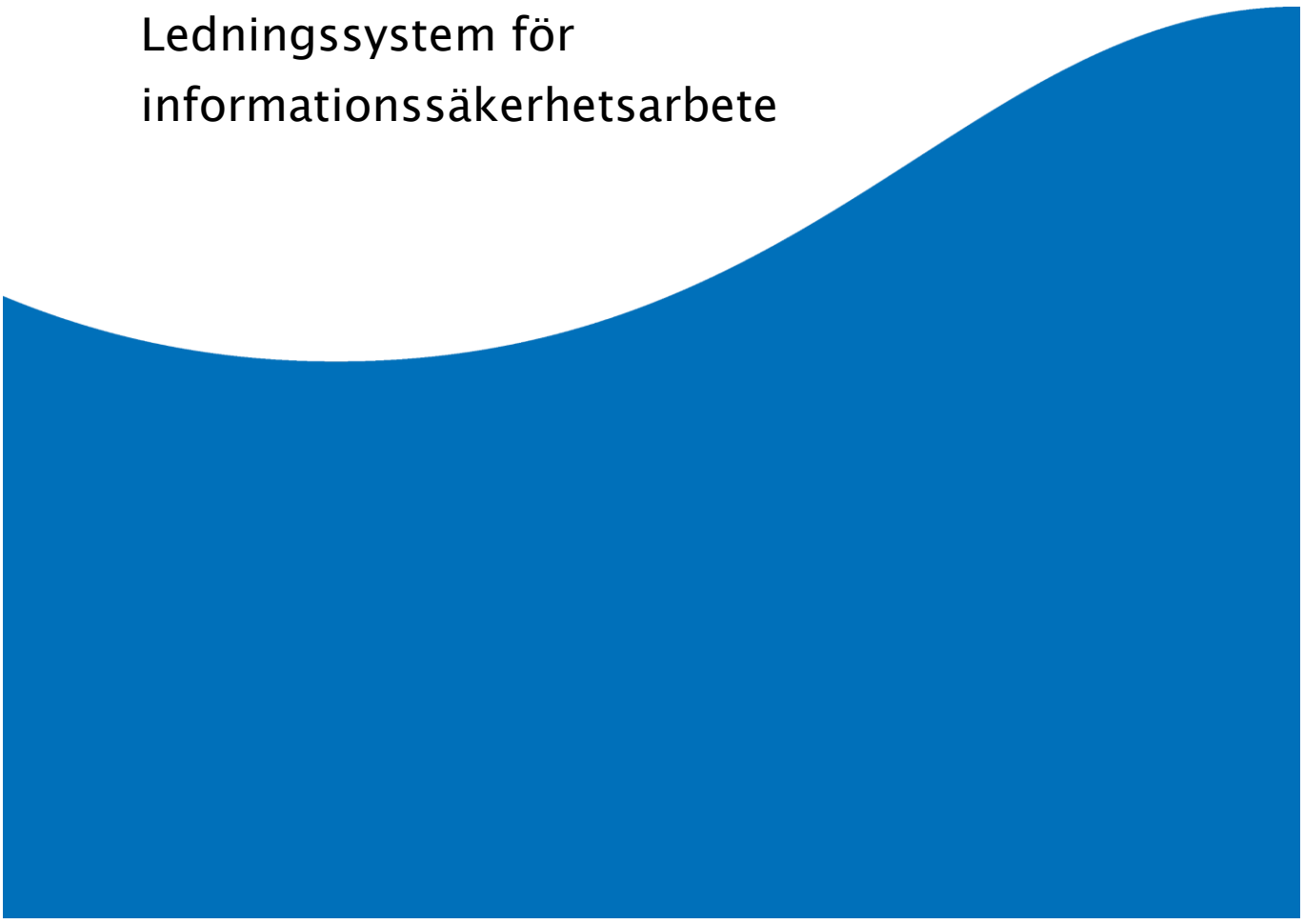
KARLSBORG

Riktlinje för systematiskt informationssäkerhetsarbete

Ledningssystem för informationssäkerhetsarbete



Gäller för:	Samtliga förvaltningar och bolag
Diarienummer:	2023-350
Beslutande:	Kommunstyrelsen
Datum för beslut:	2023-10-11
Paragraf i protokoll:	136
Gäller från och med:	2023-11-01
Dokumentansvar:	Kanslichef
Aktualitetsprövning:	Ska ske under första året av varje mandatperiod.

Innehåll

Inledning

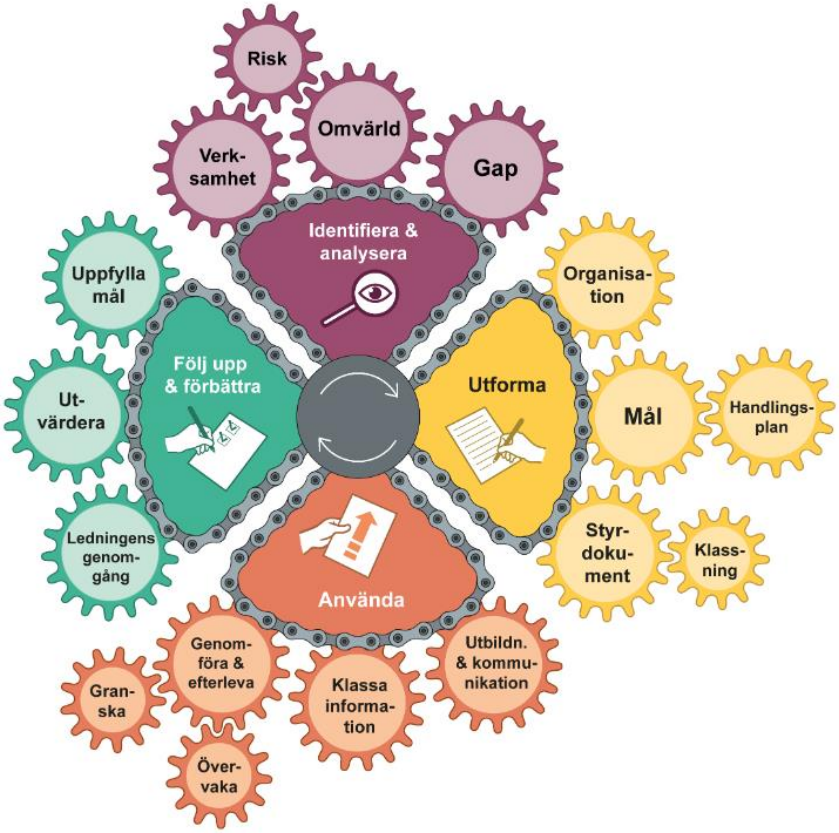
Kommunfullmäktige i Karlsborgs kommun har beslutat om en policy för informationssäkerhet. Policyn beskriver kortfattat vad arbetet med informationssäkerhet innebär, vilka de övergripande målen med informationsarbetet är, beskriva organisation, roller och ansvar samt hur arbetet med ett ledningssystem för informationssäkerhet ska bedrivas.

Ett ledningssystem för informationssäkerhet kan beskrivas som en organisations policy, mål, processer, rutiner och uppföljningsarbete för att jobba med informationssäkerhet på ett systematiskt sätt.

Kommunens ledningssystem ska bygga på MSBs metodstöd för systematiskt informationssäkerhetsarbete. Metodstödet är uppbyggt på fyra olika delar:

- Identifiera och analysera
- Utforma
- Använda
- Följ upp och förbättra

Metodstödet kan illustreras i bilden nedan och kan ses som en sammanfattning av ledningssystemets olika delar.



Identifiera och analysera

Verksamhetsanalys

En verksamhetsanalys är grunden till hur arbetet ska genomföras. Om verksamheten förändras, behöver analysen uppdateras. Analysen genomförs på kommunnivå och kommunchefens ledningsgrupp ansvarar för detta arbete genomförs.

Interna intressenter och förutsättningar

Interna intressenter kan tex vara beslutsfattare, informationsägare, medarbetare, stödenheter mfl. De olika intressenterna har olika roller/ansvar i hur kommunens arbete med informationssäkerhet bedrivs. De olika intressenterna har också olika krav. I verksamhetsanalysen kartläggs vilka dessa interna intressenter är och på vilket sätt de styr/påverkar verksamheten och arbetet med informationssäkerhet.

I analysen behöver även de interna förutsättningarna kartläggas och analyseras. Det kan tex gälla styrdokument, olika verksamhetsprocesser, organisationsstruktur/kultur, infrastruktur, kommunikation och resurser.

Interna informationstillgångar

Information är en tillgång för verksamheten, utan information fungerar verksamheten mindre bra eller inte alls. De resurser (verksamhetssystem, olika lagringsytor, pärmar, servrar, nätverk, personer mfl) som bär information kallas för informationstillgång. Alla informationstillgångar ska kartläggas och beskrivas. Kartläggningen behöver uppdateras regelbundet då det kan komma till eller försvinna informationstillgångar i verksamheterna. Dokumentation av informationstillgångarna görs i Stratsys. Varje förvaltning ansvarar för sitt register.

Omvärldsanalys

Som ett komplement till verksamhetsanalysen görs även en omvärldsanalys för att kartlägga vilka externa intressenter och krav som påverkar kommunens informationssäkerhetsarbete.

Externa intressenter

På samma sätt som verksamhetsanalysens interna intressenter görs även en kartläggning och analys av de externa intressenterna. Externa intressenter kan tex vara lagstiftare, medborgare, granskande myndigheter, media, leverantörer, samverkansparter mfl. De externa intressenterna har olika roller och krav på organisationens informationssäkerhetsarbete.

Rättsliga krav

Viktiga lagar och författningar att hålla ordning på inom ramen för informationssäkerhet är bland andra:

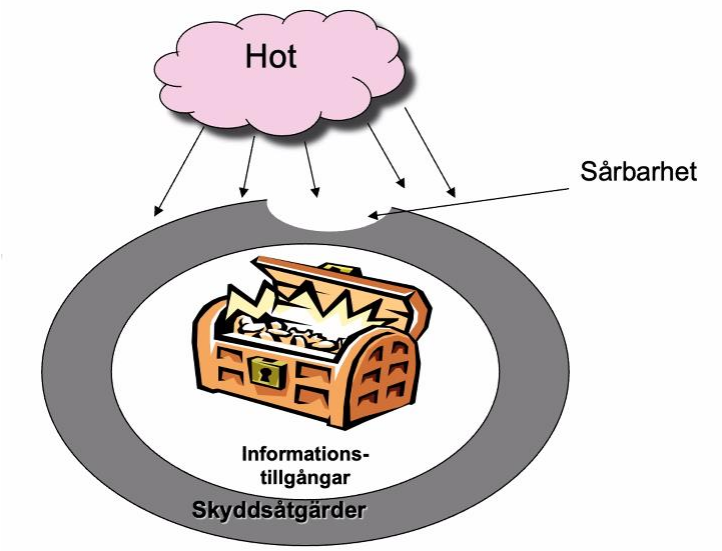
- Offentlighets- och sekretesslag (2009:400)
- Dataskyddsförordningen (GDPR)
- Kommunallag (2017:725)
- Förvaltningslag (2017:900)
- Arkivlag (1990:782)
- Socialtjänstlag (2001:453)
- Patientlag (2014:821)
- Patientdatalag (2008:355)
- Författningssamling ”journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40)
- Skollag (2010:800)

Riskanalys

Riskanalys handlar om att förutse risker i verksamheten. Genom att kartlägga hot och sårbarheter kan avvikelser och negativa konsekvenser för verksamheten förhindras.

Riskanalyser kan göras organisationsövergripande med även mer i detalj för varje informationstillgång. Riskanalyser bör genomföras regelbundet och efter fastställda kriterier. Verksamheterna ansvarar för att genomföra nödvändiga riskanalyser.

Hot och sårbarheter



Hot är en möjlig orsak till en oönskad händelse som kan medföra negativa konsekvenser för verksamheten. Hot kan delas in i kategorier:

- **Fysisk skada** (eld, vattenskada, olycka, förstörelse, stöld)
- **Naturliga händelser** (översvämning, meteorologiska fenomen, klimatförändring)
- **Tekniska fel** (utrustningsfel, överbelastning)
- **Obehöriga åtgärder** (obehörig användning, bedräglig kopiering, förvanskning av data, olaglig behandling)

Sårbarhet är brister i skyddsåtgärderna av en tillgång som kan utnyttjas av ett eller flera hot. Sårbarheter kan delas in i kategorier:

- **Maskinvara** (undermåligt underhåll och backuprutiner, oskyddad lagring, känslighet mot temperaturväxling mm)
- **Programvara** (felaktig installation, för generösa åtkomsträttigheter, okända fel)
- **Nätverk** (oskyddade kommunikationsvägar, osäker utrustning, brister i säkerheten)
- **Personal** (frånvaro av personal, otillräcklig kompetensnivå, avsaknad av säkerhetsmedvetenhet, otydliga rutiner)
- **Plats** (ingen fysisk åtkomstkontroll, utsatthet tex för översvämning)
- **Organisation** (inga rutiner för incidentrapportering, avsaknad av kontroller, inte koll på utrustning)

Konsekvenser

När hoten blir verklighet och verksamheten har sårbarhet där hotet riktas emot, kan verksamhet, medarbetare och/eller medborgare drabbas av negativa konsekvenser. Konsekvenserna kan delas in i kategorier:

- **Ekonomiska** (vite, ökade kostnader, ineffektivitet)
- **Process** (avbrott i verksamheten)
- **Juridiska** (lagbrott, avtalsbrott)
- **Sociala** (förtroende, goodwill, varumärke)
- **Individuella** (liv, hälsa och säkerhet för individer)
- **Miljömässiga** (neg påverkan på miljön)

Konsekvensen av att ett hot som inträffat bedöms på en fyrgradig skala där 1 är försumbar konsekvens och 4 är allvarlig konsekvens. Bedömningskriterierna för konsekvens är fastställda enligt nedan tabell för Karlsborgs kommun.

Konsekvens		
Allvarlig	Medborgare/medarbetare	Mycket stor påverkan på liv, hälsa, rättigheter.
	Process/verksamhet	Mycket stor negativ påverkan på verksamhetens förmåga att fullgöra sina primära uppgifter
	Social	Mycket stor förtroendeskada.
	Ekonomi	Mycket stor ekonomisk skada.
	Medborgare/medarbetare	Stor påverkan på liv, hälsa, rättigheter.

Betydande	Process/verksamhet	Stor negativ påverkan på verksamhetens förmåga att fullgöra sina primära uppgifter
	Social	Stor förtroendeskada.
	Ekonomi	Stor ekonomisk skada.
Måttlig	Medborgare/medarbetare	Viss påverkan på liv, hälsa, rättigheter.
	Process/verksamhet	Viss negativ påverkan på verksamhetens förmåga att fullgöra sina primära uppgifter
	Social	Viss förtroendeskada.
	Ekonomi	Viss ekonomisk skada.
Försumbar	Medborgare/medarbetare	Liten påverkan på liv, hälsa, rättigheter.
	Process/verksamhet	Liten negativ påverkan på verksamhetens förmåga att fullgöra sina primära uppgifter
	Social	Liten eller ingen förtroendeskada.
	Ekonomi	Liten ekonomisk skada.

Sannolikhet

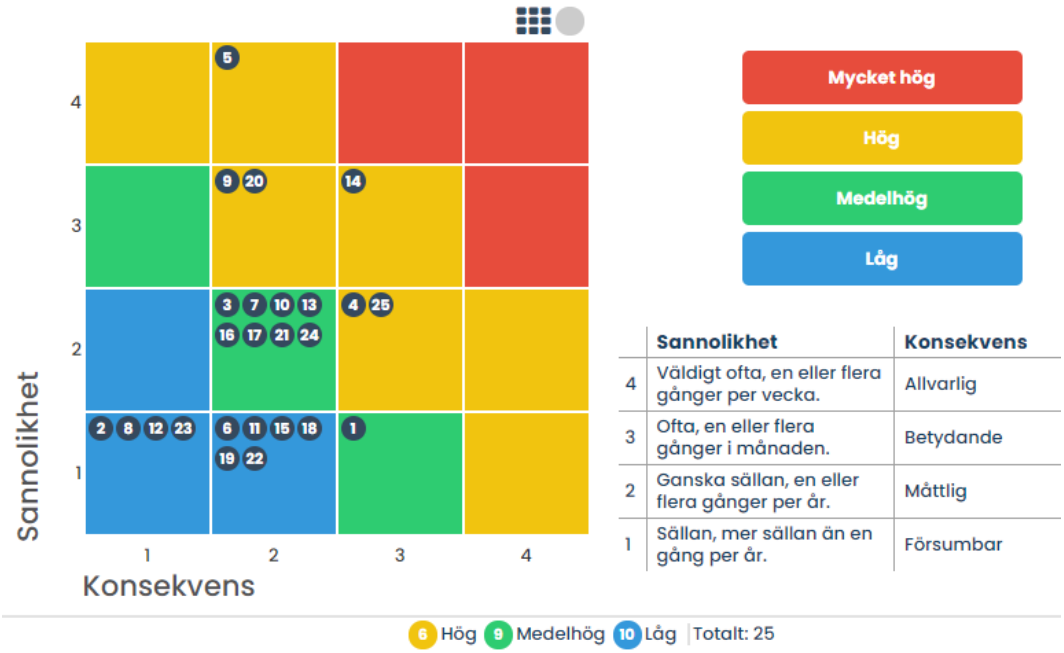
Sannolikheten för att ett hot ska inträffa och ge negativa konsekvenser för verksamheten bedöms på en fyrgradig skala där 1 är sällan och 4 är väldigt ofta. Bedömningskriterierna för sannolikhet är fastställda enligt tabellen nedan för Karlsborgs kommun.

Sannolikhet		
Väldig ofta	Inträffar en eller flera gånger i veckan.	Sannolikheten är stor att det ska inträffa. Det är bekräftat att hotet är verkligt i väsentliga delar av verksamheten redan idag eller att det väntas bli det i närtid.

Ofta	Inträffar en eller flera gånger i månaden.	Kan mycke väl inträffa, men troligtvis inte särskilt ofta. Det finns tydliga tecken på att hotet är verkligt i vissa delar av verksamheten redan idag.
Ganska sällan	Inträffar en eller flera gånger per år.	Inträffar sannolikt inte under normala omständigheter och i alla fall inte frekvent. Det finns vissa tecken på att hotet är verkligt i få delar av verksamheten.
Sällan	Inträffar mer sällan än en gång per år.	Det finns mycke få eller inga tecken på att hotet är verkligt idag.

Riskbedömning

Genom att multiplicera värdena för konsekvens och sannolikhet erhålls ett riskvärde. Riskvärdet ger vägledning om vilka verksamheter eller informationstillgångar som är mest utsatta. Riskerna placeras ut i en riskmatris för att få en överblick över vilka risker som kan accepteras, vilka som bör minimeras eller vilka som bör elimineras. Blå och gröna risker kan accepteras, gula risker bör åtgärdas på sikt och röda risker ska åtgärdas snarast.



Åtgärder från riskanalys

För risker med högt riskvärde behöver åtgärder beslutas om för att minimera eller eliminera hoten. Beslutade åtgärder behöver tids- och resurssättas samt en ansvarig ska utses. Datum för uppföljning ska också beslutas. Vid uppföljning ska det utvärderas om åtgärden fått önskad effekt och en ny riskbedömning bör visa på ett lägre riskvärde. Om åtgärden inte fått önskad effekt, ska fler åtgärder vidtagas.

GAP-analys

Syftet med att genomföra en GAP-analys är att identifiera skillnaden mellan önskad informationssäkerhetsnivå och den befintliga säkerhetsnivån vid analystillfället. Den önskade nivån utgår ifrån SS-EN ISO/IEC 27001 (bilaga A) samt 27002:2017. I denna ISO-standard finns en del säkerhetsåtgärder (kravområden) som bedöms vara mer eller mindre nödvändiga för en organisations informationssäkerhetsnivå. De områden som valts ut är:

- Ledningssystem för informationssäkerhet
- Organisation av informationssäkerhetsarbete
- Personalsäkerhet
- Hantering av informationstillgångar
- Styrning av åtkomst
- Fysisk och miljörelaterad säkerhet
- Driftsäkerhet
- Kommunikationssäkerhet
- Anskaffning, utveckling och underhåll av system

- Hantering av informationssäkerhetsincidenter
- Informationssäkerhetsaspekter avseende hantering av verksamhetens kontinuitet
- Efterlevnad och granskning

Kravområdena beskrivs mer utförligt i ”Riktlinje för informationssäkerhetsåtgärder”.

Bedömningen görs om kravområdet uppfylls helt eller delvis eller inte alls. För kravområde som inte eller bara delvis uppfylls bör åtgärder beslutas om. Kravområdets betydelse för verksamheten kan också bedömas, vilket kan underlätta prioritering av eventuella åtgärder. GAP-analysen görs på kommunövergripande nivå och dokumenteras i Stratsys.

Utforma

Organisation

För att arbetet med informationssäkerhet ska bli systematiskt och hållbart i längden krävs att flera funktioner har en roll i arbetet. En blandning av kompetenser är att föredra, då informationssäkerhet spänner över många områden i kommunens verksamheter. Det bör vara tydligt vilka roller som ingår och vilket ansvar de har. Organisationen är fastställd och beskriven i Karlsborgs kommuns policy för informationssäkerhet. Sammanfattningsvis är de nämnderna/styrelserna och ytterst kommunfullmäktige som har ansvar för organisationens informationssäkerhet. Viktiga roller i det övergripande och strategiska arbetet har säkerhetschefen och kanslichefen. För det dagliga arbetet ansvarar informationsägaren (dvs nämnd och tillhörande förvaltning) och medarbetare. Stödfunktioner så som IT-enhet, kommunikationsenhet och fastighetsenhet är viktiga för att arbetet ska kunna bedrivas på ett bra sätt.

Arbetsstruktur och nätverk

För att lyckas med informationssäkerhetsarbetet är det också viktigt att ha en struktur för hur arbetet ska bedrivas, dvs på vilket sätt ska dessa personer jobba tillsammans. Det kan även innefatta personer utanför själva organisationen, tex nätverk med andra kommuner eller myndigheter.

För att de funktioner som är en del av informationssäkerhetsorganisationen ska kunna samverka och föra arbetet framåt är det viktigt att en struktur för arbetet finns. Det är också viktigt att det finns kanaler för information, både uppåt och neråt i organisationen.

Kommunchefens ledningsgruppen

Kommunchefens ledningsgrupp (där informationssäkerhetssamordnaren ingår) fungerar som ett strategiskt forum där planering av kommande arbete sker, där beslut om åtgärder fattas och där arbetet följs upp. I kommunchefens ledningsgrupp genomförs omvärlds- och verksamhetsanalys, övergripande riskanalyser, GAP-analys samt klassning av gemensamma informationstillgångar.

I slutet av året redovisar informationssäkerhetssamordnaren för ledningsgruppen en uppföljning/genomgång av årets arbete. Därifrån kan sedan nästa års arbete planeras.

Förvaltningarnas ledningsgrupper

Varje nämnd/förvaltning ansvarar för sin egen information och dess säkerhet. Det systematiska informationssäkerhetsarbetet ska bedrivas även i förvaltningarna och det är förvaltningschef med ledningsgrupp som ansvarar för att driva detta arbete. I förvaltningarna ska övergripande riskanalyser, riskanalys per informationstillgång samt klassning av informationstillgång genomföras för de förvaltningsspecifika verksamheter och informationstillgångar.

Nätverk för informationssäkerhetsarbetet

Varje förvaltning ska utse en eller flera informationssäkerhetsombud. Informationsombudet ska vara informationssäkerhetssamordnarens kontakt med verksamheterna och driva det praktiska arbetet på förvaltningen (tex ta fram och implementera rutiner, genomföra riskanalyser, ge förslag på åtgärder mm). Samordnaren och ombuden bildar ett nätverk för informationssäkerhetsarbetet där samordnaren är sammankallande.

IT-leverantören

Informationssäkerhetssamordnaren har också regelbundna träffar med kommunens leverantör av IT-drift (Skövde kommun). På dessa träffar tas frågor om IT-drift, IT-säkerhet, åtgärder mm upp.

Externa nätverk

Det finns nätverk för informationssäkerhet på delregional nivå. Länsstyrelsen i Västra Götaland samordnar ett nätverk för fd Skaraborgs 15 kommuner. Nätverket syftar till att sprida information och knyta kontakter.

Ett mer informellt nätverk av kommunerna i fd Skaraborg finns också.

Informationssäkerhetsmål

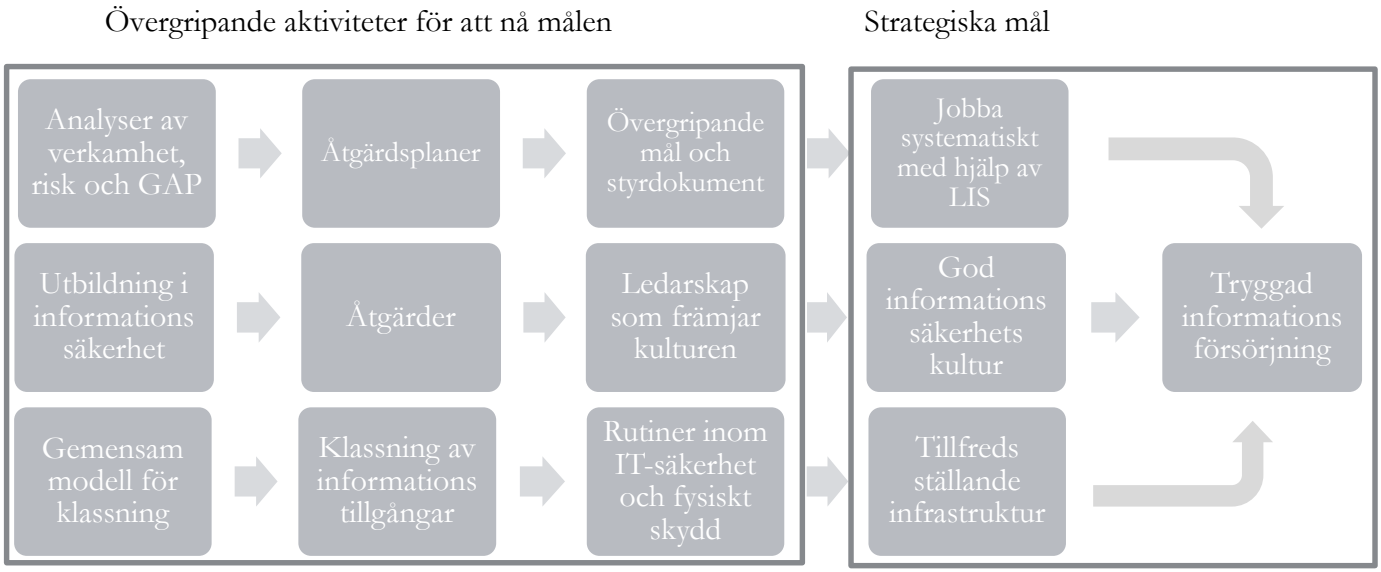
Beslut om vilka strategiska mål kommunen ska ha för informationssäkerheten fattas av kommunfullmäktige och är en del av policy för informationssäkerhet. Mer konkreta mål ska arbetas fram inom varje nämnd/förvaltning och bolag. Målen på förvaltningsnivå kan handla om tex organisationsstruktur, riskhantering, åtkomst av information, fysisk säkerhet, kunskap och kompetens hos chefer och medarbetare, hantering av incidenter, kontinuitetsplanering, drift och kommunikation mm.

Det slutliga strategiska målet med informationssäkerhetsarbetet är att trygga informationsförsörjningen genom att upprätthålla rätt nivå på skydd när det gäller tillgänglighet, riktighet och konfidentialitet.

Koppling mellan övergripande aktiviteter och de strategiska målen

En målgraf kan tydliggöra kopplingen mellan övergripande aktiviteter och strategiska mål.
Det slutgiltiga strategiska målet (tryggad informationsförsörjningen) bryts ner till tre områden:

- Systematiskt informationssäkerhetsarbete med hjälp av ledningssystemet
- Kultur som främjar hög informationssäkerhet
- Tillfredsställande teknisk och fysisk infrastruktur



Målgrafen kan vara en hjälp för förvaltningarna i deras planering och genomförande av det systematiska informationssäkerhetsarbetet. Förvaltningarnas mål och aktiviteter när det gäller arbetet med informationssäkerhet bör införlivas i de huvud- och stödprocesser som förvaltningen normalt arbetar med.

Styrdokument

Styrdokument är en viktig del i ett ledningssystem. Dokumenten kan vara övergripande och strategiska eller mer specifika för en viss verksamhet. De övergripande dokumenten ska peka ut ledningens viljeinriktning med arbetet och sätta mål. De specifika styrdokumenten ska omvandla viljeinriktningen och målen till mer konkreta rutiner för verksamheten att följa.

Policy för informationssäkerhet

Policy för informationssäkerhet är det strategiska och övergripande dokument för informationssäkerhetsarbetet som finns i Karlsborgs kommun. Dokumentet är fastställt av kommunfullmäktige. Dokumentet ska ses som ett paraplydokument för övriga styrdokument.

Enligt ISO-standard 27001 ska en policy omfatta en rad olika punkter för att den ska anses som fullgod.

Enligt ISO-standarden är det högsta ledningen som ska **upprätta och fatta beslut** om policyn. Dokumentet ska vara anpassad till **organisationens syfte**. Policyn ska ge ett ramverk för att sätta **informationssäkerhetsmål och** innehålla åtagande att uppfylla tillämpliga **krav** som måste genomföras för att uppnå målet. Policyn ska även innefatta ett åtagande att **ständigt förbättra ledningssystemet för informationssäkerhet.**

Utöver ovanstående krav ska policyn vara **dokumenterad**. Den ska **kommuniceras** i organisationen och vara **tillgänglig** för intressenter.

Riktlinje för systematiskt informationssäkerhetsarbete

Riktlinjen förtydligar och konkretiserar innehållet i policyn och beskriver de olika delarna i ledningssystemet. Riktlinjen styr hur arbetet med analyser, klassningar, målformuleringar, handlingsplaner, uppföljningar mm ska genomföras.

Riktlinje för informationssäkerhetsåtgärder

Riktlinjen går igenom ISO-standardens kravområde och förtydligar vad dessa innebär för Karlsborg. Kopplar till GAP-analysen i Stratsys.

Rutin för dokumentation av informationssäkerhetsarbetet

Anvisningen är en vägledning i hur dokumentation av informationssäkerhetsarbetet i Stratsys ska ske.

Rutin IT-säkerhet för användare

Regler för användare (förtroendevalda, medarbetare, chefer, konsulter) när det gäller tex information och lagring, nätverk och program, hemarbete, mobila enheter, incidentrapportering.

Övriga styrdokument

Förutom de styrdokument som direkt kan kopplas till arbetet med informationssäkerhet finns ett antal övriga som kan vara aktuella att ha kännedom om och som indirekt kopplar till området informationssäkerhet. Dessa är bland andra:

- Policy för integritet vid hantering av personuppgifter
- Arkivreglemente
- Dokumenthanteringsplaner
- Säkerhetsskyddsplan
- Policy för upphandling
- Riktlinjer för inköp
- Alkohol- och drogpolicy
- Kompetensförsörjningsplan
- Ledarskapspolicy
- Personalpolicy
- IT-policy
- Mobiltelefonpolicy
- Plan för digital utveckling
- Riktlinje för intern och extern kommunikation
- Riktlinje för telefoni
- Politiska reglementen
- Riktlinje för informationshantering och journalföring inom hälso- och sjukvården.

Fler ej politiskt beslutade styrdokument (tex rutiner och anvisningar) finns framtagna, tex rutin för rekrytering, anvisning för dokumentlagring, anvisning utlämnande av handlingar, rutin ärendehantering och mötesadministration mfl som berör ämnet informationssäkerhet.

Klassningsmodell

Klassning är en förutsättning för att skapa rätt skydd för informationen och undvika överskydd med onödiga kostnader och krångliga rutiner som följd.

Klassningsbesluten förbereds genom att en kartläggning av organisationens informationstillgångar genomförs. En aktuell förteckning av kommunens informationstillgångar ska finnas tillgänglig i Stratsys. Varje förvaltning ansvarar för att förteckningen hålls uppdaterad.

Data kring informationstillgången samlas in, tex

- Typ av informationstillgång
- Vilken typ av information som hanteras
- Informationstillgångens påverkan
- Antal användare
- Systemansvarig
- Legala krav

Klassning av information görs utifrån en fastställd klassningsmodell. Modellen ska innehålla perspektiven konfidentialitet, riktighet och tillgänglighet. Modellen för klassning ska vara enhetlig för hela organisationen. Modellen i Karlsborgs kommun utgår ifrån SKR´s KLASSA. Dokumentation av själva klassningen utförs i strategiverktyget Stratsys.

I klassningsförfarande ska frågan nedan ställas.
Vilka blir konsekvenserna om informationens konfidentialitet/riktighet/tillgänglighet inte upprätthålls i den utsträckning verksamheten behöver?

Konsekvenserna kan delas in i kategorier:

- *Ekonomi* (förlust av tillgångar, ökade kostnader, minskade intäkter)
- *Samhälle* (samhällsviktiga funktioner eller påverkan på andra organisationer/myndigheter)
- *Verksamhet* (organisationens möjligheter att nå målen, fullfölja uppdrag och förtroende för organisationen)
- *Individ* (påverkan på individers fysiska och psykiska hälsa samt ekonomisk skada)

Olika konsekvensnivåer ska beslutas, allt ifrån ingen konsekvens till allvarlig konsekvens. Skalan på konsekvenserna går från ingen eller försumbar skada till allvarlig skada. Varje informationstillgång ska klassas för att dess information ska kunna skyddas på bästa sätt.

I strategiverktyget Stratsys finns utvalda kravområden (säkerhetsåtgärder) samlade i GAP-analysen. Varje kravområde (med tillhörande informationssäkerhetskrav) har en konsekvensnivå. Konsekvensnivåerna kopplar till de fyra konsekvensnivåerna i klassningsmodellen (försumbar, måttlig, betydande, allvarlig) och indikerar betydelsen av informationssäkerhetskravet för verksamheten.

En vägledande tabell är framtagen för att underlätta bedömningarna.

Informationsklassning				
Nivå skada	**Ekonomisk förlust**	**Samhälle**	**Verksamhet**	**Individ**
Allvarlig skada	Allvarlig ekonomisk förlust som innebär att verksamheten kan ha allvarliga svårigheter att drivas vidare.	Allvarlig påverkan på samhällsviktiga funktioner vid egen eller annans organisation.	Allvarliga svårigheter att nå målen och fullfölja uppdraget. Allvarlig skada på förtroende genom drev i riksmedia där organisationen pekas ut.	Enskilda individer drabbas av allvarliga besvär (fysiska, psykiska eller ekonomiska) som kan vara oåterkalleliga.
Betydande skada	Betydande ekonomisk förlust som innebär verksamheten kan ha betydande svårigheter att drivas på ordinarie sätt.	Betydande påverkan på samhällsviktiga funktioner vid egen eller annans organisation.	Betydande svårigheter att nå målen och fullfölja uppdraget. Betydande skada på förtroende genom att	Enskilda individer drabbas av betydande besvär (fysiska, psykiska eller ekonomiska) som endast med stor

			missnöjda individer uttalar sig i både riks- och lokal media.	ansträngning kan övervinnas.
Måttlig skada	Måttlig ekonomisk förlust som innebär att verksamheten kan ha måttliga svårigheter att bedrivas på ordinarie sätt.	Måttlig påverkan på samhällsviktiga funktioner vid egen eller annans organisation.	Måttliga svårigheter att nå målen och fullfölja uppdraget. Måttlig skada på förtroende genom att missnöjda individer uttalar sig i både social- och lokal media.	Enskilda individer drabbas av måttliga besvär (fysiska, psykiska eller ekonomiska) som trots vissa svårigheter, kan övervinnas.
Ingen eller försumbar skada	Ingen eller mycket försumbar ekonomisk förlust som inte innebär någon påverkan på hur verksamheten kan bedrivas vidare.	Ingen påverkan på samhällsviktiga funktioner vid egen eller annans organisation.	Inga svårigheter att nå målen och fullfölja uppdraget. Ingen eller lite negativ uppmärksamhet i lokal media.	Enskilda individer påverkas inte eller kan uppleva få besvärligheter som enkelt kan övervinnas.

En nivå över ”allvarlig skada” finns också i SKR´s KLASSA, men avser skada på rikets säkerhet som ej är försumbar. Denna typ av information och verksamhet hanteras inte i strategiverktyget.

Modell för informationsmärkning

Viss information är mer känslig än annan. Behovet av skydd skiljer sig därför mellan olika typer av information och i olika situationer. Skyddsbehovet beror på legala krav och vilka konsekvenser det skulle för verksamheten eller enskilda individer om informationen sprids till obehöriga. I Karlsborgs kommun finns fyra klasser för hur känslig informationen är och hur den får spridas.

Informationsmärkning		
Nivå	**Behörighet och spridning**	**Exempel**
Hög sekretess	Endast ett mycket begränsat antal personer ska ha tillgång. Normalt sett ingen spridning.	Om informationen hamnar i orätta händer kan det medföra fara för liv, hälsa eller samhällsskada, tex skyddade personuppgifter,

		information om el- och vattenförsörjning.
Känslig - sekretess	Endast den som behöver informationen för att klara sina arbetsuppgifter ska ha tillgång. Särskild åtkomstbegränsning med god spårbarhet.	Känsliga personuppgifter, tex personnummer, hälsostatus, information om pågående upphandling, skalskyddsritningar.
Begränsad	Normal åtkomstbegränsning med viss spårbarhet	Uppgifter som inte är sekretesskyddade men ändå ska hanteras med varsamhet, tex vissa personuppgifter, ekonomisk information, kontaktuppgifter, avtal mm.
Öppen	Ingen åtkomstbegränsning	Information som är helt offentlig och som kan spridas utan restriktion, tex de flesta styrdokumenten, avgifter, öppettider, protokoll mm.

Handlingsplaner

Åtgärdsplan

En åtgärdsplan består av ett antal åtgärder som ska vidtagas för att skydda organisationens information. Åtgärderna tas fram efter till exempel utförda riskanalyser eller GAP-analys. Åtgärderna behöver anpassas till den information organisationen hanterar samt vilka risker som finns när informationen hanteras. Syftet med åtgärderna är att minimera risker.

Planen ska bestå av ett antal åtgärder som ska vidtagas för att minimera risker och för att uppnå de säkerhetskrav som ställs i ISO- standard 27001. Olika typer av åtgärder kan sättas in och oftast behöver de kombineras.

En åtgärd kan vara:

- *Organisatorisk:* Roller, ansvar och mandat fördelas i organisationen så att risken för felaktig hantering minskar.

- *Administrativ:* Framtagande av styrdokument för att fastställa vilka rutiner som ska följas. Genomförande av utbildningar.
- *Fysisk*: Skydd för obehörig fysisk åtkomst, tex larm, lås och behörighetsstrukturer.
- *Teknisk:* Olika tekniska lösningar för att skydda informationen, tex antivirusprogram, behörighetssystem, loggningar och säkerhetskopiering.

Åtgärderna i planen bör kopplas till de långsiktiga målen och övergripande aktiviteter för att nå målen samt de rättsliga krav som åligger.

Åtgärderna i planen ska vara tidsatta, ansvar och resurser ska fördelas samt metod och tidpunkt för uppföljning bör vara bestämt.

Det kanske inte är möjligt att genomföra alla åtgärder på en gång. En prioritering behöver därför göras. En avvägning mellan förväntat resultat och resurser behöver då göras.

Aktiviteterna sammanställs sedan i en handlingsplan där arbetet dokumenteras och progressen kan följas.

Årshjul för det systematiska informationssäkerhetsarbetet

För att arbetet med det systematiska informationssäkerhetsarbetet ska bli en del av verksamheten behöver de olika momenten planeras in över året och ansvar fördelas.

Utbildningsplan

Åtgärder för att höja informationssäkerheten innefattar ofta utbildning av olika grupper av medarbetare. Insatserna bör planeras och sammanställas i en utbildningsplan.

Använda

När väl analyser är gjorda, mål och organisation är satta, styrdokument framtagna, modeller är beslutade och åtgärder framtagna är det dags att börja använda ledningssystemet. I detta moment är det viktigt att se till att klassningen av informationstillgångar och åtgärder i handlingsplanen genomförs samt att styrdokument efterlevs. För detta krävs ofta utbildnings- och kommunikationsinsatser.

Utbildning och kommunikation

Alla i organisationen har ett visst ansvar för att inte äventyra innehållet i verksamhetens informationstillgångar. Informationssäkerhetssamordnaren har ett annat ansvar än tex en förskolelärare. Så för att alla ska kunna vara den där mänskliga brandväggen som behövs i verksamheten är det viktigt att anpassa utbildning och information till målgruppen. Kommunikation bör ske på olika sätt, tex muntligt, skriftlig, genom praktiska exempel osv. Då ökas chanserna för att informationen bli mottagen korrekt.

Utbildningsplanen bör innehålla olika insatser för hur förtroendevalda, chefer och medarbetare ska höja sin kompetensnivå inom området informationssäkerhet. Detta gäller både vid introduktion samt löpande under anställningstiden. Utbildning kan ske på olika sätt, tex genom nanoutbildbildning, implementering av styrdokument, externa föreläsningar, praktiska övningar och andra gruppaktiviteter.

Klassa information

Tidigare genomförd kartläggning av organisationens informationstillgångar ligger till grund för klassificeringsbesluten. Perspektiven konfidentialitet, riktighet och tillgänglighet bedöms var för sig enligt tidigare fastställ modell (konsekvensnivåer). Förklaringar till klassificeringsbeslut bör dokumenteras för att resonemanget bakom beslutet ska kunna följas. Klassningen av informationstillgången ska vara aktuell, dvs om innehållet i tillgången förändras ska klassningsbeslutet ses över. Varje förvaltning ansvarar för att klassningen av informationstillgångarna genomförs och är aktuell.

Tilldela informationsmärkning

Informationsmärkningen är en sammanvägning vad den klassifikationsbedömning som gjorts utifrån konfidentialitet, riktighet och tillgänglighet. Bedömningen ska ge användarna en fingervisning om hur informationen i informationstillgången får användas och spridas.

Genomföra och efterleva

När väl alla delarna i ledningssystemet är på plats (organisation, ansvar, roller, mål, olika analyser, klassningar, handlingsplaner med åtgärder osv) är det dags att börja genomföra de åtgärder som beslutats om och därmed förhoppningsvis förbättra organisationens informationssäkerhet. För att lyckas med detta är det viktigt att fundera kring ett antal frågor.

- Hur ska handlingsplanerna aktiviteter verkställas?

När aktiviteterna i de olika handlingsplanerna (åtgärder, årshjul och utbildning) fastställts ska arbetet med att planera genomförandet av dem. En tidplan för alla aktiviteter ska tas fram samt en uppskattning av vilka resurser (tid och pengar) som beräknas gå åt för att genomföra aktiviteten. En ansvarig person utses, men givetvis kan flera personer hjälpas åt att genomföra aktiviteten. Tidplanen och resurssättning utarbetas av kommunens ledningsgrupp. Det är även här som arbetets fortlöpande följs upp. Löpande dokumentation av arbetet sker.

- Hur säkerställer vi att styrdokument efterlevs?

För att de framtagna styrdokumenten ska få genomslag och önskad effekt i verksamheten är det viktigt att de skrivs på ett sätt som medarbetarna lätt kan ta till sig. Dokumenten behöver även finnas tillgängliga så att de är lätta att hitta. Det behöver även finnas rutiner för hur och när styrdokumenten ska uppdateras, för att säkerställa att informationen i dokumenten är korrekt.

När ett nytt styrdokument tas fram är det dessutom viktigt att informera och utbilda medarbetare som förväntas följa det som står i dokumentet. Om medarbetarna själva får vara med att ta fram rutiner och anvisningar är det större chans att de fungerar i verksamheten och att dokumentet blir känt.

- Hur hanterar vi större händelser och förändringar?

Även om det finns en framtagen tidplan för hur aktiviteterna ska genomföras, kan det inträffa händelser under året som måste prioriteras. Vissa aktiviteter i handlingsplanen kanske kan skjutas på framtiden, andra kanske måste genomföras ändå. Alternativa resurser kanske kan finnas tillgängliga och aktiviteterna kan genomföras med hjälp dessa. Om inte behöver en prioritering av aktiviteterna genomföras och konsekvenserna av att inte genomföra dem behöver utredas.

Följa upp och förbättra

I denna del av ledningssystemet gäller det att följa upp det arbete som genomförts och besluta om hur det kan bli bättre.

Ledningens genomgång

Vid ledningens genomgång tar ledningen ställning till om det systematiska informationssäkerhetsarbetet är fortsatt lämpligt, tillräckligt och har fått avsedd verkan. En sammanfattning av årets informationssäkerhetsarbete presenteras av informationssäkerhetssamordnaren. Genomgången innehåller bland annat:

- Väsentliga förändringar internt och externt
- Övergripande resultat av riskanalyser och GAP-analys

- Rapporterade incidenter och avvikelser
- Uppföljning av beslutade åtgärder
- Resultat från övervakningar och mätningar
- Måluppfyllelse

Vid ledningens genomgång ska diskussion föras om hur det systematiska informationssäkerhetsarbetet kan förbättras, om styrdokument behöver uppdateras, om det finns behov av ytterligare säkerhetsåtgärder och om det behöver tillskjutas mer medel till arbetet framåt. Informationssäkerhetssamordnaren kan rekommendera ledningen att fatta beslut om kommande förändringar.

Utvärdera

Utvärdering kan ske på olika sätt, tex genom övervakning, mätning eller måluppföljning. Utvärderingens syfte är att se om det systematiska informationssäkerhetsarbetet är utformat på ett **lämpligt** sätt, om det är **tillräckligt** omfattande och om det fått avsedd **verkan**. Resultatet av utvärderingen kan ligga till grund för intern revision och ledningens genomgång.

Hur omfattande utvärderingen ska vara kan variera beroende på behov och tillgängliga resurser.

1. *Liten* – en miniminivå som alla organisationer bör genomföra innebär att informationssäkerhetsmålen utvärderas samt om ledningssystemet bedöms som lämpligt, tillräckligt och får verkan för informationssäkerheten.
2. *Mellan* – förutom mininivån gör även en förnyad GAP-analys, uppföljning av efterlevnad av styrdokument samt en mognadsmätning.
3. *Stor* – förutom minimi- och mellannivå genomförs även en extern revision av det systematiska informationssäkerhetsarbetet.

Karlsborgs kommun ska genomföra en utvärdering som åtminstone uppfyller minimikraven enligt ovan.

Uppfylla mål

De mål som policy för informationssäkerhet pekar ut ska kunna mätas för att få reda på om de är uppfyllda eller inte. En samlad bedömning görs om de tre strategiska målen uppfyllts och där med även det slutliga målet.