Załącznik Nr 2 do zarządzenia Nr 42/07 Wójta Gminy Brańsk z dnia 8 października 2007 r.

Polityka bezpieczeństwa przetwarzania danych osobowych

w Urzędzie Gminy Brańsk

SPIS TREŚCI:

WPROWADZENIE

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemie informatycznym w Urzędzie Gminy Brańsk. Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemu informatycznego wspomagającego pracę Urzędu. Dokument określa 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 przetwarzania danych osobowych w Urzędzie Gminy Brańsk", zwany dalej „Polityką bezpieczeństwa", przeznaczony jest dla osób zatrudnionych przy przetwarzaniu tych danych.

Potrzeba jego opracowania wynika z § 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" obowiązuje wszystkich pracowników Urzędu Gminy Brańsk.

2. Administrator danych, którym jest Wójt, swoją decyzją wyznacza Administratora Bezpieczeństwa Informacji danych zawartych w systemie informatycznym Urzędu, zwanego dalej "Administratorem Bezpieczeństwa", oraz Administratora systemu informatycznego.

3. "Administrator Bezpieczeństwa" realizuje zadania w zakresie ochrony danych, wynikające z przepisów, określone w zakresie czynności.

Rozdział 1

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, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych

2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona 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. Przypadki zakwalifikowane jako naruszenie 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,
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 2

ZABEZPIECZENIE DANYCH OSOBOWYCH

1. Administrator bezpieczeństwa informacji jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemie informatycznym Urzędu, 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 ochronie, oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.

2. Do zastosowanych środków technicznych należy:

1) przetwarzanie danych osobowych w wydzielonych pomieszczeniach położonych w strefie administracyjnej,
2) zabezpieczenie wejścia do pomieszczeń, o których mowa w ppkt. 1,
3) wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji,

3. Do zastosowanych środków organizacyjnych należą przede wszystkim następujące zasady:

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 ppkt. 1, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych,

4. 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.

5. Wykaz budynków, pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe , oraz opis programów zawiera załącznik **nr 1** do niniejszego dokumentu.

6. Opis struktur zbiorów danych zawiera załącznik **nr 2** do niniejszego dokumentu.

7. W celu ochrony przed utratą danych w Urzędzie Gminy Brańsk stosowane są następujące zabezpieczenia:

1) ochrona komputerów przed zanikiem zasilania poprzez stosowanie zasilaczy zapasowych UPS,
2) ochrona przed utratą zgromadzonych danych przez robienie kopii zapasowych na nośnikach magnetycznych, z których w przypadku awarii odtwarzane są dane i system operacyjny

8. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu:

W systemie informatycznym Urzędu zastosowano autoryzację użytkownika. Autoryzacji należy dokonać uruchamiając program użytkowy, podając login użytkownika i hasło. Dostęp do wybranej bazy danych Urzędu uzyskuje się po poprawnym zalogowaniu się do systemu informatycznego Urzędu.

9. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu poprzez Internet.

W zakresie dostępu z sieci wewnętrznej Urzędu do sieci Internet zastosowano środki ochrony przed podsłuchiwaniem, penetrowaniem i atakiem z zewnątrz. Zastosowano firewall, który ma za zadanie uwierzytelnianie źródła przychodzących wiadomości oraz filtrowanie pakietów w oparciu o adres IP, numer portu i inne parametry. Ściana ogniowa składa się z bezpiecznego systemu operacyjnego i filtra pakietów. Ruch pakietów, który firewall przepuszcza jest określony przez administratora. Oprócz filtra pakietów (firewall) zastosowano również system wykrywający obecność wirusów w poczcie elektronicznej.
W efekcie zapewnione jest:

1) zabezpieczenie sieci przed atakiem z zewnątrz poprzez blokowanie wybranych portów,
2) filtrowanie pakietów i blokowanie niektórych usług,
3) objęcie ochroną antywirusową wszystkich danych ściąganych z Internetu na stacjach lokalnych,

10. Postanowienia końcowe.

1) zabezpieczenie przed nieuprawnionym dostępem do danych, prowadzone jest przez Administratora Bezpieczeństwa zgodnie z przyjętymi procedurami nadawania uprawnień do systemu informatycznego.
2) osoby mające dostęp do danych powinny być przeszkolone z zakresu ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997r. (Dz. U. Nr 133, poz. 883 z późn. zm.) i podpisują indywidualny zakres czynności osoby zatrudnionej przy przetwarzaniu danych osobowych stanowiący załącznik nr 3 do niniejszego dokumentu. Wzór wykazu osób, które zostały zapoznane z „Polityką bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy Brańsk", przeznaczonej dla osób zatrudnionych przy przetwarzaniu tych danych stanowi załącznik nr 4 do niniejszego dokumentu.

Rozdział 3

MONITOROWANIE ZABEZPIECZEŃ

1. Prawo do monitorowania systemu zabezpieczeń posiadają :
   1) Administrator Danych,
   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 4

SZKOLENIA

1. Wszyscy pracownicy Urzędu mają obowiązek brać udział w szkoleniach, organizowanych przez Administratora Bezpieczeństwa ,
2. Szkolenie powinno dotyczyć:

   1) obowiązujących przepisów i 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 5

NISZCZENIE WYDRUKÓW I 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.
5. Wydruki po wykorzystaniu należy zniszczyć w mechanicznej niszczarce do papieru.

Rozdział 6

ARCHIWIZACJA DANYCH

1. Dane systemów kopiowane są w systemie miesięcznym,
2. Kopie awaryjne danych zapisywanych w programach wykonywane są nie rzadziej niż raz w miesiącu,
3. Odpowiedzialnym za wykonywanie kopii danych i kopii awaryjnych jest Administrator systemów informatycznych,
4. Na koniec danego miesiąca wykonywane są kopie bezpieczeństwa z całego programu przetwarzającego dane. Nośniki z kopiami bezpieczeństwa przechowywane są w metalowej szafie.
5. Kopie awaryjne przechowywane są w metalowej szafie. Dyskietki , na których zapisywane są kopie bezpieczeństwa są każdorazowo wymazywane i formatowane, w taki sposób, by nie można było odtworzyć ich zawartości.
6. Płyty CD, DVD na których przechowuje się kopie awaryjne niszczy się w sposób mechaniczny , tak by nie można było użyć ich ponownie,
7. Administrator Bezpieczeństwa Informacji odpowiedzialny jest za dokonywanie wymiany kopii awaryjnych na aktualne,
8. Administrator Bezpieczeństwa Informacji dokonuje okresowej weryfikacji kopii bezpieczeństwa pod kątem ich przydatności,

Rozdział 7

POSTANOWIENIA KOŃCOWE

W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity 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).

Uwaga!

Osoby odbywające staż, praktykę mają wgląd do danych osobowych oraz do systemu informatycznego na podstawie upoważnienia nadanego przez Administratora danych.

Załącznik nr 3 do Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Brańsk

Urząd Gminy Brańsk **ul. Rynek 8** **17-120 Brańsk**	***INDYWIDUALNY ZAKRES CZYNNOŚCI*** **NR / OSOBY ZATRUDNIONEJ** **PRZY PRZETWARZANIU** **DANYCH OSOBOWYCH**
Imię i nazwisko pracownika:	
Stanowisko	Nazwa komórki organizacyjnej:

Przetwarzanie danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych ***(art. 7 pkt 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz. U. z 2002r. Nr 101, poz. 926, z późn. zm.).***

Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej ***(art. 6 ust.1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz. U. z 2002r. Nr 101, poz. 926, z późn. zm.).***

- Obowiązkiem każdego pracownika Urzędu Gminy jest zachowanie tajemnicy państwowej i służbowej, również w zakresie ochrony danych osobowych gromadzonych i przetwarzanych przez Urząd. Obowiązek ten istnieje również po ustaniu zatrudnienia.
- Dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
- Dokumentów materialnych (w formie elektronicznej, papierowej itp.) z danymi osobowymi nie można pozostawiać bez dozoru, ani udostępniać osobom nieupoważnionym.
- Dokumentacji z danymi nie wolno wykorzystywać do innych celów niż służbowe.
- Dokumentację z danymi nie wolno udostępniać nieuprawnionym.
- Pracownik musi dopilnować, aby monitor usytuowany był tak, by ekran był niewidoczny dla osób wchodzących do pomieszczenia.
- Przy krótkotrwałych przerwach w pracy należy stosować blokady stacji roboczych
- Pracownik może uzyskać dostęp do systemu tylko i wyłącznie jako użytkownik na swoje hasło. Ustala się czas, po którym system wymusza zmianę hasła na 30 dni.
- Oprogramowanie wgrywa tylko i wyłącznie administrator systemu informatycznego, nie wolno tego robić samodzielnie.
- Pracownik odpowiada za wykonany wydruk. W przypadku wykonania wydruku z użyciem drukarki sieciowej osoba po wydaniu polecenia jest obowiązana udać się niezwłocznie do pomieszczenia drukarki i przejąć drukowany dokument.
- Wydrukowane nadmiarowe, niepotrzebne lub błędne dokumenty należy niezwłocznie, trwale zniszczyć.
- Wszelkie informacje, w tym w formie tradycyjnej lub na nośnikach przesyłanych pocztą, zawierające dane osobowe wysyłane poza Urząd Gminy przekazane mogą zostać tylko po zarejestrowaniu przez kancelarię.

1/2

2. Zostałam/em zaznajomiona/y z przepisami dotyczącymi ochrony danych osobowych, Ustawy o ochronie danych osobowych z dnia 29.08.1997r. (Dz. U. 2002 r.101.926 z późn. zm.), z „Polityką bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Brańsk", „Instrukcją zarządzania systemem informatycznym w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Brańsk" oraz „Instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych".
3. Zobowiązuję, się przy przetwarzaniu danych osobowych, do szczególnej dbałości o zachowanie poufności danych związanych z dokumentami znajdującymi się w obrocie w Urzędu Gminy, także dotyczących danych osobowych pracowników, dokumentacji systemu przetwarzania danych oraz infrastruktury sprzętowo - programowej systemu informatycznego.
4. Zobowiązuję się przy przetwarzaniu danych przestrzegania zasad dostępu do danych osobowych.

Oświadczam, że treść niniejszego zakresu jest mi znana i zobowiązuję się do jego przestrzegania.

Wykonano w 3 egzemplarzach
Potwierdzam odbiór 1 egzemplarza

Administrator Danych

Brańsk, dnia .....
.....

(czytelny podpis pracownika)

2/2

Załącznik nr 4 do Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Brańsk

Wykaz osób, które zostały zapoznane z „Polityką bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy Brańsk", przeznaczonej dla osób zatrudnionych przy przetwarzaniu danych.

Przyjąłem/am/ do wiadomości i stosowania zapisy Polityki bezpieczeństwa.

Nazwisko i Imię	Komórka organizacyjna	Data, podpis

§ 2. Instrukcja 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 telekomunikacyjnej mogą wskazać na naruszenie zabezpieczeń tych danych.

pracę w programie /aplikacji/, zakończyć pracę w sieci (wylogować się) i wyłączyć komputer.
2. Osoba zatrudniona przy przetwarzaniu danych osobowych, która stwierdziła naruszenie zabezpieczenia bazy danych osobowych w systemie informatycznym, zobowiązana jest niezwłocznie powiadomić o tym administratora bezpieczeństwa informacji lub upoważnioną przez niego osobę, a w przypadku ich nieobecności – bezpośrednio administratora danych osobowych.
3. Po dokonaniu czynności, o której mowa w ust. 2, należy sporządzić notatkę służbową z opisem sytuacji wskazującej na naruszenie lub możliwość naruszenia zabezpieczeń systemu informatycznego i przekazać ją administratorowi bezpieczeństwa informacji.
4. Administrator bezpieczeństwa informacji analizuje okoliczności naruszenia bezpieczeństwa danych, przygotowuje informację o przyczynach, przebiegu i wnioskach ze zdarzenia oraz przekazuje ją administratorowi danych osobowych. Jeżeli zachodzi konieczność, przygotowuje zmiany do „Instrukcji zarządzania systemami informatycznymi" w celu wyeliminowania podobnych sytuacji w przyszłości.

R a p o r t
z naruszenia bezpieczeństwa systemu informatycznego w Urzędzie Gminy Brańsk

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

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. Podjęte działania:

.....
.....

6. Przyczyny wystąpienia zdarzenia:

.....
.....

7. Postępowanie wyjaśniające:

.....
.....

.....
data, podpis Administratora Bezpieczeństwa Informacji