REMISSVERSION

Stockholms stad

# Riktlinje för informationssäkerhet i Stockholms stad


**Riktlinje för informationssäkerhet för Stockholms stad**

Dnr: xx xxxx/xxx | Utgivningsdatum: Juli 2021 | Utgivare: Stadsledningskontoret
Kontakt: xxxxxxxxxx@stockholm.se | Produktion: Blomquist Communication
Omslagsfoto: xxxxxxxxxxxx

# Om denna riktlinje

Denna riktlinje är en del av Stockholms stads kvalitetsprogram och reglerar arbetet med informationssäkerhet inom samtliga nämnder och bolag (nedan kallade *nämnder och styrelser*) i Stockholms stad (nedan benämnt *staden*).

Riktlinjen består dels av övergripande mål och principer för informationssäkerhetsarbetet och som beskrivs i detta dokument, dels av ett antal fördjupade tillämpningsanvisningar inom särskilda områden, exempelvis informationsklassning eller åtkomsthantering.

Riktlinjen beslutas av kommunfullmäktige och utgör en central del i stadens ledningssystem för informationssäkerhet.

Tillämpningsanvisningar beslutas av kommunstyrelsen eller av den kommunstyrelsen delegerat rätten att fatta beslut om dessa till.

Denna riktlinje är en del av Stockholms stads kvalitetsprogram och reglerar arbetet med informationssäkerhet inom samtliga nämnder och bolag i Stockholms stad.

# Bakgrund och syfte med riktlinjen

Stadens kvalitetsarbete syftar till att öka kvaliteten i genomförandet av det kommunala uppdraget och samtidigt möta dagens och morgondagens utmaningar. Det ställer krav på att staden utför ett grundläggande och systematiska informationssäkerhetsarbete i alla sina verksamheter. Denna riktlinje anger kommunfullmäktiges direktiv för detta arbete. Arbetet ska i sin tur bidra till att staden upprätthåller trygghet och förtroende hos medborgare, näringsliv och besökare, men också att lagar, förordningar och riktlinjer efterlevs.

Dagens informationssamhälle har lett till att grundläggande samhällsfunktioner är beroende av information i digitala tjänster. Detta beroende innebär i sin tur risker. Därför har kraven på skydd för information skärpts avsevärt genom lagstiftning, exempelvis dataskyddförordningen och NIS-direktivet samt regeringens strategi på nationell nivå. Både stadens ambitioner och svensk lagstiftning förutsätter en ändamålsenlig informationssäkerhet i stadens nämnder och styrelser.

Stockholm har som ambition att genom digitalisering skapa bättre kvalitet i stadens tjänster, frigöra personalens tid, minska miljöpåverkan och uppnå en mer kostnadseffektiv handläggning av ärenden. Om informationen innehåller fel, inte går att komma åt eller hamnar i fel händer kan inte trygghet, effektivitet och innovation uppnås i samma utsträckning. Därför måste stadens nämnder och styrelser arbeta systematiskt med informationssäkerhet i sina verksamheter.

# Definitioner

*Informationssäkerhet* är ett teknikneutralt begrepp vilket innebär skydd av information, oavsett om den är muntlig, pappersbunden eller digital. Med informationssäkerhet avses att rätt information ska finnas tillgänglig för rätt mottagare vid rätt tillfälle.

Skyddet avser därför att upprätthålla informationens:

- konfidentialitet
- riktighet
- tillgänglighet

Begreppet *konfidentialitet* ska ses i ett vidare perspektiv och omfattar både personlig integritet för enskilda och sekretess enligt offentlighets- och sekretesslagens mening, men även andra krav på att information inte ska komma obehöriga till del.

Med begreppet *riktighet* avses att information som hanteras ska vara oförvanskad och skyddad från otillåten manipulering. Dataskyddsförordningens grundläggande princip om riktighet har vidgat betydelsen av begreppet. Begreppet omfattar numera även att informationen ska vara riktig i den meningen att den är tillförlitlig och korrekt. Det innebär bland annat att rätt uppgifter hämtas från rätt datakälla för att användas i avsett syfte ~~(även kallat informationsarkitektur).~~ Det innebär även att felaktiga uppgifter ska rättas vid behov.

Begreppet *tillgänglighet* omfattar, förutom tillgång till information vid en given tidpunkt, även tillgänglighet över tid kopplat till bevarande och gallringsplaner enligt arkivbestämmelser.

Likaså är *spårbarhet* en nödvändig del av informationssäkerhetsarbetet. Med spårbarhet menas möjligheten att i efterhand följa aktiviteter som är vidtagna med informationen, exempelvis att en person haft åtkomst till eller ändrat viss skyddsvärd information.

*Dataskydd* innebär skydd av personuppgifter enligt kraven i dataskyddsförordningen. Dataskydd är en del av informationssäkerhetsarbetet i staden.

*Systematiskt informationssäkerhetsarbete* är det arbete som ska utföras inom nämnder och styrelser för att skapa det skydd och den goda informationskvalitet som verksamheten behöver för att utföra sitt uppdrag. Arbetet utförs inom tre områden; organisatorisk säkerhet, it-säkerhet och fysisk säkerhet.

*Organisatorisk säkerhet* omfattar bland annat att roller, ansvar och arbetsuppgifter är definierade av verksamheten. Det omfattar även fastställda processer, rutiner och styrdokument som stödjer medarbetare att utföra informationssäkerhetsåtgärder i det dagliga linjearbetet.

*It-säkerhet* omfattar de tekniska åtgärder som ska vidtas som en följd av att viss information hanteras i en it- tjänst, till exempel virusskydd, tekniska filter mot bluff-mail och kryptering.

*Fysisk säkerhet* omfattar de fysiska åtgärder som ska vidtas som en följd av att information behöver skyddas, med exempel begränsat tillträde till vissa byggnader, säkerhetsskåp eller kylsystem för servrar.



*It-tjänst* används som samlingsnamn i riktlinjen och omfattar exempelvis it-system, it-tjänster, it-infrastruktur, it-plattformar, IoT (Internet of Things), molntjänster, sensorer, styrsystem (OT) och datakommunikation.

## Tillämpning av standard för informationssäkerhetsarbetet

Stadens inriktning är att informationssäkerhetsarbetet inom nämnder och styrelser ska utgå från den internationella standarden SS-ISO/IEC 27001/2. Informationssäkerhetsarbetet ska alltid utföras med hänsyn tagen till stadens övergripande mål samt till nämnders och styrelsers egna verksamhetsuppdrag.

## Omfattning och avgränsningar för riktlinjen

Samtliga nämnder och styrelser i staden ska tillämpa denna riktlinje inklusive tillhörande tillämpningsanvisningar för all informationshantering. Dessa gäller för samtliga anställda, samt för externa uppdragstagare som leverantörer och konsulter.

Riktlinjen ska tillämpas i befintlig informationshantering och i samband med förändringar, utvecklingsarbete och upphandlingar.

Stockholms stads barn, elever och studerande i ~~de pedagogiska verksamheterna~~ omfattas av regelverket i den utsträckning det är tillämpbart.

### Avgränsning

Den verksamhet och informationshantering som träffas av säkerhetsskyddslagen omfattas inte av kraven i denna riktlinje. För sådan hantering gäller Säkerhetsskyddslagen samt av staden beslutade styrdokument för området.

## Beskrivning av Stockholms stads ledningssystem för informationssäkerhet

Stadens ledningssystem för informationssäkerhet sätter ramarna för hur staden styr, genomför och följer upp informationssäkerhetsarbetet.

Ledningssystemet för informationssäkerhet består av flera delar. Dels av styrdokument som är stadsövergripande och gäller för samtliga verksamheter. Dels av lokalt framtagna styrdokument som enbart gäller för den egna verksamheten. En beskrivning av de stadsövergripande styrdokumenten följer nedan.

- Riktlinje för informationssäkerhet (detta dokument). Styrdokumentet anger kommunfullmäktiges direktiv för stadens informationssäkerhetsarbete.
- Riktlinjen kompletteras med tillämpningsanvisningar som detaljerar krav för olika delområden i informationssäkerhetsarbetet, exempelvis informationsklassning eller behörighetshantering. Tillämpningsanvisningarna beslutas var och en för sig av kommunstyrelsen eller av den kommunstyrelsen delegerat rätten att fatta beslut om dessa till.
- Metodstöd, handböcker, mallar, utbildningsmaterial och liknande som ger stöd för olika analyser och aktiviteter som ska utföras i nämnder och styrelser.

Samtliga nämnder och styrelser i staden ska tillämpa denna riktlinje inklusive tillhörande tillämpningsanvisningar för all informationshantering.

En beskrivning av lokalt framtagna styrdokument följer nedan. Nämnder och styrelser ansvarar för att de lokala styrdokumenten upprättas för den egna verksamheten.

- En lokal anvisning som beskriver hur de övergripande reglerna för informationssäkerhetsarbetet tillämpas lokalt i den egna verksamheten (exempelvis hur den lokala informationssäkerhetsorganisationen ser ut, dess mandat och resurser, vem som ansvarar för att ta fram lokala styrdokument, hur arbetet följs upp med mera).
- Lokala styrdokument och informationssäkerhetsrutiner, exempelvis en incidentrutin, som är anpassade för specifika behov i verksamheten.

## Riskbaserat informationssäkerhetsarbete

Verksamheten ska arbeta med att identifiera, bedöma och följa upp de informationssäkerhetsrisker som kan uppstå i verksamhetens informationshantering,

För att upprätthålla ett informationssäkerhetsarbete som är aktuellt över tid ska nämnder och styrelser ha ett riskbaserat förhållningssätt i sitt informationssäkerhetsarbete. Det innebär att verksamheten ska arbeta med att identifiera, bedöma och följa upp de informationssäkerhetsrisker som kan uppstå i verksamhetens informationshantering, exempelvis i linjeverksamheten eller hos externa leverantörer. Riskarbetet är en del av verksamhetens arbete med internkontroll.

### Ansvarsfördelning för informationssäkerhet

Nedan följer de övergripande principer för roller och ansvar som gäller för stadens informationssäkerhetsarbete. Ansvarsfördelningen beskrivs i detalj i tillämpningsanvisningen för roller och ansvar.

### Ansvar för stadsgemensam styrning av informationssäkerhet

Ytterst är det *kommunfullmäktige* som ansvarar för de stadsövergripande direktiven för informationssäkerhetsarbetet genom denna riktlinje.

*Kommunstyrelsen* ansvarar för den strategiska ledningen och samordningen av det stadsövergripande informationssäkerhetsarbetet. Kommunstyrelsen fattar också beslut om tillämpningsanvisningar.

### Ansvar för tillämpning av reglerna i nämnder och styrelser

Nämnder och styrelser ansvarar för att det bedrivs ett effektivt och ändamålsenligt informationssäkerhetsarbete i den egna verksamheten, samt att reglerna i denna riktlinje och tillhörande tillämpningsanvisningar tillämpas.

Förvaltnings- och bolagschef ansvarar för den operativa styrningen, resurstilldelningen och uppföljningen av det lokala informationssäkerhetsarbetet.

Samtliga medarbetare, och övriga som denna riktlinje gäller, exempelvis leverantörer och konsulter, ska följa gällande regler avseende informationssäkerhet och verka för en god säkerhetskultur.

### Informationsägare

Informationsägare är den nämnd/styrelse som ansvarar för att den information som verksamheten hanterar är riktig och tillförlitlig samt ansvarar för hur informationen hanteras och sprids. Förvaltnings- eller bolagschef är nämndens/styrelsens operativa informationsägarrepresentant i linjen.

Informationsägaren ansvarar för att verksamhetens krav på informationssäkerhet fastställs genom informationsklassning.

Informationsägaren ansvarar för att resultatet från informationsklassningen tas om hand och efterlevs. Det innebär exempelvis att tekniska säkerhetskrav från informationsklassningen ska överlämnas till den som förvaltar den tekniska it-tjänsten, exempelvis en förvaltningsledare eller en it-leverantör. ~~Organisatoriska säkerhetskrav däremot, exempelvis krav på en rutin för uppföljning av behörigheter, ska implementeras av verksamheten själv.~~

## Vägledande mål och principer

Nämnder och styrelser ska bedriva informationssäkerhetsarbetet på ett systematiskt och riskbaserat sätt och vägledas av följande mål och principer.

- Ansvaret för informationssäkerhet är känt och accepterat. Roller med ansvar för informationssäkerhet har ledningens stöd och mandat för att kunna utöva ansvaret.
- Säkerhetsnivå och inriktning för arbetet bygger på riskanalyser och informationsklassningar.
- All information och alla it-tjänster har en ägare. Ägare av informationen respektive ägare av it-tjänster ansvarar för att dessa skyddas i enlighet med kraven i denna riktlinje samt kraven från genomförd klassning och riskanalys.
- Rätt information finns tillgänglig för rätt mottagare vid rätt tidpunkt på ett spårbart sätt. Den princip som styr vilken information som en mottagare får tillgång till är att tillgång endast ges då arbetsuppgifterna motiverar det samt att sekretessregler tillåter det.
- Arbetet med dataskydd är integrerat i det generella informationssäkerhetsarbetet.
- Informationssäkerhetsarbetet i nämnder och styrelser är utformat så att det tar hänsyn till de skiftande krav, behov och lagstiftning som gäller i olika verksamheter.
- ~~Skyddsåtgärder för de it-tjänster som används av en majoritet av nämnder och styrelser är prioriterade i informationssäkerhetsarbetet.~~
- Det finns en positiv säkerhetskultur som uppmuntrar engagemang hos alla anställda och övriga som denna riktlinje gäller, och bidrar till att regler efterlevs och ständig förbättring av informationssäkerheten uppnås. Samtliga medarbetare genomgår årligen de obligatoriska utbildningar för informationssäkerhet som är beslutade.

## Uppföljning

Stadens arbete med informationssäkerhet ska följas upp genom både interna granskningar och genom externa revisioner av oberoende part. Uppföljningen ska ske såväl inom samtliga nämnder och bolagsstyrelser som på stadsövergripande nivå. Stadens beslutade processer för internkontroll ska följas.

Stadens arbete med informationssäkerhet ska följas upp genom både interna granskningar och genom externa revisioner av oberoende part.

## Fördjupade tillämpningsanvisningar

Denna riktlinje kompletteras av ett antal fördjupande tillämpningsanvisningar inom ett antal områden, exempelvis inom informationsklassning, identitet och åtkomst samt incidenthantering.

Stockholms stad

start.stockholm