Zarządzenie Nr 127/16
Wójta Gminy Dolice
z dnia 07 czerwca 2016r.

w sprawie ustalenia polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Dolicach

Na podstawie § 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. z 2004r. Nr 100. Poz. 1024), zarządzam, co następuje:

§ 1

Ustalam „Politykę bezpieczeństwa oraz instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy w Dolicach" zwaną dalej „Polityką bezpieczeństwa", która stanowi załącznik do niniejszego zarządzenia.

§ 2

Zobowiązuje się pracowników Urzędu Gminy Dolice do stosowania zasad określonych w „Polityce bezpieczeństwa" .

§ 3

Wykonanie zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§ 4

Uchyla się zarządzenia wójta Gminy Dolice Nr 118a/10 z dnia 02.12.2010r., Nr 31a/11 z dnia 23.05.2011r., Nr 52 /B/11 z dnia29.08.2011r.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT GMINY
Grzegorz Brodowski

URZĄD GMINY
ul. Ogrodowa 16, 73-115 DOLICE
woj. zachodniopomorskie
tel. centr. (91) 5640 129
tel./fax: (91) 5640 237

POLITYKA BEZPIECZEŃSTWA I INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI SŁUŻĄCYMI DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE GMINY W DOLICACH

Część I

1. Wstęp

1.1. Cel opracowania dokumentu „Polityka Bezpieczeństwa przetwarzania danych osobowych".

Pierwsze gwarancje ochrony danych osobowych zapewniły przepisy art. 47 oraz art. 51 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997r. Aktem prawnym konkretyzującym konstytucyjne gwarancje ochrony danych osobowych jest ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997r. ze zm. która zawiera regulacje prawne dotyczące tworzenia i posługiwania się zbiorami danych osobowych, a także pojedynczymi danymi, mające na celu administracyjno – prawną ochronę prawa do prywatności.

Dokument „Polityka bezpieczeństwa" oraz „Instrukcja zarządzania systemem informatycznym" jest zestawem praw, reguł i praktycznych wskazówek ochrony i dystrybucji danych osobowych w Urzędzie Gminy Dolice. Określa sposób prowadzenia dokumentacji związanej z przetwarzanymi zbiorami danych, ponadto określa środki techniczne i organizacyjne zastosowane do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Polityka bezpieczeństwa jest zbiorem reguł określającym dopuszczalne granice zachowania się wszystkich użytkowników systemów informatycznych. Polityka bezpieczeństwa zawiera instrukcje postępowania w sytuacji naruszenia ochrony danych osobowych oraz konsekwencje jakie mogą ponieść osoby naruszające przepisy. Polityka bezpieczeństwa odnosi się całościowo do problemu zabezpieczenia danych przetwarzanych w formie tradycyjnej (papierowej), jak i danych przetwarzanych w systemach informatycznych urzędzie. Wskazuje działania, zasady i reguły postępowania, które należy stosować, aby właściwie zabezpieczyć dane osobowe.

Ochrona przetwarzania danych osobowych obowiązuje wszystkich pracowników, którzy mają dostęp do przetwarzania informacji bez względu na zajmowane stanowisko oraz miejsce wykonywania pracy, jak również charakter stosunku pracy.

Pracownicy mający dostęp do danych osobowych są zobligowani do stosowania niezbędnych środków zapobiegających ujawnieniu tych danych osobom nieupoważnionym.

Każda osoba mająca dostęp do danych osobowych z upoważnienia Administratora Danych została zapoznana z polityką bezpieczeństwa i zobowiązania do jej przestrzegania. Osoby, o których mowa, złożyły pisemne oświadczenie (wg wzoru stanowiącego załącznik nr 4 do niniejszego dokumentu) o zapoznaniu się z przepisami ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych, Polityką bezpieczeństwa oraz Instrukcją zarządzania systemem informatycznym obowiązującą w Urzędzie oraz zobowiązały się do przestrzegania zawartych w nich postanowień.

Przestrzeganie zasad niniejszej Polityki bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym obowiązują wszystkich pracowników oraz osób przetwarzających dane osobowe.

1.2. Podstawa prawna

Art. 39a ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tj.: Dz. U. z 2015r., poz 2135 z późn. zm.), zwanej dalej „ustawą" oraz § 3 ust. 1 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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. 2004. 100, poz. 1024).

1.3. Słownik pojęć

Ilekroć w niniejszym dokumencie jest mowa o:
1) **urzędzie** – rozumie się Urząd Gminy Dolice,

2) **Generalny Inspektor Ochrony Danych Osobowych** („GIODO") – organ do spraw ochrony danych osobowych.

3) **ustawie** – rozumie się przez to ustawę z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2015r., poz. 2135 z późn. zm.) zwana dalej „ustawą".

4) **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny, jeden lub kilka specyficznych czynników określających jej cechy. Do danych osobowych zalicza się więc nie tylko imię, nazwisko i adres, ale również przypisane jej numery, dane o cechach fizjologicznych, umysłowych, ekonomicznych, kulturowych i społecznych.
5) **dane wrażliwe –** dane o pochodzeniu rasowym lub etnicznym, poglądach politycznych, przekonaniach religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących wyroków skazujących, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym

6) **przetwarzaniu danych** – operacje wykonywane na danych osobowych, tj. zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.

7) **zbiór danych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

8) **systemie informatycznym** – zespół współpracujących ze sobą urządzeń, programów, aplikacji, procedur wewnętrznego przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

9) **zabezpieczeniu danych w systemie informatycznym** – wdrożenie i eksploatacja stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnioną modyfikacją, zniszczeniem, dostępem, ujawnieniem lub utratą.

10) **usuwaniem danych osobowych** – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby której dotyczą

11) **Administrator Danych („ADO") –** organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych. Funkcje Administratora Danych Osobowych w urzędzie pełni Wójt Gminy Dolice.

12) **Administrator Bezpieczeństwa Informacji („ABI")** - wyznaczona przez Administratora Danych – osoba nadzorująca stosowanie środków technicznych

i organizacyjnych przetwarzanych danych osobowych, odpowiednich do zagrożeń oraz kategorii danych objętych ochroną.

13) **Administratorze Systemów Informatycznych („ASI")** – osoba odpowiedzialna za stosowanie technicznych i organizacyjnych środków ochrony danych osobowych w urzędzie.

14) **Zgoda 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 z oświadczenia woli o innej treści. Zgoda może być odwołana w każdym czasie.

15) **Osoba upoważniona** – osoba posiadająca wydane przez Administratora Danych Osobowych upoważnienie do przetwarzania danych osobowych w UG Dolice.

16) **użytkowniku systemu** – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym urzędu. Użytkownikiem może być pracownik, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno – prawnej, także osoba odbywająca praktykę lub staż w urzędzie

17) **Identyfikatorze użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym

18) **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie upoważnionej do pracy w systemie informatycznym. Hasło powinno zawierać 8 znaków.

19) **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

20) sieci lokalnej (LAN) – należy przez to rozumieć połączenie systemów informatycznych urzędu wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych

21) sieci rozległej – publicznej (WAN) – należy przez to rozumieć sieć publiczną w rozumieniu ustawy „prawo telekomunikacyjne".

Część II

1. Zasady przetwarzania i ochrony danych osobowych.

1.1. Dekalog ochrony danych osobowych

1. Dane osobowe, a w szczególności imiona i nazwiska, numery PESEL, serie i numery dowodów osobistych, numery telefonów, zdjęcia osób, nagrania z monitoringu, jak i wszelkie inne dane pozwalające zidentyfikować osobę fizyczną muszą być chronione przed dostępem osób nieupoważnionych.
2. Zabronione jest zapisywanie danych osobowych w inny sposób lub innej formie niż to wynika z zakresu obowiązków na zajmowanym stanowisku.
3. Zabrania się pobierania od osób fizycznych dokumentów tożsamości, takich jak dowód osobisty, prawo jazdy, paszport lub jakichkolwiek innych urzędowych dokumentów osobistych. Dokumenty te mogą być przedstawiane jedynie do wglądu i właściciel dokumentu tożsamości nie może tracić go z oczu.
4. Zabrania się udostępniania osobom nieupoważnionym danych osobowych, w szczególności faktur, umów, korespondencji reklamacyjnej, zamówień, jak i wszelkich innych nośników zawierających dane osobowe.

5. Zabrania się pozostawiania bez nadzoru osób upoważnionych ww. nośników danych osobowych, w szczególnie w publicznie dostępnych miejscach, do których może mieć dostęp osoba nieupoważniona, chyba że są one zabezpieczone fizycznie (pod kluczem).
6. Zabrania się ujawniania w miejscach publicznych danych osobowych, poprzez rozmowy (w tym telefoniczne), wezwania głosowe lub inne formy werbalnego ujawnienia danych identyfikujących osoby fizyczne.
7. Należy chronić szczególnie tzw. dane osobowe wrażliwe, tj. informacje o stanie zdrowia, nałogach, życiu seksualnym, wyrokach skazujących lub innych orzeczeniach sądowych (w tym również o mandatach karnych, jak i kwestionariuszach osobowych CV).
8. W przypadku kradzieży lub podejrzenia ujawnienia danych osobowych osobie nieupoważnionej należy niezwłocznie powiadomić przełożonego.
9. Wszelkie dane osobowe przetwarzane na zajmowanych stanowiskach stanowią własność Pracodawcy/Zleceniobiorcy, klientów lub podmiotów współpracujących i muszą być przekazywane osobom, których dane te dotyczą, na każde ich wezwanie. W razie wątpliwości należy skontaktować się z ABI.
10. Nieprzestrzeganie powyższych obowiązków może być potraktowane przez Pracodawcę/Zleceniobiorcę jako ciężkie naruszenie postanowień umownych i prowadzić do natychmiastowego rozwiązania stosunku umownego, dochodzenia rekompensaty za poniesione straty, jak również zgłoszenia zawiadomienia o podejrzeniu popełnienia czynu zabronionego zgodnie z przepisami karnymi do ustawy o ochronie danych osobowych.

1.2. Obowiązki informacyjne o przetwarzaniu danych

- Zbieranie danych osobowych od osób, których dane dotyczą

W przypadku zbierania danych od osoby, której dane dotyczą Administrator Danych jest zobowiązany poinformować tę osobę o: - adresie swojej siedziby i pełnej nazwie, - celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych, - prawie dostępu do treści swoich danych oraz ich poprawiania, - dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej. Podanych wyżej zasad nie stosuje się, jeżeli przepis innej ustawy zezwala na przetwarzanie danych bez ujawnienia faktycznego celu ich zbierania lub jeżeli osoba, której dane dotyczą, posiada już te informacje.

- Zbieranie danych osobowych nie od osób, których dane dotyczą

W przypadku zbierania danych nie od osoby, której te dane dotyczą Administrator Danych zobowiązany jest poinformować osobę bezpośrednio po utrwaleniu danych o: - adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku, - celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych, - źródle danych, - prawie dostępu do treści swoich danych oraz ich poprawiania, - prawie wniesienia, pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację, - prawie wniesienia sprzeciwu wobec przetwarzania jej danych w przypadku, gdy Administrator Danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych innemu administratorowi danych.

Podanych wyżej zasad **NIE STOSUJE SIĘ**, jeżeli: - dane są przetwarzane przez Administratora Danych na podstawie przepisów prawa,

- przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą , - dane te są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badań opinii publicznej, ich przetwarzanie nie narusza praw lub wolności osoby, której dane dotyczą, a spełnienie obowiązku informacyjnego wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu badania.

1.3. Upoważnienie do przetwarzania danych osobowych

Do przetwarzania danych osobowych w Urzędzie Gminy Dolice mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania danych osobowych wydane przez Administratora Danych Osobowych Wójta Gminy Dolice. (Załącznik nr 1)

1.4. Udostępnianie danych oraz powierzenie przetwarzanych danych

Udostępnianie danych

Najważniejsze przesłanki i zasady udostępniania danych:

- nie jest istotne czy udostępnianie danych ma charakter odpłatny czy nie, aby czynność była uznana za udostępnianie,

- nie ma znaczenia (ujmując problem technicznie) czy udostępnianie następuje w formie przekazu ustnego, pisemnego, za pomocą powszechnych środków przekazu lub poprzez sieć komputerową itd.,

- udostępnianie danych osobowych osobom lub podmiotom uprawnionym do ich otrzymania odbywa się na mocy przepisów prawa,

- dane osobowe, z wyłączeniem danych wrażliwych mogą być udostępniane nie w oparciu o przepisy prawa, jeżeli osoba wnioskująca w sposób wiarygodny uzasadni potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą,

- dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazać ich zakres i przeznaczenie.

- udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione

Powierzenie przetwarzania danych

W przypadku konieczności przetwarzania danych osobowych przez odrębne podmioty świadczące usługi dla Administratora Danych może on powierzyć ich przetwarzanie, w drodze umowy zawartej na piśmie, pod następującymi warunkami: - umowa powinna być zawarta niezależnie od posiadanej umowy określającej relacje obu stron, - podmiot, któremu powierzono przetwarzanie danych, może przetwarzać je wyłącznie w zakresie i celu przewidzianych w umowie. (Załącznik Nr 2)

- podmiot, któremu powierzono przetwarzanie danych, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art.

36-39 ustawy oraz spełnić wymagania określone w przepisach o których mowa w art. 39a ustawy.

W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych.

- odpowiedzialność za przestrzeganie przepisów niniejszej ustawy spoczywa na Administratorze Danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodne z tą umową.

W przypadku konieczności dostępu do obszaru przetwarzania osób, nieposiadających upoważnienia, o jaki mowa w pkt 1.2, które muszą dokonać doraźnych prac o charakterze serwisowym lub innym, podpisują oni oświadczenie o zachowaniu poufności. (Załącznik Nr 3)

Na wniosek osoby, której dane dotyczą, administrator danych jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić, odnośnie do jej danych osobowych, informacji, o których mowa w art. 32 ust. 1 pkt 1-5a ustawy o ochronie danych osobowych. Wniosek składany jest pisemnie. Załącznik Nr 6

Na wniosek osoby, której dane dotyczą, powyższych informacji udziela się na piśmie.

Część III

1. Środki organizacyjne i techniczne zastosowane do zapewnienia ochrony przetwarzanych danych w Urzędzie Gminy Dolice

1.1. Środki organizacyjne ochrony danych osobowych stosowane w urzędzie w celu stworzenia właściwych zabezpieczeń, które powinny bezpośrednio oddziaływać na procesy przetwarzania danych wprowadza się następujące środki organizacyjne:

- przetwarzanie danych osobowych w urzędzie może odbywać się wyłącznie w ramach wykonywania zadań służbowych. Zakres uprawnień wynika z zakresu tych zadań,

- do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne upoważnienie,

Dostęp zarówno do budynków, pomieszczeń jak i do urządzeń przetwarzających dane osobowe powinny mieć wyłącznie osoby uprawnione do tego.

- dane osobowe powinny być wyłącznie przetwarzane w budynkach, pomieszczeniach do tego przystosowanych i zabezpieczonych, przez osoby upoważnione przez Administratora Danych Osobowych.

- zbiory danych (bazy danych) w których dokonuje się przetwarzania danych osobowych powinny być zabezpieczone przed nieuprawnionym dostępem i zewidencjonowane w wykazie zbiorów danych osobowych, który prowadzi Administrator Bezpieczeństwa Informacji („ABI") do niniejszego dokumentu. Załącznik nr 9

- każdy pracownik urzędu co najmniej raz na dwa lata musi odbyć szkolenie z zakresu ochrony danych osobowych. Nowo przyjęty pracownik obowiązkowo odbywa szkolenie przed przystąpieniem do przetwarzania danych.

- każdy upoważniony do przetwarzania danych osobowych w urzędzie potwierdza pisemnie fakt zapoznania się z niniejszą dokumentacją i zrozumieniem wszystkich zasad

bezpieczeństwa wg wzoru stanowiącego Załącznik nr 4 do niniejszej dokumentacji. Podpisany dokument jest dołączany do akt osobowych.

- obszar przetwarzania danych osobowych określony w Załączniku nr 8 do niniejszej dokumentacji, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.

- przebywanie osób, nieuprawnionych w w/w obszarze jest dopuszczalne za zgodą Administratora Danych Osobowych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

- pomieszczenia stanowiące obszar przetwarzania danych powinny być zamykane na klucz.

- monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
- po zakończeniu pracy na stanowisku komputerowym należy wylogować się z systemu i wyłączyć komputer.
- przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna oraz usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w odpowiednich zamykanych szafach lub biurkach.

1.2. Środki techniczne ochrony danych osobowych stosowane w Urzędzie Gminy Dolice

Zbiory danych przetwarzane w urzędzie zabezpiecza się poprzez:

- Środki ochrony fizycznej

· Zbiory danych osobowych przechowywane są w pomieszczeniach zabezpieczonych przed swobodnym dostępem.

· Dostęp do budynku kontrolowany jest przez system monitoringu w budynku przy ul. Ogrodowej 16.

· Zbiory danych osobowych w formie papierowej przechowywane są w szafach zamykanych na klucz.

· Archiwalne zbiory danych osobowych przechowywane są w pomieszczeniu o nazwie archiwum. Klucz do tego pomieszczenia, przechowywany jest w zamykanej szafie na klucz, a dostęp do niego mają wyłącznie upoważnione osoby.

· Kopie bezpieczeństwa (kopie zapasowe) przechowuje się w miejscach zabezpieczonych przed nieuprawnionym przejęciem, modyfikacją uszkodzeniem lub zniszczeniem.

· Kopie bezpieczeństwa (kopie zapasowe) zbiorów danych osobowych na nośnikach danych (dysk zewnętrzny) przechowywane są w zamkniętym na klucz sejfie, a dostęp do niego mają wyłącznie upoważnione osoby.

· Pomieszczenia, w których przetwarzane są zbiory danych osobowych zabezpieczone są przed skutkami pożaru za pomocą wolnostojącej gaśnicy.

· Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów. Po zniszczeniu dokumentów spisuje się protokół zniszczenia.

- Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej

· Zbiory danych osobowych przetwarzane są przy użyciu komputerów stacjonarnych jak i przenośnych.

- Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, konie trojańskie, rootkity.

- Użyto system Firewall stanowiący element programu antywirusowego do ochrony dostępu do sieci komputerowej.

- Urząd posiada skonfigurowaną i zabezpieczoną przed spamami pocztę.

- Sieć komputerowa urzędu podłączona jest do sieci lokalnej UG Dolice. Połączenia są realizowane przy użyciu urządzenia typu UTM (firewall, IPS, IDS, antywirus). Zastosowany jest system logowania operacji wykonywanych przez użytkowników. Dostęp do zasobów sieci Internet posiadają tylko osoby, którym jest to konieczne do wykonywania obowiązków służbowych.

- Środki ochrony w ramach systemowych narzędzi programowych i baz danych

- Dostęp do zbiorów danych osobowych wymaga uwierzytelnienia z wykorzystaniem spersonalizowanego identyfikatora użytkownika oraz unikatowego hasła użytkownika.

- Identyfikator użytkownika który utracił dostęp do danych osobowych nie może być przydzielony innej osobie.

- Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu Informatycznego.

- Administrator Systemów Informatycznych sporządza okresowo (co miesiąc) kopie bezpieczeństwa danych osobowych ze wszystkich wykorzystywanych w urzędzie systemów informatycznych, programów, żeby zabezpieczyć się przed utrata danych spowodowaną awarią sprzętu komputerowego.

- Należy zabezpieczyć komputery, serwer przed skutkami awarii bądź niestabilnego napięcia z sieci elektrycznej poprzez podłączenie każdego komputera, serwera do zasilacza UPS o mocy nie mniejszej jak 1500VA.

- Zmiana haseł dostępowych następuję przynajmniej raz na 30 dni.

- Nie wolno przechowywać danych osobowych na komputerach przenośnych, a pracownik uzyskuje dostęp do tych danych tylko będąc na swoim stanowisku pracy poprzez logowanie do zbiorów danych zapisywanych w odpowiedniej lokalizacji na serwerze urzędu.

- Dyski twarde uszkodzone lub wyłączone z eksploatacji przed oddaniem do utylizacji należy trwale pozbawić zapisu lub zniszczyć dysk twardy w ten sposób aby niemożliwym stało się odzyskanie informacji z niego.

2. Zabezpieczenie danych osobowych

Dokumentacja zawierająca dane osobowe ze względu na wrażliwość danych powinna być szczególnie chroniona na każdym etapie swojego użytkowania.

2.1. Dokumentacja (dane osobowe) - w formie elektronicznej

- Dostęp do dokumentacji w szczególności danych osobowych mają tylko zalogowani użytkownicy systemu informatycznego w urzędzie z odpowiednimi uprawnieniami i jednocześnie jest możliwość identyfikacji który z użytkowników odpowiada za dane edytowane bądź wprowadzone.

- Przed zniszczeniem tych danych system zabezpieczony jest urządzeniami zabezpieczającymi system (fizycznie) oraz poprzez regularne sporządzanie kopii bezpieczeństwa które przechowywane są w wyznaczonym miejscu.

- Użytkownicy mają tak dobrane uprawnienia żeby ograniczyć do minimum możliwość wypływu informacji oraz ich przekłamania lub zmiany. Do programu komputerowego wprowadza się dane po ich fizycznej autoryzacji przez osoby uprawnione do tego.
- Użytkownicy otrzymują unikalny identyfikator, który nie może być wykorzystywany ponownie.

2.2. Dokumentacja (dane osobowe) w formie papierowej

- Dokumentacja jest własnością wytwarzającego i powinna od momentu powstawania do momentu zniszczenia, po ustaniu okresu archiwizacyjnego, być zabezpieczona przed nieuprawnionym dostępem wypłynięciem, zmianą bądź zniszczeniem.

- Dokumentację należy przechowywać w pomieszczeniach, szafach, bądź szufladach zabezpieczonych sprawnym zamkiem, a w momencie kiedy jest ona w użytku nie można jej pozostawić bez dozoru osób uprawnionych do posługiwania się nią.

- Dokumentacje archiwizujemy w wyodrębnionym pomieszczeniu (Archiwum). Dostęp do pomieszczenia archiwum mają wyłącznie osobowy upoważnione przez Administratora Danych.

- Po ustaniu okresu archiwizacyjnego dokonuje się zniszczenia dokumentacji, z której sporządza się protokół zniszczenia.

- O udostępnieniu dokumentacji, w szczególności dokumentacji zawierającej dane osobowe każdorazowo decyduję Administrator Danych Osobowych.

W sytuacjach krytycznych: - **pożar, powódź** – należy powiadomić straż pożarną **(numer telefonu alarmowy 112)** i jeśli nie jest zagrożone własne lub czyjeś zdrowie lub życie przystąpić do ratowania dokumentacji urzędu (jak też innego mienia zakładowego), - **kradzież** – należy bezzwłocznie powiadomić organy ścigania **(numer telefonu alarmowy 112)** i udzielić im wszelkiej pomocy w ujęciu sprawcy, - **klęska żywiołowa –** współdziałać ze służbami ratowniczymi i początkowymi przy ratowaniu dokumentacji (również innego mienia zakładowego).

2.3. Zabronione jest:

- przechowywanie danych osobowych w szafach na korytarzach;

- pozostawienie niezabezpieczonych pomieszczeń, w których przetwarzane są dane osobowe pod nieobecność osób upoważnionych do przetwarzania danych osobowych;

- pozostawienie dokumentów z danymi osobowymi na biurku po zakończeniu pracy na stanowisku,

- przechowywanie dokumentów z danymi osobowymi w niezamykanych szafach, na parapetach, podłodze.

3. Zasady kasacji i utylizacji sprzętu komputerowego, elementów eksploatacyjnych i nośników danych

Głównym celem jest zapewnienie bezpiecznej likwidacji sprzętu komputerowego, elementów eksploatacyjnych tegoż sprzętu oraz nośników danych. Procedurę stosuje się

w wypadku kasacji i utylizacji sprzętu komputerowego, elementów eksploatacyjnych tegoż sprzętu oraz nośników danych. Procedura przedstawia się następująco:
- Sprzęt wycofany z eksploatacji, trwale uszkodzony lub wyeksploatowany mogący zawierać dane osobowe zgłasza się niezwłocznie do: Administratora Bezpieczeństwa Informacji, Administratora Systemów Informatycznych lub bezpośrednio do Administratora Danych Osobowych.

- Kasacje należy poprzedzić zgromadzeniem w jednym miejscu sprzętu do kasacji przez Administratora Bezpieczeństwa Informacji,

- Przed zniszczeniem należy pozbawić sprzęt komputerowy oraz nośniki danych wszystkich informacji możliwych do odczytu.

- W przypadku nośników zewnętrznych nośników danych (dyski zewnętrzne, płyty DVD, CD-R, pendrivy, dyskietki) proces kasacji zostaje przeprowadzony przez Administratora Bezpieczeństwa Informacji, w obecności Administratora Systemów Informatycznych. Z przeprowadzonej kasacji sporządza się protokół zniszczenia.

- Nośniki danych należy zniszczyć w taki sposób, aby stało się niemożliwe odzyskanie z nich jakichkolwiek danych.

- Należy także pamiętać o obowiązku zgłoszenia listy sprzętu komputerowego i eksploatacyjnego, a także nośników danych pozbawionych wczesnej w sposób trwały możliwości odczytu, do pracownika odpowiedzialnego za prowadzenie ewidencji rzeczowych składników majątku w urzędzie (środków trwałych, wartości niematerialnych i prawnych, pozostałych środków trwałych, wyposażenia).

- Sprzęt w wypadku gdy jest wpisany do ewidencji środków trwałych zostaje zdjęty z ewidencji środków trwałych i przekazany firmie zajmującej się utylizacją na podstawie karty przekazania odpadu której 1 egzemplarz trafia do Administratora Bezpieczeństwa Informacji.

Część IV

1. Aktualizacja treści zawartej w „polityce bezpieczeństwa"

W związku ze zmianami w zakresie ochrony danych osobowych oraz mając na uwadze zmiany przepisów w tym zakresie, Administrator Bezpieczeństwa Informacji („ABI") zobowiązuję się dokonywać każdorazowo do dnia 30 kwietnia każdego roku aktualizacji treści zawartej w niniejszej Polityce bezpieczeństwa przetwarzania danych osobowych oraz Instrukcji zarządzania systemem informatycznym. Aktualizacja zapisów prowadzona będzie pod kątem zgodności stanu zapisanego ze stanem faktycznym, w szczególności danych zawartych w następujących dokumentach:
- „Wykaz budynków i pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe".

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

- „Ewidencji osób upoważnionych do przetwarzania danych osobowych w urzędzie.

- Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych UG Dolice.

- Sposobu przepływu danych pomiędzy poszczególnymi systemami informatycznymi w sieci lokalnej (LAN) urzędu.

2. Rejestracja zbiorów danych

1. Począwszy od dnia 1 stycznia 2015r. Administrator Danych Osobowych nie ma obowiązku zgłaszania do GIODO nowych zbiorów danych osobowych, z wyjątkiem zbiorów o których mowa w art. 27, ust. 1, art. 43, ust. 1 i 1a ustawy o ochronie danych osobowych z dnia 27 sierpnia 2009r. 2. W przypadku gdy administrator danych nie wyznaczy administratora bezpieczeństwa informacji Zgodnie z art. 40 ustawy Administrator Danych Osobowych jest zobowiązany zgłosić zbiór danych osobowych do rejestracji, której dokonuje Generalny Inspektorat Ochrony Danych Osobowych w celu przetwarzania tych danych, z wyjątkiem zbiorów które z mocy ustawy o ochronie danych osobowych nie podlegają obowiązkowi rejestracji lub gdy Administrator Danych powołał administratora bezpieczeństwa informacji oraz zgłosił go do Generalnemu Inspektorowi do rejestracji. Zgodnie z art. 41 ust. 2 ustawy o ochronie danych osobowych Administrator Danych za pośrednictwem Administratora Bezpieczeństwa Informacji („ABI") jest obowiązany zgłaszać Generalnemu Inspektorowi Danych Osobowych zbiory danych osobowych podlegające zgłoszeniu do „GIODO" oraz zgłaszanie każdą zmianę informacji w terminie 30 dni od dnia dokonania zmiany w zbiorze danych. W związku z powyższym Administrator Danych zobowiązuję wszystkich użytkowników systemu Informatycznego jednostki do niezwłocznego informowania (nie później niż w terminie 7 dni od dnia zmiany stanu poprzedniego) o likwidacji, utworzeniu lub zmianie zawartości zbioru danych, a wówczas Polityka bezpieczeństwa będzie podlegała aktualizacji w ciągu roku.

3. Konieczność przetwarzania danych osobowych w nowym zbiorze danych osobowych wymaga konsultacji z Administratorem Bezpieczeństwa Informacji jednostki w celu sprawdzenia, czy dany zbiór nie podlega, w myśl przepisów (art. 43 ust. 1 ustawy) zwolnieniu z obowiązku zgłoszenia do rejestracji. W sytuacji gdy zachodzi konieczność zgłoszenia zbioru do „GIODO" rejestracja następuje na pisemny wniosek przygotowany przez Administratora Bezpieczeństwa Informacji zatwierdzony przez Administratora Danych Osobowych. Zgodnie z ustawą Administrator Danych dokonuje zgłoszenia zbioru do rejestracji przed rozpoczęciem przetwarzania danych, to znaczy przed pierwszą czynnością, jaką można wykonać na danych osobowych tj. przed pozyskaniem pierwszych danych do zbioru. zgłoszeniu tego zbioru do rejestracji w GIODO. W sytuacji gdy Administrator Danych Osobowych zamierza przetwarzać tzw. dane szczególnie wrażliwe wymagane jest uprzednie zarejestrowanie zbioru danych przez Generalnego Inspektora Danych Osobowych („GIODO").

Administrator Bezpieczeństwa Informacji prowadzi jawny rejestr zbiorów danych osobowych.

3. Zasady nadzoru nad zainstalowanym oprogramowaniem na komputerach Urzędu Gminy Dolice

- Nadzór nad oprogramowaniem zainstalowanym na komputerach będących własnością urzędu pełni Administrator Bezpieczeństwa Informacji („ABI") za pośrednictwem Administratora Systemów Informatycznych („ASI"). .

- Użytkownik komputera który dokonuje odebrania komputera z oprogramowaniem weryfikuje prawdziwość danych zawartych w karcie komputera i potwierdza je własnoręcznym czytelnym podpisem z datą wykonania podpisu.

- Administrator Bezpieczeństwa Informacji oraz Administrator Systemów Informatycznych dokonują okresowej kontroli danych zawartych w karcie komputera ze stanem faktycznym. Jeżeli w wyniku takiej wyrywkowej kontroli wyjdzie na jaw że użytkownik dokonał samowolnej instalacji jakiegokolwiek oprogramowania na które urząd nie posiada licencji, bądź nie spełnia wymogów licencyjnych, odpowiada za to bezpośrednio użytkownik komputera.

- To użytkownik czuwa nad tym żeby zgodnie z procedurami wew. określonymi w dokumencie „Polityka bezpieczeństwa przetwarzania danych osobowych i instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy w Dolicach" nie zostawiać komputera zalogowanego i to on odpowiada za wszystkie zmiany w oprogramowaniu i sprzęcie niezgodne z zapisami w karcie komputera.
- Taka sama forma odpowiedzialności obowiązuje w wypadku kontroli przez organy upoważnione do kontroli legalności oprogramowania. Za oprogramowanie zewidencjonowane w kartach komputerów i za wszystkie licencje będące własnością urzędu odpowiada Administrator Danych, a Administrator Bezpieczeństwa Informacji w urzędzie nadzoruje jego zgodność z wymogami licencyjnymi oprogramowania .

4. Ochrona budynków, obiektów oraz pomieszczeń urzędu oraz system alarmowy

- Przedmiotem ochrony jest ochrona mienia znajdującego się w budynkach, pomieszczeniach Urzędu Gminy Dolice, łącznie z mieniem znajdującym się w granicach geodezyjnych budynków. W razie zagrożenia pracownicy urzędu zobowiązani są podjąć czynności zmierzające do zapobieżenia wystąpienia szkody, a w razie jej zaistnienia do zapobieżenia zwiększeniu jej rozmiarów i natychmiastowego powiadomienie osoby wskazanej oraz właściwych służb publicznych.

- Usługi z zakresu konserwacji systemu alarmowego dla urzędu świadczy firma zewnętrzna. Na podstawie zawartej umowy zleceniobiorca zobowiązał się do konserwacji systemu alarmowego, celem utrzymania w stałej sprawności eksploatacyjnej urządzeń i instalacji systemu alarmowego.

5. Politykę kluczy do budynków, pomieszczeń Urzędu Gminy Dolice zawiera Instrukcja dotycząca zasad gospodarki kluczami i ochrony fizycznej w budynkach Urzędu Gminy Dolice.

Część V

1. Zadania Administratora Bezpieczeństwa Informacji w Urzędzie Gminy Dolice

Zgodnie z art. 36 ust. 3 ustawy o ochronie danych osobowych Administrator Danych Osobowych wyznacza Administratora Bezpieczeństwa Informacji w UG Dolice nadzorującego przestrzeganie zasad ochrony. Administrator Bezpieczeństwa Informacji odpowiedzialny jest za ochronę danych osobowych przetwarzanych w wersji papierowej oraz w systemach informatycznych przy współudziale Administratora Systemów Informatycznych w urzędzie

Do najważniejszych obowiązków Administratora Bezpieczeństwa Informacji należy:

2. Zadania Administratora Systemów Informatycznych w Urzędzie Gminy Dolice

1. Do najważniejszych obowiązków Administratora Systemów Informatycznych (ASI) należy:

Administrator Bezpieczeństwa Informacji realizuje zadania w celu zapewnienia maksymalnego poziomu bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy w Dolicach poprzez:

- dokonywanie sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowania sprawozdania w tym zakresie

- nadzorowanie opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych osobowych odpowiednią do zagrożeń oraz kategorii objętych ochroną

- nadzorowanie przestrzegania zasad określonych w dokumentacji ochrony danych osobowych.

2. Do zadań Administratora Bezpieczeństwa Informacji (ABI) należy:

-zapewnienie przestrzegania przepisów o ochronie danych osobowych, w szczególności poprzez:

- prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych. Załącznik Nr 10

-sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla Administratora Danych

-nadzorowanie opracowania i aktualizowania dokumentacji danych osobowych oraz przestrzegania zasad w niej określonych

-zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych

-prowadzenie rejestru zbiorów danych osobowych przetwarzanych przez administratora danych zgodnie z obowiązującymi przepisami prawa

- nadzór nad wdrożeniem stosownych środków organizacyjnych i technicznych w celu ochrony przetwarzania danych osobowych

-nadawanie, zmienianie oraz cofanie uprawnień do przetwarzania danych osobowych na wniosek Właścicieli zasobów dla pracowników oraz współpracowników

- nadzór nad zapewnieniem przez Właścicieli zasobów, dostosowania funkcjonalności systemów przetwarzających dane osobowe do wymagań określonych w Rozporządzeniu.

-prowadzenie dokumentacji opisującej zastosowaną ochronę danych osobowych

-reprezentowanie Administratora Danych w kontaktach z Biurem GIODO

-przygotowywanie zgłoszeń zbiorów danych osobowych do rejestracji w Biurze GIODO

- reagowanie na zgłaszane incydenty (zdarzenia, zajścia lub wypadki nie będące częścią standardowych operacji lub usług, które powodują lub mogą spowodować spadek poziomu ochrony danych osobowych) związane z naruszeniem danych osobowych oraz analizowanie ich przyczyn i kierowanie wniosków dotyczących ukarania winnych naruszeń.

3. Administrator Bezpieczeństwa Informacji w zakresie realizacji swoich obowiązków, ma prawo żądania od pozostałych osób, bez względu na rangę ich stanowiska udzielenia natychmiastowej pomocy w razie stwierdzenia, że doszło do naruszenia przepisów o ochronie danych osobowych.

3. Obowiązki osób przetwarzających dane osobowe - użytkowników systemu informatycznego w Urzędzie Gminy Dolice

Do obowiązków użytkowników systemu informatycznego w Urzędzie Gminy w Dolicach zakresie ochrony danych osobowych należy w szczególności:
1) Przestrzeganie procedur wew. zawartych w Polityce bezpieczeństwa ochrony danych osobowych oraz w Instrukcji zarządzania systemem informatycznym w urzędzie
2) Uniemożliwienie dostępu lub podglądu danych osobowych w systemie dla osób nieupoważnionych.
3) Informowanie Administratora Bezpieczeństwa Informacji oraz Administratora Systemów Informatycznych o wszelkich naruszeniach obowiązujących w urzędzie procedur wewnętrznych w zakresie przetwarzania danych osobowych.
4) Wykonywania bez zbędnej zwłoki poleceń Administratora Bezpieczeństwa Informacji oraz poleceń Administratora Systemów Informatycznych w zakresie ochrony danych osobowych jeśli są one zgodne z przepisami prawa powszechnie obowiązującego.

4. Opis zdarzeń naruszających ochronę danych osobowych

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 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 zakłócenia 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.

5. Procedury postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Gminy Dolice

Niniejsze procedury wew. określają tryb postępowania w sytuacji naruszenia ochrony danych osobowych gromadzenia i przetwarzanych zarówno w zbiorach tradycyjnych jak i informatycznych. Niniejsze procedury wew. stosuje się w przypadku, gdy stwierdzono naruszenie zabezpieczeń sprzętu informatycznego, sieci komputerowej, systemu alarmowego i zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe. Przez naruszenie ochrony danych osobowych rozumie się niezgodne z przepisami ustawy o ochronie danych i rozporządzeń wykonawczych przetwarzanie danych oraz usuwanie danych osobowych. Osobami bezpośrednio odpowiedzialnymi za zgodną z prawem ochronę danych osobowych w UG Dolice ich zabezpieczeń są:

a) Administrator Danych Osobowych,

b) Administrator Bezpieczeństwa Informacji,

c) Administrator Systemów Informatycznych,

d) Pracownicy upoważnieni do przetwarzania danych osobowych.

1. Każdy pracownik biorący udział w przetwarzaniu danych osobowych w systemie informatycznym jest odpowiedzialny za bezpieczeństwo tych danych.

   W szczególności osoba, która zauważyła zdarzenie mogące być przyczyną naruszenia ochrony danych osobowych lub mogących spowodować naruszenie bezpieczeństwa danych, zobowiązana jest do natychmiastowego poinformowania Administratora Bezpieczeństwa Informacji lub innej osoby wskazanej przez niego.

2. Każda osoba zatrudniona w urzędzie, która stwierdzi lub podejrzewa naruszenie zabezpieczenie ochrony danych osobowych w systemie informatycznym (lub przetwarzanych w inny sposób) powinna niezwłocznie poinformować o tym fakcie Administratora Bezpieczeństwa Informacji. W przypadku braku możliwości zawiadomienia Administratora Bezpieczeństwa Informacji lub Administratora Systemów Informatycznych niezwłocznie należy powiadomić bezpośredniego przełożonego.

3. Do czasu przybycia Administratora Bezpieczeństwa Informacji należy:

a) niezwłocznie podjąć czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,

b) zabezpieczyć dostęp do miejsca lub urządzenia przez osoby trzecie,

c) wstrzymać pracę na komputerze na którym zaistniało naruszenie ochrony oraz nie uruchamiać bez koniecznej potrzeby komputerów i innych urządzeń, których funkcjonowanie w związku naruszeniem ochrony zostało wstrzymane,

d) zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę zdarzenia,

e) nie zmieniać położenia przedmiotów, które pozwalają stwierdzić naruszenie ochrony lub odtworzyć jej okoliczności,

f) podjąć stosowne do zaistniałej sytuacji, inne niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych,

g) podjąć inne działania przewidziane w instrukcjach technicznych i technologicznych stosowanie do objawów i komunikatów towarzyszących naruszeniu,

h) wstępnie udokumentować zaistniałe naruszenie,

i) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa Informacji lub osoby upoważnionej.

4. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych Administrator Bezpieczeństwa Informacji lub osoba go zastępująca powinna:
a) zapoznać się z zaistniałą sytuacją i dokonać wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy ,

b) zaprotokołować wszelkie informacje związane ze zdarzeniem,

c) wygenerować i wydrukować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia,

d) przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych niepowołanych,

e) dokonać fizycznego odłączenia urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nie uprawnionej,

f) wylogować użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych.

g) dokonać zmiany hasła na konto Administratora Bezpieczeństwa Informacji i użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania.

h) zażądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem.

5. Administrator Bezpieczeństwa Informacji (ABI) dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, który powinien zawierać w szczególności:
- wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych w zdarzeniu,

- określeniu czasu, miejsca naruszenia i powiadomienia,

- określeniu okoliczności towarzyszących i rodzaju naruszenia,

- wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,

- wstępną ocenę przyczyn wystąpienia naruszenia,

- ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

5. Raport o którym mowa w pkt. 5 Administrator Bezpieczeństwa Informacji przekazuje się niezwłocznie Administratorowi Danych Osobowych. Załącznik Nr 5

6. Administrator Bezpieczeństwa Informacji przystępuje do usuwania skutków incydentu i przywrócenia prawidłowego przebiegu procesu przetwarzania danych osobowych. W szczególności działania związane z usuwaniem skutków incydentu mogą obejmować:

- przeprowadzenie naprawy sprzętu informatycznego;

- rekonfigurację sprzętu informatycznego;

- wprowadzenie poprawek do oprogramowania;

- rekonfiguracje oprogramowania;
- odtworzenie danych z kopii awaryjnych;
- modyfikacje danych w celu odtworzenia ich integralności;
- wycofanie z użycia materiału kryptograficznego;
- inne naprawy urządzeń wchodzących w skład infrastruktury informatycznej wspomagającej lub zabezpieczających działanie systemu informatycznego

Część VII

1. Postanowienia końcowe

1.1. Wobec osoby, która w przypadku naruszenia ochrony danych osobowych lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zadaniami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie interdyscyplinarne.

1.2. Administrator Bezpieczeństwa Informacji zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych.

1.3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być traktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia ochrony danych osobowych lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym Administratora Bezpieczeństwa Informacji.

1.4. Orzeczona kara dyscyplinarna wobec osoby uchylającej się od powiadomienia zgodnie z ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tj.: Dz. U. z 2015r., poz. 2135 z późn. zm.) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

1.5. w sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tj.: Dz. U. z 2015r., poz 2135 z późn. zm.), rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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. 2004. 100, poz. 1024).

2. Załączniki do polityki bezpieczeństwa przetwarzania danych osobowych

Integralną część niniejszego dokumentu stanowią następując załączniki:

- <u>Załączniki jawne stanowią:</u>

- **załącznik nr 1:** „Upoważnienie do przetwarzania danych osobowych".

- **załącznik nr 2 :** „Umowa powierzenia przetwarzania danych osobowych"
- **załącznik nr 3:** „Oświadczenie o zachowaniu poufności".
- **załącznik nr 4:** „Oświadczenie pracownika Urzędu Gminy w Dolicach".
- **załącznik nr 5:** „Raport z naruszenia bezpieczeństwa"
- **załącznik nr 6:** „Wniosek osoby, której dane dotyczą, o podanie informacji".
- **załącznik nr 7:** „Zakres czynności pracownika zatrudnionego przy przetwarzaniu danych osobowych"

- Załączniki niejawne stanowią:

- **załącznik nr 8:** „Granice obszarów oraz osoby, które przetwarzają dane osobowe".
- **załącznik nr 9:** „Opis struktur zbiorów danych".
- **załącznik nr 10:** „Ewidencja osób upoważnionych do przetwarzania danych osobowych".

WÓJT GMINY
Grzegorz Brochocki

.....
Administrator Danych Osobowych

Załącznik nr 1

Dolice, ...
/miejscowość, data/

UPOWAŻNIENIE Nr .....

Na podstawie art.37 ustawy z dnia 29 sierpnia 1999 r. o ochronie danych osobowych (Dz. U. z 2015r., poz. 2135 z późn. zm.)

UPOWAŻNIAM

Panią / Pana

.....

zatrudnionego na stanowisku .....

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

(nazwa jednostki organizacyjnej)

Upoważnienie wydaje się na czas .....

Identyfikator/Login .....

Data i podpis osoby upoważnionej: .....

.....
Administrator Danych Osobowych

Załącznik nr 2

Umowa powierzenia przetwarzania danych osobowych

§ 1 Postanowienia ogólne

Na mocy niniejszej umowy Urząd Gminy Dolice posługujący się nr NIP ..... oraz REGON ..... działając, jako administrator danych osobowych zawartych w zbiorze ..... powierza (w zakresie określonym w §2 niniejszego dokumentu), działając zgodnie z art. 31 ustawy o ochronie danych osobowych, przetwarzanie danych osobowych zawartych w wyżej wymienionym zbiorze przetwarzającemu:
Przetwarzającym jest:
.....
.....
.....

§ 2 Określenie zakresu

Administrator powierza dane wchodzące do zbioru wymienionego w § 1 niniejszej umowy. Zakres powierzonych danych obejmuje
.....
.....

§ 3 Określenie celu

Powierzenie przetwarzania danych osobowych na mocy niniejszej umowy następuje w celu.....
.....

§ 4 Postanowienia końcowe

Przetwarzający oświadcza, że wdrożył środki bezpieczeństwa, o jakich mowa w art. 36-39a ustawy o ochronie danych osobowych. Przetwarzający zobowiązuje się do zachowania w poufności jakichkolwiek informacji związanych z uzyskaniem dostępu do powierzonych danych oraz do zabezpieczenia powierzonych danych przed jakimkolwiek nieuprawnionym dostępem.

.....
(data i podpis Administratora Danych Osobowych)

.....
(data i podpis przetwarzającego)

Załącznik nr 3

OŚWIADCZENIE
O ZACHOWANIU POUFNOŚCI

Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam, lub będę miał/a dostęp w związku z wykonywaniem jakichkolwiek czynności na rzecz ..... .

Zobowiązuję się przestrzegać wszelkich procedur obowiązujących w wyżej wymienionej jednostce organizacyjnej dotyczących ochrony danych osobowych – w szczególności określonych w Polityce Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym.

Oświadczam, że zapoznałem/am się z przepisami dotyczącymi ochrony danych osobowych, w tym z ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tj.: Dz. U. z 2015r., poz. 2135 z późn. zm.), w tym z zasadami odpowiedzialności karnej określonymi w rozdziale 8 wyżej wymienionej ustawy.

Załącznik nr 4

.....
(imię i nazwisko pracownika)
.....
.....
(adres zamieszkania)

OŚWIADCZENIE

Stwierdzam własnoręcznym podpisem, że znana mi jest treść przepisów:

- o ochronie tajemnic prawnie chronionych stanowiących tajemnicę służbową wynikającą z Kodeksu Pracy,
- o ochronie danych osobowych wynikająca z ustawy o ochronie danych osobowych (tj.: Dz. U. z 2015r., poz. 2135 z późn. zm.),
- o odpowiedzialności karnej za naruszenie ochrony danych osobowych,
- Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemami Informatycznymi do przetwarzania danych osobowych w Urzędzie Gminy w Dolicach.

Zobowiązuję się do zachowania w tajemnicy danych podlegających przetwarzaniu, również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

.....
(podpis pracownika)

.....
(podpis złożono w obecności)

Załącznik nr 5

Raport z naruszenia bezpieczeństwa systemu informatycznego w Urzędzie Gminy w Dolicach

1. Data ..... Godzina .....
(dd.mm.rr) (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 i podpis Administratora Bezpieczeństwa Informacji

Załącznik nr 6

Wniosek osoby, której dane dotyczą, o podanie informacji

.....
(imię i nazwisko)

Urząd Gminy w Dolicach
Ul. Ogrodowa 16
73-115 Dolice

Na podstawie art. 32 ust 1 pkt 1-5a ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tj.: Dz. U. z 2015r., poz 2135 z późn. zm.) proszę o przekazanie następujących informacji na temat posiadanych przez Urząd Gminy w Dolicach danych dotyczących mojej osoby:

1. czy dane przetwarzane są przez Państwa w Urzędzie Gminy, czy też powierzono je innemu administratorowi danych (jeżeli powierzono – proszę o jego pełną nazwę i adres siedziby);
2. w jaki celu, w jakim zakresie i w jaki sposób przetwarzane są te dane;
3. od kiedy firma dysponuje oraz jaki jest ich zakres (proszę podać w zrozumiałej formie treść danych);
4. z jakiego źródła lub źródeł pozyskano poszczególne elementy składowe danych;
5. komu i w jakim zakresie udostępniono te dane (proszę o kompletną listę odbiorców z adresami).

Odpowiedź proszę przesłać pod wyżej podany adres w formie pisemnej w terminie 30 dnia, zgodnie z art. 33 ustawy powołanej na wstępie niniejszego pisma.

.....
(podpis wnioskodawcy)

Załącznik nr 7

Zakres czynności pracownika zatrudnionego przy przetwarzaniu danych osobowych

I. Obowiązki pracownika

Pracownik dopuszczony do przetwarzania danych osobowych zobowiązany jest do:

1. Zapoznania się i wypełniania obowiązków wynikających z:

- przepisów ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tj.: Dz. U. z 2015r., poz. 2135 z późn. zm.) oraz przepisów wykonawczych wydanych na jej podstawie,
- przepisów Konwencji oraz Dyrektyw dotyczących ochrony danych osobowych, w tym Dyrektywy 95/46/WE Parlamentu Europejskiego I Rady z dnia 24 października 1995r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych,

2. kontrolowania dostępu do danych osobowych.

3. zachowania w tajemnicy danych oraz sposobu ich zabezpieczenia do których uzyskał dostęp w trakcie zatrudnienia, również po ustaniu zatrudnienia.

4. zapewnienia bezpieczeństwa przetwarzania danych osobowych poprzez ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem.

II. Odpowiedzialność pracownika

Za niedopełnienie obowiązków wynikających z niniejszego aneksu pracownik ponosi odpowiedzialność na podstawie przepisów Kodeksu Pracy, Regulaminu Pracy oraz powołanej wyżej ustawy o ochronie danych osobowych.

Oświadczam, że treść niniejszego zakresu jest mi znana i zobowiązuję się do jego przestrzegania.

Potwierdzam odbiór 1 egzemplarza zakresu czynności dotyczącego przetwarzania danych osobowych w Urzędzie Gminy w Dolicach.

.....
(podpis pracownika)

.....
(podpis pracodawcy)