NewDataLabS
Ułatwiamy pracę z danymi

POLITYKA HASEŁ

Cel dokumentu: Zapewnienie wysokiego poziomu bezpieczeństwa danych dostępowych oraz chronionych informacji firmy NDLS Sp. z o.o. i jej klientów. Określa ona zasady tworzenia, zarządzania i wymiany haseł.

17 MAY 2024

NDLS SP. Z O.O.
Al. Tadeusza Boya-Żeleńskiego 28/4, 51-160 Wrocław

POLITYKA HASEŁ
NDLS Sp. z o.o.

Wstęp

Niniejsza Polityka Haseł została stworzona w celu zapewnienia wysokiego poziomu bezpieczeństwa danych dostępowych oraz informacji zarówno własnych, jak i powierzonych przez klientów zewnętrznych. Obejmuje ona zasady tworzenia, zarządzania i wymiany haseł wewnątrz firmy NDLS Sp. z o.o. oraz z jej klientami.

Zakres obowiązywania

Polityka dotyczy wszystkich pracowników NDLS Sp. z o.o. oraz osób świadczących usługi na rzecz spółki, które mają dostęp do systemów informatycznych firmy i danych klientów.

Wykorzystanie menadżera haseł

1. **Obowiązkowe Używanie Menadżera Haseł**: Wszystkie hasła muszą być przechowywane i zarządzane za pomocą zatwierdzonego przez firmę menadżera haseł. Użycie menadżera haseł minimalizuje ryzyko zapomnienia hasła oraz ułatwia stosowanie skomplikowanych haseł.
2. **Współdzielenie Haseł**: Jeśli współdzielenie haseł jest konieczne w pracy zespołowej, powinno się to odbywać wyłącznie poprzez funkcje współdzielenia dostępne w menadżerze haseł.

Bezpieczna wymiana danych dostępowych z klientami

1. **Zabezpieczone kanały komunikacji**: Wszelka wymiana danych dostępowych z klientami powinna odbywać się przez zabezpieczone kanały komunikacji, takie jak szyfrowane e-maile lub bezpieczne platformy wymiany plików.
2. **Tymczasowy dostęp**: Jeżeli istnieje potrzeba udzielenia klientom dostępu do wewnętrznych zasobów, należy stosować, jeżeli istnieją takie możliwości techniczne, mechanizmy tymczasowego dostępu lub jednorazowe hasła, które są automatycznie unieważniane po określonym czasie.
3. **Kontrola i wycofywanie dostępu:** W przypadku gdy nie istnieją możliwości techniczne wykorzystania haseł tymczasowych lub jednorazowych, dostęp do zasobów formy powinien być cyklicznie rewidowany i odbierany w przypadku gdy nie jest już dłużej wykorzystywany

Dobre praktyki przy tworzeniu haseł

1. **Kompleksowość**: Hasła powinny składać się z:
    1. co najmniej 14 znaków
    2. Kombinacji liter wielkich i małych
    3. cyfr oraz znaków specjalnych, takich jak !, @, #, $, %, ^,*
2. **Unikalność**: Każde hasło musi być unikalne i niepowtarzalne dla różnych kont i usług.
3. **Niejawność:** Hasła nie powinno znajdować się na liście haseł ujawnionych.

4. **Kontrola:** Cykliczne sprawdzanie czy dane dostępowe do witryn nie zostały ujawnione w wycieku danych, z wykorzystaniem serwisu HaveIBeenPwned

Praktyki zakazane

1. **Zakaz używania haseł słownikowych i łatwych do odgadnięcia**: Hasła nie mogą być prostymi słowami lub frazami, które łatwo można znaleźć w słowniku lub są łatwe do przewidzenia, takie jak "password", "123456" czy "datacorp2024".
2. **Zakaz używania tych samych haseł na różnych platformach**: Pracownicy nie mogą używać tego samego hasła do różnych systemów lub usług.
3. **Zakaz używania nazwy użytkownika lub adres e-mail:** Ustalone hasło nie może zawierać całości lub elementów loginu lub adresu email pracownika
4. **Zakaz używania informacji personalnych**: Nie używaj personalnych informacji, takich jak imię, nazwisko, daty urodzenia, numeru telefonu itp. jako części hasła.
5. **Zakaz dzielenia się hasłami poprzez niezabezpieczone kanały**: Nigdy nie wolno przekazywać haseł za pośrednictwem niezabezpieczonych kanałów komunikacyjnych, takich jak niezaszyfrowane e-maile, wiadomości tekstowe czy notatki papierowe.
6. **Zakaz przekazywania loginów i haseł pojedynczym kanałem komunikacji:** Przy przekazywaniu danych dostępowych login i hasło powinny zostać rozdzielone i przekazane osobnymi kanałami komunikacji np. login wiadomością email natomiast hasło za pomocą bezpiecznej wiadomości z poziomu menadżera haseł.

Postępowanie w przypadku naruszenia polityki lub podejrzenia wycieku danych

W przypadku stwierdzenia naruszenia niniejszej polityki haseł lub podejrzenia naruszenia bezpieczeństwa danych, pracownik jest zobowiązany do niezwłocznego powiadomienia odpowiedniego przełożonego. Naruszenie polityki może skutkować podjęciem działań dyscyplinarnych.