

**ZARZĄDZENIE NR 48/2012
WÓJTA GMINY BORONÓW
z dnia 12 kwietnia 2012 r.**

w sprawie ustalenia polityki bezpieczeństwa danych osobowych w Urzędzie Gminy Boronów oraz przyjęcia instrukcji zarządzania systemem informatycznym.

Na podstawie: art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926, ze zm.) oraz § 3 ust. 3, § 4, § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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) zarządza się, co następuje:

§ 1

Ustala się „Politykę Bezpieczeństwa Danych Osobowych w Urzędzie Gminy Boronów” zwaną dalej „Polityką”, oraz „Instrukcję Zarządzania Systemem Informatycznym”, zwaną dalej „Instrukcją”, które stanowią załączniki do niniejszego zarządzenia.

§ 2

Zobowiązuje się pracowników Urzędu Gminy Boronów do stosowania zasad określonych w „Polityce” i „Instrukcji”

§ 3

Wszyscy pracownicy mają obowiązek zapoznać się z wymogami bezpieczeństwa zawartymi w „Polityce” oraz „Instrukcji” w ciągu 2 tygodni od wejścia w życie niniejszego zarządzenia. Zapoznanie się z wymogami bezpieczeństwa pracownik potwierdza podpisem.

§ 4

Wykonanie zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT

mgr Ruffin Majchrzyk

Załącznik Nr 1
do Zarządzenia nr 48/2012
Wójta Gminy Boronów
z dnia 12 kwietnia 2012 r.

Polityka bezpieczeństwa danych osobowych w Urzędzie Gminy Boronów

1. Wstęp

W systemie Urzędu Gminy Boronów przetwarzane są informacje stanowiące dane osobowe w rozumieniu art. 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Z 2002 r. Nr 101, poz. 926 z późn. zm.). Osobą odpowiedzialną za właściwy i niezakłócony przebieg przetwarzania danych w tym systemie jest Administrator Bezpieczeństwa Informacji.

2. Definicje

- a. Urząd – w tym dokumencie jest rozumiany, jako Urząd Gminy Boronów, z siedzibą w Boronowie, ul. Dolna 2
- b. Administrator Bezpieczeństwa Informacji (ABI) – pracownik urzędu wyznaczony przez Administratora Danych Osobowych (Wójta) do nadzorowania przestrzegania zasad ochrony danych osobowych, oraz przygotowania dokumentów wymaganych przez przepisy ustawy o ochronie danych osobowych w Urzędzie Gminy Boronów. Powołany zarządzeniem Wójta Gminy Boronów
- c. Użytkownik systemu – osoba upoważniona do przetwarzania danych osobowych w systemie. Użytkownikiem może być osoba zatrudniona w urzędzie, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w urzędzie.
- d. Identyfikator użytkownika – jest to ciąg znaków jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
- e. Administrator systemu informatycznego – pracownik odpowiedzialny za funkcjonowanie systemu teleinformatycznego, oraz stosowanie technicznych i organizacyjnych środków ochrony stosowanych w tym systemie. Powołany zarządzeniem Wójta Gminy Boronów.
- f. Sieć lokalna – połączenie komputerów pracujących w urzędzie w celu wymiany danych (informacji) dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych.
- g. Sieć publiczna – sieć telekomunikacyjna, niebędąca siecią wewnętrzną służąca do świadczenia usług telekomunikacyjnych w rozumieniu ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.).
- h. Sieć telekomunikacyjna – urządzenia telekomunikacyjne zestawione i połączone w sposób umożliwiający przekaz sygnałów pomiędzy określonymi zakończeniami sieci za pomocą przewodów, fal radiowych, bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną w rozumieniu ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne (Dz. U. Nr 73, poz.852, z późn. zm.).
- i. System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
- j. Przetwarzanie danych – rozumie się to w tym dokumencie jako jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.
- k. Zabezpieczenie danych w systemie informatycznym – wdrożenie i wykorzystywanie stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
- l. Teletransmisja – przesyłanie informacji za pomocą sieci telekomunikacyjnej.

- m. Poufność danych – jest to właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.
- n. Integralność danych – właściwość zapewniająca, że dane osobowe nie zostały zmienione, lub zniszczone w sposób nieautoryzowany.
- o. Rozliczalność – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
- p. Aplikacja – program komputerowy wykonujący konkretne zadanie.
- r. Wysoki poziom bezpieczeństwa – musi występować wtedy, gdy przynajmniej jedno urządzenie systemu informatycznego, służące do przetwarzania danych osobowych, połączone jest z siecią publiczną.
- s. Komórka organizacyjna – rozumie się przez to referat, samodzielne stanowisko pracy.

3. Obowiązki Administratora Bezpieczeństwa Informacji

- a. Przeciwdziałanie dostępowi osób niepowołanych do przetwarzania danych osobowych.
- b. Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych.
- c. Kontrola nad danymi osobowymi wprowadzanymi do zbiorów, (przez kogo zostały wprowadzone, komu są przekazywane).
- d. Podejmowanie odpowiednich działań w przypadku wykrycia naruszeń, lub podejrzenia naruszenia zabezpieczeń.
- e. Nadzór nad naprawami, konserwacją, oraz likwidacją urządzeń, na których zapisane są dane osobowe.
- f. Nadzór nad obiegiem, oraz przechowywaniem dokumentów zawierających dane osobowe.
- g. Nadzór nad prawidłowością archiwizacji, oraz usuwania danych osobowych.
- h. Monitorowanie zabezpieczeń wdrożonych w celu ochrony danych osobowych.
- i. Nadzór nad prowadzeniem odpowiedniej dokumentacji.

4. Obszar przetwarzania danych osobowych

Dane osobowe przetwarzane są w budynku Urzędu Gminy w Boronowie, ul. Dolna 2, 42-283 Boronów

5. Wykaz zbiorów danych osobowych przetwarzanych w systemie informatycznym Urzędu.

W systemie zbierane są dane zawierające informacje o osobach będących klientami i pracownikami urzędu. Dane te tworzą następujące zbiory:

1. Zbiór decyzji, postanowień i wszczęć postępowań dotyczących rozgraniczenia nieruchomości zawierający: imię i nazwisko, adres, nr działki, nr mapy, nr księgi wieczystej
2. Zbiór aktów notarialnych zawierający: imię i nazwisko, adres, nr mapy, nr księgi wieczystej.
3. Zbiór postanowień o nabyciu spadku zawierający: imię i nazwisko, adres, nr księgi wieczystej.
4. Zbiór postanowień o zasiedzeniu nieruchomości zawierający: imię i nazwisko, adres, nr działki, nr księgi wieczystej.

5. Zbiór porozumień w sprawie odszkodowań za nieruchomości zawierający: imię i nazwisko, adres, nr działki, nr księgi wieczystej.
6. Zbiór wypisów z planu zagospodarowania przestrzennego zawierający: imię i nazwisko, adres, nr działki, nr mapy.
7. Zbiór decyzji o ustaleniu opłaty planistycznej zawierający: imię i nazwisko, adres, nr działki, nr mapy, nr księgi wieczystej.
8. Zbiór decyzji o ustaleniu opłaty adiacenckiej zawierający: imię i nazwisko, adres, nr działki.
9. Zbiór zawiadomień o nadaniu numeru porządkowego nieruchomości zawierający: imię i nazwisko, adres, nr działki, nr mapy.
10. Zbiór wniosków o zmianę przeznaczenia nieruchomości w planie zagospodarowania przestrzennego zawierający: imię i nazwisko, adres, nr działki.
11. Zbiór decyzji na budowę, rozbudowę, zmianę sposobu użytkowania budynku zawierający: imię i nazwisko, adres, nr działki, nr mapy.
12. Zbiór zawiadomień o zakończeniu budowy zawierający: imię i nazwisko, adres, nr działki.
13. Ewidencja gruntów i budynków zawierająca: imię i nazwisko, adres, nr działki, nr mapy, nr księgi wieczystej, PESEL, NIP, imię ojca, imię matki, obywatelstwo, płeć.
13. Zbiór dokumentów dotyczący wycinki drzew i krzewów zawierający: imię i nazwisko, adres, nr działki.
14. Zbiór dokumentów dotyczący Programu Ograniczenia Niskiej Emisji na terenie Gminy Boronów zawierający: imię i nazwisko, adres, NIP, seria i nr dowodu osobistego.
15. Wykaz osób podlegających obowiązkowi szkolenia w zakresie powszechnej samoobrony zawierający: imię i nazwisko, rok urodzenia, adres zamieszkania.
16. Ewidencja osób wyznaczonych do pełnienia służby w formacjach obrony cywilnej - zawierająca: imię i nazwisko, imię ojca, stopień wojskowy, data urodzenia, adres zamieszkania, stanowisko w FOC, nr karty przydziału.
17. Zbiór umów z organizacjami pozarządowymi zawierający: Imię i nazwisko, seria i numer dowodu osobistego, nr telefonu osób uprawnionych do reprezentowania podmiotu.
18. Dziennik korespondencyjny (pocztą przychodząca i wychodząca) zawierający: imię i nazwisko, adres.
19. Ewidencja działalności gospodarczej zawierająca: imię i nazwisko, adres zamieszkania, miejsce działalności, PESEL, NIP, REGON, seria dowodu osobistego, obywatelstwo.
20. Płatnicy podatku od środków transportowych, zawiera: imię i nazwisko, data urodzenia, adres zamieszkania.

21. Płatnicy podatku od nieruchomości, zawiera : imię i nazwisko, NIP, PESEL, imiona rodziców, adres, numery klasy i powierzchnie działek, data urodzenia.

22. Akcyza, zawiera: imię nazwisko, NIP, PESEL, adres, imiona rodziców, data urodzenia, nr konta bankowego, powierzchnia gruntów.

23. Należności przypisane(czynsze dzierżawy, użytkowanie wieczyste, zbycie nieruchomości, opłaty adiacenckie, renty planistyczne, reklama), zawiera: imię nazwisko, NIP, PESEL, adres, imiona rodziców, data urodzenia, nr działek.

24. Zbiór wniosków i decyzji w sprawie pomocy materialnej dla uczniów o charakterze socjalnym – stypendia szkolne zawierający: imię i nazwisko, adres, data urodzenia, wysokość dochodów.

25. Zbiór osób wynajmujący lokale komunalne zawierający: imię nazwisko, adres zamieszkania, nr dowodu osobistego, PESEL.

26. Akta urzędu stanu cywilnego – zawierają:

Nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, PESEL, miejsce pracy, zawód, wykształcenie, seria i numer Dowodu osobistego, nazwisko rodowe, nazwisko z poprzedniego małżeństwa, miejsce i godzina urodzenia, data i numer aktu zgonu, data i numer aktu małżeństwa, data i numer aktu urodzenia, imię i nazwisko ojca, imię i nazwisko matki, imię i nazwisko współmałżonka , płeć, stan cywilny data i miejsce zawarcia małżeństwa, miejsc wystawienia i numer aktu urodzenia żony/męża, data i godzina miejsce zgonu, odnalezienia zwłok , data zgonu męża, nazwisko imię adres osoby zgłaszającej zgon, numer aktu zgonu żony/męża, nazwisko i imię rodowe małżonka, nazwisko rodowe matki i ojca mężczyzny, nazwisko rodowe matki i ojca kobiety, adnotacja o rozwodzie, nazwisko po zawarciu małżeństwa mężczyzny i kobiety, , numer dowodu i miejsce wydania dowodu mężczyzny i kobiety, PESEL, data unieważnienia aktu , małżeństwa, urodzenia zgonu, imię nadane z urzędu, data i numer orzeczenia z sądu ustalającego ojcostwo/ zaprzeczającego ojcostwo/przysposabiającego dziecko, imię i nazwisko osoby przysposabiającej dziecko, zmiana nazwiska dziecka, data rozwiązania poprzedniego małżeństwa/ rozwodu.

27. Ewidencja ludności Gminy Boronów i dowody osobiste:

Nazwiska i imiona, nazwisko rodowe imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, seria i numer dowodu osobistego, płeć, wzrost w cm, kolor oczu, fotografia, kod pocztowy, kod terytorialny.

28. Dane osobowe pracowników Urzędu Gminy w Boronowie, zawierają:

Imię i nazwisko, data i miejsce urodzenia, imiona rodziców, nazwisko rodowe matki, PESEL, NIP, stopień wojskowy i nr książeczki wojskowej, miejsce zamieszkania lub zameldowania/adres do korespondencji, nr telefonu, wykształcenie i dodatkowe uprawnienia, nr i seria dowodu osobistego, dane dotyczące niepełnosprawności, zajmowane stanowisko, orzeczenie lekarskie o dopuszczeniu (lub nie) na danym stanowisku., nr konta bankowego.

29. Dane osobowe kandydatów do pracy, stażystów i osób odbywających praktyki zawodowe, zawierają:

Imię i nazwisko, data i miejsce urodzenia, imiona rodziców, nazwisko rodowe matki, PESEL, NIP, stopień wojskowy i nr książeczki wojskowej, miejsce zamieszkania lub zameldowania/adres do korespondencji, nr telefonu, wykształcenie i dodatkowe uprawnienia, nr i seria dowodu osobistego, dane z rejestru bezrobotnych i poszukujących pracy.

30. Zbiór osób z dostępem do informacji niejawnych zawierający:

Imiona i nazwisko, nazwisko rodowe, data i miejsce urodzenia, PESEL, NIP, adres zamieszkania i zameldowania, nr i seria dowodu osobistego, paszportu oraz wojskowego dokumentu tożsamości, miejsce zatrudnienia lub prowadzenia firmy wraz z adresem i zajmowanym stanowiskiem, informacja o karalności, informacja o indagowaniu przez obce władze lub służby, kontakty prywatne i służbowe z obywatelami innych państw, stan zdrowia, sytuacja majątkowa

31. Zbiór uczniów dowożonych do szkół zawierający:

Imię i nazwisko ucznia dowożonego oraz jego rodziców, adres zamieszkania, data urodzenia, orzeczenie o niepełnosprawności

32. Kontrola spełniania obowiązku nauki, zawiera:

Imię i nazwisko ucznia, imię i nazwisko rodziców, data urodzenia lub PESEL, adres zamieszkania.

33. Dofinansowania kształcenia młodocianych, zawiera:

Dane dotyczące pracodawców – nazwa i adres firmy, NIP, PESEL, REGON, imię i nazwisko, data i miejsce urodzenia, wykształcenie i uprawnienia prowadzącego naukę zawodu;

Dane dotyczące młodocianych – imię i nazwisko, data i miejsce urodzenia, PESEL, adres zamieszkania, wykształcenie.

34. Dotowanie niepublicznych szkół i placówek oświatowych, zawiera:

Dane osoby prowadzącej placówkę – imię i nazwisko, adres zamieszkania, numer telefonu

Wykaz kadry pedagogicznej – imię i nazwisko, wykształcenie, data i miejsce urodzenia

Dane wychowanków – imię i nazwisko, data urodzenia, adres zamieszkania.

35. Zbiór radnych Gminy Boronów zawierający:

Imię i nazwisko, adres, data urodzenia, NIP, PESEL, nr telefonu, adres e-mail, wykształcenie.

36. Zbiór sołtysów Gminy Boronów zawierający:

Imię i nazwisko, adres, numer telefonu.

37. Kwalifikacja wojskowa, zawiera:

Imię i nazwisko, nazwisko rodowe, imiona i nazwiska rodowe rodziców, imiona i nazwiska poprzednie, data i miejsce urodzenia, stan cywilny, PESEL, adres i data zameldowania na pobyt stały, stopień wojskowy, nazw seria i numer wojskowego dokumentu osobistego, oznaczenie WKU w ewidencji której osoba pozostaje, kategoria zdrowia.

38. Rejestr wyborców zawierający:

Nazwisko imiona, PESEL, imię ojca, data urodzenia, adres stałego zamieszkania adres zameldowania, nazwa i adres miejscowości /lub okręg wyborczy w którym wyborca umieszczony jest w rejestrze wyborców przypisanie do danego okręgu i obwodu.

39. Oświadczenia majątkowe zawierające:

Imię i nazwisko, data urodzenia, adres zamieszkania, Pesel, NIP, miejsce pracy.

40. Plany urządzenia lasów niepaństwowych zawierające: Imię i nazwisko, nr działki, adres zameldowania.

41. System Informacji Oświatowej -Nauczyciele, wychowawcy i inni pracownicy pedagogiczni placówek oświatowych zawierający: PESEL, miejsce pracy, zawód, wykształcenie, stopień awansu zawodowego, płeć, stanowisko, funkcja, informacje dotyczące wynagrodzenia, staż pracy, wymiar etatu.

42. Awans zawodowy nauczycieli zawiera:

Imię i nazwisko, data i miejsce urodzenia, PESEL, wykształcenie, adres zamieszkania, nr telefonu, miejsce pracy.

43.Odprowadzenie ścieków i dostarczanie wody, zawiera: Imię i nazwisko, adres zameldowania.

44. Elektroniczny obieg dokumentów, zawiera: Imię i nazwisko, adres, nr telefonu

W skład systemu wchodzi:

- a. Dokumentacja papierowa (korespondencja obywateli, firm, innych instytucji publicznych i niepublicznych, formularze zgody na przetwarzanie danych osobowych itd.)
- b. Urządzenia i oprogramowanie komputerowe służące do przetwarzania informacji oraz procedury przetwarzania danych w tym systemie, w tym procedury awaryjne.
- c. Wydruki komputerowe.
- d. Do przetwarzania danych osobowych w systemie informatycznym urzędu stosuje się aplikacje:

System Adas - firmy Tensoft ,

System BDMB FK i Plan firmy BDMB Systemy Informatyczne,

Yuma Kadry Płace - firmy YUMA sp. z o.o. ,

Płatnik - firmy Asseco Poland SA – dostarczane przez Zakład Ubezpieczeń Społecznych,

Besti@ firmy Sputnik Software – dostarczane przez RIO,

SIO – dostarczany przez Ministerstwo Edukacji Narodowej,

System GW-MAX firmy Giga sp. z o.o.,

Selwin, Uscwin, Rwwin firmy Aram sp. z o.o.,

System Wydawania Dowodów Osobistych firmy Wasko S.A. dostarczone przez MSWiA

HomeNet firmy SoftNet – oprogramowanie do przelewów dostarczone przez Bank Spółdzielczy

IntraDOK firmy Wasko S.A.

Przepływy między systemami:

Skąd	Dokąd	Kierunek przepływu danych osobowych	Sposób przesyłania danych osobowych
Systemy BDMB	Bestia	=>	eksport/import pliku
SELWIN	USCWIN	=>	eksport/import pliku
USCWIN	Główny Urząd Statystyczny	=>	transmisja bezpośrednio z programu lub poprzez dedykowany do tego portal GUS
SELWIN	Portal Informacyjny Administracji	<=>	eksport/import pliku poprzez portal MSWiA
System ADAS	Główny Urząd Statystyczny	=>	eksport pliku poprzez portal GUS

Pozostałe programy działają niezależnie w oparciu o własne bazy danych i nie posiadają wbudowanego mechanizmu umożliwiającego przepływ danych osobowych między innymi systemami informatycznymi stosowanymi w Urzędzie Gminy Boronów.

6. Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i wyścizalności danych przetwarzanych w systemie

a. Środki ochrony fizycznej

Urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych zamkami patentowymi. Dostęp do pokoi jest kontrolowany za pomocą wydawania kluczy tylko osobom uprawnionym. Zastosowano szafę stalową do przechowywania nośników z kopiami zapasowymi zawierających dane osobowe.

b. Środki sprzętowe, informatyczne i telekomunikacyjne

Stosuje się niszczarki dokumentów.

Urządzenia wchodzące w skład infrastruktury sieciowej, serwera oraz komputery, na których przetwarzane są dane osobowe podłączone są do lokalnych awaryjnych zasilaczy UPS, zabezpieczających przed skokami napięcia i zanikiem zasilania.

Sieć lokalna skonfigurowana jest w topologii gwiazdy.

Sieć lokalna podłączona jest do Internetu poprzez router spełniający jednocześnie funkcję sprzętowego, zewnętrznego firewalla filtrującego dane przechodzące pomiędzy siecią lokalną i siecią publiczną.

Kopie zapasowe wykonywane są zgodnie z instrukcją zarządzania systemem informatycznym.

c. Środki ochrony w ramach oprogramowania urządzeń teletransmisji:

Na komputerach użytkowników systemu działa program antywirusowy.

Na komputerach użytkowników systemu działa programowy firewall.

Dostęp do komputerów i serwerów zawierających dane osobowe zabezpieczony jest hasłem.

d. Środki ochrony w ramach oprogramowania systemu:

Dostęp do baz danych osobowych zastrzeżony jest wyłącznie dla uprawnionych pracowników.

System informatyczny pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu odrębnie dla każdego pracownika. Zastosowano działający w tle program antywirusowy na komputerach użytkowników.

e. Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych.

Zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji. Dla każdego użytkownika systemu wyznaczony jest odrębny identyfikator. Użytkownicy mają dostęp do aplikacji umożliwiający dostęp tylko do tych danych osobowych, do których mają uprawnienia.

f. Środki ochrony w ramach systemu użytkowego.

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

g. Środki organizacyjne.

Wyznaczono Administratora Bezpieczeństwa Informacji. Tymczasowe wydruki z danymi osobowymi są po ustaleniu ich przydatności niszczone. Do przetwarzania danych osobowych przy użyciu systemu informatycznego dopuszczane są osoby na podstawie indywidualnego pozwolenia na dostęp do przetwarzania danych osobowych wydawanego przez Administratora Danych Osobowych.

Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane są do zachowania ich w tajemnicy.

Osoby przetwarzające dane osobowe są przed dopuszczeniem ich do tych danych szkolone w zakresie obowiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych osobowych w systemie informatycznym.

Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.

Ustalono Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych.

Zdefiniowano procedury postępowania w sytuacji naruszenia ochrony danych osobowych.

W przypadku, gdy zachodzi konieczność naprawy sprzętu poza siedzibą urzędu, należy wymontować z niego nośniki informacji zawierające dane osobowe.

7. Procedura postępowania w przypadku naruszenia ochrony danych osobowych

a. Każdy pracownik urzędu, który stwierdzi fakt naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe, bądź posiada informację mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany niezwłocznie zgłosić to Administratorowi Bezpieczeństwa Informacji.

b. W razie braku możliwości zawiadomienia Administratora Bezpieczeństwa Informacji lub osoby przez niego upoważnionej, należy zawiadomić bezpośredniego przełożonego

c. Do czasu przybycia na miejsce Administratora Bezpieczeństwa Informacji należy:

- niezwłocznie podjąć czynności niezbędne do powstrzymania skutków naruszenie ochrony (o ile to możliwe),
- ustalić przyczynę i sprawcę naruszenia ochrony, rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia, o ile to możliwe należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia ochrony i udokumentowanie zdarzenia podjąć stosowne działania, jeśli zaistniały przypadek został przewidziany w dokumentacji systemu operacyjnego, bazy danych, czy instrukcji aplikacji użytkowej,
- nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa Informacji.

d. Po przybyciu na miejsce naruszenia bezpieczeństwa danych osobowych Administrator Bezpieczeństwa Informacji podejmuje następujące kroki:

- zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości pracy urzędu,
- może zażądać dokładnej relacji z zaistniałego naruszenia bezpieczeństwa danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,
- rozważa celowość i potrzebę powiadamiania o zaistniałym naruszeniu Administratora Danych Osobowych, nawiązuje kontakt ze specjalistami spoza urzędu (jeśli zachodzi taka potrzeba).

e. Administrator Bezpieczeństwa Informacji dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych osobowych sporządzając raport wg wzoru stanowiącego załącznik Nr 1 do „Polityki”, który zawiera następujące informacje:

- wskazanie osoby zawiadamiającej o naruszeniu, oraz innych osób zaangażowanych w wyjaśnienie okoliczności naruszenia bezpieczeństwa,

- określenie czasu i miejsca zawiadomienia o naruszeniu bezpieczeństwa, jak i samego naruszenia (o ile da się ustalić),
- określenie okoliczności towarzyszących i rodzaju naruszenia,
- opis podjętego działania wraz z wyjaśnieniem wyboru sposobu działania, wstępną ocenę przyczyn wystąpienia naruszenia bezpieczeństwa,
- ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego

f. Raport z wystąpienia zdarzenia Administrator Bezpieczeństwa Informacji przekazuje Administratorowi Danych Osobowych.

g. Administrator Bezpieczeństwa Informacji zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń, oraz terminu wznowienia przetwarzania danych osobowych).

h. Zaistniałe naruszenie bezpieczeństwa może stać się przedmiotem zespołowej analizy przeprowadzanej przez kierownictwo urzędu, Administratora Danych Osobowych, Administratora Bezpieczeństwa Informacji i Pełnomocnika ds. Informacji Niejawnych.

i. Analiza ta powinna zawierać wszechstronną ocenę zaistniałego naruszenia bezpieczeństwa, wskazanie odpowiedzialnych, wnioski co do ewentualnych działań proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

8. Postanowienia końcowe.

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

b. Wobec osoby, która w przypadku naruszenia ochrony danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne.

c. Administrator Bezpieczeństwa Informacji zobowiązany jest prowadzić ewidencje osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych wg wzoru określonego w załączniku nr 2.

d. 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).

9. Załączniki

a. Załącznik Nr 1. Wzór raportu z naruszenia bezpieczeństwa danych osobowych w Urzędzie Gminy Boronów.

b. Załącznik Nr 2. Wzór wykazu osób, które zostały zapoznane z „Polityką Ochrony Danych Osobowych w Urzędzie Gminy Boronów” oraz „Instrukcją Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Boronów”.

c. Załącznik Nr 3. Wzór upoważnienia imiennego do przetwarzania danych osobowych.

d. Załącznik Nr 4. Wzór wykazu osób upoważnionych do przetwarzania danych osobowych w Urzędzie Gminy Boronów.

WZÓR
**Raport z naruszenia bezpieczeństwa danych osobowych
w Urzędzie Gminy Boronów**

1. Data: Godzina:
(dd.mm.rrrr) (gg:mm)

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....
(imię, nazwisko, stanowisko służbowe, nazwa użytkownika - jeśli występuje)

3. Lokalizacja zdarzenia:

.....
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....
.....
.....

5. Przyczyny wystąpienia zdarzenia:

.....
.....
.....

6. Podjęte działania:

.....
.....
.....

7. Postępowanie wyjaśniające:

.....
.....
.....
.....

(data, podpis Administratora Bezpieczeństwa Informacji)

Załącznik Nr 2
do „Polityki bezpieczeństwa danych osobowych
w Urzędzie Gminy Boronów”

WZÓR

Wykaz osób, które zostały zapoznane z „Polityką ochrony danych osobowych w Urzędzie Gminy Boronów” oraz „Instrukcją Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Boronów”

L.p.	Imię i nazwisko	Stanowisko	Data	Podpis



Załącznik Nr 3
do „Polityki bezpieczeństwa
danych osobowych
w Urzędzie Gminy Boronów”

WZÓR

Boronów, dnia

Upoważnienie imienne nr

do przetwarzania danych osobowych

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) upoważniam Panią / Pana:

.....

(imię i nazwisko osoby upoważnionej)

zatrudnioną (ego) w:

.....

(nazwa jednostki i komórki organizacyjnej)

na stanowisku:

do przetwarzania od dnia20..... r. danych osobowych

w zakresie

Nadaję identyfikator:

.....

(podpis administratora danych)



Załącznik Nr 4
do „Polityki bezpieczeństwa
danych osobowych
w Urzędzie Gminy Boronów”

WZÓR

Ewidencja osób upoważnionych do przetwarzania danych osobowych w systemie informatycznym

L.p	Identyfikator użytkownika*	Imię i nazwisko	Zakres upoważnienia do przetwarzania danych osobowych	Data nadania uprawnień w systemie	Data i podpis ABI	Data odebrania uprawnień w systemie oraz data i podpis ABI
1						
	Zmiany danych					
2						
	Zmiany danych					
3						
	Zmiany danych					
4						
	Zmiany danych					

R

Załącznik Nr 2
do Zarządzenia nr 48/2012
Wójta Gminy Boronów
z dnia 12 kwietnia 2012 r.

**INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM
SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH**

W

**URZĘDZIE GMINY
BORONÓW**

Informacje podstawowe.

§ 1

Niniejsza „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych” zwana dalej instrukcją, jest dokumentem wewnętrznym wydanym przez Wójta Gminy Boronów i ma zastosowanie do przetwarzania danych osobowych w systemie informatycznym Urzędu Gminy Boronów, w celu bezpiecznego ich przetwarzania.

§ 2

1. Instrukcja określa ogólne zasady i tryb postępowania Administratora Danych oraz wszystkich użytkowników przetwarzających dane osobowe w systemie informatycznym Urzędu Gminy Boronów.
2. Podstawę prawną do niniejszej instrukcji stanowią:
 - a. Ustawa z dnia 29 sierpnia 1997 o ochronie danych osobowych – tekst jednolity (DZ. U. Nr 101, poz. 926 z późn. zm.)
 - b. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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).

§ 3

1. Każdy pracownik Urzędu Gminy Boronów zobowiązany jest zapoznać się z niniejszą Instrukcją i stosować jej przepisy na swoim stanowisku pracy
2. Nadużycie przez użytkownika postanowień niniejszej Instrukcji, może stanowić podstawę do pociągnięcia go do odpowiedzialności przewidzianej właściwymi przepisami prawa.
3. Administrator Bezpieczeństwa Informacji lub Administrator Systemu Informatycznego ma prawo do monitorowania pracy urządzeń przyłączonych do sieci informatycznej pod kątem przesyłania i przetwarzania danych, rejestracji zdarzeń związanych z przesyłaniem i przetwarzaniem danych w oprogramowaniu oraz prawidłowości wykorzystania powierzonego użytkownikom sprzętu i oprogramowania.

§ 4

Określenia i skróty użyte w instrukcji oznaczają:

1. **Administrator Danych Osobowych – Wójt Gminy Boronów** zwany dalej **ADO**.
2. **Administrator Bezpieczeństwa Informacji** – osoba wyznaczona przez ADO, odpowiedzialna za bezpieczeństwo danych osobowych, zwana dalej **ABI**. W Urzędzie Gminy Boronów funkcję **ABI** pełni **Sekretarz Gminy Boronów**.
3. **Administrator Systemów Informatycznych**, zwany dalej **ASI** – osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych. W Urzędzie Gminy Boronów funkcję tę pełni **Informatyk**.
4. **System informatyczny** - sieć teleinformatyczna, stacje robocze, serwery, oraz wszelkie inne urządzenia na których można przetwarzać dane wykorzystywane do pracy Urzędzie Gminy Boronów, a także wszelkie oprogramowanie dostępne w lokalnej sieci komputerowej lub zainstalowanych na poszczególnych stacjach roboczych, zlokalizowanych w budynkach Urzędu Gminy w Boronowie ul. Dolna 2.
5. **Bezpieczeństwo systemu informatycznego** – wdrożenie przez ADO lub osobę przez niego uprawnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony

danych przed ich udostępnieniem osobom nieupoważnionym, zabranie przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz nieuprawnioną zmianą, utratą, uszkodzeniem lub zniszczeniem.

6. **Przetwarzanie danych osobowych** – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
7. **Osoba upoważniona lub użytkownik systemu** – osoba posiadająca upoważnienie wydane przez ADO lub uprawnioną przez niego osobę i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej, zwana dalej użytkownikiem.
8. **Osoba uprawniona** – osoba posiadająca upoważnienie wydane przez ADO do wykonywania w jego imieniu określonych czynności.
9. **Obszar przetwarzania danych osobowych** – budynek Urzędu Gminy w Boronowie

§ 5

Określenie sposobu przydziału haseł dla użytkowników i częstotliwość ich zmian.

1. Dla każdego użytkownika systemu informatycznego, w którym przetwarzane są dane osobowe, administrator bezpieczeństwa informacji ustala identyfikator i hasło.
2. W celu zapewnienia wysokiego poziomu bezpieczeństwa hasło musi zawierać co najmniej 8 znaków i zawierać jednocześnie duże i małe litery oraz cyfry lub znaki specjalne.
3. Hasło jest wpisywane i przechowywane w systemie informatycznym w postaci zaszyfrowanej.
4. Zmiany hasła dokonuje użytkownik.
5. Hasło użytkownika systemu musi być zmieniane nie rzadziej niż raz na 30 dni. W przypadku gdy użytkownik systemu informatycznego nie korzysta z danego systemu przez okres dłuższy niż 30 dni hasło musi zostać zmienione podczas najbliższego ponownego zalogowania. Każdorazowo po zmianie hasła użytkownik systemu zobowiązany jest zapisać nowe hasło, umieścić je w zaklejonej kopercie opatrzonej imieniem, nazwiskiem oraz datą zmiany i w tym samym dniu kopertę przekazać ASI.
6. Hasła użytkownika, umożliwiające dostęp do systemu informatycznego, utrzymywane są w tajemnicy, a po upływie ich ważności niszczone. ASI prowadzi rejestr w którym użytkownicy potwierdzają przekazanie haseł, zaś otrzymane zaklejone koperty z bieżącymi hasłami przechowuje w zamkniętej metalowej szafie.
7. Hasła użytkowników mogą zostać użyte jedynie w sytuacji awaryjnej i po bezpośredniej dyspozycji wydanej przez ADO lub ABI.
8. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielany innej osobie.
9. Hasło użytkownika, który utracił uprawnienia dostępu do danych osobowych unieważnia się bezzwłocznie oraz podejmuje inne niezbędne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych
10. Osobą odpowiedzialną za prawidłowe funkcjonowanie mechanizmów zawartych w § 5 jest ASI.
11. Użytkownik ponosi odpowiedzialność za czynności wykonane w systemie przy użyciu identyfikatora i hasła, którymi się posługuje lub posługiwał. Użytkownik zobowiązany jest do utrzymania haseł dostępu w tajemnicy, a w szczególności do dołożenia starań w celu uniemożliwienia zapoznania się z nimi osób trzecich, nawet po ustaniu ich ważności.

§ 6

Określenie sposobu rejestrowania i wyrejestrowywania użytkowników.

1. Wykaz użytkowników wraz z zakresem dostępu do określonych zbiorów tworzony jest przez ABI.
2. ABI prowadzi „Ewidencje osób zatrudnionych przy przetwarzaniu danych osobowych”, która zawiera:
 - imię i nazwisko użytkownika
 - nazwę referatu w którym jest zatrudniony
 - nazwę identyfikatora
 - datę zarejestrowania w systemie
 - datę wyrejestrowania z systemu
3. Jakakolwiek zmiana informacji wyszczególnionych w ewidencji podlega natychmiastowemu odnotowaniu.
4. Użytkownik, który utracił uprawnienia dostępu do systemu zawierającego dane osobowe, zostaje niezwłocznie wyrejestrowany z systemu przez administratora bezpieczeństwa informacji, a stosowną informację umieszcza się w ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych.

§ 7

Procedury rozpoczęcia zawieszenia i zakończenia pracy.

1. Użytkownik rozpoczynający pracę zobowiązany jest przestrzegać procedur, które mają na celu sprawdzenie zabezpieczenia pomieszczenia w którym przetwarzane są dane osobowe, swojego stanowiska pracy oraz stanu sprzętu komputerowego, a w szczególności:
 - a) przed wejściem do pomieszczenia sprawdzić czy na drzwiach nie ma widocznych śladów prób niepowołanego ich otwierania,
 - b) ocenić czy w pomieszczeniu nie ma znaków wskazujących na pobyt w nim osób nieuprawnionych,
 - c) po włączeniu komputera ocenić jakość jego pracy i stwierdzić zmiany,
 - d) sprawdzić czy nie zostało zainstalowane jakieś nowe oprogramowanie,
 - e) w przypadku stwierdzenia zmian niezwłocznie powiadomić zwierzchnika lub ASI jeśli zmiany dotyczą pkt c lub d.
2. Użytkownik przed przystąpieniem do przetwarzania danych powinien zalogować się w systemie, posługując się swoim identyfikatorem i hasłem.
3. Użytkownik w czasie pracy powinien stosować przedsięwzięcia zapewniające bezpieczeństwo przetwarzania danych osobowych w systemie:
 - ustawić ekrany monitorów w pomieszczeniach tak, aby uniemożliwić podgląd osobom nieuprawnionym
 - dopilnować, aby w pomieszczeniach, stanowiących obszar przetwarzania danych osobowych, osoby trzecie przebywały tylko za zgodą przełożonych i w obecności osób uprawnionych
 - stosować urządzenia zabezpieczające przed utratą danych, spowodowanych awarią zasilania lub zakłóceniami w sieci elektrycznej
 - w przypadku, kiedy przerwa w pracy wynosi ponad 10 minut stosować automatyczne wylogowanie z systemu bądź automatyczny wygaszacz ekranu chroniony hasłem.
4. Po zakończeniu pracy użytkownik powinien przestrzegać następujących zasad:
 - wylogować się z systemu i poczekać na jego wyłączenie się
 - sprawdzić czy nie zostały pozostawione bez nadzoru nośniki informacji (płyty CD, dyskietki, pamięci usb, itp.)

§ 8

Tworzenie kopii zapasowych

1. Kopie zapasowe należy wykonywać z częstotliwością adekwatną do częstotliwości dokonywania zmian w tych zbiorach, tj. przynajmniej raz na tydzień w przypadku danych aktualizowanych na bieżąco oraz nie rzadziej niż raz w miesiącu w przypadku zbiorów danych przetwarzanych sporadycznie.
2. W przypadku braku technicznych możliwości sporządzenia kopii zgodnie z planem, należy je wykonać w najbliższym możliwym terminie.
3. Kopie zapasowe należy tworzyć na odpowiedniej jakości nośnikach informacji i przechowywać je w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.
4. Kopiami zapasowymi, zgodnie z rozporządzeniem zabezpiecza się zarówno dane jak i programy służące do ich przetwarzania.
5. Osobą odpowiedzialną za ustalanie sposobów i standardów tworzenia kopii zapasowych jest ASI.
6. Użytkownicy we własnym zakresie odpowiadają za sporządzanie kopii zapasowych i awaryjnych wytworzonych przez siebie dokumentów i danych znajdujących się na lokalnych dyskach twardych wykorzystywanych przez nich stacji roboczych. Jednocześnie mają obowiązek dopilnowania, aby dane przetwarzane przy pomocy oprogramowania nie przeznaczonego do przetwarzania danych osobowych bądź też oprogramowania służącego przetwarzaniu danych osobowych wyłącznie w celu ich udostępnienia na piśmie, i zapisywane na nośnikach informatycznych nie zawierały danych osobowych.

§ 9

Sposób i czas przechowywania nośników informacji (w tym kopii zapasowych).

1. Kopii awaryjnych wykonywanych na nośnikach magnetycznych nie należy przechowywać w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.
2. Nośniki informacji oraz wydruki z danymi osobowymi, które nie są przeznaczone do udostępniania przechowuje się w warunkach uniemożliwiających dostęp do nich osobom niepowołanym.
3. Kopie awaryjne należy okresowo sprawdzać pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu.
4. Kopie awaryjne usuwane są niezwłocznie po ustaniu ich użyteczności

§ 10

Sposób zabezpieczenia systemu informatycznego przed działalnością szkodliwego oprogramowania

1. W celu zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych należy zastosować środki bezpieczeństwa na poziomie wysokim.
2. System informatyczny służący do przetwarzania danych osobowych powinien być zabezpieczony programem antywirusowym, który nadzoruje i automatycznie sygnalizuje obecność wirusów oraz niebezpiecznego oprogramowania ułatwiającego zdalny dostęp do informacji.
3. Program antywirusowy powinien posiadać mechanizmy uaktualniania bazy danych wirusów.

4. O każdorazowym wykryciu wirusa użytkownik zobowiązany jest niezwłocznie powiadomić ASI, który dokonuje analizy problemu i podejmuje stosowne działania naprawcze.
5. Dodatkowo należy zastosować sprzętowe urządzenie oddzielające sieć komputerową od bezpośredniego dostępu do Internetu, typu zarządzany router, stanowiące blokadę przed nieuprawnionym dostępem z zewnątrz do systemu informatycznego Urzędu Gminy Boronów.
6. W sytuacji konieczności podłączenia do systemu komputerowego nośnika informacji pochodzącego z zewnętrznego źródła (np. płyty cd/dvd, pamięci usb itp.) nośnika taki musi zostać poddany weryfikacji pod kątem infekcji szkodliwym oprogramowaniem przez ASI lub ABI.
7. Zabrania się używania do codziennej pracy urządzeń pamięci masowej nie będących na wyposażeniu Urzędu Gminy w Boronowie i nie zatwierdzonych przez ABI bądź ASI.
8. Zabrania się używania i wnoszenia urządzeń i nośników informacji wykorzystywanych do pracy w Urzędzie Gminy w Boronowie poza obszar przetwarzania danych. W przypadku zaistnienia takiej konieczności należy uzyskać zgodę ADO/ABI. Jeśli nośnik danych umożliwiający zapis (dyskietka, pamięć USB itp.) został podłączony do zewnętrznego urządzenia (np. komputer domowy, stacja robocza w jednostce podległej itp.) przed jego ponownym podłączeniem do systemu informatycznego Urzędu Gminy w Boronowie musi zostać poddany weryfikacji jak w pkt 6.

§11

Wymagania które powinien spełniać system informatyczny służący do przetwarzania danych osobowych.

1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym – z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie – system ten powinien zapewniać odnotowanie:
 - a) daty pierwszego wprowadzenia danych do systemu
 - b) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba
 - c) źródła danych w przypadku zbierania danych, nie od osoby, której one dotyczą
 - d) informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych
 - e) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.

§ 12

Sposób dokonywania przeglądów i konserwacji systemu oraz zbiorów danych osobowych

1. Okresowe oraz bieżące przeglądy i konserwacje sprzętu komputerowego, wynikające z eksploatacji, warunków zewnętrznych oraz ważności systemu dla funkcjonowania Urzędu Gminy Boronów wykonuje ASI.
2. Urządzenia, dyski lub inne informatyczne nośniki informacji, przeznaczone do naprawy w firmach zewnętrznych, pozbawia się przed naprawą zapisu danych osobowych, albo naprawia je pod nadzorem ASI.
3. Urządzenia, dyski lub inne informatyczne nośniki informacji, przeznaczone do likwidacji należy pozbawić zapisu, a w przypadku gdy jest to niemożliwe uszkodzić mechanicznie w sposób uniemożliwiający ich odczytanie.

§ 13

Postępowanie w przypadku przekazywania nośników z danymi osobowymi poza obszar przetwarzania danych.

1. Dane osobowe zapisane na urządzeniach i nośnikach informacji, o których mowa w art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, przekazywane poza obszar przetwarzania danych osobowych, w celu zapewnienia ich poufności i integralności powinny wcześniej zostać zakodowane stosownym programem przy użyciu co najmniej 8 literowego hasła, które musi zawierać duże i małe litery oraz cyfry lub znaki specjalne.

§ 14

Postanowienia końcowe.

1. Użytkownik systemu informatycznego nie ma prawa dokonywania samodzielnych instalacji, deinstalacji jakiegokolwiek oprogramowania, ani wprowadzania zmian w konfiguracji oprogramowania wykraczających poza jego normalne użytkowanie.
2. Czynności o których mowa w § 14 pkt 1 wykonuje ASI.
3. ABI prowadzi „Rejestr zbiorów danych osobowych przetwarzanych w systemach informatycznych”
4. ASI przeprowadza szkolenia dla nowozatrudnionych pracowników oraz w przypadku istotnych zmian w systemach informatycznych, w których przetwarzane są dane osobowe z zakresu stosowania Instrukcji Zarządzania Systemem Informatycznym.
5. ABI dokonuje okresowego sprawdzenia sprawności funkcjonowania zabezpieczeń systemów w których przetwarzane są dane osobowe.

§ 15

W sprawach nieuregulowanych niniejszą Instrukcją zastosowanie znajdują przepisy ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych – tekst jednolity (DZ. U. Nr 101, poz. 926 z późn. zm.) i rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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)

WÓJT
mgr Rufin Marchczyk