ZARZĄDZENIE NR 14/2008
Starosty Bielskiego
z dnia 17 kwietnia 2008 r.

w sprawie: **ustanowienia i wdrożenia Polityki Zarządzania Bezpieczeństwem Informacji Starostwa Powiatowego w Bielsku-Białej wynikającej z wdrażania Systemu Zarządzania Bezpieczeństwem Informacji zgodnego z wymaganiami normy PN ISO/IEC 27001:2007.**

Na podstawie art. 34 ust. 1 i art. 35 ust. 2 ustawy z dnia 5 czerwca 1998 roku o samorządzie powiatowym (tj. Dz. U. z 2001 r. Nr 142, poz. 1592 z późn. zm.)

zarządzam, co następuje:

§ 1

Ustanawiam i wdrażam Politykę Zarządzania Bezpieczeństwem Informacji Starostwa Powiatowego w Bielsku-Białej wynikającą z wdrażania Systemu Zarządzania Bezpieczeństwem Informacji zgodnego z wymaganiami normy PN ISO/IEC 27001:2007, której treść została określona w załączniku do niniejszego zarządzenia.

§ 2

Zobowiązuję Naczelników Wydziałów (jednostek równorzędnych) do zapoznania podległych im pracowników z Polityką Zarządzania Bezpieczeństwem Informacji Starostwa Powiatowego w Bielsku-Białej.

§ 3

Nadzór nad wykonaniem zarządzenia powierzam Pełnomocnikowi Zarządu ds. Systemu Zarządzania Bezpieczeństwem Informacji.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik do Zarządzenia nr 14/2008 Starosty Bielskiego z dnia 17 kwietnia 2008 r.

POLITYKA ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI STAROSTWA POWIATOWEGO W BIELSKU-BIAŁEJ

Spis treści – rozdziały:

ROZDZIAŁ I
DEKLARACJA O USTANOWIENIU POLITYKI ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI.

Misją Starostwa Powiatowego w Bielsku-Białej
jest profesjonalna i skuteczna realizacja prawnie przewidzianych i statutowo przypisanych mu zadań publicznych ukierunkowanych na promocję i rozwój społeczno-gospodarczy regionu oraz kompetentna, sprawa i uprzejma obsługa interesantów.

1. Istotnym elementem sprawnej realizacji *Misji* oraz *Strategii rozwoju powiatu* jest niezakłócone działanie systemów informacyjnych oraz właściwe zabezpieczenie przetwarzanych informacji przed istniejącymi zagrożeniami.
2. W związku z powyższym Zarząd Powiatu ustanawia Politykę Zarządzania Bezpieczeństwem Informacji oraz podejmuje wysiłki związane z wdrożeniem oraz doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji.
3. Zarząd Powiatu deklaruje zapewnienie optymalnych warunków i niezbędnych środków finansowych dla realizacji celów zawartych w Polityce Zarządzania Bezpieczeństwem Informacji oraz stałą współpracę z osobami i zespołem powołanymi w celu opracowania, wdrożenia i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji.
4. Właścicielem dokumentu Polityki Zarządzania Bezpieczeństwem Informacji jest Zarząd Powiatu.

ROZDZIAŁ II
CEL OPRACOWANIA I ZAWARTOŚĆ DOKUMENTU

1. Celem opracowania dokumentu Polityki Zarządzania Bezpieczeństwem Informacji jest zdefiniowanie ogólnych wymagań i zasad ochrony informacji, które będą fundamentem dla wszystkich dokumentów związanych z bezpieczeństwem informacji oraz dla tworzonego Systemu Zarządzania Bezpieczeństwem Informacji.
2. Polityka Zarządzania Bezpieczeństwem Informacji zawiera przede wszystkim deklaracje Zarządu, definicje i cele bezpieczeństwa informacji, zakres obowiązywania oraz odnośniki do innych dokumentów opracowywanych w ramach Systemu Zarządzania Bezpieczeństwem Informacji.
3. Polityka niniejsza została opracowana dla:
   - 3.1 Zapewnienia ochrony informacji przed nieupoważnionym dostępem;
   - 3.2 Zapewnienia poufności, dostępności i integralności informacji przetwarzanych w Starostwie zgodnie z określonymi wymaganiami;
   - 3.3 Zapewnienia, że eksploatowane przez Starostwo Powiatowe systemy gwarantują niezaprzeczalność odbioru, niezaprzeczalność nadania oraz rozliczalność zadań;
   - 3.4 Zapewnienia, że szkolenia z zakresu bezpieczeństwa informacji są zagwarantowane pracownikom;
   - 3.5 Zapewnienia możliwości rejestracji wszelkiego rodzaju naruszeń bezpieczeństwa informacji;
   - 3.6 Zapewnienia, że wszelkie naruszenia bezpieczeństwa informacji oraz jego słabe punkty są raportowane i badane;
   - 3.7 Zapewnienia, że plany zarządzania ciągłością działania są tworzone, utrzymywane i testowane w stopniu umożliwiającym nieprzerwaną realizację zadań publicznych.

4. Wdrożenie niniejszej Polityki Zarządzania Bezpieczeństwem Informacji jest ważne dla wykazania należytej dbałości o poufność, integralność i dostępność informacji podczas kontaktów z klientami oraz instytucjami współpracującymi.

ROZDZIAŁ III
PODSTAWY NORMATYWNE I TERMINOLOGIA

1. Do tworzenia i rozwijania Systemu Zarządzania Bezpieczeństwem Informacji stosowane będą wymagania:
   1.1 *Polskiej Normy ISO/IEC 27001 Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji – Wymagania;*
   1.2 *Polskiej Normy ISO/IEC 17799 Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji;*
   1.3 *Raportu Technicznego ISO/IEC TR 18044:2004 Information technology – Security techniques – Information security incident management.*
2. Podstawą budowy Systemu Zarządzania Bezpieczeństwem Informacji jest jego integracja z funkcjonującym w Starostwie Systemem Zarządzania Jakością zgodnym z normą ISO 9001.
3. Terminologia:
   3.1 System Zarządzania Bezpieczeństwem Informacji (SZBI) – część zintegrowanego systemu zarządzania odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji.
   3.2 Poufność informacji - zapewnienie, że informacja nie jest udostępniana lub wyjawiana osobom nieupoważnionym oraz że osoby nieuprawnione nie mają dostępu do informacji.
   3.3 Integralność informacji – zapewnienie, że informacja jest kompletna i nie została zmieniona w sposób nieuprawniony.
   3.4 Dostępność informacji – zapewnienie, że osoby upoważnione mają łatwy dostęp do informacji, które są im potrzebne, wtedy gdy tych informacji potrzebują.
   3.5 Autentyczność informacji – zapewnienie, że informacja jest zgodna z prawdą, oryginalna.
   3.6 Rozliczalność działań – zapewnienie, że wszystkie istotne czynności wykonane przy przetwarzaniu informacji zostały zarejestrowane i jest możliwe zidentyfikowanie osoby, która daną czynność wykonała.
   3.7 Niezawodność działań - zapewnienie, że wykonywane czynności prowadzą do zamierzonych skutków.
   3.8 Zarządzanie ryzykiem – skoordynowane postępowanie, którego celem jest identyfikacja, kontrolowanie i minimalizowanie ryzyka związanego z bezpieczeństwem informacji.
   3.9 Niezaprzeczalność odbioru – zdolność systemu do udowodnienia, że adresat informacji otrzymał ją w określonym czasie i miejscu.
   3.10 Niezaprzeczalność nadania – zdolność systemu do udowodnienia, że nadawca informacji faktycznie ją nadał lub wprowadził do systemu w określonym czasie i miejscu .

ROZDZIAŁ IV
PODSTAWY PRAWNE

Polityka Zarządzania Bezpieczeństwem Informacji oraz inne dokumenty szczegółowe związane z bezpieczeństwem informacji powinny być zgodne z obowiązującymi w tym zakresie przepisami prawnymi wymienionymi w załącznikach oraz innymi wymaganiami obowiązującymi Starostwo.

ROZDZIAŁ V
ZAKRES ODDZIAŁYWANIA

1. Zasady określone przez dokumenty Polityki Zarządzania Bezpieczeństwem Informacji obejmują swym zakresem wszystkie zasoby informacyjne Starostwa Powiatowego w Bielsku-Białej zaangażowane w realizację *Misji* oraz *Strategii rozwoju powiatu,* a w szczególności:
   1.1 wszystkich pracowników Starostwa w rozumieniu przepisów Kodeksu Pracy, konsultantów, stażystów oraz inne osoby i instytucje mające dostęp do informacji podlegających ochronie,
   1.2 wszystkie lokalizacje – budynki i pomieszczenia, w których są lub będą przetwarzane informacje podlegające ochronie,
   1.3 wszystkie nośniki danych, w tym papierowe, magnetyczne (np. dyskietka) lub optyczne (np. CD-R, DVD-R), na których są lub będą znajdować się informacje podlegające ochronie,
   1.4 informacje będące własnością Starostwa lub klienta Starostwa, o ile zostały przekazane na podstawie przepisów prawnych lub umów,
   1.5 wszystkie istniejące, wdrażane obecnie lub w przyszłości systemy informatyczne oraz papierowe, w których przetwarzane są lub będą informacje podlegające ochronie.
2. Do stosowania zasad określonych przez dokumenty Polityki Zarządzania Bezpieczeństwem Informacji zobowiązani są wszyscy pracownicy Starostwa w rozumieniu przepisów Kodeksu Pracy, oraz inne osoby i instytucje mające dostęp do informacji podlegającej ochronie na podstawie przyjętego na siebie zobowiązania dotyczącego przestrzegania jej zasad.

ROZDZIAŁ VI
BEZPIECZEŃSTWO W STAROSTWIE

1. Mając na uwadze fakt, że sprawna realizacja *Misji* oraz *Strategii rozwoju powiatu* zależy od niezakłóconego działania systemów informacyjnych oraz właściwego zabezpieczenia przetwarzanych informacji przed istniejącymi zagrożeniami Zarząd Powiatu stawia przez Systemem Zarządzania Bezpieczeństwem Informacji następujące cele:
   1.1 Zapewnienie zgodności prowadzonych działań z przepisami prawnymi i innymi wymaganiami obowiązującymi Starostwo;
   1.2 Zapewnienie ciągłości realizacji Misji Starostwa Powiatowego w Bielsku-Białej poprzez tworzenie, utrzymywanie i testowanie planów zarządzania ciągłością działania;
   1.3 Zapewnienie poufności, dostępności i integralności informacji przetwarzanych w Starostwie zgodnie z procedurami oraz odpowiednimi przepisami prawa;
   1.4 Zapewnienie zgodności w wymaganiami kontraktowymi odnoszącymi się do bezpieczeństwa informacji;

1.5 Zidentyfikowanie wszelkich aktywów w rozumieniu systemu zarządzania bezpieczeństwem informacji oraz określenie ich wartości i znaczenia dla Starostwa poprzez przeprowadzenie oceny ryzyka, zrozumienie ich podatności oraz zagrożeń, które mogą narazić je na ryzyko;

1.6 Zarządzanie ryzykiem na akceptowalnym poziomie poprzez zaprojektowanie, wdrożenie i utrzymanie formalnego systemu zarządzania;

1.7 Wprowadzenie mechanizmów gwarantujących ochronę zasobów informacyjnych Starostwa Powiatowego;

1.8 Wdrożenie systemu zarządzania incydentami naruszającymi bezpieczeństwo informacji oraz słabościami systemu;

1.9 Zapewnienie ochrony wizerunku i reputacji Starostwa poprzez ograniczenie wpływu zagrożeń dla realizacji zobowiązań zewnętrznych, wynikających z zawartych umów oraz zasad dobrego obyczaju;

1.10 Prowadzenie stałych działań zmierzających do poprawy poziomu bezpieczeństwa informacji przetwarzanych w Starostwie oraz doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji.

2. Zarząd Powiatu jednocześnie deklaruje chęć dołożenia wszelkich starań w celu:

2.1 Wdrożenia systemu zarządzania bezpieczeństwem informacji zgodnego z normą PN ISO/IEC 27001:2007, jego utrzymania, eksploatacji i doskonalenia;

2.2 Przestrzegania zgodności systemu zarządzania z normą PN ISO/IEC 27001:2007;

2.3 Uzyskania i utrzymania certyfikacji na zgodność systemu zarządzania z normą PN ISO/IEC 27001:2007.

ROZDZIAŁ VII
ROLE I ODPOWIEDZIALNOŚCI ZWIĄZANE Z BEZPIECZEŃSTWEM INFORMACJI

1. W celu opracowania, wdrożenia i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji zgodnego z normą PN-ISO/IEC 27001:2007 została powołana następująca struktura organizacyjna bezpieczeństwa informacji:

1.1 **Pełnomocnik Zarządu ds. SZBI** jest odpowiedzialny za prowadzenie całokształtu spraw związanych z opracowaniem, wdrożeniem i doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji.

1.2 **Administrator Bezpieczeństwa Systemów Teleinformatycznych** jest odpowiedzialny za nadzorowanie bezpiecznej eksploatacji systemów informatycznych i wspomaganie Pełnomocnika Zarządu ds. SZBI w zakresie ochrony systemowych zasobów informacyjnych.

1.3 **Zespół ds. Bezpieczeństwa Informacji** jest odpowiedzialny za inicjowanie i wspieranie wszelkich działań związanych z bezpieczeństwem informacji.

2. Załącznik nr 1 zawiera „Szczegółowe role i odpowiedzialności związane z bezpieczeństwem informacji".

3. Wszyscy pracownicy i dostawcy (wykonawcy) powiązani umowami postępują zgodnie z zasadami niniejszej Polityki Zarządzania Bezpieczeństwem Informacji oraz uzupełniającymi ją innymi dokumentami, jeśli takowe mają zastosowanie.

4. Wszyscy pracownicy oraz dostawcy (wykonawcy) powiązani umowami są odpowiedzialni za raportowanie incydentów związanych z bezpieczeństwem oraz wszelkich zidentyfikowanych słabych punktów.

5. Wszelkie celowe działania zagrażające bezpieczeństwu informacji, która jest własnością Starostwa Powiatowego w Bielsku-Białej lub instytucji z nim współpracujących podlegają stosownym konsekwencjom dyscyplinarnym i/lub prawnym.

ROZDZIAŁ VIII
ROZPOWSZECHNIENIE I ZARZĄDZANIE DOKUMENTEM POLITYKI

1. Prawo dostępu do dokumentu Polityki Zarządzania Bezpieczeństwem Informacji posiadają przede wszystkim pracownicy Starostwa oraz osoby i instytucje mające dostęp do informacji podlegającej ochronie a także interesanci, strony umów i porozumień.
2. Sposób aktualizacji i rozpowszechniania Polityki Zarządzania Bezpieczeństwem Informacji reguluje procedura *P-PP1.1/PZ Nadzorowanie dokumentacji*.
3. Niniejsza polityka podlega regularnym przeglądom przez Zarząd Powiatu podczas okresowych przeglądów Systemu. W zależności od potrzeb mogą zostać przeprowadzone dodatkowe przeglądy po stwierdzeniu istotnego naruszenia bezpieczeństwa, pojawieniu się zasadniczych zmian w Starostwie, jego strukturze lub jego otoczeniu (nowe zagrożenia, technologie). Celem przeglądów polityki jest zapewnienie jej stosowalności w stosunku do realizowanych zadań publicznych oraz możliwości obsługi interesantów w każdych warunkach niezależnie od okoliczności i zmian w Starostwie.

ROZDZIAŁ IX
ZAŁĄCZNIKI

1. Załącznik nr 1 - Szczegółowe role i odpowiedzialności związane z bezpieczeństwem informacji.
2. Załącznik nr 2 - Wykaz obowiązujących Starostwo głównych aktów prawnych związanych z bezpieczeństwem informacji.

ROZDZIAŁ X
ODWOŁANIE DO DOKUMENTÓW SYSTEMOWYCH

1. Polityka Zarządzania Bezpieczeństwem Informacji jest dokumentem nadrzędnym nad wszystkimi dokumentami dotyczącymi bezpieczeństwa informacji i stanowi dokument poziomu pierwszego.
2. Poziom drugi stanowi przede wszystkim Polityka Bezpieczeństwa danych osobowych i Polityka Bezpieczeństwa Systemów Teleinformatycznych, opracowywane zgodnie z ogólnymi wymaganiami i zasadami ochrony informacji określonymi w niniejszej Polityce Zarządzania Bezpieczeństwem Informacji.
3. Poziom trzeci stanowią bardziej szczegółowe uregulowania, które przenoszą wymagania i zasady ochrony informacji określone w niniejszej Polityce Zarządzania Bezpieczeństwem Informacji na środowisko zasobów informacyjnych Starostwa Powiatowego w Bielsku-Białej.
4. Wszystkie dokumenty związane z bezpieczeństwem informacji są podporządkowane niniejszej Polityce i stanowią jej integralną część.
5. Specyfikacja wszystkich dokumentów tworzących ramy systemu zarządzania bezpieczeństwem informacji funkcjonującego zgodnie z normą PN ISO/IEC 27001:2007 znajduje się w przewodniku Polityki Zarządzania Bezpieczeństwem Informacji Starostwa Powiatowego w Bielsku-Białej.

1. **Pełnomocnik Zarządu ds. SZBI (PZ-SZBI)** jest odpowiedzialny za prowadzenie całokształtu spraw związanych z opracowaniem, wdrożeniem i doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), a w szczególności za:
   a. współpracę z Naczelnikami Wydziałów / stanowiskami równorzędnymi na wszystkich etapach opracowania, wdrożenia i doskonalenia SZBI,
   b. współpracę z konsultantami i ekspertami zewnętrznymi, Zespołem ds. Bezpieczeństwa Informacji oraz pracownikami innych wydziałów kompetentnymi w zagadnieniach bezpieczeństwa,
   c. czuwanie nad przestrzeganiem postanowień Polityki Zarządzania Bezpieczeństwem Informacji oraz dokumentów powiązanych,
   d. nadzorowanie prawidłowości prowadzonej w ramach systemu SZBI inwentaryzacji i wyceny zasobów oraz inicjowanie i nadzorowanie wykonania analizy ryzyka przez poszczególne wydziały,
   e. weryfikację opracowywanej dokumentacji SZBI,
   f. udział w pracach Zespołu ds. Bezpieczeństwa Informacji, w tym przedstawianie opracowanych dokumentów do zaopiniowania,
   g. nadzorowanie wdrażania zabezpieczeń,
   h. nadzór nad prawidłowością funkcjonowania i doskonalenia SZBI, w tym nadzór nad przestrzeganiem wymagań procedur, weryfikowanie wdrożonych rozwiązań i zabezpieczeń, inicjowanie i koordynowanie działań zmierzających do usunięcia niezgodności SZBI z wymaganiami normy PN ISO/IEC 27001:2007,
   i. przedstawianie Zarządowi Powiatu oraz Zespołowi ds. Bezpieczeństwa Informacji sprawozdań dotyczących przebiegu prac oraz funkcjonowania SZBI i wszelkich potrzeb związanych z jego doskonaleniem (zasoby ludzkie, finansowe, wiedzy i inne konieczne do wdrożenia i zachowania zaplanowanego poziomu bezpieczeństwa),
   j. organizację i prowadzenie szkoleń personelu w ramach Systemu Zarządzania Bezpieczeństwem Informacji, w tym na temat zasad postępowania zgodnych z założeniami Polityki Zarządzania Bezpieczeństwem Informacji,
   k. współpracę z jednostkami certyfikującymi w zakresie Systemu Zarządzania Bezpieczeństwem Informacji,
   l. współdziałanie z Administratorem Bezpieczeństwa Systemów Teleinformatycznych w zakresie opracowywania / modyfikacji dokumentów polityk bezpieczeństwa systemów przetwarzania informacji, procedur bezpieczeństwa i standardów zabezpieczeń, projektów rozwoju systemów teleinformatycznych,
   m. okresową kontrolę polityk i procedur,
   n. weryfikację dopuszczenia użytkowników do przetwarzania informacji.

2. **Administrator Bezpieczeństwa Systemów Teleinformatycznych (ABST)** jest odpowiedzialny za nadzorowanie bezpiecznej eksploatacji systemów informatycznych i wspomaganie Pełnomocnika Zarządu ds. SZBI w zakresie ochrony systemowych zasobów informacyjnych, a w szczególności za:
   a. działanie zgodne z obowiązującą Polityką Zarządzania Bezpieczeństwem Informacji,
   b. analizowanie tendencji rozwojowych technologii informatycznych i technik bezpieczeństwa, pod kątem podatności, zagrożeń i zabezpieczeń,
   c. przygotowywanie danych analitycznych opisujących działanie systemów teleinformatycznych w kontekście zarządzania bezpieczeństwem informacji,
   d. okresowe raportowanie o stanie bezpieczeństwa systemów teleinformatycznych, odnotowanych incydentach bezpieczeństwa oraz statusie podejmowanych działań w odpowiedzi na incydenty,
   e. współdziałanie z Pełnomocnikiem Zarządu ds. SZBI w zakresie opracowywania i wdrażania polityk, procedur i instrukcji,
   f. przygotowanie procedur określających zasady zarządzania systemami lokalnymi,
   g. przygotowanie procedur bezpieczeństwa danego systemu przetwarzania informacji chronionych,
   h. przygotowanie dokumentów procedur zarządzania kontami użytkowników,
   i. przygotowanie dokumentów procedur kryzysowych związanych z incydentami w systemach przetwarzania informacji,
   j. udział w pracach Zespołu ds. Bezpieczeństwa Informacji,
   k. koordynację działań zapewniających sprawne funkcjonowanie i zabezpieczenie systemów teleinformatycznych Starostwa przed niepowołanym dostępem,
   l. nadzorowanie zgłaszanych incydentów i zdarzeń bezpieczeństwa dotyczących systemów teleinformatycznych,
   m. dopuszczanie systemów przetwarzania informacji do eksploatacji,
   n. nadzór nad wdrożeniem nowych aplikacji,
   o. umożliwienie przeprowadzenia kontroli systemów teleinformatycznych Starostwa przez służby Biura Generalnego Inspektora Danych Osobowych,
   p. zapewnienie, że do informacji chronionych mają dostęp wyłącznie osoby upoważnione i że mogą one wykonywać wyłącznie uprawnione operacje,
   q. kontrolę procesu przyznawania praw dostępu,
   r. przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
   s. nadzorowanie pracy Zespołu ds. Informatyki w zakresie zapewnienia bezpieczeństwa informacji.

3. **Zespół ds. Bezpieczeństwa Informacji** jest odpowiedzialny za inicjowanie i wspieranie wszelkich działań związanych z bezpieczeństwem informacji, a w szczególności za:
   a. opiniowanie dokumentów SZBI, w tym Polityki Zarządzania Bezpieczeństwem Informacji, polityk niższego rzędu, metodyk, procedur, instrukcji,
   b. uzgadnianie podziału odpowiedzialności w zakresie bezpieczeństwa informacji,
   c. wspieranie procesów zarządzania ryzykiem, w tym analizy ryzyka, monitorowania zmian stopnia narażenia zasobów na podstawowe zagrożenia,
   d. okresową analizę danych na temat naruszeń bezpieczeństwa informacji oraz monitorowanie naruszeń bezpieczeństwa informacji,
   e. analizę, ocenę i opiniowanie projektów zmierzających do podniesienia poziomu bezpieczeństwa informacji (działań korygujących i zapobiegawczych)
   f. dobór zabezpieczeń,
   g. koordynację procesów doskonalenia SZBI, w tym wdrażania określonych zabezpieczeń w systemach lub usługach,
   h. zabezpieczanie realizacji jednolitej Polityki Zarządzania Bezpieczeństwem Informacji w całym Starostwie,
   i. zgłaszanie do Pełnomocnika Zarządu ds. SZBI poprawek i aktualizacji do opracowanych dokumentów SZBI, w tym do Polityki Zarządzania Bezpieczeństwem Informacji,
   j. wspieranie inicjatyw dotyczących propagowania tematyki bezpieczeństwa informacji w całym Starostwie,
   k. wspieranie Zarządu Powiatu w planowaniu budżetu zapewniającego prawidłowe funkcjonowanie SZBI w Starostwie,
   l. przeciwdziałanie próbom naruszenia bezpieczeństwa informacji.
4. **Właściciele zasobów** (Naczelnicy / równorzędne stanowiska) są odpowiedzialni za wdrożenie, utrzymanie i doskonalenie systemu zarządzania bezpieczeństwem informacji w wydziale, a w szczególności za:
   a. wyznaczenie pracowników merytorycznych, którzy będą przy ich udziale wykonywać czynności określone im w zakresie czynności, a związane z wdrożeniem, zarządzaniem i doskonaleniem SZBI w wydziale,
   b. udostępnienie PZ ds. SZBI, ABST oraz Zespołowi ds. Bezpieczeństwa Informacji wszelkich danych i informacji niezbędnych do opracowania, wdrożenia i doskonalenia SZBI,
   c. okresowe raportowanie o poziomie bezpieczeństwa informacji w Wydziale,
   d. określanie, które osoby i na jakich prawach mają mieć dostęp do danych informacji,
   e. tworzenie i aktualizację procedur postępowania z udziałem wykonawców zadań,
   f. nadzór nad przestrzeganiem obowiązujących procedur,

g. podejmowanie decyzji w sprawie sposobu realizacji zadań w przypadku wystąpienia sytuacji nietypowej, nie opisanej w procesie, procedurze, itp. i zgłaszanie tych sytuacji PZ-SZBI,

h. powiadomienia PZ-SZBI i ABST o zakładaniu zbiorów danych na lokalnych urządzeniach komputerowych oraz w formie manualnej (dotyczy również zbiorów istniejących w momencie wprowadzenia niniejszej polityki),

i. przeciwdziałanie próbom naruszenia bezpieczeństwa informacji.

5. **Administrator aplikacji** jako osoba administrująca aplikacjami wydziałowymi niezależnie od obowiązków obowiązujących Pracownika jest odpowiedzialny za:

a. konfigurację i administrację oprogramowaniem bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem,

b. prowadzenie rejestru osób dopuszczonych do systemu baz danych (rejestr powinien zawierać: imię i nazwisko osoby, pełnioną rolę, grupę informacji, czas trwania dostępu),

c. przyznawanie na wniosek Właściciela zasobów, za zgodą Administratora Bezpieczeństwa Informacji ściśle określonych praw dostępu do informacji w danym systemie bazodanowym,

d. współpracę z dostawcami Aplikacji,

e. zarządzanie kopiami awaryjnymi danych w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie,

f. opracowanie procedur określających zarządzanie systemem bazodanowym,

g. świadczeniu pomocy technicznej w ramach aplikacji bazodanowych dla użytkowników,

h. przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,

i. wnioskowanie do ABST w sprawie procedur bezpieczeństwa i standardów zabezpieczeń.

6. **Pracownicy** są odpowiedzialni za realizację zadań służbowych w zgodzie z wymaganiami stawianymi przez system SZBI, a w szczególności za:

a. przestrzeganie tajemnicy państwowej i służbowej w zakresie przez prawo przewidzianym - pracownicy nowoprzyjęci z chwilą przyjęcia do pracy natomiast pracownicy już zatrudnieni, poprzez podpisanie stosownych oświadczeń,

b. stosowanie się do obowiązującej Polityki Zarządzania Bezpieczeństwem Informacji, obowiązujących procedur oraz instrukcji,

c. zgłaszanie wszelkich przypadków działań niezgodnych z politykami i regulaminami, mogących być zdarzeniami lub incydentami bezpieczeństwa,

d. zgłaszanie przełożonemu konieczności / propozycji zmian w dokumencie (procesie, procedurze, zarządzeniu, itp.) lub uwag do opracowywanego dokumentu,

e. ochronę identyfikatorów osobistych (loginów do systemów/aplikacji) oraz haseł przed ujawnieniem,

f. uczestnictwo w organizowanych przez Starostwo szkoleniach z zakresu bezpieczeństwa informacji,

g. przeciwdziałanie próbom naruszenia bezpieczeństwa informacji.

7. **Osoby trzecie**, przed uzyskaniem dostępu do informacji, muszą podpisać zobowiązanie do ochrony informacji w trybie art. 266 § KK; 267 § KK; 268 § KK, 269 § KK i zapisów Ustawy o zwalczaniu nieuczciwej konkurencji z dnia 16 kwietnia 1993 r. (Dz. U. Nr 47, poz. 211 wraz z późn. zm.). Jednocześnie osoby takie musza zapoznać się z Polityką Zarządzania Bezpieczeństwem Informacji Starostwa oraz podpisać zobowiązanie o jej przestrzeganiu. Do obowiązków osób trzecich należy:

   a. przestrzeganie tajemnicy państwowej i służbowej w zakresie przez prawo przewidzianym,

   b. stosowanie się do obowiązującej Polityki Bezpieczeństwa Informacji, obowiązujących procedur oraz instrukcji,

   c. zgłaszanie wszelkich przypadków działań niezgodnych z politykami i regulaminami, mogących być zdarzeniami lub incydentami bezpieczeństwa,

   d. przeciwdziałanie próbom naruszenia bezpieczeństwa informacji.

8. **Audytorzy Wewnętrzni SZBI** (AW-SZBI) są odpowiedzialni za planowanie, realizowanie i dokumentowanie audytów wewnętrznych zlecanych przez Pełnomocnika Zarządu ds. SZBI, zgodnie z wymaganiami procedury *P-PP1.1/PZ Audity Wewnętrzne.* Zespół audytorów wewnętrznych zostaje powołany osobnym zarządzeniem. W szczególności do obowiązków Audytora Wewnętrznego SZBI należy:

   a. okresowe przeprowadzanie audytów wewnętrznych działania systemu zarządzania bezpieczeństwem,

   b. określanie słabości systemu, niezgodności systemu z normą PN ISO/IEC 27001:2007 oraz miejsc wymagających wprowadzenia poprawek,

   c. wspomaganie Zespołu ds. Bezpieczeństwa Informacji wiedzą i doświadczeniem w zakresie formalnych wymagań w stosunku do systemu stawianych przez unormowania, na których bazuje system,

   d. zgodnie z potrzebami organizacji prowadzenie działań kontrolnych przewidzianych w procedurach opisujących system,

   e. w razie prowadzenia w Starostwie audytu zewnętrznego AW-SZBI jest odpowiedzialny za wspomaganie PZ-SZBI w dostarczaniu niezbędnych informacji audytorom zewnętrznym.

1. Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631 z późn. zm.) wraz z mającymi zastosowanie aktami wykonawczymi.

2. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.).
3. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. z 2004 r. Nr 100, poz. 1025).
4. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).

5. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2001 r. Nr 112, poz. 1198 z późn. zm.).
6. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu informacji publicznej (Dz. U. z 2007 r. Nr 10, poz. 68).

7. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2005 r. Nr 64, poz. 565 z późn. zm.) wraz z mającymi zastosowanie aktami wykonawczymi.

8. Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2006 r. Nr 90, poz. 631 z późn. zm.).

9. Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 1997 r. Nr 88, poz. 553 z późn. zm.).

10. Ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz. U. z 1998 r. Nr 21, poz. 94, z późn. zm.).