

ZARZĄDZENIE Nr W.0050.145. 2012

**Wójt Gminy Charsznica
z dnia 14 marca 2012 roku**

w sprawie: ochrony danych osobowych przetwarzanych w Urzędzie Gminy Charsznica

Na podstawie art. 33 ust 3 ustawy z dnia 8 marca 1990 r. *o samorządzie gminnym* (tekst jednolity - Dz. U. z 2001 r. Nr 142 poz. 1591 z późn. zm.), art. 36 ustawy z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych* (Dz. U. z 2002 r. nr 101, poz. 926 z późn. zm.), § 3 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. 2004 r. Nr 100, poz. 1024) **zarządza się, co następuje:**

§ 1

1. Przetwarzanie danych osobowych w Urzędzie Gminy Charsznica służy wyłącznie realizacji zadań zgodnie z zakresem działania.
2. Przetwarzanie danych osobowych może mieć miejsce ze względu na dobro publiczne, dobro osoby, której dane dotyczą, lub dobro osób trzecich w zakresie i trybie określonym ustawą.
3. Za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
4. Przetwarzanie danych osobowych może odbywać się w systemie informatycznym, a także w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych.

§ 2

1. Administratorem danych osobowych w Urzędzie Gminy Charsznica jest Wójt.
2. Administrator danych powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były:
 - przetwarzane w zakresie niezbędnym do wykonywanych zadań powierzonych pracownikom,
 - przetwarzane zgodnie z prawem,
 - merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
 - przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.
3. Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

4. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.

§ 3

1. W celu organizacji zasad ochrony, zabezpieczenia i kontroli przetwarzania danych osobowych w systemach informatycznych Urzędu , powołuje się administratora bezpieczeństwa informacji.
2. Obowiązki administratora bezpieczeństwa informacji Urzędu Gminy Charsznica powierza się pracownikowi ds. informatyki.
3. Zadania oraz zakres nadzoru administratora bezpieczeństwa informacji określony jest w dokumencie pod nazwą „Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Charsznica” oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Charsznica” stanowiące załącznik Nr 1 i Nr 2 do niniejszego zarządzenia.

§ 4

Traci moc zarządzenie Wójta Gminy Charsznica Nr 10/99 z dnia 15.09.1999 roku w sprawie wykonywania ustawy o ochronie danych osobowych w Urzędzie Gminy w Charsznicy.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

WOJTA GMINY
mgr inż. Jan Żelazek



WÓJT
GMINY CHARSZNICA
32-260 Charsznica
ul. Kolejowa 20

Załącznik nr 1
do Zarządzenia Nr W.0050. 145.2012
Wójta Gminy Charsznica
z dnia 14 marca 2012 r.

Polityka bezpieczeństwa danych osobowych w Urzędzie Gminy Charsznica

1. Wstęp

W systemie Urzędu Gminy Charsznica 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 Charsznica, z siedzibą w Miechów-Charsznica, ul. Kolejowa 20.
- 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 Charsznica.
- 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. W Urzędzie Gminy Charsznica zadania te wykonuje Administrator Bezpieczeństwa Informacji.
- f) Sieć lokalna – połączenie komputerów pracujących w urzędzie w celu wymiany danych (informacji) dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych.
- g) System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
- h) Przetwarzanie danych – rozumie się to w tym dokumencie, jako jakiejkolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.
- i) Zabezpieczenie danych w systemie informatycznym – wdrożenie i wykorzystywanie stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
- j) Teletransmisja – przesyłanie informacji za pomocą sieci telekomunikacyjnej.
- k) Poufność danych – jest to właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.
- l) Integralność danych – właściwość zapewniająca, że dane osobowe nie zostały zmienione, lub zniszczone w sposób nieautoryzowany.
- m) Rozliczalność – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
- n) Aplikacja – program komputerowy wykonujący konkretne zadanie.
- o) Wysoki poziom bezpieczeństwa – musi występować wtedy, gdy przynajmniej jedno urządzenie systemu informatycznego, służące do przetwarzania danych osobowych, połączone jest z siecią publiczną.
- p) 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. Wykaz osób upoważnionych do przetwarzania danych osobowych stanowi załącznik nr 1.
- c) Podejmowanie odpowiednich działań w przypadku wykrycia naruszeń, lub podejrzenia naruszenia zabezpieczeń.
- d) Nadzór nad naprawami, konserwacją, oraz likwidacją urządzeń, na których zapisane są dane osobowe.
- e) Nadzór nad prawidłowością archiwizacji, oraz usuwania danych osobowych.
- f) Monitorowanie zabezpieczeń wdrożonych w celu ochrony danych osobowych.
- g) Nadzór nad prowadzeniem odpowiedniej dokumentacji.

4. Obszar przetwarzania danych osobowych

Obszar przetwarzania danych osobowych w systemie stanowią pomieszczenia

Lp.	Adres – budynek	Nr pomieszczenia
1	Miechów-Charsznica, ul. Kolejowa 20	10,14,16,17,19,23,24

5. Wykaz zbiorów danych osobowych przetwarzanych w systemie informatycznym Urzędu

W systemie zbierane są dane zawierające informacje o osobach będących klientami urzędu, które przetwarzane są zgodnie z prawem lub zgodziły się na ich przetwarzanie. Dane te tworzą następujące zbiory:

- a) Rejestr mężczyzn objętych rejestracją
- b) Rejestr kobiet objętych rejestracją
- c) Lista stawiennictwa osób do kwalifikacji wojskowej
- d) Oświadczenia o stanie majątkowym osób zobowiązanych do ich składania.
- e) Dziennik korespondencyjny.
- f) Ewidencja wniosków i wydanych zezwoleń na utrzymywanie psa rasy uznanej za agresywną
- g) Akta Stanu Cywilnego
- h) Ewidencja Ludności Gminy Charsznica i dowody osobiste
- i) Ewidencja osób, którym udzielono zezwolenia na wycinkę drzew
- j) Ewidencja podatników i dłużników
- k) Wykaz umów dzierżawy nieruchomości będących własnością Gminy
- l) Rejestr użytkowników wieczystych gruntów gminnych
- m) Wykaz umów najmu lokali mieszkalnych i użytkowych będących własnością Gminy Charsznica.
- n) Rejestr skarg i wniosków
- o) Zwrot podatku akcyzowego zawartego w cenie oleju napędowego wykorzystywanego do produkcji rolnej
- p) Kadry
- q) Płace
- r) Rejestr wyborców

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.
- c) Wydruki komputerowe.
- d) Do przetwarzania danych osobowych w systemie informatycznym urzędu stosuje się aplikacje:

WIP 517 A – obsługa zobowiązań podatkowych, EPOD – system ewidencji działalności, POGRUN – ewidencja podatków lokalnych, ELUD – ewidencja ludności, PB-USC – wspomaganie USC, KASA – obsługa kasy, FKB – program księgowy, PŁATNIK – obsługa ZUS . KADRY + , PŁACE + , ELUD + , WYB + , POGRUN + , WIP + użytkowane programy są w wersji windowsowej. Producentem aplikacji jest firma RADIX.

W systemie informatycznym stosuje się podstawowy poziom bezpieczeństwa przy przetwarzaniu danych osobowych.

ELUD+ współpracuje z POGRUN+, KADRY+, PŁACE+, WYB+, WIP+, KASA+

POGRUN+ współpracuje z ELUD+, WIP+

PŁACE+ współpracuje z ELUD+, FKB+, KADRY+, PŁATNIK

WYB+ współpracuje z ELUD+

KADRY+ współpracuje z PŁACE+, ELUD+

WIP+ współpracuje z ELUD+, FKB+, KASA+, POGRUN+

KASA+ współpracuje z ELUD+, FKB+, WIP+

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

- a) Środki ochrony fizycznej
 - Urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych zamkami.
 - Dostęp do pokoi jest kontrolowany za pomocą wydawania kluczy tylko osobom uprawnionym.
 - Dostęp do pomieszczenia, w którym znajdują się urządzenia serwerowe ma tylko Administrator Bezpieczeństwa Informacji (ABI).
- b) Środki sprzętowe, informatyczne i telekomunikacyjne
 - Stosuje się niszcarki 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 raz w miesiącu.
- c) Środki ochrony w ramach oprogramowania urządzeń teletransmisji:
 - Na komputerach użytkowników systemu działa program antywirusowy.
 - Na komputerach użytkowników systemu działa programowy firewall.
 - Dostęp do serwera zawierającego dane osobowe zabezpieczony jest hasłem.
- d) Środki ochrony w ramach oprogramowania systemu:
 - Dostęp do baz danych osobowych zastrzeżony jest wyłącznie dla uprawnionych

pracowników.

- Konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych przechowywanych w systemie informatycznym wyłącznie za pośrednictwem aplikacji wymienionych w punkcie 5.
- 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.
- Rejestracji podlegają wszystkie przypadki awarii systemu, działania konserwacyjne w systemie oraz naprawy.
- W przypadku, gdy zachodzi konieczność naprawy sprzętu poza siedzibą urzędu, należy wymontować z niego nośniki informacji zawierające dane osobowe.
- W przypadku, gdy uszkodzenie sprzętu zawierającego nośnik danych, na którym zapisane są dane osobowe wymusza konieczność przekazania go poza siedzibę urzędu, nośnik ten należy wymontować.

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 naruszenia ochrony (o ile to możliwe),
- ustalić przyczynę i sprawcę naruszenia ochrony, gdy jest to możliwe.
- 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 2, 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.

9. Struktura baz danych osobowych określona została w załączniku nr 3 do „Polityki Bezpieczeństwa Danych Osobowych w Urzędzie Gminy Charsznica”.

WOJT GMINY
mgr inż. Jan Żebrak

WZÓR

Ewidencja osób upoważnionych do przetwarzania danych osobowych w systemie informatycznym

L.p.	Identyfikator użytkownika	Imię i nazwisko	Zakres upoważnienia do przetwarzania danych osobowych nazwa bazy danych	Data nadania uprawnień w systemie	Data i podpis ABI	Data odebrania uprawnień w systemie oraz data i podpis ABI

WOJCIŃSKI
mgr inż. J. Zembrak

WZÓR

**Raport
z naruszenia bezpieczeństwa danych osobowych w Urzędzie Gminy Charsznica**

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)

WÓJT GMINY
mgr inż. J. Debruk

Struktura baz danych osobowych w Urzędzie Gminy Charsznica.

1. Rejestr mężczyzn objętych rejestracją :

- imię i nazwisko, nazwisko rodowe, imiona i nazwiska rodowe rodziców, imiona i nazwiska poprzednie
- data i miejsce urodzenia, stan cywilny, numer PESEL
- adres i data zameldowania na pobyt stały, poprzednie adresy zameldowania na pobyt stały wraz z określeniem okresu zameldowania, tryb wymeldowania
- adres zameldowania na pobyt czasowy trwający ponad trzy miesiące wraz z określeniem okresu zameldowania, tryb wymeldowania
- data ujęcia w rejestrze
- data zgłoszenia się do rejestracji, pokwitowanie odbioru potwierdzenia
- stopień wojskowy, nazwa, seria i numer wojskowego dokumentu osobistego, oznaczenie wojskowej komendy uzupełnień, w ewidencji której osoba pozostaje
- uwagi

2. Rejestr kobiet objętych rejestracją :

- imię i nazwisko, nazwisko rodowe, imiona i nazwiska rodowe rodziców, imiona i nazwiska poprzednie
- data i miejsce urodzenia, stan cywilny, numer PESEL
- adres i data zameldowania na pobyt stały, poprzednie adresy zameldowania na pobyt stały wraz z określeniem okresu zameldowania, tryb wymeldowania
- adres zameldowania na pobyt czasowy trwający ponad trzy miesiące wraz z określeniem okresu zameldowania, tryb wymeldowania
- data ujęcia w rejestrze
- data zgłoszenia się do rejestracji, pokwitowanie odbioru potwierdzenia
- stopień wojskowy, nazwa, seria i numer wojskowego dokumentu osobistego, oznaczenie wojskowej komendy uzupełnień, w ewidencji której osoba pozostaje
- uwagi

3. Lista stawiennictwa osób do kwalifikacji wojskowej:

- nazwisko i imię, nazwisko rodowe, numer ewidencyjny PESEL
- miejsce urodzenia
- seria i numer dowodu osobistego
- miejsce pobytu stałego lub czasowego trwającego ponad trzy miesiące
- adres do korespondencji

4. Oświadczenia o stanie majątkowym osób zobowiązanych do ich składania.

- miejscowość i dzień wypełnienia oświadczenia
- imię i nazwisko, nazwisko rodowe
- data i miejsce urodzenia
- miejsce zatrudnienia, stanowisko lub funkcja
- środki pieniężne zgromadzone w walucie polskiej
- środki pieniężne zgromadzone w walucie obcej
- papiery wartościowe
- prowadzona działalność gospodarcza(forma prawna i przedmiot działalności)

- przychód i dochód osiągnięty z prowadzonej działalności gospodarczej
- zarządzana działalność gospodarcza (przedstawiciel, pełnomocnik, forma prawna, przedmiot działalności)
- dochód z zarządzania działalnością gospodarczą
- działalność w spółkach handlowych(nazwa i siedziba spółki), czy jest członkiem zarządu(od kiedy), czy jest członkiem rady nadzorczej(od kiedy), czy jest członkiem komisji rewizyjnej(od kiedy), dochody osiągnięte z tego tytułu
- działalność w spółdzielniach, czy jest członkiem zarządu(od kiedy), czy jest członkiem rady nadzorczej(od kiedy), czy jest członkiem komisji rewizyjnej(od kiedy), dochody osiągnięte
- działalność w fundacjach prowadzących działalność gospodarczą, czy jest członkiem zarządu(od kiedy), czy jest członkiem rady nadzorczej(od kiedy), czy jest członkiem komisji rewizyjnej(od kiedy), dochody osiągnięte
- inne dochody z tytułu zatrudnienia lub innej działalności zarobkowej(z podaniem kwot uzyskiwanych z każdego tytułu)
- dom(powierzchnia, wartość, tytuł prawny)
- mieszkanie(powierzchnia, wartość, tytuł prawny)
- gospodarstwo rolne(rodzaj, powierzchnia, wartość, rodzaj zabudowy, tytuł prawny, dochód)
- inne nieruchomości(powierzchnia, wartość, tytuł prawny)
- udziały w spółkach handlowych (liczba, emitent udziałów, dochód)
- akcje w spółkach handlowych (liczba, emitent akcji, dochód)
- majątek nabyty od skarbu państwa, samorządu w drodze przetargu
- składniki mienia ruchomego o wartości powyżej 10.000 zł
- zobowiązania pieniężne o wartości powyżej 10.000 zł
- adres zamieszkania osoby składającej oświadczenie
- miejsce położenia nieruchomości wymienionych w części A

5. Dziennik korespondencyjny.

- numer kolejny
- data otrzymania korespondencji
- numer-dnia otrzymanej korespondencji
- od kogo
- treść otrzymanej korespondencji
- znak referenta
- data wysłanej korespondencji
- do kogo
- treść wysłanej korespondencji
- numer korespondencji uprzedniej
- numer odpowiedzi na korespondencję wysłaną
- numer aktu
- uwagi

6. Ewidencja wniosków i wydanych zezwoleń na utrzymywanie psa rasy uznanej za agresywną.

- imię i nazwisko właściciela
- adres
- data wpływu wniosku
- data wystawienia zezwolenia
- dane dotyczące psa (imię, rasa)

- data zgonu i nr aktu zgonu
- USC aktu zgonu
- uprawnienia wyborcze
- status mieszkańca
- data wprowadzenia rekordu
- data ostatniej modyfikacji
- wykształcenie
- data przekroczenia granicy

9. Ewidencja osób, którym udzielono zezwolenia na wycinkę drzew

- imię i nazwisko
- nr działki
- adres
- data decyzji, numer decyzji

10. Ewidencja podatników i dłużników.

A. Program WIP – system windykacji opłat i podatków

- imię i nazwisko
- data urodzenia
- imię ojca
- imię matki
- PESEL
- NIP
- kod pocztowy
- miejscowość
- ulica
- nr domu
- rejon

B. Program POGRUN + system naliczania podatków od gruntów i nieruchomości

- imię i nazwisko
- adres(miejscowość, ulica, nr domu, rejon, NIP, Pesel, regon, powiat, województwo, kraj)
- podatek od nieruchomości
- podatek rolny(ha fizycznie, ha użytki, rolne, ha przeliczeniowe, podstawa podatku, zobowiązanie)
- podatek leśny

11. Wykaz umów dzierżawny nieruchomości będących własnością Gminy

- imię, nazwisko i adres
- PESEL
- NIP
- rodzaj i numer dokumentu stwierdzającego tożsamość
- oznaczenie przedmiotu umowy
- czynsz dzierżawny
- kwota do przypisu

12. Rejestr użytkowników wieczystych gruntów gminnych

- imię, nazwisko i adres
- PESEL, NIP
- rodzaj i numer dokumentu stwierdzającego tożsamość
- oznaczenie przedmiotu umowy
- opłata z tytułu użytkowania wieczystego
- kwota do przypisu

13. Wykaz umów najmu lokali mieszkalnych i użytkowych będących własnością Gminy Charsznica

- imię, nazwisko i adres
- PESEL, NIP
- rodzaj i numer dokumentu stwierdzającego tożsamość
- oznaczenie przedmiotu umowy
- czynsz najmu
- kwota do przypisu

14. Rejestr skarg i wniosków.

- data wpływu
- imię i nazwisko petenta, nazwa instytucji
- adres petenta instytucji
- przedmiot skargi, zażalenia i odwołania
- data zlecenia załatwienia
- komu zlecono załatwienie
- sposób załatwienia

15. Zwrot podatku akcyzowego zawartego w cenie oleju napędowego, wykorzystywanego do produkcji rolnej

- imię, nazwisko i adres
- PESEL
- NIP
- rodzaj i numer dokumentu stwierdzającego tożsamość
- pow. użytków rolnych
- ilość zakupionego oleju napędowego
- data decyzji, nr decyzji
- kwota zwrotu

16. Kadry

- PESEL
- imię i nazwisko
- nazwisko rodowe
- data i miejsce urodzenia
- płeć
- adres stały(miejscowość, ulica, nr domu, nr mieszkania)
- dowód osobisty(seria, nr i rodzaj, wydany przez, data wydania)
- imię ojca, imię matki
- stan cywilny
- obowiązek wojskowy(dokument wojskowy, seria i numer, stopień wojskowy, specjalność, ewidencja, przydział mobilizacyjny)
- emeryt/rencista

- obywatelstwo
- telefon
- wykształcenie, nazwa szkoły i rok
- staż pracy
- tytuł zawodowy
- zawód wyuczony zasadniczy
- zawód wykonywany
- ukończone kursy
- uzyskane kwalifikacje
- warunki zatrudnienia
- nieobecności w pracy
- historia pracy, kary, nagrody

17. Płace

- dane osobowe pracowników (imię i nazwisko, pesel, adres zamieszkania, data i miejsce urodzenia, imiona rodziców)
- dane płacowe każdego pracownika.
- numer konta bankowego
- kartoteka ZUS każdego pracownika
- deklaracje PIT – 11 , PIT – 4R

18. Rejestr wyborców

- status
- pesel
- nazwisko i imię, imiona
- adres
- imię ojca
- data urodzenia

WÓJT GMINY
mgr inż. Jan Żelazek

Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Charsznica

1. Wprowadzenie

Celem Instrukcji Zarządzania System Informatycznym jest zapewnienie bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Charsznica, oraz minimalizowanie incydentów mogących zagrozić bezpieczeństwu systemu.

Podstawa prawna tego dokumentu:

- rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024)
- ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Z 2002 r. Nr 101, poz. 926 z późn. zm.)

2. Definicje

Ilekroć w niniejszym dokumencie jest mowa o:

- a) urządzie – należy przez to rozumieć Urząd Gminy Charsznica,
- b) Administratorze Danych Osobowych – należy przez to rozumieć Wójta Gminy Charsznica ,
- c) Administratorze Bezpieczeństwa Informacji – należy przez to rozumieć pracownika urzędu wyznaczonego do nadzorowania i przestrzegania zasad ochrony, określonych w niniejszym dokumencie, Polityce Bezpieczeństwa Danych Osobowych w Urzędzie Gminy Charsznica, oraz wymagań w zakresie ochrony wynikających z powszechnie wynikających przepisów o ochronie danych osobowych oraz odpowiedzialnego za funkcjonowanie systemu informatycznego.
- d) użytkownika 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,
- e) sieci lokalnej - połączenie komputerów pracujących w urzędzie w celu wymiany danych (informacji) dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych,
- f) danych osobowych - rozumie się przez to wszystkie informacje dotyczące zidentyfikowanej lub możliwej od zidentyfikowania osoby fizycznej,
- g) zbiorze danych – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych wg określonych kryteriów,
- h) wykazie zbiorów danych osobowych – rozumie się przez to wykaz zarejestrowanych jak i nie podlegających rejestracji zbiorów danych osobowych,
- i) przetwarzaniu danych - rozumie się to w tym dokumencie, jako jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemie informatycznym,
- j) systemie informatycznym - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

3. Procedury nadawania i zmiany uprawnień do przetwarzania danych osobowych w systemie informatycznym

- a) Każdy użytkownik systemu informatycznego przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:
 - polityką bezpieczeństwa danych osobowych w Urzędzie Gminy Charsznica
 - niniejszym dokumentem
- b) Zapoznanie się z powyższymi informacjami pracownik potwierdza własnoręcznym podpisem na wykazie, którego wzór stanowi załącznik nr 1 do niniejszej instrukcji.
- c) Przetwarzanie danych osobowych może dokonywać jedynie pracownik posiadający upoważnienie Administratora Danych Osobowych, którego wzór stanowi załącznik nr 2 do niniejszej instrukcji.
- d) Administrator Bezpieczeństwa Informacji przyznaje uprawnienia w zakresie dostępu do systemu informatycznego służącego do przetwarzania danych osobowych na podstawie pisemnego upoważnienia Administratora Danych Osobowych określającego zakres uprawnień pracownika.
- e) Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora, hasła, oraz ustanowienia zakresu dostępnych danych i operacji.
- f) Hasło ustanowione podczas przyznawania uprawnień przez Administratora Bezpieczeństwa Informacji jest przekazywane użytkownikowi ustnie.
- g) Pracownik ma prawo do wykonywania tylko tych czynności, do jakich został upoważniony.
- h) Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła.
- i) Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą, jako naruszenie podstawowych obowiązków pracowniczych.
- j) Pracownik zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest do zachowania ich w tajemnicy. Tajemnica obowiązuje go również po ustaniu zatrudnienia
- k) Odebranie uprawnień pracownikowi następuje na pisemny wniosek Administratora Danych Osobowych z podaniem daty i przyczyny odebrania uprawnień
- l) Kierownicy komórek organizacyjnych zobowiązani są pisemnie informować Administratora Bezpieczeństwa Informacji o każdej zmianie dotyczącej podległych pracowników mającej wpływ na zakres posiadanych uprawnień w systemie informatycznym.
- m) Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane, oraz unieważnić jej hasło.
- n) Administrator Bezpieczeństwa Informacji zobowiązany jest do prowadzenia, ochrony rejestru użytkowników, oraz ich uprawnień w systemie informatycznym.
- o) Rejestr powinien odzwierciedlać aktualny stan systemu w zakresie użytkowników i ich uprawnień.

4. Zasady ustalania i posługiwania się hasłami.

- a) Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
- b) Hasło użytkownika musi być zmienione przynajmniej raz w miesiącu.
- c) Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.
- d) Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.
- e) Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
- f) Pracownik nie ma prawa udostępniania swojego hasła innym osobom.
- g) Hasło należy wprowadzać w sposób, który uniemożliwi innym osobom jego poznanie.
- h) W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła.

- i) Przy wyborze hasła zakazuje się stosować
 - haseł, z których użytkownik korzystał w poprzednim miesiącu,
 - swojej nazwy użytkownika w jakiejkolwiek formie,
 - swojego nazwiska czy imienia w jakiejkolwiek formie
 - ogólnie dostępnych informacji o użytkowniku takich jak numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego, nazwa ulicy, na której mieszka itp.
 - przewidywalnych sekwencji znaków z klawiatury np. „QWERTY”, „12345” itp.
- j) należy stosować:
 - hasła zawierające kombinacje liter, cyfr i znaków specjalnych,
 - hasła które można zapamiętać bez zapisywania.
- k) Zmiany hasła nie można zlecać innym osobom.

5. Procedury rozpoczęcia, zawieszania i zakończenia pracy w systemie.

- a) Przed rozpoczęciem pracy z komputerem należy zalogować się do systemu informatycznego przy użyciu własnego indywidualnego identyfikatora i hasła.
- b) W sytuacji opuszczenia stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wylogować się z systemu.
- c) Przed wyłączeniem komputera należy zakończyć pracę wszystkich używanych programów i wykonać o ile to możliwe prawidłowe zamknięcie systemu.
- d) Niedopuszczalne jest wyłączanie komputera bez prawidłowego zamknięcia wszystkich programów i wylogowania z sieci komputerowej.

6. Kopie bezpieczeństwa danych osobowych.

- a) Kopie bezpieczeństwa danych osobowych przygotowywane i archiwizowane są przez Administratora bezpieczeństwa informacji.

7. Przechowywanie elektronicznych nośników informacji zawierających dane osobowe oraz wydruków.

- 1. Elektroniczne nośniki informacji
 - Dane osobowe w postaci elektronicznej (nie licząc kopii bezpieczeństwa) zapisane na dyskach magnetoptycznych, dyskach twardych nie można wynosić poza siedzibę urzędu.
 - Wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych.
 - Po zakończeniu pracy przez użytkowników systemu, elektroniczne nośniki informacji są przechowywane wyłącznie w zamkniętych szafach biurowych.
 - Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymywania danych osobowych pozbawia się wcześniej zapisu tych danych.
 - Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych. W przypadku, gdy nie jest to możliwe uszkadza się je w sposób uniemożliwiający ich odczytanie.
 - Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej.
- 2. Wydruki
 - W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym dostęp osobom nieuprawnionym.
 - Pomieszczenie, w którym przechowywane są wydruki musi być zamknięte na klucz po godzinach pracy urzędu.

- Wydruki zawierające dane osobowe w momencie przekazania do usunięcia są niszczone w sposób uniemożliwiający ich odczytanie (w specjalnej niszczarce do papieru).

8. Ochrona przed złośliwym oprogramowaniem.

- a) Każdy komputer służący do przetwarzania danych osobowych jest wyposażony w działający cały czas program antywirusowy.
- b) Zabrania się stosowania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Za skanowanie odpowiedzialny jest użytkownik komputera.
- c) Poczta elektroniczna jest automatycznie sprawdzana przez skaner antywirusowy.
- d) Wykrycie wirusa użytkownik komputera ma obowiązek zgłosić natychmiast administratorowi bezpieczeństwa informacji.

9. Połączenie do sieci Internet.

- a) Połączenie z siecią Internet (siecią publiczną) zabezpieczone jest przez moduł firewall działający na routerze sieciowym.
- b) Na każdym komputerze w systemie informatycznym urzędu działa osobny firewall.
- c) Zabronione jest połączenie z siecią Internet z nie działającym programem antywirusowym (lub jego brakiem) i firewallem.

WÓJTA MINY
mgr inż. Jan Żebrak



WZÓR

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

Lp.	Imię i Nazwisko	Stanowisko	Data	Podpis

WÓJT GMINY
mgr inż. Jan Żebrak

WZÓR

Miechów-Charsznica, 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)

WÓJT GMINY
mgr inż. Jan Żebrak