Riktlinje för lösenord - Personligt användarkonto (ADM)

(Gäller från och med 2017-10-06, reviderad 2022-10-27)

Denna riktlinje för lösenord gäller för anställda och förtroendevalda i V6 kommunerna, Essunga, Götene, Skara, Vara, Grästorps och Lidköpings kommun samt kommunala bolag.

Syfte

Syftet med denna riktlinje är att skydda vissa utsedda interna och externa lösenordskyddade informationssystem från obehöriga användare samt att tydligt ange den lägsta nivån på krav gällande kvalitet och skydd på lösenordshantering i Göliska ITs gemensamma inloggningstjänst.

Riktlinjen gäller för inloggning på kommunernas datorer, IT-infrastrukturen och Microsoft 365 samt vissa större verksamhetssystem med personligt användarkonto i det administrativa nätverket.

Utöver personliga användarkonton kan verksamhets- och/eller systemspecifika lösenord finnas som inte omfattas av denna riktlinje.

Ansvar

För att komma åt system och resurser på det administrativa nätverket krävs ett personligt användarkonto och lösenord i Göliska ITs gemensamma inloggningstjänst. I denna inloggningstjänst finns det teknikstöd för att säkerställa god lösenordskvalitet och säker lösenordshantering.

Personligt användarkonto 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 andra system som användaren nyttjar i sin tjänst. Viss information och vissa system kan även kräva en stark autentisering där användarens identitet kontrolleras på fler sätt.

Till användarkontot hör ett lösenord som endast användaren känner till och kan ändra. Lösenordet skall endast vara känt av innehavaren som ansvarar för att det förvaras så att otillbörligt utnyttjande inte kan ske.

Undantag:

* IT-ansvariga och personal på Göliska IT som kan utföra delegerad behörighetsadministration, kan byta lösenord.

Sammanfattning

Följande förenklade sammanfattade regler för lösenordshantering gäller för personliga användarkonton i det administrativa nätverket:

- Lösenord skall bestå av minst 8 tecken
- Lösenord skall vara tillräckligt starkt och sammansatt av olika tecken som beskrivs i avsnitt Lösenordssammansättning
- Lösenord kan inte innehålla personlig information som namn eller användarnamn
- Lösenordet får inte innehålla 3 eller fler likadana bokstäver i rad
- Lösenordet måste skilja sig från det förra lösenordet med mer än bara sista tecknet
- Lösenordet får inte vara enkelt eller vanligt förekommande (svartlistat)
- Tvingande lösenordsbyte efter 180 - 270 dagar (ett längre lösenord varar längre)
- Lösenord är personliga och får inte delas med annan
- Lösenord skall inte återanvändas utanför kommunen. (t.ex. Facebook, publika e-posttjänster, privat användning, m.fl.)
- Gruppkonto får inte användas på grund av spårbarhetskrav

Undantag:

* Avsteg från gällande riktlinje för gruppkonto beslutas av person med rollen som kommunens representant i leveransgruppen, förvaltningschef/sektorchef eller motsvarande samt Göliska IT. Beslut skall dokumenteras.

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 faktorer avgör svårigheten i att gissa ett lösenord; längden och komplexiteten på lösenordet.

Lösenordssammansättning

Ett lösenord skall vara tillräckligt starkt dvs. sammansatt på följande sätt:

- **Bestå av minst 8 tecken**
- **Måste uppfylla minst 3 av följande kriterier**
    - **innehålla minst 1 liten bokstav: a-z**
    - **innehålla minst 1 stor bokstav: A-Z**
    - **innehålla minst 1 siffra: 0-9**
    - **innehålla minst 1 specialtecken: (t.ex. !, @, $, #, %, *)**
- **Lösenordet kan inte innehålla personlig information som namn eller användarnamn**
- **Lösenordet får inte innehålla 3 eller fler likadana bokstäver i rad**

Instruktioner:

- Tillåtna bokstäver är endast a-z/A-Z, d.v.s. inte de skandinaviska bokstäverna (å, ä, ö).
- Lösenord skall inte vara sammansatt av ett lätt gissat ord eller vanligt förekommande lösenord från så kallade ”ordlistor”.

Exempel på lösenord:

☺ AZ09%sep (i detta exempel är alla fyra kriterierna uppfyllda).
☺ För att lättare komma ihåg sitt lösenord kan man använda en fras, t.ex. Inattjagdromde?42.

Lösenordsskydd

Säker lösenordshantering innebär, förutom att varje användare ansvarar för att hålla sitt lösenord hemligt, att inloggningstjänsten skyddar lösenord från otillbörlig åtkomst och användning samt reducerar risken för automatiserade gissningsattacker utformat enligt följande:

- **Efter 10 felaktiga inloggningsförsök låses användarkontot automatiskt**
- **Låst användarkonto låses upp automatiskt efter 15 minuter**
- **Lösenordet kan inte vara samma som något av de senaste 24 lösenorden**
- **Lösenordet måste skilja sig från det senaste lösenordet med mer än bara sista tecknet**
- **Lösenordet får inte vara enkelt eller vanligt förekommande (svartlistat)**
- **Användarkonto som upphört att gälla inaktiveras inom 24 timmar**

Undantag:

* Låst användarkonto kan även öppnas av Göliska IT eller av utsedd personal (t.ex. IT-ansvarig på förvaltning) efter säker identifiering av användaren.

Instruktioner:

- Lösenord skall aldrig kommuniceras via e-post, telefon eller motsvarande.
- Lösenord skall aldrig presenteras i läsbar form.
- Lösenordet skall inte återanvändas utanför kommunen. (t.ex. Facebook, publika e-posttjänster, privat användning, m.m.).

Lösenordsbyte

För att ytterligare reducera risken att en obehörig avslöjar ett lösenord till Göliska ITs gemensamma inloggningstjänst skall varje användare kontinuerligt byta lösenord inom ett fastställt tidsintervall.

- **Tvingande lösenordsbyte efter 180 - 270 dagar (ett längre lösenord varar längre)**

Instruktioner:

- Initialt och tillfälligt lösenord skall bytas vid första användningen.
- När det är dags att byta lösenord kommer påminnelser att skickas via e-post till den registrerade användaren av kontot.