Göteborgs Stad

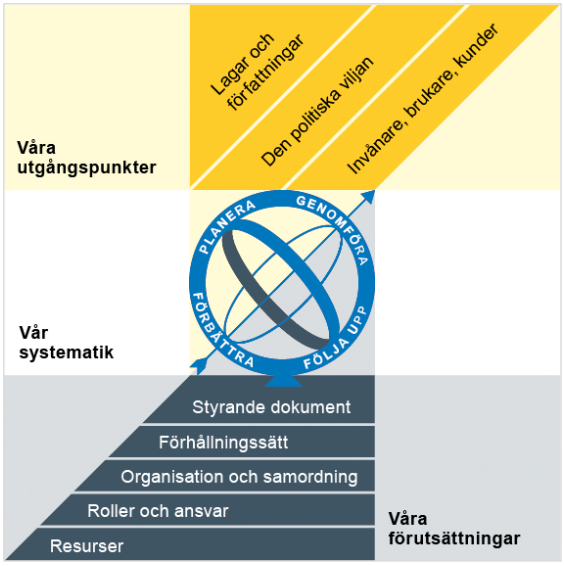
Nämnden för Intraservices anvisning för informationssäkerhet

IIFS 1

Reglerande styrande dokument

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

Göteborgs Stads styrsystem



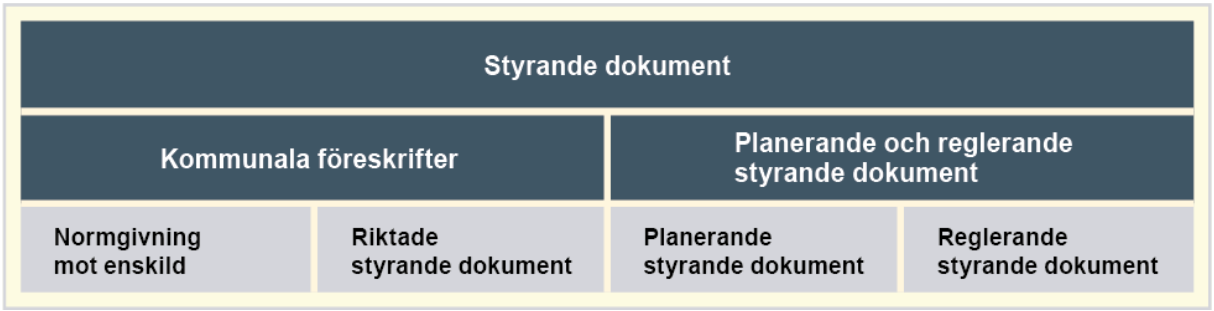
Utgångspunkterna för styrningen av Göteborgs Stad är lagar och författningar, den politiska viljan och stadens invånare, brukare och kunder. För att förverkliga utgångspunkterna behövs förutsättningar av olika slag. Stadens politiker har möjlighet att genom styrande dokument beskriva hur de vill realisera 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.



Dokumentnamn: Nämnden för Intraservices anvisning för informationssäkerhet

Beslutad av:	**Gäller för:**	**Diarienummer:**	**Datum och paragraf för beslutet:**
Nämnden för Intraservice	Samtliga medarbetare	0197/24	[Text]
Dokumentsort:	**Giltighetstid:**	**Senast reviderad:**	**Dokumentansvarig:**
Anvisning	2024-09-02 och tillsvidare	2024-06-27	Intraservices CISO

Bilagor:

Inledning

Syftet med denna anvisning

Syftet med anvisningen är att fastställa grundläggande förutsättningar för ett systematiskt informationssäkerhetsarbete på Intraservice. I detta ingår:

- Fördelning av ansvar och mandat mellan roller och befattningar på Intraservice.
- Definiera gemensamma informationssäkerhetsbegrepp
- Förutsättningar och metodik för begäran om avsteg från styrdokument inom informationssäkerhetsområdet.

Vem omfattas av anvisningen

Denna anvisning gäller för chefer och medarbetare på förvaltningen för Intraservice.

Bakgrund

Göteborgs stads riktlinje för informationssäkerhet definierar två roller kopplat till informationssäkerhet enligt följande, systemägare och informationsägare

Anvisningen syftar till att beskriva det ansvar som olika roller inom Intraservice linjen har för att stötta nämnden att ta detta ansvar. Rollerna ansvarar för olika delar och olika nivåer av arbetet. Hela vägen ifrån strategisk planering och uppföljning till att operativt arbeta med att realisera identifierade säkerhetsåtgärder. Eskalering och återrapportering tydliggörs av den anledningen i eget stycke. Situationer kan uppstå när avsteg behöver göras ifrån styrande dokument. För att dessa skall hanteras på ett systematiskt sätt och kunna beslutas och följas upp beskrivs undantagshantering.

För att skapa en tydlighet för de roller som är berörda av detta och andra styrdokument är det viktigt med gemensamt språkbruk, av denna anledning finns här också en begreppslista som skall användas i framtagande av övriga styrdokument med koppling till informationssäkerhet.

Koppling till andra styrande dokument

Styrande dokument	Koppling till denna anvisning
Göteborgs stads riktlinje för informationssäkerhet	Definierar informationsägare och systemägare
Göteborgs stads regel för IT-användare	Beskrivning av enskild användares ansvar vid användning av stadens IT-system och resurser.
Nämnden för Intraservices anvisning för informationsklassning	Beskriver hur Intraservice ska informationsklassa
Nämnden för Intraservice rutin för riskbaserat informationssäkerhetsarbete	Beskriver hur Intraservice ska arbeta med risker inom informationssäkerhet
Befattningsbeskrivningar på Intraservice	Beskriver enskilda befattningar på Intraservice

Stödjande dokument

Intraservices rutin för informationssäkerhet

Definitioner

1 §

Begrepp	Betydelse
Funktions- och säkerhetsinformation	Den information som 1. skapas endast som en förutsättning för tjänsten, eller 2. för underhåll, utveckling eller säkerhet i tjänsten.
Gemensamma innehållsinformation	Den information som 1. skapas av tjänsten för att användas i andra tjänster, eller 2. skapas av tjänsten och nyttjas av minst två kommunala myndigheter.
IIFS	Intraservices Informationssäkerhets FörfattningsSamling. Intraservices författningssamling för styrande dokument som reglerar informationssäkerhet.
Informationsbärare	Digital eller fysisk resurs för behandling av information.
Informationsmängd	En avgränsad mängd information som fyller ett meningsfullt syfte för klassningsobjektet.
Informationstillgång	Informationsmängder och informationsbärare som är av värde för en organisation.
Innehållsinformation	Den information som 1. skapas av annan kommunal myndighet i tjänsten, eller 2. skapas av Intraservice som konsument av tjänst, eller 3. skapas av Intraservice utanför tjänst.

Klassningsobjekt	Föremål för informationsklassning vid ett specifikt tillfälle.
Risk	Risk inom informationssäkerhet innebär sannolikheten att ett hot utnyttjar sårbarheten hos en informationstillgång eller en grupp av informationstillgångar och därigenom orsakar organisationen skada.
Riskanalys	Process för att förstå riskens natur och för att avgöra risknivån
Riskbehandling	Riskbehandling är processen att förändra risker i en organisation eller projekt. De åtgärder som kan vidtas för att hantera en risk inkluderar att undvika, acceptera, överföra eller reducera risken.
Riskhantering	Riskhantering är samordnade aktiviteter för att styra, leda och systematiskt hantera potentiella risker som kan påverka en organisation, projekt eller process.
Säkerhetsåtgärd	Identifierad åtgärd för att möta en organisations risker

Roller, ansvar och mandat

Eskalering samt återrapportering

2 § Inom området informationssäkerhet, och kopplat till de åtgärder och beslut däri, kan frågor behöva eskaleras eller återrapporteras. Eskalering följer ordinarie linje på så sätt att medarbetare, förvaltningsledare och chefer eskalerar frågor vidare till närmaste chef i de fall ett beslut faller utanför medarbetarens eller chefens befogenheter. Frågor av principiell karaktär eller av större vikt ska alltid eskaleras till nämnden.

Roller med särskilt ansvar

CISO

3 § Informationssäkerhets och dataskyddschef (CISO) är den som leder, styr, säkerställer och samordnar allt informationssäkerhets och dataskyddsarbete på Intraservice.

4 § CISO ansvarar för att kravställa på de säkerhetsåtgärder som ska gälla vid utveckling och leverans av gemensamma tjänster och digital infrastruktur.

5 § CISO ansvarar för att ta fram de styrdokument och säkerhetsåtgärder som krävs för systematiskt informationssäkerhetsarbete.

6 § CISO ansvarar för att genom efterlevnadskontroller bedriva tillsyn så att styrdokument och lagar inom informationssäkerhetsområdet efterlevs.

7 § CISO ansvarar för att rapportera brister i efterlevnaden enligt 6 § till nämnden för Intraservice minst årligen.

8 § CISO ska yttra sig om undantag från styrdokument kopplade till IIFS samt Göteborgs stads riktlinjer för informationssäkerhet.

9 § CISO kan underkänna specifika säkerhetsåtgärder, alternativt yttra sig inför godkännande.

10 § CISO ansvarar för att hindra eller rapportera aktiviteter som strider mot IIFS. Stadenövergripande styrdokument eller lagar kopplade till informationssäkerhet.

11 § CISO ansvarar för att analysera omvärlden och den egna organisationen avseende informationssäkerhet

12 § CISO ansvarar för att informera övriga organisationen om eventuella förestående hot eller risker kopplade till informationssäkerhet.

13 § CISO ansvarar för att utveckla informationssäkerhetsområdet genom att utforma och förvalta dokument, planer och modeller inom informationssäkerhet

14 § CISO ansvarar för att stödja Intraservice i förvaltning och utveckling så att lagar och styrdokument kan efterlevas.

Linjeroller och deras ansvar

Verksamhetschef

15 § Verksamhetschefen är informationsägare för de informationsmängder som hanteras inom verksamhetsområdets processer

16 § Verksamhetschefen är tjänsteägare för de tjänster som ligger inom verksamhetsområdets ansvar

17 § Verksamhetschefen är riskägare för de identifierade riskerna inom verksamhetsområdet

18 § Verksamhetschefen ansvarar för uppföljning av att hanteringen av informationsmängder följer styrande dokument och lagar.

19 § Verksamhetschefen ansvarar för att informationsklassningar genomförs inom verksamhetsområdet.

20 § Verksamhetschefen ansvarar för att riskanalyser genomförs inom verksamhetsområdet.

21 § Verksamhetschefen ansvarar för att risker hanteras,

22 § Verksamhetschefen ansvarar för att risker och säkerhetsåtgärder följs upp och dokumenteras.

23 § Verksamhetschefen ansvarar för att informationsklassning, risker och säkerhetsåtgärder delges berörda

24 § Verksamhetschefen ansvarar för att enhetschef uppdaterar register över informationstillgångar

25 § Verksamhetschefen ansvarar för att enhetschef vidtar säkerhetsåtgärder utifrån resultat från informationsklassning och riskanalys och bevakar uppfyllnad

26 § Verksamhetschefen ansvarar för att enhetschef upprättar, följer upp och uppdaterar kontinuitetsplan och bevakar uppfyllnad

Enhetschef

27 § Enhetschefen är systemägare för de informationsbärare som ligger inom enhetens leveranser

28 § Enhetschefen ansvar för att hanteringen av informationsmängder i process och/eller informationsbärare följer styrande dokument och samråder med informationssäkerhetssamordnare

29 § Enhetschefen ansvar för genomförande av informationsklassning

30 § Enhetschefen ansvar för genomförande av riskanalyser och samordnar riskanalyser med andra systemägare

31 § Enhetschefen ansvar för att säkerhetsåtgärder implementeras i enlighet med kravställning från informationsklassning och riskanalys.

32 § Enhetschefen ansvar för att säkerställa att förvaltningsplan innehåller säkerhetsåtgärder utifrån resultat från informationsklassning och riskanalys och ansvarar för att bevaka uppfyllnad

33 § Enhetschefen ansvar för att kontinuitetsplan upprättas, följs upp och uppdateras

34 § Enhetschefen ansvar för och beslutar om användares åtkomsträttigheter och att dessa överensstämmer med informationsägarens instruktioner

35 § Enhetschefen ansvar för att tillse att teknisk arkivredogörare utses och att gallring och arkivering utförs enligt Göteborgs stads föreskrifter och riktlinjer om arkiv- och informationshantering.

36 § Enhetschefen ansvar för att tillse att teknisk arkivredogörare tar fram och underhåller bevarandeplan för system

37 § Enhetschefen ansvar för att register över informationstillgångar hålls uppdaterade

Förvaltningsledare

38 § Förvaltningsledaren är teknisk arkivredogörare för de tjänster som förvaltningsledaren ansvarar för.

39 § Förvaltningsledaren ansvarar för att ta kontakt med dataskyddskontakt vid behov

40 § Förvaltningsledaren ansvarar för att vid behov samordna arbete med incident, problem, change, request, test och release

41 § Förvaltningsledaren ansvarar för att hanteringen av informationsmängder i process och informationsbärare följer styrande dokument,och samråder med informationssäkerhetssamordnare vid behov.

42 § Förvaltningsledaren ansvarar för implementering av säkerhetsåtgärder

43 § Förvaltningsledaren ansvarar för upprättande av förvaltningsplan och att säkerhetsåtgärder vidtas utifrån resultat från informationsklassning och riskanalys

44 § Förvaltningsledaren ansvarar för uppföljning av förvaltningsplan och återrapportering till berörda.

45 § Förvaltningsledaren ansvarar för att följa upprättad kontinuitetsplan, samt med regelbundenhet utvärdera och praktiskt testa dessa, samt rapportera uppfyllnad

46 § Förvaltningsledaren ansvarar för framtagande och underhåll av bevarandeplan för system.

Systemförvaltare

47 § Systemförvaltare ansvarar för att utföra säkerhetsåtgärder enligt förvaltningsplan

48 § Systemförvaltare ansvarar för att hantera incident, problem, change och request för det informationsbärare.

49 § Systemförvaltare ansvarar för att hanteringen av information i tjänst och informationsbärare följer styrande dokument och samråder med systemägare och förvaltningsledare

Samtliga medarbetare

50 § Medarbetare ska informera sig om de styrdokument som rör hanteringen av informationsmängder och informationsbärare.

Avsteg från styrdokument inom informationssäkerhet

Inledande bestämmelser

51 § Avsteg kan begäras för de informationstillgångar som berörs av Göteborgs Stads riktlinje för informationssäkerhet samt styrdokument tillhörande IIFS. Avsteg kan även begäras för tillhörande rutiner och processer.

52 § Då en informationstillgång etablerats i enlighet med Intraservices anvisning för definition av tillgångar, så anses tillgången omfattas av Göteborgs Stads riktlinje för informationssäkerhet samt styrdokument tillhörande Intraservices informationssäkerhetsförfattningssamling (IIFS).

53 § Beslut om avsteg från Göteborgs Stads riktlinje för informationssäkerhet samt Intraservices underliggande styrdokument, ska revideras som minst var sjätte månad om inget annat framgår av 62 §.

54 § Beslut ska revideras utöver vad som anges i 61 § genomföras vid väsentliga förändringar av risk, för den tillgång avsteg begärts för eller berörda tillgångar.

55 § Beslut om att bevilja avsteg från Göteborgs Stads riktlinje för informationssäkerhet samt Intraservices Informationssäkerhetsförfattningssamling (IIFS) fattas av Nämnden för Intraservice.

Genomförande av begäran om avsteg

56 § Genomförande av begäran om avsteg från Göteborgs Stads riktlinje för informationssäkerhet samt Intraservices Informationssäkerhetsförfattningssamling (IIFS) ska ske enligt rutin och instruktion för begäran om avsteg från riktlinje för informationssäkerhet samt underliggande styrdokument.

57 § Informationsklassning/säkerhetsdeklaration samt analys på hur avsteget påverkar risk ska utföras enligt anvisning för informationsklassning och anvisning för riskanalys.

58 § Det ska dokumenteras från vilka säkerhetskrav man begär avsteg, enligt rutin för begäran av avsteg.

Dokumentation

59 § Begäran om avsteg från riktlinje för informationssäkerhet ska dokumenteras i enlighet med rutin för begäran om avsteg.