Załącznik Nr 2
do Zarządzenia Nr 121/13
Prezydenta Miasta Łomża
z dnia 24 maja 2013r.

Łomża

Urząd Miejski Gminy Miasta Łomża
(zwany dalej Urzędem Miejskim)
Pl. Stary Rynek 14
18 - 400 Łomża

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

Data i miejsce sporządzenia dokumentu:	Łomża, 24 maja 2013 r.
Ilość stron:	22
Organ zatwierdzający:	PREZYDENT MIASTA MIECZYSŁAW LEON CZERNIAWSKI

Parafa:	

SPIS TREŚCI

Parafa:	

Parafa:	

1. WSTĘP

1.1. INFORMACJE OGÓLNE

Niniejszy dokument Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych został opracowany przez Administratora Danych – Gminę Miasta Łomża, w celu zapewnienia zgodności przetwarzania danych osobowych z obowiązującymi przepisami prawa.

Instrukcja Zarządzania Systemem Informatycznym wraz z Polityką Bezpieczeństwa stanowi dokumentację przetwarzania danych osobowych w rozumieniu § 1 pkt 1 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024 z późn. zm.).

Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych obowiązuje od dnia **24 maja 2013 r**.. Wszelkie wątpliwości dotyczące sposobu interpretacji zapisów niniejszego dokumentu Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych, powinny być rozstrzygane na korzyść zapewnienia możliwie najwyższego poziomu ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą.

Każda osoba mającą dostęp do danych osobowych na podstawie upoważnienia Administratora Danych, została zapoznana z Instrukcją Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych i zobowiązana do jej przestrzegania w zakresie wynikającym z przydzielonych zadań. Dotyczy to w szczególności pracowników zatrudnionych przez Administratora Danych (jak również stażystów oraz praktykantów Urzędu Miejskiego, a także osób fizycznych, współpracujących z Urzędem Miejskim i pozostających w jego strukturze organizacyjnej (w szczególności poprzez realizację usług w lokalizacjach Administratora Danych z wykorzystaniem stosowanych urządzeń lub systemów), które uzyskują dostęp do danych osobowych w związku ze świadczeniem na rzecz Urzędu Miejskiego usług na podstawie umów cywilnoprawnych. Wyżej wymienione osoby złożyły na piśmie oświadczenie o zapoznaniu się z treścią Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych oraz zobowiązały się do stosowania zawartych w niej postanowień.

Parafa:	

1.2. CEL PRZYGOTOWANIA INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

Podstawowym celem przygotowania i wdrożenia dokumentu Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych było zapewnienie zgodności działania Urzędu Miejskiego z ustawą o ochronie danych osobowych oraz z jej rozporządzeniami wykonawczymi. Dokument Instrukcji Zarządzania Systemem Informatycznym został opracowany na podstawie następujących aktów prawnych:

1. ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)

2. 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 z późn. zm.),

Należy przez powyższe rozumieć w szczególności realizację w niniejszym dokumencie wymogu opisania sposobu przetwarzania danych osobowych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. Zadaniem Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych jest także określenie podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych oraz wymagań w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych.

Parafa:	

1.3. ZAKRES INFORMACJI OBJĘTYCH INSTRUKCJĄ ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

Dokument Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych opisuje zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem. Obejmuje on ogólne informacje o systemie informatycznym i zbiorach danych osobowych, które są przy ich użyciu przetwarzane, o zastosowanych rozwiązaniach technicznych, jak również o procedurach eksploatacji i zasady użytkowania, jakie zastosowano w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych. Na Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych składają się w szczególności następujące informacje:

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 programowych służących do ich przetwarzania;
5) sposób, miejsce oraz okres przechowywania:
    a) elektronicznych nośników informacji zawierających dane osobowe,
    b) kopii zapasowych, o których mowa w pkt 4,
6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia;
7) sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia;
8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych;
9) Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych stosuje się do wszelkich czynności, stanowiących w myśl ustawy o ochronie danych osobowych przetwarzanie danych osobowych. Bez względu na źródło pochodzenia danych osobowych, ich zakres, cel zebrania, sposób przetwarzania lub czas przetwarzania, stosuje się zasady przetwarzania danych osobowych ujęte w niniejszym dokumencie Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych. Rygorowi Instrukcji Zarządzania Systemem Informatycznym podlegają także dane powierzone Urząd Miejski do przetwarzania na podstawie pisemnej umowy o powierzeniu przetwarzania danych osobowych oraz dane osobowe, których Urząd Miejski jest odbiorcą w rozumieniu ustawy o ochronie danych osobowych.

Parafa:	

1.4. WYJAŚNIENIE TERMINÓW UŻYWANYCH W DOKUMENCIE INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

1. **administrator danych** – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3 ustawy o ochronie danych osobowych, decydujące o celach i środkach przetwarzania danych osobowych, w niniejszej Instrukcji zwany także Gminą Miasta Łomża oraz Urzędem Miejskim,
2. **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
3. **hasło** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
4. **identyfikator użytkownika** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
5. **Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych** – dokument instrukcji zarządzania systemem informatycznym w rozumieniu § 1 pkt 1 rozporządzenia, zwaną dalej „Instrukcją”,
6. **integralność danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
7. **odbiorca danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
   7.1. osoby, której dane dotyczą,
   7.2. osoby upoważnionej do przetwarzania danych,
   7.3. przedstawiciela, o którym mowa w art. 31a ustawy o ochronie danych osobowych,
   7.4. podmiotu, o którym mowa w art. 31 ustawy o ochronie danych osobowych,
   7.5. organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,
8. **państwo trzecie** – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego,
9. **Polityka Bezpieczeństwa** – dokument polityki bezpieczeństwa w rozumieniu § 1 pkt 1 rozporządzenia, zwaną dalej „Polityką”,
10. **poufność danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,
11. **przetwarzanie danych** – rozumie się przez to jakiekolwiek operacje wykonywane na danych

Parafa:	

osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,

12. **raport** – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych,
13. **rozliczalność** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
14. **rozporządzenie** – rozumie się przez to 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 z późn. zm.), zwane dalej „rozporządzeniem",
15. **sieć publiczna** - rozumie się przez to publiczną sieć telekomunikacyjną w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2004 r. Nr 171, poz.1800 ze zm.),
16. **sieć telekomunikacyjna** - rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2004 r. Nr 171, poz.1800 ze zm.),
17. **system informatyczny** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
18. **teletransmisja** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,
19. **ustawa** – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), zwaną dalej „Ustawą",
20. **usuwanie danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
21. **uwierzytelnianie** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,
22. **zabezpieczenie danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
23. **zbiór danych** – 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,
24. **zgoda osoby, której 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 lub dorozumiana z oświadczenia woli o innej treści;

Parafa:	

2. PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMACH INFORMATYCZNYCH ORAZ WSKAZANIA OSOBY ODPOWIEDZIALNEJ ZA TE CZYNNOŚCI

2.1. PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMACH INFORMATYCZNYCH

1. Uprawnienia do przetwarzania danych osobowych w systemach informatycznych nadaje każdorazowo Administrator Systemów Informatycznych.
2. W celu nadania uprawnienia o którym mowa w pkt 1 lub zmiany jego zakresu właściwy Zarządzający Zbiorem Danych Osobowych w określonej jednostce organizacyjnej Urzędu Miejskiego występuje z umotywowanym wnioskiem do Administratora Systemów Informatycznych.
3. Uprawnienie do przetwarzania danych osobowych w systemach informatycznych może zostać nadane wyłącznie osobom, które uzyskały upoważnienie do przetwarzania danych osobowych nadane w trybie określonym w Rozdziale 3 Polityki.

   3.1. Administrator Systemów Informatycznych każdorazowo decyduje czy istnieje konieczność (w celu wykonywania obowiązków zawodowych) nadania uprawnienia do przetwarzania danych osobowych w systemach informatycznych.

   3.2. Zakres uprawnienia (zakres dostępu do danych osobowych przetwarzanych w systemach informatycznych) nie może być szerszy niż w wydanym wcześniej upoważnieniu do przetwarzania danych osobowych.
4. Przydzielanie poszczególnym pracownikom Urzędu Miejskiego uprawnień do przetwarzania danych osobowych w systemach informatycznych następuje poprzez nadanie im loginu oraz hasła tymczasowego pozwalającego na dostęp do danego systemu informatycznego (zgodnie z trybem określonym w Rozdziale 3 pkt. 1-7 niniejszej Instrukcji).
5. Administrator Systemów Informatycznych prowadzi rejestr nadanych uprawnień do przetwarzania danych w systemach informatycznych według wzoru stanowiącego Załącznik nr 2 do Polityki.
6. Jeśli Administrator Systemów Informatycznych uzna to za stosowne, uprawnienie do przetwarzania danych osobowych w systemach informatycznych może zostać w każdej chwili cofnięte poprzez ograniczenie/uniemożliwienie dostępu do przetwarzania danych w systemach informatycznych.

Parafa:	

7. Cofnięcie uprawnienia dostępu do danego systemu informatycznego Administrator Systemów Informatycznych odnotowuje w prowadzonym przez siebie w rejestrze nadanych uprawnień.

8. Zarządzający Zbiorem Danych oraz Administrator Systemów Informatycznych ponoszą odpowiedzialność służbową za przyznanie użytkownikowi zbyt szerokich uprawnień lub przywilejów w procesie, o którym mowa w niniejszym Rozdziale, w stosunku do zadań realizowanych przez użytkownika na jego stanowisku pracy.

2.2. OSOBY ODPOWIEDZIALNE ZA NADAWANIE UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMACH INFORMATYCZNYCH

Zakres odpowiedzialności	Imię i nazwisko osoby odpowiedzialnej	Pełniona funkcja / uwagi
Przegląd przestrzegania Instrukcji	Andrzej Kondraciuk	Administrator Bezpieczeństwa Informacji oraz Administrator Systemów Informatycznych
Przegląd aktualności Instrukcji	Andrzej Kondraciuk	Administrator Bezpieczeństwa Informacji oraz Administrator Systemów Informatycznych
Nadawanie uprawnień do przetwarzania danych w systemach informatycznych	Andrzej Kondraciuk	Administrator Systemów Informatycznych
Rejestrowanie uprawnień do przetwarzania danych w systemach informatycznych	Andrzej Kondraciuk	Administrator Systemów Informatycznych
Wyrejestrowanie uprawnień do przetwarzania danych w systemach informatycznych	Andrzej Kondraciuk	Administrator Systemów Informatycznych

Parafa:	

3. OPIS STOSOWANYCH METOD I ŚRODKÓW UWIERZYTELNIENIA ORAZ PROCEDUR ZWIĄZANYCH Z ZARZĄDZANIEM I UŻYTKOWANIEM STOSOWANYCH METOD I ŚRODKÓW UWIERZYTELNIENIA

1. Dla każdego użytkownika systemu informatycznego ustala się odrębne konto zawierające w szczególności: identyfikator, hasło pierwszego logowania, dane o uprawnieniach użytkownika, profil.
2. Hasła tymczasowe do konta użytkownika (w przypadku utworzenia nowego konta, a także w sytuacjach awaryjnych związanych np.: z zagubieniem, utratą lub zapomnieniem hasła osobistego przez użytkownika konta) tworzone są przez Administratora Systemów Informatycznych.
3. Tryb przekazywania ww. hasła tymczasowego odbywa się za pośrednictwem poczty elektronicznej, w sposób zapewniający bezpieczeństwo i poufność przekazywanych informacji, w szczególności: w sposób uniemożliwiający innej osobie ich podsłuchanie lub nieuprawnione wykorzystanie.
4. Zezwala się na wykorzystanie innych, niewymienionych w Rozdziale 3 pkt. 3 niniejszej Instrukcji, bezpiecznych metod i środków technicznych, w celu przekazania hasła tymczasowego, za pisemną zgodą Administratora Systemów Informatycznych.
5. Zakazuje się przekazywania haseł tymczasowych poprzez osoby trzecie lub przy użyciu metod, które nie gwarantują zachowania jego poufności oraz niezaprzeczalnego ustalenia nadawcy i odbiorcy hasła, np.: przez niechronione wiadomości przekazywane elektronicznie.
6. Po otrzymaniu hasła tymczasowego użytkownik ma obowiązek niezwłocznego zalogowania się do systemu informatycznego przy użyciu tego hasła oraz jego zmiany na hasło osobiste.
7. Ujawnianie przez użytkownika komukolwiek, jakichkolwiek aktualnych lub poprzednich haseł tymczasowych, haseł osobistych lub innych haseł mu powierzonych, jest zabronione.
8. Autoryzacja dostępu do wszystkich systemów przetwarzających dane osobowe, opisanych w niniejszej Instrukcji możliwa jest wyłącznie za pomocą loginu i hasła.
9. Jeżeli do uwierzytelniania użytkowników używa się hasła, jego zmiana musi następować nie rzadziej niż co 30 dni, hasło musi się składać z co najmniej 8 znaków długości oraz jednocześnie zawierać małe i wielkie litery, cyfry lub znaki specjalne.
10. W celu zapewnienia odpowiedniego poziomu bezpieczeństwa haseł i innych identyfikatorów pozwalających na autoryzację w programach przetwarzających dane osobowe, nie zaleca się stosowania jakichkolwiek programów i systemów umożliwiających zapamiętywanie identyfikatorów i haseł. Nie ma możliwości zapamiętania hasła użytkownika do systemu operacyjnego.
11. Dostęp do każdego z profilów użytkowników ograniczony jest wyłącznie do jednego pracownika.

Parafa:	

4. PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONE DLA UŻYTKOWNIKÓW SYSTEMU

3.1. PROCEDURA ROZPOCZĘCIA PRACY PRZEZNACZONA DLA UŻYTKOWNIKA SYSTEMU

1. Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym oraz w trakcie pracy, każdy pracownik jest obowiązany do zwrócenia bacznej uwagi, czy nie wystąpiły objawy, mogące świadczyć o naruszeniu zasad ochrony danych osobowych.

2.1. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje uruchomienie komputera, wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.

2.2. Użytkownik zobowiązany jest do:

2.2.1. zwrócenia uwagi czy w oknie logowania do systemu, w polu odpowiadającym identyfikatorowi użytkownika nie pojawił się identyfikator innej osoby nieuprawnionej do przetwarzania informacji na danym komputerze, a w przypadku stwierdzenia takiego faktu do niezwłocznego zgłoszenia podejrzenia zaistnienia incydentu naruszenia ochrony danych osobowych lub naruszenia bezpieczeństwa systemu na zasadach określonych w Rozdziale 9 niniejszej Instrukcji,

2.2.2. uważnego wprowadzania osobistych danych uwierzytelniających (identyfikatora i hasła osobistego) do odpowiednich pól wyświetlonego formularza,

2.2.3. uważnego czytania, a jeśli to konieczne zanotowania ewentualnych komunikatów pojawiających się na ekranie lub wyświetlaczu komputera oraz dalszego postępowania zgodnie z przyjętymi w Urzędzie Miejskim zasadami lub wskazówkami Administratora Systemów Informatycznych,

2.2.4. niedopuszczania w trakcie prowadzenia czynności uwierzytelniania w systemie informatycznym do ujawnienia danych uwierzytelniających użytkownika (hasła osobistego) poprzez uniemożliwienie podejrzenia lub zarejestrowania w inny sposób wprowadzanego z klawiatury hasła przez osobę trzecią. W przypadku, gdy poufne wprowadzenie hasła nie jest możliwe z przyczyn wynikających ze strony osoby trzeciej, użytkownik ma obowiązek zaprzestania dalszych działań lub nie rozpoczynania tej operacji oraz powiadamia o tym bezpośredniego przełożonego.

3. Użytkownikowi nie wolno w czasie uruchamiania systemu operacyjnego odchodzić od stanowiska. Jest to dozwolone tylko i wyłącznie zgodnie z procedurą opisującą tryb zawieszenia pracy systemu, w którym

Parafa:	

przetwarzane są dane osobowe.

4. Użytkownik informuje Administratora Systemów Informatycznych lub osobę przez niego upoważnioną do opieki nad sprzętem komputerowym o wszelkich nieprawidłowościach w dostępie do systemu informatycznego.

3.2. PROCEDURA ZAWIESZENIA PRACY PRZEZNACZONA DLA UŻYTKOWNIKA SYSTEMU

1. W przypadku konieczności zawieszenia pracy w systemie informatycznym z powodu tymczasowego opuszczenia stanowiska pracy, użytkownik zobowiązany jest, w zależności od przewidywanego okresu swojej nieobecności, do aktywowania wygaszacza ekranu, zabezpieczonego hasłem lub do zablokowania dostępu do użytkowanego systemu komputerowego, np. poprzez jednoczesne naciśnięcie klawiszy {Ctrl + Alt + Delete} i potwierdzenia klawiszem Enter podświetlonej opcji „Zablokuj komputer".

2. Jeżeli system informatyczny służący do przetwarzania danych osobowych nie pozwala na wykonanie czynności określonych powyżej w pkt 1, Użytkownik zobowiązany jest do poprawnego wyrejestrowania się (wyjścia) z tego systemu informatycznego zgodnie ze zdefiniowaną dla niego procedurą.

3. Krótkotrwałe przerwy w pracy bez opuszczania stanowiska pracy nie wymagają zamykania aplikacji i wylogowania się z systemu.

4. W przypadku stwierdzenia problemów z funkcjonowaniem systemu oraz niemożliwością wykonania żadnego z działań określonych w pkt 1 oraz pkt 2, użytkownik zobowiązany niezwłocznie wezwać Administratora Systemów Informatycznych oraz pozostać przy stanowisku pracy do czasu jego przybycia lub do przybycia wyznaczonej przez niego osoby.

3.3. PROCEDURA ZAKOŃCZENIA PRACY PRZEZNACZONA DLA UŻYTKOWNIKA SYSTEMU

1. W przypadku zakończenia przez Użytkownika pracy z systemem informatycznym służącym do przetwarzania danych osobowych, a zawsze przed zakończeniem pracy w systemie komputerowym użytkowanym przez niego na stanowisku pracy, użytkownik zobowiązany jest do poprawnego wyrejestrowania się (wyjścia) z systemu informatycznego, w szczególności poprzez:
   1.1. zapisanie wszystkich otwartych plików,
   1.2. zamknięcie wszystkich otwartych programów,
   1.3. wyrejestrowanie (wylogowanie) użytkownika z obsługiwanych przez niego systemów

Parafa:	

informatycznych służących do przetwarzania danych osobowych,

1.4. wybranie odpowiedniego polecenia systemowego umożliwiającego jego zamknięcie i zakończenie pracy,

1.5. użytkownik zobowiązany jest pozostać przy stanowisku komputerowym do chwili jego wyłączenia.

2. W przypadku stwierdzenia problemów z funkcjonowaniem systemu oraz niemożliwością wykonania żadnego z działań określonych w pkt 1 użytkownik zobowiązany niezwłocznie wezwać Administratora Systemów Informatycznych oraz pozostać przy stanowisku pracy do czasu jego przybycia lub do przybycia wyznaczonej przez niego osoby.

4. PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA ORAZ OPIS SPOSOBU, MIEJSCA I OKRESU PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE ORAZ WSKAZANYCH KOPII ZAPASOWYCH

1. Szczegółową procedurę tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania jak również opis sposobu, miejsca i okresu ich przechowywania oraz przechowywania elektronicznych nośników informacji zawierających dane osobowe zawiera Załącznik nr 1 do niniejszej Instrukcji.

5. OPIS SPOSOBU ZABEZPIECZENIA SYSTEMÓW INFORMATYCZNYCH PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, O KTÓRYM MOWA W PKT III PPKT 1 ZAŁĄCZNIKA DO ROZPORZĄDZENIA

1. Z uwagi na fakt, iż komputery przetwarzające dane osobowe posiadają dostęp do sieci publicznej, Administrator Danych wdrożył procedury oraz oprogramowanie, które chroni dane osobowe przed nieuprawnionym dostępem, zmianami, usunięciem lub uszkodzeniem. Zagrożenia te to programy zawierające złośliwy kod (wirusy), tzw. konie trojańskie oraz ataki hakerów.

2. Aby zmniejszyć to zagrożenie, zabronione jest pobieranie oraz instalowanie na komputerach, bez nadzoru Administratora Systemów Informatycznych, jakichkolwiek programów służących do przetwarzania danych

Parafa:	

osobowych.

3. Zabronione jest również używanie nośników informacji niepochodzących z zasobów Administratora Danych. Każda osoba przetwarzająca dane osobowe przy użyciu komputera została pouczona, aby w wypadku jakichkolwiek podejrzeń dotyczących obniżenia bezpieczeństwa danych osobowych, poinformowała o tym fakcie osobę upoważnioną przez Administratora Danych lub Administratora Systemów Informatycznych.

4. Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej oraz środki ochrony w ramach narzędzi programowych i baz danych jak również środki ochrony fizycznej danych przetwarzanych w systemach informatycznych służących do przetwarzania danych osobowych zawiera tabela stanowiąca Załącznik nr 2 do niniejszej Instrukcji.

6. OPIS SPOSOBU REALIZACJI WYMOGÓW STAWIANYCH SYSTEMOM INFORMATYCZNYM PRZEZ ROZPORZĄDZENIE WYKONAWCZE DO USTAWY O OCHRONIE DANYCH OSOBOWYCH

1. Opis sposobu realizacji wymogów stawianych systemom informatycznym na mocy § 7 ust. 1 pkt 4 Rozporządzenia zawiera Załącznik nr 3 do niniejszej Instrukcji.

7. PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH

1. O przeprowadzanych przeglądach i konserwacjach systemu informatycznego informowany jest Administrator Bezpieczeństwa Informacji, który może uczestniczyć w dokonywanych czynnościach.

2. Przeglądy i konserwacje systemów oraz nośników informacji służących do przetwarzania danych a także wstępne czynności serwisowe dokonywane są w siedzibie Administratora Danych przez Administratora Systemów Informatycznych.

3. W wypadku wystąpienia takiej potrzeby przegląd i konserwacja mogą być zlecone pracownikowi lub podmiotowi zewnętrznemu specjalizującemu się w tego typu działaniach, Administrator Systemów Informatycznych informuje podmiot, który na podstawie umowy zawartej z Administratorem Danych, dokonuje przeglądu i konserwacji systemów oraz nośników informacji służących do przetwarzania

Parafa:	

danych osobowych, o konieczności podjęcia stosownych czynności

4. W wypadku przekazania sprzętu lub nośników informacji służących do przetwarzania danych osobowych podmiotowi trzeciemu, pozbawia się je zapisanych danych osobowych w sposób, który uniemożliwi ich odtworzenie. W obydwu przypadkach, zostaną zachowane szczególne warunki ostrożności, w celu zabezpieczenia danych osobowych przed dostępem osób nieuprawnionych.

5. Jeśli Administrator Systemów Informatycznych nie dokonuje naprawy osobiście, podmiot dokonujący wyeliminowania opisanych nieprawidłowości, zawiadamia o podjętych czynnościach Administratora Systemów Informatycznych.

6. Wykryte podczas przeglądu i konserwacji nieprawidłowości w działaniu sprzętu lub programów służących do przetwarzania danych osobowych, usuwa się niezwłocznie.

7. Administrator Systemów Informatycznych dokonuje kwartalnej oceny stanu bezpieczeństwa danych osobowych, przetwarzanych w systemach informatycznych, niezależnie od kontroli okresowej, kontrola może być dokonywana przez Administratora Systemów Informatycznych na wniosek Administratora Danych. Ponadto każdorazowo Administrator Systemów Informatycznych dokonuje kontroli po uzyskaniu informacji o próbie nieautoryzowanego dostępu, wystąpieniu zagrożenia wirusem komputerowym lub innym złośliwym programem.

8. Za prawidłowość przeprowadzenia przeglądów i konserwacji systemu informatycznego odpowiada Administrator Systemów Informatycznych.

Parafa:	

8. POZIOM BEZPIECZEŃSTWA

Administrator Danych zastosował środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczył dane osobowe przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

8.1. OKREŚLENIE STOSOWANEGO POZIOMU BEZPIECZEŃSTWA

1. Ze względu na kategorie przetwarzanych danych osobowych oraz występujące wobec nich zagrożenia, wprowadza się trzy poziomy bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym:
   1.1 podstawowy,
   1.2 podwyższony,
   1.3 wysoki,

określające minimalne wykazy wymagań bezpieczeństwa koniecznych do spełnienia na każdym z poziomów.

2. Właściwy dla danego systemu informatycznego służącego do przetwarzania danych osobowych poziom bezpieczeństwa przetwarzania danych osobowych w wyodrębnionych w Urzędzie Miejskim systemach informatycznym określony został w tabeli stanowiącej Załącznik nr 2 do niniejszej Instrukcji.

8.1.1. PODSTAWOWY POZIOM BEZPIECZEŃSTWA

1. Podstawowy poziom bezpieczeństwa przetwarzania danych osobowych należy stosować, gdy w systemie informatycznym nie są przetwarzane dane sensytywne oraz żadne z urządzeń systemu informatycznego służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną.
2. Na środki podstawowego poziomu bezpieczeństwa w systemie informatycznym służącym do przetwarzania danych osobowych składają się w szczególności następujące elementy:
   2.1 obszar, w którym przetwarzane są dane należy zabezpieczyć przed fizycznym dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych,
   2.2 przebywanie osób nieuprawnionych w obszarze przetwarzania jest dopuszczalne jedynie za zgodą Zarządzającego Zbiorem Danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych. W przypadku pomieszczeń technicznych wchodzących w skład obszaru przetwarzania, w

Parafa:	

których rozlokowane są istotne elementy systemu informatycznego, przebywanie osób możliwe jest wyłącznie w obecności Administratora Systemu Informatycznego,

2.3 w systemie informatycznym stosuje się mechanizmy kontroli dostępu do danych osobowych w nim przetwarzanych,

2.4 jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator, a dostęp do danych był możliwy wyłącznie po wprowadzeniu tego identyfikatora i dokonaniu uwierzytelnienia,

2.5 system informatyczny musi posiadać zabezpieczenia przed działaniem oprogramowania, którego celem jest uzyskanie do niego nieuprawnionego dostępu, a także zabezpieczenia przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej,

2.6 system informatyczny służący do przetwarzania danych osobowych należy chronić przed zagrożeniami pochodzącymi z wewnętrznej sieci teleinformatycznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń monitorujących tę sieć lub system informatyczny, oraz chroniących przetwarzane w nim dane osobowe przed nieuprawnionym dostępem,

2.7 identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie,

2.8 w przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana musi następować nie rzadziej niż co 30 dni, hasło musi składać się: z co najmniej 6 znaków,

2.9 dane osobowe oraz programy służące do ich przetwarzania muszą być zabezpieczone poprzez wykonywanie ich kopii zapasowych, które należy przechowywać w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem oraz usuwać niezwłocznie po ustaniu ich użyteczności,

2.10 osoba użytkująca komputer przenośny lub elektroniczny nośnik informacji stanowiący własność Administratora Danych i zawierający dane osobowe musi zachować szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych, w tym musi stosować się do obowiązujących w Urzędzie Miejskim zasad bezpieczeństwa fizycznego w związku z użytkowaniem komputerów przenośnych. Ponadto osoba ta musi stosować na użytkowanym komputerze przenośnym lub elektronicznym nośniku informacji obowiązujące i dopuszczone w Urzędzie Miejskim środki ochrony kryptograficznej wobec przetwarzanych danych osobowych polegające na szyfrowaniu całego dysku lub elektronicznego nośnika informacji (w tym także wymiennego) zawierającego te dane, albo też szyfrowaniu samego zbioru danych zawartego na powyższych nośnikach. Na użytkowanie komputera przenośnego zawierającego dane osobowe poza

Parafa:	

obszarem przetwarzania jego użytkownik musi uzyskać zgodę wydaną przez Administratora Systemów Informatycznych,

2.11 urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe przeznaczone do likwidacji niszczy się fizycznie w sposób uniemożliwiający odczytanie,

2.12 stosuje się bezwzględny zakaz przekazywania urządzeń, dysków lub innych elektronicznych nośników informacji, zawierających dane osobowe podmiotom nieuprawnionym do przetwarzania danych,

2.13 urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe przeznaczone do naprawy pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich skuteczne odzyskanie, ich naprawy dokonuje się pod nadzorem Administratora Systemów Informatycznych bądź innej kompetentnej i upoważnionej do przetwarzania danych osoby, wyznaczonej przez Administratora Systemów Informatycznych w porozumieniu z Administratorem Bezpieczeństwa Informacji.

2.14 Wdrożone zabezpieczenia systemu informatycznego monitorowane są przez Administratora Systemów Informatycznych oraz Administratora Bezpieczeństwa.

8.1.2. PODWYŻSZONY POZIOM BEZPIECZEŃSTWA

1. Podwyższony poziom bezpieczeństwa przetwarzania danych osobowych stosuje się, gdy w systemie informatycznym są przetwarzane dane sensytywne oraz żadne z urządzeń systemu informatycznego służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną.
2. Na środki podwyższonego poziomu bezpieczeństwa w systemie informatycznym służącym do przetwarzania danych osobowych składają się środki bezpieczeństwa określone w podrozdziale 8.1.1. pkt 2 niniejszego Rozdziału z dodatkowym uwzględnieniem poniższych wymagań:
   2.1. w przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana musi następować nie rzadziej niż co 30 dni, hasło musi składać się: z co najmniej 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne,
   2.2. urządzenia i elektroniczne nośniki informacji zawierające sensytywne dane osobowe przekazywane poza obszar ich przetwarzania zabezpiecza się w sposób zapewniający poufność i integralność tych danych.

8.1.3. WYSOKI POZIOM BEZPIECZEŃSTWA

1. Wysoki poziom bezpieczeństwa przetwarzania danych osobowych stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego służącego do przetwarzania danych osobowych połączone jest z siecią publiczną.

Parafa:	

2. Na środki wysokiego poziomu bezpieczeństwa w systemie informatycznym służącym do przetwarzania danych osobowych składają się środki bezpieczeństwa określone w podrozdziale 8.1.1. pkt 2 oraz podrozdziale 8.1.2 pkt 2 niniejszego Rozdziału z dodatkowym uwzględnieniem poniższych wymagań:
   2.1 system informatyczny należy chronić przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących go przed nieuprawnionym dostępem,
   2.2 zastosowanie powyżej wskazanych logicznych zabezpieczeń, obejmuje kontrolę przepływu informacji pomiędzy systemem informatycznym Administratora Danych a siecią publiczną oraz kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego Urzędu Miejskiego.
3. Wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej, stosuje się środki ochrony kryptograficznej.

9. POSTĘPOWANIE W PRZYPADKU STWIERDZENIA NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. W przypadku stwierdzenia w szczególności:
   1.1 przetwarzania danych w sposób sprzeczny z przepisami prawa oraz zasadami opisanym w Polityce, Instrukcji,
   1.2 zagrożenia dla bezpieczeństwa systemu informatycznego,
   1.3 wystąpienia zagrożenia lub domniemania ujawnienia danych osobowych,
   1.4 nieautoryzowanego dostępu do danych osobowych,
   1.5 niedozwolonego: zatajenia, powielenia, modyfikacji, zniszczenia, utraty, nieprawidłowego wykorzystania lub kradzieży danych osobowych

   Każda osoba, która poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzająca dane osobowe bądź posiada informacje mogące mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązana ten fakt niezwłocznie zgłosić Administratorowi Systemów Informatycznych.
2. W razie braku możliwości zawiadomienia Administratora Systemów Informatycznych lub osoby przez niego upoważnionej, należy powiadomić bezpośredniego przełożonego.
3. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Systemów Informatycznych lub upoważnionej przez niego osoby, osoba powiadamiająca powinna:
   3.1. niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków, a następnie ustalić przyczyny, lub sprawców zaistniałego zdarzenia, jeżeli jest to możliwe,
   3.2. rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,

Parafa:	

3.3. zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,

3.4. podjąć stosowne działania określone w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,

3.5. udokumentować wstępnie zaistniałe naruszenie,

3.6. nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Systemów Informatycznych lub osoby przez niego upoważnionej.

4. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Administrator Systemów Informatycznych lub osoba go zastępująca:

4.1 zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metod dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Urzędu Miejskiego,

4.2 wysłuchuje dokładnej relacji osoby zgłaszające z zaistniałego naruszenia, jak również relacji każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,

4.3 nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza Urzędu Miejskiego w celu przywrócenia stanu bezpieczeństwa przetwarzania danych.

5. Administrator Systemów Informatycznych dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego Załącznik nr 4 do niniejszej Instrukcji, który powinien zawierać w szczególności:

5.1 wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych w związku z naruszeniem,

5.2 określenie czasu i miejsca naruszenia i powiadomienia,

5.3 określenie okoliczności towarzyszących i rodzaju naruszenia,

5.4 wyszczególnienie wziętych faktycznie pod uwagę przesłanek wyboru metody postępowania i opis podjętego działania,

5.5 wstępną ocenę przyczyn wystąpienia naruszenia,

5.6 ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

6. Raport, o którym mowa w pkt 5 Administrator Systemów Informatycznych niezwłocznie przekazuje Administratorowi Bezpieczeństwa Informacji a w przypadku jego nieobecności osobie przez niego wyznaczonej.

7. Po wyczerpaniu niezbędnych środków doraźnych, po zaistniałym naruszeniu Administrator Systemów Informatycznych zasięga niezbędnych opinii i proponuje postępowanie naprawcze, w tym ustosunkowuje sie do kwestii ewentualnego odtworzenia danych z zabezpieczeń, zarządza termin wznowienia

Parafa:	

przetwarzania danych.

8. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej poprzez Kierownictwo Urzędu, Administratora Bezpieczeństwa Informacji, Pełnomocnika ds. Ochrony Informacji Niejawnych oraz Audytora Wewnętrznego.

10. ZAŁĄCZNIKI

Załącznik nr 1- Procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania oraz opisu sposobu, miejsca i okresu ich przechowywania oraz przechowywania elektronicznych nośników informacji zawierających dane osobowe.

Załącznik nr 2 - Zabezpieczenia systemów informatycznych ze wskazaniem środków sprzętowych infrastruktury informatycznej i telekomunikacyjnej, środków ochrony w ramach narzędzi programowych i baz danych oraz środków ochrony fizycznej danych przetwarzanych w systemach informatycznych służących do przetwarzania danych osobowych.

Załącznik nr 3 - Opis sposobu realizacji wymogów stawianych systemom informatycznym na mocy § 7 ust. 1 pkt 4 Rozporządzenia.

Załącznik nr 4 - Raport z naruszenia bezpieczeństwa systemu informatycznego.

Dokument sporządzono:	**Pełen podpis Administratora Danych:**	**Pieczęć**
Data: 24 maja 2013 r. Miejsce: Łomża	PREZYDENT MIASTA MIECZYSŁAW LEON CZERNIAWSKI	

Parafa:	

Załącznik nr 1

Procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania oraz opisu sposobu, miejsca i okresu ich przechowywania oraz przechowywania elektronicznych nośników informacji zawierających dane osobowe

---

1. Administrator Systemów Informatycznych sprawuje ogólny nadzór nad prawidłowym przebiegiem procedury sporządzania kopii zapasowych przetwarzanych zbiorów danych osobowych oraz kopii systemów informatycznych używanych do ich przetwarzania (w ramach danych nie gromadzonych na centralnym serwerze- np. pisma, terminarze itp.).

2. Procedura tworzenia kopii zapasowych przetwarzanych zbiorów danych osobowych występujących na komputerach użytkowników:

W celu zapewnienia bezpieczeństwa systemu i możliwości odtworzenia danych po wystąpieniu awarii wykonywane są kopie bezpieczeństwa na komputerach pracujących w systemie informatycznym:

2.1. Użytkownik przystępujący do pracy w systemie informatycznym, w którym przetwarzane są dane osobowe wpisuje swój identyfikator i hasło, a po uzyskaniu akceptacji uruchamia właściwą aplikację. Kończąc pracę użytkownik zobowiązany jest zamknąć aplikację, wylogować się z systemu i wyłączyć komputer.

2.2. Użytkownik komputera określa katalogi i zbiory danych osobowych, z których robione są kopie zapasowe.

2.3. Kopia wykonywana jest automatycznie i codziennie za pomocą dedykowanego oprogramowania do tworzenia kopii.

2.4. Na Użytkowniku ciąży obowiązek weryfikacji poprawności wykonanych kopii danych w razie ich nie wykonania poinformowania Administratora Systemów Informatycznych, który weryfikuje poprawność przeprowadzonych działań, a w razie wykrycia nieprawidłowości sporządza protokół, który podpisuje Administrator Systemów Informatycznych (ASI) i Użytkownik komputera.

2.5. Sporządzone w ten sposób kopie dzienne, przechowywane są na serwerze w pomieszczeniu nr 09 serwerowni pl. Stary Rynek 14.

2.6. Dodatkowo dla bezpieczeństwa codziennie kopia zgrywana jest na nośnik optyczny.

2.7. Ponadto każdego dnia tworzony jest elektroniczny protokół wykonania kopii dziennej zapisywany w folderze dostępnym tylko dla ASI w celu weryfikacji:

2.7.1. z jakich komputerów zostały sporządzone kopie zapasowe,

2.7.2. z jakich dni zostały sporządzone kopie (zakres czasowy).

2.8. Raz w miesiącu – wybrana dzienna kopia bezpieczeństwa jest dodatkowo archiwizowana na niezależnym od dysków serwera szyfrowanym optycznym nośniku danych.

2.8.1. Kopie miesięczne przechowywane są na medium optycznym zamykanym w metalowej szafie pancernej w pomieszczeniu 09 serwerowni pl. Stary Rynek 14.

2.8.2. Kopie dzienne przechowywane są na dysku przez okres 6 dni (cykl tygodniowy).

Parafa:	

3. **Procedura tworzenia kopii zapasowych zbiorów danych osobowych przetwarzanych przez system informatyczny.**

   Dzienne kopie zbiorów danych osobowych z podsystemów bazodanowych pracujących na bazach danych zawierających dane osobowe znajdujących się na serwerach sieciowych kopiowane są codziennie na przeznaczonym do tego celu serwerze.

3.1. Kopie dzienne z serwera dodatkowo dla bezpieczeństwa zgrywane są codziennie na nośnik –optyczny,

3.2. Z procedury tworzenia kopii każdego dnia tworzy się elektroniczny protokół wykonania kopii dziennej zapisywany w folderze dostępnym tylko dla ASI, ABI w celu weryfikacji poprawności:

   3.2.1. z jakich baz danych zostały sporządzone kopie zapasowe,

   3.2.2. z jakich dni zostały sporządzone kopie (zakres czasowy).

3.3. Raz w miesiącu – tworzy się kopię bezpieczeństwa na niezależnym od dysków serwera szyfrowanym optycznym nośniku danych.

3.4. Każdy nośnik z kopią powinien zawierać:

   3.4.1. numer kolejny nośnika,

   3.4.2. datę wykonania,

   3.4.3. nazwę jednostki,

   3.4.4. typ kopii.

3.5. Nośnik z kopia miesięczną przechowywane są w zamkniętej metalowej szafie pancernej w pomieszczeniu 09 serwerowni pl. Stary Rynek 14 i w Wydziale Spraw Społecznych i Zdrowia ul. Polna16 pokój 4.

3.6. Z procedury tworzenia miesięcznych kopii serwerowych sporządzany jest protokół podpisywany przez Administratora Bezpieczeństwa Informacji.

3.7. Nośniki z kopia miesięczną przechowywane są na medium optycznym zamykanym w metalowej szafie pancernej w pomieszczeniu 09 serwerowni pl. Stary Rynek 14 i w Wydziale Spraw Społecznych i Zdrowia ul. Polna16 pokój 4.

4. Dane w archiwum przechowywane są przez okres roku.

5. Nośniki zawierające kopie zapasowe baz z danymi osobowymi po ustaniu ich użyteczności podlegają likwidacji poprzez pozbawienie ich zapisu tych danych, a gdy nie jest to możliwe, nośniki danych uszkadza się fizycznie w sposób uniemożliwiający odczytanie zapisanych danych poprzez rozdrobnienie lub spalenie. Z tych czynności Administrator Systemów Informatycznych sporządza protokół.

6. Przebywanie osób nieuprawnionych do przetwarzania danych osobowych w pomieszczeniu serwerowni 09 dopuszczalne jest za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

7. Na wniosek ASI inicjowane są działania mające na celu wzmocnienie bezpieczeństwa przy przetwarzaniu danych osobowych w systemach informatycznych, oraz informowanie Administratora Bezpieczeństwa Informacji o konieczności wprowadzenia zmian w istniejących procedurach.

Załącznik nr 2

Zabezpieczenia systemów informatycznych ze wskazaniem środków sprzętowych infrastruktury informatycznej i telekomunikacyjnej, środków ochrony w ramach narzędzi programowych i baz danych oraz środków ochrony fizycznej danych przetwarzanych w systemach informatycznych służących do przetwarzania danych osobowych.

SYSTEMY INFORMATYCZNE SŁUŻĄCE DO PRZETWARZANIA DANYCH OSOBOWYCH																			
POZIOM BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH	**1. WYSOKI**	**2. WYSOKI**	**3. WYSOKI**	**4. WYSOKI**	**5. WYSOKI**	**6. WYSOKI**	**7. WYSOKI**	**8. WYSOKI**	**9. WYSOKI**	**10. WYSOKI**	**11. WYSOKI**	**12. WYSOKI**	**13. WYSOKI**	**14. WYSOKI**	**15. WYSOKI**	**16. WYSOKI**	**17. WYSOKI**	**18. WYSOKI**	**19. WYSOKI**
ŚRODKI SPRZĘTOWE INFRASTRUKTURY INFORMATYCZNEJ I TELEKOMUNIKACYJNEJ	**1. MIESZKAŃCY**	**2. SWDO SYSTEM WYDAWANIA DOWODÓW OSOBISTYCH**	**3. FLOWER**	**4. POJAZD**	**5. GROSZEK**	**6. KIEROWCA**	**7. FISKUS ZETO SA BIAŁYSTOK**	**8. TURBO EWID**	**9. AMAZIS**	**10. NEMEZIS**	**11. PB_USC**	**12. TURBOEWID MIENIE**	**13. PAKIET DLA ADMINISTRACJI**	**14. KADRY I PŁACE- QADR, QWARK PŁATNIK**	**15. SIO- SYSTEM INFORMACJI OŚWIATOWEJ**	**16. CMPPP**	**17. BESTIA**	**18. KSIĘGOWOŚĆ BUDŻETOWA**	**19. REJESRT VAT**
1 Zbiór danych osobowych przetwarzany jest przy użyciu komputera przenośnego.	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE
2 Komputer służący do przetwarzania danych osobowych nie jest połączony z lokalną siecią komputerową.	NIE	TAK	NIE	TAK	NIE	NIE	NIE	NIE	TAK	TAK	TAK	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE
3 Zastosowano urządzenia typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

Parafa:	

danych osobowych przed skutkami awarii zasilania.																				
4 Dostęp do zbioru danych osobowych, który przetwarzany jest na wydzielonej stacji komputerowej/ komputerze przenośnym zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła BIOS.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
5 Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
6 Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem karty procesorowej oraz kodu PIN lub tokena.	NIE	TAK	NIE	TAK	NIE	TAK	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE
7 Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem technologii biometrycznej.	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE
8 Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
9 Zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł.	TAK	TAK	TAK	TAK	TAK	NIE	NIE	NIE	NIE	TAK	TAK	TAK	NIE	TAK	NIE	NIE	TAK	TAK	TAK	TAK
10 Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
11 Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.	NIE DOTYCZY	TAK	NIE	NIE	NIE	NIE DOTYCZY	NIE DOTYCZ	NIE DOTYCZY	NIE DOTYCZ	NIE DOTYCZ	-----	-----	-----	-----	------	-----	-----	-----	-----	
12 Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.	NIE DOTYCZY	TAK	NIE	NIE	NIE	NIE DOTYCZY	NIE DOTYCZY	NIE DOTYCZY	NIE DOTYCZY	NIE DOTYCZY	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	
13 Zastosowano procedurę oddzwonienia (callback) przy transmisji realizowanej za pośrednictwem modemu.	NIE DOTYCZY	NIE DOTYCZY	NIE	NIE	NIE	NIE DOTYCZY	NIE DOTYCZY	NIE DOTYCZY	NIE DOTYCZY	NIE DOTYCZY	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	
14 Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	NIE	NIE	NIE	TAK	TAK	NIE	NIE	TAK	NIE	TAK	TAK	
15 Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
16 Użyto system Firewall do ochrony dostępu	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

do sieci komputerowej.																			
17 Użyto system IDS/IPS do ochrony dostępu do sieci komputerowej.	NIE	NIE	TAK	NIE	NIE	NIE	NIE	NIE	NIE	NIE	-----	-----	-----	-----	-----	-----	-----	-----	-----
ŚRODKI OCHRONY W RAMACH NARZĘDZI PROGRAMOWYCH I BAZ DANYCH	**1. MIESZKAŃCY**	**2. SWDO**	**3. FLOWER**	**4. POJAZD**	**5. GROSZEK**	**6. KIEROWCA**	**7. FISKUS ZETO SA BIAŁYSTOK**	**8. TURBO EWID**	**9. AMAZIS**	**10. NEMEZIS**	**11. PB_USC**	**12. TURBOEWID MIENIE**	**13. PAKIET DLA ADMINISTRACJI**	**14. KADRY I PŁACE**	**15. SIO- SYSTEM INFORMACJI**	**16. CMPPP**	**17. BESTIA**	**18. KSIĘGOWOŚĆ BUDŻETOWA**	**19. REJESRT VAT**
1 Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.	TAK	TAK	TAK	TAK	NIE	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
2 Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.	TAK	TAK	TAK	TAK	TAK	TAK	NIE	NIE	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
3 Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
4 Dostęp do zbioru danych osobowych wymaga uwierzytelnienia przy użyciu karty procesorowej oraz kodu PIN lub tokena.	NIE	TAK	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE
5 Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem technologii biometrycznej.	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE
6 Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.	TAK	TAK	NIE	NIE	NIE	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
7 Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.	TAK	NIE	TAK	TAK	TAK	TAK	TAK	NIE	NIE	NIE	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
8 Zastosowano kryptograficzne środki ochrony danych osobowych.	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE
9 Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
10 Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

osobowych w przypadku dłuższej nieaktywności pracy użytkownika.																			
11 Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	TAK	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE
ŚRODKI OCHRONY FIZYCZNEJ DANYCH:	**1. MIESZKAŃCY**	**2. SWDO**	**3. FLOWER**	**4. POJAZD**	**5. GROSZEK**	**6. KIEROWCA**	**7. FISKUS ZETO SA BIAŁYSTOK**	**8. TURBO EWID**	**9. AMAZIS**	**10. NEMEZIS**	**11. PB_USC**	**12. TURBOEWID MIENIE**	**13. PAKIET DLA ADMINISTRACJI**	**14. KADRY I PŁACE**	**15. SIO- SYSTEM INFORMACJI**	**16. CMPPP**	**17. BESTIA**	**18. KSIĘGOWOŚĆ BUDŻETOWA**	**19. REJESRT VAT**
1 Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi).	TAK	TAK	TAK	TAK	TAK	TAK	NIE	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	-----	TAK	TAK	TAK
2 Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności ogniowej >= 30 min.	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	-----	NIE	NIE	NIE
3 Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności na włamanie - drzwi klasy C.	NIE	NIE	NIE	NIE	NIE	NIE	NIE	-----	-----	-----	NIE	NIE	NIE	NIE	NIE	-----	NIE	NIE	NIE
4 Zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	NIE	NIE	-----	NIE	TAK	TAK
5 Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	-----	TAK	TAK	TAK
6 Dostęp do pomieszczeń, w których przetwarzany jest zbiory danych osobowych objęte są systemem kontroli dostępu.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	NIE	NIE	TAK	TAK	TAK	TAK	TAK	-----	NIE	TAK	TAK
7 Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych.	NIE	TAK	NIE	TAK	NIE	TAK	NIE	NIE	NIE	NIE	NIE	NIE	NIE	TAK	NIE	NIE	NIE	NIE	NIE
8 Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych jest w czasie nieobecności zatrudnionych tam	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE

pracowników nadzorowany przez służbę ochrony.																			
9 Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych przez cała dobę jest nadzorowany przez służbę ochrony.	NIE	NIE	NIE	NIE	NIE	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
10 Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej niemetalowej szafie.	NIE	NIE	TAK	TAK	TAK	TAK	TAK	TAK	NIE	NIE	-----	-----	-----	-----	-----	-----	-----	-----	-----
11 Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej metalowej szafie.	TAK	TAK	NIE	TAK	NIE	NIE	NIE	NIE	NIE	NIE	TAK	NIE	NIE	TAK	NIE	NIE	TAK	NIE	NIE
12 Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętym sejfie lub kasie pancernej.	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	TAK	TAK	NIE	NIE	NIE	NIE
13 Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej niemetalowej szafie.	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE
14 Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej metalowej szafie.	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	TAK	TAK	NIE	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
15 Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętym sejfie lub kasie pancernej.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	-----	-----	-----	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
16 Zbiory danych osobowych przetwarzane są w kancelarii tajnej, prowadzonej zgodnie z wymogami określonymi w odrębnych przepisach.	NIE	TAK	NIE	NIE	TAK	TAK	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE	NIE
17 Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
18 Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

Załącznik nr 3

Opis sposobu realizacji wymogów stawianych systemom informatycznym na mocy § 7 ust. 1 pkt 4 Rozporządzenia.

WYMOGI ROZPORZĄDZENIA MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI Z DNIA 29 KWIETNIA 2004 R. W SPARWIE DOKUMENTACJI PRZETWARZANIA DANYCH OSOBOWYCH ORAZ WARUNKÓW TECHNICZNYCH I ORGANIZACYJNYCH, JAKIM POWINNY ODPOWIADAĆ URZĄDZENIA I SYSTEMY INFORMATYCZNE SŁUŻĄCE DO PRZETWARZANIA DANYCH OSOBOWYCH

Nazwa systemu informatycznego / Wymóg rozporządzenia	1. SWDO SYSTEM WYDAWANIA DOWODÓW OSOBISTYCH	2. AMAZIS	3. NEMEZIS	4. MIESZKANCY	5. KIEROWCA	6. FISKUS ZETO BIAŁYSTOK	7. TURBO EWID	8. TURBO EWID- MIENIE	9. POJAZD	10. GROSZEK	11. PB_USC	12. PAKIET DLA ADMINISTRACJI	13. KADRY I PŁACE	14. FLOWER	15. SYSTEM INFORMACJI OŚWIADTOWEJ	16. CMPPP	17. BESTIA	18. KSIĘGOWOŚĆ BUDŻETOWA	19. REJESRT VAT
Data wprowadzenia danych do systemu	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Identyfikator użytkownika	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	NIE	TAK	TAK	TAK	TAK

Parafa:	

wprowadzającego dane osobowe do systemu chyba, że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba																			
Źródło danych, w przypadku zbierania danych, nie od osoby, której one dotyczą	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**
Informacje o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia chyba, że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**
Sprzeciw, o którym mowa w art. 32 ust. 1 pkt. 8 UODO	**NIE DOTYCZY – DANE NIE SĄ PRZETWARZANE W CELACH MARKETINGOWYCH ANI PRZEKAZYWANE INNYM ADMINISTRATOROM DANYCH**																		

Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje o:																			
identyfikatorze osoby wprowadzającej dane,	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**NIE**	**NIE**	**TAK**	**TAK**	**TAK**
dacie wprowadzenia danych do systemu.	**-----**	**-----**	**-----**	**-----**	**-----**	**-----**	**-----**	**-----**	**-----**	**-----**	**-----**	**-----**	**-----**	**-----**	**TAK**	**TAK**	**------**	**-----**	**-----**
Zabezpieczenie obszaru, w którym przetwarzane są dane osobowe, przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**
Przebywanie osób nieuprawnionych, jest dopuszczalne za zgodą administratora danych lub w obecności osoby	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**	**TAK**

upoważnionej do przetwarzania danych osobowych.																			
Stosowane są mechanizmy kontroli dostępu do danych.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Jeżeli dostęp do danych posiadają, co najmniej 2 osoby to w systemie rejestrowany jest dla każdego użytkownika odrębny identyfikator oraz dostęp do danych jest możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	NIE	TAK	TAK	TAK	TAK	TAK	TAK
System jest zabezpieczony przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
System jest	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

zabezpieczony przed utratą danych spowodowaną utratą zasilania lub zakłóceniami w sieci zasilającej.																			
Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie jest przydzielany innej osobie.	TAK	TAK	TAK	TAK	NIE	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
W przypadku, gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej, niż co 30 dni. Hasło składa się, co najmniej z 8 znaków.	NIE	TAK	TAK	TAK	NIE	TAK	TAK	TAK	NIE	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

służących do przetwarzania danych osobowych.																			
Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem oraz usuwa się niezwłocznie po ustaniu ich użyteczności.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	NIE	TAK	TAK	TAK	TAK
Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym przetwarzane są dane osobowe, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.	NIE	TAK	TAK	TAK	NIE	TAK	TAK	TAK	NIE	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

Administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do: 1. likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie. 2. przekazania	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	NIE	TAK	TAK	TAK

podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
3. naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

dostępem. Logiczne zabezpieczenia obejmują: a) kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczna;	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	NIE	TAK	TAK	TAK	TAK
b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	NIE	TAK	TAK	TAK	TAK
Administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	NIE	TAK	TAK	TAK	TAK

RAPORT
Z NARUSZENIA BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO W URZĘDZIE MIEJSKIM W ŁOMŻY

1. Data: ……..…. Godzina: ……

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

…….
(imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje)

3. Lokalizacja zdarzenia:

……..……
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:
……
……...……..……
……
……
……
……

5. Przyczyny wystąpienia zdarzenia:

……
……...……..
……
…..……

6. Podjęte działania:

……
……
……
……
……
……...

7. Postępowanie wyjaśniające:

……
……
……
……
……
……

....
(data, podpis Administratora Systemów Informatycznych)

Parafa:	