Załącznik Nr 1
do Zarządzenia
Burmistrza Lubienia Kujawskiego
Nr 4/2016 z dnia 21 stycznia 2016r.

Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miejskim w Lubieniu Kujawskim

Lubień Kujawski, 2016

SPIS TREŚCI

1. WPROWADZENIE

Celem Polityki Bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miejskim w Lubieniu Kujawskim, zwanej dalej Polityką Bezpieczeństwa, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania w Urzędzie Miejskim w Lubieniu Kujawskim informacji zawierających dane osobowe, a przede wszystkim zapewnienie ochrony przetwarzanych danych osobowych przed wszelkiego rodzaju zagrożeniami, tak zewnętrznymi jak i wewnętrznymi.

Polityka Bezpieczeństwa została utworzona w związku z wymaganiami zawartymi w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz rozporządzeniu 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. Opracowany dokument jest zgodny również z dyrektywą 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osób oraz ochrony prywatności w sektorze komunikacji elektronicznej.

Obszarem przetwarzania danych osobowych w Urzędzie Miejskim w Lubieniu Kujawskim są wydzielone pomieszczenia w budynku urzędu, który mieści się przy ul. Wojska Polskiego 29.

1. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w Urzędzie Miejskim w Lubieniu Kujawskim rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych.
2. 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;
   5) dostępność informacji - rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
   6) zarządzanie ryzykiem - rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

Administratorem Danych Osobowych przetwarzanych w Urzędzie Miejskim w Lubieniu Kujawskim jest Burmistrz Lubienia Kujawskiego.

Na Administratora Bezpieczeństwa Informacji w Urzędzie Miejskim w Lubieniu Kujawskim powołuje Burmistrz Lubienia Kujawskiego odrębnym zarządzeniem.

2. PODSTAWOWE DEFINICJE

Przez użyte w Polityce Bezpieczeństwa określenia należy rozumieć:

1. **Polityka Bezpieczeństwa** – Polityka Bezpieczeństwa Ochrony Danych Osobowych w Urzędzie Miejskim w Lubieniu Kujawskim;
2. **Urząd** – rozumie się jako Urząd Miejski w Lubieniu Kujawskim;
3. **Administrator Danych Osobowych (ADO)** – organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych. Funkcje Administratora Danych Osobowych w Urzędzie pełni Burmistrz Lubienia Kujawskiego;
4. **Administrator Bezpieczeństwa Informacji (ABI)** - rozumie się przez to osobę wyznaczoną przez Administratora Danych Osobowych, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
5. **Administrator Systemów Informatycznych (ASI)** – osoba odpowiedzialna za stosowanie technicznych i organizacyjnych środków ochrony danych osobowych w Urzędzie;
6. **Ustawa** - ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2014 r. poz.1182);
7. **Rozporządzenie** - rozporządzenie 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. z 2004 r. Nr 100, poz. 1024);
8. **GIODO** – Generalny Inspektor Ochrony Danych Osobowych;
9. **Dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
10. **Zgoda osoby, które dane dotyczą** – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda nie może być domniemana z oświadczenia woli o innej treści. Zgoda może być odwołana w każdym czasie.
11. **Dane wrażliwe** – dane o pochodzeniu rasowym lub etnicznym, poglądach politycznych, przekonaniach religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących wyroków, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym;

12. **Zbiór danych osobowych** - rozumie się 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;
13. **Baza danych** - zbiór uporządkowanych powiązanych ze sobą tematycznie zapisanych np. w pamięci wewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze – rekordów lub obiektów, w których są zapisywane dane osobowe;
14. **Przetwarzanie danych** - rozumie się przez to 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;
15. **System informatyczny** – to zespół urządzeń, programów, procedur i narzędzi zastosowanych w celu przetwarzania danych;
16. **System tradycyjny** - rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;
17. **Zabezpieczenie danych w systemie informatycznym** – to wdrożenie i eksploatacja środków technicznych zapewniających ochronę danych;
18. **Usuwanie danych** – to trwałe zniszczenie danych osobowych uniemożliwiające identyfikację osoby;
19. **Odbiorca danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe;
20. **Użytkownik** - rozumie się przez to upoważnionego przez Administratora danych lub Administratora Bezpieczeństwa Informacji, wyznaczonego do przetwarzania danych osobowych pracownika Urzędu Miejskiego w Lubieniu Kujawskim, który odbył stosowne szkolenie w zakresie ochrony tych danych;
21. **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
22. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie upoważnionej do pracy w systemie informatycznym;
23. **Osoba upoważniona** – osoba posiadająca wydane przez ADO upoważnienie do przetwarzania danych osobowych w Urzędzie Miejskim w Lubieniu Kujawskim.

3. AKTUALIZACJA TREŚCI ZAWARTEJ W „POLITYCE BEZPIECZEŃSTWA"

W związku ze zmianami w zakresie ochrony danych osobowych oraz mając na uwadze zmiany przepisów w tym zakresie, Administrator Bezpieczeństwa Informacji („ABI") zobowiązuję się dokonywać każdorazowo do dnia 30 kwietnia każdego roku aktualizacji treści zawartej w niniejszej Polityce Bezpieczeństwa przetwarzania danych osobowych oraz Instrukcji Zarządzania Systemem Informatycznym.

Aktualizacja zapisów prowadzona będzie pod kątem zgodności stanu zapisanego ze stanem faktycznym, w szczególności danych zawartych w następujących dokumentach:

- „Wykaz budynków i pomieszczeń tworzących obszar, w którym przetwarzane są dane",
- „Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych",
- „Ewidencja osób upoważnionych do przetwarzania danych osobowych w Urzędzie",
- „Rejestr nośników komputerowych zawierających dane osobowe".

4. REJESTRACJA ZBIORÓW DANYCH

Począwszy od dnia 1 stycznia 2015r. Administrator Danych Osobowych nie ma obowiązku zgłaszania do GIODO nowych zbiorów danych osobowych, z wyjątkiem zbiorów o których mowa w art. 27, ust. 1, art. 43, ust. 1 i 1a ustawy o ochronie danych osobowych z dnia 27 sierpnia 2009r.

W przypadku gdy Administrator Danych Osobowych nie wyznaczy Administratora Bezpieczeństwa Informacji Zgodnie z art. 40 ustawy ADO jest zobowiązany zgłosić zbiór danych osobowych do rejestracji, której dokonuje Generalny Inspektorat Ochrony Danych Osobowych w celu przetwarzania tych danych, z wyjątkiem zbiorów które z mocy ustawy o ochronie danych osobowych nie podlegają obowiązkowi rejestracji lub gdy Administrator Danych powołał administratora bezpieczeństwa informacji oraz zgłosił go do Generalnego Inspektora do rejestracji. Zgodnie z art. 41 ust. 2 ustawy o ochronie danych osobowych Administrator Danych za pośrednictwem Administratora Bezpieczeństwa Informacji („ABI") jest obowiązany zgłaszać Generalnemu Inspektorowi Danych Osobowych zbiory danych osobowych podlegające zgłoszeniu do „GIODO" oraz zgłaszanie każdą zmianę informacji w terminie 30 dni od dnia dokonania zmiany w zbiorze danych. W związku z powyższym Administrator Danych zobowiązuję wszystkich użytkowników systemu Informatycznego jednostki do niezwłocznego informowania (nie później niż w terminie 7 dni od dnia zmiany stanu poprzedniego) o likwidacji, utworzeniu lub zmianie zawartości zbioru danych, a wówczas Polityka bezpieczeństwa będzie podlegała aktualizacji w ciągu roku. Konieczność przetwarzania danych osobowych w nowym zbiorze danych osobowych wymaga konsultacji z ABI jednostki w celu sprawdzenia, czy dany zbiór nie podlega, w myśl przepisów (art. 43 ust. 1 ustawy) zwolnieniu z obowiązku zgłoszenia do rejestracji. W sytuacji gdy

zachodzi konieczność zgłoszenia zbioru do „GIODO" rejestracja następuje na pisemny wniosek przygotowany przez ABI zatwierdzony przez ADO. Zgodnie z ustawą ADO dokonuje zgłoszenia zbioru do rejestracji przed rozpoczęciem przetwarzania danych, to znaczy przed pierwszą czynnością, jaką można wykonać na danych osobowych tj. przed pozyskaniem pierwszych danych do zbioru. W sytuacji gdy ADO zamierza przetwarzać tzw. dane szczególnie wrażliwe wymagane jest uprzednie zarejestrowanie zbioru danych przez Generalnego Inspektora Danych Osobowych („GIODO"). ABI prowadzi jawny rejestr zbiorów danych osobowych.

5. UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Do przetwarzania danych osobowych w Urzędzie Miejskim w Lubieniu Kujawskim mogą być dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych wydane przez ADO Burmistrza Lubienia Kujawskiego.

Pracownicy występują za pośrednictwem ABI do ADO z wnioskiem o wydanie upoważnienia dla użytkownika systemu informatycznego do przetwarzania danych osobowych (wg wzoru stanowiącego ***załącznik nr 2*** do niniejszego dokumentu).

Wyżej wymieniony wniosek powinien zostać złożony przed rozpoczęciem pracy na danych osobowych przez osobę zatrudnioną. We wniosku należy wskazać nazwę zbioru danych ze wskazaniem sposobu ich przetwarzania.

Wniosek o wydanie upoważnienia należy złożyć za pośrednictwem ABI Następnie ADO wydaje upoważnienie do przetwarzania danych osobowych w Urzędzie Miejskim w Lubieniu Kujawskim (wg wzoru stanowiącego ***załącznik nr 3*** do niniejszego dokumentu).

6. UDOSTĘPNIENIE DANYCH ORAZ POWIERZENIE PRZETWARZANYCH DANYCH

Udostępnianie danych:

- nie jest istotne czy udostępnianie danych ma charakter odpłatny czy nie, aby czynność była uznana za udostępnianie,
- nie ma znaczenia (ujmując problem technicznie) czy udostępnianie następuje w formie przekazu ustnego, pisemnego, za pomocą powszechnych środków przekazu lub poprzez sieć komputerową itd.,
- udostępnianie danych osobowych osobom lub podmiotom uprawnionym do ich otrzymania odbywa się na mocy przepisów prawa,
- dane osobowe, z wyłączeniem danych wrażliwych mogą być udostępniane nie w oparciu o przepisy prawa, jeżeli osoba wnioskująca w sposób wiarygodny uzasadni potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą,

- dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazać ich zakres i przeznaczenie.
- udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

Powierzenie przetwarzania danych

W przypadku konieczności przetwarzania danych osobowych przez odrębne podmioty świadczące usługi dla ADO może on powierzyć ich przetwarzanie, w drodze umowy zawartej na piśmie, pod następującymi warunkami:

- umowa powinna być zawarta niezależnie od posiadanej umowy określającej relacje obu stron,
- podmiot, któremu powierzono przetwarzanie danych, może przetwarzać je wyłącznie w zakresie i celu przewidzianych w umowie,
- podmiot, któremu powierzono przetwarzanie danych, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36 i 39 Ustawy oraz spełnić wymagania określone w przepisach o których mowa w art. 39a Ustawy. W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak ADO.
- odpowiedzialność za przestrzeganie przepisów niniejszej ustawy spoczywa na ADO, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodne z tą umową.

7. ŚRODKI ORGANIZACYJNE I TECHNICZNE ZASTOSOWANE DO ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH W URZĘDZIE MIEJSKIM W LUBIENIU KUJAWSKIM

7.1 Środki organizacyjne ochrony danych osobowych stosowane w Urzędzie

W celu stworzenia właściwych zabezpieczeń, które powinny bezpośrednio oddziaływać na procesy przetwarzania danych wprowadza się następujące środki organizacyjne:

- przetwarzanie danych osobowych w Urzędzie może odbywać się wyłącznie w ramach wykonywania zadań służbowych,
- do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne upoważnienie,
- unieważnienie upoważnienia następuje koniecznie na piśmie (wg wzoru stanowiącego załącznik nr 2 do niniejszego dokumentu),

- dane osobowe powinny być wyłącznie przetwarzane w budynkach, pomieszczeniach do tego przystosowanych i zabezpieczonych przez osoby upoważnione przez ADO urzędu (wg wzoru stanowiącego ***załącznik nr 4*** do niniejszego dokumentu),
- zbiory danych (bazy danych), których dokonuje się przetwarzania danych osobowych powinny być zabezpieczone przed nieuprawnionym dostępem i zewidencjonowane w wykazie zbiorów danych osobowych, który prowadzi ABI (wg wzoru stanowiącego ***załącznik nr 5*** do niniejszego dokumentu),
- każdy pracownik urzędu co najmniej raz na dwa lata musi odbyć szkolenie z zakresu ochrony danych osobowych. Nowo przyjęty pracownik obowiązkowo odbywa szkolenie przed przystąpieniem do przetwarzania danych,
- każdy upoważniony do przetwarzania danych osobowych w Urzędzie potwierdza pisemnie zapoznanie się z niniejszym dokumentem i zrozumieniem wszystkich zasad bezpieczeństwa (wg wzoru stanowiącego ***załącznik nr 1*** do niniejszego dokumentu). Podpisany dokument jest dołączany do akt osobowych,
- obszar przetwarzania danych osobowych określony w ***załącznik nr 4*** do niniejszego dokumentu, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych,
- przebywanie osób, nieuprawnionych w w/w obszarze jest dopuszczalne za zgodą ADO lub w obecności osoby upoważnionej do przetwarzania danych osobowych,
- pomieszczenia stanowiące obszar przetwarzania danych powinny być zamykane na klucz,
- monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane,
- przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna oraz usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w odpowiednich zamykanych szafach lub biurkach.

7.2 Środki techniczne ochrony danych osobowych stosowane w Urzędzie

- stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową, a także system Firewall stanowiący element programu antywirusowego do ochrony dostęp do sieci komputerowej.
- komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkowania i hasła,
- zbiory danych osobowych przechowywane są w pomieszczeniu zabezpieczonym przed swobodnym dostępem,
- zbiory danych osobowych w formie papierowej przechowywane są w szafach zamykanych na klucz,
- archiwalne zbiory danych osobowych przechowywane są w pomieszczeniu o nazwie archiwum. Klucz do tego pomieszczenia, przechowywany jest w zamykanej szafie na klucz, a dostęp do niego mają wyłącznie upoważnione osoby,
- kopie bezpieczeństwa (kopie zapasowe) przechowuje się miejscach zabezpieczonych przed nieuprawnionym przejęciem, modyfikacją uszkodzeniem lub zniszczeniem, a kopie zbiorów danych osobowych na nośnikach danych (np. dysk zewnętrzny) przechowywane są w zamkniętym na klucz sejfie, a dostęp do niego mają wyłącznie upoważnione osoby,
- pomieszczenia, w których przetwarzane są zbiory danych osobowych zabezpieczone są przed skutkami pożaru za pomocą wolnostojącej gaśnicy,

- dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone komisyjnie w sposób mechaniczny za pomocą niszczarek dokumentów,
- dostęp do zbiorów danych osobowych wymaga uwierzytelnienia z wykorzystaniem spersonalizowanego identyfikatora użytkownika oraz unikatowego hasła użytkownika,
- identyfikator użytkownika, który utracił dostęp do danych osobowych nie może być przydzielony innej osobie,
- systemowe środki pozwalają na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego,
- ASI sporządza okresowo kopie bezpieczeństwa danych osobowych ze wszystkich wykorzystywanych w Urzędzie systemów informatycznych, programów żeby zabezpieczyć się przed utrata danych spowodowaną awarią sprzętu komputerowego,
- zmiana haseł dostępowych następuje przynajmniej raz na 30 dni,
- nie wolno przechowywać danych osobowych na komputerach przenośnych, a pracownik uzyskuję dostęp do tych danych tylko będąc na swoim stanowisku pracy poprzez logowanie do zbiorów danych zapisywanych w odpowiedniej lokalizacji na serwerze urzędu.
- dyski twarde uszkodzone lub wyłączone z eksploatacji przed oddaniem do utylizacji należy trwale pozbawić zapisu lub zniszczyć dysk twardy w ten sposób aby niemożliwym stało się odzyskanie informacji z niego.

8. ZABEZPIECZENIE DOKUMENTACJI PAPIEROWEJ I ELEKTRONICZNEJ PRZED UTRATĄ, ZNISZCZENIEM, ZMIANĄ, SFAŁSZOWANIEM I DOSTĘPEM OSÓB NIEUPOWAŻNIONYCH

8.1 . Dokumentacja w formie papierowej

- Dokumentacja jest własnością wytwarzającego i powinna od momentu powstawania do momentu zniszczenia, po ustaniu okresu archiwizacyjnego, być zabezpieczona przed nieuprawnionym dostępem wypłynięciem, zmianą bądź zniszczeniem,
- dokumentację należy przechowywać w pomieszczeniach, szafach, bądź szufladach zabezpieczonych sprawnym zamkiem, a w momencie kiedy jest ona w użytku nie można jej pozostawić bez dozoru osób uprawnionych do posługiwania się nią,
- dokumentacje archiwizujemy w wyodrębnionym pomieszczeniu (Archiwum), w których systematycznie monitoruje się temperaturę i wilgotność. Dostęp do pomieszczenia archiwum mają wyłącznie osobowy upoważnione przez ADO,
- po ustaniu okresu archiwizacyjnego dokonuje się zniszczenia dokumentacji, z której sporządza się protokół zniszczenia,
- udostępnieniu dokumentacji, w szczególności dokumentacji zawierającej dane osobowe każdorazowo decyduje ADO.

8.2 . Dokumentacja w formie elektronicznej

- Dostęp do dokumentacji w szczególności danych osobowych mają tylko zalogowani użytkownicy systemu Informatycznego w Urzędzie z odpowiednimi uprawnieniami

i jednocześnie jest możliwość identyfikacji który z użytkowników odpowiada za dane edytowane bądź wprowadzone,

- użytkownicy mają tak dobrane uprawnienia żeby ograniczyć do minimum możliwość wypływu informacji oraz ich przekłamania lub zmiany. Do programu komputerowego wprowadza się dane po ich fizycznej autoryzacji przez osoby uprawnione do tego.

8.3 . Zasady utylizacji sprzętu komputerowego, elementów eksploatacyjnych i nośników danych

- Sprzęt wycofany z eksploatacji, trwale uszkodzony lub wyeksploatowany mogący zawierać dane osobowe zgłasza się niezwłocznie do: ABI, ASI lub bezpośrednio do ADO.
- Kasacje należy poprzedzić zgromadzeniem w jednym miejscu sprzętu do kasacji przez ABI.
- Przed zniszczeniem należy pozbawić sprzęt komputerowy oraz nośniki danych wszystkich informacji możliwych do odczytu.
- W wypadku nośników zewnętrznych nośników danych (dyski zewnętrzne, płyty DVD, CD-R, pendrive, dyskietki) proces kasacji zostaje przeprowadzony przez ABI. Z przeprowadzonej kasacji sporządza się protokół zniszczenia.
- Nośniki danych należy zniszczyć w taki sposób, aby stało się niemożliwe odzyskanie z nich jakichkolwiek danych.
- Sprzęt w wypadku gdy jest wpisany do ewidencji środków trwałych zostaje zdjęty z ewidencji środków trwałych i przekazany firmie zajmującej się utylizacją na podstawie karty przekazania odpadu której 1 egzemplarz trafia do ABI.

8.4 . Zasady nadzoru nad zainstalowanym oprogramowaniem na komputerach w Urzędzie

- Nadzór nad oprogramowaniem zainstalowanym na komputerach będących własnością urzędu pełni ABI za pośrednictwem ASI.
- Użytkownik komputera, który dokonuje odebrania komputera z oprogramowaniem weryfikuje prawdziwość danych zawartych w karcie komputera i potwierdza je własnoręcznym czytelnym podpisem z datą wykonania podpisu.
- ABI oraz ASI dokonują okresowej kontroli danych zawartych w karcie komputera ze stanem faktycznym. Jeżeli w wyniku takiej wyrywkowej kontroli wyjdzie na jaw, że użytkownik dokonał samowolnej instalacji jakiegokolwiek oprogramowania, na które urząd nie posiada licencji, bądź nie spełnia wymogów licencyjnych, odpowiada za to bezpośrednio użytkownik komputera.
- To użytkownik czuwa nad tym, żeby zgodnie z procedurami wew. określonymi w dokumencie „Polityka bezpieczeństwa przetwarzania danych osobowych" zostawiać komputera zalogowanego i to on odpowiada za wszystkie zmiany w oprogramowaniu i sprzęcie niezgodne z zapisami w karcie komputera.
- Taka sama forma odpowiedzialności obowiązuje w wypadku kontroli przez organy upoważnione do kontroli legalności oprogramowania. Za oprogramowanie zewidencjonowane w kartach komputerów i za wszystkie licencje będące własnością urzędu odpowiada SDO, a ABI w Urzędzie nadzoruje jego zgodność z wymogami licencyjnymi oprogramowania.

9. SPOSÓB POSTĘPOWANIA W SYTUACJACH KRYTYCZNYCH

W sytuacjach krytycznych:

- pożar, powódź – należy powiadomić straż pożarną (numer telefonu alarmowy 112) i jeśli nie jest zagrożone własne lub czyjeś zdrowie lub życie przystąpić do ratowania dokumentacji urzędu (jak też innego mienia zakładowego),
- kradzież – należy bezzwłocznie powiadomić organy ścigania (numer telefonu alarmowy 112) i udzielić im wszelkiej pomocy w ujęciu sprawcy,
- klęska żywiołowa – współdziałać ze służbami ratowniczymi i początkowymi przy ratowaniu dokumentacji (również innego mienia zakładowego).

Zabronione jest:

- przechowywanie danych osobowych w szafach na korytarzach,
- pozostawienie niezabezpieczonych pomieszczeń, w których przetwarzane są dane osobowe pod nieobecność osób upoważnionych do przetwarzania danych osobowych,
- pozostawienie dokumentów z danymi osobowymi na biurku po zakończeniu pracy na stanowisku,
- przechowywanie dokumentów z danymi osobowymi w niezamykanych szafach, na parapetach, podłodze.

10. OCHRONA BUDYNKÓW, OBIEKTÓW ORAZ POMIESZCZEŃ URZĘDU ORAZ SYSTEM ALARMOWY

- Przedmiotem ochrony jest ochrona mienia znajdującego się w budynkach, pomieszczeniach Urzędu Miejskiego w Lubieniu Kujawskim, łącznie z mieniem znajdującym się w granicach geodezyjnych budynków. W razie zagrożenia pracownicy Urzędu zobowiązani są podjąć czynności zmierzające do zapobieżenia wystąpienia szkody, a w razie jej zaistnienia do zapobieżenia zwiększeniu jej rozmiarów i natychmiastowego powiadomienie osoby wskazanej oraz właściwych służb publicznych.
- System alarmowy jest utrzymany w stałej sprawności eksploatacyjnej, a także okresowo sprawdzany pod kątem działania czujników ruchu i sterownika systemu.

11. ZADANIA ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI W URZĘDZIE MIEJSKIM W LUBIENIU KUJAWSKIM

Do najważniejszych obowiązków Administratora Bezpieczeństwa Informacji należy:

1. organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych,
2. zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki,
3. wydawanie i anulowanie upoważnień do przetwarzania danych osobowych,
4. prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych (wg. ***załącznika nr 6*** do niniejszego dokumentu),
5. prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych, prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
6. nadzór nad bezpieczeństwem danych osobowych,
7. kontrola działań komórek organizacyjnych w Urzędzie pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
8. inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych.

Administrator Bezpieczeństwa Informacji ma prawo:

1. wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych w Urzędzie Miejskim w Lubieniu Kujawskim;
2. wstępu do pomieszczeń, w których zlokalizowane są zbiory danych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą;
3. żądania złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego;
4. żądania okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli;
5. żądania udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych.

12. ZADANIA ADMINISTRATORA SYSTEMÓW INFORMATYCZNYCH W URZĘDZIE

Administrator Systemu Informatycznego odpowiedzialny jest za:

1. Bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych.
2. Optymalizację wydajności systemu informatycznego, baz danych, instalacje i konfiguracje sprzętu sieciowego i serwerowego.
3. Instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego.
4. Konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem.
5. Nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych.
6. Współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych.
7. Zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego.
8. Zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie.
9. Przeciwdziałanie próbom naruszenia bezpieczeństwa informacji.
10. Zarządzanie licencjami, procedurami ich dotyczącymi.
11. Prowadzenie profilaktyki antywirusowej.

Praca Administratora Systemu Informatycznego jest nadzorowana pod względem przestrzegania Ustawy o Ochronie Danych Osobowych, 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 oraz Polityki Bezpieczeństwa przez ADO.

13. OBOWIĄZKI OSÓB PRZETWARZAJĄCYCH DANE OSOBOWE

Do obowiązków użytkowników systemu informatycznego w Urzędzie Miejskim w Lubieniu Kujawskim zakresie ochrony danych osobowych należy w szczególności:

1. Przestrzeganie procedur wewnętrznych zawartych w Polityce Bezpieczeństwa ochrony danych osobowych oraz w Instrukcji Zarządzania Systemem Informatycznym w Urzędzie,
2. Uniemożliwienie dostępu lub podglądu danych osobowych w systemie dla osób nieupoważnionych,
3. Informowanie ABI oraz ASI o wszelkich naruszeniach obowiązujących w Urzędzie procedur wew. w zakresie przetwarzania danych osobowych,
4. Wykonywania bez zbędnej zwłoki poleceń ABI oraz poleceń ASI w zakresie ochrony danych osobowych jeśli są one zgodne z przepisami prawa powszechnie obowiązującego.

14.OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

Podział zagrożeń:

1. Zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
2. Zagrożenia losowe wewnętrzne – (np. niezamierzone pomyłki administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.
3. Zagrożenia zamierzone, świadome i celowe – najpoważniejsze zagrożenia, naruszenia poufności danych (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenia ciągłości pracy), zagrożenia te możemy podzielić na:
    1) nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
    2) nieuprawniony dostęp do systemu z jego wnętrza,
    3) nieuprawniony przekaz danych,
    4) pogorszenie jakości sprzętu i oprogramowania,
    5) bezpośrednie zagrożenie materialnych składników systemu.

15. PROCEDURY POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH W URZĘDZIE

Niniejsze procedury wewnętrzne określają tryb postępowania w sytuacji naruszenia ochrony danych osobowych gromadzonych i przetwarzanych zarówno w zbiorach tradycyjnych jak i informatycznych.

Niniejszą procedury wewnętrzną stosuje się w przypadku, gdy stwierdzono naruszenie zabezpieczeń sprzętu informatycznego, sieci komputerowej, systemu alarmowego i zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe.

Przez naruszenie ochrony danych osobowych rozumie się niezgodne z przepisami ustawy o ochronie danych i rozporządzeń wykonawczych przetwarzanie danych oraz usuwanie danych osobowych.

Osobami bezpośrednio odpowiedzialnymi za zgodną z prawem ochronę danych osobowych w Urzędzie Miejskim w Lubieniu Kujawskim ich zabezpieczeń są:

a) Administrator Danych Osobowych,
b) Administrator Bezpieczeństwa Informacji,
c) Administrator Systemów Informatycznych,
d) Pracownicy upoważnieni do przetwarzania danych osobowych.

Każdy pracownik biorący udział w przetwarzaniu danych osobowych w systemie informatycznym jest odpowiedzialny za bezpieczeństwo tych danych. W szczególności osoba, która zauważyła zdarzenie mogące być przyczyną naruszenia ochrony danych osobowych lub mogących spowodować naruszenie bezpieczeństwa danych, zobowiązana jest do natychmiastowego poinformowania ABI lub innej osoby wskazanej przez niego.

Każda osoba zatrudniona w Urzędzie, która stwierdzi lub podejrzewa naruszenie zabezpieczenie ochrony danych osobowych w systemie informatycznym (lub przetwarzanych w inny sposób) powinna niezwłocznie poinformować o tym fakcie ABI. W przypadku braku możliwości zawiadomienia ABI lub ASI niezwłocznie należy powiadomić bezpośredniego przełożonego.

Do czasu przybycia ABI należy:

a) niezwłocznie podjąć czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
b) zabezpieczyć dostęp do miejsca lub urządzenia przez osoby trzecie,
c) wstrzymać pracę na komputerze, na którym zaistniało naruszenie ochrony oraz nie uruchamiać bez koniecznej potrzeby komputerów i innych urządzeń, których funkcjonowanie w związku naruszeniem ochrony zostało wstrzymane,
d) zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę zdarzenia,
e) nie zmieniać położenia przedmiotów, które pozwalają stwierdzić naruszenie ochrony lub odtworzyć jej okoliczności,
f) podjąć stosowne do zaistniałej sytuacji, inne niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych,
g) podjąć inne działania przewidziane w instrukcjach technicznych i technologicznych

stosowanie do objawów i komunikatów towarzyszących naruszeniu,

h) wstępnie udokumentować zaistniałe naruszenie,
i) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ABI lub osoby upoważnionej.

Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych ABI lub osoba go zastępująca powinna:

a) zapoznać się z zaistniałą sytuacją i dokonać wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy,
b) zaprotokołować wszelkie informacje związane ze zdarzeniem,
c) wygenerować i wydrukować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia,
d) przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych niepowołanych,
e) dokonać fizycznego odłączenia urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nie uprawnionej,
f) wylogować użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych,
g) dokonać zmiany hasła na konto ABI i użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania,
h) zażądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem.

Administrator Bezpieczeństwa Informacji (ABI) dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, który powinien zawierać w szczególności:

- wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych w zdarzeniu,
- określeniu czasu, miejsca naruszenia i powiadomienia,
- określeniu okoliczności towarzyszących i rodzaju naruszenia,
- wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
- wstępną ocenę przyczyn wystąpienia naruszenia,
- ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

Sporządzony raport ABI przekazuję niezwłocznie ADO. ABI przystępuje do usuwania skutków incydentu i przywrócenia prawidłowego przebiegu procesu przetwarzania danych osobowych. W szczególności działania związane z usuwaniem skutków incydentu mogą obejmować:

- przeprowadzenie naprawy sprzętu informatycznego;
- rekonfigurację sprzętu informatycznego;
- wprowadzenie poprawek do oprogramowania;
- rekonfiguracje oprogramowania;
- odtworzenie danych z kopii awaryjnych;
- modyfikacje danych w celu odtworzenia ich integralności;
- wycofanie z użycia materiału kryptograficznego;
- inne naprawy urządzeń wchodzących w skład infrastruktury informatycznej wspomagającej lub zabezpieczających działanie systemu informatycznej.

16. POSTANOWIENIA KOŃCOWE

1. Wobec osoby, która w przypadku naruszenia ochrony danych osobowych lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zadaniami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie interdyscyplinarne.
2. ABI zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych.
3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być traktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia ochrony danych osobowych lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym ABI.
4. Orzeczona kara dyscyplinarna wobec osoby uchylającej się od powiadomienia ABI nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997r. o ochronie danych (Dz. U. z 2014r. poz. 1182 ze zm.) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
5. W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2014r., poz. 1182 ze zm), 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.2004 Nr 100, poz. 1024).

BURMISTRZ
Marek Wiliński

17. ZAŁĄCZNIKI DO POLITYKI BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

1) ***Załącznik nr 1*** - Oświadczenie o zachowaniu poufności i zapoznaniu się z przepisami,
2) ***Załącznik nr 2*** - Wniosek o wydanie/cofnięcie upoważnienia do przetwarzania danych osobowych,
3) ***Załącznik nr 3*** - Upoważnienie do przetwarzania danych osobowych,
4) ***Załącznik nr 4*** – Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe,
5) ***Załącznik nr 5*** - Wykaz zbiorów danych osobowych przetwarzanych tradycyjnie i w systemie informatycznym ze wskazaniem programów zastosowanych do przetwarzania tych danych i miejscem przetwarzania,
6) ***Załącznik nr 6*** – Ewidencja osób upoważnionych do przetwarzania danych osobowych.

BURMISTRZ
Marek Wiliński

Załącznik Nr 1
do Polityki Bezpieczeństwa Przetwarzania
Danych Osobowych w Urzędzie Miejskim
w Lubieniu Kujawskim

OŚWIADCZENIE
o zachowaniu poufności i zapoznaniu się z przepisami

Ja niżej podpisany(a) ..... oświadczam, iż zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miał(a) dostęp w związku z wykonywaniem:

Rodzaj zadań	*)*
zadań i obowiązków służbowych wynikających z umowy o pracę	
zadań wynikających z umowy cywilno-prawnej	
zadań wynikających z umowy w związku z praktyką studencką	
Zadań wynikających z umowy w związku ze stażem	

*) właściwe zaznaczyć X

zarówno **w trakcie wykonywania umowy, jak i po jej ustaniu**.

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

Oświadczam, że zostałem(am) zapoznany(a) z przepisami Ustawy o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.) oraz Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024 ze zm.).

Oświadczam, że zostałem(am) poinformowany o grożącej, stosownie do przepisów rozdziału 8 ustawy o ochronie danych osobowych, odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, że naruszenie zasad ochrony danych osobowych, obowiązujących w Koncernie może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

Lubień Kujawski, dn. .....r.

miejsce i data złożenia oświadczenia

.....
czytelny podpis osoby składającej oświadczenie

BURMISTRZ
Marek Wiliński

Załącznik Nr 2
do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Miejskim w Lubieniu Kujawskim

Lubień Kujawski, ……..……..

WNIOSEK

o wydanie/cofnięcie upoważnienia do przetwarzania danych osobowych

wnioskuję

o wydanie upoważnienia/ cofnięcie upoważnienia z dnia ……..

Pani /Panu* ……

(imię i nazwisko pracownika)

zatrudnionej/emu w ……...

na stanowisku ……

do przetwarzania danych osobowych wynikających z zakresu obowiązków pracowniczych z powodu:

a) podjęcia pracy na stanowisku

……..

b) zmiany stanowiska

……..

c) zmiany zakresu obowiązków pracowniczych

……..

d) utworzenia nowego zbioru danych osobowych

……..

e) naruszenia zasad i sposobu przetwarzania danych osobowych

……..

1. Nazwa zbioru danych osobowych:

……..

2. Rodzaj uprawnień: Z - pełne prawa do zarządzania bazą danych, P- prawo do przeglądania,

……..

3. Sposób i miejsce przetwarzania danych osobowych

……..

……..
Data i podpis Kierownika referatu

* niepotrzebne skreślić

BURMISTRZ
Marek Wiliński

Załącznik Nr 3
do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Miejskim w Lubieniu Kujawskim

Lubień Kujawski, dnia .....
(miejscowość, data)

.....
(pieczęć jednostki organizacyjnej)

Upoważnienie do przetwarzania danych osobowych

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2014 r. poz. 1182 ze zm.) upoważniam:

Pana/ią .....
(imię i nazwisko)

.....
(komórka organizacyjna)

- do przetwarzania danych osobowych w systemie informatycznym* / wersji papierowej* w celach związanych z wykonywaniem obowiązków, zadań, poleceń służbowych,
- obsługi urządzeń wchodzących w skład systemu, służących do przetwarzania danych osobowych.

Upoważnienie obejmuje przetwarzanie danych osobowych zawartych w zbiorach:

.....
.....

Zgodnie z art. 39, ust. 2 wyżej wymienionej ustawy jest Pan/i zobowiązany/a do zachowania w tajemnicy (również po ustaniu zatrudnienia) danych osobowych uzyskanych w trakcie dokonywania operacji związanych z ich przetwarzaniem oraz sposobów ich zabezpieczania.

Upoważnienie jest ważne w okresie – zgodnie z umową o pracę.

.....
(podpis upoważnionego)

.....
(podpis Administratora Bezpieczeństwa Informacji)

BURMISTRZ
Marek Wiliński

*- niepotrzebne skreślić

Załącznik Nr 4
do Polityki Bezpieczeństwa Przetwarzania
Danych Osobowych w Urzędzie Miejskim
w Lubieniu Kujawskim

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

Lp.	Pomieszczenia w których przetwarzane są dane osobowe	Komórki organizacyjne przetwarzające zbiór	Nazwa zbioru danych osobowych	Uwagi

BURMISTRZ
Marek Wiliński

Załącznik Nr 5
do Polityki Bezpieczeństwa Przetwarzania
Danych Osobowych w Urzędzie Miejskim
w Lubieniu Kujawskim

Wykaz zbiorów danych osobowych przetwarzanych tradycyjnie i w systemie informatycznym ze wskazaniem programów zastosowanych do przetwarzania tych danych i miejscem przetwarzania

Lp.	Nazwa zbioru danych osobowych	Lokalizacja zbioru danych osobowych (budynek, komórka organizacyjna, nr biura, stanowisko)	Nazwa oraz lokalizacja programu zastosowanego do przetwarzania danych	Autor programu

BURMISTRZ
Marek Wiliński

Załącznik Nr 6
do Polityki Bezpieczeństwa Przetwarzania
Danych Osobowych w Urzędzie Miejskim
w Lubieniu Kujawskim

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Imię i nazwisko	Data nadania uprawnień	Data ustania uprawnień	Identyfikator*

* identyfikator nadaje się wyłącznie pracownikowi przetwarzającemu dane osobowe w systemie informatycznym

BURMISTRZ
Marek Wiliński