ZARZĄDZENIE NR 631/2023
WÓJTA GMINY INOWROCŁAW

z dnia 29 maja 2023 r.

w sprawie wprowadzenia Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Gminy Inowrocław

Na podstawie § 20 ust. 1 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 r., poz. 2247), art. 24 i art. 32 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119) oraz ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz.U. z 2019 r., poz. 1781), zarządzam co następuje:

§ 1. Wprowadzam Instrukcję Zarządzania Systemem Informatycznym Służącym do przetwarzania danych w Urzędzie Gminy Inowrocław w brzmieniu określonym w załączniku do zarządzenia.

§ 2. Zobowiązuję wszystkich pracowników Urzędu Gminy w Inowrocławiu do zapoznania się z treścią niniejszego zarządzenia wraz z załącznikiem.

§ 3. Traci moc Zarządzenie Nr 105/2015 Wójta Gminy Inowrocław z dnia 23 września 2015 roku.

§ 4. Nadzór nad wykonaniem niniejszego zarządzenia sprawuje Sekretarz Gminy Inowrocław.

§ 5. Zarządzenie wchodzi w życie z dniem podpisania.

Wójt Gminy Inowrocław

Tadeusz Kacprzak

Załącznik do zarządzenia Nr 631/2023

Wójta Gminy Inowrocław

z dnia 29 maja 2023 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

SPIS TREŚCI

CZĘŚĆ I.

Postanowienia ogólne

1. Niniejsza "Instrukcja" ma zastosowanie do przetwarzania danych osobowych znajdujących się (bądź mogących się znaleźć) w następujących zbiorach prowadzonych w Urzędzie Gminy Inowrocław:

a) BUDŻET - Księgowość budżetowa z planowaniem;

b) PODATKI - System wymiaru podatków lokalnych od osób fizycznych;

c) KSZOB - System księgowości podatków i opłat;

d) PŁACE - System kadrowo – placowy;

e) JGU - System wymiaru podatków lokalnych od osób prawnych;

f) AUTA - System wymiaru podatku od środków transportowych;

g) MATER - Prowadzenie ewidencji materiałów;

h) Opłaty lokalne - System wymiaru i księgowania opłat lokalnych od osób fizycznych;

i) Czynsze - System wymiaru opłat czynszowych od osób fizycznych i prawnych;

j) Ewidencja Ludności - System Ewidencji Ludności Urzędu Gminy Inowrocław;

k) Dodatki mieszkaniowe oraz energetyczno, elektryczne;

l) Płatnik - program umożliwiający wysyłanie dokumentów ubezpieczeniowych do Zakładu Ubezpieczeń Społecznych w formie elektronicznej przez osoby i firmy, na których ciąży taki obowiązek.

m) wszystkie edytory tekstu oraz programy umożliwiające zapisywanie danych osobowych w formie elektronicznej, w tym skanów, zdjęć dokumentów.

2. "Instrukcja" określa zasady i tryb postępowania Administratora Danych Osobowych i osób przez niego zatrudnionych przy przetwarzaniu danych osobowych w systemie informatycznym Urzędu Gminy Inowrocław.

4. Następujące pojęcia użyte w niniejszej "Instrukcji" oznaczają:

1) Administrator danych osobowych (ADO) - organ, jednostka organizacyjna, podmiot lub osoba, decydujące o celach i środkach przetwarzania danych osobowych;

2) Zbiór danych - każdy posiadający strukturę zestaw danych o charakterze osobowym dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

3) System informatyczny - zespól współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

4) Zabezpieczenie danych w systemie informatycznym - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

5) Naruszenie bezpieczeństwa informacji - wszelkie zdarzenia lub działania, w tym również niezamierzone, które mogą stanowić przyczynę utraty zasobów, zmian poufności, integralności, dostępności informacji lub niezawodności systemów, a także odstępstwa od obowiązujących procedur postępowania, nawet, jeżeli nie prowadzą do wyżej wymienionych skutków;

6) Dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań;

7) Administrator bezpieczeństwa informacji (ABI) - osoba wyznaczona przez Administratora Danych Osobowych spośród pracowników Urzędu Gminy Inowrocław w celu sprawowania nadzoru nad przestrzeganiem zasad ochrony przetwarzanych danych osobowych, zarówno w kontekście operacji na danych wykonywanych w systemie informatycznym, jak też metodami tradycyjnymi ("papierowym"), a w szczególności nadzoru nad zabezpieczeniem danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;

8) Administrator systemu informatycznego (ASI) - osoba (podmiot, komórka organizacyjna) odpowiedzialna(y) za prawidłowe funkcjonowanie systemu informatycznego;

9) W Urzędzie Gminy Inowrocław rola administratorów systemu informatycznego jest podzielona na Administrator systemu informatycznych wewnętrznych - ASIW, stanowisko ds. IT oraz Administrator systemów informatycznego- zewnętrznych - ASIZ działających na podstawie stosownych umów;

10) Użytkownik systemu lub osoba upoważniona - osoba dopuszczona do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych w zbiorach (lub w jednym z tych zbiorów), o których mowa w punkcie l, posiadająca aktualne imienne upoważnienie wydane przez Administratora Danych Osobowych;

11) Osoba trzecia - każda osoba nieupoważniona i nieuprawniona do dostępu do danych osobowych lub zbiorów tych danych. Osobą trzecią jest ponadto osoba posiadająca upoważnienie wydane przez Administratora Danych Osobowych, podejmująca czynności wykraczające poza zakres uprawnień udzielonych jej przez ADO.

CZĘŚĆ II.

Określenie miejsca przetwarzania danych w systemie informatycznym.

Obszar przetwarzania danych stanowią pomieszczenia Urzędu Gminy Inowrocław znajdujące się w trzykondygnacyjnym biurowcu Urzędu Gminy Inowrocław, zlokalizowanym w Inowrocławiu przy ul. Królowej Jadwigi 43.

CZĘŚĆ III.

Określenie środków technicznych, aplikacji i innych zasobów wchodzących w skład systemu informatycznego.

W skład systemu informatycznego Urzędu Gminy Inowrocław wchodzą komputery stacjonarne i urządzenia peryferyjne tworzące lokalną sieć informatyczną (LAN).

Opis systemu informatycznego Urzędu Gminy Inowrocław zawiera załącznik nr 1 do niniejszej instrukcji.

CZĘŚĆ IV.

Zastosowany poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym.

W Urzędzie Gminy Inowrocław zastosowano poziom wysoki bezpieczeństwa przetwarzania danych, gdyż przynajmniej jedno urządzenie systemu informatycznego Urzędu, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną.

CZĘŚĆ V.

Zasady zarządzania systemem informatycznym.

Bieżące zarządzanie systemem informatycznym należy do obowiązków Administratora Systemu Informatycznego wewnętrznego (ASIW). Do podstawowych obowiązków ASIW należy:

1) Wdrażanie procedur warunkujących bezpieczeństwu systemów Urzędzie Gminy Inowrocław;

2) Nadzór nad wykorzystywaniem uprawnień nadanych użytkownikom przez ASIZ;

3) Konsultacje i instruktaże dla użytkowników systemów informatycznych Urzędu Gminy Inowrocław;

4) Konfigurowanie urządzeń i oprogramowania;

5) Monitorowanie zmian w systemie;

6) Wykonywanie kopii bezpieczeństwa danych i oprogramowania;

7) Informowanie Wójta Gminy Inowrocław (ADO), ABI oraz ASIZ o istotnych zdarzeniach związanych z bezpieczeństwem systemu informatycznego Urzędu Gminy Inowrocław;

Do obowiązków Administratora Systemu Informatycznego zewnętrznego (ASIZ) należą zadania wymiennie w stosownych umowach i porozumieniach:

1) Rejestracja użytkowników systemu informatycznego;

2) Przeglądanie plików zawierających informacje o wybranych zdarzeniach w systemie;

3) Konsultacje i instruktaże dla użytkowników systemów informatycznych Urzędu Gminy Inowrocław;

4) Aktualizacje oprogramowania.

CZĘŚĆ VI.

Zasady kontroli dostępu do systemu informatycznego Urzędu Gminy Inowrocław.

1. Generalne założenia wdrożonej w Urzędzie Gminy Inowrocław polityki kontroli dostępu do systemów informatycznych uwzględniają:

l) wymagania bezpieczeństwa pojedynczych aplikacji;

2) przyznawanie uprawnień użytkownikom zgodnie z zasadą wiedzy uzasadnionej;

3) zmiany w uprawnieniach użytkowników systemu informatycznego uzależnione są od decyzji właściwego kierownika komórki organizacyjnej;

2. W zakresie kontroli dostępu użytkowników do systemów obowiązują następujące uwarunkowania:

l) w aspekcie organizacyjno - prawnym:

a) Użytkownik musi posiadać ważne dopuszczenie do pracy w systemie informatycznym wydane przez ADO;

b) Użytkownik musi posiadać konto nadane mu przez ASIZ;

c) Użytkownik obowiązany jest przestrzegać procedur stosowania i zmian haseł;

d) ASIW nadzoruje wykorzystywanie kont przez użytkowników systemu;

2) W aspekcie technicznym:

a) System musi posiadać mechanizmy uwierzytelniania i kontroli dostępu;

b) ASIZ dokonuje właściwej konfiguracji mechanizmów uwierzytelnienia i kontroli dostępu oraz sprawuje systematyczny nadzór nad prawidłową eksploatacją tych mechanizmów;

3) w aspekcie fizycznym - urządzenia systemu informatycznego umieszczone są w strefach administracyjnych.

CZĘŚĆ VII.

Zarządzanie dostępem użytkowników do systemu

1. Opracowano formalne procedury kontroli przyznawania praw dostępu do systemów informatycznych Urzędu Gminy Inowrocław.

2. Procedury obejmują wszystkie etapy dostępu użytkowników - od ich początkowej rejestracji do końcowego wyrejestrowania tych, którym nie przysługuje już dostęp do systemów i usług informacyjnych.

3. Stosowne czynności w tych zakresach wykonuje ASIZ, ASIW.

CZĘŚĆ VIII.

Procedury przydzielania użytkownikowi praw dostępu do systemów

Przyznawanie lub wycofywanie uprawnień dostępu do systemów informatycznych jest oparte na formalnej procedurze rejestrowania i wyrejestrowywania użytkowników obejmującej:

1. Przyznanie każdemu użytkownikowi systemu informatycznego unikatowego identyfikatora, aby można było przypisać poszczególnym użytkownikom określone działania oraz odpowiedzialność za te działania;

2. Sprawdzenie, czy użytkownik ma przyznane przez ADO uprawnienia do korzystania z systemu informatycznego lub usługi;

3. Sprawdzenie, czy przyznany poziom dostępu jest odpowiedni dla potrzeb służbowych oraz czy jest zgodny z "Polityką bezpieczeństwa" ;

4. Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych w referacie kadr i archiwum;

5. Natychmiastowe odebranie praw dostępu użytkownikom, z którymi wygasi stosunek zatrudnienia w Urzędzie Gminy Inowrocław;

6. Zakaz ponownego użycia wykorzystanych wcześniej identyfikatorów w celu przyznania ich innym użytkownikom.

Algorytm postępowania w procedurze:

1. Wójt Gminy Inowrocław nadaje określonej osobie uprawnienia użytkownika systemu informatycznego lub zmienia/ wycofuje uprzednio nadane uprawnienia, poprzez zatwierdzenie formularza upoważnienia. Zakres nadawanych uprawnień musi być uzasadniony charakterem obowiązków służbowych potencjalnego użytkownika systemu;

2. Formularz upoważnienia sporządzony jest w dwóch egzemplarzach: pierwszy egzemplarz przekazywany jest po rozpatrzeniu sprawy osobie upoważnianej, drugi egzemplarz pozostaje w dyspozycji ASIW (po realizacji procedury nadania uprawnień formularz upoważnienia powinien być w dołączony do akt osobowych pracownika do kontynuacji umowy cywilnoprawnej);

3. ASIZ na podstawie zatwierdzonego upoważnienia, okazanego mu przez ASIW dokonuje czynności związanych z przyznaniem (lub zmiana/wycofaniem) użytkownikowi uprawnień;

4. Stażyści, praktykanci, zleceniobiorcy i wolontariusze otrzymują ograniczone uprawnienia zgodne z zakresem umowy cywilnoprawnej lub programem stażu/praktyki wolontariatu;

5. ABI przeprowadza szkolenie użytkownika w zakresie zaznajomienia z przepisami ustawy o ochronie danych osobowych, jak też obowiązującymi w Urzędzie procedurami w zakresie bezpieczeństwa informacji;

6. ASIZ na polecenie ASIW, dokonuje wyrejestrowania użytkownika z systemu i zablokowania jego uprawnień w przypadku rozwiązania z użytkownikiem stosunku zatrudnienia lub zakończenia przez niego okresu stażu lub praktyki.

7. Identyfikator użytkownika spełnia następujące wymagania:

a) jest kombinacja imienia i nazwiska użytkownika systemu;

b) jest niepowtarzalny w skali systemu;

c) jednym identyfikatorem posługiwać może się wyłącznie jeden użytkownik;

d) każdy z użytkowników jest odpowiedzialny za wszystkie czynności wykonywane w systemie przy pomocy identyfikatora, którym się posługuje.

CZĘŚĆ IX.

Procedura przydzielania i zarządzania hasłami użytkowników

1. Przydzielanie haseł jest kontrolowane przez formalny proces zarządzający, zawierający następujące wymagania:

1) użytkownicy podpisują zobowiązania do zachowania w tajemnicy danych osobowych i stosowanych w Urzędzie Gminy Inowrocław sposobów ich zabezpieczenia (w tym pojęciu mieści się ochrona haseł osobistych) - zobowiązania przechowywane są w ich aktach osobowych;

2) ASIZ zapewnia natychmiastową zmianę hasła początkowego (instalacyjnego), przydzielonego użytkownikowi, na nowe przez niego wybrane;

3) hasła nie są przechowywane w systemie informatycznym w niechronionej postaci.

2. Na wszystkich użytkownikach systemu informatycznego Urzędu Gminy Inowrocław spoczywają, w zakresie zasad posługiwania się hasłami, następujące obowiązki:

1) pierwsze hasło (instalacyjne) dla każdego z użytkowników zakłada ASIZ podczas wprowadzania do systemu identyfikatora użytkownika;

2) użytkownik, w obecności ASIW zmienia hasło na własne, samodzielnie wybrane i nie ujawnia tego hasła jakimkolwiek osobom:

3) hasła generowane są samodzielnie przez użytkowników z cyfr i liter alfabetu łacińskiego.

4) hasło musi składać się z co najmniej 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne;

5) zmiana hasła następuje nie rzadziej, niż co 30 dni. a ponadplanowo w przypadku podejrzenia lub stwierdzenia, że z hasłem zapoznać mogły się osoby trzecie;

6) użytkowników systemu informatycznego obowiązuje utrzymywanie haseł w tajemnicy(również po upływie ważności haseł) oraz przestrzeganie zasady unikania zapisywania haseł na papierze, chyba, że mogą być one przechowywane w sposób bezpieczny.

CZĘŚĆ X.

Procedury rozpoczęcia i zakończenia pracy przez użytkowników

1. Rejestrowanie użytkownika odbywa się z chwilą rozpoczęcia przez niego pracy w systemie.

2. Po poprawnym wykonaniu tej procedury użytkownik może wykonywać wszystkie czynności, na jakie pozwalają mu przydzielone prawa dostępu.

3. Czynności związane z rozpoczęciem pracy w systemie polegają na wykonywaniu przez użytkowników następujących działań:

1) włączenie UPS jeśli takowy jest użytkowany i komputera oraz ewentualnie niezbędnych innych urządzeń peryferyjnych;

2) po załadowaniu systemu operacyjnego i zalogowaniu się jako użytkownik do systemu operacyjnego użytkownik uruchomienia oprogramowanie komunikacyjne;

3) rejestracja w systemie informatycznym (podanie identyfikatora i hasła);

4) po pozytywnym przejściu procedury uwierzytelniania - uzyskanie dostępu do systemu;

4. Użytkownicy przed przystąpieniem do pracy w systemie powinni zwrócić uwagę, czy nie istnieją przesłanki do tego, że dane zostały naruszone. Jeżeli istnieje takie podejrzenie należy postępować zgodnie z procedurą opisaną w rozdziale XXII.

5. W przypadku zaistnienia trudności w dokonaniu autoryzacji, pomimo prawidłowo wykonanych czynności, użytkownik powinien skontaktować się z ASIW.

6. W przypadku, gdy użytkownik czasowo nie wykorzystuje komputera, a urządzenie jest przygotowane do pracy, obowiązuje zasada wylogowania się i zakończenia pracy z systemem. Każda następna operacja w systemie musi być ponownie oparta na wykonaniu procedury uwierzytelnienia się użytkownika.

7. Czynności związane z zakończeniem pracy w systemie polegają na wykonywaniu przez użytkowników następujących działań:

1) po zakończeniu pracy użytkownik wyrejestrowuje się z systemu;

2) zakończeniu ulega działanie oprogramowania komunikacyjnego, a następnie systemu operacyjnego;

3) użytkownik wyłącza komputer, urządzenia peryferyjne i UPS jeśli takowy jest używany.

Odpowiedzialni za bieżący nadzór nad respektowaniem wyżej określonych procedur są ASIW i ABI.

CZĘŚĆ XI.

Sposób ustawienia monitorów w pomieszczeniach, w których przebywają interesanci lub osoby trzecie.

Ekrany monitorów ustawione są w sposób uniemożliwiający interesantom i osobom postronnym bezpośredni wgląd w emitowany obraz, w tych w pomieszczeniach biurowych Urzędu, gdzie warunki lokalowe umożliwiają takie rozwiązanie. Za nadzór w tym zakresie odpowiedzialny jest ABIW.

CZĘŚĆ XII.

Stosowanie automatycznych wygaszaczy ekranów.

Wszystkie komputery wyposażone są w wygaszacze ekranów automatycznie włączające się po ustalanym przez Administratora Systemu Informatycznego czasie nieaktywność użytkownika. Za nadzór w tym zakresie odpowiedzialni są ABI oraz ASIW.

CZĘŚĆ XIII.

Zasady instalacji nowego oprogramowania lub jego aktualizacji.

1. W przypadku instalowania nowego oprogramowania lub jego aktualizacji wykonywane są obowiązkowo kopie danych zawartych w zbiorach.

2. Aplikacje przewidziane do zainstalowania podlegają sprawdzeniu programem antywirusowym.

3. Przewidziane do instalacji oprogramowanie musi być legalne i licencjonowane.

4. Wszelkie czynności związane z instalowaniem oprogramowania (bądź jego usuwaniem) wykonuje Administrator Systemu Informatycznego, względnie upoważnieni serwisanci z firm, z którymi Urząd Gminy w Inowrocławiu zawarł stosowne umowy, w tym umowy powierzenia przetwarzania danych osobowych.

CZĘŚĆ XIV.

Zasady bezpieczeństwa w pracy z komputerami przenośnymi.

W trakcie używania przenośnych urządzeń komputerowych np. typu notebook. należy zwracać szczególną uwagę, aby nie ujawniać informacji prawnie chronionych. W Urzędzie Gminy Inowrocław obowiązują następujące zasady bezpieczeństwa odnoszące się do korzystania z komputerów przenośnych:

1. Osoba użytkująca komputer przenośny, zawierający dane osobowe lub inne informacje podlegające ochronie ma obowiązek zachowania szczególnej ostrożności podczas jego transportu, przechowywania i użytkowania poza obszarem Urzędu, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych;

2. W celu ochrony przed nieuprawnionym dostępem lub ujawnieniem informacji przechowywanych i przetwarzanych w tych urządzeniach stosuje się zabezpieczenie komputera mechanizmem kontroli dostępu do danych (identyfikator i hasło);

3. W komputerze przenośnym zainstalowane jest oprogramowanie antywirusowe;

4. Wprowadzono zakaz niekontrolowanego pozostawiania komputerów zawierających informacje podlegające ustawowej ochronie w samochodach i innych środkach transportu, pokojach hotelowych;

5. Organizowane są szkolenia dla personelu używającego komputerów przenośnych dotyczące obowiązku stosowania wyżej określonych środków bezpieczeństwa.

CZĘŚĆ XV.

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych.

1. W Urzędzie Gminy Inowrocław obowiązuje zasada regularnego sporządzania kopii zapasowych danych oraz kopii oprogramowania, aby zapewnić, że wszystkie istotne informacje i oprogramowanie będą mogły być odzyskane w przypadku katastrofy lub wystąpienia błędów na nośnikach.

2. Kopie są regularnie testowane, aby spełniały wymagania planów ciągłości działania.

3. Określone są terminy przechowywania istotnych informacji oraz wymagania w zakresie utrzymywania kopii zgodnie z przepisami prawa administracyjnego, prawa pracy, prawa finansowego i prawa podatkowego.

Opis procedur i harmonogram tworzenia kopii zawiera załącznik nr 2 do niniejszej instrukcji.

CZĘŚĆ XVI.

Inne środki zabezpieczające.

1. Wójt Gminy Inowrocław wprowadził zakaz używania przez pracowników jakichkolwiek nośników danych, poza wydawanymi przez Administratora Systemu Informatycznego i stanowiącymi własność Urzędu.

2. Każdy nośnik informatyczny, który był użyty poza systemem informatycznym Urzędu Gminy Inowrocław, przed ponownym wykorzystaniem w systemie musi być sprawdzony programem antywirusowym.

3. Drzwi do poszczególnych pomieszczeń biurowych, w których odbywa się przetwarzanie danych, są zamykane na klucze w czasie nieobecności użytkowników tych pomieszczeń

4. Osoby nieuprawnione do dostępu do danych osobowych mogą przebywać w obszarze przetwarzania wyłącznie w obecności pracownika Urzędu Gminy Inowrocław upoważnionego do przetwarzania tych danych.

5. Jeżeli pomieszczenia obszaru przetwarzania danych wykorzystywane do obsługi interesantów wyposażone są jednocześnie w urządzenia z dostępem do systemów bazodanowych albo w tradycyjne kartoteki, należy w nich stosować szczególne środki ostrożności, w tym:

1) interesanci powinni wchodzić pojedynczo i pozostawać w pomieszczeniu tylko w obecności pracownika Urzędu Gminy Inowrocław upoważnionego do przetwarzania tych danych;

2) kartoteki tradycyjne należy zabezpieczyć przed dostępem osób nieuprawnionych;

3) nie należy pozostawiać dokumentów papierowych i nośników informatycznych w miejscach umożliwiających ich wykorzystanie przez osoby nieuprawnione;

4) uprawnienia dostępu do infrastruktury technicznej związanej z siecią komputerową i jej zasilaniem posiadają wyłącznie osoby upoważnione przez Wójta Gminy Inowrocław;

5) tworzenie kopii oprogramowania wykorzystywanego w Urzędzie Gminy Inowrocław dokonywane jest zgodnie z warunkami licencyjnymi zakupionych programów, a czynności tych

dokonuje ASIW.

6. Przesyłanie danych osobowych na nośnikach zewnętrznych (np. wydruk) na zewnątrz jednostki może odbywać się w formie:

a) dostarczenia nośnika (nośników) do rąk własnych uprawnianego odbiorcy, za pokwitowaniem;

b) odbioru nośnika (nośników) przez uprawnionego odbiorcę z siedziby Urzędu Gminy Inowrocław, za pokwitowaniem;

c) przesyłki poleconej.

9) Zabrania się przekazywania za pośrednictwem Internetu (poczty elektronicznej) niezaszyfrowanych informacji prawnie chronionych, w tym danych osobowych, W celu ich ochrony należy korzystać z metody szyfrowania wskazanej przez ASIW, ASIZ i uzgodnionej z Wójtem Gminy Inowrocław. Za nadzór nad realizacją powyższych procedur odpowiedzialni są ABI oraz ASIW.

CZĘŚĆ XVII.

Sposób przechowywaniu wydruków z danymi osobowymi.

1. Wydruki zawierające dane osobowe przechowywane są w zamykanych na klucz szafach znajdujących się w pomieszczeniach biurowych Urzędu Gminy Inowrocław.

2. Użytkownik dokonujący wydruku przy wykorzystaniu drukarki sieciowej zobowiązany jest udać się niezwłocznie do pomieszczenia usytuowania drukarki i przejąć wydrukowany dokument.

3. Każdy pracownik, który napotka wydruk, nośnik elektroniczny, czy inny dokument pozostawiony bez dozoru jest zobowiązany zabezpieczyć go i przekazać Administratorowi Bezpieczeństwa Informacji, za nadzór w tym zakresie odpowiedzialny jest ABI.

CZĘŚĆ XVIII.

Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego i wirusów komputerowych oraz metody ich usuwania

1. Wszystkie komputery są chronione oprogramowaniem antywirusowym z aktywnym monitorem programowym. bazy wirusów są systematycznie aktualizowane.

2. Obowiązek dokonywania tych sprawdzeń spoczywa na ASIW, każdy nośnik, w tym użyty poza systemem informatycznym Urzędu Gminy Inowrocław, jest każdorazowo przedmiotem takich sprawdzeń. Sprawdzanie ewentualnej obecności wirusów komputerowych na wszystkich nośnikach odbywa się automatycznie, z wykorzystaniem programów antywirusowych, na bieżąco aktualizowanych. W razie konieczności usunięcia wirusa postępuje się zgodnie z procedurami określonymi przez producenta oprogramowania.

3. O każdorazowym fakcie wykrycia wirusa przez program monitorujący użytkownicy niezwłocznie powiadamiają Administratora Bezpieczeństwa Informacji i ASIW.

4. Kontrola antywirusowej podlegają nośniki danych służących zarówno do przetwarzani danych osobowych w systemie, jak i do celów instalacyjnych.

5. System informatyczny Urzędu Gminy Inowrocław zabezpieczony jest przy wykorzystaniu środków sprzętowych i programowych przed sieciowymi zagrożeniami zewnętrznymi - w tym nieuprawnionym dostępem do systemu.

6. Wykorzystywane w systemie aplikacje cechują się walorami zabezpieczającymi utratę danych w przypadku przerwy w zasilaniu.

CZĘŚĆ XIX.

Procedury wykonywania napraw, przeglądów i konserwacji systemu oraz nośników informacji służących do przetwarzania danych

1. Bieżące przeglądy i konserwacje sprzętu komputerowego, w tym także przeglądy i aktualizacje oprogramowania wchodzącego w skład systemu informatycznego dokonywane są przez ASIW.

2. Przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonych przez producenta sprzętu. Za terminowość przeprowadzenia przeglądów i konserwacji urządzeń, systemów odpowiada ASIW.

3. W razie konieczności powierzenia naprawy serwisowi zewnętrznemu obowiązują zasady, aby urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe pozbawić wcześniej zapisanych danych, za pomocą oprogramowania do tego przeznaczonego, albo naprawiać je pod nadzorem osoby upoważnionej przez administratora danych.

4. W przypadku konieczności dokonania trwałego zniszczenia zbędnych lub wadliwy nośników i wydruków komputerowych czynności te wykonywane są komisyjnie - pod nadzorem ABI.

5. Nieprawidłowości ujawnione w trakcie przeglądów i konserwacji powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie ujawnienia nieprawidłowości należy zawiadomić ABI. Za nadzór w tym zakresie odpowiedzialny jest ABI.

CZĘŚĆ XX.

Zabezpieczenie fizyczne pomieszczeń w których odbywa się przetwarzanie danych osobowych

1. Urząd Gminy Inowrocław wykorzystuje w celu ochrony obiektu, zgromadzonych w nim dokumentów i mienia oraz zapewnienia bezpieczeństwa pracownikom i interesantom:

1) system sygnalizacji włamania;

2) środki zabezpieczenia mechanicznego;

3) procedury organizacyjne obowiązujące pracowników Urzędu, mające zapewnić pożądany stan bezpieczeństwa Urzędu Gminy Inowrocław.

2. Dokumenty i materiały podlegające rygorom przepisów o ochronie danych osobowych lub zawierające inne informacje prawnie chronione są zabezpieczone zgodnie z obowiązującymi w tym zakresie regulacjami ustawowymi oraz zarządzeniami Wójta Gminy Inowrocław.

CZĘŚĆ XXI.

Obowiązki pracowników Urzędu Gminy Inowrocław w zakresie ochrony obszaru przetwarzania danych osobowych

W Urzędzie Gminy Inowrocław wdrożono realizację przez pracowników następujących obowiązków:

a) dokonywanie codziennej lustracji pomieszczeń w celu ustalenia ewentualnych zdarzeń nadzwyczajnych (zaginięcia elementów wyposażenia, dokumentacji, śladów wskazujących na naruszenie zabezpieczeń itp.);

b) zamykanie drzwi pomieszczeń biurowych na klucz w przypadku konieczności opuszczenia pokoju, jeśli nie pozostają w nim inni uprawnieni użytkownicy systemu informatycznego;

c) przestrzeganie zasady dopuszczalności przebywania w obszarze przetwarzania danych osobowych osób nieuprawnionych wyłącznie w obecności osoby zatrudnionej przy przetwarzaniu tych danych.

Za nadzór w tym zakresie odpowiedzialny jest ABI.

CZĘŚĆ XXII.

Wskazania do zagrożenia naruszenia ochrony danych osobowych

Na naruszenie bezpieczeństwa danych osobowych (lub możliwość wystąpienia takiego zagrożenia) mogą wskazywać:

a) nietypowy stan pomieszczeń wchodzących w skład obszaru przetwarzania (otwarte pomieszczenia, okna, drzwi od szaf biurek, włączone urządzenia);

b) zaginięcie sprzętu lub nośników informacji;

c) nieuzasadnione modyfikacje lub usunięcie danych, nieprawidłowe lub nietypowe działanie systemu informatycznego, wykrycie wirusa w systemie;

d) obecność podejrzanych plików w poczcie elektronicznej, nietypowe komunikaty wyświetlane na monitorze;

e) ujawnienie przetwarzanych danych lub procedur ochrony przetwarzania osobom nieupoważnionym;

f) ujawnienie istnienia nieautoryzowanych kont dostępu do danych, przesłanie danych do niewłaściwego adresata;

g) znalezienie poza obszarem przetwarzania dokumentów, wydruków i innych nośników informacji;

h) niekontrolowany lub niezgodny z obowiązującymi procedurami pobyt w obszarze przetwarzania osoby nieupoważnionej.

CZĘŚĆ XXIII.

Postępowanie osób zatrudnionych przy przetwarzaniu danych

1. Użytkownicy systemu informatycznego Urzędu Gminy Inowrocław po stwierdzeniu (lub podejrzeniu) wystąpienia incydentu naruszenia bezpieczeństwa informacji są zobowiązani do:

1) powstrzymania się od wszelkich czynności w pomieszczeniu przetwarzania danych, mogących zatrzeć ślady naruszenia bezpieczeństwa informacji;

2) niepodejmowania działań w systemie informatycznym w tym nieusuwania podejrzanego oprogramowania;

3) stosowania się (po zgłoszeniu incydentu) do poleceń ABI lub ASIZ, ASIW;

4) sporządzenia na polecenie ABI lub ASIW notatki o incydencie (zdarzeniu).

2. Użytkownicy są zobowiązani do natychmiastowego zgłaszania zaistniałych przypadków naruszenia zasad bezpieczeństwa.

1) w każdym pomieszczeniu obszaru przetwarzania dostępny jest wykaz, telefonów kontaktowych do ASIW, ABI oraz osób zastępujących ich w razie nieobecności;

2) kwestie zgłaszania incydentów są przedmiotem szkoleń organizowanych dla pracowników i innych osób dopuszczonych przez ADO do przetwarzania danych.

3. Od użytkowników systemu informatycznego Urzędu Gminy Inowrocław wymaga się zgłaszania wszelkich zauważonych lub podejrzewanych słabości lub zagrożeń dla systemów. Użytkownicy zobowiązani są zgłaszać takie spostrzeżenia przełożonym lub bezpośrednio ASIW.

4. Użytkownicy są poinformowani, że w żadnych okolicznościach nie powinni usiłować potwierdzać istnienia podejrzanych słabych punktów systemu. Takie zalecenie służy ich własnemu bezpieczeństwu, bowiem testowanie słabych punktów może być interpretowane w systemie, jako potencjalne nadużycie.

5. Użytkownicy systemu zobowiązani są do:

1) obserwacji objawów niewłaściwego funkcjonowania oprogramowania i wszelkich komunikatów pojawiających się na ekranie monitora;

2) jeśli to jest możliwe komputer powinien zostać odizolowany, a jego użytkowanie powinno zostać przerwane;

3) konieczne jest natychmiastowe powiadomienie ABI i ASIW.

6. Użytkownicy systemu nie powinni próbować usuwać podejrzanego oprogramowania, wszelkie działania w tym zakresie pozostają w kompetencjach ASIW.

Postępowanie ASIW po wykryciu lub otrzymaniu zgłoszenia o incydencie:

a) ustala, czy incydent rzeczywiście miał miejsce.

b) określa, czy istnieje zagrożenie dla dalszego prawidłowego funkcjonowania systemu.

c) ocenia, czy system powinien zostać odizolowany od sieci i informuje o takim zamiarze Wójta Gminy Inowrocław oraz ABI.

d) zabezpiecza dowody zdarzenia.

e) zaleca użytkownikom systemu sposób dalszego postępowania.

7. Postępowanie ABI po otrzymaniu zgłoszenia o incydencie:

a) w razie wątpliwości ustala dalsze szczegóły incydentu w rozmowach z osobą zgłaszającą incydent oraz ASIW;

b) informuje o podjętych działaniach związanych z incydentem Wójtowi Gminy Inowrocław, a w razie zaistnienia incydentu o poważnych konsekwencjach sporządza dla niego pisemny "Raport o incydencie";

c) dokonuje analizy skutków incydentu oraz w razie potrzeby opracowuje zalecenia mające na celu podniesienie poziomu bezpieczeństwa systemu. Analizując incydent uwzględnia stan zabezpieczeń fizycznych obszaru przetwarzania danych, stan informacji (czy została zmodyfikowana, utracona lub ujawniona), dane o dostępie osób nieupoważnionych do zasobów oraz ocenia celowość lub przypadkowość ewentualnego przekroczenia uprawnień przez osoby dopuszczone do przetwarzania danych;

d) dokonuje stosownego wpisu do "Ewidencji incydentów naruszenia bezpieczeństwa informacji".

CZĘŚĆ XXIV.

Postanowienia końcowe

1. Każdy z użytkowników systemu informatycznego Urzędu Gminy Inowrocław ma obowiązek zapoznania się z niniejszą Instrukcją, jak też ścisłego przestrzegania zawartych w niej zaleceń.

2. Niezastosowanie się do postanowień niniejszej instrukcji stanowi ciężkie naruszenie podstawowych obowiązków pracowniczych.

3. Instrukcja wchodzi w życie z dniem podpisania.