Wójt Gminy
Buczkowice

ZARZĄDZENIE Nr 24

Kierownika Urzędu Gminy Buczkowice

z dnia 27 października 2004r.

w sprawie wprowadzenia „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" oraz wyznaczenia administratora bezpieczeństwa informacji.

Działając na podstawie art. 33 ust.5 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (tekst jednolity Dz.U. z 2001r. Nr 142, poz.1591 z późn. zm.) w związku z art.36 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002r. Nr101. poz.926 z późn. zm.) oraz § 3 i 5 Rozporządzenia 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. z 2004r. Nr 100 poz. 1024)

zarządzam co następuje;

§ 1

1. W celu uregulowania spraw związanych z ochroną danych osobowych, zgodnie z wymaganiami wynikającymi z obowiązujących w tym zakresie przepisów wprowadzam niniejszą „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych " stanowiącą załącznik nr 1 do zarządzenia.

2. Wyznaczam Pana Przemysława Lubińskiego jako osobę odpowiedzialną za ochronę danych osobowych w systemie informatycznym Urzędu Gminy Buczkowice, a w szczególności za przeciwdziałanie dostępowi osób nieupoważnionych do systemu, w którym są przetwarzane dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń zabezpieczeń, zwaną dalej „administratorem bezpieczeństwa informacji".

3. Zobowiązuję kierowników gminnych jednostek organizacyjnych do wyznaczenia administratora bezpieczeństwa informacji spośród podległych im pracowników oraz opracowania dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych w kierowanych przez nich jednostkach.

§ 2

1. Traci moc Zarządzenie nr 9 Kierownika Urzędu Gminy Buczkowice z dnia 30 czerwca 2003r. w sprawie ochrony danych osobowych w Urzędzie Gminy Buczkowice oraz w gminnych jednostkach organizacyjnych,
oraz Zarządzenie Nr 10 Kierownika Urzędu Gminy Buczkowice
z dnia 30 czerwca 2003r. w sprawie wprowadzenia instrukcji dotyczącej ochrony danych osobowych.

§ 3

1. Wykonanie zarządzenia powierza się Sekretarzowi Gminy.

§ 4

1. Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT
Józef Kapusta

Załącznik nr 1
do Zarządzenia Nr 24
Kierownika Urzędu Gminy Buczkowice
z dnia 27 października 2004r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

URZĄD GMINY BUCZKOWICE

2004r.

I. POSTANOWIENIA OGÓLNE

1. Instrukcję opracowano na podstawie:
- art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.jedn. Dz.U.z 2002, Nr 101,poz.926 z późń.zm),
- § 3 ust. 1 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).

2. Niniejsza instrukcja reguluje sposób zarządzania systemami informatycznymi Urzędu Gminy Buczkowice a w szczególności określa:

   1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym,
   2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem,
   3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu,
   4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania,
   5) sposób, miejsce i okres przechowywania nośników informacji i kopii zapasowych,
   6) sposób zabezpieczenia systemu informatycznego,
   7) sposób realizacji wymogów określonych w § 7 ust.1 pkt 4 w/w rozporządzenia,
   8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

3. W Urzędzie Gminy Buczkowice następujące zbiory danych osobowych są przetwarzane przy użyciu systemu informatycznego:

   1) Urząd Stanu Cywilnego –I piętro, pok. Nr 6B, Komputerowy System Rejestracji Aktów Stanu Cywilnego „Technika USC Gliwice".

2) Ewidencja ludności i dowody osobiste –
ewidencja ludności - I piętro, pok. Nr 9, program ELUD firmy Radix's software i dowody osobiste – I piętro, pok. Nr 7, SOO IDL System

3) Podatki i opłaty lokalne –
-System POSESJA- I piętro, pok. Nr 10,12,13, oprogramowanie Firma Rekord,
-System ROLNY- I piętro, pok. Nr 10,12,13, oprogramowanie Firma Rekord,
-System POJAZDY -I piętro, pok. Nr 13, oprogramowanie Firma Rekord,
-System REX - I piętro, pok. Nr 13, oprogramowanie Firma Rekord

4) Płace i podatek dochodowy od osób fizycznych- I piętro, pok.Nr 6A, oprogramowanie Firma Rekord

5) Fakturowanie- sprzedaż, I piętro, pok. Nr 6A, 12, 14A, oprogramowanie Firma Rekord

II. PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

1. Użytkownikami systemu informatycznego Urzędu Gminy Buczkowice są wyłącznie pracownicy Urzędu.

2. Osobą upoważnioną do podjęcia decyzji o dopuszczeniu nowego pracownika do systemu informatycznego jak i o utworzeniu nowego konta dla tego użytkownika w sieci jest Wójt Gminy Buczkowice – Administrator Danych Osobowych.

3. Utworzenie nowego konta wraz z nadanymi uprawnieniami dla nowego użytkownika następuje na pisemny wniosek kierownika referatu, w którym pracuje nowy użytkownik, skierowany do Wójta Gminy, zaopiniowany przez Administratora Bezpieczeństwa Informacji.
4. Wniosek o utworzenie konta w systemie informatycznym winien zawierać:
- imię i nazwisko pracownika,
- nazwę komórki organizacyjnej,
- listę aplikacji do których nowy użytkownik ma mieć dostęp (przez aplikacje określa się zasoby systemu informatycznego do których użytkownik będzie posiadał uprawnienia) wraz z zakresem uprawnień przydzielanych dla poszczególnych zasobów systemu.
- wyraźne określenie statusu konta, a w szczególności kiedy nowe konto będzie o charakterze czasowym – dotyczy pracowników z atrudnionych n a czas określony, umowę zlecenie.

5. Na wniosek Administratora Bezpieczeństwa Informacji po akceptacji wniosku przez Wójta Gminy informatyk tworzy konto na podstawie wytycznych zawartych we wniosku.

6. Administrator Bezpieczeństwa Informacji informuje kierownika referatu o dokonaniu czynności i przeprowadza szkolenie wstępne użytkownika w zakresie użytkowania przydzielonego konta, zaś w przypadku korzystania przez użytkownika z systemu przetwarzania danych osobowych przeprowadzane jest dodatkowe szkolenie w zakresie bezpieczeństwa danych osobowych.

7. Nowy użytkownik otrzymuje:
- identyfikator sieciowy wraz z hasłem sieciowym o określonym schemacie opisanym w rozdziale III, pkt 1a i 2a
- hasło dostępu niezbędne do uruchomienia stanowiska komputerowego o określonym schemacie opisanym w rozdziale III, pkt 2b
- w przypadku, kiedy nowy użytkownik będzie pracował z systemem przetwarzania danych otrzymuje identyfikator oraz hasło do tego systemu

8. Nazwa katalogu sieciowego (katalog na serwerze plików w którym użytkownik może umieszczać niezbędne do pracy zasoby) użytkownika jest taka sama jak jego identyfikator w systemie sieciowym.

9. Konto sieciowe ustawiane na serwerze plików może posiadać status
- **pełnych uprawnień** – stan normalnej pracy użytkowników posiadających pełne uprawnienia
- **czasowo zawieszone** – co oznacza brak możliwości korzystania z zasobów serwera jak i innych systemów informatycznych.

- **czasowo ograniczone** – co oznacza czasowe lub stałe ograniczenie praw dostępu do zasobów systemu informatycznego wg indywidualnie określonych kryteriów (stosowane np. w okresie wypowiedzenia umowy o pracę, lub w okresie próbnym),
- **usunięte** – np. na wniosek administratora danych.

10. Każdy użytkownik systemu informatycznego jest zobowiązany do zgłoszenia administratorowi bezpieczeństwa informacji konieczności zmiany hasła dostępu do stanowiska oraz jego hasła do konta sieciowego, nie rzadziej niż raz na 30 dni w przypadku przeoczenia przez administratora w procesie zmian haseł tegoż użytkownika.

11. System informatyczny Urzędu Gminy Buczkowice wprowadza podział na rodzaje haseł:

- **dostępu** do stanowiska pracy– hasło zdefiniowane przy starcie komputera,
- **sieciowe** – hasło do konta założonego na serwerze plików
- **do aplikacji** przetwarzania danych – oddzielne hasło do systemu przetwarzania danych.

13. Wszystkie rodzaje haseł są chronione i nie mogą być udostępniane innym osobom niż uprawnione.

14. Użytkownik ma obowiązek zamykania systemu informatycznego po zakończeniu pracy. Stanowisko komputerowe z uruchomionym systemem, programem nie może pozostawać bez kontroli pracującego na nim użytkownika.

15. Użytkownik ma obowiązek po zakończeniu pracy wyłączyć komputer oraz odłączyć go od źródła zasilania energią elektryczną (wyłączenie zasilacza awaryjnego UPS lub listwy z filtrem przeciw-przepięciowym).

16. Osoby dopuszczone do obsługi programu komputerowego obowiązane są do zachowania tajemnicy (dostępu do danych osobowych i ich merytorycznej treści), a w szczególności na temat zabezpieczeń obowiązujących w Urzędzie Gminy. Obowiązek ten istnieje również po ustaniu zatrudnienia.

17. Wszelkie wydruki zawierające dane osobowe winny być przechowywane w miejscu uniemożliwiającym ich odczyt przez osoby nieuprawnione, natomiast po upływie czasu ich przydatności powinny być zniszczone (cięte w niszczarkach lub palone).

18. Ekrany monitorów, jeśli warunki techniczne w danym pomieszczeniu związane z układem sprzętu umożliwiają taki układ powinny być ustawione tak, aby uniemożliwiały odczyt osobom postronnym.

19. Użytkownik ma obowiązek utrzymywania w czystości sprzęt komputerowy na wszystkich dostępnych zewnętrznych jego częściach.

20. Zabrania się

- korzystania z konta, haseł oraz sprzętu informatycznego za które odpowiedzialny jest inny użytkownik systemu, przez osobę nie posiadającą uprawnień. W przypadku ujawnienia takich wypadków, konto oraz hasła użytkownika, który nadużył uprawnień zostaną zablokowane przez Administratora Bezpieczeństwa Informacji i o zaistniałym nadużyciu natychmiast zostanie powiadomiony Wójt Gminy,
- udostępnienia swego konta oraz haseł innym użytkownikom lub osobom nie będących użytkownikami sieci. W przypadku ujawnienia takich wypadków, konto oraz hasła użytkownika, który nadużył uprawnień zostaną zablokowane przez Administratora Bezpieczeństwa Informacji i o zaistniałym nadużyciu natychmiast zostanie powiadomiony Wójt Gminy,
- instalowania jakiegokolwiek oprogramowania bez zgody Administratora na komputerach Urzędu,
- wykonywania przy pomocy komputerów oraz oprogramowania będących w użytkowaniu Urzędu prac na własne potrzeby,
- instalowania programów będących w użytkowaniu Urzędu na komputerach nie użytkowanych przez Urząd, chyba, że zostało to ustalone na podstawie specjalnych umów lub porozumień,
- wynoszenia z Urzędu urządzeń systemu informatycznego, danych, programów lub ich kopii,
- dokonywania jakichkolwiek zmian w systemie informatycznym mogących zagrozić stabilności samego systemu. W uzasadnionych przypadkach, gdy zachodzi potrzeba zmiany danych za pomocą programów narzędziowych jest to wykonywane za zgodą Administratora Danych,
- używania jakichkolwiek nośników (nośniki magnetyczne, optyczne,itp.) udostępnianych przez osoby postronne,
- ściągania oprogramowania z Internetu lub materiałów obciążonych prawem autorskim bez zgody samego autora,
- przenoszenia programów komputerowych z własnego stanowiska na inne stanowisko robocze nawet w Urzędzie bez zgody Administratora Danych.

- podawania nazw kont, haseł i informacji związanych z bezpieczeństwem przez telefon, pocztę elektroniczną, i inne media które narażone są na podsłuch.

21. W sytuacji naruszenia ochrony danych osobowych lub stwierdzenia innych nieprawidłowości w zabezpieczeniu systemu informatycznego użytkownik ma obowiązek natychmiast powiadomić Administratora Bezpieczeństwa Informacji.

22. Użytkownik ma obowiązek na każde życzenie Administratora Danych Osobowych lub osoby przez niego upoważnionej oraz Administratora Bezpieczeństwa Informacji udostępnić zasoby programowe komputera w celu stwierdzenia zgodnego (lub nie) z instrukcją użytkowania systemu komputerowego jak i legalności zainstalowanego oprogramowania.

III. METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM

1. Identyfikator

a)sieciowy – składa się z imienia i pierwszej litery nazwiska np. Jan Kowalski będzie posiadał identyfikator jank. Używamy tylko małych liter
b) identyfikator dostępu do aplikacji – jego symbol jest określony przez daną aplikację

2. Typy i struktura haseł

a) Hasła sieciowe - zmiana co miesiąc.
Hasło to musi zawierać:
- minimum 6 znaków
- użycie przynajmniej jednej dużej litery
- użycie jednego znaku specjalnego(~`!@#$%^&*()_-+={[}]|\:;"'<,>.?/)

b) Hasło dostępu do stanowiska generowane jest przy pomocy oprogramowania co 1 miesiąc.
Hasło to musi zawierać:
- minimum 6 znaków
- użycie przynajmniej jednej dużej litery
- użycie jednego znaku specjalnego(~`!@#$%^&*()_-+={[}]|\:;"'<,>.?/)

c) Hasło dostępu do aplikacji
są to hasła stałe, a ich schemat jest uzależniony od danego systemu przetwarzania danych.

3. Przekazywanie hasła:

Hasła przekazywane są przez Administratora Bezpieczeństwa Informacji lub informatyka.

4. Sposób przechowywania haseł

Wykaz stanowisk wraz z hasłami przechowywany jest w formie pisemnej przez Administratora Bezpieczeństwa Informacji w kasie pancernej, w pomieszczeniu Kasy Urzędu Gminy (I piętro, biuro 14, pomieszczenie objęte alarmem).

IV. PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONE DLA UŻYTKOWNIKÓW SYSTEMU

Pracownik uruchamiający system przetwarzający dane osobowe powinien upewnić się, że od czasu ostatniego ukończenia pracy nie nastąpiło naruszenie zabezpieczeń systemu.(Dane stanowisko nie nosi śladów ingerencji sprzętowej jak i systemowej)

W razie stwierdzenia lub uzasadnionego podejrzenia, że naruszenie miało miejsce, pracownik informuje natychmiast Administratora Bezpieczeństwa Informacji.

1. Użytkownik rozpoczynający pracę odnotowuje w harmonogramie rozpoczęcie pracy na danym stanowisku komputerowym (Jest to wykaz dni miesiąca z wykreślonymi dniami w których to pracownik jest na urlopie lub dni te są dniami wolnymi od pracy)
2. Wpisuje aktualne hasło dostępu do komputera.
3. Wpisuje hasło dostępu sieciowego.
4. Jeżeli istnieje konieczność skorzystania z systemu przetwarzania danych osobowych użytkownik loguje się do tego systemu podając odpowiednie hasło.
5. W przypadku zakończenia pracy z systemem przetwarzania danych osobowych użytkownik wychodzi z systemu upewniając się, że dany system został wyłączony.

6. W przypadku konieczności opuszczenia danego stanowiska pracy użytkownik obowiązany jest wylogować się z systemu sieciowego.
7. Każde stanowisko pracy powinno zawierać aktywny wygaszasz ekranu.
8. W przypadku zmiany użytkownika w trakcie pracy , fakt ten musi być odnotowany w rejestrze zawierającym listę ze szczegółowym spisem dat i godzin pracy z danym system przez innego użytkownika.

V. PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA.

1. Kopie zapasowe obejmują kopie awaryjne oraz kopie bezpieczeństwa.

2. Kopie awaryjne tworzy się poprzez dodatkowe zapisanie danych na serwerze plików w katalogu użytkownika lub na nośniku komputerowym.
   Zapisu takiego dokonuje nie mniej niż raz na tydzień, jak również przed każdym przeglądem lub konserwacją.

3. Kopie bezpieczeństwa wykonywane są poprzez funkcje dostępne w systemie przetwarzania danych osobowych. Kopie takie tworzy się w przypadkach w których jest to niezbędne dla funkcjonowania systemu . Kopie programu będące cudzą własnością , użytkowane w Urzędzie na podstawie umowy licencyjnej, mogą być stosowane równocześnie z programem pierwotnym tylko wtedy gdy umowa nie stanowi inaczej.

4. Kopie zapasowe zapisane na nośnikach należy przechowywać w zamkniętych szafach lub sejfie zlokalizowanych w innych pomieszczeniach niż pomieszczenia, w których przechowywane są dane osobowe.

5. W systemie informatycznym urzędu dla celów bezpieczeństwa informacji wykorzystuje się:
   a) Nośniki danych:
      - magnetyczne – dyskietki 3,5"
      - specjalistyczne kasety do streamer'a(DDS3 24GB 125m)
   b) urządzenia:
      - stacje dyskietek FDD 1.44
      - streamer HP DAT 12/24 GB DDS3 OEM C1554C WEWN

c) narzędzia programowe:

- oprogramowanie CA BRIGHTSTORE ARCSERVE BACK V9 FOR NW
- narzędzia systemowe do tworzenia kopii zapasowych
- funkcje archiwizacyjne dostępne w danym systemie przetwarzania danych osobowych

6. Dla poszczególnych nośników danych wykorzystywanych w urzędzie stosuje się odpowiednie terminy przydatności danego nośnika:

   a)dla nośników magnetycznych(dyskietki)- 2 m-ce
   b)dla kaset do streamer'a 1,5 roku

7. Każdy nośnik, na którym znajdują się dane, a jego okres przydatności został przekroczony lub nośnik uległ uszkodzeniu podlega procesowi niszczenia. Proces ten rozpoczyna się jeśli jest to możliwe od wyczyszczenia danych z nośnika, a kolejnym krokiem jest jego fizyczna destrukcja w taki sposób, aby nośnik nie nadawał się do użycia.

8. Administrator bezpieczeństwa Informacji jest zobowiązany do utrzymywania kopii programów pracujących w Urzędzie i danych wykorzystywanych przez te programy. Istniejące kopie powinny umożliwić odtworzenie na ich podstawie danych i programów na wypadek awarii sprzętu lub oprogramowania. Kopie programów z danymi osobowymi powinny być utrzymywane w dwóch ostatnich wersjach tj. wersja aktualnie pracująca i wersja poprzednia.

9. Dane należy archiwizować przy pomocy procedur archiwizacyjnych dostarczanych wraz z poszczególnymi programami, a dla programów, które takich procedur nie posiadają należy dane archiwizować w wybrany przez informatyka sposób np. procedurami stworzonymi we własnym zakresie.

10. Dane poszczególnych systemów przetwarzania danych osobowych są archiwizowane wg określonych możliwości tego systemu.

11. Ponadto raz w tygodniu dokonywana jest archiwizacja na serwerze przy użyciu przeznaczonego do tego celu programu o nazwie CA BRIGHTSTORE ARCSERVE BACK V9 FOR NW oraz urządzenia streamer HP DAT 12/24 GB DDS3 OEM C1554C WEWN.
Za prawidłowy przebieg procesu archiwizacji odpowiedzialny jest pracownik Urzędu Gminy wyznaczony przez Administratora Danych.

12. Nośniki zawierające zarchiwizowane dane i programy powinny być przechowywane w pewnym oddaleniu od komputerów (w innym pomieszczeniu).
Wskazane jest przechowywanie kopii w sejfie, co pozwoli uchronić je przed zniszczeniem na wypadek pożaru.
Przechowywane kopie powinny być zabezpieczone przed niepowołanym dostępem.

13. Nośniki zawierające zarchiwizowane dane i programy powinny być odpowiednio oznaczone tak aby można było zorientować się jakie dane czy programy i z jakiego dnia zawiera dany dysk.

14. Przed dokonaniem odtworzenia danych z kopii należy wykonać kopie danych aktualnych.

15. Systemy komputerowe , programy oraz nośniki sprawdzane są na obecność wirusa z częstotliwością 1 miesiąca (o ile nie zajdzie inna potrzeba).

16. Urządzenia dyski i inne informatyczne nośniki danych zawierające dane osobowe przed ich przekazaniem innemu podmiotowi należy pozbawić ich zawartości; w przypadku likwidacji uszkodzić w sposób uniemożliwiający odczytanie danych.

17. Naprawę wymienionych urządzeń zawierających dane osobowe, należy wykonać pod nadzorem administratora bezpieczeństwa informacji.

18. W przypadku przekazania sprzętu do serwisu wymagane jest oświadczenie serwisanta o zachowaniu tajemnicy.

VI. SPOSOBY, MIEJSCE I OKRES PRZECHOWYWANIA

1) Wszystkie kopie jeśli jest to możliwe powinny być wykonywane na dwóch nośnikach.
2) Jeden z nośników powinien być przechowywany w innym pomieszczeniu niż to z którego dane pochodzą
3) Drugi nośnik może być przechowywany w tym samym pomieszczeniu co źródło danych.
4) Za miejsce przechowywania nośników danych z poszczególnych źródeł ustalono pomieszczenie Kasy Urzędu - biuro 14 – kasa pancerna

Okres przechowywania w/w nośników jest uzależniony od typu nośnika i od rodzaju danych. Jeśli dany nośnik utracił termin przydatności powinien zostać poddany procesowi likwidacji.

VII. SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO

1. Każde stanowisko komputerowe przyłączone do Internetu jest narażone na ingerencję wirusów komputerowych, inne szkodliwe oprogramowanie oraz wszelkie próby włamań do systemu przez osoby nieupoważnione. Oprócz źródła jakim jest Internet system informatyczny narażony jest na fizyczną ingerencję w system tzn. fizyczne przyłączenie do sieci nośnika ze szkodliwym programem, kradzież sprzętu, itp.

2. Stosując odpowiednie metody zabezpieczeń ryzyko uszkodzeń lub wywołania niestabilności systemu informatycznego można znacznie zminimalizować. Szczególnym zabezpieczeniom podlegają stanowiska z systemami przetwarzania danych osobowych oraz servery. W systemie informatycznym Urzędu stosuje się trzy metody zabezpieczeń :

   a) Fizyczne:
      - alarmy pomieszczeń
      - zakaz wstępu do pomieszczeń chronionych osobom nieupoważnionym,
      - zakaz korzystania z systemu informatycznego przez osoby nieupoważnione

b) programowe
   - programy antywirusowe – bazy aktualizowane przynajmniej raz na dzień
   - w/w hasła

3. W sytuacji, kiedy zaistnieją okoliczności, które świadczą o przełamaniu zabezpieczeń systemu informatycznego Urzędu użytkownik systemu powinien niezwłocznie zgłosić to administratorowi bezpieczeństwa informacji.
   a) W przypadku, kiedy dowody świadczą o fizycznej ingerencji (włamanie, kradzież sprzętu, fizyczna ingerencja w sprzęt –ślady korzystania ze sprzętu ,itp) użytkownik powinien zabezpieczyć pomieszczenie wraz ze stanowiskiem komputerowym, a następnie zawiadomić administratora bezpieczeństwa informacji, który to podejmie dalsze działania.
   b) W przypadku, kiedy dowody świadczą o programowej ingerencji w system(wirus, włamanie do systemu, utrata danych, itp.) użytkownik zabezpiecza stanowisko pracy i informuje o tym fakcie administratora bezpieczeństwa informacji.

VIII. REALIZACJA WYMOGÓW § 7 Rozporządzenia

Wymogi te są w większej części spełnione, za wyjątkiem tych, które nie są zrealizowane z przyczyn funkcjonalnych poszczególnych aplikacji.

Wymogi w pełni będą zrealizowane w przypadku rozszerzenia istniejących systemów o te funkcje wymienione w rozporządzeniu, których nie spełnia obecny stan.

IX. PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH.

1. Przeglądów i konserwacji systemów informatycznych przetwarzania danych osobowych dokonuje się raz na rok. Podczas tych działań sporządza się kopie danych.

2. W przypadku przeglądów lub konserwacji wymagających unieruchomienia systemu na czas dłuższy, należy prace systemu przenieść na inne stanowisko komputerowe.

3. Ponowne podjęcie pracy w systemie, który poddano przeglądowi lub konserwacji, może nastąpić po sprawdzeniu, czy działanie systemu jest prawidłowe.

4. Administrator Bezpieczeństwa Informacji ma prawo i obowiązek dokonywania okresowych kontroli i przeglądów komputerów pod kątem legalności zainstalowanego i używanego na nich oprogramowania. Z każdej kontroli musi być sporządzona notatka, a o wszelkich nieprawidłowościach powinien być powiadomiony pisemnie Wójt Gminy.

5. Procedury wykonywania czynności konserwacyjnych:
   - wykonanie kopii danych
   - uruchomienie jeśli jest to możliwe stanowiska zastępczego
   - dokonanie przeglądu technicznego sprzętu
   - odtworzenie systemu do stanu sprzed konserwacji
   - aktualizacja komponentów systemu
   - testowanie stabilności
   - wykonanie stabilnej kopii systemu i danych

6. Nadzór administratora obejmuje wszystkie punkty systemu informatycznego Urzędu. Administrator powinien reagować na każde informacje które mogą świadczyć o niestabilności systemu.

7. Przekazywanie nośników do naprawy może nastąpić tylko za zgodą administratora, który to musi sporządzić protokół z tego przekazania.

8. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do

-likwidacji
-przekazania podmiotowi nieuprawnionemu do przetwarzania danych
-naprawy

pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie pod nadzorem administratora.

X. PRZEPISY KOŃCOWE

1. Postępowanie w sytuacji naruszenia ochrony danych osobowych

- Na fakt naruszenia systemu informatycznego mogą wskazywać:

-stan stacji roboczej (brak zasilania, problemy z uruchomieniem,)
-wszelkiego rodzaju różnice w funkcjonowaniu systemu, programu (komunikaty informujące o błędach, brak dostępu do funkcji programu, nieprawidłowości w wykonywanych operacjach)
- różnice w zawartości zbioru danych osobowych
- jakość komunikacji w sieci telekomunikacyjnej
- inne sytuacje

- W przypadku, gdy stwierdzono naruszenie zabezpieczenia systemu informatycznego należy niezwłocznie powiadomić administratora danych osobowych lub inną upoważnioną przez niego osobę oraz administratora bezpieczeństwa informacji.
- Administrator bezpieczeństwa Informacji winien skontrolować stan zabezpieczeń i wraz z pracownikiem merytorycznie odpowiedzialnym za przetwarzanie danych co do których zaistniało podejrzenie jej naruszenia – powinien określić czy dane zostały uszkodzone lub naruszone.
- Jeżeli jest to możliwe dane należy odtworzyć z nośników archiwalnych.
- W stosunku do osób naruszających ochronę danych osobowych, winny być wyciągnięte konsekwencje zgodne z ustawą o ochronie danych osobowych.

2. Ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych oraz odpowiedzialnych za archiwizację prowadzi Administrator Bezpieczeństwa Informacji wg wzoru: imię i nazwisko, referat, identyfikator, uprawnienia, nazwa programu data dopuszczenia do przetwarzania danych, data cofnięcia uprawnienia.

WÓJT
Józef Kapusta