Österåker

Österåkers kommuns styrdokument
Datum för antagande: 2026-04-27 § 2:11
Diarienummer: KS 2025/0223
Antagen av: Kommunfullmäktige
Dokumentansvarig: Avdelningen för säkerhet, trygghet och civilt försvar

Informationssäkerhetspolicy för Österåkers kommun

Infoga en bild genom att välja **Bild på startsida**
på fliken **Österåkers kommun**

POLICY • PROGRAM • STRATEGI • HANDLINGSPLAN • RIKTLINJE

Österåker

Innehåll

Syfte ..... **Fel! Bokmärket är inte definierat.**
Vilka som berörs 3
Policyns innehåll 3
Definition informationssäkerhet 3
Mål för informationssäkerhet 4
Åtaganden 4
Principer för informationssäkerhetsarbetet 4
Ansvar och roller 5
Revidering 6

Österåker

Syfte med policyn

I enlighet med Cybersäkerhetslagen 2025:1506 är kommunen skyldig att vidta lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att skydda nätverks- och informationssystem.

Syftet med policyn är att tydliggöra Österåker kommuns övergripande och långsiktiga ansvar och principer för att säkra kommunens informationstillgångar samt leva upp till aktuell lagstiftning inom området.

Vilka som berörs

Informationssäkerhetspolicyn för Österåkers kommun är ett kommunövergripande styrdokument som riktar sig till förtroendevalda och medarbetare som hanterar kommunens informationstillgångar.

Policyns innehåll

Innehållet i policyn utgår från ISO 27000:2. Policyn innehåller kommunens definition av informationssäkerhet, informationssäkerhetsmål, ansvar och roller samt de principer som styr all verksamhet som rör informationssäkerhet.

Vidare redogör policyn för kommunens åtaganden om att uppfylla tillämpliga krav på informationssäkerhet och om att ständigt förbättra kommunens ledningssystem för informationssäkerhet.

Definition informationssäkerhet

Informationssäkerhet säkerställer informationens konfidentialitet, tillgänglighet och riktighet. Informationssäkerhet inbegriper tillämpning och hantering av lämpliga säkerhetsåtgärder som tar ett brett spektrum av hot i beaktande, i syfte att säkerställa organisationens verksamhet och dess kontinuitet samt minimera konsekvenserna av informationssäkerhetsincidenter.

Med andra ord handlar informationssäkerhet om att förhindra att information läcker, förvanskas eller förstörs. Det handlar också om att göra information lättillgänglig när den behövs och för rätt person. Begreppet omfattar information tryckt på papper, lagrad elektroniskt, som överförs per mejl eller post, visas på film eller yttras i en konversation.

Österåker

Syfte och mål för informationssäkerhet

Österåkers kommuns syfte med informationssäkerhet är att informationstillgångar skyddas på en lämplig nivå.

Österåkers kommuns strategiska mål är att kommunen har ett systematiskt informationssäkerhetsarbete. Målen för informationssäkerhet finns i *Handlingsplan för informationssäkerhet,* följs upp årligen av kommunstyrelsen och uppdateras vid behov av informationssäkerhetsansvarig.

Målen ska baseras på tillämpliga informationssäkerhetskrav och resultat av genomförda riskanalyser.

Åtaganden

Österåkers kommun åtar sig att:

- uppfylla tillämpliga lag- och myndighetskrav på informationssäkerhet.
- ständigt förbättra ledningssystemet för informationssäkerhet.

Principer för informationssäkerhetsarbetet

Informationssäkerhetsarbetet i Österåkers kommun ska bedrivas systematiskt och bygga på den etablerade standardserien SS-ISO/IEC 27000.

Informationssäkerhetsarbetet ska säkerställa att kommunens, medarbetarnas och invånarnas information skyddas. Skyddet av information ska utgå ifrån informationstillgångens skyddsvärde oavsett om den hanteras manuellt eller digitalt.

Varje verksamhetsområde ansvarar för att följa lag, policy och riktlinjer gällande informationssäkerhet. Alla chefer, medarbetare och förtroendevalda ansvarar för att denna policy och relevanta riktlinjer följs då de hanterar kommunens informationstillgångar.

Informationssäkerhetsarbetet ska följas upp, utvärderas och förbättras för att säkerställa att fastställda krav, rutiner och skyddsåtgärder efterlevs och fortsätter vara ändamålsenliga.

Det systematiska informationssäkerhetsarbetet ska bidra till att Österåkers kommun upprätthåller en nivå av informationssäkerhet som:

- grundar sig i ett riskbaserat arbetssätt.
- innebär en säker och lagenlig informationshantering.
- möjliggör digitaliseringssatsningar och underlättar transformering.

- möjliggör hantering av avvikelser och undantag på ett strukturerat och ordnat sätt.
- har en tillräcklig kompetensnivå.
- har en positiv effekt på kvalitet och effektivitetsmål.
- genomsyras av en god säkerhetskultur och uppmuntrar till engagemang hos samtliga medarbetare och, förutom att följa gemensamma regler, motiverar dem att delta i att ständigt förbättra informationssäkerheten.
- gör att invånare, samarbetspartners och företagare har högt förtroende för kommunens informationshantering.

Ansvar och roller

Kommunfullmäktige beslutar om och har ägandeskapet för informationssäkerhetspolicyn.

Kommunstyrelsen har det yttersta ansvaret för kommunens informationssäkerhet och ansvarar för att leda, samordna och följa upp kommunens informationssäkerhetsarbete.

Nämnderna har det yttersta ansvaret för informationssäkerheten inom respektive verksamhetsområde.

Kommundirektör säkerställer uppföljning av informationssäkerhetsarbetet och att det finns ekonomiska och personella resurser med rätt kompetens för informationssäkerhetsarbetet.

Informationssäkerhetsansvariga ansvar för det operativa arbetet att leda och samordna informationssäkerhetsarbetet i kommunen samt att stödja ledningen och alla övriga roller som har ett informationssäkerhetsansvar.

Informationssäkerhetssamordnare på förvaltningsnivå samordnar informationssäkerhetsarbetet på sin förvaltning, säkerställer att förvaltningens arbete är i linje med kommunens övergripande riktlinjer och policy. Informationssäkerhetssamordnare på förvaltningsnivå fungerar som kontaktperson för kommunens centrala informationssäkerhetsansvariga.

Informationsägare ansvarar för information inom sin verksamhet, att riskbedömning och informationssäkerhetsklassificering genomförs och förmedlar detta till systemägare eller upphandling i ett tidigt skede. Informationsägare tillser även att lämpliga skyddsåtgärder implementeras.

Systemägare säkerställer att system uppfyller verksamhetens krav på informationssäkerhet samt genomför informationssäkerhetsklassificering och deltar i riskbedömningar och incidenthanteringar.

IT-säkerhetsansvarig samordnar arbete med säkerheten i kommunens IT-miljö. IT-säkerhetsansvarig har tillsynsansvar att IT-miljön är tillförlitlig och motsvarar interna och externa krav.

Varje enskild medarbetare som hanterar informationstillgångar har ett ansvar för att informationssäkerheten upprätthålls genom att följa kommunens övergripande policy och riktlinjer samt tar del av information och utbildningar.

Revidering

Ändringar av informationssäkerhetspolicyn ska göras i de fall en tillsyn eller revision påvisar brister i kommunens informationssäkerhetsarbete. För bibehållen enhetlighet bör översyn och uppdatering av andra relaterade dokument beaktas när en policy, styrdokument eller riktlinje ändras. En ändring av informationssäkerhetspolicyn ska beslutas av kommunfullmäktige.

Om inte annat angetts ska denna policy aktualitetsprövas minst varje mandatperiod, gärna i början av mandatperioden.