ARBONIA

IT SECURITY

Politika bezpečnosti informací

Směrnice k heslům

Verze:	1.0
Schválena:	08.07.2021
Stav:	RELEASED
Klasifikace:	RESTRICTED
Zpracoval:	ICT Security Officer
Schválena kým:	Arbonia IT Board
Směrnice:	IS-ISP-GROUP-001-PASSWORD-POLICY_DRAFT_CS
Revize:	n/a

Informace ke směrnici

Účel	Směrnice k heslům popisuje a definuje zásady týkající se vytváření hesel, zacházení s nimi a používání hesel ve skupině Arbonia.
Uživatel / příjemce	▪ Všichni zaměstnanci skupiny Arbonia ▪ Externí dodavatelé / poskytovatelé služeb / zákazníci a partneři, kteří mají přístup k systémům ICT skupiny Arbonia
Elektronická dokumentace	https:\\security.arbonia.com

Doklad o změně

Verze	Datum	Stav	Změna	provedena kým
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

Obsah

Seznam zkratek

Pojem	Popis
ICT	Informations and Communications Technology (informační a komunikační technologie)
OS	Operating System (operační systém)
ISMS	Systém pro řízení bezpečnosti informací

Glosář

Pojem	Popis
Brute Force Attacke	U pojmu Brute Force Attacke neboli útoku hrubou silou se jedná o pokus prolomení hesla nebo uživatelského jména vyzkoušením všech možností.
Systém pro řízení bezpečnosti informací	Systém pro řízení bezpečnosti informací je souhrn metod a pravidel v rámci organizace sloužících k nepřetržitému definování, řízení, ke kontrole, udržování a neustálému zlepšování bezpečnosti informací.

1 Účel, rozsah použití a uživatelé

Směrnice popisuje požadavky a ustanovení vztahující se k heslům pro přístup k systémům ICT skupiny Arbonia. Stanoví pravidla pro bezpečné řízení, používání a vytváření hesel.

Směrnice platí pro celý rozsah použití systému pro řízení bezpečnosti informací (ISMS), to znamená pro všechny systémy ICT skupiny Arbonia.

Uživateli a příjemci této směrnice jsou všichni zaměstnanci skupiny Arbonia, jakož i externí dodavatelé / poskytovatelé služeb / zákazníci / partneři atd., kteří potřebují přístup k systémům ICT skupiny Arbonia.

2 Zásady governance

2.1 Důležitost hesel

Bezpečnost systémů ICT společnosti Arbonia závisí mimo jiné na tom, jak pečlivě je s hesly zacházeno, a především na tom, jak jsou dodržovány základní principy používání hesel.

Hlavním cílem útočníků je krádež přístupových údajů uživatele za účelem získání přístupu k systémům ICT skupiny Arbonia, nalezení jejich možných slabých míst a následného využití těchto systémů. Útočníci se pokouší o přivlastnění privilegovaných oprávnění systémového administrátora, s nimiž mohou v nejhorším případě nepozorovaně vykonávat různé činnosti, jako je např. krádež dat, špionáž nebo instalace škodlivého softwaru. Z tohoto důvodu představují slabá hesla, jakož i neodborné zacházení s hesly, značné riziko. Toto riziko se ještě zvyšuje nezbytným použitím privilegovaných oprávnění, která jsou často používána pro vykonávání pracovní činnosti.

Je tedy nezbytně nutné zamezit krádeži přístupových údajů a dodržovat následující povinnosti.

2.2 Povinnosti uživatelů / vlastníků účtů

Všichni uživatelé musejí při výběru a používání hesel používat osvědčené a bezpečné metody (další podrobné informace naleznete v kapitole 3):

- Zvoleno musí být vždy "silné heslo". Délku a formát hesla je nutno zvolit tak, aby byl útok hrubou silou časově náročný a nevedl k úspěchu
- Hesla nesmějí být zpřístupněna jiným osobám. Ani nadřízeným, obchodnímu vedení nebo systémovým administrátorům
- Hesla nesmějí být zapisována nebo neodborně ukládána (např. v Excelu), s výjimkou toho, že oddělením IT byla k tomuto účelu schválena bezpečná metoda (např. nástroj pro správu hesel)
- Heslo musí být v pravidelných intervalech měněno
- Hesla je nutno změnit v případě podezření, že byla zveřejněna, to znamená zpřístupněna třetím osobám
- Podezření na zneužití hesla je nutno ihned ohlásit odpovědné osobě oddělení IT
- Pokud uživatel vlastní vyhrazený uživatelský účet s administrátorskými privilegii, nesmí použít stejné heslo jako u standardního účtu
- Vlastník účtu je v každém případě odpovědný za dodržování směrnice k heslům, i když to od něj není technicky vymáháno. V žádném případě nesmějí být používána standardní, prázdná nebo slabá hesla

3 Směrnice k heslům

3.1 Definice

Pro dosažení přiměřené úrovně bezpečnosti informací jsou v závislosti na potřebných privilegiích používány různé směrnice k heslům. Rozlišuje se mezi:

- obecným použitím typu "uživatel" bez administrátorských privilegií v systémech ICT
- specifickým použitím typu "administrátor" s administrátorskými privilegii v systému nebo více systémech ICT. U uživatelských účtů "administrátor" se rozlišují:
    - služební / systémové / servisní účty (používány pro automatizované funkce, instalaci nebo správu komponent v systémech ICT, jako např. OS, databáze, aplikace nebo účty sítě atd.)
    - administrátorské účty (používané pro jednotlivé osoby k tomu, aby jim byla umožněna privilegovaná oprávnění v systémech ICT)

3.2 Řízení hesel

1. Heslo je přiřazeno jednoznačnému ID účtu (uživatel nebo administrátor)
2. Heslo je stejně jako ID účtu osobní. Heslo je známé jen odpovědné osobě.
3. Heslo nesmí být uloženo v nešifrovaném textu
4. Doba platnosti hesla nesmí činit déle než 360 dní, příp. 540 dní (viz kapitola 3.3)
5. Nové heslo je zamítnuto v případě, že se vyskytuje mezi posledními 5 použitými hesly
6. Počet chybných pokusů o zadání hesla je omezen na 6. Po šestém pokusu je účet zablokován až do okamžiku, kdy bude administrátorem opět odblokován.
7. Čítač chybných pokusů o přihlášení nesmí být vynulován v době kratší než 60 minut
8. Dočasná hesla smějí mít platnost < 72 h a uživatel musí být při prvním přihlášení vyzván k tomu, aby dočasné heslo změnil. To platí v případě, že je to technicky realizovatelné. Pokud tomu tak není, odpovídá každý vlastník účtu za tuto změnu hesla osobně
9. Automatické zadání hesla při otevření uživatelského účtu probíhá podle stejných ustanovení

Zvláštní ustanovení pro služební / systémové / servisní účty:

- Výjimka k pravidlu č. 2: hesla spojená s tímto typem účtů mohou být uchovávána v bezpečném (zašifrovaném) nástroji pro správu hesel s přístupem chráněným heslem a sdílena více osobami přes skupiny osob s definovanými úlohami a oprávněními, pokud je to nezbytné pro provádění jejich činnosti
- Výjimka k pravidlu č. 4: hesla spojená s tímto typem účtů smějí mít v případě nutnosti aktivovánu volbu s hesly, která nikdy nevyprší
- Výjimka k pravidlu č. 6: hesla spojená s tímto typem účtů nemusejí být automaticky ukládána

Zacházení s výjimkami je popsáno v kapitole 3.5.

3.3 Ustanovení pro zadávání hesla

Heslo pro účet typu **"uživatel" bez** administrátorských privilegií v systémech ICT musí splňovat následující požadavky:

- Obsahuje nejméně 12 znaků pro dobu platnosti hesla 360 dní, příp. nejméně 16 znaků pro dobu platnosti hesla 540 dní
- Má komplexnost 4 ze 4, to znamená, že nejméně jednou musejí být použity následující znaky:
    - velká písmena
    - malá písmena
    - číslice 0–9
    - interpunkční znaménka nebo zvláštní znaky (ne všechny systémy ICT akceptují všechny znaky)
- Nesmí obsahovat název účtu
- Nesmí obsahovat číslice na prvním a posledním místě
- Nesmí obsahovat 3 po sobě jdoucí identické znaky

Pro hesla pro účet typu **"administrátor" s** administrátorskými privilegii v systémech ICT dodatečně platí následující zvláštní ustanovení:

Zvláštní ustanovení pro služební / systémové / servisní účty:

- Obsahuje nejméně 32 znaků
- Heslo musí být náhodně generováno a zdokumentováno pomocí vhodného nástroje pro správu hesel (viz výjimka k pravidlu č. 2, kapitola 3.2)

Zvláštní ustanovení pro administrátorské účty:

- Obsahuje nejméně 15 znaků

Zvláštní ustanovení pro systémy třetích stran (B2C / B2B a další) provozované skupinou Arbonia:

Ustanovení pro zadávání hesla zásadně platí také pro systémy třetích stran v oblasti obchodu, mohou však být v případě potřeby přizpůsobena příslušnému případu použití. V každém případě musejí být zvláštní ustanovení posuzována podle kapitoly 3.5.

Zvláštní ustanovení pro účty Windows – prosazována v Arbonia interně a automaticky:

- Nově stanovené heslo se nesmí vyskytovat v databázi s kompromitovanými hesly. Tomu zamezí technické ověření při stanovení hesla
- Nově stanovené heslo se nesmí vyskytovat ve slovníku definovaném uživatelem. Tento slovník je centrálně udržován a obsahuje mimo jiné např. název firmy. Nepovolená slova jsou v případě shody přímo zobrazena
- Heslo musí být změněno v případě, že se objeví v databázi s kompromitovanými hesly

3.4 Strategie hesel

Historie hesel	5
Maximální doba platnosti hesla	360 (12–15 znaků), příp. 540 dní (≥16 znaků)
Minimální doba platnosti hesla	0
Komplexnost	4/4 (velká písmena / malá písmena / číslice 0–9 / interpunkční znaménka nebo zvláštní znaky)
Minimální délka hesla o Uživatel o Služební / systémové / servisní účty o Administrátorské účty	 12 znaků 32 znaků (náhodně generovaných) 15 znaků
Invertované kódování (doména Windows)	deaktivováno
Počet chybných pokusů o přihlášení až do zablokování účtu	6
Doba trvání zablokování účtu	Až do odblokování administrátorem
Doba, než bude vynulován čítač chybných pokusů o přihlášení	≥ 60 minut
Specifika (doména Windows)	Heslo nesmí na prvním a posledním místě obsahovat číslice Heslo nesmí obsahovat 3 po sobě následující identické znaky

3.5 Výjimky / specifika

Všechny počítačem podporované autentizační metody musejí v co nejvyšší míře realizovat ustanovení této směrnice a kontrolovat jejich dodržování. Pokud chybí technické předpoklady pro implementaci, musejí být vlastníkem účtu zajištěny v manuálním procesu a rovněž musí být v rámci možností systému použito silné heslo.

Lokální specialista pro bezpečnost IT může ve vztahu k této směrnici udělit výjimky za předpokladu, že jsou dodrženy zásady bezpečnosti informací a nehrozí žádné riziko pro systémy ICT skupiny Arbonia. Tento v případě nutnosti po dohodě s bezpečnostními techniky ICT rozhodne o udělení výjimky nebo definuje další opatření pro minimalizaci rizika. Všechny výjimky musejí být písemně zdokumentovány v soupisu.

4 Vytváření silných hesel

Pro vytvoření silného hesla a jeho zapamatování existují různé techniky:

Příklad 1: vytvoření silného hesla na základě věty

Zvolte větu, kterou si můžete dobře zapamatovat, a převeďte ji do hesla.

Příklad: Dosáhnout toho, aby bylo zvoleno silné heslo, není vůbec tak obtížné.

Použijte počáteční písmena nebo více písmen jednotlivých slov a přidejte k heslu číslice a zvláštní znaky.

Příklad: Dt,abz1sh,nvto.

Příklad 2: vytvoření silného hesla nahrazením znaků

Zvolte slovo, které si můžete dobře zapamatovat, např. "Dopoledne" a definujte speciální pořadí znaků, např. "1$1". Nyní nahraďte definované části / písmena slova svou speciální posloupností znaků za účelem získání silného hesla.

Příklad. D1$1p1$1ledne

Vezměte prosím v úvahu, že pro vytvoření svého hesla nesmíte nikdy použít informace, které jsou volně přístupné na sociálních sítích. Další tipy k tématu bezpečnost hesla získáte při účasti na našich školeních IT Security Awareness.

5 Referenční dokumenty

- IS-ISS-GROUP-001-INFORMATION-SECURITY-STRATEGY
- IS-GISP-GROUP-001-GENERAL-INFORMATION-SECURITY-POLICY
- IS-SISD-GROUP-001-PSSS-SPECOPS
- Směrnice k používání systémů IT ve společnosti Arbonia

6 Nabytí platnosti

Jméno	Obchodní jednotka	Funkce	Datum	Podpis
Patrick Langeneg-ger	Corporate IT	CIO Arbonia Group / CIO Division Doors	2021-07-08	n/a
Michael Kreter	Division HVAC / Sani-tary	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 Infrastruc-ture	2021-07-08	n/a

7 Důležité přílohy

Č.	Popis	Název souboru
1	IS-ISP-GROUP-001-COM001-EMPLOYEE-INFORMATION	