# INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE GMINY KAMPINOS

Zatwierdził:

Wójt Gminy Kampinos

/-/ dr inż. Monika Ciurzyńska

**Dokumenty powiązane:**

Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Kampinos.

## § 1
## Postanowienia ogólne

1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Kampinos, określa zasady, tryb postępowania i zalecenia Administratora Danych, które muszą być stosowane przez osoby przez niego upoważnione do przetwarzania danych osobowych w systemach informatycznych.
2. Instrukcja została opracowana zgodnie z wymogami § 5 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).
3. Podstawowymi celami zabezpieczeń systemów informatycznych służących do przetwarzania danych osobowych, jest zapewnienie jak najwyższego poziomu bezpieczeństwa przetwarzanych danych osobowych w systemach informatycznych.
4. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania w systemach, charakteru poufnego wraz z zachowaniem ich integralności i rozliczalności.
5. Administrator Bezpieczeństwa Informacji powinien posiadać stosowne uprawnienia w nadzorowanych systemach informatycznych, gwarantujące skuteczne wykonywanie zadań z zakresu nadzoru wszędzie tam, gdzie jest to możliwe. Nie oznacza to automatycznego prawa dostępu do danych osobowych przetwarzanych w tych systemach.

## § 2
## Szkolenia w zakresie ochrony danych osobowych

1. Użytkownicy powinni podlegać okresowym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym (wymiana sprzętu na nowszej generacji, zmiana oprogramowania) oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmianą wewnętrznych regulacji.

## § 3
## Obowiązki Administratora Bezpieczeństwa Informacji

Do obowiązków Administratora Bezpieczeństwa Informacji w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:

1) Nadzór nad stosowaniem zabezpieczeń danych w systemach informatycznych
2) Wskazywanie zagrożeń oraz reagowanie na naruszenia ochrony danych osobowych i usuwanie ich skutków.
3) Prowadzenie ewidencji użytkowników systemów informatycznych, w których przetwarzane są dane osobowe, stanowiącej część ewidencji osób upoważnionych do przetwarzania danych osobowych w Urzędzie.
4) Kontrolowanie nadanych w systemach informatycznych uprawnień do przetwarzania danych osobowych pod kątem ich zgodności z wpisami umieszczonymi w ewidencji osób upoważnionych do przetwarzania danych osobowych.
5) Prowadzenie szkoleń dla użytkowników w zakresie stosowanych zabezpieczeń danych w systemach informatycznych.
6) Uzgadnianie z Administratorem Systemów Informatycznych szczególnych procedur regulujących wykonywanie czynności w systemach służących do przetwarzania danych osobowych w Urzędzie.

7) Zapewnienie doradztwa w zakresie przestrzegania przez współpracowników zasad ochrony danych osobowych przyjętych w Urzędzie Gminy Kampinos.

## § 4
## Obowiązki Administratora Systemów Informatycznych

Do obowiązków Administratora Systemów Informatycznych w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:

1) Realizacja zadań określonych w §6, §9, §23 i §24 Polityki bezpieczeństwa przetwarzania danych osobowych Urzędu Gminy Kampinos.
2) Operacyjne zarządzanie systemami informatycznymi w sposób zapewniający ochronę danych osobowych w nich przetwarzanych.
3) Przestrzeganie opracowanych dla systemu procedur operacyjnych i bezpieczeństwa.
4) Kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej a systemem informatycznym Administratora Danych.
5) Zarządzanie stosowanymi w systemach informatycznym środkami uwierzytelnienia, w tym rejestrowanie i wyrejestrowywanie użytkowników oraz dokonywanie zmiany uprawnień na podstawie zaakceptowanych wniosków przez osobę do tego upoważnioną.
6) Utrzymanie systemu w należytej sprawności technicznej.
7) Regularne tworzenie kopii zapasowych zasobów danych osobowych oraz programów służących do ich przetwarzania oraz okresowe sprawdzanie poprawności wykonania kopii zapasowych.
8) Wykonywanie lub nadzór nad wykonywaniem okresowych przeglądów i konserwacji, zgodnie z odrębnymi procedurami, sprzętu IT, systemów informatycznych, aplikacji oraz elektronicznych nośników informacji, na których zapisane są dane osobowe.

## § 5
## Obowiązki Właścicieli zasobów danych osobowych

Do obowiązków Właścicieli zasobów danych osobowych w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:

1) Zapewnienie, we współpracy z Administratorem Systemów Informatycznych, właściwego poziomu ochrony danych osobowych w systemach, dla danych za które są odpowiedzialni.
2) Informowanie Administratora Bezpieczeństwa Informacji o zmianie celu przetwarzania danych osobowych w systemie lub poszerzeniu zakresu zbieranych danych osobowych.
3) Udostępnianie danych osobowych wyłącznie osobom upoważnionym lub uprawnionym do ich uzyskania.

## § 6
## Obowiązki użytkowników

Do obowiązków użytkowników systemu informatycznego w zakresie ochrony danych osobowych w systemach informatycznych należy w szczególności

1) Przestrzeganie opracowanych dla systemu zasad przetwarzania danych osobowych.
2) Przestrzeganie opracowanych dla systemu procedur operacyjnych i bezpieczeństwa.
3) Uniemożliwienie dostępu lub podglądu danych osobowych w systemie dla osób nieupoważnionych.
4) Wykonywania bez zbędnej zwłoki poleceń Administratora Bezpieczeństwa Informacji w zakresie ochrony danych osobowych, jeśli są one zgodne z przepisami prawa powszechnie obowiązującego.

## § 7
## Bezpieczna eksploatacja systemów informatycznych

1. Jeżeli nic innego nie wynika z przepisów niniejszej Instrukcji użytkownikom zabrania się:
   1) wprowadzania zmian do oprogramowania, sprzętu informatycznego poprzez jego samodzielne konfigurowanie i wyposażanie.
   2) umożliwiania stronom trzecim uzyskiwania nieupoważnionego dostępu do systemów informatycznych.
   3) instalowania nowego lub aktualizowania już zainstalowanego oprogramowania.
   4) korzystania z systemów informatycznych dla celów innych niż związane z wykonywaniem obowiązków służbowych.
   5) korzystania z prywatnego sprzętu informatycznego, w tym oprogramowania oraz nośników pamięci.
   6) podejmowania prób testowania, modyfikacji i naruszenia zabezpieczeń danych w systemach informatycznych lub jakichkolwiek działań noszących takie znamiona.
   7) kopiowania plików zawierających dane osobowe z serwerów na stacje robocze użytkowników i na elektroniczne nośniki informacji, chyba że zgodę na te działania wyrazi Administrator Bezpieczeństwa Informacji.
2. Informacje przetwarzane przy użyciu współdzielonych aplikacji sieciowych na stacjach roboczych muszą być zapisywane na dyskach serwera.
3. Wszystkie aplikacje sieciowe, współdzielone zasoby użytkowe muszą być ulokowane na przeznaczonych do tego celu serwerach.

## § 8
## Nadawanie uprawnień do przetwarzania danych osobowych

1. Użytkownicy systemu przetwarzającego dane osobowe przed przystąpieniem do przetwarzania danych osobowych w tym systemie informatycznym, zobowiązani są zapoznać się z:
   1) Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 Nr 101, poz. 926 z późn. zm.).
   2) Polityką bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Kampinos.
2. Użytkownicy przed dopuszczeniem do obsługi systemu informatycznego, w którym przetwarzane są dane osobowe powinni podlegać przeszkoleniu w zakresie obsługi sprzętu informatycznego, oprogramowania systemowego oraz oprogramowania do obsługi aplikacji, którą będą wykorzystywali.
3. Pierwsze zarejestrowanie użytkownika w systemie i nadanie odpowiednich uprawnień do systemu przetwarzającego dane osobowe musi być poprzedzone złożeniem przez użytkownika oświadczenia o:
   1) Zachowaniu w tajemnicy danych osobowych i sposobów ich zabezpieczania oraz przetwarzaniu danych osobowych zgodnie z przepisami.
   2) Uzyskanie formalnego upoważnienia do przetwarzania danych osobowych.

## § 9
## Metody i środki uwierzytelniania w systemie

1. Identyfikatory i hasła są środkiem gwarantującym rozliczalność, poufność i integralność danych osobowych przetwarzanych w systemach informatycznych. Służą one do weryfikowania tożsamości użytkownika, uzyskania dostępu do określonych zasobów, kont uprzywilejowanych lub uruchomienia określonej funkcjonalności.
2. Mając na uwadze zagwarantowanie wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych oraz zagwarantowania użytkownikom pełnej rozliczalności wykonywanych przez nich operacji w systemach informatycznych, wszyscy użytkownicy przy uwierzytelnianiu do systemów informatycznych powinni stosować się do poniższych zasad:

1) Użytkownik systemu powinien posiadać unikalny identyfikator do swojego osobistego i wyłącznego użytku.
2) Hasła dostępu do systemów informatycznych powinny być tworzone przez użytkownika i stanowią tajemnicę służbową, znaną wyłącznie temu użytkownikowi.
3) Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła dostępu oraz jego przechowywanie.
4) Hasła nie mogą być ujawniane lub przekazywane komukolwiek, bez względu na okoliczności.
5) Użytkownik nie powinien przechowywać haseł w widocznych miejscach, nie powinien umieszczać haseł w żadnych automatycznych procesach logowania (skryptach, makrach lub pod klawiszami funkcyjnymi).

3. Użytkownicy są co do zasady odpowiedzialni za wszelkie działania w systemach informatycznych prowadzone z użyciem ich identyfikatora i hasła.
4. Administrator Systemów Informatycznych jest odpowiedzialny za okresowe sprawdzanie systemu pod kątem występowania w nim nieaktywnych kont użytkowników, oraz informowanie osób, na których wniosek konto zostało utworzone o występowaniu długiego okresu konta.

## § 10
## Wymogi dotyczące uwierzytelniania

1. Wszystkie konta dostępowe (identyfikatory) do systemów informatycznych powinny być chronione hasłem lub innym bezpiecznym, zaakceptowanym przez Administratora Bezpieczeństwa Informacji sposobem uwierzytelniania.
2. Identyfikator oraz nadane uprawnienia powinny umożliwiać wykonywanie czynności wyłącznie zgodnych z zakresem powierzonych obowiązków.
3. Identyfikator użytkownika powinien być niepowtarzalny a po wyrejestrowaniu z systemu informatycznego lub utracie ważności nie może być przydzielany innej osobie.
4. *usunięto*.
5. Użytkownicy powinny wybierać hasła dobrej jakości tzn.:
    1) minimalnej długości - 8 znaków
    2) - zawierające małe i wielkie litery oraz cyfry lub znaki specjalne.
6. Hasła nie mogą być takie same jak identyfikator użytkownika oraz nie mogą być zapisywane w systemach w postaci jawnej.
7. Hasła powinny być utrzymywane w tajemnicy również po upływie ich ważności.
8. Należy unikać ponownego używania starych haseł.
9. Użytkownicy o wysokich uprawnieniach (np. root, administrator) nie powinni wykorzystywać swojego konta do przetwarzania danych osobowych w systemie. Jeśli zajdzie potrzeba przetwarzania danych przez użytkownika o wysokich uprawnieniach, powinno zostać założone dla niego odrębne konto, które nie będzie związane z wysokimi uprawnieniami.
10. Hasła użytkowników o wysokich uprawnieniach powinny być przechowywane w miejscu zabezpieczonym przed dostępem osób nieupoważnionych.
11. Udostępnienie hasła osobie postronnej należy traktować jako incydent naruszenia ochrony danych osobowych.

## § 11
## Wymogi dotyczące zmiany haseł

1. Użytkownik jest zobowiązany zmieniać hasło, w którego posiadaniu się znajduje:
    1) Okresowo, zgodnie z wymaganiami dla danego systemu informatycznego (przed upływem terminu ważności hasła), jego zmiana następuje nie rzadziej niż co 30 dni.
    2) W przypadku ujawnienia lub podejrzenia ujawnienia hasła.
2. W przypadku braku dostępu do konta chronionego hasłem, w którego posiadaniu się znajduje, użytkownik zobowiązany jest wystąpić o zmianę hasła do właściwego Administratora Systemów Informatycznych, w sytuacji:

1) Zapomnienia/zgubienia hasła.
2) Wygaśnięcia ważności hasła.
3) Zablokowania konta spowodowanego nieprawidłowym wprowadzeniem hasła.
4) Braku uprawnień/interfejsu umożliwiających samodzielną zmianę hasła.

## § 12
## Procedura bezpiecznego uwierzytelniania

1. Procedura bezpiecznego uwierzytelniania w systemie informatycznym zapewnia minimalizowanie ryzyka wystąpienia nieautoryzowanego dostępu do systemu. Procedura powinna ujawniać minimum informacji o systemie informatycznym tak, aby nie pozwolić nieuprawnionemu użytkownikowi na uzyskanie dodatkowych wskazówek w celu ich wykorzystania w sposób niedozwolony. W tym celu należy zapewnić:

   1) Komputer wraz z ograniczonymi uprawnieniami dla użytkownika.
   2) Zaktualizowane oprogramowanie systemowe wraz z zabezpieczeniem typu firewall.
   3) Oprogramowanie antywirusowe z modułem kontroli i ochrony tożsamości wraz z aktualną wykupioną subskrypcją.

## § 13
## Wymagania dotyczące sprzętu i oprogramowania

1. Jednostki komputerowe w standardzie zgodnym z 32bit lub 64bit ze wskazaniem na 64bit.
2. Aktualne oprogramowanie systemowe Windows lub MacOS
3. Oprogramowanie zabezpieczające: firewall, antywiurs wraz z subskrybcją.
4. Dostęp do internetu.

## § 14
## Funkcjonalność systemu informatycznego

1. System informatyczny służący do przetwarzania danych osobowych, z wyjątkiem systemu służącego wyłącznie do edycji tekstu w celu udostępnienia go na piśmie, powinien zapewniać dla każdej osoby, której dane osobowe są przetwarzane w tym systemie — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — automatyczne odnotowywanie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych, informacji o dacie pierwszego wprowadzenia danych do systemu oraz o identyfikatorze osoby wprowadzającej dane.
2. W przypadku zbierania danych osobowych od osoby, której dane nie dotyczą należy zapewnić w systemie informatycznym odnotowywanie informacji o źródle pochodzenia danych. Proces ten nie musi odbywać się automatycznie.
3. Dla każdego systemu służącego do przetwarzania danych osobowych, z którego udostępniane są dane osobowe odbiorcom danych, należy zapewnić odnotowanie w bazie danych tego systemu informacji, komu, kiedy i w jakim zakresie dane zostały udostępnione, chyba, że dane pochodzą z jawnego zbioru danych osobowych.
4. Należy zapewnić dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym sporządzenie i wydrukowanie:
   1) Zestawień zakresu i treści przetwarzanych na jej temat danych osobowych.
   2) Zestawienia zawierającego informacje wymagane w § 7 ust. 1 Rozporządzenia.
5. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach, wymagania, o których mowa w § 7 ust. 1 pkt 4 Rozporządzenia, mogą być realizowane w jednej z nich lub w odrębnej aplikacji przeznaczonej do tego celu.

6. Treść ostatecznego rozstrzygnięcia indywidualnej sprawy osoby, której dane dotyczą, nie może być wyłącznie wynikiem operacji na danych osobowych, prowadzonych w aplikacji lub systemie informatycznym.
7. Zabronione jest nadawanie ukrytych znaczeń elementom numerów porządkowych w aplikacjach ewidencjonujących osoby fizyczne
8. Zaleca się wbudowanie do aplikacji funkcjonalności, zapewniających wymuszanie zmiany haseł po zadanym czasie, badania ich długości, jakości i powtarzalności (z użyciem funkcji skrótu).

## § 15
## Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie

1. Przed przystąpieniem do pracy z systemem, użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.
2. W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie ochrony danych osobowych, użytkownik systemu zobowiązany jest postępować zgodnie z procedurą opisaną w § 21 Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Kampinos. Przed opuszczeniem stanowiska pracy, użytkownik obowiązany jest zablokować swoją stację roboczą.
3. Kończąc pracę, użytkownik obowiązany jest do wylogowania się z systemu informatycznego i zabezpieczenia stanowiska pracy, w szczególności wszelkiej dokumentacji, wydruków oraz wymiennych nośników informacji, na których znajdują się dane osobowe i umieszczenia ich zamykanych szafkach.

## § 16
## Przetwarzanie, udostępnianie i likwidacja danych osobowych

1. W przypadku przekazywania urządzeń lub nośników zawierających dane osobowe, poza obszar przetwarzania danych osobowych, zabezpiecza się je w sposób zapewniający poufność, integralność i rozliczalność tych danych, przez co rozumie się:
   1) Ograniczenie dostępu do danych osobowych hasłem zabezpieczającym dane przed osobami nieupoważnionymi.
   2) Stosowanie metod kryptograficznych.
   3) Stosowanie odpowiednich zabezpieczeń fizycznych.
   4) Stosowanie odpowiednich zabezpieczeń organizacyjnych.

   W zależności od stopnia zagrożenia zalecane jest stosowanie kombinacji wyżej wymienionych zabezpieczeń.
2. Kopiowanie przez użytkowników plików z serwerów na stacje robocze użytkowników i na elektroniczne nośniki informacji jest zabronione bez akceptacji ze strony Administratora Danych.
3. W przypadku udostępniania danych osobowych odbiorcy danych w rozumieniu art. 7 pkt 6 Ustawy, użytkownik ma obowiązek odnotować komu i kiedy udostępniono poszczególne dane.
4. Jeżeli dane osobowe nie są pozyskane od osoby, której dotyczą, użytkownik zobowiązany jest odnotować w systemie informatycznym źródło pochodzenia danych.
5. Dla udokumentowania czynności dokonywanych w celu likwidacji zbiorów danych osobowych nie podlegających archiwizacji w odrębnym trybie dla którego cel przetwarzania ustał, Administrator Bezpieczeństwa Informacji lub osoby upoważnione sporządzają protokół, w którym zamieszcza następujące informacje:
   1) Datę dokonania likwidacji.
   2) Przedmiot likwidacji (aplikacja, baza).
   3) Podpisy osób dokonujących i obecnych przy likwidacji zbiorów danych osobowych.
6. Decyzję o likwidacji zbiorów danych osobowych, przetwarzanych w systemach informatycznych podejmują Właściciele zasobów danych osobowych.

7. W przypadku likwidacji elektronicznych nośników informacji, należy dokonać wcześniej skutecznego usunięcia danych z tych nośników. W przypadku gdy usunięcie danych nie jest możliwe, należy uszkodzić nośniki w sposób uniemożliwiający odczyt tych danych na przykład poprzez użycie odpowiedniej niszczarki, urządzenia demagnetyzującego itp.
8. Przed przekazaniem elektronicznego nośnika informacji osobie nieuprawnionej, należy usunąć z nośnika w sposób trwały dane osobowe.

## § 17
## Kopie zapasowe

1. Kopie zapasowe zbiorów danych osobowych oraz programów i narzędzi programowych służących do ich przetwarzania powinny być wykonywane przez Administratora Systemów Informatycznych lub wyznaczone przez Administratora Danych osoby.
2. Kopie zapasowe powinny być tworzone na nośnikach elektronicznych, odpowiednio opisanych, oznakowanych i ewidencjonowanych a każdy proces wykonywania kopii zapasowej powinien być dokumentowany.
3. Kopie zapasowe należy opisywać w sposób umożliwiający szybką i jednoznaczną identyfikację zawartych w nich danych.
4. W celu usystematyzowania procesu wykonywania kopi zapasowej, odpowiedzialny za ten proces Administrator Systemów Informatycznych, jest zobowiązany do sporządzenia harmonogramu wykonywania kopi zapasowej, wraz z opisem narzędzi służących do jej wykonywania, nazwą polityk, nazwą systemu, nazwą bazy danych, terminem okresu przechowywania, rodzajem wykorzystywanego nośnika wraz z numerem seryjnym nośnika.
5. Tworzenie, przechowywanie i likwidację kopii zapasowych powinny regulować szczegółowe instrukcje operacyjne dla poszczególnych systemów informatycznych, opracowywane przez Administratora Systemów Informatycznych, z uwzględnieniem niniejszych postanowień.
6. Administrator Systemów Informatycznych odpowiedzialny, zobowiązany jest przestrzegać terminów sporządzania kopii zapasowych oraz okresowo dokonywać kontroli możliwości odtworzenia danych zapisanych na tych kopiach, pod kątem ewentualnej przydatności w sytuacji awarii systemu.
7. Kopie zapasowe powinny być tworzone w bezpiecznym systemie archiwizacji, który powinien zapewniać ograniczony dostęp fizyczny do nośników oraz przyznanie uprawnień dostępu tylko wyznaczonemu imiennie Administratorowi Systemów Informatycznych oraz Administratorowi Bezpieczeństwa Informacji.
8. Dane z kopii zapasowych powinny być odtwarzane wyłącznie przez Administratora Systemów Informatycznych oraz upoważnionych przez Administratora Danych pracowników.
9. Kopie zapasowe, które uległy uszkodzeniu powinny podlegać natychmiastowemu zniszczeniu.
10. Niszczenia kopii zapasowych, na nośnikach elektronicznych dokonuje Administrator Systemów Informatycznych lub inna upoważniona przez Administratora Danych osoba.
11. Proces niszczenia kopi zapasowych powinien odbywać się komisyjnie i powinien być dokumentowany.

## § 18
## Przechowywanie nośników elektronicznych zawierających dane osobowe

1. Dane osobowe mogą być przechowywane:
   1) Na serwerach zlokalizowanych w obszarach wyznaczonych do przetwarzania danych osobowych.
   2) Na wymiennych nośnikach elektronicznych.
   3) Na poszczególnych stacjach roboczych.
2. Po wykorzystaniu dane osobowe w postaci elektronicznej należy niezwłocznie usunąć z nośnika elektronicznego w sposób uniemożliwiający ich ponowne odtworzenie.
3. Wykorzystanie wymiennych nośników elektronicznych (CD/DVD, pamięć USB, wymienna karta pamięci, dyskietka) powinno być ściśle kontrolowane i dozwolone wyłącznie dla upoważnionych użytkowników.

4. Wymienne nośniki elektroniczne, o ile nie są użytkowane, powinny być przechowywane w zamykanych szafkach.
5. Nośniki zawierające kopie zapasowe powinny być przechowywane w innym pomieszczeniu niż to, w którym umieszczony jest serwer przetwarzający dane osobowe.
6. Kopie zapasowe powinny być przechowywane w odpowiednio zabezpieczonej, ognioodpornej szafie, do której dostęp mogą mieć wyłącznie osoby upoważnione.
7. Nośniki elektroniczne z danymi osobowymi powinny być:
   1) Oznaczane i przechowywane w zamykanych szafach lub sejfach.
   2) Przechowywane maksymalnie przez okres wskazany dla danego rodzaju danych osobowych przez Administratora Bezpieczeństwa Informacji.
8. Informację o maksymalnym okresie przechowywania nośników magnetycznych oraz optycznych, na których zapisane są dane osobowe przekazują Właściciele zasobów danych osobowych do Administratora Bezpieczeństwa Informacji.

## § 19
## Ochrona systemu informatycznego przed działaniem szkodliwego oprogramowania

1. Na każdej stacji roboczej w sieci oraz serwerze przetwarzającym dane osobowe powinno być zainstalowane oprogramowanie antywirusowe skanujące na bieżąco system informatyczny.
2. Skaner poczty elektronicznej powinien być stale włączony.
3. Oprogramowanie antywirusowe powinno być zainstalowane tak, aby użytkownik nie był w stanie wyłączyć lub pominąć etapu skanowania.
4. Kontrola antywirusowa powinna być przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.
5. Należy stosować wersje programów antywirusowych z aktualną bazą sygnatur wirusów.
6. Nowe wersje oprogramowania antywirusowego oraz uaktualnienia bazy sygnatur wirusów instaluje Administrator Systemów Informatycznych niezwłocznie po ich otrzymaniu lub ściągnięciu, uprzednio weryfikując pochodzenie oprogramowania.
7. W razie zainfekowania systemu Administrator Systemów Informatycznych odpowiada za usunięcie wirusa.
8. Administrator Systemów Informatycznych ma prawo odłączyć od sieci stację roboczą, na której zostanie zlokalizowany wirus, jeśli uznają, że dalsze pozostawienie go w sieci zagraża innym stacjom roboczym.

## § 20
## Zasady komunikacji w sieci teleinformatycznej

1. Przesyłanie danych osobowych drogą teletransmisji powinno odbywać się wyłącznie przy wykorzystaniu wymaganych zabezpieczeń logicznych chroniących przed nieuprawnionym dostępem, w szczególności takich jak ochrona kryptograficzna.
2. Wyłącznie w sytuacjach wyjątkowych dopuszcza się przetwarzanie danych osobowych w plikach (MS Word, MS Excel) na stacjach roboczych użytkowników, poza bazą danych, znajdującą się w określonym systemie informatycznym. Powyższe zastrzeżenie nie obowiązuje w przypadku przetwarzania danych osobowych przy użyciu programów komputerowych wyłącznie do edycji tekstu, w celu udostępnienia danych osobowych na piśmie.
3. Zgodę na przetwarzanie danych w sytuacjach określonych w ust. 2 wydają Właściciele zasobów danych osobowych.
4. Inne technologie sieciowe takie jak sieci lokalne oparte na falach radiowych nie mogą być wykorzystywane do przekazu informacji, o ile połączenie nie jest szyfrowane. Takie połączenia mogą być używane jedynie dla wymiany poczty elektronicznej o ile wiadomo, że nie zawiera ona danych osobowych.

5. Wszystkie połączenia zewnętrzne do systemu informatycznego powinny być monitorowane, a logi połączeń archiwizowane w trybie ciągłym i bezterminowym.
6. System informatyczny służący do przetwarzania danych osobowych, powinien być chroniony przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.
7. Zabezpieczenia logiczne, o których mowa w ust. 7 powyżej, obejmują:
   1) Kontrolę przepływu informacji pomiędzy systemem informatycznym a siecią publiczną.
   2) Kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego.

## § 21
## Zasady monitorowania, przeglądu i konserwacji systemu informatycznego

1. Przeglądy, naprawy i konserwacje systemu informatycznego, które będą przeprowadzane w miejscu użytkowania tego systemu wymagają obecności Administratora Systemów Informatycznych lub innej wyznaczonej osoby.
2. Za prawidłowość przeprowadzenia przeglądów, zapewnienia jakości, konserwację i dokumentowanie zmian w systemach odpowiada Administrator Systemów Informatycznych.
3. W przypadku gdy konieczne jest dokonanie przeglądu, naprawy lub konserwacji systemu informatycznego poza miejscem jego użytkowania, z urządzenia należy wymontować element, na którym zapisane są dane osobowe, o ile jest to możliwe. W przeciwnym wypadku należy zawrzeć z podmiotem dokonujący naprawy umowę powierzenia w rozumieniu art. 31 ustawy o ochronie danych osobowych.
4. Przegląd programów i narzędzi programowych powinien być przeprowadzany w przypadku zmiany wersji oprogramowania aplikacji, zmiany wersji oprogramowania bazy danych lub wykonania zmian w projekcie systemu spowodowanych koniecznością naprawy, konserwacji lub modyfikacji systemu.
5. Przed dokonaniem zmian w systemie informatycznym należy dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych na testowej bazie danych. Sprawdzenie powinno obejmować: poprawność działania wszystkich elementów aplikacji, poprawność funkcjonalną systemu.
6. Każda zmiana parametrów systemu służącego do przetwarzania danych osobowych powinna być dokładnie dokumentowana.
7. Codziennie Administrator Systemów Informatycznych powinien przeprowadzać kontrolę logów zdarzeń zachodzących w systemie.
8. Raz do roku należy przeprowadzać weryfikację całego oprogramowania użytkowego eksploatowanego na wszystkich stacjach roboczych podłączonych do systemu informatycznego pod kątem spełnienia wymogów bezpieczeństwa.

## § 22
## Zasady postępowania z komputerami przenośnymi

1. Osoba używająca komputer przenośny zawierający dane osobowe zobowiązana jest zachować szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych.
2. Osoba używająca komputer przenośny zawierający dane osobowe w szczególności powinna:
   1) Stosować ochronę kryptograficzną wobec danych osobowych przetwarzanych na komputerze przenośnym.
   2) Zabezpieczyć dostęp do komputera na poziomie systemu operacyjnego - identyfikator i hasło.
   3) Nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych.
   4) Nie wykorzystywać komputera przenośnego do przetwarzania danych osobowych w obszarach użyteczności publicznej.

5) Zachować szczególną ostrożność przy podłączaniu do sieci publicznych poza obszarem przetwarzania danych osobowych.

3. W przypadku podłączania komputera przenośnego do sieci publicznej poza siecią Urzędu należy zastosować firewall zainstalowany bezpośrednio na tym komputerze oraz system antywirusowy.
4. Użytkownik powinien zachować wyjątkową ostrożność podczas korzystania z zasobów sieci publicznej.
5. Za wszelkie działania wykonywane na komputerze przenośnym odpowiada jego formalny użytkownik.

## § 23
## Postanowienia końcowe

1. Administrator Bezpieczeństwa Informacji zobowiązany jest zapoznać z treścią Instrukcji każdego użytkownika systemu informatycznego służącego do przetwarzania danych osobowych.
2. W sprawach nieuregulowanych w Instrukcji mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (t.j. Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.) oraz przepisy wykonawcze do tejże Ustawy.