ZATWIERDZAM
STAROSTA KAMIEŃSKI
Beata KIRYLUK
Kamień Pomorski, dn. 24 maja 2013 roku

Polityka Bezpieczeństwa Danych Osobowych

w Starostwie Powiatowym w Kamieniu Pomorskim
ul. Wolińska 7b

OPRACOWAŁ : Andrzej ZIELIŃSKI
Pełnomocnik
ds. Ochrony Informacji Niejawnych

Spis treści

Wstęp

Celem Polityki Bezpieczeństwa jest zapewnienie ochrony danych osobowych przetwarzanych przez Starostwo Powiatowe w Kamieniu Pomorskim przed wszelkiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.

Polityka określa obowiązki Administratora Danych w zakresie zabezpieczenia danych osobowych, o których mowa w art. 36 Ustawy o Ochronie Danych Osobowych. (Dz. U. z 2002 r. Nr 101, poz. 926)

Polityka określa reguły dotyczące zapewnienia bezpieczeństwa danych osobowych w postaci papierowej oraz zawartych w systemach informatycznych w Starostwie Powiatowym w Kamieniu Pomorskim.

Jako załącznik do niniejszej polityki opracowano i wdrożono „ Instrukcje zarządzania systemem informatycznym służącym do przetwarzania danych osobowych", zwaną dalej „Instrukcją zarządzania systemem informatycznym".
Określa ona sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem zapewnienia ich bezpieczeństwa.

Polityka została opracowana zgodnie z wymogami określonymi w § 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych , jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004r. Nr 100, poz. 1024).

Polityka obowiązuje wszystkich pracowników Starostwa Powiatowego w Kamieniu Pomorskim oraz dostawców, podmiotów współpracujących na zasadzie umów, mających jakikolwiek kontakt z danymi osobowymi objętymi ochroną.

Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.

Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

1. Poufność danych - rozumiana jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom .
2. Integralność danych – rozumianą jako właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
3. Rozliczalność danych – rozumiana jako właściwość zapewniająca, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie.
4. Integralność systemu rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

1. Definicje

Przez użyte w Polityce określenia należy rozumieć :

1.1 **Polityka** – rozumie się przez to politykę bezpieczeństwa danych osobowych w Starostwie Powiatowym w Kamieniu Pomorskim.

1.2 **Administrator Danych Osobowych (ADO)** – Starosta Kamieński (zwany dalej Starostą) decydujący o celach i środkach i sposobach przetwarzania danych osobowych.

1.3 **Administrator Bezpieczeństwa Informacji (ABI)** – pracownik Starostwa , wyznaczony przez Administratora Danych Osobowych (ADO), odpowiedzialny za organizacje ochrony danych osobowych

1.4 **Administrator Systemu Informatycznego (ASI)** - osoba wyznaczona przez Administratora Danych Osobowych (ADO), odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych we wskazanych systemach informatycznych nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagających specjalnych uprawnień. ASI odpowiedzialny jest za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych

1.5 **Ustawa** – ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.)

1.6 **Rozporządzenie** – Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 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 2004 r. Nr 100, poz. 1024)

1.7 **Baza danych osobowych** – zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci zewnętrznej komputera . Baza danych jest złożona z elementów o określonej strukturze.- rekordów lub obiektów.

1.8 **Dane osobowe (dane)** –wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

1.9 **Hasło** - ciąg znaków literowych, cyfrowych lub innych , znanych jedynie osobie uprawnionej do pracy w systemie informatycznym.

1.10 **Identyfikator użytkownika** – ciąg znaków literowych , cyfrowych lub innych , jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

1.11 **Integralność danych** – właściwość zapewniająca , ze dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

1.12 **Nośnik komputerowy** – nośnik służący do zapisu i przechowywania informacji, np. taśmy, dyski twarde .

1.13 **Odbiorca danych** – każdy, komu udostępnia się dane osobowe, z wyłączeniem :
- osoby, której dane dotyczą;
- osoby upoważnionej do przetwarzania danych;
- podmiotu, o którym mowa w art. 31 ustawy;
- przedstawiciela, o którym mowa w art. 31a ustawy;
- organów państwowych lub organów samorządu terytorialnego, którym dane są udostępnione w związku z prowadzonym postępowaniem.

1.14 **Poufność danych** – właściwość zapewniająca, że dane nie są udostępnione nieupoważnionym podmiotom.

1.15 **Przetwarzanie danych**- wykonywanie jakichkolwiek operacji na danych osobowych, np. zbieranie , utrwalanie, opracowywanie, udostępnianie, zmienianie , usuwanie.

1.16 **Rozliczalność**- właściwość zapewniająca , że działania podmiotu mogą być przypisane

w sposób jednoznaczny tylko temu podmiotowi.

1.17 **Raport** – przygotowane przez system informatyczny zestawienie zakresu i treści przetwarzanych danych.

1.18 **Publiczna Sieć Telekomunikacyjna** - sieć publiczna w rozumieniu art. 2 pkt. 29 z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr. 171, poz. 1800).

1.19 **Sieć telekomunikacyjna** – sieć telekomunikacyjna w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.

1.20 **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

1.21 **Teletransmisja** - przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej.

1.22 **Usuwanie danych**- zniszczenie danych osobowych lub taką ich modyfikacje , która nie pozwoli na ustalenie tożsamości osoby , której dane dotyczą .

1. 23 **Uwierzytelnienie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

1.24 **Użytkownik** – pracownik Starostwa Powiatowego w Kamieniu Pomorskim, posiadający uprawnienia do przetwarzania danych osobowych w zakresie obowiązujących przepisów o ochronie danych osobowych.

1.25 **Zabezpieczenie danych w systemie informatycznym** - wdrożenie i eksploatacja stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

1.26 **Zbiór danych** – zestaw danych osobowych posiadający określoną strukturę, prowadzony wg określonych kryteriów oraz celów np. zbiór pracowników Starostwa Powiatowego w Kamieniu Pomorskim, zbiór interesantów Starostwa Powiatowego w Kamieniu Pomorskim.

1.27 **Zgoda osoby , której dane dotyczą** – oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

2. Zadania Administratora Danych Osobowych (ADO)

Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki.

Administrator danych wyznacza administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony oraz administratora sieci informatycznej.

3. Zadania i uprawnienia Administratora Bezpieczeństwa Informacji (ABI)

Do najważniejszych obowiązków Administratora Bezpieczeństwa Informacji (ABI) należy :

3.1 Organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych.

3.2 Zapewnienie przetwarzania danych zgodnie z uregulowaniami niniejszej polityki.

3.3 Rejestracja zbiorów danych oraz wszelkich zmian z nimi związanych.
3.4 Prowadzenie „ Ewidencji osób upoważnionych do przetwarzania danych osobowych"
3.5 Prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych.
3.6 Nadzór nad bezpieczeństwem danych osobowych.
3.7 Kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych.
3.8 Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych w Starostwie Powiatowym w Kamieniu Pomorskim.
Administrator Bezpieczeństwa Informacji ma prawo :
3.9 Wstępu do pomieszczeń, w których zlokalizowane są zbiory danych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą.
3.10 Żądać złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego.
3.11 Żądać okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli.
3.12 Żądać udostępnienia do kontroli urządzeń , nośników oraz systemów informatycznych służących do przetwarzania danych.

4. Zadania Administratora Systemu Informatycznego (ASI)

Do obowiązków Administratorów Systemu Informatycznego (ASI) w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:

1) Operacyjne zarządzanie systemami informatycznymi w sposób zapewniający ochronę danych osobowych w nich przetwarzanych.
2) Przestrzeganie opracowanych dla systemu procedur operacyjnych i bezpieczeństwa.
3) Kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej a systemem informatycznym.
4) Zarządzanie stosowanymi w systemach informatycznym środkami uwierzytelnienia, w tym rejestrowanie i wyrejestrowywanie użytkowników oraz dokonywanie zmiany uprawnień na podstawie zaakceptowanych wniosków przez osobę do tego upoważnioną.
5) Utrzymanie systemu w należytej sprawności technicznej.
6) Regularne tworzenie kopii zapasowych zasobów danych osobowych oraz programów służących do ich przetwarzania oraz okresowe sprawdzanie poprawności wykonania kopii zapasowych.
7) Wykonywanie lub nadzór nad wykonywaniem okresowych przeglądów i konserwacji, zgodnie z odrębnymi procedurami, sprzętu IT, systemów informatycznych, aplikacji oraz elektronicznych nośników informacji, na których zapisane są dane osobowe.

5. Wykaz pomieszczeń lub części pomieszczeń, tworzących obszar , w którym przetwarzane są dane osobowe.

Szczegółowe rozmieszczenie zbiorów dokumentacji papierowej i elektronicznej, zawierającej dane osobowe, opisane jest w Załączniku A – „ Wykaz zbiorów danych osobowych"

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

Wykaz zbiorów danych osobowych w postaci dokumentacji papierowej i elektronicznej wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych , opisany jest w Załączniku A – „ Wykaz zbiorów danych osobowych".

7. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.

Wykaz zbiorów danych osobowych zawierających informację o rodzaju danych osobowych opisany w Załączniku B – „ Opis struktury zbiorów danych osobowych".
Programy z zakresem przetwarzanych danych osobowych zawiera Załącznik Ba – „ Struktura baz danych osobowych w Starostwie Powiatowym w Kamieniu Pomorskim".

8. Sposób przepływu danych pomiędzy poszczególnymi systemami

System / Moduł „A"	System / Moduł „B"	Kierunek przepływu danych osobowych	Sposób przesyłania danych osobowych
Program PłaceWin	Program Płatnik	Jednokierunkowo z programu PłaceWin do Programu Płatnik	Manualnie przez wskazanie wygenerowanego pliku

9. Środki techniczne i organizacje niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

9.1 Środki ochrony fizycznej:

9.1.1 Podstawowe zabezpieczenie fizyczne opisane w załączniku A – „ Wykaz zbiorów danych osobowych".
9.1.2 Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieuprawnionych.
9.1.3 Przebywanie osób nieuprawnionych w pomieszczeniach , gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych.
9.1.4 Kopie zapasowe/ archiwalne zbioru danych osobowych w formie elektronicznej przechowywane są w zamkniętej szafie metalowej.

9.2 Środki sprzętowe , informatyczne i telekomunikacyjne:

9.2.1 Pomieszczenia , w których przetwarzane są dane osobowe zabezpieczone są przed skutkami pożaru za pomocą wolnostojącej gaśnicy.
9.2.2 Dokumenty zawierające dane osobowe po ustaleniu przydatności są niszczone przez pocięcie w niszczarce.
9.2.3 Sprzęt komputerowy służący do przetwarzania danych osobowych połączony jest z siecią publiczną (Internetem) za pośrednictwem urządzeń klasy UMT pełniących rolę bramy zabezpieczającej przed niepowołanym dostępem.
9.2.4 Lokalizacja urządzeń komputerowych (komputerów typu PC , laptop, drukarek) uniemożliwia osobom niepowołanym dostęp do nich oraz wgląd do danych wyświetlanych na monitorach komputerowych.
9.2.5 Komputery przenośne wykorzystywane do przetwarzania danych osobowych , po zakończonej pracy są przechowywane w warunkach zapewniających ich bezpieczeństwo
9.2.6 Zastosowano lokalne zasilanie awaryjne (UPS) oraz Centralny UPS obiektowy urzędu, chroniące system informatyczny służący do przetwarzania danych osobowych przed awarią zasilania.

9.3 Środki ochrony w ramach oprogramowania urządzeń teletransmisji.

9.3.1 W razie wystąpienia konieczności wymiany danych pomiędzy urzędem a jednostkami zestawiany jest tunel zapewniający poufność i integralność przesyłanych danych (szyfrowanie, sumy kontrolne) oparty o IPSEC.
9.3.2 Do połączenia z serwerem poczty wykorzystywane jest połączenie w wykorzystaniem algorytmu SSL zapewniające poufność danych używanych do autoryzacji i uwierzytelnienia.
9.3.3 Dostęp do Internetu realizowany jest za pomocą urządzeń klasy UTM zapewniających ochronę przed nieautoryzowanym dostępem z zewnątrz.

9.4 Środki ochrony w ramach oprogramowania systemu

9.4.1 Dostęp do zbioru danych osobowych przetwarzanych za pomocą komputera zabezpieczony jest za pomocą hasła.
9.4.2 Zapewniono rejestrację czasu nieudanych logowań do systemu przetwarzającego dane osobowe.
9.4.3 Zastosowano system operacyjny pozwalający na określenie odpowiednich praw dostępu do zasobów informatycznych dla poszczególnych użytkowników systemu informatycznego.
9.4.4 Zastosowano oprogramowanie umożliwiające wykonanie kopii zapasowych zbiorów danych osobowych.
9.4.5 Zastosowano oprogramowanie zabezpieczające przed nieuprawnionym dostępem do systemu informatycznego.

9.5 Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych :

9.5.1 Dostęp do zbioru danych osobowych zabezpieczony jest za pomocą procesu autoryzacji i uwierzytelniania z wykorzystaniem identyfikatora użytkownika oraz hasła na poziomie aplikacji systemu służącego do przetwarzania zbioru.
9.5.2 Zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji.
9.5.3 Dla każdego użytkownika systemu jest ustalony odrębny identyfikator.

9.5.4 O ile aplikacja ta umożliwia , zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.

9.6 Środki ochrony w ramach systemu operacyjnego stacji roboczych:

9.6.1 Zastosowano zabezpieczone hasłem wygaszanie ekranu w przypadku dłuższej nieaktywności użytkownika.
9.6.2 Zastosowano działający w „tle" program antywirusowy na komputerach użytkowników.

9.7 Środki organizacyjne:

9.7.1 Wyznaczono Administratora Bezpieczeństwa Informacji (ABI) i Administratora Systemu Informatycznego (ASI).
9.7.2 Opracowano i wdrożono Politykę bezpieczeństwa i Instrukcję zarządzania systemem informatycznym.
9.7.3 Wdrożono odpowiedni podział obowiązków i kontroli.
9.7.4 Do danych osobowych mają jedynie osoby posiadające upoważnienie nadane przez Administratora Bezpieczeństwa Informacji (ABI) .
9.7.5 ABI prowadzi „ Ewidencję osób upoważnionych do przetwarzania danych osobowych".
9.7.6 Wprowadzono mechanizmy uwierzytelniania i autoryzacji odpowiednio zabezpieczone przed dostępem osób trzecich.
9.7.7 Wprowadzono procedury alarmowe i informacyjne.
9.7.8 Osoby upoważnione do przetwarzania danych osobowych przed dopuszczeniem do tych danych są szkolone w zakresie obowiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych osobowych.
Osoby te są zobowiązane do podpisania stosownego oświadczenia.
9.7.9 Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane są do zachowania ich w tajemnicy.
9.7.10 Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym .
9.7.11 Tymczasowe wydruki z danymi osobowymi są po ustaleniu ich przydatności niszczone przez pocięcie w niszczarce
9.7.12 Zapewniono bezpieczne przechowywanie nośników zawierających dane osobowe (np. dysk twardy) szczególnie , gdy sprzęt, w którym zamontowany jest dany nośnik przekazywany jest do naprawy poza siedzibę urzędu.
9.7.13 Zobowiązano użytkowników do należytego zabezpieczenia dokumentów zawierających dane osobowe po zakończeniu pracy.

10. Instrukcja alarmowa (postępowania w przypadku naruszenia ochrony danych osobowych).

Procedury reagowania na zdarzenia zagrażające bezpieczeństwu danych osobowych określające :

- Czym są zagrożenia i naruszenia danych osobowych ;
- Sposób reagowania , gdy wystąpią one w rzeczywistości;
- Sposób postępowania po wystąpieniu naruszenia;

10.1 Zdarzenia zagrażające bezpieczeństwu danych osobowych

Do zdarzeń zagrażających bezpieczeństwu danych osobowych należą:

10.1.1 próby naruszenia ochrony danych :
a) z zewnątrz – włamania do systemu , podsłuch, kradzież danych,
b) z wewnątrz - nieumyślna lub celowa modyfikacja danych, kradzież danych,

10.1.2 programy destrukcyjne :
a) wirusy
b) konie trojańskie
c) makra
d) bomby logiczne
10.1.3 awarie sprzętu lub uszkodzenie oprogramowania,
10.1.4 zabór sprzętu lub nośników z ważnymi danymi,
10.1.5 inne skutkujące utratą danych osobowych, bądź wejściem w ich posiadanie osób nieuprawnionych.
10.1.6 usiłowanie zakłócenia działania systemu informatycznego.

10.2 Procedura postępowania w przypadkach naruszenia bezpieczeństwa danych osobowych

10.2.1 W przypadku stwierdzenia faktu nieuprawnionego przetwarzania, ujawniania lub nienależytego zabezpieczenia przed osobami nieuprawnionymi danych osobowych, jak również stwierdzenia istnienia przesłanek wskazujących na prawdopodobieństwo naruszenia ochrony danych osobowych , każdy pracownik Starostwa Powiatowego w Kamieniu Pomorskim zobowiązany jest poinformować o zdarzeniu Administratora Bezpieczeństwa Informacji , a ten Administratora Danych Osobowych.
10.2.2 W sytuacji , określonej pkt. 1, Administrator Bezpieczeństwa Informacji prowadzi postępowanie wyjaśniające w toku, którego:
1) ustala czas wystąpienia naruszenia , jego zakres , przyczyny, skutki oraz wielkość szkód, które zaistniały ,
2) ustala osoby odpowiedzialne za naruszenie,
3) podejmuje działania w kierunku ograniczania szkód oraz przeciwdziałania podobnym przypadkom w przyszłości,
4) sporządza pisemną notatkę z przeprowadzonego postępowania.
10.2.3 Administrator Bezpieczeństwa Informacji (ABI) powiadamia o wynikach postępowania wyjaśniającego Administratora Danych Osobowych.
10.2.4 W przypadku zaistnienia zdarzenia , określonego w ust. 1, decyzje dyscyplinarne w stosunku do winnych oraz w sprawie wniosku o pociągnięcie ich do odpowiedzialności karnej podejmuje Administrator Danych Osobowych.

10.3 Procedura postępowania w przypadkach zagrożeń (stwierdzenia słabości systemu)

10.3.1 W przypadku jakiejkolwiek nieprawidłowości w działaniu systemu, uszkodzenia lub podejrzenia o uszkodzeniu sprzętu, oprogramowaniu lub danych należy bezzwłocznie powiadomić Administratora Bezpieczeństwa Informacji (ABI).

10.3.2 W przypadku włamania lub podejrzenia o włamanie do systemu Administrator Systemu Informatycznego (ASI) podejmuje działania w celu zabezpieczenia systemu i danych :

1) zmienia hasła administracyjne , określa rodzaj i sposób włamania,
2) podejmuje działania w celu uniemożliwienia ponownego włamania tego samego typu.
3) Szacuje straty w systemie,
4) Przywraca stan systemu sprzed włamania.

10.3.3 W przypadku uszkodzenia sprzętu lub programów z danymi Administrator Systemu Informatycznego podejmuje działania w celu :

1) Określenia przyczyny uszkodzenia ,
2) Oszacowania strat wynikłych z w/w uszkodzenia,
3) Naprawy uszkodzeń, a w szczególności naprawy sprzętu, ponownego zainstalowania danego programu , odtworzenie jego pełnej konfiguracji oraz wczytania danych z ostatniej kopi zapasowej .

10.3.4 W przypadku uszkodzenia danych Administrator Systemu Informatycznego podejmuje następujące działania:

1) Ustala przyczynę uszkodzenia danych,
2) Określa wielkości i jakość uszkodzonych danych
3) Podejmuje działania w celu odtworzenia danych z ostatniej kopii zapasowej.

10.3.5 W przypadku stwierdzenia nieprawidłowości w funkcjonowaniu sieci telekomunikacyjnej każdy użytkownik zobowiązany jest niezwłocznie powiadomić Administratora Systemu Informatycznego, który podejmuje działania w celu ustalenia przyczyn zaistniałej sytuacji oraz wyeliminowania nieprawidłowości.

W przypadku zidentyfikowania osób odpowiedzialnych za wystąpienie któregoś ze zdarzeń zagrażających bezpieczeństwu danych Administrator Bezpieczeństwa Informacji (ABI) zobowiązany jest powiadomić Administratora Danych Osobowych (ADO).

11 Procedura działań korygujących i zapobiegawczych

11.1 Celem procedury jest uporządkowanie i przedstawienie czynności związanych z inicjowaniem oraz realizacją działań korygujących i zapobiegawczych wynikających z zaistnienia incydentów naruszenia bezpieczeństwa lub słabości systemu ochrony danych osobowych .

11.2 Procedura działań korygujących i zapobiegawczych obejmuje wszystkie procesy, w których incydenty bezpieczeństwa, zagrożenia lub słabości systemu ochrony danych osobowych mogą wpłynąć na zgodność z wymaganiami ustawy, jak również na poprawne funkcjonowanie systemu ochrony danych osobowych.

11.3 Osobą odpowiedzialną za nadzór nad procedurą jest Administrator Bezpieczeństwa Informacji (ABI) Przy czym czynności związane z realizacją poszczególnych zadań , zabezpieczeń zatwierdza Administrator Danych Osobowych (ADO).

11.4 Definicje:

1) **Niezgodność**- niespełnienie wymagania, czyli potrzeby lub oczekiwania , które zostało ustalone, przyjęte zwyczajowo lub jest obowiązkowe.
2) **Incydent**- naruszenie bezpieczeństwa informacji ze względu na poufność , dostępność i integralność.
3) **Zagrożenie**- potencjalna możliwość wystąpienia incydentu.

4) **Słabość systemu**- zdarzenie, stan rzeczy zwiększający ryzyko wystąpienia incydentu
5) **Działania korygujące**- jest to działanie przeprowadzone w celu wyeliminowania przyczyny niezgodności / incydentu lub innej niepożądanej sytuacji.
6) **Działanie zapobiegawcze**- jest to działanie , które należy przedsięwziąć , aby wyeliminować przyczyny potencjalnej niezgodności / incydentu lub innej potencjalnej sytuacji niepożądanej.
7) **Korekcja**- działanie w celu wyeliminowania wykrytej niezgodności lub incydentu.
8) **Kontrola (Audyt)**- systematyczny, niezależny i udokumentowany proces oceny skuteczności systemu ochrony danych osobowych , na podstawie określonych kryteriów , wymagań , polityk i procedur.

11.5 Opis czynności Administratora Bezpieczeństwa Informacji (ABI):

11.5.1 Administrator Bezpieczeństwa Informacji (ABI) , jest odpowiedzialny za analizę incydentów naruszenia bezpieczeństwa , zagrożeń lub słabości systemu ochrony danych osobowych. Typowymi źródłami informacji o incydentach, zagrożeniach lub słabościach są:
1) zgłoszenia od pracowników;
2) alarmy z systemów informatycznych;
3) analizy incydentów;
4) wyniki audytów/ kontroli;

11.5.2 W sytuacji gdy Administrator Bezpieczeństwa Informacji (ABI) stwierdzi konieczność podjęcia działań korygujących lub zapobiegawczych , określa:
1) źródło powstania incydentu/ zagrożenia lub słabości;
2) zakres działań korygujących lub zapobiegawczych;
3) termin realizacji;
4) osobę odpowiedzialną .

11.5.3 Administrator Bezpieczeństwa Informacji (ABI) jest odpowiedzialny za nadzór nad poprawnością i terminowością wdrażanych działań korygujących i zapobiegawczych.

11.5.4 Po przeprowadzeniu działań korygujących lub zapobiegawczych, Administrator Bezpieczeństwa Informacji (ABI) jest zobowiązany do oceny efektywności ich zastosowania.

11.5.5 Powyższe zdarzenia są odnotowane przez ABI – Załącznik C – „ Rejestr incydentów".

12 Kontrola systemu ochrony danych osobowych i przegląd zarządzania

12.1 Celem procedury jest uporządkowanie i przedstawienie czynności związanych z : kontrolą stanu bezpieczeństwa danych osobowych oraz okresowa oceną Systemu Ochrony Danych Osobowych

12.2 Procedura obejmuje wszystkie procesy organizacji , gdzie przestrzeganie zasad ochrony danych osobowych jest wymagane.

12.3 Do kontroli stanu ochrony danych osobowych w Starostwie Powiatowym w Kamieniu Pomorskim upoważnieni są:
1) Administrator Danych Osobowych (ADO)
2) Administrator Bezpieczeństwa Informacji (ABI)
3) Administrator Systemu Informatycznego (ASI)

12.4 Raz w roku kontroli (audyt) podlegają wszystkie systemy informatyczne przetwarzające dane osobowe oraz zabezpieczenia fizyczne i bezpieczeństwo osobowe.

12.5 Administrator Bezpieczeństwa Informacji (ABI) przygotowuje plan ochrony uwzględniając
zakres oraz potrzebne zasoby fizyczne, czasowe, i osobowe;
12.6 Kontroli podlega warstwa sprzętowa , systemy operacyjne , aplikacje, realizacja zabezpieczeń przez pracowników Starostwa Powiatowego w Kamieniu Pomorskim oraz przestrzeganie polityki bezpieczeństwa. Kontrola (audyt przeprowadzana jest z użyciem dokumentu Załącznik D- „ Zakres kontroli (audyt) ODO")
12.7 Po dokonanej kontroli Administrator Bezpieczeństwa Informacji (ABI) przygotowuje raport poaudytowy. Na jego podstawie informuje Administratora Danych Osobowych (ADO) o konieczności podjęcia właściwych działań korygujących i doskonalących.
12.8 Raz w roku po przeprowadzonej kontroli Administrator Bezpieczeństwa Informacji (ABI) przygotowuje ocenę roczną stanu funkcjonowania systemu ochrony danych osobowych i przedstawia go Administratorowi Danych Osobowych. Potwierdzeniem przeprowadzenia przeglądu ODO jest protokół – WZÓR- Załącznik E- „ Przegląd stanu bezpieczeństwa danych osobowych".

13 Postanowienia końcowe

13.1 „ Polityka Bezpieczeństwa" jest dokumentem wewnętrznym i nie może być udostępniana osobom postronnym w żadnej formie.
13.2 Każdy urzędnik Starostwa Powiatowego w Kamieniu Pomorskim zobowiązany jest zapoznać się z treścią polityki.
13.3 Użytkownik zobowiązany jest złożyć oświadczenie o tym , iż został zaznajomiony z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u Administratora Danych Osobowych,
a także o zobowiązaniu się do ich przestrzegania.
13.4 Oświadczenie potwierdzające zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami Obowiązującymi u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania, przechowywane jest w aktach osobowych pracownika.

1) Przypadki , nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także , gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
2) Kara dyscyplinarna, orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002r . Nr 101, poz. 926) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
3) Wszystkie regulacje dotyczące systemów informatycznych określone w polityce dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.

13.5 Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej polityce.

14 Załączniki:

Załącznik A – Wykaz zbiorów danych osobowych
Załącznik B - Opis struktury zbiorów danych osobowych
Załącznik Ba - Struktura baz danych osobowych w Starostwie Powiatowym w Kamieniu Pomorskim
Załącznik C – Rejestr Incydentów
Załącznik D – Zakres kontroli (audyt) ODO
Załącznik E – Wzór - Przegląd stanu bezpieczeństwa danych osobowych

Załącznik A
do Polityki Bezpieczeństwa DO

WYKAZ ZBIORÓW DANYCH OSOBOWYCH

Legenda:

1* - zwyczajowa lub własna , np.: dane kadrowe , dane płacowe
2* - (O) – Office , (SQL)- silnik bazy danych, (F) – Firebird, (MDB) – plik bazy danych, (P)- dokumenty papierowe
3* - (I) – Indywidualne hasło dostępu, (S) – szyfrowanie transmisji danych , (F) – wydzielona fizycznie sieć
4* - (K) – miejsce przechowywania kopii bezpieczeństwa , (U) – pomieszczenie osób przetwarzających dane,
(A) – pomieszczenie administratora baz danych
5* - (K) – kraty w oknach , (W) – wzmocnienie drzwi , (ZP) – zamki patentowe, (SM) – szafa metalowa

Lp	Nazwa zbioru danych 1*	Forma danych/ Baza danych 2*	Zabezpieczenie informatyczne 3*	Bazę Danych chroni UPS? (TAK/ NIE)	Program służący do przetwarzania baz danych	Czy dane osobowe są zewnętrzne? (TAK/ NIE)	Lokalizacja	Budynek nr pokoju	Funkcja lokalizacji 4*	Zabezpieczenie fizyczne 5*
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										
11										
12										
13										
14										

Załącznik B
do Polityki Bezpieczeństwa DO

OPIS STRUKTURY ZBIORU

Lp.	Nazwa zbioru	Opis struktury zbioru
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		
29		
30		
31		
32		
33		
34		
35		
36		

Załącznik Ba
do Polityki Bezpieczeństwa DO

STRUKTURA BAZ DANYCH OSOBOWYCH W STAROSTWIE POWIATOWYM W KAMIENIU POMORSKIM

Lp.	Nazwa Programu	Zakres przetwarzanych danych osobowych
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		

Załącznik C
do Polityki Bezpieczeństwa DO

REJESTR INCYDENTÓW

Lp.	Zadanie, problem, incydent	Źródło zgłoszenia	Data rozpoczęcia	Przewidywany termin zakończenia	Czy koniec?	Odpowiedzialny za realizacje	Przyczyna niezgodności	Działanie korygujące, zapobiegawcze	Ocena skuteczności

Załącznik D
do Polityki Bezpieczeństwa DO

Zakres kontroli (audyt) ODO

L. p.	Wymaganie	Propozycja pytania audytowego	Wskazówka	Czy spełniane są wymagania T/N?
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				

Załącznik E
do Polityki Bezpieczeństwa DO

PRZEGLĄD STANU BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Uczestnicy przeglądu : **1.** **2.** **3.**	**Termin wykonania przeglądu:**

Sprawy omawiane na przeglądzie	**Komentarze/ propozycje zmian**
Omówienie zaleceń z poprzedniego przeglądu	
Podsumowanie ogólnego stanu systemu ODO	
Omówienie przeprowadzonych kontroli z okresu od ostatniego przeglądu , ilości, najważniejszych niezgodności	
Omówienie najważniejszych działań korygujących i zapobiegawczych , ile przeprowadzono, ile jest jeszcze otwartych i propozycje dalszych działań z nimi	
Omówienie zarejestrowanych incydentów oraz ilości i powodów ich wystąpienia	
Omówienie procesu szkoleń i potrzeb szkoleniowych pracowników	

Podpisy uczestników przeglądu :

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