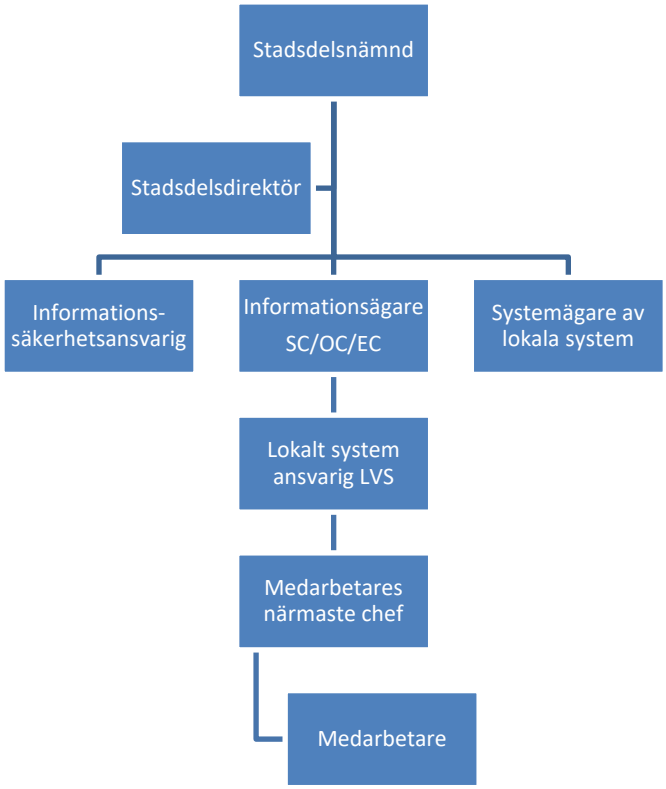
Organisation inom informationssäkerhet med klargjorda roller och ansvar



Stadsdelsnämnden Örgryte Härlanda

Nämnden har det yttersta ansvaret för IT- och informationssäkerhetsfrågor. Nämnden är ansvarig för all information som hanteras inom nämndens område. I nämndens ansvar 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 information hanteras i en kommungemensam intern tjänst eller av en extern leverantör. Intraservice är en tjänsteleverantör för kommungemensamma interna tjänster.

Genomförandet delegeras till stadsdelsdirektören.

Stadsdelsdirektören

Har delegerat ansvar för IT- och informationssäkerheten.

Ansvarar för att utse informationsägare för informationen som förvaltningen hanterar samt de system i vilken informationen finns.

Ansvarar för att utse informationssäkerhetsansvarig i förvaltningen.

Ansvarar tillsammans med förvaltningsledningen för att fastställa förvaltningens organisation för arbetet med dataskyddsförordningen. Dataskyddskontakter för respektive sektor utses av sektorchef.

Systemägare

Göteborgs Stad har utsedda systemägare för samtliga kommungemensamma interna system, som till exempel Treserva, Medidoc och Personec. Systemägarna för kommungemensamma system finns framför allt på Intraservice.

För verksamhetsspecifika system, applikationer, appar, tjänster och andra källor som hanterar information utses systemägare lokalt, vanligtvis sektorschef/stödchef eller områdeschef för mindre system/tjänst.

Informationsägare

Stadsdelsförvaltningen Örgryte Härlanda ansvarar för all information som hanteras i verksamheterna och har därför flera informationsägare lokalt. De ansvarar även för informationen som hanteras i de kommungemensamma interna systemen.

Informationsägare inom SDF Örgryte Härlanda är sektorschef, stödchef, områdes- och enhetschefer

Informationsägaren ansvarar för den information som finns och hanteras i verksamhetsområdets informationssystem.

Informationsägaren ansvarar för att:

- Alla IT-system är anpassade till verksamhetens behov.
- Informationen är rätt säkerhetsklassad enligt stadens Riktlinjer för informationssäkerhet.
- Definiera behörighetsnivå för användare av berörda IT-system. I de flesta större kommungemensamma system finns gemensam definition för behörighetsroller.
- Riskanalys genomförs och hålls uppdaterad.
- Upprätta kontinuitetsplan som beskriver hur verksamheten ska bedrivas om informationen inte är tillgänglig exempelvis vid ett längre avbrott i IT-system. I planen ska framgå vad som är längsta tid som information kan vara otillgänglig innan verksamheten påverkas negativt. Resultatet av genomförd och aktuell riskanalys ska ligga till grund för beslutet.
- Kontinuitetsplanen ska hållas aktuell och helt eller delvis testas årligen samt finnas tillgänglig för berörda i händelse av avbrott.
- Säkerställa att det finns användarinstruktion för respektive verksamhetssystem som inte är kommungemensamt.
- Det upprättas rutiner för rapportering, loggning, åtgärdande, informationsspridning, eskalering, uppföljning och analys av incidenter.
- Upprätta en rutin för hur informationssystemets användare ska agera vid incidenter.

Informationsägaren har även ett ansvar för följande punkter:

- För att utse dataskyddskontakt för sektorn (gäller endast sektorchef).
- För att det vid behov upprättas personuppgiftsbiträdesavtal enligt GDPR/DSF.
- För att personuppgiftsincidenter anmäls till förvaltningens dataskyddskontakt enligt framtagna rutiner, samt att medarbetare inom verksamheten har kunskap om rutinerna.
- För att verksamheten har utsedda resurser för att hantera begäran om utlämning av registerutdrag enligt GDPR.
- För att rapportera nya och avvecklade IT-lösningar, IT-tjänster och andra personuppgiftbehandlingar som används i verksamheten. Detta för uppdatering av förvaltningens systemförteckning och system över aktuella personuppgiftsbehandlingar enligt förvaltningens rutin för detta.

Informationsägarens ansvar innebär att ovanstående genomförs, men arbetet kan delegeras till och genomföras av lokalt systemansvarig eller chef på områdes- eller enhetschefsnivå.

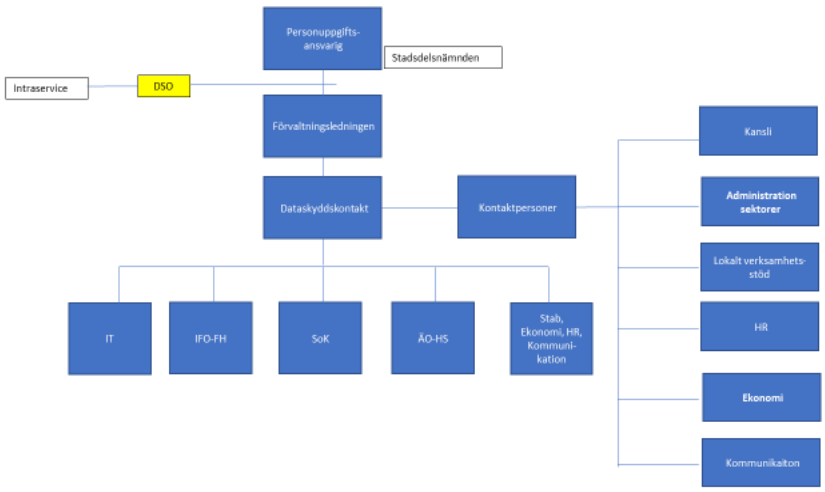
Informationssäkerhetsansvarig

Informationssäkerhetsansvarig har ett helhetsperspektiv vad gäller informationssäkerhet på förvaltningen.

Informationssäkerhetsansvarig ansvarar för att:

- Utveckla förvaltningens informationssäkerhet enligt tillämpliga lagar och stadens styrande dokument.
- Samordna genomförande av förvaltningens informationsklassning av verksamhetssystem.
- Initiera årliga informationssäkerhetsutbildningar på förvaltningen och följa upp medarbetares och chefers deltagande på dessa.
- Säkerställa att utbildningsmaterial för introduktion och återkommande årliga utbildningar om informationssäkerhet är aktuella.
  Ta fram årshjul för kontroll av verksamheternas efterlevnad av informationssäkerheten.
- Omvärldsbevaka och vidareutbilda sig inom informationssäkerhetsområdet.
- Medverka årligen i riskanalys för informationssäkerhetsområdet inom förvaltningen.

Lokalt nätverk för dataskyddskontakter (DSF/GDPR)



Lokalt systemansvarig, systemadministratör/LVS (lokalt verksamhetsstöd)

Lokalt systemansvarig är vanligtvis en medarbetare som även har rollen systemadministratör eller LVS (lokalt verksamhetsstöd) och utses av informationsägare.

I uppdraget ingår i administration, support och utbildning:

- Att ge daglig support, det vill säga, vara lokalt användarstöd samt hantera användarfrågor i aktuella system.
- Att felsöka och skicka in ärenden, som inte kan lösas lokalt, till Intraservice.
- Att utbilda nya användare samt hålla fördjupnings- och repetitionsutbildningar.
- Att sköta löpande behörighetadministration (lägga upp och ta bort användare).
- Att se till att det finns dokumenterade rutiner för behörighetsadministration samt utföra årliga behörighetskontroller för respektive system.
- Att vara kontaktperson gentemot Intraservice beträffande kommungemensamma system.

Men även att verka för god informationssäkerhet genom:

- Att initiera och kontrollera aktiviteter för att höja IT- och informationssäkerheten.
- Att rapportera händelser som kan påverka informationssäkerheten till informationsägare, och om det bedöms relevant även till informationssäkerhetsansvarig.
- Att vid behov vara behjälplig vid registersökningar enligt GDPR, exempelvis vid begäran om registerutdrag eller utredning av personuppgiftsincident.
- Att vara behjälplig vid stickprovskontroller av handhavandet.
- Att ta initiativ till systemförändringar när verksamhetens behov eller omvärldens krav förändras.
- Att behoven fångas upp i samråd med chefer och medarbetare inom verksamheten.

Medarbetares närmaste chef

- Säkerställer årligen att medarbetare har kunskap om informationssäkerhet och kontinuerligt tar del av regelverken kring informationssäkerhet.
- Genomför riskanalys och säkerställer medarbetares kunskap om kontinuitetsplan vid avbrott i IT-system.
- Beslutar och beställer tilldelning, förändring och borttag samt följer upp medarbetares IT-behörigheter till information och informationssystem. Beställning sker enligt förvaltningens rutin.
- Säkerställer att information, informationsbärande utrustning/media, passerkort, tjänstekort återlämnas samt att alla behörigheter till informationssystem, lokaler inaktiveras vid medarbetares och konsulters slut eller vid förändring av tjänst.
- Tar initiativ till systemförändringar när verksamhetens behov eller omvärldens krav förändras.
- Säkerställer att alla medarbetare har kunskap om GDPR och rutinen för att anmäla personuppgiftsincidenter till dataskyddskontakt.

Medarbetare

- Tilldelas behörighet i IT-system enligt förvaltningens behörighetsrutiner.
- Tar ansvar för och skyddar de användaruppgifter, lösenord, pin-koder och annat som erhållits. Inloggningsuppgifter, som är personliga, får inte delas med, visas för eller lånas ut till andra.

- Följer regler för IT- och informationssäkerhet, både stadens gemensamma och förvaltningens interna.
- Har kunskaper om och är följsam mot kraven på sekretess och GDPR inom hela handläggningsprocessen, i manuell bearbetning och vid arkivering.
- Rapporterar personuppgiftsincidenter (GDPR) till sektorns dataskyddskontakt enligt fastställd rutin.
- Rapporterar händelser som kan påverka informationssäkerheten till informationsägare och om det bedöms relevant även till informationssäkerhetsansvarig.