Załącznik Nr 2 do zarządzenia Nr 20/17
Wójta Gminy Nowinka
z dnia 10 marca 2017 r.

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

16-304, NOWINKA 33

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

Rozdział 1

Postanowienia ogólne

§1.

Instrukcja reguluje zasady zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Nowinka.

§2.

Przetwarzanie danych osobowych w Urzędzie Gminy Nowinka odbywa się na zasadach określonych w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. Nr 101, poz. 926, z 2002 r.).

§3.

Celem wprowadzenia niniejszej instrukcji jest ochrona danych osobowych zawartych w systemach informatycznych eksploatowanych w lokalnych sieciach komputerowych Urzędu. Instrukcja ta, zawiera w szczególności:

1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności,
2) stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem,
3) procedury rozpoczęcia, zawieszenia i zakończenia pracy oraz postępowania w przypadku zaniku napięcia dla użytkowników systemu,
4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania,
5) sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe i kopii zapasowych zbiorów danych,
6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,
7) sposób realizacji wymogu odnotowania informacji o odbiorcach, którym dane osobowe zostały udostępnione,
8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Rozdział 2
Objaśnienia

§4.

Przez użyte w instrukcji określenia należy rozumieć:

1) **dane osobowe** - wszelkie informacje o określonej lub dającej się określić osobie fizycznej,
2) **zbiór danych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
3) **Administrator Danych** - rozumie się przez to organ samorządu terytorialnego, decydujący o celach i środkach przetwarzania danych osobowych,
4) **przetwarzanie danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, zarówno w systemach informatycznych jak i metodami tradycyjnymi(kartoteki, księgi, wykazy),
5) **system informatyczny** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
6) **Administrator Systemu Informatycznego** - pracownik wyznaczony przez Wójta Gminy, posiadający uprawnienia administratora lub super użytkownika konkretnego systemu bazodanowego. Jest on odpowiedzialny za sprawność i konserwację oraz wdrożenie technicznych zabezpieczeń systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie, w przypadku umów serwisowych Administratorem Systemu Informatycznego może być też przedstawiciel firmy obsługującej program / system komputerowy,
7) **użytkownik systemu informatycznego** - pracownik Urzędu posiadający odpowiednie upoważnienia,
8) **Urząd** - Urząd Gminy Nowinka.
9) **kierownik komórki organizacyjnej** – Zastępca Wójta Gminy / Sekretarz Gminy / Skarbnik / Kierownik jednostki organizacyjnej, w którym zatrudniony jest pracownik przetwarzający dane osobowe,
10) **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 w Rzeczypospolitej Polskiej, podmiotu mającego siedzibę albo miejsce zamieszkania w państwie trzecim,
    d) podmiotu mającego zawartą umowę na piśmie, w zakresie i celu przewidzianym w umowie,
    e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,
    f) państwie trzecim - rozumie się przez to państwo nie należące do Europejskiego Obszaru Gospodarczego,
11) **Administrator Bezpieczeństwa Informacji** - pracownik wyznaczony przez Wójta Gminy. Jest on odpowiedzialny za bezpieczeństwo danych osobowych gromadzonych i przetwarzanych w systemach informatycznych Urzędu. Do jego obowiązków należy w szczególności:
    - prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych.
    - przeprowadzanie okresowych kontroli poprawności funkcjonowania zabezpieczeń systemów informatycznych,

- podejmowanie stosownych działań zgodnie z niniejszą instrukcją w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczeń systemu informatycznego.

12) **identyfikator użytkownika** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
13) **hasło** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
14) **karta mikroprocesorowa** - indywidualne karty, bez których obsługa konta w systemie operacyjnym i zalogowanie się jest niemożliwe,
15) **BIOS** - jest to program znajdujący się na stałe w komputerze, który jest uruchamiany jako pierwszy po włączeniu komputera,
16) **uwierzytelnianie** - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości użytkownika,
17) **UPS** - zasilacz awaryjny podtrzymujący pracę komputera po zaniku napięcia zasilającego,
18) **sieć LAN** - lokalna sieć komputerowa,
19) **sieć publiczna** - rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z późniejszymi zmianami z 2004 r.).

Rozdział 3
Obowiązki pracownicze wynikające z ochrony danych osobowych

§5.

1. Obowiązek przestrzegania tajemnicy danych osobowych dotyczy wszystkich pracowników, którzy mają dostęp do informacji o charakterze danych osobowych.
2. Naruszenie zasad ochrony danych osobowych, w efekcie którego nastąpiło udostępnienie danych osobie nie upoważnionej, jest ciężkim naruszeniem obowiązków pracowniczych.
3. Kierownicy komórek organizacyjnych Urzędu są zobowiązani do:
   a) zastosowania niezbędnych środków technicznych i organizacyjnych, określonych w przepisach powszechnie obowiązujących w celu zapewnienia ochrony przetwarzania danych osobowych,
   b) kontroli przestrzegania zasad i sposobu wykonywania operacji przetwarzania danych przez podległych pracowników,
   c) sygnalizowania niezgodności aktów prawnych oraz aktów wewnętrznych Urzędu z przepisami ustawowymi w zakresie ochrony danych osobowych i przedstawienia stosownych projektów zmian, mających na celu ich dostosowanie do regulacji ustawowej.
4. Czynności przetwarzania danych osobowych może dokonywać jedynie pracownik upoważniony przez Administratora Danych, w zakresie indywidualnych obowiązków pracowniczych.
5. Osoba upoważniona przez Administratora Danych osobowych, jest zobowiązana do:
   a) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych,
   b) stosowania określonych przez administratora procedur i środków, mających na celu zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym,
   c) zachowania szczególnej staranności w trakcie wykonywania operacji przetwarzania danych w celu ochrony interesów osób. których dane dotyczą,

   d) podporządkowanie się poleceniom kierownika komórki organizacyjnej i przestrzegania ustalonych przez niego szczegółowych zasad i procedur.

Rozdział 4

Postępowanie przy upoważnianiu osób do przetwarzania danych osobowych

§6.

1. W przypadku przyjęcia do pracy nowego pracownika, którego zakres obowiązków obejmować będzie przetwarzanie danych osobowych, kierownik komórki organizacyjnej obowiązany jest skierować wniosek do Administratora Bezpieczeństwa Informacji o przygotowanie upoważnienia do przetwarzania danych osobowych, którego treść stanowi załącznik nr 4 do Polityki Bezpieczeństwa Informacji.
2. Pracownik, któremu administrator danych osobowych udzieli upoważnienia, jest zobowiązany do podpisania oświadczenia, którego treść stanowi załącznik nr 5 do Polityki Bezpieczeństwa Informacji.
3. Przepisy ustępu 1, 2, 4, 5 i 6 stosuje się odpowiednio do stażystów odbywających staż w Urzędzie.
4. W przypadku zmiany stanowiska, bądź zakresu obowiązków pracowniczych, kierownik komórki organizacyjnej obowiązany jest bezzwłocznie skierować wniosek o aktualizację bądź cofnięcie upoważnienia do przetwarzania danych osobowych do Administratora Bezpieczeństwa Informacji, którego treść stanowi załącznik nr 1.
5. Wypowiedzenie umowy o pracę przez pracodawcę jest równocześnie cofnięciem upoważnienia administratora do przetwarzania danych.
6. W sytuacji wypowiedzenia umowy o pracę przez pracownika, upoważnienie traci moc z datą rozwiązania umowy o pracę.
7. W przypadku zmiany wzoru upoważnienia, nowe upoważnienie obowiązuje od daty nadania, poprzednie traci moc z datą przyjęcia nowego.
8. Upoważnienie obowiązuje aż do momentu nadania nowego, jego odwołania lub wygaśnięcia
9. Ewidencję pracowników, upoważnionych do przetwarzania danych prowadzi Administrator Bezpieczeństwa Informacji.

Rozdział 5

Postępowanie w przypadku naruszenia zbioru danych osobowych

§7.

1. Za kontrolę, przeglądy i nadzór nad konserwacją systemów służących do przetwarzania danych osobowych odpowiedzialny jest Administrator Bezpieczeństwa Informacji, a w szczególności:
   - na wniosek Administratora Danych dokonuje kontroli oraz oceny stanu bezpieczeństwa danych osobowych,
   - dokonuje kontroli systemu informatycznego po uzyskaniu informacji o próbie nieautoryzowanego dostępu, wystąpieniu zagrożenia wirusem komputerowym lub innym złośliwym programem,
2. W przypadku uzasadnionego podejrzenia naruszenia zasad ochrony danych osobowych w Urzędzie, pracownik zobowiązany jest do niezwłocznego poinformowania o tym kierownika komórki organizacyjnej.
3. Kierownik komórki organizacyjnej, po dokonaniu oceny stanu faktycznego i stwierdzeniu naruszenia, jest zobowiązany poinformować o tym fakcie Administratora Bezpieczeństwa Informacji.
4. W przypadku powtarzającego się naruszenia zasad ochrony danych osobowych, pracownik jest zobowiązany do niezwłocznego poinformowania o tym fakcie Administratora Bezpieczeństwa Informacji.

5. Osobą odpowiedzialną za bezpieczeństwo danych osobowych w systemie informatycznym jest Administrator Bezpieczeństwa Informacji, którego zadaniem jest w szczególności przeciwdziałanie dostępowi osób nieupoważnionych do systemu, w którym przetwarzane są dane osobowe oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.

Rozdział 6

Ogólne zasady eksploatacji systemów komputerowych i systemów przetwarzania danych osobowych

§8.

1. W obszarze przetwarzania danych osobowych mogą przebywać wyłącznie pracownicy zatrudnieni przy przetwarzaniu danych, osoby których dane dotyczą. Administrator Systemu oraz inne osoby indywidualnie upoważnione przez Wójta Gminy.
2. Pomieszczenia w obszarze przetwarzania danych osobowych muszą być zamykane na zamek w czasie nieobecności pracowników.
3. Monitory komputerów na których odbywa się przetwarzanie danych osobowych muszą być zlokalizowane w sposób uniemożliwiający wgląd osobom trzecim.
4. Ekrany monitorów komputerów na których odbywa się przetwarzanie danych osobowych muszą być automatycznie wyłączane po upływie 10 minut nieaktywności użytkownika.
5. Dyski i taśmy magnetyczne zawierające dane osobowe, a przeznaczone do likwidacji, naprawy lub przekazania podmiotowi nieuprawnionemu do otrzymania danych, przed oddaniem są pozbawiane zapisu.
6. Wydruki komputerowe zawierające dane osobowe, a przeznaczone do likwidacji, są w ciągu dnia gromadzone na stanowiskach pracy i na koniec dnia niszczone w niszczarce dokumentów.
7. Zabronione jest wykorzystywanie systemów informatycznych do celów niezgodnych z przeznaczeniem, a w szczególności instalowania gier oraz oprogramowania innego niż niezbędne do realizacji przetwarzania danych i/lub realizacji innych zadań służbowych oraz instalowania oprogramowania przez osoby do tego nieuprawnione i bez wiedzy Administratora Bezpieczeństwa Informacji.
8. Zabronione jest wykonywanie kopii danych osobowych oraz wydruków danych osobowych w celach innych niż wynikające z zasad przetwarzania danych, archiwizacji i/lub przekazanie danych podmiotowi uprawnionemu.
9. Nośniki danych zawierające dane osobowe muszą być przechowywane w zamkniętych szafach.

Rozdział 7

Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

§9.

1. Nadawanie uprawnień do przetwarzania danych osobowych i rejestrowanie uprawnień w systemie informatycznym odbywa się na wniosek pisemny kierownika komórki organizacyjnej.
2. Osobą odpowiedzialną za przyznanie identyfikatora i hasła jest Administrator Systemu Informatycznego. Działa on za zgodą Administratora Bezpieczeństwa Informacji.

3. Każdemu z użytkowników systemu informatycznego ustala się identyfikator i hasło dostępu jak również uprawnienia do poszczególnych funkcji systemu określone według zakresu obowiązków pracownika. Odpowiada za to Administrator Systemu Informatycznego.
4. Hasło dostępu zmienia się raz na miesiąc.
5. Użytkownik zmienia hasło w przypadku kompromitacji hasła.
6. Użytkownicy zobowiązani są do utrzymania w tajemnicy haseł dostępu, również po upływie ich ważności.
7. Przy stwierdzeniu próby włamania do systemu lub podejrzeniu o kompromitację hasła. Administrator Systemu Informatycznego blokuje konto i powiadamia Administratora Bezpieczeństwa Informacji.
8. W przypadku rozwiązania lub ustania stosunku pracy konto powinno być zablokowane w systemie informatycznym. Odpowiada za to Administrator Systemu Informatycznego. Fakt ten musi być odnotowany w ewidencji osób przetwarzających dane osobowe.

§ 10.

W przypadku gdy użytkownik systemu informatycznego zmienił stanowisko pracy stosuje się zasady z §9.

Rozdział 8

Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

§ 11.

1. Przydziału identyfikatora i hasła dokonuje osobiście Administrator Systemu Informatycznego.
2. Użytkownik przy pierwszym dostępie do systemu jest zobowiązany do zmiany hasła.
3. Hasło musi składać się z co najmniej 6 znaków, a w przypadku przetwarzania danych na poziomie podwyższonym i wysokim z minimum 8 znaków oraz zawierać małe i wielkie litery oraz cyfry i znaki specjalne.
4. Hasła są przechowywane w systemach bazodanowych w postaci zaszyfrowanej.
5. Konto użytkownika jest blokowane w przypadku trzech nieudanych prób dostępu.
6. Hasło nie może być zapisywane lub przechowywane w miejscu dostępnym dla osób niepowołanych.

Rozdział 9

Procedury rozpoczęcia, zawieszenia i zakończenia pracy oraz postępowania w przypadku zaniku napięcia dla użytkowników systemu

§ 12.

1. Przed rozpoczęciem pracy użytkownik zobowiązany jest do sprawdzenia stanu stacji komputerowej. W szczególności uszkodzeń lub ingerencji osób trzecich.
2. Rozpoczynając pracę na komputerze użytkownik wprowadza wszystkie wymagane identyfikatory i hasła w sposób uniemożliwiający ich ujawnienie innym osobom.
3. W przypadku niemożliwości dostępu do systemu informatycznego z powodu zablokowania konta poprzez nieudane próby dostępu użytkownik powiadamia o tym fakcie Administratora Bezpieczeństwa Informacji.

4. W przypadku dłuższej przerwy w korzystaniu z systemu użytkownik obowiązany jest zawiesić pracę w systemie poprzez zaktywizowanie wygaszacza ekranu zabezpieczonego hasłem, wyrejestrować się z systemu informatycznego lub w inny sposób zablokować stację roboczą .
5. W przypadku braku aktywności użytkownika w systemie informatycznym trwającej dłużej niż 10 minut automatycznie włącza się wygaszacz ekranu. Ponowny dostęp do systemu następuje po poprawnym podaniu hasła.
6. Po zakończeniu pracy użytkownik powinien, prawidłowo wylogować się z systemu, wyłączyć komputer oraz UPS.
7. W przypadku zaniku napięcia, które ma charakter trwały, użytkownik powinien:
   a) jeśli otrzymał komunikat z serwera, o braku napięcia, wyłączeniu serwera po określonym czasie, natychmiast zapisać dane, wylogować się z systemu informatycznego i bezpiecznie wyłączyć komputer,
   b) jeśli nie otrzymał komunikatu lub nie korzysta z sieci LAN powinien zapisać dane i bezpiecznie wyłączyć komputer.
8. Ponowna praca jest możliwa po przywróceniu napięcia w sieci energetycznej.
9. W przypadku serii krótkich zaników napięcia (sygnalizowane dźwiękiem przez zasilacz awaryjny lub komunikatami na ekranie monitora) należy zakończyć pracę oraz powiadomić Administratora Bezpieczeństwa Informacji o niestabilności sieci energetycznej oraz powiadomić Informatyka , który określi czy UPS jest sprawny.
10. Ustawienie monitora powinno uniemożliwiać podgląd osobom nieuprawnionym szczególnie w procesie obsługi klienta.
11. Wydruki po wykorzystaniu niszczy się w niszczarkach dokumentów.
12. Pomieszczenia, w których są przetwarzane dane osobowe zamyka się na czas nieobecności osób zatrudnionych przy przetwarzaniu danych osobowych.
13. Osoby nieuprawnione mogą przebywać w pomieszczeniach, w których są przetwarzane dane osobowe tylko w obecności osoby uprawnionej.
14. Zabrania się pod rygorem odpowiedzialności służbowej i karnej:
   a) ujawniania danych osobowych,
   b) kopiowania bazy danych lub jej części poza przewidzianymi kopiami bezpieczeństwa,
   c) przetwarzania danych w sposób inny niż opisany instrukcją,
   d) instalacji nielegalnego oprogramowania mogącego naruszyć bezpieczeństwo danych osobowych.

Rozdział 10

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

§ 13.

1. Kopie bezpieczeństwa wykonywane są nie rzadziej niż raz na dwa tygodnie na dowolnym nośniku.
2. Raz na kwartał są wykonywane kopie zapasowe na nośnikach jednorazowego zapisu.
3. Prowadzona jest ewidencja wykonywania kopii bezpieczeństwa i kopii zapasowych, wszystkie nośniki są opisane.
4. Tworzone są kopie bezpieczeństwa nowych i aktualizowanych programów oraz narzędzi programistycznych do przetwarzania zbiorów danych. Przechowuje się je w szafie pancernej.
5. Kopiowanie danych osobowych na nośniki informacji oraz robienie wydruków jest zabronione, chyba że istnieje konieczność ich sporządzania, która wynika z nałożonych na użytkownika obowiązków i dozwolona jest przepisami prawa.
6. Wykorzystywanie nośników informacji lub wydruków w celu innym niż wskazany jest zabronione.

Rozdział 11

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe i kopii zapasowych zbiorów danych

§ 14.

1. Elektroniczne nośniki danych i kopie bezpieczeństwa przechowuje się poza miejscem przetwarzania danych osobowych w szafie pancernej w zabezpieczonych pudełkach lub innym opakowaniu, które chroni przed kurzem i wilgocią.
2. Dostęp do nośników zawierających dane osobowe jest zabezpieczony poprzez:
   a) system alarmowy,
   b) szafę pancerną.
3. Szczegółowe zabezpieczenia pomieszczeń zawarte są w §5 „Polityki bezpieczeństwa Urzędu Gminy Nowinka".
4. Kopie dwutygodniowe są przechowywane przez okres miesiąca.
5. Kopie kwartalne są przechowywane przez okres 5 lat.
6. Kopie bezpieczeństwa, które uległy uszkodzeniu lub stały się niepotrzebne pozbawia się zapisu danych, a w przypadku gdy nie jest to możliwe, niszczy fizycznie w stopniu uniemożliwiającym ich odczytanie.
7. Uszkodzone nośniki magnetyczne przed ich wyrzuceniem należy fizycznie zniszczyć (przeciąć, przełamać zarysować itp.).

Rozdział 12

Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

§ 15.

1. Na każdej stacji komputerowej na której przetwarzane są dane osobowe stosuje się aktywna ochronę antywirusową działającą w czasie rzeczywistym.
2. Aktualizacja programu antywirusowego przeprowadzana jest codziennie, automatycznie bez udziału użytkownika.
3. Pełne sprawdzenie systemu operacyjnego odbywa się raz w tygodniu.
4. Wszystkie zewnętrzne nośniki danych, których zawartość jest wczytywana do komputera muszą być każdorazowo sprawdzane programem antywirusowym. Odpowiedzialnym za te czynności jest pracownik obsługujący komputer.
5. Każdy użytkownik w przypadku stwierdzenia wystąpienia komunikatu ostrzegającego lub podejrzenia działalności wirusa komputerowego lub szkodliwego oprogramowania ma obowiązek zgłosić ten fakt Administratorowi Bezpieczeństwa Informacji.
6. W przypadku naruszenia bezpieczeństwa danych użytkownik jest zobowiązany zgłosić ten fakt Administratorowi Bezpieczeństwa Informacji.
7. Do obowiązków Administratora Bezpieczeństwa Informacji należy okresowe sprawdzenie funkcjonowania i aktualność programu antywirusowego na wszystkich stacjach komputerowych przetwarzających dane osobowe.

Rozdział 13

Sposób realizacji wymogu odnotowania informacji o odbiorcach, którym dane osobowe zostały udostępnione

§16.

1. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.
2. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym należy odnotować w systemie informacje o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych.

Rozdział 14

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

§17.

1. Prace dotyczące przeglądów, konserwacji i napraw wymagające zaangażowania autoryzowanych firm zewnętrznych, są wykonywane pod nadzorem Administratora Systemu Informatycznego, bez możliwości dostępu do danych osobowych.
2. Urządzenia komputerowe, dyski twarde lub inne informatyczne nośniki danych, przeznaczone do naprawy, pozbawia się przed naprawą zapisu danych osobowych w sposób trwały lub naprawia się je pod nadzorem Administratora Systemu Informatycznego lub osoby przez niego upoważnionej.
3. Okresową weryfikację kopii bezpieczeństwa pod kontem ich przydatności do odtworzenia danych przeprowadza Administrator Systemu Informatycznego.
4. Nośniki informacji przekazywane na zewnątrz powinny być pozbawione zapisów zawierających dane osobowe. Niszczenie zapisów odbywa się poprzez usuniecie danych i formatowanie nośnika.

Rozdział 15

Zasady postępowania z komputerami przenośnymi

§18.

Komputery przenośne, używane do przetwarzania danych osobowych, powinny być zabezpieczone podczas transportu oraz użytkowania przed dostępem do tych danych osób nieuprawnionych, w szczególności należy:

a) zabezpieczyć dostęp do komputera hasłem na poziomie BIOS,
b) zabezpieczyć dostęp do systemu - operacyjnego poprzez obligatoryjne wprowadzenie nazwy użytkownika i hasła,
c) nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych,
d) nie przechowywać lokalnie zbiorów z danymi osobowymi - możliwa tylko praca zdalna w systemie przetwarzania danych osobowych.

Rozdział 16

Przepisy końcowe

§ 19.

1. Niniejsza instrukcja przeznaczona jest dla użytkowników systemu informatycznego i ich przełożonych, którzy nadzorują przetwarzanie danych osobowych.
2. Wykonanie postanowień instrukcji ma na celu ujednolicenie zarządzania systemem informatycznym w Urzędzie Gminy Nowinka.
3. Wszelkie zmiany Instrukcji mogą być wprowadzane tylko na podstawie zarządzeń Administratora Danych.
4. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne.
5. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym Administratora Bezpieczeństwa Informacji.
6. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia Administratora Bezpieczeństwa Informacji nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. Nr 101, poz. 926 z 2002 r.) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
7. W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. Nr 101, poz. 926 z 2002 r.), rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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 z 2004 r.) oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 roku w sprawie sposobu technicznego przygotowania systemów i sieci do przekazywania informacji - do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych (Dz. U. Nr 100, poz. 1023 z 2004 r.).

WÓJT
mgr Dorota Winiewicz