KANCELARIA PREZESA RADY MINISTRÓW

DEPARTAMENT SŁUŻBY CYWILNEJ

CENTRUM KOMPETENCJI PAŃSTWA

INSTRUKCJA TECHNICZNA

Wersja 2.0 (dla sprawozdania za 2017 r.)

KPRM DSC 2017

Ważne terminy, definicje i skróty

CKP – system Centrum Kompetencji Państwa

Moduł „sprawozdania” – moduł CKP, który umożliwia złożenie sprawozdania

Moduł „kompetencje” – moduł CKP, który umożliwia przekazanie informacji o wyższych stanowiskach w służbie cywilnej oraz osobach, które je zajmują

Sprawozdanie – sprawozdanie dyrektora generalnego urzędu, składane zgodnie z art. 25 ust. 5 ustawy z dnia 21 listopada 2008 r. o służbie cywilnej

KPRM – Kancelaria Prezesa Rady Ministrów

DSC – Departament Służby Cywilnej (opiekun merytoryczny CKP)

COAR – Centrum Obsługi Administracji Rządowej (administrator CKP)

Użytkownik zewnętrzny – uprawniony pracownik urzędu zobowiązanego do przekazania danych za pośrednictwem CKP (zwany dalej użytkownikiem)

Użytkownik kluczowy – pracownik Departamentu Służby Cywilnej lub Centrum Obsługi Administracji Rządowej, uprawniony do dokonywania czynności techniczno-administracyjnych lub akceptacji sprawozdań i innych danych przekazywanych za pośrednictwem CKP

Formularz – dokument w systemie CKP, który odzwierciedla zawartość tabeli sprawozdawczej.

Kolorem czerwonym zaznaczyliśmy najważniejsze informacje.

Kolorem niebieskim zaznaczyliśmy praktyczne wskazówki, które ułatwią Ci pracę.

Nadanie/odebranie uprawnień do sytemu

Uprawnienia do korzystania z systemu Centrum Kompetencji Państwa (CKP) nadaje lub odbiera administrator systemu na podstawie wniosku o nadanie/odebranie uprawnień. Wniosek możesz pobrać na stronie **www.dsc.kprm.gov.pl** → w zakładce **„Centrum Kompetencji Państwa (CKP)”.**

Uprawnienia do CKP otrzymuje wymieniona we wniosku osoba reprezentująca urząd, a nie urząd.

Nie możesz przekazywać danych logowania do CKP innym pracownikom lub osobom postronnym.

Wniosek o dostęp do systemu składa się – bez względu na liczbę wnioskodawców w urzędzie – dla każdej z osób odrębnie. Jeżeli ze względów organizacyjnych dostęp do sytemu w Twoim urzędzie powinna mieć większa liczba osób, musicie złożyć odrębne wnioski dla każdej z nich.

Dostęp do systemu

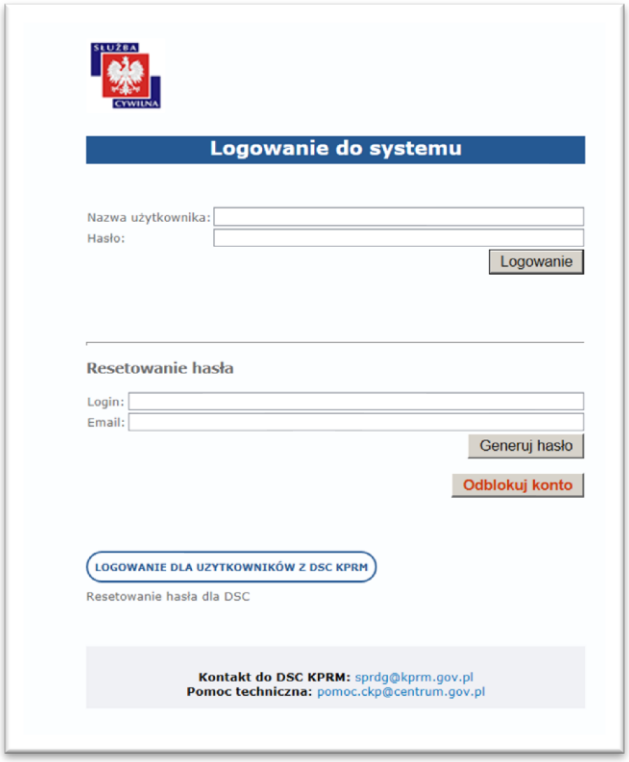
https://ckp.gov.pl lub **www.dsc.kprm.gov.pl** → w zakładce **„Centrum Kompetencji Państwa (CKP)” → „dostęp do systemu”** .

Logowanie

Pierwsze logowanie

Jeśli administrator uprawni cię do korzystania z systemu, otrzymasz email z **nazwą użytkownika**.

Przejdź na stronę startową systemu i wybierz opcję **Resetowanie hasła**.



Wpisz nazwę użytkownika i adres (taki sam jak we wniosku). Po kliknięciu polecenia **Generuj hasło**, system wygeneruje i prześle Ci hasło startowe. Po jego otrzymaniu wróć do okna logowania i zaloguj się.

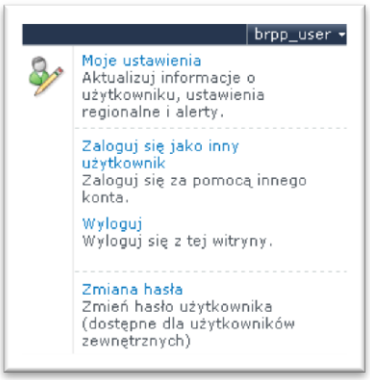
Hasło startowe służy do pierwszego logowania do CKP, dlatego pracę w systemie rozpocznij od zmiany hasła.

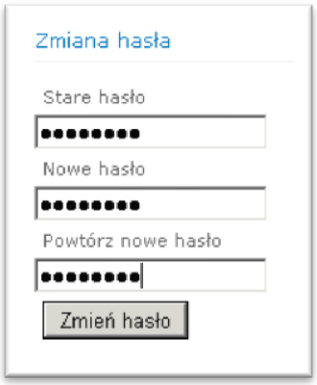
Kolejne logowanie

Wpisz nazwę użytkownika i hasło w oknie logowania oraz zatwierdź klawiszem **Logowanie**.

Zmiana hasła

Opcja zmiany hasła dostępna jest w menu użytkowniku – w prawym górnym rogu ekranu.





Parametry nowego hasła

- ☑ Hasło musi zawierać co najmniej 8 znaków.
- ☑ Hasło musi zawierać co najmniej:
  - jedną wielką literę (A-Z),
  - jedną małą literę (a-z),
  - jedną cyfrę (0-9),
  - dwa znaki specjalne niesąsiadujące ze sobą (np. !, @, $, #, %, &).
- ☑ Nowe hasło musi różnić się od poprzedniego przynajmniej 2 znakami.
- ☑ Historia haseł: 6 ostatnio wprowadzonych haseł.
- ☑ Maksymalny okres ważności hasła: 30 dni.
- ☑ Minimalny okres ważności hasła: 1 dzień.

Poradnik tworzenia i użytkowania haseł

Istnieje wiele metod tworzenia bezpiecznych haseł. Oto kilka z nich[1]:

Metoda pierwszych/ostatnich liter

Wybierz znane sobie zdanie, frazę, np. fragment refrenu piosenki, wiersza. Jako hasło wybierz pierwsze lub ostatnie litery poszczególnych słów w sekwencji uzupełniając cyframi lub znakami specjalnymi.
Przykład: fraza „szła dzieweczka do laseczka, do zielonego" tworzy rdzeń hasła „sddldz", które po uzupełnieniu o pozostałe wymagania złożoności może mieć formę „Sddldz#08%" lub „sddldZ#08*".

Metoda przeplotu

Wybierz słowo i liczbę łatwe do zapamiętania. Znaki te zestaw („przepleć") ze sobą (jedna litera, potem jedna cyfra z liczby itd.) i uzupełnij o znaki specjalne.
Przykład: słowo „**misiu**" oraz liczba „**1964**"mogą utworzyć hasło „(**m**1**S**9**i**6**u**4)".

Metoda łączenia wyrazów

Wybierz kilka krótkich, niepowiązanych ze sobą słów i połącz je, wstawiając miedzy nie znaki specjalne

[1] Na podstawie „Procedury zarządzania mechanizmami kryptograficznymi", która obowiązuje w KPRM.

lub cyfry.
Przykład: słowa „dwa”, „kiwi”, „pole” po połączeniu i uzupełnieniu o dodatkowe znaki mogą utworzyć hasło „Dwa&kiwi*pole11”.

Metoda usuwania samogłosek

Wybierz dwa lub trzy wyrazy, połącz je oraz usuń z nich samogłoski, a w miejsca łączenia wyrazów wstaw znaki specjalne lub cyfry.
Przykład: słowa „dwa”, „kiwi”, „ole” po połączeniu i uzupełnieniu o dodatkowe znaki mogą utworzyć hasło „Dw&kw*l11”.

Metoda podstawiania samogłosek/spółgłosek

Wybierz dwa lub trzy wyrazy, połącz je, a w miejsce samogłosek (lub spółgłosek), wstaw łatwą do zapamiętania liczbę i/lub znaki specjalne.
Przykład: słowa „dwa”, „kiwi”, „ole” oraz liczba 11432 po połączeniu i podstawieniu mogą utworzyć hasło „Dw1k1w43l2”.

Bezpieczne używanie i tworzenie haseł

1. Tworząc hasła, unikaj używania ciągów znaków, które sąsiadują ze sobą na klawiaturze (np. *12345*, albo *qwerty*).
2. Hasła nie mogą być powiązane z osobą użytkownika w jakikolwiek możliwy do odgadnięcia sposób (np. identyfikator użytkownika, imię, nazwisko, data urodzenia, numer telefonu).
3. Hasła nie mogą być złożone z pojedynczych wyrazów, skrótów, nazw własnych czy jakichkolwiek słów występujących w słowniku (zarówno w języku polskim, jak i językach obcych). Hasła nie mogą też być zwykłymi transformacjami tych słów (np. poprzez zapisanie wspak czy poprzez podstawienie ‘@’ zamiast ‘a’, ‘$’ zamiast ‘S’).
4. Podczas wprowadzania hasła do systemu/urządzenia zadbaj o to, aby osoby znajdujące się w pobliżu nie poznały hasła.
5. Bezwzględnie nie przekazuj haseł osobom trzecim (w tym innym użytkownikom, przełożonym i administratorom systemów teleinformatycznych).
6. Nie przechowuj swojego hasła w formie możliwej do bezpośredniego odczytania, tj. jawnie w plikach, skryptach, zapisane na kartkach, w telefonach komórkowych i w miejscach, w których osoby nieupoważnione mogłyby je odczytać.
7. Nie używaj jakichkolwiek zautomatyzowanych procesów rejestrowania haseł (np. przechowywanie
   w makrach, zapamiętywanie haseł w przeglądarce internetowej).
8. Hasła, które wykorzystujesz do celów służbowych, nie mogą być takie same jak te, które stosujesz do celów prywatnych (np. prywatna skrzynka pocztowa, fora internetowe). Jeżeli masz podejrzenie, że Twoje hasło zostało ujawnione bądź wykradzione, jak najszybciej zmień je i zgłoś incydent bezpieczeństwa informacji.
9. W przypadku, gdy wyświetlona data oraz czas logowania nie zgadza się ze stanem ostatniego faktycznego logowania, natychmiast zgłoś ten fakt jako incydent bezpieczeństwa informacji.
10. Za każdym razem, gdy opuszczasz miejsce pracy, zablokuj stację roboczą.

Pamiętaj o ochronie hasła! Nie przekazuj go innym osobom ani nie mów, z jakiej metody korzystałeś przy jego konstrukcji!

Resetowanie hasła

Gdy zapomnisz hasła lub ono wygaśnie (po upływie 30 dni od ostatniej zmiany), możesz wygenerować na stronie logowania nowe hasło, korzystając z funkcji **Resetowanie hasła** (patrz str. 3).

Zablokowanie dostępu

Jeżeli trzykrotnie błędnie wpiszesz dane logowania Twoje konto zostanie zablokowane. Aby je odblokować, skorzystaj z funkcji **Resetowanie hasła** i po wpisaniu danych wybierz polecenie **Odblokuj konto**. Nie jest to funkcja automatyczna, wymaga interwencji administratora sytemu.

Jeżeli nie zalogujesz się do sytemu przez ponad 2 lata, Twoje konto zostanie usunięte. Musisz ponownie złożyć wniosek o nadanie uprawnień.

KONTAKTY

Szanowni Państwo! W pierwszej kolejności, prosimy o kontakt za pośrednictwem poczty elektronicznej.

Dołożymy wszelkich starań, aby wszystkie odpowiedzi na pytania przekazane drogą elektroniczną docierały do Państwa niezwłocznie.

Wsparcie techniczne (informatyczne):

e-mail: pomoc.ckp@centrum.gov.pl

Nadanie/odebranie uprawnień:

Magdalena Berlińska

e-mail: sprdg@kprm.gov.pl

tel.: 22 694-76-63

Jacek Niewiarowski

e-mail: sprdg@kprm.gov.pl

tel.: 22 694-73-21