ARBONIA

IT SECURITY

Information Security Policy

Password Policy

Version:	1.0
Adopted:	2021-07-08
Status:	RELEASED
Classification:	RESTRICTED
Created by:	ICT Security Officer
Adopted by:	Arbonia IT Board
Guideline:	IS-ISP-GROUP-001-PASSWORD-POLICY_EN
Revision:	n/a

Policy information

Purpose	The password policy describes and defines principles for the creation, handling, and use of passwords in the Arbonia Group.
User / recipient	▪ All employees of the Arbonia Group ▪ External contractors / service providers / customers and partners who have access to ICT systems of the Arbonia Group
Electronic document storage	https:\\security.arbonia.com

Modification history

Version	Date	Status	Modification	by
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

Table of contents

Abbreviations

Term	Description
ICT	Information and Communications Technology
OS	Operating system
ISMS	Information Security Management System

Glossary

Term	Description
Brute Force Attack	A brute force attack is an attempt to crack a password or user name by trying all possibilities.
Information Security Management System	An information security management system is a list of procedures and rules within an organisation that serve to permanently define, manage, control, maintain, and continuously improve information security.

1 Purpose, scope of application, and users

The policy describes the password requirements and specifications for accessing the ICT systems of the Arbonia Group. It determines rules for secure management, use, and creation of passwords.

The policy applies to the entire scope of application of the Information Security Management System (ISMS), i.e. to all ICT systems of the Arbonia Group.

The users and recipients of this policy are all employees of the Arbonia Group as well as external contractors / service providers / customers / partners etc. who have access to ICT systems of the Arbonia Group.

2 Governance principles

2.1 Importance of passwords

The security of Arbonia ICT systems is based, among other things, on how carefully passwords are handled and above all on how the basic principles of password use are followed.

One of the main objectives of attackers is to steal the access data of a user in order to gain access to the Arbonia Group's ICT systems and then find and exploit possible vulnerabilities. They try to acquire privileged authorisations of a system administrator, which in the worst case allow them to carry out various activities such as data theft, espionage, or installation of malware without being noticed. For this reason, weak passwords as well as improper handling pose a considerable risk. This risk is further increased by the necessary use of privileged authorisations, which are often needed to perform work activities.

It is therefore essential to prevent theft of access data and to observe the following obligations.

2.2 Obligations of users / account holders

All users must follow best and secure practices when selecting and using passwords (see chapter 3 for further details):

- A "strong" password must always be chosen. The length and format of a password must be selected so that a brute force attack is time-consuming and does not lead to success
- Passwords must not be disclosed to other persons. Not even to superiors, management, or system administrators
- Passwords must not be written down or stored improperly (e.g. in Excel) unless the IT department has approved a secure method (e.g. a password tool) for this purpose
- The password must be changed at regular intervals
- Passwords must be changed if there is any indication that the passwords have been made publicly available, i.e. to third parties
- Indications of misuse must be reported to the responsible IT immediately
- If a user has a dedicated user account with administrative privileges, the same password must not be used as for the default account
- The account holder is responsible for complying with the password policy in all cases, even if this is not technically enforced. In no case may standard, empty, or weak passwords be used

3 Password policy

3.1 Definition

In order to achieve an appropriate level of information security, different password policies are applied according to the required privileges. A distinction is made between:

- General use of the "user" type without administrative privileges on ICT systems
- Specific use of the "administrator" type with administrative privileges on one or more ICT systems. User accounts of the "administrator" type are differentiated into:
    - Service / system / maintenance accounts (used for automated functions, installation, or administration of components in ICT systems, such as e.g. OS, databases, applications, or network accounts etc.)
    - Administrator accounts (used for individuals to give them privileged access to ICT systems)

3.2 Password management

1. The password is assigned to a unique account ID (user or administrator)
2. Like the account ID, the password is also personal. The password is only known to the responsible person.
3. The password must not be stored in plain text
4. The password validity must never exceed more than 360 days or 540 days (see chapter 3.3)
5. A new password will be rejected if it is among the last 5 passwords used
6. The number of failed password entry attempts is limited to 6. After the sixth attempt, the account will be blocked until an administrator unblocks it.
7. The counter of the failed login attempts must not be reset in less than 60 minutes
8. Temporary passwords may have a validity of <72 h, and the user must be prompted at the first login to change the temporary password. This applies to the extent that it is technically feasible. If it is not feasible, account holders are responsible for changing the password themselves
9. A password is automatically assigned according to the same requirements when a user account is opened

Special regulation for service / system / maintenance accounts:

- Exception to rule no. 2: Passwords that are associated with this type of account may be kept in a secure (encrypted) password tool with password-protected access and shared with multiple people via defined role and authorisation groups if this is necessary to perform their job
- Exception to rule number 4: Passwords that are associated with this type of account may have the "Never expiring passwords" option activated if necessary
- Exception to rule number 6: Passwords that are associated with this type of account do not have to be automatically blocked

Rules for handling exceptions can be found in chapter 3.5.

3.3 Password specifications

The password for an account of the "User" type without administrative privileges on ICT systems must meet the following requirements:

- Contains at least 12 characters for a password validity of 360 days or at least 16 characters for a password validity of 540 days
- Has a complexity of 4 of 4, in other words, the following characters must be used at least once:
  - Upper case letters
  - Lower case letters
  - Numbers 0–9
  - Punctuation marks or special characters (not all ICT systems accept all characters)
- Must not contain the account name
- Must not contain numbers in the first and last position
- Must not contain 3 consecutive identical characters

For passwords for an account of the "Administrator" type with administrative privileges on ICT systems, the following special rules additionally apply:

Special regulation for service / system / maintenance accounts:

- Contains at least 32 characters
- The password must be randomly generated and documented using a suitable password tool (see exception to rule no. 2, chapter 3.2)

Special regulation for administration accounts:

- Contains at least 15 characters

Special regulation for third-party systems (B2C / B2B and others) that are operated by the Arbonia Group:

The password requirements also basically apply to third-party systems but can be adapted to the respective business use case according to the situation if necessary. In any case, special regulations must be handled according to chapter 3.5.

Special requirements for Windows accounts – Arbonia internal and automatically enforced:

- The newly set password must not be in a database with compromised passwords. A technical check when the password is set prevents this from happening
- The newly set password must not appear in a user-defined dictionary. This dictionary is maintained centrally and contains the company name, among other things. The forbidden words are displayed directly if a hit occurs
- The password must be changed if it appears in a database with compromised passwords

3.4 Password strategy

Password history	5
Maximum password validity	360 (12–15 characters) or 540 days (≥16 characters)
Minimum password validity	0
Complexity	4/4 (upper case / lower case letters / numbers 0–9 / punctuation marks or special characters)
Minimum password length o User o Service / system / maintenance accounts: o Administration accounts:	 12 characters 32 characters (randomly generated) 15 characters
Reverse encryption (Windows domain)	deactivated
Number of failed login attempts until the account is blocked	6
Duration of account blocking	Until an administrator unblocks
Duration until the counter of failed login attempts is reset	≥ 60 minutes
Special information (Windows domain)	The password must not contain numbers in the first and last position The password must not contain 3 consecutive identical characters

3.5 Exceptions / special information

All computerised authentication procedures must implement and verify compliance with the requirements of this policy to the greatest extent possible. If technical requirements for implementation are lacking, they must be secured through a manual process by the respective account holder and a strong password must be used within the framework of the system capabilities.

The local IT security officer can grant exceptions to this policy if the principles of information security are complied with and there is no risk to the ICT systems of the Arbonia Group. This person decides on granting an exception or defines further measures to minimise the risk, if necessary in consultation with the ICT security officer. All exceptions must be recorded in writing in a directory.

4 Creating strong passwords

There are various techniques for creating and remembering a strong password:

Example 1: Creating a strong password based on a sentence

Choose a sentence that you can remember well and transform it into a password.

Example: It is not so difficult to choose a really strong password.

Use the first letters or several letters of the individual words and augment the password with numbers and special characters.

Example: Iinsdtc1rsp.

Example 2: Creating a strong password by replacing characters

Choose a word that you can easily remember, e.g. "Springtime" and define a special string, e.g. "9$9". Now replace defined parts / letters of the word with your special string in order to obtain a strong password.

Example: Spr9$9ngt9$9me

Please note that you should never use information that is freely available on social media to create your password. Further tips on the subject of password security are given in our IT security awareness training courses.

5 Reference documents

- IS-ISS-GROUP-001-INFORMATION-SECURITY-STRATEGY
- IS-GISP-GROUP-001-GENERAL-INFORMATION-SECURITY-POLICY
- IS-SISD-GROUP-001-PSSS-SPECOPS
- Guidelines for the use of Arbonia IT systems

6 Effective date

Name	Business unit	Function	Date	Signature
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 Relevant enclosures

No.	Description	File name
1	IS-ISP-GROUP-001-COM001-EMPLOYEE-INFORMATION	