Zarządzenie Nr 115/2007r.
Starosty Powiatu Wyszkowskiego
z dnia 08 października 2007r

w sprawie ustalenia „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Wyszkowie"

Na podstawie art. 34 ust. 1 ustawy z dnia 5 czerwca 1998r. o samorządzie powiatowym (Dz.U. z 2001r. Nr 142, poz. 1592 z późn. zm.) oraz § 3 ust. 3 oraz § 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 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 2004r.Nr 100, poz.1024)zarządza się, co następuje:

§ 1

Ustala się „Politykę bezpieczeństwa i instrukcję zarządzania system informatycznym służącą do przetwarzania danych osobowych w Starostwie Powiatowym w Wyszkowie" zwaną dalej „Polityką bezpieczeństwa", która stanowi załącznik do niniejszego zarządzenia.

§ 2

Zobowiązuje się pracowników Starostwa Powiatowego w Wyszkowie do stosowania zasad określonych w „Polityce bezpieczeństwa".

§ 3

Wykonanie zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji

§ 4

Nadzór nad wykonaniem i przestrzeganiem zapisów zawartych w Polityce bezpieczeństwa powierza się Sekretarzowi Powiatu.

§ 5

Zarządzenie wchodzi w życie z dniem podjęcia.

STAROSTA
Bogdan Pągowski

Załącznik
do zarządzenia Nr. 115
Starosty Powiatu Wyszkowskiego
z dnia 08 października 2007r.

Polityka bezpieczeństwa

Opracował : Andrzej Hubert Morka
Administrator Bezpieczeństwa Informacji

253

SPIS TREŚCI:

WPROWADZENIE

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych w Starostwie Powiatowym w Wyszkowie Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę Urzędu. Dokument zwraca uwagę na konsekwencje jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom informatycznym.

Dokument „Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Wyszkowie wskazujący sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w systemach informatycznych, przeznaczony jest dla osób zatrudnionych przy przetwarzaniu tych danych.

Potrzeba jego opracowania wynika z § 3 rozporządzenia Prezesa Rady Ministrów z dnia 25 lutego 1999 roku w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz.U. Nr 18 poz. 162) oraz § 3 i 4 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).

1. „Polityka bezpieczeństwa" określa tryb postępowania w przypadku, gdy:
   1) stwierdzono naruszenie zabezpieczenia systemu informatycznego,
   2) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci informatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.
2. „Polityka bezpieczeństwa" obowiązuje wszystkich pracowników Starostwa Powiatowego w Wyszkowie
3. Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemach informatycznych Urzędu.
4. Niniejszy dokument jest zgodny z następującymi aktami prawnymi:
   1) Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 103, poz. 929 z późn. zm.),
   2) Ustawą o ochronie informacji niejawnych z dnia 22 stycznia 1999 r. (Dz. U. Nr 11, poz. 95 z późn. zm.),
   3) Rozporządzeniem Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz. U. Nr 171, poz. 1433),

255

Definicje

- **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 z kilku specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne;
- **Zbiór danych osobowych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony (jego części znajdują się w różnych miejscach) lub podzielony funkcjonalnie (przetwarzany za pomocą programów realizujących różne funkcje);
- **Przetwarzanie danych osobowych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, udostępnianie i usuwanie; zwłaszcza takie, które wykorzystuje się w systemach informatycznych;
- **System informatyczny** – system przetwarzania informacji wraz ze związanymi z nimi ludźmi oraz zasobami technicznymi i finansowymi, które dostarcza i rozprowadza informacje. Systemem informacyjnym może być system, w którym nie będzie żadnego komputera, a wyłącznie dokumenty papierowe, skoroszyty oraz ludzie tam pracujący, wyposażenie pokoi, czy też organizacja pracy. Ochronie podlegają nie tylko informacje osobowe, ale także ludzie, zasoby techniczne i finansowe;
- **Bezpieczeństwo systemu informatycznego** – wdrożenie stosowanych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą;
- **Starostwo** - Starostwo Powiatowe w Wyszkowie.
- **Administrator Danych Osobowych** – organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych. Administratorem danych jest Starosta, który ponosi pełnię odpowiedzialności wynikającej z przepisów ustawy o ochronie danych osobowych w odniesieniu do zbiorów danych osobowych znajdujących się w jego ustawowej dyspozycji;
- **Administrator Bezpieczeństwa Informacji** – należy przez to rozumieć pracownika urzędu wyznaczonego przez Administratora Danych Osobowych do nadzorowania przestrzegania zasad ochrony oraz wymagań w zakresie ochrony, wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych;
- **Administrator Systemów Informatycznych** – należy przez to rozumieć pracownika lub pracowników Informatyki odpowiedzialnych za stosowanie technicznych i organizacyjnych środków ochrony danych osobowych,
- **Osoba upoważniona lub użytkownik systemu** – osoba posiadająca upoważnienie wydane przez Administratora Danych Osobowych lub osoba uprawniona przez niego i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej, w zakresie wskazanym w upoważnieniu, zwana dalej użytkownikiem;
- **Sieć Lokalna** – rozumie się przez to wewnętrzną sieć telekomunikacyjną,
- **Sieć rozległa** – rozumie się przez to zewnętrzną sieć publiczną,

- **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych, lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
- **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
- **Uwierzytelnienie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
- **Odbiorcy danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
  - osoby, której dane dotyczą,
  - osoby, upoważnionej do przetwarzania danych,
  - przedstawiciela, o którym mowa w art. 31a ustawy o ochronie danych osobowych,
  - podmiotu, o którym mowa w art. 31 ustawy o ochronie danych osobowych,
  - organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

ROZDZIAŁ I

ZASADY POSTĘPOWANIA PRZY PRZETWARZANIU DANYCH OSOBOWYCH

1. Administrator Danych Osobowych, którym jest Starosta, zarządzeniem wyznacza Administratora Bezpieczeństwa Informacji danych zawartych w systemach informatycznych Urzędu, zwanego dalej Administrator Bezpieczeństwa Informacji oraz osobę upoważnioną do jego zastępowania.
2. Administrator Bezpieczeństwa Informacji realizuje zadania w zakresie ochrony danych osobowych, a w szczególności:
   1) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Urzędu,
   2) podejmowania stosownych działań zgodnie z niniejszą „Polityką bezpieczeństwa" w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym,
   3) niezwłocznego informowania Administrator Danych Osobowych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
   4) nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.
3. Osoba zastępująca Administratora Bezpieczeństwa Informacji powyższe zadania realizuje tylko w przypadku jego nieobecności.
4. Osoba zastępująca składa Administratorowi Bezpieczeństwa Informacji relację z podejmowanych działań w czasie jego zastępstwa.
5. Pracownik upoważniony przez Administratora Danych Osobowych do przetwarzania danych osobowych, jest zobowiązany do:
   1) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych,
   2) stosowania określonych przez Administratora Danych Osobowych procedur i środków mających na celu zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym,
   3) zachowania szczególnej staranności w trakcie wykonywania operacji przetwarzania danych w celu ochrony interesów osób, których te dane dotyczą,
   4) podporządkowania się poleceniom Administratora Bezpieczeństwa Informacji oraz właściwego kierownika, w zakresie ochrony danych.
6. Czynności przetwarzania danych osobowych może dokonywać jedynie pracownik upoważniony przez Administratora Danych Osobowych. Wzór upoważnienia stanowi załącznik **Nr 1**.
7. Bezpośredni nadzór nad przetwarzaniem danych osobowych w wydziałach Starostwa sprawują kierownicy oraz naczelnicy tych wydziałów, a w przypadku pracowników na samodzielnych stanowiskach Starosta, Wicestarosta, Skarbnik – każdy w swoim pionie.
8. Naczelnicy wydziałów oraz stanowiska samodzielne w Starostwie są zobowiązani do:
   1) opracowania dla każdej osoby zatrudnionej przy przetwarzaniu danych osobowych zakresu czynności z uwzględnieniem stopnia dostępu do danych osobowych oraz przewidzenia odpowiedzialności, za naruszenie tajemnicy za danych, adekwatnej do zakresu obowiązków,
   2) sprawowanie nadzoru nad pracą podległych pracowników w zakresie wykonywania czynności służbowych w sposób zapewniający ochronę danych osobowych,

3) zwracania się do administratora danych o rozstrzygnięcie w przypadku istotnych wątpliwości co do stosowania - przepisów prawnych zakresu danych osobowych,
4) niezwłocznego zawiadomienia Administratora Danych Osobowych o konieczności utworzenia nowego zbioru danych osobowych, wymagającego rejestracji.

9. Pracownik, któremu Administrator Danych Osobowych udzielił upoważnienia, o którym mowa w ust. 3 jest zobowiązany do podpisania oświadczenia. Wzór oświadczenia stanowi załącznik **Nr 2.**
10. W przypadku zatrudnienia nowego pracownika, zmiany stanowiska, zmiany zakresu obowiązków pracowniczych, utworzenia nowego zbioru danych osobowych, zmiany sposobu przetwarzania danych lub w innych przypadkach, które wpływają bezpośrednio na rodzaj i zakres przetwarzania danych, bezpośredni przełożony jest zobowiązany bezzwłocznie skierować wniosek do administratora danych osobowych o wydanie lub cofnięcie upoważnienia. W przypadku samodzielnych stanowisk pracy cofnięcia lub wydania upoważnienia dokonuje administrator danych. Wzór pisma o cofnięciu upoważnienia stanowi załącznik **Nr 3.**
11. Wypowiedzenie umowy o pracę jest równoznaczne z cofnięciem upoważnienia do przetwarzania danych osobowych.
12. Naczelnik Wydziału Organizacyjnego i Spraw Społecznych przekazuje Administratorowi Bezpieczeństwa Informacji pisemna informację o rozwiązaniu umowy o pracę z pracownikiem posiadającym upoważnienie do przetwarzania danych osobowych.
13. W obiegu wewnętrznym między Wydziałami, referatami, a także pracownikami Starostwa wprowadza się następujące zasady udostępniania danych osobowych:
    1) informacje zawierające dane powszechnie dostępne może udostępnić pracownik przetwarzający dane w formie bezpośredniej lub telefonicznej, po sprawdzeniu tożsamości w procedurze „zwrotnej informacji telefonicznej",
    2) zgodę na udostępnienie danych osobowych w szerszym zakresie wyraża Starosta.
14. W obiegu zewnętrznym zgodę na udostępnienie danych osobowych wyraża administrator danych zgodnie z powszechnie obowiązującymi przepisami.
15. Obowiązek przestrzegania tajemnicy danych osobowych spoczywa na wszystkich pracownikach, którzy mają do nich dostęp, również po ustaniu stosunku pracy.
16. Administrator Danych Osobowych może przenieść obowiązek utrzymywania lub przetwarzania zbioru/zbiorów danych osobowych, na podmiot trzeci jednak musi się to odbyć za pośrednictwem stosownej umowy oraz z zachowaniem reguł bezpieczeństwa danych opisanych w niniejszym dokumencie.
17. Przetwarzanie danych osobowych sprzeczne z przepisami ustawy o ochronie danych osobowych może stanowić ciężkie naruszenie obowiązków pracowniczych.
18. Zbiory danych osobowych przetwarzane przez pracowników Starostwa nie będą udostępniane do celów komercyjnych.

Rozdział II

OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

1. Podział zagrożeń:
    1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu) – ich występowanie może prowadzić do utraty integralności danych, zniszczenia i uszkodzenia infrastruktury technicznej systemu, zakłócenia działania ciągłości systemu – nie dochodzi do naruszenia poufności danych,
    2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów,

administratora, awarie sprzętowe, błędy oprogramowania) – ich występowanie może doprowadzić do zniszczenia danych, zakłócenia ciągłość pracy systemu – może nastąpić naruszenie poufności danych,

3) zagrożenia zamierzone, świadome i celowe – najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

2. Naruszenie ochrony danych osobowych lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:
   1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
   2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
   3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
   4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
   5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
   6) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
   7) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
   8) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
   9) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,
   10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
   11) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki", itp.,
   12) podmieniono lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe,
   13) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).
3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze

(wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej itp.

Rozdział III

ZABEZPIECZENIE DANYCH OSOBOWYCH

1. Administratorem danych osobowych zawartych i przetwarzanych w systemach informatycznych Starostwa jest Starosta.
2. Administrator danych osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych Starostwa, a w szczególności:
   1) zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
   2) zapobiegać przed zabraniem danych przez osobę nieuprawnioną,
   3) zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.
3. Celem zapewnienia ochrony przetwarzania danych w systemach informatycznych Starostwa stosuje się następujące środki techniczne:
   1) ochrona strefy administracyjnej systemem alarmowym klasy 2,
   2) przetwarzanie danych osobowych następuje w wydzielonych pomieszczeniach położonych w strefie administracyjnej,
   3) zabezpieczenie wejść do pomieszczeń, o których mowa w pkt. 1 w drzwi opatrzone w zamki,
   4) szczególne zabezpieczenie centrum przetwarzania danych (komputer centralny, serwerownia) poprzez zastosowanie systemu kontroli dostępu,
   5) wyposażenie pomieszczeń w zamykane na klucz szafy dające gwarancję bezpieczeństwa dokumentacji.
4. Celem zapewnienia ochrony przetwarzania danych w systemach informatycznych Starostwa stosuje się następujące środki organizacyjne:
   1) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych,
   2) przeszkolenie osób, o których mowa w pkt. 1, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych,
   3) wyłączenie stref systemu alarmowego strefy administracyjnej przez upoważnione osoby,
   4) kontrolowanie otwierania i zamykania pomieszczeń, w których są przetwarzane dane osobowe, polegające na otwarciu pomieszczenia przez osobę upoważnioną, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę.
5. Niezależnie od niniejszych zasad opisanych w dokumencie „Polityka bezpieczeństwa" w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych osobowych w określonym systemie.
6. Wykaz zbiorów przetwarzanych elektronicznie stanowi załącznik **Nr 4.**
7. Opis struktur zbiorów danych załącznik **Nr 5.**
8. Wykaz pomieszczeń w których przetwarzane są dane osobowe oraz opis systemów informatycznych Starostwa i ich zabezpieczeń zawiera załącznik **Nr 6.**

Rozdział IV

KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Administrator danych Osobowych lub osoba przez niego wyznaczona, którą jest Administrator Bezpieczeństwa Informacji sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.
2. Administrator Bezpieczeństwa Informacji sporządza półroczne plany kontroli zatwierdzone przez Starostę i zgodnie z nimi przeprowadza kontrole oraz dokonuje kwartalnych ocen stanu bezpieczeństwa danych osobowych.
3. Na podstawie zgromadzonych materiałów, o których mowa w ust. 2, Administrator Bezpieczeństwa Informacji sporządza roczne sprawozdanie i przedstawia Administratorowi Danych Osobowych.

ROZDZIAŁ V

ŚRODKI TECHNICZNE I ORGANIZACYJNE PRZEWIDZIANE DO OCHRONY DANYCH ZAWARTYCH W SYSTEMACH INFORMAYCZNYCH

1. Środki organizacyjne:
   1) dostęp do danych osobowych mogą mieć tylko i wyłącznie pracownicy posiadający pisemne, imienne upoważnienia podpisane przez Administratora Danych Osobowych.
   2) każdy z pracowników powinien zachować szczególną ostrożność przy przetwarzaniu, przenoszeniu wszelkich danych osobowych,
   3) należy chronić dane przed wszelkim dostępem do nich osób nieupoważnionych,
   4) pomieszczenia, w których są przetwarzane dane osobowe, muszą być zamykane na klucz,
   5) dostęp do kluczy powinni posiadać tylko upoważnieni pracownicy,
   6) dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy urzędu; w wypadku, gdy jest wymagany poza godzinami pracy – możliwy jest tylko na podstawie pisemnego zezwolenia Administratora Danych Osobowych,
   7) dostęp do pomieszczeń, w których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy urzędu,
   8) w przypadku pomieszczeń do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych, i tylko w czasie wymaganym na wykonanie niezbędnych czynności,
   9) szafy w których przechowywane są dane osobowe muszą być zamykane na klucz.
   10) klucze do tych szaf powinni posiadać tylko upoważnieni pracownicy,
   11) szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych a następnie powinny być zamykane,
   12) dane osobowe w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych a następnie muszą być chowane do szaf.
2. Środki techniczne:
   1) dostęp do komputerów na których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy urzędu,

2) stacje komputerowe na których przetwarzane są dane osobowe powinny mieć tak ustawione monitory, aby nie miały wglądu w dane osoby nieupoważnione,
3) każdy plik, w którym są zawarte dane osobowe powinien być zabezpieczony hasłem jeśli nie jest to przetwarzanie danych w systemie informatycznym,
4) w przypadku przetwarzania danych osobowych na komputerach przenośnych (notebook) należy zachować szczególną ostrożność przy ich przewożeniu,
5) po zakończeniu pracy komputery (notebook) takie powinny być zabezpieczone w zamykanych na klucz szafach,
6) komputerów tych nie należy wynosić poza budynek,
7) w wypadku potrzeby wyniesienia (notebook-a) wcześniej należy dane osobowe przenieść na komputer stacjonarny w miejscu pracy,
8) nie należy udostępniać osobom nieupoważnionym tych komputerów,
9) w przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami należy dokonać tego z zachowaniem szczególnej ostrożności i za zgodą Administratora Bezpieczeństwa Informacji,
10) nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie), aby nie zostały na nich dane osobowe,
11) w wypadku niemożliwości skasowania danych z nośnika (płyta CD-ROM) należy taką płytę zniszczyć fizycznie,
12) w przypadku wykorzystania do przenoszenia dysków, dane należy kasować z tych dysków,
13) niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną,
14) sieć komputerowa powinna być zabezpieczona przed wszelkim dostępem z zewnątrz,
15) do zabezpieczenia sieci należy stosować:
    a) firewall – zaporę sprzętową lub programową uniemożliwiającą dostęp osób nieuprawnionych z zewnętrznej sieci,
    b) adresowanie stacji roboczych tylko adresami prywatnymi,
    c) systemy wykrywania włamań,
    d) logowanie wszelkich zdarzeń w dziennikach systemowych na serwerach,
    e) systemy antywirusowe,
    f) zabezpieczenia skrzynek poczty elektronicznej hasłami „trudnymi" (8 znaków w tym litery, cyfry, znaki dodatkowe),
    g) zabezpieczenie przed dostępem na zewnątrz ze stacji roboczych do innych usług niż strony internetowe,
    h) dostęp do poczty elektronicznej tylko na serwerach autoryzowanych przez Starostwo,
    i) zabezpieczenia stacji roboczych poprzez hasła na BIOS, w systemach MS Windows 2000, i XP poprzez użytkowników i hasła,
    j) zabezpieczenie wszelkich systemów teleinformatycznych hasłami „trudnymi" (8 znaków w tym litery, cyfry, znaki dodatkowe) zmienianymi raz na miesiąc,
    k) ustawienie odpowiednich poziomów dostępu dla odpowiednich użytkowników w systemach teleinformatycznych.

ROZDZIAŁ VI

INSTRUKCJA OKREŚLAJĄCA SPOSÓB ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM, SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH, ZE SZCZEGÓLNYM UWZGLĘDNIENIEM BEZPIECZEŃSTWA INFORMACJI

1. Określenie sposobu przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz wskazanie osoby odpowiedzialnej za te czynności.
   1) hasło nie powinno zawierać mniej niż 8 znaków,
   2) hasło nie może być takie samo jak identyfikator,
   3) hasło musi być zmieniane przynajmniej raz w miesiącu przez użytkownika, administratora bezpieczeństwa informacji lub automatycznie przez system,
   4) użytkownikowi nie wolno zapisywać hasła na papierze,
   5) użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności,
   6) komputery nie pracujące w sieci muszą mieć hasło założone na BIOS,
   7) w przypadku czasowego opuszczenia stanowiska pracy, użytkownik powinien wylogować się z systemu, lub po 5 minutach musi uruchomić się wygaszacz ekranu zabezpieczony hasłem,
   8) za gospodarkę hasłami odpowiedzialny jest administrator bezpieczeństwa informacji,
   9) hasło przy wpisywaniu nie może być wyświetlane na ekranie.
2. Określenie sposobu rejestrowania i wyrejestrowania użytkowników oraz wskazanie osoby odpowiedzialnej za te czynności.
   1) administrator bezpieczeństwa informacji prowadzi ewidencję osób upoważnionych do przetwarzania danych, zawierającą ich identyfikatory, wzór ewidencji stanowi załącznik **Nr 7,**
   2) rejestracji użytkowników w systemie dokonuje administrator bezpieczeństwa informacji, lub osoba przez niego upoważniona,
   3) zarejestrować można wyłącznie osoby, które administrator danych wpisał do ewidencji osób upoważnionych do przetwarzania danych,
   4) wyłączenie z ewidencji osób upoważnionych do przetwarzania danych, obliguje administratora bezpieczeństwa informacji do odebrania dostępu do danych osobowych,
   5) zalecane jest aby identyfikator składał się z pierwszej litery imienia i pierwszych pięciu liter nazwiska.
3. Procedury rozpoczęcia i zakończenia pracy
   1) Administrator Bezpieczeństwa Informacji w porozumieniu z Administratorem Danych Osobowych, ustala czas pracy użytkownikom systemu, na pracę poza godzinami funkcjonowania urzędu musi wyrazić zgodę na piśmie Administrator Danych Osobowych, w formie upoważnienia jednorazowego lub stałego,
   2) Administrator Bezpieczeństwa Informacji, lub osoba przez niego upoważniona, nadzoruje rozpoczęcie i zakończenie pracy systemu informatycznego,
   3) w pomieszczeniach gdzie przyjmowani są klienci , monitory powinny być tak ustawione, aby uniemożliwić osobie niepowołanej wgląd w dane,
   4) dopuszcza się pozostawianie włączonego serwera w nocy, jeżeli pomieszczenie w którym on pracuje wyposażone jest w sprawny system powiadamiania przeciw pożarowego, zasilacza awaryjnego oraz alarm antywłamaniowy.
   5) kontrola wprowadzanych danych prowadzona jest na bieżąco na każdym stanowisku

merytorycznym, nadzór prowadzi bezpośredni przełożony,
6) o przekazywaniu danych osobowych innym podmiotom decyduje Administrator Danych Osobowych,
7) osoby, których dane są przetwarzane powinny mieć możliwość zapoznania się, na tablicy ogłoszeń, z przysługującymi im prawami wynikającymi z ustawy o ochronie danych osobowych.

4. Metoda i częstotliwość tworzenia kopii awaryjnych
   1) za sporządzanie i bezpieczeństwo kopii odpowiedzialny jest Administrator Bezpieczeństwa Informacji, lub osoba przez niego upoważniona,
   2) kopii należy dokonywać poprzez przegrywanie całej bazy danych,
   3) w każdej chwili powinno być dostępnych jednocześnie pięć kopii: z ostatniego dnia, tygodnia, miesiąca, kwartału i roku; kopie dzienne i tygodniowe należy zapisywać na dysku twardym, dyskach CD lub DVD a pozostałe na taśmach magnetycznych,
   4) kopie awaryjne może tworzyć jedynie Administrator Bezpieczeństwa Informacji, lub osoba przez niego upoważniona,
   5) w czasie tworzenia kopii awaryjnej przez administratora, dostęp do bazy dla wszystkich użytkowników powinien być zablokowany,
   6) dyski wymienne z kopiami bezpieczeństwa powinny być wyjęte z komputera w czasie bieżącej pracy,
   7) Administrator Bezpieczeństwa Informacji wykonuje kopię awaryjną lub archiwizacje systemu wykorzystując jak najlepiej swoje umiejętności.
   8) Wprowadza się praktyczne zalecenia odnośnie do wykonania kopii bezpieczeństwa:
      a) przeprowadzić składowanie informacji regularnie,
      b) używać różnych typów nośników danych,
      c) kopie umieszczać w różnych, oddalonych od siebie miejscach,
      d) najlepiej do składowania wybrać tak nośnik, aby mógł w całości pomieścić kopie danych,
      e) przed składowaniem danych sprawdzić je programem antywirusowym,
      f) dokładnie opisywać składowane dane,
      g) trzymać nośniki z kopiami z daleka od źródeł pola magnetycznego i miejsc nasłonecznionych,
      h) sprawdzić, czy składowanie przebiegło prawidłowo,
      i) upewnić się, że nośnik jest niezależny od urządzenia, tzn. że dane mogą być przywrócone nie tylko na komputerze, z którego były poprawne,
      j) regularnie konserwować urządzenia do składowania.

5. Metody i częstotliwość sprawdzania obecności wirusów komputerowych oraz metody ich usuwania:
   1) za ochronę antywirusową odpowiedzialny jest Administrator Bezpieczeństwa Informacji,
   2) do ochrony antywirusowej należy stosować jednostanowiskowy program antywirusowy, zainstalowany na komputerze, gdzie odbierana jest poczta elektroniczna i sprawdzane są wszystkie dyskietki i płyty CD, przed ich uruchomieniem w sieci oraz na komputerach wolno stojących,
   3) sprawdzanie dostępnymi programami antywirusowymi odbywać się powinno przynajmniej raz w miesiącu,
   4) zalecane jest wykorzystanie programów pracujących w tle,
   5) przy kontroli szczególną uwagę należy zwrócić na makra,
   6) każdą przesyłkę otrzymaną za pomocą transmisji danych (e-mail, ftp) należy sprawdzić programem antywirusowym,
   7) korzystanie z zewnętrznych nośników informacji (dyskietek, dysków wymiennych,

płyt CD, Internetu, poczty elektronicznej) może mieć miejsce wyłącznie po uzyskaniu zgody Administratora Bezpieczeństwa Informacji,

8) w przypadku wykrycia wirusa choćby na jednym komputerze, należy sprawdzić wszystkie stacje robocze w starostwie.

6. Sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków:
   1) nie należy magazynować zbędnych plików i wydruków, kopie bezpieczeństwa po upływie okresu przechowywania muszą być skasowane, lub fizycznie zniszczone w sposób uniemożliwiający odczytanie danych,
   2) za zniszczenie zbędnych wydruków i innych dokumentów zawierających dane osobowe odpowiedzialny jest kierownik komórki organizacyjnej, za skasowanie danych, lub zniszczenie nośników elektronicznych, odpowiedzialny jest administrator bezpieczeństwa informacji,
   3) zbędne dokumenty konwencjonalne (papierowe) powinny być zniszczone w niszczarce dokumentów lub podarte na drobne fragmenty,
   4) kopie bezpieczeństwa powinny być przechowywane w zamkniętej metalowej szafie,
   5) kopie nie powinny być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowanych na bieżąco,
   6) kopie awaryjne sprawdza się pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu – co najmniej jednorazowo po przegraniu,
   7) wydruki należy przechowywać w pomieszczeniach, uniemożliwiających dostęp do nich przez osoby niepowołane,
   8) osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera, w celu zapobieżenia dostępowi do tych danych osobie niepowołanej, a w szczególności powinna zabezpieczyć dostęp do komputera hasłem i nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych, w szczególności komputera nie należy pozostawiać w samochodzie,
   9) kopie przechowuje się co najmniej:
      a) dzienne przez siedem dni,
      b) tygodniowe przez kolejny tydzień,
      c) miesięczne przez kolejny miesiąc,
      d) kwartalne przez kolejny kwartał,
      e) roczne przez cały kolejny rok od daty sporządzenia.

7. Przeglądu, konserwacji systemu i zbioru danych osobowych:
   1) przeglądu i konserwacji dokonuje Administrator Bezpieczeństwa Informacji, lub osoba przez niego upoważniona, przynajmniej dwa razy w roku,
   2) zasilacz awaryjny powinien zapewnić automatyczne zakończenie pracy i wyłączenie serwerów przy zaniku lub nadmiernym wahaniu napięcia – min. czas podtrzymania pracy wynosi 5 min,
   3) w przypadku przekazywania komputera z dyskiem lub innym nośnikiem danych osobowych do naprawy, należy nośnik zdemontować, zabezpieczyć dostęp hasłem lub dokonać naprawy w obecności osoby upoważnionej przez administratora danych, w przypadku przekazania nośnika innemu podmiotowi należy dane nieodwracalnie skasować,
   4) o wszelkich nieprawidłowościach, awariach, próbie lub naruszeniu bezpieczeństwa danych osobowych, użytkownik powinien niezwłocznie powiadomić Administratora Bezpieczeństwa Informacji,
   5) do wydzielonej sieci energetycznej zasilającej system komputerowy nie wolno

podłączać żadnych innych urządzeń (czajników elektrycznych, odkurzaczy, radioodbiorników),

6) zabronione jest dokonywanie napraw sprzętu komputerowego samodzielnie przez pracowników urzędu.

8. Sposób postępowania w zakresie komunikacji w sieci komputerowej:
   1) przy przydzielaniu uprawnień obowiązuje zasada „wszystko co nie jest dozwolone, jest zabronione",
   2) Administrator Bezpieczeństwa Informacji w porozumieniu z Administratorem Danych Osobowych określi zasoby dostępne dla każdego użytkownika,
   3) użytkownicy powinni być przydzielani do odpowiedniej grupy roboczej, automatycznie w procesie logowania,
   4) dostęp do serwerowi ma tylko Administrator Bezpieczeństwa Informacji i pracownicy upoważnieni przez Administratora Danych Osobowych,
   5) dostęp do konsoli serwera winien być zabezpieczony hasłem,
   6) Administrator Bezpieczeństwa Informacji winien monitorować pracę w sieci za pomocą dostępnego oprogramowania narzędziowego i plików *.log,
   7) w pomieszczeniu, gdzie ustawiony jest serwer powinien pracować tylko Administrator Bezpieczeństwa Informacji i osoby upoważnione przez Administratora Danych Osobowych,
   8) nie wolno instalować w sieci własnego oprogramowania bez zgody Administratora Bezpieczeństwa Informacji,
   9) nieupoważnieni użytkownicy nie powinni mieć dostępu do zasobów systemowych serwera, katalogów roboczych, danych i wolumenów z poziomu systemu operacyjnego,
   10) dostęp do archiwalnych plików pocztowych należy zabezpieczyć hasłem,
   11) wszystkie listy otrzymane pocztą elektroniczną należy przekazywać do kancelarii,
   12) w celu zwiększenia bezpieczeństwa transmisji danych osobowych należy stosować kryptografie,
   13) w czasie korzystania z Internetu za pośrednictwem linii komutowanej, końcówka powinna być fizycznie odłączona od sieci lokalnej,
   14) uczestnictwo w internetowych grupach dyskusyjnych dozwolone jest jedynie za zgodą Administratora Danych Osobowych,
   15) komunikacja w sieci lokalnej musi umożliwiać identyfikację pracujących użytkowników.

Rozdział VII

POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. W przypadku stwierdzenia naruszenia:
   1) zabezpieczenia systemu informatycznego,
   2) technicznego stanu urządzeń,
   3) zawartości zbioru danych osobowych,
   4) ujawnienia metody pracy lub sposobu działania programu,
   5) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
   6) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.)

   każda osoba zatrudniona przy przetwarzaniu danych osobowych jest obowiązana

niezwłocznie powiadomić o tym fakcie Administratora Bezpieczeństwa Informacji.

2. W razie niemożliwości zawiadomienia Administratora Bezpieczeństwa Informacji lub osoby przez niego upoważnionej, o naruszeniu ochrony danych osobowych należy powiadomić bezpośredniego przełożonego.
3. O naruszeniu ochrony danych osobowych mogą świadczyć w szczególności następujące symptomy:
   1) brak możliwości uruchomienia przez użytkownika aplikacji pozwalającej na dostęp do danych osobowych,
   2) brak możliwości zalogowania się do tej aplikacji,
   3) ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika aplikacji (np. brak możliwości wykonywania pewnych operacji normalnie dostępnych użytkownikowi) lub uprawnienia poszerzone w stosunku do normalnej sytuacji.
   4) wygląd aplikacji inny niż normalnie,
   5) inny zakres danych niż normalnie dostępny dla użytkownika – dużo więcej lub dużo mniej danych,
   6) znaczne spowolnienie działania systemu informatycznego,
   7) pojawienie się nie standardowych komunikatów generowanych przez system informatyczny,
   8) ślady włamania lub prób włamania do obszaru, w którym przetwarzane są dane osobowe,
   9) ślady włamania lub prób włamania do pomieszczeń, w których odbywa się przetwarzanie danych osobowych, w szczególności do serwerowni oraz do pomieszczeń, w których przechowywane są nośniki kopii awaryjnych,
   10) włamanie lub próby włamania do szafek, w których przechowywane są w postaci elektronicznej lub papierowej - nośniki danych osobowych,
   11) zagubienie lub kradzież nośnika danych osobowych,
   12) zagubienie lub kradzież nośnika, karty mikroprocesorowej, dyskietki, itp,
   13) kradzież sprzętu informatycznego, w którym przechowywane były dane osobowe.
   14) informacja z systemu antywirusowego o zainfekowaniu systemu informatycznego wirusami,
   15) fizyczne zniszczenie lub podejrzenie zniszczenia elementów systemu informatycznego przetwarzającego dane osobowe na skutek przypadkowych lub celowych działań albo zaistnienia siły wyższej,
   16) podejrzenie nieautoryzowanej modyfikacji danych osobowych przetwarzanych w systemie informatycznym.
4. Ujawnienie danych następuje gdy:
   1) stają się znane w całości lub części pozwalającej na określenie osobom nie uprawnionym tożsamości osoby, której dane dotyczą,
   2) dane zostały zagubione, pozostawione bez nadzoru poza obszarem bezpieczeństwa należy przeprowadzić postępowanie wyjaśniające, czy dane osobowe należy uznać za ujawnione.
5. Przypadki określone w ust. 4 wymagają przeprowadzenia postępowania wyjaśniającego które określi czy dane osobowe należy uznać za ujawnione.
6. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Bezpieczeństwa Informacji lub upoważnionej przez Administratora Danych Osobowych osoby, należy:
   1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
   2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu

zabezpieczenia miejsca zdarzenia,
3) zaniechać – o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
4) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
5) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
6) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
7) udokumentować wstępnie zaistniałe naruszenie,
8) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa Informacji lub osoby upoważnionej.

7. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych Administratora Bezpieczeństwa Informacji lub osoba go zastępująca:
1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Starostwa,
2) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
3) rozważa celowość i potrzebę powiadamia o zaistniałym naruszeniu Administratora Danych Osobowych lub Sekretarza Powiatu,
4) nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza Starostwa,
5) zapisać wszelkie informacje związane z danym zdarzeniem,
6) na bieżąco wygenerować i wydrukować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia,
7) przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby niepowołanej,
8) dokonać fizycznego odłączenia urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nie uprawnionej,
9) wylogować użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych,
10) dokonać zmiany hasła użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania.

8. Administrator Bezpieczeństwa Informacji dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego załącznik **Nr 8**, który powinien zawierać w szczególności:
1) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
2) określenie czasu i miejsca naruszenia i powiadomienia,
3) określenie okoliczności towarzyszących i rodzaju naruszenia,
4) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
5) wstępną ocenę przyczyn wystąpienia naruszenia,
6) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

9. Raport, o którym mowa w ust. 7, Administrator Bezpieczeństwa Informacji niezwłocznie przekazuje Administratorowi Danych Osobowych, a w przypadku jego nieobecności osobie uprawnionej.

10. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Administrator Bezpieczeństwa Informacji zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego

odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

11. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Sekretarza Powiatu, Administratora Bezpieczeństwa Informacji, Pełnomocnika ds. Ochrony Informacji Niejawnych.
12. Analiza, o której mowa w ust. 10, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

Rozdział VIII

MONITOROWANIE ZABEZPIECZEŃ

1. Prawo do monitorowania systemu zabezpieczeń posiadają, zgodnie z zakresem czynności:
   1) Administrator Danych Osobowych bądź upoważniona przez niego osoba,
   2) Administrator Bezpieczeństwa Informacji.

2. W ramach kontroli należy zwracać szczególna uwagę na:
   1) okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności do możliwości odtwarzania danych,
   2) kontrola ewidencji nośników magnetycznych,
   3) kontrola właściwej częstotliwości zmiany haseł .

Rozdział IX

SZKOLENIA

1. Wszyscy pracownicy Starostwa mają obowiązek brać udział w szkoleniach.
2. Szkolenie powinno dotyczyć:
   1) obowiązujących instrukcji wewnętrznych dotyczących ochrony danych osobowych, sposobu niszczenia wydruków i zapisów na nośnikach magnetycznych i optycznych,
   2) przedstawienie zasad ochrony danych osobowych dotyczących bezpośrednio wykonywanych obowiązków na stanowisku pracy.

Rozdział X

NISZCZENIE ZAPISÓW NA NOŚNIKACH MAGNETYCZNYCH

1. Nośniki magnetyczne przekazywane na zewnątrz powinny być pozbawione zapisów zawierających dane osobowe.
2. Niszczenie poprzednich zapisów powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika.
3. Poprawność przygotowania nośnika magnetycznego powinna być sprawdzona przez Administratora Bezpieczeństwa Informacji.
4. Uszkodzone nośniki magnetyczne przed ich wyrzuceniem należy fizycznie zniszczyć poprzez przecięcie, przełamanie itp.

Rozdział XI

ARCHIWIZACJA DANYCH

1. Dane systemów kopiowane są w systemie tygodniowym.
2. Kopie awaryjne danych zapisywanych w programach wykonywane są codziennie.
3. Odpowiedzialnym za wykonywanie kopii danych i kopii awaryjnych jest Administrator Bezpieczeństwa Informacji.
4. Na koniec danego miesiąca wykonywane są kopie bezpieczeństwa z całego programu przetwarzającego dane. Nośniki z kopiami bezpieczeństwa przechowywane są w kasie pancernej w pokoju wskazanym przez Administratora Danych Osobowych oraz skrytce bankowej.
5. Kopie awaryjne przechowywane są w kasie pancernej w pokoju wskazanym przez Administratora Danych Osobowych.
6. Dyskietki, na których zapisywane są kopie bezpieczeństwa są każdorazowo wymazywane i formatowane w taki sposób, by nie można było odtworzyć ich zawartości.
7. Płyty CD, DVD na których przechowuje się kopie awaryjne niszczy się w sposób mechaniczny tak, by nie można było użyć ich ponownie.
8. Administrator Bezpieczeństwa Informacji odpowiedzialny jest za dokonywanie wymiany kopii awaryjnych na aktualne.
9. Administrator Bezpieczeństwa Informacji dokonuje okresowej weryfikacji kopii bezpieczeństwa pod kątem ich przydatności.

Rozdział XII

POSTANOWIENIA KOŃCOWE

1. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.
2. Administrator Bezpieczeństwa Informacji zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych wg wzoru stanowiącego załącznik **nr 9** do niniejszego dokumentu.
3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym Administratora Bezpieczeństwa Informacji.
4. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia administratora bezpieczeństwa informacji nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
5. W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926), 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) oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych (Dz. U. Nr 100, poz. 1023).

6. Niniejsza „Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie wchodzi w życie z dniem podpisania przez Starostę.

STAROSTA
Bogdan Pągowski

222

Załącznik nr 1

U P O W A Ż N I E N I E Nr.....

Na podstawie art.37 ustawy z dnia 29 sierpnia 1999 r. o ochronie danych osobowych (Dz.U.Nr 133 poz.883 z późn.zm.)

u p o w a ż n i a m

.....
/imię i nazwisko/

zatrudnionego na stanowisku.....

do przetwarzania danych osobowych oraz do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych

w.....
/nazwa jednostki organizacyjnej/

Upoważnienie wydaje się na czas nieokreślony.

.....
Administrator Danych Osobowych

STAROSTA
Bogdan Pagowski

Załącznik nr 2

.....
/imię i nazwisko pracownika/

.....

.....
/adres zamieszkania/

OŚWIADCZENIE

1. Stwierdzam własnoręcznym podpisem, że znana jest mi treść przepisów :
   a) o ochronie tajemnic prawnie chronionych stanowiących tajemnicę służbową wynikającą z Kodeksu Pracy,
   b) o ochronie danych osobowych wynikająca z ustawy o ochronie danych osobowych (Dz. U. Nr 133, poz. 833 z późn. zm.),
   c) o odpowiedzialności karnej za naruszenie ochrony danych osobowych.

2. Zobowiązuję się nie ujawniać wiadomości, z którymi zapoznałem/am się w trakcie wykonywanych czynności służbowych .

.....
(podpis pracownika)

.....
(podpis złożono w obecności)

STAROSTA
Bogdan Pągowski

Załącznik nr 3

Wycofanie upoważnienia

Na podstawie art. 37 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)
w związku:
.....
.....
.....

cofam upoważnienie

Pana/Pani .....
zatrudnionego/zatrudnionej w.....
.....
na stanowisku .....
.....

do przetwarzania danych osobowych, wynikającego z zakresu obowiązków pracowniczych.

Wyszków, dnia .....

.....
Administrator Danych Osobowych

STAROSTA
Bogdan Pągowski

Załącznik nr 4

Wykaz zbiorów przetwarzanych elektronicznie.

Lp.	Nazwa zbioru	Program zastosowany do przetwarzania	Nazwa urządzenia, w którym znajdują się dane osobowe
1	Komputerowy system rejestracji pojazdów	Pojazd , Kierowca	Serwer
2	Powiatowy zasób Geodezyjny i kartograficzny	Ośrodek	Serwer
3	Ewidencja gruntów i budynków m. Wyszków, Gm. Wyszków, Zabrodzie, Somianka, Długosiodło, Brańszczyk	Ośrodek	Serwer

STAROSTA
Bogdan Pągowski

Załącznik nr 5

1. Zbiór danych „Komputerowy system rejestracji pojazdów" zawiera następujące pola:

• imiona i nazwiska,
• numer PESEL,
• seria i numer dowodu osobistego
• adres zamieszkania lub pobytu

2. Zbiór danych „Powiatowy zasób Geodezyjny i Kartograficzny" zawiera następujące pola:

• imiona i nazwiska,
• imiona rodziców,
• adres zamieszkania lub pobytu,

3. Zbiór danych „Ewidencja gruntów i budynków m. Wyszków, Gm. Wyszków, Zabrodzie, Somianka, Długosiodło, Brańszczyk" zawiera następujące pola:

• imiona i nazwiska,
• imiona rodziców
• PESEL
• adres zamieszkania lub pobytu,

4. Zbiór danych „Ewidencja rozpoczynanych i oddawanych do użytkowania obiektów budowlanych" zawiera następujące pola:

• imiona i nazwiska,
• imiona rodziców
• numer i seria dowodu osobistego
• adres zamieszkania lub pobytu,

5. Zbiór danych „Ewidencja pozwoleń na budowę" zawiera następujące pola:

• imiona i nazwiska,
• imiona rodziców
• numer i seria dowodu osobistego
• adres zamieszkania lub pobytu,

6. Zbiór danych „Zmiana imion i nazwisk" zawiera następujące pola:

• imiona i nazwiska,
• imiona rodziców
• data urodzenia
• numer i seria dowodu osobistego
• adres zamieszkania lub pobytu,

• miejsce pracy
• zawód
• wykształcenie

7. Zbiór danych „Ewidencja pozwoleń wodno-prawnych" zawiera następujące pola:

• imiona i nazwiska,
• adres zamieszkania lub pobytu,

8. Zbiór danych „Ewidencja kart wędkarskich" zawiera następujące pola:

• imiona i nazwiska,
• numer i seria dowodu osobistego
• adres zamieszkania lub pobytu,

STAROSTA
Bogdan Pągowski

Załącznik nr 6

Wykaz pomieszczeń lub części pomieszczeń w których przetwarzane są dane.

Lp.	Nr pokoju	Wydział/ Referat/Sam. Stanowisko	Określenie części pomieszczenia, w którym przetwarza się lub archiwizuje dane
Budynek: Starostwo Powiatowe w Wyszkowie, ul. Aleja Róż 2 07-200 Wyszków			
1	15-18	Wydział Komunikacji	Nie dotyczy
2	20-25	Wydział Geodezji i Gospodarki Nieruchomościami	Nie dotyczy
3	20-25	Wydział Geodezji i Gospodarki Nieruchomościami	Nie dotyczy
4	27	Wydział Architektoniczno - Budowlany	Nie dotyczy
5	27	Wydział Architektoniczno - Budowlany	Nie dotyczy
6		Wydział Organizacyjny i Spraw Społecznych	Nie dotyczy
Budynek: Starostwo Powiatowe w Wyszkowie, ul. Aleja Róż 1 07-200 Wyszków			
7	4	Wydział Ochrony Środowiska i Rolnictwa	Nie dotyczy
8	4	Wydział Ochrony Środowiska i Rolnictwa	Nie dotyczy

STAROSTA
Bogdan Pągowski

Załącznik nr 7

Ewidencja osób upoważnionych do przetwarzania danych osobowych.

Nazwisko i Imię	Komórka organizacyjna	Data, podpis

STAROSTA
Bogdan Pągowski

Załącznik nr 8

R a p o r t
z naruszenia bezpieczeństwa systemu informatycznego
w Starostwie Powiatowym w Wyszkowie

1. Data: ..... Godzina: .....

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....
Imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje)

3. Lokalizacja zdarzenia:

.....
nr pokoju, nazwa pomieszczenia

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....
.....

5. Podjęte działania:

.....
.....

6. Przyczyny wystąpienia zdarzenia:

.....
.....

7. Postępowanie wyjaśniające:

.....
.....

STAROSTA
Bogdan Pągowski

.....
data, podpis Administratora Bezpieczeństwa Informacji

231

Załącznik nr 9

Wykaz osób, które zostały zapoznane i zobowiązują się do stosowania „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Wyszkowie" .

Nazwisko i Imię	Komórka organizacyjna	Data i podpis

STAROSTA
Bogdan Pągowski