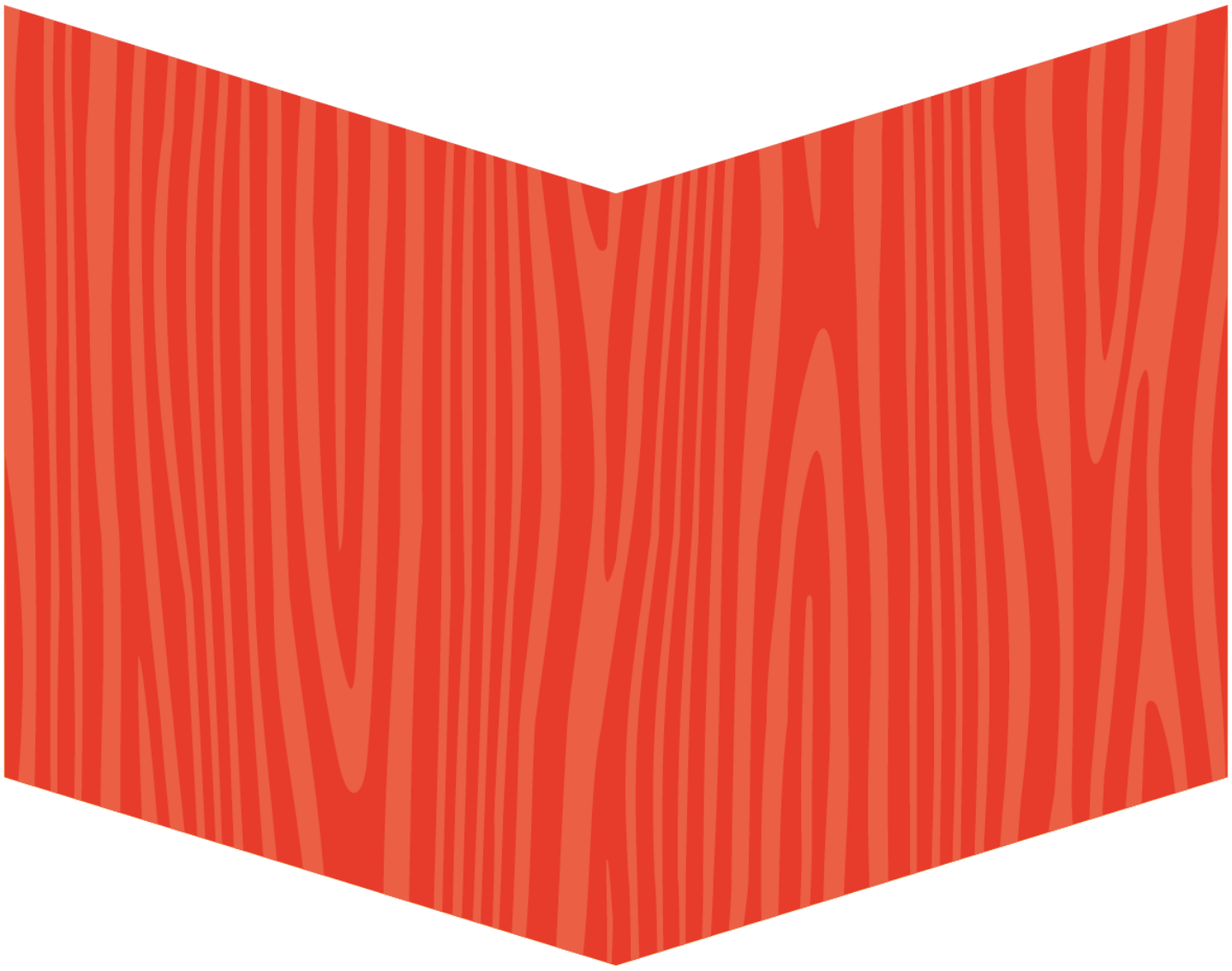
vingaker.se

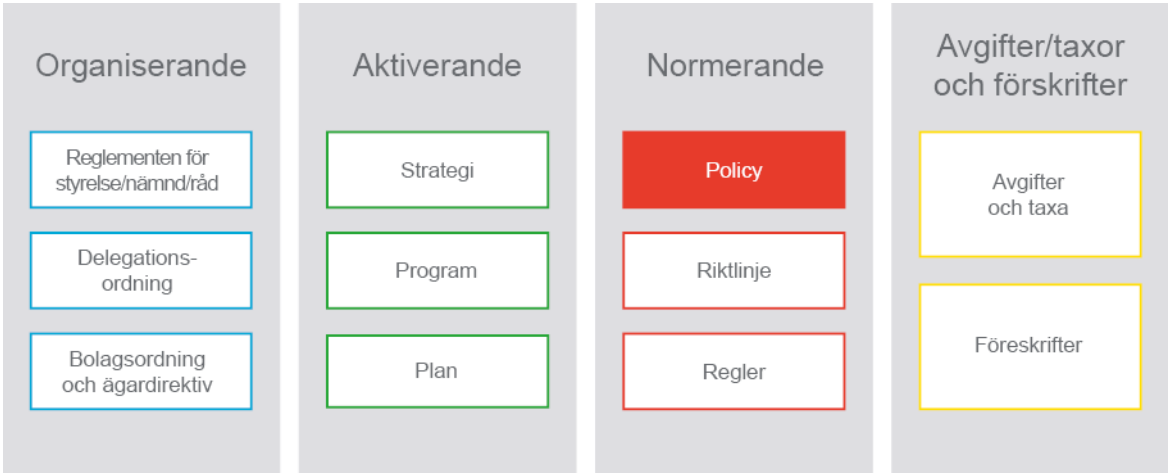
Vingåkers kommun

Informationssäkerhetspolicy för Vingåkers kommun

Kommunstyrelsen

Flik 7.14





Dokumenttyp	**Policy**
Dokumentnamn	**Informationssäkerhetspolicy för Vingåkers kommun**
Fastställd	2022-09-19
Beslutande	**Kommun**fullmäktige
Träder i kraft	2022-09-19
Giltighetstid	Tillsvidare
Processägare	**Säkerhetsskyddschef**
Senast reviderad	**2022-09-19 § 76**
Detta dokument gäller för	Vingåker kommun

Informationssäkerhetspolicy för Vingåkers kommun

Inledning

Information är en av kommunens viktigaste tillgångar och hanteringen av den är en viktig och naturlig del i alla verksamheters dagliga arbete, samt en förutsättning för exempelvis digitalisering och för att verksamheterna ska nå sina mål enligt 2 kap. 2 § säkerhetsskyddslagen (2018:585). Offentlighets- och sekretesslagen (2009:400) och GDPR.

Att information som kommunen hanterar i relationer med kommuninvånare, företag, myndigheter och organisationer såväl som inom vår egen organisation är korrekt, utgör en grund för tillit och förtroende. Det är även viktigt att information är tillgänglig när det behövs och att känslig information skyddas för att vi skall kunna fullgöra vårt uppdrag i samhället. Arbetet med informationssäkerhet ska vara långsiktigt och kontinuerligt, omfatta alla delar av kommunens verksamheter, bolag, förbund och alla de informationstillgångar som vi äger eller hanterar. Informationssäkerhetsarbete ska vara ett stöd för personal, samverkande partners och kommunens invånare.

Mål

Informationssäkerhetsarbetet ska förebygga att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs, och förebygga skadlig inverkan i övrigt på uppgifter och informationssystem som gäller säkerhetskänslig verksamhet. Det är viktigt att säkerhetsskyddarbetet bedrivs i samklang med det ordinarie verksamhetsarbetet.

Policyn beskriver de övergripande principer som skall gälla för Vingåkers kommun. Förankring och medvetande hos medarbetarna utgör själva grunden i säkerhetsarbetet. Samtliga anställda, politiker och extern personal omfattas av policyn.

Syfte

Säkerställa att verksamheten kan bedrivas effektivt utan störningar i enlighet med lagar, föreskrifter, regler och förordningar. Information ska hanteras på ett systematiskt och informationssäkert sätt enligt gällande riktlinjer för informationssäkerhet.

Ansvarsfördelning

Ansvaret för informationssäkerhet följer det ordinarie verksamhetsansvaret. Detta gäller från kommunledningen till den enskilde medarbetaren, och innebär att den som är ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten inom verksamhetsområdet. Kommunens säkerhetsskyddschef, IT-chef och övriga som arbetar med IT-säkerhet eller andra relaterade frågor fungerar som stöd till kommunens verksamheter att uppfylla informationssäkerhetsansvaret enlig 2 kap. 2 § säkerhetsskyddslagen (2018:585). 1 kap. 2 § andra stycket säkerhetsskyddslagen (2018:585) Säkerhetsskyddsklassificerade uppgifter.

Kommunfullmäktige uttrycker sin viljeinriktning rörande kommunens arbete med informationssäkerhet i denna policy.

Kommunstyrelsen ansvarar för att samordna och följa upp kommunens informationssäkerhetsarbete. Kommunstyrelsen har det övergripande ansvaret för att utarbeta, förvalta och följa upp riktlinjer för informationssäkerhet.

Nämnderna/styrelserna ansvarar för informationsägarskapet inom ramen för sina verksamheter. Informationsägaren har det yttersta ansvaret för sin information och avgör vilken information som får hanteras, hur den får hanteras och av vem den får hanteras.
Anställda, förtroendevalda och uppdragstagare ansvarar för att följa de informationssäkerhetsriktlinjer och instruktioner som finns samt att agera säkerhetsmedvetet.

Definition av information/informationstillgång

Information är allt som kommunen hanterar oavsett om det är i fysisk eller digital form.

- Tryckt och skrivet på papper
- Talad i samtal och telefon
- Lagrad i datorer, läsplattor, smartphones eller annan digital lagringsutrustning
- Intranät
- Film
- IT-system och passersystem
- Internet (sociala medier, webbtidningar, forum m.m.)
- Lagrat på skivor och USB
- Sänd och mottagen via nätet
- E-post
- Lagrad i databaser
- Medarbetares kunskap
- Dokumentarkiv
- Verksamhetssystem

Definition av informationssäkerhet

Informationssäkerhet är de åtgärder som vidtas för att förhindra att information läcker ut, förvanskas och att informationen ska vara tillgänglig för den som behöver den. Informationssäkerhetsområdet handlar om:

- **Tillgänglighet** – medarbetare kommer åt den information som deras uppdrag kräver
- **Riktighet** – information är korrekt, aktuell, komplett, begriplig och presenteras på rätt sätt. Information skall ej förändras varken av misstag eller avsiktligt.
- **Sekretess –** känslig information och program skall skyddas från obehöriga.
- **Spårbarhet –** möjlighet till att spåra vem som har gjort vad och när för att säkra drift och funktionalitet samt riktighet.

Informationssäkerhet är det samlade arbetet som görs för att skydda kommunens information. Det kan delas in i två olika delar, administrativ säkerhet och teknisk säkerhet. Administrativ säkerhet är till exempel riktlinjer, utbildning och revision. Teknisk säkerhet är till exempel det fysiska skyddet som skyddar en byggnad eller ett serverrum och IT säkerhet.

Genomförande och processägare

Informationssäkerhetsarbetet skall vara väl integrerat i ordinarie arbete med stor vikt på förebyggande genom utbildning och information. Incidenter skall rapporteras, hanteras och förebyggas i verksamheten i enlighet med gällande riktlinjer. För att vara effektivt och heltäckande skall arbetet genomföras väl strukturerat och med tydligt stöd från verksamhetsledningen. Informationssäkerhetsarbetet bygger på standarden SS/ISO/IEC 27001. För att kunna upprätthålla en god informationssäkerhet och förankra detta i organisationen skall det avsättas resurser för att systematiskt arbete genomförs enligt nedan.

Vad	*Vem*
Kommunens information **skyddas** på en lämplig **administrativ** och **teknisk** nivå, utifrån genomförda **informationssäkerhetsklassificeringar** och	Verksamhetschefer med informationssäkerhetsansvarig

riskanalyser, riskbedömning och konsekvensanalyser	
Framtagande och revidering av riktlinjer	Informationssäkerhetsansvarig med IT-chef
Informationssäkerhetshöjande åtgärder	Informationssäkerhetsansvarig och verksamheten
Utbildning och information kring riktlinjer och instruktioner	Chefer, medarbetare, förtroendevalda med stöd av informationssäkerhetsansvarig
Efterlevnad och uppföljning vid allvarliga incidenter, brister eller behov ska rapporteras	Chefer och Informationssäkerhetsansvarig
Revidering sker vid behov, dock minst en gång per mandatperiod.	Informationssäkerhetsansvarig

Inom varje avdelning skall man årligen upprätta en analys och plan för allt säkerhetsarbetet där informationssäkerheten är en del. Denna skall innehålla nulägesanalys samt planerade åtgärder för att höja informationssäkerhetsnivån och bör integreras i verksamhetsplaneringen och budgetarbetet. Den anställde skall underteckna en särskild ansvarsförbindelse. Informationssäkerheten ska regleras tydligt i alla avtal med leverantörer, uppdragsgivare eller samarbetspartners.

Informationssäkerhetsarbetet i kommunen ska bedrivas systematiskt, formaliserat och riskorienterat. Informationssäkerhet är en grundförutsättning för att uppnå kvalitet och effektivitet i verksamheten, samt en förutsättning vid upphandling, digitalisering och mobilitet. Informationssäkerheten ska vara en given del vid inköp och upphandling för att säkerställa efterlevnad av god informationssäkerhet utifrån Säkerhetsskyddslagen och GDPR.

Organisation och roller

Det finns en organisation med tydlig fördelning av ansvar för informationstillgångar och med relevanta roller för ledning och genomförande av ett systematiskt informationssäkerhetsarbete. Nedan beskrivs informationssäkerhetsansvaret för ett antal roller.

Kommunchefen har det övergripande ansvaret för informationssäkerheten och att det finns en tydlig ansvarsfördelning för att upprätthålla säkerheten. Informationsägare är den som bestämmer ändamålen för behandlingen och hanteringen av informationen. Förvaltningarna ansvarar för att ta fram riktlinjer och rutiner efter behov.

Säkerhetsskyddschef genomför säkerhetsanalyser i samarbete med verksamhetsansvarig. Informationssäkerhetsansvarig har det övergripande ansvaret för att leda, utveckla och samordna arbetet med informationssäkerhet i kommunen.

Dataskyddsombudets roll är att regelbundet utbilda, rådgöra och granska nämndernas informationssäkerhet, med särskilt fokus på att granska efterlevnaden av dataskyddsförordningen.

Informationsägaren alla medarbetare och förtroendevalda äger och ansvarar för att informationen är riktig och tillförlitlig samt för det sätt informationen sprids.

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

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.

Kontaktombud, inom varje nämnd ska det finnas ett utsett kontaktombud vilket har ansvaret att dokumentera sin nämnds behandlingar av personuppgifter i en registerförteckning

IT-chef har det operativa ansvaret för att uppfylla de krav som verksamheten ställer på den tekniska IT-infrastrukturen. IT-chefen har ett särskilt ansvar för den tekniska IT-säkerheten.