



Informationssäkerhetspolicy

DNR KS 2025/85

Gäller för: Samtliga förvaltningar och bolag
Beslutande: Kommunfullmäktige
Datum för beslut: 2025-10-27
Gäller till: Tillsvidare
Dokumentansvarig: Kansliavdelningen

Innehållsförteckning

INLEDNING	3
SYFTE.....	3
LEDNINGSSYSTEM FÖR INFORMATIONSSÄKERHET (LIS)	3
STRATEGISKA MÅL MED INFORMATIONSSÄKERHET	4
ETABLERA ETT LEDNINGSSYSTEM FÖR INFORMATIONSSÄKERHET (LIS)	4
FÖRTECKNING ÖVER SAMTLIGA INFORMATIONSTILLGÅNGAR I KOMMUNEN	4
TYDLIG ROLL- OCH ANSVARSFÖRDELNING.....	4
FORTLÖPANDE UTBILDNING	4
KRAV VID UPPHANDLING OCH I LEVERANTÖRSAVTAL	4
UTVECKLA KONTINUITETS- OCH BEREDSKAPSPLANER	4
UPPFÖLJNING AV INFORMATIONSSÄKERHETSARBETET	4
ARBETA MED INFORMATIONSSÄKERHET	4
INFORMATIONSSÄKERHETSORGANISATION, ROLLER OCH ANSVAR.....	5
KOMMUNFULLMÄKTIGE.....	5
KOMMUNSTYRELSEN	5
KOMMUNSTYRELSEN, NÄMNDER OCH BOLAGSSTYRELSER.....	5
KANSLIAVDELNINGEN.....	5
ROLLER OCH ANSVAR.....	6
KOMMUNDIREKTÖR	6
INFORMATIONSÄGARE	6
SYSTEMÄGARE.....	6
SYSTEMFÖRVALTARE.....	6
SÄKERHETSSKYDDSCHEF	6
ANSTÄLLDA OCH FÖRTROENDEVALDA.....	6
UPPFÖLJNING OCH RAPPORTERING	6
REVIDERING AV POLICY	7

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.

Information är medlet för att förmedla kunskap. Information kan kommuniceras, lagras, förädlas och styra processer. Personuppgifter är en vanligt förekommande och skyddsvärd information. Information finns överallt och kan förekomma i många olika former – tryckt eller skrivet på papper, lagrad elektroniskt i IT-utrustning och på lagringsmedia, överförs med post och elektronisk utrustning, yttras i en konversation och vara en del av en persons kunskap.

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.

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

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.

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, instruktioner, vägledningar och rutiner, ska finnas tillgängliga för det mer vardagsnära arbetet med informationssäkerhet.

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.

Strategiska mål med informationssäkerhet

Åstorps kommun strävar efter att bedriva ett långsiktigt och systematiskt informationssäkerhetsarbete med utgångspunkt i etablerade standarder inom ISO 27000-serien.

Etablera ett ledningssystem för informationssäkerhet (LIS)

- Kommunen ska etablera ett ledningssystem för informationssäkerhet (LIS) i linje med ISO/IEC 27001, anpassat efter kommunens förutsättningar och behov.

Förteckning över samtliga informationstillgångar i kommunen

- En förteckning över kommunens informationstillgångar ska upprättas, klassificeras enligt gällande modell och säkerhetsåtgärder ska implementeras utifrån bedömt skyddsvärde.

Tydlig roll- och ansvarsfördelning

- En informationssäkerhetsorganisation ska etableras, med tydligt fördelade roller och ansvar för att genomföra det systematiska informationssäkerhetsarbetet.

Fortlöpande utbildning

- Samtliga medarbetare, chefer och ledning ska fortlöpande få utbildning i informationssäkerhet som är anpassad till deras respektive roller och ansvar.

Krav vid upphandling och i leverantörsavtal

- Informationssäkerhetskrav ska ställas vid upphandlingar och inkluderas i avtal med leverantörer som hanterar information eller IT-tjänster åt kommunen.

Utveckla kontinuitets- och beredskapsplaner

- Kommunen ska utveckla och underhålla kontinuitets- och beredskapsplaner för att säkerställa driften av kritiska verksamhetsfunktioner vid avbrott.

Uppföljning av informationssäkerhetsarbetet

- Informationssäkerhetsarbetet ska följas upp regelbundet, utvärderas och förbättras för att säkerställa efterlevnad och hantera förändrade risker.

Arbeta med informationssäkerhet

De grundläggande principerna för arbetet med informationssäkerhet handlar om att skapa och upprätthålla rutiner och skydd av information utifrån fyra aspekter:

- **Konfidentialitet:** att information inte tillgängliggörs eller avslöjas till obehörig.
- **Riktighet:** att information är korrekt, aktuell och fullständig.
- **Tillgänglighet:** att information är åtkomlig och användbar av behörig när den behövs.

- **Spårbarhet** är en stödjande säkerhetsprincip som innebär att alla relevanta aktiviteter i informationssystem ska kunna kopplas till en identifierad användare. Det ska framgå vem som gjort vad, när det gjordes och vilket resultat det fick. Syftet är att möjliggöra efterhandsgranskning, upptäcka obehörig åtkomst och säkerställa ansvarstagande vid incidenter.

Dessa åtgärder inkluderar bland annat att:

- Ha fungerande **tekniskt skydd** såsom brandväggar och kryptering.
- Ha fungerande **fysiskt skydd** såsom skal- och brandskydd i kommunens lokaler.
- Att implementera och upprätthålla en **informationssäkerhetskultur** bland kommunens medarbetare.

Informationssäkerhetsorganisation, roller och ansvar

För att arbetet med informationssäkerhet ska ske på ett systematiskt och långsiktigt hållbart vis bör organisation, roller och ansvar vara tydliga. Grundprincipen är att ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret.

Kommunfullmäktige

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

Kommunstyrelsen

Kommunstyrelsen ansvarar för att samordna och följa upp kommunens arbete med informationssäkerhet. Kommunstyrelsen har det övergripande strategiska ansvaret för att samordna och följa upp kommunens informationssäkerhetsarbete.

Kommunstyrelsen, nämnder och bolagsstyrelser

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.

Kansliavdelningen

Kansliavdelningen ansvarar för informationssäkerhetsfrågor och samordnar det systematiska informationssäkerhetsarbetet på en kommunövergripande nivå. Det kan bland annat innebära framtagande av styrdokument, sammankallande till arbetsgrupper, planera och genomföra informations- och utbildningsinsatser mm.

Roller och ansvar

Kommundirektör

Kommundirektören har i uppdrag att sörja för att informationssäkerhetsarbetet bedrivs effektivt i enlighet med denna policy.

Informationsägare

Informationsägare är den som bestämmer ändamålen för behandlingen och hanteringen av informationen. Informationsägaren äger och ansvarar för att informationen är riktig och tillförlitlig samt för det sätt informationen sprids.

Systemägare

Systemägare/objektägare har ansvaret för den verksamhet som aktuellt informationssystem/-objekt stödjer.

Systemförvaltare

Systemförvaltare/objektförvaltare tar det funktionella (dagliga) helhetsansvaret för ett system/objekt. Förvaltaren fungerar i hög grad som system-/objektägarens utförare och ser till att systemets/objektets funktionalitet samt planerade och beslutade aktiviteter genomförs och upprätthålls.

Säkerhetsskyddschef

Säkerhetsskyddschef ansvarar för informationssäkerheten i verksamhet som har betydelse för Sveriges säkerhet och lyder under säkerhetsskyddslagen.

Anställda och förtroendevalda

Anställda och förtroendevalda ansvarar för att följa kommunens styrdokument kopplat till informationssäkerhet samt att rapportera uppmärksammade brister.

Uppföljning och rapportering

Kommunen ska följa upp informationssäkerhetsarbetet årligen. Kommunstyrelsen ska minst en gång per år få en övergripande redovisning av kommunens arbete med informationssäkerhet. Uppföljningen ska omfatta bland annat:

- En omvärldsanalys av faktorer som kan påverka informationssäkerheten
- Aktuell status och identifierade behov avseende utbildningsinsatser
- Resultat från genomförda revisioner eller granskningar
- Pågående och planerade informationssäkerhetsåtgärder
- Genomförda riskanalyser

Vid särskilda omständigheter – exempelvis allvarliga incidenter, identifierade brister eller andra behov – kan ytterligare rapportering tillkomma utöver den ordinarie årsvisa uppföljningen.

Revidering av policy

Informationssäkerhetspolicyn ska aktualitetsprövas vid varje ny mandatperiod. Vid lagförändringar inom området kan revidering initieras. Dokumentansvarig är kansliavdelningen.