Informationssäkerhetspolicy för Trosa kommun

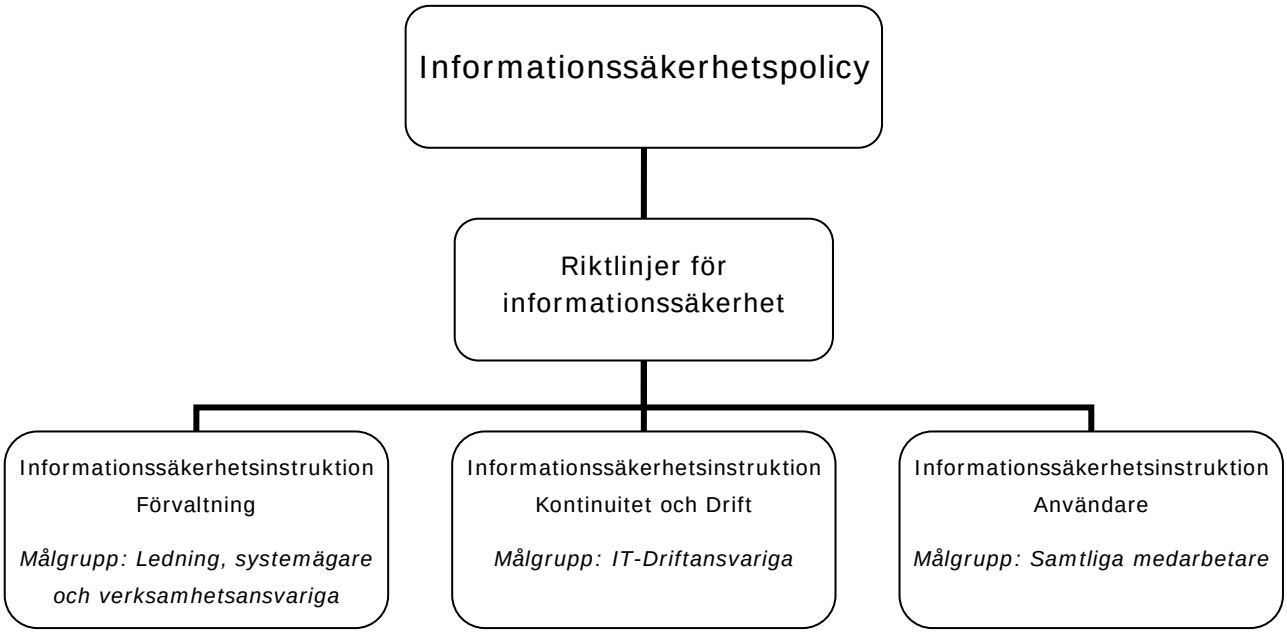
Antagen av:	Kommunfullmäktige 2020-06-10, § 55. KS 2020/122
Dokumentkategori:	Styrdokument
Dokumenttyp:	Policy

Innehållsförteckning

Inledning

Informationssäkerhetspolicyn är ett dokument som redovisar kommunens övergripande syfte och inriktning med informationssäkerhet samt hur ansvaret i dessa frågor är fördelat.

Denna informationssäkerhetspolicy gäller för informationssäkerhet inom Trosa kommun, och kompletterar kommunens övriga styrdokument inom säkerhetsområdet. Hela kommunkoncernen omfattas av policyn, vilket medför att det inte finns utrymme att besluta om lokala regler som avviker från denna. Policyn ska konkretiseras i riktlinjer och i informationssäkerhetsinstruktioner.



Syftet med Trosa kommuns informationssäkerhetsarbete är att hantera och skydda informationen i verksamheterna på sådant sätt att rättsliga och verksamhetsmässiga krav, samt medborgarintressen kan tillgodoses. Detta skapar en robust, säker och tillförlitlig informationshantering i hela organisationen.

Skyddet ska vara anpassat till informationens skyddsvärde, risk och lagkrav. En god informationssäkerhet inom kommunen främjar verksamheternas funktionalitet, kvalitet och effektivitet. Dessutom främjas medborgarnas rättigheter och personliga integritet, kommunens förmåga att förebygga och hantera allvarliga störningar och kriser samt förtroendet för kommunens informationshantering och IT-system.

Om informationssäkerhet

Information är en av kommunens viktigaste tillgångar och utgör en förutsättning för att kunna bedriva verksamheten. Trosa kommuns informationstillgångar måste därför behandlas och skyddas på ett tillfredsställande sätt.

Informationstillgångar finns i alla kommunens verksamheter och begränsas inte till säkerhet i IT-system, utan omfattar information i alla dess former och oavsett hur information lagras, bearbetas och kommuniceras. Information kan till exempel vara i form av text, ljud, bilder och film, och kan hanteras med stöd av dator, papper eller direkt av oss människor i form av tal. En informationstillgång innebär allt som innehåller information och allt som bär på information.

Informationssäkerhet handlar om att skapa och upprätthålla lämpliga rutiner och skydd av information utifrån fyra aspekter:

- Konfidentialitet – Endast den med rätt behörighet ska kunna ta del av
- viss information.
- Riktighet – Informationen är korrekt, aktuell och fullständig.
- Tillgänglighet – Informationen är tillgänglig när den behövs för rätt person i rätt tid.
- Spårbarhet – Händelser i informationsbehandlingen ska kunna spåras.

Kraven på hantering av information styrs av lagar, förordningar, avtal och Trosa kommuns egna styrdokument. Utöver det har den enskilde, företag och andra aktörer i vår omvärld behov och förväntningar som ställer krav på vår informationssäkerhet. Avbrott i tillgången till information kan vara kritiskt och felaktig information kan ge allvarliga konsekvenser.

Principer och arbetssätt

Arbetet med informationssäkerhet ska gentemot koncernens verksamheter vara normerande, stödjande och kontrollerande. Viktiga förmågor i det arbetet är att kunna identifiera hot, sårbarheter och risker rörande kommunens informationstillgångar, samt att kunna utforma och införa säkerhetsåtgärder som reducerar dessa risker till en acceptabel nivå.

Arbetet med informationssäkerhet inom Trosa kommun ska:

- vara systematiskt och bygga på etablerade standards med målet att skapa ett ledningssystem för informationssäkerhet. Systematiken innebär kontinuerliga uppföljningar med reviderade handlingsplaner enligt metodiken planera, genomföra, följa upp och åtgärda. För att säkerställa kvalitet och objektivitet sker intern och extern granskning enligt fastställd regelbundenhet.
- utifrån återkommande risk- och sårbarhetsanalyser och inträffade incidenter, vidta nödvändiga åtgärder för att se till att vår information har rätt skydd. Skyddsåtgärder ska vara kostnadseffektiva och stå i proportion till värdet av informationen och de negativa konsekvenser en otillräcklig säkerhet kan medföra.

- ställa säkerhetskrav inför upphandling, utveckling, användning och avveckling av informationstillgångar och uppföljning av ställda krav ska ske kontinuerligt.
- ska utgå från kontinuitetsplanering och ha beredskap för avbrott och störningar. Våra kritiska verksamheter ska kunna upprätthållas på fastställd nivå vid olika typer av incidenter.
- utgå ifrån att alla anställda och förtroendevalda vet vad det egna ansvaret omfattar och ha god kunskap om vilka säkerhetsregler som gäller. Detsamma gäller när tillfällig eller extern personal anlitas. Det är viktigt att alla anställda och förtroendevalda har ett högt säkerhetsmedvetande och kritiskt ifrågasätter händelser som kan påverka informationssäkerheten.
- säkerställa rätt identitet och behörighet utifrån roll, för alla som får tillgång till information. Det gäller vid nytt, ändrat eller avslutat behov.
- utgå ifrån att alla informationstillgångar är identifierade och dokumenterade. Hantering av personuppgifter ska följa särskilda riktlinjer. All information ska sparas, alternativt gallras, enligt gällande lagstiftning och finnas dokumenterat.

Verksamhetsdriven informationssäkerhet genom informationsklassning

Verksamheterna har ansvar för sin informationssäkerhet och har bäst kunskap om hur känslig och kritisk deras information är, och därmed kunskap om informationens skyddsvärde. En verksamhetsdriven informationssäkerhet innebär att verksamheterna, utifrån informationens skyddsvärde, ställer krav på de aktörer som hanterar informationen, exempelvis användare, systemansvariga samt drifts- och systemleverantörer.

För detta ändamål ska informationsklassning tillämpas, där information klassas med syftet att ge känslig och kritisk information ett starkare skydd än annan information. Därigenom kan en anpassad och effektiv informationssäkerhet skapas. Informationen ska systematiskt definieras och värderas.

Trosa kommun ska tillämpa en enhetlig modell för informationsklassning som anger olika nivåer av skyddskrav, vari information ska klassas baserat på interna och externa krav på informationens konfidentialitet, riktighet, tillgänglighet och spårbarhet.

Roller och ansvar

Grundprincipen är att ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret. Det gäller från koncernledning till den enskilde medarbetaren, och innebär att den som är ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten inom verksamhetsområdet.

Nedan beskrivs informationssäkerhetsansvaret för ett antal roller. Ansvar och tillhörande uppgifter för respektive roller beskrivs utförligare i riktlinjer och instruktioner inom informationssäkerhetsområdet.

Kommunfullmäktige fastställer den informationssäkerhetspolicy som ska gälla för kommunen.

Kommunstyrelsen ansvarar för samordningen av informationssäkerhetsarbetet i kommunen. Fastställer riktlinjer för informationssäkerhet som ska gälla för kommunen.

Varje nämnd och bolagsstyrelse ansvarar för informationssäkerheten inom sitt verksamhetsområde. Varje nämnd och bolagsstyrelse ska planlägga och löpande följa upp informationssäkerheten, och i övrigt vidta de åtgärder som krävs för att uppnå och upprätthålla en robust, säker och tillförlitlig informationshantering.

Kommunchef och Vd har kommunstyrelsens eller bolagsstyrelsens uppdrag att se till att informationssäkerhetsarbetet bedrivs så effektivt som möjligt i enlighet med denna policy och tillhörande riktlinjer och instruktioner. Kommunchefen ansvarar för att övergripande riktlinjer utarbetas och hålls aktuella i enlighet med policy. Vd ansvarar för att lokala riktlinjer och instruktioner vid behov utarbetas och hålls aktuella.

Verksamhetsansvariga, inom samtliga enheter, ansvarar för informationssäkerheten inom sin verksamhet. Varje verksamhetsansvarig ansvarar för att egna medarbetare har ett säkerhetsmedvetande och tillräcklig förståelse och kunskap för att en nödvändig informationssäkerhet i verksamheten kan uppnås.

Medarbetare och förtroendevalda har ett ansvar att följa kommunens informationssäkerhetspolicy, riktlinjer för informationssäkerhet och informationssäkerhetsinstruktioner. Man har som medarbetare och förtroendevald också ansvar att vara uppmärksam på brister och fel gällande informationshantering, utrustning och informationsinnehåll, och rapportera sådana enligt fastställda rutiner.

Systemägare (i regel produktionschef) är informationsansvarig för all data i, eller exporterat från, informationstillgången. I ansvaret ingår även att tillgången efterlever informationssäkerhetspolicy, riktlinjer för informationssäkerhet och informationssäkerhetsinstruktioner. En viktig del i ansvaret är att besluta om tillgångens informationssäkerhetsnivå genom att klassning sker enligt beslutad modell.

Systemägaren beslutar om nyanskaffning, vidareutveckling eller avveckling av IT-system inom ramen för resurstilldelningen för sin verksamhet. Systemägaren ska utse systemansvarig, samt säkerställa att avtal för personuppgiftsbiträde finns.

Systemansvarig är den eller de personer i berörda verksamheter eller hos annan part som har ansvaret för den dagliga användningen av det digitala verksamhetsstödet.

IT-säkerhetsledning Vid större oplanerade IT-relaterade händelser tillämpas kommunens beredskapsplan.

IT-beredningsgrupp leds av kommunchef och ska hantera och utreda generella frågor avseende anskaffning, drift, förvaltning och avveckling av informationshanteringsresurser. Inom ramen för detta ingår frågor som avser informationssäkerhet.

Informationssäkerhetssamordnare fungerar som stöd till kommunens verksamheter att fullfölja informationssäkerhetsansvaret.

IT-chefen är systemägare för kommunens tekniska IT-infrastruktur och ansvarar för att dess säkerhet är tillförlitlig och motsvarar interna (verksamhetens) och externa (legala) krav. Kommunens tekniska IT-infrastruktur ska även uppfylla de krav som denna informationssäkerhetspolicy och underliggande instruktioner för informationssäkerhet ställer. Bolag som inte nyttjar Trosa kommuns IT-miljö har själv detta ansvar.

IT-chefen ansvarar för att informationssäkerhetsinstruktioner utarbetas och hålls aktuella i enlighet med policy och riktlinje.

Systemadministratörerna innehar den tekniska kompetensen och ansvarar för att den dagliga driften upprätthålls enligt överenskommelse med systemägarna.