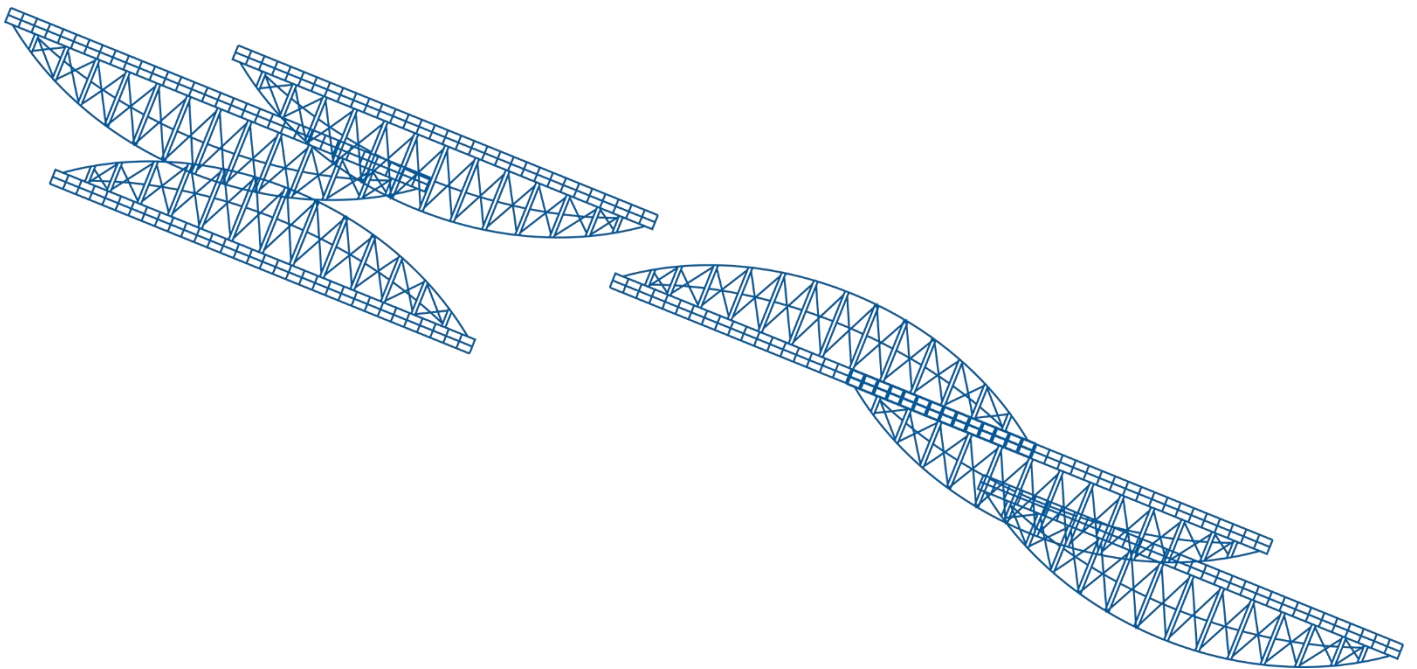




Informationssäkerhets- policy 2023-2028



Dokumenttyp Policy	Diarienummer 2022-517-167	Fastställt Kommunfullmäktige 2022-12-12 § 136
För revidering ansvarar Kommunchef	Uppföljning och tidplan Följs upp under 2028	Dokumentet gäller Samtliga
Dokumentet gäller till och med 2023 till och med 2028		



Innehållsförteckning

1	Inledning och syfte	3
2	Relation till andra styrdokument	3
3	Strategiska mål för informationssäkerhetsarbetet	4
4	Definition av informationssäkerhet	4
5	Roller och ansvar	5
6	Principer för informationssäkerhetsarbetet	6
7	Uppföljning	6

1 Inledning och syfte

Nordmalings kommuns informationssäkerhetspolicy beslutas av kommunfullmäktige och avser ledningens viljeinriktning med informationssäkerheten. Allt informationssäkerhetsarbete i Nordmalings kommun ska utgå ifrån informationssäkerhetspolicyn. Nordmalings kommun har även fastställda riktlinjer för det praktiska informationssäkerhetsarbetet.

2 Relation till andra styrdokument

Kommunfullmäktiges vision 2031 med tillhörande strategiska mål

Samtliga informationssäkerhetsriktlinjer med tillhörande rutiner som finns publicerade på Nordmalings kommuns intranät

Nordmalings kommuns digitaliseringsstrategi (ange diarienummer)

Nordmalings kommuns digitaliseringsplan med tillhörande aktivitetsplan

Nordmalings kommuns bredbandsstrategi (ange diarienummer)

Riktlinje för systemförvaltning (ange diarienummer)

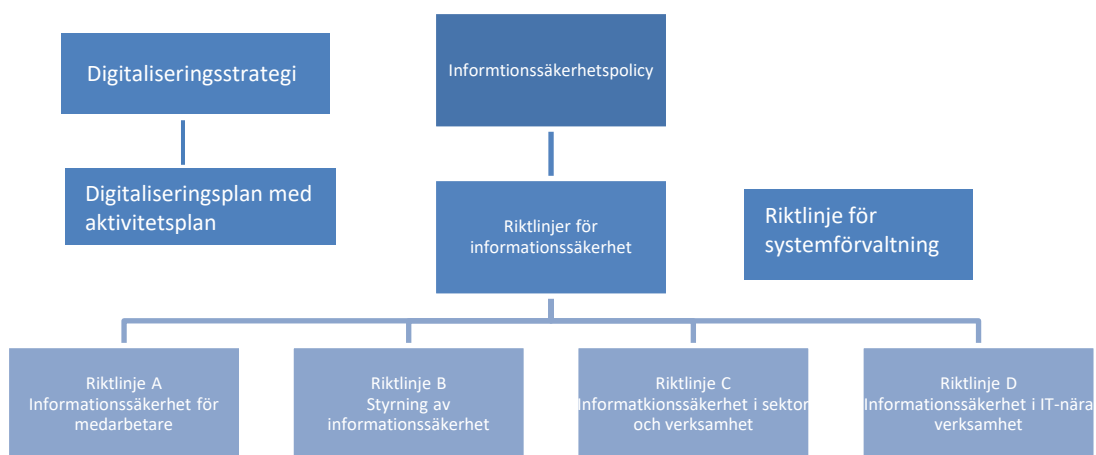


Bild 1. Figur som illustrerar hur relationen mellan de styrande dokumenten gällande informationssäkerhet ser ut.

3 Strategiska mål för informationssäkerhetsarbetet

Nordmalings kommuns långsiktiga mål med informationssäkerhetsarbetet är att:

- Informationssäkerhetsarbetet harmoniserar med kommunfullmäktiges övergripande vision och strategiska mål samt ger förutsättningar för ett långsiktigt informationssäkerhetsarbete
- Utforma en organisation för informationssäkerhetsarbetet
- Arbeta systematiskt med informationssäkerhetsarbete
- Uppnå en god säkerhetskultur i hela organisationen genom bland annat utbildningsinsatser
- Alla kritiska informationstillgångar är klassade
- Nordmalings kommuns medborgare har högt förtroende för kommunens informationssäkerhet

4 Definition av informationssäkerhet

Informationssäkerhet handlar om att skapa och upprätthålla lämpliga rutiner och skydd av fysisk och digital information utifrån aspekterna:

- Konfidentialitet - att informationen inte tillgängliggörs eller avslöjas för obehöriga
- Riktighet – att informationen är korrekt, aktuell och fullständig
- Tillgänglighet – att informationen är åtkomlig och användbar för de som behöver den

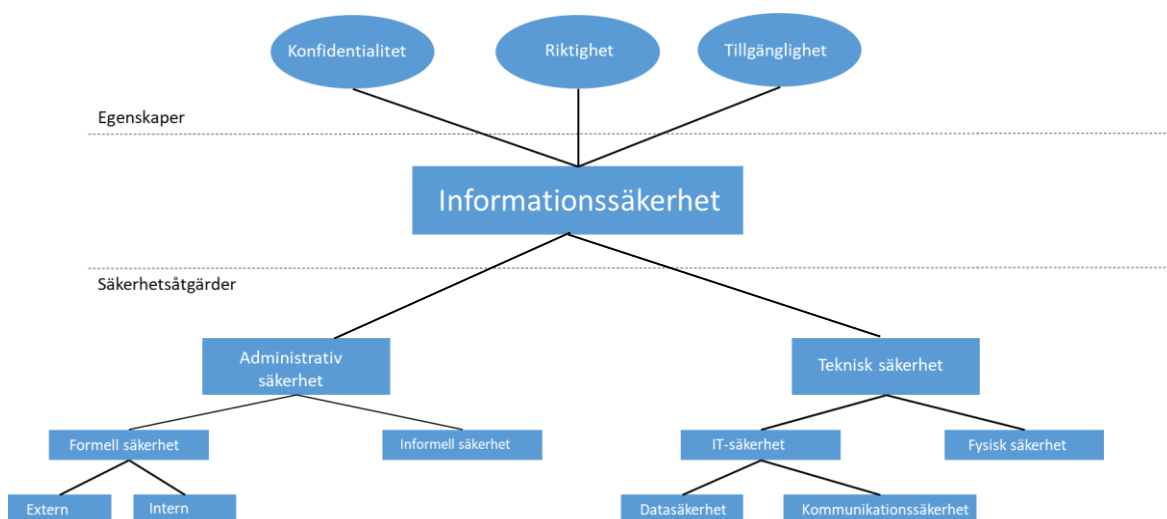


Bild 2. Illustration över informationssäkerhet i förhållande till administrativ och teknisk säkerhet.

5 Roller och ansvar

Följande roller och ansvar finns i kommunens informationssäkerhetsarbete;

- **Kommunstyrelsen**
Ansvarar ytterst för informationssäkerhetsarbetet.
- **Kommunchef**
Fastställer kommunens riktlinjer för informationssäkerhetsarbetet samt är ytterst ansvarig för IT-säkerhet (teknisk säkerhet och rutiner)
- **Ledningsgrupp (kommunchef + sektorchef)**
Ansvarar för att ledningssystem för informationssäkerhet (LIS) efterlevs.
- **Systemägare**
Ansvarar för säkerheten i informationstillgångar, klassning av informationstillgångar samt för genomförande av riskåtgärder.
- **Systemförvaltare**
Av systemägare utsedd förvaltare av ett visst system. Stödjer systemägaren i förvaltningen av systemet.
- **Chefer**
Ansvarar för att medarbetarna har förståelse för värdet av informationen och varför den ska skyddas. Detta innebär att chefer ska säkerställa att medarbetarna har utbildning som bidrar till en god säkerhetskultur och god medvetenhet om det egna ansvaret. Chefer ansvarar också för att riktlinjerna för informationssäkerhet efterlevs i respektive verksamhet. Ansvarar för informationssäkerheten inom egen verksamhet och ska verka för att arbetsmetoder som bidrar till en god informationssäkerhet används.
- **Enskilda medarbetare**
Ansvarar för att följa policys, riktlinjer, rutiner och tillämpningsanvisningar. Ska ha förståelse för värdet av informationen och varför den ska skyddas. Detta innebär att medarbetaren ska få utbildning som bidrar till en god säkerhetskultur och god medvetenhet om det egna ansvaret.
- **CISO (Chief Information Security Officer)**
Ansvarar för att leda, samordna och följa upp kommunens informationssäkerhetsarbete. Åtterrporterar till kommunstyrelsen och ledningsgrupp.
- **IT-samordnare**
Stödjer kommunchef i att IT-säkerheten motsvarar ställda krav. Stödjer CISO i informationssäkerhetsarbetet.
- **Dataskyddsombud**
Leder, samordnar och följer upp kommunens hantering av personuppgifter. Stödjer CISO i informationssäkerhetsarbetet.
- **Informationssäkerhetskontakt**
Utsedd person i varje sektor som stödjer sektorchef och chefer i det systematiska informationssäkerhetsarbetet

- **Informationssäkerhetsråd**
Stöttar CISO i det systematiska informationssäkerhetsarbetet.

6 Principer för informationssäkerhetsarbetet

- Informationssäkerhetsarbetet ska följa SS-EN ISO/IEC 27000 standard.
- CISO ska en gång per år rapportera det gångna årets informationssäkerhetsarbete till kommunstyrelsen
- Det ska finnas ett informationssäkerhetsråd som stöttar CISO i sitt arbete

7 Uppföljning

Kommunstyrelsen följer upp policyns efterlevnad av informationssäkerhetsarbetet i samband med CISO:s årliga rapportering. Den årliga rapporteringen sker i samband med rapporten för uppföljning av kommunstyrelsens dataskyddsarbete som sker vid första kommunstyrelsesammanträdet för året.

Större avvikelser rapporteras så snart som möjligt till ledningsgruppen och till kommunstyrelsen. Mindre avvikelser sammanfattas i den årliga rapporten till kommunstyrelsen.

Policyn gäller för åren 2023-2028 och ska innan 2028 har utvärderas inför att ny policy ska antas.