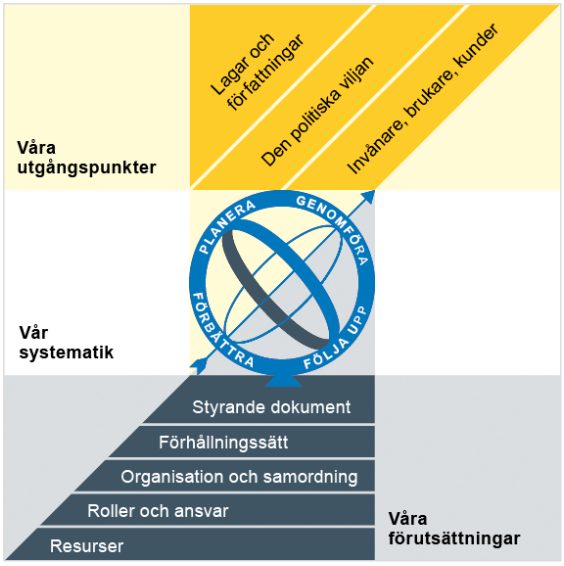
Göteborgs Stad

Förvaltningen för funktionsstöds anvisning för behörighetstilldelning och åtkomstkontroll

Reglerande styrande dokument

- Policy
- Riktlinje
- Regel
- ► **Anvisning**
- Rutin
- Instruktion

Göteborgs Stads styrsystem



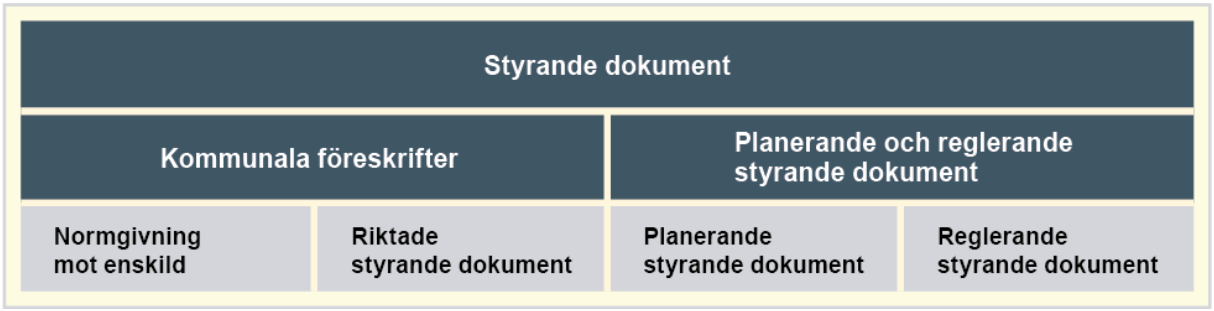
Utgångspunkterna för styrningen av Göteborgs Stad är lagar och författningar, den politiska viljan och stadens invånare, brukare och kunder. För att förverkliga utgångspunkterna behövs förutsättningar av olika slag. Stadens politiker har möjlighet att genom styrande dokument beskriva hur de vill realisera den politiska viljan. Inom Göteborgs Stad gäller de styrande dokument som antas av kommunfullmäktige och kommunstyrelsen. Därutöver fastställer nämnder och bolagsstyrelser egna styrande dokument för sin egen verksamhet. Kommunfullmäktiges budget är det övergripande och överordnade styrande dokumentet för Göteborgs Stads nämnder och bolagsstyrelser.

Om Göteborgs Stads styrande dokument

Göteborgs Stads styrande dokument är våra förutsättningar för att vi ska göra rätt saker på rätt sätt. De anger vad nämnder/styrelser och förvaltningar/bolag ska göra, vem som ska göra det och hur det ska göras. Styrande dokument är samlingsbegreppet för dessa dokument.

Stadens grundläggande principer såsom demokratisk grundsyn, principer om mänskliga rättigheter och icke-diskriminering omsätts i praktisk verksamhet genom att de integreras i stadens ordinarie beslutsprocesser. Beredning av och beslut om styrande dokument har en stor betydelse för förverkligandet av dessa principer i stadens verksamheter.

De styrande dokumenten ska göra det tydligt både för organisationen och för invånare, brukare, kunder, leverantörer, samarbetspartners och andra intressenter vad som förväntas av förvaltningar och bolag. De styrande dokumenten ligger till grund för att utkräva ansvar när vi inte arbetar i enlighet med vad som är beslutat.



Beslutad av:	**Gäller för:**	**Diarienummer:**	**Datum och paragraf för beslutet:**
AC Kvalitet och styrning	Förvaltningen för funktionsstöd		
Dokumentsort:	**Giltighetstid:**	**Senast reviderad:**	**Dokumentansvarig:**
Anvisning	Tills vidare	2025-05-09	Utvecklingsledare informationssäkerhet/dataskydd

Bilagor:
Checklista chef behörighetstilldelning och åtkomstkontroll

Innehåll

Inledning

Syftet med denna anvisning

Området behörighetstilldelning och åtkomstkontroll regleras av ett flertal lagar, förordningar och styrdokument. Anvisningen syftar till att ge en samlad bild av det som reglerar området, beskriva ansvar och roller samt vara ett stöd för de som ska ta fram liknande rutiner för olika IT-stöd.

Anvisningen omfattar lägsta nivå avseende:

- villkor för tilldelning av behörigheter till IT-system och lagringsytor som hanterar personuppgifter eller annan värdefull information och
- kontroller av tilldelade behörigheter och åtkomst till personuppgifter eller annan skyddsvärd information i IT-system och lagringsytor.

Målsättningen är att nå hög kvalitet och effektivitet genom att vår information hanteras på ett korrekt sätt av medarbetare, processer och teknik. Ett ändamålsenligt skydd av information som värnar om enskildas integritet bevarar förtroende och möjliggör en hållbar digitalisering.

Anvisningen utgår från Göteborgs Stads riktlinje för informationssäkerhet. Informationssystem används i anvisningen synonymt med IT-system.

Anvisningen ersätter *Generell rutin för IT-behörigheter inom FFS*, *Rutin för behörighetskontroller* samt *Rutin för felaktig användning av behörigheter*.

Vem omfattas av anvisningen

Denna anvisning gäller för samtliga medarbetare inom förvaltningen för funktionsstöd.

Bakgrund

Nämnden för funktionsstöd är både personuppgiftsansvarig och informationsägare. Som personuppgiftsansvarig ansvarar nämnden för att behandling av personuppgifter sker i enlighet med gällande lagar och regler.

Som informationsägare har nämnden en skyldighet att skydda informationen i verksamheten så det enbart är de som är behöriga som får ta del av den (**konfidentialitet),** att det går att lita på att den är korrekt och inte har blivit förstörd eller borttagen (**riktighet**) och att den alltid finns tillgänglig när den behövs (**tillgänglighet).**

I ansvaret ingår att införa säkerhetstekniska åtgärder och lösningar, men även organisatoriska åtgärder. Med organisatoriska åtgärder avses bland annat styrande dokument för verksamhetens behandling av personuppgifter. Styrningen av behörigheter och åtkomst till personuppgifter är en grundläggande säkerhetsåtgärd.

Behörighetsstyrningen säkerställer att medarbetare endast har tillgång till de uppgifter som de behöver för att utföra sitt arbete och att obehöriga inte får åtkomst. Finns det

många användare, stora volymer med personuppgifter, känslig information eller integritetskänsliga personuppgifter i ett system så ökar kraven på adekvat behörighetsstyrning.

Rättslig reglering

Behörigheter till förvaltningens IT-system eller lagringsytor som innehåller personuppgifter regleras av ett flertal lagar och förordningar. En av de grundläggande principerna i artikel 5 i EU:s dataskyddsförordning[1] anger att personuppgiftsansvariga ska säkerställa lämplig säkerhet för personuppgifterna. Det omfattar skydd mot obehörig eller otillåten behandling. För att skydda uppgifter från obehörig åtkomst, från såväl egna medarbetare som externa parter, krävs ett systematiskt arbetssätt och att verksamheterna vidtar säkerhetsåtgärder.

Det är viktigt att veta vilken lagstiftning som gäller för att vad man får/ska göra. Utöver EU:s dataskyddsförordning och dataskyddslagen[2] finns det andra lagbestämmelser som reglerar användningen/hanteringen av uppgifter om enskilda inom IT-systemen. För nämndens verksamhetsområde finns det reglerat i såväl socialtjänstlagen (2001:453), förkortad SoL som lagen (1993:387) om stöd och service till vissa funktionshindrade, förkortad LSS, att handlingar som rör enskildas personliga förhållanden ska förvaras så att obehöriga inte får tillgång till dem. Bestämmelserna innebär att obehöriga inte ska få tillgång till integritetskänslig information och att en anställd inte ska ges åtkomst till information i vidare omfattning än vad den anställde behöver för sitt arbete.

Behandlingen av personuppgifter är även reglerat i lag (2001:454) om behandling av personuppgifter inom socialtjänsten, förkortad SolPuL och i förordning (2001:637) om behandling av personuppgifter inom socialtjänsten, förkortad SoLPuF. Enligt 10 § SoLPuL ska den personuppgiftsansvarige bestämma villkor för tilldelning av åtkomst till uppgifter som förs helt eller delvis automatiserat, skapa förutsättningar för kontroll av åtkomst till sådana uppgifter och kontrollera obehörig åtkomst systematiserat och återkommande. Det innebär att:

• det ska finnas villkor för tilldelning av behörighet för åtkomst

• all åtkomst till uppgifter om enskilda ska dokumenteras och ska kunna kontrolleras

• systematiska och återkommande kontroller ska genomföras

• behörigheten ska begränsas till det som var och en behöver för att kunna fullgöra sina arbetsuppgifter inom socialtjänsten.

SoLPuL syftar till att den verksamhetsansvarige ska göra aktiva och individuella behörighetstilldelningar utifrån analyser av vilken information olika personalkategorier och olika verksamheter behöver (behovsanalys). Användarna behöver tilldelas rätt behörigheter, det vill säga tillräcklig behörighet, för att kunna utföra sina arbetsuppgifter på ett säkert sätt utan att behörigheten blir mer omfattande än vad som behövs.

[1]Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (dataskyddsförordningen).
[2] Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning

Oavsett om SoLPuL eller SoLPuF är tillämpliga ska personuppgiftsbehandlingen följa de grundläggande principerna och kraven i dataskyddsförordningen. Det innebär bland annat att se till att behandlingen har en rättslig grund och att informera de registrerade om hur deras personuppgifter hanteras.

All behandling av personuppgifter ska ske utifrån sex grundläggande principer. Det innebär till exempel att uppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (integritet och konfidentialitet). Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den enskilde.

Skyddade personuppgifter

Skyddade personuppgifter är benämningen för skyddsåtgärderna fingerade personuppgifter, skyddad folkbokföring och sekretessmarkering. Gemensamt för skyddsåtgärderna är att den enskilde lever med någon form av hotbild och att skyddet ska förhindra att uppgifter om den enskilde sprids. För verksamheter som hanterar skyddade personuppgifter ställs krav på särskilda rutiner i enlighet med sekretessbestämmelser i Offentlighets- och sekretesslagen (2009:400), OSL.

För att minska risken för spridning och att skyddade personuppgifter röjs ska behörighetstilldelningen i system som hanterar sådana uppgifter ske restriktivt. Detta då risken för röjning minskar om färre personer kan ta del av uppgifterna.

Hanteringen av skyddade personuppgifter ska loggas i respektive system. Detta möjliggör åtkomstkontroll och säkerställer att verksamheten kan spåra vem som tagit del av skyddade personuppgifter.

Ledningssystem för systematiskt kvalitetsarbete

Enligt Socialstyrelsens föreskrifter och allmänna råd om ledningssystem för systematiskt kvalitetsarbete (SOSFS 2011:9) så innebär kvalitet:

”att en verksamhet uppfyller de krav och mål som gäller för verksamheten enligt lagar och andra föreskrifter om hälso-och sjukvård, socialtjänst och stöd och service till vissa funktionshindrade och beslut som har med stöd av sådana förskrifter”.

Lagstiftningen anger exempelvis att obehöriga inte ska få tillgång till integritetskänslig information och att en anställd inte ska ges åtkomst till personakter med mera i vidare omfattning än vad hon eller han behöver för sitt arbete. Det gäller såväl fysiskt personakter som digitala. Om verksamheterna inte följer lagstiftningen så betyder det att det finns brister i kvalitet som också måste åtgärdas och följas upp.

Systematiskt förbättringsarbete

Risker

Om det finns risk för att händelser skulle kunna inträffa som medför brister i verksamhetens kvalitet så ska riskerna bedömas och åtgärdas. Det avser även risker för att

medarbetare exempelvis går in och dokumenterar i fel journal eller om obehöriga får tillgång till uppgifter som rör enskildas personliga förhållande.

Egenkontroll

Genom egenkontroller genomför verksamheterna en systematisk uppföljning och utvärdering av den egna verksamheten samt kontroll av att verksamheten bedrivs i enlighet med de processer och rutiner som finns i ledningssystemet. Egenkontrollen görs med den frekvens och omfattning som krävs för att säkra verksamhetens kvalitet. Åtkomstkontroller kan även vara en del av beslutad egenkontroll.

Avvikelser

Alla som arbetar inom socialtjänsten har en skyldighet att rapportera avvikelser[3]. Avvikelsehantering[4] omfattar även att rapportera brister i sekretess som kan uppstå om en medarbetare skickar post (digital som analog) till fel person, om en medarbetare obehörigt tar del av uppgifter eller har en för vid/felaktig behörighet. Det kan vidare vara avvikelser kopplat till brister i dokumentation som till exempel att en medarbetare dokumenterar i fel journal. Obehörig tillgång, att en medarbetare skriver i fel journal eller att ett brev skickas till fel mottagare kan med andra ord vara både en avvikelse och en personuppgiftsincident.

Koppling till andra styrande dokument

Styrande dokument	Koppling till denna anvisning
Säkerhetspolicy för Göteborgs Stad Göteborgs Stads riktlinje för informationssäkerhet	Riktlinjen konkretiserar säkerhetspolicyn och anvisningen konkretiserar delar av riktlinjen.
Göteborgs Stads riktlinje för styrning, samordning och finansiering av digital utveckling och förvaltning	Riktlinjen beskriver vissa nämnders ansvar som leverantör för stadengemensamma digitala tjänster och samordning av nationella digitala tjänster och standarder.
Göteborgs Stads regel för IT-användare	Under 2024 återremitterades reviderat styrdokumentet för att ytterligare utredas.

[3] Händelse som medfört eller som hade kunnat medföra något oönskat. En avvikelse är antingen en negativ händelse eller ett tillbud (Socialstyrelsens termbank).
[4] Identifiera och rapportera avvikelser, kartlägga och åtgärda orsakerna, dokumentera detta samt bedöma åtgärdernas effekt och sammanställa och återföra resultaten (Socialstyrelsens termbank).

Ordlista

Begrepp	Definition
Autentisering	Verifiering av att en användare är den person den påstår sig vara.
Behörighet	Tilldelade rättigheter att använda en informationstillgång på ett specifikt sätt.
Behörighetshantering	Arbete med att säkerställa att endast behöriga användare och informationssystem har åtkomst till IT-miljön. Behörighetshanteringen ska utformas på ett sådant sätt att varje digital identitet inte har mer åtkomst till information och informationssystem än vad den behöver (MSB[5]).
Behörighetskontroll	Kontroll för att säkerställa att det endast är de personer som ska ha (rättighet) tillgång, som har det (MSB).
Fysiskt skydd	Säkerhetsåtgärder relaterade till skydd av personer, lokaler och utrustning av betydelse för informationssäkerheten.
Hot	Något som orsakar, eller bidrar till att orsaka, att en oönskad händelse inträffar.
Incident	En inträffad oönskad händelse.
Information	Innebörd av data. I strikt mening är det skillnad mellan data och information. Data blir information när någon har tolkat innebörden av den. Vid till exempel överföring mellan datorer och lagring i datorminnen är det data, inte information, som hanteras (MSB).
Informationssystem/IT-system	System för att samla in, lagra, bearbeta och distribuera information för ett givet ändamål (MSB). Innefattar såväl ett systems tekniska utrustning som dess mänskliga aktiviteter och rutiner.
Informationsägare	Den nämnd/styrelse som ansvarar för den information som skapas och hanteras. Ansvaret för informationen och dess säkerhet följer med ansvaret för verksamheten.
IT-säkerhet	Del av informationssäkerhet som är avgränsad till IT-resurser.
Risk	En möjlig oönskad händelse.
Spårbarhet	Möjlighet att kunna härleda utförda aktiviteter i systemet till en identifierad användare.
Systemägare	Den som har ett överordnat ansvar för administration, drift och säkerhet för ett system. Ett system kan innehålla information som tillhör en eller flera informationsägare.
Sårbarhet	Brist i skyddet av en tillgång eller av en säkerhetsåtgärd som kan utnyttjas av ett eller flera hot (MSB).
Åtkomst	Interaktion mellan en användare och en resurs som resulterar i överföring av information dem emellan eller utnyttjande av resurser (MSB).
Åtkomstkontroll	Inbegriper sådana funktioner som syftar till att reglera och kontrollera en användares åtkomst till information och resurser. Detta avser således både behörighetsstyrning (tilldelning, återkallande och hantering av behörigheter och motsvarande) samt uppföljning av åtkomst till information och resurser, till exempel genom loggar och andra hjälpmedel. (SOU 2024:18[6])

[5] Källa: Myndigheten för samhällsskydd och beredskap (MSB)

[6] Nya regler om cybersäkerhet. Statens offentliga utredningar.

Anvisning

Det är skillnad på behörighet och åtkomst. Den som har teknisk möjlighet, det vill säga åtkomst att kunna titta på en uppgift, är per automatik inte behörig att ta del av uppgiften.

Inom socialtjänsten påverkar den **inre sekretessen** hur medarbetare får ta del av uppgifter om enskilda inom sin förvaltning. Den inre sekretessen utgår från att medarbetare endast får ta del av uppgifter i den utsträckning som behövs för att medarbetaren ska kunna utföra sina arbetsuppgifter. Det är med andra ord endast den personal som behöver uppgifterna i sitt arbete som får ta del av dem[7].

En kontroll av behörighet innebär även en kontroll av åtkomst och därför kan i vissa fall båda begreppen förekomma.

Villkor för behörighetstilldelning

Nedan anges lägsta nivå avseende villkoren för behörighetstilldelning, tekniska och organisatoriska säkerhetsåtgärder. För vissa roller finns det i denna anvisning ytterligare uppställda villkor som måste säkerställas, läs mer under rubriken ansvar och roller.

Åtkomst och behörigheter

- Åtkomst och behörighet till information ska ges restriktivt utifrån arbetsuppgifter och organisatorisk tillhörighet. Det är inte tillåtet att ge personal inom socialtjänsten tillgång till all information i IT-system utan behörigheten ska baseras på det behov som varje yrkeskategori och användare har i respektive verksamhet.
- Varje användare i ett IT-system eller lagringsyta (med personuppgifter eller skyddsvärd information) ska tilldelas en individuell behörighet kopplad till en personlig användaridentitet som är spårbar till en fysisk person.
- Tilldelning och användning av så kallade privilegierade åtkomsträttigheter (exempelvis administratörsrättigheter) ska begränsas och kontrolleras.
- Åtkomst till personuppgifter som behandlas helt eller delvis automatiserat via öppna nät eller molntjänst ska ske genom så kallad stark autentisering. Åtkomstkontroller ska göras.
- All åtkomst till uppgifter om enskilda ska dokumenteras och kunna kontrolleras. Det gäller både den egna personalens åtkomst och den åtkomst som bereds andra.
- Behörigheter ska kunna ändras vid behov. Det ska finnas rutiner för att ändra, ta bort och regelbundet följa upp behörigheter. Vid byte eller förändring av tjänst ska behörigheter och åtkomst till information ses över.

Tekniska säkerhetsåtgärder

[7] Socialstyrelsens Kunskapsstöd och regler, Ta del av uppgifter inom socialtjänst – sekretess. För socialtjänsten. www.socialstyrelsen.se

- I ett system ska det finnas olika behörighetsnivåer och skikt för att begränsa åtkomst. Det ska finnas tekniska begränsningar för att säkerställa att den som inte har behörighet inte heller har teknisk möjlighet att få åtkomst.
- Till varje IT-system ska det finnas en behörighetsstruktur som är kartlagd och dokumenterad. Sker förändringar och modifieringar ska behörighetsstrukturen uppdateras och förändringen dokumenteras. Dokumentation av behörighets-strukturen är viktig för att möjliggöra en översikt av uppsättningen i systemet och förenklar processen att lära upp nya behörighetsansvariga eller göra kontroller.
- Samtliga ändringar som görs i behörighetsstrukturen föregås av ett formellt godkännande från behörighetsansvarig.
- Finns det särskilda profiler/filter som inte längre används så ska de tas bort eller inaktiveras.

Organisatoriska säkerhetsåtgärder:

- Varje IT-system ska ha en **rutin** för behörighetstilldelning och kontroll av behörigheter och åtkomst. I rutinen ska det framgå hur processen med behörighetstilldelning går till, ansvar och roller, dokumentation, kontroll och spårbarhet samt hur avvikelser och incidenter ska hanteras.
- Varje IT-system ska ha en årlig kontrollplan. I kontrollplanen ska det framgå vilka kontroller som ska göras, när och hur ofta kontroller ska ske.
- Det ska finnas rutin för åtkomst till **skyddade** personuppgifter där det särskilt framgår vilka säkerhetsåtgärder som införts för att minimera risk för röjande av de skyddade personuppgifterna.
- Behovs- och riskanalyser ska ligga till grund för behörighetstilldelning och de behörighetsprofiler som används inom socialtjänsten. Verksamhetskunskap är nödvändig för att kunna göra en analys av roll- och behörighetstilldelning.

Behovs- och riskanalys

Behovs- och riskanalysen hjälper till med att ta reda på vem som behöver åtkomst, vilka uppgifter som åtkomstmöjligheten ska omfatta, vid vilka tidpunkter och i vilka situationer eller processer som åtkomsten behövs. Samtidigt analyseras de risker en för vid behörighet kan få för den enskildes fri- och rättigheter. Analysen bör också svara på om det finns risker med att **inte** tilldela behörigheten. Ju högre risk desto fler skyddsåtgärder.

Faktorer som bör beaktas vid bedömning av risken är om det rör sig om:

- personuppgifter som omfattas av sekretess,
- känsliga personuppgifter,
- extra skyddsvärda personuppgifter,
- om det sker behandling av personuppgifter rörande sårbara fysiska personer eller personer i beroendeställning, framför allt barn,
- behandling som omfattar ett stort antal personuppgifter eller gäller ett stort antal registrerade samt
- skyddade personuppgifter.

Ansvar och roller

Inom Staden finns ett stort antal gemensamma system och IT-tjänster. Det innebär en hög grad av standardisering för att säkerställa en grundläggande säkerhetsnivå. Det påverkar utformning av behörigheter och behörighetsstrukturer samt i vilken utsträckning individuella anpassningar kan göras utifrån förvaltningens behov/krav.

Systemägaren/IT-leverantören

Systemägaren är den som har ett överordnat ansvar för administration, drift och säkerhet för ett system. Ett system kan innehålla information som tillhör en eller flera informationsägare.

I nämndens verksamhetsansvar ingår bland annat att säkerställa att tillämpliga lagar, föreskrifter, styrande dokument och beslut följs samt att skyddsbehov och accepterad risk- och säkerhetsnivå uppfylls. Detta gäller oavsett om verksamhetens göromål och/eller information hanteras av en underleverantör, är verksamhetsspecifik eller är en stadengemensam tjänst.

Stadengemensamma digitala system och tjänster

Nämnder med särskilt ansvar för **Stadengemensamma** digitala bas-, tilläggs-, och specialisttjänster (nedan benämnd systemägare/leverantör av stadengemensamma system):

- Nämnden för **Intraservice**,
- Nämnden för **Demokrati- och medborgarservice** och
- **Inköps- och upphandlingsnämnden**.

Exempel på gemensamma system: Personec, Proceedo, Lotus Notes (diarium, verksamhetshandbok och databaser) /Ciceron DoÄ, Microsoft 365 (Outlook, Word, SharePoint osv.).

Leverantör av stadengemensamma system ska till exempel se till att IT-systemen minst uppfyller stadens grundsäkerhetsnivå, se Göteborgs Stads riktlinje för informationssäkerhet. Leverantören ansvarar för att löpande följa upp väsentliga störningar och brister avseende säkerhet. Leverantören ansvarar även för att informationsägarens säkerhetskrav på behörighetskontroller uppfylls tekniskt samt att loggar säkerhetskopieras, sparas och förvaras säkert.

Nämnden för Intraservice ansvarar för förvaltning och utveckling av Stadens gemensamma infrastruktur samt att det finns ramverk att tillämpa för detta. Det gäller även de verksamhetsspecifika IT-systemen.

Verksamhetsspecifika system och tjänster

För verksamhetsspecifika system och tjänster ansvarar respektive nämnd för att säkerställa en effektiv förvaltning, liksom utveckling som stödjer beslutade mål. Exempel på verksamhetsspecifika system: Treserva och Plugo (Epsilon).

- Samtliga sex socialförvaltningar ingår i samarbetet Integrerad Digitalisering (ID) som syftar till att gemensamt utveckla och förvalta digitala verktyg. Inom ramen för ID finns en operativ samordningsgrupp (OS).

- Det finns en överenskommelse med Socialförvaltning Nordost avseende systemförvaltning av de sex socialförvaltningarnas gemensamma verksamhetsspecifika system. SF Nordost är systemförvaltare via enheten Tjänsteförvaltning integrerad digitalisering (TID).
- TID är systemförvaltare medan Intraservice är förvaltare av Stadens IT-infrastruktur och kan då ses som leverantör.

Processägare

Ansvaret för en säker och korrekt informationshantering följer verksamhetsansvaret. All informationshantering i förvaltningen har en ansvarig chef. Den chef som ansvarar för en process kallas processägaren. Processägaren beslutar om vilka digitala verktyg som ska användas i sin process och hur informationen får hanteras samt ska skyddas.

Avdelningschef ansvarar för medarbetare, processer och teknik inom sitt ansvarsområde. Ett IT-system är ett stöd i en process och varje system ska ha en ansvarig avdelningschef som processägare. Vem som är processägare ska dokumenteras i förvaltningens systemförteckning.

Vid implementering av ett nytt system, där en stor mängd personuppgifter ska behandlas eller där det finns väsentliga risker kopplade till en personuppgiftsbehandling på en lagringsyta, ska nedan vara på plats innan systemet tas i bruk/personuppgiftsbehandlingen startar. Vissa delar behöver tas fram i samverkan med systemägaren/IT-leverantören.

Processägaren ska för sitt IT-system/lagringsyta säkerställa att det finns

- en dokumenterad behörighetsstruktur,
- ett gemensamt arbetssätt och ramverk för behörighetstilldelning och behörighets- och åtkomstkontroll. I behörighetstilldelning ingår arbetssätt för registrering och avregistrering av behörigheter,
- rutin för behörighetstilldelning som är baserade på de villkor för behörighetstilldelning som finns i denna anvisning,
- rutin för kontroll av behörigheter. Kontrollerna ska vara systematiska och återkommande. Rutinen ska beskriva hur kontrollerna ska göras, omfattning, frekvens och vad som ska kontrolleras. I rutinen ska det även framgå hur avvikelser ska hanteras och åtgärdas. Personuppgiftsincidenter hanteras enligt rutin för personuppgiftsincidenter.
- en årlig kontrollplan som beskriver vilka kontroller som ska genomföras under året,
- utsedda kontrollanter för systemet,
- uppföljning av att kontrollerna blir utförda och signerade på ytan för *Internkontroll* för avsett år.
- uppföljning av risker och avvikelser samt åtgärder avseende behörigheter.
- säkerhetsåtgärder för lämpligt skydd av personuppgifter i IT-systemet/lagringsytan både vid införande/förändring och för att hantera avvikelser samt incidenter. Detta sker i samverkan med systemägaren och dataskyddskontakt.
- adekvat och korrekt information till användare i IT-systemet om behörigheter, åtkomst och åtkomstkontroll.

Behörighetsbeställare (följer verksamhetsansvaret)

Det är vanligtvis en chef som beställer behörigheter till medarbetare.

Beställaren behöver följa de regler/rutin som finns kring behörighetstilldelning för det system/lagringsyta som beställningen avser. Nedan frågor är några av de frågor som kan vara viktiga att besvara innan beställningen, se också mall för behov och riskanalys:

- Vilken roll/befattning har de som ska behörigheten?
- Finns några särskilda regler eller rutiner för det aktuella IT-systemet?
- Ger behörigheten några särskilda befogenheter (ex för ekonomi eller administratörsbefogenheter), tillgång till integritetskänslig eller sekretessmarkerad information?
- Krävs behörigheter till fler enheter eller områden än de som är kopplade till rollen/profilen?
- Är du som beställare ansvarig för den verksamhet som behörigheten avser? Om nej, då behöver ansvarig chef göra beställning.

Beställaren ansvarar för att:

- Beställa rätt behörighet så att användaren kommer åt de uppgifter som behövs för att kunna utföra arbetet.
- Omedelbart anmäla till behörighetsadministrationen när en behörighet ska tas bort vid avslut av tjänst eller anpassas till förändrade arbetsuppgifter.
- Genomföra kontroller tillsammans med utsedd behörighetskontrollant.
- Konton med personlig inloggning till externa (utanför Staden) system/appar avslutas när medarbetaren ej längre ska ha inloggning.
- Utreda avvikelser och rapportera incidenter enligt rutin.

Arbetet med systematisk informationssäkerhet följer verksamhetsansvaret och ansvarig chef ska se till att:

- användaren utbildas och får en förståelse om gällande regelverk och säkerhetsrutiner innan användare ges behörighet,
- medarbetare har behörigheter utifrån angivna arbetsuppgifter,
- meddela förändringar samt borttag av behörigheter i IT-system och
- åtgärda brister som framkommer i samband med åtkomstkontroller.

Behörighetsadministration

De som tilldelar behörigheter är ofta systemadministratör, lokalt verksamhetsstöd eller annan administrativ funktion. Behörighetsadministrationen i lagringsytan I: utförs av förvaltningens IT-avdelning.

Behörighetstilldelaren ansvarar för att:

- Säkerställa att villkor för behörighetstilldelning efterlevs.
- Följa rutiner för behörighetstilldelning
- Följa behörighetsstruktur och de instruktioner som tagits fram med hjälp av behovs- och riskanalys.
- Rapportera och dokumentera risker, avvikelser och incidenter avseende behörigheter i enlighet med rutin.

- Implementera framtagna säkerhetsåtgärder.
- Delta i arbetet med att ta fram arbetssätt för regelbunden kontroll av behörigheter.
- Informera beställare av behörigheter om den rutin för behörighetstilldelning som ska finnas för varje IT-system så att beställaren kan säkerställa att användaren har fått adekvat information om de skyldigheter användaren har i förhållande till IT-systemet. Rutin för behörighetstilldelning och kontroll av behörigheter ska även omfatta beställarens skyldigheter.
- I behörighetstilldelningen ingår att anpassa och avsluta behörigheter när medarbetare byter arbetsuppgifter och roll inom organisationen eller slutar.

Behörighetskontrollant

Utsedda behörighetskontrollanter är vanligtvis de som är lokalt verksamhetsstöd för ett verksamhetssystem som exempelvis Treserva, ekonomisystem med flera.

Kontroller och uppföljning genomförs av utsedda kontrollanter och berörda chefer. Överordnad chef kontrollerar underordnad chef. Behörighetskontrollant ansvarar för att:

- Utföra kontroller enligt den plan och rutin som tagits fram för systemet.
- Dokumentera kontrollerna utifrån systemets rutin. Det ska framgå vem som utfört kontrollen, när den utförts och vad som har kontrollerats.
- Rapportera avvikelser till ansvarig chef och incidenter enligt rutin.
- Signera i systemförteckningslistan att kontroller har utförts varje kvartal.

Användare

Användare ansvarar för att:

- Ta del av information och de rutiner som tagits fram för respektive IT-system/lagringsyta samt meddela om det finns behov av mer utbildning.
- Användare ska följa de rutiner och regler som gäller för IT-användare.
- Användare ska omgående rapportera avvikelser, incidenter (se genväg Anmäl personuppgiftsincident på Digitala navet) eller misstänkta incidenter i IT-system till funktionsbrevlådan för informationssäkerhet samt till sin chef. Det gäller såväl utifrån ett systemsäkerhetsperspektiv som för skydd av registrerades personuppgifter.
- Användare ska omgående påtala för sin chef om behörigheten inte motsvarar det faktiska behovet av tillgång till uppgifter.
- Avsluta konton och inloggningar till externa system/appar.
- Användare ska omgående anmäla om det finns misstanke om inloggningsuppgifter läckt ut eller blivit kapade.

Behörighets- och åtkomstkontroller

Vissa åtkomstkontroller är inbyggda i system eller lagringsyta. Det kan till exempel vara att någon form av verifiering av en användares uppgivna identitet som autentisering (e-tjänstekort, bankid) eller lösenord. SITHS-kort är ett e-tjänstekort.

Kontroller ska göras för att säkerställa att medarbetare inte använder sina behörigheter för att läsa, ändra eller ta bort information som de inte ska hantera.

Loggkontroller får inte användas som arbets- eller prestationsmätning som kan medföra risk för intrång i medarbetares personliga integritet.

Olika typer av kontroller

- *Systematiska behörighetskontroller.* Kontroller som sker regelbundet för att se om användare har rätt att ta del av uppgifterna i ett system eller lagringsyta. Det kan ske genom att kontrollera om användaren fortfarande är anställd eller har arbetsuppgifter som motsvarar behörigheten. En medarbetare som är tjänstledig eller utlånad ska inte heller ha åtkomst. Tillfälliga åtkomsträttighet kan också kontrolleras. Regelbundna kontroller kan till exempel vara åtkomstkontroller där samtliga användare kontrolleras med viss intervall.
- *Systematiska stickprovskontroller*. Loggkontroller för att säkerställa att medarbetaren inte tagit del av uppgifter som hen inte är behörig till. Stickprovskontroller kan vara att ett antal slumpvist utvalda journaler eller medarbetare kontrolleras varje kvartal.
- *Loggkontroll vid misstanke om missbruk av behörighet.* Det kan vara vid avvikelser, misstanke om dataintrång eller om något ärende aktualiserats med en känd person eller kollega.

Kontroller kan göras av:

- Åtkomst till viss uppgift om enskild.
- Särskild händelse. Kan till exempel vara på initiativ från en enskild.
- Lokalt känd person. Kan vara åtkomst till uppgifter om kända och närstående personer eller kollegor och deras närstående.
- Om det skett åtkomst ett stort antal gånger.
- Om det skett åtkomst på för verksamheten ovanliga tider, exempel på natten eller på helger.
- Åtkomst till skyddade personuppgifter.
- Åtkomst till uppgift för barn.
- Vid avvikelser eller incidenter. Det kan till exempel vara vid felaktig dokumentation eller misstanke om dataintrång.

Rutin för behörighets- och åtkomstkontroller i IT-system

För varje IT-system ska det finnas en rutin som beskriver hur, när och med vilken frekvens och omfattning kontroller ska genomföras samt typ av kontroll.

Rutinen bör ange att det ska göras en riskanalys och att antalet kontroller bedöms utifrån identifierade risker, tidigare avvikelser och personuppgiftsincidenter, verksamhetens omfattning, antalet personer med åtkomst, modellen för behörighetstilldelning och vilken information som finns i systemet.

Hur många kontroller och vilka typer av kontroller beror också på vilken typ av information som finns i systemet och vad konsekvenserna kan bli av obehörig åtkomst eller radering av uppgifter.

Information i systemet utifrån klassning[8] och konsekvensnivåer
Allvarlig skada hög skyddsnivå, klass 3 (viktig, kritisk, känslig information) **Konfidentialitet:** Obehörig åtkomst medför mycket allvarlig skada för verksamheten och mycket allvarlig negativ påverkan på enskild individs rättigheter. **Riktighet:** Oriktig, ofullständig information i systemet medför omfattande skada för verksamheten och mycket allvarlig negativ påverkan på enskild individs rättigheter eller hälsa. **Tillgänglighet:** Verksamheterna har stora svårigheter att fullgöra en eller flera av sina primära uppgifter om informationen i IT-systemet är otillgänglig. Mycket allvarlig negativ påverkan på enskild individs rättigheter eller hälsa. ***Klass 3 information kan i vissa fall vara:*** - skyddade och känsliga personuppgifter, - sekretessklassade uppgifter enligt OSL[9] - Patientdata som till exempel ordination (säkerhetsaspekt riktighet)
Betydande skada– utökad skyddsnivå, klass 2 **Konfidentialitet:** Obehörig åtkomst medför betydande skada för verksamheten och betydande negativ påverkan på den enskildes rättigheter **Tillgänglighet:** om informationen i IT-systemet är otillgänglig kan det innebära att verksamheterna kan fullfölja primära uppgifter men med kraftigt påverkad effektivitet med betydande negativ påverkan på den enskildes rättigheter eller hälsa. **Riktighet:** Oriktig, ofullständig information i systemet medför betydande skada för verksamheten och betydande negativ påverkan på den enskildes rättigheter eller hälsa. ***Klass 2 information kan i vissa fall vara:*** Personuppgifter (ej känsliga eller skyddade, vilket är klass 3), sekretessklassade uppgifter enligt OSL
Måttlig skada - grundläggande skyddsnivå 1 **Konfidentialitet:** Obehörig åtkomst medför måttlig skada för verksamheten och enskilda **Tillgänglighet:** innebär att verksamheterna kan fullfölja primära uppgifter men med något reducerad effektivitet. Kan få en begränsad negativ påverkan på den enskildes rättigheter eller hälsa. **Riktighet:** Oriktig information medför betydande skada för verksamheten och betydande negativ påverkan på den enskildes rättigheter eller hälsa. ***Klass 1 information kan i vissa fall vara:*** arbetshandlingar, information avsedd för internt bruk, allmänna offentliga handlingar, uppgifter som inte är skyddsvärd och innehåller enstaka enskilda personuppgifter av ej känslig karaktär.
Försumbar skada – ingen skyddsnivå 0 **Konfidentialitet:** Obehörig åtkomst medför ingen skada för verksamheten eller enskild **Tillgänglighet:** information där förlust av tillgänglighet inte medför negativ skada för verksamheten eller enskild **Riktighet:** information där förlust av riktighet inte medför negativ skada för verksamheten eller enskild

[8] Riktlinje för informationssäkerhet - Bilagor Göteborgs Stads klassificeringsmodell och beskrivning av konsekvensnivåer

[9] Offentlighets- och sekretesslag (2009:400)

Ansvar för att genomföra kontroller och åtgärda avvikelser/incidenter

Kontroller och uppföljning genomförs av utsedd kontrollant och berörd chef. Överordnad chef kontrollerar underordnad chef alternativt ger annan funktion i uppdrag att genomföra kontroller. När det gäller medarbetare med priviligierade åtkomsträttigheter som systemadministratörer eller verksamhetsutvecklare, ska det utses andra med systemkunskap som kan utföra kontroller.

Kontrollanten dokumenterar vad som har kontrollerats, när kontrollen gjordes samt vem som gjorde den i ett protokoll. Vissa kontroller kan endast utföras av en chef som har god kännedom om verksamheten, uppdraget och medarbetarnas arbetsuppgifter. I de fallen tillhandahåller lokalt verksamhetsstöd underlag för kontroll till chef. Chef använder underlaget och:

- Kontrollerar om enhetens användare fortfarande ska ha behörigheten eller om de slutat/bytt arbetsuppgifter.
- Kontrollerar att användare inom enheten har rätt behörigheter utifrån arbetsuppgifter. Har det funnits förändringar i arbetsuppgifter vilket resulterat i behov av anpassningar av behörigheter ska behörighet ändras.
- Vid stickprovskontroller så kontrollerar chef om användaren sökt åtkomst till uppgifter som ligger utanför användarens behörighet. Chef kontrollerar att användaren inte använder sina behörigheter på fel sätt genom att läsa, ändra eller ta bort uppgifter. Ibland kan det även uppmärksammas att en användare till exempel har varit inne i fel ärende och skrivit i fel journal.
- Upptäcker kontrollanten exempelvis brister i sekretess eller brister i dokumentation så görs avvikelse. I de fallen kan det även vara aktuellt att göra en incidentanmälan. Dataskyddskontakt utreder sedan om en personuppgiftsincident ska anmälas till Integritetsskyddsmyndigheten (IMY).

Åtkomst- och behörighetskontroller som del av intern kontroll

Processägaren säkerställer att kontroller har genomförts under året för de system som processägaren ansvarar för.

På samarbetsytan ”*Internkontroll System*” ligger dokumentet *Behörighetskontroller* i vilket kontrollerna ska dokumenteras. Här finns också förvaltningens systemförteckning. Processägaren ansvarar för att meddela IT om vem eller vilka som ska ha behörighet till samarbetsytan. I mappen IT-system finns det en mapp för respektive IT-system som innehåller ett dokument som heter ”IT-system – Ansvar”. I detta dokument anges vem som är processägare samt vem som genomför behörighetskontroller för det aktuella IT-systemet. I mappen läggs varje systems plan för kontroller.

Loggkontroller - systemloggar

För att det ska gå att kontrollera att behörigheterna används på ett korrekt sätt måste åtkomsten till personuppgifter dokumenteras (loggas). Av loggarna ska användarens identitet framgå, vilka uppgifter användaren haft tillgång till och vid vilken tidpunkt som åtkomsten skett. Loggarna måste sparas en tid för att möjliggöra kontroll. Varje IT-system behöver ha rutiner för:

- Systematiska och återkommande stickprovskontroller av loggarna. Antalet stickprovskontroller ska vara proportionerliga i förhållande till antalet slagningar som görs i systemet.
- Att det i efterhand går att fastställa vilka användare som har tagit del av informationen i ett system genom så kallade loggkontroller.

Loggar ska minst omfatta:

- Användaridentitet
- Datum och tidpunkt för på- och avloggning
- Information om vilka uppgifter som användaren haft åtkomst till.

Uttag av systemloggar sker skriftligen och utifrån det specifika IT-systemets säkerhetsuppföljning eller vid misstanke om eller faktisk säkerhetsrelaterad händelse.

Tolkning av logg

Vid en tolkning av loggar kan följande undersökas:

- Relation/uppdrag. Har ärendet/den enskilde varit del av de arbetsuppgifter som medarbetaren ska/skulle utföra?
- Tidpunkter – är det rimligt att medarbetaren har tittat på journalen vid de loggade tidpunkterna? Är det utanför medarbetarens schema eller verksamhetens öppettider?
- Namn/släktskap. Finns det något som indikerar provat samhörighet, till exempel anhörig, arbetskamrat, eget ärende?
- Enskild med särskild diagnos som kan väcka intresse.
- Enskild där det finns ett medialt intresse.

Kontrollresultat

Om analys av loggkontrollen inte visar någon av avvikelse så dokumenteras detta i dokumentationen av loggkontrollen.

Om analysen identifierat avvikelser så ska underlaget lämnas över till ansvarig chef, se vidare under avsnitt *Olovlig tillgång till uppgifter*.

Olovlig tillgång till uppgifter

Chef ansvarar för att vid indikation på olovlig tillgång till uppgifter utreda och utvärdera om medarbetarens behörigheter omedelbart ska tas bort.

När utredningen är klar vidtar chef de åtgärder som behövs för att säkerställa ett korrekt och säkert arbetssätt. Åtgärder kan till exempel vara att en användare behöver mer utbildning innan en återgång till arbetet i systemet kan vara aktuellt. Chef kan, med stöd av behörighetskontrollanten för aktuellt system, även genomföra ett samtal med medarbetaren för att säkerställa att denne förstår vikten av rutiner och regelverk i aktuellt informationssystem.

Om utredningen visar på dataintrång eller olovlig läsning så ska ansvarig chef informera processägaren, säkerställa åtgärder samt kontrollera om regler är kända hos samtliga

medarbetare. Chef ansvarar för att dokumentera de åtgärder som vidtagits för att motverka återupprepning av felaktig hantering.

Ansvarig chef ska också ta ställning till om arbetsrättsliga åtgärder behöver vidtas. I personalärende kan chef få stöd från sitt HR-stöd. Anmäl även personuppgiftsincident till förvaltningens dataskyddskontakt.

Bedömer chef efter utredning att det inte finns någon misstanke om dataintrång eller olovlig läsning så ska detta dokumenteras på dokumentationen för loggkontrollen.

Bedömer chef att överträdelsen är så pass allvarlig så tar chef beslut om polisanmälan. Enligt lagstiftningen döms den som olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift för dataintrång till böter eller fängelse i högst två år. Detsamma gäller den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift (4 kap. 9 c § brottsbalken).

Det krävs inte att intrånget sker i visst syfte utan det är själva intrånget som straffbeläggs. Även en person som har tillgång till ett dataregister eller en databas och som i tjänsten men utan att det saknar samband med något ärende personen handlägger kontrollerar olika vänner, bekanta eller andra personer av intresse utan samband med personens myndighetsutövning begår dataintrång. Det är i sig en anledning till att se till att den som har behörighet till uppgifter i ett system känner till att det inte är tillåtet att bereda sig tillgång till andra uppgifter än de som behövs i arbetet. Det kan också vara så att utrednings- och anmälningsskyldigheter enligt 7 kap. 6 § och 14 kap. 6–7 §§ SoL (lex Sarah) aktualiseras.