Zarządzenie Nr 217/2014

Wójta Gminy Obrzycko

z dnia 27 października 2014 r.

w sprawie wprowadzenia Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Gminy Obrzycko

Na podstawie art. 36 Ustawy z dnia 29 sierpnia 1997 o ochronie danych osobowych (tekst jednolity Dz.U. z 2014 r. poz. 1182) i § 3,4 i § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024),

Zarządzam, co następuje:

§ 1

Wprowadza się do użytku służbowego „Politykę Bezpieczeństwa" w zakresie przetwarzania danych osobowych w Urzędzie Gminy Obrzycko stanowiącą załącznik nr 1 do niniejszego zarządzenia oraz „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Obrzycko", stanowiącą załącznik nr 2 do zarządzenia.

§ 2

Zobowiązuje się wszystkich pracowników Urzędu Gminy Obrzycko oraz Jednostek Organizacyjnych do przestrzegania przepisów zawartych w dokumentach, o których mowa w § 1

§ 3

Zobowiązuje się Kierowników Jednostek Organizacyjnych do sprawowania nadzoru nad ich ochroną oraz do współpracy z Administratorem Bezpieczeństwa Informacji w tym zakresie.

§ 4

Wyłącza się jawność dokumentów, o których mowa w § 1 na podstawie art. 36 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. Dokumenty te mogą być rozpowszechniane bez żadnych ograniczeń wyłącznie wewnątrz Urzędu Gminy Obrzycko, o udostępnianiu tych dokumentów na zewnątrz decyduje Administrator Bezpieczeństwa Informacji.

§5

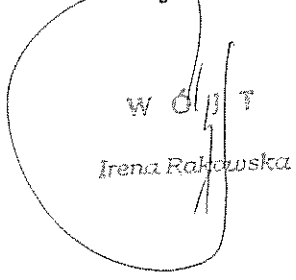
Traci moc Zarządzenie nr 3/99 Wójta Gminy Obrzycko z dnia 9 lipca 1999 w sprawie instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych i instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych w Urzędzie Gminy Obrzycko

§ 6

Wykonanie zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§ 7

Zarządzenie wchodzi w życie z dniem podpisania.



Załącznik Nr 1
do Zarządzenia Nr 217/2014
Wójta Gminy Obrzycko
z dnia 27 października 2014

POLITYKA BEZPIECZEŃSTWA INFORMACJI

W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

W

URZĘDZIE GMINY OBRZYCKO

OBRZYCKO 2014

SPIS TREŚCI

I. POSTANOWIENIA OGÓLNE

§1.

Celem Polityki Bezpieczeństwa danych osobowych, zwanej dalej Polityką Bezpieczeństwa, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych w zakresie ochrony danych osobowych, sposobu przetwarzania w Urzędzie Gminy Obrzycko grupy informacji zawierającej dane osobowe.

§2.

Określenia użyte w Polityce Bezpieczeństwa oznaczają:

1. Jednostka – Urząd Gminy Obrzycko
2. dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
3. przetwarzanie danych osobowych – gromadzenie, utrwalanie przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych osobowych, zwłaszcza w systemach informatycznych,
4. użytkownik – osoba upoważniona do przetwarzania danych osobowych,
5. administrator systemu – osoba upoważniona do zarządzania systemem informatycznym,
6. system informatyczny – system przetwarzania danych w Urzędzie Gminy Obrzycko wraz z zasobami ludzkimi, technicznymi oraz finansowymi, który dostarcza i rozprowadza informacje,
7. zabezpieczenie systemu informatycznego – należy przez to rozumieć wdrożenie stosowanych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych a także ich utratą.

II. DEFINICJA BEZPIECZEŃSTWA INFORMACJI

§3.

1. Utrzymanie bezpieczeństwa przetwarzanych przez Jednostkę informacji rozumiane jest jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z zasobem stanowiącym przedmiot niniejszej Polityki.
2. Poniżej opisane jest rozumienie wyżej wymienionych pojęć w odniesieniu do informacji i aplikacji:
   1) Poufność informacji – rozumiana jako zapewnienie, że tylko uprawnieni pracownicy mają dostęp do informacji,
   2) Integralność informacji – rozumiana jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania,
   3) Dostępność informacji – rozumiane jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,
   4) Zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych.
3. Dodatkowo zarządzanie bezpieczeństwem informacji wiąże się z zapewnieniem:
   1) Niezaprzeczalności odbioru – rozumianej jako zdolność systemu do udowodnienia, że adresat informacji otrzymał ją w określonym miejscu i czasie,
   2) Niezaprzeczalności nadania – rozumianej jako zdolność systemu do udowodnienia, że nadawca informacji faktycznie ją nadał lub wprowadził do systemu w określonym miejscu i czasie,
   3) Rozliczalności działań – rozumianej, jako zapewnienie, że wszystkie działania istotne dla przetwarzania informacji zostały zarejestrowane w systemie i możliwym jest zidentyfikowanie użytkownika, który działania dokonał.

III. ZAKRES

§4.

1. W systemie informacyjnym Jednostki przetwarzane są informacje służące do wykonywania zadań niezbędnych dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisów prawa.
2. Informacje te są przetwarzane i składowane zarówno w postaci manualnej jak i elektronicznej.

§5.

Politykę Bezpieczeństwa stosuje się do:

1. danych osobowych przetwarzanych w systemie informatycznym,
2. wszystkich informacji dotyczących danych pracowników Jednostki, w tym danych osobowych personelu i treści zawieranych umów o pracę,
3. wszystkich danych kandydatów do pracy zbieranych na etapie rekrutacji,
4. informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
5. rejestru osób dopuszczonych do przetwarzania danych osobowych,
6. innych dokumentów zawierających dane osobowe.

§6.

1. Zakresy określone przez dokumenty Polityki Bezpieczeństwa Informacji mają zastosowanie do całego systemu informacyjnego Jednostki w szczególności do:
   1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są informacje podlegające ochronie,
   2) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
   3) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, konsultantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie.
2. Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa zobowiązani są wszyscy pracownicy w rozumieniu Kodeksu Pracy, konsultanci, stażyści oraz inne osoby mające dostęp do informacji podlegających ochronie.

§7.

Informacje niejawne nie są objęte zakresem niniejszej Polityki.

IV. STRUKTURA DOKUMENTÓW POLITYKI BEZPIECZEŃSTWA INFORMACJI

§8.

1. Dokumenty Polityki Bezpieczeństwa Informacji ustanawiają metody zarządzania oraz wymagania niezbędne do zapewnienia skutecznej i spójnej ochrony przetwarzanych informacji.
2. Zestaw dokumentów Polityki Bezpieczeństwa Informacji składa się z:
   1) Niniejszego dokumentu Polityki Bezpieczeństwa Informacji,
   2) Instrukcji zarządzania systemami informatycznymi w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych, opisującej sposób zarządzania systemami przetwarzania danych osobowych w Jednostce - załącznik nr 1,
   3) Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych, opisującej tryb postępowania w sytuacjach naruszenia zabezpieczenia zasobów danych osobowych, zaobserwowanych prób naruszenia tego zabezpieczenia, a także uzasadnionego podejrzenia o przygotowywanej próbie naruszenia- załącznik nr 2.

V. DOSTĘP DO INFORMACJI

§9.

Wszystkie osoby, których rodzaj wykonywanej pracy będzie wiązał się z dostępem do danych osobowych, przed przystąpieniem do pracy, podlegają przeszkoleniu w zakresie obowiązujących przepisów prawa dotyczących ochrony danych osobowych oraz obowiązujących w Jednostce zasad ochrony danych osobowych.

§10.

Zakres czynności dla osoby dopuszczonej do przetwarzania danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę danych osobowych w stopniu odpowiednim do zadań tej osoby realizowanych przy przetwarzaniu tych danych.

§11.

Udostępnianie danych osobowych podmiotom upoważnionym do ich otrzymania, na podstawie przepisów prawa, mogą być udostępnione jeżeli w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą.

§12.

Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.

§13.

Dane osobowe udostępnia się na pisemny, umotywowany wniosek, który powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać zakres i przeznaczenie.

VI. ZARZĄDZANIE DANYMI OSOBOWYMI

§14.

Administratorem danych osobowych Wójt Gminy Obrzycko

§15.

1. Za bezpieczeństwo danych osobowych Jednostki, odpowiadają:
   1) Administrator danych osobowych - Wójt
   2) Administrator Bezpieczeństwa Informacji Jednostki
   3) Administrator Systemów Informatycznych
2. Administrator Bezpieczeństwa Informacji Jednostki realizując politykę bezpieczeństwa informacji ma prawo wydawać instrukcje regulujące kwestie związane z ochroną danych w strukturach Jednostki.
3. W umowach zawieranych przez Jednostkę winny znajdować się postanowienia zobowiązujące podmioty zewnętrzne do ochrony danych udostępnionych przez Jednostkę.

§16.

1. Zapoznanie się z dokumentami określonymi w §8 pkt 2 pracownicy Jednostki potwierdzają podpisem na „Indywidualnym zakresie czynności osoby zatrudnionej przy przetwarzaniu danych osobowych" (wzór w załączniku nr 3) i przekazują Administratorowi Bezpieczeństwa Informacji.

§17.

Ochrona zasobów danych osobowych Jednostki jako całości przed ich nieuprawnionym użyciem lub zniszczeniem jest jednym z podstawowych obowiązków pracowników Jednostki.

VII. ZAKRESY ODPOWIEDZIALNOŚCI

§18.

Za bezpieczeństwo informacji odpowiedzialny jest każdy pracownik Jednostki.

§19.

Administrator bezpieczeństwa informacji w Jednostce:

1. odpowiada za realizację ustawy o ochronie danych osobowych w zakresie dotyczącym Administratora Bezpieczeństwa Informacji,
2. sprawuje nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których dane są przetwarzane oraz kontrolą przebywających w nich osób,
3. określa strategię zabezpieczania systemów informatycznych Jednostki,
4. sprawuje nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
5. sprawuje nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych na których zapisane są dane osobowe,
6. identyfikuje i analizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych Jednostki,
7. określa potrzeby w zakresie zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe,
8. sprawuje nadzór nad bezpieczeństwem danych zawartych w komputerach przenośnych, dyskach wymiennych, palmtopach, w których przetwarzane są dane osobowe,

9. sprawuje nadzór nad obiegiem oraz przechowywaniem dokumentów i wydawnictw zawierających dane osobowe,
10. monitoruje działanie zabezpieczeń wdrożonych w celu ochrony danych osobowych w systemach informatycznych,
11. sprawuje nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane oraz kontrolą dostępu do danych,
12. zatwierdza wnioski o przyznaniu danemu użytkownikowi identyfikatora oraz praw dostępu do informacji chronionych w danym systemie przetwarzania,
13. powiadamia administratora systemu o konieczności utworzenia identyfikatora użytkownika w systemie oraz zmianie/nadaniu uprawnień dostępu użytkownika do systemu,
14. prowadzi ewidencję baz danych w systemach informatycznych, w których przetwarzane są dane osobowe,
15. prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych,
16. prowadzi ewidencję miejsc przetwarzania danych osobowych w systemach informatycznych,
17. prowadzi rejestr zbiorów danych osobowych Jednostki (przetwarzanych metodą tradycyjną lub w systemach informatycznych).

§20.

Administrator danych osobowych zobowiązany jest do przestrzegania wszystkich przepisów ustawy o ochronie danych, w szczególności poprzez:

1. określanie indywidualnych obowiązków i odpowiedzialności osób zatrudnionych przy przetwarzaniu danych osobowych, wynikających z ustawy o ochronie danych osobowych,
2. określenie budynków, pomieszczeń lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego,
3. zapoznawanie osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami obowiązującymi w tym zakresie,
4. wykonywania zaleceń Administratora Bezpieczeństwa Informacji Jednostki w zakresie ochrony danych osobowych,
5. wdrażanie i nadzorowanie przestrzegania Polityki bezpieczeństwa informacji,
6. wdrażanie i nadzorowanie przestrzegania instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
7. działanie zgodnie z instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych,

8. stwarzanie warunków organizacyjnych i technicznych umożliwiających spełnienie wymogów wynikających z obowiązywania ustawy o ochronie danych osobowych,
9. odpowiedzialność za poprawność merytoryczną danych gromadzonych w systemach informacyjnych,
10. określanie, które osoby i na jakich prawach mają dostęp do danych informacji,

Praca Administratora Danych Osobowych jest nadzorowana pod względem bezpieczeństwa przez Administratora Bezpieczeństwa Informacji.

§21.

Administrator Systemu Informatycznego odpowiedzialny jest za:

1. bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
2. optymalizację wydajności systemu informatycznego, baz danych,
3. instalacje i konfiguracje sprzętu sieciowego i serwerowego,
4. instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego,
5. konfigurację i administrację oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem,
6. współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,
7. zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
8. zarządzanie kopiami awaryjnymi danych w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
9. przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
10. przyznawanie na wniosek Administratora Danych, za zgodą Administratora Bezpieczeństwa Informacji ściśle określonych praw dostępu do informacji w danym systemie,
11. wnioskowanie do Administratora Bezpieczeństwa Informacji w sprawie procedur bezpieczeństwa i standardów zabezpieczeń,
12. zarządzanie licencjami, procedurami ich dotyczącymi,
13. prowadzenie profilaktyki antywirusowej.

Praca Administratora Systemu Informatycznego jest nadzorowana pod względem bezpieczeństwa przez Administratora Bezpieczeństwa Informacji.

VIII. PRZETWARZANIE DANYCH OSOBOWYCH

§22.

1. Przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach zamykanych na klucz przez wyznaczone do tego celu osoby.
2. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.

§23.

2. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia należy niszczyć w stopniu uniemożliwiającym ich odczytanie.
3. Urządzenia, dyski lub inne informatyczne nośniki danych, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

IX.OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DO ZAPEWNIENIA POUFNOŚCI PRZETWARZANYCH DANYCH

§24.

W Jednostce rozróżnia się następujące kategorie środków zabezpieczeń danych osobowych:

1. Zabezpieczenia fizyczne:
   - pomieszczenia zamykane na klucz,
   - szafy pancerne z zamkami,
2. Zabezpieczenia procesów przetwarzania danych w dokumentacji papierowej:
   - przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach,
   - przetwarzanie danych osobowych następuje przez wyznaczone do tego celu osoby.
   -

3. Zabezpieczenia organizacyjne:
   - osobą odpowiedzialną za bezpieczeństwo danych jest Administrator Bezpieczeństwa Informacji (ABI),
   - Administrator Bezpieczeństwa Informacji i wszyscy powołani przez niego administratorzy na bieżąco kontrolują pracę systemu informatycznego z należytą starannością, zgodnie z aktualnie obowiązującą w tym zakresie wiedzą i z obowiązującymi procedurami,
4. Organizacja pracy przy przetwarzaniu danych osobowych i zasady przetwarzania:
   - wykaz pracowników Jednostki uprawnionych do przetwarzania danych osobowych, znajduje się u Administratora Bezpieczeństwa Informacji- zał. nr 6
   - przetwarzać dane osobowe mogą jedynie pracownicy, którzy posiadają stosowne upoważnienie przyznane przez Administratora Danych Osobowych- zał. Nr 5,
   - w trakcie przetwarzania danych osobowych, pracownik jest osobiście odpowiedzialny za bezpieczeństwo powierzonych mu danych,
   - przed przystąpieniem do realizacji zadań związanych z przetwarzaniem danych osobowych, pracownik winien sprawdzić, czy posiadane przez niego dane były należycie zabezpieczone, oraz czy zabezpieczenia te nie były naruszone,
   - w trakcie przetwarzania danych osobowych, pracownik winien dbać o należyte ich zabezpieczenie przed możliwością wglądu, bądź zmiany przez osoby do tego celu nieupoważnione,
   - po zakończeniu przetwarzania danych pracownik winien należycie zabezpieczyć dane osobowe przed możliwością dostępu do nich osób nieupoważnionych.

X. ARCHIWIZOWANIE INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE

§25.

Archiwizacja informacji zawierających dane osobowe odbywa w formie elektronicznej oraz papierowej. Nośniki danych przechowywane są w wydzielonych pomieszczeniach, które są zabezpieczone przed dostępem osób nieupoważnionych (wykaz pomieszczeń załącznik nr 4)

Załącznik nr 1
do Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy Obrzycko

Wykaz osób,

które zostały zapoznane z „Polityką bezpieczeństwa systemów informatycznych" służących do przetwarzania danych osobowych w Urzędzie Gminy Obrzycko

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

Lp	Nazwisko i imię	Komórka organizacyjna	Data, podpis

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

w

Urzędzie Gminy Obrzycko

§1

Instrukcja jest przeznaczona dla osób zatrudnionych przy przetwarzaniu danych osobowych.

§2

Za naruszenie ochrony danych osobowych uznaje się przypadki, gdy:

1. stwierdzono naruszenie zabezpieczenia systemu informatycznego lub naruszenie zabezpieczenia zbioru danych osobowych zebranych i przetwarzanych w innej formie,
2. stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych.

§3

Każdy pracownik Jednostki, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych w systemie informatycznym (lub przetwarzanych w inny sposób) zobowiązany jest do niezwłocznego poinformowania o tym administratora tego systemu informatycznego lub w przypadku jego nieobecności administratora bezpieczeństwa informacji Jednostki.

§4

1. Dane osobowe zostają ujawnione, gdy stają się znane w całości lub części pozwalającej na określenie osobom nieuprawnionym tożsamości osoby, której dane dotyczą.

2. W stosunku do danych, które zostały zagubione, pozostawione bez nadzoru poza obszarem bezpieczeństwa należy przeprowadzić postępowanie wyjaśniające, czy dane osobowe należy uznać za ujawnione.

§5

1. Administrator bazy danych osobowych, który stwierdził lub uzyskał informację wskazującą na naruszenie ochrony tej bazy danych zobowiązany jest do niezwłocznego:

1) zapisania wszelkich informacji i okoliczności związanych z danym zdarzeniem, a w szczególności dokładnego czasu uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnym wykryciu tego faktu,

2) jeżeli zasoby systemu na to pozwalają, wygenerowania i wydrukowania wszystkich dokumentów i raportów, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzenia ich datą i podpisania,

3) przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym do określenia skali zniszczeń, metody dostępu osoby niepowołanej do danych itp.

4) podjęcia odpowiednich kroków w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych, w tym m.in.

   a) fizycznego odłączenia urządzeń i segmentów sieci które mogły umożliwić dostęp do bazy danych osobie niepowołanej,

   b) wylogowania użytkownika podejrzanego o naruszenie ochrony danych,

   c) zmianę hasła na konto administratora i użytkownika poprzez którego uzyskano nielegalny dostęp w celu uniknięcia ponownej próby uzyskania takiego dostępu.

5) szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych,

6) przywrócenia normalnego działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, odtworzenia jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności mających na celu uniknięcie ponownego uzyskania dostępu przez osobę nieupoważnioną, tą samą drogą.

2. Po przywróceniu normalnego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

3. Jeżeli przyczyną zdarzenia był błąd użytkownika systemu informatycznego, należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych.

4. Jeżeli przyczyną zdarzenia była infekcja wirusem należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe i organizacyjne wykluczające powtórzenie się podobnego zdarzenia w przyszłości.

5. Jeżeli przyczyną zdarzenia było zaniedbanie ze strony użytkownika systemu należy wyciągnąć konsekwencje dyscyplinarne wynikające z kodeksu pracy oraz ustawy o ochronie danych osobowych.

§6

1. Administrator bazy danych osobowych, w której nastąpiło naruszenie ochrony danych osobowych przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia i w terminie 14 dni od daty jego zaistnienia przekazuje i administratorowi bezpieczeństwa informacji Jednostce.

2. Administrator bezpieczeństwa informacji w Jednostce przeprowadza analizę raportów i uwzględnia je w opracowywaniu corocznego raportu dla administratora danych w Jednostce.

Załącznik nr 3
do Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy Obrzycko

R a p o r t

z naruszenia bezpieczeństwa systemu informatycznego w Urzędzie Gminy Obrzycko

1. Data:.....Godzina:.....
2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....

(Imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje))

3. Lokalizacja zdarzenia:

.....

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....

.....

5. Podjęte działania:

.....

.....

6. Przyczyny wystąpienia zdarzenia:

.....

.....

7. Postępowanie wyjaśniające:

.....

.....

.....

data, podpis Administratora Bezpieczeństwa Informacji

WYKAZ POMIESZCZEŃ, W KTÓRYCH SĄ PRZETWARZANE, PRZECHOWYWANE, NISZCZONE DANE OSOBOWE W URZĘDZIE GMINY OBRZYCKO

a/ pomieszczenia znajdujące się w budynku Jednostki przy ul. Rynek 19

- (biura) pokoje nr : 1, 2, 3, 4,

b/ budynek przy ul. Rynek 1

c/budynek przy ul. Rynek 2

Załącznik Nr 2.
do Zarządzenia Nr 217/214
Wójta Gminy Obrzycko
z dnia 27.10.2014

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

I. Cel instrukcji

Instrukcja określa sposób zarządzania systemem informatycznym wykorzystywanym do przetwarzania danych osobowych przez administratora danych w celu zabezpieczenia danych osobowych przed zagrożeniami, w tym zwłaszcza przed ich udostępnianiem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem, opisuje nadawanie uprawnień użytkownikom, określa sposoby pracy w systemie informatycznym oraz czynności mające wpływ na zapewnienie bezpieczeństwa systemu informatycznego Urzędu Gminy Obrzycko.

II. Definicje

§1. Ilekroć w instrukcji jest mowa o:
1) ustawie – rozumie się przez to ustawę z 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz.U. z 2014 r. poz. 1182),
2) rozporządzeniu – rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 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) administratorze danych – należy przez to rozumieć Wójta Gminy Obrzycko,
4) administratorze bezpieczeństwa informacji – reprezentowanym przez p. Jacka Michałowskiego,
5) administratorze systemu – rozumie się przez to informatyka,
6) osobie upoważnionej do przetwarzania danych osobowych – rozumie się przez to osobę zatrudnioną na podstawie umowy o pracę, umowy zlecenia lub innej umowy, osobę odbywającą u administratora danych staż absolwencki, praktykę studencką, wolontariat, której nadane zostało przez administratora danych upoważnienie do przetwarzania danych osobowych,
7) użytkowniku – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano uprawnienia do przetwarzania danych w systemie informatycznym,
8) sieci lokalnej – należy przez to rozumieć połączenie systemów informatycznych Urzędu Gminy Obrzycko wyłącznie do własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych,
9) sieci rozległej – należy przez to rozumieć sieć publiczną w rozumieniu ustawy– prawo telekomunikacyjne
10) systemie informatycznym administratora danych – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych,
11) identyfikatorze użytkownika – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną

do przetwarzania danych osobowych w wyznaczonych przez administratora danych osobowych obszarach systemu informatycznego administratora danych,

12) haśle – rozumie się przez to ośmioznakowy ciąg znaków literowych, cyfrowych, zawierający duże i małe litery oraz znaki specjalne, znany jedynie osobie, której nadano identyfikator użytkownika,

13) odbiorcy danych – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
   a) osoby, której dane dotyczą,
   b) osoby, upoważnionej do przetwarzania danych,
   c) przedstawiciela, o którym mowa w art. 31a ustawy,
   d) podmiotu, o którym mowa w art. 31 ustawy,
   e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;

12) serwisancie – rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego.

III. Poziom bezpieczeństwa

§1. Uwzględniając kategorie danych osobowych oraz konieczność zachowania bezpieczeństwa ich przetwarzania w systemie informatycznym połączonym z siecią publiczną, wprowadza się „poziom wysoki" bezpieczeństwa w rozumieniu §6 rozporządzenia.

IV. Nadawanie i rejestrowanie (wyrejestrowywanie) uprawnień do przetwarzania danych w systemie informatycznym

§2. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z :

- Ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst. jedn. Dz. U. z 2014r. poz. 1182),
- Polityką bezpieczeństwa systemów informatycznych do przetwarzania danych osobowych w Urzędzie Gminy Obrzycko,
- niniejszym dokumentem,

oraz posiadać upoważnienie do przetwarzania danych osobowych.

§3. Administrator Systemu Informatycznego przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego upoważnienia (wniosku) określającego zakres uprawnień pracownika, którego wzór stanowi **załącznik nr 1**, z wyłączeniem osób kierujących Urzędem.

§4. Administrator Systemu jest zobowiązany upoważnić co najmniej jednego pracownika - do rejestracji użytkowników w systemie informatycznym w czasie swojej nieobecności dłuższej niż 21 dni.

§5. Rejestracja użytkownika, polega na nadaniu unikalnego identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.

§6. Wyrejestrowanie użytkownika z systemu informatycznego dokonuje administrator systemu na wniosek przełożonego **załącznik nr 1**, któremu pracownik podlega z podaniem daty oraz przyczyny odebrania uprawnień, zatwierdzonego przez Administratora bezpieczeństwa informacji.

§7.Wyrejestrowanie, o którym mowa w §6, może mieć charakter czasowy lub trwały.

§8.Wyrejestrowanie następuje przez:
1) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe)
2) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

§9. Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego może być:
1) wypowiedzenie umowy o pracę;
2) wszczęcie postępowania dyscyplinarnego względem osoby upoważnionej do przetwarzania danych osobowych.
3) zawieszenie w pełnieniu obowiązków służbowych

§10. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik.

§11. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane oraz unieważnić jej hasło.

§12. Administrator Systemu Informatycznego zobowiązany jest do prowadzenia i ochrony rejestru użytkowników i ich uprawnień w systemie informatycznym, rejestr stanowi **załącznik nr 2**.

V. Metody i środki uwierzytelniania oraz procedury związane z ich zarządzeniem i użytkowaniem

§13. Identyfikator składa się z co najmniej sześciu znaków oraz pomija się polskie znaki diakrytyczne.

§14. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika administrator systemu. Za zgodą administratora bezpieczeństwa informacji, nadaje inny identyfikator.

§15. W systemie stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do sieci lokalnej oraz dostępu do aplikacji.

§16. Identyfikator użytkownika w aplikacji (o ile działanie aplikacji na to pozwala), powinien być tożsamy z tym, jaki jest mu przydzielany w sieci lokalnej.

§17. Kierownicy komórek organizacyjnych zobowiązani są pisemnie informować Administratora Bezpieczeństwa Informacji o każdej zmianie dotyczącej podległych pracowników mających wpływ na zakres posiadanych uprawnień w systemie informatycznym.

§18. Bezpośredni dostęp do systemu informatycznego może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.

§19. Hasło użytkownika powinno być zmieniane nie rzadziej niż co 90 dni.

§20. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.

§21. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.

§22. Hasło użytkownika utrzymuję się również w tajemnicy po upływie ich ważności.

§23. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.

§24. W sytuacji kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do powiadomienia Administratora Systemu w celu nadania nowego hasła.

§25. Hasło powinno składać się z niepowtarzalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne o ile system informatyczny na to pozwala. Hasło nie może być identyczne z identyfikatorem użytkownika w jakiejkolwiek formie(pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę itp.), ani z jego imieniem lub nazwiskiem.

§26. Zakazuję się stosować haseł, które użytkownik stosował uprzednio w okresie minionego roku, imion osób z najbliższej rodziny, ogólnie dostępnych informacji o użytkowniku takich jak numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego, nazwa ulicy na której mieszka lub pracuje, przewidywanych sekwencji z klawiatury (np.: „QWERTY" i „12345" itp.

§27. Zmiany hasła nie wolno zlecać innym osobom, oprócz Administratora Systemu..

§28. Nie należy korzystać opcji zapamiętywania hasła w systemie oraz użytkowanych aplikacjach.

§29. Hasło administratora systemu przechowywane jest w zamkniętej kopercie w sejfie ognioodpornym w pomieszczeniu serwerowni, do którego mają dostęp wyłącznie Wójt i zastępca Wójta, Administrator Systemu oraz Administrator Bezpieczeństwa Informacji.

VI. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

§30. Rozpoczęcie pracy na stacji roboczej następuje po włączeniu napięcia w listwie podtrzymującej napięcie (w przypadku posiadania listwy), włączeniu zasilacza awaryjnego (UPS) i komputera, a następnie wprowadzeniu identyfikatora indywidualnego oraz hasła identyfikatora znanego tylko użytkownikowi,

§31. W pomieszczeniu, w którym przetwarzane są dane osobowe, mogą znajdować się osoby postronne tylko za zgodą i w towarzystwie użytkownika.

§32. Przed osobami postronnymi należy chronić ekrany komputerów (ustawienie monitora powinno uniemożliwiać podgląd), wydruki leżące na biurkach oraz w otwartych szafach,

§33. Monitory komputerów wyposażone są we włączające po 5 minutach od przerwania pracy wygaszacze ekranu. Wznowienie wyświetlenia następuje dopiero po wprowadzeniu odpowiedniego hasła,

§34. W przypadku opuszczenia stanowiska pracy użytkownik obowiązany jest wylogować się z systemu aktywizować lub w inny sposób zablokować stację robocza,

§35. Obowiązuje zakaz robienia kopii całych zbiorów danych. Całe zbiory danych mogą być kopiowane tylko przez Administratora Systemu lub automatycznie przez system, z zachowaniem procedur ochrony danych osobowych,

§36. Jednostkowe dane mogą być przekazywane pocztą elektroniczną między komputerami Administratora Danych a komputerami przenośnymi użytkowników tylko po ich zabezpieczeniu hasłem.,

§37. Wypisy ze zbiorów danych udostępniane na podstawie art. 29 ustawy podmiotom nie będącym odbiorcami danych można przesyłać poczta elektroniczną tylko w postaci zaszyfrowanej,

§38. Obowiązuje zakaz wynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz obszernych z nich wypisów, nawet w postaci zaszyfrowanej,

§39. Przetwarzając dane osobowe, należy odpowiednio często robić kopie robocze danych, na których się właśnie pracuje, tak aby zapobiegać ich utracie,

§40. Zakończenie pracy na stacji roboczej następuje po wprowadzeniu danych programów, a następnie prawidłowym zamknięciu aplikacji uruchomionych oraz wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w zasilaczu awaryjnym (UPS) i listwie (jeżeli jest podłączona).

§41. Przed opuszczeniem pokoju należy:

a) zniszczyć w niszczarce lub schować do zamykanych na klucz szaf wszelkie wykonane wydruki zawierające dane osobowe,
b) schować do zamykanych na klucz szaf akta zawierające dane osobowe,
c) umieścić klucze do szaf w ustalonym, przeznaczonym do tego miejscu,
d) zamknąć okna.

§42. Opuszczając pokój, należy zamknąć za sobą drzwi na klucz. Jeśli niemożliwe jest umieszczenie wszystkich zawierających dane osobowe dokumentów w zamykanych szafach, to należy powiadomić o tym Sekretarza Gminy, który zgłasza osobom sprzątającym jednorazową rezygnację z wykonania usługi sprzątania.

§43. Jeżeli jest to możliwe, to przy przetwarzaniu danych osobowych na komputerach przenośnych obowiązują procedury określone w niniejszej instrukcji dotyczące pracy na komputerach stacjonarnych,

§44. Użytkownicy, którym zostały powierzone komputery przenośne powinny chronić je przed uszkodzeniem, kradzieżą i dostępem osób postronnych; szczególną ostrożność należy zachować podczas ich transportu,

§45. Obowiązuje zakaz używania komputerów przenośnych przez osoby inne niż użytkownicy, którym zostały one powierzone,

§46. Praca na komputerze przenośnym możliwa jest po wprowadzeniu hasła i indywidualnego identyfikatora użytkownika,

§47. Obowiązuje zakaz przetwarzania na komputerach przenośnych całych zbiorów danych lub obszernych z nich wypisów, nawet w postaci zaszyfrowanej,

§48. Obowiązuje zakaz samodzielnej modernizacji oprogramowania i sprzętu w powierzonych komputerach stacjonarnych oraz przenośnych. Wszelkie zmiany mogą być dokonywane tylko pod nadzorem Administratora Systemu, stosownie do wymagań niniejszej instrukcji. W razie wystąpienia usterek w pracy komputerów przenośnych lub w razie wystąpienia konieczności aktualizacji ich oprogramowania należy zgłosić to Administratorowi Systemu,

§49. Komputery stacjonarne oraz przenośne wyposażone są w odpowiednie programy ochrony antywirusowej, których aktualizację pobierana jest automatyczne lub przez Administratora Systemu.

VII. Procedury tworzenia kopii zapasowych

§50. Kopie zapasowe tworzy się:
1) codziennie – wszystkie systemy
2) raz w tygodniu – wszystkie systemy,

§51. Wybrane kopie wykonywane są po zakończeniu pracy wszystkich użytkowników w sieci komputerowej.

§52. Kopia bezpieczeństwa wykonywana jest:
1) Rynek 19 (sieć posiadająca serwer danych):
   a) kopia dzienna – dysk sieciowy
   b) kopia tygodnia – nośnik DVD
2) Rynek 1 oraz Rynek 2 (sieć posiadająca serwer danych):
   a) kopia tygodnia – nośnik DVD

§53. W przypadku wykonywania zabezpieczeń długoterminowych na płytach DVD, nośniki te należy dwa razy w roku sprawdzać pod kątem ich dalszej przydatności.

§54. Stwierdzenie utraty przez kopie awaryjne waloru przydatności do celu, o którym mowa w §54, upoważnia Administratora Systemu do ich zniszczenia.

VIII. Przechowywanie elektronicznych nośników informacji zawierających dane osobowe oraz wydruków ich kopii zapasowych

§55.Elektroniczne nośniki informacji.
1) Dane osobowe w postaci elektronicznej – zapisywane na dyskietkach, dyskach magnetooptycznych, dyskach twardych oraz innych nośnikach informacji nie są wynoszone poza siedzibę Urzędu Gminy.

2) Wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych określonych w Polityce bezpieczeństwa systemów informatycznych do przetwarzania danych osobowych.
3) Po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji są przechowywane w zamykanych szafach biurowych.
4) Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe uszkadza się w sposób mechaniczny uniemożliwiając ich odczytanie.
5) Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych pozbawia się wcześniej zapisu tych danych.
6) Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej.

§56. Zakazuje się przetwarzania danych osobowych na zewnętrznych nośnikach magnetycznych, optycznych i innych oraz ich przesyłania pocztą, elektroniczną bez ich uprzedniego zaszyfrowania.

§57. Na nośnikach, o których mowa w §57 , dopuszczalne jest przetwarzanie jedynie jednostkowych danych osobowych.

§58. W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnętrznego użytkownik jest zobowiązany do sprawdzenia go programem antywirusowym na swoim komputerze.

§59. Nośniki magnetyczne z zaszyfrowanymi, jednostkowymi danymi osobowymi są – na czas ich użyteczności – przechowywane w zamkniętych na klucz szafach, a po ich wykorzystaniu dane na nich zawarte są trwale usuwane lub nośniki te są niszczone.

§60. Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione do przetwarzania danych osobowych.

§61. Kopie zapasowe programów, których przydatność nie nadaje się do dalszego wykorzystania są trwale niszczone mechanicznie w niszczarce.

§62. Kopie zapasowe.
1) Kopie bezpieczeństwa są przechowywane w sejfie Urzędu Gminy Obrzycko.
2) Dostęp do danych opisanych w punkcie 1 ma Administrator Systemu Informatycznego.

§63.Wydruki.
1) W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym.
2) Pomieszczenia, w którym przechowywane są wydruki robocze musi być należycie zabezpieczone po godzinach pracy.
3) Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

IX. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego oraz wirusami komputerowymi

§64 Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe pracujące w trybie monitora (ciągła praca w tle).

§65. Każdy e-mail oraz załączniki muszą być sprawdzone przez program antywirusowy pod kątem obecności wirusów.

§66. Definicje wzorców wirusów aktualizowane są nie rzadziej niż raz w miesiącu.

§67. Jeżeli oprogramowanie antywirusowe pozwala, to należy ustawić harmonogram zadań tak aby raz w tygodniu lub więcej razy sprawdzał daną jednostkę komputerową pod kątem obecności wirusów.

§68. Do obowiązków Administratora Systemu należy aktualizacja oprogramowania antywirusowego oraz określenie częstotliwości automatycznych aktualizacji definicji wirusów dokonywanych przez to oprogramowanie.

§69. Zabrania się używania nośników niewiadomego pochodzenia (pendrive, karty pamięci, dyski wymienne, nośniki CD i DVD) bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje użytkownik, który nośnik zamierza użyć.

§70. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.

§71. Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje pracownik, który pocztę otrzymał.

§72. Administrator Systemu Informatycznego przeprowadza cyklicznie kontrole antywirusowe na wszystkich komputerach – minimum co trzy miesiące.

§73. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku stwierdzenia nieprawidłowości zgłoszonych przez pracownika w funkcjonowaniu sprzętu komputerowego lub oprogramowania.

§74 W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe na którym wykryto wirusa oraz wszystkie posiadane przez użytkownika nośniki.

§75. Użytkownik jest obowiązany zawiadomić administratora systemu o pojawiających komunikatach wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.

§76. Użytkownicy mogą korzystać z zewnętrznych nośników danych tylko po uprzednim sprawdzeniu zawartości nośnika oprogramowaniem antywirusowym.

§77. Pracownicy nie są upoważnieni do instalacji jakiegokolwiek prywatnego oprogramowania. W przypadku zainstalowania takiego oprogramowania bez odpowiedniej akceptacji pracownik ponosi odpowiedzialność porządkową i prawną.

§78. Oprogramowanie na komputerach może być zainstalowane wyłącznie przez Administratora Systemów Informatycznych.

X. Kontrola nad wprowadzaniem, dalszym przetwarzaniem i udostępnianiem danych osobowych

§79. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie osobom uprawnionym.

§80. Udostępnienie danych osobowych nie może być realizowane drogą telefoniczną.

§81. Aplikacje danych osobowych do obsługi baz danych osobowych powinny zapewniać odnotowanie informacji o udzielonych odbiorcom danych. Zakres informacji powinien obejmować co najmniej dane odbiorcy, datę wydania, zakres udostępnionych danych.

XI. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

§82. Przeglądu i konserwacji systemu dokonuje administrator systemu doraźnie.

§83. Przeglądu i konserwacji urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonych przez producenta sprzętu.

§84. Nieprawidłowości ujawnione w trakcie tych działań powinny być niezwłocznie usunięte, a ich przyczyny powinny być przeanalizowane. O fakcie ujawnienia nieprawidłowości należy zawiadomić Administratora Bezpieczeństwa Informacji.

§85. Przeglądu pliku zawierającego raport dotyczący działalność aplikacji bądź systemów serwerowych (log systemowy) Administrator Systemu dokonuje nie rzadziej niż raz na miesiąc.

§86. Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje użytkownik przy współudziale Administratora Systemu nie rzadziej niż raz na miesiąc.

XII. Naprawa urządzeń komputerowych z chronionymi danymi osobowymi

§87. Wszelkie naprawy urządzeń komputerowych oraz zmiany w systemie informatycznym Administratora Danych przeprowadzane są – jeżeli jest to możliwe – przez Administratora Systemu.

§88. Naprawy i zmiany w systemie informatycznym Administratora Danych przeprowadzane przez serwisanta prowadzone są pod nadzorem Administratora Systemu, jeżeli jest to możliwe – w siedzibie administratora danych lub poza siedzibą Administratora Danych, po uprzednim nieodwracalnym usunięciu danych w nich przetwarzanych, a jeśli wiązałoby się to

z nadmiernymi utrudnieniami, to po podpisaniu umów powierzenia przetwarzania danych osobowych.

§89. Jeśli nośnik danych (dysk, dyskietka, płyta lub inne) zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, to należy go zniszczyć mechanicznie.

XIII. Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego

§90. Użytkownik zobowiązany jest zawiadomić Administratora Systemu lub Administratora Bezpieczeństwa Informacji o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu, a w szczególności o :

1) naruszeniu hasła dostępu i identyfikatora (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzania hasła),
2) częściowym lub całkowitym braku danych albo dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień,
3) braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów serwera,
4) wykryciu wirusa komputerowego,
5) zauważeniu elektronicznych śladów próby włamania do systemu informatycznego Administratora Danych,
6) znacznym spowolnieniu działu informatycznego,
7) podejrzeniu kradzieży sprzętu komputerowego lub dokumentów zawierających dane osobowe,
8) zmianie położenia sprzętu komputerowego,
9) zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf.

§91. Do czasu przybycia na miejsce Administratora Bezpieczeństwa Informacji lub Administratora Systemu:

1) jeżeli istnieje taka możliwość, niezwłocznie podjąć czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego zdarzenia a następnie uwzględnić w działaniu również ustalenie jego przyczyny lub sprawców,
2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
3) zaniechać – jeżeli to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
4) zastosować się do instrukcji i regulaminów lub dokumentacji aplikacji, jeśli odnoszą się one do zaistniałego przypadku,
5) przygotować opis incydentu,
6) nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa Informacji lub Administratora Systemu.

§92. Administrator Systemu przyjmujący zawiadomienie jest obowiązany niezwłocznie poinformować Administratora Bezpieczeństwa Informacji o naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu.

§93. Administrator Bezpieczeństwa Informacji po otrzymaniu zawiadomienia, o którym mowa w §92, powinien niezwłocznie:

1) przeprowadzić postępowanie wyjaśniające, w celu ustalenia okoliczności naruszenia ochrony danych osobowych,
2) podjąć działania chroniące system przed ponownym naruszeniem,
3) w przypadku stwierdzenia faktycznego naruszenia bezpieczeństwa systemu sporządzić raport naruszenia bezpieczeństwa systemu informatycznego Administratora Danych, a następnie niezwłocznie przekazać jego kopie Administratorowi Danych,

§94. Administrator Bezpieczeństwa Informacji w uzgodnieniu z Administratorem Systemu może zarządzić, w razie potrzeby, odłączenie części systemu informatycznego dotkniętej incydentem od pozostałej jego części.

§95. W razie odtwarzania danych z kopii zapasowych Administrator Systemu obowiązany jest upewnić się, że odtwarzane dane zapisane zostały przed wystąpieniem incydentu; dotyczy to zwłaszcza przypadków infekcji wirusowej.

§96. Administrator danych po zapoznaniu się z raportem, o którym mowa w §94 pkt 3, podejmuje decyzję o dalszym trybie postępowania, powiadomieniu właściwych organów oraz podjęciu innych, szczególnych czynności zapewniających bezpieczeństwo systemu informatycznego Administratora Danych bądź zastosowaniu środków ochrony fizycznej.

§97. Administrator Bezpieczeństwa Informacji i Administrator Systemu zobowiązani są do informowania Administratora Danych o awariach systemu informatycznego, zauważonych przypadkach naruszenia niniejszej instrukcji przez użytkowników, a zwłaszcza o przypadkach posługiwania się przez użytkowników nieautoryzowanymi programami, nieprzestrzegania zasad używania oprogramowania antywirusowego, niewłaściwego wykorzystania sprzętu komputerowego lub przetwarzania danych w sposób niezgodny z procedurami ochrony danych osobowych.

§98. Administrator Bezpieczeństwa Informacji składa raz w roku Administratorowi Danych kompleksową analizę zarządzania systemem informatycznym.

XIV. Postanowienia końcowe

§99. W sprawach nieokreślonych niniejszą instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.

§100. Naruszenie obowiązków wynikających z niniejszej instrukcji oraz przepisów o ochronie danych osobowych może zostać potraktowane jako naruszenie obowiązków pracowniczych i powodować określoną przepisami Kodeksu pracy odpowiedzialność pracownika.

Załącznik nr 1
do Instrukcji Zarządzania
Systemem Informatycznym

WNIOSEK
O NADANIE UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

☐ Nowy użytkownik	☐ Modyfikacja uprawnień	☐ Odebranie uprawnień w systemie informatycznym

Imię i nazwisko użytkownika:	**Wydział/biuro/samodzielne stanowisko**
Opis i zakres uprawnień użytkownika w systemie informatycznym	
Data wystawienia:	Podpis bezpośredniego przełożonego użytkownika systemu:
Podpis Administratora Systemu:	Akceptacja ABI

Załącznik nr 2
do Instrukcji Zarządzania Systemem Informatycznym

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRACY W SYSTEMIE INFORMATYCZNYM ORAZ UPOWAŻNINYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Nazwisko, Imię	System/aplikacja	Zakres upoważnienia do przetwarzania danych osobowych	Data nadania uprawnień	Data ustania uprawnień	Identyfikator użytkownika

Załącznik nr 3
do Instrukcji Zarządzania
Systemem Informatycznym

Dziennik zawiera opisy wszelkich zdarzeń istotnych dla działania systemu informatycznego w szczególności:
- w przypadku awarii – opis awarii, przyczyna awarii, szkody wynikłe na skutek awarii, sposób usunięcia awarii, opis systemu po awarii, wnioski,
- w przypadku konserwacji systemu – opis podjętych działań, wnioski.

DZIENNIK SYSTEMU INFORMATYCZNEGO
URZĘDU GMINY W OBRZYCKO

L.p.	Data i godzina zdarzenia	Opis zdarzenia	Podjęte działania/wnioski	Podpis