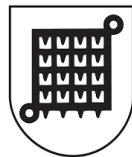




Strategi Program Plan Policy Riktlinjer **Regler**

INFORMATIONSSÄKERHET



Beslutad av: Kommunstyrelsen

Datum för beslut: 15 april 2026 § 67

Giltighetstid: Tills vidare

Berörda verksamheter: Åmåls kommun

Dokumentansvarig: Kommundirektör

Innehållsförteckning

Syfte	3
Ansvar	3
Informationssäkerhetsmål	3
Systematik	4
Analys.....	4
Informationsklassificering	4
Incidenthantering.....	4
Säkerhetsåtgärder	5
Utbildning och medvetenhet	5
Hantering av information i kommunens informationshanteringssystem	6
Artificiell intelligens (AI).....	6
Samarbete med externa parter	6
Uppföljning och revision.....	6
Efterlevnad av lagstiftning	6
Dokumentation och rapportering.....	7

Syfte

Syftet med dessa regler är att säkerställa en hög nivå av informationssäkerhet. Reglerna omfattar också de kommunala bolagen. Detta ska bidra till att skydda kommunens och invånarnas information mot obehörig åtkomst, förlust eller skada, samtidigt som vi säkerställer att verksamheten kan fortsätta utan störningar.

Ansvar

- **Kommunfullmäktige:** Har det övergripande ansvaret för informationssäkerheten inom kommunen och dess helägda bolag
- **Kommunstyrelsen:** Ansvarar för uppföljning och fastställer riktlinjer samt tar emot och granskar rapporter från organisationen
- **Nämnd:** Respektive nämnd ansvarar för att säkerställa att deras verksamheter arbetar i enlighet med rådande styrdokument
- **Informationssäkerhetsorganisation:** Varje kommun ansvarar för att ha en organisation kring informationssäkerhet.
- **Medarbetare:** Ansvarar för att följa kommunens riktlinjer för informationssäkerhet och rapportera säkerhetsincidenter. Genomgår utbildningar enligt utbildningsplan och sträva efter en god informationshanteringshygien. Tillse att leverantörer som hanterar kommunens information lever upp till de riktlinjer och informationssäkerhetsnivåer som gäller inom kommunen

Informationssäkerhetsmål

Kommunens informationssäkerhetsmål är att säkerställa **konfidentialitet**¹, **riktighet**² och **tillgänglighet**³ för all information som hanteras av kommunen och de kommunala bolagen genom att:

- Alla verksamheter ska vara medvetna om vilken typ av information man hanterar och hur man ska klassificera den
- Alla medarbetare ska vara utbildade inom informationssäkerhet
- Alla verksamheter ska ha uppdaterade verksamhets-, omvärlds- och riskanalyser
- Alla verksamheter ska veta vilka typer av incidenter som ska rapporteras och hur man gör detta
- Alla verksamheter arbetar aktivt med frågor som rör informationssäkerhet där det är en naturlig del av det dagliga arbetet
- En informationssäkerhetsorganisation ska finnas
- Varje år öva informationssäkerhet på ledningsnivå med stöd av informationssäkerhetsorganisationen

¹ Informationen är tillgänglig endast för de personer som har behörighet ta del av den.

² Informationen är korrekt och har inte blivit ändrade eller manipulerad.

³ Informationen är tillgänglig när den behövs och för rätt person.

Systematik

För att genomföra informationssäkerhetsarbetet systematiskt ska kommunens chefer arbeta med analys, informationsklassificering och incidenthantering.

Analys

Chefer inom alla verksamheter ansvarar för att ta fram nedanstående analyser. Arbetet kan ske med stöd av medarbetare och den lokala informationssäkerhetsorganisationen. Analyserna ska årligen ses över och vid behov revideras.

- **Verksamhetsanalys**⁴
- **Risikanalys**⁵
- **Gapanalys**⁶

Informationsklassificering

All information inom kommunen och de kommunala bolagen ska klassificeras utifrån dess känslighet och betydelse för verksamheten där man ska utgå från KLASSA⁷. En bra grund är att tänka:

- **Offentlig information**⁸
- **Kommunintern information**⁹
- **Konfidentiell och/eller sekretessbelagd information**¹⁰

Indelning sker enligt följande konsekvensnivåer om incident uppstår:

- **Allvarlig** - Kraftig/avgörande/mycket allvarlig effekt
- **Betydande** - Påtaglig/betydande/begränsade negativa effekter
- **Måttlig** - Viss/måttlig påverkan och effekter
- **Försumbar** - Inte märkbart/ingen negativ effekt

Incidenthantering

- **Incidenthanteringsplan:** En incidenthanteringsplan ska finnas i varje verksamhet. Vid händelse av incident så ska verksamheterna följa den plan som satts upp för hantering och rapportering av informationssäkerhetsincidenter. Rapportering måste alltid ske skyndsamt både internt och till externa tillsynsmyndigheter.

⁴ En analys där verksamheten går igenom vilken typ av information man hanterar och hur man hanterar denna information.

⁵ En analys där verksamheten ser över vad som händer om informationen inte är konfidentiell, riktig eller tillgänglig.

⁶ En analys där verksamheten får fram ett nuläge och ett önskat läge, detta blir i sin tur en att göra lista.

⁷ KLASSA är en metod som hjälper verksamheten att välja rätt åtgärder för att skydda information. Det är Sveriges kommuner och regioner (SKR) som tagit fram KLASSA.

⁸ Information som är öppen och inte innehåller uppgifter av känslig karaktär eller som är belagd med sekretess

⁹ Information som enbart ska hanteras internt, exempelvis arbetsdokument som inte är fastställda

¹⁰ Information som bedöms innehålla känslig information, exempelvis personuppgifter, kontinuitetsplaner och dokument om krishantering

Säkerhetsåtgärder

IT- och digitaliseringsenheten har ett ansvar att stödja verksamheterna med att skydda den digitala informationen och säkerhetsorganisationen ansvarar för att stödja med det fysiska skyddet som krävs för att skydda kommunens lokaler och den information kommunerna har i fysisk form. När verksamheter genomför eller reviderar sina analyser så ska man med stöd av informationssäkerhetsorganisationen uppmärksamma IT och/eller säkerhetsorganisationen om man hittar brister eller om man har information som behöver utökat skydd.

- **Tekniska åtgärder:** Brandväggar, antivirusprogram, kryptering och säker autentisering ska användas för att skydda information och system.
- **Fysiska åtgärder:** Säkerställ att servrar och andra IT-utrustningar är skyddade mot obehörig åtkomst genom lås och kontrollerad åtkomst. Även fysiska dokument och information ska skyddas med lås och kontrollerad åtkomst.
- **Processer och rutiner:** Rutiner kring säkerhetsincidenter, säkerhetskopiering och återställning av information ska alltid följas
- **Behörighetsstyrning:** Aktivt arbeta med att styra behörigheter till information både i IT-system och fysisk behörighet i form av nycklar, tagg och larmbehörigheter. Man ska enbart ha tillgång till den information som krävs för att kunna utföra sitt arbete.

Vid behov av nya tekniska lösningar eller system ska verksamheter inom kommunerna alltid föra dialog med IT- och digitaliseringsenheten innan upphandling sker. Detta för att kommunen ska ha kontroll på sin systemflora men även för att kunna säkerställa kompatibiliteten och säkerheten gentemot redan existerande system.

Utbildning och medvetenhet

Alla medarbetare ska genomgå utbildning i informationssäkerhet. Utbildningen ska bland annat omfatta:

- Identifiering och hantering av säkerhetsincidenter
- Säker hantering av personuppgifter och annan klassad information
- Användning av säkra lösenord och autentisering
- IT- och cyberhygien

Utbildningar för informations- och cybersäkerhet finns tillgängliga via kommunens intranät. Närmaste chef ansvarar för att upprätta en utbildningsplan för varje anställd, närmaste chef ansvarar även för att säkerställa att medarbetare genomför föreskrivna utbildningar enligt gällande utbildningsplan.

Hantering av information i kommunens informationshanteringssystem

Kommunen har idag en stor mängd olika typer av system som hanterar olika typer av information med olika typer av klassning. Alla medarbetare är ansvariga att klassa information som man har genererat på sin arbetsplats. De ska också veta vilka system som informationen får hanteras i.

Bedöms informationen ha högre klassning än vad systemet kan hantera eller om verksamheten behöver stöd i frågan ska lokal informationssäkerhetsorganisation kontaktas. IT- och digitaliseringsenheten stödjer med att eventuellt rensa bort den information som finns lagrad på serverna.

Artificiell intelligens (AI)

Alla medarbetare ska alltid tänka sig för innan information skrivs in i ett AI-verktyg. Sekretessklassificerad eller säkerhetsskyddsklassificerad information får inte hanteras i AI-baserade verktyg. För stöd finns kommunens riktlinjer för AI.

Samarbete med externa parter

Vid samarbete med externa leverantörer och andra kommuner eller myndigheter ska alltid säkerställas att de följer kraven vi har för informationssäkerhet, dessa är aldrig lägre än kraven vi ställer på oss själva. Det ska finnas avtal som reglerar informationssäkerheten, inklusive sekretess, dataskydd och incidenthantering.

Uppföljning och revision

Informationssäkerheten ska kontinuerligt följas upp och revideras för att säkerställa att riktlinjerna efterlevs. Det inkluderar såväl tekniska som organisatoriska revisioner. Löpande under året genomförs tester och granskningar av den tekniska miljön som en del i att arbeta systematiskt med IT-säkerhet.

Efterlevnad av lagstiftning

Alla verksamheter inom kommunen ska följa all gällande men även framtida lagstiftningar och föreskrifter som påverkar hur vi hanterar och skyddar vår information, inklusive:

- Dataskyddsförordningen (GDPR) för hantering av personuppgifter.
- Säkerhetsskyddslagen för hantering av säkerhetsklassificerad information.
- Lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (SFS 2018:1174).
- The Directive on security of network and information systems – NIS 2-direktivet

Allt arbete sker i enlighet med standarden ISO 27001.

Dokumentation och rapportering

Allt arbete med informationssäkerhet, inklusive riskbedömningar, incidenter och vidtagna åtgärder, ska dokumenteras och vara tillgängligt för revision.

Reglerna utgör en ram för hur kommunen och dess bolag ska arbeta med informationssäkerhet. De är baserade på bästa praxis och relevanta myndighetskrav. Reglerna revideras vid behov för att anpassas till förändrade förutsättningar eller lagstiftning.