JÖNKÖPING UNIVERSITY

Lösenordspolicy

2019-10-01

Inledning

Detta dokument anger Jönköping University policy för kvalitet på samt hantering av lösenord i enlighet med identitetsfederationen SWAMIDs[1] policy.

Syfte

Syftet med denna policy är att skydda högskolans lösenordskyddade informationssystem från obehörig åtkomst och hantering.

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.

Lösenordskvalitet

Dina lösenord ska vara starka. Starka lösenord kan skapas antingen genom att kombinera enskilda tecken till ett relativt kort men komplext lösenord, eller skapa lösenordsfraser genom att kombinera flera ord.

Komplext lösenord

Ett komplext lösenord består av minst tio tecken som inkluderar en slumpmässig blandning av versaler, gemener, siffror eller specialtecken. Komplexa lösenord ger god säkerhet, går snabbt att skriva på vanligt tangentbord, men är i allmänhet svåra att komma ihåg och svåra att skriva på t.ex. mobiltelefon.

Lösenordsfras

En lösenordsfras är sammansatt av minst sex slumpmässiga ord som bildar en längre mening. Det är viktigt att orden verkligen är slumpmässiga och inte en läsbar mening. Lösenordsfraser ger oftast högre säkerhet än komplexa lösenord, är enklare att komma ihåg, och är typiskt enklare att skriva på t.ex. mobiltelefon.

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

Oavsett om du väljer komplext lösenord eller en lösenordsfras ska ett lösenord innehålla minst en versal, minst en gemen och minst en siffra eller specialtecken.

✓ Innehålla minst 10 tecken som kan bestå av följande tecken.

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

✗ Ett lösenord ska INTE vara sammansatt på följande sätt:

- samma som eller likna användarnamnet.
- knutet till personlig information som till exempel namn, personnummer, telefonnummer, namn på husdjur eller barn, exempelvis AnnaJonkoping036
- vara en vanlig teckenkombination eller ord som finns i ordböcker, exempelvis 12345678aB, Sommar2019, Hemligt000, Password01!
- inte en mening som är läsbar, exempelvis MyPetMaxIsOld3

(Eftersom WiFi-lösenord inte skyddas tillräckligt vid anslutning till WiFi-nätverk innebär det att det inte är tillåtet att använda samma lösenord till WiFi som används till ditt användarkonto. Det medför att lösenordet för eduroam ska vara exakt 7 tecken enligt samma som ovan vilket gör att de inte är lika.)

Lösenordshantering

Tänk på att ditt lösenord ska vara hemligt och unikt för högskolans tjänster, använd inte ditt JU-lösenord för tjänster utanför högskolan. Genom att använda samma lösenord på tjänster utanför högskolan har du i praktiken uppgett ditt lösenord för någon annan och ditt lösenord är inte längre hemligt.

Undantag från denna regel finns för funktionskonto som kan innehas av personal och studenter, ex registrator eller ordförande vid studentföreningar.

Om ditt lösenord blir känt av andra personer eller tjänster är ditt lösenord inte längre hemligt och du måste då byta lösenord snarast. Vid informationssäkerhetsincidenter eller om högskolan får kännedom om att ditt lösenord inte längre är hemligt, kan IT-service initiera en tvingande lösenordsåterställning enligt avsnitt **Lösenordsåterställning**.

Lösenordsbyte

Lösenordet gäller normalt tillsvidare, detta gäller även för tjänsten eduroam (WiFi).

I högskolans gemensamma inloggningstjänst gäller följande för lösenordsbyte:

- Tillsvidare giltigt lösenord för studenter, anställda och övriga verksamma.
- Tvingande lösenordsbyte senast inom 1 år för systemadministratörer.

Lösenordsbyte sker alltid i självserviceportalen, https://myaccount.ju.se aldrig på annan plats.

Lösenordsåterställning

För att återställa lösenord krävs att högskolan har bekräftad kännedom om personliga kontaktuppgifter såsom en privat e-post, SMS eller tredjepartsverifierad postadress, exempelvis via statens personadressregister[2] kallat SPAR. Personliga kontaktuppgifter anges vid aktivering av användarkonto eller i självserviceportalen för användarkonto. Återställning kan även ske genom antagning.se eller eduid.se med ett bekräftat konto.

Om ovan metoder inte fungerar, krävs ett personligt besök vid IT-helpdesk med giltig legitimation enligt Skatteverkets definition. För utlandsboende finns alternativet att skicka fotobevis av hemadress i form av exempelvis en elräkning samt giltig legitimation enligt Skatteverkets definition till IT-helpdesk.

Lösenordsåterställning sker alltid i återställningsportalen, https://passwordreset.ju.se aldrig på annan plats.

Lösenordskontroll

I högskolans gemensamma inloggningstjänst finns teknikstöd för att säkerställa god lösenordskvalitet. (Microsoft Active Directory, Azure Password Protection)
Vid lösenordsbyte kontrolleras lösenord med avseende på att de:

- är sammansatta enligt punkt lösenordskvalitet ovan, att lösenordet är av god kvalitet samt att varianter av lösenord inte finns med på publika lösenordslistor.
- inte är detsamma som de närmast 8 föregående lösenorden.

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

Systemkrav

Detta avsnitt innehåller krav på system vid JU som använder eller hanterar lösenord.
Enskilda studenter eller medarbetare behöver normalt inte ta hänsyn till dessa.

Avgränsning

Policy för lösenordsanvändning gäller alla IT-tjänster och system (applikationer) vid högskolan. Policyns omfattning omfattar två områden, lösenordskvalitet och skydd av lösenord.

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.

Undantag. 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: https://ju.se/helpdesk

Ansvar

För system som är kopplade till högskolans gemensamma autentiserings- och inloggningstjänst, finns systemstöd för efterlevnad av policyn. (Microsoft Active Directory, Azure Password Protection)

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

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.
- 30 minuters automatisk kontolåsning efter maximalt antal felaktiga gissningar.

Strategier

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

JÖNKÖPING UNIVERSITY

Lösenordspolicy

2019-10-01

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

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 hantering av lösenord.

- Lösenord ska aldrig presenteras i läsbar form.
    - Undantag för besökskonton.
    - Undantag kan göras i processer där t.ex. en engångskod ska kommuniceras till en enskild användare. Detta ska göras till en på förhand känd e-postadress, SMS eller postadress.
- Lösenord ska aldrig kommuniceras via epost, telefon eller motsvarande.
    - Undantag för besökskonton.
    - Undantag kan göras i processer där t.ex. en engångskod ska kommuniceras till en enskild användare. Detta ska göras till en på förhand känd e-postadress, SMS eller postadress.
- Lösenord ska transporteras i krypterad form och bör använda minst TLS 1.2 med aktuell ”bästa praxis” för TLS.
- Lösenord som lagras permanent ska helst lagras som saltad hash. Det förekommer att lösenord i klartext är nödvändiga. I dessa fall ska lösenorden lagras krypterade, företrädesvis med krypteringsnyckel som inte finns permanent på systemet.