Göteborgs Stad

**Tjänsteutlåtande**
Utfärdat 2024-06-12
Diarienummer 0206/24

Handläggare
Marcus Broman
Telefon: 031- 367 00 00
E-post: marcus.broman@intraservice.goteborg.se

# Intraservices anvisning för riskbaserat informationssäkerhetsarbete

## Förslag till beslut

I nämnden för Intraservice:

Intraservice anvisning för riskbaserat informationssäkerhetsarbete fastställs

## Sammanfattning

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.

I riktlinjens kravställning framgår tydligt att nämnder och styrelser ska ha ett riskbaserat förhållningssätt i informationssäkerhetsarbetet. Varje verksamhet ska identifiera, bedöma och följa upp informationssäkerhetsrisker.

Metoden för säker hantering av information innefattar flera steg och det åligger Intraservice att realisera hur detta ska ske. Först klassificerar informationsägaren informationen, sedan genomförs en riskanalys för att sedan vidta passande organisatoriska, personrelaterade, fysiska och tekniska åtgärder för säkerheten

Informationssäkerhet handlar om att skydda informationstillgångar genom att säkerställa konfidentialitet, riktighet och tillgänglighet. Konfidentialitet innebär att information inte delas med obehöriga, riktighet innebär att information skyddas mot oönskade förändringar och är korrekt, medan tillgänglighet innebär att informationen är tillgänglig och användbar när den behövs

Riskhantering innebär att säkerställa att konfidentialitet, riktighet och tillgänglighet av informationstillgångar skyddas. Genom riskanalyser kan potentiella hot och sårbarheter identifieras, vilket möjliggör att lämpliga åtgärder kan vidtas för att skydda informationen. På så sätt blir riskanalyser en central del av att säkerställa att informationen är skyddad och tillgänglig när den behövs.

Anvisning för riskbaserat informationssäkerhetsarbete syftar till att etablera en standardiserad hantering för att hantera risker för Intraservice. Målet är att minimera negativa effekter på verksamheten och säkerställa en systematisk och proaktiv hantering av potentiella hot.

Anvisningen konkretiserar stadens riktlinjer för informationssäkerhet avseende ett riskbaserat informationssäkerhetsarbete. Anvisningen ska säkerställa att Intraservice riskhantering avspeglar de specifika behoven och förutsättningarna inom den för

Intraservice, både för den egna förvaltningen och för leverans av tjänster till stadens verksamheter, specifikt vad gäller Intraservice uppdrag som leverantör av digital infrastruktur.

Förvaltningen bedömer därför att nämnden för Intraservice bör fastställa *Anvisning för riskbaserat informationssäkerhetsarbete* för att säkerställa att utförs systematiskt kvalitativt och med en standardiserad metodik

Förvaltningen bedömer även att nämnden för Intraservice bör fastställa en uppdatering av Anvisning för styrning, uppföljning och kontroll för att säkerställa att arbete med riskanalyser för informationssäkerhet kan utföras i underliggande nivåer. Ett separat tjänsteutlåtande behandlar uppdateringen av Anvisning för styrning, uppföljning och kontroll

## Bedömning ur ekonomisk dimension

Förvaltningen anser att implementeringen av en standardiserad grundmetod för riskhantering är nödvändig, särskilt med tanke på den ekonomiska dimensionen. Initialt förväntas arbetet med riskhantering medföra en betydande belastning på personella resurser.

Enligt Göteborgs Stads riktlinje för informationssäkerhet ska beaktas vid anskaffning, utveckling, underhåll och avveckling av IT-system. Vid upphandling av system ska informationssäkerhetskraven integreras och specificeras baserat på informationsägarens klassificering av informationen samt riskbedömningen.

Riskhanteringen ska också integreras vid implementering av fysiska säkerhetsåtgärder. Nämnder och styrelser är ansvariga för att säkerställa att informationsklassning, riskbedömning och informationens skyddsvärde tas i beaktande vid utformningen av det fysiska skalskyddet för att säkra informationstillgångar. Vid planeringen av centrala IT-utrymmen ska behovet av brandskydd, tillträdesskydd, skalskydd, el och reservkraft, miljö och kyla, skydd mot vätska, interiör, teknisk övervakning och larm samt andra relevanta faktorer utvärderas. Detta utgår från informationsklassning och riskanalys.

På längre sikt förutser förvaltningen att bedömningen av risker kommer att öka kostnaderna för införandet och förvaltningen av säkerhetsåtgärder. Dessa ökade kostnader beror inte direkt på själva riskhanteringsarbetet utan på de säkerhetskrav som kommer att kopplas till säkerhetsåtgärderna.

De åtgärder som vidtas förväntas markant förbättra säkerheten för information, vilket sannolikt kommer att leda till betydande kostnadsbesparingar över tid. Riskhantering är en viktig del av ett proaktivt och riskbaserat arbete för informationssäkerhet, vilket också kommer att vara ett krav enligt den föreslagna nya cybersäkerhetslagen (den svenska implementeringen av NIS2).[1]

För att undvika administrativa avgifter i samband med tillsyn bedömer förvaltningen att en standardiserad metod för riskhantering är nödvändig. Genom riskhantering kan

[1] se Nya regler om cybersäkerhet (SOU 2024:18) *Delbetänkande av Utredningen om genomförande av NIS2- och CER-direktiven.*

förvaltningen bedöma vilka risker som behöver hanteras med högre prioritet och vilka som inte kräver lika omfattande åtgärder. Det finns potential för kostnadsbesparingar då skyddsåtgärderna kan anpassas efter riskbedömningen.

## Bedömning ur ekologisk dimension

Förvaltningen har inte funnit några särskilda aspekter på frågan utifrån denna dimension

## Bedömning ur social dimension

En standardiserad modell för standardiserad grundmetod för riskhantering hjälper förvaltningen i bedömningen av vilken information som är särskild värd att skydda. För den enskilda invånaren innebär det sannolikt ett förhöjd skydd för känsliga personuppgifter och den personliga integriteten.

Särskilt utsatta grupper inom exempelvis socialförvaltningarnas eller Äldre samt vård- och omsorgsförvaltningens verksamheter kommer sannolikt omfattas av ett utökad skydd som ett resultat av arbete med riskhantering och informationsklassning.

En central aspekt i riskhantering leder tillsammans med informationsklassning till att bedöma krav på tillgänglighet för informationsmängder. Förvaltningen bedömer därför att åtgärden kommer stärka arbetet med Agenda 2030 kopplat till mål 16.10 *Säkerställa allmän tillgång till information och skydda grundläggande friheter.* Förvaltningen bedömer att arbetet med riskbaserat informationssäerkehtsarbete kommer stärka skyddet för den information som behövs för att upprätthålla kritiska samhällstjänster som bedrivs i kommunal regi och kommer därför även stärka mål 11B *Utveckla strategier för inkludering, resurseffektivitet och katastrofriskreducering.*

## Samverkan

Samverkan har skett med de fackliga representanterna i FSG 2024-05-23

## Bilagor

1. Anvisning för riskbaserat informationssäkerhetsarbete - nämnden för Intraservice
2. Process för riskhantering

## Ärendet

Föreslagen ny anvisning för riskbaserat informationssäkerhetsarbete och ändring i anvisning för styrning uppföljning och kontroll anger hur Intraservice ska arbeta riskhantering utifrån Göteborgs Stads riktlinje för informationssäkerhet. De två anvisningarna ska säkerställa att Intraservice riskhantering sker med en förutsägbar, standardiserad och kvalitetssäkrad metodologi

## Beskrivning av ärendet

### Bakgrund

Kommunfullmäktige fastställde den 25 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.

> *I takt med att omvärlden och den interna verksamheten förändras så förändras även behovet av informationssäkerhet. Göteborgs Stad behöver därför ha kunskap om de hot, risker och sårbarheter som påverkar eller som kan komma att påverka staden. Detta uppnås genom omvärldsanalys och genom att ha ett riskbaserat förhållningssätt i informationssäkerhetsarbetet.*
>
> *Ett riskbaserat förhållningssätt i informationssäkerhetsarbetet innebär att varje verksamhet ska identifiera, bedöma och följa upp informations-säkerhetsrisker och utifrån detta vidta lämpliga säkerhetsåtgärder.*
>
> Göteborgs Stads riktlinje för informationssäkerhet (KF 2023-05-25, § 7)

I riktlinjens kravställning framgår tydligt att nämnder och styrelser ska ha ett riskbaserat förhållningssätt i informationssäkerhetsarbetet. Riskbedömning samt informationsägarens klassificering av informationen är utgångspunkt vid anskaffning, utveckling, underhåll och avveckling av IT-system.

Metoden för säker hantering av information enligt riktlinjen innefattar flera steg och det åligger Intraservice att realisera hur detta ska ske. Först klassificerar informationsägaren informationen, sedan genomförs en riskanalys för att sedan vidta passande organisatoriska, personrelaterade, fysiska och tekniska åtgärder för säkerheten.

Göteborgs Stads riktlinje för informationssäkerhet anger att konfidentialitet, riktighet och tillgänglighet ska säkerställas:

- Konfidentialitet, att information inte tillgängliggörs eller avslöjas för obehöriga.
- Riktighet, att informationen skyddas mot oönskad förändring, att information är korrekt och inte manipulerad eller förstörd.
- Tillgänglighet, att information är tillgänglig och användbar när den behövs.

Riskhantering innebär att säkerställa konfidentialitet, riktighet och tillgänglighet av informationstillgångar är det nödvändigt att genomföra riskanalyser. Genom riskanalyser kan potentiella hot och sårbarheter identifieras, vilket möjliggör att lämpliga åtgärder kan vidtas för att skydda informationen. Genom att analysera risker kan man förutse potentiella hot mot konfidentialitet, riktighet och tillgänglighet och vidta åtgärder för att

minimera eller eliminera dessa risker. På så sätt blir riskanalyser en central del av att säkerställa att informationen är skyddad och tillgänglig när den behövs.

För att riktlinjen ska kunna efterlevas i praktiken krävs det ytterligare styrning från nämndens i syfte att konkretisera hur ett riskbaserat arbetssätt för informationssäkerhet ska genomföras i praktiken.

### Nuvarande modell

Intraservice ska enligt Göteborgs stads riktlinje för informationssäkerhet ha ett riskbaserat förhållningssätt i göra riskbedömningar av informationstillgångar vid anskaffning, utveckling, underhåll och avveckling av IT-system för den information som myndigheten innehar informationsägarskap för. Förvaltningen har i dagsläget ingen fastställd modell för riskhantering. Den befintliga modellen baseras på bästa praxis och ad hoc-lösningar som tillämpas oregelbundet och med varierande metoder beroende på den individ som leder arbetet.

Gemensamt för nuvarande tillvägagångssätt för riskhantering är att fokus ligger på den information som hanteras i Intraservices tekniska system, vilket resulterar i att det har varit svårt att särskilja den information som Intraservice är ansvarig för och den information som Intraservice förvaltar åt andra. Metodiken leder till att tjänsterna ofta måste göra en riskbedömning på information som tillhör Intraservices kunder som utgångspunkt för att kunna genomföra en riskanalys. I bästa fall har tjänsterna involverat ett urval av kunder vid riskanalysen. Detta tillvägagångssätt medför sina egna utmaningar, särskilt att urvalet av kunder är svårt att definiera, då antalet verksamheter som använder Intraservice tjänster är många.

Nuvarande modell försvårar bedömningen av var säkerhetskraven bör riktas eftersom det ofta finns bakomliggande infrastrukturkomponenter eller applikationer som är avgörande för att säkra informationen i systemet. Dessutom saknas en samordning av risker som kan uppstå på olika nivåer. Eftersom riskhanteringen i dess nuvarande utformning ofta endast tar hänsyn till systemet eller tjänsten som direkt berörs vid tillfället, uppstår utmaningar med att rikta krav mot tjänster, infrastrukturkomponenter eller applikationer som inte för närvarande är föremål för riskanalys, trots att dessa är avgörande för systemets funktion. Denna metodik riskerar därför att leda till att säkerhetskrav på understödjande komponenter i praktiken inte kommuniceras till ansvarig för dessa komponenter. En samordnad bedömning av risker är därför nödvändig för att säkerställa en effektiv och enhetlig hantering av säkerhetskrav.

Den nuvarande modellen för riskhantering inom Intraservice är heller inte sammanlänkad med *Anvisning för styrning, uppföljning och kontroll* för nämnden för Intraservice. Detta leder till bristande översyn och samordning för nämnden. Enligt Anvisning för styrning, uppföljning och kontroll ska riskhantering ske i Stratsys. Dock behöver riskhanteringen i förvaltningen genomföras på flera underliggande nivåer för olika typer av informationssäkerhetsrisker som inkluderar strategiska risker, finansiella risker, risker kopplade till efterlevnad av lagar/regelverk/styrande dokument och operativa risker.

### Föreslagen modell

Modellen består av två styrdokument, ett nytt och en ändring, med tillhörande bilagor:

- **Ny**: *Anvisning för riskbaserat informationssäkerhetsarbete - nämnden för Intraservice*. Anvisningen fördelar ansvar, mandat, terminologi och

grundläggande krav. Förvaltningens bedömning är att anvisningen behöver fastställas av nämnden eftersom den utpekar ansvar för genomförande av informationsklassning. Det ansvaret är sedan tidigare fördelat till nämnder och styrelser genom Göteborgs stads riktlinjer för informationssäkerhet. Anvisningen fördelar mandat till Intraservices informationssäkerhetschef (CISO[2]) att fastställa rutiner och instruktioner tillhörande anvisningen

- **Ändring**: *Anvisning för styrning, uppföljning och kontroll - nämnden för Intraservice*. En uppdatering föreslås som medger annat systemstöd än Stratsys. Ändringen hanteras i ett separat tjänsteutlåtande.[3]

Intraservice tillämpar en omfattande anvisning för informationssäkerhetsrisker, som inkluderar alla aspekter av risker, såsom konfidentialitet, riktighet och tillgänglighet. Metoden inkluderar riskanalysprocesser, hotanalys och övervakning av hot och sårbarheter. Strategisk, teknisk och operativ beslutsfattning integrerar riskhantering enligt stadens riktlinjer och enligt bästa praxis med ISO-standarder. En grundläggande process för riskanalys är basen, men utökade analyser kan användas vid behov.

### *Övergripande*

Övergripande hot-, risk- och sårbarhetshantering inom Intraservice baseras på Göteborgs Stads riktlinje för informationssäkerhet och ISO/IEC 27005-standarden. Riskhantering integreras i strategiska, tekniska och operativa beslut, där roller och ansvar tydligt definieras. Detaljerad information om roller, ansvar och befogenheter i detta sammanhang fastställs genom *Nämnden för Intraservices anvisning för informationssäkerhet*. Chefer innehar riskägaransvar, vilket inkluderar att identifiera, acceptera och hantera risker, vilket kräver tillgång till resurser och beslutsmandat. Slutligen har Intraservices CISO befogenhet att fastställa rutiner och instruktioner som stödjer denna ram för informationssäkerhet.

### *Hot- och riskbedömning*

Nu föreslagen modell bygger på att Intraservice har en grundmetod för riskanalys. Denna grundmetod utgör en bas och är enkel att genomföra, vilket gör den till en lämplig utgångspunkt för riskhanteringsprocessen. Grundmetoden kan tillämpas för olika typer av informationssäkerhetsrisker som inkluderar strategiska risker, finansiella risker, risker kopplade till efterlevnad av lagar/regelverk/styrande dokument och operativa risker.

Vid behov av djupare analys och för att hantera större risker eller prioritera hot, kan utökande riskanalyser användas. Utökande analysmetoder kräver mer av tid och kunskap för att genomföra, men ger samtidigt ett mer välgrundat underlag. Resultatet för utökade riskanalysmetoder ger ett detaljerat underlag för beslutsfattande och åtgärdsplanering. Denna metodik möjliggör en flexibel och anpassningsbar strategi för att hantera olika risknivåer och säkerhetsutmaningar inom Intraservice.

---

[2] CISO är en förkortning av *Chief Information Security Officer* och är ett vedertaget begrepp inom informationssäkerhetsområdet. Rollen/befattningen motsvaras av begreppet informationssäkerhetschef.

[3] Se 2024-06-10, Diarienummer 0483/23 *Tjänsteutlåtande - Anvisning för styrning, uppföljning och kontroll – nömnden för Intraservice.*

### *Hotunderrättelser och sårbarheter*

Anvisningen anger att Intraservices hantering av hot och sårbarheter följer en strukturerad process. Hot och hotunderrättelser samlas in och analyseras kontinuerligt för att hålla riskbedömningar uppdaterade. Informationssäkerhetssamordnare prioriterar sedan de identifierade hoten för att effektivt allokera resurser. Vikten av att identifiera hotaktörer och deras motiv betonas för att utforma effektiva skyddsstrategier. Genom att aktivt använda hotinformation kan hot förebyggas, upptäckas och hanteras proaktivt, vilket minskar risken för skada på informationstillgångar. Denna strategi syftar till att skydda Intraservice och stadens verksamhet mot potentiella hot och säkerhetsrisker.

### *Riskhanteringsprocess*

Riskhanteringsprocessen ska bidra till ökad medvetenhet inom informationssäkerhetsrisker och där det ingår att ge ett systematiskt sätt att identifiera hot och sårbarheter samt åtgärdsplaner för riskminimering.

Riskhanteringsprocessen och dess stödjande material ska tillhandahållas internt för samtliga medarbetare. Processen ska årligen tillämpas för att hantera tjänster, system och infrastruktur. Den ska även tillämpas vid utvecklingsinitiativ för att säkerställa robust informationssäkerhet i nya eller förändrade områden. Vid behov kan processen också användas för spontana riskanalyser (ad hoc), med en grundmetod som utgångspunkt.

### *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. För att säkerställa en effektiv riskhantering tillämpas en särskild instruktion för riskförvaltning. Samtliga riskhanteringsaktiviteter dokumenteras i en riskförteckning (riskregister), vilket bidrar till ökad översikt och transparens. För att hålla informationen aktuell och relevant, revideras riskförteckningen minst årligen. Genom att spåra riskuppföljning, riskanalysresultat och beslut om behandling av säkerhetsrisker över tid möjliggörs lärande och förbättringar baserade på tidigare erfarenheter och insikter.

## Riskhantering för gemensam säkerhet

Intraservice som tjänsteleverantör ska genomföra riskhantering för den information som ingen annan kan ta ansvar för. Det inkluderar främst information som Intraservice genererar i gemensamma databaser vid tjänstleverans. Dessutom ska tjänsterna genomföra riskhantering för information som uppstår i samband med tjänstleverans, inklusive funktions- och säkerhetsinformation enligt anvisningen. Detta säkerställer att eventuella risker identifieras och hanteras på samma strukturerade och proaktiva sätt för att skydda informationstillgångarna och säkerställa en säker och pålitlig tjänstleverans.

## Konkretisering, syfte och mål

Anvisning för riskbaserat informationssäkerhetsarbete konkretiserar stadens riktlinjer för informationssäkerhet avseende ett riskbaserat informationssäkerhetsarbete. Anvisningen ska säkerställa att Intraservice riskhantering avspeglar de specifika behoven och förutsättningarna som Intraservice har, både för den egna förvaltningen och för leverans av tjänster till stadens verksamheter, specifikt vad gäller Intraservice uppdrag som leverantör av digital infrastruktur.

Anvisningen syftar till att etablera en standardiserad hantering för att hantera risker för Intraservice. Målet är att minimera negativa effekter på verksamheten och säkerställa en systematisk och proaktiv hantering av potentiella hot.

Förvaltningen bedömer därför att nämnden för Intraservice bör fastställa Anvisning för riskbaserat informationssäkerhetsarbete för att säkerställa att utförs systematiskt kvalitativt och med en standardiserad metodik.

Förvaltningen bedömer även att nämnden för Intraservice bör fastställa en uppdatering av Anvisning för styrning, uppföljning och kontroll för att säkerställa att arbete med riskanalyser för informationssäkerhet kan utföras i underliggande nivåer enligt Anvisning för riskbaserat informationssäkerhetsarbete istället för i systemstödet Stratsys

*Delegering av mandat att fastställa rutin och instruktioner*

Förvaltningen bedömer att den tidigare modellen för riskhantering inte har uppfyllt förväntningarna som skett varierat och inte sammanhållet. Därför har en process utvecklats för att öka efterlevnaden med en grundmetod samt olika andra metoder. Emellertid kommer den höga detaljeringsgraden kräva kontinuerlig uppdatering, vilket kan bli betungande för både förvaltningen och nämnden att hantera regelbundet. Förvaltningen föreslår därför att Nämnden för Intraservices informationssäkerhetschef (CISO) delegeras att fastställa förändringar i processen kopplat till anvisningen.

## Förvaltningens bedömning

Riskhantering tillsammans med informationsklassning ställer krav på organisatoriska och tekniska säkerhetsåtgärder för Intraservices information. Syftet är att etablera en standardiserad hantering för att hantera risker för Intraservice. Målet är att minimera negativa effekter på verksamheten och säkerställa en systematisk och proaktiv hantering av potentiella hot. Bristfällig efterlevnad av ett riskbaserat informationssäkerhetsarbete kan resultera i att informationen får ett bristfälligt skydd med allvarliga konsekvenser

Utan en standardiserad metodologi riskerar Intraservice att inte uppfylla kraven i stadens styrande dokument samt uppfylla kommande cybersäkerhetslagstiftning (NIS2-direktivet).

Behovet av styrning och förtydligande på nämndnivå är angelägen med tanke på Intraservices särställning som tjänsteleverantör till övriga Staden. Det är avgörande att löpande bedriva en kvalitativ riskhantering för informationssäkerhet.

För att säkerställa enhetlig och samordnad hantering behövs detaljerade rutiner som regelbundet uppdateras.

Den omfattande detaljnivån i genomförandet i riskhanteringsprocessen innebär att regelverket periodvis måste anpassas för att hålla jämna steg med utvecklingen av systemstöd, lagar, styrdokument och andra relevanta faktorer.

Förvaltningen bedömer därför att nämnden bör fördela mandat att fastställa detaljerade rutiner och instruktioner för det riskbaserade informationssäkerhetsarbetets genomförande till Intraservices informationssäkerhetchef (CISO).

Stina Hall Hellqvist
Avdelningschef styrning och stöd

Peter Söderström
Förvaltningsdirektör