Göteborgs Stad

Handling 2023 nr 71

Revidering av Göteborgs Stads riktlinje för informationssäkerhet

Till Göteborgs kommunfullmäktige

Kommunstyrelsens förslag

Kommunstyrelsen tillstyrker stadsledningskontorets förslag i tjänsteutlåtande den 10 mars 2023 och föreslår att kommunfullmäktige beslutar:

1. Göteborgs Stads riktlinje för informationssäkerhet revideras i enlighet med bilaga 4 till stadsledningskontorets tjänsteutlåtande.
2. Göteborgs Stads regel för chefers informationssäkerhetsansvar upphör att gälla.
3. Göteborgs Stads regel gällande driftsdokumentation för IT-baserade informationssystem upphör att gälla.

Vid behandling av ärendet i kommunstyrelsen antecknade Jörgen Fogelklou (SD) som yttrande en skrivelse från den 4 april 2023.

Göteborg den 5 april 2023
Göteborgs kommunstyrelse

Jonas Attenius

Mathias Sköld

Yttrande
2023-04-04

Ärende nr: 2.1.11
Dnr: 0160/23

Yttrande angående – Revidering av Göteborgs Stads riktlinje för informationssäkerhet

Yttrandet:
Bristen på informationssäkerhetsarbete kan påverka samhällsviktig verksamhet. Det ska vara möjligt att upprätthålla driften av staden även vid kriser och därmed är det välkomnat att staden jobbar systematiskt med att höja nivån på informationssäkerheten. Inte nog med att en lättförståelig klassificeringsmodell av information föreslås till revideringen av *Göteborgs Stads riktlinje för informationssäkerhet*, dessutom kommer även två styrande dokument upphöra/slås samman för att bidra till ökad ändamålsenlighet och underlätta tillämpningen av denna riktlinje. Vi anser det vara exemplariskt att jobba med att förtydliga och förenkla genom att dra ner på antalet styrande dokument inom staden. Därmed ser vi gärna att detta tankesätt appliceras vid alla framtida revideringar av stadens styrande dokument.

Göteborgs Stad

Tjänsteutlåtande
Utfärdat 2023-03-10
Diarienummer 0160/23

Handläggare
Linda Larsson, Alberita Olluri
Telefon: 031-386 03 09, 031-368 01 82
E-post: linda.larsson@stadshuset.goteborg.se.
alberita.olluri@stadshuset.goteborg.se

Revidering av Göteborgs Stads riktlinje för informationssäkerhet

Förslag till beslut

I kommunstyrelsen och kommunfullmäktige:

1. Göteborgs Stads riktlinje för informationssäkerhet revideras i enlighet med bilaga 4 till stadsledningskontorets tjänsteutlåtande.
2. Göteborgs Stads regel för chefers informationssäkerhetsansvar upphör att gälla.
3. Göteborgs Stads regel gällande driftsdokumentation för IT-baserade informationssystem upphör att gälla.

Sammanfattning

Stadsledningskontoret har reviderat Göteborgs Stads riktlinje för informationssäkerhet utifrån behov av ökad användbarhet, tydligare styrning och vägledning samt ändrad och tillkommen lagstiftning inom informationssäkerhetsområdet.

De ändringar som gjorts i riktlinjen innefattar i huvudsak uppdatering av Göteborgs Stads klassificeringsmodell för att underlätta klassificering och säkerställa att informationen får ett tillräckligt och lämpligt skydd.

Avsnitten integritet och skydd av personuppgifter, informationssäkerhet vid införandet av nya system samt leverantörsrelationer har tillkommit i den omarbetade riktlinjen eftersom stadsledningskontoret bedömer att det finns behov att stärka dessa områden.

I revideringen av riktlinjen har även innehåll från Göteborgs Stads regel för chefers informationssäkerhetsansvar samt Göteborgs Stads regel gällande driftsdokumentation för IT-baserade informationssystem omhändertagits. Dessa stadsövergripande regler bedöms därmed kunna upphöra.

Stadsledningskontoret bedömer att den omarbetade riktlinjen, i jämförelse med nuvarande riktlinje, ger en tydligare styrning inom området informationssäkerhet.

Bedömning ur ekonomisk dimension

I stadens nuvarande klassificeringsmodell finns endast en nivå (2) för utökat skydd vilket gör att en stor mängd informationstillgångar får ett överskydd. Ett överskydd är både kostsamt och försvårar samarbete, kunskapsutbyte och hantering av information.

I den nya föreslagna klassificeringsmodellen blir det lättare att ge information och personuppgifter lämpligt skydd till rätt kostnad.

Ett systematiskt arbete med informationssäkerhet och en tydligare klassificeringsmodell underlättar för verksamheterna att vidta lämpliga säkerhetsåtgärder och medför ökad kvalitet och effektivitet. Det medför även minskad risk för cyberattacker, att informationen läcker till obehöriga, onödiga sanktionsavgifter, samt minskad risk för att samhällsviktig verksamhet råkar ut för avbrott.

Bedömning ur social dimension och ekologisk dimension

Bristande informationssäkerhetsarbete kan drabba samhällsviktig verksamhet. För att stadens verksamheter även vid kriser och IT-avbrott ska kunna upprätthållas på en acceptabel nivå krävs ett systematiskt arbete med informationssäkerhet.

Bilagor

1. Nuvarande Göteborgs Stads riktlinje för informationssäkerhet
2. Göteborgs Stads regel för chefers informationssäkerhetsansvar
3. Göteborgs Stads regel gällande driftsdokumentation för IT-baserade system
4. Förslag till reviderad Göteborgs Stads riktlinje för informationssäkerhet

Ärendet

Stadsledningskontoret har reviderat Göteborgs Stads riktlinje för informationssäkerhet. Den reviderade riktlinjen avser att ersätta nuvarande riktlinje vilken beslutades av kommunfullmäktige 2013-09-05 § 21. Göteborgs Stads regel för chefers informationssäkerhetsansvar samt Göteborgs Stads regel gällande driftsdokumentation för IT-baserade informationssystem har inarbetats i den reviderade riktlinjen och bedöms därmed kunna upphöra.

Beskrivning av ärendet

Information är viktig för Göteborg Stad och behöver skyddas efter behov. Ett bra informationssäkerhetsarbete skapar förtroende både inom och utanför organisationen.

Information som går förlorad eller hanteras felaktigt kan leda till allvarliga konsekvenser både för organisationer och för den enskilda människan.

Informationssäkerhet innebär skydd av informationstillgångar avseende:

- *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.

Informationsklassificering möjliggör att information skyddas på ett lämpligt sätt vilket höjer kvalitet och effektivitet genom att undvika att information får ett överskydd med höga kostnader som följd eller tvärtom att information inte får det skydd som den behöver.

Nuvarande Göteborgs Stads riktlinje för informationssäkerhet togs fram 2013. Sedan 2013 har lagstiftning som ställer ökade krav på informationshantering trätt i kraft. Däribland Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-direktivet) samt Dataskyddsförordningen (GDPR).

Vidare har EU-parlamentet och Europiska rådet antagit en revidering av NIS-direktivet (NIS-2) vilket förväntas träda i kraft i Sverige september 2024. Revideringen av NIS innebär bland annat att kraven skärps på systematiskt informationssäkerhetsarbete, att fler offentliga verksamheter kommer att beröras och att sanktionsavgifterna kommer att höjas. Genom att revidera Göteborgs Stads riktlinje för informationssäkerhet tar staden höjd för kommande ändring i lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-direktivet).

Digitalisering, artificiell intelligens (AI) och andra smarta produkter påverkar både staden och vår omvärld. Behovet och beroendet av tillgång till digital information ökar allt mer. Det innebär möjligheter men också ökad risk för sårbarheter, cyberattacker och intrång i stadens system. För att lyckas med den digitala resan måste staden arbeta systematiskt med informationssäkerhet. Ett systematiskt informationssäkerhetsarbete bidrar till att minimera risken för att samhällsviktiga verksamheter drabbas av avbrott, samt för att undvika att konfidentiell information och känsliga personuppgifter görs tillgängliga för obehöriga.

Ny klassificeringsmodell

Klassificering av information utgår från de tre säkerhetsaspekterna konfidentialitet, riktighet och tillgänglighet. Klassificeringen görs utifrån de konsekvenser eller skada som bristande säkerhet skulle kunna medföra med avseende på perspektiven verksamhet, samhälle, individ, ekonomi och förtroende för stadens verksamheter. Genom att klassificera information är det möjligt att identifiera känslig och kritisk information och därefter vidta lämpliga säkerhetsåtgärder så att informationen får ett tillräckligt och lämpligt skydd.

I nuvarande riktlinje finns en modell för klassificering som bygger på tre nivåer (nivå 0- inga skyddsåtgärder, nivå 1 - grundsäkerhetsnivå och nivå 2 - ökad skyddsnivå). Det saknas tydlig beskrivning av konsekvensnivåerna, vilket normalt är standard för en klassificeringsmodell. Det gör att verksamheterna har svårt förstå och använda dagens modell.

Med endast en nivå (2) för utökat skydd så har verksamheten svårt att hantera information utifrån lag- och verksamhetskrav. Det gör att en stor mängd informationstillgångar får ett överskydd vilket både blir kostsamt och försvårar samarbete, kunskapsutbyte och hantering av information.

Stadens nya klassificeringsmodell bygger i stället på fyra nivåer:

- Nivå 0 Försumbar skada – inga skyddsåtgärder
- Nivå 1 Måttlig skada – grundsäkerhetsnivå
- Nivå 2 Betydande skada – utökad skyddsnivå
- Nivå 3 Allvarlig skada – hög skyddsnivå.

Modellen har utformats i enlighet med riktlinjer från såväl Myndigheten för samhällsskydd (MSB) som Sveriges kommuner och regioner (SKR). I modellen framgår det även att det finns en nivå 4 för Sveriges säkerhet (information som går under säkerhetsskyddsslagstiftningen). Nivå 4 är enbart för kännedom och hanteras utanför denna riktlinje i enlighet med Göteborgs Stads riktlinje för säkerhetsskydd.

Den nya klassificeringsmodellen ger nämnder och styrelser större möjlighet att klassificera information rätt och möjliggör för verksamheten att vidta lämpliga skyddsåtgärder så att informationen varken får ett för lågt eller ett för högt skydd.

Tillägg i den reviderade riktlinjen

Informationssäkerhet handlar om att arbeta förebyggande genom ett systematiskt informationssäkerhetsarbete. I stadens nuvarande riktlinje saknas styrning för flera viktiga områden. Områden som har tillkommit är: integritet och skydd av personuppgifter, informationssäkerhet vid införande av nya system samt leverantörsrelationer. Nedan redogörs för innehållet i dessa områden.

Integritet och skydd av personuppgifter

Avsnittet innefattar riktlinjer om att verksamheten ska upprätthålla personlig integritet och skydd av personuppgifter enligt tillämpliga lagar, författningar och avtalskrav. Dataskydd är en del av informationssäkerhetsarbetet eftersom även personuppgifter ska klassificeras för att lämpliga säkerhetsåtgärder ska kunna vidtas.

Informationssäkerhet vid införandet av nya system

Det är viktigt att informationssäkerhet beaktas tidigt i samband med införande av nya system. Det behöver tidigt upprättas krav för att säkerställa att informationssäkerheten är tillräcklig, detta för att undvika kostnader och att stadens verksamheter har system som inte kan användas.

Avsnittet innefattar riktlinjer gällande verifiering av leverantörers informationssäkerhet och handlar om att säkerställa att de system som staden inför har det förväntade skyddet på säkerhet som staden betalat för. Det handlar också om att säkerställa att det inte finns några okända sårbarheter i systemets säkerhet som kan skada staden.

Leverantörsrelationer

I takt med att staden köper in molntjänster och att stadens information hanteras av externa leverantörer blir det viktigt att granska informationssäkerheten hos leverantör. Det är även viktigt att reglera vad leverantören får göra med information och personuppgifter samt ange återställningstid för hur länge en tjänst får ligga nere. Sårbarheter i en tjänst som staden integrerar med kan orsaka störningar som kan påverka hela stadens nätverk och system. I den kommande ändringen av NIS-direktivet ligger stort fokus på att kravställa leverantörer av digitala tjänster.

Tre stadenövergripande styrande dokument blir ett

I Göteborgs Stads plan för digitalisering 2023-2026 finns en insats om att genomföra en översyn av riktlinjen för informationssäkerhet och de styrande dokument som angränsar till denna för att säkerställa ändamålsenlig styrning och tillämpning.

Stadsledningskontoret har i detta ärende reviderat riktlinjen och påbörjat översynen av angränsande dokument. Tre stadenövergripande styrande dokument, Göteborgs Stads riktlinje för informationssäkerhet, Göteborgs Stads regel för chefers informationssäkerhetsansvar samt Göteborgs Stads regel gällande driftsdokumentation för IT-baserade system, slås samman och blir till ett styrande dokument.

Det som tidigare var under Göteborgs Stads regler för chefers informationssäkerhetsansvar ligger i huvudsak under avsnittet personalrelaterade åtgärder i den omarbetade riktlinjen. Innehåll från Göteborgs Stads regler gällande driftsdokumentation för IT-baserade system har i huvudsak hamnat under avsnittet tekniska säkerhetsåtgärder.

Sammanslagningen bedöms bidra till ökad ändamålsenlighet och underlättar tillämpningen av styrande dokument och därigenom arbetet med informationssäkerhet.

Tydligare ansvarsfördelning

Utöver uppdatering av klassificeringsmodell och tillagda avsnitt gällande integritet, leverantörsrelationer och informationssäkerhet vid införande av nya system har innehållet i den omarbetade riktlinjen strukturerats på ett sätt så att ansvar och roller blir tydligare.

I riktlinjen för informationssäkerhet beskrivs hur staden ska arbeta systematiskt med informationssäkerhet på en övergripande nivå. Nämnder och styrelser ansvarar för att tillämpa riktlinjen utifrån den egna verksamhetens behov av att skydda sin information.

Genomförande av den omarbetade riktlinjen

Stadsledningskontoret har i omarbetningen av riktlinjen för informationssäkerhet haft dialogmöten med stadens verksamheter, samt haft löpande kontakt med berörda funktioner i stadens nämnder och styrelser.

Det är ett önskemål från stadens nämnder och styrelser att få en standardiserad klassificeringsmodell likt SKR:s och MSB:s metodstöd för klassificering. Stadens verksamheter har både svårt att klassificera den egna informationen, och svårt att tyda inkommen klassificerad information från andra myndigheter, kommuner och organisationer. Verksamheterna är redan bekanta med den uppdaterade klassificeringsmodellen, och stadsledningskontoret bedömer att det finns ett positivt mottagande i förvaltningar och bolag för de förändringar som föreslås i riktlinjen.

Stadsledningskontorets bedömning

Syftet med Göteborgs Stads riktlinje för informationssäkerhet är att skapa förutsättningar för ett systematiskt och långsiktigt informationssäkerhetsarbete. Revideringen av riktlinjen och stadens klassificeringsmodell möjliggör för detta.

Nya lagkrav, förändringar i omvärlden, införandet av digitala system och artificiell intelligens (AI) kräver nya sätt att tänka kring informationssäkerhet. Stadsledningskontorets bedömning är att den omarbetade riktlinjen och klassificeringsmodellen är en förutsättning för att staden ska kunna arbeta systematiskt med informationssäkerhet.

Vid sidan av riktlinjen för informationssäkerhet har det även initierats ett nätverk för informationssäkerhet bestående av representanter från alla staden förvaltningar och bolag. Nätverket syftar till kunskaps- och erfarenhetsutbyte och bidrar också till att stärka arbetet med informationssäkerhet.

I nuvarande styrmiljö för informationssäkerhet finns flera underliggande stadsövergripande reglerande styrande dokument i form av regler. Styrmiljön upplevs som svår att överskåda och tillämpa. Stadsledningskontoret har därför i revideringen av riktlinjen för informationssäkerhet omhändertagit innehåll från Göteborgs Stads regel för chefers informationssäkerhetsansvar samt Göteborgs Stads regler gällande driftsdokumentation för IT-baserade system. Detta bedöms bidra till en mer överblickbar och sammanhållen styrmiljö. Stadsledningskontoret avser att se över resterande närliggande styrande dokument och vid behov återkomma i frågan.

Stadsledningskontoret bedömer att de ändringar som gjorts i riktlinjen, vad gäller ny klassificeringsmodell, tillkommen styrning, tydligare ansvarsfördelning, sammanslagning av styrande dokument samt språkliga justeringar, förväntas medföra en mer ändamålsenlig styrning.

Christina Eide
Direktör Utveckling av stadens verksamheter

Eva Hessman
Stadsdirektör

Göteborgs Stad

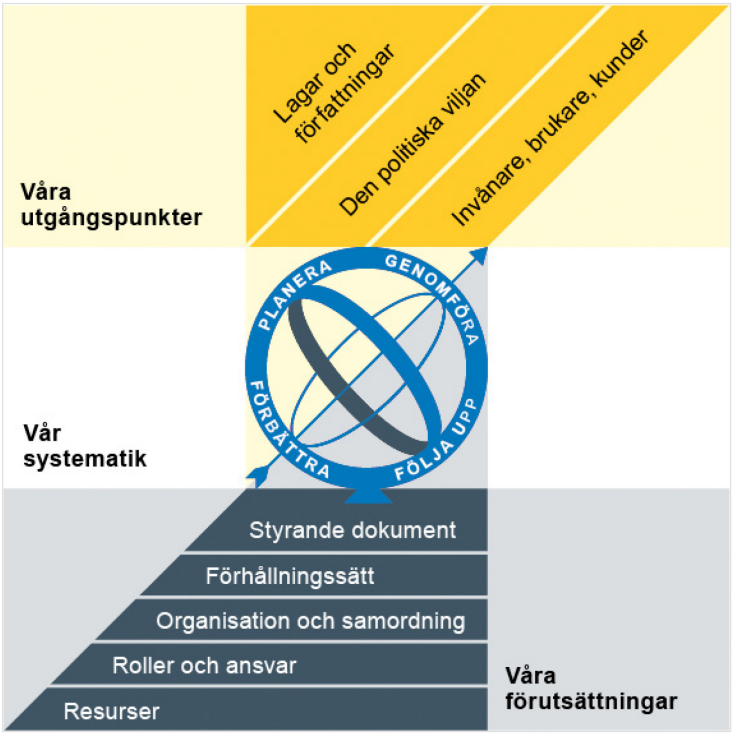
Göteborgs Stads riktlinje för informationssäkerhet

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.

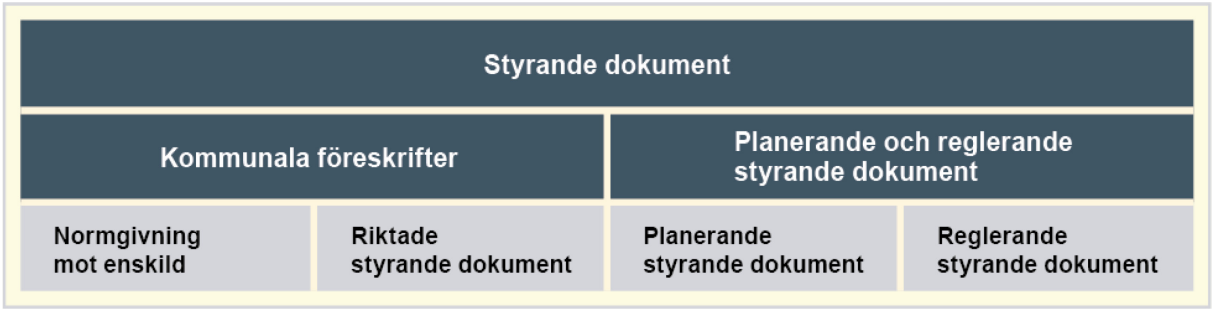


Om Göteborgs Stads styrande dokument

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.



Dokumentnamn: Göteborgs Stads riktlinje för informationssäkerhet			
Beslutad av: Kommunfullmäktige	Gäller för: Stadens nämnder och styrelser	Diarienummer: 0540/14 (0110/19)	Datum och paragraf för beslutet: 2013-09-05, § 21
Dokumentsort: Riktlinje	Giltighetstid: Tillsvidare	Senast reviderad: 2019-12-16	Dokumentansvarig: Informationssäkerhetschef
Bilagor: [Bilagor]			

Innehåll

Inledning

Syftet med denna riktlinje

Denna riktlinje syftar till att konkretisera säkerhetspolicyn avseende informationssäkerhetsområdet. Med informationssäkerhet avses att upprätthålla:

- Konfidentialitet, informationstillgångar är tillgängliga endast för behöriga
- Riktighet, informationstillgångar förändras eller påverkas inte oönskat eller utom kontroll
- Tillgänglighet, informationstillgångar kan nyttjas efter behov i förväntad utsträckning och inom önskad tid

Med informationstillgångar avses all information och informationshanterande resurser såsom manuella samt digitaliserade och IT-baserade informationssystem

Vem omfattas av riktlinjen

Denna riktlinje gäller tillsvidare för Stadens nämnder och styrelser.

Koppling till andra styrande dokument

Riktlinjen konkretiseras i underliggande regler.

Riktlinje

Inledning

Denna riktlinje beskriver den grundsäkerhetsnivå som gäller för all informationshantering i Göteborgs Stad som blivit klassad i nivå 1 för ett eller flera av skyddsområdena konfidentialitet, riktighet eller tillgänglighet.

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

För information som klassats i nivå 0 avseende alla de tre skyddsområdena konfidentialitet, riktighet eller tillgänglighet finns inga stadsövergripande krav på skyddsåtgärder.

Klassning av information

- Informationsklassning ska göras kontinuerligt av informationsägaren
- Informationslassningen ska ligga till grund för hur informationen ska hanteras i verksamheten
- Informationsklassningen skall utformas så att tillgången till information och öppenheten inom stadens verksamheter förblir så stor som möjligt för intressenter och allmänhet
- Tillämpliga lagar och andra giltiga styrdokument skall alltid uppfyllas och vägas in i informationsklassningen
- Nedanstående modell ska användas vid informationsklassningen

Kravnivå		Konfidentialitet	Riktighet	Tillgänglighet
Nivå 2	**Klassningsaspekt**	Känslig information som kan medföra **allvarlig skada** för egen eller annan organisations verksamhet eller för enskild person om den röjs för obehörig	Information som kan medföra **allvarlig skada** för egen eller annan organisations verksamhet eller för enskild person om den är felaktig.	Information som ingår i eller stöder kontinuerlig och kritisk verksamhet där avbrott innebär att man inte kan upprätthålla nödvändig tillgänglighet och servicenivå. Avbrott kan medföra **allvarlig skada** för egen eller annan organisations verksamhet eller för enskild person
Nivå 1 **GRUNDSÄKERHETSNIVÅ**	**Klassningsaspekt**	Information som kan medföra **skada** för egen eller annan organisations verksamhet eller för enskild person om den röjs för obehörig	Information som kan medföra **skada** för egen eller annan organisations verksamhet eller för enskild person om den är felaktig	Information som ingår i eller stöder kontinuerlig verksamhet där avbrott kan medföra **skada** för egen eller annan organisations verksamhet eller för enskild person
Nivå 0	**Klassningsaspekt**	Information som är öppen och avsedd för eller kan spridas till en obestämd krets mottagare utan risk för negativa konsekvenser. Spridning medför **ingen skada.**	Information som kan förändras utan risk för negativa konsekvenser Oriktig information medför försumbar eller **ingen skada**	Information med lågt verksamhetsberoende. Kan vara otillgänglig en längre tid utan risk för negativa konsekvenser. Brist på åtkomst medför försumbar eller **ingen skada.**

Hantering av informationstillgångar

- Samtliga informationssystem ska finnas förtecknade. I förteckningen beskrivs ändamål samt ansvarsfördelning såsom informationsägare, systemägare etc

- Tillämpliga regler, lagar, avtalsrättsliga åtaganden etc ska klart och tydligt definieras och dokumenteras för respektive informationssystem
- Informationsägaren ansvarar för informationsklassningen och att erforderligt skydd införs samt att säkerheten uppfyller ställda och rättsliga krav
- Alla som hanterar informationstillgångar har ett ansvar att upprätthålla informationssäkerheten

Personalresurser och säkerhet

- Kraven som ställs på personer som ska få tillgång till information och informationssystem ska vara definierade
- Personer som ska få tillgång till information och informationssystem ska ha tillräckliga kunskaper om informationssäkerhet i förhållande till sina arbetsuppgifter
- Det ska finnas användarinstruktion för respektive informationssystem
- Användarinstruktionen ska utformas på ett sådant sätt att en användares behov av att sätta sig in i detaljer kring gällande lagstiftning/regler för informationssystemet minimeras

Fysisk och miljörelaterad säkerhet

- Tillträde till lokaler som behöver skyddas mot obehörigt tillträde ska regleras och styras utifrån de krav som ställs av vederbörandes arbetssituation
- För säkerställande av centrala utrymmen med IT-baserade informationssystem, såsom datorhallar, ska
    - det fysiska skyddet ska vara entydigt definierat och dokumenterat där dokumentationen är skyddad från åtkomst av obehöriga
    - vara försett med ett skalskydd som är motståndskraftigt mot forcering och som är i nivå med skyddsklass 3 enligt Svenska Stöldskyddsföreningen
    - tillträde regleras restriktivt och strikt styras utifrån de krav som ställs av vederbörandes arbetssituation
    - det finnas dokumenterade besöksrutiner som inkluderar säkerställd besökslogg
    - besökare lätt kunna identifieras
    - besökare övervakas av behörig personal
    - larm med larmmottagare finnas för inbrott, brand, temperatur och fukt
    - systematiskt brandskyddsarbete enligt statens Räddningsverks allmänna råd bedrivas

Styrning av kommunikation och drift

- Det ska finnas en formellt beslutad driftdokumentation för IT-baserade informationssystem som minst omfattar återstarts- och återställningsrutiner, incidenthantering, ändringshantering samt hantering av logginformation. Ansvar gällande drift inkl system- och säkerhetsadministration ska också vara tydliggjort
- Loggning och skapande av spårbarhet för viktiga och säkerhetskritiska händelser ska ske. Loggning och loggarna ska skyddas för obehöriga samt vid behov analyseras och kunna nyttjas vid incidentutredningar
- Det ska för IT-baserade informationssystem finnas upptäckts- och skyddsåtgärder mot oönskad programkod och obehörigt nyttjande

Styrning av åtkomst

- Åtkomst och behörighet till informationstillgångar ska ges restriktivt och strikt styras utifrån de krav som ställs av vederbörandes arbetssituation
- Ansvarsfördelning och uppdelning av arbetsuppgifter ska tillämpas så att risken för missbruk begränsas
- För IT-baserade informationssystem ska endast ett fåtal personer erhålla privilegierade behörighet samt åtkomst till källprogramarkiv, operativsystem, systemhjälpmedel och revisionshjälpmedel
- Regelverk och rutin för registrering och avregistrering av behörigheter och åtkomst samt tilldelning av lösenord för IT-baserade informationssystem ska dokumenteras och finnas formellt beslutad
- Autentisering och åtkomstkontroll till IT-baserade informationssystem (gäller ej för öppen information) ska baseras på minst lösenord och bygga på unika användaridentiteter som är personliga och som ej får delas med andra
- Det ska finnas dokumenterade regler för vad som är tillåtet för anslutningar mellan IT-baserade informationssystem

Anskaffning, utveckling och underhåll

- Säkerhetsaspekter ska beaktas vid utveckling och anskaffning av informationssystem så att tillräckligt skydd uppnås. Att säkerhetsrutiner och regelverk efterlevs och motsvarar verksamhetens krav under informationssystemets hela livscykel inklusive avveckling och destruktion ska säkerställas och följas upp regelbundet
- System-/programutveckling och tester av modifierade IT-baserade informationssystem ska ske åtskilt från driftmiljön
- Det ska finnas formellt beslutade rutiner för ändringshantering för att inte åsidosätta befintliga skyddsåtgärder samt för att skapa ändringshistorik
- Det ska finnas regler för hur system- och programutveckling ska genomföras samt för installation av programvaror i IT-baserade informationssystem som är i drift
- Upphovsrättsliga frågor ska vara reglerade i avtal
- All systemdokumentation ska i rimlig omfattning och grad vara fullständig och aktuell samt uppdateras vid förändringar i informationssystem. Systemdokumentationen ska minst omfatta vad informationssystemets olika delar består av, en övergripande beskrivning av de olika delarnas uppgift samt en dokumentation över de funktioner som är relevanta för säkerheten
- IT-baserade informationssystem ska regelbundet analyseras för att identifiera sårbarheter eller problem som eventuellt kan orsaka incidenter så att bedömning och åtgärdande kan ske

Hantering av incidenter

- Det ska finnas en formell fastlagd rutin för hur informationssystemets användare ska agera vid incidenter
- Det ska finnas rutiner för rapportering, loggning, åtgärdande, informationsspridning, eskalering, uppföljning och analys av incidenter

Kontinuitetsplanering i verksamheten

- Det ska finnas formella beslut gällande den längsta tid som information kan vara otillgänglig eller informationssystemet bedöms kunna vara ur funktion innan

verksamheten påverkas i oacceptabel omfattning. Till grund för beslut ligger resultat från genomförda riskanalyser

- Grundat på verksamhetskraven ska det finnas en dokumenterad och formellt beslutad kontinuitetsplan. Övervägande om det finns behov av katastrofplanering ska ske
- Kontinuitetsplaner som inkluderar IT-baserade informationssystem ska omfatta återstarts- och reservrutiner för driftverksamheten som vidtas inom ramen för ordinarie drift så att återstart kan ske inom fastställd tid
- Återstarts- och reservrutiner för IT-baserade informationssystem såsom säkerhetskopiering och återläsning ska finnas och vara dokumenterade samt verifierade och anpassade för aktuell verksamhet
- Kontinuitetsplanen ska hållas aktuell och helt eller delvis testas årligen samt finnas tillgänglig för berörda i händelse av avbrott

Uppföljning av säkerhetsnivå

- Verksamhetens ledning ska kontinuerligt följa upp att säkerhetsnivån är acceptabel
- Uppföljning av informationssäkerhetsnivån i form av intern kontroll ska ske minst årligen. Resultatet rapporteras till nämnd/styrelse

Definitioner

Nedan återfinns definitioner på begrepp som tillämpas i denna riktlinje.

Begrepp	Definition
Autentisering	Verifiering av uppgiven identitet.
Identitet	Unik beteckning för en viss individ eller ett visst föremål
Incident	Händelse som resulterat eller som kunnat resultera i en skada eller oönskade konsekvenser för verksamheten
Informationssystem	Rutiner, metoder, procedurer etc organiserade för behandling av information, såväl manuella som helt eller delvis IT-baserade
Informationssäkerhet	Säkerhet beträffande informationstillgångar rörande förmågan att bevara och upprätthålla konfidentialitet, riktighet och tillgänglighet.
Informationstillgång	All information och informationshanterande resurser såsom manuella samt digitaliserade och IT-baserade informationssystem
Informationsägare	Generellt den som bestämmer ändamålen med och medlen för behandling och hantering av informationen. Ansvaret för informationen och dess säkerhet följer med ansvaret för verksamheten.
Kontinuitetsplan	Beskriver hur verksamheten ska bedrivas när kritiska verksamhetsprocesser allvarligt påverkas under en längre tid.
Logg	Insamlad information om händelser som sker/utförs
Lösenord	Teckensträng som anges för att verifiera en identitet
Revisionshjälpmedel	System, program, funktioner etc som kan användas för att identifiera brister och/eller tydliggöra uppfyllelse av krav, regelverk, standarder etc
Skalskydd	Skyddet som finns för den omslutningsyta, såsom väggar, golv, tak, dörrar etc, som avgränsar en lokal från omvärlden
Skyddsåtgärd	Handling, procedur eller tekniskt arrangemang som, genom att minska sårbarheten möter identifierat hot.
Spårbarhet	Möjlighet att entydigt kunna härleda utförda aktiviteter i systemet till en identifierad användare.

Göteborgs Stad

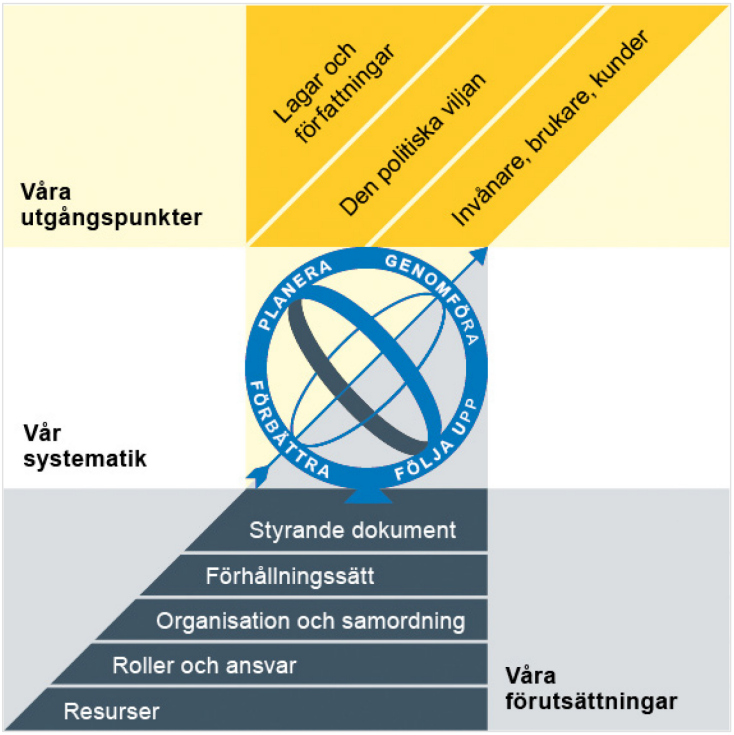
Göteborgs Stads regel för chefers informationssäkerhetsansvar

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.

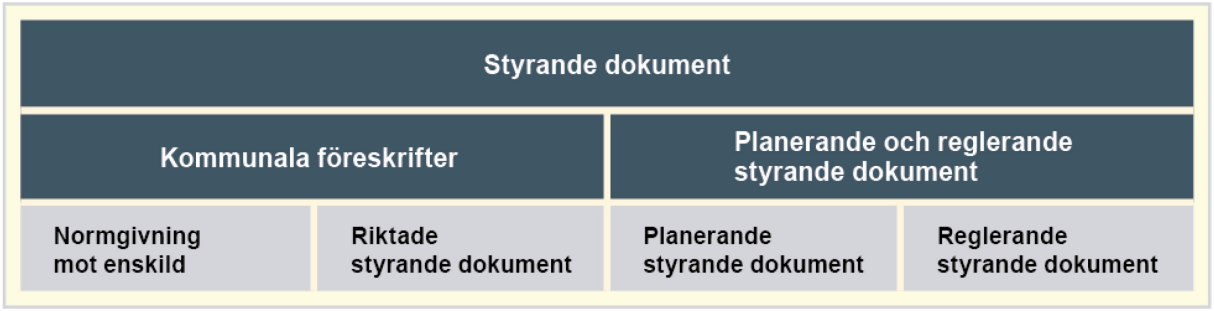


Om Göteborgs Stads styrande dokument

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: Göteborgs Stads regel för chefers informationssäkerhetsansvar			
Beslutad av: Kommunfullmäktige	Gäller för: Stadens nämnder och styrelser	Diarienummer: 0347/08 (0110/19)	Datum och paragraf för beslutet: 2009-09-10 §17
Dokumentsort: Regel	Giltighetstid: Tillsvidare	Senast reviderad: 2019-12-16	Dokumentansvarig: Informationssäkerhetschef
Bilagor: [Bilagor]			

Innehåll

Inledning

Syftet med dessa regler

Dessa regler fastställer ansvar och åtagande för chefer gällande informationssäkerhet i Göteborgs Stad.

Vem omfattas av dessa regler

Reglerna gäller tillsvidare för Stadens nämnder och styrelser.

Koppling till andra styrande dokument

Dessa regler konkretiserar Stadens säkerhetspolicy samt riktlinjen för informationssäkerhet.

Regler

Som chef i Göteborgs Stad har man för sitt chefsområde ett ansvar att

- Vid rekrytering av nya medarbetare, i proportion till kommande arbetsuppgifter, genomföra referenstagning och registerkontroll. Identitetskontroll ska alltid ske, företrädesvis via fullgod legitimationshandling såsom körkort, pass eller identitetskort utfärdat av bank
- I säkerhetshänseende, regelbundet informera sin personal, även inhyrd/inlånad sådan, om regelverk, rutiner och ansvar samt vidta åtgärder för att minska personberoendet såsom att dokumentera processer, rutiner etc
- Säkerställa att personalen har kunskap om och förståelse för tillämpliga säkerhetsrutiner och regelverk
- Säkerställa och regelbundet följa upp att säkerhetsrutiner och regelverk efterlevs
- Följa upp samt initiera upplägg, förändring och borttag av behörigheter till informationssystem, lokaler etc
- Säkerställa att information, informationsbärande utrustning/media, passerkort, tjänstekort etc återlämnas samt att alla behörigheter till informationssystem, lokaler etc inaktiveras vid medarbetares avslut

Göteborgs Stad

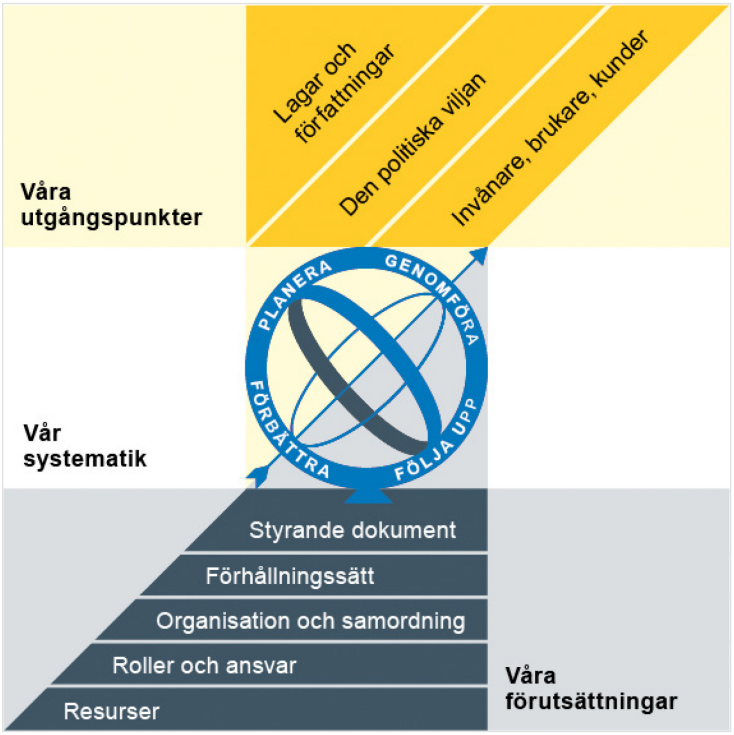
Göteborgs Stads regel gällande driftsdokumentation för IT-baserade informationssystem

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.

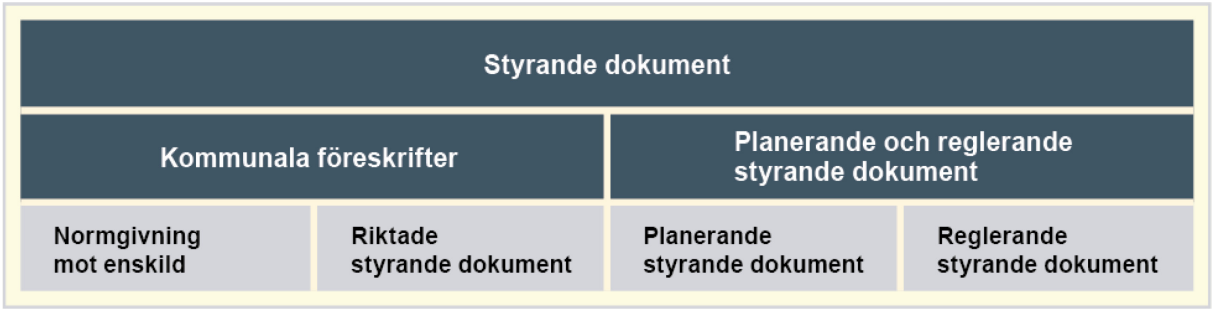


Om Göteborgs Stads styrande dokument

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: Göteborgs Stads regel gällande driftsdokumentation för IT-baserade informationssystem			
Beslutad av: Kommunfullmäktige	Gäller för: Stadens nämnder och styrelser	Diarienummer: 0347/08 (0110/19)	Datum och paragraf för beslutet: KF 2009-09-10, § 17
Dokumentsort: Regel	Giltighetstid: Tillsvidare	Senast reviderad: 2019-12-16	Dokumentansvarig: Informationssäkerhetschef
Bilagor: [Bilagor]			

Innehåll

Inledning

Syftet med dessa regler

Dessa regler fastställer den driftsdokumentation som minst måste finnas för IT-baserade informationssystem. Reglerna gäller oavsett om driften sker internt eller verkställs hos extern part. Driftsdokumentationen ska hållas uppdaterad.

Ansvaret för att driftsdokumentationen uppfyller dessa regler åligger informationsägaren. Framtagande och förvaltning av driftsdokumentationen kan den som verkställer driften svara för.

Vem omfattas av dessa regler

Reglerna gäller tillsvidare för Stadens nämnder och styrelser.

Koppling till andra styrande dokument

Dessa regler konkretiserar Stadens säkerhetspolicy samt riktlinjen för informationssäkerhet.

Regler

Följande dokumentation ska minst ingå i driftsdokumentationen för IT-baserade informationssystem

- En förteckning som tydligt visar de informationstillgångar, programtillgångar, fysiska tillgångar och tjänster som tillhör systemet (allt som erfordras för att systemet ska kunna vara i drift). Exempel på tillgångar är
    - Informationstillgångar: Databaser och filer, systemdokumentation, användarmanualer, utbildningsmaterial, administrativa rutiner, drift- och servicerutiner
    - Programtillgångar: Tillämpningsprogram, nätverks- och operativsystemprogram, utvecklingsverktyg
    - Fysiska tillgångar: Datorer, bildskärmar, kommunikationsutrustning, lagringsmedia, annan teknisk utrustning som reservaggregat och klimatutrustning
- Ansvarsfördelning och uppdelning av arbetsuppgifter inom driftsåtagandet. Fördelningen ska vara gjord så att risken för missbruk begränsas
- Regler och rutiner för rapportering, loggning, åtgärdande, informationsspridning, eskalering, uppföljning och analys av funktionsfel och incidenter
- Regler och rutiner för ändringshantering inklusive installation av programvaror
- Regler och anvisningar som beslutats gälla för klassning av datamedia samt hur dessa datamedia ska förvaras, märkas och förtecknas
- Regler och rutiner för säkerhetskopiering som omfattar
    - vilken information som ska omfattas av säkerhetskopiering
    - intervallen för kopiering o antal generationer säkerhetskopior som ska finnas
    - hur säkerhetskopior ska förvaras
    - vilka säkerhetskopior som ska förvaras på plats geografiskt skild från driftstället
    - hur säkerhetskopiorna ska verifieras
    - åtgärder som ska vidtas för att säkra att informationen är läsbar under hela förvaringstiden
    - återläsning
- Regler och rutiner för logghantering som omfattar
    - hur länge de ska sparas
    - hur de ska förvaras
    - hur ofta de ska analyseras
    - vem som ansvarar för analyser av dem
    - återrapportering av analysresultat
- Återstarts- och reservrutiner

Följande dokumentation ska också finnas. Denna kan dock ingå i den övergripande dokumentationen för de centrala utrymmena med driftsatta IT-baserade informationssystem, såsom datorhallar

- Hur det fysiska skyddet är uppbyggt inklusive brandsektionering

- Regler och rutiner för tillträde inklusive besöksrutiner. Tillträde ska regleras restriktivt och strikt styras utifrån de krav som ställs av vederbörandes arbetssituation
- Beskrivning, regler och rutiner över larm och larmmottagning för inbrott, brand, temperatur och fukt

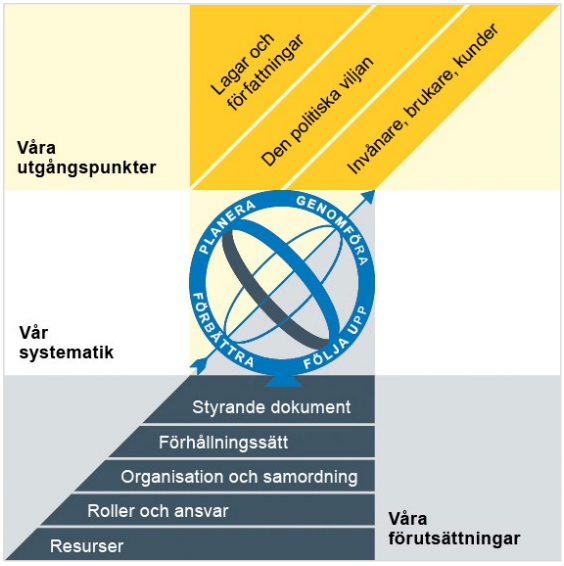
Göteborgs Stad

Göteborgs Stads riktlinje för informationssäkerhet

Reglerande styrande dokument

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

Göteborgs Stads styrsystem



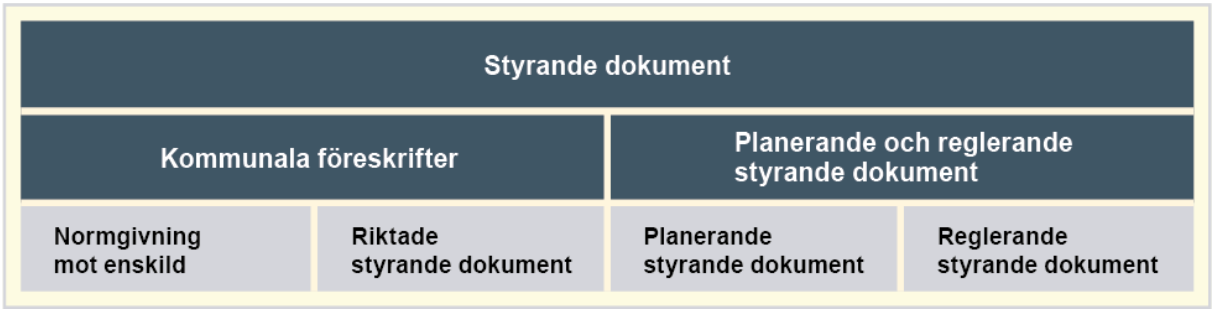
Utgångspunkterna för styrningen av Göteborgs Stad är lagar och författningar, den politiska viljan och stadens invånare, brukare och kunder. För att förverkliga utgångspunkterna behövs förutsättningar av olika slag. Stadens politiker har möjlighet att genom styrande dokument beskriva hur de vill realisera 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:**
Kommunfullmäktige	Stadens nämnder och styrelser	[Nummer]	[Text]
Dokumentsort:	**Giltighetstid:**	**Senast reviderad:**	**Dokumentansvarig:**
Riktlinje	Tills vidare	[Datum]	Säkerhetschef

Bilagor:
Göteborgs Stads klassificeringsmodell
Göteborgs Stads klassificeringsmodell - beskrivning av konsekvensnivåer
Begreppsdefinition

Innehåll

Inledning

Syftet med denna riktlinje

Syftet med Göteborgs Stads riktlinje för informationssäkerhet är att skapa förutsättningar för ett systematiskt och långsiktigt informationssäkerhetsarbete.

Riktlinjen omfattar alla informationstillgångar oavsett om de behandlas manuellt eller digitalt och oberoende av i vilken form eller miljö de förekommer.

Säkerhetsskyddsklassificerad information med betydelse för Sveriges säkerhet hanteras utanför denna riktlinje. Se Göteborgs Stads riktlinje för säkerhetsskydd.

Vem omfattas av riktlinjen

Denna riktlinje gäller tillsvidare för Göteborgs Stads nämnder och styrelser.

Koppling till andra styrande dokument

Denna riktlinje konkretiserar Göteborgs Stads säkerhetspolicy avseende informationssäkerhet.

Stödjande dokument

Göteborgs Stads klassificeringsmodell inklusive beskrivning av konsekvensnivåer. Utöver stödjande dokument finns även ett nätverk för informationssäkerhet med representanter från stadens nämnder och styrelser som syftar till kunskaps- och erfarenhetsutbyte.

Riktlinje

Inledning

Denna riktlinje anger hur Göteborgs Stad ska arbeta med informationssäkerhet.

Information är viktig för Göteborg Stad och behöver skyddas efter behov. Ett bra informationssäkerhetsarbete skapar förtroende både inom och utanför organisationen.

Information är värdefull för Göteborg Stad. Information inhämtas, bearbetas, lagras och kommuniceras på olika sätt. Information som går förlorad eller hanteras felaktigt kan leda till allvarliga konsekvenser både för organisationer och för den enskilda människan.

Göteborgs Stads metod för säker informationshantering

Inom Göteborg Stad ska ett systematiskt och långsiktigt informationssäkerhetsarbete bedrivas. Göteborgs Stads metod för säker informationshantering bygger på ett antal steg där informationsägaren inleder med att klassificera information, genomför en riskanalys för att därefter vidta lämpliga organisatoriska, personrelaterade, fysiska och tekniska säkerhetsåtgärder. De olika stegen beskrivs i riktlinjen.

Informationssäkerhet innebär skydd av informationstillgångar avseende:

- *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.

Det är verksamhetens behov och informationens skyddsvärde som styr hur informationen ska skyddas. Informationens klassificering och de krav som det medför ska efterlevas under hela informationens livscykel inklusive avveckling.

Riskbaserat informationssäkerhetsarbete

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 informationssäkerhetsrisker och utifrån detta vidta lämpliga säkerhetsåtgärder.

Ansvar och roller i informationssäkerhet

I enlighet med vad som gäller för övrig verksamhet, är ansvaret för informationssäkerheten kopplat till ordinarie verksamhetsansvar. Det innebär att ansvarig nämnd/styrelse för en verksamhet också är ansvarig för att informationssäkerheten upprätthålls och efterföljs i denna verksamhet.

Informationsägare är den nämnd/styrelse som ansvarar för den information som skapas och hanteras. Ansvaret för informationen och dess säkerhet följer med ansvaret för verksamheten. Informationssägaren klassificerar och beslutar om informationshantering inom ramen för befintlig lagstiftning och verksamhetskrav.

Systemägare är den som har ett överordnat ansvar för administration, drift och säkerhet för ett system. Ett system kan innehålla information som tillhör en eller flera informationsägare. Systemägaren ansvarar för att system uppfyller lagkrav och verksamhetskrav som fastställts av informationsägare.

Klassificering av information

Informationsklassificering möjliggör att information skyddas på ett adekvat sätt vilket höjer kvalitet och effektivitet genom att undvika att information får ett överskydd med höga kostnader som följd eller tvärtom att information inte får det skydd som den behöver.

Nämnder och styrelser ansvarar för att:

- säkerställa att informationen klassificeras utifrån säkerhetsaspekterna konfidentialitet, riktighet och tillgänglighet och det är Göteborgs Stads klassificeringsmodell som ska användas (se bilaga 1). Klassificering görs utifrån de konsekvenser eller skada som bristande informationssäkerhet skulle kunna medföra utifrån perspektiven: verksamhet, samhälle, individ, ekonomi och varumärke/förtroende (se bilaga 2).
- säkerställa att lagar, föreskrifter och verksamhetskrav vägs in i informationsklassificeringen.

Organisatoriska säkerhetsåtgärder

Hantering av informationstillgångar

Med informationstillgångar menas verksamhetens information och de resurser som hanterar informationen. Exempel på informationstillgångar finns i bilaga 3 begreppsdefinitioner.

Nämnder och styrelser ansvarar för att:

- säkerställa att det finns en förteckning över verksamhetens informationstillgångar
- säkerställa att förteckningen innehåller sådan information som är nödvändig för återhämtning efter en störning eller allvarlig incident
- säkerställa att förteckningen minst omfattar ändamål för behandling eller lagring av information, informationsägare, systemägare och tillgångens informationsklass utifrån säkerhetsaspekterna konfidentialitet, riktighet och tillgänglighet.
- säkerställa att det i förteckning definieras och dokumenteras regler, lagar samt avtalsrättsliga åtaganden för respektive informationstillgång
- säkerställa att anställda och externa användare lämnar tillbaka de informationstillgångar som de förfogar över då deras anställning, uppdrag eller avtal ändras.

Åtkomst till information

Nämnder och styrelser ansvarar för att:

- säkerställa att åtkomst och behörighet till information ges restriktivt utifrån arbetsuppgifter och organisatorisk tillhörighet
- säkerställa att behörigheter följs upp vid behov. Vid byte eller förändring av tjänst ska behörigheter och åtkomst till information ses över
- säkerställa att åtkomst till information bygger på personliga användaridentiteter och är spårbar till en fysisk person
- säkerställa att autentisering och åtkomstkontroll till administratörs-och systemkonton sker med unika lösenord och baseras på flerfaktorsautentisering
- säkerställa att regelverk och rutin för registrering och avregistrering av behörigheter fastställs innan system tas i bruk.

Integritet och skydd av personuppgifter

Nämnder och styrelser ansvarar för att:

- säkerställa att krav för upprätthållande av personlig integritet och skydd av personuppgifter, enligt tillämpliga lagar och författningar samt avtalskrav, identifieras och uppfylls
- säkerställa att det finns rutiner för behandling av personuppgifter och informationstexter till registrerade
- säkerställa att lämpliga säkerhetsåtgärder införs för att skydda personuppgifter.

Informationssäkerhet vid införande av nya system

Nämnder och styrelser ansvarar för att:

- säkerställa att informationssäkerhet integreras i projektledningen,
- säkerställa verifiering av leverantörens informationssäkerhet innan verksamheten inför ett nytt system. Leverantören kan åläggas att uppvisa verifiering.

Leverantörsrelationer

Nämnder och styrelser ansvarar för att:

- säkerställa att informationssäkerheten integreras i upphandling av system. I leverantörsavtalet ska det förutom säkerhetskrav även framgå ansvarsfördelning, hur informationen ska hanteras, återlämnas och avvecklas
- säkerställa att det finns avtal med leverantörer som får åtkomst och behandlar information som ägs av Göteborgs Stad. Vid åtkomst till sekretessbelagd information ska även sekretessavtal ingås
- säkerställa att det finns personuppgiftsbiträdesavtal i de fall leverantör behandlar personuppgifter på uppdrag av Göteborgs Stad.

Hantering av incidenter

Nämnder och styrelser ansvarar för att:

- säkerställa att inträffade incidenter hanteras och åtgärdas skyndsamt för att minimera skador i verksamheten
- säkerställa att informationssäkerhetsincidenter där anmälningsskyldighet finns enligt lag eller förordning, anmäls till ansvarig myndighet.

Informationssäkerhet vid störning - kontinuitetshantering

Nämnder och styrelser ansvarar för att:

- säkerställa att det finns en åtgärdsplan, så kallad kontinuitetsplan, för att kritisk verksamhet fortsatt kan bedrivas på en acceptabel nivå vid en allvarlig störning eller avbrott.

Personalrelaterade säkerhetsåtgärder

Nämnder och styrelser ansvarar för att:

Före anställning

- säkerställa att arbetssökandes referenser och formella meriter (såsom utbildning, yrkeslegitimation, etcetera), kontrolleras och att den arbetssökandes identitet verifieras. Vid rekrytering till särskilt informationssäkerhetskritiska arbetsuppgifter ska fler och mer detaljerade kontroller övervägas.

Under anställning

- säkerställa att anställda under anställningstiden görs medvetna om sitt ansvar för informationssäkerhet.

Utbildning

- säkerställa att anställda inom Göteborgs Stad får den utbildning i informationssäkerhet som krävs för att de ska kunna utföra sina arbetsuppgifter på ett säkert sätt. Utbildningens omfattning ska vara anpassad till det ansvar och de befogenheter som gäller för befattningen. Detsamma gäller även vid förflyttning och omplacering av redan anställda och när tillfällig personal och externa konsulter anlitas.

Avslut eller ändring av anställning

- säkerställa att det finns en fastställd rutin för hantering av anställda som avslutar sin anställning. Rutinen ska säkerställa att information, datorer/utrustning, passerkort, tjänstekort etcetera återlämnas och att åtkomsträttigheter upphör vid anställningens slut.

Fysiska säkerhetsåtgärder

Nämnder och styrelser ansvarar för att:

- säkerställa att informationsklassning, riskbedömning och informationens skyddsvärde ligger till grund för det fysiska skalskydd som ska finnas för att skydda informationstillgångar. Vid utformning av centrala IT-utrymmen ska behovet av brandskydd, tillträdesskydd, skalskydd, el och reservkraft, miljö och kyla, skydd mot vätska, interiör, teknisk övervakning och larm med mera, utvärderas
- säkerställa att säkerhetsåtgärder testas regelbundet.

Tekniska säkerhetsåtgärder

Driftsäkerhet

Göteborgs Stad ska som regel ha en systemmiljö med åtskilda produktions-, utvecklings-, test- och utbildningsmiljöer.

Nämnder och styrelser ansvarar för att:

- säkerställa att säkerhetskopiering och testning för att återskapa information görs regelbundet
- säkerställa att det finns spårbarhet för viktiga och säkerhetskritiska händelser
- säkerställa att det finns ett installerat skydd av skadlig kod på enheter som kan drabbas av skadlig kod och obehörigt nyttjande
- säkerställa skyndsam installering av leverantörers säkerhetsuppdateringar. För att säkerställa att driften inte påverkas negativt ska säkerhetsuppdateringarna testas och analyseras innan de installeras i produktionsmiljön.

Systemdokumentation

Det ska finnas dokumentation för varje system. Dokumentationen ska bestå av system- och driftdokumentation.

Nämnder och styrelser ansvarar för att:

- säkerställa att det finns systemdokumentationen som minst omfattar vilka olika komponenter systemet består av, en övergripande beskrivning av de olika delarnas uppgift samt en dokumentation över de funktioner som är relevanta för informationssäkerheten. Det ska även framgå vem som är systemägare.
- säkerställa att det finns driftdokumentationen som minst omfattar rutiner för säkerhetskopiering, återstarts- och återställningsrutiner, incidenthantering, ändringshantering samt information om logghantering. Det ska även framgå vem som är driftansvarig.
- säkerställa att det finns en kopia av dokumentationen som förvaras skild från originalen och de ska vara åtkomliga även om lagringsytan de normalt sett förvaras på är otillgänglig.

Nätverkssäkerhet och säkerhet i nätverkstjänster

Göteborgs Stads verksamheter är beroende av ett fungerande nätverk. För att förhindra obehörig åtkomst till nätverk och anslutna tjänster ska det finnas säkerhetsåtgärder på plats för att säkerställa konfidentialitet och riktighet för information som överförs. Detsamma gäller för att upprätthålla tillgänglighet till nätverkets tjänster.

Nämnder och styrelser ansvarar för att:

- säkerställa att loggning och övervakning tillämpas för att upptäcka avvikelser som kan påverka eller vara relevanta för informationssäkerheten
- säkerställa att det finns rutiner och uppdaterad dokumentation för hantering av nätverksenheter.

Anskaffning, utveckling, underhåll och avveckling av IT-system

Informationssäkerhetskraven ska vara en del av en upphandling av system och definieras utifrån informationsägarens informationsklassificering och riskbedömning.

Nämnder och styrelser ansvarar för att:

- säkerställa att det finns rutiner för utveckling och testning av system samt ändringshantering
- säkerställa att alla system regelbundet analyseras för att identifiera sårbarheter som kan påverka informationssäkerheten.

Uppföljning av informationssäkerhet

Varje nämnd och styrelse ska följa upp informationssäkerheten och vidta de åtgärder som krävs för att säkerställa att styrande dokument, lagar och andra regelverk inom informationssäkerhet efterlevs inom den egna verksamheten.

Bilaga 1 Göteborgs Stads klassificeringsmodell

	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

Bilaga 2 Göteborgs Stads klassificeringsmodell – beskrivning av konsekvensnivåer

Allvarlig skada (hög skyddsnivå 3)

- *Övergripande*: Mycket allvarlig skada för Göteborgs verksamhet, dess tillgångar, annan organisation eller enskilda individer.
- *Verksamhet*: Det är stora svårigheter för verksamheten att fullfölja en eller flera av sina uppdrag. Omfattande skador på verksamhetens tillgångar. Kan ge stor påverkan på andra myndigheter och organisationer (ekonomiskt eller genom extraordinära åtgärder).
- *Samhälle*: Samhällsviktiga funktioner i egen eller annans organisation påverkas.
- *Individ*: Mycket allvarlig negativ påverkan på enskild individs (medarbetares, medborgares och andra individers) rättigheter, liv och hälsa.
- *Ekonomi:* Resultera i mycket hög skadekostnad för verksamheten
- *Varumärke:* Mycket allvarlig/katastrofal påverkan på varumärke och förtroende.

Betydande skada (utökad skyddsnivå 2)

- *Övergripande:* Betydande skada för Göteborgs verksamhet, dess tillgångar, annan organisation eller enskilda individer.
- *Verksamhet:* Verksamheten kan ha besvär med att fullfölja ett eller flera av sina uppdrag. Resulterar i betydande skador på verksamhetens tillgångar. Andra myndigheter och organisationer kan påverkas (ekonomiskt eller genom extraordinära åtgärder).
- *Samhälle:* Samhällsviktiga funktioner i egen eller annans organisation påverkas i liten utsträckning.
- *Individ:* Betydande negativ påverkan på enskild individs (medarbetares, medborgares och andra individers) rättigheter, liv och hälsa.
- *Ekonomi:* Resultera i betydande skadekostnad för verksamheten.
- *Varumärke:* Allvarlig/betydande skada på varumärke - förtroende.

Måttlig skada (grundläggande skyddsnivå 1)

- *Övergripande:* Måttlig skada för Göteborgs verksamhet, dess tillgångar, annan organisation eller enskilda individer.
- *Verksamhet:* Verksamheten har inte några större svårigheter att fullfölja och utföra sina uppdrag. Resultera endast i mindre skador på verksamhetens tillgångar.
- *Samhälle:* Obetydlig påverkan på samhällsviktiga funktioner vid egen eller annan organisation.
- *Individ:* Enstaka personuppgifter som inte är känsliga kan komma att spridas och förorsaka begränsad negativ påverkan på enskilds individs (medarbetares, medborgares och andra individers) rättigheter, liv och hälsa.
- *Ekonomi:* Resultera i viss skadekostnad för verksamheten.
- Viss påverkan på varumärke och förtroende.

Försumbar skada (ingen skyddsnivå 0)

- *Övergripande:* Ingen/försumbar skada för Göteborgs verksamhet, dess tillgångar, annan organisation eller enskilda individer.
- *Verksamhet:* Inga svårigheter för verksamheten att fullfölja sina uppdrag. Ingen skada på verksamhetens tillgångar och ingen påverkan på andra myndigheter eller organisationer.
- *Samhälle:* Ingen påverkan på samhällsviktiga funktioner vid egen eller annan organisation.

- *Individ:* Enskild individs (medarbetares, medborgares och andra individers) rättigheter, liv och hälsa påverkas minimalt.
- *Ekonomi:* Resulterar i ingen eller mycket begränsad skadekostnad.
- *Varumärke:* Ingen påverkan på varumärket eller förtroendet.

Bilaga 3 Begreppsdefinition

Nedan återfinns definitioner på begrepp som tillämpas i denna riktlinje. Myndigheten för samhällsskydd och beredskap tillhandahåller en termbank för informationssäkerhet.

Begrepp	Definition
Autentisering	Verifiering av att en användare är den person den påstår sig vara
Behörighet	Tilldelade rättigheter att använda en informationstillgång på ett specifikt sätt.
Fysiskt skydd	Säkerhetsåtgärder relaterade till skydd av personer, lokaler och utrustning av betydelse för informationssäkerheten.
Informationstillgång	Med informationstillgång menas verksamhetens information och de resurser som hanterar informationen. Exempel på informationstillgångar är: • information (avtal, lösenord, rutiner, anteckningar, dokument etcetera) • program (applikation, operativsystem etcetera) • tjänster (kommunikationstjänst, abonnemang etcetera) • fysiska tillgångar (dator, telefon, lokala nätverk, skrivare etcetera) • människor och deras kompetens, färdigheter och erfarenheter • immateriella tillgångar (rykte och image etcetera)
Skalskydd	Skalskydd är den gräns i ett utrymme, lokal eller fastighet som har ett fysiskt skydd vilket försvårar obehörigt tillträde
Spårbarhet	Möjlighet att kunna härleda utförda aktiviteter i systemet till en identifierad användare.
System	Informationssystem för att samla in, lagra, bearbeta och distribuera information för ett givet ändamål, innefattar såväl ett systems tekniska utrustning som dess mänskliga aktiviteter och rutiner.
Säkerhetsåtgärd	Identifierad uppsättning åtgärder för att möta en organisations risker