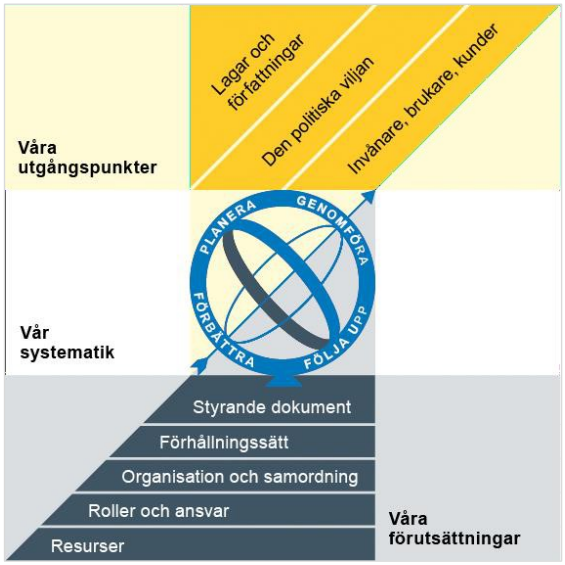
Göteborgs Stad

Äldre samt vård- och omsorgsförvaltningens rutin för informationssäkerhet

Reglerande styrande dokument

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

Göteborgs Stads styrsystem



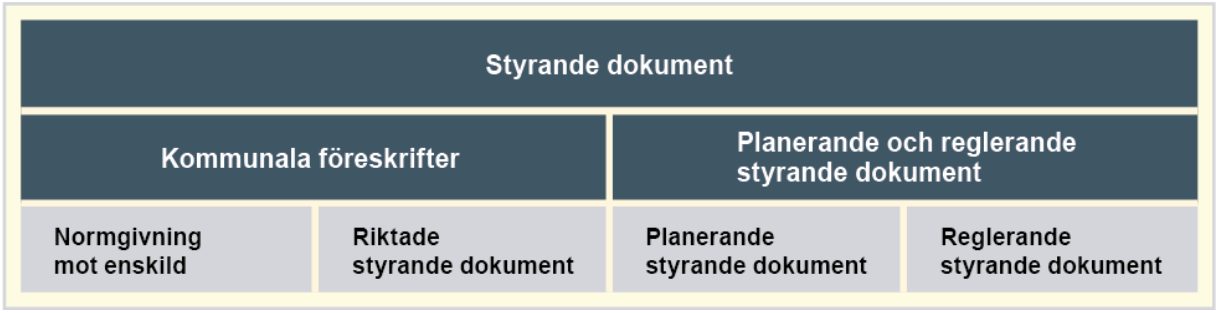
Utgångspunkterna för styrningen av Göteborgs Stad är lagar och författningar, den politiska viljan och stadens invånare, brukare och kunder. För att förverkliga utgångspunkterna behövs förutsättningar av olika slag. Stadens politiker har möjlighet att genom styrande dokument beskriva hur de vill realisera 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:**
Förvaltningsdirektör	Alla medarbetare	N160-1306/21	2021-11-30
Dokumentsort:	**Giltighetstid:**	**Senast reviderad:**	**Dokumentansvarig:**
Rutin	Tillsvidare	2021-11-30	Enheten för säkerhet

Bilagor:
[Bilagor]

Innehåll

Inledning

Syftet med denna rutin

Beskriva hur förvaltningens chefer och medarbetare ska arbeta med informationssäkerhet för att leva upp till Göteborgs Stads säkerhetspolicy och riktlinje för informationssäkerhet.

Vem omfattas av rutin

Denna rutin gäller tillsvidare för chefer och medarbetare i Äldre samt vård- och omsorgsförvaltningen.

Bakgrund

Information är en grundläggande byggsten och utgör en viktig tillgång för en organisation. Verksamheter och medarbetare i förvaltningen omfattas av flera olika lagar som direkt eller indirekt ställer krav på att ha en god informationssäkerhet. Dagligen hanteras värdefull information i förvaltningens verksamheter. Informationen är väsentlig för den enskilde individen och för att kunna bedriva verksamheten. Om personuppgifter eller annan känslig information sprids till obehöriga eller viktig information inte finns tillgänglig, kan det innebära allvarliga konsekvenser för såväl enskilda personer som samhället i stort.

Information är värdefullt och behöver skyddas efter behov. Ett bra informations-säkerhetsarbete är en förutsättning för effektiv och korrekt informationshantering. Detta skapar förtroende både inom och utanför organisationen. Därför behöver förvaltningen ha en god informationssäkerhet för att kunna säkerställa informationens tillgänglighet, riktighet och konfidentialitet.

Koppling till andra styrande dokument

Göteborgs Stads säkerhetspolicy

Göteborgs Stads riktlinje för informationssäkerhet samt tillhörande regler och råd

Göteborgs Stads riktlinjer för hantering av säkerhetsrisker samt tillhörande regler och råd

Rutin för informationssäkerhet

Informationssäkerhet inom Äldre samt vård- och omsorgsförvaltningen

Informationssäkerhet är de åtgärder som görs för att minimera risken för att information förvanskas, förstörs eller är otillgänglig när den behövs samt är tillgänglig för obehöriga. Rutinen gäller oavsett i vilken form informationen finns, till exempel på papper, elektroniska medier, film, ljudfil, eller uttalas muntligen.

Dataskyddsförordningen (DSF)

Hantering av personuppgifter enligt Dataskyddsförordningen är en del i informationssäkerhetsarbetet. De beslutade riktlinjer, rutiner, roller och den ansvarsfördelning som gäller för informationssäkerhet gäller även för hantering av personuppgifter.

Exempelvis kan nämnas att begreppet informationsägare, och det ansvar som följer med det, även omfattar ansvar för att personuppgifter hanteras enligt Dataskyddsförordningen och gällande underliggande bestämmelser inom förvaltningen.
Det ska, utöver vad som anges i detta dokument, inom förvaltningen finnas en särskild dataskyddsorganisation med rutiner som ingående tydliggör förvaltningens ansvar avseende efterlevnad av Dataskyddsförordningen.

NIS-direktivet och Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster och tillhörande förordningar

NIS-direktivet är också en del i informationssäkerheten. Direktivet ställer särskilda krav på att arbeta aktivt och systematiskt med informationssäkerhet inom Hälso- och sjukvård. Särskilda rutiner gäller kring identifiering och rapportering av NIS-incident samt förvaltningens efterlevnad av NIS-direktivet. För vidare information se förvaltningens rutin för hantering av NIS-incidenter. Ytterligare information om NIS-direktivet och lagen finns på Myndigheten för samhällsskydd och beredskaps hemsida på www.msb.se.

Roller och ansvar

Ansvaret för informationssäkerheten följer linjeorganisationen.
Verksamhetens chef på respektive nivå är alltid informationsägare.

Tabellen nedan visar de specifika roller och ansvar som gäller inom förvaltningen, utöver Göteborgs Stads riktlinjer, råd och regler kring informationssäkerhet.

Funktion	Ansvar
Förvaltningsdirektör	Säkerställer att förvaltningen löpande arbetar med och följer upp informationssäkerhetsarbetet. Ansvarar för att hålla Äldre samt vård- och omsorgsnämnden informerad.
Avdelningschef	Ansvarar för det löpande arbetet och uppföljning av informationssäkerhet inom verksamheten. Ansvarar för att föreslå informationssäkerhetsrisker till förvaltningens internkontrollplan. Ansvarar för att avdelningens chefer får adekvat utbildning i informationssäkerhet.
Verksamhetschef	Ansvarar för det löpande arbetet och uppföljning över informationssäkerheten för sin verksamhet och att stödja enhetschefer i frågor som rör informationssäkerhet, exempelvis vid bedömning och hantering av informationssäkerhets- samt personuppgiftsincidenter. Ansvarar för att informera om informationssäkerhetsrisker till avdelningschefen. Ansvarar för att se till att verksamhetens chefer får utbildning i grundläggande informationssäkerhet.
Enhetschef och annan chefsbefattning med direkt verksamhets- och/eller personalansvar	Ansvarar för: • att arbete och uppföljning genomförs gällande informationssäkerhet inom verksamheten. • att identifiera och utifrån en riskanalys, klassa information som hanteras på enheten. • att tillräckliga skyddsåtgärder finns. • att händelser och avvikelser avseende informationssäkerhet hanteras enligt gällande rutin. • att diarieföra incident/skador. • att enheten har en aktuell kontinuitetsplan rörande tillgänglighet av information. • att medarbetare har rätt kunskap i förhållande till sina arbetsuppgifter.
Förvaltningscontroller	Ansvarar för att ta med identifierade risker till förvaltningens samlade riskbild och internkontrollplan. Ansvarar för att rapportering av informationssäkerhets-arbetet ingår i årsrapporten.
Säkerhetschef	Ansvarar för att hålla ihop, initiera och genom stöd och uppföljning utveckla informationssäkerhetsarbetet.
Utvecklingsledare säkerhet / Informationssäkerhetsansvarig	Sammanställer rapporterade informations-säkerhetsrelaterade incidenter och skador till årsrapporten.

	Inhämtar och sammanställer adekvat information till avsnittet informationssäkerhet till årsrapporten.
Utvecklingsledare IT	Ansvar för upprätta och underhålla en förteckning över förvaltningens IT-lösningar. Ansvarar för stöd och uppföljning kring att regel- och säkerhetsmässiga krav uppfylls för kommungemensamma samt egna IT-system och tjänster.
Alla medarbetare	Ska ha relevant kunskap om IT- och informationssäkerhet i förhållande till sina arbetsuppgifter och ansvarar för att rapportera till sin närmaste chef om det finns behov av att få utbildning eller ytterligare information för sin uppgift. Ska som minst ha genomgått Göteborgs Stads grundläggande utbildning i informationssäkerhet eller motsvarande, antingen vid nyanställning eller senast inom ett år efter senaste utbildningstillfälle. Ska rapportera händelser eller avvikelser kopplat till informationssäkerhet till sin närmsta chef.

Informationsägare och ansvar

Informationsägare är den som ansvarar för att verksamhetens information är riktig, tillförlitlig och för hur informationen sprids. Det gäller oavsett om informationen finns i ett system bygger på manuell hantering eller en IT-lösning.

För att hantera eventuella risker ska informationsägaren genomföra en riskanalys. Om det finns flera informationsägare som använder IT-systemet/lösningen är det lämpligt att göra en gemensam riskanalys. Riskanalysen ligger till grund för informationsklassning.

Informationsägaren har ansvar att hantera de eventuella konsekvenser som kan uppstå vid bristande säkerhet.

Identifiering och klassning av informationstillgångar

Alla chefer, enligt tabellen ”Roller och ansvar”, ansvarar för att identifiera och klassa sina informationstillgångar.

Inom Göteborgs Stad delas information in i fem skyddsklasser (0, 1, 2, 3, 4) baserat på dess konfidentialitet, riktighet och tillgänglighet.

För information i skyddsklass ett, två och tre kan brister leda till skada, -allvarlig skada - eller mycket allvarlig skada för verksamheten, förvaltningen, annan organisation eller enskild. Därför behövs restriktioner gällande hantering, bevarande och gallring beroende på vilken klassning informationen har.

Bild 1: Göteborgs Stads informationsklassningsmodell

	Konsekvensnivå	Konfidentialitet	Riktighet	Tillgänglighet
4	Sveriges Säkerhet Säkerhetsskydd	**K4** Information som omfattas av Säkerhetsskyddslagstiftningen *Särskild hantering - Riktlinje för säkerhetsskydd.*		
3	Allvarlig skada (hög skyddsnivå)	**K3** Viktig information som, om den tillgängliggörs, röjs eller sprids till obehöriga, kan medföra allvarliga konsekvenser för Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer.	**R3** Viktig information som, om den ej är riktig och fullständig, kan medföra allvarliga konsekvenser för Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer.	**T3** Viktig information som, om den ej är tillgänglig, kan medföra allvarliga konsekvenser för Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer.
2	Betydande (utökad skyddsnivå)	**K2** Information som, om den tillgängliggörs, röjs eller sprids till obehöriga, kan medföra betydande negativ påverkan på Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer	**R2** Information som, om den ej är riktig och fullständig, kan medföra betydande negativ påverkan på Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer	**T2** Information som, om den ej är tillgänglig, kan medföra betydande negativ påverkan på Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer.
1	Måttlig (grundläggande nivå)	**K1** "Intern" information som om den tillgängliggörs, röjs eller sprids till obehöriga kan medföra måttlig negativ påverkan på Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer	**R1** Information som, om den ej är riktig och fullständig, kan medföra måttlig negativ påverkan på Göteborgs Stads verksamhet, tillgångar, annan organisation eller på individer	**T1** Information som, om den ej är tillgänglig, kan medföra måttlig negativ påverkan på Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer
0	Försumbar skada (ingen skyddsnivå)	**K0** Information som, om den tillgängliggörs, röjs eller sprids till obehöriga, inte medför någon negativ skada för Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer	**R0** Information där förlust av riktighet inte medför någon negativ skada för Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer	**T0** Information där förlust av tillgänglighet inte medför någon negativ skada för Göteborgs Stads verksamhet, tillgångar, annan organisation eller individer

Skyddsåtgärder

Informationsägaren ansvarar för att rätt skydd finns för aktuell information.
När det gäller kommungemensamma IT-system och tjänster ansvarar utvecklingsledare IT för att följa upp att överenskomna regel- och säkerhetsmässiga krav.
För andra IT-system och tjänster och annan media ansvarar respektive informationsägare för att regel- och säkerhetsmässiga krav är uppfyllda.

Grundläggande skyddsnivå - Klass 1

Hantering av incidenter

Med incidenter avses, när en avvikelse kunde ha lett till en skada. Med skada avses hantering av information som bedöms innebära betydande eller allvarliga konsekvenser för verksamheten, förvaltningen, annan organisation eller enskild individ.

Informationsägaren ansvarar för att det finns en rutin för rapportering, loggning, åtgärd, informationsspridning, eskalering, uppföljning och analys av incidenter för varje informationssystem.

Den medarbetare som upptäcker en incident eller skada, ska anmäla den till sin närmaste chef. Chef ansvarar för att incidentrapport blir ifylld och diarieförd.
För incidenter där förvaltningen har avtal med Intraservice om hanteringen av informationssystem, ska chef anmäla den till utvecklingsledare IT för vidare handläggning.

Särskilda rapporteringsrutiner gäller för incidenthantering av personuppgifter enligt Dataskyddsförordningen eller rapportering av incident enligt NIS-direktivet.

Kontinuitetsplanering

Informationsägaren ansvarar för att besluta om tillgänglighetskrav. Det innebär den längsta tid som information i skyddsklass ett, -två och tre, kan vara otillgänglig, eller informationssystemet kan vara ur funktion innan verksamheten påverkas i oacceptabel omfattning.

Alla verksamheter ska ha en kontinuitetsplan för information i skyddsklass ett, två och tre som säkerställer verksamheten utifrån tillgänglighetskraven.

Kontinuitetsplanen ska beskriva hur den information som behövs för att bedriva samhällsviktig verksamhet kan nås, under ett avbrott eller en störning. Exempel på sådan information kan vara:

- Rutiner
- Planering och annan viktig information som behövs för att bedriva samhällsviktig verksamhet.
- Handlingsplaner för avvikande händelser
- Dokumentation över system/instruktioner
- Kontaktlistor med ansvarsfördelning

För informationshantering som blivit klassad i nivå 2 och nivå 3 och som därmed har ett utökat skyddsbehov ska kompletterande åtgärder införas. Dessa skyddsåtgärder utformas specifikt och tas ej upp i denna riktlinje.

Kontinuitetsplaner som inkluderar IT-baserade informationssystem ska omfatta de återstarts- och reservrutiner som krävs för att återstart kan ske inom fastställd tid.

Utvecklingsledare IT ansvarar för att följa upp att de återstarts- och reservrutiner, inklusive säkerhetskopiering och återläsning, som avtalats med Intraservice.

Verksamhetsansvarig chef ansvarar för att följa upp återstarts- och reservrutiner, inklusive säkerhetskopiering och återläsning, för icke-kommungemensamma IT-system.

Kontinuitetsplaner ska hållas aktuella och helt eller delvis testas årligen samt finnas tillgänglig för berörda i händelse av avbrott.

Förteckning över informationssystem

Förvaltningen ska ha en förteckning som redovisar de system där information i skyddsklass ett, - två och tre kan lagras, behandlas eller distribueras samt hur den hanteras.

Förteckningen ska innehålla uppgifter om

- System för hantering
- Systemets skyddsklass för konfidentialitet, riktighet och tillgänglighet
- Systemägare
- Tillgänglighetskrav
- Skyddsåtgärder

- Informationsägare
- Kontinuitetsplanering

Utvecklingsledare IT ansvarar för förteckningen.
Respektive systemägare ansvarar för att bidra med och uppdatera uppgifterna.

Utbildning

Alla medarbetare ska årligen genomföra den grundläggande informations-säkerhetsutbildning som beslutats inom förvaltningen.

Informationsägaren ansvarar för uppföljning av att medarbetarna har aktuell utbildning.

Förvaltningens samtliga chefer ska genomföra informationssäkerhets utbildning vid nyintroduktion, vartannat år eller vid behov. Utvecklingsledare säkerhet och utvecklingsledare IT finns som stöd vid behov.

Uppföljning

Samlad riskbild med Internkontrollplan
Förvaltningsdirektören ansvarar för att i förslaget till förvaltningens samlade riskbild med internkontrollplan ta med relevanta risker utifrån arbetet med informationssäkerhet.

Säkerhetsnivå
Utvecklingsledare säkerhet/Informationssäkerhetsansvarig sammanställer rapporterade informationsäkerhetsincidenter till årsrapporten. Utvecklingsledare säkerhet ska årligen följa upp med informationsägare om deras medarbetare har genomfört informationssäkerhetsutbildning och omfattningen av chefer som har genomfört utbildningen.

Utvecklingsledare säkerhet/Informationssäkerhetsansvarig ska årligen följa upp att verksamheterna har en kontinuitetsplan.