WÓJT GMINY
WIŚLICA

Zarządzenie Nr 42/2014
Wójta Gminy Wiślica
z dnia 2 kwietnia 2014 roku

w sprawie: wprowadzenia Polityki Bezpieczeństwa Informacji w Urzędzie Gminy w Wiślicy

Na podstawie art. 3 ust. 1 i art. 36 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity: Dz. U. z 2002 r. Nr 101 poz. 926, z późn. zm.) oraz rozporządzenia ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100 poz. 1024), **w celu wytyczenia podstawowych zasad i wymagań bezpieczeństwa zasobów informacji, jako filaru bezpieczeństwa realizacji zadań gminy przez Urząd Gminy Wiślica, zarządza co następuje:**

§ 1

Powołuje się Administratora Bezpieczeństwa Informacji (ABI) w osobie pani Edyty Szostak, który jest jednocześnie pełnomocnikiem Wójta Gminy Wiślica jako Administrator Danych Osobowych (ADO) – osobą odpowiedzialną za ochronę i bezpieczeństwo przetwarzanych danych w tym w szczególności za przeciwdziałanie dostępowi do nich osób niepowołanych oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszenia zabezpieczeń.

§ 2

W celu zapewnienia przestrzegania przepisów ustawy o ochronie danych osobowych wprowadza się Politykę Bezpieczeństwa Informacji w brzmieniu określonym w załączniku do niniejszego zarządzenia.

§ 3

Zobowiązuje się osoby przetwarzające dane osobowe w Urzędzie Gminy do zapoznania się z treścią zarządzenia oraz załącznika i ich stosowania.

§ 4

Traci moc Zarządzenie Nr 66/2004 Wójta Gminy Wiślica.

§ 5

Wykonanie Zarządzenia i nadzór nad wykonaniem zarządzenia powierza się Sekretarzowi Gminy.

§ 6

Zarządzenie wchodzi w życie z dniem podpisania i podlega publikacji w Biuletynie Informacji Publicznej bez załącznika, który stosownie do art. 36 ust. 1 ustawy o ochronie danych osobowych stanowi chronione środki organizacyjne zapewniające bezpieczne przetwarzanie danych osobowych.

WÓJT GMINY
mgr inż. Stanisław Krzak

Załącznik do zarządzania
Wójta Gminy Wiślica
nr 42/2014 z 02.04.2014 r.

Polityka Bezpieczeństwa Informacji Urzędu Gminy Wiślica

§ 1.

Niniejszą Politykę Bezpieczeństwa Urzędu Gminy Wiślica opracowano na podstawie:

1. art. 39 a ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (t.j. Dz. U. z 2002 r, Nr 101 poz. 926 z późn. zm.);
2. 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. z 2004 r, Nr 100 poz. 1024);

§ 2.

Ilekroć Polityki Bezpieczeństwa lub w jej załącznikach mowa jest o:

- **Polityce Bezpieczeństwa** - należy przez to rozumieć Politykę Bezpieczeństwa Urzędu Gminy Wiślica;
- **Urzędzie** - należy przez to rozumieć Urząd Gminy Wiślica;
- **Administratorze Danych** (ADO) - rozumie się przez to organ, instytucję, jednostkę organizacyjną, podmiot lub osobę, do których stosuje się ustawę o ochronie danych osobowych, decydujące o celach i środkach przetwarzania danych osobowych;
- **Administratorze Bezpieczeństwa Informacji** (ABI) – należy przez to rozumieć pracownika Urzędu wyznaczonego przez Administratora Danych Osobowych do wdrażania oraz nadzorowania przestrzegania zasad ochrony oraz wymagań w zakresie ochrony, wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych;
- **Administratorze Systemu Informatycznego** (ASI) – należy przez to rozumieć pracownika lub pracowników obsługi informatycznej wyznaczonej przez Administratora Danych Osobowych, odpowiedzialnych za stosowanie technicznych i organizacyjnych środków ochrony danych osobowych przetwarzanych w systemie informatycznym;
- **Osobie upoważnionej** - należy przez to rozumieć osobę posiadająca upoważnienie wydane przez ADO do przetwarzania danych osobowych
- **Użytkowniku** – należy przez to rozumieć osobę posiadająca upoważnienie wydane przez ADO do przetwarzania danych osobowych w systemie informatycznym;

- **Danych Osobowych** – należy przez to rozumieć 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 osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań,

- **zbiorze 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 czy podzielony funkcjonalnie,

- **przetwarzaniu danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,

- **usuwaniu danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,

- **zgodzie osoby, której dane dotyczą** - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści,

- **systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,

- **zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatacją stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,

Na politykę składają się niniejszy dokument wraz z załącznikami:

1. Instrukcją realizacji polityki bezpieczeństwa w zakresie ochrony danych osobowych oraz zasady postępowania w sytuacji ich naruszenia w Urzędzie Gminy Wiślica.
2. Instrukcją przetwarzania danych osobowych w Urzędzie Gminy Wiślica.
3. Instrukcją Zarządzania Systemami Teleinformatycznymi w Urzędzie Gminy Wiślica wraz z załącznikiem „Zasadami wykorzystania sprzętu teleinformatycznego w Urzędzie Gminy Wiślica".
4. Upoważnieniem do przetwarzania danych osobowych.
5. Oświadczeniem użytkownika
6. Wzorem zgłoszenia rozpoczęcia pracy.

§ 3.

Podmiotami odpowiedzialnymi za zgodne z prawem przetwarzanie danych osobowych są:

1. Administrator Danych Osobowych;
2. Administrator Bezpieczeństwa Informacji;
3. Administrator Systemów Informatycznych;
4. Osoby, upoważnione do przetwarzania danych osobowych w Urzędzie;

§ 4.

1. Polityka bezpieczeństwa określa środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczności danych osobowych, przetwarzanych za pomocą systemu informatycznego w Urzędzie.
2. Zasady określone w Polityce bezpieczeństwa, obowiązują wszystkich pracowników Urzędu bez względu na sposób nawiązania stosunku pracy, wymiar czasu pracy i zajmowane stanowisko.
3. Do ich przestrzegania są zobowiązane osoby, które uzyskały upoważnienie do przetwarzania danych osobowych, na podstawie innego niż zatrudnienie stosunku prawnego.
4. Osoby, o których mowa powyżej, są zobowiązane do złożenia stosownego oświadczenia, którego wzór stanowi załącznik do Polityki bezpieczeństwa.
5. Użytkownicy przed dopuszczeniem do pracy w systemach teleinformatycznych urzędu podpisują oświadczenie o zapoznaniu się z zasadami wykorzystania sprzętu teleinformatycznego.

§5

Osoby niezaangażowani bezpośrednio w procesy przetwarzania danych chronionych zaliczeni zostają do grupy podwyższonego ryzyka i nie powinni być dopuszczeni do obszarów oraz systemów mających związek z procesami przetwarzania, bez asysty osoby wyznaczonej przez Administratora Bezpieczeństwa Informacji.

§ 6

Pracownicy urzędu zobowiązani są do przestrzegania zasad ochrony fizycznej dokumentów i materiałów zawierających informacje chronione w Urzędzie Gminy, polegających na:

- przechowywaniu ich w pomieszczeniach i szafach odpornych na włamania lub zniszczenie na skutek awarii bądź klęsk żywiołowych,
- opracowywaniu ich w strefach bezpieczeństwa,
- obowiązkowego udziału w okresowo organizowanych szkoleniach.

§ 7

1. W celu zapobieżenia nadużyciom, kradzieżom informacji, nośników i innych zasobów, po zakończeniu pracy należy uporządkować swoje stanowisko i zabezpieczyć nośniki oraz dokumenty w specjalnie do tego przeznaczonych szafkach - zasada „czystego biurka".
2. Ekrany monitorów należy usytuować w ten sposób, aby uniemożliwić podgląd osobom trzecim

§ 8

W celu monitorowania incydentów i niesprawności, minimalizacji szkód z nich wynikających i wyciągania wniosków na przyszłość, istnieje:

1. obowiązek raportowania Administratorowi Bezpieczeństwa Informacji naruszeń (incydentów), zauważonych podatności i innych słabych punktów oraz przypadków błędnego działania sprzętu i oprogramowania,
2. obowiązek analizowania przez Administratora Bezpieczeństwa Informacji incydentów i popełnionych błędów, wnioskowanie w powyższych sprawach do Wójta o wyciągnięcie wniosków służbowych.

§ 9

1. Zatrudnienie w Urzędzie Gminy w Wiślicy wymaga zgłoszenia faktu zatrudnienia Administratorowi Bezpieczeństwa Informacji przez Kierownika Referatu UG, w terminie nie później niż w pierwszym dniu rozpoczęcia pracy.
2. Zgłoszenie, o którym mowa w pkt. 1, zawiera imię i nazwisko zatrudnionego, wskazanie formy i miejsca zatrudnienia oraz zakres dostępu do danych chronionych lub do systemów teleinformatycznych, jeżeli taki dostęp jest konieczny.
3. Wnioskowany zakres dostępu do danych chronionych i do systemów teleinformatycznych określa Kierownik Referatu.
4. W przypadku wnioskowania o udzielenie dostępu do systemów teleinformatycznych do zgłoszenia należy dołączyć wypełniony formularz dostępu do systemów teleinformatycznych.
5. Przed dopuszczeniem osoby do danych chronionych Administrator Bezpieczeństwa Informacji, przy udziale Administratora Systemów Informatycznych, opiniują konieczność dopuszczenia i określają zakres dostępu do danych.
6. Zgłoszenie, o którym mowa w pkt.1 podlega zatwierdzeniu przez Wójta.
7. Wszelkie zmiany w zakresie obowiązków powodujące zmianę w dostępie do danych lub systemów teleinformatycznych, lub rozwiązanie stosunku pracy, wymagają zastosowania trybu określonego w niniejszym Zarządzeniu, nie później niż 3. dni przed tym faktem.

§ 10

Użytkownicy uzyskują dostęp do systemów informatycznych po:

- zdobyciu formalnych uprawnień od właściwych przełożonych,
- odbyciu przeszkolenia,
- utworzeniu konta i przyporządkowaniu hasła dostępu zgodnie z obowiązującą procedurą określoną w Instrukcji Zarządzania Systemami Teleinformatycznymi

§ 11

Do zadań Administratora Bezpieczeństwa Informacji należy jako osoby odpowiedzialnej za ochronę i bezpieczeństwo przetwarzanych danych w tym w szczególności za przeciwdziałanie dostępowi do nich osób niepowołanych oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszenia zabezpieczeń. należy:

- analiza ryzyka i zarządzanie nim,
- opracowanie planu wdrożenia zabezpieczeń,
- opracowanie treści programów szkoleniowych i prowadzenie szkoleń, prowadzenie działań uświadamiających w urzędzie,
- nadzór nad funkcjonowaniem mechanizmów kontroli dostępu do systemu i jego urządzeń,
- opracowanie planów reakcji na incydenty, planów awaryjnych, regulaminów,
- monitorowanie skuteczności zabezpieczeń, sprawdzanie osiągnięcia celów w zakresie bezpieczeństwa,
- opracowanie Planów Zabezpieczenia Systemów w Urzędzie Gminy,
- aktualizacja dokumentów polityki, zwłaszcza wpływu nowelizacji ustaw, rozporządzeń i zawieranych umów na wymagania bezpieczeństwa określone w dokumentach polityki,
- doradztwo dla informatyków i kierownictwa urzędu,
- określanie niezbędnych zasobów (ludzkich, finansowych, wiedzy) potrzebnych do wdrożenia i utrzymania stanu bezpieczeństwa.

§ 12

Do zadań Administratora Systemów Informatycznych należy eksploatacja systemów teleinformatycznych zgodnie z polityką bezpieczeństwa. Do szczegółowych zadań należy:

- pomoc przy analizie ryzyka i zarządzaniu ryzykiem,
- monitorowanie zmian środowiska, w tym pojawiania się nowych zagrożeń,
- właściwa konfiguracja mechanizmów kontroli dostępu do systemu i jego urządzeń,
- zarządzanie konfiguracją systemów i urządzeń,
- reagowanie na incydenty w zakresie bezpieczeństwa,
- odpowiedzialność za wdrażanie zabezpieczeń,
- planowanie szkoleń i działań uświadamiających wg ustalonych programów,
- analizowanie incydentów związanych z bezpieczeństwem,

§ 13

Szczegółowe określenie zadań, o których mowa w § 3 i § 4 zawierają dodatkowe przepisy wewnętrzne, instrukcje i procedury bezpiecznej eksploatacji stanowiące załączniki do niniejszej polityki.

§ 14

Administrator Bezpieczeństwa Informacji (ABI) może przekazać Administratorowi Systemów Informatycznych dodatkowe obowiązki w formie pisemnego upoważnienia.