ZARZĄDZENIE NR 5 /2013
Wójta Gminy Krasocin

z dnia 28 styczeń 2013 r.

w sprawie wprowadzenia Instrukcji zarządzania systemem informatycznym

Na podstawie § 3 ust. 3 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 zarządza się, co następuje:

§ 1

Przyjmuje się do stosowania ,,*Instrukcję zarządzania systemem informatycznym* ", stanowiącą załącznik Nr 1 do niniejszego zarządzenia.

§ 2

1. Wykonanie zarządzenia powierza się pracownikom Urzędu Gminy Krasocin .
2. Kierownicy komórek organizacyjnych są obowiązani zapoznać się z treścią Instrukcji każdego użytkownika.
3. Wszyscy pracownicy potwierdzają własnoręcznym podpisem fakt zapoznania się z treścią niniejszego zarządzenia.
4. Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik nr 1 do Zarządzenia nr 5/2013
z dnia 28.012013 r.
Wójta Gminy Krasocin
w sprawie wprowadzenia Instrukcji zarządzania systemem informatycznym

INSTRUKCJA
ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje systemach informatycznych,

3) systemie informatycznym – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
4) kartotece – rozumie się przez to zewidencjonowany, usystematyzowany zbiór wykazów, skoroszytów, wydruków komputerowych i innej dokumentacji gromadzonej w formie papierowej, zawierającej dane osobowe,
5) Administratorze Danych – rozumie się przez to Urząd Gminy Krasocin ,
6) Wójcie – rozumie się przez to Wójta Gminy Krasocin ,
7) Administratorze Bezpieczeństwa Informacji – rozumie się przez to osobę nadzorującą przestrzeganie zasad ochrony przetwarzanych danych osobowych. Nadzoruje on stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych , a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz zmianą utratą, uszkodzeniem lub zniszczeniem, a także przeprowadza kontrole w zakresie określonym regulacjami wewnętrznymi Administratora danych,
8) osobie odpowiedzialnej za prawidłowe funkcjonowanie sprzętu, oprogramowania i jego konserwację – rozumie się przez to wyznaczonego przez Wójta informatyka odpowiedzialnego za powyższe zadania, zwanej dalej „Informatykiem",
9) komórce organizacyjnej – rozumie przez to każdą wydzieloną organizacyjnie i funkcjonalnie komórkę wewnętrzną, zgodnie z regulaminem organizacyjnym,
10) użytkowniku – rozumie się przez to osobę wykonującą zadania w systemie informatycznym oraz kartotekach,
11) pracowniku ochrony – rozumie się przez to osobę wykonującą zadania z zakresu ochrony osób i mienia na rzecz Administratora Danych,
12) pomieszczeniach – rozumie się przez to budynki, pomieszczenia lub części pomieszczeń określone przez Administratora Danych, tworzące Krasocin

r, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego lub gromadzone w kartotekach.

§ 4

1. Podstawowym celem zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych jest zapewnienie jak najwyższego standardu bezpieczeństwa tych danych. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania, charakteru. poufnego wraz zachowaniem ich integralności oraz integralności systemu informatycznego.
2. Za przestrzeganie zasad ochrony i bezpieczeństwa danych w komórkach organizacyjnych odpowiedzialni są kierownicy tych komórek.

§ 5

Realizację zamierzeń określonych w § 4 powinny zagwarantować następujące założenia:

1) wdrożenie procedur określających postępowanie osób dopuszczonych do przetwarzania danych osobowych oraz ich odpowiedzialność za ochronę tych danych,

2) przeszkolenie użytkowników w zakresie bezpieczeństwa i ochrony danych osobowych,

3) przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła, identyfikatory) oraz zapewniających dostęp użytkowników do różnych poziomów zbiorów danych osobowych – stosownie do indywidualnego zakresu upoważnienia,

4) podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie zabezpieczeń,

5) okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych,

6) opracowanie procedur odtwarzania systemu w przypadku wystąpienia awarii,

7) śledzenie osiągnięć w dziedzinie zabezpieczania systemów informatycznych i - w miarę możliwości organizacyjnych i techniczno-finansowych – wdrażanie nowych narzędzi i metod pracy oraz sposobów

zarządzania systemem informatycznym, które będą służyły wzmocnieniu bezpieczeństwa danych osobowych.

ROZDZIAŁ II
Przydział uprawnień i identyfikatorów

§ 6

1. Każdy użytkownik dopuszczony do przetwarzania danych osobowych posiada *stosowne upoważnienie. Wzór upoważnienia do przetwarzania danych* osobowych, stanowi załącznik nr 1 do Instrukcji.
2. Każdy u użytkownik posiada indywidualny identyfikator umożliwiający logowanie do tych aplikacji, z którymi może pracować.
3. Identyfikator umożliwia wykonanie czynności zgodnie z zakresem powierzonych obowiązków, które wyznaczają poziom uprawnień.
4. Postanowienia ust, 2 dotyczą użytkowników, którzy jako jedyni mają dostęp do danych przetwarzanych w systemie informatycznym oraz użytkowników, którzy mają dostęp wyłącznie do danych osobowych gromadzonych w kartotekach.
5. Informatyk zobowiązany jest do prowadzenia ewidencji przyznanych poszczególnym użytkownikom uprawnień związanych z dostępem do zbiorów danych oraz dokonywaniem zmian w zakresie przyznanych uprawnień.

§ 7

Każdy użytkownik systemu informatycznego przetwarzającego dane osobowe *powinien posiadać umiejętność bezpiecznej obsługi komputera i dobrą znajomość* oprogramowania systemowego i operacyjnego, z którego będzie korzystał.

§ 8

1. Każdy użytkownik – przed dopuszczeniem do obsługi systemu *informatycznego, w którym przetwarzane są dane osobowe – podlega* przeszkoleniu w zakresie:
   1) obsługi komputera, oprogramowania systemowego oraz oprogramowania do obsługi aplikacji, którą będzie wykorzystywał,
   2) przepisów o ochronie danych osobowych oraz wynikających z nich zadań oraz obowiązków.

2. wszyscy użytkownicy podlegają 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.

§ 9

Do uwierzytelniania użytkowników w systemie używa się haseł lub innych metod zapewniających weryfikację tożsamości użytkownika.

§ 10

Każdy użytkownik zobowiązany jest do zachowania w tajemnicy własnych haseł, także po upływie ich ważności.

§ 11

1. Identyfikator dla użytkowników upoważnionych do przetwarzania danych osobowych w systemie informatycznym, niezbędne do logowania się do określonej aplikacji, ustala i przydziela Informatyk lub inna osoba upoważniona przez Administratora Danych
2. Identyfikator użytkownika nie podlega zmianie.
3. Identyfikator użytkownika podlega rejestracji w systemie informatycznym.

§ 12

1. Pierwsze hasło użytkownika ustala Informatyk przy wprowadzaniu *identyfikatora użytkownika systemu*.
2. Hasła muszą odpowiadać następującym wymogom:

a) dla poziomu bezpieczeństwa podwyższonego i wysokiego 8 znaków, i powinny zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,

b) nie mogą być zapisywane w systemie w postaci jawnej,

c) nie mogą być w nich używane imiona, nazwiska, przezwiska, inicjały i inne kombinacje znaków mogących doprowadzić do łatwego rozszyfrowania haseł przez osoby nieupoważnione,

d) nie mogą być w nich stosowane wyłącznie znaki następujące po sobie na klawiaturze bądź te same litery czy cyfry.

§ 13

1. Po otrzymaniu hasła użytkownik zobowiązany jest załogować się do systemu i powinien zmienić hasło. Przy wpisaniu hasło nie może być wyświetlane na ekranie.
2. Hasło zmieniane jest nie rzadziej niż co 30 dni. Za systematyczną, terminową zmianę hasła odpowiada użytkownik.

§ 14

Hasło podlega natychmiastowej zmianie w przypadku podejrzenia jego odkrycia przez nieupoważnioną osobę.

§ 15

1. Hasła nie mogą być nigdzie zapisywane, z wyjątkiem haseł Informatyka, które przechowywane są w opieczętowanych kopertach, w miejscu wyznaczonym przez Administratora Bezpieczeństwa Informacji.
2. Tryb przechowywania i udostępniania haseł Informatyka określa załącznik nr 2 do Instrukcji.

ROZDZIAŁ III
Rejestrowanie i wyrejestrowanie użytkowników

§ 16

1. Ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzi Informatyk lub osoba upoważniona przez Administratora Danych.
2. Ewidencja zawiera:

1) imię i nazwisko użytkownika,
2) datę nadania i ustania upoważnienia,
3) zakres upoważnienia,
4) identyfikator użytkownika,

2. Postanowienia ust. 2 pkt. 4) nie dotyczą użytkowników, którzy mają dostęp wyłącznie do danych osobowych gromadzonych w kartotekach.

3. Ewidencja użytkowników może być prowadzona w systemie informatycznym.

§ 17

Nośniki magnetyczne (optyczne), na których gromadzone są wykazy zawierające ewidencje użytkowników przechowywane są w wyznaczonych szafach lub sejfach, do których dostęp ma wyłącznie Informatyk lub osoba upoważniona przez Administratora Bezpieczeństwa Informacji.

§ 18

Zmiany dotyczące użytkownika sieci, takie jak:

1) zmiana imienia lub nazwiska,
2) zmiana zakresu upoważnienia,

podlegają niezwłocznemu odnotowaniu w ewidencji.

§ 19

1. Zmiany dotyczące użytkownika, takie jak:
   1) rozwiązanie umowy o pracę,
   2) utrata upoważnienia do przetwarzania danych osobowych,
   3) zmiana zakresu obowiązków służbowych skutkująca ustaniem upoważnienia, powodują wyrejestrowanie użytkownika przez Informatyka, w trybie natychmiastowym, z ewidencji zablokowanie identyfikatora oraz unieważnienie hasła tego użytkownika.

2. Kierownicy komórek organizacyjnych odpowiadają za natychmiastowe zgłoszenie do Informatyka, użytkowników, którzy utracili uprawnienia do dostępu do danych osobowych, celem zablokowania im dostępu do systemu informatycznego poprzez zablokowanie identyfikatora i wyrejestrowanie z ewidencji.

§ 20

1. Identyfikator, który utracił ważność nie może być ponownie przydzielony innemu użytkownikowi.
2. Osoba prowadząca ewidencję, obowiązana jest odrębnie gromadzić identyfikatory, które utraciły ważność lub też stosować odpowiednie ich oznaczenia.

ROZDZIAŁ IV
Procedury rozpoczęcia, zawieszenia i zakończenia pracy

§ 21

Przed przystąpieniem do pracy z systemem informatycznym lub kartotekami, użytkownik *obowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych* oraz dokonać oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie poufności danych osobowych.

§ 22

W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie systemu, użytkownik obowiązany jest poinformować przełożonego.

§ 23

1. Rozpoczynając pracę na komputerze użytkownik loguje się do systemu informatycznego.
2. Użytkownik wprowadza identyfikator i dokonuje uwierzytelnienia.
3. *Jeśli system umożliwia, po przekroczonej liczbie prób logowania* system blokuje dostęp do systemu informatycznego na poziomie danego użytkownika.
4. Informatyk ustala przyczyny zablokowania systemu oraz w zależności od zaistniałej sytuacji podejmuje odpowiednie działania. O zaistniałym incydencje powiadamia Administratora Bezpieczeństwa Informacji lub osobę przez niego wyznaczoną.

§ 24

Przed opuszczeniem stanowiska pracy, użytkownik obowiązany jest wylogować się z *sytemu informatycznego*.

§ 25

Kończąc pracę należy:

1) *wylogować się z systemu informatycznego, a następnie wyłączyć* sprzęt komputerowy,

2) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe, przed dostępem osób nieuprawnionych.

ROZDZIAŁ V
Procedury tworzenia kopii zapasowych

§ 26

1. Zbiory danych osobowych oraz programy i narzędzia programowe służące do ich przetwarzania, zapisywane na nośnikach zewnętrznych (streamer, dyski: wymienne, magnetyczne, optyczne) tworzące kopie zapasowe kolejnych okresów, powinny być odpowiednio oznakowane i przechowywane w wyznaczonych, odpowiednio zabezpieczonych pomieszczeniach.
2. Kopie zapasowe określone w ust. 1 niniejszego paragrafu powinny być sporządzane regularnie w okresach wyznaczonych w załączniku nr 3 do Instrukcji.
3. Za prawidłowe sporządzanie kopii zapasowych, ich oznakowanie i przechowywanie, odpowiedzialny jest Informatyk Urzędu Gminy .
4. Odpowiada on również za sprawdzanie poprawności wykonania kopii zapasowych na nośnik zewnętrzny.
5. Kopie zapasowe powinny być przechowywane w pomieszczeniu odrębnym od pomieszczeń, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.

§ 27

1. Użytkownicy obowiązani są przestrzegać terminów tworzenia doraźnych kopii zapasowych, o ile zostali do tego upoważnieni przez Informatyka.

2. Użytkownicy określeni w ust. 1 są odpowiedzialni za prawidłowe sporządzenie kopii zapasowych, ich oznakowanie i przechowywanie.

§ 28

1. Kopie zapasowe, które uległy uszkodzeniu lub ustała ich użyteczność, podlegają natychmiastowemu zniszczeniu z zachowaniem procedur określonych niniejszą Instrukcją.

2. Zniszczenia kopii zapasowych, na nośnikach magnetycznych i optycznych dokonuje Informatyk w obecności Administratora Bezpieczeństwa Informacji lub osoby przez niego wyznaczonej.

3. Z nośników magnetycznych i optycznych wielokrotnego użytku np. CDRW dane należy usunąć w sposób uniemożliwiający ich odczytanie, a w przypadku, gdy usunięcie danych nie jest możliwe, nośniki podlegają zniszczeniu w stopniu uniemożliwiającym odzyskanie danych.

4. Dane zawarte na nośnikach jednokrotnego użytku np. CDR należy usuwać poprzez całkowite zniszczenie nośnika.

ROZDZIAŁ VI
Przetwarzanie danych osobowych

§ 29

1. Dane osobowe przetwarzane są w kartotekach oraz w komputerach do tego *przeznaczonych (serwerach, stacjach roboczych)* zlokalizowanych w obszarach przetwarzania danych osobowych.
2. W wypadku przekazywania urządzeń lub nośników zawierających dane osobowe, tzw. „wrażliwe", o których mowa w art. 27 ust. 1 ustawy o ochronie danych osobowych, poza obszar przetwarzania danych osobowych, zabezpiecza się je w sposób zapewniający poufność i integralność tych danych, przez co rozumie się:
    1) ograniczenie dostępu do danych osobowych hasłem zabezpieczającym dane przed osobami nieupoważnionymi, lub
    2) stosowanie metod kryptograficznych, lub
    3) stosowanie odpowiednich zabezpieczeń fizycznych, lub
    4) w zależności od stopnia zagrożenia zalecane jest stosowanie kombinacji wyżej wymienionych zabezpieczeń.
3. Dane osobowe zapisywane na nośnikach zewnętrznych (streamer, dyski: wymienne, magnetyczne, optyczne) tworzące kopie zapasowe kolejnych okresów, powinny być przechowywane w wyznaczonych, odpowiednio zabezpieczonych, pomieszczeniach.

4. Kartoteki powinny być przechowywane w szafach, znajdujących się w wyznaczonych, odpowiednio zabezpieczonych, pomieszczeniach.

5. Wydruki robocze, błędne lub zdezaktualizowane powinny być niezwłocznie niszczone przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie lub zanonimizowanie.

6. Szczegółowy opis obszaru przetwarzania danych osobowych oraz środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności danych osobowych określony jest w Polityce bezpieczeństwa.

§ 30

1. Kartoteka przekazywana jest do archiwum zgodnie z procedurami archiwizacji *dokumentów*.
2. Likwidacji zbiorów archiwalnych dokonuje się przy użyciu niszczarki do papieru lub w inny sposób zapewniających skuteczne ich usunięcie lub zanonimizowanie.

§ 31

Decyzje o likwidacji zbiorów danych osobowych, przetwarzanych w kartotekach oraz systemach informatycznych podejmuje Administrator Danych na wniosek Administratora Bezpieczeństwa Informacji.

§ 32

Dla udokumentowania czynności dokonywanych w celu likwidacji zbiorów danych osobowych, Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona sporządza protokół , w którym zamieszcza następujące informacje:

1. datę dokonania likwidacji,
2. przedmiot likwidacji,
3. przedział czasowy likwidowanych zbiorów danych osobowych,
4. podpisy osób dokonujących i obecnych przy likwidacji zbiorów danych osobowych.

ROZDZIAŁ VII
Zabezpieczenie systemu informatycznego

§ 33

System informatyczny zabezpiecza się przed:

1. działaniem, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,
2. utratą danych spowodowanych:
    a) działaniem nielegalnego oprogramowania,
    b) awarią zasilania lub zakłóceniami w sieci zasilającej.

§ 34

1. Informatyk odpowiada za niezwłoczne instalowanie na sprzęcie najnowszych wersji oprogramowania zabezpieczającego system informatyczny.
2. Nowe wersje oprogramowania instaluje wyłącznie Informatyk niezwłocznie po *ich otrzymaniu lub osoba upoważniona przez Informatyka.*
3. Okresowych kontroli w zakresie instalowania najnowszych wersji oprogramowania zabezpieczającego system informatyczny dokonuje Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona.

§ 35

1. Na serwerach i stacjach roboczych używanych przez Administratora Danych powinno instalować się przynajmniej jeden program antywirusowy.
2. Program antywirusowy należy również instalować również na komputerach przenośnych.

§ 36

W komputerach przenośnych zawierających dane osobowe stosuje się środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.

§ 37

1. Kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie informatycznym, jak i do celów informacyjnych.
2. *Na serwerach, w miarę możliwości technicznych,* oprogramowanie antywirusowe powinno być aktywne cały czas.
3. Na stacjach roboczych oprogramowanie antywirusowe powinno być aktywne cały czas i powinno dokonywać sprawdzenia każdego otwieranego lub uruchomianego pliku.

§ 38

Użytkownicy są zobowiązani do dokonywania kontroli antywirusowej wszystkich *nośników magnetycznych lub optycznych przychodzących z zewnątrz* oraz okresowo nośników własnych.

§ 39

1. W razie stwierdzenia zainfekowania systemu, użytkownik obowiązany jest *poinformować niezwłocznie o tym fakcie Informatyka.*
2. Informatyk usuwa wirusa, jeśli automatycznie nie dokonał tego program antywirusowy oraz informuje Administratora Bezpieczeństwa Informacji lub osobę przez niego upoważnioną o dokonanych czynnościach i rodzaju wirusa.

§ 40

W razie niemożności usunięcia wirusa, Informatyk za zgodą Administratora Bezpieczeństwa Informacji, korzysta z usług zewnętrznych specjalistów w tej dziedzinie.

§ 41

1. W sytuacji korzystania z usług zewnętrznych specjalistów, należy podjąć działania uniemożliwiające tym osobom dostęp do danych osobowych.
2. Prace określone w ust. 1 są wykonywane pod nadzorem informatyka lub upoważnionego użytkownika i w mirę możliwości bez dostępu do danych osobowych.

§ 42

1. Informatyk jest odpowiedzialny za kontrole antywirusowe serwerów i zasobów *sieciowych.*
2. Użytkownicy są odpowiedzialni za kontrole antywirusowe na dyskach lokalnych i dyskietkach.

§ 43

1. Po usunięciu wirusa Informatyk sprawdza zainfekowany system informatyczny oraz przywraca go do pełnej sprawności i funkcjonalności.
2. Informatyk sporządza raport o wystąpieniu wirusa. Raport powinien zawierać następujące informacje:
    1) nazwę wirusa,
    2) datę wykrycia wirusa,

3) miejsce zainfekowania,

4) źródło infekcji.

3. Raport, o którym mowa w ust. 2 przekazywany jest Administratorowi Bezpieczeństwa Informacji, lub osobie przez niego wyznaczonej, wraz z wnioskami, stosownymi do zaistniałej sytuacji.

§ 44

1. Przy przetwarzaniu danych osobowych zakwalifikowanych do poziomu bezpieczeństwa wysokiego system informatyczny służący do przetwarzania danych osobowych chroni przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.
2. W przypadku zastosowania logicznych zabezpieczeń, o których mowa w ust. 1, obejmują one:
   1) kontrolę przepływu informacji pomiędzy systemem informatycznym a siecią publiczną,
   2) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego.
3. Wobec danych wykorzystywanych do uwierzytelniania, które są przesyłane w sieci publicznej stosuje się środki ochrony kryptograficznej.

§ 45

Informatyk prowadzi wykaz przypadków zainfekowania komputerów i nośników wykorzystywanych do przetwarzania danych osobowych w systemie oraz przechowuje kopie raportów.

§ 46

Procedura wyrażona w niniejszym rozdziale ma zastosowanie także do *przypadków awarii systemu spowodowanych błędem programu* bądź użytkownika.

ROZDZIAŁ VIII
Wymagania dotyczące sprzętu i oprogramowania

§ 47

1. Sprzęt obsługujący zbiór danych osobowych składa się z komputerów stacjonarnych klasy PC.

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.

§ 48

1. Sieć komputerowa służąca do przetwarzania danych osobowych powinna mieć zapewnione prawidłowe zasilane energetyczne gwarantujące właściwe i zgodne z wymaganiami producenta działanie sprzętu komputerowego.
2. Sieć komputerowa powinna być podłączona do zasilania zapasowego (zasilanie dwustronne, agregat prądotwórczy lub UPS). Oprogramowanie powinno zapewnić bezpieczne wyłączanie systemu informatycznego, po dokonaniu operacji zamknięcia w pracujących aplikacjach i oprogramowaniu systemowym.
3. Serwer sieci powinien być zasilany przez UPS o odpowiednich parametrach, *pozwalających na podtrzymanie napięcia przez min. 15 minut oraz na* wykonanie, bezpiecznego wyłączenia serwera, tak aby przed zanikiem zasilania zostały prawidłowo zakończone operacje rozpoczęte na zbiorze danych osobowych.

§ 49

1. Za prawidłowe zasilanie energetyczne sieci komputerowej odpowiedzialny jest Informatyk.
2. Infrastruktura techniczna związana z siecią komputerową i jej zasilaniem *(rozdzielnie elektryczne, skrzynki z bezpiecznikami)* powinna być zabezpieczona przed dostępem osób nieupoważnionych.
3. Wszystkie urządzenia w sieci komputerowej (pozostałe stacje robocze, drukarki, modemy itd.) powinny być w miarę możliwości technicznych, włączone do wydzielonej sieci energetycznej, zapewniającej odpowiednie uziemienie i zabezpieczenie przed przepięciami.
4. Gniazda zasilania sieci komputerowej powinny być odpowiednio oznakowane, zabezpieczone przed włączeniem do nich odbiorników lub wykonane w specjalnym standardzie.

§ 50

1. Dane osobowe przesyłane na nośnikach magnetycznych i optycznych oraz za pomocą systemów teleinformatycznych powinny być zabezpieczone w sposób uniemożliwiający dostęp do nich osób nieupoważnionych.
2. Dane osobowe przesyłane na łączach telekomunikacyjnych wewnątrz danej sieci powinny być dodatkowo zabezpieczone w sposób uniemożliwiający dostęp do danej sieci LAN z innej sieci.
3. Dane osobowe przesyłane po łączach telekomunikacyjnych na zewnątrz powinny być w miarę możliwości technicznych szyfrowane za pomącą algorytmu kryptograficznego.

§ 51

1. Programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych muszą być użytkowane z zachowaniem praw autorskich i posiadać licencje.
2. Uprawnienie do instalowania programów na komputerach służbowych posiada wyłącznie Informatyk.

§ 52

Informatyk odpowiada za wyposażenie systemu informatycznego w mechanizmy uwierzytelnienia użytkownika oraz za sprawowanie kontroli dostępu do danych osobowych jedynie osób upoważnionych.

§ 53

1. Ekrany monitorów powinny być w miarę możliwości wyposażone w wygaszacze zabezpieczone hasłem, które aktywują się automatycznie po upływie określonego czasu od ostatniego użycia komputera.
2. Ekrany monitorów, powinny być ustawione w taki sposób, żeby w miarę możliwości uniemożliwić odczyt wyświetlanych informacji osobom nieupoważnionym.
3. Za spełnienie obowiązku określonego w ust. 2 odpowiadają użytkownicy i kierownicy komórek organizacyjnych.

§ 54

1. Informatyk odpowiedzialny jest za to, aby dla każdej osoby, której dane osobowe są przetwarzane, system informatyczny zapewniał odnotowanie:
   1) daty pierwszego wprowadzenia danych do systemu,
   2) identyfikatora użytkownika wprowadzającego dane, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba,
   3) źródła danych, w przypadku zbierania danych nie od osoby, które one dotyczą,
   4) informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy o ochronie danych osobowych, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych,
   5) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy o ochronie danych osobowych.

Wymagania określone w niniejszym ustępie nie dotyczą systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie.

2. Odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.
3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust.1.
4. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust. 1 pkt 4, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.
5. Do czasu spełnienia przez system informatyczny wszystkich wyżej wymienionych wymogów, system informatyczny powinien zapewnić odnotowanie:
   1) daty pierwszego wprowadzenia danych,

2) identyfikatora użytkownika wprowadzającego dane, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba.

6. Do chwili spełnienia przez system informatyczny wszystkich wymogów określonych w niniejszym paragrafie, odnotowanie informacji określonych w ust. 1 pkt. 3, 4 i 5 należy prowadzić w formie tradycyjnej (papierowej) lub komputerowo poza systemem.

ROZDZIAŁ IX
Procedury wykonywania przeglądów i konserwacji

§ 55

1. Bieżących oraz okresowych przeglądów, napraw i konserwacji systemów oraz *nośników informacji służących do przetwarzania danych osobowych*, niewymagających angażowania zewnętrznych firm serwisowych, dokonuje informatyk.
2. Przeglądów i konserwacji zbiorów danych osobowych dokonują użytkownicy, zgodnie z indywidualnymi zakresami upoważnień i odpowiedzialności.

§ 56

Prace dotyczące przeglądów, konserwacji i napraw, wymagające zaangażowania *firm zewnętrznych, są wykonywane za wiedzą Administratora* Bezpieczeństwa Informacji przez uprawnionych przedstawicieli tych firm pod nadzorem Informatyka lub upoważnionego użytkownika i w miarę możliwości bez dostępu do rzeczywistych danych osobowych.

§ 57

1. W przypadku gdy zaistnieje potrzeba naprawy lub wymiany sprzętu komputerowego służącego do przetwarzania lub przechowywania danych osobowych należy usunąć dane, w sposób uniemożliwiający ich odzyskanie.
2. *Jeżeli nie ma możliwości usunięcia danych należy urządzenie uszkodzić* w sposób uniemożliwiający ich odczytanie.

§ 58

Nadzór nad instalowaniem, sprawnym funkcjonowaniem i wymianą uszkodzonych urządzeń oraz ich likwidacją sprawuje Informatyk lub osoba wyznaczona przez Administratora Bezpieczeństwa Informacji.

ROZDZIAŁ X
Kontrola użytkowników systemów komputerowych

§ 59

1. Wyłączne uprawnienia do instalowania, wymiany uszkodzonych urządzeń oraz ich likwidacji posiada Informatyk lub osoba wyznaczona przez Administratora Bezpieczeństwa Informacji.
2. *Do przetwarzania danych osobowych mogą być wykorzystywane wyłącznie* komputery służbowe.
3. Informatyk umożliwia pracownikom korzystanie z sieci internet w celu wykonywania zadań służbowych .
4. Korzystanie z sieci internet w innym celu jest zabronione.
5. Pracownik ds. obsługi informatycznej monitoruje i rejestruje odwiedzane przez poszczególnych pracowników strony internetowe.
6. W przypadku stwierdzenia naruszenia zakazu, o którym mowa w ust. 4. Informatyk informuje bezpośredniego przełożonego użytkownika.

§ 60

Zakres dostępu poszczególnych pracowników do zasobów informatycznych (poszczególnych programów) określa pracownik Informatyk za zgodą bezpośredniego przełożonego.

ROZDZIAŁ XI
Postanowienia końcowe

§ 61

1. Użytkownik zobowiązany jest złożyć oświadczenie, o tym, iż został zaznajomiony z przepisami ustawy o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych oraz dokumentacją

obowiązującą u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania.

2. Wzór oświadczenia potwierdzającego zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych oraz dokumentacją obowiązującą u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania , stanowi załącznik nr 4 do Instrukcji.
3. Oświadczenia przechowywane są w aktach osobowych pracownika.

Załącznik nr 1 do instrukcji zarządzania
Systemem informatycznym

Krzysztof Nyga

Krasocin , dnia 28.01.2013

UPOWAŻNIENIE

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (t. j. Dz. U. z 2002r. Nr 101, poz. 926 ze zm.), upoważniam Panią*/Pana* do przetwarzania danych osobowych.

Upoważnienie obejmuje prawo wglądu, wprowadzania, modyfikowania i usuwania danych osobowych.

Zobowiązuje Panią*/Pana* do przestrzegania przepisów dotyczących ochrony danych osobowych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Danych polityki bezpieczeństwa danych osobowych oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

.....

(podpis Administratora Danych)

*- niepotrzebne skreślić

Załącznik nr 3 do instrukcji zarządzania systemem informatycznym

CZĘSTOTLIWOŚĆ TWORZENIA KOPII ZAPASOWYCH

Ustala się następującą częstotliwość tworzenia kopii awaryjnych na nośnikach zewnętrznych – magnetycznych i optycznych:

1. Kopie dobowe i tygodniowe, wykonywane przez Informatyka lub użytkowników obejmujące:
   a. serwery danych,
   b. dział finansowy.
2. Kopie miesięczne, umieszczone w zapieczętowanych kopertach, deponowane przez Informatyka w miejscu określonym w § 29 instrukcji obejmujące:
   a. serwer danych,
   b. dział finansowy,
   c. stacje robocze.
3. Kopie tygodniowe przechowywane są do czasu zdeponowania kopii miesięcznych.
4. Niszczenie kopii awaryjnych należy wykonywać w sposób określony w Instrukcji.
5. W sytuacjach awaryjnych zaistniałych pod nieobecność Informatyka lub w razie jego niedyspozycji Wójt udostępnia kopie awaryjne osobie przez siebie wyznaczonej.

.....

(podpis Administratora Danych)

Załącznik nr 2 do instrukcji zarządzania systemem informatycznym

TRYB PRZECHOWYWANIA I UDOSTĘPNIANIA HASEŁ INFORMATYKA

Ustala się następujący tryb postępowania z hasłami Informatyka:

1. Hasła Informatyka przechowywane są w formie pisemnej w zabezpieczonej kopercie.
2. Koperta złożona jest w specjalnej szafie, do której dostęp posiada Wójt i osoby przez niego upoważnione.
3. Hasła, o którym mowa w pkt 1 dają najwyższe uprawnienia administratorskie do korzystania i obsługi systemu informatycznego.
4. Hasła zmieniane są co najmniej co 30 dni bądź natychmiast w przypadku podejrzenia odkrycia przez inną , nieupoważniona osobę.
5. Nowe, aktualne hasło zabezpiecza się według procedur opisanych w pkt 1 i 2.
6. Koperta wraz z hasłem, które straciło ważność podlega zniszczeniu przy użyciu niszczarki dokumentów.
7. Niszczenia, o których mowa w pkt 6 dokonuje Informatyk w obecności Wójta lub osoby przez niego upoważnionej.
8. W sytuacjach awaryjnych zaistniałych pod nieobecność Informatyka lub w razie jego niedyspozycji Wójt udostępnia hasło osobie przez siebie upoważnionej.

.....

(podpis Administratora Danych)

Załącznik nr 4 do instrukcji zarządzania systemem informatycznym

.....
.....

(imię i nazwisko) *(miejscowość, data)*

OŚWIADCZENIE

Oświadczam, iż zostałam*/zostałem* zaznajomiona*/zaznajomiony* z przepisami dotyczącymi ochrony danych osobowych, w szczególności ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (t. j. Dz. U. z 2002r. Nr 101, poz. 926 ze zm.), wydanych na jej podstawie aktów wykonawczych oraz wprowadzonymi i wdrożonymi do stosowania przez Administratora Danych Polityka bezpieczeństwa danych osobowych oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Jednocześnie zobowiązuję się do ich przestrzegania.

.....

(podpis osoby składającej oświadczenie)

*- niepotrzebne skreślić