Handläggare, telefon
Gustavo Navarro 46 (0)790603180

Ert datum

Er referens

Lösenordspolicy

1 Inledning

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

2 Ansvar

2.1 Efterlevnad

Som användare av Kungl. Konsthögskolans informationssystem 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 Kungl. Konsthögskolans gemensamma inloggnings- och autentiseringsrutiner (Webbinloggning, LDAP och Active Directory) finns systemstöd för efterlevnad av policyn.

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

4 Syfte

Det övergripande syftet med denna policy är att så långt det är möjligt skydda Kungl. Konsthögskolans lösenordsskyddade informationssystem från obehöriga användare.

5 Strategier

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

Kungl. Konsthögskolans gemensamma inloggningstjänst innehåller teknikstöd för god lösenordskvalitet och säker lösenordshantering, se pkt. 6.1 och 6.2.

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

Tvåfaktorautentisering ska användas för åtkomst till IT-tjänster eller system (applikationer) som enligt Kungl. Konsthögskolans policy för informationsklassificering innehåller konfidentiell information med HÖGA eller SÄRSKILDA KRAV på att skydda informationen från obehöriga användare.

Handläggare, telefon
Gustavo Navarro 46 (0)790603180

Ert datum

Er referens

6 Omfattning

Policyn för lösenordshantering gäller för alla IT-tjänster och system (applikationer) vid Kungl. Konsthögskolan.
Policyn omfattar två områden, lösenordskvalitet och lösenordsskydd.

6.1 Lösenordskvalitet

6.1.1 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.
- Användaren ska uppmanas att inte sätta samma lösenord som de använder i antingen andra interna eller externa IT-tjänster.

6.1.2 Lösenordskontroll

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

- är sammansatta enligt pkt. 6.1.1 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
- inte är samma som användarens övriga lösenord i den gemensamma inloggningstjänsten, t.ex. lösenordet för inloggning i trådlösa nät1.

Lösenordet går inte att spara förrän det uppfyller minimikraven.

[1]I Active Directory och andra nyckelfärdiga system är det inte alltid möjligt att genomföra kontroller enligt punkt två och fyra. Om detta gäller er är det rekommenderat att kravet på minsta lösenordslängd ökas med två tecken till tio tecken.

6.1.3 Undantag

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

Handläggare, telefon
Gustavo Navarro 46 (0)790603180

Ert datum

Er referens

6.2 Lösenordsskydd

6.2.1 Datalagring och transport av lösenord

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

- Lösenord ska alltid lagras och transporteras i krypterad form. Detta gäller även backupmedia.
- 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.

6.2.2 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 Kungl. Konsthögskolans gemensamma inloggningstjänst är detta utformat enligt följande:

- 10 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.

6.2.3 Lösenordsbyte

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

I Kungl. Konsthögskolans gemensamma inloggningstjänst gäller följande regler för lösenordsbyte:

- Tvingande lösenordsbyte senast inom 12 månader för anställda, övriga verksamma samt för s.k. funktionskonton.
- Tvingande lösenordsbyte senast inom 5 år för studenter.

6.2.4 Undantag

Om det i enskilda system föreligger särskilda tekniska skäl för att inte följa ovanstående policy för lösenordsskydd ska undantag godkännas av systemägare och dokumenteras i systemets förvaltningsspecifikation eller motsvarande dokument. Vidare måste särskild hänsyn tas vid åtkomst av data hämtade från andra system.

Handläggare, telefon
Gustavo Navarro 46 (0)790603180

Ert datum

Er referens

7 Definitioner

7.1 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. Med hjälp av dessa kan man räkna ut lösenordets entropi. Ju högre entropi ett lösenord har desto svårare är det att gissa det. Se pkt. 6.1 och bilaga 1 för vidare information.

7.2 Lösenordsskydd.

Säker lösenordshantering innebär, förutom att varje användare ansvarar för att hålla sina lösenord hemliga, att inloggningstjänsten skyddar lösenord från otillbörlig åtkomst och användning. Se pkt. 6.2 för vidare instruktioner.

7.3 Tvåfaktorautentisering.

Inloggning med två skilda faktorer; till exempel ett lösenord och ett godkännande i en autentiseringsapp.