BURMISTRZ
MIASTA I GMINY
OSTRORÓG
ul. Wroniecka 14, 64-560 Ostroróg

Zarządzenie nr 52 /2011

Burmistrza Miasta i Gminy Ostroróg

z dnia 29 grudnia 2011 roku

w sprawie wprowadzenia do użytku służbowego „Polityki bezpieczeństwa informacji" oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" w Urzędzie Miasta i Gminy Ostroróg.

Na podstawie art. 31 oraz art. 33 ust. 3 w związku z art. 11a ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2002 r. Nr 142, poz. 1591 z późn. zm.) i art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz § 1 pkt 1 w związku z § 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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. z 2004 r. Nr 100, poz. 1024.)

zarządza się co następuje:

§ 1.

Wprowadza się do użytku służbowego „Politykę bezpieczeństwa informacji" w brzmieniu stanowiącym załącznik nr 1 do zarządzenia.

§ 2.

Wprowadza się do użytku służbowego „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy Ostroróg" w brzmieniu stanowiącym załącznik nr 2 do zarządzenia.

§ 3.

Wykonanie zarządzenia powierza się administratorowi bezpieczeństwa informacji - Sekretarzowi Miasta i Gminy Ostroróg .

§ 4.

Zarządzenie wchodzi w życie z dniem podjęcia.

BURMISTRZ

inż. Roman Napierała

Załącznik Nr 1do Zarządzenia Nr 52/2011
Burmistrza Miasta i Gminy Ostroróg
Z dnia 29 grudnia 2011r.

POLITYKA BEZPIECZEŃSTWA

INFORMACJI

OSTRORÓG

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE MIASTA I GMINY OSTRORÓG.

W celu zabezpieczenia danych gromadzonych i przetwarzanych w Urzędzie Miasta i Gminy Ostroróg oraz jego systemie informatycznym, a w szczególności w celu ochrony danych osobowych, wprowadza się określone w niniejszym dokumencie zasady bezpieczeństwa.

Mając świadomość, że żadne zabezpieczenie techniczne nie gwarantuje 100%-towej szczelności systemu, konieczne jest, aby każdy pracownik pełen świadomej odpowiedzialności, postępował zgodnie z przyjętymi zasadami i minimalizował zagrożenia wynikające z ludzkich błędów.

Podstawa prawna.

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

2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. Nr 100, poz. 1024).

Definicje

Ilekroć w niniejszym dokumencie jest mowa o:

1. Urzędzie – należy przez to rozumieć Urząd Miasta i Gminy Ostroróg.

2. Administratorze Danych – należy przez to rozumieć Burmistrza Miasta i Gminy Ostroróg..

3. Administratorze Bezpieczeństwa Informacji – należy przez to rozumieć pracownika urzędu lub inna osobę wyznaczona do nadzorowania przestrzegania zasad ochrony określonych w niniejszym dokumencie oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych. Na to stanowisko powołany został przez Burmistrza Miasta i Gminy Ostroróg Sekretarz Gminy- Stanisław Żołądkowski.

4. Administratorze Systemu Informatycznego – należy przez to rozumieć osobę odpowiedzialna za funkcjonowanie systemu informatycznego urzędu oraz stosowanie technicznych i organizacyjnych środków ochrony. Funkcję tą pełni osoba powołana przez Burmistrza Miasta i Gminy Ostroróg- Informatyk Pan Piotr Glabiszewski.

5. System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu przetwarzania danych.

6. Użytkownik systemu – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym urzędu. Użytkownikiem może być pracownik urzędu, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno prawnej, osoba odbywająca staż w urzędzie wolontariusz.

7. Sieci lokalnej – należy przez to rozumieć połączenie systemów informatycznych urzędu wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych.

8. Sieci rozległej – należy przez to rozumieć sieć publiczną w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. z 2004 r. Nr 171, poz. 1800, z późn. zm.).

9. Zbiorze danych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

10. Przetwarzanie danych – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

11. Zabezpieczenie danych w systemie informatycznym – wdrożenie i eksploatacja stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

12. Identyfikator użytkownika – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

13. Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

14. Uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

15. Rozliczalność – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

16. Integralność danych – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

17. Poufność danych – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym osobom.

Polityka bezpieczeństwa określa.

1. Wykaz budynków oraz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe.

2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

3. Opis struktury zbiorów danych wskazujących zawartości poszczególnych pól informacyjnych i powiązań miedzy nimi.

4. Sposób przepływu danych pomiędzy systemami. Systemy, w których przetwarza się dane osobowe są rozproszone i nie są ze sobą połączone, co uniemożliwia przepływ danych pomiędzy nimi.

5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności i rozliczalności przetwarzanych danych.

Ad. 1

Obszar przetwarzania danych osobowych

Miejscem przetwarzania danych osobowych są pomieszczenia pracy komórek organizacyjnych Urzędu Miasta i Gminy Ostroróg.

Wykaz budynków oraz pomieszczeń stanowiących obszar przetwarzania danych osobowych :

Lp.	Adres- budynek	Numery pomieszczeń
1.	Budynek główny ul. Wroniecka 14	
	I piętro	12, 14, 15, 16, 17
	II piętro	21, 22, 24, 25, 26, 27
	III piętro	32, 33, 34

Ad.2

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

Za zbiór danych osobowych przetwarzanych w Urzędzie Miasta I Gminy Ostroróg uważa się:

1. dokumentację papierową (korespondencja, wnioski, deklaracje, itd.),

2. systemy informatyczne przetwarzania danych oraz oprogramowanie komputerowe służące do przetwarzania informacji,

3. wydruki komputerowe.

Wykaz zbiorów danych osobowych, sposób ich prowadzenia oraz programy służące do ich przetwarzania w UMiG w Ostrorogu:

Lp.	Nazwa zbioru	Opis	Forma prowadzenia	Nazwa programu
1.	**Ewidencja ludności Miasta i Gminy Ostroróg**	Zbiór mieszkańców zameldowanych na pobyt stały na terenie gminy, mieszkańców zameldowanych na pobyt czasowy oraz zbiór byłych mieszkańców, prowadzony na podstawie ustawy o ewidencji ludności i dowodach osobistych,w którym rejestruje się dane o miejscu pobytu osób, o urodzeniach, obowiązku wojskowym, zamianach stanu cywilnego, obywatelstwa, imion i nazwisk oraz zgonach	papierowa elektroniczna	RADIX ELUD
2.	**Dokumenty Stwierdzające Tożsamość Miasta i Gminy Ostroróg,**	Do zbiory tego należą dane zawarte w złożonych wnioskach o wydanie dowody osobistego, przetwarzane na podstawie ustawy o ewidencji ludności i dowodach osobistych, wprowadzane w celu wyprodukowania i wydania dokumentu tożsamości	papierowa elektroniczna	System Wydawania Dowodów Osobistych
3.	**Urząd Stanu Cywilnego Miasta i Gminy Ostroróg**	Do zbiory tego należą dane związane z rejestracją aktów stanu cywilnego a w szczególności rejestracją urodzeń, małżeństw, zgonów oraz innych zdarzeń mających wpływ na stan cywilny, przetwarzanych na podstawie ustawy prawo o aktach stanu cywilnego	papierowa elektroniczna	PB USC
4.	**Rejestr Wyborców**	Zbiór zawiera rejestr wyborców wpisanych z urzędu i rejestru wyborców	papierowa elektroniczna	RADIX, WYB

		wpisanych na wniosek prowadzony na postawie ustawy Kodeks Wyborczy, służy do przygotowania spisów wyborców		
5.	**Rejestr Testamentów**	Zbiór zawiera rejestr testamentów sporządzonych zgodnie z art. 951 k.c	papierowa	
6.	**Rejestr Przedpoborowych**	Zbiór zawiera mieszkańców gminy podlegającej kwalifikacji wojskowej	papierowa	
7.	**Akcja Kurierska**	Zbiór zawiera dane osób biorących udział w Akcji kurierskiej	papierowa	
8.	**Podatki i opłaty Miasta i Gminy Ostroróg oraz zwrot podatku akcyzowego producentom rolnych**	Do zbioru tego należą dane związane z rejestrami podatkowymi podatników oraz dane związane z składanymi wnioskami o zwrot podatku akcyzowego zawartego w cenie oleju napędowego wykorzystywanego do produkcji rolnej	papierowa elektroniczna	SIGID- podatek Rolny/Leśny/ Nieruchomości, dla osób fizycznych
9.	**Kadry i Płace**	Do zboru tego należą dane pracowników związane z naliczaniem i wypłata wynagrodzeń	papierowa elektroniczna	Płatnik BOMA SOFT KADRY PŁACE
10.	**Wieczyste użytkowanie**		Papierowa	B5 FK 5.01 BOMA SOFT
11.	**Dzierżawa gruntów**	Nazwisko, Imiona, adres, nr dowodu osobistego, nr nieruchomości	Papierowa elektroniczna	
12.	**Umowy najmu lokali użytkowych i mieszkalnych**	Nazwisko, Imiona, adres zamieszkania, adres lokalu, nr nieruchomości	papierowa	
13.	**Decyzja o warunkach zabudowy**	Nazwisko, Imię, adres zamieszkania, adres i nr nieruchomości	papierowa	
14.	**Decyzja na usunięcie drzew i krzewów**	Nazwisko, Imię, adres zamieszkania, adres i nr nieruchomości	papierowa	
15.	**Umowy na wywóz odpadów stałych i ciekłych**	Nazwisko, Imię adres zamieszkania nr nieruchomości	papierowa	

16.	**Dostęp do informacji o środowisku**	Nazwisko,Imię Adres	elektroniczna	SIOS
17.	**Internetowy Manager Punktów Adresowych**	Ulica, nr posesji, nr działki, właściciel	elektroniczna	IMPA
18.	**Internetowy Rejestr Mienia Komunalnego**	Nr działki, adres	elektroniczna	iRMK

Ad. 3

Opis struktury zbiorów danych osobowych oraz sposób przepływu danych pomiędzy systemami informatycznymi.

Opis struktury przetwarzanych danych osobowych oraz relacji pomiędzy danymi, procesy przetwarzania oraz struktura danych zostały zawarte w dokumentacji technicznej systemów informatycznych dostępnej u dostawców oprogramowania informatycznego. Licencje oprogramowania nie obejmują listingu danych źródłowych lecz jedynie prawo korzystania z rozwiązań.

Struktura zbiorów danych przetwarzanych w systemach informatycznych oraz powiązań między nimi:

Lp.	Nazwa zbioru	Nazwy rekordów wprowadzanych do programu
1	**RADIX ELUD**	PESEL, Nazwisko, imiona, nazwisko rodowe, obywatelstwom data i podstawa zmiany, adres zamieszkania, data zameldowania, Imiona, Nazwiska i nazwiska rodowe rodziców, data miejsce urodzenia, płeć, nr aktu urodzenia i USC. Rodzaj, seria i nr dokumentu tożsamości, książeczki wojskowej, stopień wojskowy, wykształcenie, wzrost, kolor oczu. Stan współmałżonka data zmiany, nr aktu, forma ustania, data zgonu współmałżonka, nr aktu i USC. Poprzednie nazwiska, imiona, adres, stan cywilny, dokument tożsamości.

2	**PB USC**	PESEL, Nazwiska i imiona,nazwiska rodowe, nazwiska z poprzedniego małżeństwa, imiona rodziców, nazwiska rodowe rodziców,imię nazwisko, nazwisko rodowe współmałżonka, PESEL współmałżonka, data miejsce godzina urodzenia, data i miejsce zawarcia małżeństwa, data i miejsce zgonu, nr aktu, adres zamieszkania lub pobytu, adres zamieszkania lub pobytu, adres zamieszkania rodziców, wykształcenie, płeć, stan cywilny, dokument tożsamości, adnotacje o rozwodzie, data unieważnienia aktu małżeństwa,urodzenia, zgonu
3	**SYSTEM WYDAWANIA DOWODÓ OSOBISTYCH**	PESEL, Nazwisko imiona, nazwisko rodowe, imiona rodziców, nazwisko rodowe matki, data i miejsce urodzenia, kolor oczu, wzrost, płeć, adres zamieszkania, seria i nr dowodu tożsamości, data zameldowania
4	**RADIX WYB**	PESEL, imiona, nazwisko, nazwisko rodowe, imię ojca, data urodzenia, płeć, adres zamieszkania, obywatelstwo, dokument tożsamości
5	**SIGID- Podatek Rolny/Leśny/Nieruchomości , dla osób fizycznych**	PESEL, imiona, nazwisko, imię ojca, imię matki, data urodzenia, adres zamieszkania, dokument tożsamości, NIP, nr konta bankowego
6	**PŁATNIK**	PESEL, imiona, nazwisko, data urodzenia, adres zameldowania, adres do korespondencji, dokument tożsamości, NIP, wysokość wynagrodzenia i jego pochodne
7	**BOMA SOFT KADRY, PŁACE**	PESEL, imiona, nazwisko, imię ojca, imię matki, data urodzenia adres zamieszkania, dokument tożsamości,stan cywilny, wykształcenie, NIP, płeć, wysokość wynagrodzenia i jego pochodne
8	**BS FK 5.01 BOMA SOFT**	Imię, Nazwisko

Ad. 5

Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

A. Dane w postaci elektronicznej.

Dane przetwarzane są przy użyciu komputerów pracujących wyłącznie w wewnętrznej sieci komputerowej oddzielonej fizycznie od sieci publicznej przy pomocy bramy internetowej wyposażonej w firewall oraz programowe firewalle na stacjach roboczych,

dodatkowo zabezpieczonych oprogramowaniem antywirusowym.
Dostęp do danych następuje po autoryzacji. Autoryzacja polega na podaniu identyfikatora oraz hasła przydzielonego przez Administratora bezpieczeństwa informacji na podstawie zgody Administratora danych.

Uwzględniając kategorie przetwarzanych danych wprowadza się podstawowy poziom bezpieczeństwa. Środki bezpieczeństwa na poziomie podstawowym określa instrukcja zarządzania systemem informatycznym.

B. Dane w rejestrach papierowych.

Dane przetwarzane przy użyciu tradycyjnych środków pisarskich gromadzone są w rejestrach, księgach, zeszytach papierowych oraz segregatorach i przechowywane w zamykanych szafach oraz według obowiązującej Instrukcji Kancelaryjnej.

C. Środki organizacyjne.

Administrator danych powołuje Administratora bezpieczeństwa informacji (ABI), który nadzoruje przestrzeganie zasady ochrony danych określonych w instrukcji zarządzania systemem informatycznym z uwzględnieniem spraw dotyczących ochrony danych osobowych przetwarzanych w tradycyjnych rejestrach.

D. Środki organizacyjne oraz środki ochrony fizycznej.

1. Wejście do budynku Urzędu Miasta i Gminy Ostroróg zabezpieczone jest zamkami drzwiowymi. Poszczególne pokoje, w których odbywa się przetwarzanie danych osobowych i ich składowanie muszą być wyposażone w niezależne zamki i muszą być zamykane podczas nieobecności pracownika. Odpowiedzialność za właściwą ochronę pomieszczeń ponosi pracownik oraz kierownik komórki organizacyjnej.

2. Przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osoby zatrudnionej przy przetwarzaniu danych lub w obecności Administratora Bezpieczeństwa Informacji.

3. Pomieszczenia, o których mowa wyżej, zamykane są na czas nieobecności pracownika zatrudnionego przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich. Klucze do pomieszczeń służbowych znajdują się w budynku Urzędu – sekretariat. Pozostawienie kluczy w zamkach pomieszczeń gdzie przetwarzane są dane osobowe jest niedopuszczalne (także podczas pobytu pracownika w pokoju).

4. W pomieszczeniach, w których przewiduje się przyjmowanie interesantów monitory stanowisk komputerowych ustawione są w sposób uniemożliwiający wgląd w przetwarzane dane.

5. Pracownicy przetwarzający dane osobowe obowiązani są do prawidłowego ich zabezpieczenia na swoich stanowiskach pracy. Przed rozpoczęciem pracy klucze pobierane zostają z zabezpieczonej gabloty pod nadzorem pracownika sekretariatu i tam też składowane po zakończeniu pracy.

E. Środki sprzętowe, informatyczne i telekomunikacyjne.

1. Urządzenia wychodzące w skład systemu informatycznego podłączone są do odrębnego obwodu elektrycznego, zabezpieczonego na wypadek zaniku napięcia albo awarii w sieci zasilającej listwą filtrujących oraz urządzeniem UPS.

2. Dostęp fizyczny do sieci lokalnej jest ograniczony, koncentrator umieszczony jest w specjalnie przygotowanej zamykanej szafie.
3. Serwer umieszczony jest w podpiwniczeniu budynku . w pomieszczeniu zamykanym drzwiami obitymi blacha, zabezpieczonymi zamkami patentowymi oraz kratą metalową, zakluczoną dwiema kłódkami.

4. Dostęp do sieci WAN zabezpieczony jest Firewall –em wraz z oprogramowaniem antywirusowym.

5. Kopie awaryjne wykonywane są w cyklach:

.
-dzienna na taśmie,
- w kasetach przechowywanych w szafie metalowej

6. Każdy dokument papierowy zawierający dane osobowe przeznaczony do wyrzucenia zostaje zniszczony w sposób uniemożliwiający jego odczytanie przy pomocy niszczarki.

7. Inne środki przetwarzania: drukarki, skanery, modemy, niszczarki dokumentów.

F. **Środki ochrony w ramach oprogramowania.**

1. Każda jednostka komputerowa zabezpieczona została , hasłem wejściowym do systemu operacyjnego lub do profilu użytkownika, oraz hasłem do każdej aplikacji przy pomocy której przetwarzane są dane osobowe.

2. Zastosowano wygaszanie ekranu w przypadku dłuższej nieaktywności użytkownika.

3. Zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji.

4. Zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (unikalny identyfikator i hasło).

Do zapoznania się z niniejszym dokumentem oraz stosowania zawartych w nim zasad zobowiązani są wszyscy pracownicy urzędu upoważnieni do przetwarzania danych osobowych.

BURMISTRZ

inż. Roman Napierała

Załącznik Nr 2do Zarządzenia Nr 52/2011
Burmistrza Miasta i Gminy Ostroróg
z dnia 29 grudnia 2011r.

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI W URZĘDZIE MIASTA I GMINY OSTRORÓG

Procedury nadawania i zmiany uprawnień do przetwarzania danych.

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych jest zobowiązany do zapoznania się:

- ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych,

- polityką bezpieczeństwa przetwarzania danych osobowych w Urzędzie,

- instrukcją zarządzania systemami informatycznymi w Urzędzie.

2. Administrator Bezpieczeństwa Informacji przyznaje uprawnienia w zakresie dostępu do systemu informatycznego.

3. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora, hasła oraz zakresu dostępnych danych i operacji.

4. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.

5. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.

6. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako naruszenie podstawowych obowiązków pracowniczych.

7. Pracownik zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest do zachowania ich w tajemnicy. Tajemnica obowiązuje go również po ustaniu zatrudnienia.

8. Odebranie uprawnień pracownikami następuje na pisemny wniosek kierownika, któremu pracownik podlega z poddaniem daty oraz przyczyny odebrania uprawnień.

9. Kierownicy komórek organizacyjnych zobowiązani są pisemnie informować Administratora Bezpieczeństwa Informacji o wszelkich zmianach kadrowych mających wpływ na zakres posiadanych uprawnień w systemie informatycznym.

10. Identyfikator osoby, która utraciła uprawnienia dostępu do danych osobowych należy niezwłocznie wyrejestrować z systemu informatycznego oraz unieważnić jej hasło.

11. Administrator Bezpieczeństwa Informacji zobowiązany jest do prowadzenia rejestru użytkowników i ich uprawnień w systemie informatycznym.

12. Rejestr użytkowników i ich uprawnień w systemie informatycznym, powinien zawierać:
- imię i nazwisko użytkownika systemów informatycznych,
. rodzaj uprawnienia,
. datę nadania uprawnienia,
. datę odebrania uprawnienia,
. przyczynę odebrania uprawnienia,
. podpis Administratora Bezpieczeństwa Informacji.

Zasady posługiwania się hasłami.

1. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.

2. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.

3. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.

4. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.

5. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.

6. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie.

1. Przed rozpoczęciem pracy w systemie komputerowym należy zalogować się do systemu przy użyciu indywidualnego identyfikatora oraz hasła.

2. Po opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wylogować się z systemu (zablokować dostęp), lub jeżeli taka możliwość nie istnieje wyjść z programu.

3. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów oraz wykonać zamknięcie.

4. Niedopuszczalne jest zamknięcie komputera przed zamknięciem oprogramowania.

Zasady instalacji oprogramowania.

1. Dopuszcza się instalację na serwerze nowego oprogramowania do przetwarzania danych osobowych lub aktualizacji istniejących pod warunkiem spełnienia określonych wymagań.

2. Instalacji oprogramowania lub aktualizacji dokonuje Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona, odnotowuje ten fakt w prowadzonym dzienniku pracy systemu.

3. Na wszystkich komputerach Urzędu Miasta i Gminy Ostroróg dopuszcza się instalację tylko legalnego, licencjonowanego oprogramowania.

4. Dopuszczone do zainstalowania programy użytkowe do przetwarzania danych osobowych obejmuje odrębny rejestr.

5. Zabrania się instalowania oprogramowania bez zgody Administratora Bezpieczeństwa Informacji.

Procedury tworzenia zabezpieczeń.

1. Za systematyczne przygotowanie kopii bezpieczeństwa odpowiada Administrator Bezpieczeństwa Informacji, a w przypadku jego nieobecności Administrator Systemu Informatycznego.

2. Kopie bezpieczeństwa wykonywane są w systemie dziennym na nośnik zewnętrzny.

3. Nośnik z kopiami bezpieczeństwa przechowywane są w szafie pancernej urzędu gminy.

4. Na każdym stanowisku komputerowym oraz serwerze zainstalowane jest oprogramowanie antywirusowe pracujące w trybie monitora.

5. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym.

6. Zabrania się pobierania plików z Internetu niewiadomego pochodzenia.

7. Administrator Systemu Informatycznego przeprowadza cyklicznie kontrole antywirusowe na wszystkich komputerach – minimum raz na miesiąc.

Zasady dokonywania napraw.

1. Dokonywanie napraw, przeglądów i konserwacji systemu przez pracowników serwisu mogą odbywać się jedynie w obecności Administratora Bezpieczeństwa Informacji lub osoby przez niego upoważnionej.

2. Przeglądów należy dokonywać nie rzadziej niż raz na kwartał.

3. Fakt dokonania naprawy, przeglądów lub konserwacji musi być udokumentowany w dokumentacji systemu.

4. Uszkodzone nośniki magnetyczne lub inne zawierające dane osobowe nie mogą być użytkowane. Muszą być odpowiednio zabezpieczone przed nieuprawnionym udostępnieniem, a następnie zniszczone lub naprawione pod nadzorem osoby upoważnionej przez Administratora Danych

Nośniki papierowe danych – wydruki.

1. W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym.

2. Pomieszczenie, w którym przechowywane są wydruki robocze musi być należycie zabezpieczone po godzinach pracy.

3. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

Profilaktyka antywirusowa.

1. Każdy użytkownik komputera w urzędzie gminy zobowiązany jest do używania w pracy płyt CD zakupionych przez urząd (nie prywatnych).

2. Informacje i dane przechowywane na płytach CD mogą mieć wyłącznie charakter związany z pracą.

3. Każdy komputer minimum raz w miesiącu powinien zostać sprawdzony aktualną wersją programu antywirusowego.

Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego

1. Użytkownik jest zobowiązany zawiadomić administratora bezpieczeństwa informacji o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu, a w szczególności o:

- naruszeniu hasła dostępu i identyfikatora (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzenia hasła),
- częściowym lub całkowitym braku danych albo dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień,
- braku dostępu do właściwej aplikacji ,
- wykryciu wirusa komputerowego,
- znacznym spowolnieniu działania systemu informatycznego,
- podejrzeniu kradzieży sprzętu komputerowego lub dokumentów zawierających dane osobowe,
- zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf.

2. Administrator bezpieczeństwa informacji i administrator systemu zobowiązani są do informowania administratora danych o awariach systemu informatycznego, zauważonych przypadkach naruszenia niniejszej instrukcji przez użytkowników, a zwłaszcza o przypadkach posługiwania się przez

użytkowników nieautoryzowanymi programami, nieprzestrzegania zasad używania oprogramowania antywirusowego, niewłaściwego wykorzystania sprzętu biurowego lub przetwarzania danych w sposób niezgodny z procedurami ochrony danych osobowych.

Postanowienie końcowe

1. W sprawach nieokreślonych niniejszą instrukcją należy stosować instrukcję obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.

2. Każda osoba upoważniona do przetwarzania danych osobowych jest zobowiązana zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszą instrukcją oraz złożyć stosowne oświadczenie potwierdzające znajomości jej treści.

3. Naruszenie obowiązków wynikających z niniejszej instrukcji oraz przepisów o ochronie danych osobowych może być uznane za ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnych oraz sankcjom karnym, w szczególności wynikającym z art. 51 ustawy.

BURMISTRZ
inż. Roman Napierała