ZARZĄDZENIE NR 113/2016
BURMISTRZA MIASTA i GMINY DALESZYCE
dnia 17 października 2016r.

w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji oraz Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Daleszycach

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz.U.2016.446 ze zm.) oraz art. 7 pkt 4 i art. 36 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. 2016.922 ze zm.) w związku z § 3, § 4 i § 5 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) Burmistrz Miasta i Gminy Daleszyce zarządza co następuje:

§ 1

Celem określenia reguł i zasad obowiązujących przy przetwarzaniu danych osobowych w Urzędzie Miasta i Gminy w Daleszycach, wprowadza się w brzmieniu określonym w załącznikach:
1. Politykę Bezpieczeństwa Informacji, która stanowi załącznik Nr 1 do niniejszego zarządzenia,
2. Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych, która stanowi załącznik Nr 2 niniejszego zarządzenia.

§ 2

Wprowadza się elektroniczny system pn. „Bezpieczeństwo Informacji Urzędu Miasta i Gminy w Daleszycach (BI)", służący do ewidencji zbiorów danych osobowych i osób upoważnionych do ich przetwarzania.

§ 3

Zobowiązuje się pracowników wszystkich komórek organizacyjnych Urzędu Miasta i Gminy w Daleszycach do przestrzegania postanowień zawartych w Polityce Bezpieczeństwa Informacji oraz Instrukcji Zarządzania Systemem Informatycznym, o których stanowi § 1 niniejszego zarządzenia.

§ 4

Nadzór nad przestrzeganiem postanowień zawartych w Polityce Bezpieczeństwa Informacji oraz Instrukcji Zarządzania Systemem Informatycznym powierza się Kierownikom referatów oraz Administratorowi Bezpieczeństwa Informacji.

§ 5

Traci moc zarządzenie nr 65/2012 z dnia 3 września 2012 r. w sprawie wdrożenia polityki bezpieczeństwa informacji w Urzędzie Miasta i Gminy w Daleszycach.
Wydane na jej podstawie upoważnienia do przetwarzania danych osobowych – zachowują ważność.

§ 6

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
Dariusz Wiesiński

RADCA PRAWNY
KL-K-612
mgr Krzysztof Jermak

Załącznik Nr 1 do ZARZĄDZENIA NR 113/2016
Burmistrza Miasta i Gminy Daleszyce z dnia 17 października 2016 r.

TYTUŁ DOKUMENTU	**Polityka Bezpieczeństwa Informacji Urzędu Miasta i Gminy Miasta w Daleszycach**		
WYDAŁ:	***Dariusz Meresiński*** *IMIĘ I NAZWISKO*	*PODPIS*	*10.10.2016* *DATA*
DOKUMENT OBOWIĄZUJE OD DNIA: 17 października 2016			

BURMISTRZ
Dariusz Meresiński

1. POSTANOWIENIA OGÓLNE

Realizując obowiązki wynikające z przepisów dotyczących ochrony danych osobowych zmierzamy do spełnienia wymagań chroniących prywatność i godność każdego pracownika oraz klientów naszego urzędu.

Sposób przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Daleszycach oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych ujęte zostają zbiorczo w niniejszym dokumencie określającym Politykę bezpieczeństwa informacji oraz w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Administratorem Danych Osobowych w Urzędzie Miasta i Gminy w Daleszycach jest Burmistrz Miasta i Gminy Daleszyce. Administrator danych osobowych odpowiedzialny jest za bezpieczeństwo danych. Zobowiązany jest zastosować takie środki, procedury, aby uniemożliwić uszkodzenie, kradzież, dostęp osobom nieupoważnionym oraz przetwarzanie niezgodnie z ustawą. W tym celu powołuje Administratora Bezpieczeństwa Informacji, który nadzoruje przestrzeganie zasad ochrony.

Pracownicy zobowiązani są przestrzegać zasad bezpieczeństwa danych określonych w polityce bezpieczeństwa, a także współpracować we wdrażaniu oraz doskonaleniu procedur ochrony informacji. Zgłaszają uwagi i opiniują zastosowane rozwiązania.

1.1.Polityka Bezpieczeństwa Informacji została opracowany na podstawie:

- ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych;
- rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;

1.2.Cel opracowania Polityki Bezpieczeństwa Informacji

Celem opracowania Polityki Bezpieczeństwa Informacji jest określenie zasad ochrony danych osobowych przetwarzanych w Urzędzie Miasta i Gminy w Daleszycach. Zasady określone w Polityce Bezpieczeństwa Informacji mają zastosowanie do wszystkich osób upoważnionych przez Administratora Danych do przetwarzania danych osobowych, niezależnie od formy ich zatrudnienia. Utrzymanie bezpieczeństwa przetwarzanych przez Urząd Miasta i Gminy w Daleszycach danych osobowych oraz informacji rozumiane jest jako zapewnienie ich poufności, integralności i dostępności oraz rozliczalności na wysokim poziomie bezpieczeństwa.

1.3.Ilekroć w Polityce Bezpieczeństwa Informacji mowa o:

- ustawie, należy przez to rozmieć - Ustawę z dnia 29 sierpnia 1997r. o ochronie danych osobowych
- rozporządzeniu, należy przez to rozumieć - Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych
- Administratorze Danych Osobowych, należy przez to rozumieć - Burmistrza Miasta i Gminy Daleszyce, który decyduje o celach i środkach przetwarzania danych osobowych oraz jest jednocześnie Administratorem Bezpieczeństwa Informacji;
- sieci lokalnej, należy przez to rozumieć - system umożliwiający bezpośrednią komunikację wielu niezależnych urządzeń rozmieszczonych na stosunkowo niewielkim obszarze za pośrednictwem fizycznych kanałów komunikacyjnych;

- sieci rozległej, należy przez to rozumieć - publiczną sieć telekomunikacyjną w rozumieniu ustawy z dnia z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne

- poziomie wysokim bezpieczeństwa przetwarzania danych osobowych, należy przez to rozumieć - poziom bezpieczeństwa, w którym w systemie informatycznym przetwarzane są dane osobowe i informacje, a przynajmniej jedno urządzenie systemu informatycznego połączone jest z siecią publiczną. Zabezpieczenia dla poziomu wysokiego bezpieczeństwa zostały określone w rozporządzeniu;

- zbiorze danych, należy rozumieć przez to - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

- przetwarzaniu danych, należy przez to rozumieć - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;

- zabezpieczeniu danych w systemie informatycznym, należy przez to rozumieć – wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

- usuwaniu danych, należy przez to rozumieć - zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

- zgodzie osoby której dane dotyczą, należy przez to rozumieć - oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie;

- odbiorcy danych, należy przez to rozumieć - każdego, komu udostępnia się dane osobowe, z wyłączeniem: osoby której dane dotyczą, osoby upoważnionej do przetwarzania danych, organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem, podmiotu z którym została zatarta umowa powierzenia;

- rozliczalności, należy przez to rozumieć - właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

- integralności danych, należy przez to rozumieć - właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

- poufności danych, należy przez to rozumieć - właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;

- uwierzytelnianiu, należy przez to rozumieć - działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

- dostępności - należy przez to rozumieć właściwość zapewniająca, że dane są możliwe do wykorzystania przez osoby i podmioty uprawnione na każde żądanie i w określonym czasie;

- zarządzania ryzykiem utraty bezpieczeństwa danych, należy przez to rozumieć - proces identyfikowania, oceniania oraz postępowania z ryzykiem;

- GIODO, należy przez to rozumieć Generalnego Inspektora Danych Osobowych,

- system BI (Bezpieczeństwo Informacji), to elektroniczny rejestr zbiorów danych osobowych, użytkowników oraz wydanych upoważnień do przetwarzania danych osobowych. System dostępny poprzez przeglądarkę internetową.

1.4 Odpowiedzialność:

Za bezpieczeństwo danych osobowych odpowiedzialny jest Burmistrz Miasta i Gminy Daleszyce (Administrator Danych Osobowych), oraz każda osoba upoważniona przez Burmistrza Miasta i Gminy Daleszyce do przetwarzania danych osobowych, niezależnie od formy zatrudnienia. Zgodnie z wymaganiami ustawy - do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby

posiadające pisemne upoważnienie nadane przez Administratora Danych Osobowych. Administrator Danych Osobowych upoważniając osoby do przetwarzania danych osobowych zachowuje zasadę, że dostęp do danych osobowych będą miały tylko te osoby, którym jest to niezbędne do relacji powierzonych im zadań, oraz tylko w takim zakresie, jaki jest konieczny do realizacji powierzonych zadań. Każda z osób upoważnionych do przetwarzania danych osobowych zostanie, przed dopuszczeniem do przetwarzania danych osobowych, przeszkolona z wymagań ochrony danych osobowych, oraz poinformowana o konsekwencjach prawnych jakie jej grożą za naruszenie tych zasad.

Odpowiedzialność Administratora Danych Osobowych została wskazana w ustawie o ochronie danych osobowych, wraz z aktami wykonawczymi do niej. Nie mniej, z uwagi na obowiązek znajomości Polityki Bezpieczeństwa Informacji przez wszystkich pracowników Urzędu Miasta i Gminy w Daleszycach poniżej wskazuje się na podstawowe obowiązki Administratora Danych Osobowych:

- ustanowienie zasad przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Daleszycach,
- decydowanie o celach i środkach przetwarzania danych osobowych,
- ustanowienie Administratora Bezpieczeństwa Informacji w Urzędzie Miasta i Gminy w Daleszycach,
- podpisywanie umów powierzenia z podmiotami zewnętrznymi, którym Urząd Miasta i Gminy w Daleszycach zamierza powierzyć dane osobowe. Powierzenie przetwarzania danych, w imieniu i na rzecz Urzędu Miasta i Gminy w Daleszycach, odrębnemu podmiotowi może przebiegać tylko i wyłącznie z zachowaniem zasad przewidzianych w powołanym przepisie ustawy o ochronie danych osobowych,
- ewidencjonowanie udostępniania danych osobowych zgodnie z ustawą o ochronie danych osobowych.

Odpowiedzialność Administratora Bezpieczeństwa Informacji (skrót: ABI):

- organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych oraz sprawowanie nadzoru nad bezpieczeństwem danych osobowych przetwarzanych w Urzędzie Miasta i Gminy w Daleszycach,
- wydawanie upoważnień do przetwarzania danych osobowych dla pracowników z upoważnienia Burmistrza Miasta i Gminy Daleszyce oraz nadzorowanie aktualności przyznanych upoważnień do przetwarzania danych osobowych w związku ze zmianami kadrowymi;
- zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki Bezpieczeństwa Informacji i Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych,
- zgłaszanie i aktualizowanie zbiorów danych osobowych do GIODO, jeżeli jest to wymagane,
- identyfikacja i analiza ryzyka utraty bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Miasta i Gminy w Daleszycach oraz monitorowanie wdrożonych zabezpieczeń w celu ochrony danych osobowych,
- prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych przy współpracy z Administratorem Danych Osobowych,
- organizowanie okresowych szkoleń z zakresu przetwarzania i ochrony danych osobowych,
- prowadzenie szkoleń z zakresu ochrony danych osobowych dla osób przed przyznaniem upoważnienia do przetwarzania danych osobowych,
- prowadzenie Ewidencji osób upoważnionych do przetwarzania danych osobowych.

Do zadań Administratora Bezpieczeństwa Informacji należy również:

1) zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:

a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,

b) nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2, oraz przestrzegania zasad w niej określonych,

c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

2) prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje.

3. Rejestr, o którym mowa prowadzony jest w wersji elektronicznej, jest jawny tj. dostępny na żądanie osób uprawnionych w siedzibie Urzędu w dyspozycji ABI.

Stanowisko ds. kadr niezwłocznie informuje ABI:

- o zatrudnieniu pracownika w celu przetwarzania danych osobowych,
- o zmianach w zakresie czynności pracownika przetwarzającego dane osobowe,
- ustaniu stosunku pracy ww. pracownika.

Obowiązki każdego kierownika referatu i pracownika Urzędu Miasta i Gminy w Daleszycach:

- identyfikacja zbiorów danych osobowych przetwarzanych w komórce organizacyjnej i zgłaszanie zbiorów do ABI. Zgłoszenia pracownika dokonuje kierownik referatu poprzez system BI lub na formularzu – *Załącznik nr 1 – Wniosek o nadanie upoważnienia do przetwarzania danych osobowych*,
- wnioskowanie o nadanie (odwołanie) lub zmianę uprawnień dla pracowników, stażystów, praktykantów, z uwzględnieniem zastępstw pracowników,
- identyfikacja ryzyka w bezpieczeństwie informacji, ocena ryzyka i szacowanie ryzyka zgodnie z Zarządzeniem Burmistrza Miasta i Gminy Daleszyce w sprawie zarządzania ryzykiem w Urzędzie Miasta i Gminy w Daleszycach i Jednostkach organizacyjnych,
- ochronę zasobów danych osobowych przetwarzanych w Urzędzie Miasta i Gminy w Daleszycach przed ich utratą, nieuprawnionym użyciem lub zniszczeniem,
- zachowanie szczególnej staranności przy gromadzeniu i przetwarzaniu danych osobowych, aby dane te były:
    a. przetwarzane zgodnie z prawem,
    b. zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
- zgłaszanie ABI wszelkich zauważonych nieprawidłowości dotyczących ochrony danych osobowych przetwarzanych w systemach informatycznych i w tradycyjnej papierowej formie,
- poprawne korzystanie z aplikacji zgodnie z powierzonymi obowiązkami służbowymi,
- informowanie interesantów o ADO oraz prawach osób związanych z ochroną danych osobowych, zgodnie z klauzulą informacyjną zawartą w pkt. 8 Polityki.

2. WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe – prowadzony jest w elektronicznym systemie BI.

3. WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA DANYCH OSOBOWYCH – prowadzony jest w elektronicznym systemie BI.

Kierownicy referatów mają obowiązek zgłaszania ABI faktu powstania nowego zbioru danych, jego aktualizacji oraz usunięcia.

ABI, zgodnie z wymaganiami Ustawy o ochronie danych osobowych, ma 30 dni na podjęcie działań związanych z aktualizacją zbiorów danych osobowych (w tym zgłoszenia zmian do GIODO, jeżeli zbiór podlegał rejestracji) lub dla nowych zadań, niezwłoczne wszczęcie procedury identyfikacji ewentualnego nowego zbioru danych osobowych.

4. SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI – określony jest w elektronicznym systemie BI.

5. ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH OSOBOWYCH

I.

Do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora Danych Osobowych.

W elektronicznym systemie BI prowadzona jest ewidencja osób upoważnionych do przetwarzania danych.

Została opracowana i wdrożona Polityka Bezpieczeństwa Informacji (PBI) oraz została opracowana i wdrożona Instrukcja Zarządzania Systemem Informatycznym (IZSI).

Przed dopuszczeniem pracownika do przetwarzania danych osobowych musi zostać on przeszkolony z zasad ochrony danych osobowych ustanowionych w Urzędzie Miasta i Gminy w Daleszycach. Przeszkolenia może dokonać ABI. Fakt dokonania przeszkolenia pracownik potwierdza na Upoważnieniu do przetwarzania danych osobowych.

Dokumenty zawierające dane osobowe, w wyjątkowych sytuacjach (np. sesja Rady Miasta) mogą być wynoszone poza miejsce przetwarzania jedynie w wypadku otrzymania pełnomocnictwa Administratora Danych Osobowych z jednoczesnym zapewnieniem ochrony fizycznej ich przed niepożądanym dostępem osób nieupoważnionych. Odpowiedzialność za dokumentację ponosi pracownik, który otrzymał pełnomocnictwo. Pełnomocnictwo przechowuje Kierownik Komórki Organizacyjnej, który powiadamia ABI oraz udziela instruktażu odnośnie bezpieczeństwa informacji.

Dane osobowe utrwalone na jakimkolwiek nośniku, należy po zakończeniu przetwarzania, skutecznie usunąć lub zniszczyć wraz z nośnikiem.

Przy przetwarzaniu danych osobowych w systemach teleinformatycznych stosuje się zasady „czystego biurka i ekranu", realizowane poprzez stosowanie wygaszaczy ekranu, ustawianie monitorów w taki sposób aby nie była widoczna informacja dla osób postronnych. Zasada „czystego biurka", sprowadza się do zabezpieczenia w czasie i po pracy danych osobowych w formie papierowej w taki sposób, aby uniemożliwiony był ich odczyt przez osoby nieuprawnione.

Zabrania się udostępniania indywidualnego kodu dostępu i haseł innym osobom. Zabronione jest usuwanie danych przez wyrzucenie ich do kosza na odpadki. Zabrania się korzystania z prywatnych nośników informacji w systemach przetwarzających dane osobowe.

II.

W przypadku konieczności przekazania urządzeń, dysków lub innych nośników zawierających dane osobowe podmiotowi zewnętrznemu do przetwarzania danych osobowych, np. na wypadek prac serwisowych i naprawczych, ustalona została następująca zasada: nośniki wymontowuję się i pozostawia się zabezpieczone u ABI/ASI, lub nośniki informacji pozbawia się wcześniejszego zapisu w sposób uniemożliwiający ich odzyskanie przez osoby nieupoważnione. Preferowaną formą realizacji prac serwisowych i naprawczych jest wykonywanie ich pod nadzorem ABI/ASI na terenie Urzędu Miasta i Gminy w Daleszycach, lub w sytuacjach koniecznych - poza nią. Wymagany jest pisemny protokół z zakresu wykonanych prac wraz z klauzulą poufności, który każdorazowo stworzy ABI/ASI.

III.

W celu zabezpieczenia danych osobowych przed ich utratą lub uszkodzeniem:

1. wdrożono procedury tworzenia kopii zapasowych,

2. kluczowe urządzenia informatyczne wyposażono w awaryjne zasilanie,

3. wdrożono oprogramowanie antywirusowe,

4. ewentualny dostęp do systemów z sieci publicznej jest kontrolowany za pomocą reguł zapory sieciowej i wymaga zgody ABI/ASI,

5. przy przesyłaniu danych osobowych przez sieć publiczną (np. poczta e-mail) użytkownicy są zobowiązani stosować oprogramowanie szyfrujące (np. 7zip);

6. zastosowano środki fizyczne chroniące kluczowe urządzenia przed osobami nieupoważnionymi do dostępu do danych osobowych oraz zagrożeniami ze strony sił natury.

IV.

1. Zabezpieczenia fizyczne budynków Urzędu Miasta i Gminy w Daleszycach wskazane są w dokumencie IZSI.

2. Urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych zamkami zwykłymi lub patentowymi.

3. W pomieszczeniu serwerowni Urzędu zainstalowano instalacją przeciwwłamaniową, monitoring oraz dodatkowo klimatyzację. Drzwi do pomieszczenia serwerów są zamykane magnetycznie i otwierają się po użyciu kodu i karty magnetycznej.

4. Przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osoby zatrudnionej przy przetwarzaniu danych lub w obecności kierownika komórki organizacyjnej.

5. Pomieszczenia, o których mowa w pkt. 4, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.

6. Do przebywania w pomieszczeniu serwerów uprawnieni są:

   1) Administratorzy Systemu Informatycznego;

   2) Administrator Bezpieczeństwa Informacji;

8. Przebywanie w pomieszczeniu serwerów osób nieuprawnionych (konserwator, elektryk, sprzątaczka) dopuszczalne jest tylko w obecności jednej z osób upoważnionych, a w przypadku ich nieobecności - w obecności osoby wyznaczonej pisemnie przez Administratora Systemów Informatycznych.

V.

1. Dla każdego użytkownika systemu operacyjnego jest ustalony odrębny identyfikator i stosowane jest unikalne hasło.

2. Dodatkowo zastosowano identyfikator i hasło dostępu do danych na poziomie kluczowych aplikacji.

3. Zdefiniowano prawa dostępu użytkowników do danych osobowych na poziomie aplikacji.

6. PROCEDURA POSTĘPOWANIA Z INCYDENTAMI OCHRONY DANYCH OSOBOWYCH

Każde niepożądane zdarzenie (incydent bezpieczeństwa), które spowodowało naruszenie bezpieczeństwa danych osobowych musi być natychmiast zgłoszone do Administratora Bezpieczeństwa Informacji, celem podjęcia dalszych działań, dążących do minimalizacji skutków wystąpienia tego incydentu. Zgłoszeniu podlegają również zdarzenia, mogące potencjalnie doprowadzić do incydentu bezpieczeństwa.

Każde naruszenie zasad ochrony danych osobowych przez osoby zatrudnione w Urzędzie Miasta i Gminy w Daleszycach (niezależnie od formy, umowa o pracę, staż, umowa o dzieło) zostaną potraktowane jako incydent bezpieczeństwa danych osobowych.

Utrzymywany jest Rejestr incydentów bezpieczeństwa - *Załącznik nr 2 - Rejestr incydentów bezpieczeństwa danych osobowych.* Rejestr może być prowadzony w wersji elektronicznej.

7. OBOWIĄZEK INFORMACYJNY. UDOSTĘPNIANIE DANYCH OSOBOWYCH

Urząd Miasta i Gminy w Daleszycach nie udostępnia danych osobowych bez zgody osoby, której dane dotyczą.

Zasada przyjęta przez Urzędzie Miasta i Gminy w Daleszycach jest, że udostępnianie danych osobowym stronom trzecim może nastąpić jedynie na podstawie przepisów prawnych (np. organów państwowych w związku z prowadzonym postępowaniem) bądź wskazywać interes faktyczny strony trzeciej połączony ze zgodą osoby, której dane dotyczą. W takim przypadku, udostępnienie danych może nastąpić jedynie na podstawie pisemnego wniosku strony trzeciej. Wniosek musi zawierać, co najmniej, dane wnioskodawcy, dane Administratora Danych Osobowych (celem potwierdzenia właściwości skierowania wniosku o udostępnienie danych osobowych), podstawę prawną upoważniającą do pozyskania informacji, wskazanie przeznaczenie dla udostępnionych danych, wskazania zbioru, z którego dane mają być udostępnione, zakres informacji. Wniosek podlega rozpatrzeniu przez ABI.

Kierownicy referatów prowadzą Rejestr wniosków o udostępnienie danych osobowych.

Każda osoba ma prawo do kontroli swoich danych osobowych, które może realizować m. in. poprzez żądanie informacji, odnośnie przetwarzania swoich danych.

Dane osobowe muszą zostać natomiast udostępnione osobie, której dane dotyczą. Na wniosek osoby, której dane są przetwarzane przez Urząd Miasta i Gminy w Daleszycach, w terminie 30 dni od otrzymania wniosku, ADO przekazuje pisemną odpowiedź, którą przegotowuje ABI.

Administrator obowiązany jest poinformować osobę zwracającą się do niego o przysługujących jej prawach oraz udzielić informacji - odnośnie przetwarzania jej danych osobowych - o których mowa w art. 32 ust. 1 pkt 1 - 5a, czyli:

- czy zbiór istnieje,
- kto jest jego administratorem (poprzez określenie jego pełnej nazwy i adresu /siedziby/, a w przypadku, gdy administratorem danych jest osoba fizyczna - jej imienia i nazwiska oraz miejsca zamieszkania),
- od kiedy dane są przetwarzane,

- jakie jest źródło pozyskania danych (chyba, że w tym zakresie administrator musi zachować tajemnicę państwową, służbową lub zawodową),
- w jaki sposób dane są udostępniane (w szczególności administrator jest zobowiązany do poinformowania o odbiorcach lub kategoriach odbiorców danych),
- jakie przesłanki przesądziły o podjęciu rozstrzygnięcia wyłącznie w wyniku operacji na danych osobowych prowadzonych w systemie informatycznym,
- podania w powszechnie zrozumiałej formie treści przetwarzanych danych.

W szczególności, administrator danych jest obowiązany do wskazania w formie zrozumiałej:

- jakie dane osobowe zawiera zbiór,
- w jaki sposób zebrano dane,
- w jakim celu i zakresie dane są przetwarzane,
- w jakim zakresie oraz komu dane zostały udostępnione.

Z żądaniem udzielenia powyższych informacji (wyłączając prawo ustalenia przesłanek, które przesądziły o podjęciu rozstrzygnięcia wyłącznie w wyniku operacji na danych osobowych prowadzonych w systemie informatycznym) osoba, której dane dotyczą, może skorzystać nie częściej niż raz na 6 miesięcy.

W celu realizacji obowiązku informacyjnego wskazanego w ustawie o ochronie danych osobowych w art. 24 (od osoby, której dane dotyczą) ADO na stronie internetowej BIP Urzędu w zakładce „Sprawy do załatwienia" umieszcza klauzulę informacyjną o treści podanej w ramce. Pozostałe informacje przekazywane są ustnie przez pracownika urzędu zbierającego dane osobowe.

Tam gdzie jest to możliwe, klauzula obowiązku informacyjnego umieszczana jest na drukach wniosków rozpoczynających daną sprawę.

Zgodnie z Art. 24 Ustawy o ochronie danych osobowych informujemy, że Administratorem Danych Osobowych jest Urząd Miasta i Gminy w Daleszycach, ul. Plac Staszica 9, 26-021 Daleszyce. Dane osobowe będą przetwarzane dla celu realizacji zadania publicznego, zgodnie ze złożonym wnioskiem. Dane przekazywane do Urzędu Miasta i Gminy w Daleszycach są dobrowolnie i istnieje prawo dostępu do treści danych oraz możliwość ich poprawiania.

Ponadto każdy z pracowników załatwiający indywidualną sprawę interesanta informuje go o ADO zgodnie z powyższą klauzulą. Czyni to zwłaszcza w tych przypadkach, gdy na wniosku, piśmie inicjującej sprawę nie zawarto klauzuli informacyjnej.

8. OCENA SYSTEMU OCHRONY DANYCH OSOBOWYCH W URZĘDZIE MIASTA I GMINY W DALESZYCACH

ABI raz w roku dokona podsumowania funkcjonowania systemu ochrony danych osobowych w Urzędzie Miasta i Gminy w Daleszycach. W tym celu realizowane jest sprawdzenie systemu ochrony danych osobowych wykonywany przez ABI lub osoby przez niego wskazane.

8.1 Definicje

sprawdzenie - należy przez to rozumieć czynności mające na celu zweryfikowanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

sprawozdanie - należy przez to rozumieć dokument, o którym mowa w art. 36c ustawy, opracowany przez administratora bezpieczeństwa informacji po dokonaniu sprawdzenia

8.2 Procedura postępowania

ABI przygotowuje Plan sprawdzeń systemu ochrony danych osobowych w cyklu rocznym wskazując komórki organizacyjne, które podlegać będą sprawdzeniu. W Planie sprawdzeń określony jest przedmiot, zakres oraz termin przeprowadzenia poszczególnych sprawdzeń. W tym celu przygotowuje *Załącznik nr 3 - Plan sprawdzeń*. Plan Sprawdzeń podlega akceptacji ADO.

Zakres sprawdzenia obejmuje weryfikację wymagań zawartych:

- w ustawie o ochronie danych osobowych,
- w dokumentacji systemu ochronnych danych osobowych, w szczególności:
    1) opracowanie i kompletności dokumentacji przetwarzania danych;
    2) zgodność dokumentacji przetwarzania danych z obowiązującymi przepisami prawa;
    3) stanu faktycznego w zakresie przetwarzania danych osobowych;
    4) zgodność ze stanem faktycznym przewidzianych w dokumentacji przetwarzania danych środków technicznych i organizacyjnych służących przeciwdziałaniu zagrożeniom dla ochrony danych osobowych;
    5) przestrzeganie zasad i obowiązków określonych w dokumentacji przetwarzania danych.

Sprawdzenie doraźne jest przeprowadzane niezwłocznie po powzięciu wiadomości przez ADO lub ABI o naruszeniu ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia.

W przypadku wykrycia podczas weryfikacji nieprawidłowości ABI ustala ich przyczyny zaleca wdrożenie działań korekcyjnych (usuwających nieprawidłowości) i korygujących (usuwających przyczyny zaistniałych nieprawidłowości). Ustalania zapisywane są w sprawozdaniu.

Podczas kolejnego sprawdzenia sprawdzana jest skuteczność wykonanych działań.

ADO może zarządzić sprawdzenie doraźne celem weryfikacji skuteczności wykonanych działań po stwierdzonych nieprawidłowościach.

Pracownik odpowiedzialny za obszar danych osobowych, którego dotyczy sprawdzenie (dotyczy to również ASI) jest zobowiązany udostępnić wszystkie żądane dane, dokumenty, zapisy, udzielić wyczerpujących wyjaśnień oraz dokonywać okazania pomieszczeń, urządzeń na życzenie sprawdzającego oraz zapewnić pełną, merytoryczną współpracę.

Po zakończeniu sprawdzenia administrator bezpieczeństwa informacji przygotowuje Sprawozdanie z funkcjonowania systemu ochrony danych osobowych - *Załącznik nr 4 - Sprawozdanie z funkcjonowania systemu ochrony danych osobowych*.

9. UMOWY POWIERZENIA DANYCH OSOBOWYCH

Umowy powierzenia danych osobowych przechowywane są w referatach. Kierownik referatu każdorazowo informuje ABI o zawartej umowie powierzenia danych osobowych.

Na tej podstawie ABI prowadzi Rejestr zawartych umów powierzenia – *Załącznik nr 5*.

10. DOKUMENTY ZWIĄZANE

- Instrukcja Zarządzania Systemem Informatycznym

Załącznik nr 1
do Polityki Bezpieczeństwa Informacji

.....
(pieczęć komórki organizacyjnej urzędu)

WNIOSEK Nr ...../.....[1]
o nadanie upoważnienia do przetwarzania danych osobowych

.....
Imię i nazwisko

.....
Zatrudnioną/nym (nazwa komórki organizacyjnej)

- dane przetwarzane na nośnikach papierowych*
- w systemach informatycznych*

1. Czas obowiązywania[2] .....
2. Zakres uprawnień (dostępnych czynności)

.....
Data i podpis wnioskującego o nadanie upoważnienia
(kierownik komórki organizacyjnej)

.....
Data przyjęcia wniosku i podpis ABI

1 Numer nadaje ABI.
2 Na czas nieokreślony lub na czas określony od-do.
* - niepotrzebne skreślić

Załącznik nr 2
do Polityki Bezpieczeństwa Informacji

Rejestr incydentów naruszenia bezpieczeństwa danych osobowych

Lp.	Data zdarzenia	Opis i miejsce incydentu	Podjęte działania	Uwagi
1				
2...				

Otrzymuje:
Administrator Danych Osobowych

Załącznik nr 3
do Polityki Bezpieczeństwa Informacji

Plan sprawdzeń systemu ochrony danych osobowych

Lp.	Referat / stanowisko	Termin	Zakres sprawdzenia
1	Referat Planowania i Finansów, stanowiska ds. wymiaru i windykacji podatków, stanowiska ds. obsługi oświaty	wrzesień	Środki techniczne i organizacyjne służące przeciwdziałaniu zagrożeniom dla ochrony danych osobowych. Rejestr wniosków o udostępnienie danych osobowych. Rejestr umów powierzenia przetwarzania danych osobowych (jeśli jest prowadzony). Wydawane dokumenty pod względem zgodności z przepisami ochrony d.o. Przestrzeganie i obowiązków określonych w dokumentacji przetwarzania danych
2	Referat Gospodarki, Mienia Komunalnego i Rolnictwa, stanowisko ds. gospodarki odpadami oraz stanowisko ds. zagospodarowania przestrzennego	październik	Środki techniczne i organizacyjne służące przeciwdziałaniu zagrożeniom dla ochrony danych osobowych. Rejestr wniosków o udostępnienie danych osobowych. Rejestr umów powierzenia przetwarzania danych osobowych (jeśli jest prowadzony). Wydawane dokumenty pod względem zgodności z przepisami ochrony d.o. Przestrzeganie i obowiązków określonych w dokumentacji przetwarzania danych
3	Referat Organizacyjny i Spraw Obywatelskich, stanowiska ds. ewidencji ludności i dowodów osobistych, stanowisko ds. wydawania zezwoleń na sprzedaż napojów alkoholowych	listopad	Środki techniczne i organizacyjne służące przeciwdziałaniu zagrożeniom dla ochrony danych osobowych. Rejestr wniosków o udostępnienie danych osobowych. Rejestr umów powierzenia przetwarzania danych osobowych (jeśli jest prowadzony). Wydawane dokumenty pod względem zgodności z przepisami ochrony d.o. Przestrzeganie i obowiązków określonych w dokumentacji przetwarzania danych
4	Urząd Stanu Cywilnego	grudzień	Środki techniczne i organizacyjne służące przeciwdziałaniu zagrożeniom dla ochrony danych osobowych. Rejestr wniosków o udostępnienie danych osobowych. Rejestr umów powierzenia przetwarzania danych osobowych (jeśli jest prowadzony). Wydawane dokumenty pod względem zgodności z przepisami ochrony d.o. Przestrzeganie i obowiązków określonych w dokumentacji przetwarzania danych

Opracował:

.....
Administrator Bezpieczeństwa Informacji

Akceptuję:

.....
Administrator Danych Osobowych

Daleszyce, ...

Załącznik nr 4
do Polityki Bezpieczeństwa Informacji

SPRAWOZDANIE
z funkcjonowania systemu ochrony danych osobowych

.....
imię i nazwisko
administratora bezpieczeństwa informacji

Administrator Danych Osobowych
Burmistrz Miasta i Gminy Daleszyce

Sprawozdanie

W dniach od ..... do ..... , jako administrator bezpieczeństwa informacji dokonałam/em sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych w zakresie wskazanym w Planie sprawdzeń systemu ochrony danych osobowych z dnia .....

I. W toku sprawdzenia podjęto następujące czynności:

1) ...
2)...
3)...

II. W czynnościach tych uczestniczyli (imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach):

1) ...
2) ...
3) ...

III. Przedmiotem i zakresem sprawdzenia objęto (wskazać zakres określony w Wystąpieniu GIODO).

IV. Opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych (powołać dowody potwierdzające ww. ustalony stan faktyczny).

V. Stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem*(wskazać należy uzasadnienie prawne poprzez podanie konkretnego przepisu prawa materialnego,* który został naruszony oraz uzasadnienie faktyczne, tj. opis stwierdzonego naruszenia wraz ze *wskazaniem terminu do przywrócenia stanu zgodnego z prawem).*

VI. Załączniki stanowiące składową część sprawozdania:

1) ...
2) ...
3) ...

.....
data i miejsce podpisania
sprawozdania

.....
podpis administratora
bezpieczeństwa informacji,

UWAGA w przypadku sprawozdania
w postaci papierowej - dodatkowo parafy
administratora bezpieczeństwa informacji na
każdej stronie sprawozdania

Załącznik nr 5
do Polityki Bezpieczeństwa Informacji

Rejestr zawartych umów powierzenia

Lp.	Nr / oznaczenie umowy	Umowa dotyczy	Dane powierzającego	Dane wykonawcy
1				
2...				

Załącznik Nr 2 do ZARZĄDZENIA NR 113/2016
Burmistrza Miasta i Gminy Daleszyce z dnia 17 października 2016 r.

TYTUŁ DOKUMENTU	**Instrukcja Zarządzania Systemem Informatycznym Urzędu Miasta i Gminy Miasta w Daleszycach**		
WYDAŁ:	***Dariusz Meresiński*** *IMIĘ I NAZWISKO*	*PODPIS*	*10.10.2016* *DATA*
DOKUMENT OBOWIĄZUJE OD DNIA: 17 października 2016			

BURMISTRZ
Dariusz Meresiński

§ 1

Zgodnie z Rozporządzeniem 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 wdraża dokument o nazwie „Instrukcja zarządzania systemem informatycznym" zwany dalej „instrukcją". Zapisy tego dokumentu wchodzą w życie z dniem 17 października 2016 r.

Ilekroć w „instrukcji" jest mowa o:
1) podmiocie - rozumie się przez to spółkę prawa handlowego, podmiot gospodarczy nie posiadający osobowości prawnej, jednostkę budżetową;
2) ustawie - rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, zwaną dalej „ustawą";
3) identyfikatorze użytkownika - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
4) haśle - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
5) sieci telekomunikacyjnej - rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.)
6) sieci publicznej - rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne;
7) teletransmisji - rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej
8) rozliczalności - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
9) integralności danych - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
10) raporcie - rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
11) poufności danych - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
12) uwierzytelnianiu - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
Za przestrzeganie w URZĘDZIE MIASTA I GMINY W DALESZYCACH zapisów „instrukcji" odpowiedzialny jest Administrator danych lub zgodnie z zapisem 1.4 „Polityki Bezpieczeństwa" wyznaczony Administrator Systemu Informatycznego

§2

W związku z tym, że w URZĘDZIE MIASTA I GMINY W DALESZYCACH przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną, oraz uwzględniając kategorie przetwarzanych danych i zagrożenia wprowadza się poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym na poziomie wysokim, a w związku z tym wprowadza się poniższe postanowienia:

I

Obszar, w który są przetwarzane dane, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. Przebywanie osób nieuprawnionych w obszarze, w którym są przetwarzane dane, jest dopuszczalne za zgodą Administratora Danych, Administratora Bezpieczeństwa Informacji lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

II

Przetwarzanie danych osobowych w formie elektronicznej odbywa się wyłącznie na komputerach służbowych i obsługiwanych przez uprawnione osoby na podstawie upoważnienia wydanego przez Administratora Danych Osobowych (ADO).

III

Każda osoba użytkująca komputer przenośny jest zobowiązana do zachowania szczególnej ostrożności podczas jego użytkowania poza obszarem przetwarzania danych osobowych w tym stosuje hasła dostępu do komputera oraz do zasobów sieci LAN, jak również podczas transportu oraz przechowywania (transportowanie jako bagażu podręcznego w torbie do tego przeznaczonej, nie pozostawianie go w samochodzie, przechowalni lub innych ogólnie dostępnych miejscach).

IV

W przypadku zagubienia (kradzieży) komputera przenośnego, jego użytkownik jest zobowiązany do niezwłocznego powiadomienia o powyższym przełożonego oraz osoby funkcyjne (ABI, ASI).

V

Zainstalowane w systemach informatycznych oprogramowanie umożliwia kontrolę dostępu użytkowników do zasobów tych systemów i rejestrację dokonywanych w nich operacji.

VI

1. W systemie informatycznym służącym do przetwarzania danych osobowych, przetwarzać dane mogą wyłącznie osoby posiadające aktualne upoważnienie nadane przez Administratora Bezpieczeństwa Informacji. Użytkownik przetwarzający dane po otrzymaniu upoważnienia oraz loginu i hasła jest zobowiązany niezwłocznie dokonać zmiany hasła oraz zachować je w tajemnicy. Użytkownik jest zobowiązany do zmiany hasła nie rzadziej niż co 30 dni. Hasło nadane przez użytkownika musi składać się z co najmniej z 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
2. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator oraz aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

VII

System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:
1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego:
- poprzez zainstalowanie programu antywirusowego o nazwie NOD ANTYWIRUS
- poprzez zainstalowanie firewall (zapora sieciowa),
- poprzez filtrowanie treści przeglądarek internetowych i zapytań do DNS

2) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez zastosowanie zasilacza awaryjnego UPS.

VIII

Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Kopie wszystkich danych osobowych muszą być tworzone nie rzadziej niż raz na tydzień.
Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem w pomieszczeniu zamkniętym - SERWEROWNI, przez okres 30 dni.

IX

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
1) likwidacji - pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się mechanicznie w sposób uniemożliwiający ich odczytanie;
2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych - pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
3) naprawy - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie lub wymontowanie nośnika danych, albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

§3

1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym - z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie - system ten zapewnia odnotowanie:
1) daty pierwszego wprowadzenia danych do systemu;
2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;
3) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;
4) informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;
5) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.
2. Odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.
3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.
4. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust. 1 pkt 4, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

§4

Po odejściu od stanowiska użytkownik ma obowiązek zablokowania pulpitu oraz zabezpieczenia karty kryptograficznej (jeżeli posiada).
W przypadku braku czynności ze strony użytkownika w systemie informatycznym przez 20 minut, system operacyjny samoczynnie zablokuje pulpit użytkownika przetwarzającego dane osobowe.

Po zakończeniu pracy użytkownik ma obowiązek wylogować się z systemu, wyłączenia komputera, zabezpieczenia karty kryptograficznej (jeżeli posiada) oraz dokumentów.

§5

Administrator Systemu Informatycznego ma obowiązek dokonywać przeglądów technicznych sprzętu informatycznego w podmiocie oraz dbać o ich dobry stan techniczny. Zaleca się dokonywanie przeglądów okresowych co 30 dni oraz podczas prowadzonych prac technicznych na stanowisku.

§6

W przypadku stwierdzenia przez Administratora Systemu Informatycznego uchybień dotyczących przetwarzania danych w URZĘDZIE MIASTA I GMINY W DALESZYCACH powinien o tym fakcie niezwłocznie powiadomić Administratora Danych oraz wprowadzić takie zabezpieczenia i procedury, które w przyszłości wyeliminują takie zdarzenia.

§ 7

W sprawach nieuregulowanych w niniejszej „instrukcji" mają zastosowanie przepisy ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. oraz Rozporządzeniem 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.