

# Informacja dla Użytkowników logowania do zewnętrznych usług sieciowych poprzez system PIONIER Id.

## §1

Państwowa Akademia Nauk Stosowanych w Krośnie, we współpracy z Polską Federacją Zarządzania Tożsamością PIONIER.Id, umożliwia dostęp do zewnętrznych usług sieciowych.

## §2

Mechanizm logowania federacyjnego polega na wykorzystaniu systemów informatycznych Uczelni do potwierdzania uprawnień pracowników i studentów do korzystania z zewnętrznych usług internetowych. Logowanie do tych usług następuje za pośrednictwem mechanizmu logowania federacyjnego PIONIER Id na zasadach opisanych poniżej.

## §3

1. O ile regulamin danej usługi nie stanowi inaczej, użytkownik może korzystać z usługi wyłącznie na swoje potrzeby związane z jego statusem w PANS w Krośnie, tj. pracy lub studiów.
2. Udostępnianie własnego konta użytkownika innym osobom jest zabronione.
3. Użytkownik, przed rozpoczęciem korzystania z mechanizmu logowania federacyjnego PIONIER Id, powinien zapoznać się z niniejszą informacją oraz zasadami dotyczącymi korzystania z poszczególnych usług, z których zamierza korzystać.

## §4

1. W trakcie logowania do usługi zewnętrznej konieczne jest przekazanie pewnej listy danych dotyczących konta użytkownika.
2. Przed przesłaniem danych użytkownik jest pytany o zgodę, która może być wydana jednorazowo lub na stałe. Fakt wydanie zgody stałej jest odnotowywany w bazie Centralnego Punktu Logowania.
3. PANS w Krośnie działa w roli pośrednika przy przekazaniu danych użytkownika do Usługodawcy i nie odpowiada za proces przetwarzania danych osobowych w Usłudze. Ewentualne zapytania o proces przetwarzania, wnioski o bycie zapomnianym itp. Użytkownik powinien kierować bezpośrednio do Usługodawcy.
4. Z uwagi na uniwersalny charakter usługi, PANS w Krośnie nie ma możliwości weryfikacji odbiorcy końcowego usługi, w szczególności odnotowania informacji o jego działalności na terenie EOG dlatego też Użytkownik, przy każdorazowym korzystaniu z Usługi, powinien mieć świadomość, że jego dane, użyte w procesie logowania, mogą zostać przekazane poza obszar EOG.
5. Mechanizm logowania federacyjnego służy do użytku przez pracowników i studentów PANS w Krośnie, na potrzeby związane z pracą lub studiami, o ile regulamin danej Usługi nie stanowi inaczej.

6. Użytkownik powinien zapoznać się z regulaminami usług zewnętrznych, z których chce korzystać za pośrednictwem Usługi.

## **Dane osobowe podlegające przetwarzaniu**

1. W procesie logowania Użytkownika do Usługi przekazywane są dane ze sfery przynależności do środowiska akademickiego. Katalog ten jest zróżnicowany, w zależności od rodzaju usługi ale obejmuje następujące dane: imię, nazwisko, e-mail, specyficzny dla usługi identyfikator, identyfikator w usłudze (np. w POLON), status w instytucji (pracownik, student) i identyfikator ORCID.
2. Uczelnia, przekazując te dane w procesie logowania federacyjnego, nie odpowiada za ich prawidłowe przetwarzanie przez dostawcę usług, który jest samodzielnym administratorem danych osobowych. Realizacja praw określonych w art. 15-22 RODO powinna być realizowana przez dostawcę danej usługi.
3. Użytkownik przed uzyskaniem możliwości zalogowania się do systemu powinien zapoznać się z zamieszczonymi na stronie logowania informacjami na temat prywatności i bezpieczeństwa usługi oraz wyrazić zgodę na przekazanie danych wskazanych przy logowaniu na potrzeby realizacji usługi.
4. Użytkownik musi przestrzegać ew. dodatkowych ograniczeń opisanych na stronach usług, np. zakazu masowego pobierania danych, ich nieautoryzowanej publikacji itp. oraz stosować się do wewnętrznych regulaminów danej usługi, w szczególności zasad dotyczących bezpieczeństwa.

## **Procedura nadawania uprawnień**

### **§1 Procedura nadawania uprawnień**

1. Użytkownicy przed dopuszczeniem do obsługi systemu informatycznego, powinni zapoznać się z funkcjonalnością usług, z których będą korzystali.
2. Pierwsze zarejestrowanie użytkownika w systemie i nadanie odpowiednich uprawnień do systemu musi być poprzedzone uzyskaniem formalnego upoważnienia do pracy w danym systemie.
3. Użytkownikowi zostaje przyznany unikalny login wraz z poufnym hasłem. Loginy i hasła są sposobem zagwarantowania rozliczalności, poufności i integralności danych przetwarzanych w systemach informatycznych. Służą do weryfikowania tożsamości użytkownika, uzyskania dostępu do określonych zasobów, kont uprzywilejowanych lub uruchomienia określonej funkcjonalności.
4. Login wraz z prawidłowym hasłem ma na celu umożliwienie użytkownikowi dostęp do systemu.
5. Po zakończeniu operacji w systemie użytkownik zobowiązany jest wylogować się z systemu.
6. W przypadku awarii, zagubienia hasła lub innych nieprzewidzianych sytuacji zagrażających bezpieczeństwu każdy z użytkowników obowiązany jest niezwłocznie powiadomić administratora systemów informatycznych.

## **§2 Wyrejestrowanie użytkownika z systemu informatycznego**

1. Wyrejestrowania użytkownika z systemu informatycznego dokonuje administrator systemów informatycznych po ustaniu przyczyny dla której został nadany dostęp.
2. Wyrejestrowanie, o którym mowa w ust. 1, może mieć charakter czasowy lub trwały.
3. Wyrejestrowanie następuje poprzez:
  - 1) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
  - 2) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).
4. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy, lub innego stosunku prawnego, w ramach którego użytkownik uzyskał dostęp do systemu, w tym także utrata statusu studenta.
5. W przypadku zastosowania awaryjnego dostępu do systemu na poziomie użytkownika (zapomniane hasło, blokada dostępu), administrator systemu informatycznego nadpisuje hasło użytkownika za pomocą nowego hasła, po dokonaniu uprzedniej weryfikacji tożsamości użytkownika.