Introduction

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

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.

For systems that are connected to the university's centralised login and authentication (Novell eDirectory or Microsoft Active Directory) there is inbuilt support for compliance with this policy.

For systems with own, inbuilt password handling it is the responsibility of the system owner to ensure compliance with this policy.

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 minimised. 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.hj.se/helpdesk

Purpose

The overall purpose of this policy is to protect university's password protected information systems from unauthorized users, as much as possible.

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.

HÖGSKOLAN I JÖNKÖPING

Password policy

2015-03-01

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.

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.

Safeguarding of passwords

To reduce the risk of unauthorised 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)
- Passwords must never be divulged over email, telephone or any other communicable manner.
- Passwords must always be stored and transported in encrypted form where it is technically possible.
- Passwords must be kept secret and not shared with others. (Exception for function accounts)

Password quality

The user should warned not to use the same password in other internal or external IT services.

A password must be composed as follows:

Contains at least 8 characters and may be comprised with the following characters.

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

The password must contain at least one upper case, and at least one lower case letter and at least one number, and may advantageously contain special characters.

(For Wireless network service eduroam exactly 7 characters are needed following the rules above)

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 an ordinary combination of characters or words found in dictionaries, for example, 12345678, Summer2014, Secret10, Password2, car brands etc.

Password control

In the university's central login service there is technical support that maintains good password quality. During a password change, the password is validated so that:

- it is comprised according to the rules for *password quality* above.
- it is not the same as the 8 previous passwords

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 5 minutes.

In the university's self-service for user accounts is designed as follows:

- Maximum of 3 incorrect guesses.
- Thereafter automatic lock out from self-service for 30 minutes.

Password change

To further reduce the risk that an intruder discovers a password that belongs to the university's IT and information systems, every user must change their password within a defined time period.

In the university's central login service the following rules apply for password change:

- Forced password change every 1 year for students, employees and affiliates.
- Forced password change every 2 months for system administrators
- Forced password change every 4 years for eduroam services for all accounts.