

Checklista – behörighetstilldelning och åtkomstkontroll för chef

Om det finns en instruktion eller rutin avseende behörigheter så följ den. Saknar du instruktion eller rutin – be den som är systemadministratör/behörighetsadministratör (oftast lokalt verksamhetsstöd, LVS) om information.

När en medarbetare börjar sin anställning

- Beställ behörigheter utifrån de arbetsuppgifter (roll) som medarbetaren ska ha och organisatorisk tillhörighet.
- Saknas behörighet utifrån roll och tillhörighet, stäm av med behörighetsadministratören för en behörighet som inte är för vid eller för snäv.
- Avser behörigheten någon annans enhet/verksamhetsområde än det du är chef för? Lämna över beställningen/lägg för attest till den som är chef för den enheten/verksamhetsområdet.
- Säkerställ att medarbetaren får information/utbildning kring vad som gäller kring behörigheter. Ta med information i introduktioner eller på APT om att det sker åtkomstkontroller och vad följderna kan bli om de obehörigt tar del av uppgifter som de inte är behöriga till. Be dina medarbetare att de informerar dig om deras behörighet inte motsvarar det de behöver utifrån sin roll och organisatoriska tillhörighet. Till exempel kan en för snäv behörighet innebära risk för att arbetsuppgifter inte kan utföras korrekt.

När en medarbetaren får nya/andra arbetsuppgifter

- Ska en medarbetare tillfälligt hantera andra arbetsuppgifter? Beställ/meddela behörighetsadministratören så att behörigheterna kan tidsbegränsas.
- Ska en medarbetare få permanent ändrade arbetsuppgifter? Stämmer behörigheten fortfarande? Meddela ändring.
- Ska din medarbetare vara studieledig, tjänstledig eller föräldraledig under en lång period? Beställt borttag/ändring av behörigheten.

När en medarbetare slutar i förvaltningen/eller i Staden

- Ta fram en rutin för hur du hanterar beställning av borttag av behörigheter när medarbetare slutar. Säkerställ att borttag av behörigheter beställs.
- Finns det behörigheter till andra konton som t ex tankkort, SITHS-kort? Stäm av med den som slutar och gå igenom vilka konton/behörigheter som ska avslutas och om fysiska kort/tags ska lämnas tillbaka. Säkerställ att behörigheterna avslutats och hur kort/tags ska återlämnas.
- Har din medarbetare konton/behörigheter till interna eller externa appar? Har du bett hen att avslutar konton/behörigheter till appar eller liknande innan anställningen upphör?

Till dig som ska genomföra **åtkomstkontroller, åtgärda och följa upp avvikelser**

- **Kontrollera**

Utför kontrollerna i enlighet med den rutin som tagits fram för IT-stödet. Oftast är det LVS som dokumenterar och tar fram protokoll samt skickar dig listor med instruktion om vad du ska kontrollera. Saknar du information om hur kontrollerna ska utföras så kontaktar du den som ansvarar för IT-stödet eller den som gett dig i uppdrag att göra kontrollerna, oftast LVS – det ska framgå i systemets rutin.

- **Resultat utan anmärkning** dokumenteras och signeras av den som utför kontrollen.

- **Resultat med avvikelse och åtgärder**

Om kontrollen resulterar i en avvikelse så behöver du som har kunskap om användarens arbetsuppgifter och tjänst undersöka detta vidare. Är behörigheter felaktiga så behöver du omedelbart åtgärda detta genom att beställa borttag/förändring av behörigheten. Du behöver även säkerställa att den obehörige användaren inte har fått tillgång till uppgifter. Har den obehörige användare varit inne och tittat i en journal ska detta även anmälas som en personuppgiftsincident. Det kan också gälla för andra avvikelser som du upptäcker i samband med kontrollen.

- **Rapportera avvikelser och åtgärda dem**

Du rapporterar obehörig åtkomst som en **avvikelse**. Inom socialtjänstens område gör du en avvikelse i Treserva. Har du inte tillgång till Treserva gör du en avvikelse till ansvarig enhetschef. Rör avvikelse exempelvis ett HR-system så görs avvikelsen enligt rutin för systemet. Den som ansvarar för systemet ska beskriva hur avvikelser hanteras.

Andra avvikelser eller personuppgiftsincidenter som kan identifieras vid en kontroll:

Exempel avvikelse: brister i dokumentation, brister i sekretess

Exempel personuppgiftsincident: medarbetare har obehörigt skrivit i fel journal, medarbetare har obehörigt skickat dokument (fel uppgifter har skickats).

Avvikelser och incidenter dokumenteras även i kontrollprotokollet. Om du upptäcker avvikelser som kan bedömas som dataintrång så kan detta också behöva polisanmälas.

- **Följ upp dina avvikelser och åtgärder**

Vad har du för avvikelser? Hur kan du minimera risken för nya avvikelser? Är dina åtgärder tillräckliga? Behöver du följa upp dem?

Kontakta förvaltningens dataskyddskontakter om du har frågor om behörighetstilldelning eller åtkomstkontroll:

dataskyddskontakt@funktionsstod.goteborg.se