Göteborgs Stad

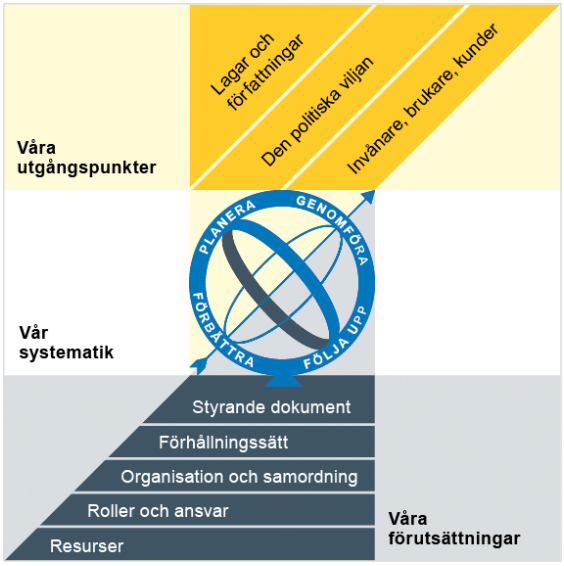
Nämnden för Intraservice anvisning för riskbaserat informationssäkerhetsarbete

IIFS 3

Reglerande styrande dokument

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

Göteborgs Stads styrsystem



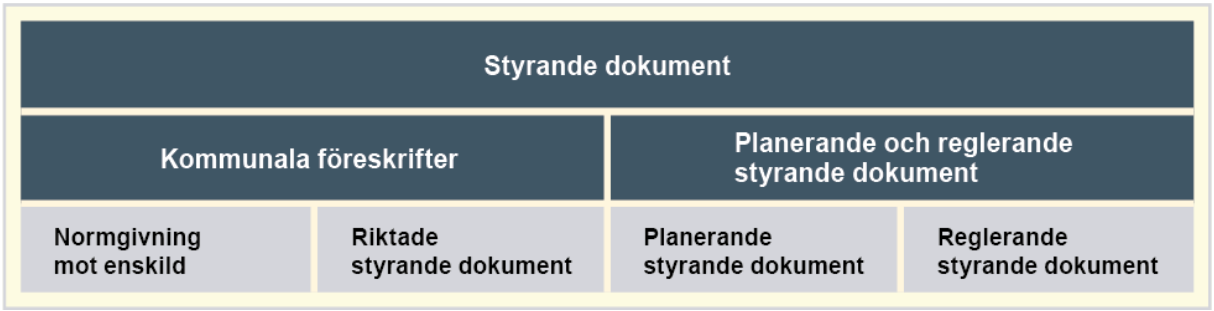
Utgångspunkterna för styrningen av Göteborgs Stad är lagar och författningar, den politiska viljan och stadens invånare, brukare och kunder. För att förverkliga utgångspunkterna behövs förutsättningar av olika slag. Stadens politiker har möjlighet att genom styrande dokument beskriva hur de vill realisera 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:**
Nämnden för Intraservice	Intraservice	0206/24	[Text]
Dokumentsort:	**Giltighetstid:**	**Senast reviderad:**	**Dokumentansvarig:**
Anvisning	Tills vidare	2024-06-27	CISO Intraservice

Bilagor:
-

Innehåll

Inledning

Syftet med denna anvisning

Denna anvisning syftar till att etablera en standardiserad hantering för att hantera risker i organisationen. Målet är att minimera negativa effekter på verksamheten och säkerställa en systematisk och proaktiv hantering av potentiella hot.
Vidare integreras denna rutin med andra relevanta regleringar och processer inom stadens och Intraservices verksamheter.
Målsättning är att implementeringen av rutinen sker med hållbara, förutsägbara, standardiserade och kvalitetssäkrade metoder för att säkerställa en effektiv, ändamålsenlig och samstämd riskhantering.

Vem omfattas av anvisningen

Denna anvisning gäller för samtliga medarbetare på Intraservice.

Bakgrund

Kommunfullmäktige fastställde i maj 2023 en ny riktlinje för informationssäkerhetsområdet: Göteborgs Stads riktlinje för informationssäkerhet. Enligt riktlinjen ska Göteborg Stad bedriva ett systematiskt och långsiktigt arbete för informationssäkerhet.
Göteborgs Stad anpassar sitt arbete med informationssäkerhet efter förändringar i både omvärlden och den interna verksamheten, enligt Göteborgs stads riktlinje för informationssäkerhet.
För att hantera hot, risker och sårbarheter som kan påverka staden, är det nödvändigt att genomföra omvärldsanalyser och använda ett riskbaserat förhållningssätt i informationssäkerhetsarbetet. Detta innebär att varje verksamhet inom staden behöver identifiera, bedöma och kontinuerligt följa upp informationssäkerhetsrisker för att prioritera vad som är väsentligt och kunna vidta lämpliga säkerhetsåtgärder. Agerande på risker sker som en följd av riskhantering.
Denna anvisning konkretiserar stadens riktlinjer för informationssäkerhet med avseende på ett riskbaserat informationssäkerhetsarbete. Rutinen ska säkerställa att Intraservices riskhantering avspeglar de specifika behoven och förutsättningarna för och inom Intraservices. Med detta menas behov och förutsättningar både för den egna förvaltningen samt för vårt uppdrag som tjänsteleverantör av gemensamma tjänster och tjänster inom digital infrastruktur.

Koppling till andra styrande dokument

Styrande dokument	Koppling till denna rutin
Göteborgs stads riktlinje för informationssäkerhet, kommunfullmäktige	Fördelar ansvar till stadens verksamheter och ställer krav på ett riskbaserat informationssäkerhetsarbete.
Nämnden för Intraservices anvisning för informationssäkerhet	Grundläggande bestämmelser för informationssäkerhetsarbetet
Nämnden för Intraservice anvisning för informationsklassning	Gör stadens riktlinjer för informationssäkerhet mer konkret för Intraservice vad gäller säkerhets-klassificering av information.
anvisning för processkarta och processarkitektur	Definierar process.
Nämnden för Intraservice anvisning för styrning uppföljning och kontroll	Reglerar hur övergripande risker ska rapporteras

Stödjande dokument

Stödjande dokument är mallar, presentationer och processbeskrivning, underlag för terminologi som fungerar som stöd när man genomför riskanalyser eller riskförvaltning. Riskhantering behöver ske inom många olika områden; vid verksamhetsplanering, i projekt, i verksamhetsutveckling där till exempel riskanalysen kan vara ett underlag i eller ett komplement till processkartläggningar, i samband med säkerhetsfrågor, vid riskinventeringar eller andra tillfällen. Riskprocessen är därför generisk.

Stödjande dokument	Koppling till denna anvisning
Utföra riskhantering för informations-säkerhet v 2.0	Ger stöd till riskhanteringsprocessen Ersätter tidigare ”Riskhantering processbeskrivning” v1.0
Excelmall för riskanalys (grundmetod)	Excelmall Ersätter tidigare Excelmall (v.7)
Presentation av riskhantering	Förklarar processen samt är ett stöd vid genomförande vid workshop
Guide för grundmetod för riskanalys	Ersätter tidigare praxisstöd stöd vid workshop

Anvisning

Anvisningen ska tillämpas för hela Intraservices förvaltning, inklusive alla avdelningar och enheter. Den täcker alla aspekter av informationssäkerhetsrisker, som normalt delas in i konfidentialitet, riktighet och tillgänglighet (KRT).

Arbete med informationssäkerhetsrisker innefattar riskhanteringsprocess, analysmetoder samt riskförvaltning med dokumentation och rapportering samt hotanalys.

Definitioner

1. § Definitioner för denna anvisning finns i Nämnden för Intraservices anvisning för informationssäkerhet.

Övergripande

2. § Riskhantering för Intraservice baseras på Göteborgs Stads riktlinje för informationssäkerhet samt standarden ISO/IEC 27005.

3. § Riskhantering är en central del i strategiska, tekniska och operativa beslut. Därför ska säkerhetsrisker hanteras i alla i beslutsprocesser.

4. § Roller, ansvar och mandat beskrivs i Nämnden för Intraservices anvisning för informationssäkerhet.

5. § Riskägaransvar ska innehas av en chef, eftersom ansvaret förutsätter tillgång till resurser, beslutsmandat och delaktighet i centrala beslut.

6. § Riskägare ansvarar för att risker identifieras och antingen accepteras eller hanteras, exempelvis med säkerhetsåtgärder.

7. § Nämnden för Intraservices informationssäkerhetschef (CISO), kan besluta rutiner och instruktioner inom ramen för denna anvisning.

Hot och riskbedömning

Intraservice har en grundmetod för riskanalys. Grundmetoden är utgångspunkten och är enkel att genomföra. Utökande riskanalyser kan användas vid större risker eller vid hotprioritering. Utökande analysmetoder kräver mer tid och kunskap för att genomföra, men ger samtidigt ett mer välgrundat underlag.

8. § Riskanalyser ska genomföras vid större förändringar enligt riskhanteringsprocessen, beskriven nedan i processen utföra riskhantering för informationssäkerhet.

9. § Riskhantering ska baseras på informationens skyddsnivå, en informationsklassning som sker enligt rutin för informationsklassning.

10. § För hotprioritering kan jämförande relativ kvalitativ metod användas, enligt instruktion för utökad riskanalys.

11. § För bedömning av enskilda komplexa risker eller risker där kostnaderna för säkerhetsåtgärder är höga kan dessa bedömas med en faktoranalys, som är en kvantitativ metod.

Hotunderrättelser och sårbarheter

Hotunderrättelser (Threat Intelligence) kan sammanfattas som insamling, analys och användning av information om aktuella och potentiella hot mot informationssäkerheten. Syftet med hotunderrättelser är att ge Intraservice insikter och förståelse för att bättre kunna identifiera, förebygga och reagera på säkerhetshot.

12. § Hot och hotunderrättelser ska inhämtas och analyseras för att löpande uppdatera hotbedömningar och risker.
13. § Hot och sårbarheter ska prioriteras av informationssäkerhetssamordnare.
14. § Om möjligt ska olika typer av hotaktörer och deras motiv identifieras kopplat till riskerna. Detta för att kunskap om vilka aktörer som utgör ett hot är kritiskt för att kunna formulera effektiva skyddsstrategier.
15. § Information om hot ska användas för att förebygga, upptäcka och hantera hot och därigenom proaktivt motverka risker riktat mot informationstillgångar.

Riskhanteringsprocess

Processen Utföra riskhantering för informationssäkerhet riktar sig till alla medarbetare inom Intraservice. Systematisk riskhantering av informationssäkerhet bidrar till förbättringar som kan kopplas till säkerheten i de tjänster som Intraservice levererar till andra samt till Intraservices egen användning av dessa tjänster och den riskhantering för informationssäkerhet som är kopplat till det egna användandet.

16. § Riskhanteringsprocessen samt stödjande material ska publiceras internt för alla medarbetare.
17. § Riskhanteringsprocessen ska användas minst årligen avseende förvaltning av tjänster, system och infrastruktur.
18. § Riskhanteringsprocessen ska också användas vid större utvecklingsinitiativ för att säkerställa god informationssäkerhet, i såväl nya som ändrade tjänster, system och infrastruktur.
19. § Riskhanteringsprocessen ska också gå att använda vid spontant behov av riskanalys (ad hoc) i sin helhet eller delar av den.
20. § Riskhanteringsprocessen utgår från att minst grundmetoden används. Användning kan också ske med en förenklad eller en utökad metod.

Riskförvaltning

Risker behöver följas upp och bevakas löpande för att ha en konkret och uppdaterad översikt över alla identifierade risker och de åtgärder som vidtagits.

21. § Risker ska följas upp genom att riskinformation från riskhantering som sker i förvaltningen samlas in, analyseras och grupperas i fyra nivåer: strategiskt, taktiskt, operativt och tekniskt.
22. § Risker och riskhantering ska dokumenteras i en riskförteckning för Intraservice (riskregister).
23. § Riskförteckningen ska revideras minst årligen.

24. § Riskuppföljning, riskanalysresultat och beslut om behandling av säkerhetsrisker ska kunna spåras över tid, vilket underlättar för framtida referens och lärande.

Övergripande risker dokumenteras och rapporters enligt Nämnden för Intraservice anvisning för styrning uppföljning och kontroll