

**Regulamin dostępu w trybie chronionym
do Geoportalu Powiatu Krasnostawskiego znajdującego się pod adresem:**

<https://powiatkrasnostawski.geoportal2.pl/>

**Procedura tworzenia i bezpiecznego użytkowania Systemu Geoportal Powiatu Krasnostawskiego
(w trybie chronionym) zlokalizowanego w infrastrukturze informatycznej Starostwa Powiatowego
w Krasnymstawie, pod adresem: <https://powiatkrasnostawski.geoportal2.pl/>**

1. Zasady uzyskania dostępu.

- 1) W celu uzyskania dostępu, w trybie chronionym, do zasobów Systemu informatycznego tj. Geoportalu Powiatu Krasnostawskiego, zwanego dalej Systemem, Wnioskodawca składa do Starosty Krasnostawskiego pisemny wniosek o założenie/aktualizację/odebranie dostępu do Systemu, zgodny z udostępnionymi wzorem znajdującym się na stronie BIP Starostwa.
- 2) Dostęp do Geoportalu Powiatu Krasnostawskiego w trybie chronionym dotyczy następujących modułów Systemu: Geoportal – tryb chroniony, Obsługa Wykonawcy prac geodezyjnych, Dane RCN, Dane opisowe EGiB, Zapytania komornicze, Internetowe narady koordynacyjne – ZUD.
- 3) Każdy wniosek jest rejestrowany z nadanym numerem rejestru korespondencji przychodzącej zgodnie z Instrukcją kancelaryjną obowiązującą w Starostwie.
- 4) Warunkiem uzyskania dostępu do zasobów Systemu jest poprawnie złożony wniosek oraz jego akceptacja przez Starostę lub osobę upoważnioną.
- 5) Zaakceptowany wniosek przekazywany jest Administratorowi Systemu Informatycznego lub osobie upoważnionej, zwanej dalej: ASI w Starostwie.
- 6) ASI jest odpowiedzialny za nadawanie i odbieranie praw dostępu do Systemów i usług wszystkim użytkownikom zgodnie z Polityką Bezpieczeństwa Informacji wdrożonej w Starostwie.
- 7) ASI nadaje nazwę Użytkownika (login) i hasło do pierwszego logowania i przekazuje Użytkownikowi telefonicznie, pocztą e-mail, osobiście lub w innej uzgodnionej formie.
- 8) Hasło składa się z unikalnego zestawu, zawierającego co najmniej osiem znaków, w tym małe i wielkie litery oraz cyfry i znaki specjalne. Hasło nie może być identyczne z identyfikatorem Użytkownika ani jego imieniem lub nazwiskiem.
- 9) Przed przekazaniem danych do uwierzytelnienia Użytkownikowi następuje weryfikacja poprawności przydzielonych praw dostępu.
- 10) Każdy Użytkownik posiadający konto w Systemie zobowiązany jest przestrzegać poniższych zasad bezpieczeństwa oraz zgłaszać wszelkie stwierdzone fakty lub podejrzenia naruszenia atrybutów bezpieczeństwa (poufności, integralności, dostępności).
- 11) Blokada dostępu do Systemu następuje w przypadkach:
 - braku aktywności w Systemie przez okres 12 miesięcy licząc od ostatniego logowania Użytkownika,
 - zaistnienia podejrzenia naruszenia zasad bezpieczeństwa.
- 12) W przypadku blokady dostępu do Systemu Użytkownik zostanie powiadomiony o tym fakcie drogą e-mail.
- 13) Usunięcie konta następuje na pisemny wniosek Użytkownika.

2. Podstawowe zasady bezpiecznego użytkowania Systemu.

- 14) W momencie zakładania Użytkownika w Systemie informatycznym generowane jest jednorazowe hasło. Użytkownik zobligowany jest do jego zmiany przy pierwszym logowaniu.
- 15) Uwierzytelnianie Użytkownika w Systemie realizowane jest za pomocą przypisanego unikalnego loginu oraz hasła.
- 16) Użytkownicy Systemu zobowiązani są do zmiany hasła nie rzadziej niż co 30 dni i nie częściej niż co 1 dzień. ASI może w uzasadnionych sytuacjach polecić dokonanie zmiany hasła przez Użytkownika.
- 17) Użytkownicy zobowiązani są do zachowania w poufności haseł, tj. niezapisywania ich w miejscach ogólnodostępnych i korzystania z nich w sposób uniemożliwiający odczyt osobom postronnym.
- 18) Zabrania się Użytkownikom Systemu udostępniania swojego loginu i hasła innym osobom oraz korzystania z loginu lub hasła innego Użytkownika.
- 19) Logowanie do Systemu następuje wyłącznie z komputera służbowego i w celach służbowych.
- 20) Użytkownicy Systemu mają obowiązek przetwarzać dane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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.Urz. UE L 119, s. 1) oraz ustawy z 10 maja 2018r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000) i przepisów powszechnie obowiązującego prawa. Klauzule informacyjna dotycząca przetwarzania danych osobowych dołączona jest do Wniosku.
- 21) Udostępnione informacje nie mogą być powielane w innym celu niż służbowy, ujawniane osobom nieupoważnionym, stanowią tajemnice wynikające z przepisów powszechnie obowiązującego prawa.
- 22) Obowiązki wobec udostępnionych danych z Systemu ma charakter bezterminowy, obowiązuje zarówno w trakcie trwania dostępu, jaki i po jego zakończeniu.
- 23) Postępowanie sprzeczne z powyższymi zobowiązaniami może zostać uznane za ciężkie naruszenie i może spowodować sankcje przewidziane przepisami prawa.
- 24) W przypadku, gdy wystąpiło choćby podejrzenie naruszenia zasad bezpieczeństwa użytkowanego Systemu należy zgłosić wystąpienie incydentu bezpieczeństwa bezpośrednio do Administratora Danych, czyli Starosty Krasnostawskiego poprzez powiadomienie ASI i Inspektora Ochrony Danych, wysyłając zgłoszenie na adres: informatycy@krasnystaw-powiat.pl, telefonicznie 82 576 52 11 (wew. 166, 167).