Password regulations for Karolinska Institutet

Dnr 1-213/2015

Version 2.0
Applicable from 2015-05-18

Karolinska Institutet

Password regulations for Karolinska Institutet - Summary

Purpose

The main purpose of these regulations is to keep Karolinska Institutet's password-protected information systems safe from unauthorised use and to define the lowest quality and security requirements for password management at Karolinska Institutet.

Summary

The following rules (in summary) for password management apply to all IT services and systems (applications) at Karolinska Institutet.

- Passwords are personal and may not be disclosed to anyone else
- Passwords must be at least ten characters long[1]
- Passwords must contain letters, numbers and special characters
- Passwords may not be tied to personal information, such as name, civic registration number, phone number or username
- Passwords are to be changed every six months[2]
- Passwords may not be reused outside KI

For more detailed descriptions of Karolinska Institutet's password regulations, please read this entire document, which defines responsibilities, strategies, requirements and implementation rules for passwords at Karolinska Institutet.

Publisher:
Karolinska Institutet
Universitetsförvaltningen
Version: 2.0
Contact: it-support@ki.se

[1] Other requirements apply to accounts that are not personal user accounts
[2] See note 1

Karolinska Institutet's password regulations

Purpose

The main purpose of these regulations is to keep Karolinska Institutet's password-protected information systems safe from unauthorised use and to define the lowest quality and security requirements for password management at Karolinska Institutet.

Responsibilities

Compliance

As a user of Karolinska Institutet's information systems you are responsible for ensuring that

- your passwords meet the quality and management criteria set out in these regulations
- your user accounts, passwords and codes are kept personal and used exclusively by you
- your passwords are kept secret
- you never disclose your passwords to anyone requesting them, whether it be by email, phone or otherwise.

For systems integrated to Karolinska Institutet's central login and authentication service (Webbinloggning, LDAP and Active Directory) system support for compliance with these regulations is available.

For systems with their own password management function, compliance with these regulations is the responsibility of the system owner.

Strategies

All information systems (applications) are to be integrated to Karolinska Institutet's central login and authentication service unless exceptional reasons dictate otherwise.

Karolinska Institutet's central login and authentication service includes technical support for good password quality and safe password management.

Every user has a user ID and password for logging in to Karolinska Institutet's IT services; for some IT services, the user might have one or more additional user IDs/passwords. There might also be system-specific passwords. All

passwords used at Karolinska Institutet must at least meet the demands for password quality that is defined in these regulations.

Two-factor authentication (2FA) must be used to access IT services or systems (applications) classified as particularly sensitive or confidential. If 2FA is used, exceptions may be made to these regulations, although a risk analysis and documentation must be made per system, service or application that implements 2FA.

Scope

The password management regulations apply to all IT services and systems (applications) at Karolinska Institutet.

Password regulations

Personal user account

Passwords must:

- be at least 10 characters long
- be sufficiently strong, i.e. composed of the following:
  - A – Z (note: not the Scandinavian vowels Å, Ä, Ö, etc.)
  - a – z (note: not the Scandinavian vowels å, ä, ö, etc.)
  - 0 – 9
  - blank spaces
  - special characters: ~,!, @, #, $, %, ^, &, (,), _, +, -, *, /, =, {, }, [,], |, \, :, ;, ’ (single quote mark), ” (double quote mark), <, >, , (comma), . (full-stop), and ?
- contain at least two alphabetical and either at least two special characters or a number
- not be the same as your past 24 passwords
- remain unchanged for at least one day
- not be composed of an easily guessed word or common passwords from so-called “word lists”
- be changed within:
  - 6 months for employees, affiliates and doctoral students
  - 12 months for students

A reminder will be sent by email to the registered user of the account when it is time to change his or her password.

It is prohibited to reuse your KI username password for other than KI services (e.g. Facebook, public email addresses or private use) and to use your KI email address for private purposes.

The above requirements apply to all identities in all IT services and systems (applications) at Karolinska Institutet. The following account types are subject to additional regulations.

Administrator accounts

All accounts with high access (administrator) rights are to be personal. Use of the general root/administrator account or the equivalent is only allowed in exceptional circumstances. Administrator accounts are subject to the following additional regulations:

- Passwords must be at least 15 characters long
- Passwords must be changed within 6 months

Service accounts

Service accounts are subject to the following additional regulations:

- Passwords must be at least 15 characters long
- Passwords must be changed every 12 months, and the change recorded in the system's management documentation.

Functional accounts

The primary use for a functional account is when multiple users need access to the same function, such as a shared e-mail address for a function such as registry@ki.se or it-support@ki.se. Access to the functional account should be delegated to the individual personal user accounts, so that full audit trails can be kept. There must not be any shared functional accounts/group accounts. If technical restrains makes it impossible to delegate access, functional accounts adhere to the same regulations as Service Accounts.

Password protection

Storage and transfer of passwords

To reduce the risk of unauthorised access to passwords, the following storage and transfer regulations must be observed:

- Passwords must always be stored and transferred in encrypted form.
- Passwords must never be presented in a readable format.
- Passwords may never be shared by email, phone, etc.
- IT staff with access to the computers and media on which passwords are stored must sign a special commitment of responsibility. An updated list of employees with these privileges must be kept by the organisation running the system.

Protection against net-based "brute force attacks" (rate limiting)

To reduce the risk of automated password guessing ("brute force attacks"), logins are to be protected by rate limiting, which prevents a hacker from attempting repeated password guesses in a short space of time.

Karolinska Institutet's login service has the following settings:

- 30 incorrect guesses before the account is automatically locked.
- 30 minutes' automatic account locking after the maximum number of incorrect guesses.
- The login counter is reset after a successful login or 60 minutes after the latest incorrect login attempt.

Exceptions

If a particular system that is not connected to KI's login service has technical reasons for not following the above regulations for password quality and protection, an exception must be approved by the system owner and recorded in the system's management documentation or the equivalent. Special considerations must also be paid for access to data stored on other systems.

Control

The central IT-department, ITA, reserves the right to regularly audit the compliance of the KI password regulations

Definitions

Personal user account: is a user identity linked to a unique person and that this person uses to access his or her personal resources, such as email and the applications/systems needed for his or her work.

Administrator account: is a user account linked to a unique person and that this person uses to administrate a system resource that is not his or her own personal resource. All administrator accounts are to be personal. Administrator accounts can be set up for systems or servers, for example.

Service account: is an account in which a subsystem or service is the user and regulates which parts of another system the subsystem has access to. All service accounts are to be made unique to each system and restricted exclusively to the system for which they are intended. An example of a service account is when an application (e.g. web service) uses its own database on another server.

Functional account: is an account used for a shared function, for example the registry@ki.se or it-support@ki.se functions. The functional account is used to share an e-mail address between one or more regular personal accounts. The functional account doesn't have its own user-ID or password, instead access is granted to each personal user account that needs access to the functional account while still providing full audit trails.

Password quality: Good password quality means that a password is long and complex enough to reduce the risk of being guessed by a hacker. Two factors determine how difficult a password is to guess: length and complexity.

Password protection: Safe password management means not only that passwords are kept secret by their users, but also that the login service protects them from unauthorised access and use.

Change of password: To reduce the risk of a hacker uncovering a password to Karolinska Institutet's IT and information system, each user must regularly change his or her password within a fixed time interval.

Two factor/multifactor authentication (2FA/MFA): Login (authentication) using two or more distinct factors: something known (e.g. a password) and something possessed (e.g. a smart card or USB device).