ARBONIA

IT SECURITY

Polityka bezpieczeństwa informacji

Wytyczne dotyczące haseł

Wersja:	1.0
Przyjęto dnia:	08.07.2021
Status:	RELEASED
Klasyfikacja:	RESTRICTED
Utworzył:	ICT Security Officer
Przyjęte przez:	Arbonia IT Board
Wytyczna:	IS-ISP-GROUP-001-PASSWORD-POLICY_PL
Rewizja:	n/a

Informacje dotyczące wytycznych

Przeznaczenie	Wytyczne dotyczące haseł opisują i określają zasady tworzenia i używania haseł oraz obchodzenia się z nimi w Grupie Arbonia.
Użytkownik/odbiorca	▪ Wszyscy pracownicy Grupy Arbonia ▪ Zewnętrzni kontrahenci / usługodawcy / klienci i partnerzy mający dostęp do systemów ICT Grupy Arbonia
Elektroniczne przechowywanie dokumentów	https:\\security.arbonia.com

Dowód zmiany

Wersja	Data	Status	Zmiana	przez
0.1	2021-06-14	Draft	Draft of the policy	ICT Security Officer
0.9	2021-07-07	Draft	Draft for adoption	ICT Security Officer
0.9	2021-07-07	Review		Arbonia IT Board
1.0	2021-07-08	Adoption		Arbonia IT Board

Spis treści

Wykaz skrótów

Pojęcie	Opis
ICT	Informations and Communications Technology (technologia informacyjno-komunikacyjna)
OS	Operating System (system operacyjny)
ISMS	System zarządzania bezpieczeństwem informacji

Glosariusz

Pojęcie	Opis
Atak brute force	Atak brute force to próba złamania hasła lub nazwy użytkownika poprzez wypróbowanie wszystkich możliwych opcji.
System zarządzania bezpieczeństwem informacji	System zarządzania bezpieczeństwem informacji to ustanowienie procedur i zasad w organizacji, które służą do stałego definiowania, kontrolowania, monitorowania, utrzymywania i ciągłego doskonalenia bezpieczeństwa informacji.

1 Cel, zakres zastosowania i użytkownik

Wytyczna opisuje wymagania dotyczące haseł i specyfikacje dostępu do systemów ICT Grupy Arbonia. Reguluje zasady bezpiecznego zarządzania, używania i tworzenia haseł.

Wytyczna dotyczy całego zakresu systemu zarządzania bezpieczeństwem informacji (ISMS), tj. wszystkich systemów ICT Grupy Arbonia.

Użytkownikami i odbiorcami niniejszej wytycznej są wszyscy pracownicy Grupy Arbonia oraz zewnętrzni kontrahenci / usługodawcy / klienci i partnerzy, którzy potrzebują dostępu do systemów ICT Grupy Arbonia.

2 Zasady zarządzania

2.1 Ważność haseł

Bezpieczeństwo systemów ICT Arbonia opiera się między innymi na tym, jak ostrożnie obchodzić się z hasłami, a przede wszystkim na tym, jak przestrzegane są podstawowe zasady posługiwania się hasłami.

Jednym z głównych celów atakujących jest kradzież danych dostępowych użytkownika w celu uzyskania dostępu do systemów ICT Grupy Arbonia, a następnie znalezienie i wykorzystanie możliwych luk w zabezpieczeniach. Starają się oni uzyskać uprzywilejowane uprawnienia administratora systemu, dzięki którym, w najgorszym przypadku, mogą niezauważenie wykonywać różne czynności, takie jak kradzież danych, szpiegostwo czy instalacja złośliwego oprogramowania. Z tego powodu słabe hasła i niewłaściwe użycie stanowią znaczne ryzyko. Ryzyko to wzrasta ponownie przy koniecznym korzystaniu z uprawnień uprzywilejowanych, które często są potrzebne do wykonywania pracy.

Dlatego konieczne jest zapobieganie kradzieży danych dostępowych i przestrzeganie poniższych obowiązków.

2.2 Obowiązki użytkowników / właścicieli kont

Wszyscy użytkownicy muszą stosować sprawdzone i bezpieczne procedury podczas wybierania i używania haseł (więcej szczegółów w rozdziale 3):

- Należy zawsze wybierać „silne" hasło. Długość i format hasła należy dobrać tak, aby atak brute force był czasochłonny i nie prowadził do sukcesu
- Haseł nie należy ujawniać innym osobom. Nawet przełożonym, zarządowi czy administratorom systemu
- Hasła nie mogą zostać zanotowane lub nieodpowiednio zapisane (np. w Excelu), chyba że dział IT zatwierdził do tego bezpieczną metodę (np. narzędzie do haseł)
- Hasło należy zmieniać w regularnych odstępach czasu
- Hasła należy zmienić, jeśli istnieją przesłanki, że hasła zostały upublicznione, tj. udostępnione osobom trzecim
- Oznaki niewłaściwego użytkowania należy niezwłocznie zgłaszać do odpowiedzialnego działu IT
- Jeśli użytkownik posiada dedykowane konto użytkownika z uprawnieniami administracyjnymi, nie można używać tego samego hasła, co w przypadku konta standardowego
- Właściciel konta jest odpowiedzialny za przestrzeganie wytycznych dotyczących haseł w każdym przypadku, nawet jeśli nie jest ona technicznie egzekwowana. W żadnym przypadku nie wolno używać standardowych, pustych lub słabych haseł

3 Wytyczne dotyczące haseł

3.1 Definicja

W celu uzyskania odpowiedniego poziomu bezpieczeństwa informacji stosuje się różne wytyczne dotyczące haseł w zależności od wymaganych uprawnień. Rozróżnia się:

- Ogólne zastosowanie typu „Użytkownik", bez uprawnień administracyjnych w systemach ICT
- Specyficzne zastosowanie typu „Administrator", z uprawnieniami administracyjnymi w jednym lub kilku systemach ICT. Konta użytkowników typu „Administrator" dzielą się na:
    - Konta służbowe/systemowe/serwisowe (służące do zautomatyzowanych funkcji, instalacji lub zarządzania komponentami w systemach ICT takich jak np. OS, bazy danych, aplikacje czy konta sieciowe itp.)
    - Konta administratorów (używane dla pojedynczych osób w celu nadania im uprzywilejowanego dostępu do systemów ICT)

3.2 Zarządzanie hasłami

1. Hasło jest przypisane do ID konta (użytkownika lub administratora)
2. Podobnie jak ID konta, hasło jest również osobiste. Hasło jest znane tylko odpowiedzialnej osobie.
3. Nie wolno zapisywać tego hasła w postaci zwykłego tekstu
4. Ważność hasła nigdy nie może przekraczać 360 dni lub 540 dni (patrz rozdział 3.3)
5. Nowe hasło zostanie odrzucone, jeśli znajduje się wśród ostatnich 5 używanych haseł
6. Liczba nieudanych prób wprowadzenia hasła jest ograniczona do 6. Po szóstej próbie konto zostanie zablokowane, dopóki administrator nie odblokuje go ponownie.
7. Licznik nieudanych prób logowania nie może zostać zresetowany w czasie krótszym niż 60 minut
8. Hasła tymczasowe mogą mieć ważność < 72 h, a użytkownik musi zostać poproszony o zmianę hasła tymczasowego przy pierwszym logowaniu. Ma to zastosowanie, jeśli jest to technicznie wykonalne. Jeśli nie, każdy właściciel konta jest odpowiedzialny za zmianę swoich haseł
9. Automatyczne przydzielanie hasła podczas otwierania konta użytkownika odbywa się zgodnie z tymi samymi wymaganiami

Specjalna regulacja dotycząca kont służbowych/systemowych/serwisowych:

- Wyjątek od reguły nr 2: Hasła powiązane z tego typu kontami mogą być przechowywane w bezpiecznym (zaszyfrowanym) narzędziu do haseł z dostępem chronionym hasłem i udostępniane kilku osobom za pośrednictwem zdefiniowanej roli i grup autoryzacyjnych, jeśli jest to konieczne do wykonywania ich pracy
- Wyjątek od reguły nr 4: Hasła powiązane z tego typu kontami mogą, jeśli to konieczne, mieć aktywowaną opcję z hasłami, które nigdy nie wygasają
- Wyjątek od reguły nr 6: Hasła powiązane z tego typu kontami nie muszą być automatycznie blokowane

Postępowanie z wyjątkami znajduje się w rozdziale 3.5.

3.3 Instrukcje dotyczące haseł

Hasło do konta typu „**Użytkownik**" **bez** uprawnień administracyjnych w systemach ICT musi spełniać następujące wymagania:

- Zawiera co najmniej 12 znaków dla ważności hasła wynoszącej 360 dni lub co najmniej 16 znaków dla ważności hasła wynoszącej 540 dni
- Ma złożoność 4 na 4, co oznacza, że następujące znaki muszą zostać użyte przynajmniej raz:
  - Wielkie litery
  - Małe litery
  - Cyfry 0–9
  - Znaki interpunkcyjne lub znaki specjalne (nie wszystkie systemy ICT akceptują wszystkie znaki)
- Nie może zawierać nazwy konta
- Nie może zawierać cyfr na pierwszej lub ostatniej pozycji
- Nie może zawierać 3 kolejnych identycznych znaków

Dla haseł do kont typu „**Administrator**" **z** uprawnieniami administracyjnymi w systemach ICT zastosowanie mają również poniższe specjalne regulacje:

Specjalna regulacja dotycząca kont służbowych/systemowych/serwisowych:

- Zawiera co najmniej 32 znaki
- Hasło musi być generowane losowo i udokumentowane za pomocą odpowiedniego narzędzia do haseł (patrz wyjątek od reguły nr 2, rozdział 3.2)

Specjalna regulacja dotycząca kont administratorów:

- Zawiera co najmniej 15 znaków

Specjalna regulacja dotycząca systemów zewnętrznych (B2C/B2B i innych) obsługiwanych przez Grupę Arbonia:

Wymagania dotyczące hasła zasadniczo dotyczą również systemów innych firm, ale w razie potrzeby można je dostosować do odpowiedniego biznesowego przypadku użycia. W każdym przypadku szczególne regulacje muszą być przestrzegane zgodnie z rozdziałem 3.5.

Specjalne wytyczne dotyczące kont Windows – Arbonia egzekwowane wewnętrznie i automatycznie:

- Nowo ustanowione hasło nie może znajdować się w bazie danych ze skompromitowanymi hasłami. Kontrola techniczna podczas ustawiania hasła zapobiega temu
- Nowo ustanowione hasło nie może pojawić się w słowniku zdefiniowanym przez użytkownika. Słownik ten jest prowadzony centralnie i zawiera między innymi nazwę firmy. Niedozwolone słowa są wyświetlane bezpośrednio w przypadku użycia
- Hasło należy zmienić, jeśli znajdzie się w bazie danych ze skompromitowanymi hasłami

3.4 Strategia dotycząca haseł

Historia haseł	5
Maksymalna ważność hasła	360 dni (12–15 znaków) lub 540 dni (≥ 16 znaków)
Minimalna ważność hasła	0
Złożoność	4/4 (wielkie / małe litery / cyfry 0–9 / znaki interpunkcyjne lub znaki specjalne)
Minimalna długość hasła o Użytkownik o Konta służbowe/systemowe/serwisowe o Konta administratorów	 12 znaków 32 znaki (wygenerowane losowo) 15 znaków
Szyfrowanie zwrotne (domena Windows)	dezaktywowane
Liczba nieudanych prób logowania nim dojdzie do zablokowania konta	6
Czas trwania blokady konta	Dopóki administrator nie odblokuje
Czas do zresetowania licznika nieudanych prób logowania	≥ 60 minut
Informacje specjalne (domena Windows)	Hasło nie może zawierać cyfr na pierwszej lub ostatniej pozycji Hasło nie może zawierać 3 kolejnych identycznych znaków

3.5 Wyjątki / informacje specjalne

Wszystkie komputerowe procedury uwierzytelniania powinny w miarę możliwości wdrażać wymagania niniejszych wytycznych i sprawdzać zgodność. Jeśli nie ma technicznych uwarunkowań do wdrożenia, muszą one zostać zapewnione przez odpowiedniego posiadacza konta w procesie manualnym i należy użyć silnego hasła w zakresie możliwości systemu.

Lokalny specjalista ds. bezpieczeństwa IT może przyznać odstępstwa od tej wytycznej, jeżeli przestrzegane są zasady bezpieczeństwa informacji i nie ma zagrożenia dla systemów ICT Grupy Arbonia. Ten decyduje, w razie potrzeby w porozumieniu ze specjalistą ds. bezpieczeństwa ICT, czy zezwolić na wyjątek lub określić dalsze procedury minimalizujące ryzyko. Wszystkie wyjątki muszą być odnotowane na piśmie w rejestrze.

4 Tworzenie silnych haseł

Istnieje kilka technik tworzenia i zapamiętywania silnego hasła:

Przykład 1: Tworzenie silnego hasła na podstawie zdania

Prosimy wybrać zdanie, które łatwo Państwo zapamiętają i przekształcić je w hasło.

Np.: To wcale nie jest takie trudne, aby wybrać jedno silne hasło.

Należy użyć pierwszych liter lub kilku liter poszczególnych słów oraz wzbogacać hasło o cyfry i znaki specjalne.

Np.: Twnjtt,aw1sh.

Przykład 2: Tworzenie silnego hasła zastępując znaki

Należy wybrać słowo, które łatwo Państwo zapamiętają np. „Teleskop" i zdefiniować specjalny ciąg znaków np. „1$1". Teraz należy zastąpić zdefiniowane części / litery słowa specjalnym ciągiem znaków, aby uzyskać silne hasło.

Np.: „T1$1l1$1skop"

Należy mieć na uwadze, że nigdy nie powinno używać się informacji do tworzenia hasła, które są swobodnie dostępne w mediach społecznościowych. Dalsze wskazówki dotyczące bezpieczeństwa haseł można znaleźć w naszych szkoleniach uświadamiających w zakresie bezpieczeństwa IT.

5 Dokumenty referencyjne

- IS-ISS-GROUP-001-INFORMATION-SECURITY-STRATEGY
- IS-GISP-GROUP-001-GENERAL-INFORMATION-SECURITY-POLICY
- IS-SISD-GROUP-001-PSSS-SPECOPS
- Wytyczne dot. korzystania z systemów IT w firmie Arbonia

6 Wejście w życie

Nazwa	Jednostka biznesowa	Funkcja	Data	Podpis
Patrick Langenegger	Corporate IT	CIO Arbonia Group / CIO Division Doors	2021-07-08	n/a
Michael Kreter	Division HVAC / Sanitary	CIO Division HVAC / Sanitary	2021-07-08	n/a
Tobias Shibli	Division Windows	CIO Division Windows	2021-07-08	n/a
Reto Knechtle	Corporate IT	Head of IT Infrastructure	2021-07-08	n/a

7 Odpowiednie załączniki

Nr	Opis	Nazwa pliku
1	IS-ISP-GROUP-001-COM001-EMPLOYEE-INFORMATION	