Załącznik nr 1 do Zarządzenia Nr 630/2018
Wójta Gminy Janów z dnia 13.07.2018r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

W URZĘDZIE GMINY JANÓW

W celu zabezpieczenia danych gromadzonych i przetwarzanych w Urzędzie Gminy Janów oraz w jego systemie informatycznym, a w szczególności w celu ochrony danych osobowych, wprowadza się określone w niniejszym dokumencie zasady bezpieczeństwa.

Mając świadomość, że żadne zabezpieczenie techniczne nie gwarantuje 100%-towej szczelności systemu, konieczne jest aby każdy pracownik pełen świadomej odpowiedzialności, postępował zgodnie z przyjętymi zasadami i minimalizował zagrożenia wynikające z ludzkich błędów.

Podstawa prawna:

1. Ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz. U. z 2018 r., poz. 926 z późn. zm.),
2. Rozporządzenie 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. Urz. UE.L.4.5.2016.119.1),
3. Rozporządzenie 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. z 2004 r. Nr 100, poz. 1024).

Definicje

Ilekroć w niniejszym dokumencie jest mowa o:

1. **Urzędzie** – należy przez to rozumieć Urząd Gminy Janów.
2. **Administratorze Danych** – należy przez to rozumieć Wójta Gminy Janów.
3. **Inspektora Ochrony Danych** – należy przez to rozumieć pracownika Urzędu lub inną osobę wyznaczoną do nadzorowania przestrzegania zasad ochrony określonych w niniejszym dokumencie oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych.
4. **Administratorze Systemu Informatycznego** – należy przez to rozumieć osobę odpowiedzialną za funkcjonowanie systemu informatycznego urzędu oraz stosowanie technicznych i organizacyjnych środków ochrony.
5. **Systemie informatycznym** – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu przetwarzania danych.
6. **Użytkowniku systemu** – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym urzędu. Użytkownikiem może być pracownik urzędu, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno – prawnej, osoba odbywająca staż w urzędzie, wolontariusz.
7. **Sieci lokalnej** – należy przez to rozumieć połączenie systemów informatycznych urzędu wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych.
8. **Sieci rozległej** – należy przez to rozumieć sieć publiczna w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2017 r., poz. 1907 z późn. zm.).
9. **Zbiorze danych** – każdy posiadający strukturę, zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
10. **Przetwarzanie danych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, ketów wykonuje się w systemach informatycznych.
11. **Zabezpieczenie danych w systemach informatycznych** – wdrożenie i eksploatacja stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

12. **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
13. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
14. **Uwierzytelnienie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
15. **Rozliczalność** – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
16. **Integralność danych** – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
17. **Poufność danych** – właściwość zapewniająca, ze dane nie są udostępniane nieupoważnionym osobom.

Polityka bezpieczeństwa określa:

1. Wykaz budynków oraz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe.
2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.
3. Opis struktury zbiorów danych wskazujących zawartości poszczególnych pól informacyjnych.
4. Sposób przepływu danych pomiędzy systemami.
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności i rozliczalności przetwarzanych danych.

Ad. 1

Obszar przetwarzania danych osobowych.

Miejscem przetwarzania danych osobowych są pomieszczenia pracy komórek organizacyjnych Urzędu Gminy Janów.

Wykaz pomieszczeń stanowiących obszar przetwarzania danych osobowych.

L. p.	Adres budynku	Określenie pomieszczeń
1.	42-253 Janów, ul. Częstochowska 1 – Urząd Gminy Janów	Gabinety od nr 1 do 18, Serwerownia, Magazyny Archiwum

Ad. 2

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

Za zbiór danych osobowych przetwarzanych w Urzędzie Gminy Janów uważa się:

1. dokumentację papierową (korespondencja, wnioski, deklaracje, itd.),
2. systemy informatyczne przetwarzania danych oraz oprogramowanie komputerowe służące do przetwarzania informacji,
3. wydruki komputerowe.

Wzór rejestru zbiorów oraz programów służących do ich przetwarzania określa załącznik nr 3 do niniejszego Zarządzenia.

Ad. 3

Opis struktury zbiorów danych osobowych oraz sposób przepływu danych pomiędzy systemami informatycznymi.

Opis struktury przetwarzanych danych osobowych oraz realizacji pomiędzy danymi, procesy przetwarzania oraz struktura danych zostały zawarte w dokumentacji technicznej systemów informatycznych dostępnej u dostawców oprogramowania informatycznego. Licencje oprogramowania stanowią prawo korzystania z systemów informatycznych.

Ad. 4

Przepływ danych pomiędzy systemami.

Systemy, w których przetwarza się dane osobowe są rozproszone i nie są ze sobą połączone, co uniemożliwia przepływ danych pomiędzy nimi.

Ad. 5

Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

A. Dane w postaci elektronicznej.

Dane przetwarzane są przy użyciu komputerów pracujących wyłącznie w wewnętrznej sieci komputerowej oddzielonej fizycznie od sieci publicznej przy pomocy bramy internetowej wyposażonej w firewall oraz programowe firewalle na stacjach roboczych, dodatkowo zabezpieczonych oprogramowaniem antywirusowym.

Dostęp do danych następuje po autoryzacji. Autoryzacja polega na podaniu identyfikatora oraz hasła przydzielonego przez Administratora danych.

Uwzględniając kategorie przetwarzanych danych wprowadza się podstawowy poziom bezpieczeństwa. Środki bezpieczeństwa na poziomie podstawowym określa instrukcja zarządzania systemem informatycznym.

B. Dane w rejestrach papierowych.

Dane przetwarzane są przy użyciu tradycyjnych środków pisarskich gromadzone są w rejestrach, księgach, zeszytach papierowych oraz segregatorach i przechowywane w zamykanych szafach.

C. Środki organizacyjne.

Powołany przez Inspektor ochrony danych (IOD) nadzoruje przestrzeganie zasady ochrony danych określonych w instrukcji zarządzania systemem informatycznym z uwzględnieniem spraw dotyczących ochrony danych osobowych przetwarzanych w tradycyjnych rejestrach.

D. Środki organizacyjne oraz środki ochrony fizycznej.

1. Wejście do budynku Urzędu Gminy Janów zabezpieczone winno być zamkami drzwiowymi oraz alarmem. Poszczególne pokoje, w których odbywa się przetwarzanie danych osobowych i ich składowanie muszą być zamykane podczas nieobecności pracownika. Odpowiedzialność za właściwą ochronę pomieszczeń ponosi pracownik oraz kierownik komórki organizacyjnej.
2. Przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osoby zatrudnionej przy przetwarzaniu danych lub w obecności Inspektora Danych Osobowych.
3. Pomieszczenia, o których mowa wyżej, zamykane są na czas nieobecności pracownika zatrudnionego przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich. Klucze do pomieszczeń służbowych znajdują się w Sekretariacie Urzędu Gminy.

Pozostawienie kluczy w zamkach pomieszczeń gdzie przetwarzane są dane osobowe jest niedopuszczalne (także podczas pobytu pracownika w pokoju).

4. W pomieszczeniach, w których przewiduje się przyjmowanie interesantów monitory stanowisk komputerowych ustawione są w sposób uniemożliwiający wgląd w przetwarzane dane.
5. Pracownicy przetwarzający dane osobowe obowiązani są do prawidłowego ich zabezpieczenia na swoich stanowiskach pracy. Przed rozpoczęciem pracy klucze pobierane zostają z zabezpieczonej gabloty pod nadzorem wyznaczonych pracowników i tam też są składowane po zakończeniu pracy.

E. Środki sprzętowe, informatyczne i telekomunikacyjne.

1. Urządzenia wchodzące w skład systemu informatycznego podłączone są do odrębnego obwodu elektrycznego, zabezpieczonego na wypadek zaniku napięcia albo awarii w sieci zasilającej listwą filtrującą oraz urządzeniem UPS.
2. Dostęp fizyczny do sieci lokalnej jest ograniczony, koncentrator umieszczony jest w specjalnie przygotowanej zamykanej szafie.
3. Dostęp logiczny do sieci lokalnej zabezpieczony jest adresem IP oraz MC – adresem karty sieciowej.
4. Dostęp do sieci WAN zabezpieczony jest Firewall-em wraz z oprogramowaniem antywirusowym.
5. Kopie awaryjne wykonywane są w cyklach:

- dzienna na dysku twardym,

- kwartalne dysku zewnętrznym.

6. Każdy dokument papierowy zawierający dane osobowe przeznaczony do wyrzucenia zostaje zniszczony w sposób uniemożliwiający jego odczytanie przy pomocy niszczarki.
7. Inne środki przetwarzania: drukarki, skanery, modemy, niszczarki dokumentów.

F. Środki ochrony w ramach oprogramowania.

1. Każda jednostka komputerowa zabezpieczona została hasłem uruchomieniowym (BIOS), hasłem wejściowym do systemu operacyjnego lub do profilu użytkownika oraz hasłem do każdej aplikacji przy pomocy, której przetwarzane są dane osobowe.
2. Zastosowano wygaszanie ekranu w przypadku dłuższej nieaktywności użytkownika.
3. Zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji.
4. Dala każdego użytkownika systemu jest ustalony odrębny identyfikator.
5. Zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (unikalny identyfikator i hasło).
6. Hasła do aplikacji zmieniane są co 30 dni.