HÖGSKOLAN I SKÖVDE

Anvisningar för lösenord

Dessa anvisningar har fastställts av Magnus Annerfalk, avdelningschef för service, IT och säkerhet 2021-11-15 och träder i kraft samma datum.

Dnr HS 2021/726

Innehållsförteckning

1 Inledning

Denna anvisning ingår i Högskolans i Skövdes (Högskolan) ledningssystem för informationssäkerhet. (LIS)

Detta dokument anger Högskolans anvisning för kvalitet på samt hantering av lösenord i enlighet med identitetsfederationen SWAMIDs policy. Det övergripande syftet med denna anvisning är att så långt det är möjligt skydda Högskolans lösenordskyddade informationssystem från obehöriga användare.

2 Ansvar

Som användare av Högskolans informationssystem ansvarar du själv för

- att dina lösenord uppfyller den kvalitet och hantering som anges i denna anvisning.
- att du håller dina lösenord hemliga.
- att, som en del av ovanstående punkt, aldrig lämna ut dina lösenord till någon som efterfrågar dem via e-post, i telefon, sms eller på annat sätt.

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

För system med egen lösenordshantering är det systemägaren för systemet på Högskolan som ansvarar för efterlevnad av denna anvisning.

3 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 eller tecken från flera ord. Lösenordsfraser är rekommenderade.

3.1 Komplext lösenord

Ett komplext lösenord består av minst åtta slumpmässigt valda tecken och inkluderar versaler, gemener, siffror och specialtecken. Tecknen bör inte väljas med någon systematik.

3.2 Lösenordsfras

En lösenordsfras är sammansatt av flera ord som bildar en mening. T.ex JagGillarInteSpindlarISovrummet. En lösenordsfras kan även bestå av första bokstaven i orden från en mening. Lösenordsfraser ger oftast högre säkerhet än komplexa lösenord, kan vara lättare att memorera och är typiskt enklare att skriva på t.ex. mobiltelefon.

3.3 Lösenordssammansättning

Ett lösenord ska vara sammansatt på följande sätt:

- Bestå av minst 8 tecken.
- Vara sammansatt av följande tecken:
- A – Z
- a – z
- 0 – 9
- mellanslag
- följande specialtecken: ~,!, @, #, $, %, ^, &, (,), _, +, -, *, /, =, {, }, [,], |, \, :, ;, ’ (enkelt citationstecken), ” (dubbelt citationstecken), <, >, , (kommatecken), . (punkt), och ?.

Innehålla minst en versal, minst en gemen och antingen minst ett specialtecken eller en siffra.

3.4 Lösenordshantering

Det är inte tillåtet att uppge sitt lösenord för någon annan. Ingen har rätt att fråga dig efter ditt lösenord, och du ska inte under några omständigheter uppge det – inte heller till medarbetare vid Högskolan.

Använd olika lösenord till olika system. Använd aldrig de lösenord du använder i tjänsten till tjänster utanför Högskolan. Genom att göra det har du i praktiken uppgett ditt lösenord för åtkomst till Högskolans IT-infrastruktur för en annan leverantör av tjänst.

Om ditt lösenord blir känt av andra personer eller tjänster/leverantörer är ditt lösenord och din information inte längre hemlig/skyddad och du ska då snarast byta lösenord.

Vid informationssäkerhetsincidenter eller om Högskolan får kännedom om att ditt lösenord inte längre är hemligt, kan Helpdesk tillfälligt inaktivera ditt användarkonto och begära ett lösenordsbyte. Om du är osäker på om en begäran om att byta lösenord är legitim, kontakta Helpdesk och uppge det ärendenummer du fått.

I Högskolans gemensamma inloggningstjänst gäller följande för lösenordsbyte:

- Tillsvidare giltigt lösenord för studenter
- Tvingande lösenordsbyte efter 180 dagar för personal

4 Systemkrav

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

4.1 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.

Varje användare har ett lösenord för inloggning till Högskolans IT-tjänster. Därutöver kan verksamhets- och/eller systemspecifika lösenord finnas.

4.2 Omfattning

Anvisningar för lösenordshantering gäller för alla IT-tjänster och system (applikationer) vid Högskolan.

Anvisningarna omfattar två områden, lösenordskvalitet och lösenordsskydd.

4.2.1 Lösenordskvalitet

Lösenordskontroll

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

- är sammansatta enligt punkten Lösenordssammansättning ovan,
- *inte återfinns i en katalog med lösenord av dålig kvalitet (123456, egennamn, årstider, bilmärken etc.)1,*
- inte är detsamma som det närmast föregående och

Lösenordet går inte att spara förrän det uppfyller minimikraven.

Undantag

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

4.2.2 Lösenordsskydd

Datalagring och transport av lösenord

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

- Lösenord ska aldrig presenteras i läsbar form.
- Lösenord ska aldrig kommuniceras via epost, telefon eller motsv.
- 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 IT-service på SITS.

4.2.3 Undantag

I de fall konsulter anlitas vid akuta ärenden såsom t.ex säkerhetsincident eller en systemincident som påverkar Högskolans verksamhet kommuniceras ett tillfälligt lösenord via telefon.

4.2.4 Skydd mot nätbaserade gissningsattacker (Rate limiting)

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

I Högskolans gemensamma inloggningstjänst är detta utformat enligt följande:

- 50 felaktiga gissningar innan automatisk kontolåsning.
- 5 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 föreligger särskilda tekniska skäl för att inte följa ovanstående anvisning för lösenordsskydd ska undantag godkännas av systemägare och dokumenteras i systemets systemdokumentation eller motsvarande dokument. Vidare måste särskild hänsyn tas vid åtkomst av data hämtade från andra system.

5 Ikraftträdande

Dessa anvisningar träder i kraft 2021-11-15