Antagen av Kommunfullmäktige 2020-09-16 § 65 Dnr: 2020.000202.005

Behörighetspolicy

DALS-EDS KOMMUN

1 - Inledning

Dals-Eds kommuns behörighetspolicy visar på de värderingar och tankar som ska styra och prägla kommunens behörighetshantering kring de informationstillgångar vi hanterar för dem vi är till för.

2 - Relation till andra styrdokument

Tillsammans med Digital Agenda, Dataskyddspolicy och Informationssäkerhetspolicy är en Behörighetsspolicy ett ramverk för Digitaliserings- och IT-handlingsplan, Riktlinjer för informationshantering, Riktlinjer för Internetanvändare och vår ständigt pågående process kring systemförvaltning.

3 - Syfte och omfattning

3.1 - Syfte

Denna behörighetspolicy för Dals-Eds kommun är en beskrivning för hur all behörighetstilldelning ska ske för att alla användares åtkomst inte ska stå i konflkt med kraven på sekretess, riktighet, tillgänglighet och spårbarhet.

3.2 - Omfattning

Behörighetspolicyn avser samtliga användarkategorier i Dals-Eds IT-infrastruktur.

4 - Mål och viljeinriktning

Det yttersta målet med en säker hantering av behörigheter i kommunen är att fördjupa förtroendet för kommunen hos medborgare kring hur vi som kommun ansvarsfullt och med stor fokus på personlig integritet hanterar all den datamängd vi har tillgång till.

5 - Behörighetspolicy i Dals-Eds kommun

5.1 - Behörighetshantering

Syftet med behörighetshanteringen är att samtliga användare ska få åtkomst till information de behöver för att utföra sina arbetsuppgifter (tillgänglighet) samtidigt som informationens riktighet (integritet) säkerställs, ingen obehörig åtkomst till information kan ske (sekretess) samt att det går att se vem som har haft åtkomst till information och vid vilken tidpunkt (spårbarhet).

5.1.1 - Behovsenlig behörighetstilldelning

Behörigheter ska tilldelas utifrån att man inte ska ha mer behörighet än vad som behövs för att utföra sina arbetsuppgifter.

5.1.2 - Användarkonton

Användare i digitala system ska i första hand skapas per automatik via HR-systemet alternativt från Cybercom Directory Access (CDA).

I andra hand ska det ske genom manuell uppläggning.

5.1.3 - Gruppkonton

Ett gruppkonto används av flera individer. Gruppkonton ska aldrig ha fullständiga administratörsrättigheter (root-admin) i ett system. Gruppkonton ska i normalfallet ej vara tillåtet. Samtliga användare ska ha unika identiteter och gruppkonton ska endast tillåtas i undantagsfall.

Beslut om undantag samordnas av systemförvaltaren och fattas av systemägaren i samråd med informationssäkerhetssamordnaren.

5.1.4 - Systemkonton

Ett systemkonto kan användas av flera personer och har oftast en hög behörighet i ett system. Alla standardlösenord i system och komponenter ska ändras före produktionssättning. Detta inkluderar t.ex. applikationer, operativsystem, routrar, brandväggar och åtkomstpunkter. Inaktiva konton som inte kan knytas till en affärsprocess och inte har en ägare ska inaktiveras.

5.1.5 - Leverantörskonton

Ett leverantörskonto kan i vissa fall vara ett systemkonto. Då ska access för leverantören regleras på andra sätt än med inloggningen. Om inte, konton som inte används kontinuerligt (”vilande” konton, exempelvis en leverantörs konto som används för support och systemunderhåll) ska inaktiveras och endast aktiveras för den tidsperiod som är nödvändig. Kontot ska även ha så låg behörighet som möjligt men ändå kunna lösa uppdraget. Vilande kontons användning ska övervakas för att upptäcka obehörig användning. Hanteringen av leverantörskonton och eventuella undantag ska dokumenteras.

5.1.6 - Utökade rättigheter

Användandet av privilegierade/utökade rättigheter, dvs användande av olika administratörsrättigheter i en persons vanliga användarkonto, ska endast användas av utpekade personer och endast för arbetsuppgifter då utökade behörigheter är nödvändigt.

Användandet av separata adminstratörskonton ska även de endast användas av utpekade personer och endast för arbetsuppgifter då utökade behörigheter är nödvändigt.

Tilldelande av utökade rättigheter ska tilldelas skriftligen av systemförvaltaren och godkännas av systemägaren och personens chef. För dokumentation se avsnitt spårbarhet.

5.1.7 - Distansarbete

Särskild vikt ska läggas vid att ha kontroll på behörighet till access via VPN från dator.

5.2 - Autentiseringsmetod

Användarroll	Autentiseringsmetod
Användare i ett system	Om hantering av [KÄNSLIG] data= Tvåfaktorsautensiering
Superanvändare	Tvåfaktorautentisering
Systemadministratör kommunnivå	Tvåfaktorautentisering
Systemadministratör förvaltningsnivå	Tvåfaktorautentisering
Systemadministratör delsystemnivå	Tvåfaktorautentisering

5.2.1 - Användarnamn

Strävan är att personens e-postadress inte ska användas.

5.2.2 - Lösenord

Inför ändring eller nyinförande av modell för lösenord i ett system ska Myndigheten för Samhällsskydd och Beredskap (MSB) checklista Säkra dina lösenord användas som en parameter bland andra.

Där flerfaktorsautentisering inte stöds och det förekommer känslig data bör användarkonton tvingas använda unika, långa och starka lösenord för systemet.

Lösenord ska alltid beakta följande kriterier:

- Att det inte är möjligt att sätta för få tecken
- Syn på komplexitet av lösenord ändras över tid
- Tidigare lösenord ska ej återanvändas

Användaren har ett personligt ansvar för att skydda sina lösenord.

En långsiktig strävan är inloggning till en persons konton via Single Sign On (SSO).

5.3 - Behörighetstilldelning

5.3.1 - Ansöka om behörighet

Ansökan om behörighet sker av användares chef till systemförvaltaren i skriftlig form.

För dokumentation se avsnitt spårbarhet.

5.3.2 - Attest av behörighet

Ansökan om behörighet granskas och godkänns enligt tabellen nedan.

Roll	Behörig attesterare	Kriterier
Användarkonto - ej systemadministratör	Chef	Behovsprövning av chef
Systemadministratör - Inte avancerad	Systemförvaltare och chef	Kompetensnivå verifieras av systemförvaltare
Systemadministratör - Avancerad	Systemägare och chef	Kompetensnivå och eventuell säkerhetsklassning verifieras av systemförvaltare

5.3.3 - Tilldela behörighet

Efter godkänd ansökan tilldelas behörighet av systemförvaltaren.

5.3.4 - Spårbarhet

Beslut om tilldelad behörighet och borttagning av behörighet ska dokumenteras och lagras skriftligt av systemförvaltaren i kvalitetsledningssystemet.

5.3.5 - Återkalla behörighet

Strävan är att användarbehörigheter i system ska avslutas automatiskt vid borttagning i kommunens Löne- och Personaladministrations-system.

5.3.6 - Internkontroll

Tilldelade administratörsbehörigheter ska minst gås igenom med en period om 3 månader.

Tilldelade användarrättigheter som hanteras manuellt ska minst gås igenom med en period om 12 månader.

Ansvarig är systemförvaltaren.

5.4 - Utbildning

Systemägare och Systemförvaltare ska genomgå utbildning för användarhantering enligt denna behörighetspolicy. Systemförvaltarna ska även genomgå praktisk utbildning i användarhantering.

6 - Levandegöra

Regelbunden praktisk utbildning av chefer, projektledare och medarbetare läggs in i årshjulet.

7 - Uppföljning

Det dagliga arbetet kring behörighetshantering i kommunen vilar på systemförvaltaren i det aktuella systemet. Systemförvaltaren kan i sin tur ha tillgång till systemadministratörer som utförare.

Efterlevnaden av behörighetspolicyn bygger på att systemägaren har tillsatt systemförvaltare och att systemförvaltaren har den kompetens och tid som erfordras för uppdraget.

Alla verksamheter och individer ska själva löpande följa upp om de lever efter policyn eller inte. Med det menas att om man har för hög behörighet i ett system har man en skyldighet att anmäla det till minst sin chef.