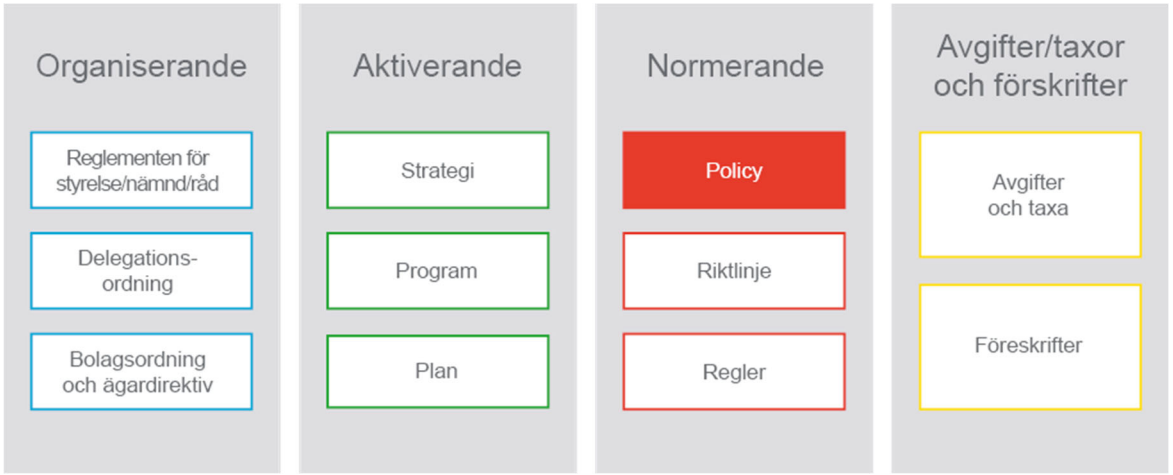
vingaker.se

Vingåkers kommun

Informationssäkerhetspolicy för Vingåkers kommun

Kommunstyrelsen

Flik 7.14



Dokumenttyp	Policy
Dokumentnamn	Informationssäkerhetspolicy för Vingåkers kommun
Fastställd	2022-09-19
Beslutande	Kommunfullmäktige
Giltighetstid	Tillsvidare
Processägare	Säkerhetsskyddschef
Senast reviderad	2023-11-27, Kf § 165
Detta dokument gäller för	Vingåker kommun

Innehållsförteckning

Innehållsförteckning ... 3
Informationssäkerhetspolicy för Vingåkers kommun ... 4
1. Inledning ... 4
2. Mål ... 4
3. Syfte ... 4
4. Ansvarsfördelning ... 4
5. Definition av information/informationstillgång ... 5
6. Definition av informationssäkerhet ... 5
7. Genomförande och processägare ... 6
8. Organisation ansvar och roller ... 7
9. Ledningssystem för informationssäkerhet (LIS) ... 8
10. Förvaltning, uppföljning och utvärdering ... 8
11. Informationsklassning ... 10
12. Kontinuitetshantering ... 10
13. Incidenthantering ... 10
14. Uppföljning och rapportering ... 11

Informationssäkerhetspolicy för Vingåkers kommun

1. 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. Informationssäkerhetsarbete ska bedrivas på ett systematiskt, strukturerat och riskbaserat sätt i enligt med säkerhetspolicyn samt ta sin utgångspunkt i gällande lagar, MSB:s föreskrifter samt aktuell version av den internationella ledningssystemstandarden för informationssäkerhet, SS-ISO/IEC 27001.

Att information som kommunen hanterar i relationer med kommuninvånare, företag, myndigheter och organisationer såväl som inom 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.

2. 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.

3. 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.

4. 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.

5. Definition av information/informationstillgång

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

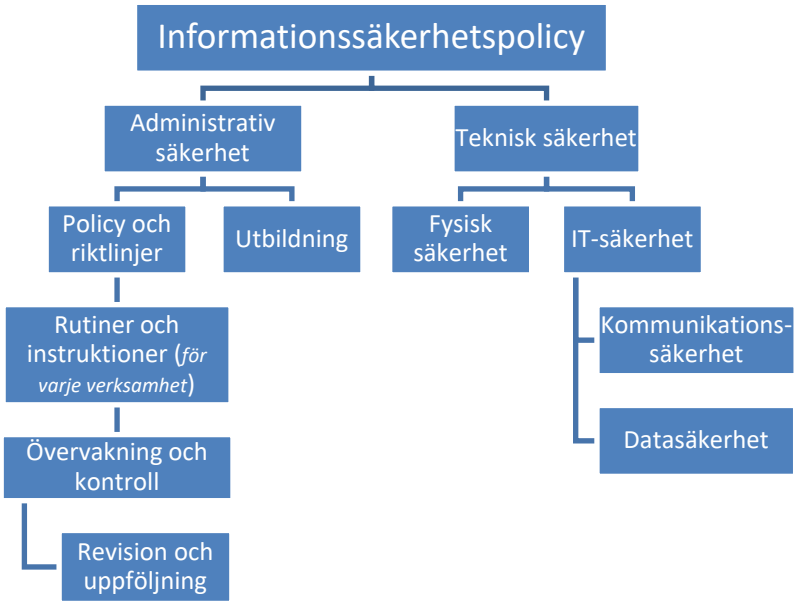
- Tryckt och skrivet på papper
- Talad i samtal och telefon
- Lagrad i datorer, läsplattor, smartphones eller annan digital lagringsutrustning
- Intranät
- Film
- IT-system och passersystem
- Internet (sociala medier, webbtidningar, forum m.m.)
- Lagrat på skivor och USB
- Sänd och mottagen via nätet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

6. 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.



7. 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 **riskanalyser, r**iskbedömning och konsekvensanalyser	Verksamhetschefer med informationssäkerhetsansvarig
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 säkerhetsarbete 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.

8. Organisation ansvar 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.

Kommundirektör 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

Informationssäkerhetsråd inom varje nämnd ska det finnas ett utsett kontaktombud vilket har ansvaret att dokumentera sin nämnds informationstillgångar 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.

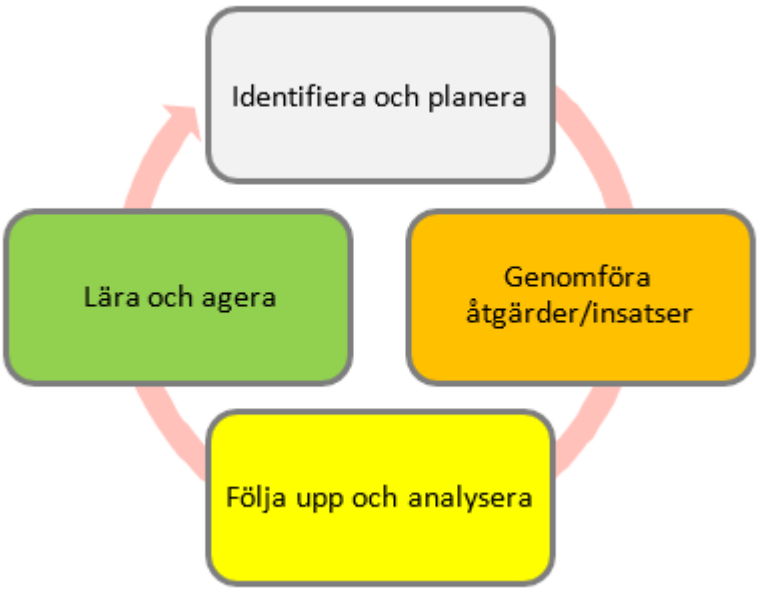
9. Ledningssystem för informationssäkerhet (LIS)

Ledningssystemet är ett verktyg för Vingåkers kommuns ledning att styra så att kommunens informationshantering sker med den säkerhet som ledningen bedömt lämplig utifrån verksamhetens behov och externa krav. Styrningen omfattar att planera, genomföra, kontrollera, följa upp, utvärdera och förbättra säkerheten i verksamhetens informationshantering. Ett LIS består av beslutade styrdokument med tillhörande rutiner, personella och tekniska resurser och aktiviteter för hantering av informationssäkerheten inom Vingåkers kommunorganisation och syftar till att skydda kommunens informationstillgångar. Vingåkers kommuns LIS dokumenteras i denna policy samt i riktlinjer, rutiner och instruktioner för chefer och medarbetare. Ledningssystemets dokumentation ska ses som en helhet och det ska finnas en spårbarhet mellan olika ingående dokument. Ledningssystemets viktigaste del är en säkerhetskultur som uppmuntrar medarbetarna att aktivt engagera sig i kommunens säkerhetsarbete. Därför är ledningens engagemang liksom medarbetarnas kunskap, medvetenhet och motivation viktiga faktorer i ledningssystem.

10. Förvaltning, uppföljning och utvärdering

För att Vingåkers kommun ska upprätthålla god informationssäkerhet använder vi oss av PDCA-modellen ("Plan-Do-Check-Act"), för att strukturera processer för LIS.

Verksamhetens informationssäkerhetskrav och förväntningar ska på ett effektivt sätt, omhändertas och ge utfall i säker informationshantering.



Process för informationssäkerhet. Processen består av fyra delprocesser a) identifiera och planera b) genomföra åtgärder/insatser c) följa upp och analysera d) lära, agera och förbättra.

Identifiera och Planera ("Plan"), Identifiera, etablera och hantera policy, mål, processer och styrande dokument som är relevanta för LIS.

- Informationssäkerhetspolicy för Vingåkers kommun ska uppfylla verksamheternas behov externa krav samt kort- och långsiktiga mål.
- All information och informationshantering ska vara kopplad till en ägare (informationsägare) med en tydlig ansvarsfördelning.
- Målbilden ska vara att kommuns informationssäkerhetsrisker identifieras, analyseras och hanteras i enlighet med de lagar och förordningar.

Genomföra (”Do”), driva och tillämpa säkerhetsåtgärder, processer och styrande dokument.

- Formulera och genomföra planer, aktiviteter, resurser, ansvar och prioriteringar för att hantera informationssäkerhetsrisker både på kort och lång sikt.

Följa upp (”Check”), granska och mäta processers effektivitet i förhållande till policy, mål och praktisk erfarenhet samt rapportera till ledningen för återkoppling och fastställande om fortsatt inriktning.

- Genomföra regelbundna granskningar av LIS effekt med hänsyn till efterlevnad, revisioner, incidenter, förslag och återkoppling ifrån verksamheten via Informationssäkerhetsråd.
- Granska informationsklassningar och riskanalyser regelbundet för att kontrollera kvarvarande risker med hänsyn till förändringar i verksamhet, skyddsteknik, hotbild och författningar/regelverk.
- Regelbundet genomföra genomgång av LIS för ledningen för att säkerställa korrekt omfattning och att lämpliga förbättringar av LIS identifieras.

Förbättra (”Act”), vidta förbättrande åtgärder, baserade på resultaten av uppföljning av LIS för att ständigt förbättra LIS.

- Genomföra identifierade förbättringsåtgärder av LIS.
- Säkerställa att LIS har följsamhet gentemot författningsändringar, externa krav och erfarenheter ifrån andra organisationer.

11. Informationsklassning

Informationsklassning ska vara en central aktivitet i informationssäkerhetsarbetet och har till syfte att bedöma informationens värde för kommunens verksamheter. Bedömning sker både utifrån den egna verksamhetens behov och utifrån externa krav. Avsikten är att varje informationstillgång ska omges med rätt skydd. Informationsklassningen är en process som innebär en kravställning på säkerhetsåtgärder från verksamheten till interna och externa leverantörer av tjänster samt IT (drift och förvaltning) och av resurser som lokaler och annan utrustning som påverkar informationshanteringen. Klassningen innebär även krav på användare av informationstillgångar. Informationsklassning ska ses som en form av riskanalys som gäller specifika informationstillgångar.

För att klassningen ska medföra en säkerhetshöjande effekt krävs att det finns systematiserade skyddsåtgärder som hanterar alla risker.

12. Kontinuitetshantering

Kontinuitetshantering avser förmågan att reducera negativa effekter i verksamheten orsakade av olika former av störningar i tillgång till information. Kontinuitetshanteringen ur informationssäkerhetsperspektivet ska riktas mot att reducera avbrott och allvarliga störningar som påverkar informationshanteringen och därmed skapar störningar i verksamheten oavsett var de uppstår. Incidenten kan ha sitt ursprung i exempelvis en brand eller ett inbrott men få påverkan på informationshanteringen. Störningarna kan vara av olika karaktär, allt från mindre störningar till katastroftillstånd. Avsikten är att verksamhetsprocesserna så snabbt som möjligt efter en störning kan återgå till normalläge och att minimera risken för informationsförluster under störningen. För att uppnå detta måste kontinuitetshanteringen, ur informationssäkerhetssynpunkt, integreras med verksamhetens ordinarie risk- och sårbarhetsarbete. Kontinuitetshanteringen ur informationssäkerhetssynpunkt innehåller dels den kontinuitetshanteringen som verksamheten har ansvar för, dels den avbrottsplanering som IT-enheten och andra teknikresursägare ska ha för att kunna leverera stöd till verksamheten. Kontinuitetshantering ska finnas för varje verksamhet samt för stödfunktioner, t.ex. IT-enhetens plan ska utformas efter de krav som verksamheten formulerar. Planerna ska finnas tillgängliga för behöriga medarbetare och förvaras och hanteras utifrån kravställning enligt genomförd informationsklassning.

13. Incidenthantering

En väl fungerande hantering av säkerhetsincidenter är en mycket viktig del av både det reaktiva och proaktiva säkerhetsarbetet. Det ger dels möjlighet att snabbt och effektivt agera på uppkomna hot och händelser, dels möjlighet att i efterhand vidta förebyggande åtgärder för att motverka att liknande

incidenter inträffar på nytt. En grundläggande förutsättning för att detta ska fungera är att samtliga anställda och förtroendevalda har kunskap om vad som definieras som en incident, samt var och hur dessa ska anmälas internt inom organisationen.

14. Uppföljning och rapportering

I Enligt SS-ISO/IEC 27001 och MSB:s föreskrifter om informationssäkerhet kommunen ska följa upp informationssäkerhetsarbetet genom att rapportera avvikelser, åtgärda informationssäkerhetsbrister och i förekommande fall rapportera incidenter till berörda myndigheter. Informationssäkerhetspolicy för Vingåkers kommun följs upp och revideras en gång per mandatperiod.

Informationssäkerhetsansvarig ska en gång per år rapportera läge och status gällande informationssäkerhet till kommunledningen och kommunstyrelsen. Särskilda skäl, som exempelvis allvarliga incidenter, brister eller behov, kan motivera ytterligare rapporteringar. Efterlevnaden av informationssäkerhetsarbetet ska följas upp kontinuerligt inom informationssäkerhetsråd. Förbättringsarbetet ska genomföras genom kontinuerlig återrapportering till kommunledningen.