ARBONIA
IT SECURITY

Information Security Policy

Wachtwoordbeleid

Versie:	1.0
Goedgekeurd:	08-07-2021
Status:	RELEASED
Classificatie:	RESTRICTED
Opgesteld door:	ICT Security Officer
Goedgekeurd door:	Arbonia IT Board
Richtlijn:	IS-ISP-GROUP-001-PASSWORD-POLICY_NL
Revisie:	n.v.t.

Informatiebeleid

Doel	Het wachtwoordbeleid beschrijft en definieert principes voor het aanmaken van, omgaan met en gebruiken van wachtwoorden in de Arbonia-groep.
Gebruikers/ontvangers	▪ Alle medewerkers van de Arbonia-groep ▪ Externe contractanten/dienstverleners/klanten en partners die toegang hebben tot de ICT-systemen van de Arbonia-groep
Elektronische documentarchivering	https:\\security.arbonia.com

Bewijs van wijziging

Versie	Datum	Status	Wijziging	door
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

Inhoudsopgave

Lijst van afkortingen

Begrip	Beschrijving
ICT	Informations and Communications Technology (Informatie- en communicatietechnologie)
OS	Operating System (besturingssysteem)
ISMS	Information Security Management System (informatiebeveiligingsbeheersysteem)

Verklarende woordenlijst

Begrip	Beschrijving
Brute force-aanval	Een brute force-aanval is een poging om een wachtwoord of gebruikersnaam te kraken door alle mogelijke opties uit te proberen.
Information Security Management System (informatiebeveili-gingsbeheersysteem)	Een informatiebeveiligingmanagementsysteem is de combinatie van procedures en regels binnen een organisatie die dienen om de informatiebeveiliging permanent te definiëren, beheersen, bewaken, onderhouden en continu te verbeteren.

1 Doel, toepassingsgebied en gebruikers

Het beleid beschrijft de wachtwoordvereisten en -specificaties voor toegang tot de ICT-systemen van de Arbonia-groep. Het stelt regels vast voor het veilig beheren, gebruiken en aanmaken van wachtwoorden.

Het beleid geldt voor het gehele toepassingsgebied van het informatiebeveiligingsmanagementsysteem (ISMS), dus voor alle ICT-systemen van de Arbonia-groep.

De gebruikers en ontvangers van dit beleid zijn alle medewerkers van de Arbonia-groep en externe contractanten/dienstverleners/klanten/partners enz. die toegang nodig hebben tot de ICT-systemen van de Arbonia-groep.

2 Governance-principes

2.1 Belang van de wachtwoorden

De beveiliging van de Arbonia ICT-systemen is onder meer gebaseerd op hoe zorgvuldig met wachtwoorden wordt omgegaan en vooral op hoe de basisprincipes van wachtwoordgebruik worden gevolgd.

Een van de belangrijkste doelen van aanvallers is het stelen van toegangsgegevens van een gebruiker om toegang te krijgen tot de ICT-systemen van de Arbonia-groep en vervolgens mogelijke zwakke punten te vinden en te misbruiken. Ze proberen de geprivilegieerde autorisaties van een systeembeheerder te bemachtigen waarmee ze in het ergste geval ongemerkt verschillende activiteiten kunnen uitvoeren, zoals diefstal van gegevens, spionage of het installeren van malware. Daarom vormen zwakke wachtwoorden en het oneigenlijk gebruik ervan een aanzienlijk risico. Dit risico wordt nog vergroot door het noodzakelijke gebruik van geprivilegieerde autorisaties, die vaak nodig zijn voor het uitvoeren van werkzaamheden.

Het is daarom absoluut noodzakelijk om diefstal van toegangsgegevens te voorkomen om de volgende verplichtingen in acht te nemen.

2.2 Plichten van de gebruikers/houders van de account

Alle gebruikers moeten beproefde en veilige procedures toepassen bij het selecteren en gebruiken van wachtwoorden (meer details in hoofdstuk 3):

- Er moet altijd een 'sterk' wachtwoord worden gekozen. De lengte en het formaat van een wachtwoord moeten zo worden gekozen dat een brute force-aanval tijdrovend wordt en niet succesvol is
- Wachtwoorden mogen niet aan andere mensen worden verstrekt. Zelfs niet aan leidinggevenden, management of systeembeheerders
- Wachtwoorden mogen niet worden opgeschreven of verkeerd worden opgeslagen (bijvoorbeeld in Excel), tenzij de IT-afdeling hiervoor een veilige methode heeft goedgekeurd (bijvoorbeeld een wachtwoordtool)
- Het wachtwoord moet regelmatig worden gewijzigd
- Wachtwoorden moeten worden gewijzigd als er aanwijzingen zijn dat de wachtwoorden openbaar zijn gemaakt, d.w.z. beschikbaar zijn gesteld aan derden
- Aanwijzingen van oneigenlijk gebruik moeten onmiddellijk worden gemeld aan de verantwoordelijke IT-afdeling
- Als een gebruiker een speciaal gebruikersaccount met beheerdersrechten heeft, mag niet hetzelfde wachtwoord worden gebruikt als voor het standaardaccount
- Als houder van de account bent u in ieder geval verantwoordelijk voor de naleving van het wachtwoordbeleid, ook als dit technisch niet wordt afgedwongen. Er mogen in geen geval standaard, lege of zwakke wachtwoorden worden gebruikt

3 Wachtwoordbeleid

3.1 Definitie

Om een passend niveau van informatiebeveiliging te bereiken, worden verschillende wachtwoordrichtlijnen toegepast, afhankelijk van de vereiste bevoegdheden. Er wordt onderscheid gemaakt tussen:

- Algemene toepassing van het type '**Gebruiker**' **zonder** beheerdersrechten op ICT-systemen
- Specifieke toepassing van het type '**Beheerder**', **met** beheerdersrechten op één of meerdere ICT-systemen. Gebruikersaccounts van het type 'Beheerder' zijn onderverdeeld in:
    - Dienst-/systeem-/service-accounts (gebruikt voor geautomatiseerde functies, installatie of beheer van componenten in ICT-systemen zoals OS, databases, applicaties of netwerkaccounts, enz.)
    - Beheerdersaccounts (gebruikt om personen bevoorrechte toegang tot ICT-systemen te geven)

3.2 Wachtwoordbeheer

1. Het wachtwoord is toegekend aan een unieke account-ID (gebruiker of beheerder)
2. Net als de account-ID is ook het wachtwoord persoonlijk. Het wachtwoord is alleen bekend bij de verantwoordelijke.
3. Het wachtwoord mag niet in platte tekst worden opgeslagen
4. De geldigheid van het wachtwoord mag nooit meer dan 360 dagen of 540 dagen zijn (zie hoofdstuk 3.3)
5. Een nieuw wachtwoord wordt geweigerd als het hetzelfde als de laatste 5 gebruikte wachtwoorden is
6. Het aantal mislukte pogingen om een wachtwoord in te voeren is beperkt tot 6. Na de zesde poging wordt het account vergrendeld totdat een beheerder het weer ontgrendelt.
7. De teller van mislukte inlogpogingen mag niet binnen 60 minuten worden gereset
8. Tijdelijke wachtwoorden kunnen een geldigheidsduur hebben van <72 uur en de gebruiker moet gevraagd worden om het tijdelijke wachtwoord te wijzigen wanneer hij/zij de eerste keer inloggen. Dit geldt als het technisch haalbaar is. Zo niet, dan is elke houder van een account verantwoordelijk voor het wijzigen van zijn wachtwoord
9. De automatische wachtwoordtoewijzing bij het openen van een gebruikersaccount wordt uitgevoerd volgens dezelfde richtlijnen

Speciale regeling voor dienst-/systeem-/service-accounts:

- Uitzondering op regel nr. 2: Wachtwoorden die aan dit type account zijn gekoppeld, kunnen worden opgeslagen in een veilige (versleutelde) wachtwoordtool met wachtwoordbeveiligde toegang en worden gedeeld met meerdere personen via gedefinieerde rol- en autorisatiegroepen, als dit voor hun werk nodig is
- Uitzondering op regel nr. 4: Wachtwoorden die aan dit type account zijn gekoppeld, kunnen indien nodig de optie hebben met wachtwoorden die nooit verlopen
- Uitzondering op regel 6: Wachtwoorden die aan dit type account zijn gekoppeld, hoeven niet automatisch te worden geblokkeerd

Afhandeling van uitzonderingen vindt u in hoofdstuk 3.5.

3.3 Wachtwoordvereisten

Het wachtwoord voor een account van het type '**Gebruiker**' **zonder** beheerdersrechten op ICT-systemen moet aan de volgende eisen voldoen:

- Bevat minimaal 12 tekens voor een wachtwoordgeldigheid van 360 dagen of minimaal 16 tekens voor een wachtwoordgeldigheid van 540 dagen
- Heeft een complexiteit van 4 op 4, wat betekent dat de volgende tekens minimaal één keer moeten worden gebruikt:
    - Hoofdletters
    - Kleine letters
    - Cijfers 0–9
    - Leestekens of speciale tekens (niet alle ICT-systemen accepteren alle tekens)
- Mag de accountnaam niet bevatten
- Mag geen cijfers op de eerste of laatste positie bevatten
- Mag geen 3 opeenvolgende identieke tekens bevatten

De volgende speciale regels zijn ook van toepassing op wachtwoorden voor een account van het type '**Beheerder**' **met** beheerdersrechten op ICT-systemen:

Speciale regeling voor dienst-/systeem-/service-accounts:

- Bestaat uit minimaal 32 tekens
- Het wachtwoord moet willekeurig worden gegenereerd en gedocumenteerd met een geschikte wachtwoord-tool (zie uitzondering op regel nr. 2, hoofdstuk 3.2)

Bijzondere regeling voor administration-accounts:

- Bestaat uit minimaal 15 tekens

Bijzondere regeling voor systemen van derden (B2C/B2B en andere) die worden beheerd door de Arbonia-groep:

De wachtwoordvereisten zijn over het algemeen ook van toepassing op systemen van derden, maar kunnen indien nodig worden aangepast aan de respectieve business use case, afhankelijk van de situatie. Bijzondere regelingen dienen in ieder geval conform hoofdstuk 3.5 te worden afgehandeld.

Speciale vereisten voor Windows-accounts – intern voor Arbonia en wordt automatisch afgedwongen:

- Het nieuw ingestelde wachtwoord mag niet in een database met gecompromitteerde wachtwoorden staan. Een technische controle bij het instellen van het wachtwoord voorkomt dit
- Het nieuw ingestelde wachtwoord mag niet voorkomen in een door de gebruiker gedefinieerd woordenboek. Dit woordenboek wordt centraal bijgehouden en bevat onder meer de bedrijfsnaam. De niet toegestane woorden worden direct weergegeven als ze voorkomen
- Het wachtwoord moet worden gewijzigd als het wordt gevonden in een database met gecompromitteerde wachtwoorden

3.4 Wachtwoordstrategie

Wachtwoordgeschiedenis	5
Maximale geldigheid van een wachtwoord	360 dagen (12–15 tekens) of 540 dagen (≥16 tekens)
Minimale geldigheid van een wachtwoord	0
Complexiteit	4/4 (hoofdletters/kleine letters/cijfers 0–9/ leestekens of speciale tekens)
Minimale lengte van het wachtwoord o Gebruikers o Dienst-/systeem-/service-accounts o Administration-account	 12 tekens 32 tekens (willekeurig gegenereerd) 15 tekens
Omgekeerde encryptie (Windows-domein)	gedeactiveerd
Aantal mislukte inlogpogingen voor het account wordt vergrendeld	6
Duur van de vergrendeling van de account	Totdat een beheerder ontgrendelt
Duur tot de teller van mislukte inlogpogingen wordt gereset	≥ 60 minuten
Speciaal (Windows-domein)	Het wachtwoord mag geen cijfers op de eerste of laatste positie bevatten Het wachtwoord mag geen 3 opeenvolgende identieke tekens bevatten

3.5 Uitzonderingen/speciaal

Alle computergebaseerde authenticatieprocedures moeten de vereisten van dit beleid zoveel mogelijk implementeren en de naleving ervan controleren. Als er geen technische vereisten voor implementatie zijn, moeten deze door de respectieve houder van de account worden gegarandeerd via een handmatig proces en moet een sterk wachtwoord worden gebruikt binnen de mogelijkheden van het systeem.

De lokale IT Security Officer kan vrijstellingen verlenen voor dit beleid als de principes van de informatiebeveiliging worden nageleefd en er geen risico is voor de ICT-systemen van de Arbonia-groep. Hij beslist, zo nodig in overleg met de ICT Security Officer, om een uitzondering toe te kennen of verdere maatregelen vast te stellen om het risico te minimaliseren. Alle uitzonderingen moeten schriftelijk worden vastgelegd in een register.

4 Sterke wachtwoorden aanmaken

Er zijn verschillende technieken om een sterk wachtwoord aan te maken en te onthouden:

Voorbeeld 1: een sterk wachtwoord aanmaken gebaseerd op een zin

Kies een zin die u gemakkelijk kunt onthouden en zet deze om in een wachtwoord.

Bijv.: Het is helemaal niet moeilijk om een sterk wachtwoord te kiezen.

Gebruik de eerste paar letters of meerdere letters van de afzonderlijke woorden en verrijk het wachtwoord met cijfers en speciale tekens.

Bijv.: Hihnmo1swtk.

Voorbeeld 2: een sterk wachtwoord aanmaken door tekens te vervangen

Kies een woord dat u gemakkelijk kunt onthouden, bijvoorbeeld "Namiddag" en definieer een speciale tekenreeks, bijvoorbeeld "1$1". Vervang nu gedefinieerde delen/letters van het woord door de door u speciale tekenreeks om een sterk wachtwoord te krijgen.

Bijv.: N1$1midd1$1g

Houd er rekening mee dat u nooit informatie gebruikt om uw wachtwoord aan te maken die vrij toegankelijk is op sociale media. Meer tips over wachtwoordbeveiliging vindt u in onze trainingen voor IT Security Awareness.

5 Referentiedocumenten

- IS-ISS-GROUP-001-INFORMATION-SECURITY-STRATEGY
- IS-GISP-GROUP-001-GENERAL-INFORMATION-SECURITY-POLICY
- IS-SISD-GROUP-001-PSSS-SPECOPS
- Beleid voor het gebruik van IT-systemen bij Arbonia

6 Inwerkingtreding

Naam	Bedrijfseenheid	Functie	Datum	Handtekening
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 Relevante bijlagen

Nr.	Beschrijving	Bestandsnaam
1	IS-ISP-GROUP-001-COM001-EMPLOYEE-INFORMATION	