ARBONIA

IT SECURITY

Information Security Policy

Passwortrichtlinie

Version:	1.0
Verabschiedet:	08.07.2021
Status:	RELEASED
Klassifizierung:	RESTRICTED
Erstellt durch:	ICT Sicherheitsbeauftragter
Verabschiedet durch:	Arbonia IT Board
Richtlinie:	IS-ISP-GROUP-001-PASSWORD-POLICY_DE
Revision:	n/a

Richtlinieninformation

Zweck	Die Passwortrichtlinie beschreibt und definiert Grundsätze für die Erstellung, Umgang und Gebrauch von Passwörtern in der Arbonia Gruppe.
Anwender / Empfänger	▪ Alle Mitarbeitenden der Arbonia Gruppe ▪ Externe Auftragnehmer / Dienstleister / Kunden und Partner, welche Zugang zu ICT-Systemen der Arbonia Gruppe haben
Elektronische Dokumentenablage	https:\\security.arbonia.com

Änderungsnachweis

Version	Datum	Status	Änderung	durch
0.1	14.06.2021	Draft	Entwurf der Richtlinie	ICT Sicherheitsbeauftragter
0.9	07.07.2021	Draft	Entwurf zur Verabschiedung	ICT Sicherheitsbeauftragter
0.9	07.07.2021	Review		Arbonia IT Board
1.0	08.07.2021	Adoption		Arbonia IT Board

Inhaltsverzeichnis

Abkürzungsverzeichnis

Begriff	Beschreibung
ICT	Informations and Communications Technology (Informations- und Kommunikationstechnik)
OS	Operating System (Betriebssystem)
ISMS	Informationssicherheits-Managementsystems

Glossar

Begriff	Beschreibung
Brute Fore Attacke	Bei einer Brute Force Attacke handelt es sich um den Versuch, ein Passwort oder einen Benutzernamen durch Ausprobieren aller Möglichkeiten zu knacken.
Informationssicherheits-Management-systems	Ein Informationssicherheits-Managementsystem ist die Aufstellung von Verfahren und Regeln innerhalb einer Organisation, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

1 Zweck, Anwendungsbereich und Anwender

Die Richtlinie beschreibt die Passwortanforderungen und Vorgaben für den Zugang zu den ICT-Systemen der Arbonia Gruppe. Sie legt Regeln für ein sicheres Management, Gebrauch und Erstellung von Passwörtern fest.

Die Richtlinie gilt für den gesamten Anwendungsbereich des Informationssicherheits-Managementsystems (ISMS), d.h. für alle ICT-Systeme der Arbonia Gruppe.

Anwender und Empfänger dieser Richtlinie sind alle Mitarbeitenden der Arbonia Gruppe sowie externe Auftragnehmer / Dienstleister / Kunden / Partner u.w., welche Zugang zu ICT-Systemen der Arbonia Gruppe benötigen.

2 Governance Grundsätze

2.1 Wichtigkeit der Passwörter

Die Sicherheit der Arbonia ICT-Systeme basiert unter anderem darauf, wie sorgfältig mit Passwörtern umgegangen wird, und vor allem, wie die Grundprinzipien der Passwortverwendung befolgt werden.

Ein Hauptziel von Angreifern ist das Stehlen von Zugangsdaten eines Benutzers um sich Zugang zu den ICT-Systemen der Arbonia Gruppe zu verschaffen und dann mögliche Schwachstellen zu finden und auszunutzen. Sie versuchen sich privilegierte Berechtigungen eines Systemadministrators anzueignen, mit denen sie im schlimmsten Fall unbemerkt verschiedene Tätigkeiten wie z.B. Datendiebstahl, Spionage oder Installation von Schadsoftware durchführen können. Aus diesem Grund stellen schwache Passwörter sowie ein unsachgemässer Umgang ein erhebliches Risiko dar. Dieses Risiko wird mit dem notwendigen Einsatz von privilegierten Berechtigungen, welche vielfach für die Ausübung der Arbeitstätigkeit gebraucht werden, nochmals erhöht.

Es ist daher zwingend notwendig, einen Diebstahl von Zugangsdaten zu verhindern und die nachfolgenden Pflichten zu beachten.

2.2 Pflichten der Anwender / Kontoinhaber

Alle Anwender müssen bei der Auswahl und Anwendung der Passwörter bewährte und sichere Verfahren anwenden (weitere Details im Kapitel 3):

- Es muss immer ein "starkes" Passwort gewählt werden. Die Länge und das Format eines Passworts muss so gewählt werden, damit eine Brute Force Attacke zeitintensiv wird und nicht zum Erfolg führt
- Passwörter dürfen gegenüber anderen Personen nicht offengelegt werden. Auch nicht gegenüber Vorgesetzten, Geschäftsführung oder Systemadministratoren
- Passwörter dürfen nicht aufgeschrieben oder unsachgemäss (z.B. in Excel) gespeichert werden, ausser die IT Abteilung hat hierfür eine sichere Methode (z.B. ein Passworttool) zugelassen
- Das Passwort muss in regelmässigen Abständen geändert werden
- Passwörter müssen geändert werden, falls es Anzeichen dafür gibt, dass die Passwörter öffentlich d.h. Drittpersonen zugänglich gemacht wurden
- Anzeichen für missbräuchliche Nutzung müssen sofort der verantwortlichen IT gemeldet werden
- Besitzt ein Anwender/in ein dediziertes Benutzerkonto mit administrativen Privilegien darf nicht das gleiche Passwort verwendet werden wie beim Standardkonto
- Der Kontoinhaber ist in jedem Fall für die Einhaltung der Passwortrichtlinie verantwortlich auch wenn diese technisch nicht erzwungen wird. In keinem Fall dürfen Standard-, leere oder schwache Passwörter verwendet werden

3 Passwortrichtlinie

3.1 Definition

Um ein angemessenes Informationssicherheitsniveau zu erreichen, werden entsprechend den benötigten Privilegien verschiedene Passwortrichtlinien angewendet. Es wird unterschieden zwischen:

- Allgemeine Anwendung vom Typ "**Benutzer**", **ohne** administrativen Privilegien auf ICT-Systemen
- Spezifische Anwendung vom Typ "**Administrator**", **mit** administrativen Privilegien auf einem oder mehreren ICT-Systemen. Benutzerkonten vom Typ "Administrator" werden unterschieden in:
    - Dienst- / System- / Servicekonten (Eingesetzt für automatisierte Funktionen, Installation oder Verwaltung von Komponenten in ICT-Systemen wie z.B. OS, Datenbanken, Applikationen oder Netzwerkkonten u.w.)
    - Administratorenkonten (Eingesetzt für Einzelpersonen um ihnen privilegierte Berechtigungen auf ICT-Systeme zu ermöglichen)

3.2 Passwort Management

1. Das Passwort ist einer eindeutigen Konto ID zugeordnet (Benutzer oder Administrator)
2. Wie die Konto ID ist auch das Passwort persönlich. Das Passwort ist nur der verantwortlichen Person bekannt.
3. Das Passwort darf nicht im Klartext gespeichert werden
4. Die Passwortgültigkeit darf nie mehr als 360 Tage bzw. 540 Tage betragen (siehe Kapitel 3.3)
5. Ein neues Passwort wird abgelehnt werden, wenn es unter den letzten 5 verwendeten Passwörtern vorhanden ist
6. Die Anzahl der fehlgeschlagenen Passworteingabeversuche ist auf 6 begrenzt. Nach dem sechsten Versuch wird das Konto gesperrt werden, bis es ein Administrator wieder entsperrt.
7. Der Zähler der fehlgeschlagenen Anmeldeversuche darf nicht in weniger als 60 Minuten zurückgesetzt werden
8. Temporäre Passwörter dürfen eine Gültigkeit von <72h haben und der Benutzer muss beim ersten Login dazu aufgefordert werden, das temporäre Passwort zu ändern. Dies gilt sofern es technisch umsetzbar ist. Falls nicht, ist jeder Kontoinhaber für diese Passwortänderung selbst verantwortlich
9. Die automatische Passwortvergabe bei Eröffnung eines Benutzerkontos erfolgt gemäss den gleichen Vorgaben

Sonderregelung für Dienst- / System- / Servicekonten:

- Ausnahme zur Regel Nr. 2: Passwörter, welche mit dieser Art von Konten verbunden sind, können in einem sicheren (Verschlüsselten) Passworttool mit passwortgeschützten Zugriff aufbewahrt und über definierte Rollen- und Berechtigungsgruppen mit mehreren Personen geteilt werden, sofern dies zur Ausführung ihrer Tätigkeit notwendig ist
- Ausnahme zur Regel Nr. 4: Passwörter, welche mit dieser Art von Konten verbunden sind, dürfen, wenn nötig die Option mit nie Ablaufenden Passwörtern aktiviert haben
- Ausnahme zur Regel Nr. 6: Passwörter, welche mit dieser Art von Konten verbunden sind, müssen nicht automatisch gesperrt werden

Umgang mit Ausnahmen befinden sich im Kapitel 3.5.

3.3 Passwortvorgaben

Das Passwort für ein Konto vom Typ **"Benutzer" ohne** administrativen Privilegien auf ICT-Systemen muss folgende Anforderungen erfüllen:

- Enthält mindesten 12 Zeichen für eine Passwortgültigkeit von 360 Tagen bzw. mindestens 16 Zeichen für eine Passwortgültigkeit von 540 Tagen
- Hat eine Komplexität 4 von 4, das bedeutet, dass folgende Zeichen mindestens einmal verwendet werden müssen:
    - Grossbuchstaben
    - Kleinbuchstaben
    - Ziffern 0-9
    - Interpunktionszeichen oder Sonderzeichen (nicht alle ICT-Systeme akzeptieren alle Zeichen)
- Darf den Kontonamen nicht enthalten
- Darf keine Ziffern an der ersten und letzten Stelle enthalten
- Darf keine 3 aufeinanderfolgenden identischen Zeichen enthalten

Für Passwörter für ein Konto vom Typ **"Administrator" mit** administrativen Privilegien auf ICT-Systemen gelten zusätzlich folgende Sonderregelungen:

Sonderregelung für Dienst- / System- / Servicekonten:

- Enthält mindesten 32 Zeichen
- Das Passwort muss zufallsbasiert generiert und mittels einem geeigneten Passworttool (siehe Ausnahme zur Regel Nr. 2, Kapitel 3.2) dokumentiert werden

Sonderregelung für Administrationskonten:

- Enthält mindesten 15 Zeichen

Sonderregelung für Drittsysteme (B2C / B2B und weitere) welche von der Arbonia Gruppe betrieben werden:

Die Passwortvorgaben gelten grundsätzlich auch für Drittsysteme, können aber situativ auf den jeweiligen Business Use Case angepasst werden sofern es erforderlich ist. In jedem Fall müssen Sonderregelungen gemäss Kapitel 3.5 behandelt werden.

Spezielle Vorgaben für Windows Konten – Arbonia intern und automatisch durchgesetzt:

- Das neu gesetzte Passwort darf nicht in einer Datenbank mit kompromittierten Passwörtern vorhanden sein. Eine technische Prüfung beim Setzen des Passworts verhindert dies
- Das neu gesetzte Passwort darf nicht in einem benutzerdefinierten Wörterbuch vorkommen. Dieses Wörterbuch wird zentral gepflegt und beinhaltet unter anderem z.B. den Firmennamen. Die nicht erlaubten Wörter werden im Falle eines Treffers direkt angezeigt
- Das Passwort muss geändert werden, wenn es in einer Datenbank mit kompromittierten Passwörtern aufgetaucht ist

3.4 Passwortstrategie

Passworthistorie	5
Maximale Passwortgültigkeit	360 (12-15 Zeichen) bzw. 540 Tage (≥16 Zeichen)
Minimale Passwortgültigkeit	0
Komplexität	4/4 (Gross- / Kleinbuchstaben / Ziffern 0-9 / Interpunktionszeichen oder Sonderzeichen)
Minimale Passwortlänge o Benutzer o Dienst- / System- / Servicekonten o Administrationskonten	 12 Zeichen 32 Zeichen (zufallsbasiert generiert) 15 Zeichen
Umgekehrte Verschlüsselung (Windows Domain)	deaktiviert
Anzahl fehlgeschlagener Anmeldeversuche bis das Konto gesperrt wird	6
Dauer der Kontosperrung	Bis ein Administrator entsperrt
Dauer bis der Zähler fehlgeschlagener Anmeldeversuche zurückgesetzt wird	≥ 60 Minuten
Spezielles (Windows Domain)	Das Passwort darf keine Ziffern an der ersten und letzten Stelle enthalten Das Passwort darf keine 3 aufeinanderfolgenden identischen Zeichen enthalten

3.5 Ausnahmen / Spezielles

Alle computergestützten Authentifizierungsverfahren sollen so weit wie möglich die Vorgaben dieser Richtlinie umsetzen und die Einhaltung überprüfen. Wenn technische Voraussetzungen für die Implementierung fehlen, müssen sie durch einen manuellen Prozess von dem jeweiligen Kontoinhaber sichergestellt werden und ein starkes Passwort im Rahmen der Systemmöglichkeiten verwendet werden.

Der lokale IT-Security Officer kann Ausnahmegenehmigungen von dieser Richtlinie erteilen, wenn die Grundsätze der Informationssicherheit eingehalten werden und kein Risiko für die ICT-Systeme der Arbonia Gruppe besteht. Dieser entscheidet, wenn nötig in Absprache mit dem ICT-Sicherheitsbeauftragten über die Erteilung einer Ausnahme oder definiert weitere Massnahmen um das Risiko zu minimieren. Alle Ausnahmen müssen schriftlich in einem Verzeichnis festgehalten werden.

4 Erstellen von starken Passwörtern

Es gibt verschiedene Techniken um ein starkes Passwort zu erstellen und sich dieses zu merken:

Beispiel 1: Ein starkes Passwort basierend auf einem Satz bilden

Wählen Sie einen Satz, welchen Sie sich gut merken können und transformieren Sie ihn in ein Passwort.

Bsp.: Es ist gar nicht so schwierig, ein starkes Passwort zu wählen.

Verwenden Sie die Anfangsbuchstaben oder mehrere Buchstaben der einzelnen Wörter und reichern Sie das Passwort mit Ziffern und Sonderzeichen an.

Bsp.: Eignss,1sPzw.

Beispiel 2: Ein starkes Passwort durch Ersetzen der Zeichen bilden

Wählen Sie ein Wort, welches Sie sich gut merken können z.B. "Nachmittag" und definieren Sie eine spezielle Zeichenfolge z.B. "1$1". Nun ersetzen Sie definierte Teile / Buchstaben des Wortes mit Ihrer speziellen Zeichenfolge um ein starkes Passwort zu erhalten.

Bsp. N1$1chmitt1$1g

Bitte beachten Sie, dass Sie niemals Informationen für die Erstellung Ihres Passwortes einsetzen sollten, welche in den Sozialen Medien frei zugänglich sind. Weiter Tipps zum Thema Passwortsicherheit, erhalten Sie in unseren IT Security Awareness Schulungen.

5 Referenzdokumente

- IS-ISS-GROUP-001-INFORMATION-SECURITY-STRATEGY
- IS-GISP-GROUP-001-GENERAL-INFORMATION-SECURITY-POLICY
- IS-SISD-GROUP-001-PSSS-SPECOPS
- Richtlinie zur Nutzung der IT-Systeme in der Arbonia

6 Inkrafttreten

Name	Geschäftseinheit	Funktion	Datum	Unterschrift
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 Anhänge

Nr.	Beschreibung	Dateiname
1	IS-ISP-GROUP-001-COM001-EMPLOYEE-IN-FORMATION	