



**Dokumentnamn:** Utbildningsförvaltningens anvisning för roller och ansvar inom informationssäkerhet och dataskydd

**Beslutad av:**  
Förvaltningschef

**Gäller för:**  
All personal

**Diarienummer:**  
0904/23

**Datum och paragraf för beslutet:**  
2023-05-01

**Dokumentsort:**  
Rutin

**Giltighetstid:**  
Tills vidare

**Senast reviderad:**  
2023-05-01

**Dokumentansvarig:**  
Avdelningschef  
administration och ekonomi

# Utbildningsförvaltningens anvisning för roller och ansvar inom informationssäkerhet och dataskydd

## Bakgrund

Information är en av utbildningsförvaltningens viktigaste tillgångar och utgör en förutsättning för att kunna bedriva verksamheten. Utbildningsförvaltningens information i analog och digital form måste därför behandlas och skyddas samtidigt som tillgången till information och öppenheten inom verksamheten förblir så stor som möjligt.

Informationssäkerhet är också en viktig del av skyddet för den personliga integriteten. Det är varje organisations ansvar att planera och genomföra säkerhetsarbetet så att det uppfyller kraven i dataskyddsförordningen på bästa sätt. Därför är det viktigt att dataskyddsarbetet blir integrerad del i verksamhetens informationssäkerhetsarbete.

En tillräcklig nivå av informationssäkerhet och dataskydd säkerställs genom ett systematiskt informationssäkerhetsarbete, tydliga roll- och ansvarsfördelningar samt genom utbildning av anställda i förhållande till deras arbetsuppgifter och ansvar.

## Syfte

I denna anvisning beskrivs vilka roller som finns inom förvaltningens informationssäkerhets- och dataskyddsarbete samt vilket ansvar respektive roll har. Anvisningen är en förutsättning för att kunna informera personer om vilket ansvar som följer av deras roll och för att säkerställa en tillräcklig nivå av informationssäkerhet och dataskydd inom verksamheten.

## Vem omfattas av anvisningen

Anvisningen vänder sig till anställda alla anställda i förvaltningen.

# Förvaltningschef

Förvaltningschefen har ett delegerat övergripande ansvar för genomförandet av informationssäkerhets- och dataskyddsåtgärder.

Förvaltningschefen ansvarar för att

- informationsägare utses
- dataskyddskontakt utses
- fastställa utbildningsförvaltningens organisation för arbetet med informationssäkerhet och dataskydd
- säkerställa att externa parter såsom entreprenörer, inhyrd personal, konsulter och leverantörer uppfyller och följer relevanta delar inom säkerhets- och dataskyddsområdet

## Informationsägare

Informationsägare är den som äger och ansvarar för den information som skapas och används inom verksamheten. Varje chef ansvarar för informationssäkerheten och dataskyddet samt att organisera arbetet inom den egna verksamheten. Ansvaret kan inte delegeras utan ingår i det övriga chefsansvaret. Cheferna ansvarar därmed för informationssäkerheten för sitt chefsområde/verksamhetsområde. Detta gäller både digital och analog information i manuella samt digitaliserade och IT-baserade informationssystem.

Informationsägaren är den som är beroende av informationen som resurs för sin verksamhet och därför måste säkerställa att informationen fyller avsedd funktion med tillräcklig kvalitet och att känslig information som skapas i eller kommuniceras till eller från den egna verksamheten skyddas på ett säkert sätt.

Informationsägare är också riskägare och kan bedöma vilka risker som är acceptabla inom det egna ansvaret. För att hantera risken bör informationsägaren genomföra en riskanalys. Om det finns flera informationsägare som ska använda IT-systemet/lösningen bör samtliga delta i riskanalysen.

För personuppgiftsbehandling är informationsägaren den som äger ändamålet med behandlingen. Informationsägaren ansvarar för att personuppgifterna hanteras enligt gällande regelverk för personuppgiftsbehandling/dataskydd (till exempel att gallring görs).

Utbildningsförvaltningen ska utse informationsägare för alla system som används i förvaltningen. Ett IT-system kan ha flera informationsägare.

Informationsägare ska även

- ansvara för informationens säkerhet samt att säkerheten uppfyller ställda och rättsliga krav
- ansvara för att det finns beslutade rutiner för behörigheter och åtkomst registrering och avregistrering av behörigheter och åtkomst.
- se till att bara behörig personal har tillgång till information. I IT-system styrs tillgången av behörigheter
- ansvara för att informationsklassning genomförs och hålls uppdaterade
- ansvara för att det finns en dokumenterad och formellt beslutad kontinuitetsplan

- utveckla och upprätthålla kompetens hos egen personal avseende informationssäkerhet och dataskydd genom utbildning, informationsinsatser och övning
- bidra med uppgifter till Utbildningsförvaltningens förteckning över samtliga informationssystem och personuppgiftsbehandlingar
- följa upp samt initiera upplägg, förändring och borttag av behörigheter till informationssystem, lokaler etcetera
- säkerställa att information, informationsbärande utrustning/media, passerkort, tjänstekort etcetera återlämnas samt att alla behörigheter till informationssystem, lokaler etcetera inaktiveras vid medarbetares avslut

## Systemägare

Systemägaren har huvudansvaret för planering, styrning och vidareutveckling av systemet. I arbetet ingår:

- att säkerställa tjänstens/förvaltningsobjektets långsiktiga utveckling och att beskriva denna i en tjänsteplan.
- ta beslut om nyutveckling, vidareutveckling och avveckling av system.
- leda system- och tjänsteutvecklingsforum i syfte att tillvarata skolverksamheternas övergripande behov
- i samråd med informationsägare besluta om behörighetsstruktur och rättigheter.
- budgetera och regelbundet följa upp kostnader för tjänsten/förvaltningsobjektet.
- att lagar, förordningar, avtal, interna regelverk och överenskommelser följs.
- att nödvändiga avtal för systemet tecknas och följs upp.
- ansvara för respektive IT-systems säkerhet och för framtagande av kontinuitetsplaner för systemet

## Systemförvaltare

Systemförvaltaren ansvarar för det löpande arbetet med de system som ingår i tjänsten/förvaltningsobjektet. I arbetet ingår:

- att svara för löpande användar- och behörighetsadministration, inklusive uppföljning av att tilldelade behörigheter är korrekta, för respektive system.
- informera om respektive system, dess funktioner och nytta i verksamheten, till användarna. Beakta särskilt:
  - nya användares introduktion till systemet
  - nyckelpersoners introduktion till systemet
- hålla i relevanta användarforum och användarutbildningar
- ta fram och underhålla rutiner, användarinstruktioner och annan relevant systeminformation samt säkerställa att den är tillgänglig för användarna.
- samla in och dokumentera förslag till vidareutveckling av tjänsten/förvaltningsobjektet samt lyfta dessa till samordnande systemförvaltare.
- rapportera eventuella informations- eller personuppgiftsincidenter till informationssäkerhetssamordnare, samordnande systemförvaltare och systemägare
- uppdatera förvaltningsplanen i samråd med samordnande systemförvaltare
- regelbundet utvärdera nyttan och användningen av systemet
- testa och verifiera nya och förändrade funktioner samt informera användarna om hur ny funktionalitet påverkar kritiska verksamhetsprocesser
- delta i change- och releasehantering
- hantera support och incidenter som inkommer från verksamheten

- eskalera supportärenden till leverantör
- delta i leverantörskontroller
- delta i samarbetsforum med leverantör vid behov
- säkerställa att systemet efterlever Göteborgs stads regler och aktuell lagstiftning

## Systemansvarig/LVS

Systemansvarig/LVS kan utses för kommungemensamma tjänster där förvaltningen av tjänsten sköts av Intraservice. I de fall en systemansvarig/LVS är utsedd ansvarar denne för att:

- svara för löpande användar- och behörighetsadministration, inklusive uppföljning av att tilldelade behörigheter är korrekta, för respektive system.
- informera om respektive system, dess funktioner och nytta i verksamheten, till användarna. Beakta särskilt:
  - nya användares introduktion till systemet
  - nyckelpersoners introduktion till systemet
- hålla i relevanta användarforum och användarutbildningar
- ta fram och underhålla rutiner, användarinstruktioner och annan relevant systeminformation samt säkerställa att den är tillgänglig för användarna.
- rapportera eventuella informations- eller personuppgiftsincidenter till informationssäkerhetssamordnare, samordnande systemförvaltare och systemägare
- testa och verifiera nya och förändrade funktioner samt informera användarna om hur ny funktionalitet påverkar kritiska verksamhetsprocesser
- hantera support och incidenter som inkommer från verksamheten
- eskalera supportärenden till leverantör
- delta i samarbetsforum med leverantör vid behov

## Chef

Som chef på utbildningsförvaltningen har man för sitt chefsområde ett ansvar att:

- Vid rekrytering av nya medarbetare, i proportion till kommande arbetsuppgifter, genomföra referenstagning och registerkontroll. Identitetskontroll ska alltid ske, företrädesvis via fullgod legitimationshandling såsom körkort, pass eller identitetskort utfärdat av bank
- I säkerhetshänseende, regelbundet informera sin personal, även inhyrd/inlånad sådan, om regelverk, rutiner och ansvar samt vidta åtgärder för att minska personberoendet såsom att dokumentera processer, rutiner etc
- Säkerställa att personalen har kunskap om och förståelse för tillämpliga säkerhetsrutiner och regelverk
- Säkerställa och regelbundet följa upp att säkerhetsrutiner och regelverk efterlevs
- Följa upp samt initiera upplägg, förändring och borttag av behörigheter till informationssystem, lokaler etc
- Säkerställa att information, informationsbärande utrustning/media, passerkort, tjänstekort etc återlämnas samt att alla behörigheter till informationssystem, lokaler etc inaktiveras vid medarbetares avslut
- rapportera personuppgiftsincidenter internt till förvaltningens dataskyddskontakt
- rapportera händelser som kan påverka informationssäkerheten och dataskyddet till informationssäkerhetssamordnare

# Informationssäkerhetssamordnare

Informationssäkerhetssamordnaren har ett helhetsperspektiv vad gäller informationssäkerhet inklusive dataskydd inom Utbildningsförvaltningens alla verksamhetsområden. Det gäller både digital och analog information.

Informationssäkerhetssamordnaren har befogenhet att vara drivande och hålla ihop, initiera och genom stöd och uppföljning utveckla informationssäkerhetsarbetet inom alla verksamhetsområden.

Informationssäkerhetssamordnaren är förvaltningens dataskyddskontakt och håller ihop förvaltningens dataskyddsfrågor gentemot organisationen. Rollen beskrivs nedan.

Informationssäkerhetssamordnaren ska även

- ha ett övergripande ansvar för att system följer säkerhetsregler och uppnår rätt säkerhetsnivå och dataskydd, exempelvis genom leverantörskontroller
- ansvara för att skyddsåtgärder fastställs för system utifrån informationsklassning
- ansvara för framtagande av förvaltningsspecifika rutiner för informationsklassning
- vara delaktig i informationsklassning av verksamhetssystem
- vid behov initiera informationssäkerhetsutbildningar på förvaltningen
- stötta verksamheten i arbetet med riskanalyser
- säkerställa och regelbundet följa upp verksamhetens följsamhet mot regelverk, säkerhetsrutiner och beslut genom bland annat internkontroll, samt se till att skyddsbehov och accepterad risk- och säkerhetsnivå uppfylls
- regelbundet informera nämnd och ledningsgrupp om status på informationssäkerhetsarbetet samt resultat från uppföljningar och kontroller samt bidra till den årliga säkerhetsrapporten
- se till att det upprättas rutiner för incidenthantering: rapportering, loggning, åtgärdande, informationsspridning, eskalering, uppföljning och analys av incidenter
- omvärldsbevaka sårbarheter och tillsammans med systemförvaltare se till att de åtgärdas för drabbade system eller lösningar

## Medarbetare

Alla medarbetare ska aktivt arbeta för ökad säkerhet och ta ett ansvar för att säkerheten fungerar samt för att informera om och rapportera störningar och avvikelser i säkerheten.

Medarbetare ska särskilt:

- ta ansvar för och skydda de användaruppgifter, lösenord, pin-koder och annat som erhållits
- följa regler för IT- och informationssäkerhet samt dataskydd
- ha kunskaper om och vara följsam mot kraven på sekretess och dataskydd inom hela handlägningsprocessen
- rapportera personuppgiftsincidenter internt till närmaste chef
- rapportera händelser som kan påverka informationssäkerheten och dataskyddet till närmaste chef
- informera närmaste chef om upptäckta brister inom informationssäkerheten och dataskyddet

## Dataskyddsombud

Dataskyddsombudet ska ha särskild sakkunskap i fråga om dataskyddslagstiftning och praxis och utses för att bistå den personuppgiftsansvarige med att övervaka den interna efterlevnaden av förordningen.

Dataskyddsombudet ska

- samla in information om hur Utbildningsförvaltningen behandlar personuppgifter
- kontrollera att Utbildningsförvaltningen följer bestämmelser och interna styrdokument
- informera och ge råd inom Utbildningsförvaltningen
- ge råd om konsekvensbedömningar
- vara kontaktperson för Integritetsskyddsmyndigheten
- vara kontaktperson för de registrerade
- samarbeta med Integritetsskyddsmyndigheten, till exempel vid inspektioner och personuppgiftsincidenter.

## Dataskyddskontakt

Har ett helhetsperspektiv vad gäller dataskyddsarbete inom Utbildningsförvaltningens alla verksamhetsområden. Är kontaktperson gentemot Utbildningsförvaltningens tilldelade dataskyddsombud på Intraservice dataskyddsenhet.

Dataskyddskontakten ska

- informera och ge råd i frågor som handlar om personuppgiftsbehandlingar
- informera dataskyddsombudet om hur personuppgiftsbehandlingar hanteras och dokumenteras
- ansvara för kontakten mellan Utbildningsförvaltningen och dataskyddsombudet
- ha ett övergripande ansvar för personuppgiftsregistret
- upprätta anmälningar om personuppgiftsincidenter och vid behov skicka dessa till Integritetsskyddsmyndigheten
- vara samordnande i arbetet med konsekvensbedömningar
- i samråd med informationsägare eller systemägare ansvara för utredningar om personuppgiftsincidenter
- stödja verksamheten i att hantera och internt anmäla personuppgiftsincidenter
- ge stöd och vägledning i frågor om dataskydd, registrering och behandling av personuppgifter
- granska och ta fram personuppgiftsbiträdesavtal

## Koppling till andra styrande dokument

- Dataskyddsförordningen, Europaparlamentets och rådets förordning (EU) 2016/679
- Göteborgs Stads riktlinje för informationssäkerhet (2019-12-06, Dnr 0540/14, 0110/19)

- Årlig rapport för dataskyddsarbetet inom utbildningsförvaltningen.
- Utbildningsförvaltningen. (2023-05-03, 0796/23). Utbildningsförvaltningens rutin för behörighetshantering i verksamhetssystem inom skola.

Rutinen konkretiseras vidare i form av instruktioner per system.