Contents

Scope 2
Policy 2
Password complexity rules 2
Notes 2

Scope

This password policy is valid for all passwords for computer systems at IST Austria, especially for the IST account, the primary account for all IT services at IST Austria.

Policy

- Choose a password that would be very difficult to guess, avoid peoples names, words found in the dictionary or anything similar to your user id.
- Don't write your password down — but you can use a password manager (e.g. KeePass)
- Don't share your password with anyone.
- Do not communicate your password to anyone by any means (telephone, email, website, instant messaging etc.). We will never ask you for your password.
- Never use your IST Austria user id and password combination for any other service / site.
- Never respond to 'phishing' emails – (emails attempting to obtain sensitive information for malicious purposes)
- Always check for "https" or the lock symbol before typing your password in a browser.
- Consider using a "standard" user account on your computer instead of an admin account — only use the admin account when needed.
- Always log off or lock the computer, before leaving a computer unattended
- The password has to be changed at least once a year.
- If you think your account or password may have been compromised, inform the IST IT department and change your password immediately.
  it@ist.ac.at / tel: (+43 2243 9000) 1300

Password complexity rules

- Passwords must not contain the user's user name or screen name (eg. first name and last name)
- Passwords have to be at least eight characters long
- Passwords must contain characters from at least three of the following four character sets:
  - Numbers: 0, 1, 2, …
  - Uppercase letters: A, B, C, …
  - Lowercase letters: a, b, c, …
  - Special characters: ! @ # % ^ & * ( ) – _ + ~ ` , . / < > ? ; : ' " = + [ ] { } |

Notes

1. Always use a strong password — keep in mind that just because your password meets our minimum requirement does not mean it's strong. Use your favorite internet search tool to search the key words "create a strong password that's easy to remember" — there are some good links in there.
2. There is one exception: You may receive one-time passwords by one of the mentioned channels. These are passwords which have to be changed at the first access.