KARLSBORG

Policy för informationssäkerhet

Gäller för:	Samtliga förvaltningar och bolag
Diarienummer:	2023-348
Beslutande:	Kommunfullmäktige
Datum för beslut:	2023-10-23
Paragraf i protokoll:	§ 157
Gäller från och med:	2023-11-01
Dokumentansvar:	Kanslichef
Aktualitetsprövning:	2025-11-01 (Aktualitetsprövning ska ske av dokumentansvarig två år efter beslut/senaste revidering)

Innehåll

Inledning

Information är värdefullt och behöver skyddas efter behov. Ett bra informationssäkerhetsarbete är en förutsättning för effektiv och korrekt informationshantering. Detta skapar förtroende både inom och utanför organisationen. Alla medarbetare hanterar information dagligen och därför är det viktigt att informationssäkerhet inte bara ses som en ”IT-fråga” eller något som en enskild person arbetar med.

Syfte

Syfte med en policy för informationssäkerhet är att kortfattat beskriva 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.

Övriga styrdokument, tex riktlinjer, rutiner och anvisningar, ska finnas tillgängliga för det mer vardagsnära arbetet med informationssäkerhet.

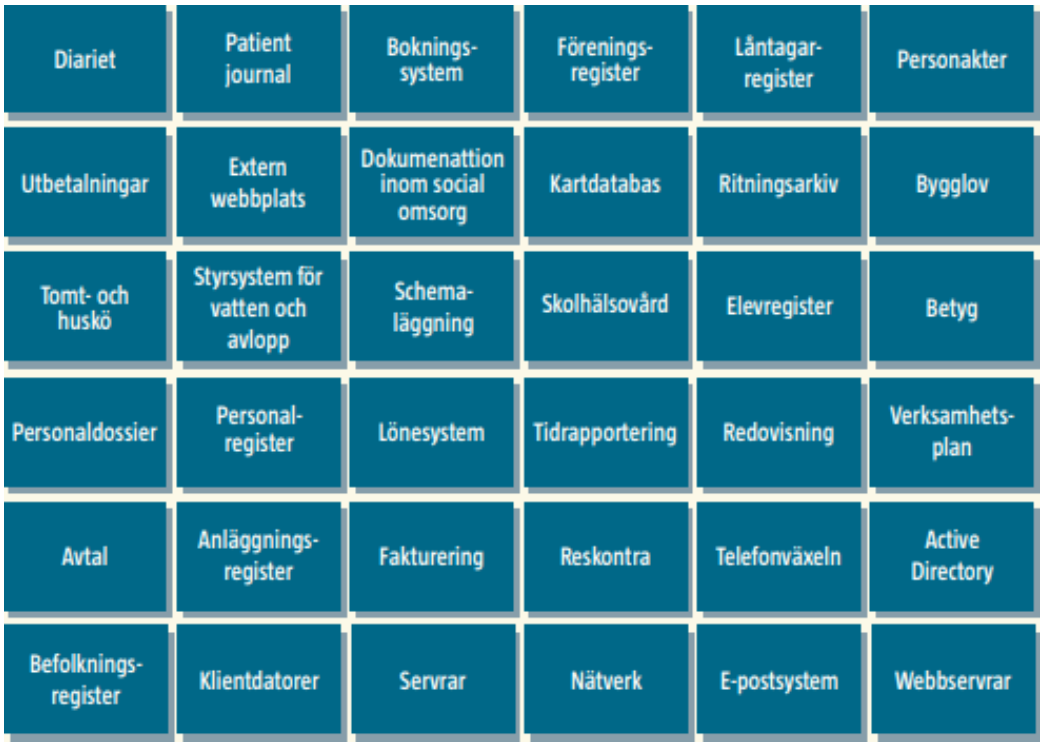
Information

Information är medlet för att förmedla kunskap. Information kan kommuniceras, lagras, förädlas och styra processer. Information behövs för det mesta som en kommun gör, helt enkelt.

En del information är värdefull, både för organisationer och enskilda individer. Information är allt från forskningsresultat och fotografier till fastighetsförteckningar och saldot på bankkontot. Ibland är information livsviktig, tex information i patientjournaler och styrsystem för vattenverk. Om informationen går förlorade eller är felaktig kan det få katastrofala följder. Information är en tillgång och därför är det viktigt att skydda informationen. Det är det som informationssäkerhet handlar om och är viktigt.

Informationstillgångar

Med informationstillgångar avses all information och relaterade resurser (tillgångar) som behövs för att hantera information. Exempel på sådana tillgångar är IT-system, IT-infrastruktur (tex servrar, wifi mm), digital lagringsmedia och papper. Exempel på informationstillgångar som en kommun har visas i bilden nedan.



Informationssäkerhet

Information är värd att skydda utifrån fyra perspektiv:

- *Tillgänglighet* – att information finns när den behövs och är lätt att hitta.
- *Riktighet* – att informationen går att lita på, att den är korrekt och inte förstörd eller manipulerad.
- *Konfidentialitet* – att endast behöriga personer får ta del av informationen och att den skyddas från obehöriga.

Skyddet av informationen ska anpassas efter behovet så att det är tillräckligt bra, så enkelt som möjligt att använda och så kostnadseffektivt som möjligt. Brister i hanteringen av information kan bland annat leda till försämrat förtroende hos medborgarna, ökade ekonomiska kostnader och bristande effektivitet.

Arbetet med informationssäkerhet handlar om att:

- Ta fram och fastställa **styrande dokument** för arbetet (tex policy för informationssäkerhet).
- Ha fungerande **tekniskt skydd** så som brandväggar och kryptering.
- Ha fungerande **fysiskt skydd** så som skal- och brandskydd i kommunens lokaler.

För att få ett väl fungerande arbete med informationssäkerhet behöver alla delar i kommunens verksamhet engageras eftersom information hanteras dagligen i alla verksamheter.

Mål med informationssäkerhetsarbetet

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

För att uppnå detta krävs att:

- Verksamheterna jobbar systematiskt med sitt informationssäkerhetsarbete där de med hjälp av ledningssystem för informationssäkerhet tar fram mål och styrdokument, beslutar om åtgärder och följer upp arbetet.
- Det finns en kultur i verksamheterna som främjar god informationssäkerhet, där både chefer och medarbetare känner ansvar och har tillräcklig kunskap.
- Det finns en tillfredsställande teknisk och fysisk infrastruktur som främjar hög informationssäkerhet. Rutiner för IT-säkerhet och fysiskt skydd tas fram efter att klassning visar vilka informationstillgångar som är mest kritiska och skyddsvärda.

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.

Ledningssystem för informationssäkerhet (LIS)

Ett ledningssystem för informationssäkerhet hjälper ansvariga att analysera, planera, genomföra och följa upp informationssäkerhetsarbetet. Arbetet med att införa ett ledningssystem innebär kortfattat att göra olika typer av analyser av verksamheten och dess risker. Därefter utformas organisation, mål, styrdokument, klassningsmodeller och handlingsplaner som sedan används i verksamheten. Utvärdering av arbetet sker regelbundet.

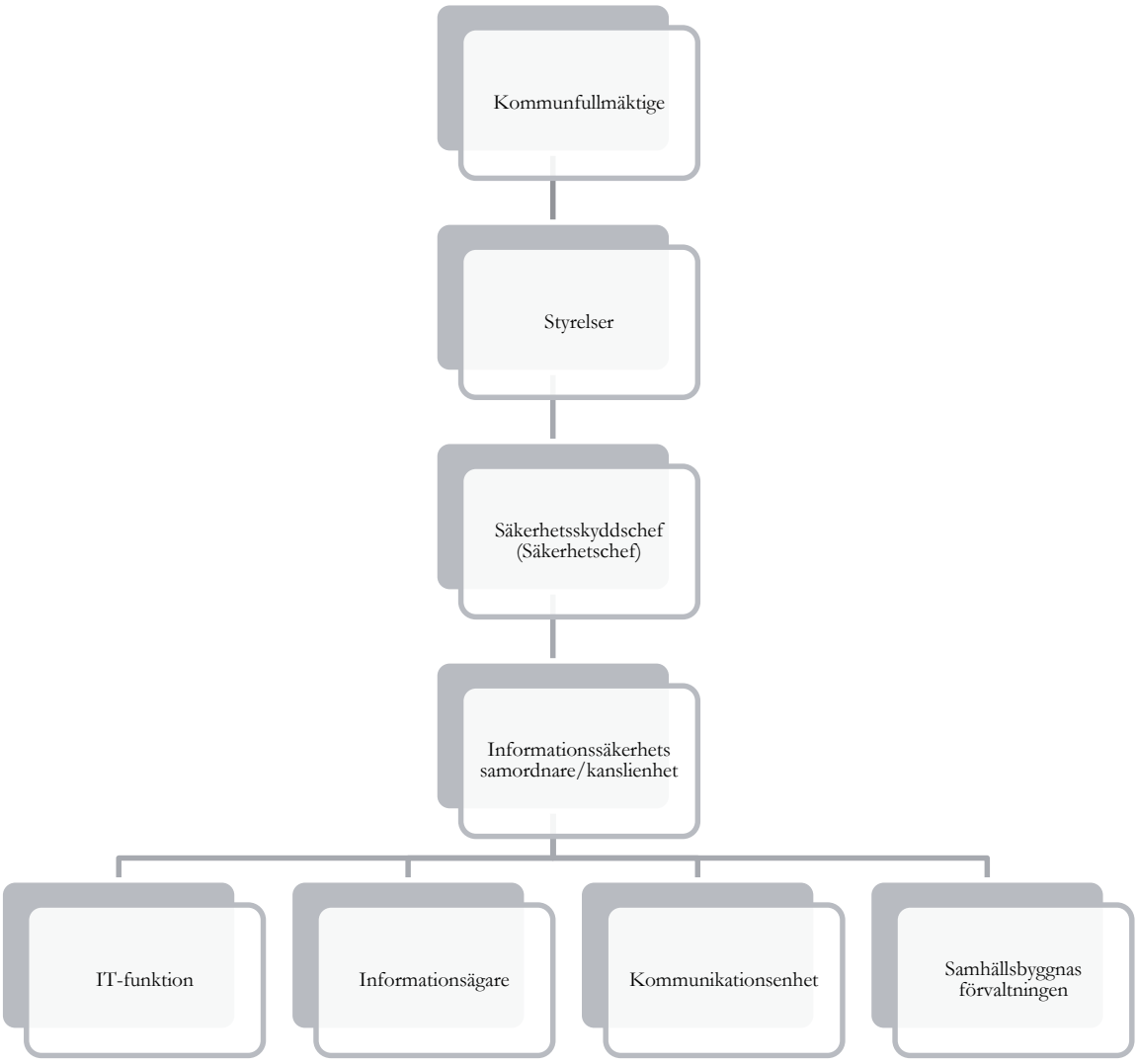
Arbetet med ledningssystem för informationssäkerhet i Karlsborgs kommun bör anpassas till en nivå som är rimlig för verksamheten. Metodstöd från tex

Myndigheten för samhällsskydd och beredskap kvalitetssäkrar arbetet. Samverkansmöjligheter med andra kommuner bör ses över.

Organisation, roller och ansvar

För att arbetet med informationssäkerhet ska ske på ett systematiskt och långsiktigt hållbart vis bör organisation, roller och ansvar vara tydliga.

Säkerhetsskyddsorganisationen för



Karlsborgs kommun

Roller och ansvarsfördelning

Kommunfullmäktige

Kommunfullmäktige är ytterst ansvarig för informationssäkerhetsarbetet och beslutar om policy för informationssäkerhet.

Styrelser

Kommunstyrelsen och bolagsstyrelser ansvarar för att samordna och följa upp kommunens arbete med informationssäkerhet. Kommunstyrelsen har det övergripande ansvaret för att utarbeta, förvalta och följa upp styrande dokument för kommunens verksamheter.

Säkerhetschefen

Säkerhetschefen ansvarar för:

- Säkerhetsskyddsklassificering av information
- Tillträdes- och behörighetsanalyser
- Hantering av hemliga handlingar
- Säkerhetsprövningar
- Säkerhetsklassning av personal
- Säkerhetsanalyser
- Säkerhetschefen är tillika signalskyddschef (SigneK)

Informationssäkerhetssamordnare och kanslienhet

Kanslichefen är tillika informationssäkerhetssamordnare och ansvarar för att på en kommunövergripande nivå samordna det systematiska informationssäkerhetsarbetet. Det kan bland annat innebära framtagande av styrdokument, sammankallande till arbetsgrupper, planera och genomföra informations- och utbildningsinsatser mm. Kanslienheten ansvarar för administration av SigneK kryptosystem.

IT-funktion

Drift av IT-miljön ansvarar Skövde kommun för. I det ansvar ligger även IT- och telefonisäkerhetsfrågor.

Informationsägare

Informationsägare (tex nämnder med förvaltning och kommunala bolag) ansvarar för informationshanteringen inom sina verksamheter och avgör vilken information som får hanteras, hur den ska hanteras och av vem den får hanteras. Chefer i kommunens förvaltningar och bolag ansvarar för att tillräcklig kunskap om informationssäkerhet finns i den egna verksamheten, se till att verksamheten följer styrande informationssäkerhetsdokument, se till att det finns resurser samt att följa upp informationssäkerhetsarbetet i den egna verksamheten. Medarbetare i verksamheten har ansvar för att följa kommunens styrdokument kopplat till informationssäkerhet samt rapportera uppmärksammade brister.

Kommunikationsenheten

Kommunikationsenheten ansvarar för att:

- Skapa förutsättningar för informationsägare att upprätthålla hög informationssäkerhet i kommunens digitala kanaler såsom extern webb, intranät och sociala medier.
- Administration av SigneK kryptosystem

Samhällsbyggnadsförvaltningen

Samhällsbyggnadsförvaltningen ansvarar för:

- Fysiskt tillträdesskydd
- Hantering av taggar, koder, nycklar