Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

w Urzędzie Gminy w Cielądzu

Wersja 1		**Pieczęć firmowa:** WÓJT GMINY CIELĄDZ powiat rawski, woj. łódzkie	
Opracował:	**Data:**	**Zatwierdził:**	**Data:**
Sylwester Krawczyk Sekretarz Gminy	12.04.2016 r.	WÓJT mgr Paweł Krołak	.

1. Wstęp

Instrukcja stanowi zestaw procedur opisujących zasady zapewnienia bezpieczeństwa danych osobowych w systemach i aplikacjach informatycznych wykorzystywanych w Urzędzie Gminy w Cielądzu.

2. Definicje

ADO – Administrator Danych Osobowych
ABI Administrator Bezpieczeństwa Informacji
ASI – Administrator Systemu Informatycznego

3. Poziom bezpieczeństwa

W Urzędzie obowiązuje wysoki poziom bezpieczeństwa systemu informatycznego.

4. Bezpieczna eksploatacja sprzętu i oprogramowania

Celem procedury jest określenie wymagań bezpieczeństwa dla sprzętu i oprogramowania eksploatowanego w Urzędzie Gminy w Cielądzu.

1. Sprzęt służący do przetwarzania zbioru danych osobowych składa się z: komputerów stacjonarnych klasy PC, komputerów przenośnych oraz serwerów.
2. Komputery przenośne mogą być używane do przetwarzania danych osobowych po odpowiednim ich zabezpieczeniu.
3. Użytkownik korzystający z komputera przenośnego jest zobowiązany do zachowania szczególnej ostrożności podczas transportu komputera oraz nie może udostępnić komputera osobom nieupoważnionym.
4. Sieć komputerowa służąca do przetwarzania danych osobowych posiada zapewnione prawidłowe zasilanie energetyczne gwarantujące właściwe i zgodne z wymaganiami producenta działanie sprzętu komputerowego.
5. Główne węzły są podtrzymywane przez UPS zapewniający odpowiedni czas pracy systemu na poprawne zakończenie pracy w systemie przetwarzania danych osobowych.
6. Programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych są użytkowane z zachowaniem praw autorskich i posiadają licencje.
7. ASI odpowiada za wyposażenie systemu informatycznego w mechanizmy uwierzytelniania użytkownika oraz za sprawowanie kontroli dostępu do danych osobowych przez osoby upoważnione.
8. Systemy operacyjne są wyposażone w wygaszacze ekranów, które aktywują się automatycznie po upływie określonego czasu od ostatniego użycia komputera.
9. Wygaszacze ekranów posiadają funkcję automatycznego blokowania dostępu do systemu operacyjnego poprzez konieczność ponownego wprowadzenia hasła.
10. Ekrany monitorów, są ustawione w taki sposób, żeby w miarę możliwości uniemożliwić odczyt wyświetlanych informacji osobom nieupoważnionym.
11. Za spełnienie obowiązku określonego w powyższym rozdziale odpowiadają użytkownicy i kierownicy komórek organizacyjnych.

5. Procedura dostępu podmiotów zewnętrznych

Celem procedury jest zapewnienie bezpiecznej współpracy z podmiotami zewnętrznymi, ponieważ dostęp podmiotów zewnętrznych (osób fizycznych lub prawnych) do systemu informatycznego Urzędu i danych osobowych wiąże się zarówno z ryzykiem nie zapewnienia właściwej ochrony informacjom, jak również z pozyskaniem informacji nieprzeznaczonych dla tej osoby.

1. Podmiot zewnętrzny mający dostęp do systemu informatycznego i danych osobowych administrowanych przez Urząd podpisuje umowę zawierającą klauzulę poufności.
2. Podmiot zewnętrzny jest zobowiązany do zapewnienia ochrony danych osobowych pozyskanych lub udostępnionych mu przy / lub w związku z wykonywaniem umowy, na zasadach wynikających z obowiązujących przepisów prawa oraz polityk, instrukcji lub innych regulacji o charakterze wewnętrznym w tym przedmiocie, obowiązujących w Urzędzie Gminy w Cielądzu.
3. Dostęp do danych osobowych, przetwarzanie lub usuwanie tych danych, administrowanych przez Urząd, wymaga odrębnego upoważnienia. Uprawnienia lub czynności te mogą być przyznane lub wykonywane wyłącznie dla celów związanych z wykonywaniem umowy i wyłącznie na/lub w okresie niezbędnym dla realizacji tych celów.
4. Tworzenie przez podmiot zewnętrzny zbiorów danych osobowych wykorzystujących dane administrowane przez Urząd wymaga każdorazowo pisemnej zgody ADO.
5. Urządzenia i systemy informatyczne podmiotu zewnętrznego, na których będą przetwarzane dane osobowe, pozyskane lub udostępnione w związku z wykonywaniem umowy, winny spełniać wymagania techniczne odpowiednie dla urządzeń służących do przetwarzania danych osobowych.
6. Podmiot zewnętrzny ponosi odpowiedzialność za będące następstwem jego zachowań szkody wyrządzone niezgodnym z umową przetwarzaniem danych osobowych, w szczególności szkody wyrządzone utratą, niewłaściwym przechowywaniem lub posłużeniem się dokumentami, które zawierają dane osobowe.
7. W przypadku, gdy umowa z podmiotem zewnętrznym uprawnia do jej wykonywania przy udziale osób trzecich, postanowienia paragrafów poprzedzających rozciągają się również na te osoby, przy czym podmiot zewnętrzny odpowiada za działania lub zaniechania osób, którymi się posługuje, lub którym powierza wykonanie niniejszej umowy, jak za działania lub zaniechania własne.
8. Administrator Bezpieczeństwa Informacji prowadzi rejestr podmiotów zewnętrznych posiadających dostęp do systemu informatycznego Urzędu Gminy i danych osobowych celem identyfikacji i zapewnienia Urzędowi nadzoru nad bezpiecznym ich przetwarzaniem. Patrz Załącznik nr 6 – Rejestr podmiotów zewnętrznych.

6. Procedura korzystania z Internetu i poczty elektronicznej

Celem procedury jest uregulowanie zasad korzystania z Internetu i poczty elektronicznej, aby zagwarantować bezpieczeństwo danych osobowych przesyłanych tymi kanałami.

Użytkownicy Internetu zobowiązani są do przestrzegania następujących zasad:

1. Zakazuje się ściągania przez użytkowników plików lub przeglądania zasobów informacyjnych o treści prawnie zabronionej, obscenicznej bądź pornograficznej.
2. Do wymiany korespondencji w czasie korzystania z systemu informatycznego Urzędu może być wykorzystywana jedynie służbowa poczta elektroniczna.

3. Szczególne rygory należy stosować wobec ściągania z Internetu plików wykonywalnych. Pliki takie powinny być ściągane tylko za każdorazową zgodą ASI i tylko w uzasadnionych przypadkach.. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie samowolnie ściągnięte z Internetu i przez niego zainstalowane.
4. Do korzystania z Internetu użytkownicy mogą wykorzystywać jedynie zaakceptowane przez ASI formy dostępu.
5. ASI nadaje się uprawnienia do monitorowania przeglądania Internetu przez użytkowników. Uwzględniają one:
    - blokowanie stron internetowych określonego typu,
    - blokowanie określonych stron internetowych,
    - analizę przesyłanych informacji pod kątem niebezpiecznego oprogramowania.

Użytkownicy systemu poczty elektronicznej zobowiązani są do przestrzegania następujących zasad:

1. Przesyłanie informacji za pośrednictwem poczty elektronicznej winno odbywać się zgodnie z uprawnieniami adresatów do korzystania z określonego typu danych. W przypadku wątpliwości nadawca powinien sprawdzić, czy dana osoba ma uprawnienia do korzystania z dokumentów danego typu lub o określonej klauzuli poprzez skonsultowanie się z Administratorem Bezpieczeństwa Informacji.
2. Przesyłanie informacji poza obręb Urzędu może odbywać się tylko przez osoby do tego upoważnione.
3. Użytkownicy powinni zwrócić szczególną uwagę na poprawność adresu odbiorcy dokumentu.
4. W przypadku przesyłania informacji wrażliwych nie należy wykorzystywać systemu poczty elektronicznej.
5. Jeżeli istotne jest potwierdzenie otrzymania przez adresata przesyłki, użytkownik winien skorzystać, o ile jest to technicznie możliwe, z opcji systemu poczty elektronicznej informującej o dostarczeniu i otwarciu dokumentu. Dodatkowo zaleca się, aby użytkownik zawarł w treści dokumentu prośbę o potwierdzenie otrzymania i zapoznania się z informacją. Adresat zobowiązany jest w takiej sytuacji przesłać nadawcy potwierdzenie.
6. Informacje przesyłane za pośrednictwem poczty elektronicznej muszą być zgodne z prawem i z zasadami obowiązującymi w Urzędzie.
7. Użytkownicy nie powinni otwierać przesyłek od nieznanych sobie osób, których tytuł nie sugeruje związku z wypełnianymi przez nich obowiązkami służbowymi. W przypadku otrzymania takiej przesyłki, użytkownik powinien ją zniszczyć lub skontaktować się z ASI.
8. Użytkownicy nie powinni uruchamiać wykonywalnych załączników dołączonych do wiadomości przesyłanych pocztą elektroniczną. W takim przypadku użytkownik powinien poinformować o zdarzeniu ASI, który winien sprawdzić, czy załącznik stanowi zagrożenie dla przetwarzanych w systemie informatycznym informacji
9. Użytkownicy nie powinni rozsyłać za pośrednictwem poczty elektronicznej informacji o zagrożeniach dla systemu informatycznego, „łańcuszków szczęścia" itp.
10. Użytkownicy nie powinni rozsyłać, wiadomości zawierających załączniki o dużym rozmiarze dla większej liczby adresatów - określenie krytycznych rozmiarów przesyłek i krytycznej liczby adresatów jest uzależnione od wydajności systemu poczty elektronicznej.
11. Użytkownicy powinni okresowo kasować niepotrzebne wiadomości pocztowe.

7. Procedura nadawania uprawnień do przetwarzania danych osobowych.

Celem procedury jest zapewnienie użytkownikom odpowiednich uprawnień do przetwarzania danych osobowych, aby redukować zagrożenie nieuprawnionego dostępu do danych osobowych i utraty poufności.

A. Podstawowe zasady nadawania uprawnień w systemie.

1. Przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych każdy pracownik Urzędu powinien zostać zapoznany przez ASI lub ABI z przepisami dotyczącymi ochrony danych osobowych, a na dowód przeszkolenia złożyć stosowne oświadczenie u Administratora Bezpieczeństwa Informacji. Wzór oświadczenia określa załącznik nr 1
2. Kierownik właściwej komórki organizacyjnej Urzędu zobowiązany jest do włączenia do indywidualnych zakresów obowiązków służbowych każdego pracownika zatrudnionego przy przetwarzaniu danych osobowych – obowiązku ochrony danych osobowych oraz odpowiedzialności za nieuzasadnioną ich modyfikację lub zniszczenie bądź nielegalne ujawnienie lub pozyskanie.

B. Procedura nadawania uprawnień do przetwarzania danych osobowych

1. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, mogą zostać dopuszczone wyłącznie osoby posiadające upoważnienia wydane przez Administratora Bezpieczeństwa Informacji.
2. Dostęp do pomieszczenia, w którym znajduje się serwer oraz urządzeń wchodzących w jego skład mają tylko osoby posiadające stosowne upoważnienie – Załącznik nr 2.
3. Procedury wydawania i anulowania upoważnień do obsługi systemu informatycznego oraz nadawania, modyfikacji i anulowania uprawnień użytkowników do systemu realizowane są wg następujących zasad:
    a) ASI składa do ABI wniosek o „Upoważnienie / anulowanie upoważnienia lub jego aktualizację do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych". Wzór Wniosku określa Załącznik nr 3;
    b) ABI wydaje wnioskowane Upoważnienie, a następnie przekazuje go ASI i zleca zarejestrowanie użytkownika w systemie oraz nadanie mu identyfikatora;
    c) ASI, po otrzymaniu dokumentów określonych w Załączniku nr 4, rejestruje użytkownika w systemie nadając mu identyfikator i wnioskowane uprawnienia. Wzór ewidencja osób upoważnionych do przetwarzania danych osobowych określa zał. nr 5.
    d) Oryginał Upoważnienia pozostaje u ASI, a jego kopia zostaje przekazana osobie, dla której upoważnienie zostało wydane.
    e) W przypadku utraty przez użytkownika uprawnień do obsługi danego systemu informatycznego (np. rozwiązanie stosunku pracy, nieobsługiwanie systemu z powodu zmiany stanowiska pracy) ASI występuje do ABI z wnioskiem o anulowanie upoważnienia do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, zgodnie z Załącznikiem nr 3;
    f) ASI informuje ABI o wyrejestrowaniu użytkownika z systemu (zablokowanie dostępu do systemu), przekazując mu wydane „Upoważnienie / anulowanie upoważnienia do obsługi systemu informatycznego oraz urządzeń

wchodzących w jego skład, służących do przetwarzania danych osobowych", którego wzór przedstawia Załącznik nr 4;

g) Administrator systemu, po otrzymaniu dokumentów określonych w Załączniku nr 3, wyrejestrowuje użytkownika z systemu (blokuje jego dostęp do systemu) oraz zwraca ABI wypełnione anulowanie upoważnienia;

h) Oryginał anulowania upoważnienia pozostaje u ABI, a kopia zostaje przekazana osobie, której upoważnienie zostało anulowane.

4. Identyfikator użytkownika nadany na podstawie wniosku „Zlecenia nadania zmiany anulowania zakresu uprawnień użytkownika", wraz z imieniem i nazwiskiem właściciela identyfikatora, ASI wpisuje do „Ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych", zgodnie z Załącznikiem 5.
5. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielany innej osobie.

8. Metody i środki uwierzytelnienia

Celem procedury jest zapewnienie, że do systemów informatycznych przetwarzających dane osobowe mają dostęp jedynie osoby do tego upoważnione.

Zasady ogólne

1. Pierwsze hasło dla użytkownika ustala przydziela ASI przy wprowadzaniu identyfikatora użytkownika do systemu.
2. Użytkownik systemu niezwłocznie ustala swoje, znane tylko jemu hasło, po nadaniu hasła przez ASI.
3. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło dostępu.
4. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
5. Hasło nie może być ujawnione nawet po utracie przez nie ważności.
6. Hasła mają charakter poufny są znane tylko jego właścicielowi.
7. Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.
8. Hasła w bazie są zapisywane w systemie w postaci szyfrowanej.
9. Hasła zmienia się nie rzadziej niż raz na 30 dni.
10. Osobą odpowiedzialną za przydział haseł i częstotliwość ich zmiany, a także w zakresie rejestrowania i wyrejestrowania użytkowników jest Administrator Systemu Informatycznego. Wyznacza się jako Administratora Systemu Informatycznego w Urzędzie Gminy w Cielądzu Pana Artura Wąsiewicza.

Hasła administratora

1. Administrator systemu zobowiązany jest zmienić swoje hasło nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
2. Hasła administratora powinny być spisanie oraz umieszczone w zamkniętych kopertach, odrębnych dla każdego z systemów, w miejscu uniemożliwiającym dostęp do nich osób nieupoważnionych, chroniącym przed utratą lub zniszczeniem oraz gwarantującym ich odczytanie upoważnionemu użytkownikowi, a także kierownikowi właściwej jednostki, bądź komórki organizacyjnej Urzędu w przypadkach nadzwyczajnych.

3. Zarejestrowane hasła administratora, oprócz treści hasła winny posiadać adnotację o dacie ich wprowadzenia do systemu oraz być przechowywane przez okres 5 lat.
4. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp.

Uwierzytelnianie na poziomie systemu operacyjnego

1. Hasło na poziomie dostępu do systemu operacyjnego może składać się z co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
2. Za systematyczną, terminową zmianę hasła odpowiada użytkownik.
3. Zmiana hasła do systemu operacyjnego następuje nie rzadziej, niż co 30 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.

Uwierzytelnianie na poziomie dostępu do aplikacji

1. Hasło na poziomie dostępu do wszystkich programów, w których przetwarzane są dane osobowe, może składać się z co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
2. Za systematyczną, terminową zmianę hasła odpowiada użytkownik.
3. Zmiana hasła do systemu operacyjnego następuje nie rzadziej, niż co 30 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.

9. Procedura rozpoczęcia, zawieszenia i zakończenia pracy

Celem procedury jest zabezpieczenie danych osobowych przed nieuprawnionym dostępem i utratą poufności w sytuacji, gdy użytkownik rozpoczyna, przerywa lub kończy pracę w systemie informatycznym przetwarzającym dane osobowe.

1. Rozpoczynając prace na komputerze użytkownik sprawdza, czy stanowisko znajduje się w takim stanie, w jakim pozostawił je opuszczone, jeżeli stwierdza naruszenie stanowiska, niezwłocznie informuje o tym fakcie ABI, następnie loguje się do systemu informatycznego.
2. Dostęp do danych osobowych możliwy jest jedynie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia użytkownika.
3. ASI ustala przyczyny zablokowania systemu oraz w zależności od zaistniałej sytuacji podejmuje odpowiednie działania. O zaistniałym incydencie powiadamia Administratora Bezpieczeństwa Informacji lub osobę przez niego wyznaczoną.
4. Przed opuszczeniem stanowiska pracy, użytkownik obowiązany jest:
   a) wylogować się z systemu informatycznego lub,
   b) wywołać blokowany hasłem wygaszacz ekranu lub,
   c) wywołać sekwencję klawiszy aby zablokować system informatyczny
5. Kończąc pracę należy:
   a) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,
   b) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.

10. Procedura tworzenia kopii zapasowych

Tworzenie kopii bezpieczeństwa programu Płatnik

1. Kopie zapasowe wykonuje się na nośniku zewnętrznym w cyklu miesięcznym, półrocznym i rocznym. Kopie te są wykonywane na nośnikach optycznych jednokrotnego użytku np. CD-R.
2. Kopie zapasowe są odpowiednio oznakowane datą i godziną ich sporządzenia.
3. ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.
4. W przypadku wystąpienia problemów z archiwizacją, konieczny jest kontakt z ASI.

Tworzenie kopii bezpieczeństwa programów: (wymieniono po kolei: nazwa skrócona, nazwa pełna, dostawca oprogramowania)
KSZOB (Księgowość Zobowiązań) (Groszek S.C.)
PODATKI (Podatki w administracji) (Groszek S.C.)
PŁACE (Płace w administracji) (Groszek S.C.)
GOMIG (Gospodarka Odpadami Gminy) (ARISCO)
WODA (Woda) (Groszek)

1. Kopie wykonywane są przez dedykowane oprogramowanie do archiwizacji automatycznie w cyklach dziennych. Nadzór nad wykonywaniem kopii oraz ich poprawność i integralność sprawdza cyklicznie ASI.
2. Kopie zapisywane są na nośniku cyfrowym w wyznaczonym folderze na komputerze przeznaczonym do przechowywania kopii bezpieczeństwa.
3. Kopie oznakowane są znacznikami w postaci daty i czasu ich wykonania oraz zawierają nazwę skróconą programu i kod jednostki organizacyjnej np. REF_FIN_KSZOB_11-11-2013_12:00

Tworzenie kopii bezpieczeństwa katalogów na dyskach lokalnych:

1. Kopie zapasowe dokumentów użytkowników znajdujących się w wyznaczonych folderach na dyskach lokalnych wykonuje się na nośniku zewnętrznym każdorazowo w momencie wylogowania się z systemu komputerowego.
2. Poprawność sporządzenia kopii katalogu potwierdza wyświetlony na ekranie komunikat.
3. Kopie zapasowe są odpowiednio oznakowane na nośniku kopii zapasowej poprzez utworzenie identycznego folderu z przypisanymi prawami do zapisu i odczytu dokumentów jak na komputerze użytkownika.
4. ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.
5. W przypadku wystąpienia problemów z archiwizacją konieczny jest kontakt z ASI.

11. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji i wydruków

Procedura określa sposób postępowania z nośnikami, na których znajdują się dane osobowe, celem zabezpieczenia ich przez niszczeniem, kradzieżą, dostępem osób nieupoważnionych.

A. Elektroniczne nośniki informacji

Dane osobowe w postaci elektronicznej należy usuwać z nośnika informacji w sposób uniemożliwiający ich ponowne odtworzenie, nie później niż po upływie 3 dni, po wykorzystaniu tych danych chyba, że z odrębnych przepisów wynika obowiązek ich przechowywania. Nośniki danych są przechowywane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych).

B. Kopie zapasowe

1. Kopie zapasowe zbioru danych osobowych oraz oprogramowania i narzędzi programowych zastosowanych do przetwarzania danych są przechowywane w wyznaczonym, zabezpieczonym pomieszczeniu na wyznaczonym komputerze.
2. Dostęp do kopii zapasowych mają tylko upoważnieni pracownicy, tj. ABI oraz ASI.
3. Kopie bezpieczeństwa przechowywane do momentu wykonania następnej kopii bezpieczeństwa.
4. Kopie archiwalne miesięczne przechowywane są przez okres 1 roku, a kopie roczne przez 5 lat, licząc od pierwszego dnia roku następującego po roku, za który wykonana jest kopia.

C. Wydruki

1. Wydruki/dokumenty typu umowy, faktury, decyzje, rejestry, wykazy, zaświadczenia, zezwolenia, ewidencje, zawierające dane osobowe, przechowuje się w pokojach stanowiących obszar przetwarzania danych osobowych, określony w Polityce bezpieczeństwa.
2. Wydruki/dokumenty, zawierające dane osobowe, należy niszczyć przez pocięcie w niszczarce.
3. Za bezpieczeństwo danych osobowych zapisanych w formie papierowej odpowiedzialne są osoby je przetwarzające oraz kierownicy właściwych jednostek lub komórek organizacyjnych Urzędu.

12. Procedura zabezpieczenia systemu informatycznego, w tym przed wirusami komputerowymi

A. Ochrona antywirusowa

1. Za ochronę antywirusową odpowiada ASI.
2. System antywirusowy zainstalowany jest na każdym komputerze z dostępem do danych osobowych
3. Programy antywirusowe, o których mowa poprzednio, winny być uaktywnione cały czas podczas pracy danego systemu.

4. Wszystkie pliki otrzymywane z zewnętrz, jak również wysyłane na zewnątrz, należy sprawdzać pod kątem występowania wirusów najnowszą dostępną wersją programu antywirusowego. Sprawdzenie odbywa się automatycznie przez system antywirusowy
5. W przypadku stwierdzenia pojawienia się wirusa, każdy użytkownik winien powiadomić ASI.

B. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej

1. ASI jest odpowiedzialny za aktywowanie i poprawne konfigurowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku:
   a) sieci lokalnej i sieci rozległej,
   b) stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej.
2. Użytkownicy systemu obowiązani są do utrzymywania stałej aktywności zainstalowanego na ich stanowiskach komputerowych specjalistycznego oprogramowania monitorującego wymianę danych na styku tego stanowiska i sieci lokalnej.

13. Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych

1. Odbiorcą danych jest każdy, komu udostępnia się dane osobowe, z wyłączeniem:
   a) osoby, której dane dotyczą,
   b) osoby użytkownika systemu lub innej osoby upoważnionej do przetwarzania danych osobowych w Urzędzie,
   c) przedstawiciela, o którym mowa w art. 31a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,
   d) podmiotu, któremu powierzono przetwarzanie danych,
   e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
2. Dane osobowe administrowane przez Urząd mogą być udostępnione osobom lub podmiotom uprawnionym do ich otrzymania na mocy Ustawy o Ochronie Danych Osobowych oraz innych przepisów powszechnie obowiązujących.
3. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej.
4. Dane udostępnione Urzędowi przez inny podmiot można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
5. ABI prowadzi ewidencję udostępniania danych, o których mowa w pkt. 2. Odnotowanie obejmuje informacje o:
   a) Nazwie jednostki organizacyjnej lub imieniu i nazwisku osoby, której udostępniono dane,
   b) Zakresie udostępnianych danych,
   c) Dacie udostępnienia.
6. Odnotowanie informacji powinno nastąpić niezwłocznie po udostępnieniu danych.
7. Na żądanie osoby, której dane zostały udostępnione, informacje o udostępnieniu danych są zamieszczane w pisemnym raporcie i przekazywane tej osobie.

14. Procedura wykonywania przeglądów i konserwacji

1. Przeglądy i konserwacja systemu informatycznego powinny być wykonywane w terminach określonym przez producentów systemu oraz zgodnie z harmonogramem ASI
2. Aktualizacja oprogramowania powinna być przeprowadzana zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji.
3. Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ASI.
4. Nieprawidłowości w działaniach systemu informatycznego oraz oprogramowania powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane.
5. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego, wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych i rejestrowane zgodnie z zał. nr 6.
6. W przypadku naprawy sprzętu komputerowego dane osobowe należy zabezpieczyć, natomiast w przypadku naprawy sprzętu poza terenem danej jednostki, po zabezpieczeniu - usunąć z dysku. Gdy nie ma możliwości usunięcia danych naprawa powinna być nadzorowana przez osobę upoważnioną przez administratora systemu.

Załącznik nr 1

.....

.....
(imię i nazwisko)

.....
(miejscowość, data)

OŚWIADCZENIE

Oświadczam, iż zostałam/zostałem* zapoznana/zapoznany* z przepisami dotyczących ochrony danych osobowych, w szczególności ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tj. Dz. U. z 2002r. Nr 101, poz. 926 ze zm.), wydanych na jej podstawie aktów wykonawczych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Danych „Polityki Bezpieczeństwa Informacji" oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

1. Jednocześnie oświadczam, iż jestem zatrudniony/zatrudniona* przez Pracodawcę na podstawie umowy o pracę zawartej w dniu..... r.

2. Zobowiązuję się do:
- nieujawniania danych osobowych nieuprawnionym osobom lub instytucjom w jakiejkolwiek formie bez zgody Administratora Danych Osobowych,
- przestrzegania regulaminu ochrony danych osobowych,
- korzystania z oprogramowania wyłącznie w związku z wykonywaniem obowiązków pracowniczych,
- wykorzystywania jedynie legalnego oprogramowania pochodzącego od Pracodawcy,
- nie podejmowania prób samodzielnego instalowania oprogramowania pochodzącego z innych źródeł,
- wnoszenia, wynoszenia i użytkowania komputerów przenośnych bądź innych nośników danych wyłącznie za wiedzą i zgodą Administratora Bezpieczeństwa Informacji,
- należytej dbałości o sprzęt i oprogramowanie wymienione w metryczce komputera,
- korzystanie z produktów w wersjach ewaluacyjnych, testowych lub w jakikolwiek inny sposób ograniczony umowami licencyjnymi może być użytkowane zgodnie z ich przeznaczeniem, wyłącznie za zgodą Administratora Bezpieczeństwa Informacji.

Naruszenie przez Pracownika jego podstawowych obowiązków pracowniczych w zakresie wskazanym powyżej, będzie stanowić podstawę do podjęcia przez Pracodawcę przysługujących mu środków prawnych, a w szczególności, może stanowić przyczynę uzasadniającą wypowiedzenie przez Pracodawcę umowy o pracę lub rozwiązanie przez Pracodawcę tejże umowy, bez wypowiedzenia, z winy pracownika, zgodnie z przepisami ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy (tekst jedn.: Dz. U. z 1998 r., Nr 21, poz. 94, ze zm.).

.....
/podpis pracownika/

* niepotrzebne skreślić

Załącznik nr 2

.....
(pieczęć URZĘDU)

UPOWAŻNIENIE

Niniejszym upoważniam

.....

(imię i nazwisko pracownika)

do dostępu do pomieszczenia, w którym znajduje się serwer systemu informatycznego służącego do przetwarzania danych osobowych w budynku URZĘDU GMINY CIELĄDZ POD ADRESEM CIELĄDZ 59.

..... dnia .....

.....

(podpisy Administratora Bezpieczeństwa Informacji)

Załącznik nr 3

WNIOSEK

Wnoszę o wydanie/anulowanie z dniem ..... upoważnienia
(data)

Nr ..... Pani/Panu* .....,
(nazwisko i imię)

pracownikowi ....., do obsługi systemu
(nazwa jednostki i komórki organizacyjnej)

informatycznego: .....
(nazwa systemu lub programu)

w zakresie: ..... danych osobowych.
(wprowadzania, utrwalania, przechowywania, modyfikacji, usuwania itp.)

.....
(miejscowość i data)

.....
(pieczęć i podpis ASI)

Załącznik nr 4

UPOWAŻNIENIE/ANULOWANIE UPOWAŻNIENIA* Nr .....

do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych

Z dniem ..... upoważniam/anuluję upoważnienie nr .....
(data)

Panią/Pani/Pana*: .....
(nazwisko i imię)

pracownika ..... do obsługi systemu
(nazwa jednostki i komórki organizacyjnej)

informatycznego: .....
(nazwa systemu lub programu)

w zakresie: ..... danych osobowych.
(wprowadzania, utrwalania, przechowywania, modyfikacji, usuwania itp.)

Zobowiązuję Panią*/Pana* do przestrzegania przepisów dotyczących ochrony danych osobowych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Danych Osobowych „Polityki bezpieczeństwa informacji" oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

.....
(miejscowość i data)

.....
(pieczęć i podpis ABI)

Wypełnia Administrator Systemu Informatycznego:

Identyfikator użytkownika: .....

Data zarejestrowania w systemie: ..... **

Data wyrejestrowania użytkownika
(zablokowania dostępu) z systemu: ..... ***

Podpis Administratora: .....

*) niepotrzebne skreślić
**) wypełnić w przypadku wydania upoważnienia
***) wypełnić w przypadku anulowania upoważnienia

Załącznik nr 5

Ewidencja osób upoważnionych do przetwarzania danych osobowych.

Imię i nazwisko	Data nadania upoważnienia	Data wygaśnięcia upoważnienia

Załącznik nr 6 – Rejestr podmiotów zewnętrznych	Sporządził	ABI
	Data:	
	Strona:	1 z 1

Lp.	Nazwa firmy	Zakres świadczonych usług	Numer umowy	Uwagi
1				