjny PESEL - seria i nr DO - nr telefonu
3.	Zwrot akcyzy dla rolników	- nazwiska i imiona - adres zam. lub pobytu - nr ewidencyjny PESEL - NIP
4.	Płatnik UM (bez rejestracji w GIODO)	- nazwiska i imiona - data urodzenia - adres zam. lub pobytu - nr ewidencyjny PESEL - inne: - przynależność do NFZ - NIP
5.	Płace i Kadry UM (bez rejestracji w GIODO)	- nazwiska i imiona - imiona rodziców - data urodzenia - miejsce urodzenia - adres zam. lub pobytu - nr ewidencyjny PESEL - NIP - seria i nr DO - nr telefonu - wykształcenie - zawód - miejsce pracy - przynależność do NFZ - numer konta bankowego

6.	Rejestr decyzji o ustaleniu warunków zabudowy	- nazwiska i imiona - adres zam. lub pobytu - oznaczenie nieruchomości (nr dz. ew.)
7.	Rejestr decyzji o ustaleniu lokalizacji inwestycji celu publicznego	- nazwiska i imiona - adres zam. lub pobytu - oznaczenie nieruchomości (nr dz. ew.)
8.	Ewidencja gruntów	- nazwiska i imiona - imiona rodziców - adres zam. lub pobytu - nr ewidencyjny PESEL - inne: - dane o współwłaścicielach: - NIP - seria i nr DO
9.	Rejestr dzierżawców gruntów oraz opłat za użytkowanie wieczyste	- nazwiska i imiona - adres zam. lub pobytu
10.	Rejestr nabywców nieruchomości	- nazwiska i imiona - imiona rodziców - adres zam. lub pobytu - nr ewidencyjny PESEL - seria i nr DO - nr telefonu
11.	Dowody osobiste	- nazwiska i imiona - imiona rodziców - data urodzenia - miejsce urodzenia - adres zam. lub pobytu - seria i nr DO - nr ewidencyjny PESEL - - nazwisko rodowe - nazwisko rodowe matki - kolor oczu - wzrost - płeć

12.	Ewidencja ludności	- nazwiska i imiona - imiona rodziców - data urodzenia - miejsce urodzenia - adres zam. lub pobytu - nr ewidencyjny PESEL - seria i nr DO - wykształcenie - płeć - stan cywilny - data zawarcia małżeństwa, zgonu - data rozwiązania małżeństwa - obywatelstwo - nazwiska i imiona poprzednie - imię, nazwisko, nazwisko rodowe małżonka - nazwiska rodowe rodziców - adres poprzedniego zameldowania - obowiązek wojskowy
13.	Baza danych osobowych w postępowaniu o wykroczenia	- nazwiska i imiona - imiona rodziców - data urodzenia - miejsce urodzenia - adres zam. lub pobytu - nr ewidencyjny PESEL - seria i nr DO - miejsce pracy - zawód - wykształcenie - nr telefonu
14.	Rejestr świadczeń na rzecz obrony	- nazwiska i imiona - imiona rodziców - data urodzenia - miejsce urodzenia - adres zam. lub pobytu - nr ewidencyjny PESEL - miejsce pracy - zawód - nr telefonu
15.	Rejestracja i pobór do odbycia zasadniczej służby wojskowej	- nazwiska i imiona - imiona rodziców - data urodzenia - miejsce urodzenia - adres zam. lub pobytu - seria i nr DO - miejsce pracy - zawód - wykształcenie

16.	Rejestracja i kwalifikacja wojskowa	- nazwiska i imiona - imiona rodziców - data urodzenia - miejsce urodzenia - adres zam. lub pobytu - nr ewidencyjny PESEL - seria i nr DO - inne: kategoria wojskowa
17.	Ochrona ludności i sprawy obronne	- nazwiska i imiona - imiona rodziców - data urodzenia - miejsce urodzenia - adres zam. lub pobytu - nr ewidencyjny PESEL - NIP - seria i nr DO - miejsce pracy - zawód - wykształcenie - nr telefonu
18.	Ochrona przeciwpożarowa	- nazwiska i imiona - imiona rodziców - data urodzenia - miejsce urodzenia - adres zam. lub pobytu - nr ewidencyjny PESEL - NIP - seria i nr DO - miejsce pracy - zawód - wykształcenie - nr telefonu
19.	Zarządzanie kryzysowe	- nazwiska i imiona - imiona rodziców - data urodzenia - miejsce urodzenia - adres zam. lub pobytu - nr ewidencyjny PESEL - NIP - seria i nr DO - miejsce pracy - zawód - wykształcenie - nr telefonu

20.	Dłużnik alimentacyjny	- nazwiska i imiona - data urodzenia - miejsce urodzenia - adres zam. lub pobytu - nr ewidencyjny PESEL - seria i nr DO
21.	Stypendia szkolne	- nazwiska i imiona - imiona rodziców - data urodzenia - miejsce urodzenia - adres zam. lub pobytu - nr ewidencyjny PESEL - miejsce pracy - nr telefonu
22.	Zasiłki szkolne	- nazwiska i imiona - imiona rodziców - data urodzenia - miejsce urodzenia - adres zam. lub pobytu - nr ewidencyjny PESEL - nr telefonu
23.	Oświadczenia majątkowe	- nazwiska i imiona - miejsce pracy - data urodzenia - miejsce urodzenia - dochody własne i współmałżonka, oszczędności, zobowiązania pieniężne, posiadane nieruchomości i składniki mienia ruchomego
24.	Ewidencja obiektów w których świadczone są usługi hotelarskie (bez rejestracji w GIODO)	- nazwiska i imiona - adres zam. lub pobytu - nr telefonu - adres obiektu - nazwa obiektu
25.	Rejestr decyzji zezwalających na usunięcie drzew i krzewów	- nazwiska i imiona - adres zam. lub pobytu - imiona, nazwiska i adresy zam. osób występujących w spółkach cywilnych
26.	Ewidencja właścicieli psów na posiadanie których wymagane jest zezwolenie	- nazwiska i imiona - adres zam. lub pobytu
27.	Rejestr skarg i wniosków	- nazwiska i imiona - adres zam. lub pobytu

28.	Ewidencja działalności gospodarczej (bez rejestracji w GIODO)	- nazwiska i imiona - NIP - adres zam. lub pobytu - nr ewidencyjny PESEL - nr telefonu
29.	Ewidencja osób posiadających zezwolenie na sprzedaż alkoholu	- nazwiska i imiona - NIP - adres zam. lub pobytu - nr ewidencyjny PESEL - nr telefonu - adresy miejsc wykonywania działalności
30.	Zezwolenie na prowadzenie krajowego, drogowego przewozu osób	- nazwiska i imiona - NIP - zawód - adres zam. lub pobytu - nr ewidencyjny PESEL - nr telefonu
31.	Ewidencja osób ubiegających się o przydział mieszkania	- nazwiska i imiona - data urodzenia - miejsce urodzenia - nr telefonu
32.	Rejestr zezwoleń na lokalizację zjazdów	- nazwiska i imiona - adres zam. lub pobytu - nr telefonu
33.	Rejestr zezwoleń na zajęcie pasa drogowego	- nazwiska i imiona - adres zam. lub pobytu - nr telefonu
34.	Płace BOFKSIP (bez rejestracji w GIODO)	- nazwiska i imiona - imiona rodziców - data urodzenia - miejsce urodzenia - adres zam. lub pobytu - nr ewidencyjny PESEL - NIP - seria i nr DO - nr telefonu - miejsce pracy - zawód - wykształcenie - przynależność do NFZ - numer konta bankowego
35.	Płatnik BOFKSIP (bez rejestracji w GIODO)	- nazwiska i imiona - NIP - data urodzenia - adres zam. lub pobytu - nr ewidencyjny PESEL - przynależność do NFZ

36.	Rejestr radnych i sołtysów	- nazwiska i imiona - imiona rodziców - data urodzenia - miejsce urodzenia - adres zam. lub pobytu - nr ewidencyjny PESEL - NIP - seria i nr DO - miejsce pracy - zawód - wykształcenie - nr telefonu - numer konta bankowego
37.	Awans zawodowy nauczycieli	- nazwiska i imiona - data urodzenia - miejsce urodzenia - adres zam. lub pobytu - zawód

38.	Urząd Stanu Cywilnego w Drawsku Pomorskim	- nazwiska i imiona - imiona rodziców - data urodzenia - miejsce urodzenia - adres zam. lub pobytu - nr ewidencyjny PESEL - seria i nr DO - wykształcenie - miejsce pracy - stan cywilny - płeć - nazwisko: panieńskie, z poprzedniego małżeństwa, rodowe - nazwisko i imię: ojca, matki, współmałżonka - nazwisko po zawarciu małżeństwa: mężczyzny, kobiety - godzina urodzenia - data i numer aktu: urodzenia, małżeństwa, zgonu - data i miejsce zawarcia małżeństwa - miejsce wystawienia i numer aktu urodzenia żony, męża - data, godzina, miejsce zgonu, odnalezienia zwłok - nazwisko, imię, adres osoby zgłaszającej zgon - adnotacje o rozwodzie - miejsce wydania dowodu osobistego - data unieważnienia aktu małżeństwa, urodzenia, zgonu - imię nadane z urzędu - data i numer orzeczenia sądu ustalającego ojcostwo, zaprzeczającego ojcostwo, przysposabiającego dziecko - imię i nazwisko osoby przysposabiającej dziecko - zmiana nazwiska dziecka
39.	Ewidencja zbiorników bezodpływowych	- nazwiska i imiona - adres nieruchomości, na których znajdują się zbiorniki bezodpływowe
40.	Rejestr działalności regulowanej w zakresie odbierania odpadów komunalnych (bez rejestracji w GIODO)	- nazwiska i imiona - NIP - oznaczenie siedziby przedsiębiorcy.
41.	Rejestr właścicieli nieruchomości składających deklaracje o wysokości opłaty za gospodarowanie odpadami komunalnymi	- nazwiska i imiona - adres zam. lub pobytu - nr ewidencyjny PESEL - NIP - nr telefonu

Załącznik Nr 4 do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Miejskim w Drawsku Pomorskim

SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY SYSTEMAMI INFORMATYCZNYMI

1. Systemy, w których przetwarza się dane osobowe nie są ze sobą połączone, co uniemożliwia przepływ danych pomiędzy nimi. Wyjątek stanowi baza danych z aplikacji „Płace", z której dane są eksportowane do aplikacji „Płatnik". Przekazywane są następujące dane: imiona i nazwiska, data urodzenia, adres zamieszkania lub pobytu, numery PESEL i NIP, przynależność do NFZ. Pozostałe programy są niezależne i posiadają samodzielne bazy danych.
2. Sposób przepływu danych – z programu „Płace" generowany jest plik o strukturze akceptowanej prze program „Płatnik". Następnie program „Płatnik" importuje dane z przygotowanego pliku. Przepływ danych odbywa się w lokalnej sieci LAN pomiędzy serwerem a stacją roboczą.
3. Pomiędzy programem finansowo-księgowym Gmina2 a programem GOMiG –Odpady przesyłane są informacje pomiędzy serwerami.
4. Jeden raz na kwartał generowany jest plik tekstowy z programu SELWin zawierający informacje o aktualnym stanie meldunkowym (nazwa miejscowości, ulica, numer domu, numer lokalu, ilość osób zameldowanych na stałe, ilość osób zameldowanych czasowo), tymi danymi zasilany jest program GOMiG – Odpady.

Załącznik Nr 5 do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Miejskim w Drawsku Pomorskim

REJESTR INCYDENTÓW

Lp.	Data	Godzina	Osoba powiadamiająca o zdarzeniu	Osoby towarzyszące	Lokalizacja zdarzenia	Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące	Podjęte działania	Przyczyny wystąpienia zdarzenia	Postępowanie wyjaśniające

Załącznik nr 6 do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Miejskim w Drawsku Pomorskim

Rozmieszczenie elementów infrastruktury informatycznej w Urzędzie Miejskim w Drawsku Pomorskim

Lp.	Adres - budynek	Nr pokoju	Rodzaj infrastruktury informatycznej

Załącznik Nr 3 do Zarządzenia Nr 78/2011
Burmistrza Drawska Pomorskiego
z dnia 25 maja 2011r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE MIEJSKIM W DRAWSKU POMORSKIM

Podstawa prawna:

1. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926, ze zm.).
2. Rozporządzenie 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. z 2004 r. Nr 100, poz. 1024)

Administratorem Danych Osobowych w Urzędzie Miejskim w Drawsku Pomorskim jest Burmistrz Drawska Pomorskiego.

Administrator Danych Osobowych zobowiązuje wszystkich pracowników Urzędu do przestrzegania postanowień tej instrukcji.

Spis treści

1. Postanowienia ogólne 3

2. Procedury nadawania i zmiany uprawnień do przetwarzania danych, rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności 4

3. Stosowane metody i środki uwierzytelniania użytkownika oraz procedury związane z ich zarządzaniem i użytkowaniem 6

4. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu 7

5. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania 8

6. Sposób, miejsce i okres przechowywania elektronicznych nośników danych zawierających dane osobowe oraz kopii zapasowych 8

7. Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego 10

8. Ochrona przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej 11

9. Udostępnianie danych osobowych i sposób odnotowywania informacji o udostępnianiu danych 11

10. Wykonywanie przeglądów i konserwacji systemu oraz nośników danych służących do przetwarzania danych 12

11. Szczegółowe zasady korzystania ze sprzętu komputerowego i systemów informatycznych, poczty elektronicznej oraz Internetu 13

12. Lista załączników 13

1. Postanowienia ogólne

1. „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Drawsku Pomorskim", zwana dalej "Instrukcją", określa procedury dotyczące zasad bezpieczeństwa przetwarzania danych osobowych oraz zasady postępowania Administratora Danych Osobowych, osób przez niego wyznaczonych i użytkowników systemu, przetwarzających dane osobowe w Urzędzie Miejskim w Drawsku Pomorskim, zwanego dalej "Urzędem".
2. Burmistrz Drawska Pomorskiego wykonuje obowiązki Administratora Danych Osobowych w odniesieniu do prowadzonych w Urzędzie zbiorów danych.
3. Administrator Danych Osobowych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
3. W celu zrealizowania tych obowiązków Administrator Danych Osobowych wprowadza „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Drawsku Pomorskim" jako dokument, którego stosowanie obowiązuje wszystkich pracowników Urzędu.
4. Administrator Danych Osobowych wyznacza:
    a. Administratora Bezpieczeństwa Informacji, który z jego upoważnienia nadzoruje przestrzeganie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych na terenie Urzędu. Administratorem Bezpieczeństwa Informacji w Urzędzie Miejskim w Drawsku Pomorskim jest Paweł Górzyński.
    b. Administratora Systemu Informatycznego, który jest odpowiedzialny za funkcjonowanie systemu teleinformatycznego oraz stosowanie technicznych i organizacyjnych środków ochrony stosowanych w tym systemie. Administratorem Systemu Informatycznego w Urzędzie Miejskim w Drawsku Pomorskim jest Mirosław Hnatewicz.
5. W systemie informatycznym Urzędu, służącym do przetwarzania danych osobowych, stosuje się środki bezpieczeństwa na poziomie wysokim (warunek konieczny – przynajmniej jedno urządzenie systemu informatycznego służącego do przetwarzania danych osobowych połączone jest z siecią publiczną).
6. Przetwarzanie danych osobowych to wykonywanie na nich operacji, takich jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie (zarówno w systemie informatycznym, jak i ręcznie).
7. Przebywanie w pomieszczeniach znajdujących się wewnątrz obszaru, w którym przetwarzane są dane osobowe osób nieuprawnionych do dostępu do danych

osobowych jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych.

8. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane w sposób uniemożliwiający dostęp do nich osób trzecich, na czas nieobecności w nich osób zatrudnionych.
9. Dostęp do danych osobowych mogą mieć jedynie osoby do tego upoważnione.

2. Procedury nadawania i zmiany uprawnień do przetwarzania danych, rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:
   a. Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.),
   b. Polityką Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Miejskim w Drawsku Pomorskim,
   c. niniejszym dokumentem.
2. Zapoznanie się z powyższymi informacjami pracownik potwierdza własnoręcznym podpisem na wykazie, którego wzór stanowi Załącznik Nr 1a oraz oświadczeniu, którego wzór stanowi Załącznik nr 1b.
3. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, mogą zostać dopuszczone, z zastrzeżeniem ust. 4, wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych, wydane przez Administratora Danych Osobowych.
4. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, mogą zostać dopuszczone również osoby, którym udzielono upoważnień do przetwarzania danych osobowych na podstawie porozumień zawartych w sprawie powierzenia przetwarzania danych osobowych.
5. Wydanie upoważnienia oraz rejestracja użytkownika w systemie informatycznym przetwarzającym dane osobowe następuje na wniosek Administratora Bezpieczeństwa Informacji, zatwierdzony przez Administratora Danych Osobowych.
6. Procedury wydawania i odwoływania upoważnień dla użytkowników do przetwarzania danych osobowych realizowane są według następujących zasad:
   a. Administrator Bezpieczeństwa Informacji, w porozumieniu z bezpośrednim przełożonym użytkownika, składa do Administratora Danych Osobowych pisemny wniosek o wydanie upoważnienia (Załącznik nr 2), który zawiera:
      - imię i nazwisko użytkownika,

- stanowisko zajmowane przez użytkownika,
- nazwę zbioru danych osobowych oraz nazwę systemu informatycznego, do którego użytkownik będzie miał dostęp,
- poziom uprawnień do poszczególnych systemów informatycznych oraz zbiorów tradycyjnych,
- datę, z jaką upoważnienie ma być wydane,
- okres ważności upoważnienia;

b. Po uzyskaniu akceptacji Administrator Danych Osobowych wydaje upoważnienie do przetwarzania danych osobowych wg. wzoru określonego w załączniku nr 3.

c. Upoważnienie w 3 egzemplarzach zostaje przekazane:
   - 1 egz. do akt osobowych pracownika,
   - 2 egz. dla upoważnionego pracownika,
   - 3 egz. dla Administratora Bezpieczeństwa Informacji.

7. Przyznanie uprawnień do przetwarzania danych osobowych w systemie informatycznym polega na wprowadzeniu do systemu identyfikatora (loginu), tymczasowego hasła oraz ustanowienia zakresu dostępnych programów, danych i operacji dla każdego użytkownika.
8. Za przydzielenie i wygenerowanie identyfikatora i hasła użytkownikowi, który po raz pierwszy korzysta z systemu informatycznego, odpowiada Administrator Systemu Informatycznego .
9. Wyrejestrowania użytkownika z systemu informatycznego dokonuje Administrator Systemu Informatycznego po uzyskaniu zgody Administratora Danych Osobowych.
10. W przypadku, gdy osoba traci trwale upoważnienie do przetwarzania danych osobowych, na wniosek bezpośredniego przełożonego zatwierdzony przez Administratora Danych Osobowych, Administrator Systemu Informatycznego usuwa jego konto z systemu po wcześniejszym zabezpieczeniu stosownych danych. W przypadku czasowej utraty upoważnienia, konto zostaje zablokowane, co również uniemożliwia zalogowanie.
11. Identyfikator użytkownika nie może być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego - nie może być przydzielany innej osobie.
12. Użytkownik systemu informatycznego nie może mieć nadanych uprawnień administratora.
13. Przełożeni użytkowników zobowiązani są pisemnie informować Administratora Danych Osobowych lub Administratora Bezpieczeństwa Informacji o każdej zmianie dotyczącej użytkowników, mającej wpływ na zakres posiadanych uprawnień do przetwarzania danych osobowych.
14. Administrator Bezpieczeństwa Informacji jest zobowiązany do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych (załącznik nr 4 do instrukcji).
15. Jeśli specyfika programu stosowanego do przetwarzania danych osobowych tego wymaga, nadawane są dodatkowe hasła dostępu.

16. Pracownik zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest do zachowania ich w tajemnicy. Tajemnica obowiązuje go również po ustaniu zatrudnienia.
17. Administrator Systemu Informatycznego musi posiadać prawa administracyjne umożliwiające dokonanie zmian praw innych użytkowników.

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

1. Użytkownik uzyskuje dostęp do danych osobowych przetwarzanych w systemie informatycznym wyłącznie po podaniu identyfikatora i hasła.
2. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik jest odpowiedzialny za wszystkie czynności wykonane przy użyciu swojego identyfikatora.
3. Identyfikator składa się minimalnie z 6 znaków, które nie są rozdzielone spacjami ani znakami interpunkcyjnymi. Identyfikator jest tworzony przy użyciu małych liter, z wyłączeniem polskich znaków.
4. Użytkownik, z chwilą przystąpienia do pracy w systemie informatycznym, otrzymuje hasło początkowe i jest zobowiązany zmienić je natychmiast po rozpoczęciu pracy, na sobie tylko znany ciąg znaków.
5. Hasło składa się co najmniej z 8 znaków.
6. Hasło powinno zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
7. System informatyczny wyposażony jest w mechanizmy wymuszające zmianę hasła po upływie 30 dni od dnia ostatniej jego zmiany.
8. W sytuacji gdy system informatyczny nie wymusza okresowej zmiany hasła, za jego zmianę co 30 dni odpowiada użytkownik.
9. Kolejne hasła nie mogą się powtarzać (do 12 haseł wstecz).
10. Hasło nie może być zapisane w miejscu dostępnym dla osób nieuprawnionych i należy je zachować w tajemnicy, również po upływie jego ważności.
11. Użytkownik nie może udostępniać osobom nieuprawnionym swojego identyfikatora oraz hasła.
12. Po uwierzytelnieniu w systemie, użytkownik nie może udostępniać osobom nieuprawnionym swojego stanowiska pracy.
13. Jeśli istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest niezwłocznie je zmienić oraz powiadomić o tym fakcie Administratora Bezpieczeństwa Informacji.
14. W systemach informatycznych służących do przetwarzania danych osobowych stosuje się środki bezpieczeństwa na poziomie wysokim.

4. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

1. Użytkownik, rozpoczynając pracę na komputerze, loguje się do systemu informatycznego.
2. Dostęp do danych osobowych możliwy jest jedynie po dokonaniu uwierzytelnienia użytkownika.
3. Maksymalna liczba prób wprowadzenia hasła przy logowaniu się do systemu informatycznego wynosi 5. Po przekroczeniu tej liczby prób logowania, system blokuje dostęp do zbioru danych na poziomie danego użytkownika. Odblokowania dostępu do zbioru danych może dokonać Administrator Systemu Informatycznego w porozumieniu z Administratorem Bezpieczeństwa Informacji.
4. W przypadku braku aktywności użytkownika na komputerze przez czas dłuższy niż 10 minut, następuje automatyczne włączenie wygaszacza ekranu.
5. W przypadku braku aktywności użytkownika na komputerze przez czas dłuższy niż 15 minut następuje automatyczne wylogowanie użytkownika z systemu informatycznego służącego do przetwarzania danych osobowych.
6. Monitory stanowisk komputerowych, na których przetwarzane są dane osobowe, znajdujące się w pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień do przetwarzania danych osobowych, należy ustawić w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
7. Przebywanie osób nieuprawnionych w pomieszczeniach znajdujących się na obszarze, w którym są przetwarzane dane osobowe, jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania.
8. Pomieszczenia, w których przetwarzane są dane osobowe, należy zamykać na czas nieobecności osób upoważnionych, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.
9. Przed opuszczeniem stanowiska pracy użytkownik jest obowiązany:
    a. wylogować się z systemu informatycznego lub
    b. wywołać blokowany hasłem wygaszacz ekranu.
10. Kończąc pracę użytkownik jest obowiązany:
    a. wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,
    b. zabezpieczyć stanowisko pracy.
11. Wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe, użytkownicy systemu przechowują w szafach zamykanych na klucz.

5. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu, poprzez tworzenie kopii zapasowych.
2. Całościowa archiwizacja zbiorów danych osobowych znajdujących się na serwerach wykonywana jest jeden raz w tygodniu i zapisywana na zewnętrzną macierz dyskową oraz zaszyfrowany dysk zewnętrzny.
3. Kopie danych, o których mowa w ust.1 wykonuje Administrator Systemu Informatycznego lub osoba przez niego upoważniona.
4. W przypadku lokalnego przetwarzania danych osobowych na służbowych komputerach, użytkownicy systemu informatycznego zobowiązani są do centralnego przechowywania kopii danych, tak aby możliwe było zabezpieczenie ich dostępności poprzez wykonanie kopii zapasowych.
5. Przez centralne przechowywanie kopii danych rozumie się cotygodniowe przegrywanie zbioru danych na specjalnie wydzielony do tego celu obszar dysku na serwerze.
6. Kopie zapasowe zbiorów danych skopiowanych z serwera należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu informatycznego. Za przeprowadzanie tej procedury odpowiedzialny jest Administrator Systemu Informatycznego .
7. Próby odtwarzania danych muszą zostać udokumentowane poprzez wpis w Dzienniku Administratora stanowiący załącznik Nr 5.
8. Kopie zapasowe wykonywane są zgodnie z następującym harmonogramem:
   a. kopia zapasowa bazy Gmina2 oraz baz QNT (program kadrowo-płacowy) wykonywana codziennie w godzinach nocnych od poniedziałku do piątku na zewnętrzną macierz dyskową;
   b. kopia zapasowa wszystkich serwerów wirtualnych wykonywana jeden raz w tygodniu na zewnętrzną macierz dyskową oraz po kompresji i zaszyfrowaniu na dysk zewnętrzny, który jest przechowywany w siedzibie ZWiK w Drawsku Pom. przy ul. Podmiejskiej 3.

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

1. Nośniki z danymi przechowywane są w ognioodpornej kasie metalowej, w pomieszczeniu, do którego wyłączny dostęp ma Administrator Bezpieczeństwa Informacji, Administrator Systemu Informatycznego lub osoba przez niego upoważniona.
2. Użytkownicy nie mogą wynosić z terenu Urzędu nośników danych z zapisanymi danymi osobowymi, bez zgody Administratora Danych Osobowych lub Administratora Bezpieczeństwa Informacji.
3. Dostęp do nośników z kopiami zapasowymi danych osobowych mają wyłącznie Administrator Bezpieczeństwa Informacji oraz Administrator Systemu Informatycznego .
4. Usunięcie danych z nośników danych powinno zostać zrealizowane przy pomocy oprogramowania przeznaczonego do bezpiecznego usuwania danych z nośnika danych.
5. Za zniszczenie kopii zapasowych sporządzanych indywidualnie przez użytkownika odpowiada użytkownik.
6. Dane osobowe w postaci elektronicznej należy usuwać z nośnika danych w sposób uniemożliwiający ich ponowne odtworzenie, nie później niż po upływie 5 dni po wykorzystaniu tych danych, chyba że z odrębnych przepisów wynika obowiązek ich przechowywania.
7. Nośniki danych podlegają komisyjnemu zniszczeniu 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. Z przeprowadzonych czynności komisja sporządza protokół, a Administrator Systemu Informatycznego odnotowuje ten fakt w Dzienniku Administratora.
8. Przez zniszczenie nośników danych należy rozumieć ich trwałe i nieodwracalne zniszczenie fizyczne do stanu uniemożliwiającego ich rekonstrukcję i odzyskanie danych.
9. Dyski twarde komputerów wycofanych z eksploatacji są komisyjnie demontowane, metalowe talerze magnetyczne są cięte mechanicznie na minimum 4 części.

7. Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1. Za ochronę antywirusową systemu informatycznego odpowiada Administrator Systemu Informatycznego .
2. System antywirusowy zainstalowany jest w każdym komputerze z dostępem do danych osobowych. Ustawienie poziomu bezpieczeństwa i wysyłanie aktualizacji bazy sygnatur wirusów zarządzane jest centralnie.
3. Skanowanie serwerów wykonywane jest co najmniej raz w tygodniu przez Administratora Systemu Informatycznego lub osobę przez niego upoważnioną.
4. Skanowanie stacji roboczych wykonują ich użytkownicy.
5. Użytkownicy systemu mają również obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, a także plików danych pobieranych z zasobów sieci Internet oraz otrzymanych na pocztę elektroniczną.
6. Programy antywirusowe są uaktywnione przez cały czas pracy każdego komputera w systemie informatycznym.
7. Wszystkie pliki otrzymywane z zewnątrz, jak również wysyłane na zewnątrz, podlegają automatycznemu sprawdzeniu przez system antywirusowy pod kątem występowania wirusów, z zastosowaniem najnowszej dostępnej wersji programu antywirusowego.
8. W przypadku pojawienia się wirusa, użytkownik obowiązany jest zaprzestać wykonywania jakichkolwiek czynności w systemie i niezwłocznie powiadomić o tym fakcie Administratora Systemu Informatycznego lub Administratora Bezpieczeństwa Informacji.
9. Niedozwolone jest otwieranie wiadomości poczty elektronicznej i załączników od „niezaufanych" nadawców.
10. Niedozwolone jest wyłączanie, blokowanie i odinstalowywanie programów zabezpieczających komputer przed oprogramowaniem złośliwym oraz nieautoryzowanym dostępem (skaner antywirusowy, firewall).
11. Każda jednostka komputerowa jest zabezpieczona hasłem do BIOS.
12. Administrator Systemu Informatycznego jest odpowiedzialny za aktywowanie i poprawne konfigurowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku:
    1) sieci lokalnej i rozległej,
    2) stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej.
13. Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona monitoruje stan systemu, ruch użytkowników w sieci oraz próby ingerencji z zewnątrz w system.

8. Ochrona przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej

1. System, w którym przetwarzane są dane osobowe powinien posiadać mechanizmy pozwalające zabezpieczyć je przed ich utratą lub nieautoryzowaną zmianą spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
2. Dane osobowe przetwarzane w systemie informatycznym chroni się stosując filtry zabezpieczające przed skutkami spadku napięcia oraz urządzenia podtrzymujące zasilanie sieciowe 230 V do momentu poprawnego zapisania danych i zamknięcia przez użytkownika systemu komputerowego.
3. Dane osobowe przetwarzane z wykorzystaniem lokalnych serwerów Urzędu Miejskiego w Drawsku Pomorskim zabezpieczone są przed utratą, poprzez zastosowanie urządzenia podtrzymującego napięcie (UPS), skonfigurowanego w ten sposób, aby po wyznaczonym czasie zależnym od poziomu ilości energii w akumulatorach, system został zamknięty automatycznie.
4. Urządzenia wchodzące w skład systemu informatycznego podłączone są do odrębnego obwodu elektrycznego.

9. Udostępnianie danych osobowych i sposób odnotowywania informacji o udostępnianiu danych

1. Dane osobowe przetwarzane w Urzędzie mogą być udostępnione osobom lub podmiotom uprawnionym do ich otrzymania, na mocy Ustawy o Ochronie Danych Osobowych oraz innych przepisów powszechnie obowiązujących.
2. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepisy odrębne stanowią inaczej.
3. Dane udostępnione Urzędowi przez inny podmiot można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
4. Tworzy się centralną ewidencję udostępniania danych prowadzoną w formie elektronicznej oraz papierowej, która w szczególności powinna zawierać co najmniej następujące pola: nazwa odbiorcy, data udostępnienia, zakres udostępnienia. Wzór ewidencji stanowi Załącznik nr 6.
5. Ewidencję, o której mowa w pkt. 4, prowadzi Administrator Bezpieczeństwa Informacji.
6. Kierownicy komórek organizacyjnych są zobowiązani do tego, aby o fakcie udostępniania danych informować Administratora Bezpieczeństwa Informacji, który dokonuje odpowiednich zapisów w ewidencji. o której mowa w pkt 1.
7. Zgodę na udostępnienie danych osobowych wyraża Administrator Danych Osobowych, poprzez złożenie podpisu pod pismem przygotowanym przez pracownika merytorycznego.

10. Wykonywanie przeglądów i konserwacji systemu oraz nośników danych służących do przetwarzania danych

1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe mogą być wykonywane przez Administratora Systemu Informatycznego
2. Administrator Systemu Informatycznego okresowo sprawdza możliwość odtworzenia danych z kopii zapasowej. Częstotliwość wykonywania procedury odtwarzania danych jest uzgadniana z Administratorem Bezpieczeństwa Informacji.
3. Aktualizacja oprogramowania powinna być przeprowadzana zgodnie z zaleceniami producentów oraz opinią rynkową, co do bezpieczeństwa i stabilności nowych wersji.
4. Za terminowość przeprowadzania przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada Administrator Systemu Informatycznego
5. Nieprawidłowość w działaniu systemu informatycznego oraz oprogramowania są niezwłocznie usuwane przez Administratora Systemu Informatycznego, a ich przyczyny analizowane.
6. Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jego lokalizacji, może być dokonana tylko przez Administratora Systemu Informatycznego.
7. Dokonanie istotnych zmian w systemie informatycznym przez Administratora Systemu Informatycznego, polegających na:
   a. zmianie oprogramowania w systemie,
   b. zmianie lokalizacji składników systemu,
   c. zmianie uregulowań określonych w niniejszej instrukcji

   wymaga uzgodnienia z Administratorem Bezpieczeństwa Informacji.

11. Szczegółowe zasady korzystania ze sprzętu komputerowego i systemów informatycznych, poczty elektronicznej oraz Internetu

Szczegółowe zasady korzystania ze sprzętu komputerowego i systemów informatycznych, poczty elektronicznej oraz Internetu określa Regulamin Użytkownika Systemów Teleinformatycznych Urzędu Miejskiego w Drawsku Pomorskim, który stanowi załącznik Nr 7 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Drawsku Pomorskim.

12. Lista załączników

Załącznik Nr 1a –Wykaz osób, które zostały zapoznane z „Polityką Bezpieczeństwa Danych" i „Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Drawsku Pomorskim"

Załącznik Nr 1b - Oświadczenie

Załącznik Nr 2 – Wniosek o nadanie, modyfikację lub odebranie uprawnień do przetwarzania danych osobowych

Załącznik Nr 3 – Upoważnienie do przetwarzania danych osobowych

Załącznik Nr 4 – Ewidencja osób upoważnionych do przetwarzania danych osobowych i ich uprawnień w systemie informatycznym

Załącznik Nr 5 – Dziennik Administratora

Załącznik Nr 6– Ewidencja udostępnionych danych

Załącznik Nr 7 - Regulamin użytkownika systemów teleinformatycznych Urzędu Miejskiego w Drawsku Pomorskim

Załącznik Nr 1a do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Drawsku Pomorskim

WYKAZ OSÓB, KTÓRE ZOSTAŁY ZAPOZNANE Z „POLITYKĄ BEZPIECZEŃSTWA DANYCH" I „INSTRUKCJĄ ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE MIEJSKIM W DRAWSKU POMORSKIM"

Lp.	Imię i nazwisko	Stanowisko	Data	Podpis

Załącznik Nr 1b do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Drawsku Pomorskim

OŚWIADCZENIE

.....

(imię i nazwisko)

Niniejszym oświadczam, że:

1. Zapoznałam(-em) się z obowiązującymi w Urzędzie Miejskim w Drawsku Pomorskim przepisami, dotyczącymi bezpieczeństwa systemów informatycznych i ochrony danych osobowych.
2. Jestem świadomy odpowiedzialności karnej, o której mowa w artykułach: 278 § 2, 293 w związku z 291 oraz art. 292 ustawy z dnia 6 czerwca 1997 r. kodeks karny (tekst jednolity - Dz. U. z 1997 r., Nr 88, póz. 553, ze zmianami) oraz odpowiedzialności karnej i cywilnej przewidzianej w artykułach: 74, 79, 115, 116, 117, 118, 118(1) ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (tekst jednolity - Dz. U. z 2000, Nr 80, póz. 904, ze zmianami) za niezgodne z prawem korzystanie, rozpowszechnianie, utrwalanie, uzyskiwanie lub zwielokrotnianie oprogramowania oraz wszelkich utworów muzycznych, filmowych etc.
3. Zobowiązuję się do zachowania tajemnicy służbowej, a przede wszystkim do nieujawniania nikomu, prócz osobie do tego powołanej, żadnych wiadomości ani informacji poufnych dotyczących haseł dostępu do systemów informatycznych, zakładu pracy, jego sytuacji finansowej lub interesów oraz kontrahentów, które poznam w czasie swego zatrudnienia i w związku z nim.
4. Zobowiązuję się do zachowania poufności udostępnionych danych osobowych, na podstawie rozdz. 8 Ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zmianami)
5. Zobowiązuję się do przestrzegania powyższych zobowiązań.
6. Za brak przestrzegania powyższych zobowiązań mogą być wyciągane surowe konsekwencje, zgodnie z przepisami prawa wymienionymi w pkt. 2, aż do art. 52 Kodeksu Prawa Pracy włącznie.

....

(miejscowość , data) (czytelny podpis pracownika)

Otrzymują:

1. Pracownik
2. Dział kadr (do akt osobowych)
3. Administrator Bezpieczeństwa Informacji

Załącznik Nr 2 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Drawsku Pomorskim

Drawsko Pomorskie, dnia.....

WNIOSEK O NADANIE, MODYFIKACJĘ LUB ODEBRANIE UPRAWNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH

Nadanie uprawnień nowej osobie	**Modyfikacja uprawnień**	**Odebranie uprawnień**

Imię i nazwisko użytkownika:	**Referat/stanowisko zajmowane przez użytkownika:**

Nazwa zbioru (ów) danych osobowych oraz nazwa systemu informatycznego, do którego użytkownik będzie miał dostęp:

Zakres uprawnień do przetwarzania danych:		
Lp.	Nazwa aplikacji / Zbiór tradycyjny	Uprawnienia

Identyfikator użytkownika ***[wypełnia się, jeżeli dane przetwarzane są w systemie informatycznym]:***

Data nadania i okres ważności upoważnienia:	**Podpis Administratora Bezpieczeństwa Informacji:**

Załącznik Nr 3 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim Drawsku Pomorskim

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Drawsko Pomorskie, dnia.....

UPOWAŻNIENIE NR ...../.....

Z dniem ..... upoważniam Panią/Pana .....

zatrudnioną/ego na stanowisku .....do przetwarzania danych osobowych:

Nazwa zbioru (ów) danych osobowych oraz nazwa systemu informatycznego, do którego użytkownik będzie miał dostęp:		
Zakres uprawnień do przetwarzania danych:		
Lp	Nazwa aplikacji / Zbiór tradycyjny	Uprawnienia
Identyfikator użytkownika [wypełnia się, jeżeli dane przetwarzane są w systemie informatycznym]:		
Okres ważności upoważnienia:	**Podpis Administratora Danych Osobowych**	

Zatwierdzam i zobowiązuję Administratora Systemu Informatycznego do przyznania uprawnień do przetwarzania danych osobowych w systemie informatycznym zgodnie z upoważnieniem.

1 egz. do akt osobowych pracownika, 2 egz. dla upoważnionego pracownika,

3 egz. dla Administratora Bezpieczeństwa Informacji

Załącznik Nr 4 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Drawsku Pomorskim

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH I ICH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

Lp.	Imię i nazwisko	Data nadania upoważnienia	Data ustania upoważnienia	Zakres uprawnień do przetwarzania danych		**Identyfikator**
				Nazwa aplikacji / Zbiór tradycyjny	Uprawnienia	

Załącznik Nr 5 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Drawsku Pomorskim

DZIENNIK ADMINISTRATORA

Lp.	Data	Godzina	Opis wydarzenia w systemie	Podpis administratora	Uwagi

Załącznik Nr 6 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Drawsku Pomorskim

EWIDENCJA UDOSTĘPNIONYCH DANYCH

Lp.	Data udostępnienia danych	Podmiot, któremu udostępniono dane	Podstawa prawna udostępniania danych	Zakres udostępnionych danych	Podpis pracownika

Załącznik Nr 7 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Drawsku Pomorskim

REGULAMIN UŻYTKOWNIKA SYSTEMÓW TELEINFORMATYCZNYCH URZĘDU MIEJSKIEGO W DRAWSKU POMORSKIM

§1. Zasady korzystania ze sprzętu komputerowego i systemów informatycznych:

1) Użytkownik zobowiązany jest do bezterminowego zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić Pracodawcę na szkodę.

2) Tworzenie kont w systemach, nadawanie, modyfikacja oraz usunięcie uprawnień, instalacja lub deinstalacja oprogramowania, grupowa instalacja lub deinstalacja, wydanie lub przekonfigurowanie sprzętu odbywa się na pisemny wniosek osoby zainteresowanej. Wnioski realizowane są przez Administratora Systemu Informatycznego po wydaniu zgody przez Administratora Bezpieczeństwa Informacji i zatwierdzeniu przez Administratora Danych Osobowych.

3) Sprzęt komputerowy oraz zainstalowane na nim oprogramowanie, jakie zostało oddane użytkownikowi w okresie jego pracy są wykorzystywane tylko do celów służbowych.

4) Użytkownik dba o powierzony mu sprzęt oraz chroni go przed szkodliwym wpływem warunków zewnętrznych.

5) Użytkownik zabezpiecza w miarę posiadanych możliwości sprzęt przed kradzieżą.

6) Hasła użytkowników do systemów podlegają następującym zasadom:

   a) hasło składa się z minimum 8 znaków, przy czym zawiera wielkie i małe litery oraz cyfry lub znaki specjalne,
   b) hasło musi być zmieniane minimum co 30 dni,
   c) kolejne hasła muszą być różne,
   d) hasła należy przechowywać w sposób gwarantujący ich poufność,
   e) zabrania się udostępniania haseł innym osobom.

7) Zabrania się tworzenia haseł na podstawie:

   a) cech i numerów osobistych (np. dat urodzenia, imion itp.),
   b) sekwencji klawiszy klawiatury (np. qwerty, 12qwaszx),
   c) identyfikatora użytkownika,
   d) innych haseł łatwych do odgadnięcia.

8) Użytkownicy nie mogą udostępniać innym osobom indywidualnych identyfikatorów (nazwa użytkownika, token, karta inteligentna i inne dane umożliwiające uwierzytelnienie).

9) Użytkownik zobowiązany jest przestrzegać zasady „czystego biurka" i „czystego ekranu". Stosowanie tych zasad sprowadza się do:
   a) schowania wszystkich dokumentów, nośników danych, związanych z informacjami chronionymi w miejsce niedostępne dla innych osób po zakończeniu pracy,
   b) odchodząc od stacji roboczej, użytkownik blokuje komputer, uniemożliwiając zalogowanie się do systemu osobie nieuprawnionej,
   c) kończąc pracę użytkownik zamyka wszystkie aplikacje, wylogowuje się z systemu i wyłącza komputer.

10) Zabrania się użytkownikom uruchamiać (mowa również o aplikacjach przenośnych ang. portable) i instalować na sprzęcie służbowym jakiegokolwiek oprogramowania. Instalacji oprogramowania dokonuje Administrator Systemu Informatycznego, na podstawie pisemnych wniosków.

11) Zabrania się użytkownikom:

   a) omijania mechanizmów kontroli (np. używania serwerów Proxy),
   b) testowania wdrożonych zabezpieczeń,
   c) skanowania urządzeń sieciowych, serwerów oraz stacji roboczych pod kątem badania świadczonych usług,
   d) wyłączania programów uruchamianych automatycznie przy starcie systemu,
   e) odinstalowania programów,
   f) dezaktywacji oprogramowania antywirusowego,
   g) przyłączania i użytkowania prywatnego sprzętu, w tym używania prywatnych nośników danych,
   h) podejmowania jakichkolwiek prób ingerencji w sprzęt komputerowy, poza czynnościami związanymi z codzienną eksploatacją.

12) Ważne pliki należy przechowywać w wyznaczonych folderach na serwerach, które gwarantują bezpieczeństwo danych.

13) Za bezpieczeństwo danych przechowywanych lokalnie na komputerze odpowiada użytkownik.

14) Zabrania się przechowywania na sprzęcie służbowym gier oraz plików multimedialnych np. filmów, obrazów, dźwięków nie związanych z zadaniami służbowymi.

15) Na sprzęcie komputerowym instaluje się oprogramowanie do ilościowej jak i jakościowej kontroli użytkowników, które stosuje się w celu okresowej kontroli wykorzystania sprzętu służbowego przez użytkowników. Oprogramowanie to zbiera informacje m.in. na temat:

a. odwiedzanych stron internetowych,
b. wykorzystywanych aplikacji,
c. drukowanych dokumentów,
d. wysyłanych e-maili (bez wglądu w ich treść),
e. czasie przerw w wykorzystywaniu komputera.

16) W przypadku używania zewnętrznych nośników danych na stacji roboczej użytkownik wcześniej wykonuje skanowanie programem antywirusowym wszystkich danych na nośniku.

17) W przypadku gdy użytkownik wykryje zainfekowane dane niezależnie od źródła (np. strona internetowa, załącznik poczty elektronicznej, dane na nośniku) bezzwłocznie powiadamia o tym fakcie Administratora Systemu Informatycznego.

18) Zabrania się użytkownikom samodzielnego przenoszenia i podłączania sprzętu teleinformatycznego między stanowiskami pracy. Czynności te wykonuje Administrator Systemu Informatycznego.

19) Kończąc świadczenie pracy dla Pracodawcy, użytkownik ma obowiązek przekazać wszystkie dane (dokumenty papierowe, pliki oraz inne posiadane informacje) związane z wykonywanymi zadaniami służbowymi przełożonemu.

§2.Zasady korzystania z poczty elektronicznej:

1) Nadzór i opiekę techniczną nad systemem poczty elektronicznej sprawuje Administrator Systemu Informatycznego. Użytkownik zobowiązany jest do sprawdzania własnej skrzynki poczty elektronicznej.
2) Poczta elektroniczna jest wykorzystywana tylko do celów służbowych.
3) zabrania się rozsyłania m.in.:
   a) ogłoszeń komercyjnych,
   b) tzw. łańcuszków szczęścia (listów, które wykorzystując elementy socjotechniki, generują niepożądany ruch na serwerach poczty elektronicznej),
   c) treści wulgarnych,
   d) materiałów erotycznych,
   e) treści niezgodnych z obowiązującymi przepisami prawa,
   f) treści prawem chronionych bez odpowiedniego zabezpieczenia np. szyfrowanie;
4) Korespondencja, którą przechowuje i dostarcza system pocztowy jest własnością Pracodawcy.
5) Pracodawca w celach dowodowych oraz bezpieczeństwa systemów ma prawo do kontroli skrzynek pocztowych użytkowników. O wynikach kontroli powinien być poinformowany użytkownik.
6) Nie należy otwierać linków oraz załączników poczty elektronicznej ze źródeł niewiadomego pochodzenia.

7) W przypadku dostępu do poczty elektronicznej z sieci Internet należy przeczytać uważnie pojawiające się w przeglądarce komunikaty o alertach bezpieczeństwa i nigdy nie ignorować ostrzeżeń.

8) Nie zaleca się logowania do systemów poczty elektronicznej z komputerów dostępnych publicznie (np. kafejki internetowe).

9) Skrzynki pocztowe posiadają ograniczoną wielkość. Użytkownik zobowiązany jest do okresowej archiwizacji wiadomości.

10) Zabrania się korzystania ze skrzynek prywatnych w miejscu pracy, a w szczególności używania ich do prowadzenia korespondencji urzędowej i wysłania jakichkolwiek załączników służbowych.

§3. Zasady korzystania z Internetu.

1) Użytkownicy korzystają z dostępu do Internetu tylko w celach służbowych.

2) Praca w sieci Internet nie może zagrażać bezpieczeństwu systemów informatycznych.

3) Pracodawca może wprowadzić kategoryzację stron internetowych oraz zablokować dostęp do wybranych kategorii.

4) Odblokowanie witryny internetowej może nastąpić na pisemny wniosek kierownika komórki organizacyjnej.

5) Zabrania się:

   a) wykorzystywania sieci Internet w sposób, który mógłby narazić Pracodawcę na utratę dobrego imienia,
   b) pobierania oprogramowania (w tym w wersjach darmowych), nie związanego z wykonywanymi obowiązkami służbowymi,
   c) podłączania sieci Internet do fizycznie odseparowanych sieci,
   d) udostępniania łącza internetowego dostarczonego przez pracodawcę innym osobom bez zgody kierownika komórki organizacyjnej oraz Administratora Systemu Informatycznego,
   e) instalowania urządzeń udostępniających Internet na sprzęcie Pracodawcy bez zgody kierownika komórki organizacyjnej oraz Administratora Systemu Informatycznego.

§4. Sankcje karne

1. W przypadku korzystania ze sprzętu komputerowego i oprogramowania pracodawcy w sposób sprzeczny z postanowieniami Regulaminu pracodawca ma prawo nakładać kary porządkowe — upomnienie lub naganę na podstawie art. 106 § 1 ustawy z dnia 26.06.1974 r. Kodeks Pracy,

2. W przypadku uporczywego niestosowania się pracownika do postanowień Regulaminu pracodawca może rozwiązać stosunek pracy z pracownikiem w trybie natychmiastowym na podstawie art. 52 ustawy z dnia 26.06.1974 r. Kodeks Pracy,