ARBONIA
IT SECURITY

New password policy of the Arbonia Group

Dear Employees,

A strong password is the first line of defence for our systems and data.

The main goal of attackers is, among other things, to steal the access data of a user account in order to gain initial access to our networks, severs, and IT systems and, in the worst case, to carry out activities such as data theft, espionage, or the installation of malware without being noticed. For this reason, weak or compromised passwords as well as improper handling of them pose a considerable risk. In order to meet our security requirements even better and to protect you better from these threats, a new password policy has been defined for the Arbonia Group.

Change of the password policy

The complete password strategy is clearly presented below. The change mainly concerns the minimum password length, the maximum password validity, and the complexity.

The minimum password length is increased from currently 8 to 12 characters to make it more difficult to crack a password, and the password validity is simultaneously extended to at least 360 days. If you use a longer password (≥ 16 characters), the password validity is extended to 540 days. In all cases, a high complexity (= strong password) must be ensured for the new passwords. This is achieved through a combination of upper case / lower case letters / numbers 0–9 / punctuation marks or special characters.

Furthermore, the use of passwords that have already been compromised and are freely available on the Internet as well as words from a blacklist (e.g. company names) is automatically prevented.

If the password should appear in a data base of compromised passwords during its validity, you will automatically be prompted to change the password.

The new password policy will automatically become active at your next Windows password change or by request from your local IT department. You will receive a reminder each time, 14 days before the password expires. **However, the policy applies to all ICT systems of the Arbonia Group, i.e., to non-Windows systems as well. As an account holder, you are responsible for complying with the password policy in all cases, even if this is not technically enforced.**

Creating a strong password

There are various techniques for creating and remembering a strong password. For example, create a strong password based on a sentence or by substituting defined strings:

- Choose a sentence that you can remember well and transform it into a password. e.g.: *"It is not so difficult to choose a strong password"* Use the first letters or several letters of the individual words and augment the password with numbers and special characters. e.g.: *"Iinsdtc1sp."*
- 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 chosen string in order to obtain a strong password. e.g.: *"Spr9$9ngt9$9me"*

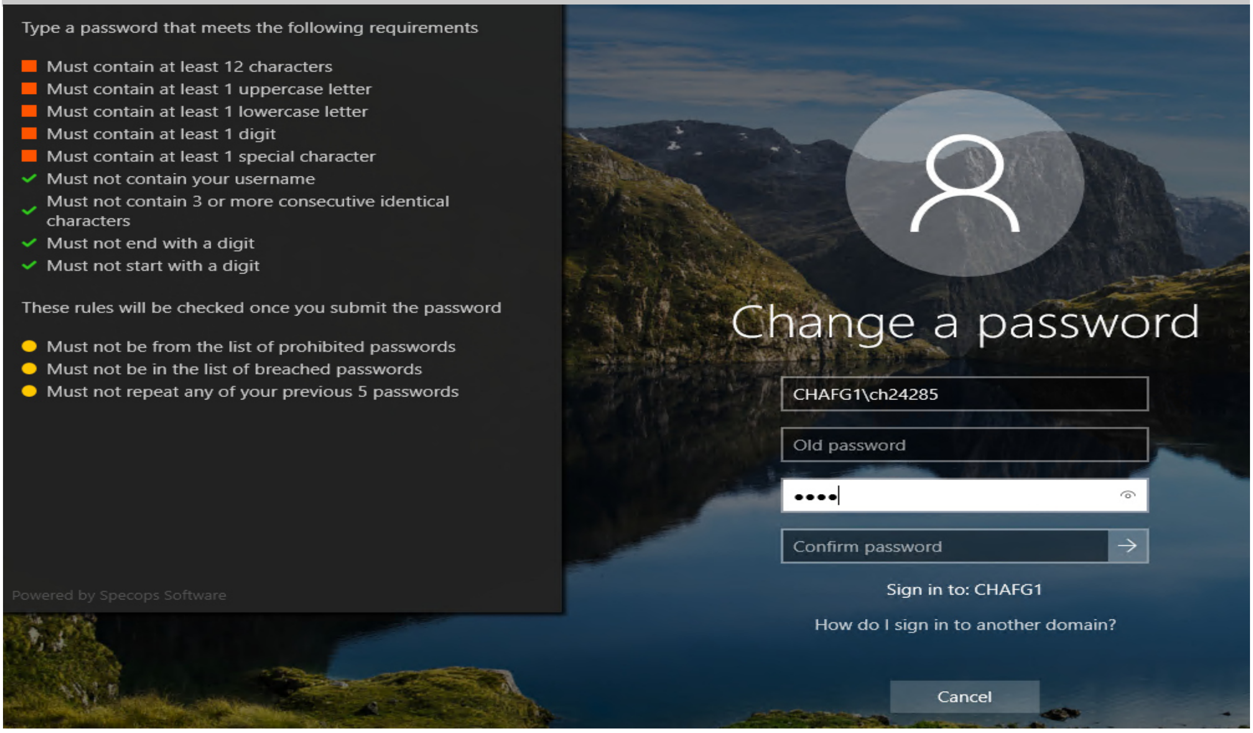
Thank you very much for your attention and best regards
Arbonia Security Team

Password strategy			
Password history (number of last passwords that may not be reused)	5	Number of failed login attempts until the account is blocked	6
Minimum password length	12 characters	Duration of account blocking	Until an administrator unblocks
Maximum password validity	360 days (12–15 characters) or 540 days (≥16 characters)	Duration until the counter of failed login attempts is reset	≥ 60 minutes
Complexity	➢ Upper case letters ➢ Lower case letters ➢ Numbers 0–9 ➢ Punctuation marks or special characters	Special information (Windows passwords – Arbonia internal and automatically enforced)	The password must not contain numbers in the first and last position or 3 consecutive identical characters

Do not use any passwords that are given as examples in this document. These example passwords are now "compromised" and contained in the blacklist.

In addition to this information notice, also observe the valid password policy (IS-ISP-GROUP-001-PASSWORD-POLICY) at https://security.arbonia.com

When you change your Windows password, you will be directly shown the requirements that have to be met.



Type a password that meets the following requirements

- ■ Must contain at least 12 characters
- ■ Must contain at least 1 uppercase letter
- ■ Must contain at least 1 lowercase letter
- ■ Must contain at least 1 digit
- ■ Must contain at least 1 special character
- ✓ Must not contain your username
- ✓ Must not contain 3 or more consecutive identical characters
- ✓ Must not end with a digit
- ✓ Must not start with a digit

These rules will be checked once you submit the password

- ● Must not be from the list of prohibited passwords
- ● Must not be in the list of breached passwords
- ● Must not repeat any of your previous 5 passwords

Powered by Specops Software

Change a password

CHAFG1\ch24285

Old password

••••

Confirm password

Sign in to: CHAFG1

How do I sign in to another domain?