

Password Policy for the IT University of Copenhagen

Your username and password at ITU give you access to ITU's network and ITU's data. It is therefore vital that you help protect the IT-systems and data at ITU, to avoid systems and services being hacked or crashing.

As a user at the IT University, you are personally responsible for choosing and using the password(s) required for access to the IT University's IT systems and data. You are required to change all default passwords given to you as soon as possible.

Change password

To change your password, go to www.itu.dk/password.

Password recommendations for regular user accounts

We recommend that you use the passphrase approach for your password, as they are longer yet easier to remember than a password of random, mixed characters. A passphrase is a memorized phrase consisting of a sequence of mixed words with or without spaces. Your passphrase should be at least 20 characters in length with 5 or more unrelatable words.

When following the outlined password policy there is no requirement for a periodic change of password. It is still recommended that you change a regular password at least every other year unless you have used a password manager tool to create and store a very complex password.

However, you are required to change your password immediately if you or the IT Department at ITU suspect that your password has been compromised or in case of a security breach.

Requirements for a regular password and for a passphrase type password, respectively

<i>Requirement</i>	<i>Regular password</i>	<i>Passphrase type password</i>
Length	<ul style="list-style-type: none"> 16 characters or longer 	<ul style="list-style-type: none"> 20 characters or longer. You must use 5 or more unrelatable words
Complexity	Your password must consist of 3 or more of the following types of characters: <ul style="list-style-type: none"> Uppercase (A..Z) Lowercase (a..z) Digit (0..9) Special characters: +!/(:_ 	
We strongly recommend that you observe the following:	<ul style="list-style-type: none"> Your password must not consist of any 3 consecutive characters from: <ul style="list-style-type: none"> Your user name Your given name(s) Your password must not consist of words, family, pets, names or places that can be associated with you in an internet search Do not reuse your ITU password for personal use. Do not use the same ITU password for accessing internal ITU systems to access external services e.g. Cloud services not delivered by the IT department at ITU. 	
Periodic change	<ul style="list-style-type: none"> It is recommended that you change your password at least every other year 	<ul style="list-style-type: none"> Your passphrase does not require a periodic change.
Password Manager	<ul style="list-style-type: none"> Allowed 	<ul style="list-style-type: none"> Allowed

Password recommendations for privileged user accounts

Administrative systems at ITU have an appointed system owner. The system owner defines the segregation of user roles into related accounts and will specify the rules and potential additional strengthening for privileged user account e.g., administrator accounts and in certain administrative systems, Super User accounts. Additional strengthening can involve the following:

- A privileged user accounts must be a separate account from a regular user account, and
- Your password must be at least 16 characters long and preferably longer.
OR
- If you do not have a separate account, your password should be changed at regular intervals of 6 months unless you have used a password manager tool to create and store a very complex password.

Best practice for use of passwords

In addition to complying with the current password policy, the choice and use of passwords must comply with best practice, as stated below:

Best practice when creating passwords

- Choose a password that:
 - Is as long as possible
 - Is easy to remember.
 - Cannot be guessed or derived from personal information such as name, username, telephone number, birthday or other dates, etc.
 - Is not found in any dictionary or glossary. Example:
 - “international” can be found in a dictionary
 - “butterlamm1cturecant1ck” cannot be found in a dictionary, as they are unrelatable words
 - Does not contain consecutive or identical digits, characters or letters. Example: aaaabbbbcccc
 - Does not begin with a uppercase letter or end with a digit

Best practice to protect passwords or passphrases

- Always keep your password secret.
- Always keep your method or strategy for making a new password secret.
- Never share your password with others including online or over the phone. Not even with the IT Department at ITU.
- Do not write down or store your password in any way, with the exception of a password manager tool.
- Use a Multifactor Authentication App (i.e., Microsoft Authenticator App) or VPN with Multifactor Authentication to log into your ITU account, if either is NOT possible then:
 - Avoid using public computers, such as those at hotels, cafes, or conferences.
 - Avoid using public open wifi, such as at hotels, cafes, or airports.
- Log off and sign out of accounts and websites when you are done using them.

- Change your password immediately if you suspect that it has been compromised.
- Contact it@itu.dk if you know that your password has been compromised.

In case of violation

The IT Department reserve the right to review compliance with the current password policy for all user profiles at regular intervals. If your account does not comply with the current password policy, you will be notified hereof.

The IT Department is allowed to change your ITU password or disable your account e.g., if your user account has been exposed to a phishing attack or has been reported for spamming. In this case contact the IT Department to get a new password.

Further guidelines

You can find further guidelines concerning Information Security including the Information Security Policy on the ITU intranet, by following this link https://intranet.itu.dk/guides/information_security

Version history

Ver.	Date:	Performed by:	Changes:	Approved by:
2.0	15 th of January 2020	Lilian Schelde Baunbæk	Revised password policy, addition on the use of passphrases	ITSU
2.1	18 th of March 2022	Lilian Schelde Baunbæk	Updated with minor changes, correcting spelling mistakes etc.	
2.2	6 th of November 2023	Lilian Schelde Baunbæk	Adding a table to clarify the difference between the use of a regular password and a passphrase. Updating minor recommendations to reflect best practices	SCB Tier 2