WÓJT GMINY
CZŁUCHÓW

Zarządzenie Nr 42/15
Wójta Gminy Człuchów
z dnia 10 czerwca 2015r.

w sprawie polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym w Urzędzie Gminy Człuchów.

Na podstawie art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. z 2014 r. Dz.U. poz.1182) oraz § 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024 ze zm.)
– zarządza się, co następuje:

§ 1

Wprowadza się:
1. „Politykę bezpieczeństwa w Urzędzie Gminy Człuchów" określoną w załączniku Nr 1 do niniejszego zarządzenia.
2. „Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Człuchów", określoną w załączniku Nr 2 do niniejszego zarządzenia.

§ 2
§ 6

Traci moc zarządzenie Nr 38/11 Wójta Gminy Człuchów z dnia 24 czerwca 2011 r. w sprawie polityki bezpieczeństwa danych osobowych oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Człuchów.

§ 7

Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT
Adam Marciniak

Załącznik Nr 1
do zarządzenia Nr 42/15
Wójta Gminy Człuchów
z dnia 10 czerwca 2015 r.

POLITYKA BEZPIECZEŃSTWA
w Urzędzie Gminy Człuchów

Część I – Wstęp

§ 1

Zgodnie z art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz.U. z 2014 r. poz. 1182), 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. z 2004 r. Nr 100, poz. 1024 z późn. zm.), zwanego dalej „rozporządzeniem", ustanawia się „Politykę Bezpieczeństwa".

§ 2

Ilekroć w niniejszym dokumencie jest mowa o jednostce organizacyjnej, należy przez to rozumieć Urząd Gminy Człuchów.

Część II – Zasady przetwarzania i ochrony danych osobowych

§ 3

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

§ 4

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.

§ 5

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.

§ 6

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).

§ 7

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 § 2 Instrukcji Zarządzania Systemem Informatycznym.

§ 8

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).

§ 9

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

§ 10

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.

§ 11

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.

§ 12

Zasady przetwarzania danych osobowych w systemie informatycznym określone są w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Człuchów".

§ 13

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 tj. Wójt Gminy. Upoważnienie wyznaczające ABI stanowi załącznik nr 5 do niniejszego dokumentu. ABI jest również zobowiązany do podpisania oświadczenia, stanowiącego załącznik nr 4 do niniejszego dokumentu.

§ 14

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.

§ 15

ABI prowadzi również następujące wykazy:

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

2. wykaz pomieszczeń, w których przetwarzane są dane osobowe, stanowiących obszar przetwarzania (załącznik nr 1 do niniejszego dokumentu);
3. wykaz podmiotów i osób, którym udostępniono dane (załączniki nr 7 i nr 9 do niniejszego dokumentu);
4. wykaz podmiotów, którym powierzono dane osobowe do przetwarzania (załącznik nr 8 do niniejszego dokumentu).

§ 16

Osoby upoważnione do przetwarzania danych mają obowiązek:

1. przetwarzać je zgodnie z obowiązującymi przepisami, w szczególności z ustawą i rozporządzeniem;
2. nie udostępniać ich oraz uniemożliwiać dostęp do nich osobom nieupoważnionym;
3. zabezpieczać je przed zniszczeniem.

§ 17

W przypadku otrzymania wniosku o udostępnienie danych osobowych od osoby, której one dotyczą, wyznaczona przez Administratora Danych Osobowych osoba przygotowuje odpowiedź w ciągu 30 dni.

§ 18

W przypadku zbierania danych osobowych od osoby, której one dotyczą, Administrator Danych Osobowych (lub osoba przez niego wyznaczona) jest obowiązany poinformować tę osobę o:

a) adresie swojej siedziby i pełnej nazwie, a w przypadku, gdy Administratorem Danych Osobowych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku,

b) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,

c) prawie dostępu do treści swoich danych oraz ich poprawiania,

d) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

Część III – Postanowienia końcowe

§ 19

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

§ 20

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.

.....

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.				
2.				
3.				
4.				
5.				
6.				
7.				

WÓJT
Adam Marciniak

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.					
2.					
3.					
4.					

WÓJT
Adam Marciniak

Data nadania upoważnienia: .....

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Upoważniam Panią/Pana .....
   o numerze PESEL .....
   zatrudnioną/-ego na stanowisku .....
   w .....

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

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

2. Identyfikator/Login: .....

3. Okres trwania upoważnienia: .....

Wystawił: .....

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

4. 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: .....

WÓJT
Adam Marciniak

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 ..... .

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 (tekst jedn. Dz. U. z 2014 r. poz. 1182), w tym z zasadami odpowiedzialności karnej określonymi w rozdziale 8 wyżej wymienionej ustawy.

.....

(data i podpis osoby oświadczającej)

WÓJT
Adam Marciniak

.....

(miejscowość, data)

UPOWAŻNIENIE DLA ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI (ABI)

Na podstawie art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. (tekst jedn. Dz. U. z 2014 r. poz. 1182) 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. Wyznaczanie Administratora Systemu Informatycznego (ASI)
6. 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)

WÓJT
Adam Marciniak

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Imię i nazwisko	Stanowisko/komórka organizacyjna	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.						

WÓJT
Adam Marciniak

WYKAZ UDOSTĘPNIEŃ DANYCH OSOBOWYCH INNYM PODMIOTOM

L.p.	Imię i Nazwisko/Nazwa zbioru *(możliwie najpełniejszy opis osoby, której dane zostały udostępnione lub całego zbioru)*	Data udostępnienia	Nazwa podmiotu, któremu udostępniono dane *(np. upoważniony organ, instytucja lub inny, który wykazał uprawnienie do udostępnienia mu danych)*	Cel udostępnienia *(podstawa prawna/numer umowy)*	Zakres udostępnionych danych *(jakie dane zostały udostępnione)*	Rodzaj zbioru/zasobu i jego lokalizacja *(np. papierowy wydruk, dane w formie elektronicznej)*
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						

WÓJT
Adam Marciniak

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.					

WÓJT
Adam Marciniak

WYKAZ UDOSTĘPNIEŃ DANYCH OSOBOWYCH OSOBOM KTÓRYCH DOTYCZĄ

L.p.	Imię i nazwisko osoby, której dane są udostępniane	Data udostępnienia	Rodzaj zbioru/zasobu i jego lokalizacja *(np. papierowy wydruk danych zawartych w określonym zbiorze)*
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			

WÓJT
Adam Marciniak

Załącznik Nr 2
do zarządzenia Nr 42/15
Wójta Gminy Człuchów
z dnia 10 czerwca 2015 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH w Urzędzie Gminy Człuchów

I – Część ogólna

§ 1

Zgodnie z art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz.U. z 2014 r. poz. 1182) 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. z 2004 r. 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 Gminy Człuchów,

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 Gminy Człuchów",

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 § 4 lit. c, § 5 oraz § 8 lit. c niniejszego dokumentu.

§ 3

ASI wyznaczany jest przez ABI lub 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 § 6 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 uzyskaniu upoważnienia stanowiącego załącznik nr 3 do Polityki Bezpieczeństwa, oraz podpisaniu oświadczenia stanowiącego załącznik nr 4 do Polityki Bezpieczeństwa, składa ustnie wniosek 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 do dopełnienia czynności uniemożliwiających ponowne wykorzystanie identyfikatora użytkownika, którego uprawnienia wygasły.

§ 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, co każde 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 30 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) raz na miesiąc ASI wykonuje kopię przyrostową,

b) raz na rok ASI wykonuje kopię pełną,

c) wykonane kopie zapasowe przechowuje się na pamięci przenośnej (*pendrive*) lub na nośnikach CD\DVD, nośniki zawierające kopie zapasowe są przechowywane w szafie zamykanej na klucz, do której dostęp posiada wyłącznie ASI lub w sytuacji wyjątkowej, osoba przez niego wyznaczona. Kopie zapasowe przechowywane są w pomieszczeniu Nr 10 Urzędu.

§ 10

Elektroniczne nośniki informacji zawierające dane osobowe przechowywane są w szafach zamykanych na klucz, do których dostęp ma jedynie ASI oraz, w sytuacjach wyjątkowych, osoba przez niego wyznaczona, dane są przechowywane 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 pomieszczeniu Nr 10 Urzędu.

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: NOD 32 ANTIVIRUS 8.

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

Odnotowanie informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia (z wyłączeniem osób, których dane dotyczą, osób posiadających upoważnienie do przetwarzania danych, organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem), odbywa się poprzez zapisanie tej informacji w utworzonym na dysku twardym komputera pliku dotyczącym danej osoby, zgodnie z systemem zapisywania informacji opisanym, w § 12 niniejszej części.

§ 13

Stosuje się następujące procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych:

a) ASI raz na 3 miesiące wykonuje generalny przegląd systemu informatycznego, polegający na ustaleniu poprawności działania tych jego elementów, które są niezbędne do zapewnienia realizacji funkcji wynikających z niniejszej Instrukcji

b) w przypadku stwierdzenia przez ASI nieprawidłowości w działaniu elementów systemu opisanych w lit. a niniejszego paragrafu podejmuje on niezwłocznie czynności zmierzające do przywrócenia ich prawidłowego działania

c) jeżeli do przywrócenia prawidłowego działania systemu niezbędna jest pomoc podmiotu zewnętrznego, wszelkie czynności na sprzęcie komputerowym dokonywane w obszarze przetwarzania danych osobowych, powinny odbywać się w obecności ASI lub w sytuacji wyjątkowej – osoby przez niego wyznaczonej

§ 14

System informatyczny służący do przetwarzania danych osobowych jest zabezpieczony przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez stosowanie (alternatywnie a lub b, lub oba na raz):

a) UPS EUER ECO 1200,

b) EATON UPS 650,

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

§ 15

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.

§ 16

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

§ 17

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

§ 18

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 § 12 lit. a-e.

§ 19

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

§ 20

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 (tekst jedn. Dz.U. z 2014 r. poz. 1182) 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. z 2004 r. Nr 100, poz. 1024 z późn. zm.).

.....

podpis Administratora Danych Osobowych

WÓJT
Adam Marciniak

.....

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 Bezpieczeństwa Informacji

lub 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)

WÓJT
Adam Marciniak