



## UCHWAŁA NR 432/2026 ZARZĄDU POWIATU W BUSKU-ZDROJU

z dnia 27 sierpnia 2026 r.

### w sprawie zmiany Regulaminu Organizacyjnego Starostwa Powiatowego w Busku-Zdroju

Na podstawie art. 32 ust. 2 pkt 6 i art. 35 ust. 1 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz.U. z 2025 r. poz. 1684 z późn. zm.) Zarząd Powiatu w Busku-Zdroju uchwala, co następuje:

#### § 1.

W Regulaminie Organizacyjnym Starostwa Powiatowego w Busku-Zdroju uchwalonym Uchwałą Nr 1247/2024 Zarządu Powiatu w Busku-Zdroju z dnia 28 czerwca 2024 r. wprowadza się następujące zmiany:

1) § 5 pkt 3 otrzymuje brzmienie:

„3) Wydział Geodezji, Katastru i Gospodarki Nieruchomościami – „GKN” a w nim:

a) Referat Katastru – „GKN-I”,

b) Referat Gospodarki Nieruchomościami – „GKN-II”,

c) Referat – Powiatowy Ośrodek Dokumentacji Geodezyjnej i Kartograficznej – „GKN-III”,”;

2) w § 5 po pkt 15 dodaje się pkt 16 i 17 w brzmieniu:

„16) Samodzielne stanowisko pracy - Inspektor Ochrony Danych – „IOD”,

17) Samodzielne stanowisko pracy ds. cyberbezpieczeństwa – „CB”.”;

3) § 10 otrzymuje następujące brzmienie:

„§ 10. 1. Pracownicy zatrudnieni w wydziałach pozostają w bezpośredniej zależności służbowej od naczelnika wydziału. Dotyczy to również zastępcy naczelnika wydziału.

2. Pracownicy zatrudnieni w referatach funkcjonujących w ramach wydziału pozostają w bezpośredniej zależności służbowej od kierownika referatu, którego bezpośrednim przełożonym jest naczelnik wydziału.”;

4) w § 12 po pkt 12 dodaje się pkt 13-15 w brzmieniu:

„13) Kierownik Referatu Katastru,

14) Kierownik Referatu Gospodarki Nieruchomościami,

15) Kierownik Powiatowego Ośrodka Dokumentacji Geodezyjnej i Kartograficznej.”;

5) w § 15 po pkt 8 dodaje się pkt 9 i 10 w brzmieniu:

„9) Samodzielnego stanowiska pracy - Inspektora Ochrony Danych,

10) Samodzielnego stanowiska pracy ds. cyberbezpieczeństwa.”;

6) w § 38 po ust. 3 dodaje się ust. 4 i 5 w brzmieniu:

„4. **Samodzielne stanowisko pracy - Inspektor Ochrony Danych** - odpowiada za koordynowanie, monitorowanie i wspieranie realizacji przez Starostwo oraz - w zakresie, w jakim przepisy prawa lub organizacja obsługi wspólnej przewidują realizację zadań na rzecz jednostek organizacyjnych Powiatu - obowiązków w zakresie ochrony danych osobowych.

**5. Samodzielne stanowisko pracy ds. cyberbezpieczeństwa** - odpowiada za koordynowanie, monitorowanie i wspieranie realizacji przez Starostwo oraz - w zakresie, w jakim przepisy prawa lub organizacja obsługi wspólnej przewidują realizację zadań na rzecz jednostek organizacyjnych Powiatu - obowiązków w zakresie cyberbezpieczeństwa, wynikających w szczególności z ustawy o krajowym systemie cyberbezpieczeństwa, przepisów wykonawczych, przepisów wdrażających dyrektywę NIS2 oraz innych właściwych przepisów prawa.”;

7) w § 52 po ust. 3 dodaje się ust. 4 i 5 w brzmieniu:

„4. Do zakresu działania samodzielnego stanowiska pracy - Inspektora Ochrony Danych należy:

- 1) informowanie Starosty jako Administratora Danych Osobowych, zwanego dalej „Administratorem” oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów dotyczących ochrony danych osobowych, a także doradzanie im w sprawie ochrony danych osobowych,
- 2) monitorowanie przestrzegania RODO oraz innych przepisów dotyczących ochrony danych osobowych oraz polityk Administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,
- 3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z RODO,
- 4) współpraca z organem nadzorczym,
- 5) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych, w tym z uprzednimi konsultacjami, o których mowa w RODO oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,
- 6) pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz wykonywaniem praw przysługujących im na mocy RODO oraz innych przepisów.

5. Do zakresu działania samodzielnego stanowiska pracy ds. cyberbezpieczeństwa należy:

- 1) Koordynowanie i realizacja obowiązków Starostwa wynikających z ustawy o krajowym systemie cyberbezpieczeństwa, w tym monitorowanie zmian przepisów prawa, wymagań właściwych organów oraz rekomendacji i standardów dotyczących cyberbezpieczeństwa.
- 2) Koordynowanie i realizacja obowiązków formalnych podmiotu kluczowego, w tym obowiązków związanych z Wykazem podmiotów kluczowych i podmiotów ważnych, aktualizacją danych oraz przekazywaniem wymaganych informacji właściwym organom i podmiotom krajowego systemu cyberbezpieczeństwa.
- 3) Koordynowanie i realizacja obowiązków związanych z wykorzystywaniem właściwych systemów teleinformatycznych krajowego systemu cyberbezpieczeństwa, w tym zapewnienie aktualności danych kontaktowych osób wyznaczonych do współpracy z właściwymi podmiotami KSC.
- 4) Koordynowanie opracowania, wdrożenia, utrzymywania, aktualizowania, monitorowania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), z uwzględnieniem wymagań ustawy o krajowym systemie cyberbezpieczeństwa i właściwych przepisów wykonawczych.
- 5) Opracowywanie, aktualizowanie i koordynowanie wdrażania wewnętrznych polityk, regulacji, procedur i instrukcji dotyczących cyberbezpieczeństwa i bezpieczeństwa informacji oraz monitorowanie ich przestrzegania.
- 6) Koordynowanie procesu identyfikacji, analizy, oceny i monitorowania ryzyka w zakresie cyberbezpieczeństwa, w tym ryzyka związanego z systemami informacyjnymi, procesami realizowanymi przez Starostwo, dostawcami oraz usługami świadczonymi z wykorzystaniem systemów informacyjnych.
- 7) Koordynowanie identyfikacji zagrożeń, podatności i innych słabości bezpieczeństwa oraz inicjowanie i monitorowanie działań mających na celu ograniczenie zidentyfikowanego ryzyka.

- 8) Koordynowanie doboru i wdrażania, odpowiednich do poziomu ryzyka, środków technicznych i organizacyjnych służących zapewnieniu bezpieczeństwa systemów informacyjnych, w szczególności ich poufności, integralności, dostępności i autentyczności.
- 9) Współpraca z komórkami organizacyjnymi właściwymi do spraw informatyki oraz administratorami systemów w zakresie projektowania, nabywania, wdrażania, utrzymywania, modyfikowania i wycofywania systemów informacyjnych, w celu zapewnienia uwzględnienia wymagań cyberbezpieczeństwa na wszystkich etapach ich cyklu życia.
- 10) Opiniowanie pod względem cyberbezpieczeństwa projektów nowych systemów informacyjnych, zmian w istniejących systemach, rozwiązań infrastrukturalnych, usług chmurowych, oprogramowania oraz innych rozwiązań teleinformatycznych, w zakresie wynikającym z przeprowadzonej oceny ryzyka.
- 11) Monitorowanie stosowania środków ochrony systemów informacyjnych, w szczególności w zakresie zarządzania dostępem, uwierzytelniania, ochrony przed złośliwym oprogramowaniem, aktualizacji i zarządzania podatnościami, kopii zapasowych, kryptografii, bezpieczeństwa fizycznego, bezpiecznej konfiguracji oraz innych zabezpieczeń wynikających z oceny ryzyka.
- 12) Koordynowanie działań dotyczących bezpieczeństwa łańcucha dostaw, w tym identyfikowanie i monitorowanie ryzyka związanego z dostawcami produktów ICT, usług ICT i procesów ICT oraz udział w określaniu wymagań dotyczących cyberbezpieczeństwa w postępowaniach zakupowych i umowach.
- 13) Koordynowanie procesu wykrywania, identyfikowania, klasyfikowania, obsługi, dokumentowania i zarządzania incydentami cyberbezpieczeństwa oraz monitorowanie zdarzeń mogących mieć wpływ na bezpieczeństwo systemów informacyjnych.
- 14) Koordynowanie realizacji obowiązków związanych ze zgłaszaniem incydentów właściwym zespołom CSIRT, w tym przygotowywanie i przekazywanie wymaganych informacji w terminach i formie określonych przepisami prawa.
- 15) Koordynowanie działań podejmowanych w związku z wystąpieniem incydentu, w tym działań mających na celu ograniczenie jego skutków, usunięcie przyczyn, przywrócenie prawidłowego funkcjonowania systemów oraz zapobieganie ponownemu wystąpieniu podobnych incydentów.
- 16) Przeprowadzanie analiz poincydentalnych oraz monitorowanie realizacji działań korygujących i zapobiegawczych wynikających z incydentów, analiz, kontroli i ocen bezpieczeństwa.
- 17) Koordynowanie przygotowania, aktualizacji, testowania i doskonalenia planów ciągłości działania, planów odtworzenia systemów oraz procedur postępowania na wypadek awarii, incydentu lub innego zdarzenia mogącego zakłócić realizację zadań publicznych.
- 18) Koordynowanie działań w zakresie zapewnienia odporności systemów informacyjnych i usług realizowanych z ich wykorzystaniem, z uwzględnieniem wyników analiz ryzyka oraz wymagań dotyczących ciągłości działania.
- 19) Koordynowanie realizacji obowiązków związanych z przeprowadzaniem audytów cyberbezpieczeństwa wymaganych przepisami prawa, w tym przygotowywanie Starostwa do audytu, współpraca z audytorem, zapewnienie zgromadzenia wymaganej dokumentacji i informacji oraz monitorowanie realizacji zaleceń poaudytowych.
- 20) Organizowanie i koordynowanie wewnętrznych przeglądów, analiz i ocen poziomu cyberbezpieczeństwa oraz monitorowanie realizacji wynikających z nich działań naprawczych i doskonalących.
- 21) Monitorowanie zgodności stosowanych rozwiązań, procesów, procedur i dokumentacji z obowiązującymi przepisami prawa w zakresie cyberbezpieczeństwa, w szczególności z ustawą o krajowym systemie cyberbezpieczeństwa, oraz – w zakresie przyjętym przez Starostwo – z normami, standardami i dobrymi praktykami.
- 22) Koordynowanie współpracy z właściwymi zespołami CSIRT, organami właściwymi do spraw cyberbezpieczeństwa oraz innymi podmiotami krajowego systemu cyberbezpieczeństwa, a także z podmiotami zewnętrznymi świadczącymi usługi związane z cyberbezpieczeństwem.

23) Koordynowanie wyznaczenia i aktualizacji danych osób odpowiedzialnych za utrzymywanie kontaktów z właściwymi podmiotami krajowego systemu cyberbezpieczeństwa oraz zapewnienie ciągłości realizacji tych zadań.

24) Koordynowanie działań związanych z zapewnieniem pracownikom dostępu do aktualnej wiedzy dotyczącej cyberzagrożeń, sposobów ochrony przed nimi oraz zasad bezpiecznego korzystania z systemów i usług teleinformatycznych.

25) Koordynowanie organizacji szkoleń, ćwiczeń, kampanii informacyjnych i innych działań podnoszących świadomość pracowników w zakresie cyberbezpieczeństwa.

26) Koordynowanie działań dotyczących bezpieczeństwa zasobów ludzkich, w tym – w zakresie wynikającym z przepisów prawa – realizacji wymagań dotyczących osób wykonujących zadania związane z cyberbezpieczeństwem.

27) Koordynowanie zapewnienia mechanizmów umożliwiających pracownikom i użytkownikom usług zgłaszanie cyberzagrożeń, incydentów oraz podatności, zgodnie z obowiązującymi przepisami i procedurami wewnętrznymi.

28) Prowadzenie i aktualizowanie dokumentacji związanej z realizacją zadań z zakresu cyberbezpieczeństwa, w szczególności dokumentacji SZBI, ocen ryzyka, incydentów, audytów, przeglądów, działań naprawczych i szkoleń – w zakresie właściwym dla zadań Pełnomocnika ds. cyberbezpieczeństwa podmiotu kluczowego.

29) Przygotowywanie dla Starosty oraz właściwych osób funkcyjnych Starostwa analiz, opinii, rekomendacji, raportów i informacji dotyczących poziomu cyberbezpieczeństwa, ryzyka, incydentów, realizacji obowiązków podmiotu kluczowego oraz funkcjonowania SZBI.

30) Niezwłoczne informowanie Starosty o istotnych zagrożeniach, incydentach, niezgodnościach lub innych okolicznościach mogących mieć istotny wpływ na cyberbezpieczeństwo, ciągłość realizacji zadań publicznych lub wykonanie obowiązków wynikających z ustawy o krajowym systemie cyberbezpieczeństwa.

31) Przedstawianie Staroście rekomendacji dotyczących działań niezbędnych do zapewnienia zgodności Starostwa z wymaganiami ustawy o krajowym systemie cyberbezpieczeństwa oraz podnoszenia poziomu cyberbezpieczeństwa, w tym rekomendacji dotyczących środków organizacyjnych, technicznych, finansowych i kadrowych.

32) Współpraca z Inspektorem Ochrony Danych, komórkami organizacyjnymi Starostwa, administratorami systemów, osobami odpowiedzialnymi za bezpieczeństwo informacji, audytem wewnętrznym oraz innymi osobami i podmiotami realizującymi zadania związane z bezpieczeństwem, w celu zapewnienia spójności działań w zakresie cyberbezpieczeństwa, bezpieczeństwa informacji i ochrony danych.

33) Monitorowanie realizacji zaleceń wynikających z audytów, kontroli, ocen ryzyka, analiz bezpieczeństwa oraz innych działań weryfikacyjnych dotyczących cyberbezpieczeństwa.

34) Inicjowanie działań doskonalących system zarządzania cyberbezpieczeństwem, z uwzględnieniem wyników ocen ryzyka, incydentów, audytów, kontroli, zmian technologicznych oraz zmieniającego się poziomu zagrożeń.

35) Wykonywanie innych zadań związanych z koordynowaniem realizacji obowiązków w zakresie cyberbezpieczeństwa, wynikających z ustawy o krajowym systemie cyberbezpieczeństwa, przepisów wykonawczych, innych obowiązujących przepisów prawa oraz wewnętrznych regulacji Starostwa.”;

8) Załącznik nr 1 do Regulaminu Organizacyjnego Starostwa Powiatowego w Busku-Zdroju otrzymuje brzmienie określone w załączniku do niniejszej uchwały.

## § 2.

Wykonanie Uchwały powierza się Przewodniczącemu Zarządu Powiatu.

**§ 3.**

Uchwała wchodzi w życie z dniem 1 września 2026 r., z zastrzeżeniem zmian określonych w § 1 pkt 1, które wchodzi w życie z dniem 1 stycznia 2027 r.

Przewodniczący Zarządu

**mgr inż. Jerzy Kolarz**

Załącznik do uchwały nr 432/2026  
Zarządu Powiatu w Busku-Zdroju  
z dnia 27 sierpnia 2026 r.

**Schemat struktury organizacyjnej Starostwa Powiatowego w Busku-Zdroju**



## **Uzasadnienie**

Zmiany w Regulaminie Organizacyjnym Starostwa Powiatowego w Busku-Zdroju podyktowane są potrzebą uregulowania planowanych zmian organizacyjnych.

W strukturze Starostwa planowane jest utworzenie nowego samodzielnego stanowiska pracy odpowiedzialnego za bezpieczeństwo informacji i cyberbezpieczeństwo.

Ponadto, w związku z planowanym wdrożeniem od 1 stycznia 2027 r. nowego systemu elektronicznego obiegu dokumentów, w którym - ze względu na jego wymagania techniczne - konieczne jest stosowanie oznaczeń identyfikujących poszczególne referaty, zachodzi potrzeba nadania referatom funkcjonującym w ramach Wydziału Geodezji, Katastru i Gospodarki Nieruchomościami odrębnych symboli stanowiących ich wyróżniki na potrzeby nadawania numerów prowadzonych spraw.

Jednocześnie uregulowano kwestię podległości służbowej kierowników tych referatów oraz uwzględniono wprowadzone zmiany na graficznym schemacie struktury organizacyjnej Starostwa.