# ZARZĄDZENIE Nr 0050/52//2018
# Wójta Gminy Lisków
# z dnia 31.08.2018r.

**w sprawie wprowadzenia „Polityki Bezpieczeństwa Informacji w Urzędzie Gminy w Liskowie"**

Na podstawie art. 30 ust. 1, art. 33 ust. 1 i 3 stawy z dnia 8 marca 1990r. o samorządzie gminnym (t. j. Dz. U. z 2018r. poz. 994 ze zm.), art. 24 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) zarządza się, co następuje:

§ **1.**Wprowadza się „Politykę Bezpieczeństwa Informacji w Urzędzie Gminy w Liskowie" stanowiącą załącznik do niniejszego zarządzenia.

§ **2.**Zobowiązuje się wszystkie osoby przetwarzające dane osobowe w Urzędzie Gminy w Liskowie do przestrzegania zasad i realizacji zadań określonych w załączniku, o którym mowa w § 1.

§ **3.** Traci moc zarządzenie nr 9/2008 Wójta Gminy Lisków z dnia 15.04.2008r. w sprawie ustalenia w Urzędzie Gminy w Liskowie instrukcji dotyczących przetwarzania danych osobowych

§ **4.** Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
Maria Krawiec

**Załącznik**
**do Zarządzenia nr 0050/52/2018**
**Wójta Gminy Lisków**
**z dnia 31.08.2018r.**

# Polityka Bezpieczeństwa Informacji w Urzędzie Gminy w Liskowie

Lisków 2018r.

## § 1.

## Część ogólna

1. Głównym celem wprowadzenia Polityki Bezpieczeństwa jest zapewnienie zgodności działania Urzędu Gminy w Liskowie z przepisami prawa regulującymi kwestię administrowania i przetwarzania danych osobowych. Niniejsza Polityka Bezpieczeństwa opisuje w szczególności zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem.
2. Polityka określa zasady przetwarzania danych osobowych oraz ich zabezpieczenia, jako zestaw praw, reguł i zaleceń, regulujących sposób i zarządzania, ochrony i dystrybucji wewnątrz Urzędu Gminy w Liskowie.
3. Polityka zawiera informacje dotyczące rozpoznawania procesów przetwarzania danych osobowych oraz wprowadzonych zabezpieczeń technicznych i organizacyjnych, zapewniających ochronę przetwarzania danych osobowych.
4. Niniejszą Politykę stosuję się do:

a) danych osobowych:

- przetwarzanych w systemach informatycznych,
- zapisanych na zewnętrznych nośnikach informacji,
- przetwarzanych tradycyjnie.

b) Informacji dotyczących bezpieczeństwa przetwarzania danych osobowych:

- służących do uwierzytelnienia w systemach informatycznych, w których są przetwarzane dane osobowe,
- dotyczących wdrożonych zabezpieczeń technicznych i organizacyjnych.

5. Bez względu na zajmowane stanowisko w Urzędzie Gminy w Liskowie, miejsce wykonywanej pracy oraz charakter stosunku pracy, zasady określone w niniejszej Polityce oraz dokumentach powiązanych powinny być znane i stosowane przez pracowników oraz w niezbędnym zakresie przez współpracowników przetwarzających dane osobowe.

## § 2.

## Definicje

Użyte w niniejszej Polityce pojęcia są wspólne dla wszystkich dokumentów powiązanych z niniejszą Polityką oraz wszystkich pozostałych dokumentów, które zostały przyjęte przez Urząd Gminy w Liskowie, w zakresie ochrony przetwarzania danych:

1. **Administrator Danych Osobowych** - Wójt Gminy Lisków.

2. **Inspektor Ochrony Danych Osobowych** – osoba wyznaczona przez ADO do nadzorowania przestrzegania zasad ochrony danych osobowych w urzędzie.
3. **Bezpieczeństwo przetwarzania danych osobowych** – zachowanie poufności, integralności i rozliczalności danych osobowych; dodatkowo mogą być brane pod uwagę inne własności, takie jak dostępność, autentyczność, niezaprzeczalność i niezawodność.
4. **Dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
5. **Naruszenie danych osobowych** – zamierzone lub przypadkowe naruszenie środków technicznych i organizacyjnych zastosowanych w celu ochrony danych osobowych. W szczególności, gdy stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie ochrony danych osobowych.
6. **Poufność** – właściwość zapewniająca, że informacja jest dostępna jedynie osobom upoważnionym.
7. **Przetwarzanie danych osobowych** – operacje lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczenie, usuwanie lub niszczenie.
8. **System informatyczny** – zespół współpracujących urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
9. **Urząd** – Urząd Gminy w Liskowie.
10. **Użytkownik systemu** – osoba upoważniona do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym, która posiada ustalony identyfikator i hasło.

## § 3
## Cel i zakres Polityki Bezpieczeństwa

1. Wprowadzenie niniejszej Polityki ma na celu określenie jednolitych zasady dla całego systemu przetwarzania danych.
2. Procesy i procedury podlegające wdrożeniu to:

1) ochrona przetwarzanych i gromadzonych informacji, w tym danych osobowych w urzędzie i dotyczy:
   a) zabezpieczenia przed dostępem do danych osób nieupoważnionych, na każdym etapie ich przetwarzania tj. wprowadzania, aktualizacji lub usuwania, wyświetlania lub drukowania zestawień i raportów, przemieszczania danych w sieci lokalnej pomiędzy programami i osobami je przetwarzającymi,
   b) metod archiwizacji oraz ochrony danych zarchiwizowanych na nośnikach zewnętrznych i wydrukach,
   c) procedur niszczenia niepotrzebnych wydruków lub nośników z danymi,
   d) ustalenia i wdrożenia zabezpieczeń przed dostępem osób niepowołanych do pomieszczeń, w których są eksploatowane urządzenia gromadzące i przetwarzające dane,
   e) określenia polityki i sposobów dostępu do tych pomieszczeń przez pracowników, personel pomocniczy oraz serwis zewnętrzny,
2) oszacowanie i zmniejszenie ryzyka utraty informacji,
3) określenia zakresu obowiązków pracowników – w części dotyczącej bezpieczeństwa danych w tym danych osobowych,
4) podnoszenie świadomości pracowników i ich pełne zaangażowanie w ochronę przetwarzanych informacji.

3. Powyższe procedury systemu teleinformatycznego, odnoszą się w szczególności do:
1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są lub będą informacje podlegające ochronie,
2) informacji będących własnością Urzędu Gminy w Liskowie lub jednostek organizacyjnych gminy, o ile zostały przekazane do urzędu na podstawie umów lub porozumień,
3) wszystkich nośników papierowych, magnetycznych lub optycznych, na których są lub będą znajdować się informacje podlegające ochronie,
4) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
5) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

§ 4.

**Obszar przetwarzania danych osobowych**

W Urzędzie Gminy w Liskowie przetwarzane są dane osobowe w następujących lokalizacjach:

1) budynek urzędu przy ul. Ks. Wacława Blizińskiego 43,
2) budynek urzędu przy ul. Ks. Wacława Blizińskiego 56.

§ 5.

**Wykaz zbiorów danych, w tym danych osobowych**

1. Dane gromadzone są w zbiorach:
   1) Ewidencja ludności Gminy Lisków,
   2) Urząd Stanu Cywilnego w Liskowie,
   3) Kadry i płace,
   4) Podatki i opłaty lokalne,
   5) Ewidencja gruntów i budynków,
   6) Akcyza paliwowa,
   7) Kwalifikacja wojskowa,
   8) Woda i ścieki,
   9) Zarządzanie nieruchomościami,
   10) System Informacji Oświatowej,
   11) Ewidencja działalności gospodarczej,
   12) Ewidencja pracowników,
   13) Budownictwo,
   14) Zezwolenia na sprzedaż i podawanie napojów alkoholowych,
   15) Obrona cywilna,
   16) Przelewy bankowe,
   17) Rejestr korespondencji przychodzącej,
   18) Oświadczenia majątkowe,
   19) Poczta elektroniczna,
   20) Ewidencja skarg i wniosków,
   21) Wycinka drzew i krzewów.
2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych stanowi załącznik Nr 7 do niniejszej polityki.

§ 6.

**Obowiązki i odpowiedzialność Administratora Ochrony Danych Osobowych**

Do obowiązków Administratora Ochrony danych Osobowych należy w szczególności:

1) Organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami RODO oraz innych przepisów regulujących zasady bezpieczeństwa i ochrony danych osobowych.
2) Zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki Bezpieczeństwa.
3) Wydawanie i anulowanie upoważnień do przetwarzania danych osobowych.
4) Zapewnienie szkoleń użytkowników przed dopuszczeniem do pracy na zbiorach i w systemach informatycznych przetwarzających dane osobowe.
5) Prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych.
6) Nadzór nad bezpieczeństwem danych osobowych.
7) Kontrola działań pracowników pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych.
8) Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych.
9) Powołanie Inspektora Ochrony Danych, który jest odpowiedzialny za nadzór nad stosowaniem środków organizacyjnych i technicznych, zapewniający ochronę przetwarzanych danych, w szczególności przed ich udostępnieniem osobom nieupoważnionym, przetwarzaniem z naruszeniem ustawy, uszkodzeniem lub zniszczeniem.

§ 7.

**Obowiązki i odpowiedzialność Inspektora Ochrony Danych**

1. Inspektor Ochrony Danych powinien:

1) posiadać pełną zdolność do czynności prawnych oraz korzystać z pełni praw publicznych,
2) posiadać fachową wiedzę na temat prawa i praktyk w dziedzinie ochrony danych osobowych oraz umiejętności wypełniania zadań, o których mowa w art. 39 RODO, ustawie i aktach prawa wewnętrznego,
3) wykonywać zadania niezależnie i bez konfliktu interesów,
4) posiadać wiedzę na temat systemów informatycznych służących do przetwarzania, a także potrzeb i sposobów zabezpieczania danych osobowych przetwarzanych i nie może być karany za przestępstwo popełnione z winy umyślnej.

2. Obowiązki Inspektora Ochrony Danych:

1) Inspektor danych Osobowych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań,
2) informowanie Administratora oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy powszechnie obowiązujących przepisów prawa oraz aktów prawa wewnętrznego w zakresie ochrony danych osobowych i doradzanie im w tej sprawie,
3) nadzorowanie i monitorowanie przestrzegania przepisów prawa o ochronie danych oraz aktów prawa wewnętrznego w dziedzinie ochrony danych osobowych,
4) weryfikacja zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie raz w roku sprawozdania dla Administratora,
5) opracowanie i aktualizacja Polityki Bezpieczeństwa Danych Osobowych oraz dokumentacji związanej z przetwarzaniem danych osobowych
6) informowanie Administratora o wystąpieniu incydentu,
7) przygotowanie wzoru klauzuli informacyjnej,
8) przygotowanie upoważnień do przetwarzanie danych osobowych,
9) prowadzenie ewidencji upoważnień do przetwarzania danych osobowych.

## § 8.

## Uprawnienia do przetwarzania danych

1. Pracownik może przetwarzać dane, tylko i wyłącznie w sytuacji, gdy:
1) posiada pisemne upoważnienie do przetwarzania danych osobowych (chyba, że chodzi o usunięcie danych); (wzór upoważnienia stanowi zał. Nr 6 do niniejszej polityki)
2) jest umieszczony w Ewidencji Osób Upoważnionych do przetwarzania danych;
3) w celu i zakresie wskazanym w upoważnieniu;
4) przez okres na jaki upoważnienie zostało udzielone;
5) jest to niezbędnie do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa;
6) jest to konieczne do realizacji umowy, gdy osoba , której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą;
7) jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego;

8) niezbędne do wypełniania prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

2. Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana przestrzegać następujących zasad:
   1) przed rozpoczęciem przetwarzania należy złożyć oświadczenie o zapoznaniu się z dokumentacją ochrony danych osobowych, (wzór oświadczenia stanowi zał. Nr 5 do niniejszej polityki)
   2) przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia, a także po ustaniu stosunku pracy lub odwołania z pełnionej funkcji, przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres realizacji umowy, a także po zakończeniu jej realizacji,
   3) stosowanie określonych przez Administratora procedur oraz wytycznych mających na celu przetwarzanie danych zgodnie z obowiązującym prawem,
   4) zabezpieczenie danych osobowych przed udostępnieniem osobom nieupoważnionych,
   5) w aktach osobowych pracownika przechowuje się egzemplarz oryginalny upoważnienia do przetwarzania danych osobowych podpisany własnoręcznie przez pracownika, co jednocześnie jest potwierdzeniem, że pracownik przyjął treść upoważnienia do wiadomości,
   6) w przypadku naruszenia przez pracownika przepisów lub zasad postępowania może podlegać on odpowiedzialności służbowej lub karnej,
   7) upoważnienia do przetwarzania danych osobowych udzielane są również wolontariuszom, praktykantom, stażystom, zakończenie stażu, praktyki, wolontariatu powoduje wygaśnięcie upoważnienia.

## § 9.

## Informowanie o przetwarzanych danych osobowych

1. Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych osobowych przetwarzanych i przechowywanych w Urzędzie Gminy w Liskowie, a zwłaszcza do uzyskania informacji o przetwarzanych danych osobowych, które jej dotyczą.

2. Na wniosek osoby, której dane dotyczą, Administrator Danych jest zobowiązany do udzielania informacji zgodnie z pkt. 1). Informacja powinna być udzielona w formie pisemnej oraz powszechnie zrozumiałej.

3. Osoba, której dane dotyczą, ma prawo wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach przetwarzania niezbędnego do wykonania określonych prawem zadań realizowanych dla dobra publicznego lub niezbędnego dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazania jej danych osobowych innemu administratorowi danych.

## § 10
## Powierzanie przetwarzania danych osobowych

1. Administrator:
   a) przekazuje dane do podmiotów trzecich zgodnie z przepisami prawa powszechnie obowiązującego, w szczególności do: Zakładu Ubezpieczeń Społecznych, Urzędu Skarbowego, Państwowej Inspekcji Pracy, sądów powszechnych, policji i prokuratury, etc.,
   b) powierza przetwarzanie danych osobowych innemu podmiotowi w drodze umowy zawartej na piśnie, która określa zasady przetwarzania i zabezpieczenia danych osobowych.
2. Umowa powierzenia danych osobowych do przetwarzania musi być zawarta w formie pisemnej w dwóch jednobrzmiących egzemplarzach dla obu stron.
3. W przypadku zawarcia umowy powierzenia przetwarzania danych osobowych z podmiotem trzecim, ADO jednocześnie zobowiązuje ten podmiot w formie pisemnej do zachowania poufności powierzanych do przetwarzania danych osobowych oraz sposobów ich zabezpieczeń. Zobowiązanie powinna pozostać w mocy również po zakończeniu przetwarzania.
4. Podmiot, któremu powierzono przetwarzanie danych osobowych, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.
5. Podmiot, któremu powierzono przetwarzanie danych osobowych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie ryzyka dla danych objętych ochroną, a szczególności powinien stosować techniczne i organizacyjne środki bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

## § 11.

### Przekazanie danych do państwa trzeciego lub organizacji międzynarodowej

1. Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić, gdy Komisja Europejska stwierdzi, że to państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Takie przekazywanie nie wymaga specjalnego zezwolenia.
2. W razie braku decyzji, o której mowa w pkt. 1 Administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego lub organizacji międzynarodowej wyłącznie, gdy zapewnią odpowiednie zabezpieczenia, i pod warunkiem, że obowiązują egzekwowane prawa osób, których dane dotyczą i skuteczne środki ochrony prawnej.
3. W razie braku decyzji stwierdzającej odpowiedni stopień ochrony określonej w pkt. 1 oraz braku odpowiednich zabezpieczeń, o których mowa w pkt. 2 , jednorazowe lub wielokrotne przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej mogą nastąpić wyłącznie pod warunkiem, że:
    a) osoba, której dane dotyczą, poinformowała o ewentualnym ryzyku, z którymi – ze względu na brak decyzji stwierdzającej odpowiedni stopień ochrony oraz na brak odpowiednich zabezpieczeń – może się dla niej wiązać proponowane przekazanie, wyraźnie wyraziła na nie zgodę,
    b) przekazanie jest niezbędne ze względu na ważne względy interesu publicznego,
    c) przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń,
    d) szczegółowe zasady przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej określone zostały w RODO. O wyrazenie zgody na przekazanie danych występuje właściciel zbioru, wskazując cel i zakres przekazywanych danych. Zgodę na ich przekazywanie do państwa trzeciego lub organizacji międzynarodowej może wydać kierownik jednostki organizacyjnej po zasięgnięciu opinii Inspektora Ochrony Danych. Administrator zobowiązany jest bezwzględnie przestrzegać postanowień RODO przy przekazywaniu danych do państwa trzeciego lub organizacji międzynarodowej.

## § 12.

## Postępowanie w sytuacji naruszenia bezpieczeństwa danych osobowych

1. Każdy użytkownik w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest o tym fakcie natychmiast poinformować ADO.
2. W przypadku stwierdzenia wystąpienia zagrożenia, ADO prowadzi postępowanie wyjaśniające w toku którego:
   a) informuje o tym fakcie IODO,
   b) ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,
   c) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,
   d) zabezpiecza ewentualne dowody,
   e) ustala osoby odpowiedzialne za naruszenie,
   f) podejmuje działania naprawcze,
   g) inicjuje działania dyscyplinarne,
   h) wyciąga wnioski i rekomenduje działania korygujące oraz prewencyjne zmierzające do eliminacji podobnych incydentów w przyszłości.
3. Rejestr naruszeń prowadzi IODO
4. Wzór rejestru naruszeń stanowi załącznik Nr 1 do niniejszej Polityki Bezpieczeństwa Informacji.

## § 13.

## Zasady bezpiecznego użytkowania sprzętu IT, dysków, programów

1. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT, zobowiązany jest do jego ochrony przed jakimkolwiek zniszczeniem lub uszkodzeniem. Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy.
2. Użytkownik ma obowiązek natychmiast zgłosić zagubienie, utratę lub zniszczenie powierzonego mu sprzętu IT.
3. Samowolne otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urzadzeń (np. twardych dysków, pamięci) lub podłączenie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.
4. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym wgląd do danych wyświetlanych na monitorach komputerowych.

5. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszać ekranu lub wylogować się z systemu bądź z programu.
6. Po zakończeniu pracy , użytkownik zobowiązany jest:
    a) wylogować się z systemu informatycznego, a jeśli to wymagane- następnie wyłączyć komputer,
    b) zabezpieczyć stanowisko pracy, w szczególności wszelkie nośniki magnetyczne i optyczne na których znajdują się dane osobowe.
7. Użytkownik jest zobowiązany do usuwania plików z nośników/dysków, do których mają dostęp inni użytkownicy nieupoważnieni do dostępu do takich plików.
8. Jeśli użytkownik jest upoważniony do niszczenia nosników, powinien trwale zniszczyć sam nośnik lub trwale usunąć z niego dane, np. zniszczenie płyt DVD w niszczarce, zniszczenie twardego dysku, pendrive młotkiem.

**§ 14.**

**Zarządzanie uprawnieniami – procedura rozpoczęcia, zawieszenia i zakończenia pracy**

1) Każdy użytkownik z dostępem do danych osobowych (np. na swoim komputerze, na dysku sieciowym, w programie lub aplikacji, w poczcie elektronicznej) musi posiadać swój własny indywidualny identyfikator (login) do logowania się.
2) Użytkownik otrzymuje dostęp i odpowiednie uprawnienia do zasobów i aplikacji na polecenie przełożonych i przy realizacji informatyka.
3) Użytkownika obowiązuje zasada pracy na własnym koncie. Zabronione jest zatem umożliwianie innym osobom pracy na koncie innego użytkownika.
4) Użytkownik jest zobowiązany do powiadomienia informatyka o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.
5) Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym wglądu do danych wyświetlanych na monitorach, tzw. Polityka czystego ekranu.
6) Zabrania się uruchamiania jakiejkolwiek aplikacji lub programu na prośbę innej osoby, o ile nie została ona zweryfikowana przez informatyka. Dotyczy to zwłaszcza programów przesłanych za pomocą poczty elektronicznej lub wskazanych w formie odnośnika internetowego.
7) Po zakończeniu pracy, użytkownik zobowiązany jest:
    a) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,

b) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nosniki na których znajdują się dane osobowe.

## § 15
## Polityka haseł

1. Hasła powinny składać się z minimum 8 znaków.
2. Hasła powinny zawierać duże litery + małe litery + cyfry (lub znaki specjalne).
3. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów.
4. Hasła nie powinny być ujawniane innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie.
5. W przypadku ujawnienia hasła – należy natychmiast go zmienić.
6. Użytkownik systemu w trakcie pracy może zmienić swoje hasło do systemu.
7. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
8. Zabrania się używania w serwisach internetowych takich samych lub podobnych haseł jak w systemach komputerowych.
9. Zabrania się stosowania tego samego hasła jako zabezpieczenia w dostępie do różnych systemów.

## § 16.
## Zabezpieczenie dokumentacji papierowej z danymi osobowymi

1. Upoważnieni pracownicy są zobowiązani do stosowania tzw. „Polityki czystego biurka". Polega ona na zabezpieczaniu (zamykaniu) dokumentów, np. w szafkach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.
2. Upoważnieni pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach lub utylizacji ich w specjalnych bezpiecznych pojemnikach z przeznaczeniem do bezpiecznej utylizacji.
3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach.
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik.

## § 17.

## Zasady wynoszenia nośników z danymi poza urzędem

1. Użytkownicy nie mogą wynosić za zewnątrz organizacji wymiennych elektronicznych nośników informacji zapisanymi danymi osobowymi bez zgody pracodawcy. Do takich nośników zaliczy się: wymienne twarde dyski, płyty CD, DVD, pendrive.
2. W przypadku, gdy dokumenty przewozi pracownik, zobowiązany jest do zabezpieczenia przewożonych dokumentów przed zagubieniem lub kradzieżą.

## § 18.

## Zasady korzystania z Internetu

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera uruchamiania jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
4. Nie należy w opcjach przeglądarki internetowej włączyć opcji autouzupełniania formularzy i zapamiętywania haseł.
5. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą ''https". Dla pewności należy ''kliknąć" na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.

## § 19.

## Zasady korzystania z poczty elektronicznej

1. Przesyłanie danych osobowych z użyciem maila poza jednostkę może odbywać się tylko przez osoby do tego upoważnione.
2. W przypadku przesyłania danych osobowych poza jednostkę należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych dokumentów lub plików zzipowanych, podpis elektroniczny).
3. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu
4. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.

5. Nie należy otwierać załączników (plików) w mailach nawet rzekomo znanych nam nadawców bez weryfikacji tegoż nadawcy.
6. Należy zgłaszać informatykowi przypadki podejrzanych emaili.
7. Użytkownicy nie powinni rozsyłać maili zawierających załączniki o dużym rozmiarze.
8. Użytkownicy powinni okresowo kasować niepotrzebne maile.
9. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.
10. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.
11. Użytkownicy maja prawo korzystać z poczty mailowej do celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.

**§ 20.**

**Środki ochrony fizycznej**

1. Wszystkie pomieszczenia (biura), w których znajdują się zbiory danych osobowych, są zamykane na klucz, a dostęp do nich odbywa się wyłącznie w obecności pracowników.

**§ 21.**

**Sprawozdanie roczne z funkcjonowania systemu ochrony danych**

1) Corocznie do dnia 31 grudnia IOD przygotowuje sprawozdanie roczne z funkcjonowania systemu ochrony danych i przekazuje do Administratora.
2) Sprawozdanie przygotowane jest w formie pisemnej.

**§ 22.**

**Postanowienia końcowe**

1. Niniejsza Polityka powinna być aktualizowana wraz z zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz zmianami faktycznymi w ramach funkcjonowania Urzędu Gminy w Liskowie, które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne.
2. ADO ma obowiązek zapoznać z treścią Polityki każdego Użytkownika.
3. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce.
4. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami można wszcząć postępowanie dyscyplinarne.

5. Karna dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z RODO oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
6. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy RODO.

## § 23
## Obowiązywanie dokumentu

Polityka Bezpieczeństwa wchodzi w życie z dniem 31.08.2018r. i obowiązuje na wszystkich stanowiskach oraz obszarach gdzie dochodzi do przetwarzania informacji podlegających ochronie

**Zbiór załączników:**

Załącznik Nr 1 – Rejestr naruszeń ochrony danych osobowych

Załącznik Nr 2 – Wykaz miejsc przetwarzania danych

Załącznik Nr 3 – Rejestr osób upoważnionych do przetwarzania danych osobowych

Załącznik Nr 4 – Zgłoszenie w sprawie naruszenia ochrony danych osobowych

Załącznik Nr 5 – Oświadczenia

Załącznik Nr 6 – Upoważnienie do przetwarzania danych osobowych

Załącznik Nr 7 - Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

**Załącznik Nr 1**
**Do Polityki Bezpieczeństwa Informacji**
**w Urzędzie Gminy w Liskowie**

# REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

Na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i wsprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

Administrator: Wójt Gminy Lisków
Inspektor Ochrony Danych: Ewa Błaszczyk

| Lp. | Rodzaj naruszenia | Data naruszenia | Opis okoliczności | Możliwe skutki naruszenia | Podjęte działania w celu zminimalizowania możliwych skutków naruszenia | Zgłoszenie do prezesa Urzędu Ochrony Danych |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

**Załącznik Nr 2**
**Do Polityki Bezpieczeństwa Informacji**
**w Urzędzie Gminy w Liskowie**

# Wykaz miejsc przetwarzania danych

| Lp. | Nazwa pomieszczeń | Adres |
|---|---|---|
| 1. | | |
| 2. | | |
| 3. | | |
| 4. | | |
| 5. | | |
| 6. | | |
| 7. | | |
| 8. | | |
| 9. | | |
| 10. | | |
| 11. | | |
| 12. | | |
| 13. | | |
| 14. | | |

.....

(podpis ADO)

**Załącznik Nr 3**
**Do Polityki Bezpieczeństwa Informacji**
**w Urzędzie Gminy w Liskowie**

# REJESTR OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. U. UE.L.2016.119.1), Administrator Danych Osobowych udziela upoważnienia do przetwarzania danych osobowych osobom:

| NR UPOWAŻNIENIA | IMIĘ I NAZWISKO | NR ZBIORU | ZMIANY I PRZYCZYNY WYGASNIĘCIA UPOWAŻNIENIA |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

.....

(podpis ADO)

**Załącznik Nr 4**
**Do Polityki Bezpieczeństwa Informacji**
**w Urzędzie Gminy w Liskowie**

# ZGŁOSZENIE W SPRAWIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Na podstawie art. 30 Rozporządzenia Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

Administrator: Wójt Gminy Lisków
Inspektor Ochrony Danych: Ewa Błaszczyk

Zgłoszenie dotyczy danych ze zbioru: .....

Zgłaszający: .....

Data zgłoszenia: .....

| | | |
|---|---|---|
| 1. | Charakter naruszenia | |
| 2. | Kategoria i liczba osób, których dane dotyczą | |
| 3. | Możliwe skutki naruszenia | |
| 4. | Podjęte działania w celu zminimalizowania możliwych skutków naruszenia | |
| 5. | Data wpisania do rejestru naruszeń i nr w rejestrze | |

**Załącznik Nr 5**
**Do Polityki Bezpieczeństwa Informacji**
**w Urzędzie Gminy w Liskowie**

Lisków, .....

# OŚWIADCZENIE

Oświadczam, że zapoznałem/am się z treścią Zarządzenia Wójta Gminy Lisków w sprawie wprowadzenie Polityki Bezpieczeństwa Informacji w Urzędzie Gminy w Liskowie z dnia .....
Zobowiązuje się przestrzegać zawartych w nich zapisów oraz informować o każdym naruszeniu zasad ochrony danych osobowych Administratora Danych Osobowych Urzędu Gminy w Liskowie.

.....
(podpis)

**Załącznik Nr 6**
**Do Polityki Bezpieczeństwa Informacji**
**w Urzędzie Gminy w Liskowie**

Lisków, dn. .....

# UPOWAŻNIENIE NR ...../.....
# DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. U. UE.L.2016.119.1) upoważniam Pana/ią:

.....

pracownika Urzędu Gminy w Liskowie na stanowisku:

.....

**do przetwarzania danych osobowych**

w Urzędzie Gminy w Liskowie w celach i zakresie związanym z wykonywaniem obowiązków służbowych.

Okres trwania upoważnienia od dnia wydania do momentu rozwiązania lub wygaśnięcia stosunku pracy.

Osoba upoważniona do przetwarzania danych objętym zakresem, o którym mowa wyżej jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia, oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

.....
(podpis ADO)

.....
(podpis pracownika)

**Załącznik Nr 7**
**Do Polityki Bezpieczeństwa Informacji**
**w Urzędzie Gminy w Liskowie**

# WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

| Lp. | Nazwa zbioru | Sposób gromadzenia | Nazwa programu |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |