Inledning

Detta dokument anger Högskolan i Jönköpings policy för kvalitet på samt hantering av lösenord i enlighet med identitetsfederationen SWAMIDs policy.

Ansvar

Som innehavare av ett användarkonto på högskolan ansvarar du själv för:

- att dina lösenord uppfyller den kvalitet och hantering som anges i denna policy.
- 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 högskolans gemensamma autentiserings- och inloggningstjänst, finns systemstöd för efterlevnad av policyn. (Novell eDirectory eller Microsoft Active Directory)

För system med egen lösenordshantering är det systemägaren som ansvarar för efterlevnad av denna policy.

Definitioner

Lösenordskvalitet. God lösenordskvalitet innebär att ett lösenord är tillräckligt långt och komplext sammansatt för att reducera risken för att en obehörig kan gissa sig till rätt lösenord. Två saker avgör svårigheten i att gissa ett lösenord: längden och komplexiteten på lösenordet. Med hjälp av dessa kan man räkna ut ett lösenords entropi. Ju högre entropi ett lösenord har desto svårare är det att gissa det.

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

Kontotyper. Olika kontotyper har olika undantag från denna policy. Exempel på kontotyper där undantag sker, är kortvariga besökskonton som kan utfärdas av all personal på högskolan, eller funktionskonton där fler personer inom samma funktion kan dela på kontot. För mer information om kontotyper se: www.hj.se/helpdesk

Syfte

Det övergripande syftet med denna policy är att så långt det är möjligt skydda högskolans lösenordskyddade informationssystem från obehöriga användare.

Strategier

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

Högskolans gemensamma inloggningstjänst innehåller teknikstöd för god lösenordskvalitet och säker lösenordshantering.

HÖGSKOLAN I JÖNKÖPING

Lösenordspolicy

2015-03-01

Varje användare har normalt ett lösenord för inloggning till högskolans IT-tjänster. För inloggning till vissa IT-tjänster som t.ex. det trådlösa nätverket eduroam har varje användare dessutom ytterligare ett lösenord. Därutöver kan verksamhets- och/eller systemspecifika lösenord finnas.

Lösenordsskydd

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

- Lösenord ska aldrig presenteras i läsbar form. (Undantag för besökskonton)
- Lösenord ska aldrig kommuniceras via epost, telefon eller motsv. till okänd part.
- Lösenord ska alltid lagras och transporteras i krypterad form där det är tekniskt möjligt.
- Lösenord ska hållas hemliga och ska inte delas med andra. (Undantaget funktionskonton)

Lösenordskvalitet

Ett bra lösenord ska vara sammansatt på följande sätt:

Innehålla minst 8 tecken som kan bestå av följande tecken:

- A – Z
- a – z
- 0 – 9
- specialtecken: ! , @, # , $, % , & , (,) , * , + , - , [, \ ,] , ^ , _ , ` , { , | , } , ~ ’(enkelt citationstecken), ” (dubbelt citationstecken), , (kommatecken), . (punkt)

Ditt lösenord ska innehålla minst en versal, minst en gemen och minst en siffra samt kan med fördel innehålla specialtecken.

(För trådlös nätverkstjänst eduroam krävs exakt 7 tecken enligt samma som ovan.)

Ett lösenord ska INTE vara sammansatt på följande sätt:

- samma som eller likna användarnamnet.
- knutet till personlig information som t ex namn, personnummer, telefonnummer.
- vara en vanlig teckenkombination eller ord som finns i ordböcker, exempelvis 12345678, Sommar2014, Hemligt1, Password2, bilmärken etc.

Lösenordskontroll

I högskolans gemensamma inloggningstjänst finns teknikstöd för att säkerställa god lösenordskvalitet. Vid lösenordsbyte kontrolleras dessa lösenord med avseende på att de

- är sammansatta enligt punkt lösenordskvalitet ovan.
- inte är detsamma som de närmast 8 föregående lösenorden.

Skydd mot nätbaserade gissningsattacker (Rate limiting)

För att reducera risken för automatiserade gissningsattacker mot lösenord ska inloggningen vara skyddad genom s.k. rate limit som förhindrar en obehörig att göra många upprepade lösenordsgissningar på kort tid.

I högskolans gemensamma inloggningstjänst är detta utformat enligt följande:

- 20 felaktiga gissningar innan automatisk kontolåsning.
- 5 minuters automatisk kontolåsning efter maximalt antal felaktiga gissningar.

I högskolans självservice för användarkonto är detta utformat enligt följande:

- 3 felaktiga gissningar innan inloggning spärras för självservice.
- 30 minuters inloggningsspärr till självservice efter maximalt antal felaktiga gissningar.

Lösenordsbyte

För att ytterligare öka säkerheten till dina kontouppgifter ska varje användare kontinuerligt byta lösenord inom ett fastställt tidsintervall.

I högskolans gemensamma inloggningstjänst gäller följande regler för lösenordsbyte:

- Tvingande lösenordsbyte senast inom 1 år för studenter, anställda och övriga verksamma.
- Tvingande lösenordsbyte senast inom 2 månader för systemadministratörer.
- Tvingande lösenordsbyte senast inom 4 år för eduroam-tjänster för alla verksamma.