Ansvarig namn Verksamhetsområdeschef	Upprättad av Camilla Lindvall (SAS) Lotta Tyrberg (MAS)	Berörda verksamheter Hälsa- och omsorg	Fastställd datum 2024-06-12
Dokumentnamn **Rutin för behörigheter**	**Ledningssystem** Enligt SOSFS 2011:9	Reviderad	Diarienummer

Rutin för behörigheter 2

1. Bakgrund 2
2. Syfte 2
3. Styrning av behörighet 2
4. Begränsning av behörigheter 2
5. Inloggning och lösenord 2
6. Ny behörighet 3
7. Byta behörighet 3
8. Uppföljning av behörigheter 3
9. Avsluta behörigheter 3
10. Loggkontroller 3
11. Kommunövergripande rutiner 4

Rutin för behörigheter

1. Bakgrund

Med behörighet menas att rättigheter att använda information eller en IT-resurs på ett specificerat sätt tilldelas en person.

Vårdgivaren ansvarar för att varje användare tilldelas en individuell behörighet för åtkomst till personuppgifter i gällande verksamhetssystem. Behörigheten ska begränsas till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter. (gäller hälso- och sjukvården).

2. Syfte

Syftet med rutinen är att säkerställa att behörighetstilldelningen följer gällande lagstiftning för att begränsa möjligheten att personuppgifter sprids, förändras eller på annat sätt används för ändamål som inte är godkända.

3. Styrning av behörighet

Behörigheten till verksamhetssystemen styrs via användaridentiteten och användarens personliga lösenord.

Detta möjliggör spårbarhet i systemet genom loggning. Förutom att loggen kan användas som underlag vid utredning av felaktig eller obehörig användning utgör den även en säkerhet för användarna mot ogrundade misstankar.

För att uppfylla kravet på individuella behörigheter ska tabell *Beslutsunderlag för behörigheter följas.*

4. Begränsning av behörigheter

Behörigheter till verksamhetssystemen ska endast tilldelas på den enhet där personen ska arbeta. Arbetar personen på flera enheter tilldelas behörighet även där, efter att en individuell behovs- och riskanalys utförts. För att få behörighet på mer än en enhet krävs att medarbetaren arbetar med regelbundenhet även på denna enhet, minimum en gång i månaden.

5. Inloggning och lösenord

För att få tillgång till olika nätverk och verksamhetssystem krävs inloggning.

Kraven på säkerhet gällande inloggning varierar beroende på system. Det kan vara lösenord, mobilt bank-id, eller specifika autentiseringsmetoder.

Stark autentisering, så kallad tvåfaktorsautentisering, innebär en verifiering i två steg. Exempel på detta kan vara lösenord samt en engångskod som skickas via SMS eller lösenord och ett elektroniskt identifikationskort som tex SITHS.

Lösenord och inloggningsmetoder är personliga och ska hanteras så att obehöriga inte får tillgång till dem.

6. Ny behörighet

Vid nyanställning ansvarar närmaste chef för beställning av behörigheter vilket görs till systemförvaltare eller systemadministratör på avsedd blankett.

Närmaste chef ska informera personen om ansvaret som medföljer behörigheterna:

- att lösenord och SITHS-kort är personligt och inte får lånas ut
- att behörig användare alltid ska göra ett aktivt val om rätten att ta del av information om kunder/patienter
- att behörigheterna är individuella och inte får lånas ut/överlåtas till annan person
- att sekretess råder
- att behörigheterna följs upp med regelbundna loggkontroller
- att överträdelse gällande informationssäkerhet kan leda till arbetsrättsliga och/eller straffrättsliga åtgärder
- att rapportera till närmaste chef om oegentligheter i behörigheter eller system upptäcks

7. Byta behörighet

Vid byte av tjänst ansvarar nyanställande chef för ändring av behörigheten. Tabell *Beslutsunderlag för behörigheter* ska följas. Behörigheter som inte längre är aktuella för tjänsten ska samtidigt avslutas av chefen som inte längre kommer ha personalen anställd.

8. Uppföljning av behörigheter

Ansvarig chef ansvarar för att regelbundet, minst var tredje månad, följa upp att endast giltiga behörigheter finns tillgängliga. Speciellt viktigt är detta att följa upp då visstidsanställda och semestervikarier avslutar sin anställning

9. Avsluta behörigheter

Vid avslutad anställning ansvarar närmaste chef för att personens behörighetstilldelning avslutas omgående.

Avsedd blankett skickas till systemförvaltare/systemadministratör som avslutar behörigheterna.

10. Loggkontroller

Närmaste chef ansvarar att via loggkontroll följa upp och kontrollera att användare följer de regler och rutiner som gäller.

Se separat rutin för loggkontroll.

11. Kommunövergripande rutiner

Samtliga medarbetare ska ha god kännedom om kommunövergripande rutiner för hantering av:

- Dataskydd (GDPR)
- Dokument och ärendehantering
- Informationsförvaltning och informationssäkerhet

Närmaste chef ansvarar för att delge medarbetare relevant information relaterat till profession och arbetsuppgifter.