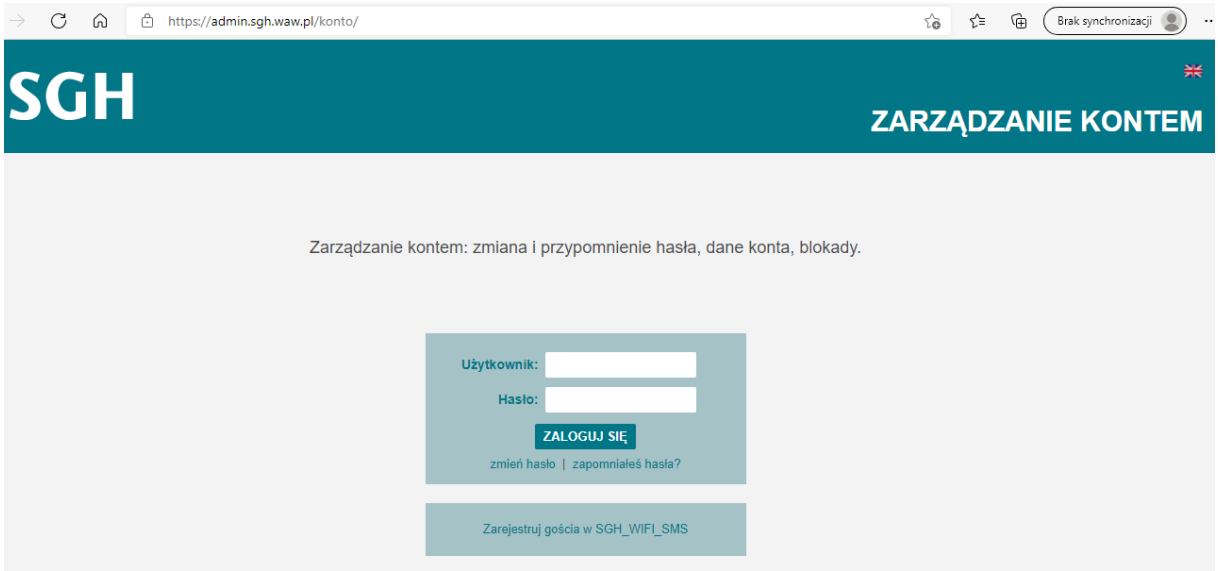
ZARZĄDZANIE KONTEM

(ZMIANA I ODZYSKIWANIE HASŁA, STOPKA MAILOWA, BLOKADY)

Spis treści

1. Logowanie do ZARZĄDZANIA KONTEM

Logowanie odbywa się na stronie https://admin.sgh.waw.pl/konto.



Strona służy do blokowania legitymacji pracowniczej, studenckiej i doktoranckiej, wygenerowania stopki mailowej (dla pracowników).

Wszystkie opcje są dostępne po zalogowaniu się na stronie https://admin.sgh.waw.pl/konto.

Dostęp do strony możliwy jest z komputerów niebędących w sieci SGH poprzez usługę VPN. Instrukcje instalacji klienta VPN dostępne są na stronie http://www.sgh.waw.pl/vpn. Po nawiązaniu połączenia VPN należy wejść na stronę: https://admin.sgh.waw.pl/konto.

2. Zmiana i odzyskiwanie hasła

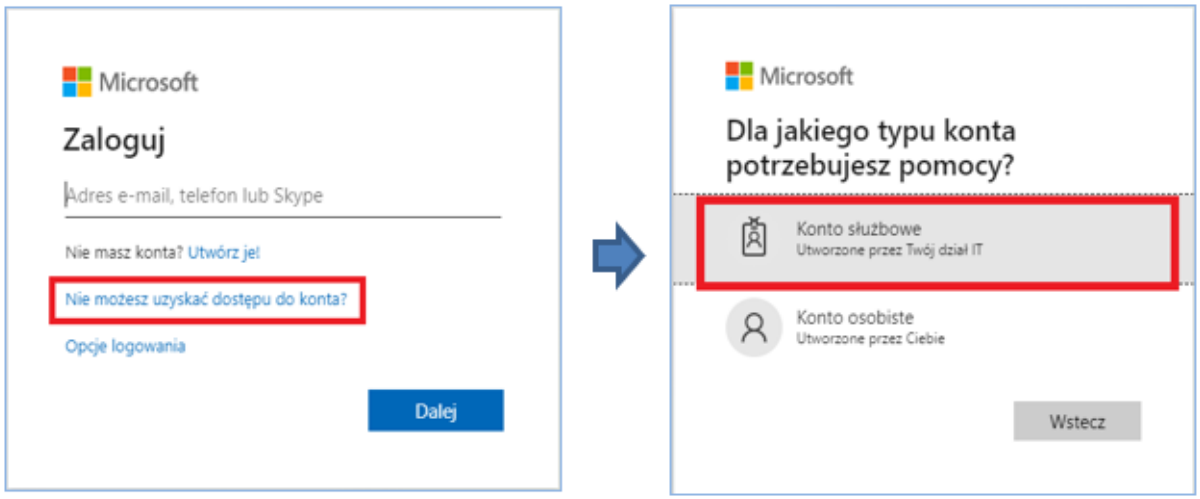
Zmienić lub odzyskać hasło można za pomocą strony https://chmura.sgh.waw.pl. Aby to zrobić, należy mieć skonfigurowane Wieloskładnikowe Uwierzytelnianie (MFA). Instrukcja konfiguracji MFA na koncie SGH znajduje się pod linkiem KONFIGURACJA WIELOSKŁADNIKOWEGO UWIERZYTELNIANIA.

Zmienić lub odzyskać hasło można za pomocą numeru telefonu lub aplikacji mobilnej wykorzystywanej również do wieloskładnikowego uwierzytelnienia.

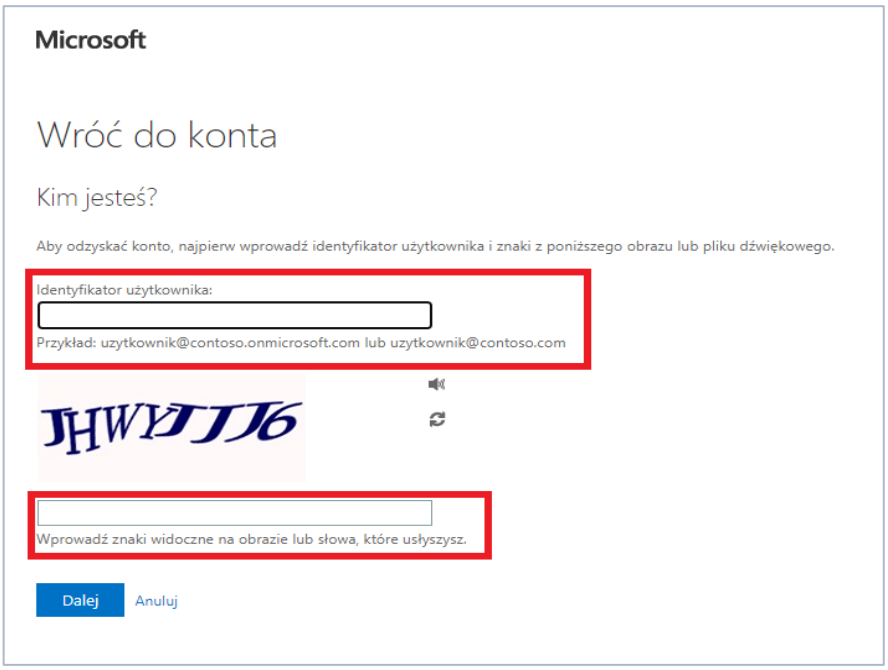
1. Zmiana i odzyskiwanie hasła za pomocą numeru telefonu

Jeśli podczas konfigurowania MFA została wybrana opcja uwierzytelniania poprzez numer telefonu, hasło można zmienić za pomocą wysłanego kodu na podany numer telefonu. Aby to zrobić należy:

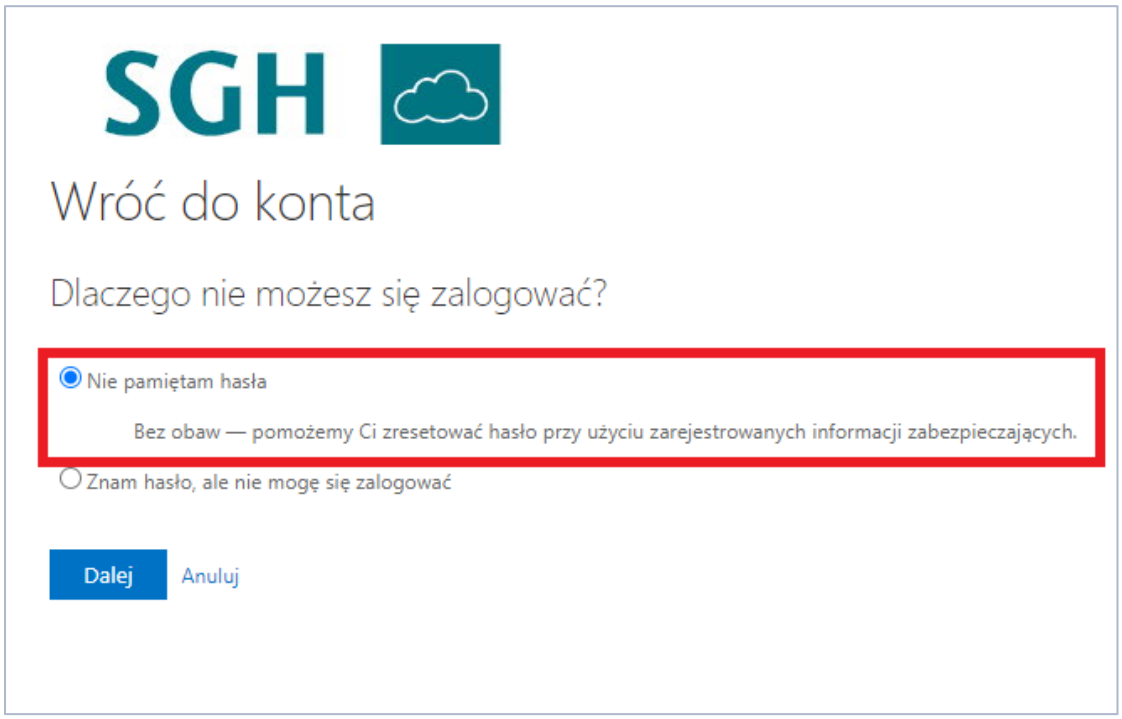
1. Wejść na stronę https://chmura.sgh.waw.pl/
2. Wybrać opcję **NIE MOŻESZ UZYSKAĆ DOSTĘPU DO KONTA?**, następnie **KONTO SŁUŻBOWE.**



3. W polu **IDENTYFIKATOR UŻYTKOWNIKA** wpisać adres mailowy SGH, np. login@sgh.waw.pl lub login@student.sgh.waw.pl ,a w polu poniżej przepisać kod kontrolny z obrazka i kliknąć **DALEJ**.

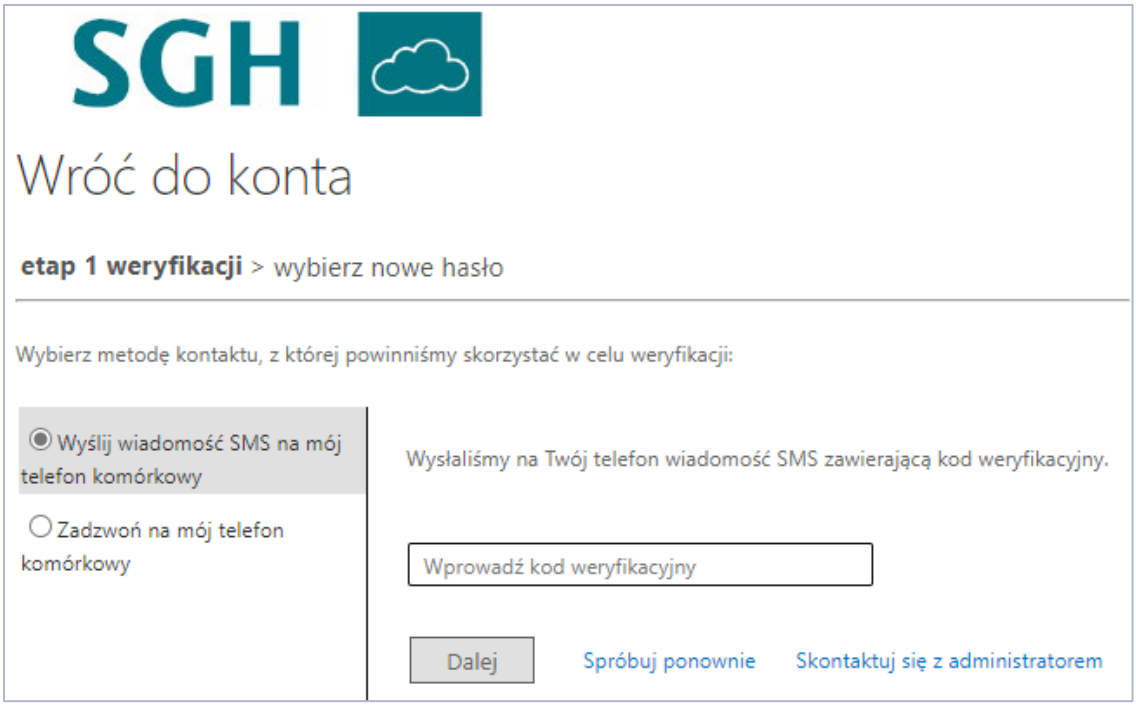


4. W kolejnym kroku wybrać odpowiednią opcję (w tym wypadku: NIE PAMIĘTAM HASŁA) i kliknąć **DALEJ**.

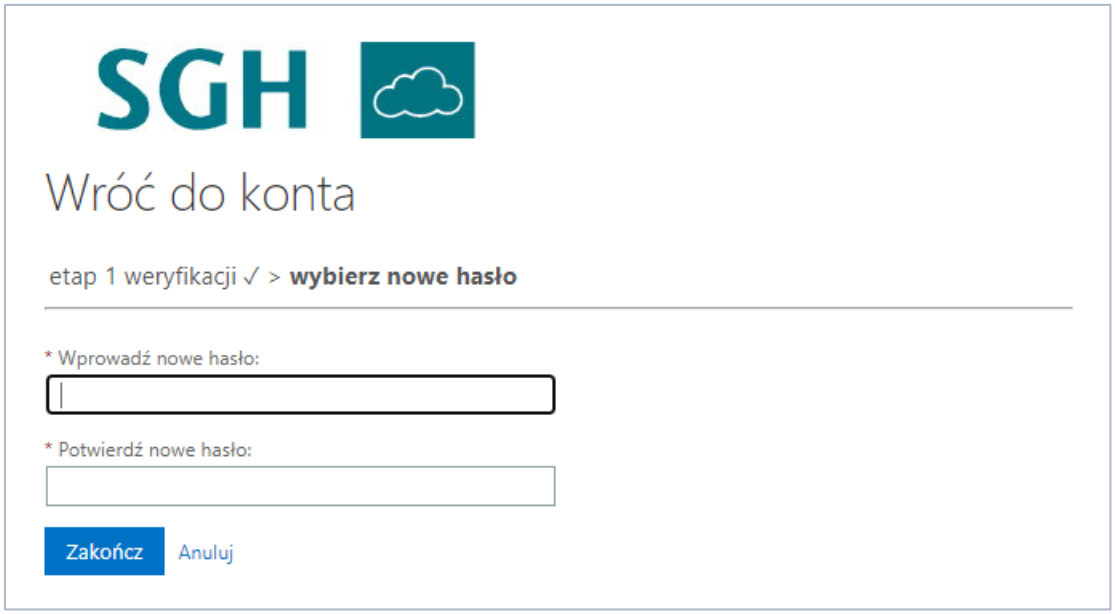


5. Następnie wpisać numer telefonu dodany podczas konfiguracji MFA i kliknąć przycisk TEKST**.** Zostanie wysłana wiadomość z kodem na podany numer.

6. Otrzymany kod wpisać w polu **WPROWADŹ KOD WERYFIKACYJNY** i kliknąć **DALEJ**.



7. Wprowadzić dwa razy nowe hasło do konta i kliknąć **ZAKOŃCZ.**



WAŻNE!!! Dostęp do niektórych serwisów zostanie przywrócony po pewnym czasie – hasło musi się zsynchronizować z każdą aplikacją SGH. Zmiana hasła we wszystkich systemach może potrwać ok. 15 minut.

UWAGA!

- Hasło powinno składać się z co najmniej dziesięciu znaków, nie może zawierać nazwy konta użytkownika, ani części jego imienia i nazwiska dłuższej niż dwa kolejne znaki,
- Hasło musi zawierać znaki z trzech spośród następujących czterech kategorii:
  - wielkie litery alfabetu łacińskiego (od A do Z)
  - małe litery alfabetu łacińskiego (od a do z)
  - cyfry systemu dziesiętnego (od 0 do 9)
  - znaki niealfabetyczne (na przykład !, $, #, %)
- Nie należy używać pojedynczych słów, które można znaleźć w słowniku. Jako hasła należy używać wyrażeń i kilkuwyrazowych fraz, połączonych znakami innymi niż cyfry lub litery,
- siła hasła musi być co najmniej średnia (im większa siła, tym hasło lepiej zabezpiecza dostęp do konta),
- W przypadku trzykrotnie wprowadzonego błędnego hasła dalsze próby zostaną zablokowane na 15 minut.

Po przyjęciu hasła przez system pojawi się następujący komunikat:

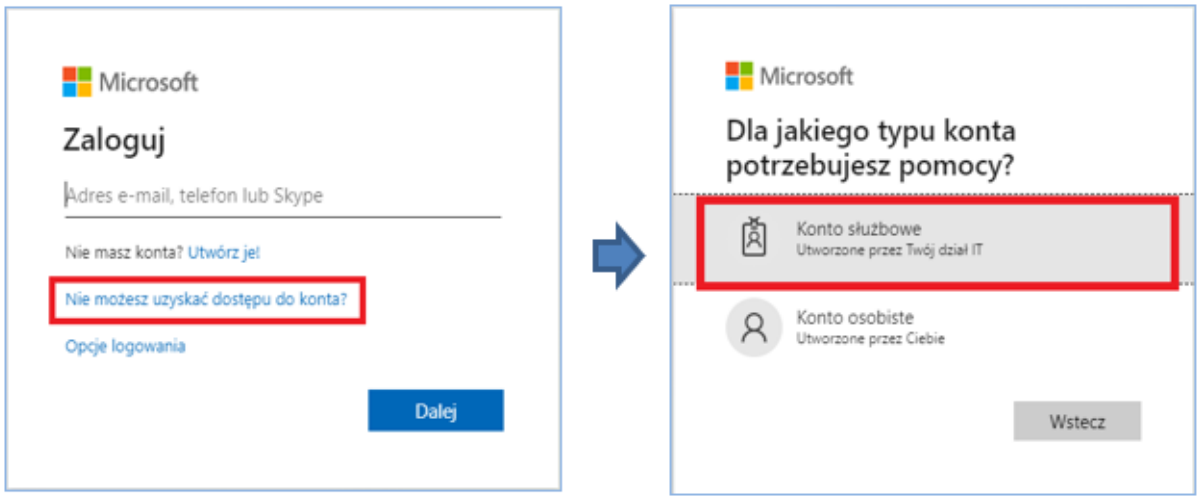
Jeśli system po upływie 15 minut od zmiany hasła nadal nie zezwala na zalogowanie, należy skontaktować się z pracownikami Zespołu Wsparcia Rozwiązań Informatycznych.

UWAGA! Zespół Wsparcia Rozwiązań Informatycznych nie zmienia haseł zdalnie!

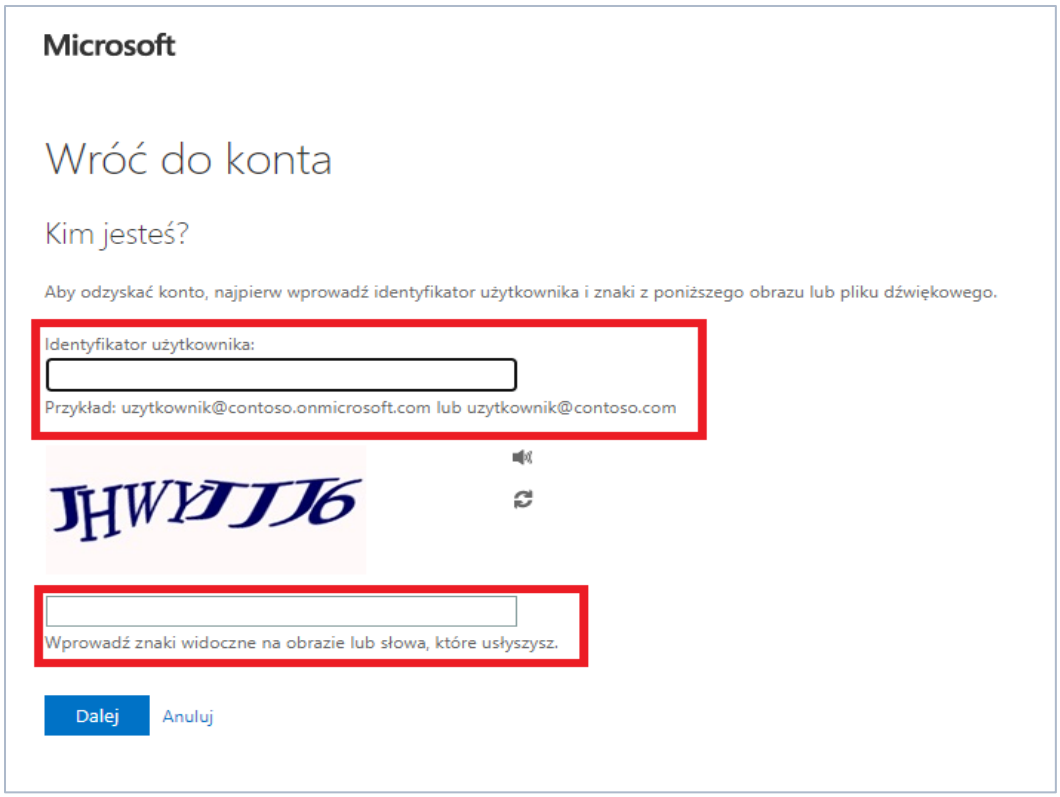
2. Zmiana i odzyskiwanie hasła za pomocą aplikacji Microsoft Authenticator

Jeśli podczas konfigurowania MFA została wybrana opcja uwierzytelniania poprzez aplikację Microsoft Authenticator, hasło można zmienić za pomocą kodu wygenerowanego w aplikacji. Aby to zrobić należy:

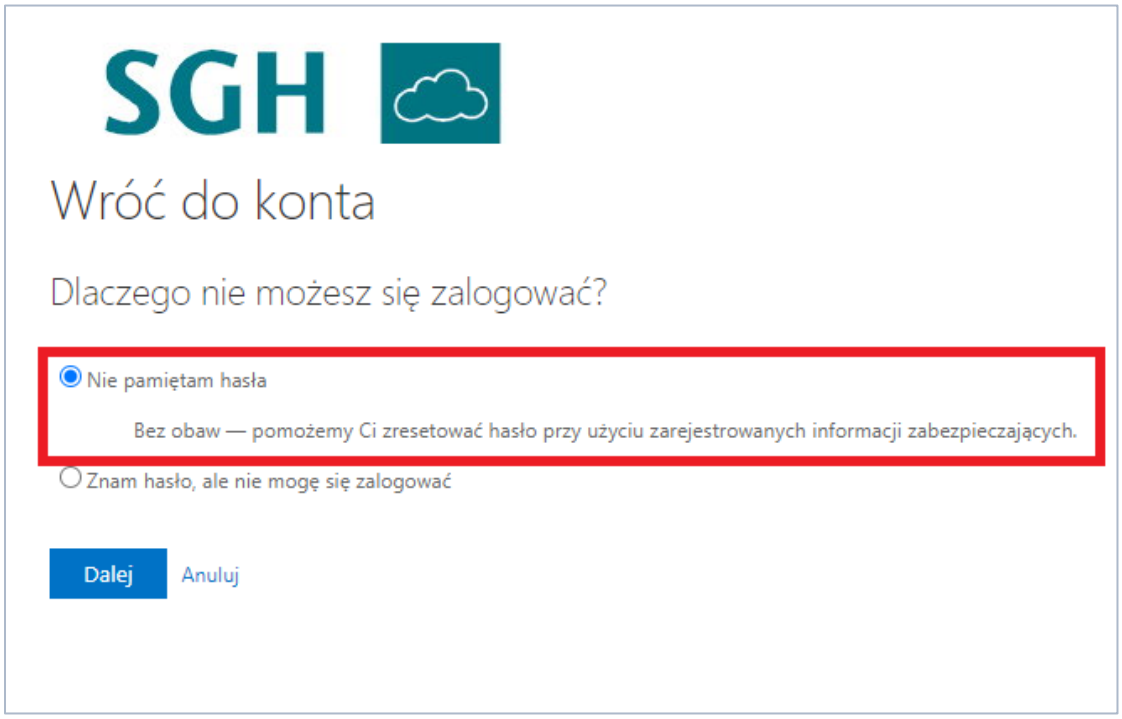
1. Wejść na stronę https://chmura.sgh.waw.pl/
2. Wybrać opcję **NIE MOŻESZ UZYSKAĆ DOSTĘPU DO KONTA?**, następnie **KONTO SŁUŻBOWE.**



3. W polu **IDENTYFIKATOR UŻYTKOWNIKA** wpisać adres mailowy SGH, np. login@sgh.waw.pl lub login@student.sgh.waw.pl, a w polu poniżej przepisać kod kontrolny z obrazka i kliknąć **DALEJ**.

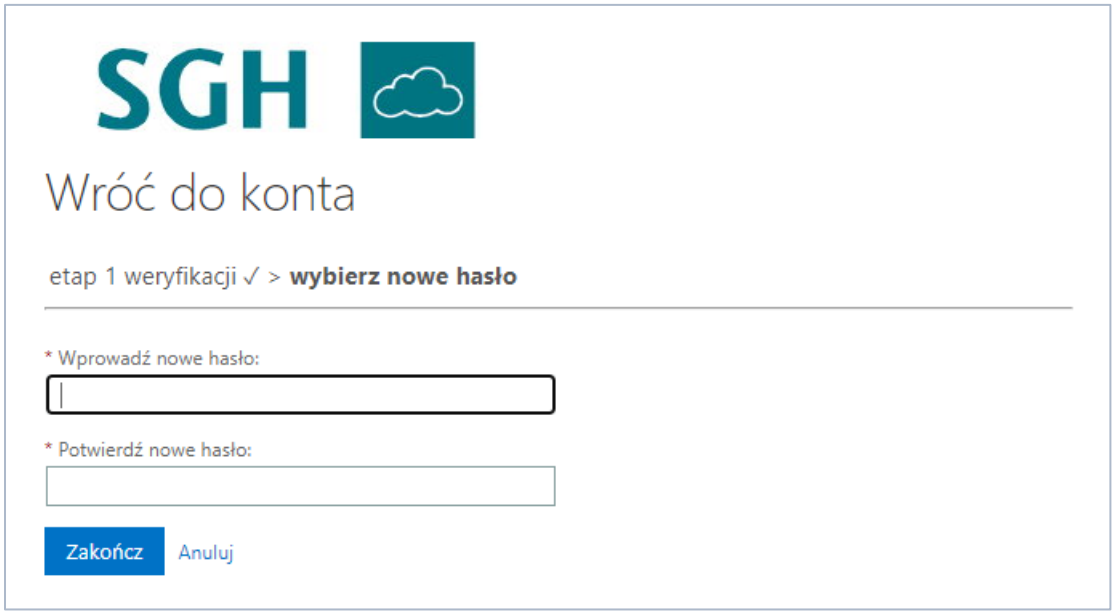


4. W kolejnym kroku wybrać odpowiednią opcję (w tym wypadku: **NIE PAMIĘTAM HASŁA**) i kliknąć **DALEJ**.



5. Wybrać opcję **WPROWADŹ KOD Z APLIKACJI WYSTAWCY UWIERZYTELNIANIA**. Następnie uruchomić aplikację **MICROSOFT AUTHENTICATOR** zainstalowaną na urządzeniu mobilnym, wybrać konto, do którego resetujemy hasło i przepisać kod, który będzie tam wyświetlony do pola **WPROWADŹ KOD WERYFIKACYJNY**. Po wprowadzeniu kodu kliknąć **DALEJ**.

6. Wprowadzić dwa razy nowe hasło do konta i kliknąć **ZAKOŃCZ.**



WAŻNE!!! Dostęp do niektórych serwisów zostanie przywrócony po pewnym czasie – hasło musi się zsynchronizować z każdą aplikacją SGH. Zmiana hasła we wszystkich systemach może potrwać ok. 15 minut.

UWAGA!

- Hasło powinno składać się z co najmniej dziesięciu znaków, nie może zawierać nazwy konta użytkownika, ani części jego imienia i nazwiska dłuższej niż dwa kolejne znaki,
- Hasło musi zawierać znaki z trzech spośród następujących czterech kategorii:
  - wielkie litery alfabetu łacińskiego (od A do Z)
  - małe litery alfabetu łacińskiego (od a do z)
  - cyfry systemu dziesiętnego (od 0 do 9)
  - znaki niealfabetyczne (na przykład !, $, #, %)
- Nie należy używać pojedynczych słów, które można znaleźć w słowniku. Jako hasła należy używać wyrażeń i kilkuwyrazowych fraz, połączonych znakami innymi niż cyfry lub litery,
- siła hasła musi być co najmniej średnia (im większa siła, tym hasło lepiej zabezpiecza dostęp do konta),
- W przypadku trzykrotnie wprowadzonego błędnego hasła dalsze próby zostaną zablokowane na 15 minut.

Po przyjęciu hasła przez system pojawi się następujący komunikat:

Jeśli system po upływie 15 minut od zmiany hasła nadal nie zezwala na zalogowanie, należy skontaktować się z pracownikami Zespołu Wsparcia Rozwiązań Informatycznych.

UWAGA! Zespół Wsparcia Rozwiązań Informatycznych nie zmienia haseł zdalnie!

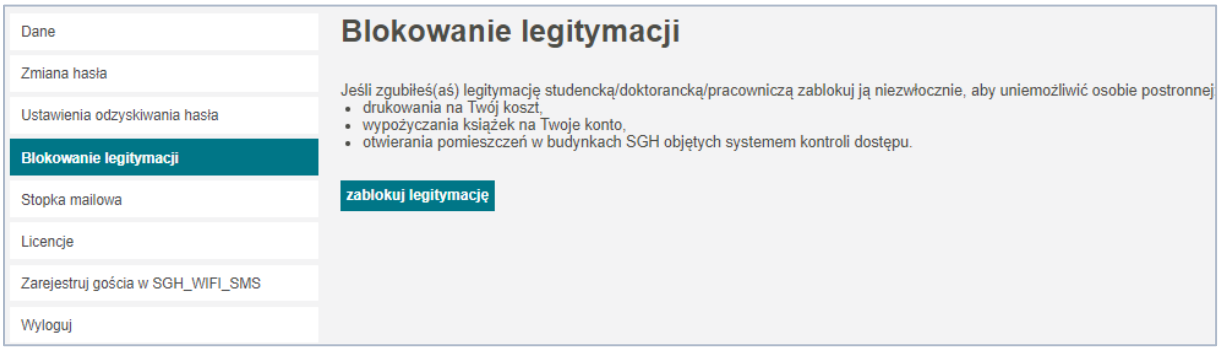
3. Ustawianie opcji odzyskiwania hasła

Każdy użytkownik ma domyślnie ustawioną opcję odzyskiwania hasła za pomocą MFA (wieloskładnikowego uwierzytelniania). Instrukcja jak odzyskać hasło znajduje się w pkt. 1 i 2.

Instrukcja konfiguracji MFA znajduje się pod linkiem KONFIGURACJA WIELOSKŁADNIKOWEGO UWIERZYTELNIANIA.

4. Blokowanie legitymacji

W przypadku utraty legitymacji pracowniczej, studenckiej lub doktoranckiej należy ją zablokować. W tym celu należy wybrać zakładkę **BLOKOWANIE LEGITYMACJI***:*

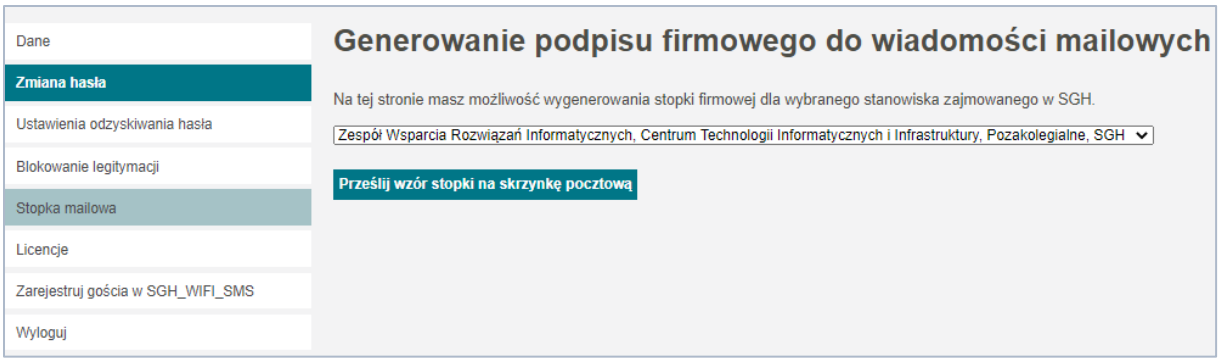


Zablokowanie legitymacji spowoduje brak dostępu do Centralnego Wydruku, Biblioteki SGH oraz otwierania pomieszczeń w budynkach SGH objętych Systemem Kontroli Dostępu.

W przypadku znalezienia zablokowanej legitymacji można ją odblokować w tym serwisie bądź skontaktować się w tej sprawie z Zespołem Wsparcia Rozwiązań Informatycznych. Legitymacja zostanie odblokowana po 3 godzinach od zgłoszenia w przypadku Systemu Centralnego Wydruku i maksymalnie po 24 godzinach w przypadku Systemu Kontroli Dostępu.

5. Stopka mailowa (tylko pracownicy)

W celu wygenerowania podpisu firmowego do wiadomości mailowych należy wybrać zakładkę **STOPKA MAILOWA:**



System wygeneruje stopkę dla wybranego stanowiska i wyśle ją na naszą pocztę w domenie SGH.