ZARZĄDZENIE NR 045/2014

Burmistrza Nowego Warpna
z dnia 28 maja 2014 roku

w sprawie **ustalenia "Polityki bezpieczeństwa przetwarzania danych osobowych oraz instrukcji zarządzania systemem informatycznym służących do przetwarzania danych osobowych w Urzędzie Gminy w Nowym Warpnie".**

Na podstawie art. 30 ust.1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U z 2013 r., poz. 594 z późn. zm.) oraz § 3 ust. 3 oraz § 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004r., 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 2004r.), zarządza się co następuje:

§ 1. Ustala się „Politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Nowym Warpnie zwaną dalej „Polityką bezpieczeństwa", która stanowi załącznik nr 1 do niniejszego zarządzenia oraz „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Nowym Warpnie zwaną dalej „Instrukcją", która stanowi załącznik nr 2 do niniejszego zarządzenia.

§ 2. Zobowiązuje się pracowników Urzędu Gminy w Nowym Warpnie do stosowania zasad określonych w „Polityce bezpieczeństwa" i „Instrukcji".

§ 3. Wykonanie zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Nowego Warpna

Władysław Kiraga

Załącznik nr 1 do Zarządzenia Nr 045/2014
Burmistrza Nowego Warpna
z dnia 28 maja 2014 roku

Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Nowym Warpnie

Opracował: Administrator Bezpieczeństwa Informacji Krystian Lamparski

Nowe Warpno, 2014r

SPIS TREŚCI:

Wstęp....4

Rozdział 1. Opis zdarzeń naruszających ochronę danych osobowych....5

Rozdział 2. Zabezpieczenie danych osobowych....6

Rozdział 3. Kontrola przestrzegania zasad zabezpieczenia danych osobowych....8

Rozdział 4. Postępowanie w przypadku naruszenia ochrony danych osobowych....8

Rozdział 5. Monitorowanie zabezpieczeń....10

Rozdział 6. Postanowienia końcowe....10

Załącznik nr 1 - Wykaz pomieszczeń w budynku Urzędu Gminy w Nowym Warpnie, w których przetwarzane są dane osobowe oraz opis systemów informatycznych i wykaz zbiorów danych osobowych oraz programy zastosowane do przetwarzania tych danych 12

Załącznik nr 2 - Opis struktur zbiorów danych....14

Załącznik nr 3 - Raport z naruszenia bezpieczeństwa systemu informatycznego w Urzędzie Gminy – wzór....15

Załącznik nr 4 - Wykaz osób, które zostały zapoznane z Polityką Bezpieczeństwa systemu informatycznego oraz Wykaz osób mających prawo wglądu do danych osobowych z uwagi na wykonywane zakresy czynności....17

Załącznik nr 5 - Oświadczenie - wzór....19

Załącznik nr 6 - Upoważnienie - wzór....20

WSTĘP

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych oraz w systemie tradycyjnym w Urzędzie Gminy w Nowym Warpnie. Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów wspomagających pracę Urzędu. Dokument zwraca uwagę na konsekwencje jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

Dane osobowe w Urzędzie są gromadzone, przechowywane, edytowane, archiwizowane w kartotekach, skorowidzach, księgach, wykazach, zestawieniach oraz w innych zestawach i zbiorach ewidencyjnych poszczególnych komórek organizacyjnych na dokumentach papierowych, jak również w systemach informatycznych na elektronicznych nośnikach informacji.

Bezpośredni nadzór nad przetwarzaniem danych osobowych sprawują kierownicy komórek organizacyjnych. Z polityką bezpieczeństwa obowiązkowo są zapoznawani wszyscy użytkownicy systemów informatycznych i tradycyjnych.

Do informacji przechowywanych w systemach informatycznych jak i dokumentów tradycyjnych mają dostęp jedynie upoważnieni pracownicy jednostki oraz osoby mające imienne zarejestrowane upoważnienie. Wszyscy pracownicy zobowiązani są do zachowania tych danych w tajemnicy.

Dokument „Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Nowym Warpnie, zwany dalej „Polityką bezpieczeństwa", wskazuje sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w systemach informatycznych oraz informacji zgromadzonych, przetwarzanych w formie tradycyjnej i przeznaczony jest dla osób zatrudnionych przy przetwarzaniu tych danych. Polityka Bezpieczeństwa została utworzona w związku z wymaganiami zawartymi w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926, ze zm.) oraz zgodnie z § 3 i 4 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 (Dz. U. Nr 100, poz. 1024) oraz § 13 i § 14 rozporządzenia Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. Nr 159, poz. 948).

1. „Polityka bezpieczeństwa" określa tryb postępowania w przypadku, gdy:

a) stwierdzono naruszenie zabezpieczenia systemu informatycznego,
b) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci informatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.
c) stwierdzono naruszenie zabezpieczeń fizycznych tj. zamków drzwi, szaf, w których przechowywane są dane osobowe przetwarzane w systemie tradycyjnym.

2. Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemach tradycyjnym i informatycznym Urzędu.

3. Za bezpieczeństwo danych osobowych przetwarzanych w systemach przetwarzania danych osobowych odpowiada administrator danych. Kierownicy komórek organizacyjnych obowiązani są zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinni zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą utratą uszkodzeniem lub

zniszczeniem.
4. Administrator danych, którym jest Burmistrz Nowego Warpna, wyznacza Administratora Bezpieczeństwa Informacji danych zawartych w systemach tradycyjnym i informatycznym Urzędu, zwanego dalej ”Administratorem Bezpieczeństwa” oraz osobę upoważnioną do zastępowania „Administratora Bezpieczeństwa”.

5. Administrator Bezpieczeństwa realizuje zadania w zakresie ochrony danych, a w szczególności:

a) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych i tradycyjnych Urzędu,
b) podejmowania stosownych działań zgodnie z niniejszą „Polityką bezpieczeństwa” w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym lub tradycyjnym,
c) niezwłocznego informowania Administratora danych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
d) nadzoru i kontroli systemów informatycznych i tradycyjnych służących do przetwarzania danych osobowych, i osób przy nich zatrudnionych.

6. Osoba zastępująca Administratora Bezpieczeństwa powyższe zadania realizuje w przypadku nieobecności Administratora Bezpieczeństwa.

7. Osoba zastępująca składa Administratorowi Bezpieczeństwa relację z podejmowanych działań w czasie jego zastępstwa.

Rozdział 1
OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

I. Podział zagrożeń:

1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.
3) zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

II. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:

1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,

3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
6) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
7) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
8) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
9) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,
10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
11) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.,
12) podmieniono lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe,
13) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej itp.

Rozdział 2
ZABEZPIECZENIE DANYCH OSOBOWYCH

1. Dostęp do danych wprowadzonych przez użytkowników systemów informatycznych mają jedynie upoważnieni pracownicy oraz administrator systemu zapewniający jego prawidłową eksploatację. Wszyscy pracownicy, będący użytkownikami systemu zobowiązani są do zachowania tych danych w tajemnicy.

2. Ochronie podlegają dane osobowe gromadzone i przetwarzane w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych oraz w urządzeniach i systemie informatycznym Urzędu.

3. Nie zezwala się na korzystanie z jakiegokolwiek nowego oprogramowania bez zgody Administratora Bezpieczeństwa Informacji. Dodatkowe oprogramowanie może być instalowane wyłącznie po uzyskaniu zezwolenia. Używanie oprogramowania prywatnego w sieci jest kategorycznie zabronione. Na stacjach roboczych powinno być zainstalowane jedynie niezbędne oprogramowanie.

4. Administratorem danych osobowych zawartych i przetwarzanych w systemach informatycznym i tradycyjnym Urzędu Gminy w Nowym Warpnie jest Burmistrz Nowego Warpna.

5. Administrator danych osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznym i tradycyjnym, a w szczególności:

a) zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
b) zapobiegać przed zabraniem danych przez osobę nieuprawnioną,
c) zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.

6. Środki bezpieczeństwa fizycznego są konieczne dla zapobiegania niepowołanemu dostępowi do informacji, nieautoryzowanym operacjom w systemie, kontroli dostępu do zasobów oraz w celu zabezpieczenia sprzętu teleinformatycznego.
Do zastosowanych środków technicznych należy:

1) przetwarzanie danych osobowych w wydzielonych pomieszczeniach położonych w strefie administracyjnej zabezpieczone przed dostępem osób nieuprawnionych,
2) zabezpieczenie wejścia do pomieszczeń, o których mowa w pkt. 1, tzn. zainstalowanie odpowiednich zamków do drzwi, zabezpieczeń w oknach oraz być wyposażone w środki ochrony ppoż.,
3) szczególne zabezpieczenie centrum przetwarzania danych (komputer centralny, serwerownia) poprzez zastosowanie systemu kontroli dostępu,
4) wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji przed dostępem osób nieupoważnionych do przetwarzania danych.

7. Do zastosowanych środków organizacyjnych należą przede wszystkim następujące zasady:

1) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych,
2) przeszkolenie osób, o których mowa w pkt. 1, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych,
3) kontrolowanie otwierania i zamykania pomieszczeń, w których są przetwarzane dane osobowe, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę.

8. Niezależnie od niniejszych zasad opisanych w tym dokumencie w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych osobowych w określonym systemie.

9. Wykaz pomieszczeń, w których przetwarzane są dane osobowe oraz wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych - ***załącznik nr 1*** do niniejszego dokumentu. Załącznik ten zawiera również wykaz zbiorów danych osobowych oraz programy zastosowane do przetwarzania tych danych

10. Opis struktur zbiorów danych określa ***załącznik nr 2.***

11. Sposób przepływu danych pomiędzy poszczególnymi systemami:

1) Komunikacja tradycyjna:
   - obieg dokumentów zawierających dane osobowe, pomiędzy komórkami organizacyjnymi Urzędu, winien odbywać w sposób zapewniający pełną ochronę przed ujawnieniem zawartych w tych dokumentach danych .
2) Komunikacja w sieci komputerowej:

- Przekazywanie informacji (danych) w systemie informatycznym poza sieć lokalną Urzędu odbywa się w relacji:
  Urząd - mieszkańcy, Zakład Ubezpieczeń Społecznych, Urząd Skarbowy, Banki, Narodowy Fundusz Zdrowia, Zachodniopomorski Urząd Wojewódzki, Urząd Marszałkowski i inne komórki samorządowe i rządowe.

Zabronione jest jednoczesne podłączanie komputerów do sieci wewnętrznej Urzędu i sieci zewnętrznych (Plus, Era, Orange, Play, pozostałe sieci komórkowe, WiFi , WiMAX itp.).

Rozdział 3
KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Administrator danych lub osoba przez niego wyznaczona, którą jest „Administrator Bezpieczeństwa Informacji" sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.

2. Administrator Bezpieczeństwa na bieżąco kontroluje stan bezpieczeństwa danych osobowych i przestrzeganie zasad ochrony danych.

3. Podczas kontroli kontrolujący zwraca szczególną uwagę na:

a) kopie bezpieczeństwa pod względem przydatności do możliwości odtwarzania danych (co miesiąc),
b) ewidencję nośników magnetycznych,
c) częstotliwość zmiany haseł .

Rozdział 4
POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. W przypadku stwierdzenia naruszenia:

1) zabezpieczenia systemu informatycznego,
2) technicznego stanu urządzeń,
3) zawartości zbioru danych osobowych,
4) ujawnienia metody pracy lub sposobu działania programu,
5) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
6) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.)

każda osoba zatrudniona przy przetwarzaniu danych osobowych jest obowiązana niezwłocznie powiadomić o tym fakcie Administratora Bezpieczeństwa.

2. W razie niemożliwości zawiadomienia Administratora Bezpieczeństwa lub osoby przez niego upoważnionej, należy powiadomić bezpośredniego przełożonego,
3. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Bezpieczeństwa lub upoważnionej przez niego osoby, należy:

1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
3) zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
4) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
5) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
6) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
7) udokumentować wstępnie zaistniałe naruszenie,
8) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa lub osoby upoważnionej.

4. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Administrator Bezpieczeństwa lub osoba go zastępująca:

1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Urzędu,
2) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
3) rozważa celowość i potrzebę powiadamiania o zaistniałym naruszeniu Administratora danych,
4) nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami zewnętrznymi.

5. Administrator Bezpieczeństwa dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego ***załącznik nr 3,*** który powinien zawierać w szczególności:

1) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
2) określenie czasu i miejsca naruszenia i powiadomienia,
3) określenie okoliczności towarzyszących i rodzaju naruszenia,
4) wyszczególnienie wziętych pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
5) wstępną ocenę przyczyn wystąpienia naruszenia,
6) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

6. Raport, o którym mowa w pkt. 5, Administrator Bezpieczeństwa niezwłocznie przekazuje Administratorowi danych , a w przypadku jego nieobecności osobie uprawnionej.

7. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Administrator Bezpieczeństwa zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

8. Zaistniałe naruszenie podlega szczegółowej, zespołowej analizie prowadzonej przez Administratora danych i Administratora Bezpieczeństwa Informacji.

9. Analiza, o której mowa w ust. 9, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski, co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

Rozdział 5
MONITOROWANIE ZABEZPIECZEŃ

1. Prawo do monitorowania systemu zabezpieczeń posiadają, zgodnie z zakresem czynności:

1) Administrator Danych,
2) Administrator Bezpieczeństwa Informacji.

2. W ramach kontroli należy zwracać szczególna uwagę na:

1) okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności do możliwości odtwarzania danych,
2) kontrola ewidencji nośników magnetycznych,
3) kontrola właściwej częstotliwości zmiany haseł.

Rozdział 6
POSTANOWIENIA KOŃCOWE

1. 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, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.

2. Administrator Bezpieczeństwa zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych wg wzoru stanowiącego ***załącznik nr 4*** do niniejszego dokumentu. Załącznik ten zawiera również wykaz osób mających prawo wglądu do danych osobowych w kartotekach z uwagi na wykonywane zakresy czynności. Pracownicy obsługi technicznej podpisują oświadczenie, którego wzór stanowi ***załącznik nr 5***. Osoby odbywające staż, praktykę mają wgląd do danych osobowych oraz do systemu informatycznego na podstawie upoważnienia, którego wzór stanowi ***załącznik nr 6*** nadanego przez Administratora oraz ww. oświadczenia.

3. 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.

4. 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. z 2002 r. Nr 101, poz. 926) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

5. W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity (Dz. U. z 2002 r. Nr 101, poz. 926), 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 (Dz. U. Nr 100, poz. 1024) oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. 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).

Wykaz pomieszczeń w budynku Urzędu Gminy w Nowym Warpnie, w których przetwarzane są dane osobowe.

Numer pokoju	Komórka organizacyjna	System

Wykaz zbiorów danych osobowych oraz programy zastosowane do przetwarzania tych danych

Nazwa zbioru	Program

Opis struktury zbiorów danych

R a p o r t

z naruszenia bezpieczeństwa systemu informatycznego w Urzędzie Gminy w Nowym Warpnie

1. Data: ..... Godzina: .....
(dd.mm.rrrr) (00:00)

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

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

3. Lokalizacja zdarzenia:

.....
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....

.....

.....

.....

5. Podjęte działania:

.....

.....

6. Przyczyny wystąpienia zdarzenia:

.....

.....

7. Postępowanie wyjaśniające:

.....

.....

.....

.....

.....

….....

(data, podpis Administratora Bezpieczeństwa Informacji)

Wykaz osób, które zostały zapoznane z „Polityką bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy w Nowym Warpnie przeznaczonej dla osób zatrudnionych przy przetwarzaniu tych danych.

Przyjąłem/Przyjęłam do wiadomości i stosowania zapisy Polityki bezpieczeństwa.

Nazwisko i Imię	Komórka organizacyjna	Data, podpis

Wykaz osób mających prawo wglądu do danych osobowych w kartotekach z uwagi na wykonywane zakresy czynności

Sprawowana funkcja	Imię i nazwisko
Administrator Danych	
Administrator Bezpieczeństwa Informacji	
Radca Prawny	
Audytor Wewnętrzny	

Uwaga!

1. Obsługa techniczna Urzędu Gminy w Nowym Warpnie, (sprzątaczki, pracownicy gospodarczy) podpisują oświadczenie, którego wzór stanowi **załącznik nr 5** do „Polityki bezpieczeństwa”.
2. Osoby odbywające staż, praktykę mają wgląd do danych osobowych oraz do systemu informatycznego na podstawie upoważnienia (**załącznik nr 6**) nadanego przez Administratora oraz oświadczenia (**załącznik nr 5**).

……..…….....……...
(imię i nazwisko pracownika)

……...

……...
(miejsce zamieszkania)

OŚWIADCZENIE

1. Stwierdzam własnoręcznym podpisem, że znana jest mi treść przepisów :
   a) o ochronie tajemnic prawnie chronionych stanowiących tajemnicę służbową wynikającą z Kodeksu Pracy,
   b) o ochronie danych osobowych wynikająca z ustawy o ochronie danych osobowych ,
   c) o odpowiedzialności karnej za naruszenie ochrony danych osobowych.

2. Zobowiązuję się nie ujawniać wiadomości, z którymi zapoznałem/am się w trakcie wykonywanych czynności służbowych .

(podpis pracownika) (podpis złożono w obecności)

…….....
/miejscowość, data/

U P O W A Ż N I E N I E Nr.....

Na podstawie art.37 ustawy z dnia 29 sierpnia 1999 r. o ochronie danych osobowych (t.j. z 2002r. Dz. U. Nr 101 poz.926 z późn. zm.)

U p o w a ż n i a m

.....
(imię i nazwisko)

zatrudnionego na stanowisku

…….....

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

w.....
(nazwa jednostki organizacyjnej)

Upoważnienie wydaje się na czas nieokreślony/określony.

Załącznik Nr 2 do Zarządzenia Nr 045/2014
Burmistrza Nowego Warpna
z dnia 28 maja 2014 roku

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Nowym Warpnie

Nowe Warpno 2014

I
Postanowienia ogólne

1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej „Instrukcją", określa procedury dotyczące zasad bezpieczeństwa przetwarzania danych osobowych oraz zasady postępowania administratora danych osobowych, osób przez niego wyznaczonych i użytkowników przetwarzających dane osobowe w Urzędzie Gminy w Nowym Warpnie
2. W systemach informatycznych służących do przetwarzania danych osobowych stosuje się środki bezpieczeństwa na poziomie wysokim.

II
Nadawanie uprawnień do przetwarzania danych osobowych oraz ich rejestrowanie w systemie informatycznym

1. Przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych, każdy użytkownik powinien zostać zapoznany przez przełożonego lub Administratora Bezpieczeństwa Informacji z przepisami dotyczącymi ochrony danych osobowych oraz obowiązującymi wewnętrznymi regulacjami w tym zakresie.
2. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, mogą zostać dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych, wydane przez administratora danych osobowych.
3. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, mogą zostać dopuszczone również osoby, którym udzielono upoważnień do przetwarzania danych osobowych na podstawie porozumień zawartych w sprawie powierzenia przetwarzania danych osobowych.
4. Wydanie upoważnienia oraz rejestracja użytkownika w systemie informatycznym przetwarzającym dane osobowe następuje na wniosek przełożonego użytkownika.
5. Procedury wydawania i odwoływania upoważnień dla użytkowników do przetwarzania danych osobowych realizowane są według następujących zasad:
a) przełożony użytkownika składa do administratora danych osobowych pisemny wniosek o wydanie upoważnienia, który zawiera:
   - imię i nazwisko użytkownika,
   - stanowisko zajmowane przez użytkownika,
   - nazwę zbioru danych osobowych oraz nazwę systemu informatycznego, do którego użytkownik będzie miał dostęp
   - zakres upoważnienia do przetwarzania danych osobowych
   - datę, z jaką upoważnienie ma być wydane,
   - okres ważności upoważnienia;
b) oryginał upoważnienia zostaje przekazany użytkownikowi za potwierdzeniem odbioru, kopia zaś jest przechowywana u Administratora Bezpieczeństwa Informacji.
6. Wyrejestrowania użytkownika z systemu informatycznego dokonuje na wniosek administratora danych osobowych lub przełożonego użytkownika administrator sieci po uzgodnieniu z Administratorem Bezpieczeństwa Informacji.
7. Osobie niebędącej pracownikiem administrator danych udziela upoważnienia na wniosek Administratora Bezpieczeństwa Informacji.
8. Użytkownik niebędący pracownikiem otrzymuje oryginał upoważnienia za potwierdzeniem odbioru. Kopia upoważnienia przechowywana jest u Administratora Bezpieczeństwa Informacji.
9. Przyznanie uprawnień do przetwarzania danych osobowych w systemie informatycznym polega na wprowadzeniu do systemu identyfikatora, hasła oraz ustanowienia zakresu dostępnych danych i operacji dla każdego użytkownika.
10. Za przydzielenie i wygenerowanie identyfikatora i hasła użytkownikowi, który po raz pierwszy korzysta z systemu informatycznego, odpowiada administrator sieci.

11. Identyfikator użytkownika nie może być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielany innej osobie.
12. Przełożeni użytkowników zobowiązani są pisemnie informować administratora danych osobowych lub Administratora Bezpieczeństwa Informacji o każdej zmianie dotyczącej użytkowników. mającej wpływ na zakres posiadanych uprawnień do przetwarzania danych osobowych.
13. Administrator Bezpieczeństwa Informacji jest zobowiązany do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych.

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

1. Użytkownik uzyskuje dostęp do danych osobowych przetwarzanych w systemie informatycznym wyłącznie po podaniu identyfikatora i hasła.
2. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik jest odpowiedzialny za wszystkie czynności wykonane przy użyciu swojego identyfikatora.
3. Identyfikator składa się minimalnie z 4 znaków, które nie są rozdzielone spacjami ani znakami interpunkcyjnymi.
4. Użytkownik, z chwilą przystąpienia do pracy w systemie informatycznym, otrzymuje hasło początkowe i jest zobowiązany zmienić je natychmiast po rozpoczęciu pracy, na sobie tylko znany ciąg znaków.
5. Hasło składa się co najmniej z 8 znaków.
6. Hasło powinno zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
7. Hasło nie może być zapisane w miejscu dostępnym dla osób nieuprawnionych i należy je zachować w tajemnicy, również po upływie jego ważności.
8. Hasło należy zmieniać co 30 dni.
9. Użytkownik nie może udostępniać osobom nieuprawnionymi swojego identyfikatora oraz hasła. Po uwierzytelnieniu w systemie, użytkownik nie może udostępniać osobom nieuprawnionym swojego stanowiska pracy.
10. Jeśli istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest niezwłocznie je zmienić oraz powiadomić o tym fakcie. Instrukcja określa procedury dotyczące zasad bezpieczeństwa przetwarzania danych osobowych oraz zasady postępowania administratora danych osobowych, osób przez niego wyznaczonych i użytkowników przetwarzających dane osobowe w Urzędzie Gminy w Nowym Warpnie.
11. Burmistrz wykonuje obowiązki administratora danych osobowych w odniesieniu do prowadzonych w Urzędzie zbiorów danych.
12. W systemach informatycznych służących do przetwarzania danych osobowych stosuje się środki bezpieczeństwa na poziomie wysokim.

IV

Administrator Bezpieczeństwa Informacji

Osoby uprawnione do wykonywania prac administracyjnych w systemie informatycznym posiadają własne konta administracyjne oraz hasła.

V
Rozpoczęcie, zawieszenie i zakończenie pracy przez użytkowników systemu

1. Użytkownik, rozpoczynając pracę na komputerze, loguje się do systemu informatycznego.
2. Dostęp do danych osobowych możliwy jest jedynie po dokonaniu uwierzytelnienia użytkownika.

3. Maksymalna liczba prób wprowadzenia hasła przy logowaniu się do systemu informatycznego wynosi 3. Po przekroczeniu tej liczby prób logowania system blokuje dostęp do danych na poziomie danego użytkownika. Odblokowania dostępu do zbioru danych może dokonać administrator sieci w porozumieniu z Administratorem Bezpieczeństwa Informacji.
4. W przypadku braku aktywności użytkownika na komputerze przez czas dłuższy niż 10 minut następuje automatyczne włączenie wygaszacza ekranu.
5. Monitory stanowisk komputerowych, na których przetwarzane są dane osobowe, znajdujące się w pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień do przetwarzania danych osobowych, należy ustawić w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
6. Przebywanie osób nieuprawnionych w pomieszczeniach znajdujących się na obszarze, w którym są przetwarzane dane osobowe, jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania.
7. Pomieszczenia, w których przetwarzane są dane osobowe, należy zamykać na czas nieobecności osób upoważnionych, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.
8. Przed opuszczeniem stanowiska pracy użytkownik jest obowiązany:
a) wylogować się z systemy informatycznego albo
b) wywołać blokowany hasłem wygaszacz ekranu
9. Kończąc pracę użytkownik jest obowiązany wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy.
10. Wszelką dokumentację oraz nośniki magnetyczne i optyczne , na których znajdują się dane osobowe, przechowuje się w szafach zamykanych na klucz.

VI
Tworzenie kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu, poprzez tworzenie kopii zapasowych.
2. Za tworzenie kopii zapasowych zbiorów danych osobowych odpowiedzialny jest administrator sieci.
3. W przypadku lokalnego przetwarzania danych osobowych na służbowych komputerach, użytkownicy systemu informatycznego zobowiązani są do centralnego przechowywania kopii danych, tak aby możliwe było zabezpieczenie ich dostępności poprzez wykonanie kopii zapasowych.
4. Przez centralne przechowywanie kopii danych rozumie się cotygodniowe przegrywanie zbioru danych na specjalnie wydzielony do tego celu obszar dysku na serwerze. Jeśli z przyczyn technicznych nie jest to możliwe, użytkownicy systemu są zobowiązani do sporządzania kopii zapasowych zbiorów danych na nośniku danych i przechowywania w szafie zamykanej na klucz.
5. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu informatycznego. Za przeprowadzanie tej procedury odpowiedzialny jest administrator sieci.
6. Kopie zapasowe wykonywane są zgodnie z następującym harmonogramem:
a) kopia zapasowa aplikacji przetwarzającej dane osobowe - pełna kopia wykonywana jest po wprowadzeniu zmian do aplikacji i zapisywana na nośnikach danych;
b) kopia zapasowa danych osobowych przetwarzanych przez aplikację - pełna kopia wykonywana jest raz w tygodniu, a w przypadku wprowadzenia znacznych zmian danych osobowych, może być wykonywana częściej;
c) kopia zapasowa danych konfiguracyjnych systemu informatycznego przetwarzającego dane osobowe, w tym uprawnień użytkowników systemu - pełna kopia wykonywana jest raz w miesiącu.
7. Kopie zapasowe przechowywane są w szafie zamykanej na klucz.
8. W celu ochrony danych na serwerze zastosowano potrójne zabezpieczenie przeciwko utracie danych. Stanowiska pracowników są jedynie komputerami klienckimi. Zainstalowane oprogramowanie w oparciu o usługę Active Directory oraz częściowo kontroler domeny, umożliwia łączenie się do baz danych zainstalowanych na serwerze i wszelkie zmiany zostają zapisane na dysku

serwerowym. Eliminuje to niebezpieczeństwo utraty danych w momencie awarii komputera klienckiego.
Wykonywanie kopii zapasowych na serwerze odbywa się w następujący sposób:
a) serwer podłączony jest do macierzy zewnętrznej wyposażonej w 3 dyski twarde, działające w RAID 5,
b) uruchomiona została usługa backupu danych, która kopiuje dane z serwera głównego na drugi serwer – udział dysku sieciowego – następnie tworzone jest skompresowane archiwum, które zostaje nagrane na nośnik wymienny DVD,
c) stworzony obraz archiwum pozostaje nadpisany danymi z następnego dnia i procedura nagrywania zostaje powtórzona codziennie.

VII
Sposób, miejsce i okres przechowywania elektronicznych nośników danych zawierających dane osobowe oraz kopii zapasowych

1. Użytkownicy nie mogą wynosić z ośrodka nośników danych z zapisanymi danymi osobowymi, bez zgody administratora danych osobowych lub Administratora Bezpieczeństwa Informacji.
2. Okresowe kopie zapasowe wykonywane są na dyskietkach, płytach CD, DVD lub innych nośnikach danych. Kopie przechowuje się w innych pomieszczeniach niż te, w których przechowywane są zbiory danych wykorzystywane na bieżąco. Kopie zapasowe przechowuje się w sposób uniemożliwiający nieuprawnione przejęcie, modyfikacje, uszkodzenie lub zniszczenie.
3. Dostęp do nośników z kopiami zapasowymi danych osobowych mają wyłącznie Administrator Bezpieczeństwa Informacji oraz administrator sieci.
4. Usunięcie danych z systemu powinno zostać zrealizowane przy pomocy oprogramowania przeznaczonego do bezpiecznego usuwania danych z nośnika danych.
5. Za zniszczenie kopii zapasowych sporządzanych indywidualnie przez użytkownika odpowiada użytkownik.
6. Dane osobowe w postaci elektronicznej należy usuwać z nośnika danych w sposób uniemożliwiający ich ponowne odtworzenie, nie później niż po upływie 5 dni po wykorzystaniu danych, chyba że z odrębnych przepisów wynika obowiązek ich przechowywania.
7. Nośniki danych podlegają komisyjnemu zniszczeniu w przypadku wycofania z eksploatacji sprzętu komputerowego, na którym przetwarzane były dane osobowe oraz po przeniesieniu danych osobowych do zbiorów danych w systemie informatycznym z nośników, których ponowne wykorzystanie nie jest możliwe. Z przeprowadzonych czynności komisja sporządza protokół.
8. Przez zniszczenie nośników danych należy rozumieć ich trwałe i nieodwracalne uszkodzenie fizyczne do stanu uniemożliwiającego ich rekonstrukcję i odzyskanie danych.

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

1. Za ochronę antywirusową systemu informatycznego odpowiada administrator sieci.
2. System antywirusowy zainstalowany jest w każdym komputerze z dostępem do danych osobowych. Ustawienie poziomu bezpieczeństwa i pobieranie aktualizacji bazy sygnatur wirusowych zarządzane jest indywidualnie (automatycznie).
3. Programy antywirusowe są uaktywnione przez cały czas pracy każdego komputera w systemie informatycznym.
4. Wszystkie pliki otrzymywane z zewnątrz, jak również wysyłane na zewnątrz, podlegają automatycznemu sprawdzeniu przez system antywirusowy pod kątem występowania wirusów z stosowaniem najnowszej dostępnej wersji programu antywirusowego.
5. W przypadku pojawienia się wirusa, użytkownik obowiązany jest zaprzestać wykonywania jakichkolwiek czynności w systemie i niezwłocznie powiadomić o tym fakcie administratora sieci lub Administratora Bezpieczeństwa Informacji.

6. Niedozwolone jest otwieranie wiadomości poczty elektronicznej i załączników od „niezaufanych" nadawców.
7. Niedozwolone jest wyłączanie, blokowanie i odinstalowywanie programów zabezpieczających komputer przed oprogramowaniem złośliwym oraz nieautoryzowanym dostępem.
8. Administrator sieci jest odpowiedzialny za aktywowanie i poprawne konfigurowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku:
a) sieci wewnętrznej i zewnętrznej;
b) stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci wewnętrznej.
9. W celu zabezpieczenia sieci przed nieautoryzowanym dostępem do baz danych ośrodka przez Internet zastosowano następujące środki:
- w zakresie dostępu z sieci zewnętrznej WAN do sieci wewnętrznej urzędu – LAN – zastosowano podwójne środki ochrony. Łącze internetowe podpięte jest do routera z firewallem. Drugim zabezpieczeniem jest serwer filtrujący i monitorujący dostęp do i z sieci wewnętrznej do którego podpięty jest router programowy – serwer Linux.
Zabezpieczenie pierwsze polega na blokadzie portów i usług, natomiast zabezpieczenie drugie polega na blokowaniu nieautoryzowanych komputerów – filtrowanie MAC adresów – oraz blokowanie dodatkowo wszystkich portów wychodzących i przychodzących poprzez translacje adresów i rozbudowany routing wraz z regułami firewall. Oprócz wymienionych powyżej zabezpieczeń zastosowano również system antywirusowy który monitoruje obecność wirusów w poczcie elektronicznej oraz wszystkich pozostałych dokumentach.

IX
Udostępnianie danych osobowych i sposób odnotowywania informacji o udostępnianiu danych

1. Dane osobowe przetwarzane w Urzędzie Gminy w Nowym Warpnie mogą być udostępnione osobom lub podmiotom uprawnionym do ich otrzymania, na mocy ustawy o ochronie danych osobowych oraz innych przepisów powszechnie obowiązujących.
2. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepisy odrębne stanowią inaczej.
3. Dane udostępnione Urzędowi Gminy w Nowym Warpnie przez inny podmiot można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
4. Administrator Bezpieczeństwa Informacji prowadzi ewidencję udostępnionych danych, która zawiera:
a) numer ewidencyjny wydruku;
b) zakres udostępnionych danych;
c) adresata udostępnionych danych;
d) datę udostępnienia.
5. Odnotowanie informacji powinno nastąpić niezwłocznie po udostępnieniu danych.

X
Wykonywanie przeglądów i konserwacji systemu oraz nośników danych służących do przetwarzania danych

1.Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe mogą być wykonywane przez pracowników firmy mającej zawartą umowę na wykonywanie wymienionych prac oraz stosowne upoważnienie administratora ochrony danych osobowych.
2. Administrator sieci okresowo sprawdza możliwość odtworzenia danych z kopii zapasowej. Częstotliwość wykonywania procedury odtwarzania danych jest uzgadniana z Administratorem Bezpieczeństwa Informacji.
3. Aktualizacja oprogramowania powinna być przeprowadzana zgodnie z zaleceniami producentów co do bezpieczeństwa i stabilności nowych wersji.

4. Za terminowość przeprowadzania przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada administrator sieci.
5. Nieprawidłowości w działaniu systemu informatycznego oraz oprogramowania są niezwłocznie usuwane przez administratora sieci, a ich przyczyny analizowane.
6. Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe zmiana jego lokalizacji, może być dokonana tylko za wiedzą i zgodą Administratora Bezpieczeństwa Informacji.