Zarządzenie Nr 30/16

Burmistrza Miasta Wysokie Mazowieckie

z dnia 12 kwietnia 2016r.

w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji i Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Miasta Wysokie Mazowieckie.

Na podstawie art. 31 oraz art. 33 ust. 3 w związku z art. 11a ust. 1 pkt 2 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2016r. poz. 446 t.j.) w związku z art. 36 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2015 poz. 2135 t.j. z późn. zm) oraz § 3 ust. 3, § 4 i § 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024),zarządza się, co następuje:

§ 1

1. Wprowadza się „Politykę Bezpieczeństwa Informacji w Urzędzie Miasta Wysokie Mazowieckie” w zakresie przetwarzania danych osobowych w Urzędzie Miasta Wysokie Mazowieckie, stanowiącą załącznik nr 1 do niniejszego zarządzenia
2. Wprowadza się „Instrukcję Zarządzania Systemem Informatycznym" służącym do przetwarzania danych osobowych w Urzędzie Miasta Wysokie Mazowieckie, stanowiącą załącznik nr 2 do zarządzenia.

§ 2

Zobowiązuje się pracowników przetwarzających dane osobowe oraz przebywających w pomieszczeniach biurowych tworzących obszar, w którym przetwarzane są dane osobowe do przestrzegania przepisów zawartych w dokumentach, o których mowa w § 1.

§ 3

Zobowiązuje się Kierowników Referatów korzystających z zasobów informatycznych Urzędu Miasta Wysokie Mazowieckie, w których przetwarzane są dane osobowe do sprawowania nadzoru nad ich ochroną oraz do współpracy z Administratorem Bezpieczeństwa Informacji w tym zakresie.

§ 4

Wykonanie zarządzenia powierza się Sekretarzowi Miasta Wysokie Mazowieckie, Administratorowi Bezpieczeństwa Informacji oraz Administratorowi Systemu Informatycznego.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Miasta

Jarosław Siekierko

Załącznik nr 1
do Zarządzenia nr 30/16
Burmistrza Miasta Wysokie Mazowieckie
z dnia 12.04.2016r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI W URZĘDZIE MIASTA WYSOKIE MAZOWIECKIE

Część I – Wstęp

§ 1

O skuteczności działania i rozwoju każdej organizacji świadczy stopień osiągania zamierzonego celu. W procesie tym kluczowe jest stosowanie współczesnych technik i technologii, narzędzi i systemów informatycznych oraz przetwarzania i zarządzania informacją. Informacja jest jednym z najważniejszych zasobów Urzędu, dlatego powinna być chroniona na każdym szczeblu organizacji. Najwyższe kierownictwo Urzędu zobowiązuje się do podejmowania niezbędnych działań mających na celu zapewnienie ochrony informacji na pożądanym poziomie, a tym samym spełnienie wymaganego poziomu bezpieczeństwa systemów informatycznych.

Zgodnie z art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2015 r., poz. 2135 t.j. z późn.zm.), zwanej dalej „ustawą" oraz z § 3 ust. 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. Nr 100, poz. 1024 z późn. zm.), zwanego dalej „rozporządzeniem", ustanawia się „Politykę Bezpieczeństwa".

§ 2

Definicje:

1) **Bezpieczeństwo informacji** - zachowanie poufności, integralności i dostępności informacji.
2) **Ryzyko** - prawdopodobieństwo wystąpienia zagrożenia, które wykorzystując podatność(ci) aktywu, może doprowadzić do jego uszkodzenia lub zniszczenia.
3) **Szacowanie ryzyka** - całościowy proces analizy i oceny ryzyka.
4) **Aktyw/zasób** - wszystko to, co ma wartość dla organizacji w zakresie informacji (zarówno informacje, jak i środki techniczne oraz organizacyjne do ich przetwarzania).
5) **Poufność** - zapewnienie dostępu do informacji tylko osobom upoważnionym.
6) **Integralność** - funkcja bezpieczeństwa polegająca na tym, że dane nie zostały zmienione, dodane lub usunięte w nieautoryzowany sposób
7) **Dostępność** - zapewnienie, że osoby upoważnione będą miały dostęp do informacji tylko wtedy, gdy jest to uzasadnione.
8) **Postępowanie z ryzykiem** - proces wyboru i wdrażania środków modyfikujących ryzyko.
9) **Zarządzanie ryzykiem** - proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych, przy zachowaniu akceptowalnego poziomu kosztów.
10) **Zdarzenie związane z bezpieczeństwem informacji** - określony stan systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji, błąd

zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem.

11) Incydent związany z bezpieczeństwem informacji - pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.

12) Dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

§ 3

Ilekroć w niniejszym dokumencie jest mowa o jednostce organizacyjnej, należy przez to rozumieć Urząd Miasta Wysokie Mazowieckie.

§ 4

Priorytetowym celem kierownictwa jest spełnienie wymagań prawnych oraz zapewnienie ciągłości działania organizacji, poufności danych wrażliwych i dostępności wymaganych informacji. Przez bezpieczeństwo informacji w Urzędzie rozumie się zapewnienie dostępności, zabezpieczenie przed nieuprawnionym dostępem, naruszeniem integralności bądź zniszczeniem aktywów związanych z przechowywaniem i przetwarzaniem informacji.

Zakres ochrony i podjęte środki są adekwatne do własności aktywów związanych z systemami przetwarzania informacji.

Główne cele stawiane przed systemem zarządzania bezpieczeństwem informacji:

1) zapewnienie spełnienia wymagań prawnych,
2) ochrona systemów przetwarzania informacji przed nieuprawnionym dostępem bądź zniszczeniem,
3) podnoszenie świadomości pracowników,
4) zmniejszenie ryzyka utraty informacji,
5) zaangażowanie wszystkich pracowników w ochronę informacji.

Część II – Zasady przetwarzania i ochrony danych osobowych

§ 5

Każda osoba, mająca dostęp do danych osobowych przetwarzanych w jednostce organizacyjnej jest zobowiązana do zapoznania się z niniejszym dokumentem.

§ 6

Wymagany przez rozporządzenie wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe (zwany dalej „obszarem przetwarzania") stanowi załącznik nr 1 do niniejszego dokumentu.

§ 7

Wymagany przez rozporządzenie wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami, stanowi załącznik nr 2 do niniejszego dokumentu.

§ 8

Osoby, które przetwarzają w jednostce organizacyjnej dane osobowe, muszą posiadać pisemne upoważnienie do przetwarzania danych nadane przez Administratora Danych Osobowych (załącznik nr 3 do niniejszego dokumentu) oraz podpisać oświadczenie o zachowaniu poufności tych danych (załącznik nr 4 do niniejszego dokumentu).

§ 9

Każda osoba posiadająca upoważnienie do przetwarzania danych osobowych posiada swój identyfikator oraz hasło, pozwalające na zalogowanie się do systemu informatycznego, w którym przetwarzane są dane osobowe. Techniczne wymagania, jakie musi spełniać hasło, określone zostały w części II § 7 Instrukcji Zarządzania Systemem Informatycznym.

§ 10

W przypadku konieczności dostępu do obszaru przetwarzania osób, nieposiadających upoważnienia, o jakim mowa w § 4 (załącznik nr 3 do niniejszego dokumentu), które muszą dokonać doraźnych prac o charakterze serwisowym lub innym, podpisują oni oświadczenie o zachowaniu poufności (załącznik nr 4 do niniejszego dokumentu).

§ 11

Zlecenie podmiotowi zewnętrznemu przetwarzania danych osobowych może nastąpić wyłącznie w ramach umowy powierzenia przetwarzania danych osobowych, zgodnie z art. 31 ustawy.

§ 12

Udostępnienie danych osobowych podmiotowi zewnętrznemu może nastąpić wyłącznie po pozytywnym zweryfikowaniu ustawowych przesłanek dopuszczalności takiego udostępnienia, przez co rozumie się w szczególności pisemny wniosek podmiotu uprawnionego

§ 13

Dokumenty zawierające dane osobowe przechowywane w formie papierowej, upoważnione osoby przechowują w obszarze przetwarzania danych w szafach zamykanych na klucz.

W przypadku konieczności zniszczenia papierowych dokumentów zawierających dane osobowe, ich zniszczenie dokonuje się poprzez pocięcie w niszczarce.

§ 14

Zasady przetwarzania danych osobowych w systemie informatycznym określone są w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta Wysokie Mazowieckie".

§ 15

Nadzór nad przetwarzaniem danych osobowych w jednostce organizacyjnej sprawuje Administrator Bezpieczeństwa Informacji (zwany dalej „ABI") wyznaczony przez Administratora Danych Osobowych. W przypadku niewyznaczenia ABI, funkcje mu przypisane pełni Administrator Danych Osobowych osobiście. Upoważnienie wyznaczające ABI stanowi załącznik nr 5 do niniejszego dokumentu. ABI jest również zobowiązany do podpisania oświadczenia, stanowiącego załącznik nr 4 do niniejszego dokumentu.

§ 16

ABI prowadzi wykaz zbiorów danych osobowych przetwarzanych w jednostce organizacyjnej (załącznik nr 2 do niniejszego dokumentu) oraz, kiedy jest to wymagane przez przepisy, zgłasza zbiory do rejestracji do GIODO. W ramach nadzoru nad przetwarzaniem danych, ABI sprawdza w szczególności cele, zakres przetwarzania, czas przetwarzania oraz sposoby zabezpieczenia danych osobowych. Upoważnienie do przetwarzania danych osobowych (załącznik nr 3 do niniejszego dokumentu) nadaje Administrator Danych Osobowych lub ABI. ABI jest zobowiązany do przeprowadzania analizy ryzyk związanych z zagrożeniami związanymi z przetwarzaniem danych osobowych w jednostce organizacyjnej.

§ 17

ABI prowadzi również następujące wykazy:

a) ewidencję osób, którym nadano upoważnienia do przetwarzania danych osobowych (załącznik nr 6 do niniejszego dokumentu)

b) wykaz pomieszczeń, w których przetwarzane są dane osobowe, stanowiących obszar przetwarzania (załącznik nr 1 do niniejszego dokumentu)

c) wykaz podmiotów, którym powierzono dane osobowe do przetwarzania (załącznik nr 7 do niniejszego dokumentu)

§ 18

Osoby upoważnione do przetwarzania danych mają obowiązek:

a) przetwarzać je zgodnie z obowiązującymi przepisami, w szczególności z ustawą i rozporządzeniem

b) nie udostępniać ich oraz uniemożliwiać dostęp do nich osobom nieupoważnionym

c) zabezpieczać je przed zniszczeniem

§ 19

W przypadku otrzymania wniosku o udostępnienie danych osobowych od osoby, której one dotyczą, wyznaczona przez Administratora Danych Osobowych osoba zobowiązana jest do udzielenia informacji w ciągu 30 dni.

Część III – Postanowienia końcowe

§ 20

Nieprzestrzeganie zasad ochrony danych osobowych grozi odpowiedzialnością karną wynikającą z art. 49-54a ustawy o ochronie danych osobowych.

§ 21

W sprawach nieuregulowanych niniejszym dokumentem, znajdują zastosowanie przepisy ustawy o ochronie danych osobowych oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

§ 22

Niniejszy dokument wchodzi w życie z dniem podpisania.

……..……

podpis Administratora Danych Osobowych

WYKAZ POMIESZCZEŃ, W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE

(wszystkie miejsca, pomieszczenia, pokoje, w których dokonuje się operacji na danych osobowych)

L.p.	Lokalizacja – adres	Precyzyjne określenie pomieszczenia	Dział/osoba użytkująca pomieszczenie	Zabezpieczenie pomieszczenia
1.	Urząd Miasta Wysokie Mazowieckie ul. Ludowa 15 18-200 Wysokie Mazowieckie parter	Pokój nr 5, 6,	Urząd Stanu Cywilnego	Alarm budynku, drzwi zamykane na klucz, szafa pancerna, szafki zamykane na klucz
		Pokój nr 7	Kierownik Urzędu Stanu Cywilnego	Alarm budynku, drzwi zamykane na klucz, szafki zamykane na klucz
2.	Urząd Miasta Wysokie Mazowieckie ul. Ludowa 15 18-200 Wysokie Mazowieckie I piętro	Pokój nr 10	Referat Organizacyjny	Alarm budynku, drzwi zamykane na klucz, szafa pancerna, szafki zamykane na klucz
		Pokój nr 11, 12, 13, 19		Alarm budynku, drzwi zamykane na klucz, szafki zamykane na klucz
3.	Urząd Miasta Wysokie Mazowieckie ul. Ludowa 15 18-200 Wysokie Mazowieckie I piętro	pokój Burmistrza Miasta pokój Zastępcy Burmistrza/Sekretarza	Burmistrz Miasta, Zastępca Burmistrza/Sekretarz	Alarm budynku, drzwi zamykane na klucz, szafki zamykane na klucz
4.	Urząd Miasta Wysokie Mazowieckie ul. Ludowa 15 18-200 Wysokie Mazowieckie I piętro	Pokój nr 15,16,17,	Referat Finansowy	Alarm budynku, drzwi zamykane na klucz, szafa pancerna, szafki zamykane na klucz
		Pokój nr 18	Skarbnik	Alarm budynku, drzwi zamykane na klucz, szafki zamykane na klucz
5.	Urząd Miasta Wysokie Mazowieckie ul. Ludowa 15 18-200 Wysokie Mazowieckie II piętro	Pokój nr 24, 25	Referat Mienia Komunalnego, Inwestycji i Remontów oraz Rolnictwa	Alarm budynku, drzwi zamykane na klucz, szafki zamykane na klucz
		Pokój nr 23	Kierownik Referatu Mienia Komunalnego, Inwestycji i Remontów oraz Rolnictwa	
6.	Urząd Miasta Wysokie Mazowieckie ul. Ludowa 15 18-200 Wysokie Mazowieckie II piętro	Pokój nr 27, 28	Straż Miejska	Alarm budynku, drzwi zamykane na klucz, szafki zamykane na klucz
		Pokój nr 26	Komendant Straży Miejskiej	
7.	Urząd Miasta Wysokie Mazowieckie ul. Ludowa 15 18-200 Wysokie Mazowieckie parter	Archiwum	Archiwum	Alarm budynku, drzwi zamykane na klucz

WYKAZ ZBIORÓW DANYCH OSOBOWYCH

L.p.	Nazwa zbioru danych osobowych	Cel przetwarzania	Nazwa systemu, ewidencji lub aplikacji, w której przetwarzane są dane osobowe	Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	Sposób przepływu danych pomiędzy poszczególnymi systemami
1.	Oświadczenia majątkowe Radnych Rady Miasta Wysokie Mazowieckie	zgodnie z przepisami prawa wskazanie stanu majątkowego radnych rady miasta	MS Office, ewidencja papierowa	Nazwiska i imiona, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, miejsce pracy, zawód,	
2.	Oświadczenia majątkowe osób sprawujących funkcje kierownicze oraz pracowników wydających decyzje administracyjne w imieniu Burmistrza	zgodnie z przepisami prawa wskazanie stanu majątkowego radnych rady miasta	MS Office, ewidencja papierowa	Nazwiska i imiona, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, miejsce pracy, zawód,	
3.	wykaz uczniów, którym udzielono pomocy na zakup podręczników w formie wyprawki szkolnej	ustalenie uczniów do udzielania pomocy finansowej na zakup podręczników w ramach Rządowego Programu Wyprawka szkolna	MS Office, ewidencja papierowa	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL	
4.	wnioski dotyczące zwrotu kosztów wyszkolenia uczniów	Gromadzenie niezbędnej dokumentacji osób ubiegających się o zwrot kosztów wyszkolenia uczniów	MS Office, ewidencja papierowa	Nazwiska i imiona, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, miejsce pracy, zawód, wykształcenie	
5.	Wykaz uczestników wyjazdów profilaktycznych organizowanych w formie kolonii z programem profilaktycznym	Ustalenie osób korzystających z wyjazdu z programem profilaktycznym	MS Office, ewidencja papierowa	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu,	
6.	PŁATNIK	posiadanie niezbędnych danych pracowników Urzędu Miasta Wysokie Mazowieckie	PŁATNIK	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, NIP, miejsce pracy, zawód, wykształcenie, seria i numer dowodu osobistego	
7.	System kadrowo-płacowy	Rejestr pracowników zawierający dane osobowe, określenie i naliczenie	PŁACE	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, NIP, miejsce pracy, zawód,	

		wynagrodzeń oraz pochodnych		wykształcenie, seria i numer dowodu osobistego	
8.	Wnioski dotyczące stypendium za osiągnięcia w nauce	Określenie uczniów ubiegających się o stypendium	MS Office, ewidencja papierowa	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, wykształcenie, seria i numer dowodu osobistego	
9.	Ulgi podatkowe	Określenie podatnika ubiegającego się o ulgę podatkową	MS Office, ewidencja papierowa	Nazwiska i imiona, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, miejsce pracy, uzyskiwane dochody	
10.	Rejestr wydanych zaświadczeń	Potwierdzenie stanu faktycznego lub prawnego osoby ubiegającej się o zaświadczenie	MS Office, ewidencja papierowa	Nazwiska i imiona, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, miejsce pracy,	
11.	Ewidencja mandatów karnych przetwarzanych przy pomocy programu SUMPRO	nałożenie mandatu za wykroczenie	SUMPRO	Nazwiska i imiona, imiona rodziców, adres zamieszkania lub pobytu, numer ewidencyjny PESEL,	
12.	Decyzje na zwrot podatku akcyzowego za zakupione paliwo	Określenie producenta rolnego ubiegającego się o zwrot podatku akcyzowego zawartego w cenie oleju napędowego wykorzystanego w produkcji rolnej	FISKUS, ewidencja papierowa	Nazwiska i imiona, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, Numer Identyfikacji Podatkowej, seria i numer dowodu osobistego	
13.	Rejestr posiadanych psów rasy uznawanej za agresywną	zgodnie z przepisami prawa dokonanie rejestracji osób posiadających psy rasy uznanej za agresywną	MS Office, ewidencja papierowa	Nazwiska i imiona, adres zamieszkania lub pobytu	
14.	Rejestr podań o przydział mieszkań	dokonanie rejestracji osób ubiegających się o przydział mieszkania z zasobów miasta	MS Office, ewidencja papierowa	Nazwiska i imiona, adres zamieszkania lub pobytu, numer ewidencyjny PEEL	
15.	Zbiór decyzji podziałowych nieruchomości	dane przetwarzane w zbiorze mają na celu wydanie decyzji podziałowych nieruchomości	MS Office, ewidencja papierowa	Nazwiska i imiona, adres zamieszkania lub pobytu, dane z aktu notarialnego nieruchomości do podziału	
16.	Zbiór decyzji rozgraniczających nieruchomości	przetwarzanie danych w zbiorze m a na celu postępowanie w sprawie	MS Office, ewidencja papierowa	Nazwiska i imiona, adres zamieszkania lub pobytu, dane z aktu notarialnego nieruchomości do rozgraniczenia	

		rozgraniczenia nieruchomości			
17.	Zbiór decyzji o środowiskowych uwarunkowaniach zgody na realizację przedsięwzięcia	przetwarzanie danych w zbiorze m a na celu postępowanie w sprawie środowiskowych uwarunkowań zgody na realizacje przedsięwzięcia	MS Office, ewidencja papierowa	Nazwiska i imiona, adres zamieszkania lub pobytu	
18.	Wnioski dotyczące zmian w studium uwarunkowań i zagospodarowania przestrzennego	Przetwarzanie danych osobowych związane jest z wnioskami składanymi przez osoby zainteresowane zmianami w studium uwarunkowań i zagospodarowania przestrzennego	MS Office, ewidencja papierowa	Nazwiska i imiona, adres zamieszkania lub pobytu	
19.	Wnioski dotyczące zmian w miejskim planie zagospodarowania przestrzennego	Przetwarzanie danych w zbiorze ma na celu ustalenie zmian w miejskim planie zagospodarowania przestrzennego	MS Office, ewidencja papierowa	Nazwiska i imiona, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, miejsce pracy, zawód,	
20.	Zbiór decyzji na usunięcie drzew	Przetwarzanie danych w zbiorze ma na celu zgromadzenie dokumentacji w postępowaniu administracyjnym w sprawie decyzji na usunięcie drzew	MS Office, ewidencja papierowa	Nazwiska i imiona, adres zamieszkania lub pobytu	
21.	Zbiór decyzji aktualizacyjnych opłaty rocznej	Przetwarzanie danych w zbiorze ma na celu wydanie decyzji aktualizacyjnej opłaty rocznej	MS Office, ewidencja papierowa	Nazwiska i imiona, adres zamieszkana lub pobytu, dane zawarte w księdze wieczystej	
22.	Zbiór decyzji przekształcających użytkowanie wieczyste w prawo własności	Przetwarzanie danych w zbiorze ma na celu przekształcenie użytkowania wieczystego w prawo własności	MS Office, ewidencja papierowa	Nazwiska i imiona, adres zamieszkania lub pobytu, dane zawarte w księdze wieczystej	
23.	Wnioski o wydanie wypisów i wyrysów z planu przestrzennego zagospodarowania miasta	Przetwarzanie danych w zbiorze niezbędne jest w celu wydania wypisów i wyrysów z planu przestrzennego zagospodarowania miasta	MS Office, ewidencja papierowa	Nazwiska i imiona, adres zamieszkania lub pobytu	
24.	Decyzje zezwalające na zajęcie pasa	Przetwarzanie danych w zbiorze ma na	MS Office, ewidencja papierowa	Nazwiska i imiona, adres zamieszkania lub pobytu	

	drogowego	celu wydanie decyzji w sprawie zezwolenia na zajęcie pasa drogowego			
25.	Rejestr wniosków o ukaranie skierowanych do sądu	Przetwarzanie danych w zbiorze ma na celu prowadzenie zgodnie z przepisami prawa rejestru wniosków o ukaraniu skierowanych do sądu	MS Office, ewidencja papierowa	Nazwiska i imiona, imiona rodziców, adres zamieszkania lub pobytu, numer ewidencyjny PESEL,	
26.	Rejestr kart PRD 5/15 przesłanych do Policji	Przetwarzanie danych w zbiorze ma na celu prowadzenie zgodnie z przepisami prawa rejestru kart PRD 5/1 do Policji	MS Office, ewidencja papierowa	Nazwiska i imiona, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, seria i numer dowodu osobistego	
27.	Wykaz nałożonych mandatów karnych	Przetwarzanie danych w zbiorze ma na celu prowadzenie wykazu nałożonych mandatów karnych	MS Office, ewidencja papierowa	Nazwiska i imiona,	
28.	Rejestr wniosków o ukaranie	Przetwarzanie danych w zbiorze ma na celu prowadzenie rejestru wniosków o ukaranie	MS Office, ewidencja papierowa	Nazwiska i imiona, adres zamieszkania lub pobytu, numer ewidencyjny PESEL,	
29.	Rejestr osób podejrzanych o popełnienie wykroczenia	Przetwarzanie danych w zbiorze ma na celu prowadzenie rejestru osób podejrzanych o popełnienie wykroczenia	MS Office, ewidencja papierowa	Nazwiska i imiona, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, dane wynikające z tytułu prawnego do nieruchomości	
30.	Wykaz wniosków o dofinansowanie zmiany pokrycia dachowego zawierającego azbest	Przetwarzanie danych w zbiorze ma na celu prowadzenie wykazu wniosków o dofinansowanie zmiany pokrycia dachowego zawierającego azbest	MS Office, ewidencja papierowa	Nazwiska i imiona, adres zamieszkania lub pobytu, numer ewidencyjny PESEL,	
31.	Numeracja porządkowa nieruchomości	Przetwarzanie danych w zbiorze ma na celu nadanie numeracji porządkowej nieruchomości	MS Office, ewidencja papierowa	Nazwiska i imiona, adres zamieszkania lub pobytu, numer telefonu	
32.	Deklaracje o wysokości opłaty za gospodarowanie odpadami komunalnymi	Przetwarzanie danych w zbiorze ma na celu utrzymanie czystości w gminie	FISKUS, MS Office, ewidencja papierowa	Nazwiska i imiona, adres zamieszkania, numer ewidencyjny PESEL	

33.	Ewidencja zbiorników bezodpływowych i przydomowych oczyszczalni	Przetwarzanie danych w zbiorze ma na celu prowadzenie ewidencji zbiorników bezodpływowych i przydomowych oczyszczalni ścieków	MS Office, ewidencja papierowa	Nazwiska i imiona, adres zamieszkania lub zameldowania	
34.	Rejestr zamieszkania cudzoziemców	Rejestracja określonych w ustawie podstawowych danych identyfikujących tożsamość oraz status administracyjnoprawny osób fizycznych	SELWIN ŹRÓDŁO, ewidencja papierowa	- nazwisko i imię (imiona); - numer PESEL, o ile został nadany; - datę i miejsce urodzenia; - kraj urodzenia; - adres dotychczasowego miejsca pobytu stałego; - adres dotychczasowego miejsca pobytu czasowego; - deklarowany czas pobytu; - przewidywany okres pobytu poza granicami Rzeczypospolitej Polskiej; - data wyjazdu; - kraj wyjazdu; - kraj poprzedniego miejsca zamieszkania; - adres nowego miejsca pobytu stałego; - podpis właściciela lokalu lub innego podmiotu dysponującego tytułem prawnym do lokalu; - nazwisko i imię pełnomocnika, o ile został ustanowiony; - adres elektroniczny służący do doręczeń; - data powrotu z wyjazdu poza granice RP	
35.	Rejestr mieszkańców	Rejestracja określonych w ustawie podstawowych danych identyfikujących tożsamość oraz status administracyjnoprawny osób fizycznych	SELWIN, ŹRÓDŁO, ewidencja papierowa	- nazwisko i imię (imiona); - nazwisko rodowe; - imiona i nazwiska rodowe rodziców; - data urodzenia; - miejsce urodzenia; - kraj urodzenia; - stan cywilny; -oznaczenie aktu urodzenia i urzędu stanu cywilnego, w którym został on sporządzony; - płeć; - numer PESEL; - obywatelstwo albo status bezpaństwowca;	

				- imię i nazwisko rodowe oraz numer PESEL małżonka, jeżeli został mu nadany; -data zawarcia związku małżeńskiego, oznaczenie aktu małżeństwa i urzędu stanu cywilnego, w którym został on sporządzony, data rozwiązania związku małżeńskiego, sygnatura akt i oznaczenie sądu, który rozwiązał małżeństwo, sygnatura akt i oznaczenie sądu, który ustalił nieistnienie małżeństwa, sygnatura akt i oznaczenie sądu, który unieważnił małżeństwo, data zgonu małżonka albo data znalezienia jego zwłok, oznaczenie jego aktu zgonu i urzędu stanu cywilnego, w którym ten akt został sporządzony; - adres i data zameldowania na pobyt stały; - kraj miejsca zamieszkania; - kraj poprzedniego miejsca zamieszkania; - data wymeldowania z miejsca pobytu stałego; - adres i data zameldowania na pobyt czasowy oraz data upływu deklarowanego terminu pobytu; - data wymeldowania z miejsca pobytu czasowego; - data wyjazdu poza granice Rzeczypospolitej Polskiej trwającego dłużej niż 6 miesięcy i wskazanie kraju wyjazdu; - data powrotu z wyjazdu poza granice Rzeczypospolitej Polskiej trwającego dłużej niż 6 miesięcy; - seria, numer i data ważności ostatniego wydanego dowodu osobistego obywatela polskiego oraz oznaczenie organu wydającego dokument; - seria, numer i data ważności ostatniego wydanego paszportu obywatela polskiego; - seria, numer i data ważności dokumentu podróży cudzoziemca, a w przypadku cudzoziemców, o których mowa w art. 7 ust. 1 pkt 3 lit. a i b, ważnego dokumentu podróży lub innego ważnego dokumentu potwierdzającego tożsamość i obywatelstwo; - data upływu deklarowanego przez cudzoziemca terminu pobytu; - data zgonu albo data znalezienia zwłok, numer aktu zgonu i oznaczenie urzędu stanu cywilnego, w którym ten akt został sporządzony.'	

36.	Rejestr wyborców	Rejestr wyborców służy do sporządzenie spisu wyborców uprawnionych do udziału w wyborach i referendach, ponadto potwierdza prawo wybierania i wybieralności.	SELWIN, ewidencja papierowa	nazwiska i imiona, imię ojca, data urodzenia, numer ewidencyjny PESEL, adres zamieszkania wyborcy, obywatelstwo państwa członkowskiego Unii Europejskiej, numer paszportu lub innego dokumentu stwierdzającego tożsamość	
37.	Akta Stanu Cywilnego	Dokonywanie czynności z zakresu rejestracji stanu cywilnego	ŹRÓDŁO, ewidencja papierowa	imiona, nazwiska: panieńskie, z poprzedniego małżeństwa, rodowe; miejsce i godzina urodzenia; kraj urodzenia; data i numer aktów: urodzenia, małżeństwa, zgonu; nazwisko i imię: ojca, matki, współmałżonka; stan cywilny; płeć; data i miejsce zawarcia związku małżeńskiego; miejsce wystawienia i numer aktu urodzenia żony, męża; data, godzina, miejsce zgonu, odnalezienia zwłok; nazwisko, imię, adres osoby zgłaszającej zgon; nazwisko rodowe: ojca, matki, współmałżonka; adnotacja o rozwodzie; nazwisko po zawarciu małżeństwa: mężczyzny, kobiety; miejsce wydania dowodu osobistego; data unieważnienia katu małżeństwa, urodzenia, zgonu; imię nadane z urzędu; data i numer orzeczenia sądu ustalającego ojcostwo, zaprzeczającego ojcostwo, przysposabiającego dziecko; zmiana nazwiska dziecka;	
38.	Dowody osobiste	wydanie dowodu osobistego, prowadzenie rejestru wydanych i unieważnionych dowodów osobistych	ŹRÓDŁO, ewidencja papierowa	nazwisko, imię (imiona), nazwisko rodowe, imiona rodziców, data i miejsce urodzenia, płeć, wizerunek twarzy, numer PESEL, obywatelstwo, seria i numer dowodu osobistego, data wydania , data ważności, oznaczenie organu wydającego dowód osobisty	
39.	Rejestr na potrzeby kwalifikacji wojskowej	Dopełnienie obowiązków określonych w przepisach prawa	MS Office, ewidencja papierowa	nazwisko, imię (imiona), nazwisko rodowe, data i miejsce urodzenia, płeć, numer PESEL, seria i numer dowodu osobistego, adres zamieszkania lub pobytu	
40.	Stypendia i zasiłki szkolne	Dopełnienie obowiązków określonych w przepisach prawa	MS Office, ewidencja papierowa	nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, miejsce nauki, miejsce pracy, zawód, wykształcenie, seria i numer dowodu osobistego, numer telefonu	
41.	Licencje na wykonywanie transportu	Dopełnienie obowiązków określonych	MS Office,	nazwiska i imiona, imiona rodziców, data urodzenia, miejsce	

	drogowego taksówką	w przepisach prawa	ewidencja papierowa	urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, zawód, wykształcenie,	
42.	Rejestr skargi i wniosków	Dopełnienie obowiązków określonych w przepisach prawa	MS Office, ewidencja papierowa	nazwiska i imiona, adres zamieszkania lub pobytu	
43.	Dzienniki korespondencji	Dopełnienie obowiązków określonych w przepisach prawa	SMART DOC	nazwiska i imiona, adres zamieszkania lub pobytu	
44.	Rejestr przesyłek specjalnych	Dopełnienie obowiązków określonych w przepisach prawa	MS Office, ewidencja papierowa	nazwiska i imiona, adres zamieszkania lub pobytu	
45.	Adresy radnych Rady Miasta	Dopełnienie obowiązków określonych w przepisach prawa	MS Office, ewidencja papierowa	nazwiska i imiona, adres zamieszkania lub pobytu, numer telefonu	
46.	Rejestr osób, którym nadano medal - "Zasłużony dla miasta Wysokie Mazowieckie"	Dopełnienie obowiązków określonych w przepisach prawa	MS Office, ewidencja papierowa	nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, miejsce pracy, wykształcenie, zawód	
47.	Podatki i opłaty lokalne - przetwarzany przy pomocy programu FISKUS	Dopełnienie obowiązków określonych w przepisach prawa	MS Office, ewidencja papierowa, FISKUS	nazwiska i imiona, imiona rodziców, numer ewidencyjny PESEL, adres zamieszkania lub pobytu,	
48.	System Informacji Oświatowej	Dopełnienie obowiązków określonych w przepisach prawa	SIO	data urodzenia, numer ewidencyjny PESEL, zawód, wykształcenie	

Data nadania upoważnienia: .....

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Upoważniam Panią/Pana …….…….
   o numerze PESEL…….…….……..
   zatrudnioną/-ego na stanowisku…….…….…….
   w …….....
   (nazwa referatu)
   Urzędu Miasta Wysokie Mazowieckie

   do dostępu do następujących zbiorów danych osobowych w celu ich przetwarzania:
   (należy określić zbiory zgodnie z załącznikiem numer 2 do Polityki Bezpieczeństwa)

- .....
- .....
- .....
- .....
- .....

2. Okres trwania upoważnienia: .....

Wystawił: .....

(podpis Administratora Danych Osobowych lub ABI zgodnie z § 12 Polityki Bezpieczeństwa)

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

Data i podpis osoby upoważnionej: .....

OŚWIADCZENIE

Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam, lub będę miał/-a dostęp w związku z wykonywaniem jakichkolwiek czynności na rzecz Urzędu Miasta Wysokie Mazowieckie.

Zobowiązuję się przestrzegać wszelkich procedur obowiązujących w wyżej wymienionej jednostce organizacyjnej dotyczących ochrony danych osobowych – w szczególności określonych w Polityce Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym.

Oświadczam, że zapoznałem/-am się z przepisami dotyczącymi ochrony danych osobowych, w tym z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2015 r., poz. 2135 z późn.zm.), w tym z zasadami odpowiedzialności karnej określonymi w rozdziale 8 wyżej wymienionej ustawy.

.....
(data i podpis osoby oświadczającej)

.....
(miejscowość, data)

UPOWAŻNIENIE DLA ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI (ABI)

Na podstawie art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. (t.j. Dz.U. z 2015 r., poz. 2135 z późn.zm.), o ochronie danych osobowych, z dniem..... wyznaczam Administratora Bezpieczeństwa Informacji i powierzam tę funkcję Panu/Pani .....
posługującemu/-ej się numerem PESEL: .....

Do obowiązków Administratora Bezpieczeństwa Informacji będzie należało wdrożenie i nadzór nad prawidłową realizacją Polityki Bezpieczeństwa obowiązującej w jednostce organizacyjnej, w szczególności:

1. Zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną
2. Zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym lub zabraniem przez osobę nieuprawnioną
3. Zabezpieczenie danych przed ich przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem
4. Prowadzenie dokumentacji opisującej sposób przetwarzania danych oraz zastosowane środki techniczne służące ich zabezpieczeniu
5. Nadawanie upoważnienia do przetwarzania danych osobowych

.....
podpis w imieniu Administratora Danych Osobowych

Ja, niżej podpisany/-a, zobowiązuję się do pełnienia obowiązków Administratora Bezpieczeństwa Informacji w oparciu o przepisy wewnętrzne obowiązujące w jednostce organizacyjnej, ustawę o ochronie danych osobowych oraz rozporządzenie wykonawcze wydane na podstawie art. 39a do wyżej wymienionej ustawy.

.....
podpis Administratora Bezpieczeństwa Informacji (ABI)

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Imię i nazwisko	Stanowisko/referat	Zakres *(określenie, do jakich zbiorów dana osoba ma dostęp, zgodnie z załącznikiem numer 2 do Polityki Bezpieczeństwa)*	Data nadania upoważnienia	Data ustania upoważnienia	Identyfikator/Login w danym systemie informatycznym
1.						
2.						
3.						
4.						
5.						
6.						
7.						

WYKAZ PODMIOTÓW, KTÓRYM POWIERZONO PRZETWARZANIE DANYCH OSOBOWYCH

L.p.	Nazwa podmiotu, któremu powierzono dane	Data powierzenia	Cel powierzenia oraz numer umowy powierzenia	Zakres powierzonych danych *(jakie dane zostały powierzone)*	Określenie zbioru/zasobu
1.					
2.					
3.					
4.					
5.					
6.					
7.					

Załącznik nr 8 do Polityki Bezpieczeństwa

WNIOSEK

O NADANIE/ODEBRANIE/MODYFIKACJĘ UPRAWNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH

Nowy użytkownik	☐	Modyfikacja uprawnień	☐	Odebranie uprawnień	☐

Imię i nazwisko użytkownika	Referat
Nazwa systemu informatycznego	
Opis zakresu uprawnień użytkownika w systemie informatycznym	
Data wystawienia	Podpis bezpośredniego przełożonego użytkownika systemu
Data akceptacji	Akceptacja Administratora Bezpieczeństwa Informacji
Data realizacji	Podpis Administratora Systemu Informatycznego

Załącznik nr 2
do Zarządzenia nr 30/16
Burmistrza Miasta Wysokie Mazowieckie
z dnia 12.04.2016r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE MIASTA WYSOKIE MAZOWIECKIE

I – Część ogólna

§ 1

Zgodnie z art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2015 r., poz. 2135 z późn.zm.), oraz z § 3 ust. 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. Nr 100, poz. 1024 z późn. zm.), ustanawia się „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

§ 2

Ilekroć w niniejszym dokumencie jest mowa o:

a) ustawie – należy przez to rozumieć ustawę, o której mowa w § 1 niniejszej części
b) rozporządzeniu – należy przez to rozumieć rozporządzenie, o którym mowa w § 1 niniejszej części
c) jednostce organizacyjnej – należy przez to rozumieć Urząd Miasta Wysokie Mazowieckie
d) ADO – należy przez to rozumieć Administratora Danych Osobowych w rozumieniu ustawy
e) ABI – należy przez to rozumieć Administratora Bezpieczeństwa Informacji w rozumieniu ustawy
f) ASI – należy przez to rozumieć Administratora Systemu Informatycznego w rozumieniu § 3 niniejszej części
g) Instrukcji – należy przez to rozumieć niniejszy dokument
h) Polityce Bezpieczeństwa – należy przez to rozumieć przyjęty do stosowania w jednostce organizacyjnej dokument zatytułowany: „Polityka Bezpieczeństwa w Urzędzie Miasta Wysokie Mazowieckie".
i) użytkowniku – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym w drodze upoważnienia, o jakim mowa w części II §

4 Polityki Bezpieczeństwa. Postanowienia dotyczące użytkowników należy stosować odpowiednio do ADO oraz ABI.

j) systemie informatycznym – należy przez to rozumieć system informatyczny, w którym przetwarzane są dane osobowe w jednostce organizacyjnej

k) kopii pełnej – należy przez to rozumieć kopię zapasową całości danych osobowych przetwarzanych w systemie informatycznym

l) osobie wyznaczonej przez ASI w sytuacji wyjątkowej – należy przez to rozumieć osobę, która podpisała oświadczenie stanowiące załącznik nr 4 do Polityki Bezpieczeństwa, otrzymała upoważnienie stanowiące załącznik nr 3 do Polityki Bezpieczeństwa, oraz została ustnie upoważniona przez ASI do dokonania określonych działań wchodzących w zakres jego obowiązków, o których mowa w części II § 9 lit. b, § 10 oraz § 17 lit. b niniejszego dokumentu.

§ 3

ASI wyznaczany jest przez ADO drogą pisemnego upoważnienia. W przypadku nie wyznaczenia ASI, jego funkcję pełni ABI lub osoba pełniąca funkcję ABI. Wzór upoważnienia ASI stanowi załącznik nr 1 do niniejszego dokumentu. ASI jest również zobowiązany do podpisania oświadczenia, stanowiącego załącznik nr 4 do Polityki Bezpieczeństwa.

§ 4

ASI jest odpowiedzialny za przestrzeganie zasad bezpieczeństwa przetwarzania danych osobowych w zakresie systemu informatycznego służącego do tego celu. Do obowiązków ASI należy także kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej i systemu informatycznego (patrz część II § 11 lit. b niniejszego dokumentu). Obowiązkiem ASI jest również zabezpieczenie sprzętu komputerowego przed nieuprawnionym dostępem oraz przeprowadzanie analizy ryzyka uwzględniającej realne zagrożenia dla systemu informatycznego.

§ 5

Zgodnie z rozporządzeniem, uwzględniając fakt, że użytkowany w jednostce organizacyjnej system informatyczny służący do przetwarzania danych osobowych jest połączony z siecią Internet, wprowadza się wysoki poziom bezpieczeństwa.

II – Część szczegółowa

§ 6

Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym określa się w sposób następujący:

a) Użytkownik zamierzający przetwarzać dane osobowe, po podpisaniu oświadczenia stanowiącego załącznik nr 4 do Polityki Bezpieczeństwa uzyskuje upoważnienie stanowiące załącznik nr 3 do Polityki Bezpieczeństwa. Kierownik właściwego referatu składa wniosek stanowiący załącznik nr 8 do Polityki Bezpieczeństwa do ASI o nadanie identyfikatora i hasła w celu umożliwienia wykonywania przetwarzania danych osobowych w systemie informatycznym, ASI zobowiązany jest niezwłocznie przydzielić użytkownikowi identyfikator i hasło. Podanie użytkownikowi hasła nie może nastąpić w sposób umożliwiający zapoznanie się z nim osobom trzecim.

b) w przypadku wygaśnięcia przesłanek uprawniających użytkownika do przetwarzania danych osobowych, w szczególności cofnięcia upoważnienia, stanowiącego załącznik nr 3 do Polityki Bezpieczeństwa, ASI zobowiązany jest, na wniosek Kierownika właściwego referatu (stanowiący załącznik nr 8 do Polityki Bezpieczeństwa), do odebrania uprawnień użytkownikowi.

§ 7

Stosuje się następujące metody oraz środki uwierzytelniania, a także procedury związane z ich zarządzaniem i użytkowaniem:

a) hasło składa się, z co najmniej 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne

b) osobą odpowiedzialną za przydział identyfikatora i pierwszego hasła jest ASI

c) użytkownik, po pierwszym zalogowaniu się do systemu jest zobowiązany do zmiany hasła, jest również zobowiązany do zmiany hasła, nie rzadziej niż co 30 dni

d) użytkownik jest zobowiązany do zabezpieczenia swojego hasła przed nieuprawnionym dostępem osób trzecich.

§ 8

Stosuje się następujące procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu:

a) w celu zalogowania do systemu informatycznego, użytkownik podaje swój identyfikator oraz hasło

b) system jest skonfigurowany w taki sposób, aby po okresie 10 minut bezczynności uruchamiany był wygaszacz ekranu. Do ponownego wznowienia pracy konieczne jest ponowne zalogowanie się przy użyciu identyfikatora i hasła

c) po zakończeniu pracy użytkownik jest zobowiązany do wylogowania się, a następnie do wyłączenia komputera.

§ 9

Stosuje się następujące procedury tworzenia oraz przechowywania kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania:

a) na koniec dnia ASI wykonuje kopię pełną

b) wykonane kopie zapasowe przechowuje się na pamięci przenośnej (*pendrive*) lub na nośnikach CD\DVD, nośniki zawierające kopie zapasowe są przechowywane w szafie metalowej zamykanej na klucz. Należy przechowywać kopie z poprzednich pięciu dni roboczych.

§ 10

Elektroniczne nośniki informacji zawierające dane osobowe przechowywane są przez okres, w którym istnieją przesłanki do ich przetwarzania, po ustaniu przesłanek do przetwarzania, dane muszą zostać usunięte w sposób uniemożliwiający ich odtworzenie. Dane przechowywane są w pokoju nr 10.

Sprzęt komputerowy, na którego dyskach twardych zawarte są dane osobowe, przechowywany jest w obszarze przetwarzania danych osobowych, w pomieszczeniach zabezpieczonych zgodnie z załącznikiem nr 1 do Polityki Bezpieczeństwa.

§ 11

System informatyczny zabezpiecza się przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do tego systemu poprzez stosowanie specjalistycznego oprogramowania, o jakim mowa w lit. a niniejszego paragrafu:

a) oprogramowaniem antywirusowym stosowanym w jednostce organizacyjnej jest: ESET Endpoint Antywirus.

b) użytkownikom nie wolno otwierać na komputerach, na których odbywa się przetwarzanie danych osobowych, plików pochodzących z niewiadomego źródła bez zgody ASI

c) za wdrożenie i korzystanie z oprogramowania antywirusowego, określonego w lit. a oraz oprogramowania firewall, określonego w lit. b niniejszego paragrafu, odpowiada ASI.

§ 12

System informatyczny służący do przetwarzania danych osobowych jest zabezpieczony przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez stosowanie:

a) zasilacza awaryjnego UPS

b) listew przepięciowych, połączonych pomiędzy siecią zasilającą a komputerami.

§ 13

Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych, w tym dodatkowo zabezpiecza hasłem pliki lub foldery zawierające dane osobowe.

§ 14

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

a) likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie

b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie

c) naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem ASI.

§ 15

Dla każdej osoby, której dane są przetwarzane, system informatyczny służący do przetwarzania danych osobowych (z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie) zapewnia odnotowanie:

a) daty pierwszego wprowadzenia danych do systemu (automatycznie)

b) identyfikatora użytkownika wprowadzającego dane osobowe do systemu (automatycznie)

c) źródła danych (jedynie w przypadku zbierania danych nie od osoby, której dotyczą)

d) informacji o odbiorcach w rozumieniu art. 7 pkt 6 ustawy o ochronie danych osobowych

e) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy o ochronie danych osobowych.

§ 16

Dla każdej osoby, której dane osobowe są przetwarzane system informatyczny, zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 15 lit. a-e.

§ 17

Stosuje się następującą procedurę w przypadku stwierdzenia naruszenia zasad bezpieczeństwa systemu informatycznego:

a) w przypadku stwierdzenia przez użytkownika naruszenia zabezpieczeń przez osoby nieuprawnione jest on zobowiązany niezwłocznie poinformować o tym fakcie ASI

b) ASI jest zobowiązany niezwłocznie podjąć czynności zmierzające do ustalenia przyczyn naruszeń zasad bezpieczeństwa i zastosować środki uniemożliwiające ich naruszanie w przyszłości.

§ 18

Usuwanie danych osobowych utrwalonych na nośnikach elektronicznych następuje poprzez powierzenie tych nośników w celu usunięcia zapisanych na nich danych wyspecjalizowanej w tej dziedzinie firmie informatycznej, lub poprzez nadpisanie usuwanych informacji przez ASI w taki sposób, by nie istniała możliwość ich ponownego odczytania. W celu usunięcia danych zapisanych na elektronicznych nośnikach ASI może dokonać ich fizycznego uszkodzenia w taki sposób, by nie istniała możliwość odtworzenia zapisanych na nich danych.

III – Postanowienia końcowe

§ 21

W sprawach nieuregulowanych niniejszą Instrukcją, znajdują zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2015 r., poz. 2135 t.j. z późn. zm.) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024 z późn. zm.).

§ 22

Niniejszy dokument wchodzi w życie z dniem podpisania.

……..…..……

podpis Administratora Danych Osobowych

.....
miejscowość, data

UPOWAŻNIENIE DLA ADMINISTRATORA SYSTEMU INFORMATYCZNEGO (ASI)

Na podstawie części I §3 Instrukcji Zarządzania Systemem Informatycznym, z dniem ..... wyznaczam Administratora Systemu Informatycznego (ASI), powierzając tę funkcję Panu/Pani ..... posługującemu/-ej się numerem PESEL: .....

.....
podpis Administratora Danych Osobowych

Ja, niżej podpisany/-a, zobowiązuję się do pełnienia obowiązków Administratora Systemu Informatycznego w oparciu o przepisy wewnętrzne obowiązujące w jednostce organizacyjnej, ze szczególnym uwzględnieniem obowiązków przewidzianych w części I § 4 Instrukcji Zarządzania Systemem Informatycznym.

.....
podpis Administratora Systemu Informatycznego (ASI)