JÖNKÖPING UNIVERSITY

Password policy

2019-10-01

Introduction

This document describes Jönköping University's policy for the quality and usage of passwords in accordance with the policy of SWAMID[1].

Purpose

The overall purpose of this policy is to protect the university's password protected information systems from unauthorized access and use.

Responsibilities

As a user of the computer systems at the university, you are responsible for the following:

- that your passwords fulfil the quality and usage described in this policy.
- that you keep your passwords secret.
- that, in accordance with the point above, you never divulge your passwords to anyone who asks for them via email, telephone or in any other way.

Password quality

Your passwords must be strong. Strong passwords can be created by combining single characters making up a short but complex password, or by using a passphrase made from randomly combined words.

Complex password

A complex password consists of at least ten characters that include a random mix of uppercase letters, lowercase letters, numbers, or special characters. Complex passwords provide good security, can be typed quickly on a regular keyboard, but are generally difficult to remember and difficult to type, for example on a mobile phone.

Passphrase

A passphrase is composed of at least six random words that form a longer sentence. It's very important that the words are truly random and not a part of a regular readable sentence. Password phrases usually provide higher security than complex passwords, are easier to remember, and are typically easier to type, for example on a mobile phone.

[1] https://www.sunet.se/swamid - (Swedish Academic Identity Federation)

Whether you choose a complex password or a passphrase, a password must contain at least one capital letter, at least one lower case, and at least one digit or special character.

✓ Contains at least 10 characters and may be comprised with the following characters.

- At least one character: A-Z
- At least one character: a-z
- At least one character of:
    - 0-9
    - the following special characters: ! , @, # , $, % , (,) , * , - , [, \ ,] , ^ , _ , ` , { , | , } , ~ , ’ (single quote), " (double quote), ,(comma), .(full stop)

✗ A password shall NOT be composed as follows:

- same as or similar to the username.
- linked to personally identifiable information such as a name, social security number, telephone number.
- be a common character combination or words found in dictionaries, for example 12345678aB, Summer2019, Secret0000, Password01!
- Not a part of a regular readable sentence, for example MyPetMaxIsOld3

(Because WiFi passwords are not adequately protected when connecting to WiFi networks, it is not allowed to use the same WiFi password as used with your user account. This means that the password for eduroam must be exactly 7 characters according to the same as above which means that they are not the same.)

Password Management

Keep in mind that your password should be secret and unique to our services, do not use your JU password for services outside the university. By using the same password on services outside of the university, you have in effect stated your password to someone else and your password is no longer a secret.

Exceptions to this rule exist for functional accounts that can be held by staff or students, e.g. registrar or chair of student associations.

If your password becomes known by other persons or services, your password is no longer secret, and you must change your password as soon as possible. In the event of information security incidents or if the university becomes aware that your password is no longer secret, IT service can initiate a mandatory password reset according to the **Password Recovery section**.

Password Change

The password is normally valid in perpetuity, this also applies to the eduroam (WiFi) service.

In the university's common login service, the following applies to password change:

- perpetuity valid password for students, employees and other operatives.
- mandatory password change within 1 year for system administrators.

Password change is always done in the self-service portal https://myaccount.ju.se , never elsewhere.

Password recovery / reset

In order to recover a password, the university must have confirmed knowledge of personal contact information such as a private e-mail, SMS or third-party verified postal address, for example via the Statens personadressregister, called SPAR[2] which includes all persons who are registered as a resident in Sweden. Personal contact information is provided when activating a user account or in the user account service portal itself. Recovery can also be done through antagning.se or eduid.se with a confirmed account.

If the above methods are not pertinent, a personal visit to the IT helpdesk with valid identification is required as defined by the Swedish Tax Agency. For foreign residents, there is the option to send photo proof of home address in the form of, for example, an electricity bill and valid identification according to the Swedish Tax Agency's definition to the IT helpdesk.

Password recovery is always done in the recovery portal https://passwordreset.ju.se , never elsewhere.

Password control

The university's common login service contains technical support to ensure good password quality. (Microsoft Active Directory, Azure Password Protection)
During a password change, the password is validated so that:

- passwords are composed according to the password quality section above, that the password is of good quality and that variants of passwords are not included in public password lists.
- new password is not the same as the 8 previous passwords.

[2] https://www.statenspersonadressregister.se

System Requirements

This section contains requirements for systems at JU that use or manage passwords. Individual students or staff do not normally have to take these into account.

Scope

The policy for password usage applies to all IT services and systems (applications) at the university. The scope of the policy covers two areas, password quality and safeguarding of passwords.

Definitions

Password Quality. Good password quality means that a password is both sufficiently long and complicated in such a way that the risk that an attacker can guess the password is minimized. Two variables determine the difficulty when guessing a password: length and complexity. These can be used to calculate the password's entropy. The higher the entropy, the harder it is to guess.

Password protection. Secure password usage means, apart from the fact that every user is responsible for keeping his/her passwords secret, that the login service protects passwords from unauthorized access and use.

Account types. Some account types have exceptions from this policy. Examples of account types where the exception occurs are short-term visitor accounts that may be issued by all staff at the university, or function accounts where people within the same function can share the account. For more information about account types please visit: www.ju.se/helpdesk

Responsibilities

For systems linked to the university's common authentication and login service, there is system support for compliance with the policy. (Microsoft Active Directory, Azure Password Protection)

For systems with their own password management, the system owner is responsible for compliance with this policy.

Protection against network-based brute force attacks (Rate limiting)

To reduce the risk of brute force attacks against passwords, logins must be protected via so-called rate limiting that prevents an attacker from making repeated password guesses during a short time frame.

In the university's central login service this is designed as follows:

- Maximum of 20 incorrect guesses.
- Thereafter automatic lock out of account for 30 minutes.

Strategies

All information systems (applications) must be connected to the university's central login service unless specific reasons apply.

The university's central login service contains support for strong password quality and secure password management.

Every user has a password for login to the IT services of the university. To login to some IT services, for example the Wireless network eduroam, the user must have an additional password. Furthermore, additional system-specific or business-specific passwords may exist.

Safeguarding of passwords

To reduce the risk of unauthorized access to passwords the following policy applies to the storage and transport of passwords:

- Passwords must never be visible in a readable format.
    - Exception for visitor accounts
    - Exceptions can be made in processes where e.g. a one-time code is communicated to an individual user. This should be done to a known e-mail address, SMS or postal address.
- Passwords must never be divulged over email, telephone or any other communicable manner.
    - Exception for visitor accounts
    - Exceptions can be made in processes where e.g. a one-time code is communicated to an individual user. This should be done to a known e-mail address, SMS or postal address.
- Passwords must be transported in encrypted form and should use at least TLS 1.2 with current "best practice" for TLS.
- Passwords stored permanently should preferably be stored as salted hash. If storing passwords in plain text are necessary, the passwords should be stored encrypted, preferably with an encryption key that is not permanently on the system.