ZARZĄDZENIE Nr. 66/2013
BURMISTRZA MIASTA LĘBORKA
z dnia 10 września 2013r.

w sprawie:
- wprowadzenia w Urzędzie Miejskim w Lęborku **„Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Lęborku"**,
- wprowadzenia w Urzędzie Miejskim w Lęborku dokumentu o nazwie **„Polityka bezpieczeństwa ochrony danych osobowych w Urzędzie Miejskim w Lęborku"**,
- wprowadzenia w Urzędzie Miejskim w Lęborku **„Instrukcji postępowania w sytuacjach awaryjnych"**

na podstawie: § 3 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 (Dz. U. 2004r. Nr 100, poz.1024)

zarządzam, co następuje:

§ 1

Wprowadzam w Urzędzie Miejskim w Lęborku :

1) „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Lęborku" stanowiącą załącznik nr 1 do niniejszego zarządzenia,
2) dokument o nazwie „Polityka bezpieczeństwa ochrony danych osobowych w Urzędzie Miejskim w Lęborku" stanowiący załącznik nr 2 do niniejszego zarządzenia,
3) „Instrukcję postępowania w sytuacjach awaryjnych" stanowiącą załącznik nr 3 do niniejszego zarządzenia.

§ 2

Traci moc zarządzenie Nr 91/2004 Burmistrza Miasta Lęborka z dnia 29 października 2004r. w sprawie wprowadzenia w Urzędzie Miejskim w Lęborku „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Lęborku" oraz dokument o nazwie „Polityka bezpieczeństwa" stanowiące odpowiednio załącznik nr 1 i nr 2 do zarządzenia.

§ 3

Wykonanie zarządzenia powierza się Sekretarzowi Miasta.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

Sprawdzono pod względem formalno-prawnym
RADCA PRAWNY
Artem Baranowski

BURMISTRZ MIASTA
Witold Namyślak

Załącznik Nr 1
do zarządzenia Nr 66/2013
Burmistrza Miasta Lęborka
z dnia 10.09.2013 r.

Instrukcja

zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Lęborku

BURMISTRZ MIASTA
Witold Namyślak

Zatwierdzam do stosowania:

Instrukcja

zarządzania systemem informatycznym służącym do

przetwarzania danych osobowych w Urzędzie Miejskim w Lęborku

Rozdział I

Postanowienia ogólne

§ 1

Podstawę prawną niniejszej instrukcji stanowi: ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.), rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. (Dz. U. z 2004r. Nr 100, poz. 1024) oraz ustawa z dnia 5 sierpnia 2010r. o ochronie informacji niejawnych (Dz. U. z 2010r. Nr 182, poz. 1228 ze zm.) wraz z aktami wykonawczymi do obu ustaw.
Niniejsza instrukcja, /zwana dalej: **instrukcją**/, jest wewnętrznym dokumentem Urzędu Miejskiego w Lęborku /zwanego dalej: **Urzędem/** i ma zastosowanie do wszelkich danych osobowych znajdujących się, bądź mogących znajdować się w systemie informatycznym Urzędu.

§ 2

Instrukcja określa, w szczególności:

1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności
2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem
3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu
4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi służących do ich przetwarzania
5) sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych
6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego oraz utratą danych spowodowaną awarią zasilania.
7) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych.

§ 3

Następujące słowa, użyte w Instrukcji, oznaczają:

- **administrator danych** – Burmistrza Miasta Lęborka
- **administrator bezpieczeństwa informacji** - osoba wyznaczona przez Burmistrza, odpowiedzialna za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń;
- **administrator systemu** - osoba odpowiedzialna za funkcjonowanie systemu informatycznego, jego bezpieczeństwo i ochronę danych osobowych;
- **osoba upoważniona lub użytkownik** – osoba posiadająca upoważnienie wydane przez administratora danych i dopuszczona w zakresie w nim wskazanym, jako użytkownik do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych lub uprawniona we wskazanym zakresie do dostępu do dokumentacji Urzędu;
- **osoba trzecia** – to każda osoba nieupoważniona i przez to nieuprawniona do dostępu do danych osobowych lub zbiorów tych danych, w tym w szczególności interesanci Urzędu. Osobą trzecią jest również osoba posiadająca upoważnienie wydane przez Burmistrza w zakresie czynności przekraczających ramy udzielonego jej upoważnienia;
- **system informatyczny** - system przetwarzania informacji w Urzędzie wraz ze związanymi z nim ludźmi oraz zasobami technicznymi i finansowymi, który dostarcza i rozprowadza informacje;
- **zabezpieczenie systemu informatycznego** – wdrożenie w Urzędzie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą.

Rozdział II

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

§ 4

1. Przetwarzanie danych osobowych jest możliwe tylko przez uprawione osoby.
2. Naczelnicy wydziałów i kierownicy komórek organizacyjnych wnioskują o nadanie/zmianę/anulowanie uprawnień i upoważnień do przetwarzania danych osobowych dla podległych im pracowników, zgodnie z załącznikiem nr 1.
3. Rejestracji i wyrejestrowywania użytkowników w systemie informatycznym dokonuje administrator systemu w uzgodnieniu z administratorem bezpieczeństwa informacji, który prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych w Urzędzie Miejskim w Lęborku.
4. Ewidencja zawiera :
    - nazwę zbioru danych osobowych
    - nazwisko i imię użytkownika
    - identyfikator użytkownika
    - rodzaj uprawnień
    - datę zarejestrowania
    - datę wyrejestrowania

5. Jakakolwiek zmiana w zakresie informacji zawartych w ewidencji podlega niezwłocznemu odnotowaniu.

§ 5

Dana osoba jest rejestrowana w systemie informatycznym, jako użytkownik po spełnieniu następujących warunków:

1. uzyskaniu przez tę osobę - upoważnienia wydanego przez administratora danych dopuszczającego daną osobę w zakresie w nim wskazanym, jako użytkownika, do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych,
2. uzyskaniu przez administratora bezpieczeństwa informacji – informacji koniecznych do zdefiniowania dla danej osoby jej profilu jako użytkownika oraz jej uprawnień. Informacji takich udziela osoba odpowiedzialna pod względem merytorycznym co do charakteru pracy danej osoby, mającej być użytkownikiem, mając na względzie treść wydanego tej osobie upoważnienia. Uprawnienia i profil danej osoby są definiowane ściśle do zakresu udzielonego jej upoważnienia.

§ 6

1. Z chwilą zarejestrowania w systemie informatycznym, zgodnie z postanowieniami § 5, dana osoba jest informowana ustnie przez administratora systemu o ustalonym dla niej identyfikatorze i konieczności posługiwania się hasłami.

2. Bez spełnienia wymogów wynikających z postanowień § 5 administrator systemu nie może zarejestrować jakiejkolwiek osoby w systemie informatycznym.

§ 7

1. Użytkownik jest wyrejestrowywany z systemu informatycznego w każdym przypadku utraty przez niego uprawnień do dostępu do danych osobowych, co ma miejsce w przypadku:
   - ustania zatrudnienia tego użytkownika w Urzędzie – o czym informację administrator systemu i administrator bezpieczeństwa informacji uzyskuje od upoważnionego pracownika działu kadr Urzędu, bądź
   - zmiany zakresu obowiązków tego użytkownika - o czym informację administrator systemu i administrator bezpieczeństwa informacji uzyskuje od przełożonego użytkownika.
2. Poza przypadkami wskazanymi w ust. 1 użytkownik jest wyrejestrowywany z systemu informatycznego w każdym przypadku odwołania wydanego temu użytkownikowi upoważnienia.

§ 8

W przypadkach wskazanych w § 7 administrator systemu w uzgodnieniu z administratorem bezpieczeństwa informacji co do użytkownika, który utracił uprawnienia do dostępu do systemu informatycznego, dokonuje niezwłocznie następujących czynności:

1. blokuje jego profil, co powoduje, że osoba ta nie ma możliwości „zalogowania się" do sieci lub aplikacji;
2. wyrejestrowuje jego identyfikator;
3. unieważnia jego hasło;
4. podejmuje inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych osobowych.

§ 9

1. Identyfikator, który utracił ważność nie może być ponownie przydzielony innemu użytkownikowi.
2. Administrator systemu obowiązany jest gromadzić odrębnie identyfikatory, które utraciły ważność.

Rozdział III

Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

§ 10

Mając na względzie, iż system informatyczny przetwarzający dane osobowe powinien być wyposażony w mechanizmy uwierzytelnienia użytkownika oraz kontroli dostępu do tych danych dla każdej osoby upoważnionej ustalany jest odrębny identyfikator i hasło, tak aby bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym mógł mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła. Hasła dostępu i identyfikatory przyznawane są indywidualnie dla każdego z użytkowników .

§ 11

Identyfikator użytkownika:

1) jest niepowtarzalny ;
2) po wyrejestrowaniu użytkownika z systemu informatycznego Urzędu nie jest przydzielany innej osobie;
3) nie podlega zmianie;
4) jest wpisywany do ewidencji osób upoważnionych do przetwarzania danych osobowych wraz z imieniem i nazwiskiem użytkownika i rejestrowany w systemie informatycznym.

§ 12

Hasło użytkownika:

1) jest zmieniane indywidualnie przez użytkownika i znane tylko użytkownikowi, który się nim posługuje;
2) nie jest zapisywane w systemie w postaci jawnej;
2) jest zmieniane co najmniej raz na miesiąc;
3) jest utrzymywane w tajemnicy, również po upływie jego ważności.

§ 13

Osobą odpowiedzialną w Urzędzie za definiowanie parametrów haseł użytkowników jest administrator systemu (minimalną długość hasła, częstotliwość jego zmiany, unikalność hasła).

§ 14

Zmiany haseł dokonuje się w następujący sposób:

1) Hasło powinno być skonstruowane z co najmniej 8 znaków alfanumerycznych.
2) Hasła zmieniane są co najmniej raz na miesiąc.
3) Zachowując wymóg zmieniania haseł przez użytkowników co najmniej raz na miesiąc, hasła użytkowników nie mogą się powtarzać.
4) Hasła nie mogą składać się z kombinacji znaków mogących prowadzić do odszyfrowania ich przez osoby nieupoważnione.
5) Niezależnie od wymogu zmieniania haseł przez użytkowników co najmniej raz na miesiąc, hasło winno być zmienione przez użytkownika niezwłoczne w przypadku powzięcia podejrzenia lub stwierdzenia, że z hasłem mogły zapoznać się osoby trzecie.

§ 15

1. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu hasła, którym się posługuje lub posługiwał.
2. Użytkownik obowiązany jest utrzymywać hasła którymi się posługuje lub posługiwał w ścisłej tajemnicy, co obejmuje, w szczególności dołożenie przez niego wszelkich starań w celu uniemożliwienia zapoznania się przez osoby trzecie z hasłem nawet po ustaniu jego ważności, czy też użycia hasła przez te osoby.
3. W przypadku powzięcia przez użytkownika podejrzenia lub stwierdzenia, że z hasłem mogły zapoznać się osoby trzecie, obowiązany jest on niezwłocznie powiadomić o tym administratora systemu.
4. Naruszenie przez użytkownika postanowień pkt. 2 lub 3 może stanowić podstawę dla pociągnięcia użytkownika do odpowiedzialności dyscyplinarnej, odszkodowawczej lub karnej w trybie i na zasadach przewidzianych przepisami prawa.
5. Użytkownicy obowiązani są utrzymywać hasła w tajemnicy również po upływie ich ważności

§ 16

1. Hasła użytkownika posiadającego uprawnienia administratora systemu informatycznego przechowuje się poza serwerownią.
2. W przypadkach awaryjnych uprawnienia dostępu do haseł administratora systemu ma administrator bezpieczeństwa informacji.
3. Każdorazowe awaryjne użycie hasła administratora systemu musi być odnotowane.

Rozdział IV

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

§ 17

1. Przed przystąpieniem do pracy w systemie użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych służących do przetwarzania danych osobowych oraz dokonać oględzin swojego stanowiska pracy, ze szczególnym uwzględnieniem czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.
2. W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie zabezpieczenia systemu informatycznego użytkownik obowiązany jest zgłosić ten fakt swojemu przełożonemu, ten zaś administratorowi systemu lub administratorowi bezpieczeństwa informacji

§ 18

1. Użytkownik rozpoczynając pracę obowiązany jest „zalogować się" do systemu komputerowego Urzędu posługując się swoim identyfikatorem i hasłem, dokładając jednocześnie szczególnej staranności aby przy tych czynnościach osoby trzecie nie powzięły wiadomości o treści używanego przez niego hasła. Następnie po podaniu dodatkowego hasła użytkownik ma możliwość „zalogowania się" do aplikacji zawierających dane osobowe.
2. Bez wykonania procedury opisanej w ust.1 jakakolwiek praca w systemie komputerowym Urzędu nie jest możliwa.

§ 19

W sytuacji tymczasowego zaprzestania pracy na skutek opuszczenia stanowiska pracy lub w okolicznościach kiedy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba należy wylogować się z aplikacji zawierającej dane osobowe lub zastosować wygaszacz ekranu zabezpieczony hasłem.

§ 20

Po zakończeniu pracy należy wykonać operację wyrejestrowania się z systemu informatycznego, a następnie wyłączyć stację komputerową.

Rozdział V

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

§ 21

Zbiory danych osobowych oraz programy i narzędzia programowe służące do ich przetwarzania są archiwizowane przez administratora systemu.

§ 22

1. Kopie zapasowe tworzone są raz w tygodniu na odpowiednio opisanych i oznakowanych nośnikach.
2. Administrator systemu obowiązany jest przestrzegać terminów sporządzania kopii zapasowych oraz okresowo dokonywać kontroli możliwości odczytu danych zapisanych na tych kopiach i ich przydatności do odtworzenia danych w przypadku awarii systemu informatycznego

Rozdział VI

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopie zapasowe

§ 23

1. Elektroniczne nośniki informacji oraz wydruki komputerowe przechowuje się w zamykanym pomieszczeniu wyłącznie wówczas, gdy jest to konieczne i dozwolone przepisami prawa.
2. Kopie zapasowe przechowywane są w innych pomieszczeniach niż zbiory danych osobowych eksploatowane na bieżąco.
3. Administrator systemu przechowuje kopie zapasowe poza miejscami przetwarzania danych, w metalowej szafie, do której dostęp mają wyłącznie osoby upoważnione.

§ 24

1. Wydruki komputerowe są bezzwłocznie usuwane po ustaniu ich użyteczności, czego dokonać można w szczególności poprzez zniszczenie ich w sposób trwały, tj. za pomocą niszczarki.
2. Urządzenia, dyski lub inne informatyczne nośniki informacji, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie, czego dokonać można w szczególności poprzez zniszczenie ich w sposób trwały, tj. przez ich mechaniczne zniszczenie.

3. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych, pozbawia się wcześniej zapisu tych danych, postępując zgodnie z pkt. 2.
4. Trwałego zniszczenia zbędnych nośników i wydruków komputerowych dokonuje się na bieżąco w czasie pracy, nie później jednak niż przed opuszczeniem stanowiska pracy.

§ 25

1. Kopiowanie danych osobowych na nośniki informacji i robienie wydruków tych danych jest zabronione, chyba że konieczność ich sporządzenia wynika z nałożonego na użytkownika zakresu obowiązków i jest uzasadniona potrzebą ich wykonania oraz dozwolona przepisami prawa.
2. Wykorzystywanie nośników informacji lub wydruków w innym celu niż wskazany w pkt.1 jest zakazane.

§ 26

1. Kopie zapasowe po ustaniu ich użyteczności są bezzwłocznie usuwane.
2. Kopie zapasowe, które uległy uszkodzeniu podlegają natychmiastowemu zniszczeniu.
3. Niszczenia kopii zapasowych na nośnikach magnetycznych, dokonuje administrator systemu lub upoważniona przez niego osoba.
4. Z nośników magnetycznych dane należy usunąć w sposób uniemożliwiający ich odczytanie, a w przypadku gdy usunięcie danych nie jest możliwe, nośniki podlegają zniszczeniu w stopniu uniemożliwiającym dostęp do zawartych na nich danych.
5. Z nośników podlegających zniszczeniu nie wolno sporządzać wydruków.

Rozdział VII

Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego oraz utratą danych spowodowaną awarią zasilania.

§ 27

1. Na bieżące i bezpośrednie sprawdzanie obecności wirusów komputerowych pozwala oprogramowanie automatycznie monitorujące występowanie wirusów w trakcie załączania lub wczytywania danych z zewnętrznych nośników.
2. Kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych , służących zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.

§ 28

Osobą odpowiedzialną za instalację oprogramowania antywirusowego i jego bieżącą aktualizację jest administrator systemu.

§ 29

1. O każdorazowym wykryciu wirusa przez oprogramowanie monitorujące użytkownik obowiązany jest niezwłocznie poinformować administratora systemu .
2. W sytuacji korzystania z usług specjalistów zewnętrznych należy podjąć działania uniemożliwiające tym osobom dostęp do danych osobowych. Osoby te mogą dokonywać operacji na zainfekowanym komputerze wyłącznie pod opieką administratora systemu.

§ 30

1. Urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, powinny być zabezpieczone przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
2. Stanowiska komputerowe, na których przetwarzane są dane osobowe wyposażone są w zasilacze awaryjne /UPS/.

Rozdział VIII

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

§ 31

1. Przeglądów i konserwacji sprzętu komputerowego dokonuje się w miarę potrzeb wynikających z obciążenia sprzętu komputerowego, warunków w których eksploatowane są dane urządzenia oraz ważności sprzętu dla funkcjonowania całości systemu informatycznego Urzędu.
2. Bieżące przeglądy, konserwacje oraz naprawy dokonywane są przez administratora systemu.

§ 32

Urządzenia, dyski lub inne informatyczne nośniki informacji, przeznaczone do naprawy, gdzie wymagane jest zaangażowanie autoryzowanych firm zewnętrznych, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem administratora systemu.

Rozdział IX

Postanowienia końcowe

§ 33

W sprawach nie uregulowanych niniejszą Instrukcją zastosowanie mają przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych i 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.

§ 34

Instrukcja wchodzi w życie z dniem podpisania.

Załącznik nr 1
do „Instrukcji zarządzania systemem informatycznym
służącym do przetwarzania danych osobowych
w Urzędzie Miejskim w Lęborku

Wniosek o nadanie/zmianę/anulowanie zakresu uprawnień użytkownika oraz o wydanie upoważnienia do przetwarzania danych osobowych

☐ Nowy użytkownik	☐ Modyfikacja uprawnień	☐ Odebranie uprawnień w systemie informatycznym

Imię i nazwisko użytkownika:	Nazwa komórki organizacyjnej:
Miejsce przetwarzania/numer pokoju:	Stanowisko:
Opis zakresu uprawnień użytkownika w systemie informatycznym: WG –wgląd, W – wprowadzanie, M – modyfikacja, U – usuwanie, A – archiwizacja *) zakreślić odpowiednio krzyżykiem	

Uprawnienia	WG	W	M	U	A
Nazwy programów komputerowych/modułów					

Data i podpis bezpośredniego przełożonego użytkownika systemu:	
Data i podpis AS:	Data i podpis ABI:

Wypełnia Administrator Systemu:

Identyfikator użytkownika:.....
Data zarejestrowania użytkownika w systemie:.....
Data wyrejestrowania użytkownika z systemu.....

Podpis administratora:.....

Załącznik Nr 2
do zarządzenia Nr .66./2013
Burmistrza Miasta Lęborka
z dnia 10.09.2013 r.....

Polityka Bezpieczeństwa Ochrony Danych Osobowych

w Urzędzie Miejskim w Lęborku

BURMISTRZ MIASTA
Witold Namyślak
Zatwierdzam do stosowania

Rozdział I

Postanowienia ogólne

§ 1

Podstawę prawną niniejszego dokumentu stanowi: ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych /tekst jednolity: Dz. U. 2002r. Nr 101 poz. 926 ze zm./, rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. /Dz. U. 2004r. Nr 100 poz. 1024/ oraz ustawa z dnia 5 sierpnia 2010r. o ochronie informacji niejawnych /Dz. U. 2010r. Nr 182 poz. 1228/ wraz z aktami wykonawczymi do obu ustaw. Niniejszy dokument jest wewnętrznym dokumentem Urzędu Miejskiego w Lęborku opisującym politykę bezpieczeństwa w zakresie odnoszącym się do sposobu przetwarzania danych osobowych oraz środków ich ochrony.

§ 2

Polityka bezpieczeństwa jest to zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych wewnątrz określonej organizacji.
Odnosi się ona całościowo do problemu zabezpieczenia danych osobowych u administratora danych tj. zabezpieczenia danych przetwarzanych tradycyjnie i danych przetwarzanych w systemach informatycznych.
Celem polityki bezpieczeństwa jest zapewnienie ochrony danych osobowych przetwarzanych przez Urząd Miejski w Lęborku przed wszelakiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.
Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.
Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

1. poufność danych - rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
2. integralność danych - rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
3. rozliczalność danych - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
4. integralność systemu - rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

§ 3

Polityka bezpieczeństwa zawiera w szczególności:

1. wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe;
2. wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;

3. opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
4. sposób przepływu danych pomiędzy poszczególnymi systemami;
5. określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Rozdział II

Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe

§ 4

1. Stacjonarny sprzęt komputerowy, przy użyciu którego przetwarzane są dane osobowe, znajduje się w budynkach i pomieszczeniach, zwanych dalej obszarem, wyszczególnionych w załączniku nr 1 do dokumentu „Polityka bezpieczeństwa". Załącznik ten otrzymuje brzmienie: „Wykaz budynków i pomieszczeń, w którym przetwarzane są dane osobowe".
2. Tradycyjne nośniki danych /dokumenty źródłowe/ stanowiące podstawę do przetwarzania danych w systemie informatycznym zgodnie z instrukcją kancelaryjną podlegają archiwizowaniu i przechowywane są w archiwum Urzędu.
3. W pomieszczeniach, w których znajduje się stacjonarny sprzęt komputerowy służący do eksploatowania na bieżąco zbiorów danych osobowych, nie mogą być przechowywane kopie awaryjne.
4. Przebywanie wewnątrz obszaru, o którym mowa w ust. 1, osób nieuprawnionych do dostępu do danych osobowych jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych /osoby upoważnionej/ i za zgodą administratora danych lub osoby przez niego upoważnionej.
5. Budynki lub pomieszczenia, o których mowa w ust. 1, powinny być zamykane na czas nieobecności w nich osób upoważnionych, w sposób uniemożliwiający dostęp do nich osób trzecich.

Rozdział III

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

§ 5

1. Polityka bezpieczeństwa identyfikuje zbiory danych osobowych w postaci dokumentacji papierowej i elektronicznej wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

2. Wykaz zbiorów danych osobowych przetwarzanych w systemach informatycznych w Urzędzie wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych przedstawia załącznik nr 2 do dokumentu „Polityka bezpieczeństwa".
3. Załącznik ten otrzymuje brzmienie: „Wykaz zbiorów danych osobowych przetwarzanych w Urzędzie Miejskim w Lęborku w systemach informatycznych".

Rozdział IV

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między mini

§ 6

1. W polityce bezpieczeństwa należy wskazać poszczególne grupy informacji oraz istniejące między nimi relacje identyfikujące w ten sposób pełen zakres danych osobowych, jakie przetwarzane są w określonym zbiorze.
2. Wymóg wskazania powiązań pomiędzy polami informacyjnymi w strukturze zbiorów danych należy rozumieć jako wymóg wskazania wszystkich tych danych, występujących w strukturze zbioru, które poprzez występujące relacje można skojarzyć z określoną osobą.

§ 7

Opis struktury zbiorów danych osobowych przetwarzanych w Urzędzie Miejskim w Lęborku i powiązania między nimi przedstawia się następująco:

1. W zbiorze danych osobowych **„Ewidencja ludności i dowody osobiste"** przetwarzane są dane mieszkańców miasta Lęborka w zakresie:
   a/ danych osobowych mieszkańca /numer ewidencyjny PESEL, nazwisko, imię, kod terytorialny miejscowości, nazwa miejscowości, ulica, numer domu, numer mieszkania, kod pocztowy, płeć, nazwisko rodowe, imię ojca, nazwisko ojca, nazwisko rodowe ojca, imię matki, nazwisko matki, nazwisko rodowe matki, data urodzenia, miejsce urodzenia, kod terytorialny USC, nr aktu urodzenia, stan cywilny, data zmiany, kod terytorialny organu, nazwa organu, numer akt, nazwisko współmałżonka, imię współmałżonka, nr PESEL współmałżonka, forma ustania małżeństwa, nazwa dokumentu tożsamości, seria i numer, data wystawienia, kod terytorialny wystawcy, nazwa wystawcy, wzrost w cm, kolor oczu, znak szczególny, obowiązek wojskowy, nazwa dokumentu wojskowego, seria i numer, stopień wojskowy/;
   b/ danych o zgonie osoby i współmałżonka /data zgonu, kod terytorialny USC, numer aktu zgonu/;
   c/ danych o zawarciu związku małżeńskiego /data, kod terytorialny USC, nr aktu małżeństwa, imię i nazwisko współmałżonka, nr ewidencyjny PESEL współmałżonka/;

d/ danych o ustaniu związku małżeńskiego /data, kod terytorialny organu, nazwa organu, sygnatura akt, forma ustania/;
e/ danych o zmianie obywatelstwa /data zmiany, podstawa prawna, kod obywatelstwa/;
f/ danych o zmianie miejsca zamieszkania /rodzaj zameldowania, data zameldowania, data wymeldowania, kod terytorialny miejscowości, miejscowość, ulica, nr domu, nr mieszkania, kod pocztowy/;
g/ danych o zmianie dokumentu tożsamości /rodzaj dokumentu, seria, numer, nazwa wystawcy, kod terytorialny wystawcy, data wystawienia, termin ważności, fotografia/;
h/ danych o zmianie nazwiska lub imienia /nowe nazwisko lub imię, organ rejestrujący, kod terytorialny organu, nr akt, data zmiany/;
i/ informacji o sprzeciwie przeciwko udostępnianiu danych osobowych /od kiedy/;
j/ informacji o uprawnieniach wyborczych
k/ informacji o osobach dopisanych do rejestru wyborców /data złożenia wniosku, nr decyzji, data wydania decyzji, podstawa prawna, data skreślenia z rejestru, nr decyzji, podstawa skreślenia/.

2. W zbiorach danych osobowych **„Podatki i opłaty lokalne oraz inne opłaty"** i **„Akta referatu ds. księgowości majątkowej"** przetwarzane są dane osobowe w zakresie:
   a/ danych osobowych podatników /Numer Identyfikacji Podatkowej NIP, numer ewidencyjny PESEL, nazwisko, imiona, imię ojca, imię matki, data urodzenie, seria i numer dowodu osobistego, adres zamieszkania-kod pocztowy, miejscowość, ulica, numer domu, numer mieszkania, stan cywilny, imię współmałżonka, nazwisko współmałżonka/
   b/ danych dotyczących dzierżaw nieruchomości /numer ewidencyjny dzierżawcy, numer działki, obręb, położenie nieruchomości-kod pocztowy, miejscowość, ulica, numer domu, typ dzierżawy, rodzaj dzierżawy, powierzchnia dzierżawy lokalu lub gruntu, kwota czynszu/
   c/ danych dotyczących użytkowania wieczystego /numer ewidencyjny użytkownika wieczystego, obręb działki, numer działki, numer mapy, położenie działki-ulica, numer porządkowy, numer księgi wieczystej, data zawarcia aktu notarialnego, data wyceny, wartość/
   d/ danych dotyczących płatników opłaty targowej
   e/ danych dotyczących płatników podatku od środków transportowych /nr rejestracyjny środka transportu, marka, data zarejestrowania, kod środka transportu, rodzaj, kwota podatku, data wyrejestrowania/
   f/ danych dotyczących tytułów egzekucyjnych /nr tytułu egzekucyjnego, kwota/
   g/ danych dotyczących płatników podatku rolnego /kod płatnika, imię ojca współmałżonka, data urodzenia współmałżonka, rodzaj użytków rolnych, kwota podatku/
   h/ danych dotyczących płatników podatku od posiadania psa.

3. W zbiorze danych osobowych **„System Informacji o Terenie"** przetwarzane są dane w zakresie:
   a/ danych osobowych użytkowników wieczystych lub dzierżawców gruntów /nr ewidencyjny PESEL, nazwisko, imiona, imię ojca, imię matki, kod pocztowy, miejscowość, ulica, nr domu, nr mieszkania/
   b/ danych dotyczących budynków na gruntach dzierżawionych lub w użytkowaniu wieczystym /nr decyzji, data decyzji, typ budynku, typ własności, kubatura, powierzchnia zabudowy, powierzchnia całkowita, powierzchnia użytkowa, ilość izb/.

4. W zbiorze danych osobowych **„Akta Stanu Cywilnego"** przetwarzane są dane w zakresie:
   a/ danych osobowych /nr ewidencyjny PESEL, nazwisko, imiona, imię ojca, nazwisko ojca, imię matki, nazwisko matki, data urodzenia, miejsce urodzenia, kod pocztowy, miejscowość, ulica, nr domu, nr mieszkania, seria i nr dowodu osobistego, zawód, wykształcenie, nazwisko rodowe, nazwisko z poprzedniego małżeństwa/
   b/ danych dotyczących urodzenia /płeć, godzina urodzenia, data urodzenia, miejsce urodzenia, data i numer aktu urodzenia, imię i nazwisko ojca, imię i nazwisko matki/
   c/ danych dotyczących zgonu lub odnalezienia zwłok /data, godzina, miejsce zgonu lub odnalezienia zwłok, data i numer aktu zgonu, nazwisko, imię, adres osoby zgłaszającej zgon/
   d/ danych dotyczących zawarcia małżeństwa /data i miejsce zawarcia małżeństwa, data i numer aktu małżeństwa, imię i nazwisko współmałżonka, nr ewidencyjny współmałżonka, stan cywilny, miejsce wystawienia i nr aktu urodzenia żony lub męża, nazwiska po zawarciu małżeństwa/
   e/ danych dotyczących rozwiązania lub unieważnienia małżeństwa /data, sygnatura akt, nazwa organu, miejsce organu, nazwiska po rozwiązaniu lub unieważnianiu małżeństwa/
   f/ danych dotyczących orzeczeń sądu o ustaleniu ojcostwa, zaprzeczeniu ojcostwa, przysposobieniu dziecka /imię i nazwisko osoby przysposabiającej dziecko/.

5. W zbiorze danych osobowych **„Ewidencja spełniania obowiązku nauki"** przetwarzane są dane w zakresie:
   a/ nazwisk i imion,
   b/ imion rodziców,
   c/ daty urodzenia,
   d/ adresu zamieszkania lub pobytu.

6. W zbiorze danych osobowych **„Awans zawodowy nauczycieli"** przetwarzane są dane w zakresie:
   a/ nazwisk i imion,
   b/ imion rodziców,
   c/ daty urodzenia,
   d/ miejsca urodzenia,
   e/ adresu zamieszkania lub pobytu,
   f/ miejsca pracy,
   g/ zawodu,
   h/ wykształcenia,
   i/ numeru telefonu.

7. W zbiorze danych osobowych **„Stypendia szkolne"** przetwarzane są dane w zakresie:
   a/ nazwisk i imion,
   b/ imion rodziców,
   c/ daty urodzenia,
   d/ miejsca urodzenia,
   e/ adresu zamieszkania i pobytu,
   f/ numeru ewidencyjnego PESEL,
   g/ miejsca pracy.

8. W zbiorze danych osobowych **„Uzależnienie od alkoholu"** przetwarzane są dane w zakresie:

a/ nazwisk i imion,
b/ imion rodziców,
c/ daty urodzenia,
d/ miejsca urodzenia,
e/ adresu zamieszkania lub pobytu,
f/ numeru ewidencyjnego PESEL,
g/ numeru telefonu,
h/ stanu zdrowia,
i/ nałogów.

9. W zbiorze danych osobowych **„System Informacji Oświatowej"** przetwarzane są dane w zakresie:

a/ daty urodzenia,
b/ numeru ewidencyjnego PESEL,
c/ miejsca pracy,
d/ zawodu,
e/ wykształcenia.

10. W zbiorze danych osobowych **„Ewidencja wniosków o ukaranie i osób ukaranych"** przetwarzane są dane w zakresie:

a/ nazwisk i imion,
b/ imion rodziców,
c/ daty urodzenia,
d/ adresu zamieszkania lub pobytu,
e/ numeru ewidencyjnego PESEL,
f/ serii i numeru dowodu osobistego.

11. W zbiorze danych osobowych **„Sprawy wojskowe i obrony cywilnej"** przetwarzane są dane w zakresie;

a/ nazwisk i imion,
b/ imion rodziców,
c/ daty urodzenia,
d/ adresu zamieszkania lub pobytu,
e/ numeru ewidencyjnego PESEL,
f/ serii i numeru dowodu osobistego,
g/ miejsca pracy,
h/ zawodu,
i/ wykształcenia.

12. W zbiorze danych osobowych **„Oświadczenia majątkowe"** przetwarzane są dane w zakresie:

a/ nazwisk i imion,
b/ daty urodzenia,
c/ miejsca urodzenia,
d/ adresu zamieszkania lub pobytu,
e/ Numeru Identyfikacji Podatkowej,
f/ miejsca pracy,
g/ nazwisk rodowych,
h/ stanowisk lub funkcji,

i/ informacji o stanie majątkowym,
j/ informacji dotyczącej działalności gospodarczej,
k/ informacji dotyczącej współmałżonka,
l/ informacji zawartych w zeznaniach o wysokości osiągniętego dochodu (PIT).

13. W zbiorze danych osobowych **„Oświadczenia majątkowe radnych"** przetwarzane są dane w zakresie:
a/ nazwisk i imion,
b/ daty urodzenia,
c/ miejsca urodzenia,
d/ adresu zamieszkania lub pobytu,
e/ Numeru Identyfikacji Podatkowej,
f/ miejsca pracy,
g/ nazwisk rodowych,
h/ stanowisk lub funkcji,
i/ informacji o stanie majątkowym,
j/ informacji dotyczącej działalności gospodarczej,
k/ informacji dotyczącej współmałżonka,
l/ informacji zawartych w zeznaniach o wysokości osiągniętego dochodu (PIT).

14. W zbiorze danych osobowych **„Elektroniczny obieg dokumentów"** przetwarzane są dane w zakresie:
a/ nazwisk i imion,
b/ adresu zamieszkania lub pobytu,
c/ numeru ewidencyjnego PESEL,
d/ Numeru Identyfikacji Podatkowej,
e/ numeru telefonu,
f/ REGON-u,
g/ adresu e-mail.

Rozdział V

Sposób przepływu danych pomiędzy systemami informatycznymi

§ 8

Przepływ informacji pomiędzy zbiorami danych osobowych a systemem informatycznym ma charakter dwukierunkowy, co oznacza, że informacje pobierane są do odczytu i zapisu.

§ 9

Wszystkie dane osobowe przenoszone są między systemami informatycznymi automatycznie .

§ 10

1. Pliki aktualizacyjne zbioru danych osobowych "Ewidencja ludności i dowody osobiste" przesyłane są drogą elektroniczną /poczta e-mail/ w postaci zaszyfrowanej do Pomorskiego Urzędu Wojewódzkiego w Gdańsku.
2. Dane związane z wydawaniem dowodów osobistych przesyłane są do Centrum Personalizacji Dokumentów przy Ministerstwie Spraw Wewnętrznych w Warszawie, w postaci zaszyfrowanej z wykorzystaniem transmisji radiowej.

Rozdział VI

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

§ 11

A) Zabezpieczenia organizacyjne:

1. został wyznaczony administrator bezpieczeństwa informacji
2. została opracowana i wdrożona polityka bezpieczeństwa
3. została opracowana i wdrożona instrukcja zarządzania systemem informatycznym
4. do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych
5. prowadzona jest ewidencja osób upoważnionych do przetwarzania danych
6. osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego
7. osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy
8. przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych
9. przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych
10. stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami przetwarzającymi dane osobowe.

B) Zabezpieczenia ochrony fizycznej danych osobowych:

1. obiekty oraz mienie Urzędu Miejskiego w Lęborku objęte jest dozorem fizycznym wykonywanym przez pracowników dozoru lub licencjonowanych pracowników ochrony w godzinach od 15.00 do 18.00 w dni robocze, oraz w soboty według zgłoszonych potrzeb w tym zakresie
2. stosowany jest monitoring systemu alarmowego wykonywany przez pracowników dozoru lub licencjonowanych pracowników ochrony codziennie całodobowo, z wyjątkiem godzin dozoru fizycznego oraz godzin pracy urzędu

3. wejścia i wyjścia pracowników poza godzinami pracy, w czasie dozoru fizycznego Urzędu są odnotowywane w rejestrze dozoru

C) Zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej:

1. zabezpieczenia stosuje się dla fizycznych elementów systemu, ich połączeń oraz systemów operacyjnych
2. bazy danych osobowych przetwarzane są na serwerach zabezpieczonych zasilaczem awaryjnym.

D) Zabezpieczenia narzędzi programowych i baz danych.

Zabezpieczenia (techniczne i programowe) stosuje się dla procedur, aplikacji, programów i innych narzędzi programowych przetwarzających dane osobowe.

§ 12

1. Ekrany monitorów ustawione są do wewnątrz sali wydzielonej do przetwarzania danych osobowych, w taki sposób, by uniemożliwić wgląd lub spisanie zawartości aktualnie wyświetlanej na ekranie monitora.
2. Programy zainstalowane na komputerach stacjonarnych obsługujących przetwarzanie danych osobowych użytkowane są z zachowaniem praw autorskich i posiadają licencje.
3. Decyzję o instalacji oprogramowania systemowego oraz oprogramowania użytkowego obsługującego przetwarzanie danych osobowych, podejmuje administrator systemu.
4. Używanie sprzętu komputerowego przez użytkownika w trakcie przetwarzania danych osobowych do innych celów jest zabronione.

§ 13

1. Stały dostęp do pomieszczeń, w których przetwarzane są dane osobowe, mają tylko użytkownicy.
2. Inne osoby mogą przebywać w tych pomieszczeniach wyłącznie w obecności co najmniej jednego użytkownika.
3. Zakaz wyrażony w ust. 2, nie dotyczy innych, niż określeni w ust. 1, pracowników Administratora Danych oraz pracowników służb technicznych, porządkowych, itp.
4. W trakcie prac technicznych wykonywanych przez osoby trzecie, przetwarzanie danych na wydzielonych stanowiskach jest zabronione, a sprzęt komputerowy musi być wyłączony.

§ 14

1) Administrator bezpieczeństwa informacji dokonuje kontroli sprawności funkcjonowania zabezpieczeń.
2) Administrator systemu jest odpowiedzialny za właściwe funkcjonowanie mechanizmów uwierzytelniania użytkownika oraz kontroli dostępu do danych osobowych.

Rozdział VII

Postanowienia końcowe

§ 15

W sprawach nie uregulowanych niniejszym dokumentem zastosowanie mają przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2002 r. nr 101, poz. 926 ze zm.) i 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. 2004 r. nr 100, poz. 1024).

§ 16

Dokument wchodzi w życie z dniem podpisania.

Załącznik nr 1

do dokumentu

„Polityka bezpieczeństwa"

Wykaz budynków i pomieszczeń, w którym przetwarzane są dane osobowe

Lp.	Budynek – dane adresowe	Pomieszczenie
1.	Urząd Miejski w Lęborku, 84-300 Lębork, ul. Armii Krajowej 14	A1, A4, A7, A8, A9, A10, A12, A16, A201, A202, B118, B119, B120, B121, B208, B300, B301, C1, C2, C3, C4, C201, D126, BOX 1, BOX 2
2.	Szkoła Podstawowa Nr 3 w Lęborku, 84-300 Lębork, ul. Kossaka 103	nr 10, 11, 13, 20, 21, 25, 34, 35, 36, 38, 39
3.	Szkoła Podstawowa Nr 5 w Lęborku, 84-300 Lębork, ul. Kościuszki 14	nr 1, 3, 4, 5, 10, 14, 16, 18, 53
4.	Szkoła Podstawowa Nr 8 w Lęborku, 84-300 Lębork, ul. Mireckiego 10	nr 1, 2, 3, 5, 15, 24
	84-300 Lębork, ul. Plater 13	nr 3, 3a, 3b, 5, 6, 7, 8
5.	Zespół Szkół Nr 3 w Lęborku, 84-300 Lębork, ul. Aleja Wolności 31	nr 2, 12, 27, 31, 32, 33

załącznik nr 2
do dokumentu
„Polityka bezpieczeństwa"

Wykaz zbiorów danych osobowych przetwarzanych w Urzędzie Miejskim w Lęborku w systemach informatycznych

L.p.	Nazwa zbioru danych osobowych (1)	Program służący do przetwarzania baz danych	Zabezpieczenie bazy (2)	Nr pokoju
1.	**EWIDENCJA LUDNOŚCI I DOWODY OSOBISTE**			
	Ewidencja ludności	ELUD+	I, UPSB	C3, C4
	Rejestr Wyborców	WYB+	I, UPSB	C3, C4
	System Wydawania Dowodów Osobistych	SWDO	I, UPSB	C4
2.	**A. PODATKI I OPŁATY LOKALNE ORAZ INNE OPŁATY** **B. AKTA REFERATU DS. KSIĘGOWOŚCI MAJĄTKOWEJ**			
	System Windykacji Opłat i Podatków	WIP+	I, UPSB	A7, A8,A9,A10,A12
	System Naliczania Podatków od Gruntów i Nieruchomości	POGRUN+	I, UPSB	A9, A10, A12
	System Naliczania Podatków od Środków Transportu	POST+	I, UPSB	A7, A10
	System Informacji o Mieszkańcach, Właścicielach i Użytkownikach	INFO+	I, UPSB	A7, A8,A9,A10,A12
	System Naliczania Opłat za Użytkowanie Wieczyste Gruntów	EGW+	I, UPSB	A8, B119
	Ewidencja opłat i podatków	OPERA	I, UPSB	A8, B119
	Ewidencja kont i operacji księgowych z tytułu sprzedaży nieruchomości – bieżący okres	NIERUCH	I, UPSB	A8

	Ewidencja kont i operacji księgowych z tytułu sprzedaży nieruchomości – przyszły okres	WU	I, UPSB	A8
	Ewidencja kont i operacji księgowych dot. opłaty za wieczyste użytkowanie gruntu	HIPO	UPSB	A8
	Egzekucja komornicza	EGZ.KOM	I, UPSB	A8
3.	**SYSTEM INFORMACJI O TERENIE**	SIT	I, UPSB	A8, B119, B118
4.	**AKTA STANU CYWILNEGO**	PB_USC	I	A1
5.	**EWIDENCJA SPEŁNIANIA OBOWIĄZKU NAUKI**	Microsoft Excel		B121
6.	**AWANS ZAWODOWY NAUCZYCIELI**	Microsoft Word		B121
7.	**STYPENDIA SZKOLNE**	Microsoft Excel		C1, C2
8.	**UZALEŻNIENIE OD ALKOHOLU**	Microsoft Excel		C1, C2
9.	**SYSTEM INFORMACJI OŚWIATOWEJ**	SIO		B121
10.	**ELEKTRONICZNY OBIEG DOKUMENTÓW**	SIDAS EZD	I, UPSB	BOX 1, BOX 2

Legenda:
(1) nazwa zwyczajowa lub opis
(2) (I) indywidualne hasło dostępu do bazy, (UPSB) UPS Bazy

Załącznik Nr 3
do zarządzenia Nr..66/2013
Burmistrza Miasta Lęborka
z dnia 10.09.2013r.....

Instrukcja postępowania w sytuacjach awaryjnych

Instrukcja definiuje katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Celem instrukcji jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

§ 1

Każdy pracownik Urzędu Miejskiego w Lęborku w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować bezpośredniego przełożonego, administratora bezpieczeństwa informacji lub administratora systemu.

§ 2

Do typowych zagrożeń bezpieczeństwa danych osobowych należą:

a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
b. niewłaściwe zabezpieczenie sprzętu IT wraz z oprogramowaniem przed wyciekiem, kradzieżą i utratą danych osobowych
c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady tzw. czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).

§ 3

Do typowych incydentów bezpieczeństwa danych osobowych należą:

a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)
b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych)
c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

§ 4

W przypadku stwierdzenia wystąpienia zagrożenia administrator bezpieczeństwa informacji w porozumieniu z administratorem systemu prowadzi postępowanie wyjaśniające w toku, którego:

a. ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki
b. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości.

§ 5

W przypadku stwierdzenia incydentu (naruszenia) administrator bezpieczeństwa informacji w porozumieniu z administratorem systemu prowadzi postępowanie wyjaśniające w toku, którego:

a. ustala czas wystąpienia naruszenia, jego zakres, przyczyny oraz skutki
b. zabezpiecza ewentualne dowody
c. ustala osoby odpowiedzialne za naruszenie
d. podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody)
e. wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości.

§ 6

Każda organizacja powinna mieć plan działania na wypadek wystąpienia awarii. Celem planu awaryjnego jest umożliwienie funkcjonowania organizacji w czasie wystąpienia sytuacji kryzysowej. Plan ten z reguły składa się z dwóch głównych części:

- Planu Zapewnienia Ciągłości Działania,
- Planu Odtwarzania.

Plan Zapewnienia Ciągłości działania jest jednym z kluczowych czynników sukcesu działania organizacji. Możliwość sprawnego i szybkiego przywrócenia stanu sprzed awarii oraz kontynuowanie działalności podczas jej trwania ogranicza ryzyko utraty reputacji i ewentualnych strat finansowych.

§ 7

O wystąpieniu sytuacji kryzysowej i potrzebie uruchomienia planu awaryjnego należy niezwłocznie powiadomić administratora bezpieczeństwa danych lub administratora systemu.

§ 8

Administrator systemu dokonuje sprawdzenia stopnia uszkodzenia bazy danych i podejmuje działania mające na celu jej odtworzenie lub w przypadku awarii technicznych organizuje sprzęt zastępczy.

§ 9

Plan postępowania w sytuacjach awaryjnych, zmierzający do odtworzenia utraconych danych przedstawia poniższy schemat:

Schemat blokowy planu awaryjnego