Dokumentansvarig:
Dataskyddskontakt ÄVO

Metodstöd för behovs- och riskanalys vid behörighetstilldelning i socialtjänstens IT-system

Syftet

Detta metodstöd syftar till att ge ett strukturerat, spårbart och integritetssäkert arbetssätt för att fastställa behörigheter i socialtjänstens verksamhetssystem som till exempel Treserva. Behörigheter ska alltid tilldelas utifrån ett tydligt identifierat verksamhetsbehov, med beaktande av risker för den enskildes personliga integritet och gällande rättsliga krav.

Målet är att skapa en systematik för behörighetsstyrning som:

- grundar sig i tydlig arbetsuppgiftsfördelning och faktisk roll i ärendet
- vilar på rättsliga grunder enligt SoLPuL, SoL och GDPR
- tillämpar principen om minsta möjliga åtkomst (”need to know”)
- förebygger integritetsrisker, felaktig behandling och regelefterlevnadsbrister
- möjliggör transparent, spårbar och korrekt dokumentation
- stärker verksamhetens efterlevnad av krav på ansvar, säkerhet och proportionalitet i personuppgiftsbehandlingen.

Metoden ska användas vid:

- införande eller omdefiniering av roller och behörigheter
- organisatoriska förändringar som påverkar åtkomstbehov
- systemupphandling eller uppdatering av behörighetsprofiler
- regelbunden översyn av befintliga behörigheter enligt SoLPuL och GDPR.

Målgrupp

Metoden riktar sig till personer med ansvar eller funktion i behörighetsstyrning inom socialtjänstens verksamhet och IT-miljö, särskilt:

- chefer med behörighetsansvar
- systemägare och superanvändare
- verksamhetsrepresentater i projekt
- projektledare vid förändringsarbete
- IT- och informationssäkerhetsfunktion
- dataskyddskontakt eller informationssäkerhetsansvarig

Begrepp och definitioner

Nedan förklaras centrala begrepp som används i metodstödet. Definitionerna syftar till att skapa en gemensam förståelse och enhetlig tillämpning i arbetet med behörighetsstyrning.

Behörighet Tilldelad rätt att utföra vissa åtgärder i ett IT-system, såsom att läsa, registrera, ändra eller besluta. Ska alltid motsvara en konkret arbetsuppgift och ges enligt principen om minsta möjliga åtkomst.
Åtkomst Möjlighet att ta del av eller hantera information i ett system. Åtkomst ska alltid vara behovsprövad och dokumenterad.
Behovsprincipen ("need to know") Endast den som behöver viss information för att kunna utföra sitt arbete ska ha åtkomst till den.
Behörighetsprofil Fördefinierad samling av systemrättigheter kopplad till en viss roll eller funktion. Ska utformas utifrån verksamhetsbehov, riskbedömning och gällande regelverk.
Roll/funktion Tjänst eller uppdrag med tydligt definierade arbetsuppgifter. Används som grund för att bedöma behov av behörighet.
Sekretessreglerade uppgifter är uppgifter som skyddas av offentlighets- och sekretesslagen (OSL)
För vid behörighetstilldelning (överåtkomst) Behörighet som ger mer information än vad som är nödvändigt. Ökar risken för integritetsintrång, felhantering och personuppgiftsincidenter.
För snäv behörighetstilldelning (underåtkomst) behörighet som är för begränsad. Kan hindra arbetets genomförande eller leda till felaktiga beslut.
Skyddsåtgärder Tekniska eller organisatoriska åtgärder för att minska identifierade risker. Exempel: behörighetsstyrning, loggning, stark autentisering.
Behörighetsansvarig Person med mandat att fatta beslut om behörighet. Ansvarar för att behovs- och riskanalys genomförs och dokumenteras korrekt.
Systemägare Ansvarar för verksamhetsdelen av ett IT-system, inklusive att säkerställa att behörighetstilldelning följer lagstiftning och interna regler.
Behörighetsstyrning Samlat begrepp för processer som rör analys, beslut, tilldelning, ändring, uppföljning och återkallelse av behörigheter.

Metodöversikt och rättsligt ramverk

Rättslig bakgrund – krav på behörighetstilldelning och åtkomstkontroll

Från den 1 mars 2024 gäller nya bestämmelser i lagen (2001:454) om behandling av personuppgifter inom socialtjänsten (SoLPuL). De skärper kraven på behörighetstilldelning, åtkomstkontroll och loggning i verksamhetssystem som Treserva. Bestämmelserna gäller all behandling av personuppgifter som sker helt eller delvis automatiserat inom verksamheter enligt socialtjänstlagen (SoL) och lagen om stöd och service till vissa funktionshindrade (LSS).

De nya reglerna konkretiserar redan gällande skyldigheter enligt flera rättskällor:

- **Dataskyddsförordningen** (GDPR): Behandling av personuppgifter ska vara ändamålsenlig, nödvändig och proportionerlig i enlighet med artikel **5.1 c** (uppgiftsminimering) och **5.1 f** (integritet och konfidentialitet).
- Enligt **artikel 24** GDPR åläggs den personuppgiftsansvarige att säkerställa att behandlingen sker med hjälp av lämpliga tekniska och organisatoriska åtgärder, baserat på en riskbedömning.
- **Artikel 32** specificerar dessutom att den personuppgiftsansvarige ska vidta lämpliga säkerhetsåtgärder för att skydda personuppgifter – däribland åtkomstkontroller, behörighetsstyrning, loggning och andra tekniska lösningar som förhindrar obehörig åtkomst eller behandling.
- **Socialtjänstlagen (SoL):** Dokumentation ska hanteras med respekt för den enskildes integritet och skyddas från obehörig åtkomst. Endast personer med faktisk arbetsuppgift i ärendet ska ha tillgång till uppgifterna. Åtkomst ska därför begränsas enligt principerna för behörighetsstyrning i enlighet med 14 kap. 6–7 §§ SoL.

Den personuppgiftsansvarige har ett tydligt lagkrav att aktivt styra och kontrollera åtkomsten till personuppgifter. Det innebär att följande krav ska uppfyllas:

- **Behörigheter ska tilldelas individuellt och behovsprövat** – utifrån den anställdes faktiska arbetsuppgifter.
- **Åtkomst ska begränsas till det som är nödvändigt** – ingen ska ha bredare tillgång än vad uppdraget kräver.

- **Tekniska skyddsåtgärder ska användas** – till exempel behörighetsnivåer, rollstyrning och stark autentisering.
- **All åtkomst ska loggas och dokumenteras** – så att det går att spåra vem som har gjort vad, när och varför.
- **Logguppföljning ska ske regelbundet** – inte bara vid misstanke, utan som en kontinuerlig kontroll.

Dessa krav innebär att behörigheter i system som Treserva aldrig får vara generella eller rutinmässiga. Åtkomst ska vara begränsad, ändamålsenlig och rättssäker, med ett tydligt och dokumenterat integritetsskydd för den enskilde.

Från regelverk till tillämpning – en strukturerad metod i sex steg

För att möta kraven på ett systematiskt och rättssäkert sätt används en analysmodell i sex steg. Analysmodellen bygger på IMY:s vägledning för behörighetstilldelning. Den utgör en sammanhållen och strukturerad process där varje moment bygger på det föregående och tillsammans skapar ett välgrundat beslutsunderlag inför tilldelning av behörighet. Med stöd av modellen kan behörighet tilldelas på ett rättssäkert sätt utifrån en samlad bedömning av behov och risk i enlighet med tillämpliga regelverk.

Nedan beskrivs varje steg och dess funktion i analysprocessen.

1. **Analysera och fastställ verksamhetens behov**
   Identifiera vilka uppgifter och ansvar som föreligger i rollen eller funktionen. Klargör vilket informationsbehov som finns för att möjliggöra ett ändamålsenligt utförande av uppdraget. Det handlar om att tydligt svara på frågan: *Vad behöver medarbetaren ha åtkomst till – och varför?* Detta steg utgör grunden för hela analysen.

2. **Identifiera och analysera riskerna för enskildas personliga integritet**
   Med utgångspunkt i verksamhetens behov analyseras vilka risker som uppstår vid åtkomst till personuppgifter, särskilt uppgifter av känslig natur enligt GDPR, OSL och SoLPuL. Riskanalysen kopplas direkt till behovsanalysen och ska belysa potentiella konsekvenser för den enskilde vid till exempel obehörig åtkomst, bristande loggning eller otillräcklig behörighetsavgränsning.

3. **Identifiera och vidta lämpliga tekniska och organisatoriska åtgärder**
   Utifrån riskanalysen föreslås tekniska och organisatoriska skyddsåtgärder. Exempel på tekniska åtgärder är rollstyrd behörighet, loggning och behörighetsstyrda vyer. Exempel på organisatoriska är utbildning, ansvarsfördelning och instruktioner. Dessa åtgärder syftar till att minska de risker som identifierats och ska vara proportionerliga i förhållande till behovet.

4. **Fastställ en behörighetsstruktur som stödjer behoven och minimerar riskerna**
   Efter att behov, risker och åtgärder har identifierats fastställs en lämplig behörighetsstruktur. Den ska vara anpassad för att tillgodose verksamhetens behov utan att exponera mer information än nödvändigt. Här konkretiseras besluten genom till exempel behörighetsprofiler eller individuella tilldelningar.

5. **Dokumentera samtliga steg**
   All analys, bedömning och beslut ska dokumenteras på ett transparent och spårbart sätt. Dokumentationen fungerar som grund för beslut om behörighet,

men även för revision, rättsutredning eller vid incidenter. Den är även central för att möjliggöra efterhandskontroll och lärande.

6. **Följ upp och se över behörighetsstrukturen kontinuerligt**
   Slutligen är processen inte avslutad vid beslut. Behörighetsstrukturer ska följas upp regelbundet och anpassas vid förändringar i organisation, uppdrag eller regelverk. Uppföljning är en nödvändig förutsättning för att säkerställa att tidigare antaganden fortsatt är giltiga.

Systematiskt tillvägagångssättet för behov- och riskanalysen

Nu när den övergripande modellen är på plats är det dags att gå från princip till praktik. Det görs genom att steg för steg arbeta med **behovsanalys** och **riskanalys** anpassat till den aktuella verksamheten eller rollen. För att underlätta arbetet finns några mallar och stödmaterial som konkretiserar varje steg. Detta gör det lättare att dokumentera och följa upp analysen på ett enhetligt sätt.

Bilaga A och B innehåller just sådana praktiska stöd. Bilaga A hjälper dig att kartlägga och dokumentera vilka behov av åtkomst som finns i en viss roll eller funktion. Bilaga B, tillsammans med en riskmatris, ger struktur för att identifiera risker och föreslå lämpliga skyddsåtgärder. Du kan använda dem både för enskilda roller och för hela verksamhetsområden – vilket bidrar till att arbetet blir rättssäkert och jämförbart över tid.

Nästa steg är alltså att använda **Bilaga A (behovsanalys**) och **Bilaga B (riskanalys**), tillsammans med mallar för dokumentation, beslut och uppföljning, för att genomföra analysen i praktiken.

Dokumentansvarig:
Dataskyddskontakt ÄVO

Bilaga A – Behovsanalys vid behörighetstilldelning

Syfte

Behovsanalysen görs inför tilldelning eller ändring av behörigheter för att säkerställa att åtkomst till personuppgifter vilar på rättslig grund och följer principen om minsta möjliga åtkomst.
Analysen utgår från medarbetarens anställning och arbetsuppgifter och tillämplig av lagstiftning, exempelvis socialtjänstlagen (SoL) eller SoLPUL.

Beskrivning av verksamhetsbehovet

Innan behörighet tilldelas, ändras eller avslutas – exempelvis i Treserva – ska verksamhetens faktiska behov av åtkomst analyseras. Det gäller vid nyanställning, ändrade arbetsuppgifter eller avslut. Det ska tydligt framgå vilken information medarbetaren behöver för sitt uppdrag och varför.

Otillräcklig behovsanalys riskerar att leda till för bred åtkomst med ökade personuppgiftsincidenter och risker. För snäv åtkomst kan försvåra för genomförande av uppgift eller uppdrag. En strukturerad behovsanalys minimerar båda riskerna.

För att stödja analysen finns vägledande frågor som hjälper till att identifiera minsta nödvändiga informationsutrymme. Dessa bör användas i dokumentationen och ligga till grund för beslut om behörighet. Målet är att varje åtkomst ska vara motiverad, spårbar och rättssäker.

Bilaga A.1 - Stödfrågor vid tilldelning, revidering eller uppföljning av behörigheter

1. Arbetsuppgifter och uppdrag

- Vilka konkreta arbetsuppgifter ska medarbetaren utföra?
- Kräver uppdraget administrativ, operativ eller beslutsfattande roll (t.ex. planerare, sjuksköterska, socialsekreterare)?
- Arbetar medarbetaren inom flera verksamhetsområden eller organisatoriska enheter?

2. Informationsbehov och tillgång till personuppgifter

- Vilken typ av information krävs för att uppgifterna ska kunna utföras rättssäkert och effektivt?
- Behövs åtkomst till uppgifter om brukare med pågående eller avslutade insatser?
- Behövs åtkomst till brukare från andra enheter, exempelvis andra stadsdelar eller boenden?
- Behövs åtkomst till avlidna brukare för uppföljning eller utvärdering?

3. Åtkomstens omfattning

- Gäller åtkomsten alla brukare eller endast en specifik målgrupp/enhet?
- Behövs åtkomst till skyddade personuppgifter?
- Behövs åtkomst till brukare som är offentliga eller medieprofilerade personer?

4. Åtkomstens typ och nivå

- Ska medarbetaren kunna läsa information, registrera uppgifter eller fatta beslut i ärenden?
- Krävs möjlighet att söka på namn eller personnummer?
- Krävs användning av ärendenummer?
- Behövs åtkomst till andra geografiska områden?

Bilaga A.2 – Mallar och exempel

Namn för medarbetare:
Anställning som:

Behov	**Ja/nej**	**Undantag**	**Överväganden**	**Övriga omständigheter**
handlägga				
läsa				
rätta				

Exempel 2: Roll planerare i hemtjänsten

Planerare i hemtjänsten behöver tillgång till individärenden inom sitt geografiska område för att kunna planera, följa upp och justera insatser enligt biståndsbeslut enligt SoL. Behörighet krävs för att se relevanta uppgifter om brukare, schemalägga insatser, samordna personal och dokumentera förändringar. Åtkomst till hela förvaltningens brukare är vanligtvis inte motiverad och bedöms utgöra en onödig vid behörighetstilldelning.

Dokumentationsmall – Behovsanalys exempel

Nr	**Fält**	**Beskrivning/Exempel**
1	Verksamhetsområde	Hemtjänst
2	Roll/funktion/anställning	Planerare
3	Arbetsuppgifter kopplade till behörighet	Planera hemtjänstinsatser, uppdatera schema i verksamhetssystem, justera insatser enligt biståndsbeslut
4	System/IT-tjänster	Treserva,
5	Typ av personuppgifter som kommer att hanteras	Namn, personnummer, hälsouppgifter,

		biståndsbeslut, daganteckningar, information om insatser osv
6	Rättslig grund	Verkställa och planera insatser enligt SoL Socialtjänstlagen (SoL) SoLPUL 10 kap.
7	Motivering till behovet	• För att kunna planera och följa upp beviljade insatser i hemtjänsten i xxxx, för att effektivisera arbetsuppgifterna • Eventuell tillfällig utökad behörighet vid behov av samverkan mellan enheter
8	Bedömning av minsta åtkomst	Behörighet ska begränsas till brukare inom egen enhet/grupp Finns möjligheter att begränsa åtkomst eller lösa behovet på annat sätt? Finns alternativa lösningar?
9	Proportionalitetsbedömning – är åtkomsten rimlig?	Är åtkomsten nödvändig i relation till arbetsuppgifter? Kan ett mindre integritetskänsligt alternativ användas? Hur länge behöver åtkomsten gälla?
10	Övriga omständigheter?	Motivera om åtkomsten behöver vara vid.
11	Typ av profil som används idag	

Beslut och dokumentation

Beslut	

Beslutsfattare	
Datum för beslut	
Uppföljning och revidering	

Bilaga B – Riskanalys, en kompletterande och nödvändig del av behörighetsstyrningen

Varför riskanalysen är viktig

Riskanalysen är ett centralt verktyg för att säkerställa att åtkomst till personuppgifter sker på ett säkert, korrekt och rättsligt sätt. Genom att identifiera och värdera risker – såsom obehörig åtkomst eller felaktig behandling – förebygger analysen lagöverträdelser och stärker skyddet för den enskildes integritet. Den uppfyller också kraven i 10 § SoLPuL om styrning, dokumentation och uppföljning av åtkomst. Tillsammans med behovsanalysen utgör den ett nödvändigt beslutsstöd vid behörighetstilldelning.

Riskkategorier och stöd vid analys av över- och underåtkomst

En strukturerad riskanalys ger stöd för att identifiera risker kopplade till både överåtkomst (för bred behörighet) och underåtkomst (för snäv behörighet). Båda kan leda till konsekvenser som påverkar rättssäkerhet, effektivitet och skyddet för personuppgifter. Det kan vara ett stöd att tänka inom ramen för riskkategorier.

Nedan följer exempel som kan hjälpa att identifiera risker.

Exempel på risker vid för snäva behörigheter

- Medarbetare kan inte fullgöra sitt uppdrag korrekt eller i tid.
- Dubbelarbete vid återkommande informationsförfrågningar.
- Felaktiga beslut eller bristande dokumentation på grund av otillräcklig information.
- Otillgänglighetsincidenter i handläggning eller utförande.

Exempel på risker vid för vida behörigheter

• Tillgång till ärenden utanför eget ansvarsområde
Exempel: En utförare ser brukarärenden från annan enhet utan uppdrag.

• Åtkomst till känsliga uppgifter utan koppling till aktuellt uppdrag
Exempel: En administratör ser uppgifter om anhöriga eller tidigare ärenden.

• Obehörig åtkomst till sekretessreglerad dokumentation
Exempel: Enhetschef kan se information utan att omfattas av sekretessbrytande bestämmelser.

- Nyfikenhetsåtkomst och intressekonflikter
  Exempel: Personal läser i journaler om egna barn, grannar eller bekanta.

- Otillåtna ändringar i beslut eller insatser
  Exempel: Medarbetare med bred behörighet ändrar biståndsbeslut utan rätt funktion.

- Komplexitet vid logguppföljning och incidentutredning
  Exempel: Det blir svårt att spåra vem som gjort vad när många har samma åtkomstnivå.

- Regelefterlevnadsrisk och bristande uppgiftsminimering
  Exempel: Bred behörighet bryter mot GDPR:s och SoLPuL:s krav på åtkomstbegränsning.

Riskkategorier – sammanställning

Riskkategori	Beskrivning	Exempel (SoL)
Obehörig åtkomst	Medarbetare får tillgång till information som inte är relevant för deras uppdrag.	En planerare kan läsa journalanteckningar som rör annan enhet eller brukare.
Otillgänglig information	Åtkomsten är för snäv, vilket försvårar uppdragets genomförande.	En biståndshandläggare saknar åtkomst till dokumentation om genomförda insatser.
Felaktig informationsanvändning	Information används i fel sammanhang eller utan rättslig grund.	Personal dokumenterar i fel ärende.
Informationsförlust	Oavsiktlig radering eller förvanskning av information på grund av felaktig behörighet.	En praktikant med bred behörighet raderar anteckningar av misstag.
Dubbelarbete och ineffektivitet	Bristande åtkomst leder till upprepade informationsförfrågningar eller parallell dokumentation.	En utförare kontaktar handläggare upprepade gånger för att få beslut bekräftade.
Fördröjd eller felaktig handläggning	Bristande tillgång till helhetsbild påverkar ärendets kvalitet och rättssäkerhet.	En socialsekreterare saknar beslutsunderlag och behöver begära det manuellt.

Rekommendation för metodstödsarbete

Dessa exempel och kategorier bör användas som stöd i riskanalysens systematik, både i dokumentationsmallar, i workshops och som beslutsunderlag vid behörighetstilldelning. Dessa får gärna kompletteras med andra identifierade kategorier.

Analys och värdering av risk

För varje identifierad risk görs en **bedömning av sannolikhet och konsekvens** enligt riskmatrisen. Riskens allvarlighetsgrad klassificeras och kvantifieras (till exempel försumbar, måttlig, allvarlig eller mycket allvarlig) och **förslag på skyddsåtgärder** dokumenteras i samma matris.

Skyddsåtgärder kan exempelvis innefatta:

- Tidsbegränsning av behörighet

- Begränsning till viss målgrupp eller enhet
- Ändring av behörighet och skapandet av ny roll/profil
- Loggning, behörighetsprofilering eller uppföljning

Stödmaterial för analys och workshop

För att genomföra riskanalysen på ett strukturerat och enhetligt sätt finns särskilt framtagna verktyg som stödjer dokumentation, visualisering och gemensam diskussion. Verktygen syftar till att skapa en gemensam förståelse för risker och att underlätta det praktiska arbetet i organisationen – särskilt när flera funktioner är involverade.

Följande stödmaterial kan användas:

- **Riskmatris (Excel)**
  Innehåller exempel på riskkällor, sannolikhetsnivåer och konsekvenser. Kan anpassas efter aktuell verksamhet eller roll eller analysobjekt och ger stöd för att identifiera, värdera och dokumentera risker på ett konsekvent sätt.
- **Workshoppresentation (PowerPoint)**
  Ett presentationsunderlag som analysledaren kan använda vid genomgång av riskanalysens syfte, metod och hur resultatet kopplas till beslut om behörighet.
- **I workshoppresentationen förklaras också de olika riskvärderingskriterier**

Verktygen är särskilt användbara i samverkan mellan enhetschefer, systemförvaltare, dataskyddsombud och andra nyckelpersoner i behörighetsstyrningen.

Sammanfattning i punktform

- Riskanalysen kompletterar behovsanalysen och fokuserar på konsekvenserna av åtkomst.
- Den hjälper till att bedöma om behörighetstilldelning är proportionerlig utifrån risknivån.
- Riskanalysen utgår från lagkrav, informationens känslighet, sannolikhet och konsekvens.
- Resultatet avgör om föreslagen åtkomst är rimlig eller om särskilda skyddsåtgärder krävs.
- Riskanalys är en förutsättning för att kunna motivera, spåra och följa upp beslut om åtkomst i socialtjänsten.

Framåtblickande aspekter att beakta för vidareutveckling av metodstödet

För att säkerställa ett långsiktigt hållbart, rättssäkert och verksamhetsnära arbete med behörighetstilldelning bör följande områden beaktas i den fortsatta utvecklingen av metodstödet:

- **Tydliga roller och ansvar:** Säkerställ att det finns utpekade funktioner med tydliga mandat – till exempel behörighetsansvarig chef, systemägare, dataskyddskontakt – som gemensamt ansvarar för att analysen genomförs, dokumenteras och följs upp.
- **Beslutsstruktur och undantagshantering:** Inför en beslutsmodell för behörighetstilldelning (ordinarie vs tillfällig/undantag) med krav på dokumentation, motivering och uppföljning – särskilt vid avsteg från standardprofil.
- **Kompetens och stödmaterial:** Utveckla kort utbildningsstöd (t.ex. presentation eller lathund) för chefer och systemförvaltare. Använd workshopmallar och riskmatriser för att underlätta samverkan.
- **Regelbunden uppföljning och kontroll:** Integrera behovs- och riskanalysen i rutiner för årlig översyn, logguppföljning och intern kontroll, enligt SoLPuL och GDPR:s ansvarsskyldighet.
- **Samordning och långsiktig förvaltning:** Utse en förvaltningsansvarig (funktion, inte person) för metodstödet som ansvarar för revidering, versionshantering och bevakning av förändringar i regelverk eller system.