



## Bilag

### Ændringer til Forretningscirkulære for informationsikkerhed

#### 4.1.8. Tilsyn med autorisationer (nuværende cirkulære tekst)

Medarbejderens nærmeste leder skal ud fra en risikobaseret tilgang føre periodiske tilsyn med, at tildelte autorisationer i it-systemer afspejler medarbejderens arbejdsmæssige behov.

For it-systemer, der behandler personoplysninger, skal der dog som udgangspunkt føres tilsyn med, om tildelte autorisationer afspejler medarbejdernes arbejdsmæssige behov, mindst hver sjette måned.

Tilsyn med autorisationer vedrører også eksterne konsulenter autorisationer. Vær her opmærksom på særlige kontraktuelle bestemmelser for det enkelte it-system.

Tabel 23: Ansvars- og rollefordeling ift. "Tilsyn med autorisationer"

<b>Aktivitet</b>	<b>Udførende</b>	<b>Ansvarlig</b>	<b>Rådgivende</b>	<b>Informeret</b>
Tilsyn med autorisationer	Nærmeste leder	Forvaltningsdirektion	Koncern IT	-

Udover dette forretningscirkulære gælder følgende regler, forretningsgange, standarder mm.:

- Forretningscirkulære for ledelsestilsyn

#### 4.1.8 Ledelsestilsyn med autorisationer (forslag til ny cirkulære tekst)

Medarbejderens nærmeste leder skal føre periodiske tilsyn med, at tildelte autorisationer i it-systemer afspejler medarbejderens arbejdsbetingede behov.

Kravene til, hvordan tilsynene skal foretages, følger bl.a. databeskyttelsesforordningens artikel 5, stk. 1, omhandlende adgangsrettigheder efter behov samt artikel 32, stk. 1, omhandlende periodisk kontrol af adgangsrettigheders aktualitet.

Tilsyn med autorisationer vedrører alle KK-brugeridentiteter, herunder eksterne konsulenter, faste vikarer, elever m.m.

Formålet med et ledelsestilsyn er at opdage og rette eventuelle fejl i aktiviteterne i en autorisations livscyklus, herunder tildeling, vedligehold og fratagelse, fx som følge af ændringer i medarbejderes arbejdsbetingede behov eller ansættelsesforhold.

21-10-2024

Sagsnummer i F2  
2024 - 17281

Dokumentnummer i F2  
6393020

Sagsnummer eDoc  
2024-0308072

Sagsbehandler  
Mads Nikolaj Nielsen

For it-systemer, der behandler personoplysninger, skal der dog som udgangspunkt føres tilsyn med, om tildelte autorisationer afspejler medarbejdernes arbejdsmæssige behov, mindst hver sjette måned.

It-systemer, der er onboardet til kommunens brugerstyringsløsning, gør brug af løsningens systemunderstøttede arbejdsgange og forbyggende foranstaltninger ift. it-brugerens livscyklus, som sikrer styringsoverblik og højt sikkerhedsniveau. Tillige understøtter brugerstyringsløsningen, at muligheden for systemunderstøttet ledelsestilsyn til autorisationer foreligger.

It-systemer, der ikke er integreret til kommunens brugerstyringsløsning, kan ikke gøre brug af brugerstyringsløsningens systemunderstøttede arbejdsgange og forbyggende foranstaltninger.

Ud fra følgende kriterier kan systemer eller specifikke autorisationer fravige kravet om at føre ledelsestilsyn:

1. Systemet har ingen brugere.
2. Systemet indeholder i sig selv ikke data.
3. Systemet indeholder kun åbne data.
4. Systemet indeholder ikke autorisationer eller kræver særlig licens.
5. Systemet udelukkende behandler personoplysninger, der udtrykker en medarbejders funktion i Københavns Kommune
6. Autorisationer onboardet i brugerstyringsløsningen, der automatisk tildeles til medarbejdere baseret på organisatorisk data, uden krav om yderligere godkendelse.

Fælles for alle ovenstående situationer, hvor et eventuelt ledelsestilsyn undtages, skal Systemer dokumentere og journalisere på hvilket sagligt og oplyst grundlag vurderingen er foretaget.

Tablet 23: Ansvars- og rollefordeling ift. "Tilsyn med autorisationer"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Tilsyn med autorisationer	Nærmeste leder	Forvaltningsdirektion	Koncern IT	-