BURMISTRZ
MIASTA I GMINY
FROMBORK

Zarządzenie Nr 53/2012
Burmistrza Miasta i Gminy Frombork
z dnia 09 października 2012

w sprawie wprowadzenia polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Na podstawie art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) 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) zarządzam, co następuje:

§1

1. Wprowadza się w Urzędzie Miasta i Gminy we Fromborku szczegółowe zasady ochrony danych osobowych, opisane w załącznikach do niniejszego zarządzenia.
2. Wszystkich pracowników Urzędu Miasta i Gminy we Fromborku, a w szczególności przetwarzających dane osobowe, zobowiązuje się do zapoznania z niniejszym zarządzeniem wraz z załącznikami i do przestrzegania zawartych w nim zasad.

§2

Wprowadzam do stosowania w Urzędzie Miasta i Gminy we Fromborku:

1. Politykę Bezpieczeństwa, która stanowi załącznik nr 1 do niniejszego zarządzenia.
2. Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych, która stanowi załącznik nr 2 do niniejszego zarządzenia.
3. Upoważnienie do przetwarzania danych osobowych, które stanowi załącznik nr 3 do niniejszego zarządzenia.
4. Oświadczenie, które stanowi załącznik nr 4 do niniejszego zarządzenia.

§3

Traci moc Zarządzenie Nr 17/2012 Burmistrza Miasta i Gminy Frombork z dnia 22 marca 2012 roku w sprawie wprowadzenia polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

§4

Zarządzenie wchodzi w życie z dniem podjęcia

BURMISTRZ
Krystyna Lewańska

Załącznik nr 1
do Zarządzenia nr 53/2012
Burmistrza Miasta i Gminy Frombork
z dnia 09 października 2012r.

RO.142.1.2012.DK

POLITYKA BEZPIECZEŃSTWA

I. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

Dane osobowe przetwarzane są w budynku Urzędu Miasta i Gminy Frombork, ul. Młynarska 5a, 14-530 Frombork.

Lp.	Nazwa zbiorów danych osobowych	Pomieszczenia w których przetwarzane są zbiory danych osobowych	Stanowisko przetwarzające zbiory danych
1.	Ewidencja Najemców Mieszkaniowego Zasobu Gminy Frombork	pok. Nr 4	Inspektor ds. obsługi gospodarki mieszkaniowej
2.	Podatek od Nieruchomości i Analiza Wpłat PN	pok. Nr 5	Inspektor ds. wymiaru podatków i opłat lokalnych
3.	Łączne Zobowiązania Pieniężne	pok. Nr 8	Inspektor ds. windykacji i wynagrodzeń
4.	Urząd Stanu Cywilnego we Fromborku	pok. Nr 10	Zastępca Kierownika Urzędu Stanu Cywilnego
5.	Rejestracja i Kwalifikacja Wojskowa	pok. Nr 10	Zastępca Kierownika Urzędu Stanu Cywilnego
6.	Ewidencja Ludności	pok. Nr 10	Zastępca Kierownika Urzędu Stanu Cywilnego
7.	Umowy Dzierżawne i Najem, Przekształcenie Prawa Użytkowania Wieczystego w Prawo Własności, Użytkowanie Wieczyste Gruntu, Zbywanie Lokali Mieszkalnych	Pok. Nr 12	Inspektor ds. gospodarki gruntami, lokalami i rolnictwa
8.	Rejestr - Wycinka drzew	pok. Nr 12	Młodszy referent ds. ochrony środowiska
9.	Ewidencja Umów na Odbiór Odpadów Komunalnych od Właścicieli Nieruchomości	pok. Nr 12	Młodszy referent ds. ochrony środowiska
10.	Plany Obronne Gminy Frombork, Obrony Cywilnej Gminy Frombork, Zarządzania Kryzysowego Gminy Frombork	pok. nr 14	Inspektor ds. wojskowych, obrony cywilnej i zarządzania kryzysowego
11.	Oświadczenia Majątkowe Radnych	pok. Nr 16	Referent ds. obsługi Rady Miejskiej we Fromborku
12.	System Informacji Oświatowej	pok. Nr 17	Sekretarz Gminy Frombork
13.	Rejestr Wydanych Decyzji o Warunkach Zabudowy i Zagospodarowania Terenu, Renty Planistyczne, Zawiadomienie Stron o Przeznaczeniu Terenu	pok. Nr 18	Inspektor ds. budownictwa, gospodarki przestrzennej, inwestycji i zamówień publicznych

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

Lp.	Nazwa zbiorów danych osobowych	Pomieszczenia w których przetwarzane są zbiory danych osobowych	Oprogramowanie/wersja
1.	Ewidencja Najemców Mieszkaniowego Zasobu Gminy Frombork	pok. Nr 4	GRAVIS/Czynsz/2007.05
2.	Podatek od Nieruchomości i Analiza Wpłat PN	pok. Nr 5	GRAVIS/Podatki/2006.04
3.	Łączne Zobowiązania Pieniężne	pok. Nr 8	GRAVIS Podatki/2006.04 Płatnik/ 8.01.001
4.	Urząd Stanu Cywilnego we Fromborku	pok. Nr 10	PUMA/Moduł USC/03.061
5.	Rejestracja i Kwalifikacja Wojskowa	pok. Nr 10	PUMA/Moduł EL/03.061
6.	Ewidencja Ludności	pok. Nr 10	PUMA/Moduł EL/03.061
7.	Umowy Dzierżawne i Najem, Przekształcenie Prawa Użytkowania Wieczystego w Prawo Własności, Użytkowanie Wieczyste Gruntu, Zbywanie Lokali Mieszkalnych	pok. Nr 12	Word/2002
8.	Rejestr - Wycinka drzew	pok. Nr 12	Word/2002
9.	Ewidencja Umów na Odbiór Odpadów Komunalnych od Właścicieli Nieruchomości	pok. Nr 12	Word/2002
10.	Plany Obronne Gminy Frombork, Obrony Cywilnej Gminy Frombork, Zarządzania Kryzysowego Gminy Frombork	pok. nr 14	Word/2002
11.	Oświadczenia Majątkowe Radnych	pok. Nr 16	Word/2002
12.	System Informacji Oświatowej	pok. Nr 17	SIO/3.12.0
13.	Rejestr Wydanych Decyzji o Warunkach Zabudowy i Zagospodarowania Terenu, Renty Planistyczne, Zawiadomienie Stron o Przeznaczeniu Terenu	pok. Nr 18	Word/2002

III. Opis struktury zbiorów danych osobowych wskazujących zawartość poszczególnych pól informacyjnych i powiązania pomiędzy nimi:

1. Zbiór danych **„Ewidencja Najemców Mieszkaniowego Zasobu Gminy Frombork"** zawiera następujące pola:
   - Nazwiska i imiona
   - Adres zamieszkania lub pobytu

2. Zbiór danych **„Podatek od Nieruchomości i Analiza Wpłat PN"** zawiera następujące pola:
   - Nazwiska i imiona
   - Imiona rodziców
   - Data urodzenia
   - Adres zamieszkania lub pobytu
   - Nr PESEL
   - Nr NIP
   - Miejsce pracy

3. Zbiór danych **„Łączne Zobowiązania Pieniężne"** zawiera następujące pola:
   - Nazwiska i imiona
   - Imiona rodziców
   - Data urodzenia
   - Adres zamieszkania lub pobytu
   - Nr PESEL
   - Nr NIP
   - Miejsce pracy

4. Zbiór danych **„ Urząd Stanu Cywilnego we Fromborku"** zawiera następujące pola:
   - Nazwiska i imiona
   - Imiona rodziców
   - Data urodzenia
   - Adres zamieszkania lub pobytu
   - Nr PESEL
   - Zawód
   - Wykształcenie
   - Seria i nr dowodu osobistego
   - Kolor oczu
   - Wzrost w cm
   - Płeć
   - Kod pocztowy
   - Przyczyna wystawienia dowodu
   - Podpis osoby

5. Zbiór danych **„ Rejestracja i Kwalifikacja Wojskowa"** zawiera następujące pola:
   - Nazwiska i imiona
   - Imiona rodziców
   - Data urodzenia
   - Adres zamieszkania lub pobytu
   - Nr PESEL
   - Seria i nr dowodu osobistego
   - Nazwisko rodowe przedpoborowych

6. Zbiór danych: **„Ewidencja Ludności"** zawiera następujące pola:
   - Imiona i nazwiska
   - Imiona i nazwiska rodowe rodziców
   - Nazwisko rodowe
   - Data urodzenia
   - Miejsce urodzenia
   - Numer PESEL
   - Kolor oczu
   - Wzrost w cm
   - Płeć
   - Adres zamieszkania
   - Rodzaj zameldowania
   - Kod pocztowy
   - Posiadany dotychczasowy dokument tożsamości (seria, nr, nazwa i siedziba wystawcy)
   - Przyczyna wystawienia dowodu
   - Data i przyczyna utraty
   - Dane osobowe (nazwiska i imiona, nazwisko rodowe i z poprzedniego małżeństwa, imiona rodziców, data urodzenia, miejsce urodzenia, akta urodzenia, data i nr USC)
   - Dane osobowe archiwalne (nazwiska i imiona, nazwisko rodowe i z poprzedniego małżeństwa)
   - Adres zamieszkania lub pobytu stałego oraz data zameldowania
   - Adres czasowy oraz czas pobytu czasowego
   - Archiwalne adresy zamieszkania lub pobytu stałego oraz data zameldowania
   - Dokument tożsamości (rodzaj dokumentu, seria i numer dowodu, wystawca dokumentu, rysopis: wzrost, kolor oczu, znaki szczególne)
   - Numer ewidencyjny PESEL
   - USC i nr aktu urodzenia
   - Stan cywilny (imię i nazwisko współ małżonka, nazwisko rodowe i nazwisko z poprzedniego małżeństwa, data zawarcia małżeństwa, USC i numer aktu małżeństwa)
   - Data wydania i wydający dokument tożsamości
   - Stan cywilny archiwalny (imię i nazwisko współmałżonka, nazwisko rodowe i nazwisko z poprzedniego małżeństwa, data zawarcia małżeństwa, USC i numer aktu małżeństwa
   - Archiwalne dokumenty tożsamości
   - Obowiązek wojskowy (czy podlega obowiązkowi, nazwa i nr wojskowego dokumentu tożsamości, stopień wojskowy)

- Data zgonu, USC i numer aktu zgonu
- Imiona i nazwiska rodowe
- Narodowość
- Obywatelstwo (data zmiany, podstawa prawna)
- Adnotacje o rozwodzie

7. Zbiór danych **„Umowy Dzierżawne i Najem, Przekształcenie Prawa Użytkowania Wieczystego w Prawo Własności, Użytkowanie Wieczyste Gruntu, Zbywanie Lokali Mieszkalnych"** zawiera następujące pola:
   - Nazwiska i imiona
   - Adres zamieszkania lub pobytu
   - Imiona rodziców
   - Numer ewidencyjny PESEL
   - Numer, powierzchnia, położenie działki
   - Seria i numer DO
   - Numer, powierzchnia, położenie lokalu mieszkalnego

8. Zbiór danych **„ Rejestr - Wycinka Drzew"** zawiera następujące pola:
   - Nazwiska i imiona
   - Adres zamieszkania lub pobytu
   - Lokalizacja drzew przeznaczonych do wycinki
   - Nr telefonu

9. Zbiór danych **„Ewidencja Umów na Odbiór Odpadów Komunalnych od Właścicieli Nieruchomości"** zawiera następujące pola:
   - Nazwiska i imiona
   - Adres zamieszkania lub pobytu

10. Zbiór danych **„Plany Obronne Gminy Frombork, Obrony Cywilnej i Zarządzania Kryzysowego Gminy Frombork"** zawiera następujące pola:
    - Nazwiska i imiona
    - Imiona rodziców
    - Data urodzenia
    - Miejsce urodzenia
    - Adres zamieszkania
    - Nr telefonu

11. Zbiór danych **„Oświadczenia Majątkowe Radnych"** zawiera następujące pola:
    - Nazwiska i imiona
    - Adres zamieszkania lub pobytu
    - Miejsce urodzenia
    - Miejsce pracy
    - Seria i nr dowodu osobistego
    - Informacje o stanie majątkowym

- Informacje o prowadzonej działalności gospodarczej

12. Zbiór danych **„ System Informacji Oświatowej"** zawiera następujące pola:
    - Data urodzenia
    - Nr PESEL
    - Wykształcenie
    - Płeć
    - Formy i wymiar zatrudnienia
    - Stopień awansu zawodowego
    - Przygotowanie pedagogiczne
    - Formy kształcenia i doskonalenia
    - Sprawowane funkcje i zajmowane stanowiska
    - Rodzaj prowadzonych zajęć albo przyczyny nieprowadzenia zajęć
    - Staż pracy
    - Wysokość wynagrodzenia, z wyszczególnieniem jego składników
    - Wysokość dodatków

13. Zbiór danych **„Rejestr Wydanych Decyzji o Warunkach Zabudowy i Zagospodarowania Terenu, Zawiadomieniu Stron o Przeznaczeniu Terenu, Renty Planistyczne"** zawiera następujące pola:
    - Nazwiska i imiona
    - Adres zamieszkania lub pobytu
    - Rodzaj, charakterystyka i lokalizacja zamierzonej inwestycji

IV. Sposób przepływu danych pomiędzy poszczególnymi systemami

- Brak przepływu danych pomiędzy poszczególnymi systemami

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

A. Środki ochrony fizycznej:

1. Budynek Urzędu, w którym zlokalizowany jest obszar przetwarzania danych osobowych jest zamykany po zakończeniu pracy oraz zabezpieczany alarmem.
2. Budynek Urzędu, w którym zlokalizowany jest obszar przetwarzania danych osobowych jest podłączony do systemu monitoringu wizualnego z rejestracją całodobową.
3. Urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonymi zamkami patentowymi.
4. Przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osoby zatrudnionej przy przetwarzaniu danych lub obecności Burmistrza Miasta i Gminy.
5. Pomieszczenia, o których mowa wyżej, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.
6. W przypadku przebywania osób postronnych w pomieszczeniach, o których mowa wyżej,

monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.

7. Po zakończeniu pracy przy przetwarzaniu danych osobowych pracownik powinien kierować się zasadą „czystego biurka" - **uprzątnąć i zabezpieczyć dokumenty, pieczątki oraz wszelkiego rodzaju nośniki na których znajdują się dane osobowe, a także odpowiednio zabezpieczyć sprzęt komputerowy – wyłączyć stację roboczą, monitor oraz urządzenia peryferyjne np. drukarki.**
8. Do przebywania w pomieszczeniu serwera uprawnieni są: Administrator Bezpieczeństwa Informacji (ABI), osoby odpowiedzialne za obsługę informatyczną Urzędu oraz Burmistrz Miasta i Gminy.
9. Przebywanie w pomieszczeniu serwera osób nieuprawnionych (konserwator, elektryk, sprzątaczka) dopuszczalne jest tylko w obecności jednej z osób upoważnionych, o których mowa w pkt. 8, a w przypadku ich nieobecności - w obecności osoby pisemnie upoważnionej przez kierownika urzędu.

B. Środki sprzętowe, informatyczne i telekomunikacyjne:

1. Każdy dokument papierowy przeznaczony do wyrzucenia powinien być uprzednio zniszczony w sposób uniemożliwiający jego odczytanie (np. przy pomocy niszczarki dokumentów)
2. Urządzenia wchodzące w skład systemu informatycznego podłączone są do obwodu elektrycznego UPS, zabezpieczonego na wypadek zaniku napięcia albo awarii w sieci zasilającej
3. Zakupiono komputer – serwer NAS w celu archiwizacji danych z poszczególnych komputerów użytkowych.
4. Na wszystkich serwerach oraz stacjach roboczych zainstalowano oprogramowanie antywirusowe. Poczta elektroniczna wpływająca do Urzędu skanowana jest programem antywirusowym przed przesłaniem jej do Użytkowania.
5. Archiwizacje wykonywane są na płytach CD w cyklu miesięcznym, oraz na odrębnym komputerze w zamykanym pomieszczeniu w cyklu tygodniowym.

C. Środki ochrony w ramach oprogramowania systemu:

1. Dostęp fizyczny do baz danych osobowych zastrzeżony jest wyłącznie dla osób zajmujących się obsługą informatyczną Urzędu.
2. Konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych jedynie za pośrednictwem aplikacji.
3. System informatyczny pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu.
4. W sieciowym systemie operacyjnym zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do sieci.

D. Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych:

1. Zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji, chyba że program tego nie przewiduje, wówczas jedynym środkiem zabezpieczającym jest hasło systemowe.
2. Dla każdego użytkownika systemu jest ustalony odrębny identyfikator.

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

E. Środki ochrony w ramach systemu użytkowego:

1. Zastosowano wygaszenie ekranu w przypadku dłuższej nieaktywności użytkownika.
2. Komputer, z którego możliwy jest dostęp do danych osobowych zabezpieczony jest hasłem uruchomieniowym.

F. Środki organizacyjne:

1. Administrator Danych Osobowych (ADO) wyznacza ABI, który przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego upoważnienia kierownika urzędu określającego zakres uprawnień pracownika.
2. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.
3. Wprowadzono instrukcję zarządzania systemem informatycznym.
4. Za kontrolę prawidłowego działania urządzeń i oprogramowania odpowiedzialny jest Administrator Systemu Informatycznego (ASI).
5. Za monitorowanie zabezpieczeń systemów informatycznych odpowiedzialny jest ASI oraz ABI.
6. ABI wspólnie z ASI dokonuje przeglądu systemu informatycznego pod względem prawidłowości zabezpieczeń w cyklu półrocznym. W szczególności należy zwrócić uwagę na:
   - zakres uprawnień użytkowników,
   - przestrzeganie zasad ochrony dostępu do informacji (zabezpieczenie pomieszczeń, blokowanie stacji roboczych, zachowanie zasady czystego biurka),
   - przestrzeganie zasad tworzenia kopii bezpieczeństwa,
   - konfigurację systemu pod względem jego bezpieczeństwa.
7. Z dokonania przeglądu ABI sporządza protokół ze szczególnym wskazaniem braków w systemie zabezpieczeń.
8. Protokoły z przeprowadzonej kontroli przechowuje ABI po uprzednim zaakceptowaniu wyników przez ADO.
9. W przypadku stwierdzenia niezgodności ABI wspólnie z ASI opracowują plan naprawy i przywrócenia działania systemu informatycznego do stanu zgodnego z prawem. Plan naprawy każdorazowo akceptuje ADO.

BURMISTRZ
Krystyna Lewańska

Załącznik nr 2
do Zarządzenia nr 53/2012
Burmistrza Miasta i Gminy Frombork
z dnia 09 października 2012r.

Urząd Miasta i Gminy we Fromborku,
Ul. Młynarska 5a,
14-530 Frombork

RO.142.2.2012.DK

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

Zgodnie z § 3 Rozporządzenia Ministra Sprawa 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), zwanego dalej „rozporządzeniem", wdraża się niniejszy dokument stanowiący „Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych", w celu stworzenia kompleksowych rozwiązań służących zapewnieniu bezpieczeństwa systemów informatycznych służących do przetwarzania danych.

Cel instrukcji

Celem wydania instrukcji jest realizacja zapisów Polityki Bezpieczeństwa przetwarzania danych osobowych obowiązującej w Urzędzie Miasta i Gminy we Fromborku oraz zaleceń § 5 rozporządzenia. Instrukcja ma charakter ***uniwersalny*** i precyzuje zagadnienia zarządzania ***wszystkimi*** systemami informatycznymi znajdującymi się w Urzędzie Miasta i Gminy we Fromborku.

I. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności:

1. Administrator Danych Osobowych (ADO):
   - nadaje upoważnienie w zakresie dostępu do systemu informatycznego osobie, która w związku z wykonywanymi przez siebie obowiązkami będzie miała dostęp do danych osobowych w systemie,
   - przekazuje wypełniony dokument w postaci papierowej:
     - 1 egz. do inspektora ds. organizacyjno – kadrowych - celem umieszczenia w teczce akt osobowych,
     - 1 egz. do osoby której upoważnienie dotyczy,
     - 1 egz. do Administrator Bezpieczeństwa Informacji (ABI).

2. ABI:
   - aktualizuje ewidencję osób upoważnionych do przetwarzania danych osobowych w systemie informatycznym.

3. Administrator Systemu Informatycznego (ASI):
   - rejestruje użytkownika w systemie i nadaje mu określone uprawnienia oraz hasło.

4. Użytkownik:
   - uwierzytelnia się w systemie po podaniu identyfikatora oraz hasła uzyskanego od Informatyka,
   - użytkownik zmienia hasło na swoje, którego nie przekazuje nikomu i może rozpocząć pracę w aplikacji.

5. Użytkownik jest wyrejestrowany z systemu informatycznego w każdym przypadku utraty przez niego uprawnień dostępu do danych osobowych, co ma miejsce w przypadku:
   - ustania zatrudnienia,
   - zmiany zakresu obowiązków,
   - utraty uprawnienia,
   - informację pisemną o ustaniu zatrudnienia, zmianie zakresu obowiązków i utracie upoważnienia, przekazują kadry do ABI z chwilą ich zaistnienia.

II. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzeniem i użytkowaniem:

1. W systemie informatycznym stosuje się uwierzytelnienia dwustopniowe; na poziomie:
   - dostępu do stacji roboczej,
   - dostępu do aplikacji.

2. Do uwierzytelnienia użytkownika w systemie na obu poziomach stosuje się hasła.
3. Hasło dostępu do stacji roboczej składa się co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry i znaki specjalne.
4. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
5. Hasło nie może być ujawnione nawet po utracie przez nie ważności.
6. Zmiana hasła do systemu następuje nie rzadziej, niż co 30 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.
7. Dla każdej osoby upoważnionej instalowany jest odrębny identyfikator i hasło tak, aby bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym mogła mieć tylko ta osoba, która poda właściwy identyfikator i hasło.
8. Identyfikator użytkownika jest wpisywany do ewidencji osób upoważnionych do przetwarzania danych osobowych w systemie informatycznym wraz z zakresem upoważnienia oraz datą nadania uprawnień.
9. System zostanie zablokowany po trzykrotnej próbie nieudanego logowania się.

III. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu:

1. Rozpoczęcia pracy:
   - uruchomienie komputera w systemie podając hasło,
   - uruchomić komputer i zalogować się podając swój identyfikator dostępu do stacji roboczej,
   - uruchomić aplikację, wpisując swój identyfikator i hasło dostępu - uzależnione od programu,
   - rozpocząć pracę.

2. Procedura zawieszenia pracy w systemie:
   - przy każdym opuszczeniu stanowiska komputerowego, dopilnować, aby na ekranie nie były wyświetlone dane osobowe,
   - przed opuszczeniem miejsca pracy na dłuższy czas użytkownik obowiązany jest poczekać, aż zaktywizuje się wygaszacz ekranu.

3. Procedura zakończenia pracy w systemie:
   - zarchiwizować dane,
   - zamknąć aplikację,
   - zamknąć system,
   - wyłączyć monitor i drukarkę.

IV. Procedury tworzenia kopii zapasowych i zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania:

1. W cyklu cotygodniowym kopie wykonywane są w serwerze oraz na odrębnym stanowisku komputerowym pełniącym funkcję archiwum.
2. W cyklu miesięcznym kopie zapisywane są na płytach cd.
3. W razie potrzeby kopie zapasowe wykonywane są przez użytkowników aplikacji na płytach lub innych nośnikach pamięci w cyklu codziennym.
4. ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.

V. Sposób, miejsce i okres przechowywania:

1. Wydruki archiwalne lub bieżące przechowywane mogą być wyłącznie w pomieszczeniach uniemożliwiających dostęp do nich przez osoby nieupoważnione.
2. Wydruki, zawierające dane osobowe, należy zniszczyć przez pocięcie w niszczarce nie później niż po upływie 3 dni, po ich wykorzystaniu chyba, że z odrębnych przepisów wynika obowiązek ich przechowywania.
3. Za bezpieczeństwo danych zapisanych w komputerach przenośnych oraz w innych urządzeniach przenośnych w całości odpowiada użytkownik komputera lub urządzenia przenośnego.
4. Po zakończeniu pracy przez użytkowników systemu, elektroniczne nośniki informacji są przechowywane w zamykanych na klucz szafach biurowych lub szafach pancernych.
5. Przeznaczone do likwidacji elektroniczne i optyczne nośniki informacji, mogące zawierać dane

osobowe, pozbawia się w sposób trwały zapisu tych danych, a w przypadku gdy nie jest to możliwe, niszczy lub uszkadza się w sposób trwale uniemożliwiający ich odczytanie, nie później niż po upływie 3 dni.

6. Za skasowanie zbędnych danych lub zniszczenie zbędnych nośników elektronicznych odpowiedzialny jest ASI.
7. Kopie zapasowe zbioru danych osobowych przechowywane są w serwerowni.
8. Dostęp do serwerowni mają tylko upoważnieni pracownicy, tj. ABI i ASI oraz Burmistrz Miasta i Gminy.
9. Kopie zapasowe przechowuje się przez okres:
   - dzienne - przez siedem dni,
   - tygodniowe -do końca następnego tygodnia,
   - miesięczne -dwunastu miesięcy następujących po miesiącu sporządzenia kopii, dopuszcza się dłuższy okres przechowywania, o ile pozwalają na to warunki.
10. Dane osobowe zapisane w formie papierowej inne niż wydruki z systemu (pisma, ankiety itp.) są przechowywane na podobnych zasadach, co wydruki.
11. W przypadku konieczności przekazywania elektronicznych lub optycznych nośników informacji zawierających dane osobowe podmiotom zewnętrznym w sytuacjach nie związanych z wykonywanymi działaniami służbowymi, nośniki te pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie.
12. W przypadku konieczności przekazywania elektronicznych lub optycznych nośników informacji zawierających dane osobowe podmiotom zewnętrznym w sytuacjach nie związanych z wykonywanymi działaniami służbowymi oraz brakiem możliwości pozbawienia się wcześniej zapisanych na nich danych, na czas przekazania sporządza się stosowną umowę powierzenia danych osobowych.

VI. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego lub inna ingerencja w ten system:

1. Nadzór nad instalowaniem nowego oprogramowania antywirusowego oraz nad bieżącą jego aktualizacją sprawuje ASI.
2. Oprogramowanie zastosowane w systemach informatycznych automatycznie monitoruje występowanie wirusów w trakcie załączania lub wczytywania danych z zewnętrznych nośników informacji.
3. Kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.
4. Czynności związane z ochroną antywirusową systemu informatycznego wykonuje ASI, wykorzystując w trakcie pracy moduł programu antywirusowego z aktualną bazą antywirusową.
5. ASI ma obowiązek zgłaszać na piśmie ADO wszelkie potrzeby lub zauważone niedociągnięcia w zakresie zapewnienia bezpieczeństwa systemu informatycznego.
6. O każdorazowym wykryciu wirusa przez oprogramowanie antywirusowe użytkownik obowiązany jest niezwłocznie poinformować ABI lub ASI.
7. W przypadku, gdy system zabezpieczeń wskazuje zaistnienie zagrożenia, użytkownicy są

zobowiązani bezzwłocznie powiadomić o tym fakcie ASI, który po jego usunięciu sprawdza system i przywraca go do pełnej funkcjonalności.

8. ASI jest odpowiedzialny za aktywowanie i poprawne konfigurowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku:
   - sieci lokalnej,
   - stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej.
9. Ochrona systemu informatycznego używanego w urzędzie polega na:
   - ochronie przez identyfikator,
   - ochronie za pomocą hasła,
   - przydzielaniu praw.
10. Bezwzględnie zakazuje się użytkownikom samowolnego korzystania z prywatnych lub pochodzących ze źródła innego niż miejsce pracy nośników informacji (magnetycznych, optycznych, urządzeń podłączanych do stacji roboczych). Korzystanie z takich nośników może mieć miejsce wyłącznie po uzyskaniu zgody ASI, po uprzednim sprawdzeniu nośnika informacji przez ASI pod względem bezpieczeństwa dla systemu informatycznego.
11. Bezwzględnie zabrania się użytkownikom łamania lub obchodzenia zabezpieczeń systemów informatycznych. O każdym przypadku znalezienia luki w zabezpieczeniach użytkownik ma obowiązek powiadomić ABI oraz ASI.

VII. Zasady i sposób odnotowania w systemie informacji o udostępnianiu danych osobowych.

1. W komórce organizacyjnej w której przetwarzane są dane osobowe prowadzi się rejestr. W niektórych aplikacjach możliwe jest odnotowanie informacji o odbiorcach danych z tego systemu.
2. Odbiorcą danych jest każdy, komu udostępnia się dane osobowe, z wyłączeniem:
   - osoby, której dane dotyczą,
   - osoby użytkowania systemu lub innej osoby upoważnionej do przetwarzania danych osobowych w urzędzie,
   - przedstawiciela, o którym mowa w art. 31a ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych,
   - podmiotu, któremu powierzono przetwarzanie danych,
   - organów państwowych lub organów samorządu terytorialnego, któremu dane są udostępnione w związku z prowadzonym postępowaniem.
3. Odnotowanie obejmuje informacje o:
   - nazwie jednostki organizacyjnej lub imieniu i nazwisku osoby, której udostępniono dane,
   - zakresie udostępniania danych,
   - dacie udostępniania.
4. Udostępnianie danych osobowych może nastąpić wyłącznie na pisemną prośbę odbiorcy danych.
5. Nadzór nad prawidłowością odnotowywania w systemie ww. informacji sprawuje ABI.

VIII. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych:

1. O przeprowadzonych przeglądach i konserwacjach systemu każdorazowo informowany jest ABI, który może nadzorować przebieg prac.
2. Przeglądu i konserwacji sprzętu w sieci informatycznej, systemów informatycznych i nośników informacji dokonuje stosownie do potrzeb ASI w porozumieniu z ABI.
3. Za terminowość przeprowadzania przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ASI.
4. Bezwzględnie zabronione jest samodzielne dokonywanie przez użytkowników napraw sprzętu informatycznego, wymiana jego podzespołów oraz wykonywanie innych czynności nie związanych bezpośrednio z jego eksploatacją lub nie dopuszczonych do wykonywania przez producenta sprzętu w instrukcji obsługi.
5. Użytkownik ma obowiązek niezwłocznie powiadomić ABI o wszelkich nieprawidłowościach i awariach sprzętu informatycznego, mogących prowadzić do próby naruszenia lub naruszenia bezpieczeństwa danych osobowych.
6. Sprawdzanie poprawności działania programów i narzędzi programowych przeprowadza się w następujących przypadkach:
   - zmiany wersji oprogramowania serwera plików,
   - zmiany wersji oprogramowania stanowiska komputerowego użytkownika systemu,
   - zmiany systemu operacyjnego serwera plików,
   - zmiany systemu operacyjnego stanowiska komputerowego użytkownika systemu,
   - wykonania zmian w projekcie systemu spowodowanych koniecznością naprawy, konserwacji lub modyfikacji systemu.
7. Przed dokonaniem zmian w systemie informatycznym należy dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych na testowej bazie danych. Sprawdzanie powinno obejmować:
   - poprawność logowania się do systemu w zależności od posiadanych uprawnień (zasymulować pracę wszystkich typów uprawnień użytkownika),
   - poprawność działania wszystkich elementów aplikacji (menu, zestawienia, formularze, raporty).
8. Poprawność funkcjonowania aplikacji polega na symulacji działania wykonujące następujące operacje:
   - wprowadzania danych osobowych,
   - edytowania danych osobowych,
   - wyszukiwania danych osobowych,
   - wydruku danych osobowych.
9. Przegląd przeprowadza projektant nowego systemu w obecności ASI.
10. Za prawidłowość przeprowadzania przeglądów i konserwacji systemu odpowiada ASI.
11. Konserwację oprogramowania przeprowadza się po zgłoszeniu przez użytkownika systemu potrzeby wprowadzenia zmian pozwalających utrzymać funkcjonalność systemu w dynamicznie zmieniającym się środowisku pracy.
12. Przed dokonaniem zmian w systemie informatycznym należy dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych na testowej bazie danych na podobnych zasadach jak ma to miejsce w przypadku przeglądu oprogramowania.

BURMISTRZ
Krystyna Lewańska

Załącznik nr 3
do Zarządzenia nr 53/2012
Burmistrza Miasta i Gminy Frombork
z dnia 09 października 2012 r.

RO.142.3. ... .2012.DK

Upoważnienie do przetwarzania danych osobowych

Na podstawie art. 37 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.) oraz §4 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)

Upoważniam Panią/Pana: .....

Zatrudnioną/ zatrudnionego na stanowisku: .....

do dostępu do następujących zbiorów danych osobowych: .....

Ustalam Panu/ Pani następujący zakres odpowiedzialności za ochronę zbioru danych przed nieupoważnionym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem:

I. Zobowiązuję Pana/Panią do przestrzegania postanowień:
   - Polityki Bezpieczeństwa,
   - Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych.

II. Zobowiązuję Pana/Panią do stosowania przepisów ustawy przy przetwarzaniu danych osobowych w:
   - systemie informatycznym,
   - kartotekach,
   - skorowidzach,
   - księgach,
   - wykazach i innych zbiorach ewidencyjnych.

III. Zobowiązuję Pana/Panią do zachowania w tajemnicy danych osobowych w czasie zatrudnienia po ustaniu zatrudnienia:

.....
(Podpis Administratora Danych Osobowych)

.....
(Data i podpis pracownika)

Zobowiązanie pracownika:
Zobowiązuje się do zachowania w tajemnicy przetwarzanych danych osobowych i sposobów ich zabezpieczeń, zgodnie z art. 39 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), również po ustaniu stosunku pracy, oraz do przestrzegania instrukcji i procedur związanych z ochroną danych osobowych.

.....
Data i Podpis Pracownika

BURMISTRZ
Krystyna Lewańska

Załącznik nr 4
do Zarządzenia nr 53/2012
Burmistrza Miasta i Gminy Frombork
z dnia 09 października 2012 r.

RO.142.4. ... .2012.DK

Imię i nazwisko:

.....

Stanowisko pracy:

.....

OŚWIADCZENIE

Niniejszym oświadczam, że zapoznałem się z:

- ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz Rozporządzeniem 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)
- Polityką Bezpieczeństwa oraz Instrukcją Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych

i zobowiązuję się do ich przestrzegania.

.....
(Data i podpis pracownika)

BURMISTRZ
Krystyna Lewańska