Kungsbacka

# Informationssäkerhet

## Riktlinjer perioden 2023-2026

| | |
|---|---|
| **Dokumentegenskaper:** | Titel: Informationssäkerhet |
| **Beslutad av:** | Kommunfullmäktige 7 maj 2024 § 80, redaktionella ändringar 2025-01-03, KS 2023-00670 |
| **Gäller från:** | 2024-05-07 |
| **Ansvarig förvaltning:** | Kommunstyrelsens förvaltning |
| **Kontakt:** | Kungsbacka direkt 0300-83 40 00 \| info@kungsbacka.se<br>Kungsbacka kommun, 434 81 Kungsbacka<br>www.kungsbacka.se |

Inledning

Information och hur den hanteras spelar en avgörande roll för att Kungsbacka kommun ska kunna leverera säker och effektiv service inom en rad olika verksamhetsområden. Informationssäkerhet handlar om att skapa och upprätthålla lämpligt skydd för den information som hanteras. Detta gäller information i alla dess former, såsom text, ljud, bild och film. Det gäller oavsett hur informationen lagras, bearbetas och kommuniceras.

## Mål och inriktning

Kommunens informationssäkerhetsarbete ska stödja arbetet med att Kungsbacka kommun ska vara en trygg och säker kommun samt säkerställa en säker, effektiv och hållbar digitalisering, med särskilt fokus på medborgarnas rättigheter och personliga integritet.

Kommunen ska säkerställa att samtliga informationstillgångar:

- skyddas för obehörig insyn och manipulation (konfidentialitet)
- är tillförlitliga, korrekta och fullständiga (riktighet)
- är nåbara vid rätt tillfälle (tillgänglighet)

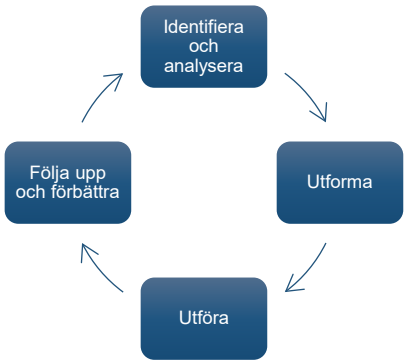
## God informationssäkerhetskultur

Kommunens informationssäkerhetskultur ska vara en naturlig del av verksamheten och kännetecknas av en engagerad ledning och engagerade chefer på alla nivåer. Ledningen ska hålla sig informerade om informationssäkerhetsarbetet, fatta beslut om inriktningen på arbetet och uppmuntra till en lärande kultur med förtroende till sina medarbetare. Medarbetarna ska uppmuntras att påtala brister och rapportera incidenter samt få rätt förutsättningar för att arbeta på ett informationssäkert sätt.

## Systematiskt informationssäkerhetsarbete

För att uppnå de övergripande informationssäkerhetsmålen ska Kungsbacka kommun bedriva ett systematiskt informationssäkerhetsarbete baserat på den internationella säkerhetsstandardserien SS-ISO/IEC 27000. Som stöd i arbetet ska Myndigheten för samhällsskydd och beredskaps (MSB:s) metodstöd för informationssäkerhet användas.

Arbetet ska bedrivas genom att upprätta, införa, driva, underhålla och ständigt förbättra organisationens informationssäkerhet i en kontinuerlig process.




## Identifiera och analysera tillgångar, krav och risker

Varje förvaltning ska arbeta systematiskt med behovsanalyser för att säkerställa att informationssäkerheten i verksamheten utformas med utgångspunkt i ett tydligt definierat nuläge. Utifrån resultatet av dessa analyser ska det fortsatta informationssäkerhetsarbetet utformas.

## Utforma informationssäkerhetsarbetet

Det samlade resultatet från behovsanalyserna ska styra hur varje förvaltning utformar säkerhetsåtgärder och prioriteringar för sitt informationssäkerhetsarbete. En tydlig organisation för informationssäkerhet, inklusive roller, ansvar och arbetsuppgifter ska skapas.

## Utföra informationssäkerhetsarbetet

Resultatet av informationssäkerhetsarbetet och konstaterade behov av säkerhetsåtgärder ska tas om hand av varje förvaltning på ett riskbaserat sätt för att prioritera och säkerställa ett systematiskt arbetssätt för informationssäkerhetsarbetet.

## Följa upp och förbättra

Varje förvaltning ska på årlig basis följa upp resultatet av föregående års informationssäkerhetsarbete inför nästkommande år. Detta görs genom ledningens genomgång och årsrapport.

Förvaltningsledningen ska minst en gång om året ta del av status på förvaltningens systematiska informationssäkerhetsarbete vid ledningens genomgång. Förvaltningsledningen fattar sedan beslut om prioriteringar och insatser inför nästkommande år.

Varje nämnd ska en gång om året ta del av årsberättelse i informationssäkerhet.

# Ansvarsfördelning för systematiskt informationssäkerhetsarbete

## Varje nämnd är informationsägare

Varje nämnd är informationsägare och har det yttersta ansvaret för förvaltningens information, oavsett var den hanteras. Varje nämnd ansvarar därför för att ett systematiskt informationssäkerhetsarbete bedrivs på förvaltningen i enlighet med denna riktlinje.

## Kommunstyrelsen

Kommunstyrelsens förvaltning följer upp kommunens systematiska informationssäkerhetsarbete. Det inbegriper bland annat att ta fram och samordna övergripande information, rutiner och dokumentmallar. Kommunstyrelsens förvaltning sammankallar också kommunens nätverk för informationssäkerhetssamordnare, samt granskar det systematiska informationssäkerhetsarbetet i hela kommunen.

## Förvaltningscheferna

Förvaltningscheferna ansvarar för resurstilldelningen och uppföljningen av det förvaltningsspecifika informationssäkerhetsarbetet.

## Informationssäkerhetssamordnare

Varje förvaltning ska utse en informationssäkerhetssamordnare. Denna har till uppdrag att samordna förvaltningens systematiska informationssäkerhetsarbete.

## Kommunövergripande nätverk

Det kommunövergripande informationssäkerhetsnätverk för informationssäkerhetssamordnare ska stödja förvaltningarna i det systematiska informationssäkerhetsarbetet.

## Prioriterade områden

Samtliga områden som listas nedan ingår i det systematiska informationssäkerhetsarbetet och är särskilt prioriterade utifrån dess centrala roll i arbetet.

## Informationsklassificering

Grunden i allt systematiskt och riskbaserat informationssäkerhetsarbete är klassificering av information. Det ger oss kännedom om hur känsliga de olika informationsmängderna vi hanterar är, och vi kan utifrån det skapa rätt skydd för informationen. Resurser som används för att hantera informationen, till exempel programvaror, system, tjänster och fysiska tillgångar ska utformas och anpassas till de krav som klassificeringen i förlängningen ställer på dessa.

Varje förvaltning ska klassificera den information som hanteras inom den egna verksamheten enligt kommunens *Rutin för informationsklassificering*. För information som hanteras i digitala tjänster ska Kungsbacka kommuns *Modell för digitala tjänster och system* efterlevas.

## Information och utbildning

Alla anställda ska få rätt förutsättningar för att bidra till en god informationssäkerhetskultur i Kungsbacka kommun. De anställda ska ha den kunskap som krävs för att förstå sitt ansvar för informationssäkerhet, vara medvetna om hot och problem som rör informationssäkerhet samt känna till och följa kommunens regelverk för informationssäkerhet när de utför sitt arbete.

Kommunstyrelsen ansvarar för att det i Kungsbacka kommun finns en kommungemensam plan för informations- och utbildningsinsatser i informationssäkerhet.

Varje förvaltning ska införa informations- och utbildningsinsatser kopplat till förvaltningsspecifika processer och informationshantering.

## Incidenthantering och rapportering

Informationssäkerhetsrelaterade incidenter är oönskade händelser som kan leda till brister i konfidentialitet, riktighet eller tillgänglighet hos informationen vi hanterar i kommunen. Samtliga medarbetare behöver ha kunskap om vad som definieras som en incident, samt var och hur dessa ska anmälas internt inom organisationen, för att kunna arbeta förebyggande och för att effektivt agera på hot.

Kommunstyrelsen ansvarar för att det i Kungsbacka kommun finns en kommungemensam modell för rapportering av informationssäkerhetsincidenter och avvikelser.

Varje förvaltning ska hantera, följa upp och förbättra sitt informationssäkerhetsarbete utifrån rapporterade informationssäkerhetsincidenter och avvikelser inom den egna verksamheten.

## Anskaffning, utveckling och underhåll av externa IT-resurser

Varje förvaltning ska inför anskaffning av förvaltningsspecifika externa IT-resurser:

- klassa informationen som ska hanteras i tjänsten och analysera informationssäkerhetsrisker för det som ska anskaffas
- ställa krav på den kontrakterade parten utifrån informationsklassningen och riskanalysens resultat
- följa upp att de ställda kraven är ändamålsenliga och tillräckliga
- följa upp om den kontrakterade parten har infört de säkerhetsåtgärder som avtalats och att dessa följer med under hela avtalsperioden
- införa säkerhetsåtgärder som den egna organisationen ska utföra utifrån informationsklassningen

Vid anskaffning av kommunövergripande IT-resurser ansvarar Kommunstyrelsens förvaltning för ovan angivna krav.

## Kontinuitetshantering för IT-resurser

Kontinuitetshantering handlar om att planera för att upprätthålla verksamheten på en tolerabel nivå oavsett vilken störning den utsätts för och att så snabbt som möjligt kunna återgå till normalläge efter en störning. I de allra flesta av våra verksamhetsprocesser är vi idag starkt beroende av IT-resurser. Det är därför av största vikt att identifiera kritiska IT-resurser och deras beroenden och att skapa, öva, underhålla och informera berörda om kontinuitetsplaner för dessa.

## Kontinuitetshantering tillsammans med stödfunktioner

IT-resurser som förvaltningarna använder har en eller flera stödfunktioner eller leverantörer. Stödfunktionen består antingen av kommunens IT-enhet Digitalt center eller av en extern leverantör. Kontinuitetshanteringen innebär dels den hantering som varje förvaltning ansvarar för, dels den avbrottsplanering som förvaltningarnas stödfunktioner ska ha för att kunna leverera stöd till förvaltningen. Förvaltningarna ska arbeta tillsammans med sina stödfunktioner för att tydliggöra ansvarsfördelning och arbetsuppgifter vid en eventuell IT-relaterad störning.

Kommunstyrelsens förvaltning ansvarar för att det i Kungsbacka kommun finns en kommungemensam modell för kontinuitetshantering för IT-resurser.

Varje förvaltning ska identifiera de IT-resurser som stödjer samhällskritiska och verksamhetskritiska processer och skapa, öva och underhålla kontinuitetsplaner för dessa resurser. Varje förvaltning ska också göra kontinuitetsplanerna kända inom den egna verksamheten så att rätt personer kan komma åt informationen vid händelse av störning. I arbetet ska Digitalt center och externa leverantörer inkluderas.

## Efterlevnad och uppföljning

Kungsbacka kommuns informationssäkerhetsarbete ska följas upp systematiskt och regelbundet. Under mandatperioden ska särskilt fokus ligga på uppföljning av hantering av informationsmängder med höga skyddskrav samt uppföljning av implementeringen av den här riktlinjen och tillhörande stöddokument på kommungemensam och förvaltningsspecifik nivå.

Kommunstyrelsen ansvarar för att genomföra granskningarna och resultatet rapporteras till den kommungemensamma ledningsgruppen (KLG) samt varje nämnds förvaltningsledning.