



ZASADY BEZPIECZEŃSTWA LSI 2021

KATOWICE, STYCZEŃ 2023

1. Podstawowym zbiorem zasad bezpieczeństwa obowiązującym pracowników UM WSL jest dokumentacja zarządzania systemem bezpieczeństwa informacji zgodnie z wymaganiami normy ISO 27001:2017.
2. Podstawowym zbiorem zasad bezpieczeństwa obowiązującym użytkowników UM WSL, IP FE SL – WUP i IP FE SL – ŚCP jest Polityka bezpieczeństwa odpowiednia dla danej instytucji.
3. **Każdy użytkownik rejestrując konto w LSI 2021 zobowiązany do zapoznania się, zaakceptowania i przestrzegania Regulaminu użytkownika LSI 2021 oraz Zasad bezpieczeństwa LSI 2021. W celu potwierdzenia powyższego, użytkownik składa oświadczenie**.
4. Warunkiem uzyskania dostępu do LSI 2021 jest złożenie oświadczenia, o którym mowa w pkt. 3. Informacja o dacie i godzinie złożenia przez użytkownika oświadczenia jest przechowywana w systemie.
5. W przypadku pracowników UM WSL uprawnienia do LSI 2021 nadawane są zgodnie z obowiązującymi w Urzędzie zasadami kontroli dostępu do systemów informatycznych – aktualną Procedurą Zarządzania Dostępem i Uprawnieniem.
6. W przypadku pracowników IP FE SL - ŚCP uprawnienia do LSI 2021 nadawane są zgodnie z obowiązującą Polityką bezpieczeństwa informacji Śląskiego Centrum Przedsiębiorczości.
7. W przypadku pracowników IP FE SL – WUP uprawnienia do LSI 2021 nadawane są zgodnie z obowiązującą Polityką Bezpieczeństwa Informacji Wojewódzkiego Urzędu Pracy.
8. Użytkownik ma obowiązek zachować w tajemnicy przetwarzane dane, w tym dane osobowe oraz informacje o sposobach ich zabezpieczenia zarówno w okresie zatrudnienia we właściwym podmiocie, jak i po jego ustaniu.
9. Użytkownik powinien niezwłocznie powiadamiać o podatności lub o zdarzeniu bądź serii niepożądanych czy też niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłóceń i zagrażają bezpieczeństwu informacji w systemie. Każdy użytkownik, w przypadku podejrzenia wystąpienia podatności lub zdarzenia bądź serii zdarzeń, o których mowa w pkt 4, powinien niezwłocznie poinformować o tym fakcie Głównego Administratora LSI 2021 poprzez adres mailowy: [lsi2021@slaskie.pl](mailto:lsi2021@slaskie.pl). W przypadku użytkowników wewnętrznych zgłaszanie podatności i zdarzeń, w tym naruszeń ochrony danych osobowych, powinno się odbywać zgodnie z obwiązującymi w Urzędzie zasadami wskazanymi w aktualnej Instrukcji Użytkownika.
10. Po 120 minutach braku aktywności w systemie, następuje automatyczne wylogowanie użytkownika z LSI 2021.
11. W LSI 2021 stosowane jest uwierzytelnienie użytkownika przy pomocy jego loginu oraz hasła, zgodnie z następującymi zasadami:

* minimalna długość hasła wynosi 12 znaków[[1]](#footnote-2),
* hasło musi zawierać małe i duże litery oraz cyfry i znaki specjalne;
* użytkownik ma obowiązek okresowej zmiany hasła, nie rzadziej niż co 90 dni;

1. Nie należy tworzyć haseł używając:

* danych (np. imię, data urodzenia) i innych danych kojarzących się z użytkownikiem;
* pojęć słownikowych w żadnym języku;
* całości lub części loginu;
* słów zapisanych od tyłu, częstych błędów ortograficznych i skrótów;
* przewidywalnych ciągów znaków, ciągów powtórzonych znaków lub ciągów sąsiadujących klawiszy z klawiatury.

Ponadto nie należy:

* używać tego samego hasła do różnych kont;
* tworzyć nowych haseł na bazie wcześniejszych („hasło1”, „hasło2” itp.);
* zapamiętywać loginów i haseł w przeglądarce

1. Hasło należy chronić przed dostępem innych osób.
2. W przypadku nieumyślnego ujawnienia hasła osobie nieuprawnionej lub podejrzenia ujawnienia, **należy bezzwłocznie dokonać zmiany hasła na nowe.**
3. Zakazuje się udostępniania loginu i hasła osobom nieuprawnionym. Główny administrator LSI 2021 nie ponosi odpowiedzialności za czynności wykonane przez osobę nieuprawnioną przy użyciu loginu i hasła użytkownika. Działania takie są traktowane jak działania samego użytkownika.
4. W przypadku braku możliwości dokonania przez użytkownika zmiany hasła (braku działania funkcjonalności „Nie pamiętasz hasła?” lub możliwości zmiany   
   w zakładce „Zmień hasło” dostępnej po zalogowaniu), należy niezwłocznie powiadomić o tym fakcie Głównego administratora LSI 2012 za pomocą adresu e-mail: **lsi2021@slaskie.pl.**
5. Zmiana hasła przy użyciu formularza odzyskiwania hasła - „**Nie pamiętasz hasła?”** odbywa się za pomocą wiadomości e-mail analogicznie jak przy aktywacji konta.
6. W celu zapobieżenia nieautoryzowanemu dostępowi do LSI 2021 użytkownik:

* nie może przechowywać danych służących do logowania do LSI 2021 w miejscach dostępnych dla innych osób;
* nie może ujawniać danych służących do logowania innym osobom;
* zobowiązany jest do sprawdzenia podczas logowania się do LSI 2021, czy certyfikat usługi jest poprawny. W przypadku zgłoszenia przez przeglądarkę problemów   
  z certyfikatem SSL, zabrania się użytkownikowi pracy w systemie.

1. Zabronione jest korzystanie z LSI 2021 z użyciem danych dostępowych innej osoby.

**ZALECENIA DOTYCZĄCE KONFIGURACJI I UŻYTKOWANIA SPRZĘTU KOMPUTEROWEGO UŻYTKOWNIKA**

1. Podczas pracy z LSI 2021 na komputerze użytkownika nie powinien być nie powinny być uruchomione żadne usługi znacznie obciążające stację roboczą lub łącze internetowe.
2. Oprogramowanie komputera powinno być regularnie aktualizowane, w szczególności dotyczy to systemu antywirusowego oraz przeglądarki internetowej.
3. Oprogramowanie antywirusowe powinno być ciągle aktywne, a użytkownik jest zobowiązany do stałego monitorowania komunikatów pochodzących z oprogramowania antywirusowego zainstalowanego na stacji roboczej i reagowania na nie.
4. Sygnatury wirusów powinny być aktualizowane nie rzadziej niż raz na tydzień.
5. Komputer użytkownika powinien być chroniony zaporą sieciową (firewall).
6. Ekrany komputerów powinny zostać ustawione w taki sposób, aby uniemożliwić osobom nieuprawnionym wgląd do informacji aktualnie wyświetlanej na ekranie monitora.
7. Komputery powinny zostać ustawione również w taki sposób, aby osoby nieuprawnione miały utrudniony dostęp do portów zewnętrznych lub przynajmniej dostęp do portów zewnętrznych był pod kontrolą wizualną użytkowników.
8. Użytkownik powinien przestrzegać zasady czystego biurka. W szczególności przed opuszczeniem swego stanowiska pracy użytkownik powinien schować wszelkie dokumenty związane z używanym Systemem oraz informatyczne nośniki danych (płyty CD, DVD, BD, pendrive itp.).
9. Użytkownik podczas logowania się do LSI 2021 jest zobowiązany sprawdzić:

* czy w pasku adresowym przeglądarki adres zaczyna się od **https**,
* czy w obrębie okna przeglądarki znajduje się mała kłódka informująca bezpieczeństwie,
* czy po kliknięciu na kłódkę pojawia się informacja o tym, że certyfikat został wydany dla: \*lsi2021.slaskie.pl i jest on ważny.

1. Użytkownik powinien korzystać z bezpiecznej sieci teleinformatycznej.

# **ROZPOCZYNANIE I KOŃCZENIE PRACY UŻYTKOWNIKÓW W LSI 2021**

1. Rozpoczęcie pracy użytkownika w LSI 2021 następuje po uruchomieniu przeglądarki oraz wprowadzeniu adresu: https://lsi2021.slaskie.pl (wersja produkcyjna) lub https://lsi2021-szkol.slaskie.pl (wersja szkoleniowa) oraz w przypadku rejestracji eksperta <https://lsi2021-ekspert.slaskie.pl>.
2. Połączenie z LSI 2021 jest szyfrowane.
3. Po poprawnym zalogowaniu do LSI 2021 i wybraniu profilu, użytkownik otrzymuje podgląd do aktywnych modułów, do których ma nadany dostęp.
4. W celu chwilowego zawieszenia pracy w systemie użytkownik musi zablokować ekran stacji roboczej (zablokować pulpit lub włączyć wygaszacz ekranu zabezpieczony hasłem). Jeśli komputer użytkownika nie pozwala na zabezpieczenie ekranu hasłem, to należy bezwzględnie wylogować się z LSI 2021.
5. Po zakończeniu pracy należy wylogować się z LSI 2021 poprzez wybranie funkcji „Wyloguj” zlokalizowanej w prawym górnym rogu ekranu. Nie należy kończyć pracy poprzez zamknięcie okna przeglądarki znakiem „x”.

# **POCZTA ELEKTRONICZNA, INTERNET**

1. Użytkownik jest zobowiązany do dbania o bezpieczeństwo kont mailowych wskazanych w systemie w szczególności do:

* używania silnego hasła dostępu,
* nieotwierania załączników do poczty i linków pochodzących z nieznanych źródeł,
* zachowania ostrożności podczas otwierania nieoczekiwanych załączników w korespondencji pochodzącej od znanych nadawców.

1. Użytkownik powinien korzystać z sieci Internet w sposób, który nie zagraża bezpieczeństwu LSI 2021.
2. Użytkownik zobowiązany jest do niezwłocznego uaktualniania swoich danych w LSI 2021, w tym adresu e-mailowego, gdy te ulegną zmianie.

1. Zaleca się tworzenie dłuższych haseł, w celu zminimalizowania ryzyka dostępu do systemu przez osoby nieuprawnione. [↑](#footnote-ref-2)