Załącznik Nr 2
do zarządzenia Nr VI/110/2011
Wójta Gminy Dobroń
z dnia 29 listopada 2011 roku

Instrukcja zarządzania systemem informatycznym z uwzględnieniem wymogów bezpieczeństwa informacji w Urzędzie Gminy w Dobroniu

Instrukcja określa środki techniczne, aplikacje i inne zasoby wchodzące w skład systemu informatycznego przetwarzającego dane osobowe według Ustawy o ochronie danych osobowych (Dz.U. Nr 133, poz. 883) w Urzędzie Gminy w Dobroniu, a także ustala niezbędne wymogi bezpieczeństwa przetwarzania informacji osobowych oraz odpowiedzialność karną za działania niezgodne z Ustawą o ochronie danych osobowych.

1. **System informatyczny Urzędu Gminy w Dobroniu:**

Pracę Urzędu Gminy w Dobroniu wspomaga system informatyczny oparty na kilkudziesięciu stanowiskach komputerowych z zainstalowanym odpowiednim oprogramowaniem, które jest niezbędne do przetwarzania danych osobowych.

2. **Środki techniczne:**

System informatyczny Urzędu Gminy w Dobroniu oparty jest na sieci komputerowej w skład którego wchodzą: 2 serwery i 24 stanowiska robocze. Wszystkie komputery w sieci są kompatybilne ze standardem PC i pracują pod kontrolą systemu operacyjnego Windows XP oraz Windows 7. Na wszystkich stanowiskach podłączonych do sieci są przetwarzane dane osobowe.

Ponadto, system informatyczny tworzą dodatkowo 2 samodzielne stanowiska robocze, wyposażone w komputery typu PC, na których przetwarzane są dane osobowe.

3. **Określenia fizycznego położenia systemu informatycznego przetwarzającego dane osobowe:**

Dane przetwarzane są w budynku Urzędu Gminy w Dobroniu przy ul. 11 Listopada 9

Wykaz pomieszczeń ze stanowiskami pracującymi w sieci:

- pokój 8,9,10,11 – przetwarzanie danych finansowo-księgowych oraz danych dot. ewidencji podatników podatku rolnego, leśnego i nieruchomości

- pokój 10 - przetwarzanie danych finansowo-księgowych, danych dotyczących płac i wynagrodzeń oraz danych dotyczących ewidencji podatników podatku rolnego, leśnego i nieruchomości

- pokój nr 18 - przetwarzanie danych dotyczących ewidencji odbiorców wody i ścieków

- pokój nr 19 - przetwarzanie danych dotyczących płac i wynagrodzeń

Serwer sieci znajduje się w serwerowni zlokalizowanej w piwnicach budynku

Wykaz pomieszczeń ze stanowiskami samodzielnymi:

- pokój nr 12 i 14 - przetwarzanie danych dotyczących dowodów osobistych

4. Wykaz używanych aplikacji przetwarzających dane osobowe

- program podatkowy PG – firmy MacroSoft z siedzibą w Warszawie

- program płacowy KALI – firmy MacroSoft z siedzibą w Warszawie

- program finansowo-księgowy FIKS – firmy MacroSoft z siedzibą w Warszawie

- program Ewidencji Ludności – firmy Aram Sp z o.o. Warszawa

- program ewidencji odbiorców wody i dostawców ścieków WODA – firmy ????????

Ponadto na serwerze zainstalowany jest program Płatnik ZUS.

5. Instrukcja przydziału identyfikatorów użytkowników:

Identyfikatory i hasła pierwotne pracowników są przydzielane przez administratora systemu informatycznego.

Wymagania dotyczące identyfikatora użytkownika:

- długość: od 3 do 6 znaków alfanumerycznych

- unikalność w skali całego systemu informatycznego

- przynależność identyfikatora do TYLKO jednego użytkownika

- przynależność identyfikatora do TYLKO jednego identyfikatora

- w wypadku wygaśnięcia stosunku pracy pracownika, jego identyfikator podlega natychmiastowej blokadzie oraz nie może zostać przydzielony innej osobie

- system informatyczny nie może pozwalać na jednoczesną pracę jednego użytkownika na dwóch terminalach lub stacjach roboczych

- bezpośredni dostęp do danych osobowych przetwarzanych w systemie może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła

6. Instrukcja przydziału haseł użytkowników:

Administrator tworząc profil nowego użytkownika (określając jego identyfikator)zakłada dla niego hasło pierwotne, które winno zostać zmienione przez nowego użytkownika w obecności administratora systemu.

Wymagania dotyczące hasła użytkownika

- długość: co najmniej 6 znaków alfanumerycznych lub innych

- wprowadzanie hasła musi być bezpieczne – nie może ono być widoczne na ekranie

- każdy użytkownik systemu posiadający identyfikator jest zobowiązanych do posiadania hasła

- hasło (pierwotne) jest zakładane jednocześnie z utworzeniem nowego profilu dla użytkownika i utworzeniem jego identyfikatora

- hasło pierwotne musi zostać zmienione przez użytkownika

- hasło użytkownika powinno być niepospolite i trudne do odgadnięcia

- hasło użytkownika nie może być identyczne jak jego identyfikator

- użytkownik jest zobowiązany do systematycznego zmieniania hasła na nowe; jednak nie rzadziej niż co 30 dni

- użytkownik jest zobowiązany do utrzymania hasła w tajemnicy; w szczególności nie wolno go nigdzie notować, bądź utrwalać w jakiejkolwiek postaci trwałej

- użytkownik jest jedynym właścicielem swojego hasła

- w przypadku ujawnienia hasła musi ono zostać niezwłocznie zmienione oraz należy poinformować o tym osobę odpowiedzialną za bezpieczeństwo systemu informatycznego

- w wypadku wygaśnięcia stosunku pracy pracownika, jego hasło ulega natychmiastowemu unieważnieniu

- lista haseł musi być w systemie przechowywana w postaci pliku utworzonego przy pomocy metod kryptograficznych (szyfrowanie)

7. **Instrukcja przydziału użytkownikowi uprawnień dostępu do systemu informatycznego:**

   Każda osoba dopuszczona do pracy przy przetwarzaniu danych osobowych powinna być zaznajomiona z przepisami dotyczącymi ochrony danych osobowych.

   Uprawnienia dostępu do systemu informatycznego użytkownik może otrzymać po przejściu odpowiedniego przeszkolenia w zakresie wykonywanych obowiązków oraz ustaleniu zakresu prac w systemie informatycznym niezbędnych do prawidłowego i wydajnego wykonywania powinności służbowych. Użytkownikowi uprawnienia dostępu zostają nadane przez administratora bezpieczeństwa informacji lub administratora systemu informatycznego.

8. **Instrukcja rejestrowania się użytkownika:**

   Poprzez rejestrowanie się (logowanie) użytkownika do systemu należy rozumieć podanie przez niego jego identyfikatora oraz wprowadzenie hasła. Jedynie pozytywne rozpoznanie użytkownika (odpowiedni identyfikator + odpowiednie hasło) przez system umożliwia rozpoczęcie pracy związanej z przetwarzaniem danych osobowych i to tylko w takim zakresie, na jaki pozwalają uprawnienia dostępu danego użytkownika.

   Jeżeli używany system operacyjny i/lub oprogramowanie sieciowe bądź aplikacje, w których jest zastosowany system uwierzytelniający, wyświetlają podczas rejestracji datę i czas ostatniej próby logowania oraz liczbę nieudanych prób, użytkownik jest obowiązany dane te weryfikować. W wypadku gdy informacje te różnią się od oczekiwanych, należy bezwzględnie powiadomić administratora systemu informatycznego lub inną osobę odpowiedzialną za bezpieczeństwo danych osobowych.

   Po zakończonej pracy przy przetwarzaniu danych osobowych należy bezzwłocznie się wyrejestrować z systemu informatycznego. Dotyczy to również sytuacji gdy pracownik jest zmuszony opuścić stanowisko pracy na dłuższy okres.

9. **Instrukcja rozpoczęcia i zakończenia pracy:**

   - uruchomienie komputera

- ładowanie systemu operacyjnego
- ładowanie oprogramowania komunikacyjnego
- rejestracja w systemie informatycznym
- uzyskanie dostępu do zasobów – tylko po pozytywnym przejściu procedury uwierzytelniającej
- wyrejestrowanie się z systemu po zakończeniu pracy
- zakończenie działania oprogramowania komunikacyjnego
- zamknięcie systemu operacyjnego
- wyłączenie komputera

10. Awaryjne kopie danych:

- kopie bezpieczeństwa (awaryjne) należy tworzyć poprzez przegranie całej bazy danych bez stosowania żadnych algorytmów kompresji na nośnik, który zostanie specjalnie zabezpieczony przed niepowołanym dostępem jak również przed zdarzeniami losowymi
- kopie bezpieczeństwa może tworzyć jedynie administrator bezpieczeństwa informacji lub osoba przez niego upoważniona
- kopia bezpieczeństwa powinna być czytelnie opisana poprzez umieszczenie na niej następujących informacji:
    - imię i nazwisko osoby, która ją wykonała
    - data utworzenia kopii
    - nazwa aplikacji
    - nazwa zbioru danych
- w czasie tworzenia kopii awaryjnej bazy danych dostęp do zbiorów powinien być zablokowany dla wszystkich użytkowników
- dyski wymienne z kopiami bezpieczeństwa powinny być wyjęte z komputera w czasie bieżącej pracy
- częstotliwość sporządzania kopii awaryjnych:
    - pełna kopia bazy danych – co najmniej raz na tydzień
    - kopia przyrostowa bazy danych (jeżeli aplikacja udostępnia funkcję sporządzania kopii przyrostowej) – co najmniej raz na dzień
- kopie bezpieczeństwa powinny być okresowo poddawane kontroli ich przydatności do użycia
- z uwagi na możliwość fizycznego uszkodzenia nośników magnetycznych bądź ich zużycia, nie należy stosować tego samego nośnika do zapisywania kopii awaryjnej więcej niż 50 razy.

11. Awaryjne kopie systemu operacyjnego i oprogramowania:

Po dokonaniu jakiejkolwiek modyfikacji systemu operacyjnego, zmianie jego konfiguracji lub zainstalowaniu bądź usunięciu jego komponentów należy bezwzględnie utworzyć kopię bezpieczeństwa systemu operacyjnego. Kopię awaryjną należy wykonać również w wypadku

zainstalowania nowego oprogramowania lub deinstalacji już istniejącego. Nośnik zawierający kopię systemu operacyjnego i oprogramowania musi być opisany: data utworzenia oraz przyczyna utworzenia kopii.

12. Zabezpieczenie kopii danych i kopii systemu operacyjnego:

Kopie awaryjne danych oraz kopie awaryjne systemu operacyjnego i oprogramowania powinny być właściwie zabezpieczone przed dostępem osób nieupoważnionych oraz przed skutkami zdarzeń losowych (pożar, powódź, kradzież, i in.)

13. Sposób i czas przechowywania nośników informacji:

- nie należy magazynować zbędnych plików i wydruków
- kopie bezpieczeństwa przechowuje się co najmniej:
  - dzienne – przez 7 dni
  - tygodniowe – przez 1 tydzień
  - miesięczne – przez 1 miesiąc
  - kwartalne – przez 1 kwartał
  - roczne – przez 1 rok
- kopie bezpieczeństwa po upływie okresu przechowywania muszą być skasowane lub fizycznie zniszczone w sposób uniemożliwiający odczytanie danych
- zbędne dokumenty konwencjonalne powinny być zniszczone w niszczarce lub podarte na drobne fragmenty
- wydruki powinno przechowywać się w pomieszczeniach, gdzie nie mają wstępu osoby trzecie

14. Metody i częstotliwość sprawdzania obecności wirusów komputerowych:

Wszystkie komputery osobiste muszą być sprawdzane za pomocą aktualnej wersji programu antywirusowego przez użytkownika danego stanowiska nie rzadziej niż raz w miesiącu. Ponadto, każdorazowo po umieszczeniu dyskietki lub dysku CDROM w komputerze, należy dokonać sprawdzenia nośnika przy pomocy skanera antywirusowego pracującego w tle.

Użytkownik stanowiska podłączonego do sieci Internet jest zobowiązany do każdorazowego sprawdzenia otrzymanej poczty e-mail jak również wszelkich zbiorów uzyskanych z sieci (np. poprzez ftp).

W wypadku wykrycia obecności wirusa na choćby jednym stanowisku, należy dokonać sprawdzenia programem antywirusowym wszystkich komputerów wchodzących w skład systemu informatycznego.

15. Instrukcja instalacji nowego oprogramowania w systemie informatycznym:

- instalacja nowego oprogramowania musi zostać odnotowana przez administratora systemu komputerowego; w szczególności należy zapisać cel i sposób przeprowadzenia instalacji
- należy wykonać kopię bezpieczeństwa systemu operacyjnego oraz zbiorów danych
- instalacja może zostać wykonana tylko z nośników dostarczonych przez producenta aplikacji lub jej dystrybutora
- dopuszcza się stosowanie jedynie aplikacji licencjonowanych

- jeżeli nowo instalowana aplikacja posiada Kartę Rejestracyjną, należy ją wypełnić i wysłać na adres producenta oprogramowania, co umożliwi korzystanie z pomocy technicznej i pozwoli na otrzymywanie wiadomości o nowych wersjach aplikacji i jej uaktualnieniach
- oryginalne nośniki aplikacji należy przechowywać w bezpiecznym miejscu i nie wolno i wypożyczać osobom postronnym

16. Instrukcja korzystania z komputerów przenośnych:

Osoba korzystająca z komputera przenośnego, służącego do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera, w celu zapobiegnięcia dostępowi do danych osobie nieupoważnionej. Komputer przenośny powinien być zabezpieczony hasłem dostępu. Komputera przenośnego nie wolno pozostawiać w samochodzie.

17. Instrukcja korzystania z monitorów i wyświetlaczy komputerowych:

Jeżeli jest to możliwe, w pomieszczeniach gdzie są stanowiska komputerowe przetwarzające dane osobowe, monitory i inne urządzenia wyświetlające powinny być ustawione w sposób uniemożliwiający wgląd w nie osobom postronnym. Ponadto, jeżeli środki techniczne na to pozwalają, monitory i inne urządzenia wyświetlające powinny być zaopatrzone w automatyczne wygaszacze ekranu wyłączające monitor po czasie nieaktywności użytkownika nie dłuższym niż 5 minut. Dodatkowo wygaszacze ekranu powinny być chronione hasłem dostępu.

18. Instrukcja postępowania z uszkodzonymi dyskami zawierającymi dane:

- naprawy i serwis nośników danych dokonują tylko osoby do tego upoważnione
- urządzenia, dyski i inne nośniki informatyczne zawierające dane osobowe przeznaczone do naprawy i/lub serwisu pozbawia się danych przed wykonaniem naprawy lub czynności serwisowych
- jeżeli z powodu awarii urządzenia nie można danych z nośnika usunąć, to naprawa może się odbyć tylko pod kontrolą osoby odpowiedzialnej za bezpieczeństwo informacji osobowych

19. Urządzenia podtrzymujące zasilanie na wypadek przerwy w dostawie energii elektrycznej:

Wszystkie stanowiska wchodzące w skład systemu informatycznego, na których przetwarzane są dane osobowe powinny być zaopatrzone w zasilacze (UPS) zabezpieczające przed przerwami w dopływie prądu. W zasilacz UPS obowiązkowo powinno być wyposażone stanowisko gdzie znajduje się serwer sieci komputerowej.

Zasilacz UPS powinien zapewnić automatyczne zakończenie pracy i wyłączenie serwerów przy zaniku lub nadmiernym wahaniu napięcia – minimalny czas podtrzymywania pracy wynosi 10 minut.

20. Pomieszczenia, w których odbywa się przetwarzanie danych osobowych:

Wszystkie pomieszczenia, w których są stanowiska przetwarzające dane osobowe lub inne urządzenia umożliwiające dostęp do systemu informatycznego, powinny być zaopatrzone w zamknięcia.

Pomieszczenia te muszą być każdorazowo zamykane, gdy nie ma w nich pracowników.

zainstalowania nowego oprogramowania lub deinstalacji już istniejącego. Nośnik zawierający kopię systemu operacyjnego i oprogramowania musi być opisany: data utworzenia oraz przyczyna utworzenia kopii.

12. Zabezpieczenie kopii danych i kopii systemu operacyjnego:

Kopie awaryjne danych oraz kopie awaryjne systemu operacyjnego i oprogramowania powinny być właściwie zabezpieczone przed dostępem osób nieupoważnionych oraz przed skutkami zdarzeń losowych (pożar, powódź, kradzież, i in.)

13. Sposób i czas przechowywania nośników informacji:

- nie należy magazynować zbędnych plików i wydruków
- kopie bezpieczeństwa przechowuje się co najmniej:
  - dzienne – przez 7 dni
  - tygodniowe – przez 1 tydzień
  - miesięczne – przez 1 miesiąc
  - kwartalne – przez 1 kwartał
  - roczne – przez 1 rok
- kopie bezpieczeństwa po upływie okresu przechowywania muszą być skasowane lub fizycznie zniszczone w sposób uniemożliwiający odczytanie danych
- zbędne dokumenty konwencjonalne powinny być zniszczone w niszczarce lub podarte na drobne fragmenty
- wydruki powinno przechowywać się w pomieszczeniach, gdzie nie mają wstępu osoby trzecie

14. Metody i częstotliwość sprawdzania obecności wirusów komputerowych:

Wszystkie komputery osobiste muszą być sprawdzane za pomocą aktualnej wersji programu antywirusowego przez użytkownika danego stanowiska nie rzadziej niż raz w miesiącu. Ponadto, każdorazowo po umieszczeniu dyskietki lub dysku CDROM w komputerze, należy dokonać sprawdzenia nośnika przy pomocy skanera antywirusowego pracującego w tle.

Użytkownik stanowiska podłączonego do sieci Internet jest zobowiązany do każdorazowego sprawdzenia otrzymanej poczty e-mail jak również wszelkich zbiorów uzyskanych z sieci (np. poprzez ftp).

W wypadku wykrycia obecności wirusa na choćby jednym stanowisku, należy dokonać sprawdzenia programem antywirusowym wszystkich komputerów wchodzących w skład systemu informatycznego.

15. Instrukcja instalacji nowego oprogramowania w systemie informatycznym:

- instalacja nowego oprogramowania musi zostać odnotowana przez administratora systemu komputerowego; w szczególności należy zapisać cel i sposób przeprowadzenia instalacji
- należy wykonać kopię bezpieczeństwa systemu operacyjnego oraz zbiorów danych
- instalacja może zostać wykonana tylko z nośników dostarczonych przez producenta aplikacji lub jej dystrybutora
- dopuszcza się stosowanie jedynie aplikacji licencjonowanych

- jeżeli nowo instalowana aplikacja posiada Kartę Rejestracyjną, należy ją wypełnić i wysłać na adres producenta oprogramowania, co umożliwi korzystanie z pomocy technicznej i pozwoli na otrzymywanie wiadomości o nowych wersjach aplikacji i jej uaktualnieniach
- oryginalne nośniki aplikacji należy przechowywać w bezpiecznym miejscu i nie wolno i wypożyczać osobom postronnym

16. Instrukcja korzystania z komputerów przenośnych:

Osoba korzystająca z komputera przenośnego, służącego do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera, w celu zapobiegnięcia dostępowi do danych osobie nieupoważnionej. Komputer przenośny powinien być zabezpieczony hasłem dostępu. Komputera przenośnego nie wolno pozostawiać w samochodzie.

17. Instrukcja korzystania z monitorów i wyświetlaczy komputerowych:

Jeżeli jest to możliwe, w pomieszczeniach gdzie są stanowiska komputerowe przetwarzające dane osobowe, monitory i inne urządzenia wyświetlające powinny być ustawione w sposób uniemożliwiający wgląd w nie osobom postronnym. Ponadto, jeżeli środki techniczne na to pozwalają, monitory i inne urządzenia wyświetlające powinny być zaopatrzone w automatyczne wygaszacze ekranu wyłączające monitor po czasie nieaktywności użytkownika nie dłuższym niż 5 minut. Dodatkowo wygaszacze ekranu powinny być chronione hasłem dostępu.

18. Instrukcja postępowania z uszkodzonymi dyskami zawierającymi dane:

- naprawy i serwis nośników danych dokonują tylko osoby do tego upoważnione
- urządzenia, dyski i inne nośniki informatyczne zawierające dane osobowe przeznaczone do naprawy i/lub serwisu pozbawia się danych przed wykonaniem naprawy lub czynności serwisowych
- jeżeli z powodu awarii urządzenia nie można danych z nośnika usunąć, to naprawa może się odbyć tylko pod kontrolą osoby odpowiedzialnej za bezpieczeństwo informacji osobowych

19. Urządzenia podtrzymujące zasilanie na wypadek przerwy w dostawie energii elektrycznej:

Wszystkie stanowiska wchodzące w skład systemu informatycznego, na których przetwarzane są dane osobowe powinny być zaopatrzone w zasilacze (UPS) zabezpieczające przed przerwami w dopływie prądu. W zasilacz UPS obowiązkowo powinno być wyposażone stanowisko gdzie znajduje się serwer sieci komputerowej.

Zasilacz UPS powinien zapewnić automatyczne zakończenie pracy i wyłączenie serwerów przy zaniku lub nadmiernym wahaniu napięcia – minimalny czas podtrzymywania pracy wynosi 10 minut.

20. Pomieszczenia, w których odbywa się przetwarzanie danych osobowych:

Wszystkie pomieszczenia, w których są stanowiska przetwarzające dane osobowe lub inne urządzenia umożliwiające dostęp do systemu informatycznego, powinny być zaopatrzone w zamknięcia.

Pomieszczenia te muszą być każdorazowo zamykane, gdy nie ma w nich pracowników.

Poza godzinami pracy Urzędu, każdorazowo należy uaktywniać system alarmowy umożliwiający natychmiastowe powiadomienie służb bezpieczeństwa o ewentualnym włamaniu lub innym zdarzeniu.