

Tekst jednolity opracowany na podstawie:

- Zarządzenia Nr 58/2014 Starosty Bielskiego z dnia 23 grudnia 2014 roku;
 - Zarządzenia Nr 27/2016 Starosty Bielskiego z dnia 19 maja 2016 roku;
 - Zarządzenia Nr 35/2017 Starosty Bielskiego z dnia 3 lipca 2017 roku.
-

ZARZĄDZENIE Starosty Bielskiego

w sprawie: **ustanowienia i wdrożenia Polityki Zarządzania Bezpieczeństwem Informacji Starostwa Powiatowego w Bielsku-Białej.**

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 2016 r. poz. 814 z późn. zm.)

zarządzam, co następuje:

§ 1

Ustanawiam i wdrażam Politykę Zarządzania Bezpieczeństwem Informacji Starostwa Powiatowego w Bielsku-Białej zgodnie z normą ISO/IEC 27001:2013, 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.

§ 3

Nadzór nad wykonaniem Zarządzenia powierzam Pełnomocnikowi Zarządu ds. Systemu Zarządzania Jakością i Bezpieczeństwem Informacji.

§ 4

Traci moc Zarządzenie Nr **4/2009** Starosty Bielskiego z dnia **14 stycznia 2009** r. w sprawie ustanowienia i wdrożenia Polityki Zarządzania Bezpieczeństwem Informacji Starostwa Powiatowego w Bielsku-Białej wynikającej z wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji zgodnego z wymaganiami normy PN ISO/IEC 27001:2007 zmienione Zarządzeniem Nr **12/2010** Starosty Bielskiego z dnia **24 marca 2010** r., Zarządzeniem Nr **18/2011** Starosty Bielskiego z dnia **21 marca 2011** r., Zarządzeniem **13/2012** Starosty Bielskiego z dnia **17 lutego 2012** r. oraz Zarządzeniem Nr **39/2013** Starosty Bielskiego z dnia **30 sierpnia 2013** r.

§ 5


Zarządzenie wchodzi w życie z dniem podpisania.

*Starosta Bielski
Andrzej Płonka*

POLITYKA ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI STAROSTWA POWIATOWEGO W BIELSKU-BIAŁEJ

Spis treści – rozdziały:

I.	Deklaracja o ustanowieniu Polityki Zarządzania Bezpieczeństwem Informacji
II.	Cel opracowania i zawartość dokumentu
III.	Podstawy normatywne i terminologia
IV.	Podstawy prawne
V.	Zakres Systemu Zarządzania Bezpieczeństwem Informacji
VI.	Bezpieczeństwo w Starostwie.....
VII.	Role i odpowiedzialności związane z bezpieczeństwem informacji
VIII.	Rozpowszechnienie i zarządzanie dokumentem Polityki
IX.	Załączniki.....
X.	Odwołanie do dokumentów systemowych

System Zarządzania Bezpieczeństwem Informacji – ISO 27001		
 POWIAT BIELSKI	POLITYKA ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI	STR. 2/7
	STAROSTWA POWIATOWEGO W BIELSKU-BIAŁEJ	Nr wydania: 3.2

ROZDZIAŁ I **DEKLARACJA O USTANOWIENIU POLITYKI ZARZĄDZANIA BEZPIECZEŃSTWEM** **INFORMACJI.**


Misją Starostwa Powiatowego w Bielsku – Białej

jest profesjonalna, skuteczna i efektywna realizacja prawnie przewidzianych i statutowo przypisanych mu zadań publicznych w sposób zgodny z prawem, oszczędny i terminowy, ukierunkowanych na promocję i rozwój społeczno-gospodarczy regionu oraz kompetentna, sprawna i uprzejma obsługa interesantów według zasad określonych w Kodeksie Etyki.

1. Istotnym elementem sprawnej realizacji *Misji* oraz *Strategii Rozwoju Powiatu Bielskiego* 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 deklarację Zarządu, definicje i cele bezpieczeństwa informacji, zakres systemu 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 zachowania ciągłości działania są tworzone, utrzymywane i testowane w stopniu umożliwiającym nieprzerwaną realizację zadań publicznych.


System Zarządzania Bezpieczeństwem Informacji – ISO 27001		
 <small>POWIAT BIELSKI</small>	POLITYKA ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI	STR. 3/7
	STAROSTWA POWIATOWEGO W BIELSKU-BIAŁEJ	Nr wydania: 3.2

4. Wdrożenie niniejszej Polityki Zarządzania Bezpieczeństwem Informacji jest ważne dla wykazania należytej dbałości o poufność, integralność i dostępność informacji podczas kontaktów ze stronami zainteresowanymi.

ROZDZIAŁ III

PODSTAWY NORMATYWNE I TERMINOLOGIA

1. Do tworzenia i rozwijania Systemu Zarządzania Bezpieczeństwem Informacji stosowane będą wymagania:
 - 1.1 *Normy ISO / IEC 27001 : 2013 Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji – Wymagania;*
 - 1.2 *Normy ISO / IEC 27002 : 2013 Technika informatyczna – Techniki bezpieczeństwa – Zasady zabezpieczenia informacji.*
2. Podstawą budowy Systemu Zarządzania Bezpieczeństwem Informacji jest jego integracja z Systemem Zarządzania Jakością zgodnym z normą ISO 9001 oraz wspieranie rozwiązaniami Systemu kontroli zarządczej funkcjonującego w Starostwie.
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 Strony zainteresowane (interesariusze) – osoby, grupy osób lub organizacje, które wnoszą do organizacji swój wkład, stawiają wymagania i oczekują spełnienia tych wymagań (np. klienci zewnątrzni i wewnątrzni, lokalne społeczności, urzędy, pracownicy, służby państwowe, dostawcy, media, organy regulacyjne).
 - 3.3 Poufność informacji - zapewnienie, że informacja nie jest udostępniana lub wyjawiana osobom nieupoważnionym oraz że osoby nieuprawnione nie mają dostępu do informacji.
 - 3.4 Integralność informacji – zapewnienie, że informacja jest kompletna i nie została zmieniona w sposób nieuprawniony.
 - 3.5 Dostępność informacji – zapewnienie, że osoby upoważnione mają łatwy dostęp do informacji, które są im potrzebne, wtedy gdy tych informacji potrzebują.
 - 3.6 Autentyczność informacji – zapewnienie, że informacja jest zgodna z prawdą, oryginalna.
 - 3.7 Rozliczalność działań – zapewnienie, że wszystkie istotne czynności wykonane przy przetwarzaniu informacji zostały zarejestrowane i jest możliwe zidentyfikowanie osoby, która daną czynność wykonała.
 - 3.8 Niezawodność działań - zapewnienie, że wykonywane czynności prowadzą do zamierzonych skutków.
 - 3.9 Zarządzanie ryzykiem – skoordynowane postępowanie, którego celem jest identyfikacja, kontrolowanie i minimalizowanie ryzyka związanego z bezpieczeństwem informacji i ciągłością działania.
 - 3.10 Niezaprzeczalność odbioru – zdolność systemu do udowodnienia, że adresat informacji otrzymał ją w określonym czasie i miejscu.
 - 3.11 Niezaprzeczalność nadania – zdolność systemu do udowodnienia, że nadawca informacji faktycznie ją nadał lub wprowadził do systemu w określonym czasie i miejscu.


System Zarządzania Bezpieczeństwem Informacji – ISO 27001		
 POWIAT BIELSKI	POLITYKA ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI	STR. 4/7
	STAROSTWA POWIATOWEGO W BIELSKU-BIAŁEJ	Nr wydania: 3.2

ROZDZIAŁ IV PODSTAWY PRAWNE

Polityka Zarządzania Bezpieczeństwem Informacji oraz inne udokumentowane informacje szczegółowe związane z bezpieczeństwem informacji powinny być zgodne z obowiązującymi w tym zakresie przepisami prawnymi wymienionymi w załączniku nr 2 oraz innymi wymaganiami obowiązującymi Starostwo.

ROZDZIAŁ V ZAKRES SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI


1. W ramach prowadzonej działalności Starostwo Powiatowe w Bielsku-Białej jako jednostka budżetowa powiatu bielskiego zapewnia organom powiatu pomoc w realizacji zadań i kompetencji w zakresie przewidzianym przez prawo, do których należy w szczególności wykonywanie:
 - 1.1 zadań własnych powiatu,
 - 1.2 zadań administracji rządowej w granicach upoważnień ustawowych,
 - 1.3 zadań powierzonych na podstawie porozumień zawartych przez powiat,
 - 1.4 innych zadań, określonych uchwałami Rady, Zarządu oraz przepisami prawa.
2. Zakres Systemu Zarządzania Bezpieczeństwem Informacji Starostwa Powiatowego w Bielsku-Białej obejmuje realizację zadań publicznych określonych przepisami prawa, w tym aktów prawnych związanych z bezpieczeństwem informacji wymienionych w załączniku nr 2, zgodnie z obowiązującą Deklaracją stosowania.
3. Zakres Systemu Zarządzania Bezpieczeństwem Informacji odnosi się do:
 - 3.1 Komórek organizacyjnych znajdujących się w strukturze organizacyjnej, która zamieszczona jest w Regulaminie Organizacyjnym Starostwa Powiatowego w Bielsku-Białej.
 - 3.2 Pomieszczeń, w których przetwarzane są informacje podlegające ochronie, zlokalizowanych w Bielsku-Białej, przy ulicy Piastowskiej 40 a także Oddziału Zamiejscowego Wydziału Komunikacji i Transportu (Czechowice-Dziedzice, Plac Jana Pawła II 4/5) oraz Stanowisko Zamiejscowe ds. Budownictwa (Czechowice-Dziedzice, ul. Ks. Barabasa 1).
 - 3.3 Zasobów informacyjnych (aktywów) zaangażowanych w realizację zadań publicznych, a w szczególności:
 - a. potencjału ludzkiego, czyli wszystkich pracowników Starostwa w rozumieniu przepisów Kodeksu Pracy, konsultantów, praktykantów, stażystów oraz inne osoby i instytucje mające dostęp do informacji podlegających ochronie;
 - b. dokumentów papierowych i elektronicznych będących własnością Starostwa lub stron zainteresowanych, o ile zostały przekazane na podstawie przepisów prawnych lub umów;
 - c. sprzętu komputerowego, urządzeń mobilnych oraz innych nośników danych (np. magnetycznych – dyskietka, optycznych – CD-R, DVD-R), na których znajdują się informacje podlegające ochronie.
 - 3.4 Technologii służących pozyskiwaniu, selekcjonowaniu, analizowaniu, przetwarzaniu, zarządzaniu i udostępnianiu informacji, do których zalicza się zarówno systemy papierowe jak i elektroniczne wspomagające realizację zadań publicznych.

System Zarządzania Bezpieczeństwem Informacji – ISO 27001		
 POWIAT BIELSKI	POLITYKA ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI	STR. 5/7
	STAROSTWA POWIATOWEGO W BIELSKU-BIAŁEJ	Nr wydania: 3.2

4. Do stosowania zasad określonych przez udokumentowane informacje 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. Sprawna realizacja *Misji* i *Strategii Rozwoju Powiatu Bielskiego* oraz zapewnienie zgodności prowadzonych działań z przepisami prawnymi i innymi wymaganiami obowiązującymi Starostwo zależy od niezakłóconego działania systemów informacyjnych a także właściwego zabezpieczenia przetwarzanych informacji przed istniejącymi zagrożeniami. Mając to na uwadze, Zarząd Powiatu stawia przez Systemem Zarządzania Bezpieczeństwem Informacji następujące cele:
 - 1.1 Zapewnienie ciągłości realizacji Misji Starostwa Powiatowego w Bielsku-Białej poprzez tworzenie, utrzymywanie i testowanie planów zachowania ciągłości działania;
 - 1.2 Zapewnienie poufności, dostępności i integralności informacji przetwarzanych w Starostwie zgodnie z procedurami oraz odpowiednimi przepisami prawa;
 - 1.3 Zapewnienie zgodności z przepisami prawnymi, wymaganiami kontraktowymi i innymi wymaganiami obowiązującymi Starostwo a odnoszącymi się do bezpieczeństwa informacji;
 - 1.4 Zidentyfikowanie wszelkich zasobów w rozumieniu systemu zarządzania bezpieczeństwem informacji oraz określenie ich znaczenia, uwzględnienie podatności oraz zagrożeń dla zasobów w procesie zarządzania ryzykiem;
 - 1.5 Zarządzanie ryzykiem na akceptowalnym poziomie poprzez zaprojektowanie, wdrożenie i utrzymanie formalnego systemu zarządzania;
 - 1.6 Wprowadzenie mechanizmów gwarantujących ochronę zasobów informacyjnych Starostwa Powiatowego;
 - 1.7 Wdrożenie systemu zarządzania incydentami naruszającymi bezpieczeństwo informacji oraz słabościami systemu;
 - 1.8 Zapewnienie ochrony wizerunku i reputacji Starostwa poprzez ograniczenie wpływu zagrożeń dla realizacji zobowiązań zewnętrznych, wynikających z zawartych umów oraz zasad dobrego obyczaju;
 - 1.9 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, jego utrzymania, eksploatacji i doskonalenia;
 - 2.2 Przestrzegania zgodności systemu zarządzania z normą ISO/IEC 27001:2013;
 - 2.3 Uzyskania i utrzymania certyfikatu na zgodność systemu zarządzania z normą ISO/IEC 27001:2013.

System Zarządzania Bezpieczeństwem Informacji – ISO 27001		
 <small>POWIAT BIELSKI</small>	POLITYKA ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI	STR. 6/7
	STAROSTWA POWIATOWEGO W BIELSKU-BIAŁEJ	Nr wydania: 3.2

ROZDZIAŁ VII


ROLE I ODPOWIEDZIALNOŚCI ZWIĄZANE Z BEZPIECZEŃSTWEM INFORMACJI

1. W celu opracowania, wdrożenia i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji zgodnego z normą ISO/IEC 27001:2013 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 i Ciągłości Działania** jest odpowiedzialny za inicjowanie i wspieranie wszelkich działań związanych z bezpieczeństwem informacji i ciągłością działania.
2. Załącznik nr 1 zawiera „Szczegółowe role i odpowiedzialności związane z bezpieczeństwem informacji i ciągłością działania”.
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 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.


System Zarządzania Bezpieczeństwem Informacji – ISO 27001		
 POWIAT BIELSKI	POLITYKA ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI	STR. 7/7
	STAROSTWA POWIATOWEGO W BIELSKU-BIAŁEJ	Nr wydania: 3.2

ROZDZIAŁ IX ZAŁĄCZNIKI


1. Załącznik nr 1 - Szczegółowe role i odpowiedzialności związane z bezpieczeństwem informacji i ciągłością działania.
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 stanowią polityki tematyczne a przede wszystkim Polityka Bezpieczeństwa danych osobowych i Plan ochrony informacji niejawnych, Strategia zarządzania ciągłością działania oraz Plan ciągłości działania, 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 udokumentowane informacje związane z bezpieczeństwem informacji są podporządkowane niniejszej Polityce i stanowią jej integralną część.
5. Specyfikacja głównych dokumentów tworzących ramy systemu zarządzania bezpieczeństwem informacji funkcjonującego zgodnie z normą ISO/IEC 27001:2013 znajduje się w przewodniku Polityki Zarządzania Bezpieczeństwem Informacji Starostwa Powiatowego w Bielsku-Białej.

System Zarządzania Bezpieczeństwem Informacji – ISO 27001		
 POWIAT BIELSKI	POLITYKA ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI	STR. 1/5
	STAROSTWA POWIATOWEGO W BIELSKU-BIAŁEJ	Nr wydania: 3.2
Załącznik nr 1 – Szczegółowe role i odpowiedzialności związane z bezpieczeństwem informacji i ciągłością działania		


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 i Ciągłości Działania 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 zasobów oraz inicjowanie i nadzorowanie prowadzenia szacowania ryzyka w poszczególnych wydziałach,
 - e. weryfikację opracowywanej dokumentacji SZBI,
 - f. udział w pracach Zespołu ds. Bezpieczeństwa Informacji i Ciągłości Działania, 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 ISO/IEC 27001:2013,
 - i. przedstawianie Zarządowi Powiatu oraz Zespołowi ds. Bezpieczeństwa Informacji i Ciągłości Działania 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.

System Zarządzania Bezpieczeństwem Informacji – ISO 27001		
 POWIAT BIELSKI	POLITYKA ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI	STR. 2/5
	STAROSTWA POWIATOWEGO W BIELSKU-BIAŁEJ	Nr wydania: 3.2
Załącznik nr 1 – Szczegółowe role i odpowiedzialności związane z bezpieczeństwem informacji i ciągłością działania		


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 i Ciągłości Działania,
 - k. koordynację działań zapewniających sprawne funkcjonowanie i zabezpieczenie systemów teleinformatycznych Starostwa przed niepożądanym 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 Administratorów aplikacji.

System Zarządzania Bezpieczeństwem Informacji – ISO 27001		
	POLITYKA ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI	STR. 3/5
	STAROSTWA POWIATOWEGO W BIELSKU-BIAŁEJ	Nr wydania: 3.2
Załącznik nr 1 – Szczegółowe role i odpowiedzialności związane z bezpieczeństwem informacji i ciągłością działania		


3. **Zespół ds. Bezpieczeństwa Informacji i Ciągłości Działania** jest odpowiedzialny za inicjowanie i wspieranie wszelkich działań związanych z bezpieczeństwem informacji, a w szczególności za:
- opiniowanie dokumentów SZBI, w tym Polityki Zarządzania Bezpieczeństwem Informacji, polityk niższego rzędu, metodyk, procedur, instrukcji,
 - uzgadnianie podziału odpowiedzialności w zakresie bezpieczeństwa informacji ciągłości działania,
 - wspieranie procesów zarządzania ryzykiem, w tym szacowania ryzyka, monitorowania zmian stopnia narażenia zasobów na podstawowe zagrożenia,
 - okresową analizę danych na temat naruszeń bezpieczeństwa informacji i ciągłości działania oraz monitorowanie naruszeń bezpieczeństwa informacji i ciągłości działania,
 - analizę, ocenę i opiniowanie projektów zmierzających do podniesienia poziomu bezpieczeństwa informacji i ciągłości działania (działania doskonalące),
 - dobór zabezpieczeń,
 - koordynację procesów doskonalenia SZBI, w tym wdrażania określonych zabezpieczeń w systemach lub usługach,
 - zabezpieczanie realizacji jednolitej Polityki Zarządzania Bezpieczeństwem Informacji w całym Starostwie,
 - zgłaszanie do Pełnomocnika Zarządu ds. SZBI poprawek i aktualizacji do opracowanych dokumentów SZBI, w tym do Polityki Zarządzania Bezpieczeństwem Informacji,
 - wspieranie inicjatyw dotyczących propagowania tematyki bezpieczeństwa informacji i ciągłości działania w całym Starostwie,
 - wspieranie Zarządu Powiatu w planowaniu budżetu zapewniającego prawidłowe funkcjonowanie SZBI w Starostwie,
 - przeciwdziałanie próbom naruszenia bezpieczeństwa informacji i ciągłości działania,
 - opracowanie i wdrożenie Planu ciągłości działania (budowa świadomości pracowników o wadze zarządzania ciągłością działania, przeprowadzanie szkoleń dla personelu zaangażowanego w realizację Planu ciągłości działania),
 - przeprowadzanie testowania, oceny i aktualizacja Planu ciągłości działania.
4. **Właściciele zasobów** (Naczelnicy / równorzędne stanowiska) są odpowiedzialni za wdrożenie, utrzymanie i doskonalenie systemu zarządzania bezpieczeństwem informacji w wydziale, a w szczególności za:
- 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,
 - udostępnienie PZ ds. SZBI, ABST oraz Zespołowi ds. Bezpieczeństwa Informacji i Ciągłości Działania wszelkich danych i informacji niezbędnych do opracowania, wdrożenia i doskonalenia SZBI,
 - zapewnienie inwentaryzacji zasobów,

System Zarządzania Bezpieczeństwem Informacji – ISO 27001		
	POLITYKA ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI	STR. 4/5
	STAROSTWA POWIATOWEGO W BIELSKU-BIAŁEJ	Nr wydania: 3.2
Załącznik nr 1 – Szczegółowe role i odpowiedzialności związane z bezpieczeństwem informacji i ciągłością działania		


- d. zapewnienie prawidłowej klasyfikacji i ochrony zasobów,
 - e. określanie, które osoby i na jakich prawach mają mieć dostęp do danych informacji,
 - f. określenie i okresowe sprawdzanie ograniczeń dostępu i klasyfikacji istotnych zasobów, z uwzględnieniem stosowanych polityk kontroli dostępu,
 - g. zapewnienie odpowiedniej obsługi podczas usuwania lub niszczenia zasobów,
 - h. okresowe raportowanie o poziomie bezpieczeństwa informacji w Wydziale,
 - i. 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),
 - j. przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
 - k. przegląd praw dostępu użytkowników w regularnych odstępach czasu.
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 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 prawnie chronionej 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,

System Zarządzania Bezpieczeństwem Informacji – ISO 27001		
	POLITYKA ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI	STR. 5/5
	STAROSTWA POWIATOWEGO W BIELSKU-BIAŁEJ	Nr wydania: 3.2
Załącznik nr 1 – Szczegółowe role i odpowiedzialności związane z bezpieczeństwem informacji i ciągłością działania		

- 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. z 2003 r., Nr 153, poz. 1503 z późn. zm.). Jednocześnie osoby takie muszą zapoznać się z Polityką Zarządzania Bezpieczeństwem Informacji Starostwa oraz podpisać zobowiązanie o jej przestrzeganiu. Do obowiązków osób trzecich należy:
- a. przestrzeganie tajemnicy prawnie chronionej w zakresie przez prawo przewidzianym,
 - b. stosowanie się do obowiązującej Polityki Zarządzania Bezpieczeństwem Informacji oraz uzupełniających ją innych dokumentów, jeśli takowe mają zastosowanie.
 - c. zgłaszanie wszelkich przypadków działań niezgodnych z politykami i regulaminami, mogących być zdarzeniami lub incydentami bezpieczeństwa,
 - d. przeciwdziałanie próbom naruszenia bezpieczeństwa informacji.
- Zabrania się osobom trzecim auditowania zagadnień dotyczących informacji niejawnych, do kontroli których uprawnionymi są wyłącznie Agencja Bezpieczeństwa Wewnętrznego i Pełnomocnik Ochrony.
8. **Audytorzy Wewnętrzni SZBI** (AW-SZBI) są odpowiedzialni za planowanie, realizowanie i dokumentowanie audytów wewnętrznych zleczanych przez Pełnomocnika Zarządu ds. SZBI, zgodnie z wymaganiami procedury *P-PP1.4/PZ Audyty 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 ISO/IEC 27001:2013 oraz miejsc wymagających wprowadzenia poprawek,
 - c. wspomaganie Zespołu ds. Bezpieczeństwa Informacji i Ciągłości Działania 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.

System Zarządzania Bezpieczeństwem Informacji – ISO 27001		
 <small>POWIAT BIELSKI</small>	POLITYKA ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI	STR. 1/2
	STAROSTWA POWIATOWEGO W BIELSKU-BIAŁEJ	Nr wydania: 3.2
Załącznik nr 2 – Wykaz obowiązujących Starostwo głównych aktów prawnych związanych z bezpieczeństwem informacji		

1. **Ustawa** z dnia 21 listopada 2008r. o **pracownikach samorządowych** (t.j. Dz.U. z 2016r. poz. 902).
2. **Ustawa** z dnia 27 sierpnia 2009r. o **finansach publicznych** (t.j. Dz.U. z 2016r. poz. 1870 z późn. zm.)
3. **Ustawa** z dnia 14 czerwca 1960r. – **Kodeks postępowania administracyjnego** (t.j. Dz.U. z 2017 r. poz. 1257).
4. **Ustawa** z dnia 5 sierpnia 2010r. o **ochronie informacji niejawnych** (Dz.U. z 2016r. poz. 1167) wraz z mającymi zastosowanie aktami wykonawczymi.
5. **Ustawa** z dnia 29 sierpnia 1997r. o **ochronie danych osobowych** (t.j. Dz.U. z 2016r. poz. 922).
6. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz.U. z 2008 r. Nr 229, poz. 1536).
7. 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 urzędnicy i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004r. Nr 100, poz. 1024).
8. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz.U. z 2014r. poz. 1934).
9. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz.U. z 2015r. poz. 719).
10. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. z 2015r. poz. 745).
11. **Rozporządzenie** Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie **ochrony osób fizycznych w związku z przetwarzaniem danych osobowych** i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – Dz.U.UE.L.2016.119.1.
12. **Ustawa** z dnia 6 września 2001r. o **dostępie do informacji publicznej** (t.j. Dz.U. z 2016r. poz. 1764).
13. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007r. w sprawie Biuletynu informacji publicznej (Dz.U. z 2007r. Nr 10, poz. 68).
14. Ustawa z dnia 25 lutego 2016r. o ponownym wykorzystaniu informacji sektora publicznego (Dz.U. z 2016r. poz. 352).
15. **Ustawa** z dnia 29 stycznia 2004r. **Prawo zamówień publicznych** (Dz.U. z 2015r. poz. 2164).

System Zarządzania Bezpieczeństwem Informacji – ISO 27001		
 <small>POWIAT BIELSKI</small>	POLITYKA ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI	STR. 2/2
	STAROSTWA POWIATOWEGO W BIELSKU-BIAŁEJ	Nr wydania: 3.2
Załącznik nr 2 – Wykaz obowiązujących Starostwo głównych aktów prawnych związanych z bezpieczeństwem informacji		

16. **Ustawa** z dnia 16 kwietnia 1993r. o **zwalczaniu nieuczciwej konkurencji** (Dz.U. z 2003r. Nr 153, poz. 1503 z późn. zm.).
17. **Ustawa** z dnia 4 lutego 1994r. o **prawie autorskim i prawach pokrewnych** (t.j. Dz.U. z 2017r. poz. 880).
18. **Ustawa** z dnia 17 lutego 2005r. o **informatyzacji działalności podmiotów realizujących zadania publiczne** (t.j. Dz.U. z 2017r. poz. 570) wraz z mającymi zastosowanie aktami wykonawczymi.
19. **Rozporządzenie** Rady Ministrów z dnia 12 kwietnia 2012r. 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 2016r. poz. 113 z późn. zm.).
20. **Ustawa** z dnia 18 lipca 2002r. o **świadczeniu usług drogą elektroniczną** (t.j. Dz.U. z 2017r. poz. 1219).
21. **Ustawa** z dnia 27 lipca 2001r. o **ochronie baz danych** (Dz.U. z 2001r. Nr 128, poz. 1402 z późn. zm.).
22. **Ustawa** z dnia 5 września 2016r. o **usługach zaufania oraz identyfikacji elektronicznej** (Dz.U. z 2016r. poz. 1579).
23. **Ustawa** z dnia 29 czerwca 1995r. o **statystyce publicznej** (t.j. Dz.U. z 2016r. poz. 1068).
24. **Ustawa** z dnia 6 czerwca 1997r. **Kodeks karny** (Dz.U. z 2016r. poz. 1137 z późn. zm.).
25. **Ustawa** z dnia 26 czerwca 1974r. – **Kodeks pracy** (t.j. Dz.U. z 2016r. poz. 1666 z późn. zm.).
26. **Ustawa** z dnia 23 kwietnia 1964r. - **Kodeks cywilny** (t.j. Dz.U. z 2017r. poz. 459).
27. **Ustawa** z dnia 29 września 1994r. o **rachunkowości** (t.j. Dz. U. z 2016r. poz. 1047 z późn. zm.).