Piteå kommun

Anvisning för lösenordshantering

Dokumentnamn	Dokumenttyp	Senast reviderad	Beslutsinstans
Anvisning för lösenordshantering	Anvisning	2023-03-31	Kommunchef
Administrationsansvarig	**Version**	**Diarienummer**	**Giltig till**
Kommunledningsförvaltningen	1	22KS300	2027-06-30
Dokumentinformation	Anvisning för lösenordshantering		
Dokumentet gäller för	Alla förvaltningar och bolag		

Piteå kommun

Inledning

Av Policy för informationssäkerhet i Piteå kommunkoncern framgår att målet för koncernens arbete med informationssäkerhet är att skydda koncernens verksamhet mot avbrott i informationsflödet samt förebygga och begränsa skador till följd av oönskade händelser.

Denna anvisning syftar till att skapa styrning för säker åtkomst till och behörighetstilldelning i interna och externa IT-system oavsett driftplattform.

Anvisningen gäller för kommunens förvaltningar och bolag som nyttjar IT-system och/eller nätverksutrustning.

Anvisningen innebär att krav kan behöva ställas på extern part, t.ex. leverantör av IT-system eller IT-tjänster.

Övergripande ställningstagande

- Tillgång till information i IT-system och systembehörigheter ska begränsa till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter.
- Konton ska skyddas med motståndskraftiga lösenord
- Kommunens digitala tillgångar ska skyddas från obehörig åtkomst.

Krav i denna anvisning på lösenord gäller alla system där det är tekniskt möjligt att efterleva dessa. Om det inte är tekniskt möjligt att efterleva kraven för ett visst system ska funktionen för informationssäkerhet rådfrågas i syfte att uppnå en likvärdig säkerhetsnivå.

Roller och ansvar

Här beskrivs de olika rollernas grundläggande ansvar. I andra kapitel av anvisningen kan finnas mer detaljerade anvisningar.

Chef för IT-avdelningen
IT-avdelningen ansvarar för att upprätta de rutiner som är nödvändiga för att efterleva denna anvisning och övrig implementering.

Chef för verksamhet
Chef för respektive verksamhet ansvarar för att anställda och andra som deltar i kommunens eller det kommunala bolagets verksamhet förbinder sig att skydda åtkomstuppgifter till kommunens IT-miljö från obehörig åtkomst.

IT-användare
IT-användare ansvarar för att lösenord och hjälpmedel inte tillgängliggörs för andra på något sätt, t.ex. muntligt, via chattmeddelande eller post it-lapp.

Systemägare
Ansvarar för att genom avtal och systeminställningar säkerställa att leverantör av IT-system eller IT-tjänster efterlever denna anvisning.

Informationssäkerhetsstrateg
Informationssäkerhetsstrateg ansvarar för att utöva tillsyn över informationssäkerhet i kommunkoncernen samt för råd och stöd i frågor kopplade till informationssäkerhet.

Anvisningar för IT-användare i Piteå Kommuns IT-miljö

Med IT-användare avses alla som på något sätt har åtkomst till Piteå kommuns IT-miljö, t.ex. elever, tjänstepersoner inom kommunen och de kommunala bolagen, förtroendevalda, leverantörer och externa konsulter.

Krav på lösenord för IT-användare

Lösenord ska vara unika och erbjuda på motståndskraft, och förbli okända för andra. Bestämmelsen ska särskilt beaktas vid skapande av konton och återställande av lösenord.

Lösenordet ska bestå av

- Minst 15 tecken
- Minst en stor bokstav
- Minst en liten bokstav
- Minst en siffra

Lösenord får inte

- Innehålla den anställdes förnamn, efternamn eller inloggningsnamn
- Inte innehålla något av årstider, lokala ortnamn, månader eller bokstäverna Å, Ä, Ö
- Bestå av gamla lösenord
- Vara identiska med lösenord som används till privata konton

Lagring av lösenord

- Lösenord får inte lagras i klartext, till exempel i en applikation för anteckningar.
- Lösenord får endast lagras i av IT-avdelningen särskilt anvisad lösenordshanterare.

Lösenordsbyte

- Lösenord ska bytas senast 12 månader efter senast lösenordsbyte
- Lösenordsbyte ska alltid ske omedelbart vid misstanke om olovlig spridning

Möjligheten att logga in låses efter fem felaktiga inloggningsförsök.

Anvisningar för IT-användare av priviligerade konton i Piteå kommuns IT-miljö

Systemägare ansvarar för att genom avtal och systeminställningar säkerställa att leverantör av IT-system eller IT-tjänster efterlever följande krav för priviligierade konton.

Med priviligierade konton avses konton med högre systemadministrativa rättigheter.

Det innefattar såväl konton kopplade till Microsofts systemmiljö, som konton kopplade till hårdvara inom nätverksmiljön och konton kopplade till verksamhetssystem.

Exempel på priviligerade konton kopplade till Microsofts systemmiljö är Domain Admin Accounts, Domain Service Accounts, Local Administrator Account, Emergency Accounts, Service Accounts, Application Accounts och Privileged Data User Account.

Exempel på priviligierade konton kopplade till hårdvara inom nätverksmiljön är Root konton, Wi-Fi konton, hårdvarukonton som t.ex. BIOS och vPro, nätverksutrustning, brandväggskonton och konton som används för säkerhetslösningar.

Exempel på priviligierade konton kopplade till verksamhetssystem är superadministratörs-konton och administratörskonton som har möjligheter att göra systeminställningar.

Krav på lösenord för IT-användare av priviligierade konton

Privilegierade konton ska skyddas med lösenord som har starkare skydd än lösenord för IT-användare.

Lösenord till priviligierade konton ska vara unika för varje enskilt konto.

Lösenordet ska bestå av

- Minst 30 tecken
- Minst en stor bokstav
- Minst en liten bokstav
- Minst en siffra

Lösenord får inte

- Innehålla den anställdes förnamn, efternamn eller inloggningsnamn
- Inte innehålla något av årstider, lokala ortnamn, månader eller bokstäverna Å, Ä, Ö
- Bestå av gamla lösenord
- Vara detsamma som förinställda lösenord för leverantörskonton

Lagring av lösenord

- Lösenord får inte förekommer eller lagras i klartext i filer eller vara kodade i script.
- Lösenord får endast lagras i av IT-avdelningen särskilt anvisad lösenordshanterare.

Möjligheten att logga in låses efter fem felaktiga inloggningsförsök.

Anvisningar för systemägare rörande styrning av åtkomst och behörighet

Tillfälliga lösenord

Vid skapande av nytt konto eller vid återställning av befintligt konto kan tillfälligt lösenord skapas. För tillfälliga lösenord gäller samma krav som ordinarie lösenord, vilket bland annat innebär att tillfälliga lösenord behöver vara unika.

Lagring av lösenord

- IT-avdelningen ska tillhandahålla en teknisk lösning för att förhindra att lösenord lagras på annan plats än i av IT-avdelningen särskilt anvisad lösenordshanterare.
- IT-avdelningen ska använda krypteringstekniker som *hashing* och *saltning* där det är möjlig för att skapa en säker lagring av lösenord.

Återställning eller byte av lösenord

- Systemägare ska tillhandahålla och underhålla nödvändig dokumentation som underlättar för användare att på egen hand byta lösenord.
- Systemägare ska vid tillhandahållande av självhjälpsportal för lösenordsåterställning ställa krav på multifaktorautentisering.
- IT-avdelningen ska i händelse av konstaterat intrång av allvarlig art i kommunens IT-miljö genomföra en global lösenordsåterställning. IT-avdelning ska säkerställa att de rutiner som är nödvändiga för att global lösenordsåterställning ska kunna ske skyndsamt finns upprättade.
- Systemägare ska stänga av konton som inte använts på 90 dagar.
- Systemägare ska säkerställa att konton låses efter fem felaktiga inloggningsförsök.

Multifaktorautentisering

När ska multifaktorautentisering tillämpas?
Multifaktorautentisering, det vill säga kontroll av uppgiven identitet på minst två olika sätt, ska använda för att förstärka skyddet av infrastrukturella komponenter som IT-system och nätverksrustning.

Multifaktorautentisering ska användas för att skydda åtkomst till skyddsvärd information som omfattas eller kan omfattas av sekretess samt personuppgifter av kategorierna integritetskänsliga eller känsliga personuppgifter, samt vid förekommande risk på grund bristande informationshantering.

Multifaktorautentisering ska användas där intrång innebär risk för att inkräktaren kan utge sig för att vara Piteå kommun eller anställd inom kommunen, t.ex. konton på sociala medier.

Multifaktorautentisering ska även i annat fall användas där det behövs för att skydda skyddsvärd information och andra skyddsvärda tillgångar.

Multifaktorautentisering ska oberoende av mjukvaruleverantör alltid användas för att skydda extern åtkomst till applikationer och tjänster utanför det interna nätverket.

Val av multifaktorautentiseringsmetod ska fattas i samråd med relevanta parter, som systemägare, informationsägare och IT-avdelningen. Piteå kommun ska sträva efter en enhetlig användning av multifaktorautentisering.

Vem ansvarar för att multifaktorautentisering tillämpas?
IT-avdelningen ansvarar för att multifaktorautentisering används för;

- Externt tillgängliga applikationer där det är möjligt.
- Fjärråtkomst till det interna nätverket från det publika nätet (Internet).
- Vid systemadministrativa systemåtkomst till IT-system och nätverksutrustning oavsett driftform och placering, internt (on-prem), utkontrakterat (outsourced) eller molntjänst.
- System som ingår i kommunens centraliserade system för kontohantering (Active Directory).

Systemägare ansvarar för att multifaktorautentisering används:

- där systemet inte ingår i kommunens centraliserade system för kontohantering (Active Directory).

Undantag
IT-chef kan bevilja undantag från krav på multifaktorautentisering för konton med befintlig tillgänglighet via internet. Vid undantag ska följande aktiviteter genomföras.

- Systemet ska nätverkssegmenteras från övriga system
- Systemet ska säkerhetskonfigureras enligt IT-avdelningens rutiner för att skydda IT-system mot obehörig åtkomst
- Det ska upprättas en skriftlig åtgärdsplan för implementering av multifaktorautentisering för det aktuella systemet

Mekanism för att identifiera och hantera risker

IT-avdelningen ska tillhandahålla teknisk lösning för att automatisera identifiering och reparation av identitetsbaserade risker i syfte att säkerställa en förmåga att upptäcka och agera på olika cyberattack metoder som t.ex. lösenordsspray och läckta autentiseringsuppgifter.

Granskning

Alla konton och behörigheter till dessa ska fortlöpande granskas för att säkerställa behovsenlig behörighetstilldelning. Granskning av priviligierade konton ska ske minst två gånger per år och granskning av allmänna konton ska ske minst en gång per år.

Granskningen ska dokumenteras och hanteras enligt informationshanteringsplan för verksamheten.