ZARZĄDZENIE Nr 65/2012
BURMISTRZA MIASTA i GMINY DALESZYCE
z dnia 3 września 2012 r.

w sprawie wdrożenia polityki bezpieczeństwa informacji w Urzędzie Miasta i Gminy w Daleszycach

Na podstawie § 3 ust.1 i 3 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) oraz w związku z art.3 ust.1 i art. 7 ust. 4 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz art. 31 i art. 33 ust. 1 i 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2001 r. Nr 142, poz. 1591 z późn. zm.) zarządza się co następuje:

§1

Wprowadza się do użytku „Politykę bezpieczeństwa informacji w Urzędzie Miasta i Gminy w Daleszycach" stanowiącą załącznik do niniejszego zarządzenia.

§ 2

1. Wykonanie zarządzenia powierza się Kierownikom Referatów Urzędu Miasta i Gminy w Daleszycach oraz osobom na samodzielnych stanowiskach pracy.
2. Nadzór nad wykonaniem zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§ 3

Nadzór nad przestrzeganiem Polityki powierzam informatykowi, wykonującemu czynności Administratora Bezpieczeństwa Informacji w Urzędzie Gminy w Daleszycach.

§ 4

Traci moc Zarządzenie Nr 64/2005 Wójta Gminy Daleszyce z dnia 7 września 2005 r. w sprawie wprowadzenia w Urzędzie Gminy Daleszyce „Instrukcji przetwarzania danych osobowych".

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ

Wojciech Furmanek

Załącznik
do Zarządzenia Nr 65/2012
Burmistrza Miasta i Gminy Daleszyce
z dnia 3.09.2012r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

Daleszyce, wrzesień 2012r.

ROZDZIAŁ I
Przepisy ogólne

§ 1. Polityka bezpieczeństwa informacji, zwana dalej polityką, określa zasady ochrony danych osobowych oraz postępowania w przypadku jej naruszenia przy przetwarzaniu danych osobowych we wszystkich zbiorach danych osobowych Urzędu Miasta i Gminy w Daleszycach, a także zasady pracy z każdym systemem informatycznym służącym do przetwarzania danych osobowych.

Szczegółowy wykaz systemów informatycznych służących do przetwarzania danych osobowych określa administrator danych.

§ 2. Przetwarzanie danych osobowych w Urzędzie Miasta i Gminy w Daleszycach jest dopuszczalne tylko pod warunkiem przestrzegania Ustawy i wydanych na jej podstawie przepisów wykonawczych oraz odpowiednich Zarządzeń Burmistrza Miasta i Gminy Daleszyce, a także innych przepisów regulujących przetwarzanie danych osobowych.

§ 3. Definicje polityki bezpieczeństwa informacji

1) Ustawa – w tym dokumencie rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Gz.U. z 2002 r. Nr 101, poz. 929 z późn. zm.).
2) Urząd – w tym dokumencie jest rozumiany, jako Urząd Miasta i Gminy w Daleszycach z siedzibą na Placu Stanica 9, 26-021 Daleszyce.
3) Rozporządzenie – rozumie się przez to rozporządzenie z dnia 29 kwietnia 2004 r. Ministra Spraw Wewnętrznych i Administracji 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).
4) Zbiór danych, przetwarzanie danych, usuwanie danych – rozumie się przez to objaśnienia określone w art. 7 ust. 1 ustawy.
5) Administrator danych – rozumie się przez to Burmistrza Miasta i Gminy Daleszyce, który decyduje o celach i środkach przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Daleszycach.
6) Administrator bezpieczeństwa informacji – rozumie się przez to pracownika Urzędu wyznaczonego przez administratora danych nadzorującego przestrzeganie zasad ochrony, o których mowa w art. 36 ust. 1 ustawy.
7) Lokalny administrator bezpieczeństwa informacji – rozumie się przez to wyznaczonego przez administratora danych Kierownika Referatu nadzorującego w Referacie przestrzeganie zasad ochrony, o których mowa w art. 36 ust. 1 ustawy.
8) System informatyczny – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
9) Osoby zatrudnione przy przetwarzaniu danych osobowych – rozumie się przez to wszystkie osoby, które przetwarzają dane osobowe w ramach wykonywanych zadań na danym stanowisku w Urzędzie oraz osoby z zewnątrz Urzędu mające dostęp do danych osobowych w ramach prac zleconych, czy realizacji danej umowy,
10) Użytkownik – rozumie się przez to każdą osobę, której przydzielono uprawnienia w określonym przez te uprawnienia zakresie oraz zapewniono fizyczny dostęp do systemu,
11) Kierownik Referatu – rozumie się przez to Kierownika Referatu Urzędu lub kierującego pracą równorzędnej komórki organizacyjnej oraz samodzielne stanowiska pracy,

§ 4. 1. Dostęp do zbioru danych osobowych oraz ich przetwarzania mają tylko osoby upoważnione przez administratora danych i wpisane do ewidencji prowadzonej przez administratora bezpieczeństwa informacji – Załącznik nr 2.

2. Osoby zatrudnione przy przetwarzaniu danych osobowych są zobowiązane do przechowywania danych osobowych we właściwych zbiorach, nie dłużej niż jest to niezbędne dla osiągnięcia celu ich przetwarzania.

3. Osoby zatrudnione przy przetwarzaniu danych osobowych są zobowiązane zachować w tajemnicy dane osobowe oraz sposoby ich zabezpieczania.

§ 5. Osoby zatrudnione przy przetwarzaniu danych osobowych są zobowiązane powiadomić administratora bezpieczeństwa informacji o ewentualnych naruszeniach bezpieczeństwa informacji.

§ 6. Zabrania się przetwarzania w Urzędzie danych wymienionych w art. 27 ust. 1 ustawy, za wyjątkiem dopuszczalnych art. 27 ust. 2 ustawy.

§ 7. Osoba zatrudniona przy przetwarzaniu danych osobowych w Urzędzie, która:

1) Przetwarza w zbiorze danych dane osobowe, do których przetwarzania nie jest upoważniona lub których przetwarzanie jest zabronione albo przetwarza dane osobowe niezgodne z celem stworzenia zbioru danych,
2) Udostępnia lub umożliwia dostęp do danych osobowych osobom nieupoważnionym,
3) Nie zgłasza administratorowi bezpieczeństwa informacji zbiorów danych podlegających rejestracji przez Generalnego Inspektora Ochrony Danych Osobowych,
4) Nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o przysługujących jej prawach,
5) Uniemożliwia osobie, której dane dotyczą, korzystanie z przysługujących jej praw,

podlega odpowiedzialności karnej zgodnie z Ustawą oraz przepisami Ustawy o pracownikach samorządowych i Kodeksu Pracy.

§ 8. Niniejsza polityka reguluje następujące zagadnienia z zakresu systemów informatycznych:

1) Zasady eksploatacji systemów informatycznych,
2) Bezpieczeństwo systemów informatycznych,
3) Zasady dostępu do systemów informatycznych,
4) Procedury rozpoczęcia i zakończenia pracy w systemach informatycznych,
5) Zasady tworzenia i przechowywania kopii awaryjnych,
6) Zabezpieczenia antywirusowe systemów informatycznych,
7) Zasady postępowania z nośnikami informacji,
8) Zasady komunikacji w sieciach komputerowych,
9) Zasady monitorowania, przeglądu i konserwacji systemów informatycznych,
10) Odpowiedzialność i obowiązki użytkowników systemów informatycznych.

§ 9. Wszystkie osoby zatrudnione przy przetwarzaniu danych osobowych w systemach informatycznych i pozainformatycznych Urzędu, bez względu na zajmowane stanowisko i miejsce pracy oraz charakter stosunku pracy są zobowiązane do postępowania zgodnie z zasadami określonymi w niniejszej polityce.

§ 10. Polecenia osób wyznaczonych przez administratora danych do realizacji zadań w zakresie ochrony informacji i bezpieczeństwa systemu informatycznego muszą być bezwzględnie wykonywane przez wszystkich użytkowników systemów.

ROZDZIAŁ II
Gromadzenie danych osobowych

§ 11. Dane osobowe przetwarzane w Urzędzie Miasta i Gminy w Daleszycach mogą być uzyskiwane:

1) Bezpośrednio od osób, których te dane dotyczą,
2) Z innych źródeł, w granicach dozwolonych przepisami prawa.

§ 12. 1. Zebrane dane osobowe mogą być wykorzystane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Po wykorzystaniu dane osobowe powinny być przechowywane w postaci uniemożliwiającej identyfikację osób, których dotyczą.

2. W przypadku konieczności udostępnienia dokumentów i danych, wśród których znajdują się dane osobowe nie mające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych osobowych.

ROZDZIAŁ III
Obowiązek informacyjny

§ 13. 1. Kierownicy tych komórek organizacyjnych Urzędu Miasta i Gminy w Daleszycach, które zbierają i przetwarzają dane osobowe, są odpowiedzialni za poinformowanie osób, których dane przetwarzają o:

1) Adresie siedziby urzędu, pod którym dane są zbierane i przetwarzane.
2) Celu zbierania danych, dobrowolności lub obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.
3) Prawie wglądu do treści swoich danych oraz możliwości ich poprawiania.

2. W przypadku zbierania danych osobowych nie bezpośrednio od osoby, której one dotyczą, osobę tę należy poinformować ponadto o:

1) Źródle danych.
2) Uprawnieniach wynikających z art. 32 ust. 1 pkt. 7 i 8 Ustawy.

§ 14. 1. Kandydaci do pracy w Urzędzie w postępowaniu naboru muszą podpisać pisemną zgodę na przetwarzanie danych osobowych do celu rekrutacji.

2. Dokumenty wymienione w ust. 1 są przechowywane przez stanowisko ds. kadr, które przetwarza te dane.

ROZDZIAŁ IV
Udzielanie informacji o przetwarzaniu danych osobowych

§ 15. 1. Osobom, których dane przetwarza się w zbiorze danych Urzędu Miasta i Gminy w Daleszycach, przysługuje zgodnie z Ustawą prawo kontroli ich danych osobowych, a w szczególności prawo do uzyskania wyczerpujących informacji na temat tych danych.

2. Każda osoba, która wystąpi z wnioskiem o otrzymanie informacji, musi otrzymać odpowiedź na piśmie w terminie nieprzekraczającym niż 30 dni od daty wpłynięcia wniosku.

3. Informacja, o której mowa w ust. 1, powinna być udzielana w zrozumiałej formie oraz na piśmie, jeśli osoba o to wnioskuje

§ 16. W przypadku, gdy dane osoby są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem Ustawy, albo są zbędne do realizacji celu, dla którego zostały zebrane, Administrator Danych Osobowych jest zobowiązany do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

ROZDZIAŁ V
Rejestracja zbiorów danych osobowych

§ 17. 1.Kierownicy Referatów, w których przetwarzane są dane osobowe, są zobowiązani do:

1) Przygotowania zgłoszenia zbioru danych do rejestracji lub jego zmian do Generalnego Inspektora Ochrony Danych Osobowych,
2) Uzyskania akceptacji administratora bezpieczeństwa informacji na kopii zgłoszenia,
3) Po podpisaniu przez administratora danych, przekazania zgłoszenia do Generalnego Inspektora Ochrony Danych Osobowych.

2. Kierownicy Referatów prowadzą wydziałowe rejestry zbiorów danych osobowych w systemach informatycznych i nie informatycznych według wzoru stanowiącego załącznik nr 1 do tej instrukcji.

§ 18. 1. Kopie rejestrów Kierownicy Referatów przekazują w formie papierowej oraz na nośniku elektronicznym Administratorowi bezpieczeństwa informacji.

2. Rejestry, o których mowa w ust. 1, Kierownicy Referatów aktualizują, co najmniej raz na kwartał.

§ 19. 1. Administrator bezpieczeństwa informacji na podstawie rejestrów wydziałowych prowadzi zbiorczy rejestr zbiorów danych osobowych w Urzędzie.

2. Administrator bezpieczeństwa informacji sporządza i przekazuje administratorowi danych w okresach półrocznych informację o zbiorach danych osobowych i dokonanych w nich zmianach.

ROZDZIAŁ VI
Ochrona przetwarzania danych osobowych

§ 20. Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane są do stosowania środków organizacyjnych i technicznych zapewniających ochronę przetwarzania danych, w szczególności przed ich udostępnieniem, kradzieżą, uszkodzeniem lub zniszczeniem przez osoby nieupoważnione.

§ 21. 1. Administrator danych wydaje na wniosek Kierownika Referatu indywidualne upoważnienia osobom przetwarzającym dane osobowe z zachowaniem postępowania w sprawie wydawania upoważnień określonego w Regulaminie Organizacyjnym Urzędu.

2. Wydanie upoważnienia następuje po złożeniu przez osobę upoważnianą oświadczenia o zachowaniu w tajemnicy danych osobowych oraz o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych.

3. Wzór oświadczenia o zachowaniu w tajemnicy danych osobowych oraz o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych, składany przez pracowników etatowych oraz pobierany w przyszłości od osób nowozatrudnionych przy przetwarzaniu danych osobowych, określa załącznik nr 3 do niniejszej polityki.

4. Wzór oświadczenia o zachowaniu w tajemnicy danych osobowych oraz o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych składanego przez osoby zatrudnione na podstawie umowy zlecenia, umowy o dzieło lub innej umowy cywilno-prawnej oraz żądania ich przy nowo zawieranych umowach określa załącznik nr 4 do niniejszej polityki.

5. Stanowisko ds. kadr:
1) Niezwłocznie informuje na piśmie administratora bezpieczeństwa informacji o wszelkich zmianach w zatrudnieniu, w tym w szczególności o nawiązaniu i rozwiązaniu stosunku pracy oraz zmianie stanowiska pracy.
2) Uwzględnia rozliczenie pracownika, z którym rozwiązano stosunek pracy, z administratorem bezpieczeństwa informacji w karcie obiegowej.

§ 22. Administrator bezpieczeństwa informacji zobowiązany jest do:
1) Rejestrowania i przechowywania upoważnień, o których mowa w ust. 1,
2) Prowadzenia ewidencji osób zatrudnionych przy przetwarzaniu danych, zgodnie z art. 39 Ustawy. Wzór określa załącznik 5 do niniejszej polityki,
3) Prowadzenia ewidencji oświadczeń. Wzór określa załącznik nr 6 do niniejszej polityki,

4) Nadzorowania Kierowników Referatów lub osób przez nich upoważnionych w zakresie zapoznawania osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami dotyczącymi ochrony danych osobowych.

§ 23. W celu realizacji powierzonych zadań administrator bezpieczeństwa informacji ma prawo:

1) Kontrolować Referaty i samodzielne stanowiska pracy w zakresie właściwego zabezpieczenia systemów informatycznych oraz pomieszczeń, w których przetwarzane są dane osobowe,
2) Wydawać polecenia Kierownikom Referatów w zakresie bezpieczeństwa danych osobowych,
3) Informować administratora danych o przypadkach naruszenia bezpieczeństwa danych osobowych,
4) Żądać od wszystkich pracowników Urzędu wyjaśnień w sytuacjach naruszenia bezpieczeństwa danych osobowych.

ROZDZIAŁ VII
Zasady udostępniania danych osobowych

§ 24. Administrator Danych Osobowych udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

§ 25. 1. Zbiory danych udostępnia się na pisemny, umotywowany wniosek, chyba, że odrębne przepisy prawa stanowią inaczej.

2. Wniosek powinien zawierać informacje, umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie.

3. Wniosek jest rozpatrywany przez Lokalnego Administratora Bezpieczeństwa Informacji lub, w przypadku nieobecności Lokalnego Administratora Bezpieczeństwa Informacji, przez Administratora Bezpieczeństwa Informacji, który jednocześnie prowadzi ewidencję wniosków.

4. Decyzję w sprawie udostępnienia danych podejmuje wyłącznie Lokalny Administrator Bezpieczeństwa Informacji lub, w przypadku nieobecności Lokalnego Administratora Bezpieczeństwa Informacji, Administrator Bezpieczeństwa Informacji.

§ 26. Administrator Danych Osobowych może odmówić udostępnienia danych osobowych, jeżeli:

1. spowodowałoby to istotne naruszenia dóbr osobistych osób, których dane dotyczą lub innych osób.
2. dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania wnioskodawcy.

§ 27. 1. Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej.

2. Podmiot, o którym mowa w ust.1 jest zobowiązany do zastosowania środków organizacyjnych i technicznych, zabezpieczających zbiór przed dostępem osób nieupoważnionych na zasadach określonych w przepisach o ochronie danych osobowych.

3. Podmiot, o którym mowa w ust.1 jest zobowiązany przetwarzać dane osobowe wyłącznie w zakresie, w jakim reguluje to zawarta umowa.

4. W przypadkach opisanych w ust. 1, 2 i 3, odpowiedzialność za ochronę przetwarzanych danych osobowych spoczywa na Administratorze Danych Osobowych, co nie wyłącza w żadnym przypadku odpowiedzialności podmiotu, z którym zawarto umowę, z tytułu przetwarzania danych niezgodnie z ustawą.

5. Przy kontroli zgodności przetwarzanych danych przez upoważniony przez Administratora Danych Osobowych podmiot, o którym mowa w ust. 1, stosuje się odpowiednio przepisy art.14 –19 ustawy.

ROZDZIAŁ VIII
Ochrona pomieszczeń

§ 28. 1. Wszystkie pomieszczenia, w których przetwarzane są dane osobowe w systemach informatycznych Urzędu powinny posiadać drzwi zabezpieczone zamkiem oraz systemy przeciwpożarowe i oznaczone drogi ewakuacji.

2. Przebywanie w pomieszczeniach, o których mowa w ust. 1 osób nieuprawnionych do dostępu do danych osobowych zawartych w systemach informatycznych jest możliwe tylko w obecności użytkownika uprawnionego do korzystania ze sprzętu informatycznego znajdującego się w danym pomieszczeniu.

3. Pomieszczenia, o których mowa w ust. 1 powinny być zamykane na czas nieobecności w nich użytkowników uprawnionych do korzystania ze sprzętu informatycznego znajdującego się w danym pomieszczeniu, w sposób uniemożliwiający dostęp do nich osób trzecich.

§ 29. 1. Pomieszczenia, w których znajdują się newralgiczne elementy sieci komputerowych, a w szczególności serwery sieciowe, serwery aplikacji, serwery baz danych, serwery komunikacyjne, aktywne urządzenia sieciowe, modemy powinny być zabezpieczone w sposób uniemożliwiający dostęp osób nieupoważnionych.

2. Pomieszczenia przewidziane na miejsca dla newralgicznych elementów sieci komputerowych powinny w szczególności:

1) Znajdować się w budynkach objętych całodobową ochroną,
2) Znajdować się w części budynku, gdzie ruch interesantów jest ograniczony,
3) Być oddzielone trwałymi wewnętrznymi ścianami od innych pomieszczeń,
4) Być zaopatrzone, w co najmniej dwa zamki o skomplikowanym mechanizmie otwierania,
5) Posiadać okna odpowiednio zabezpieczone przed dostaniem się z zewnątrz,

3. Administrator bezpieczeństwa informacji może zastosować inne, co najmniej tak samo skuteczne metody zabezpieczeń.

4. Zasady i sposób przechowywania kluczy do pomieszczeń, w których znajdują się newralgiczne elementy sieci komputerowych, określa administrator bezpieczeństwa informacji.

ROZDZIAŁ IX
Przyznawanie praw dostępu

§ 30. 1. Dostęp do pomieszczeń i systemu, w którym przetwarzane są dane osobowe jest przyznawany pisemnie osobom uprawnionym do przetwarzania danych osobowych, które formalnie zobowiązały się do:

1) Zachowania w tajemnicy przetwarzanych danych osobowych oraz informacji dotyczących środków ich przetwarzania,
2) Niewykraczanie poza przyznane uprawnienia.

2. Pracownik przetwarzający dane osobowe w tym systemie potwierdza własnoręcznym podpisem zapoznanie się z indywidualnym zakresem czynności dotyczącym przetwarzania danych. Pracownik podlega szkoleniu w zakresie ochrony danych osobowych gromadzonych i przetwarzanych w systemie.

3. Pracownik otrzymuje pisemne upoważnienie do obsługi systemu w zakresie gromadzenia i przetwarzania danych osobowych podpisane przez Administratora Danych.

4. O zmianie odsunięcia lub dopuszczenia pracownika, jako użytkownika systemu Administrator Lokalny zawiadamia niezwłocznie Administratora Bezpieczeństwa Informacji.

5. Po otrzymaniu uprawnień dostępu do systemu Administrator Lokalny przekazuje nadany login Administratorowi Bezpieczeństwa Informacji.

ROZDZIAŁ X
Identyfikatory użytkowników i hasła dostępu

§ 31. Dostęp do systemów informatycznych Urzędu musi być zabezpieczony, co najmniej przez system identyfikatorów i haseł użytkownika.

§ 32. Identyfikator użytkownika nadany jest przez Administratora Bezpieczeństwa Informacji.

§ 33. 1. Hasła dostępu do systemów komputerowych tworzone są przez użytkownika i stanowią tajemnicę Urzędu znaną wyłącznie temu użytkownikowi i Administratorowi Bezpieczeństwa Informacji.

2. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła i jego przechowywanie.

§ 34. 1. Hasła dostępów do systemów informatycznych powinny być zmieniane zgodnie z ustaleniami Administratora Danych Osobowych. Zmiana powinna być wymuszana w sposób automatyczny przez odpowiednie oprogramowanie.

2. Zmiana haseł następuje nie rzadziej niż co 30 dni.

3. Wszystkie hasła muszą zostać zmienione w przypadku podejrzenia, że zostały odkryte lub wiadomo, że znajdują się w posiadaniu osoby nieupoważnionej.

ROZDZIAŁ XI
Rozpoczęcie i zakończenie pracy w systemach informatycznych

§ 35. 1. Użytkownik systemu rozpoczyna pracę od uwierzytelniania się w systemie operacyjnym. Czynności te wykonuje w sposób uniemożliwiający ujawnienie lub podejrzenie ich przez innych pracowników lub osoby trzecie.

2. W przypadku braku możliwości rozpoczęcia pracy lub podejrzeń, że z konta mogły korzystać inne osoby bądź stwierdza, że zostało nienaruszone bezpieczeństwo systemu powiadamia niezwłocznie Administratora Bezpieczeństwa Informacji.

3. Użytkownik systemu przetwarzający dane osobowe ustawia monitor pod takim kątem widzenia by podgląd ekranu był niemożliwy przez osoby postronne.

4. Użytkownik przed opuszczeniem stanowiska pracy zabezpiecza stację roboczą przed dostępem osób trzecich aktywując wygaszasz ekranowy zabezpieczony hasłem.

5. Wymieniony wygaszasz ekranu jest aktywizowany automatycznie po 20 min od niewykorzystywania stacji.

6. Każdorazowo użytkownik po zakończeniu pracy w systemie wylogowuje się z systemu.

7. Wydruki robocze papierowe zawierające dane osobowe są niszczone. Niszczenia dokonuje się w niszczarce.

ROZDZIAŁ XII
Kopie awaryjne

§ 36. Ze względu na bezpieczeństwo wprowadza się obowiązek sporządzania kopii awaryjnych baz danych.

§ 37. Kopie awaryjne mogą być użyte jedynie dla odbudowy uszkodzonych struktur danych.

§ 38. Kopie awaryjne powinny być sporządzane nie rzadziej niż raz na tydzień oraz po każdej ważniejszej modyfikacji.

§ 39. 1. Kopie awaryjne powinny być przechowywane w szafach ognioodpornych lub powinny być zastosowane środki bezpieczeństwa o podobnej skuteczności.

2. Pomieszczenia, w których przechowywane są kopie awaryjne muszą być zabezpieczone przed dostępem osób nieupoważnionych.

3. Miejsca przechowywania kopii awaryjnych określa Administrator Bezpieczeństwa Informacji.

§ 40. 1. Kopie awaryjne danych z poszczególnych systemów informatycznych należy usunąć po ustaniu ich użyteczności.

2. Decyzje o usunięciu kopii awaryjnych z systemu informatycznego podejmuje Administrator Bezpieczeństwa Informacji.

ROZDZIAŁ XIII
Elektroniczne nośniki informacji

§ 41. 1. Elektroniczne nośniki danych używane w Urzędzie, na których są gromadzone dane osobowe są przechowywane w pomieszczeniach Referatu oraz w serwerowni systemu.

2. Wprowadzenie i wycofanie z użycia elektronicznych nośników informacji zainstalowanych na dyskach twardych stacji i serwera odbywa się za zgodną Administratora Bezpieczeństwa Informacji.

3. Zabrania się kopiowania danych osobowych z systemu na dodatkowe nośniki z wyjątkiem sporządzonych kopii bezpieczeństwa.

ROZDZIAŁ XIV
Ochrona przed szkodliwym oprogramowaniem

§ 42. 1. Ochroną przed szkodliwym oprogramowaniem zapewnia się przez zainstalowanie oprogramowania antywirusowego na serwerze i stacjach roboczych.

2. Instalację, aktualizacje oraz poprawność działania programów antywirusowych wykonuje Administrator Bezpieczeństwa Informacji.

3. Oprogramowanie antywirusowe i bazy sygnatur szkodliwego oprogramowania są aktualizowane okresowo przez Administratora Bezpieczeństwa Informacji.

ROZDZIAŁ XV
Monitorowanie, przegląd i konserwacja systemów informatycznych

§ 43. 1. Wprowadza się okresową weryfikację uprawnień poszczególnych użytkowników aplikacji.

2. Wprowadza się obowiązek prowadzenia rejestru pracy systemów informatycznych, w którym notuje się wszystkie sytuacje awaryjne oraz sposoby ich usuwania i wszelkich modyfikacji.

3. Odpowiedzialnym za wykonywanie obowiązków określonych w ust. 1 i 2 jest Administrator Bezpieczeństwa Informacji.

§ 44. 1. Każdy system informatyczny powinien zawierać odpowiednie, automatyczne narzędzia pozwalające Administratorowi na weryfikację stanu bezpieczeństwa systemu.

2. Poszczególne systemy informatyczne muszą w sposób bezpieczny prowadzić zapis wszystkich znaczących zdarzeń systemowych mających wpływ na bezpieczeństwo przetwarzanych w nich danych osobowych a w szczególności:

1) Zmian identyfikatora użytkownika w czasie sesji,

2) Prób odgadywania haseł,
3) Prób wykorzystania uprawnień, do których użytkownik nie uzyskał autoryzacji,
4) Modyfikacji oprogramowania aplikacyjnego,
5) Modyfikacji oprogramowania systemowego,
6) Zmian uprawnień użytkowników,
7) Prób inferencji w systemowe rejestry zdarzeń.

§ 45. 1. Rejestry zdarzeń systemowych związanych z bezpieczeństwem systemów informatycznych muszą być przechowywane przez okres, co najmniej 1 roku.

2. Podczas tego okresu muszą być zabezpieczone w taki sposób, aby nie była możliwa modyfikacja oraz aby były one dostępne jedynie dla upoważnionych pracowników.

3. Rejestry zdarzeń systemowych są istotne w przypadku usuwania błędów, rekonstrukcji po włamaniu do systemu, badania, itp.

§ 46. 1. Administrator Bezpieczeństwa Informacji powinien okresowo kontrolować zbiory systemowe dla prawidłowego funkcjonowania systemu.

2. Raz na kwartał Administrator Bezpieczeństwa Informacji przeprowadza kontrolę możliwości zdalnego dostępu do poszczególnych systemów.

3. Co kwartał należy przeprowadzić weryfikację całego oprogramowania użytkowego eksploatowanego na wszystkich komputerach podłączonych do systemu informatycznego pod kątem spełnienia wymogów bezpieczeństwa informacji.

§ 47. Administrator Bezpieczeństwa Informacji, co najmniej raz na kwartał powinien przeprowadzić weryfikację usług sieciowych dostępnych w systemach informatycznych oraz blokować usługi niewykorzystywane.

§ 48. Administrator bezpieczeństwa informacji jest odpowiedzialny za uaktualnianie systemów operacyjnych i aplikacji.

ROZDZIAŁ XVI
Konserwacja i naprawy systemu

§ 49. 1. Prace serwisantów wykonywane są pod nadzorem pracownika Urzędu.

2. Jeżeli wykonanie czynności serwisowych wymaga dostępu do danych osobowych to serwisant zobowiązany jest do podpisania zobowiązania o zachowaniu poufności.

3. Urządzenia komputerowe, dyski twarde lub inne nośniki danych przeznaczone do naprawy poza Urzędem pozbywa się zapisów danych osobowych.

4. Wymieniony sprzęt w ust. 3 może być naprawiony pod nadzorem pracownika Urzędu i nie wymaga wtedy usuwania danych osobowych.

ROZDZIAŁ XVII
Obowiązki i odpowiedzialności Administratora Bezpieczeństwa Informacji oraz innych użytkowników

§ 50. Administrator Bezpieczeństwa Informacji jest odpowiedzialny za prawidłowe działanie podległego mu systemu informatycznego.

§ 51. 1. Administrator Bezpieczeństwa Informacji odpowiedzialny jest za określenie właściwych uprawnień użytkowników, monitorowanie zapisów związanych z bezpieczeństwem dotyczącym administrowanych przez nich systemów.

2. Administrator Bezpieczeństwa Informacji odpowiedzialny jest również za przekazywanie osobom wyznaczonym do ochrony wszelkich informacji dotyczących podejrzanej działalności związanej z bezpieczeństwem komputerów i sieci komputerowych.

§ 52. Użytkownicy odpowiedzialni są za wypełnianie wszystkich postanowień dotyczących bezpieczeństwa informacji w systemach informatycznych Urzędu.

§ 53. Lokalni administratorzy bezpieczeństwa informacji odpowiedzialni są za bieżące przestrzeganie zasad ustalonych w instrukcjach ochrony danych osobowych oraz zasad użytkowania urządzeń i systemów informatycznych w Urzędzie.

§ 54. Nieprzestrzeganie postanowień niniejszej polityki oraz brak nadzoru nad bezpieczeństwem informacji stanowi ciężkie naruszenie obowiązków pracowniczych i może być przyczyną zastosowania odpowiednich sankcji.

BURMISTRZ

Wojciech Furmanek

Załącznik Nr 1

Rejestru zbiorów danych osobowych prowadzonych
w Urzędzie Miasta i Gminy Daleszyce
(wzór)

POLE	*OPIS*
Nazwa zbioru	.....
Opis zbioru	.....
Pola informacyjne	.....
Opis powiązań pól informacyjnych	.....
Postać zbioru (papierowa, papierowo-elektroniczna)	papierowa/ elektroniczna
Czy zbiór podlega rejestracji w GIODO	Tak/Nie
Data rejestracji w GIODO	rrrr/mm/dd
Miejsce przetwarzania formy papierowej	Pokój nr ....
Miejsce przetwarzania formy elektronicznej	Pokój nr .....
Program komputerowy wykorzystywany do przetwarzania zbioru	.....
Data rozpoczęcia przetwarzania	.....
Data zakończenia przetwarzania	.....

Załącznik Nr 2

Upoważnienie

uprawniające do przetwarzania danych osobowych

Na podstawie art.37 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926) upoważniam Pana/Panią .... do przetwarzania danych osobowych:

1) w systemie informatycznym*)
2) w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych*)

Miejsce przetwarzania danych osobowych: referat .....

Nazwa zbioru danych: .....

Daleszyce, dnia 20...-.....

.....

Administrator Danych Osobowych

*) – niepotrzebne skreślić

Załącznik nr 3

Daleszyce, dnia.....

.....

Znak sprawy (wypełnia administrator bezpieczeństwa informacji)

.....

Imię i nazwisko

.....

Stanowisko

.....

Referat

.....

Oświadczenie*

Ja niżej podpisany(a) zobowiązuję się do zachowania w tajemnicy danych osobowych, do których mam lub będę miał(a) dostęp w związku z wykonywaniem przeze mnie zadań służbowych i obowiązków pracowniczych w Urzędzie Miasta i Gminy w Daleszycach, zarówno w trakcie obecnie wiążącego mnie stosunku pracy, jak i po ustaniu zatrudnienia.

Zobowiązuję się przestrzegać regulaminów, instrukcji i procedur obowiązujących w Urzędzie Miasta i Gminy w Daleszycach wiążących się z ochroną danych osobowych, a w szczególności nie będę bez upoważnienia służbowego wykorzystywać danych osobowych ze zbiorów Urzędu Miasta i Gminy w Daleszycach.

Stwierdzam, że jest mi znana definicja danych osobowych w rozumieniu art. 6 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz zostałem (am) zaznajomiony(a) z przepisami o ochronie danych osobowych.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane za ciężkie naruszenie obowiązków pracowniczych w rozumieniu Kodeksu Pracy.

.....

Data i podpis składającego oświadczenie

.....

Przyjmujący oświadczenie (administrator bezp. Info.)

.....

Data i podpis osoby zaznajamiającej z przepisami

o ochronie danych osobowych

*dotyczy umów o pracę

Załącznik Nr 4

Daleszyce, dnia.....

.....

Znak sprawy (wypełnia administrator bezpieczeństwa informacji)

.....

Imię i nazwisko

.....

Adres zamieszkania

Oświadczenie*

Ja niżej podpisany(a) zobowiązuję się do zachowania w tajemnicy danych osobowych, do których mam lub będę miał(a) dostęp w związku z wykonywaniem umowy zawartej z ..... W dniu..... (Nr umowy.....) zarówno w trakcie trwania umowy jak i po jej wygaśnięciu lub rozwiązaniu.

Zobowiązuję się do ścisłego przestrzegania warunków ww. umowy, które wiążą się z ochroną danych osobowych, a w szczególności nie będę bez upoważnienia administratora danych osobowych wykorzystywał(a) danych osobowych ze zbiorów w Urzędzie Miasta i Gminy w Daleszycach w celach nie związanych z wykonywaniem tej umowy.

Stwierdzam, że jest mi znana definicja danych osobowych w rozumieniu art. 6 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz zostałem(am) zaznajomiony(a) z przepisami o ochronie danych osobowych.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane za ciężkie naruszenie obowiązków pracowniczych w rozumieniu Kodeksu Pracy.

.....

Data i podpis składającego oświadczenie

.....

Przyjmujący oświadczenie (administrator bezp. Info.)

*dotyczy umów cywilno-prawnych

Załącznik Nr 5

Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Lp.	Nazwisko i imię	Stanowisko	Komórka organizacyjna	Nazwa zbioru	Data nadania upoważnienia	Data ustania upoważnienia

Załącznik Nr 6

Wzór ewidencji oświadczeń do zachowania w tajemnicy danych osobowych

Lp.	Imię i nazwisko	Stanowisko/komórka organizacyjna	Data dołączenia oświadczenia