~~Projekt~~

ZARZĄDZENIE Nr 39/2013
Starosty Bielskiego
z dnia 30 sierpnia 2013 r.

w sprawie: zmiany Zarządzenia Nr 4/2009 Starosty Bielskiego z dnia 14 stycznia 2009 roku 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 2013 r. poz. 595)

zarządzam, co następuje:

§ 1

W Zarządzeniu Nr 4/2009 Starosty Bielskiego z dnia 14 stycznia 2009 roku 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 zmienionego Zarządzeniem Nr 12/2010 Starosty Bielskiego z dnia 24 marca 2010 roku oraz Zarządzeniem Nr 18/2011 Starosty Bielskiego z dnia 21 marca 2011 roku i Zarządzeniem Nr 13/2012 Starosty Bielskiego z dnia 17 lutego 2012 roku wprowadzam następujące zmiany:

W treści Załącznika – Polityka Zarządzania Bezpieczeństwem Informacji:

1. W Rozdziale III – „Podstawy normatywne i terminologia” pkt 3.8 po słowie „informacji” dopisuje się słowa „i ciągłością działania.”

2. W Rozdziale VI – „Bezpieczeństwo w Starostwie” pkt 1.4 otrzymuje brzmienie:

   „1.4 Zidentyfikowanie wszelkich aktywów w rozumieniu systemu zarządzania bezpieczeństwem informacji oraz określenie ich wartości i znaczenia dla Starostwa poprzez przeprowadzenie oceny ryzyka, według kryteriów przyjętych w procesie zarządzania ryzykiem, zrozumienie ich podatności oraz zagrożeń, które mogą narazić je na ryzyko;”

3. W Rozdziale VII – „Role i odpowiedzialności związane z bezpieczeństwem informacji”:

1) pkt 1.3 otrzymuje brzmienie:

„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) pkt 2 po słowie „informacji” dodaje się słowa „i ciągłością działania.”

4. W Rozdziale IX – „Załączniki” pkt 1 po słowie „informacji” dodaje się słowa „i ciągłością działania.”

5. W Rozdziale X – „Odwołanie do dokumentów systemowych” pkt 2 otrzymuje brzmienie:

   „Poziom drugi stanowi 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.”

6. Załącznik nr 1 – „Szczegółowe role i odpowiedzialności związane z bezpieczeństwem informacji” otrzymuje brzmienie stanowiące załącznik 1 do niniejszego zarządzenia.

7. Załącznik nr 2 – „Wykaz obowiązujących Starostwo głównych aktów prawnych związanych z bezpieczeństwem informacji” otrzymuje brzmienie stanowiące załącznik 2 do niniejszego zarządzenia.

§ 2

Zobowiązuję Naczelników Wydziałów (jednostek równorzędnych) do zapoznania podległych im pracowników z niniejszym Zarządzeniem.

§ 3

Wykonanie Zarządzenia powierzam Pełnomocnikowi Zarządu ds. Systemu Zarządzania Jakością i Bezpieczeństwem Informacji.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

Starosta

Andrzej Płonka

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 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 PN ISO/IEC 27001:2007,
   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.

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 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. Obsługi Informatycznej w zakresie zapewnienia bezpieczeństwa informacji

t. nadzorowanie pracy Administratorów aplikacji.

3. **Zespół ds. Bezpieczeństwa Informacji i Ciągłości Działania** 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 ciągłości działania,

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 i ciągłości działania oraz monitorowanie naruszeń bezpieczeństwa informacji i ciągłości działania,

e. analizę, ocenę i opiniowanie projektów zmierzających do podniesienia poziomu bezpieczeństwa informacji i ciągłości działania (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 i ciągłości działania w całym Starostwie,

k. wspieranie Zarządu Powiatu w planowaniu budżetu zapewniającego prawidłowe funkcjonowanie SZBI w Starostwie,

l. przeciwdziałanie próbom naruszenia bezpieczeństwa informacji i ciągłości działania,

m. opracowanie i wdrożenie Planu ciągłości działania (budowa świadomości pracowników o wadze zarządzania ciągłością działania, przeprowadzanie szkoleń dla personelu zaangażowanego w realizacje Planu ciągłości działania),

n. 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:
   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 i Ciągłości Działania 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 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. z 2003 r., Nr 153, poz. 1503 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 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 zlecanych przez Pełnomocnika Zarządu ds. SZBI, zgodnie z wymaganiami procedury *P-PP1.4/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 i Ciągłością 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.

Załącznik 2 do Zarządzenia
Nr 39/2013 z dnia 30.08.2013 roku

1. **Ustawa** z dnia 21 listopada 2008 r. **o pracownikach samorządowych** (Dz. U. z 2008 r. Nr 223, poz. 1458 z późn. zm.).
2. **Ustawa** z dnia 27 sierpnia 2009 r. **o finansach publicznych** (Dz. U. z 2013 r. poz. 885)
3. **Ustawa** z dnia 14 czerwca 1960 r. – **Kodeks postępowania administracyjnego** (Dz. U. z 2013 r. poz. 267).
4. **Ustawa** z dnia 5 sierpnia 2010 r. **o ochronie informacji niejawnych** (Dz. U. z 2010 r. Nr 182, poz. 1228) wraz z mającymi zastosowanie aktami wykonawczymi.
5. **Ustawa** z dnia 29 sierpnia 1997 r. **o ochronie danych osobowych** (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.).
6. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. 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 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).
8. **Ustawa** z dnia 6 września 2001 r. **o dostępie do informacji publicznej** (Dz. U. z 2001 r. Nr 112, poz. 1198 z późn. zm.).
9. 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).
10. **Ustawa** z dnia 29 stycznia 2004 r. **Prawo zamówień publicznych** (Dz. U. z 2013 r. poz. 907)

11. **Ustawa** z dnia 16 kwietnia 1993 r. **o zwalczaniu nieuczciwej konkurencji** (Dz. U. z 2003 r. Nr 153, poz. 1503 z późn. zm.)
12. **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.).
13. **Ustawa** z dnia 17 lutego 2005 r. **o informatyzacji działalności podmiotów realizujących zadania publiczne** (Dz. U. z 2013 poz. 235) wraz z mającymi zastosowanie aktami wykonawczymi.
14. **Ustawa** z dnia 18 lipca 2002 r. **o świadczeniu usług drogą elektroniczną** (Dz. U. z 2002 r. Nr 144, poz. 1204 z późn. zm.)
15. **Ustawa** z dnia 27 lipca 2001 r. **o ochronie baz danych** (Dz. U. z 2001 r. Nr 128, poz. 1402 z późn. zm.).
16. **Ustawa** z dnia 18 września 2001 r. **o podpisie elektronicznym** (Dz. U. z 2013 r. poz. 262)
17. **Ustawa** z dnia 29 czerwca 1995 r. **o statystyce publicznej** (Dz. U. z 2012 r. poz. 591 z późn. zm.)
18. **Ustawa** z dnia 6 czerwca 1997 r. **Kodeks karny** (Dz. U. z 1997 r. Nr 88, poz. 553 z późn. zm.).
19. **Ustawa** z dnia 26 czerwca 1974 r. – **Kodeks pracy** (Dz. U. z 1998 r. Nr 21, poz. 94, z późn. zm.).
20. **Ustawa** z dnia 23 kwietnia 1964 r. - **Kodeks cywilny** (Dz. U. z 1964 r. Nr 16, poz. 93, z późn. zm.).