Zarządzenie nr 1136/VI/2014
Burmistrza Gminy Chojna
z dnia 19 września 2014 r.

w sprawie wdrożenia do stosowania w Urzędzie Miejskim w Chojnie „Polityki bezpieczeństwa Informacji w Urzędzie Miejskim w Chojnie" i „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Chojnie".

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182) i § 3, 4, 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 2004,Nr 100, poz. 1024) **zarządzam, co następuje:**

§ 1 Ustalam „Politykę bezpieczeństwa informacji Urzędu Miejskiego w Chojnie" i „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Chojnie" i zobowiązuję do ich przestrzegania oraz stosowania przez pracowników Urzędu Miejskiego w Chojnie zgodnie z załącznikiem nr 1 i 2 do zarządzenia.

§2. Zobowiązuje wszystkich pracowników Urzędu do zapoznania się z treścią „Polityki bezpieczeństwa Urzędu Miejskiego w Chojnie" i „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Chojnie" potwierdzonego podpisem w stosownym wykazie oraz do przyjęcia i podpisania upoważnień zezwalających na przetwarzanie danych osobowych.

§3 Z dniem wejścia w życie niniejszego zarządzenia, traci ważność zarządzenie Nr 981/V/2009 Burmistrza Gminy Chojna z dnia 30 listopada 2009r. w sprawie ustalenia i wdrożenia polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miejskim w Chojnie

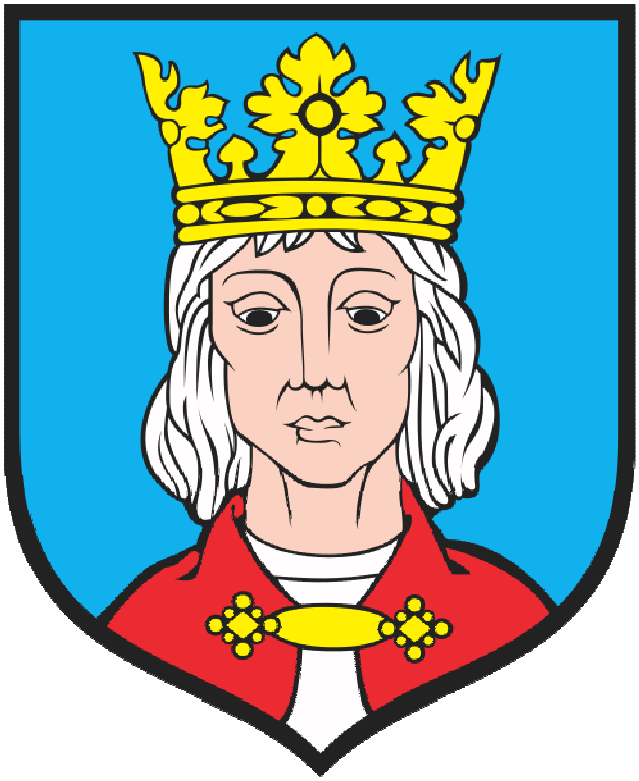
§4. Wykonanie zarządzenia powierzam Sekretarzowi Gminy Chojna.

§5 Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
mgr Adam Fedorowicz

Załącznik nr 1 do zarządzenia Nr 1136/VI/2014
Burmistrza Gminy Chojna z dnia 19.09.2014 r.

Polityka Bezpieczeństwa Informacji Urzędu Miejskiego w Chojnie



Rozdział I
Dfinicje

§ 1

Określenia i skróty użyte w Polityce Bezpieczeństwa Informacji oznaczają:

1. **Urząd –** Urząd Miejski w Chojnie,
2. **Administrator Danych Osobowych (ADO)** – Burmistrz Gminy Chojna, zwany dalej **Administratorem.**
3. **Administrator Bezpieczeństwa Informacji (ABI)** - osoba wyznaczona przez Burmistrza Chojny, odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych oraz za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych w przetwarzanych zbiorach danych osobowych. W Urzędzie Miejskim w Chojnie funkcją Administratora Bezpieczeństwa Informacji pełni Pan mgr inż. Mariusz Hadrzyński, naczelnik wydziału ZBF.
4. **Administrator Systemów Informatycznych (ASI) –** osoba wyznaczona przez Burmistrza Chojny.
5. **Zarządzający oprogramowaniem –** osoba wyznaczona przez Burmistrza Chojny, odpowiedzialna za zarządzanie oprogramowaniem komputerowym w Urzędzie Miejskim w Chojnie.
6. **u.o.d.o.** – ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 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. **Bezpieczeństwo systemu informatycznego** – wdrożenie przez Administratora lub osobę przez niego uprawnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz nieuprawnioną zmianą, utratą, uszkodzeniem lub zniszczeniem.
9. **Przetwarzanie danych osobowych** – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
10. **Osoba upoważniona lub użytkownik systemu** – osoba posiadająca upoważnienie wydane przez Administratora lub uprawnioną przez niego osobę

i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej w zakresie wskazanym w upoważnieniu, zwana dalej **użytkownikiem.**

11. **Przełożony użytkownika** – Kierownik Wydziału lub Sekretarz Gminy, zwany dalej **przełożonym.**
12. **Osoba uprawniona** – osoba posiadająca upoważnienie wydane przez Administratora do wykonywania w jego imieniu określonych czynności.
13. **Użytkownik uprzywilejowany** – osoba posiadająca najwyższy stopień uprawnień do zarządzania systemem informatycznym.

Rozdział II
Postanowienia ogólne

§ 2

1. Niniejsza „Polityka Bezpieczeństwa Informacji", ma zastosowanie do ochrony zbiorów danych osobowych przetwarzanych w Urzędzie Miejskim w Chojnie, w celu ich bezpiecznego wykorzystania oraz określa zasady korzystania z systemów informatycznych.
2. Polityka Bezpieczeństwa została opracowana na podstawie art. 36 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182) w celu realizacji § 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r., Nr 100, poz. 1024).
3. Na Politykę Bezpieczeństwa składają się poszczególne instrukcje i procedury zawierające informacje dotyczące rozpoznania procesów ich przetwarzania oraz wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

W skład Polityki Bezpieczeństwa wchodzą:

a. Realizacja podstawowych założeń rozporządzenia,
b. Zarządzanie przetwarzaniem danych osobowych oraz ich bezpieczeństwem,
c. Zasady przetwarzania danych osobowych (załącznik nr 3 do Polityki Bezpieczeństwa Informacji)
d. Ochrona obszaru przetwarzania i monitorowanie ochrony zasobów danych osobowych (załącznik nr 4 do Polityki Bezpieczeństwa Informacji)

e. Instrukcja zarządzania sprzętem komputerowym (załącznik nr 5 do Polityki Bezpieczeństwa Informacji)
f. Instrukcja zarządzania oprogramowaniem (załącznik nr 6 do Polityki Bezpieczeństwa Informacji)
g. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Chojnie (Załącznik nr 2 do Zarządzenia nr Nr 1136/VI/2014 Burmistrza Gminy Chojna).

Rozdział III
Realizacja podstawowych założeń Rozporządzenia.

§ 3

1. Obszar przetwarzania danych osobowych w Urzędzie Miejskim w Chojnie obejmuje budynki, pomieszczenia i części pomieszczeń, w których przetwarzane są dane osobowe, tzn. miejsca, w których wykonuje się operacje na danych osobowych (wpisuje, modyfikuje, kopiuje), jak również miejsca gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające komputerowe nośniki informacji, a także pomieszczenia, gdzie składowane są uszkodzone komputerowe nośniki danych). Obszar przetwarzania danych osobowych określony został w „Wykazie pomieszczeń, w których przetwarzane są dane osobowe", stanowiącym Załącznik nr 1 do Polityki Bezpieczeństwa Informacji.
2. Zawiera następujące informacje:
   a) lokalizację,
   b) numer pomieszczenia/przeznaczenie,
   c) piętro,
   d) wydział, referat, samodzielne stanowisko pracy użytkujący pomieszczenie,
   e) osoby pracujące w pomieszczeniu,
   f) zabezpieczenie pomieszczenia.
3. Wymogi dotyczące ochrony obszaru przetwarzania danych określone zostały w załączniku nr 4 do Polityki Bezpieczeństwa Informacji (Zasady ochrony pomieszczeń, w których Przetwarzane są dane osobowe).

§ 4

Wykaz zbiorów danych przetwarzanych w Urzędzie Miejskim w Chojnie i programów zastosowanych do przetwarzania danych.

1. Wykaz zbiorów znajduje się w odrębnym dokumencie „Wykaz zasobów danych osobowych i systemów ich przetwarzania", stanowiącym Załącznik Nr 2 do Polityki Bezpieczeństwa Informacji i zawiera następujące informacje:
   a) nazwa zbioru danych,
   b) system przetwarzania (Tradycyjny, Informatyczny),
   c) zastosowane oprogramowanie,
   d) lokalizacja miejsca przetwarzania,
   e) data rejestracji zbioru w GIODO.

   Systemy działające w urzędzie, przetwarzające dane osobowe:
   - SIGID – zestaw oprogramowania finansowo – księgowego i kadrowego,
   - Clanet – zestaw oprogramowania ewidencji ludności i ewidencji wyborców,
   - PB_USC – oprogramowanie do obsługi aktów urodzenia i zgonów,
   - Płatnik - obsługa dokumentów ubezpieczeniowych i wymiana informacji z Zakładem Ubezpieczeń Społecznych,
   - SWDO – system wydawania dowodów osobistych.

§ 5

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól Informacyjnych i powiązania między nimi.

1. Przetwarzanie odbywa się częściowo na serwerze, częściowo na stacjach roboczych użytkowników (dostęp możliwy wyłącznie ze specjalizowanego oprogramowania klienckiego, z komputerów podłączonych do urzędowej sieci lokalnej).
2. SWDO (System Wydawania Dowodów Osobistych) znajduje się na komputerach dostarczonych przez Ministerstwo i dostęp do tego zbioru danych jest możliwy tylko z tych stanowisk. Tylko pięć osób jest upoważnionych przez Ministerstwo do pracy na tych komputerach.

§ 6

Sposób przepływu danych pomiędzy poszczególnymi systemami.

1. W ramach procesów przetwarzania danych nie dochodzi do przepływu danych pomiędzy różnymi systemami informatycznymi. Szczegółowe informacje

dotyczące przepływu danych osobowych pomiędzy danymi systemami informatycznymi znajdują się w poszczególnych instrukcjach zarządzania danym systemem.

2. W ramach procesów przetwarzania danych dochodzi do przepływu danych pomiędzy różnymi modułami systemów informatycznych.

§ 7

Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzania danych.

1. W systemie informatycznym obowiązują zabezpieczenia na poziomie podstawowym. Szczegółowe omówienie środków zabezpieczenia technicznego i organizacyjnego znajduje się w „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miejskim w Chojnie" - Załącznik nr 2 do Zarządzenia nr Nr 1136/VI/2014 Burmistrza Gminy Chojna.

Rozdział IV

Zarządzanie przetwarzaniem danych osobowych oraz ich bezpieczeństwem

§ 8

Zakres praw i obowiązków administratora danych osobowych oraz ich bezpieczeństwem

1. Administratorem danych osobowych w Urzędzie Miejskim w Chojnie w rozumieniu Art. 7 pkt 4 u.o.d.o. jest Burmistrz Gminy Chojna.
2. Administrator, powołuje Administratora Bezpieczeństwa Informacji (ABI) oraz jego zastępcę, który w jego imieniu wykonuje zadania w zakresie:
   a) nadzoru nad przestrzeganiem zasad ochrony danych osobowych w Urzędzie Miejskim w Chojnie,
   b) przeprowadzania czynności kontrolnych w Urzędzie w celu oceny zgodności przetwarzania danych osobowych z u.o.d.o.,
   c) przekazywania do Administratora sprawozdań z kontroli zgodności przetwarzania danych osobowych w Urzędzie z u.o.d.o.,
   d) prowadzenia dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zabezpieczenia danych osobowych – niniejsza polityka oraz wynikające z niej instrukcje, Załącznik Nr 3, 5 i 6,

e) nadzoru nad prowadzeniem ewidencji osób upoważnionych do przetwarzania danych osobowych,
f) zgłaszania zbiorów danych osobowych do rejestracji GIODO - przygotowywania nowych wniosków rejestracyjnych lub aktualizacji wniosków zgłoszonych wcześniej,
g) wdrażania znajomości przepisów dot. ochrony danych osobowych,
h) kontrolowania procesów udostępniania danych osobowych,
i) przygotowywania projektów umów powierzania przetwarzania danych osobowych innemu podmiotowi,
j) wydawania zaleceń dla kierowników komórek organizacyjnych w zakresie podwyższenia standardów zabezpieczeń danych osobowych,
k) monitorowania ochrony zasobów danych osobowych w Urzędzie,
l) współpracy z Administratorem Systemu Informatycznego w zakresie nadzoru i kontroli nad bezpieczeństwem systemu informatyczneg, w którym przetwarzane są dane osobowe,
m) prowadzenia wykazu obszarów przetwarzania danych osobowych – spis budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe,
n) przeprowadzania kontroli stanu zabezpieczeń fizycznych i technicznych obszaru przetwarzania danych,
o) podejmowania działań zgodnych z obowiązującymi w Urzędzie procedurami w sytuacji naruszenia ochrony danych osobowych.

3. Administrator powołuje zastępcę ABI, który wykonuje zadania ABI podczas jego nieobecności.
4. Administrator powołuje Zarządzającego oprogramowaniem, który przeprowadza okresową inwentaryzację oprogramowania i ustanawia zasady i procedury ciągłego utrzymania oprogramowania.
5. Burmistrz wyznacza Właścicieli (Opiekunów) poszczególnych zasobów danych osobowych (zwanych dalej Właścicielami ZDO).
6. Rolę Właścicieli zasobów danych osobowych pełnią naczelnicy Wydziałów, kierownicy Referatów oraz pracownicy na samodzielnych stanowiskach pracy odpowiedzialni za dany zasób danych osobowych (wynikający z zakresu pełnionych obowiązków).

7. Do obowiązków Właścicieli ZDO należy:
   a) zarządzanie zasobem danych osobowych w ramach zadań realizowanych przez swe wydziały, referaty oraz samodzielne stanowiska pracy,

b) występuje z wnioskiem do Administratora o nadawanie upoważnień dotyczących dostępu do zasobu danych osobowych podległym pracownikom,
c) zgłaszanie do ABI zamiaru utworzenia zbioru danych osobowych oraz informacji dotyczących zmian w zakresie i sposobach przetwarzania tego zbioru,
d) realizacja procesu udostępniania danych osobowych innemu podmiotowi lub osobie, której dane dotyczą,
e) wypełnianie obowiązków określonych w załączniku nr 1 dotyczących obszaru przetwarzania, wykazu osób upoważnionych do przetwarzania danych osobowych, zastosowania zabezpieczeń zbiorów,
f) prowadzenie ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w podległym wydziale, referacie oraz na samodzielnym stanowisku pracy z uwzględnieniem zakresu odpowiedzialności za ochronę tych danych w stopniu odpowiednim do zadań tej osoby przy przetwarzaniu danych osobowych, przekazywanie ABI aktualnej ewidencji tych osób wraz z priorytetami im przydzielonymi,
g) prowadzenie w podległym wydziale, referacie oraz na samodzielnym stanowisku pracy nadzoru nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe generowane przez system informatyczny,
h) dopilnowanie aby monitory stanowisk dostępu do danych osobowych w podległym wydziale, referacie oraz na samodzielnym stanowisku pracy były tak ustawione, aby uniemożliwić postronnym osobom wgląd w dane oraz dopilnowanie stosowania wygaszaczy ekranów na tych stanowiskach,
i) zapoznawanie pracowników mających dostęp do danych osobowych z przepisami dotyczącymi ochrony danych osobowych.

8. Za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych Urzędu, odpowiada Administrator Systemu Informatycznego (ASI).
9. Do obowiązków ASI w zakresie ochrony danych osobowych należy:
   a) zapewnienie bezawaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych w Urzędzie,
   b) prowadzenia nadzoru nad naprawami, konserwacją i likwidacją urządzeń komputerowych, na których zapisane są dane osobowe,
   c) prowadzenie w Urzędzie nadzoru nad przeglądami, konserwacją, uaktualnianiem systemów służących do przetwarzania danych osobowych oraz podejmowanie natychmiastowych działań zabezpieczających stan systemu informatycznego w Urzędzie w przypadku otrzymania informacji o naruszeniu

zabezpieczeń informatycznych, powiadomienie o zaistnieniu tego faktu Administratora,

d) prowadzenie nadzoru nad przesyłaniem danych osobowych drogą teletransmisji,
e) nadzór nad przestrzeganiem zasad bezpieczeństwa w przypadku udostępniania danych osobowych innym podmiotom drogą teletransmisji danych.
f) przeciwdziałanie dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe,
g) podejmowanie odpowiednich działań w przypadku naruszeń w systemie zabezpieczeń,
h) właściwy nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,
i) podejmowanie działań zgodnie przepisami w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego,
j) nadzór nad wykonywaniem kopii awaryjnych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu,
k) zapisy dotyczące zadań poszczególnych osób muszą zostać wpisane w ich zakresy obowiązków i być przechowywane w ich aktach osobowych. Rozdział V – Odpowiedzialność karna.

Rozdział V

Sankcje

§ 9

1. Naruszenie przepisów o ochronie danych osobowych jest zagrożone sankcjami karnymi określonymi w art. 49 – 54a u.o.d.o. oraz w art. 130, 266 – 269, 287 Kodeksu Karnego.
2. Niezależnie od odpowiedzialności przewidzianej w przepisach, o których mowa w ust. 1, naruszenie zasad ochrony danych osobowych obowiązujących w Urzędzie Miejskim w Chojnie może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

Rozdział VI

Postanowienia końcowe

§ 10

1. Niniejsza Instrukcja przeznaczona jest dla użytkowników i ich przełożonych, którzy nadzorują przetwarzanie danych osobowych.
2. Wykonanie postanowień Instrukcji ma na celu wprowadzenie jednolitego systemu zarządzania systemem informatycznym w Urzędzie Miejskim w Chojnie.

§ 11

W sprawach nieuregulowanych Instrukcją znajdują zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182) i rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100. poz. 1024).

§ 12

Wszelkie zmiany w Polityce Bezpieczeństwa mogą być wprowadzone tylko na podstawie zarządzeń Administratora.

Załącznik nr 1 do Polityki Bezpieczeństwa Informacji

Wykaz pomieszczeń, w których przetwarzane są dane osobowe.

Lp.	Lokalizacja adres i numer budynku	Numer pomieszczenia (przeznaczenie)	Piętro	Dział/pion użytkujący pomieszczenie	Osoby pracujące w pomieszczeniu	Zabezpieczenie pomieszczenia
1						
2						
3						
4						
5						
6						

Załącznik nr 2 do Polityki Bezpieczeństwa Informacji

Ewidencja zbiorów danych przetwarzanych w Urzędzie Miejskim w Chojnie

Lp.	NAZWA ZBIORU	System przetwarzania T – tradycyjny I - informatyczny	Nazwa programu	Lokalizacja adres, nr pokoju	Data rejestracji zbioru w GIODO
1					
2					
3					
4					
5					
6					
7					
8					
9					

Załącznik nr 3 do
Polityki Bezpieczeństwa Informacji.

Zasady przetwarzania danych osobowych

§. 1

Rejestracja zbiorów danych osobowych

1. Właściciel ZDO zgłasza ABI zamiar utworzenia nowego zbioru danych osobowych.
2. ABI przygotowuje projekt zgłoszenia zbioru danych osobowych do rejestracji GIODO, jeżeli takie zgłoszenie jest ustawowo wymagane, na podstawie obowiązującego wzoru wniosku określonego w Rozporządzeniu do u.o.d.o.
3. ASI w uzgodnieniu z ABI określa warunki techniczne dotyczące zabezpieczeń w systemie informatycznym, o których mowa w części E i F zgłoszenia zbioru danych osobowych do rejestracji GIODO.
4. ABI sprawdza opisane w części E i F zgłoszenia zbioru danych osobowych do rejestracji GIODO warunki techniczne dotyczące zabezpieczeń w systemie informatycznym, a w przypadku niewystarczającego poziomu zabezpieczeń występuje z wnioskiem do ASI o podniesienie poziomu zabezpieczeń.
5. Przygotowany przez ABI projekt zgłoszenia zbioru danych osobowych do rejestracji GIODO parafują Właściciel ZDO oraz ASI.
6. Parafowany wniosek ABI przedstawia do akceptacji Sekretarzowi Gminy
7. Sekretarz Gminy przedkłada wniosek o rejestrację zbioru danych osobowych Administratorowi i zgłasza go do GIODO.
8. Tryb określony w niniejszym paragrafie stosuje się odpowiednio w razie konieczności aktualizacji zgłoszenia zbioru danych osobowych do rejestracji GIODO.
9. Właściciel ZDO zgłasza w ciągu 5 dni wszelkie zmiany dotyczące przetwarzania danych w zarejestrowanym zbiorze danych osobowych do ABI.
10. IAS zgłasza w ciągu 5 dni wszelkie zmiany dotyczące sposobu przetwarzania danych osobowych oraz ich zabezpieczeń w systemie informatycznym.
11. ABI przygotowuje aktualizację zgłoszenia zbioru danych osobowych do GIODO w terminie 30 dni od dnia dokonania zmiany w zbiorze, na podstawie obowiązującego wzoru określonego w Rozporządzeniu do u.o.d.o.
12. Wniosek aktualizacyjny zgłoszenie zbioru danych osobowych do rejestracji GIODO parafuje Właściciel ZDO oraz ASI.
13. Parafowany wniosek ABI przedstawia do akceptacji Sekretarzowi Gminy.
14. Sekretarz Gminy przedkłada Administratorowi do podpisania wniosek aktualizacyjny zgłoszenie zbiór danych osobowych i wysyła go do GIODO.

§. 2
Udostępnianie danych osobowych

1. Dane osobowe mogą być udostępniane w następujących przypadkach:
   a) na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów,
   b) na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych,
   c) wniosku osoby, której dane dotyczą.
2. Dane osobowe, udostępnia się na pisemny, umotywowany wniosek, chyba, że inny przepis stanowi inaczej.
3. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
4. W przypadku żądania udzielenia informacji na temat przetwarzanych danych osobowych na pisemny wniosek pochodzący od osoby, której dane dotyczą, odpowiedź na nie następuje w terminie 30 dni od daty jego otrzymania.
5. Wniosek o udostępnienie przekazywany jest do Właściciela ZDO, który podejmuje decyzję o udostępnieniu i informuje o tym ABI.
6. ABI akceptuje decyzję o udostępnieniu i przekazuje ją do Właściciela ZDO.
7. Właściciel ZDO jest odpowiedzialny za przygotowanie danych osobowych do udostępnienia w zakresie wskazanym we wniosku.
8. Odpowiedź na wniosek o udostępnienie danych osobowych jest akceptowana i parafowana przez Właściciela ZDO.
9. Informacje zawierające dane osobowe są przekazywane uprawnionym podmiotom lub osobom za potwierdzeniem odbioru w następujący sposób:
   a) listem poleconym za potwierdzeniem odbioru,
   b) poprzez teletransmisję danych, zgodnie z procedurami ochrony danych podczas transmisji – określonymi w instrukcji zarządzania danym systemem teleinformatycznym służącym do przetwarzania danych osobowych,
   c) inny, określony konkretnym wymogiem prawnym lub umową.
10. ASI nadzoruje przestrzeganie zasad bezpieczeństwa w przypadku udostępniania danych osobowych drogą teletransmisji danych.

§. 3
Powierzanie przetwarzania danych osobowych

1. Powierzenie przetwarzania danych osobowych odbywa się zgodnie z art.31 u.o.d.o. na podstawie umowy zawartej na piśmie pomiędzy Urzędem Miejskim w Chojnie

a danym podmiotem, któremu zleca się czynności związane z przetwarzaniem danych osobowych.

2. Decyzje powierzenia przetwarzania danych osobowych podejmuje właściciel ZDO, który będzie zlecać podmiotom zewnętrznym czynności związane z przetwarzaniem danych osobowych.
3. Właściciel ZDO informuje ABI o zamiarze powierzenia danych osobowych do przetwarzania.
4. ABI przygotowuje projekt umowy powierzenia danych osobowych innemu podmiotowi.
5. W projekcie umowy należy wyspecyfikować zakres czynności związanych z przetwarzaniem powierzonych danych osobowych, zakres danych oraz wymagania dotyczące ochrony danych.
6. Każda osoba delegowana do wykonywania zadań na rzecz Urzędu Miejskiego w Chojnie, związanych z powierzeniem przetwarzania danych osobowych musi podpisać oświadczenie o zachowaniu w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia (wzór w załączniku nr 1 do „Zasad przetwarzania danych osobowych").
7. Projekt umowy parafują:
   a) ABI,
   b) właściciel ZDO,
   c) ASI – jeżeli zlecenie czynności dotyczyć będzie przetwarzania danych w systemie informatycznym,
   d) Radca Prawny.
8. Zaparafowany projekt umowy jest przedkładany przez ABI do akceptacji i podpisu Administratorowi.
9. W sytuacji powierzenia czynności związanych z archiwizacją zasobów danych osobowych innemu podmiotowi, w umowie nie określa się zakresu powierzonych danych osobowych a jedynie wymagania co do bezpieczeństwa danych osobowych.
10. Projekt umowy powierzenia danych osobowych w celach archiwalnych parafują:
    a) ABI,
    b) ASI – jeżeli zlecenie dotyczyć będzie archiwizacji danych przetwarzanych w systemie informatycznym (kopie danych lub wykonywanie czynności archiwalnych),
    c) Radca Prawny.
11. Zaparafowany projekt umowy jest przedkładany przez ABI do akceptacji i podpisu Administratorowi.

BURMISTRZ
mgr Adam Fedorowicz

Załącznika nr 1 do
Zasad przetwarzania danych osobowych

OŚWIADCZENIE

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 wynikających z umowy o pracę zarówno w trakcie wykonywania umowy i po jej ustaniu.	
Zadań wynikających z umowy cywilnoprawnej zarówno w trakcie wykonywania umowy i po jej ustaniu.	
Zadań wynikających z umowy praktyki zarówno w trakcie wykonywania umowy i po jej ustaniu.	

*właściwe zaznaczyć

Zobowiązuje się przestrzegać regulaminów, instrukcji i procedur obowiązujących w Urzędzie Miejskim w Chojnie dotyczących ochrony danych osobowych, w szczególności oświadczam, że bez upoważnienia służbowego nie będę wykorzystywał(a) danych osobowych ze zbiorów Urzędu Miejskiego w Chojnie.

Oświadczam, że zostałem(am) poinformowany(a) o obowiązujących w Urzędzie Miejskim w Chojnie zasadach dotyczących przetwarzania danych osobowych określonych w Polityce Bezpieczeństwa danych Osobowych.

Oświadczam, że zostałem(am) zapoznany(a) z przepisami o ochronie danych osobowych oraz o grożącej stosownie do przepisów rozdziału 8 ustawy o ochronie danych osobowych odpowiedzialności karnej (Dz. U. z 2014 r., poz. 1182)

……	……	……
Miejsce złożenia oświadczenia	data złożenia oświadczenia	numer PESEL

……

Podpis osoby składającej oświadczenie

Załącznik nr 4 do
Polityki Bezpieczeństwa Informacji

Ochrona obszaru przetwarzania i monitorowania ochrony zasobów danych osobowych

§. 1
Zasady ochrony pomieszczeń, w których przetwarzane są dane osobowe

1. Sekretarz Gminy wspólnie z Kierownikami wydziałów, referatów i osobami zajmującymi samodzielne stanowiska pracy odpowiadają za należyte zabezpieczenie fizyczne zasobów danych osobowych w podległych komórkach.
2. ABI przeprowadza bezpośrednią kontrolę stanu zabezpieczeń fizycznych zbiorów danych osobowych oraz zgłasza do Sekretarza Gminy swoje uwagi lub rekomenduje zlecenie kontroli specjalistycznej firmie.
3. Obszarem, w którym przetwarzane są dane osobowe są budynki Urzędu Miejskiego w Chojnie, ul. Jagiellońska 4, ul. Jagiellońska 2 oraz ul. Piastów 3.
4. ABI jest odpowiedzialny za prowadzenie aktualnego wykazu pomieszczeń, w których przetwarzane są dane osobowe.
5. Przebywanie wewnątrz pomieszczeń osób niebędących pracownikami Urzędu, o których mowa w pkt. 4, osób nieuprawnionych do dostępu do danych osobowych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych lub za zgodą Właściciela ZDO.
6. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do przestrzegania zasad dotyczących wprowadzania osób trzecich do obszaru, o którym mowa w pkt. 3. Ruch osób z zewnątrz w wymienionym obszarze powinien odbywać się pod kontrolą osób upoważnionych.
7. Sekretarz Gminy zezwala na przebywanie w pomieszczeniach (o których mowa w pkt. 4) osobom sprzątającym te pomieszczenia poza godzinami pracy Urzędu bez konieczności obecności osoby dopuszczonej do przetwarzania danych. Osoby te podpisują oświadczenie o zachowaniu poufności.
8. Budynki lub pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób dopuszczonych do danych osobowych, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.
9. Pomieszczenia, w których przetwarzane są dane wrażliwe oraz pomieszczenia serwerowni i archiwów powinny podlegać specjalnej ochronie w postaci zastosowania systemu sygnalizacji alarmu i włamania,
10. Właściciel ZDO zabezpiecza zgodnie z wytycznymi pkt 8, 9, 10 obszar przetwarzania danych.

11. Budynek i pomieszczenia Urzędu Miejskiego w Chojnie posiadają następujące zabezpieczenia:
    a) Budynek administracyjny Urzędu Miejskiego przy ul. Jagiellońskiej 2 posiada trzy pary drzwi wejściowych, zamykanych na klucz. Dodatkowo drzwi wejściowe USC zabezpieczone są od zewnątrz kratą stalową .
    b) Budynek administracyjny Urzędu Miejskiego przy ul. Jagiellońskiej 4 posiada dwie pary drzwi wejściowych. Każda para drzwi posiada dwa zamki.
    c) Budynek administracyjny Urzędu Miejskiego przy ul. Piastów 3 posiada jedną parę drzwi wejściowych, zamykanych jednym zamkiem.
    d) Klucze do w/w budynków posiadają wyznaczenie i upoważnienie pracownicy. Wykaz osób znajduje się w Wydziale Organizacyjnym u pracownika d/s organizacyjnych i budżetowo – gospodarczych.
    e) Zapasowe klucze do pomieszczeń biurowych budynku administracyjnego Urzędu Miejskiego przy ulicy Jagiellońskiej 4 znajdują się w gablocie w pokoju nr 16,
    f) W systemy alarmowe wyposażone są pomieszczenia:
        - USC – przy ulicy Jagiellońskiej 2; klucze do pomieszczeń posiada Kierownik USC i z-ca Kierownika,
        - Sekretariat w budynku przy ul. Jagiellońskiej 4; klucze dostępu posiada pracownik d/s techniczno-kancelaryjnych, pracownik d/s organizacyjnych i budżetowo-gospodarczych, oraz Naczelnik Wydziału.
    g) Dokumenty z danymi osobowymi powinny być przechowywane w szafach na akta wyposażonych w zamki,

§. 2

Przetwarzanie danych osobowych poza obszarem przetwarzania

1. W sytuacji przetwarzania danych osobowych na komputerach przenośnych lub dokumentach papierowych poza obszarem wymienionym w § 1 pkt 3, należy bezwzględnie chronić te dane przed dostępem do nich osób nieupoważnionych.
2. Zasady ochrony komputerów przenośnych, na których przetwarzane są dane osobowe, określa ASI w „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miejskim w Chojnie”.

§. 3

Monitorowanie ochrony zasobów danych osobowych

1. Właściciele ZDO i Sekretarz Gminy aktualizują (w formie elektronicznej) ABI:

a) aktualny wykaz zasobów danych osobowych przetwarzanych w danej komórce organizacyjnej,
b) wykaz osób upoważnionych do przetwarzania określonego zasobu danych osobowych,
c) wykaz pomieszczeń, w których przetwarzany jest poszczególny zasób danych osobowych w podległej komórce organizacyjnej i ich zabezpieczeń.

2. Pracownik ds. Kadr na bieżąco informuje ABI o:
   a) ustaniu zatrudnienia w Urzędzie określonej osoby, celem kontroli aktywności jego kont w systemie informatycznym,
   b) przeniesieniu pracownika do innego wydziału Urzędu, celem kontroli jego praw do dostępu do danych osobowych.
3. ASI przekazuje ABI:
   a) aktualny wykaz systemów teleinformatycznych – aplikacji, w których przetwarzane są dane osobowe z informacją o programach zastosowanych do przetwarzania tych danych,
   b) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,
   c) sposób przepływu danych pomiędzy poszczególnymi systemami.
4. ABI ustala szczegółowe zakresy potrzebnych informacji oraz formę i tryb ich przekazywania.
5. Każda zmiana informacji w zakresie ujętym w pkt 1-3 wymaga bieżącej aktualizacji przez osoby wskazane w wymienionych punktach.
6. Na podstawie przekazywanych informacji ABI prowadzi aktualny wykaz zasobów danych osobowych przetwarzanych w Urzędzie, który zamieszcza w dokumencie „Wykaz zasobów danych osobowych i systemów ich przetwarzania”.

Załącznik nr 5 do
Polityki Bezpieczeństwa Informacji

Instrukcja zarządzania sprzętem komputerowym

1) **Procedura zgłaszania zapotrzebowania na sprzęt komputerowy.**
    a. Zgłoszenie ASI zapotrzebowania na sprzęt komputerowy poprzez wypełnienie formularza zapotrzebowania stanowiący załącznik Nr 1 do Instrukcji Zarządzania Systemem Komputerowym.
    b. ASI konsultuje zgłoszenie z Skarbnikiem Gminy
    c. Decyzje o zakupie oraz o trybie zakupu podejmuje Burmistrz.
    d. Jeżeli nie jest to pilny zakup , ale został pozytywnie zaopiniowany przez ASI i Skarbnika Gminy, to zostaje on wpisany do Rejestru Zapotrzebowania Sprzętu Komputerowego.
2) **Procedura zakupu sprzętu komputerowego.**
    a. Na początku roku kalendarzowego, po przyjęciu budżetu, ASI wraz Skarbnikiem Gminy decydują o strategii zakupów inwestycyjnych. Analizowany jest Rejestr Zapotrzebowania na Sprzęt Komputerowy i podejmowane są decyzje o kolejności zakupów,
    b. Zakupy sprzętu komputerowego dokonywane są w oparciu o ustawę o zamówieniach publicznych,
    c. ASI przygotowuje Specyfikacje Istotnych Warunków Zamówienia, która jest zatwierdzana przez Burmistrza,
    d. Rozstrzygnięcie postępowania przetargowego regulują odrębne przepisy,
    e. W sytuacjach awaryjnych (nagła awaria sprzętu, itp.) procedura przewiduje zakupy z wolnej ręki.
3) **Procedura przyjęcia do ewidencji sprzętu komputerowego.**
    a. ASI wypełnia zgłoszenie sprzętu komputerowego do Wydziału Finansowego prowadzącego Ewidencję Środków Trwałych, które stanowi załącznik Nr 2 do Instrukcji Zarządzania Sprzętem Komputerowym. Tam nadawany jest nr inwentarzowy.
    b. Wydział Finansowy wprowadza do Ewidencji Środków Trwałych zakupiony sprzęt komputerowy.
4) **Procedura instalacji sprzętu komputerowego na stanowisku pracy.**
    a. Przed instalacją sprzętu komputerowego na stanowisku pracy ASI sprawdza działanie urządzeń, aby w razie problemów zgłosić reklamacje.

b. Po zainstalowaniu sprzętu komputerowego na stanowisku pracy ASI dokonuje instruktarzu pracownika i zapoznaniu z ewentualnymi nowymi funkcjami urządzeń i programów zainstalowanych na komputerze.

5) Procedura zmiany lokalizacji/osoby użytkującej sprzęt komputerowy

a. W razie zmiany lokalizacji, zmiany osoby użytkującej sprzęt komputerowy ASI aktualizuje wszystkie rejestry i ewidencje dotyczące tego pracownika i sprzętu komputerowego.

b. O zmianie osoby przypisanej do sprzętu komputerowego bądź lokalizacji urządzeń ASI powiadamia poprzez wypełnienie Protokołu Przeniesienia znajdującego się w załączniku nr 3 Instrukcji zarządzania sprzętem komputerowym, a Wydział Finansowy dokonuje aktualizacji w Ewidencji Środków Trwałych.

6) Procedura likwidacji sprzętu komputerowego.

a. Jeśli sprzęt komputerowy:
   - Jest uszkodzony i jego naprawa jest nieopłacalna lub niemożliwa;
   - Jest przestarzały i niespełna wymagań technicznych zainstalowanego oprogramowania w Urzędzie;
   - Został uszkodzony a zakup nowego podzespołu naruszałby umowę licencyjną oprogramowania dołączoną do tego sprzętu;

   To zostaje on poddany Procedurze likwidacji.

b. Sprzęt komputerowy do likwidacji typuje ASI i w porozumieniu Sekretarzem Gminy oraz Burmistrzem przygotowuje Wniosek typowania sprzętu komputerowego do likwidacji, stanowiący załącznik Nr 4 do Instrukcji Zarządzania Sprzętem Komputerowym. Wniosek ten jest przekazany do Wydziału Finansowego, który powołuje Komisję likwidacyjną.

c. Komisja likwidacyjna składająca się z trzech członków dokonuje likwidacji sprzętu komputerowego.

d. Komisja sporządza Protokół likwidacji sprzętu komputerowego w dwóch egzemplarzach dla Wydziału Finansowego i ASI.

e. Wydział Finansowy wykreśla z Ewidencji Środków Trwałych zlikwidowany sprzęt komputerowy. Także ASI zaznacza w swojej Ewidencji sprzętu komputerowego, że dane urządzenie zostało zlikwidowane.

7) Procedura utylizacji sprzętu komputerowego.

a. Po zgromadzeniu odpowiedniej ilości zlikwidowanego sprzętu komputerowego zostaje on poddany Procedurze utylizacji.

b. W wyniku wewnętrznych konsultacji zostaje wyłoniona firma utylizacyjna.

a) aktualny wykaz zasobów danych osobowych przetwarzanych w danej komórce organizacyjnej,
b) wykaz osób upoważnionych do przetwarzania określonego zasobu danych osobowych,
c) wykaz pomieszczeń, w których przetwarzany jest poszczególny zasób danych osobowych w podległej komórce organizacyjnej i ich zabezpieczeń.

2. Pracownik ds. Kadr na bieżąco informuje ABI o:
   a) ustaniu zatrudnienia w Urzędzie określonej osoby, celem kontroli aktywności jego kont w systemie informatycznym,
   b) przeniesieniu pracownika do innego wydziału Urzędu, celem kontroli jego praw do dostępu do danych osobowych.
3. ASI przekazuje ABI:
   a) aktualny wykaz systemów teleinformatycznych – aplikacji, w których przetwarzane są dane osobowe z informacją o programach zastosowanych do przetwarzania tych danych,
   b) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,
   c) sposób przepływu danych pomiędzy poszczególnymi systemami.
4. ABI ustala szczegółowe zakresy potrzebnych informacji oraz formę i tryb ich przekazywania.
5. Każda zmiana informacji w zakresie ujętym w pkt 1-3 wymaga bieżącej aktualizacji przez osoby wskazane w wymienionych punktach.
6. Na podstawie przekazywanych informacji ABI prowadzi aktualny wykaz zasobów danych osobowych przetwarzanych w Urzędzie, który zamieszcza w dokumencie „Wykaz zasobów danych osobowych i systemów ich przetwarzania".

BURMISTRZ
mgr Adam Fedorowicz

Załącznik nr 1 do
Instrukcji zarządzania sprzętem komputerowym

Chojna dnia ……r.

Zapotrzebowanie na sprzęt komputerowy

Imię i nazwisko: ……

Wydział: ……

e-mail: ……

Zgłasza zapotrzebowanie na sprzęt komputerowy.

1. Opis zapotrzebowania.

Rodzaj sprzętu	*
Jednostka Centralna	
Monitor	
Drukarka	
Skaner	
Klawiatura	
Mysz	
Nagrywarka	
UPS	
Dysk Twardy	
Czytnik Kart Pamięci	
**……	

*- właściwe zaznaczyć X

** - wpisz rodzaj sprzętu

2. Przyczyna zapotrzebowania na nowy sprzęt komputerowy:

……

……

……

……

……

Podpis pracownika

Załącznik nr 2 do
Instrukcji zarządzania sprzętem komputerowym

<table>
<tr><td rowspan="2"></td><td colspan="2">Przyjęcie środka trwałego</td><td rowspan="2">OT</td></tr>
<tr><td>Numer</td><td>Data przyjęcia</td></tr>
<tr><td colspan="4">Nazwa:</td></tr>
<tr><td colspan="4">Charakterystyka:</td></tr>
<tr><td rowspan="2">Dostawca – Wykonawca:</td><td colspan="3">Wartość ogółem:</td></tr>
<tr><td rowspan="2">Symbol układu klasyfikacyjnego</td><td colspan="3">Miejsce użytkowania lub przeznaczenia:

Urząd Miejski w Chojnie</td></tr>
<tr><td>Numer inwentarzowy:</td><td colspan="3">Sporządził :

.....
Podpis i pieczątka</td></tr>
</table>

.....

Podpis ASI

Załącznik nr 3 do
Instrukcji zarządzania sprzętem komputerowym

<table>
<tr><td rowspan="2"></td><td>Przemieszczenie środka trwałego</td><td>MT</td></tr>
<tr><td>Data przeniesienia</td></tr>
<tr><td colspan="3">Nazwa przedmiotu przemieszczenia:</td></tr>
<tr><td colspan="3">Charakterystyka przedmiotu przemieszczenia:</td></tr>
<tr><td rowspan="2">Nr inwentarzowy</td><td colspan="2">Wartość przedmiotu przeniesienia:</td></tr>
<tr><td rowspan="2">Symbol układu klasyfikacyjnego</td><td>Miejsce użytkowania przed przemieszczeniem
Pok.</td><td>Miejsce użytkowania po przemieszczeniu
Pok.</td></tr>
<tr><td>Sporządził:</td><td>Osoba odpowiedzialna</td><td>Osoba odpowiedzialna</td></tr>
</table>

……

Podpis ASI

Załącznik nr 4 do
Instrukcji zarządzania sprzętem komputerowym

Urząd Miejski w Chojnie
Ul. Jagiellońska 4
74-500 Chojna

Chojna dnia …….r.

Protokół typowania do likwidacji sprzętu komputerowego

W dniu …….r. skierowano do likwidacji następujący sprzęt komputerowy:

Lp.	Rodzaj sprzętu	NUMER INWENTARZOWY	Powód wytypowania do likwidacji
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			

……

Sporządził

Załącznik nr 6 do
Polityki Bezpieczeństwa Informacji

Instrukcja Zarządzania Oprogramowaniem

§1
Wstęp

1. Urząd Miejski w Chojnie zna wagę legalnego i etycznego użytkowania oprogramowania. Ten dokument jest drogowskazem dla naszych pracowników jak upewnić się, że nasza firma używa oprogramowanie zarówno legalnie jak i w sposób etyczny. Wszystkie zasoby oprogramowania są wykorzystywane w celach handlowych i nie są używane przez pracowników we własnych celach.

§2

Polityka ogólna

1. Urząd Miejski w Chojnie posiada licencjonowane egzemplarze programów komputerowych różnych producentów oprogramowania. Licencjonowane i zarejestrowane egzemplarze programów zostały zainstalowane na komputerach oraz sporządzono odpowiednie kopie zapasowe oprogramowania zgodnie z warunkami umów licencyjnych. Bez pisemnej zgody producenta oprogramowania nie wolno wykonywać żadnych dodatkowych kopii programów ani też ich dokumentacji.
2. Poza oprogramowaniem komercyjnym w Urzędzie Miejskim w Chojnie wykorzystuje się oprogramowanie darmowe, czyli freeware, oraz na licencji GPL.

§3

Oprogramowanie z innych źródeł

1. Urząd Miejski w Chojnie wyposażył stanowiska komputerowe pracowników w legalne oprogramowanie. Używanie oprogramowania pochodzącego z jakiegokolwiek innego źródła, bez konsultacji z ASI może stanowić zagrożenie dla bezpieczeństwa Urzędu Miejskiego w Chojnie oraz grozić może wszczęciem postępowania prawnego – używanie takiego oprogramowania jest ściśle zabronione.
2. Pracownicy są zobowiązani do zapoznania się z odpowiednimi przepisami o ochronie praw autorskich oraz kodeksu karnego przedstawionymi im przez ASI. Przepisy te

mówią o odpowiedzialności pracownika w przypadku korzystania z nielegalnego oprogramowania.

§4

Oprogramowanie stwarzające zagrożenia bezpieczeństwa danych

1. Programy zainstalowane przez pracowników Urzędu Miejskiego w Chojnie w celu pobierania danych (plików mp3, filmów, itp.) stanowią ogromne zagrożenie dla bezpieczeństwa sieci oraz jej wydajności. Wykorzystywanie tego rodzaju oprogramowania jest zabronione.
2. Pracownik w oświadczeniu zobowiązuje się, iż nie będzie korzystał z zainstalowanego oprogramowania do nielegalnych celów oraz, że nie będzie używał szkodliwych i niebezpiecznych programów (typu p2p, torrentów itp.) w miejscu pracy, gdzie wykorzystywałby je do zabronionych celów. Oświadczenie pracownika Urzędu Miejskiego w Chojnie stanowi Część C załącznika nr 3 z Oświadczenia do Instrukcji zarządzania Oprogramowaniem.

§5

Dodatkowe kopie

1. W niektórych przypadkach umowa licencyjna pozwala na sporządzenie dodatkowej kopii określonego programu, przeznaczonej do użytkowania na komputerze przenośnym lub komputerze domowym wykorzystywanym do celów służbowych. Pracownicy nie mogą wykonywać dodatkowych kopii oprogramowania lub dokumentacji.
2. Łamanie, czy obchodzenie zabezpieczeń oprogramowania jest dopuszczalne wtedy i tylko wtedy, gdy chcemy wykonać jedną kopię danego oprogramowania do celów zabezpieczenia się w przypadku zniszczenia oryginalnego nośnika programu.
3. Niedopuszczalne jest wykonanie więcej niż jednej kopii oprogramowania. Chyba, że umowa licencyjna na to pozwala.

§6

Wewnętrzna kontrola

1. Urząd Miejski w Chojnie zastrzega sobie prawo do ochrony swojej reputacji i swoich inwestycji w programy komputerowe poprzez ustanowienie wewnętrznych

mechanizmów kontroli zapobiegających wykonywaniu lub użytkowaniu nielegalnych kopii oprogramowania. Mechanizmy te obejmują częste, regularne kontrole sposobu wykorzystywania oprogramowania, zapowiedziane i niezapowiedziane przeglądy zawartości służbowych komputerów umożliwiające stwierdzenie zgodności zainstalowanego oprogramowania z umowami licencyjnymi, usuwanie wszelkich programów zainstalowanych na służbowych komputerach, dla których nie da się stwierdzić ważności licencji lub przedstawić jej dowodu, a także podjęcie postępowania dyscyplinarnego – łącznie ze zwolnieniem z pracy – w stosunku do pracowników naruszających postanowienia niniejszych zasad użytkowania oprogramowania**.**

2. Mechanizmy kontroli wewnętrznej określa „Procedura audytu/inwentaryzacji oprogramowania".

§7

Procedury zarządzania oprogramowaniem w Urzędzie Miejskim w Chojnie.

1. Procedura zgłaszania zapotrzebowania na oprogramowanie.
    a. Zgłoszenie ASI zapotrzebowania na oprogramowanie odbywa się poprzez wypełnienie formularza Zapotrzebowania na oprogramowanie, stanowiący załącznik Nr 1 do Instrukcji Zarządzania Oprogramowaniem.
    b. ASI konsultuje zgłoszenie z Skarbnikiem Gminy.
    c. Decyzje o zakupie oprogramowania podejmuje Burmistrz.
    d. Jednocześnie tworzony jest Rejestr Zapotrzebowania na oprogramowanie, do którego trafiają zgłoszenia pracowników, jeżeli ich zgłoszenie nie wymaga natychmiastowej realizacji.
2. Procedura zakupu oprogramowania komputerowego.
    a. ASI kontaktuje się z dystrybutorem oprogramowania w celu uzgodnienia szczegółów zakupu oprogramowania i licencji.
    b. Dostawca dostarcza nośnik z oprogramowaniem, licencję oraz fakturę zakupu, które stanowią podstawę legalności oprogramowania.
    c. W przypadku przedłużenia licencji, opieki autorskiej bądź aktualizacji oprogramowania ASI pisemnie kontaktuje się z odpowiednimi dystrybutorami.
    d. Wszelkie zakupy oprogramowania zatwierdza Burmistrz i Skarbnik Gminy.
3. Procedura przyjęcia do Ewidencji Oprogramowania Komputerowego.
    a. Po zakupie oprogramowania komputerowego ASI wpisuje je do Ewidencji Oprogramowania Komputerowego oraz przypisuje mu odpowiedni komputer.

b. ASI wypełnia zgłoszenie oprogramowania do Wydziału Finansowego. Zgłoszenie to stanowi załącznik Nr 2 do Instrukcji Zarządzania Oprogramowaniem.
c. ASI aktualizuje Metrykę Komputera, w której znajdują się parametry komputera wraz zainstalowanym na nim oprogramowaniem. Wzór Metryki znajduje się w części B załącznika Nr 3 do Instrukcji Zarządzania Oprogramowaniem.
d. Wszystkie licencje i płyty instalacyjne oprogramowania przechowywane są w serwerowi nr 212 na I piętrze w Urzędzie Miejskim w Chojnie.

4. Procedura instalacji oprogramowania.
   a. Proces instalacji dokonuje tylko ASI lub pracownik firmy zewnętrznej, ale tylko i wyłącznie w obecności ASI.
   b. ASI zapoznaje pracownika z nowo zainstalowanym oprogramowaniem i poucza o legalnym wykorzystaniu oprogramowania.
5. Procedura aktualizacji oprogramowania.
   a. W przypadku, kiedy pozwala na to licencja programu aktualizacja może być darmowa. Wykonuje ją pracownik lub ASI.
   b. W przypadku programów o określonym czasie licencji i płatnej aktualizacji, ASI wypełnia stosowne wnioski o aktualizacje oprogramowania.
6. Procedura likwidacji oprogramowania.
   a. W przypadku licencji OEM, program jest likwidowany razem ze sprzętem komputerowym.
   b. Programy, które są uważane za nieprzydatne mogą zostać zlikwidowane po trzech latach ich nieużytkowania.
7. Procedura audytu/inwentaryzacji oprogramowania.
   a. Procedura inwentaryzacji oprogramowania odbywa się dwa razy w roku. Przeprowadza ją ASI, a wyniki przedstawia Sekretarzowi Gminy.
   b. Jeżeli zostaną wykryte jakieś nieprawidłowości zastosowane zostaną odpowiednie procedury.
   c. ASI po inwentaryzacji aktualizuje Ewidencję Oprogramowania Komputerowego.
8. Procedura podpisania Oświadczenia pomiędzy Burmistrzem a Pracownikiem.
   a. W związku z wprowadzeniem Polityki Bezpieczeństwa i Instrukcji Zarządzania Oprogramowaniem każdy pracownik jest zobowiązany do podpisania Oświadczenia, które określa odpowiedzialność pracownika za użytkowany komputer i zainstalowane na nim oprogramowanie.
   b. Oświadczenie składa się z trzech części: A, B i C. Część A stanowi wstęp do oświadczenia, w części B znajduje się Metryka Komputera, za który pracownik

jest odpowiedzialny, natomiast część C jest oświadczeniem pracownika o nie wykorzystywaniu zainstalowanego oprogramowania do nielegalnych celów oraz o nie korzystaniu ze szkodliwych i niebezpiecznych programów (typu p2p, torrentów itp.) w miejscu pracy, gdzie wykorzystywałby je do zabronionych celów, użytkowaniu i posługiwaniu się sprzętem komputerowym.

c. Lista programów jest aktualizowana po ewentualnych zakupach oprogramowania.
d. Oświadczenie zostaje sporządzone w dwóch egzemplarzach po jednej dla stron.
e. Wzór Oświadczenia stanowi załącznik Nr 3 do Instrukcji Zarządzania Oprogramowaniem.
f. ASI prowadzi rejestr osób, które podpisały oświadczenie. Wzór rejestru stanowi załącznik nr 4 do Instrukcji zarządzania oprogramowaniem.

BURMISTRZ
mgr Adam Fedorowicz

Załącznik nr 1 do
Instrukcji zarządzania oprogramowaniem

Chojna dnia ……r.

Zapotrzebowanie na oprogramowanie komputerowe

Imię i nazwisko: ……

Wydział: ……

E-mail: ……

Zgłasza zapotrzebowanie na oprogramowanie komputerowe.

1. Opis zapotrzebowania.

Rodzaj lub nazwa oprogramowania komputerowego	*
Edytor tekstu	
Arkusz kalkulacyjny	
Program do tworzenia prezentacji	
Program graficzny	
RADIX	
Edytor Aktów Prawnych XML	
Podpis elektroniczny	
**……	

*- właściwe zaznaczyć X

** - wpisz rodzaj oprogramowania

2. Opis przeznaczenia programu:

……

……

……

……

……

Podpis pracownika

Załącznik nr 2 do
Instrukcji zarządzania oprogramowaniem

<table>
<tr><td rowspan="2"></td><td colspan="2">Przyjęcie środka trwałego</td><td rowspan="2">OT</td></tr>
<tr><td>Numer</td><td>Data przyjęcia</td></tr>
<tr><td colspan="4">Nazwa:</td></tr>
<tr><td colspan="4">Charakterystyka:</td></tr>
<tr><td rowspan="2">Dostawca - Wykonawca:</td><td colspan="3">Wartość ogółem:</td></tr>
<tr><td rowspan="2">Symbol układu klasyfikacyjnego</td><td colspan="3">Miejsce użytkowania lub przeznaczenia:

Urząd Miejski w Chojnie</td></tr>
<tr><td>Numer inwentarzowy:</td><td colspan="3">Sporządził:

.....
Podpis i pieczątka</td></tr>
</table>

.....

Podpis ASI

Załącznik nr 3 do
Instrukcji zarządzania oprogramowaniem

Część A

OŚWIADCZENIE

Niniejsze Oświadczenie (zwane dalej „Oświadczeniem") zostało zawarte w dniu . . . . . w Chojnie pomiędzy Urzędem Miejskim z siedzibą w Chojnie reprezentowaną/ego przez Burmistrza . . . . . (zwaną/ego dalej „Pracodawcą") oraz Panią/Panem . . . . . (zwaną/ym dalej „Pracownikiem").

Wstęp:

(A) Pracownik zatrudniony jest przez Pracodawcę na podstawie umowy o pracę.
(B) Pracodawca wyposażył stanowisko pracy Pracownika w oprogramowanie, na używanie, którego nabył licencję („Oprogramowanie"). Odpowiednie przepisy regulują w sposób szczegółowy zasady korzystania z Oprogramowania.
(C) Pracownik korzysta z komputera/notebooka i oprogramowania w związku z wykonywaniem obowiązków pracowniczych w miejscu pracy.
(D) Oświadczenie składa się z części A – ogólnej, części B - metryki komputera, w której znajduje się wykaz sprzętu i zainstalowanego dozwolonego oprogramowania i części C- oświadczeniu pracownika o nie wykorzystywaniu zainstalowanego oprogramowania do nielegalnych celów oraz o nie korzystaniu ze szkodliwych i niebezpiecznych programów (typu p2p, torrentów itp.) w miejscu pracy, gdzie wykorzystywałby je do zabronionych celów, użytkowaniu i posługiwaniu się sprzętem komputerowym.

1. Pracodawca i Pracownik uzgadniają, że do podstawowych obowiązków Pracownika należy korzystanie z Oprogramowania w związku z wykonywaniem obowiązków pracowniczych, zgodnie z obowiązującymi przepisami prawa oraz wyłącznie w celach wykonywania obowiązków pracowniczych jak również nie korzystanie z jakiegokolwiek Oprogramowania komputerowego, do używania którego Pracodawca nie jest uprawniony, w czasie pracy, w miejscu pracy ani przy użyciu sprzętu Pracodawcy.
2. Pracownik oświadcza, iż jest świadomy odpowiedzialności karnej, o której mowa w artykułach: 278 § 2, 293 w związku z 291 oraz 292 ustawy z dnia 6 czerwca 1997 r. kodeks karny, (tekst jednolity - Dz. U. z 1997, Nr 88, póz. 553, ze zmianami) oraz odpowiedzialności karnej i cywilnej przewidzianej w artykułach 116 i nast. ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (tekst jednolity - Dz. U. z 2000, Nr 80, póz. 904, ze zmianami) za niezgodne z prawem korzystanie, rozpowszechnianie, utrwalanie, uzyskiwanie lub zwielokrotnianie Oprogramowania.
3. Pracodawca i Pracownik uzgadniają, że naruszenie przez Pracownika jego podstawowych obowiązków pracowniczych w zakresie wskazanym powyżej, może stanowić podstawę do podjęcia przez Pracodawcę przysługujących mu środków prawnych, a w szczególności, może stanowić przyczynę uzasadniającą wypowiedzenie przez Pracodawcę umowy o pracę, łączącej Pracodawcę z Pracownikiem, lub rozwiązanie przez Pracodawcę tejże umowy o pracę bez wypowiedzenia, z winy pracownika, zgodnie z przepisami ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy (tekst jedn.: Dz. U. z 1998 r., Nr 21, póz. 94, ze zm.).

Niniejsze Oświadczenie zostało sporządzone w trzech egzemplarzach, po jednym dla każdej ze stron i dla Administratora Systemu Informatycznego. Zmiana, uzupełnienie oraz rozwiązanie niniejszego Oświadczenia za zgodą obu stron wymaga formy pisemnej pod rygorem nieważności.

podpis pracownika

podpis osoby upoważnionej do reprezentowania Pracodawcy

Część B

Nazwa użytkownika:
Nazwa komputera:
DOMENA: ug.local
Adres IP:10.0.0.__

Specyfikacja sprzętowa (hardware) i oprogramowania (software).

System operacyjny:
Procesor:
Nazwa płyty głównej:
Pamięć:
Dysk twardy:
Karta graficzna:
Karta dźwiękowa:

Numer inwentarzowy:

Licencje komercyjne

L.p	Nazwa programu	Producent programu
1.		
2.		
3.		
4.		
5.		

Licencje freeware, GPL

L.p	Nazwa programu	Producent programu
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		

Przyjmuję do użytkowania wyżej wymieniony sprzęt i oprogramowanie.

..... **.....**
Podpis ASI **data i podpis użytkownika**

Część C

Pracownik nie może korzystać z nielegalnie nabytych plików i oprogramowania, plików mp3 oraz szkodliwych, niebezpiecznych programów (np typu p2p, czy też nabytych z nielegalnego źródła plików) w miejscu pracy, gdzie wykorzystywałby ich do zabronionych celów.

Pracownik oświadcza, iż nie będzie instalował żadnego oprogramowania, bez wcześniejszej konsultacji z Administratorem Systemu Informatycznego.

W przypadku, gdy użytkownik pracuje na komputerze przenośnym (notebook, netbook) nie jest dopuszczalne by wynosił go poza teren miejsca pracy, ze względów na bezpieczeństwo informacji znajdujących się na dyskach twardych.

Użytkownik odpowiada za uszkodzenia wynikłe podczas złego/nieprawidłowego eksploatowania sprzętu.

Wszelkie urządzenia magazynujące dane (pendrive, karty pamięci, przenośne dyski twarde) zakupione do celów służbowych, mają być używane do celów służbowych i nie mogą być używane, czy wynoszone poza teren Urzędu Miejskiego w Chojnie.

Potwierdzam, iż zapoznałem(am) się z oświadczeniem i będę się stosować do wyżej wymienionych zaleceń oraz jestem świadomy(ma) odpowiedzialności karnej, o której mowa w artykułach: 278 § 2, 293 w związku z 291 oraz 292 ustawy z dnia 6 czerwca 1997r. kodeks karny, (tekst jednolity - Dz. U. z 1997, Nr 88, póz. 553, ze zmianami) oraz odpowiedzialności karnej i cywilnej przewidzianej w artykułach 116 i nast. ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (tekst jednolity - Dz. U. z 2000, Nr 80, póz. 904, ze zmianami) za niezgodne z prawem korzystanie, rozpowszechnianie, utrwalanie, uzyskiwanie lub zwielokrotnianie Oprogramowania.

_____

Podpis pracownika

Załącznik nr 4 do
Instrukcji zarządzania oprogramowaniem

Rejestr oświadczeń pracowników Urzędu Miejskiego w Chojnie

L.p	Nazwisko i imię	Data	Podpis
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			
21.			
22.			
23.			
24.			
25.			
26.			
27.			
28.			
29.			
30.			
31.			

Załącznik nr 2 do zarządzenia Nr 1136/VI/2014
Burmistrza Chojny z dnia 19.09.2014 r.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Chojnie.

§. 1
Przetwarzanie danych w systemie teleinformatycznym

1. Dane osobowe mogą być przetwarzane w systemach spełniających wymogi u.o.d.o. oraz Rozporządzenia.
2. „Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miejskim w Chojnie" określa zasady zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w zakresie:
   a) określenia sposobu przydziału i zarządzania hasłami użytkowników,
   b) określenia uprawnień użytkowników oraz sposobu ich rejestrowania i wyrejestrowania w systemie informatycznym,
   c) zasad rozpoczęcia i zakończenia pracy w systemie,
   d) ochrony antywirusowej,
   e) przeglądów i konserwacji systemu,
   f) postępowania w zakresie komunikacji w sieci komputerowej,
   g) zarządzania systemem informatycznym,
   h) przechowywania i niszczenia nośników informacji.
3. Zasady zarządzania poszczególnymi systemami informatycznymi regulują szczegółowe instrukcje zarządzania danym systemem.
4. Szczegółowe instrukcje określają:
   a) sposób administracji i obsługę zmian w systemie,
   b) sposób przepływu danych osobowych pomiędzy poszczególnymi systemami,
   c) opis struktury zbiorów danych osobowych wskazujący na zawartość poszczególnych pól informacyjnych i powiązania pomiędzy nimi,
   d) sposób realizacji wymogów zapewniających odnotowywanie informacji zgodnie z zapisem niniejszej polityki.
5. Za stworzenie i aktualizację Instrukcji wymienionej w pkt 2 oraz instrukcji dla poszczególnych systemów w Urzędzie Miejskim w Chojnie odpowiada ASI. Instrukcję aprobuje ABI, a wprowadza w życie zarządzeniem Burmistrz Gminy Chojna.

§. 2
Wymagania dla systemu teleinformatycznego

1. System informatyczny służący do przetwarzania danych osobowych wyposażony jest w mechanizmy uwierzytelniania użytkownika oraz kontroli dostępu do tych danych.
2. Identyfikator użytkownika wraz z jego imieniem i nazwiskiem wpisuje się do ewidencji osób upoważnionych do przetwarzania danych osobowych prowadzonej przez Właścicieli ZDO.
3. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.
4. Identyfikator osoby, która utraciła uprawnienia dostępu do danych osobowych, należy bezzwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane, unieważnić jej hasło oraz podjąć stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych osobowych.
5. Ekrany monitorów stanowisk dostępu do danych osobowych powinny być automatycznie wyłączane po upływie, co najwyżej 5 minut nieaktywności użytkownika, a po wykonaniu „akcji" przez użytkownika (np. poruszenie myszą), komputer powinien domagać się podania loginu i hasła użytkownika.
6. W pomieszczeniach, w których przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, żeby uniemożliwić tym osobom wgląd w te dane.

§. 3
Przetwarzanie danych osobowych w systemie informatycznym poza zbiorem danych

1. Jeżeli zachodzi taka konieczność dopuszcza się przetwarzanie danych osobowych w plikach (MS Word, MS Excell) poza bazą danych, znajdującą się w określonym systemie informatycznym.
2. Zgodę na przetwarzanie danych poza systemem informatycznym wydaje właściciel ZDO wg wzoru upoważnienia określonego w Załączniku Nr 1 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Chojnie.
3. Dane przetwarzane w plikach mogą stanowić kopie części bazy znajdującej się w systemie lub być nową celową ewidencją tworzoną na potrzeby realizacji zadań związanych z przetwarzaniem danych osobowych przez uprawnionych pracowników.
4. Dostęp do plików z danymi powinien być ograniczony jedynie do osoby tworzącej taki plik na swojej stacji roboczej. W tej sytuacji pliki:

- nie mogą być udostępnione przez sieć komputerową innym użytkownikom,
- możliwe są do otwarcia jedynie po załogowaniu się na profil danego użytkownika,
- muszą być chronione hasłem, jeżeli mają być dostępne dla innych Użytkowników.

5. W sytuacji umieszczenia plików z danymi osobowymi na serwerze plików, dostęp do niego powinien być ograniczony do określonej grup uprawnionych użytkowników.
6. Grupę użytkowników określa dany Właściciel ZDO.
7. ASI jest obowiązany określić szczegółowe zasady zabezpieczenia plików z danymi osobowymi znajdującymi się w komputerach pracowników lub na serwerze plików.

§. 4

Przetwarzanie danych osobowych znajdujących się na nośnikach Papierowych

1. Dane osobowe zawarte w dokumentacji papierowej przetwarzane są przez osoby upoważnione zgodnie z zasadami niniejszej polityki.
2. Rejestracje, obieg i udostępnianie – w tym na zewnątrz Urzędu – dokumentów papierowych zawierających dane osobowe reguluje „Instrukcja Kancelaryjna" Urzędu Miejskiego w Chojnie oraz u.o.od.o.
3. Przechowywanie i likwidację dokumentów papierowych wykorzystywanych w Urzędzie reguluje „Instrukcja Archiwalna" Urzędu Miejskiego w Chojnie.

§ 5

Nadawanie/cofanie uprawnień do przetwarzania danych osobowych.

1. W celu nadania uprawnień do przetwarzania danych osobowych i rejestracji tych uprawnień w systemie informatycznym ma zastosowanie „Procedura nadawania/cofania uprawnień do przetwarzania danych osobowych". Osobą odpowiedzialną za rejestrację osoby upoważnionej do przetwarzania danych osobowych w ewidencji osób upoważnionych (art. 39 ust. 1 ustawy o ochronie danych osobowych) jest Sekretarz Gminy, natomiast za rejestrację uprawnień użytkownika w systemach informatycznych osobą odpowiedzialną jest ASI.
    a) Sekretarz Gminy przygotowuje upoważnienie do przetwarzania danych osobowych dla użytkownika systemu. Upoważnienie przygotowane jest na piśmie w dwóch egzemplarzach (wzór upoważnienia stanowi załącznik nr 2 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Chojnie).
    b) Administrator podpisuje upoważnienie do przetwarzania danych osobowych i przekazuje Sekretarzowi Gminy.

c) Po potwierdzeniu odbioru upoważnienia przez użytkownika systemu pracownik ds. Kadr rejestruje użytkownika oraz okres, na który upoważnienie zostało nadane w ewidencji osób uprawnionych. Wzór Ewidencji osób uprawnionych znajduje się w załączniku nr 3 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Chojnie. Egzemplarz upoważnienia Sekretarz Gminy przekazuje ASI w celu rejestracji uprawnień użytkownika w systemach informatycznych.

2. Ustanie stosunku pracy jest równoważne z cofnięciem uprawnień do przetwarzania danych osobowych.
3. Osoby dopuszczone do przetwarzania danych osobowych zobowiązane są do zachowania tajemnicy w zakresie tych danych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje również po ustaniu zatrudnienia.
4. Administrator Bezpieczeństwa Informacji i ASI są jednocześnie użytkownikami uprzywilejowanymi.
5. Sekretarz Gminy wydaje Pozwolenie na dostęp do systemu informatycznego, w którym przetwarzane są dane osobowe, podmiotom zewnętrznym.

§6
Zarządzanie metodami oraz środkami uwierzytelniania

1. W celu zarządzania metodami oraz środkami uwierzytelniania mają zastosowanie „Procedura uwierzytelniania użytkownika w systemie informatycznym” oraz „ Procedura rejestrowania/wyrejestrowania użytkownika z systemu informatycznego”.
    1) Procedura uwierzytelniania użytkownika w systemie informatycznym**.**
        a) Niepowtarzalny identyfikator oraz pierwsze hasło jest przydzielone użytkownikowi przez ASI po nadaniu uprawnień do przetwarzania danych osobowych.
        b) Pierwsze hasło jest przekazane użytkownikowi systemu przez ASI w formie pisemnej.
        c) Bezpośredni dostęp do danych użytkownik uzyskuje po podaniu identyfikatora i właściwego hasła.
    2) Procedura rejestrowania/wyrejestrowania użytkownika z systemu informatycznego.
        a) Użytkownicy systemu informatycznego są niezwłocznie rejestrowani lub wyrejestrowywani przez ASI, gdy uzyskują lub tracą prawo

dostępu do systemu, zgodnie z procedurą nadawania/cofania uprawnień do przetwarzania danych osobowych.

b) Identyfikator po wyrejestrowaniu użytkownika zostaje zablokowany przez ASI.

c) Identyfikator po wyrejestrowaniu użytkownika nie jest przydzielany innej osobie.

§7

Rozpoczęcie, zawieszenie i zakończenie pracy w systemie informatycznym

1. W celu rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym mają zastosowanie następujące procedury:
    1) Procedura rozpoczęcia pracy w systemie informatycznym.
        a) W celu rozpoczęcia pracy w systemie informatycznym użytkownik obowiązany jest do podania hasła dostępu do systemu.
        b) Podczas pierwszego uwierzytelniania w systemie użytkownik ma obowiązek zmiany hasła.
        c) Hasło składa się, z co najmniej z 8 znaków. Jego długość jest uzależniona od poziomu bezpieczeństwa. Hasło zawiera wielkie i małe litery oraz cyfry lub znaki specjalne.
        d) Użytkownik ma obowiązek zmieniać hasło nie rzadziej, niż co 30 dni kalendarzowych.
        e) Zabrania się wpisywania hasła lub jego zmiany w obecności innych osób.
        f) Hasło nie może być zapisywane lub przechowywane w miejscu dostępnym dla osób nieuprawnionych.
        g) W przypadku zagubienia hasła użytkownik musi skontaktować się z ASI w celu uzyskania nowego hasła.
        h) Użytkownikowi wolno używać tylko zainstalowanego oprogramowania, wyłącznie zgodnie z instrukcją obsługi, warunkami licencji i bezpieczeństwa przetwarzania danych.
    2) Procedura zawieszenia/odwieszenia pracy w systemie informatycznym.
        a. W celu zawieszenia/wstrzymania pracy w systemie informatycznym służącym do przetwarzania danych osobowych użytkownik zobowiązany jest do wylogowania się z systemu operacyjnego.
        b. W przypadku komputerów PC po wylogowaniu się z systemu operacyjnego użytkownik blokuje pulpit uniemożliwiając dostęp do danych osobom niepowołanym.

c. W celu ponownego przystąpienia do pracy w systemie użytkownik loguje się na swoje konto w komputerze i rozpoczyna pracę w systemie informatycznym zgodnie z procedurą rozpoczęcia pracy w systemie informatycznym.
d. Zabrania się pozostawiania stanowiska komputerowego z odblokowanym systemem bez kontroli pracującego na nim użytkownika.
e. Na komputerach, na których przetwarzane są dane osobowe wygaszacz ekranu zabezpieczony hasłem jest ustawiony na 10 min.

3) Procedura zakończenia pracy w systemie informatycznym.
a. W celu zakończenia pracy w systemie informatycznym użytkownik wyrejestrowuje się z programu służącego do obsługi danych osobowych.
b. Użytkownik „zamyka system operacyjny" i wyłącza komputer.

§8

Podejrzenie lub stwierdzenie naruszenia ochrony danych osobowych

1. W przypadku podejrzenia lub stwierdzenia naruszenia ochrony danych osobowych ma zastosowanie procedura postępowania w sytuacjach naruszenia ochrony danych osobowych.
1) Procedura postępowania w sytuacja naruszenia ochrony danych osobowych.
a. Na fakt naruszenia zabezpieczeń systemu informatycznego mogą wskazywać:
- stan stacji roboczej (np. brak zasilania, problemy z uruchomieniem, naruszenie lub uszkodzenie obudowy stacji roboczej)
- wszelkiego rodzaju różnice w funkcjonowaniu systemu (np. komunikaty informujące o błędach, brak dostępu do funkcji systemu, nieprawidłowości w wykonywanych operacjach),
- różnice w zawartości zbioru danych osobowych (np. brak lub nadmiar danych)
- jakości komunikacji w sieci telekomunikacyjnej (gwałtowne opóźnienia lub przyśpieszenia wykonywanych czynności)
- inne sytuacje nadzwyczajne.

b. W przypadku podejrzenia naruszenia zabezpieczenia systemu informatycznego użytkownik niezwłocznie powiadamia bezpośredniego przełożonego oraz Administratora Bezpieczeństwa.

c. Administrator Bezpieczeństwa niezwłocznie wszczyna postępowanie wyjaśniające i o jego wynikach informuje Administratora.

§9
Zabezpieczenie danych i programów

1. W celu zabezpieczenia danych i programów służących do przetwarzania danych osobowych ma zastosowanie poniższa procedura:
    1) Procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.
        a. Kopie zapasowe baz danych wykonywane są codziennie w dni robocze, po zakończeniu czasu pracy na macierzy dyskowej i nośnikach RDX.
        b. Kopie bezpieczeństwa utworzone na nośnikach RDX przechowywane są poza pomieszczeniami, w których zostały utworzone.
    2) Procedura zabezpieczenia systemu przetwarzania danych osobowych przed złośliwym oprogramowaniem.
        a. Skanowanie komputerów osobowych programami antywirusowymi działa w czasie rzeczywistym, czyli podczas pracy komputera oprogramowanie antywirusowe skanuje używane programy i pliki w poszukiwaniu potencjalnie niebezpiecznego złośliwego oprogramowania.
        b. W celu wykrycia potencjalnych dziur bezpieczeństwa w systemach komputerowych wykonywane jest sieciowe skanowanie zabezpieczeń systemu informatycznego.
        c. Procedura zaleca, w miarę możliwości, aktualizowanie systemów operacyjnych. Po aktualizacji systemu, odłączeniu komputera od sieci zewnętrznej, należy przeskanować komputer oprogramowaniem antyszpiegowskim.

§. 10
Zabezpieczenie systemu informatycznego

1. W Urzędzie Miejskim w Chojnie każdy komputer w sieci jest zabezpieczony oprogramowaniem antywirusowym.
2. Sieć posiada dostęp do Internetu. Głównym urządzeniem zabezpieczającym sieć zewnętrzną Urzędu Miejskiego w Chojnie jest Router Cisco RV082. Urządzenie to umożliwia blokowanie wielu obszarów dostępu do Internetu, w tym portów

i protokołów sieciowych. Ponadto „za routerem" uruchomiony jest serwer Proxy do filtrowania niepożądanych treści i pełniący funkcje dodatkowej ochrony przed złośliwym oprogramowaniem.

3. Serwery znajdujące się w sieci posiadają własne programowe zapory systemowe. To samo tyczy się komputerów działających w sieci.
4. Do zdanego zarządzania serwerami używane są szyfrowane kanały transmisji VPN oraz SSH.

§. 11

Zasady archiwizowania danych osobowych przetwarzanych papierowo

1. Archiwizowanie papierowych zbiorów danych osobowych odbywa się w oparciu o obowiązująca w Urzędzie Miejskim w Chojnie „Instrukcję Kancelaryjną" oraz Jednolity rzeczowy wykaz akt.
2. Kopie papierowe z danymi osobowymi muszą być oznaczone i przechowywane w zamykanych na klucz szafach.

§. 12

Zasady napraw i likwidacji sprzętu komputerowego służącego do przetwarzania danych osobowych

1. Urządzenia przekazywane do naprawy należy pozbawić możliwości zapisu danych oraz możliwości ich odczytania przez nieupoważnione osoby, które dokonują naprawy.
2. Jeśli naprawa sprzętu lub oprogramowania musi zostać wykonana w miejscu przetwarzania danych osobowych albo na komputerze gdzie są przetwarzane dane osobowe, to naprawy mogą być dokonywane w obecności osoby upoważnionej przez Administratora danych.
3. Dyski i inne nośniki danych zawierające dane do likwidacji, należy pozbawić możliwości zapisu i odczytu tych danych, a w przypadku, gdy nie jest to możliwe należy uszkodzić nośnik w sposób uniemożliwiający odzyskanie danych z nośnik

BURMISTRZ
mgr Adam Fedorowicz

Załącznik Nr 1 do
Instrukcji zarządzania systemem informatycznym służącym do
przetwarzania danych osobowych w Urzędzie Miejskim w Chojnie

Data nadania upoważnienia: .....

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH POZA BAZĄ DANYCH SYSTEMU INFORMATYCZNEGO URZĘDU MIEJSKIEGO W CHOJNIE

1. Upoważniam Panią/Pana .....
zatrudnioną/-ego na stanowisku .....
w Urzędzie Miejskim w Chojnie do przetwarzania poza bazą danych systemu informatycznego następujących danych osobowych:
– .....
– .....
– .....
(zakres upoważnienia: wskazanie kategorii danych, które może przetwarzać określona w upoważnieniu osoba, lub rodzaj czynności lub operacji, jakich może dokonywać na danych osobowych)

2. Identyfikator: .....

3. Okres trwania upoważnienia: .....
(okres obowiązywania upoważnienia)

Wystawił:

.....
(podpis Właściciela Zbioru Danych Osobowych)

4. Osoba upoważniona do przetwarzania danych, objętych zakresem, o którym mowa wyżej, jest zobowiązana do zachowania ich w tajemnicy, nie kopiowania ich i nie udostępniania, również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

Data i podpis osoby upoważnionej: .....

Załącznik Nr 2 do
Instrukcji zarządzania systemem informatycznym służącym do
przetwarzania danych osobowych w Urzędzie Miejskim w Chojnie

Chojna, dnia <<Data>>

UPOWAŻNIENIE

do przetwarzania danych osobowych

Na podstawie art. 31 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2013 r., poz. 594 z późn. zm.) w związku z art. 268a ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz.U. z 2013 r., poz. 267 z późn. zm.) oraz art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2014, poz. 1182)

Upoważniam Panią /Pana:

<<Imię i Nazwisko>>

zatrudnioną / zatrudnionego **w Urzędzie Miejskim w Chojnie** do przetwarzania danych osobowych, w celach związanych z wykonywaniem obowiązków na stanowisku:

<<Stanowisko>>

oraz do obsługi systemu informatycznego i urządzeń wchodzących w jego skład.

Niniejsze upoważnienie obejmuje przetwarzanie danych osobowych w formie tradycyjnej (kartoteki, ewidencje, rejestry, spisy itp.[*]) i elektronicznej ze szczególnym uwzględnieniem zadań zawartych w rozporządzeniu 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. Nr 100, poz. 1024*).

Upoważniam Panią/ Pana do przetwarzania danych osobowych zawartych w następujących zbiorach:

Z dniem podpisania niniejszego upoważnienia **traci moc upoważnienie** udzielone Pani/Panu dnia: **<<data starego upoważnienia>>**

…….

Podpis

Administratora Danych Osobowych

Załącznik Nr 3 do
Instrukcji zarządzania systemem informatycznym służącym do
przetwarzania danych osobowych w Urzędzie Miejskim w Chojnie

Ewidencja osób upoważnionych do przetwarzania danych osobowych

L.p.	Imię i nazwisko	Stanowisko komórka/jednostka organizacyjna	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia (czynności) *	Identyfikator w danym systemie informatycznym

* Wskazówki do wypełniania kolumn: w kolumnie nr 6 należy podać zakres upoważnienia związany z czynnościami przy przetwarzaniu danych osobowych: zbieranie danych, wprowadzanie danych pracowniczych, odczyt, zapis, modyfikacja, drukowanie, usuwanie/niszczenie; w kolumnie nr 7 należy podać identyfikator (id, login) dla każdego systemu, do którego dana osoba ma dostęp.