Lösenordsregelverk för Karolinska Institutet

Dnr 1-213/2015

Version 2.0
Gäller från och med 2015-05-18

Karolinska Institutet

Karolinska Institutet

Lösenordsregelverk för Karolinska Institutet - Sammanfattning

Syfte

Det övergripande syftet med detta regelverk är att så långt det är möjligt skydda Karolinska Institutets lösenordsskyddade informationssystem från obehöriga användare samt att tydligt ange den lägsta nivån på krav gällande kvalitet och skydd på lösenordshantering inom Karolinska Institutet.

Sammanfattning

Följande förenklade sammanfattade regler för lösenordshantering gäller för alla IT-tjänster och system (applikationer) vid Karolinska Institutet.

- Lösenord är personliga och får inte delas med annan
- Lösenord ska bestå av minst 10 tecken[1]
- Lösenord ska vara sammansatt av både bokstäver, siffror och specialtecken
- Lösenord får inte vara knutet till personlig information som till exempel namn, personnummer, telefonnummer eller användarnamn
- Lösenord ska bytas var sjätte månad[2]
- Lösenord får inte återanvändas utanför KI

För detaljerade beskrivningar av kraven i Karolinska Institutets lösenordsregelverk ska hela detta dokument läsas. Det är det fullständiga dokumentet som anger ansvar, strategier, krav och implementation som gäller som lösenordsregelverk för Karolinska Institutet.

Utgivare:
Karolinska Institutet
Universitetsförvaltningen
Version: 2.0
För frågor kontakta it-support@ki.se

[1] För andra typer av konton än personliga användarkonton gäller andra krav
[2] Enligt not nr 1

Karolinska Institutet

Lösenordsregelverk för Karolinska Institutet

Syfte

Det övergripande syftet med detta regelverk är att så långt det är möjligt skydda Karolinska Institutets lösenordsskyddade informationssystem från obehöriga användare samt att tydligt ange den lägsta nivån på krav gällande kvalitet och skydd på lösenordshantering inom Karolinska Institutet.

Ansvar

Efterlevnad

Som användare av Karolinska Institutets informationssystem ansvarar du själv för

- Att dina lösenord uppfyller den kvalitet och hantering som anges i detta regelverk.
- Att användarkonton, lösenord och koder är personliga och endast får användas av innehavaren.
- Att du håller dina lösenord hemliga.
- Att, som en del av ovanstående punkt, aldrig uppge dina lösenord till någon som efterfrågar dem via e-post, i telefon eller på annat sätt.

För system som är kopplade till Karolinska Institutets gemensamma inloggnings- och autentiseringsrutiner (Webbinloggning, LDAP och Active Directory) finns systemstöd för efterlevnad av detta lösenordsregelverk.

För system med egen lösenordshantering är det systemägare som ansvarar för efterlevnad av detta lösenordsregelverk.

Strategier

Alla informationssystem (applikationer) ska vara kopplade till Karolinska Institutets gemensamma inloggningstjänst om inte särskilda skäl föreligger.

Karolinska Institutets gemensamma inloggningstjänst innehåller teknikstöd för god lösenordskvalitet och säker lösenordshantering,

Varje användare har ett användar-ID och ett lösenord för inloggning till Karolinska Institutets IT-tjänster. För inloggning till vissa IT-tjänster kan användaren dessutom ha ytterligare ett eller flera användar-ID/lösenord. Därutöver kan verksamhets- och/eller systemspecifika lösenord finnas. Alla

lösenord på Karolinska Institutet ska minst uppnå kraven för lösenordskvalitet i enlighet med detta regelverk.

Tvåfaktorautentisering ska användas för åtkomst till IT-tjänster eller system (applikationer) som kan klassas som synnerligen känsliga eller konfidentiella. Används tvåfaktorsautentisering kan undantag till delar av detta regelverk göras, dock ska det tydligt analyseras och dokumenteras per system, tjänst eller applikation som använder tvåfaktorsautentisering.

Omfattning

Regelverket för lösenordshantering gäller för alla IT-tjänster och system (applikationer) vid Karolinska Institutet.

Lösenordsregelverk

Personligt användarkonto

Lösenordet ska vara sammansatt på följande sätt:

- Bestå av minst 10 tecken
- Vara tillräckligt starkt, dvs. vara sammansatt av följande tecken:
  - A – Z
  - a – z
  - 0 – 9
  - Mellanslag
  - Följande specialtecken: ~,!, @, #, $, %, ^, &, (,), _, +, -, *, /, =, {, }, [,], |, \, :, ;, ’ (enkelt citationstecken), ” (dubbelt citationstecken), <, >, , (kommatecken), . (punkt), och ?
- Innehålla minst två alfabetiska och antingen minst två specialtecken eller en siffra
- Observera att till de bokstäver som kan användas hör endast a-z/A-Z, d.v.s. inte de skandinaviska bokstäverna (å,ä,ö osv)
- Lösenordet får inte vara samma som de senaste 24 lösenorden
- Minsta tillåtna tid mellan lösenordsbyte är 1 dagar
- Lösenordet får inte vara sammansatt av ett lätt gissat ord eller vanligt förekommande lösenord från så kallade ”ordlistor”
- Tvingande lösenordsbyte ska ske senast inom:
  - 6-månader för anställda, anknutna samt doktorander.
  - 12-månader för studenter.
- Ett påminnelse mail kommer skickas till den registrerade användaren av kontot när det är dags att byta lösenord

Det är inte tillåtet att återanvända lösenordet för KIs användarnamn för andra tjänster än KIs tjänster. (som. t.ex. Facebook, publika e-posttjänster, privat användning, m.fl.) likaväl som det inte är tillåtet att använda sin KI e-post adress för privata tjänster på Internet.

Ovan angivna krav gäller för alla identiteter i alla IT-tjänster och system (applikationer) vid Karolinska Institutet. Utöver ovan gäller följande krav för nedanstående kontotyper.

Administratörskonto

Alla konton som har höga åtkomsträttigheter, så kallade administratörsrättigheter ska vara personliga. Användandet av de generella root-/administrator-kontot eller motsvarande är bara tillåtet i undantagsfall. För administratörskonton gäller utöver anvisningarna för personligt konto följande:

- Lösenordet ska bestå av minst 15 tecken
- Tvingande lösenordsbyte ska ske senast inom 6 månader

Servicekonton

För servicekonto gäller utöver anvisningarna för personligt konto följande:

- Lösenordet ska bestå av minst 15 tecken
- Lösenordet ska bytas var 12e månad samt att detta ska dokumenteras i systemets förvaltningsdokumentation.

Funktionskonton

Ett funktionskonto är främst avsett för en delad funktion, där flera användare behöver ha åtkomst till en gemensam funktion. För funktionskonton ska behörighet till funktionskontot delegeras så att varje unik användares personliga användarkonto används så att spårbarhet alltid uppnås. Det får inte förekomma delade funktionskonton. Skulle det vara teknisk omöjligt att efterleva detta så gäller kraven för Servicekonto även för funktionskonto.

Lösenordsskydd

Datalagring och transport av lösenord

För att reducera risken för obehörig åtkomst till lösenord gäller följande för lagring och transport av lösenord:

- Lösenord ska alltid lagras och transporteras i krypterad form.
- Lösenord ska aldrig presenteras i läsbar form.
- Lösenord ska aldrig kommuniceras via epost, telefon eller motsvarande.
- IT-personal med teknisk åtkomst till de datorer och datamedia där lösenord lagras ska underteckna särskilda ansvarsförbindelser. En uppdaterad lista över medarbetare med dessa priviligierade behörigheter ska finnas vid den organisation som sköter driften av systemet, t.ex. ITA

Skydd mot nätbaserade gissningsattacker (Rate limiting)

För att reducera risken för automatiserade gissningsattacker mot lösenord (s.k. Brute force attacker) ska inloggningen vara skyddad genom s.k. rate limiting som förhindrar en inkräktare från att göra många upprepade lösenordsgissningar på kort tid.

I Karolinska Institutets gemensamma inloggningstjänst är detta utformat enligt följande:

- 30 felaktiga gissningar innan automatisk kontolåsning.
- 30 minuters automatisk kontolåsning efter maximalt antal felaktiga gissningar.
- Räknaren över antalet felaktiga gissningar nollställs efter korrekt inloggning eller efter 60 minuter efter senaste felaktiga inloggningsförsök.

Undantag

Om det i enskilda system som inte är kopplade till den gemensamma inloggningstjänsten föreligger särskilda tekniska skäl för att inte följa ovanstående lösenordsregelverk för god lösenordskvalitet eller lösenordsskydd ska undantag godkännas av systemägare och dokumenteras i systemets förvaltningsdokumentation eller motsvarande dokument. Vidare måste särskild hänsyn tas vid åtkomst av data hämtade från andra system.

Kontroll

Centrala IT-avdelningen förbehåller sig rätten att regelbundet granska efterlevnaden av KIs regelverk för lösenord.

Definitioner

Personliga användarkonton: är en användaridentitet som är kopplad till en unik person och som personen använder för att komma åt sina individuella resurser såsom e-post och applikationer/system som användaren nyttjar i sin tjänst.

Administratörskonton: användarkonton som är kopplat till en person och som används för att administrera någon systemresurs som inte är den personens individuella resurs. Alla administratörskonton ska vara personliga. Exempelvis kan det finnas administratörskonton för system eller servrar.

Servicekonton: användarkonton där ett delsystem är användaren och som används för att styra vilka delar av ett annat system som det delsystemet får komma åt. Alla servicekonton ska vara unika för respektive system och ska begränsas till att enbart få använda det system det är avsett för. Ett exempel på servicekonto är när en applikation (ex Webbtjänst) använder sin egen databas som ligger på en annan server.

Funktionskonto: Ett funktionskonto är främst avsett för en delad funktion, där flera användare behöver ha åtkomst till exempelvis ett delat e-post konto i centrala e-postsystemet som möjliggör att flera användare kan ta emot, läsa och svara på e-post skickade till en funktion, exempelvis registrator@ki.se eller it-support@ki.se. Ett funktionskonto har inget eget användarnamn eller lösenord utan varje användare med behörighet till funktionskontot använder sitt personliga användarkonto för att arbeta i funktionsrollen.

Lösenordskvalitet. God lösenordskvalitet innebär att ett lösenord är tillräckligt långt och komplext sammansatt för att reducera risken för att en inkräktare kan gissa sig till rätt lösenord. Två saker avgör svårigheten i att gissa ett lösenord: längden och komplexiteten på lösenordet.

Lösenordsskydd. Säker lösenordshantering innebär, förutom att varje användare ansvarar för att hålla sina lösenord hemliga, att inloggningstjänsten skyddar lösenord från otillbörlig åtkomst och användning.

Lösenordsbyte. För att ytterligare reducera risken att en inkräktare avslöjar ett lösenord till Karolinska Institutets IT- och informationssystem ska varje användare kontinuerligt byta lösenord inom ett fastställt tidsintervall.

Tvåfaktorautentisering/multifaktorautentisering. (förkortas vanligen 2FA/MFA) Inloggning (autentisering) med minst två skilda faktorer; ”något man vet” (t.ex. ett lösenord) och ”något man har” (t.ex. ett smart kort eller USB-sticka).