Załącznik Nr 1 do zarządzenia Nr 20/17
Wójta Gminy Nowinka
z dnia 10 marca 2017 r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

URZĘDU GMINY NOWINKA

16-304, NOWINKA 33

ZARZĄDZENIE NR 20/17
WÓJTA GMINY NOWINKA

z dnia 10 marca 2017 r.

w sprawie ustalenia Polityki Bezpieczeństwa Urzędu Gminy Nowinka i zatwierdzenia Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Nowinka

Na podstawie art. 30 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz.U. 2016 r. poz. 446,) w związku z §20 ust. 1 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U. z 2016 r. poz. 113) zarządzam, co następuje:

§ 1. 1. Ustalić Politykę Bezpieczeństwa Urzędu Gminy Nowinka, stanowiącą załącznik Nr 1 do Zarządzenia.

2. Zatwierdzić Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Nowinka stanowiącą załącznik Nr 2 do Zarządzenia.

§ 2. Traci moc Zarządzenie nr 63/13 z dnia 30.10.2013 r. w sprawie ustalenia Polityki Bezpieczeństwa Urzędu Gminy Nowinka i zatwierdzenia Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Nowinka oraz Zarządzenie nr 52/16 z dnia 30.09.2016r. w sprawie zmiany Zarządzenia Wójta Gminy Nowinka z 30 października 2013 r. nr 63/13 w sprawie ustalenia Polityki bezpieczeństwa Urzędu Gminy Nowinka i zatwierdzenia Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Nowinka

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

Wójt Gminy Nowinka
Dorota Winiewicz

POLITYKA BEZPIECZEŃSTWA INFORMACJI
URZĘDU GMINY NOWINKA

§1. Cel Polityki

1. Polityka Bezpieczeństwa Informacji, zwana dalej PBI ma na celu zapewnienie bezpieczeństwa informacji przetwarzanej w Urzędzie i działanie zgodnie z wymaganiami prawa oraz normami nadzorczymi.

2. Polityką Bezpieczeństwa Informacji objęte są dane osobowe, którymi zgodnie z Ustawą o Ochronie Danych Osobowych są wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

3. Kierownictwo wskazuje obszary działania oraz przyjmuje odpowiedzialność w zakresie bezpieczeństwa informacji.

§2. Zakres PBI

1. Niniejsza PBI określa podstawowe zasady, normy i wymagania zgodności w zakresie bezpieczeństwa informacji przetwarzanej na obszarze Urzędu Gminy Nowinka. Dotyczy wszystkich pracowników Urzędu, a także innych osób mających dostęp do chronionych informacji (np. pracowników firm zewnętrznych realizujących prace w Urzędzie).

2. Dokument ma zastosowanie do wszystkich informacji chronionych niezależnie od formy, w jakiej są przechowywane (papierowej, elektronicznej i innej) na całym obszarze Urzędu Gminy Nowinka, z wyjątkiem informacji niejawnych. Obszar ochrony informacji niejawnych posiada własne regulacje prawne i stosowne mechanizmy ochronne oraz struktury organizacyjne dedykowane do ochrony informacji niejawnych wytwarzanych, przetwarzanych oraz przechowywanych w wydzielonych systemach teleinformatycznych.

3. Niniejszy dokument został opracowany w oparciu o najlepsze praktyki z obszaru bezpieczeństwa informacji oraz zgodnie wymaganiami normy PN-EN ISO 9001:2009.

§3. Przeglądy PBI

1. PBI ustalona dnia 10 marca 2017r. podlega przeglądom zarządczym i weryfikacji co najmniej raz do roku lub też w trakcie roku w przypadku wystąpienia znaczących zmian. Powinny one obejmować weryfikację zasad i ewentualne dostosowanie PBI do zmieniającego się profilu ryzyka Urzędu, zmian środowiska organizacyjnego, warunków biznesowych, środowiska technicznego, a także w zakresie zachowania zgodności z przepisami prawa i normami nadzorczymi.

2. Wszelkie zmiany w niniejszej PBI przyjmowane są Zarządzeniami Wójta Gminy.

§4. Terminologia

1. Ogólne definicje związane z bezpieczeństwem informacji:

1) dane osobowe- każda informacja, która pozwala na bezpośrednią lub pośrednią identyfikację żyjącej osoby fizycznej

2) informacja - treści wszelkiego rodzaju przechowywane na dowolnym nośniku informacji. Informacja może być wyrażona za pomocą mowy, pisma, obrazu, rysunku, znaku, kodu, dźwięku lub w jakikolwiek inny sposób

3) zbiór danych osobowych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów

4) zbiór nieinformatyczny- każdy posiadający strukturę zestaw danych o charakterze osobowym prowadzony poza systemem informatycznym, w szczególności w formie kartoteki, skorowidza, księgi, wykazu lub innego zbioru ewidencyjnego

5) bezpieczeństwo informacji - zachowanie poufności, integralności i dostępności informacji; w ramach bezpieczeństwa informacji mogą być uwzględniane również inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność

6) integralność danych – właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany

7) incydent naruszenia bezpieczeństwa środowiska teleinformatycznego - pojedyncze niepożądane lub niespodziewane zdarzenie bezpieczeństwa środowiska teleinformatycznego (tj. wystąpienie stanu komponentu środowiska teleinformatycznego wskazującego na potencjalne naruszenie jego bezpieczeństwa, błąd mechanizmu kontrolnego lub uprzednio nieznaną sytuację, która może być istotna z perspektywy bezpieczeństwa) lub seria takich zdarzeń, w przypadku których występuje znaczne prawdopodobieństwo zakłócenia działalności lub naruszenia bezpieczeństwa informacji

8) poufność danych - właściwość danych polegająca na tym, że pozostają one niedostępne lub niejawne dla nieuprawnionych osób, procesów lub innych podmiotów;

9) profil ryzyka - skala i struktura ekspozycji na ryzyko

10) zagrożenie - potencjalna przyczyna niepożądanego incydentu, który może spowodować szkodę dla systemu lub organizacji

11) Urząd – Urząd Gminy Nowinka, Nowinka 33, 16-304 Nowinka

12) Ustawa – Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1996r.)Dz.U. z 2002 r. Nr 101, poz.926 z późn. Zm.).

2. Systemy przetwarzania informacji stosowane w Urzędzie Gminy Nowinka:

1) PBI - Polityka Bezpieczeństwa Informacji;

2) infrastruktura teleinformatyczna - zespół urządzeń, oprogramowania i łączy transmisyjnych obejmujący w szczególności platformy sprzętowe (w tym: serwery, macierze, stacje robocze), sieć teleinformatyczną (w tym: routery, przełączniki, zapory sieciowe oraz inne urządzenia sieciowe), oprogramowanie systemowe (w tym systemy operacyjne i systemy zarządzania bazami danych) oraz inne elementy umożliwiające bezawaryjną i bezpieczną pracę ww. zasobów (w tym zasilacze UPS, generatory prądotwórcze, urządzenia klimatyzacyjne)

3) przetwarzanie danych osobowych- jakiekolwiek operacje wykonywane na danych osobowych: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie zarówno w systemie papierowym jak cyfrowym

4) system informatyczny - aplikacja komputerowa lub zbiór powiązanych aplikacji komputerowych, którego celem jest przetwarzanie danych;

5) nośnik informacji - medium magnetyczne, optyczne lub papierowe, na którym zapisuje się i przechowuje informacje.

3. Terminy dotyczące ról w zakresie zapewniania bezpieczeństwa informacji:

1) Administrator Danych Osobowych –Wójt Gminy Nowinka;

2) Administrator Bezpieczeństwa Informacji (ABI) - osoba powołana przez Administratora Danych Osobowych, nadzorująca przestrzeganie zasad ochrony danych obejmujących środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną;

3) Administrator Systemu Informatycznego (ASI) - osoba odpowiedzialna za prawidłowy stan i działanie środowiska teleinformatycznego od strony technicznej. W Urzędzie rolę ASI pełni pracownik na stanowisku Informatyk;

4) Użytkownik zasobów danych osobowych- osoba, która otrzymała upoważnienie do przetwarzania danych osobowych zgodnie z obowiązującym wzorem, nadane przez Administratora Danych Osobowych

§5. Dokumenty powiązane

Na dokumentację ochrony danych osobowych w Urzędzie Gminy Nowinka składają się;

1. Ewidencja osób upoważnionych przez Administratora Danych Osobowych do przetwarzania danych osobowych. (wzór Zal. Nr 1)

- prowadzona przez Administratora Bezpieczeństwa Informacji, w przypadku modyfikacji każdorazowo aktualizowana w wersji cyfrowej oraz papierowej

2. Ewidencja zbiorów danych osobowych (wraz z opisem struktur) przetwarzanych w Urzędzie Gminy Nowinka oraz programów zastosowanych do ich przetwarzania. (wzór Zal. Nr 2)

- prowadzona przez Administratora Bezpieczeństwa Informacji, w przypadku modyfikacji każdorazowo aktualizowana w wersji cyfrowej oraz papierowej

3. Opis sposobu przepływu danych pomiędzy systemami

- prowadzone przez Administratora Systemów Informatycznych, w przypadku modyfikacji każdorazowo aktualizowana w wersji cyfrowej oraz papierowej

4. Oryginały i Kopie dokumentów dotyczących ochrony danych osobowych (w tym kopie wniosków o rejestrację/aktualizację zbiorów danych osobowych do GIODO oraz uchwały, zarządzenia, polityki itd. dotyczące ochrony danych osobowych)

- prowadzone przez Administratora Bezpieczeństwa Informacji

5. Protokoły z przeprowadzonych kontroli wewnętrznych i zewnętrznych w zakresie ochrony danych osobowych

- prowadzone przez Administratora Bezpieczeństwa Informacji

6. Plany archiwizacji danych osobowych i programów służących do ich przetwarzania

- prowadzone przez Administratora Systemów Informatycznych

§6. Odpowiedzialność Administratora Danych Osobowych

1. Administrator Danych Osobowych jest odpowiedzialny za przetwarzanie i ochronę danych osobowych zgodnie z przepisami prawa, w tym wprowadzenie do stosowania procedur postępowania zapewniających prawidłowe przetwarzanie danych osobowych, rozumiane jako ochronę danych przed ich udostępnieniem osobom nieupoważnionym, zmianą lub zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz utratą, uszkodzeniem lub zniszczeniem.

2. Do kompetencji Administratora Danych Osobowych należy w szczególności:

1) Wyznaczenie Administratora Bezpieczeństwa Informacji.

2) Określenie celów i strategii ochrony danych osobowych.

3) Podział zadań i obowiązków związanych z organizacją ochrony danych osobowych.

3. Do obowiązków Administratora Danych Osobowych należy:

1) Zapewnienie szkoleń dla pracowników w zakresie przepisów o ochronie danych osobowych oraz zagrożeń związanych z ich przetwarzaniem.

2) Przyjmowanie i zatwierdzanie niezbędnych, wymaganych przez przepisy prawa dokumentów regulujących ochronę danych osobowych w Urzędzie

3) Nadawanie upoważnień pracownikom Urzędu oraz Użytkownikom zewnętrznym do przetwarzania danych osobowych.

4) Zapewnienie środków finansowych na ochronę fizyczną pomieszczeń, w których przetwarzane są dane osobowe.

5) Zapewnienie środków finansowych niezbędnych do ochrony danych osobowych przetwarzanych w systemach informatycznych oraz w zbiorach nieinformatycznych.

6) Zapewnienie środków finansowych na merytoryczne przygotowanie osób odpowiedzialnych za nadzór nad ochroną danych osobowych.

7) Zapewnienie realizacji obowiązku zgłoszenia i aktualizacji zbiorów danych osobowych do rejestracji GIODO.

§7. Odpowiedzialność Administratora Bezpieczeństwa Informacji

1. Administrator Danych Osobowych wyznacza Administratora Bezpieczeństwa Informacji, który nadzoruje przestrzeganie zasad ochrony danych osobowych zarówno w systemach informatycznych, jak również w zbiorach danych osobowych prowadzonych w formie papierowej i elektronicznej

2. Do kompetencji Administratora Bezpieczeństwa Informacji należy:

1) Określenie zasad ochrony danych osobowych.

2) Wnioskowanie o ukaranie osób winnych naruszenia przepisów i zasad dotyczących ochrony

danych osobowych.

3. Do obowiązków Administratora Bezpieczeństwa Informacji należy:

1) Zapewnienie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,

2) Prowadzenie ewidencji zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art.43 ust. 1 Ustawy o Ochronie Danych Osobowych, zawierającego nazwę zbioru oraz informacje, o których mowa w art.41 ust. 1 pkt.2-4a i 7.

3) Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych

4) Prowadzenie dokumentacji opisującej zastosowaną ochronę danych osobowych (niniejsza Polityka oraz wynikające z niej instrukcje i procedury) w tym zapewnienie ich publikacji i dystrybucji oraz prowadzenia stosownej dokumentacji.

5) Zapoznawanie pracowników oraz współpracowników Urzędu Gminy z przepisami i zasadami ochrony danych osobowych oraz informowanie o zagrożeniach związanych z ich przetwarzaniem.

6) Reprezentowanie Gminy w kontaktach z Biurem GIODO.

7) Przygotowywanie zgłoszeń zbiorów danych osobowych do rejestracji w Biurze GIODO.

8) Przygotowywanie upoważnień do przetwarzania danych Osobowych.

9) Reagowanie na zgłaszane incydenty związane z naruszeniem ochrony danych osobowych oraz analizowanie ich przyczyn i kierowanie wniosków dotyczących ukarania winnych naruszeń.

10) Sprawdzanie wypełnienia obowiązków technicznych i organizacyjnych związanych z ochroną danych osobowych.

11) Administrator Bezpieczeństwa Informacji w zakresie realizacji swoich obowiązków, ma prawo żądania od pozostałych osób, bez względu na rangę ich stanowiska udzielania natychmiastowej pomocy w razie stwierdzenia, że doszło do naruszenia przepisów o ochronie danych osobowych, które może skutkować postawieniem zarzutu popełnienia Urzędowi albo Administratorowi Danych jednego z przestępstw, wskazanych ww. Rozdziale 8 Ustawy o ochronie danych osobowych.

§8. Odpowiedzialność Administratora Systemów Informatycznych

1. Rolę ASI pełni pracownik wyznaczony przez Administratora Danych Osobowych.

2. Do kompetencji Administratora Systemów Informatycznych należy:

1) Zabezpieczenie systemów przetwarzania danych osobowych zgłoszonych ASI

2) Zapewnienie poufności, integralności, dostępności i rozliczalności danych przetwarzanych w systemach informatycznych.

3. Do obowiązków Administratora Systemów Informatycznych należy:

1) Bieżący nadzór oraz zapewnianie optymalnej ciągłości działania systemu informatycznego w tym opracowanie procedur określających zarządzanie systemem informatycznym przetwarzającym dane osobowe.

2) Reagowanie bez zbędnej zwłoki, w przypadku naruszenia bądź powstania zagrożenia bezpieczeństwa danych osobowych.

3) Przeciwdziałanie próbom naruszenia bezpieczeństwa danych osobowych.

4) Analizę raportów wszelkich zdarzeń w tym incydentów związanych z bezpieczeństwem systemów przetwarzania danych.

5) Zapewnienie zgodności wszystkich wdrażanych systemów przetwarzania danych osobowych z Ustawą oraz z niniejszą Polityką bezpieczeństwa i Instrukcją Zarządzania Systemem Informatycznym w Urzędzie Gminy Nowinka.

6) Instalację i konfigurację oprogramowania i sprzętu typu „stand-alone", sieciowego i serwerowego używanego do przetwarzania danych osobowych.

7) Konfigurację i administrację oprogramowaniem systemowym i sieciowym zabezpieczającym dane osobowe przed nieupoważnionym dostępem.

8) Nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności szkodliwego oprogramowania.

9) Nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji.

10) Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe.

11) Świadczenie pomocy technicznej w ramach oprogramowania a także serwis sprzętu komputerowego będącego na stanie Urzędu Gminy Nowinka, służącego do przetwarzania danych osobowych.

12) Diagnozowanie i usuwanie awarii sprzętu komputerowego oraz realizacje umów z firmami świadczącymi usługi pogwarancyjnego sprzętu komputerowego.

13) Wykonywanie i zarządzanie kopiami awaryjnymi oprogramowania systemowego (w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie) i sieciowego.

14) Wykonywanie i przechowywanie dokumentacji adekwatnie do obowiązujących przepisów.

15) Nadzór nad wdrożeniem i zarządzanie aplikacjami (przeglądanie, nadawanie i odbieranie uprawnień użytkownikom, itp.), w których przetwarza się dane osobowe.

16) Umożliwienie przeprowadzenia kontroli systemu informatycznego przez służby Biura Generalnego Inspektora Ochrony Danych Osobowych.

§9. Odpowiedzialność użytkowników zasobów danych osobowych

1. Do kompetencji użytkowników zasobów danych osobowych należy:

1) Określanie celów w jakich mają być przetwarzane dane osobowe, zakresu oraz czasu trwania przetwarzania danych osobowych.

2) Określenie sposobu przetwarzania danych osobowych (czy w systemach informatycznych, czy w zbiorach nieinformatycznych).

3) Ustalenie, czy dane przetwarzane dla określonego celu mają mieć charakter poufny.

3. Do obowiązków użytkowników zasobów danych osobowych należy:

1) Zapewnienie podstaw prawnych do przetwarzania danych osobowych od chwili zebrania danych osobowych do chwili ich usunięcia.

2) Zapewnienie aktualności, adekwatności oraz merytorycznej poprawności danych osobowych przetwarzanych w określonym przez nich celu.

3) Realizację obowiązku informowania o przetwarzaniu danych osobowych osób, których dane osobowe są pozyskiwane.

4) Zapewnienie na żądanie uprawnionych osób, udostępnianie informacji o przetwarzanych danych osobowych oraz podmiotach, którym zostały one udostępnione.

5) Złożenie oświadczenia o znajomości przepisów o ochronie danych osobowych oraz zobowiązania do zachowania w tajemnicy danych osobowych oraz informacji na temat zabezpieczania danych osobowych.

6) W przypadku utworzenia nowego zbioru danych osobowych ustalenie, kogo dotyczą dane osobowe, jaki jest ich zakres (np. imię i nazwisko, adres zamieszkania, NIP, PESEL itp.), cel przetwarzania oraz komu dane osobowe mają być udostępniane. Wszystkie te informacje powinny zostać przekazane do Administratora Bezpieczeństwa Informacji na formularzu Zgłoszenia (wzór- zał.nr 3)

7) W celu osiągnięcia i utrzymania wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych konieczne jest zaangażowanie ze strony każdego pracownika i użytkownika zewnętrznego w zakresie ochrony danych osobowych.

8) Pracownicy Urzędu Gminy oraz Użytkownicy zewnętrzni są zobowiązani do informowania o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe bezpośrednio do Administratora Bezpieczeństwa Informacji.

9) Pracownicy / Użytkownicy zewnętrzni są zobowiązani do:

a) Postępowania zgodnie z Polityką Bezpieczeństwa Informacji.

b) Zachowania w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia zarówno w okrese zatrudnienia jak i po ustaniu stosunku pracy.

10) Ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem.

11) Pracownicy / Użytkownicy zewnętrzni powinni mieć świadomość możliwości zaistnienia sytuacji naruszenia ochrony danych osobowych. W tym celu powinni:

a) Przestrzegać procedur związanych z otwieraniem i zamykaniem pomieszczeń, a także z wejściem do obszarów przetwarzania danych osobowych osób nieupoważnionych.

b) Informować Administratora Bezpieczeństwa Informacji o podejrzanych osobach

c) Pracownicy / Użytkownicy zewnętrzni powinni na podstawie dokonanej identyfikacji ewentualnych zagrożeń, przedkładać Administratorowi Bezpieczeństwa Informacji projekty i propozycje nowych rozwiązań, których celem jest zwiększenie poziomu ochrony danych osobowych.

§10. Zakres ochrony informacji

1. Urząd chroni informacje podlegające ochronie z mocy prawa, a także istotne z uwagi na prawidłowość realizacji kluczowych procesów.

2. W sytuacjach kryzysowych, ujawnienie informacji wrażliwych pod względem poufności uznawane jest jako zagrożenie mniejsze od zniszczenia informacji.

3. Użytkownicy Urzędu zobowiązani są do używania zasobów informacyjnych wyłącznie do celów służbowych. Wszyscy użytkownicy zasobów informacyjnych podlegają kontroli dostępu do tych zasobów.

4. Każdy pracownik posiada uprawnienia dostępu na poziomie i zakresie niezbędnym do wykonywania obowiązków służbowych.

5. Użytkownicy Urzędu posiadają wiedzę o zasobach Urzędu ograniczoną do informacji wymaganych do realizacji powierzonych zadań.

6. Ochrona zasobów musi opierać się na co najmniej dwóch mechanizmach zabezpieczeń.

7. Użytkownicy przetwarzający informacje zobowiązani są do ścisłego przestrzegania przepisów prawa oraz przepisów wewnętrznych Urzędu oraz do nie rozpowszechniania wiadomości stanowiących tajemnicę urzędową lub objętych ochroną danych osobowych.

8. Naruszenie ww. zasad jest naruszeniem obowiązków pracowniczych i może pociągnąć za sobą odpowiedzialność karną, wynikającą z przepisów:

1) ustawy o ochronie danych osobowych;

2) kodeksu karnego dot. przestępstw przeciwko ochronie informacji;

3) przepisów chroniących tajemnicę skarbową.

9. Użytkownicy zobowiązani są do przestrzegania Instrukcji pracy na stanowisku wyposażonym w monitor i drukarkę, Polityki Bezpieczeństwa Informacji, a także do przestrzegania zakazu udostępniania hasła do swojego komputera, zakazu korzystania z nielegalnego oprogramowania oraz zakazu instalowania jakiegokolwiek oprogramowania bez zgody ASI.

§11. Klasyfikacja informacji

1. Kryteriami klasyfikacji informacji jest wymagany poziom: poufności, integralności, dostępności, rozliczalności.

2. W przypadku konieczności stosowania wielu kryteriów rozstrzygające jest kryterium przyjmujące najwyższy poziom.

3. Ocenę wrażliwości aktywów prowadzi się w Urzędzie przez identyfikowanie konsekwencji biznesowych, w szczególności przez analizę

1) poufności informacji;

2) integralności informacji;

3) dostępności informacji (potrzeby dostępności);

4) wymiernych kosztów odtworzenia:

a) aktywów,

b) informacji i danych,

c) odtworzenia działalności operacyjnej,

d) niewymiernych kosztów odtworzenia informacji w kontekście:

- dobrego imienia Urzędu,

- konsekwencji karnych, cywilnoprawnych lub służbowych.

4. W celu identyfikacji poziomu istotności informacji i wymaganego poziomu ochrony informacja klasyfikowana jest wg następujących kategorii:

1) informacje wrażliwe - informacje chronione prawnie (kryterium poufności) lub chronione z powodu uznania za podlegające ochronie, np. w związku z istotną wagą informacji dla prawidłowej realizacji procesów krytycznych (kryterium integralności, dostępności), dane osobowe;

2) informacje niewrażliwe — informacje nie należące do informacji wrażliwych (kryterium integralności, dostępności);

3) informacje publiczne - informacje publicznie dostępne (kryterium integralności, dostępności);

4) informacje niejawne - informacje, do których stosuje się przepisy o ochronie informacji niejawnych.

§12. Podstawowe zasady zapewnienia bezpieczeństwa informacji

1. Poprzez zapewnienie bezpieczeństwa informacji należy rozumieć działania oparte na systematycznym zarządzaniu ryzykiem, obejmujące wybór, wdrożenie i utrzymanie zabezpieczeń składających się z technicznych i organizacyjnych środków ochrony danych i infrastruktury teleinformatycznej.

2. W celu zapewnienia bezpieczeństwa zasobów Urzędu stosuje się następujące ogólne zasady:

1) zasada przywilejów koniecznych - każdy pracownik posiada prawa dostępu do zasobów Urzędu ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu obowiązków;

2) zasada wiedzy koniecznej - użytkownicy posiadają wiedzę o zasobach Urzędu ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych im zadań;

3) zasada asekuracji zabezpieczeń - ochrona zasobów winna opierać się na co najmniej dwóch mechanizmach zabezpieczenia;

4) zasada rozliczalności - Urząd dąży do zapewnienia jednoznacznej odpowiedzialności pracowników za powierzone im zasoby;

5) wszyscy użytkownicy zasobów informacyjnych ponoszą odpowiedzialność za zaniedbanie swoich obowiązków w zakresie bezpieczeństwa informacji;

6) zasada czystego biurka - należy unikać pozostawiania dokumentów na biurku bez opieki. Po zakończeniu pracy należy uprzątnąć biurko z dokumentów papierowych oraz informatycznych nośników informacji. Zaleca się przechowywanie pod zamknięciem (najlepszym rozwiązaniem jest sejf, szafa lub inna forma zabezpieczenia) dokumentów i nośników zawierających wrażliwe lub krytyczne informacje służbowe;

7) zasada czystego ekranu - zamykanie sesji lub blokowanie komputera i terminala pozostawionego bez opieki lub czasowo nieużywanego (za pomocą mechanizmu blokowania ekranu i klawiatury kontrolowanego hasłem, tokenem lub innego podobnego mechanizmu). Po zakończonym dniu pracy komputer powinien zostać wyłączony.

3. W szczególności zapewnienie bezpieczeństwa obejmuje obszary :

1) bezpieczeństwa organizacyjnego,

2) bezpieczeństwa fizycznego i środowiskowego,

3) bezpieczeństwa systemów i infrastruktury teleinformatycznej,

4) zarządzanie ciągłością działania,

5) reagowania na incydenty bezpieczeństwa informacji,

6) zarządzania jakością danych.

§13. Wymiana Informacji dotyczących danych osobowych

1. Pracownicy Urzędu Gminy oraz użytkownicy zewnętrzni w celu ochrony wymienianych informacji dotyczących danych osobowych powinni podczas przetwarzania uwzględniać następujące zasady:

1) Wykorzystywanie technik kryptograficznych do ochrony poufności, integralności i rozliczalności danych osobowych przesyłanych publicznymi sieciami telekomunikacyjnymi.

2) Ochrona wymienianych danych osobowych przed przechwyceniem, kopiowaniem, modyfikacją, błędnym wyborem drogi komunikacji i zniszczeniem.

3) Zabezpieczenia i ograniczenia związane z możliwościami przekazywania wiadomości za pomocą środków komunikacji, np. automatyczne przekazywania poczty elektronicznej na zewnątrz, także dbałość o zachowanie bezpieczeństwa adresów mailowych w przypadku wysyłania wiadomości grupowych

4) Zakaz pozostawiania informacji zawierających dane osobowe przy urządzeniach drukujących, np. kopiarkach, drukarkach, faksach, do których mogą mieć dostęp osoby nieupoważnione.

5) Upewnienie się przed przekazaniem danych osobowych, czy rozmówca jest osobą upoważnioną do uzyskania określonych danych osobowych.

6) Zachowania szczególnej ostrożności w trakcie rozmów telefonicznych, zapobieganie podsłuchania danych osobowych przez osoby nieupoważnione.

7) Nie pozostawianie wiadomości zawierających dane osobowe w automatycznych sekretarkach.

8) Właściwe postępowanie z faksami i fotokopiarkami, ponieważ mają one podręczną pamięć i przechowują w niej strony zawierające np. dane osobowe na wypadek błędów transmisji. Transport danych osobowych w formie elektronicznej i papierowej pomiędzy obszarami, w których są przetwarzane dane osobowe powinien być prowadzony przez osoby upoważnione w sposób ograniczający możliwość ich pozyskanie i odczyt przez osoby nieupoważnione.

§14. Przetwarzanie danych osobowych w obszarach bezpiecznych

1. Dane osobowe w Urzędzie Gminy mogą być przetwarzane wyłącznie w pomieszczeniach przetwarzania danych osobowych.

2. Na pomieszczenia przetwarzania danych osobowych składają się pomieszczenia biurowe oraz części pomieszczeń, gdzie Urząd Gminy prowadzi działalność.

3. Do pomieszczeń przetwarzania danych osobowych zalicza się:

1) Serwerownia.

2) Pomieszczenia biurowe, w których zlokalizowane są stacje robocze.

3) Pomieszczenia, w których przechowywane są sprawne oraz uszkodzone elektroniczne nośniki informacji, kopie zapasowe.

4) Pomieszczenia, w których przechowuje się dokumenty źródłowe oraz wydruki z systemu informatycznego.

5) Pomieszczenia, w których zlokalizowane są zbiory nieinformatyczne.

4. Przebywanie wewnątrz obszarów, o których mowa w ust. 3, osób nieuprawnionych do przetwarzania danych osobowych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych.

5. Budynki lub pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane podczas nieobecności osób upoważnionych do przetwarzania danych osobowych, w sposób ograniczający możliwość dostęp do nich osobom nieupoważnionym.

§15. Dopuszczenie osób do przetwarzania danych osobowych

1 Przetwarzanie danych osobowych jest możliwe wyłącznie po uzyskaniu przez pracownika / Użytkownika zewnętrznego formalnego upoważnienia do przetwarzania danych osobowych wystawianego przez Administratora Danych Osobowych. W tym celu Administrator Bezpieczeństwa Informacji przed dopuszczeniem pracownika do pracy przy przetwarzaniu danych osobowych:

1) zapoznaje pracownika / użytkownika zewnętrznego z przepisami dotyczącymi ochrony danych osobowych oraz uregulowaniami wewnętrznymi obowiązującymi w tym zakresie w Urzędzie;

2) przyjmuje od pracownika / użytkownika zewnętrznego podpisane oświadczenie o zachowaniu danych osobowych i sposobów ich zabezpieczania w tajemnicy, przetwarzania danych osobowych zgodnie z przepisami oraz oświadczenia o znajomości niniejszego dokumentu, a także o znajomości „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Nowinka, którego wzór stanowi zał. Nr 5a niniejszej Polityki.

3) Wnioskuje do Administratora Bezpieczeństwa Informacji o formalne upoważnienie (wzór zał. Nr 4) pracownika do przetwarzania danych osobowych sporządzane wg wzoru stanowiącego zał. Nr 5b niniejszej Polityki.

2. Oświadczenia i upoważnienia przechowuje się w aktach osobowych pracownika, a także w dokumentacji prowadzonej przez Administratora Bezpieczeństwa Informacji.

3. Przełożony pracownika / Użytkownika zewnętrznego jest zobowiązany niezwłocznie po ustaniu potrzeby przetwarzania danych osobowych przez pracownika / Użytkownika zewnętrznego złożyć rezygnację do Administratora Bezpieczeństwa Informacji dotyczącą jego dostępu do danych osobowych.

4. W przypadku aktualizacji wzorów dokumentacji dotyczącej ochrony danych osobowych nowe wnioski/upoważnienia obowiązują od momentu podpisania ich przez ADO i automatycznie unieważniają uprzednio funkcjonujące formularze.

§16. Ewidencja osób upoważnionych do przetwarzania danych osobowych

1. Osoby upoważnione do przetwarzania danych osobowych powinny być wpisywane do ewidencji. Ewidencja osób upoważnionych do przetwarzania danych osobowych powinna być prowadzona przez Administratora Bezpieczeństwa Informacji. Jakakolwiek zmiana w zakresie informacji zawartych w ewidencji powinna podlegać natychmiastowemu odnotowaniu.

2. Przełożeni pracowników / Użytkowników zewnętrznych odpowiadają za natychmiastowe zgłoszenie do Administratora Bezpieczeństwa Informacji osób, które utraciły uprawnienia dostępu do danych osobowych.

3. Administrator Bezpieczeństwa Informacji w oparciu o informacje, o których mowa w ust. 2 powinien podjąć działania, których celem jest uniemożliwienie tym osobom dostępu do danych osobowych i wyrejestrować z ewidencji, o której mowa w ust. 1.

4. Elektroniczne nośniki informacji, na których gromadzone są wykazy zawierające ewidencję osób upoważnionych do przetwarzania danych osobowych powinny być przechowywane w szafie zamykanej, do której ma dostęp Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona.

5. W ewidencji ujęci są także z odpowiednią adnotacją pracownicy upoważnieni do przebywania w obszarze przetwarzania danych osobowych. Sekretarz informuje Administratora Bezpieczeństwa Informacji o konieczności nadania upoważnienia. ABI przygotowuje wniosek (wzór Zał. Nr 4) do ADO i upoważnienie sporządzane wg wzoru stanowiącego Zał. Nr 5c niniejszej Polityki.

§17. Postępowanie z kluczami oraz zabezpieczenia pomieszczeń Urzędu Gminy Nowinka

1. Ochrona Urzędu

1)Budynek Urzędu podlega ochronie polegającej na całodobowym monitorowaniu przez system alarmowy, zainstalowany w budynku przez **Zakład Elektroniki SUWAR Liliana Sadowska ul. 1 Maja 24, 16-400 Suwałki**

2) Szczegółowy zakres obowiązków i ustaleń w zakresie ochrony i dozoru reguluje umowa zawarta pomiędzy Gminą Nowinka , a Zakładem Elektroniki SUWAR Lilianna Sadowska

3) Z uwagi na publiczny charakter Urzędu, w czasie jego pracy nie obowiązuje system przepustek, ani też inny system określający uprawnienia do wejścia, przebywania i wyjścia z budynku Urzędu.

2. Zobowiązuje się pracowników Urzędu do:

1) zwracania uwagi na zachowanie osób wchodzących i wychodzących z budynku Urzędu;

2) reagowania na wejście do budynku i przebywanie w nim osób będących pod wpływem alkoholu lub innych środków odurzających;

3) reagowania na próby niszczenia, wynoszenia lub wywożenia mienia z budynku Urzędu;

4) reagowania na próby wnoszenia do budynku przedmiotów niebezpiecznych, materiałów lub substancji budzących podejrzenie itp.;

5) natychmiastowego reagowania poprzez powiadomienie odpowiednich służb (Straż Miejska, Policja, Straż Pożarna, Pogotowie Ratunkowe) o zaobserwowanych próbach stworzenia zagrożenia dla życia i zdrowia, a także utraty lub zniszczenia mienia.

3.Zabezpieczenie pomieszczeń i procedura postępowania z kluczami i kodami cyfrowymi do systemu alarmowego:

1) Wójt wyznacza pracowników, którzy są upoważnieni do otwierania głównych drzwi wejściowych do budynku oraz do rozkodowywania systemu alarmowego przed rozpoczęciem pracy Urzędu.

2) Zamknięcia dostępu zewnętrznego do budynku Urzędu po godzinie 15:00 dokonuje sprzątaczka, która po zakończeniu prac porządkowych koduje system alarmowy i zamyka budynek.

3) Wójt Gminy wyznacza także pracowników, którzy są upoważnieni do otwierania drzwi wejściowych do budynku oraz rozkodowywania systemu alarmowego poza regulaminowym czasem pracy Urzędu.

4. Pracownik, któremu zostały powierzone klucze oraz kod cyfrowy do systemu alarmowego zobowiązany jest do:

a) wykorzystywania ich zgodnie z przeznaczeniem,

b) nie kopiowania powierzonych kluczy bez zgody Wójta oraz nie udostępniania osobom trzecim,

c) nie udostępniania kodu cyfrowego do systemu alarmowego osobom trzecim.

5. Wzór upoważnienia do zarządzania kluczami oraz kodem cyfrowym do systemu alarmowego budynku Urzędu, stanowi Załącznik 6 nr do PBI:

1) Pracownicy przed rozpoczęciem pracy podpisują listę obecności znajdującą się w kancelarii urzędu oraz pobierają klucze do swoich pomieszczeń biurowych.

2) Po otwarciu pomieszczeń biurowych, przed przystąpieniem do pracy, pracownicy sprawdzają stan zastosowanych zabezpieczeń sprzętu biurowego i komputerowego, dokumentacji i innego wyposażenia.

3) W przypadku stwierdzenia nieprawidłowości lub naruszenia stanu zabezpieczeń, o których mowa w ust. 2, pracownik, który to stwierdził, natychmiast powiadamia o tym swojego bezpośredniego przełożonego.

4) Od momentu pobrania kluczy do momentu ich zdania, na pracownikach spoczywa pełna odpowiedzialność za zabezpieczenie pomieszczeń biurowych, w których pracują.

6. Po zakończeniu pracy, pracownicy zobowiązani są do uporządkowania swoich stanowisk pracy oraz wykonania czynności zabezpieczających, w szczególności do:

1) zabezpieczenia dokumentacji i pieczęci urzędowych;

2) zabezpieczenia komputerów i nośników informacji;

3) wyłączenia wszystkich urządzeń zasilanych energią elektryczną (czajniki, wentylatory itp.) zgodnie z zasadami bhp;

4) zamknięcia okien i drzwi;

5) pozostawienia kluczy od pomieszczeń biurowych w kancelarii.

7. Klucze od biurek i szaf biurowych są w posiadaniu pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.

8. Duplikaty kluczy, będące kluczami zapasowymi do pomieszczeń Urzędu są przechowywane w sejfie z zamkiem elektronicznym w pomieszczeniu kancelarii.

9. Osobą odpowiedzialną za należyte przechowywanie, zabezpieczenie oraz udostępnianie kluczy zapasowych jest osoba zatrudniona na stanowisku ds. Obsługi kancelaryjnej, obrony cywilnej i zarządzania kryzysowego.

10. Wydawanie kluczy zapasowych (o których mowa w ust. 8) pracownikom może odbywać się tylko w uzasadnionych sytuacjach oraz w przypadkach awaryjnych za pokwitowaniem.

11. Klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić do depozytu .

12. Otwarcie Urzędu w soboty, niedziele oraz święta możliwe jest wyłącznie za zgodą Wójta.

13. Do otwierania pomieszczeń dla potrzeb wykonania czynności związanych ze sprzątaniem wykorzystywane są klucze zapasowe znajdujące się w sejfie z zamkiem elektronicznym.

14. Szczególnej ochronie podlegają klucze do :

1) pomieszczeń o strategicznym znaczeniu, tj. do pomieszczeń Urzędu Stanu Cywilnego. Klucze do Urzędu Stanu Cywilnego są wyłączone z procedury i chronione zgodnie z Ustawą Prawo o aktach stanu cywilnego.

2) pokoju Sekretarza. Klucze do pokoju Sekretarza są wyłącznie w posiadaniu Sekretarza i Wójta i ponoszą oni odpowiedzialność za należyte ich zabezpieczenie.

§18. Bezpieczeństwo organizacyjne

1. W Urzędzie dokonuje się wewnętrznego podziału użytkowników ze względu na ich role i poziomy uprawnień.

2. Urząd podejmuje systematyczne działania związane z edukacją i szkoleniem pracowników w zakresie zagrożeń i istniejących regulacji wewnętrznych odpowiednio do ich obowiązków.

§19. Bezpieczeństwo fizyczne i środowiskowe

1. Stosowane w Urzędzie mechanizmy bezpieczeństwa adekwatne są do potrzeb i skali działalności Urzędu, w taki sposób aby pozwalało to na bieżące funkcjonowanie kluczowych procesów oraz ich odtworzenie w przypadku wystąpienia sytuacji awaryjnej.

2. Wrażliwe środki przetwarzania informacji są umieszczane w obszarach bezpiecznych, chronionych fizyczną granicą przez odpowiednie bariery bezpieczeństwa oraz zabezpieczenia wejścia. Zapewnia się, aby były one chronione fizycznie przed nieuprawnionym dostępem fizycznym, uszkodzeniami lub zakłóceniami pracy.

3. Stosowana jest ochrona sprzętu (łącznie ze sprzętem wykorzystywanym poza siedzibą Urzędu) niezbędna do redukowania ryzyka nieautoryzowanego dostępu do informacji i ochrony przed utratą lub uszkodzeniem. Ochrona obejmuje również odpowiednią lokalizację (miejsce instalacji), konserwację, zbywanie lub przekazanie sprzętu podmiotom zewnętrznym w sposób zapewniający bezpieczeństwo informacji.

4. Chroni się przed zagrożeniami instalacje wspomagające, takie jak zasilanie lub okablowanie sieciowe.

§20. Bezpieczeństwo systemów i infrastruktury teleinformatycznej

1. Stosowana jest zasada, że wszystkie komponenty środowiska teleinformatycznego (systemy, komponenty infrastruktury teleinformatycznej) powinny być zinwentaryzowane i udokumentowane oraz mają wyznaczonego właściciela odpowiedzialnego za właściwą ochronę i utrzymanie zabezpieczeń danego komponentu.

2. Stosowane są następujące mechanizmy bezpieczeństwa:

1) rozdzielanie obowiązków zapobiegające celowej lub nieumyślnej modyfikacji lub niewłaściwego użycia systemów;

2) regulacje wewnętrzne w zakresie eksploatacji komponentów;

3) zarządzanie zmianami w środowisku teleinformatycznym;

4) świadczenie pomocy technicznej użytkownikom systemów;

5) ochrona przed złośliwym oprogramowaniem;

6) stosowanie zabezpieczeń kryptograficznych;

7) stosowanie regularnego dokonywania i testowania kopii zapasowych;

8) zapewnianie bezpieczeństwa sieci teleinformatycznych;

9) zapewnianie bezpieczeństwa nośników informacji;

10) zapewnianie bezpieczeństwa wymiany informacji;

11) kontrola dostępu i nadawanie uprawnień;

12) zarządzanie oprogramowaniem użytkownika końcowego.

§21. Zarządzanie ciągłością działania

Odpowiedni poziom ciągłości działania w zakresie środowiska teleinformatycznego uzyskiwany jest poprzez stosowanie kombinacji zabezpieczeń prewencyjnych i środków służących do odtwarzania komponentów środowiska teleinformatycznego.

§22. Reagowanie na incydenty bezpieczeństwa informacji

1. Urząd wdraża i stosuje regulacje wewnętrzne dotyczące zgłaszania i reagowania na zidentyfikowane incydenty bezpieczeństwa informacji, w tym incydenty naruszenia bezpieczeństwa środowiska teleinformatycznego opisane szczegółowo w Procedurze Alarmowej (Załącznik nr 7 do BPI).

2. Obowiązkiem wszystkich pracowników jest stosowanie zasad w zakresie zgłaszania incydentów.

3. Informacje dotyczące stwierdzonych incydentów wraz z opisem ich przyczyny i podjętymi działaniami korygującymi są rejestrowane w celu dalszej analizy.

4. Urząd podejmuje działania zmierzające do ustalenia przyczyn i usunięcia skutków incydentów bezpieczeństwa.

5. Informacje dotyczące incydentów są uwzględniane w procesie analizy ryzyka.

§23. Publikowanie lub udostępnianie informacji niewrażliwych

1. Z uwagi na zagrożenie ryzykiem utraty reputacji, a także możliwość zwiększenia poziomu innych rodzajów ryzyka należy dochować jak największej ostrożności i staranności związanej z publikowaniem lub udostępnianiem informacji niewrażliwych podmiotom zewnętrznym - pomimo, że istnieje pewność, że informacja taka nie jest objęta ochroną prawa.

2. Szczególną uwagę należy zwrócić na informacje publikowane w sieci Internet, w tym w tzw. mediach społecznościowych, Biuletynie Informacji Publicznych, stronach internetowych Urzędu.

3. Publikowanie lub udostępnianie informacji niewrażliwych podmiotom zewnętrznym jest możliwe wyłącznie z zachowaniem zasad prawa, przepisów wewnętrznych i za każdym razem wymaga weryfikacji treści udostępnianej informacji pod kątem poprawności i zagrożenia dla reputacji Urzędu przez odpowiedniego dla sprawy pracownika.

§24. Dystrybucja Polityki

1. Z treścią niniejszego dokumentu, jak i innych regulacji związanych z PBI zapoznani są wszyscy pracownicy Urzędu będący użytkownikami zasobów danych osobowych.

2. Niniejszy dokument może być przedstawiany wszystkim innym podmiotom, w tym organom władzy i administracji publicznej, w celu prezentacji zasad ochrony informacji i środowiska teleinformatycznego obowiązujących w Urzędzie.

§25. Sposób przepływu danych pomiędzy poszczególnymi systemami

Administrator Systemów Informatycznych prowadzi dokumentację systemów informatycznych zawierającą opis współpracy pomiędzy różnymi systemami informatycznymi oraz sposób przepływu danych pomiędzy systemami, w których te dane są przetwarzane.

§26. Zasady ochrony danych osobowych w zbiorach nieinformatycznych

1. Zbiory nieinformatyczne powinny być odpowiednio zabezpieczone przed nieuprawnionym dostępem i zniszczeniem.
2. Dokumenty i wydruki, zawierające dane osobowe, należy przechowywać w zamykanych pomieszczeniach, do których dostęp mają jedynie uprawnione osoby.
3. Na czas nieużytkowania, dokumenty i wydruki zawierające dane osobowe powinny być zamykane w szafach biurowych lub zamykanych szufladach.
4. Wydruki robocze, błędne lub zdezaktualizowane powinny być niezwłocznie niszczone przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie lub zanonimizowanie.
5. Dla udokumentowania czynności dokonywanych w celu likwidacji zbiorów archiwalnych, powinny być stosowane odpowiednie przepisy dot. zasad archiwizacji i brakowania dokumentacji Urzędu.

§27. Postanowienia końcowe

1. Niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, naruszenie zasad określonych w niniejszej Polityce może być podstawą rozwiązania stosunku pracy bez wypowiedzenia z osobą, która dopuściła się naruszenia.
2. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (t.j. Dz.U. z 2002 r., Nr 101, poz. 926 z poźn. zm.) oraz przepisy wykonawcze do tej Ustawy.

Deklaracja

1. Administrator Danych Osobowych zobowiązuje się do podjęcia odpowiednich kroków mających na celu zapewnienie prawidłowej ochrony danych osobowych. Zapewnia zaangażowanie w zakresie bezpieczeństwa informacji poprzez:

1) Przetwarzanie danych osobowych zgodnie z prawem,

2) Zbieranie dla oznaczonych, zgodnych z prawem celów i nie poddawanie dalszemu przetwarzaniu niezgodnemu z tymi celami,

3) Aktualizację Polityki Bezpieczeństwa Informacji, w której cele bezpieczeństwa informacji są ustanowione i zgodne z potrzebami właściwego funkcjonowania Urzędu;

4) Wspieranie osób przyczyniających się do osiągnięcia skuteczności funkcjonowania zasad ustalonych w Polityce Bezpieczeństwa Informacji;

5) Promowanie ciągłego doskonalenia;

6) Podnoszenia świadomości pracowników Urzędu o zagrożeniach związanych z bezpieczeństwem informacji.

1. Zasady, działania, kompetencje i zakresy odpowiedzialności opisane w dokumentach Polityki Bezpieczeństwa Informacji obowiązują wszystkich pracowników Urzędu Gminy Nowinka.

2. Zobowiązuję się do spełnienia wymagań dotyczących bezpieczeństwa informacji, podejmowania wszelkich niezbędnych działań zmierzających do ciągłego doskonalenia

Wójt Gminy Nowinka

Dorota Winiewicz

Ewidencja osób upoważnionych do przetwarzania danych osobowych Urzędu Gminy Nowinka (wzór)

L.p.	Imię i nazwisko	Data nadania upoważnienia	Data ustania upoważnienia	Zbiory danych	Uwagi (np. login /zakres upoważnienia jeśli system informatyczny)
1.					
2.					
3.					

Załącznik nr 2
Do Polityki Bezpieczeństwa Informacji
Urzędu Gminy Nowinka

Ewidencja zbiorów danych osobowych przetwarzanych w Urzędzie Gminy Nowinka (wzór)

Nazwa zbioru danych	Program (modul programu) zastosowany do przetwarzania danych	Numer pokoju w którym znajduje się zbiór	Nośnik informacji	Opis struktury zbioru	Data wpisania do Rejestru oraz daty i rodzaj aktualizacji (modyfikacja,zakończenie przetwarzania)	Osoby upoważnione do przetwarzania zbioru,zakres upoważnienia (użytkownik,administrator)	Nr ewidencyjny zbioru	Data i numer zgloszenia do GIODO

Zgłoszenie Zbioru Danych Osobowych do Ewidencji Zbiorów Danych Osobowych przetwarzanych w Urzędzie Gminy Nowinka (wzór)

1. Informuję o planowanym przetwarzaniu niezewidencjonowanego zbioru danych osobowych o nazwie

   .....

2. Data planowanego rozpoczęcia/zakończenia przetwarzania Zbioru Danych Osobowych:

   .....

3. Osoba zgłaszająca Zbiór Danych Osobowych:

   .....

INFORMACJA O ZBIORZE DANYCH OSOBOWYCH			
1. Nazwa zbioru			
NALEŻY WPISAĆ NAZWĘ ZBIORU			
2. Administrator danych: **WÓJT GMINY NOWINKA**			
Administrator:	Gmina Nowinka		
Regon:	790670987		
Miejscowość:	Nowinka	Kod pocztowy:	16-304
Ulica:	brak	Nr domu: 33	Nr lokalu:
Województwo:	podlaskie	Powiat:	augustowski
Gmina:	Nowinka	Poczta:	Nowinka
3. Przedstawiciel Administratora danych, o którym mowa w art. 31a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych:			
4. Powierzenie przetwarzania danych osobowych:			
☐ administrator danych powierzył w drodze umowy zawartej na piśmie przetwarzanie danych innemu podmiotowi (art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych)			
5. Podstawa prawna upoważniająca do prowadzenia zbioru danych:			
☐ zgoda osoby, której dane dotyczą, na przetwarzanie danych jej dotyczących			
☐ przetwarzanie jest niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa:			
NALEŻY WPISAĆ PODSTAWĘ PRAWNĄ PRZETWARZANIA ZBIORU DANYCH OSOBOWYCH			

☐ przetwarzanie jest 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
☐ przetwarzanie jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego
☐ przetwarzanie jest niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą
6. Cel przetwarzania danych w zbiorze:
NALEŻY WPISAĆ CEL PRZETWARZANIA DANYCH
7. Opis kategorii osób, których dane są przetwarzane w zbiorze:
NALEŻY WSKAZAĆ KATEGORIĘ OSÓB, KTÓRYCH DANE SA PRZETWARZANE
8. Zakres danych przetwarzanych w zbiorze:
☐ -imiona i nazwiska ☐ -imiona rodziców ☐ -data urodzenia ☐ - miejsce urodzenia ☐ - adres zamieszkania lub pobytu ☐ - PESEL ☐ - NIP ☐ - miejsce pracy ☐ - zawód ☐ - wykształcenie ☐ - seria i numer dowodu osobistego ☐ - numer telefonu
inne dane osobowe, przetwarzanie w zbiorze:
NALEŻY WSKAZAĆ WSZYSTKIE DANE OSOBOWE PRZETWARZANE W ZBIORZE
dane przetwarzane w zbiorze:
a) ujawniają bezpośrednio lub w kontekście (odpowiednie podkreślić)
Pochodzenie rasowe, pochodzenie etniczne, poglądy polityczne, przekonania religijne, przekonania filozoficzne, przynależność wyznaniową, przynależność partyjną, przynależność związkową, stan zdrowia, kod genetyczny, nałogi, życie seksualne
b) dotyczą (odpowiednie podkreślić) skazań, mandatów karnych, orzeczeń o ukaraniu, innych orzeczeń wydawanych w postępowaniu sądowym lub administracyjnym
podstawa prawna przetwarzania danych wskazanych w pkt 9:
☐ osoby, których dane dotyczą, będą wyrażać na to zgodę na piśmie
☐ przepis szczególny innej ustawy zezwala na przetwarzanie bez zgody osoby, której dane dotyczą, jej danych osobowych (należy podać odniesienie do przepisu)

NALEŻY WSKAZAĆ JEŚLI DOTYCZY
☐ przetwarzanie danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora
☐ przetwarzanie jest niezbędne do wykonania statutowych zadań kościoła, innego związku wyznaniowego, stowarzyszenia, fundacji lub innej niezarobkowej organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, a przetwarzanie danych dotyczy wyłącznie członków tej organizacji lub instytucji albo osób utrzymujących z nią stałe kontakty w związku z jej działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych
☐ przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem
☐ przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie
☐ przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych
☐ przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą
☐ przetwarzanie jest niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego, a publikowanie wyników badań naukowych uniemożliwia identyfikację osób, których dane zostały przetworzone
☐ przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym
9. Dane do zbioru będą zbierane:
☐ od osób, których dotyczą, ☐ z innych źródeł niż osoba, której dotyczą,
10. Dane ze zbioru będą udostępniane:
Dane nie będą udostępniane innym podmiotom niż upoważnione na podstawie przepisów prawa
11. Odbiorcy lub kategorie odbiorców, którym dane mogą być przekazywane: (należy podać nazwę i adres siedziby lub nazwisko i imię oraz adres zamieszkania odbiorcy danych
12. Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego: (należy podać nazwę państwa)

Nowinka, dn. .....

(imię i nazwisko pracownika)

.....
(stanowisko)
.....
(nazwa zakładu pracy)

WNIOSEK

o nadanie / cofnięcie uprawnień do przetwarzania/przebywania w obszarze danych osobowych*)
Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 101, poz. 926 z 2002 r. z późniejszymi zmianami) proszę o nadanie / cofnięcie wszystkich*) uprawnień dla

Pani / Pana .....
Pracownika .....
.....do
wykonywania czynności związanych z przetwarzaniem danych osobowych zawartych w zbiorach o następujących numerach Ewidencji Zbiorów Danych Osobowych przetwarzanych w Urzędzie Gminy Nowinka/ we wszystkich zbiorach dla których Administratorem Danych Osobowych jest Wójt Gminy Nowinka
.....
.....
.....
na okres od ..... do .....

....
Kierownik Komórki Organizacyjnej Administrator Danych Osobowych
*) Niepotrzebne skreślić

.....
Administrator Bezpieczeństwa Informacji

Załącznik nr 5a
Do Polityki Bezpieczeństwa Informacji
Urzędu Gminy Nowinka

.....
(imię i nazwisko pracownika)

Nowinka, dn.....

.....
(stanowisko)

.....
(nazwa zakładu pracy)

OŚWIADCZENIE (wzór)

1. Stwierdzam własnoręcznym podpisem, że znana mi jest treść przepisów:
   a) ustawy o ochronie danych osobowych , ustawy o ochronie informacji niejawnych,
   b) zapoznałem / zapoznałam się z przyjętą polityką bezpieczeństwa i instrukcją zarządzania systemem informatycznym.
2. Jednocześnie zobowiązuję się nie ujawniać wiadomości, z którymi zapoznałem/zapoznałam się z racji wykonywanej pracy w Urzędzie Gminy, a w szczególności nie będę:
   a) ujawniać danych zawartych w eksploatowanych w Urzędzie systemach informatycznych, zwłaszcza danych osobowych znajdujących się w tych systemach,
   b) ujawniać szczegółów technologicznych używanych w Urzędzie systemów oraz oprogramowania,
   c) instalować jakiegokolwiek oprogramowania bez wcześniejszego uzgodnienia z Administratorem Bezpieczeństwa Informacji,
   d) udostępniać osobom nieupoważnionym nośników magnetycznych i optycznych oraz wydruki komputerowe z zapisanymi danymi osobowymi,
   e) kopiować lub przetwarzać danych w sposób inny niż dopuszczony obowiązującą instrukcją.

.....
(data i podpis pracownika)

Oświadczenie sporządza się w 3 egzemplarzach:
-do dokumentacji prowadzonej przez ABI,
-do akt osobowych,
-kopia dla osoby oświadczającej

Załącznik nr 5b
Do Polityki Bezpieczeństwa Informacji
Urzędu Gminy Nowinka

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym, jako Administrator Danych Osobowych Urzędu Gminy Nowinka na podstawie art. 37 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2014 r. poz.1182 **upoważniam:**

Imię i nazwisko upoważnionego pracownika	
Zbiory danych objęte zakresem upoważnienia	

Osoba upoważniona obowiązana jest przetwarzać dane osobowe zawarte w ww. zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administratora Danych.

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2014 r., poz. 1182), wydanymi na jej podstawie aktami wykonawczymi i obowiązującymi w wewnętrznymi regulacjami w sprawie ochrony danych osobowych.

Naruszenie ww. obowiązków może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów określonych w Ustawie o ochronie danych osobowych oraz stanowi ciężkie naruszenie obowiązków pracowniczych, które może być podstawą rozwiązania umowy o pracę w trybie art. 52 Kodeksu Pracy.

Upoważnienie jest ważne do odwołania lub do dnia wprowadzenia nowego wzoru upoważnień. Upoważnienie staje się nieważne z dniem ustania stosunku pracy pomiędzy osobą upoważnioną, a ADO.

Data i podpis ADO

Data i podpis osoby upoważnionej

Oświadczenie sporządza się w 3 egzemplarzach:
-do dokumentacji prowadzonej przez ABI,
-do akt osobowych,
-kopia dla osoby oświadczającej

Załącznik nr 5c
Do Polityki Bezpieczeństwa Informacji
Urzędu Gminy Nowinka

UPOWAŻNIENIE DO PRZEBYWANIA W OBSZARZE PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym, jako Administrator Danych Osobowych Urzędu Gminy Nowinka na podstawie art. 37 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2014 r. poz.1182 **upoważniam:**

Imię i nazwisko upoważnionego pracownika	

do przebywania w pomieszczeniach, w których przetwarzane są dane osobowe w zakresie niezbędnym do wykonywania

- ☐ obowiązków służbowych
- ☐ prac zleconych
- ☐ szczegółowych zadań, jak .....

Upoważnienie jest ważne do dnia ..... / do odwołania

Data i podpis ADO

Data i podpis osoby upoważnionej

Oświadczenie sporządza się w 3 egzemplarzach:
-do dokumentacji prowadzonej przez ABI,
-do akt osobowych,
-kopia dla osoby oświadczającej

Załącznik nr 6
Do Polityki Bezpieczeństwa Informacji
Urzędu Gminy Nowinka

Upoważnienie do zarządzania kluczami oraz kodem cyfrowym do systemu alarmowego budynku Urzędu Gminy Nowinka (wzór)

Na podstawie **Polityki Bezpieczeństwa Informacji Urzędu Gminy Nowinka** wprowadzonej Zarządzeniem Nr 20/17 z dnia 10 marca 2017r. Wójta Gminy Nowinka **powierzam Pani(u)** **(niepotrzebne skreślić)**

.....

zatrudnionej(mu) na stanowisku

.....

1. Komplet kluczy/klucz do .....

W skład kompletu wchodzą następujące klucze:

1. .....
2. .....
3. .....
4. .....

.....
(data i podpis pracownika)

.....
(podpis ADO)

.....
(podpis ABI)

2. Kod cyfrowy do systemu alarmowego, który należy zachować w ścisłej tajemnicy i wykorzystywać zgodnie z postanowieniami w/w instrukcji.

.....
(data i podpis pracownika)

.....
(podpis ADO)

.....
(podpis ABI)

Oświadczenie pracownika

Oświadczam, że przyjmuję pełną odpowiedzialność za powierzone klucze oraz kod cyfrowy do systemu alarmowego *(niepotrzebne skreślić)* i zobowiązuję się do ich wykorzystywania jedynie w celach realizacji powierzonych mi zadań zgodnie z niniejszym upoważnieniem i postanowieniami zawartymi w Polityce Bezpieczeństwa Informacji.

.....
(data i podpis pracownika)

Procedura Alarmowa
Polityki Bezpieczeństwa w Urzędzie Gminy Nowinka

1. **Procedura alarmowa.** Procedura alarmowa wskazuje na możliwe zagrożenia oraz definiuje **„Dziennik Uchybień i Zagrożeń"**, związany z niewłaściwym przetwarzaniem danych osobowych lub ich wyciekiem. Celem Procedury Alarmowej jest skatalogowanie możliwych uchybień i zagrożeń oraz opisanie procedur działania w przypadku ich wystąpienia, jak i również ograniczenie ich powstania w przyszłości. Integralną częścią Procedury Alarmowej jest **„Dziennik Uchybień i Zagrożeń"**- (załącznik nr 1), **„Protokół Zagrożenia"** - (załącznik nr 2), **„Protokół Uchybienia"** - (załącznik nr 3), prowadzony przez ABI w przypadku stwierdzenia naruszenia ochrony danych osobowych w podmiocie.

2. **Charakterystyka możliwych „Uchybień i Zagrożeń".**

I. Uchybienia i zagrożenia nieświadome wewnętrzne i zewnętrzne. Do uchybień i zagrożeń nieświadomych wewnętrznych i zewnętrznych należą działania pracowników podmiotu lub osób nie będących pracownikami podmiotu, w następstwie których może dojść lub doszło do zniszczenia danych, wycieku danych lub naruszenia ich poufności. W szczególności są to działania takie jak:

- *niewłaściwe zabezpieczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe,*
- *niewłaściwe zabezpieczenie sprzętu komputerowego,*
- *dopuszczenie do przetwarzania danych przez osoby nieposiadające upoważnienia,*
- *pomyłki informatyków,*
- *kradzież danych,*
- *kradzież sprzętu informatycznego,*
- *działanie wirusów i innego szkodliwego oprogramowania oraz inne działania, wskutek których dojdzie do utraty danych osobowych lub uszkodzenia nośników danych.*

II. Uchybienia i zagrożenia umyślne wewnętrzne i zewnętrzne. Do uchybień i zagrożeń umyślnych wewnętrznych i zewnętrznych należą celowe działania pracowników podmiotu, w następstwie których może dojść lub doszło do zniszczenia danych, wycieku danych lub naruszenia ich poufności. W szczególności są to działania takie jak:

- *celowe zniszczenie danych osobowych lub nośników danych,*
- *kradzież danych osobowych,*
- *dopuszczenie do przetwarzania danych przez osoby nieposiadające upoważnienia,*
- *kradzież danych,*
- *kradzież sprzętu informatycznego,*
- *działanie wirusów i innego szkodliwego oprogramowania oraz inne działania, wskutek których dojdzie do utraty danych osobowych lub uszkodzenia nośników danych.*

III. Uchybienia i zagrożenia losowe. Do uchybień i zagrożeń losowych należą sytuacje losowe, w następstwie których może dojść lub doszło do zniszczenia danych, wycieku danych lub naruszenia ich poufności. W szczególności są to sytuacje takie jak:

- *klęski żywiołowe,*
- *przerwy w zasilaniu,*
- *awarie serwera,*
- *pożar,*
- *zalanie wodą.*

3. **Procedura postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych.** Każdy pracownik podmiotu posiadający upoważnienie do przetwarzania danych osobowych, w przypadku stwierdzenia uchybienia lub zagrożenia ma obowiązek niezwłocznie powiadomić o tym fakcie Administratora Bezpieczeństwa Informacji. Administrator Bezpieczeństwa Informacji w przypadku stwierdzenia **uchybienia** ma obowiązek:

1. odnotować każde uchybienie w „**Dzienniku Uchybień i Zagrożeń**",

2. sporządzić „**Protokół Uchybienia**",

3. wprowadzić procedury uniemożliwiające ponowne powstanie uchybienia. Administrator Bezpieczeństwa Informacji w przypadku stwierdzenia **zagrożenia** ma obowiązek:

1. zabezpieczyć dowody, powiadomić policję (w przypadku włamania),

2. zabezpieczyć dane osobowe oraz nośniki danych,

3. odnotować każde zagrożenie w „**Dzienniku Uchybień i Zagrożeń**",

4. sporządzić „**Protokół Zagrożenia**",

5. wprowadzić procedury uniemożliwiające ponowne powstanie zagrożenia,

6. podjąć próbę przywrócenia stanu sprzed zaistnienia zagrożenia,

7. Administrator Bezpieczeństwa Informacji składa wniosek do Administratora Danych Osobowych o wyciągnięcie konsekwencji dyscyplinarnych wobec osób odpowiedzialnych za zagrożenie.

4. **Rejestr Uchybień i Zagrożeń oraz szczegółowa instrukcja postępowania dla osób posiadających upoważnienie do przetwarzania danych osobowych w podmiocie**

Kod uchybienia lub zagrożenia	Uchybienia i zagrożenia nieświadome wewnętrzne i zewnętrzne	Postępowanie w przypadku uchybienia lub zagrożenia
1	Pomieszczenie, w którym przechowywane są dane osobowe pozostaje bez nadzoru.	Należy zabezpieczyć dane osobowe oraz powiadomić ABI. ABI sporządza protokół uchybienia.
2	Komputer nie jest zabezpieczony hasłem.	Należy zabezpieczyć dane osobowe oraz powiadomić ABI. ABI sporządza protokół uchybienia.
3	Dostęp do danych osobowych mają osoby nieposiadające upoważnienia.	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić ABI. ABI sporządza protokół uchybienia.
4	Nieuprawniony dostęp do otwartych aplikacji w systemie informatycznym.	Należy powiadomić ABI, który we współpracy z ASI powinien sprawdzić system uwierzytelniania oraz czy nie doszło do kradzieży lub zniszczenia danych. ABI sporządza protokół uchybienia.
5	Próba kradzieży danych osobowych poprzez zewnętrzny nośnik danych.	Należy nie dopuścić do kradzieży danych i powiadomić ADO. ABI powinien zabezpieczyć nośnik danych i sporządzić protokół zagrożenia.
6	Próba kradzieży danych osobowych w formie papierowej.	Należy nie dopuścić do kradzieży danych i powiadomić ABI. ABI powinien zabezpieczyć dane i sporządzić protokół zagrożenia.
7	Nieuprawniony dostęp do danych osobowych w formie papierowej.	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić ABI. ABI sporządza protokół uchybienia.
8	Dane osobowe przechowywane są w niezabezpieczonym pomieszczeniu.	Należy powiadomić ABI. ABI powinien zabezpieczyć pomieszczenie. ABI sporządza protokół uchybienia.
9	Próba włamania do pomieszczenia/budynku.	Należy zabezpieczyć dowody i powiadomić ABI. ABI sprawdza stan uszkodzeń, zabezpiecza dowody i wzywa policję. ABI sporządza protokół zagrożenia.
10	Działanie zewnętrznych aplikacji, wirusów, złośliwego oprogramowania.	Należy zrobić audyt systemów zabezpieczeń, a w szczególności systemów antywirusowych, firewall. ABI we współpracy z ASI powinien ocenić, czy nie doszło do

		utraty danych osobowych i w zależności od tego sporządzić protokół uchybienia lub zagrożenia.
11	Brak aktywnego oprogramowania antywirusowego.	Należy powiadomić ABI. ABI powinien zlecić ASI aktualizację lub zakup oprogramowania antywirusowego. ABI sporządza protokół uchybienia.
12	Zniszczenie lub modyfikacja danych osobowych w formie papierowej.	Należy zabezpieczyć dowody i powiadomić ABI. ABI sprawdza stan uszkodzeń, zabezpiecza dowody i sporządza protokół zagrożenia.
13	Zniszczenie lub modyfikacja danych osobowych w systemie informatycznym.	Należy zabezpieczyć dowody i powiadomić ABI. ABI we współpracy z ASI sprawdza stan uszkodzeń, zabezpiecza dowody i sporządza protokół zagrożenia.
14	Uszkodzenie komputerów, nośników danych.	Należy powiadomić ABI. ABI we współpracy z ASI powinien ocenić w wyniku czego doszło do zniszczenia, sporządzić protokół zagrożenia. ASI powinien przywrócić dane z kopii zapasowej.
15	Próba nieuprawnionej interwencji przy sprzęcie komputerowym.	Należy uniemożliwić dostęp osób do sprzętu komputerowego oraz powiadomić ABI. ABI sporządza protokół uchybienia.
16	Zdarzenia losowe.	Należy oszacować powstałe straty i sporządzić protokół zagrożenia lub uchybienia.

„Dziennik Uchybień i Zagrożeń"

Kod	Data i godzina zdarzenia	Rodzaj zdarzenia *(uchybienie/ zagrożenie)*	Opis zdarzenia	Skutki zdarzenia	Działania naprawcze	Podpis ABI/ASI

Nazwa i adres podmiotu

.....

Miejscowość i data

.....

„Protokół Zagrożenia"

Data i godzina wystąpienia zagrożenia

.....

.....

Kod zagrożenia

.....

Opis zagrożenia

.....

.....

.....

.....

.....

Przyczyny powstania zagrożenia

.....

.....

.....

.....

.....

Zaistniałe skutki zagrożenia

.....

.....

.....

.....

.....

.....

Podjęte działania naprawczo-zapobiegawcze

.....

.....

.....

.....

.....

Administrator Bezpieczeństwa Informacji

.....

Nazwa i adres podmiotu

Miejscowość i data

.....
.....

„Protokół Uchybienia"

Data i godzina wystąpienia uchybienia.....

Kod uchybienia

.....

Opis uchybienia

.....
.....
.....
.....
.....

Przyczyny powstania uchybienia

.....
.....
.....
.....
.....

Zaistniałe skutki uchybienia

.....
.....
.....
.....
.....

Podjęte działania naprawczo-zapobiegawcze

.....
.....
.....
.....
.....

Administrator Bezpieczeństwa Informacji

.....