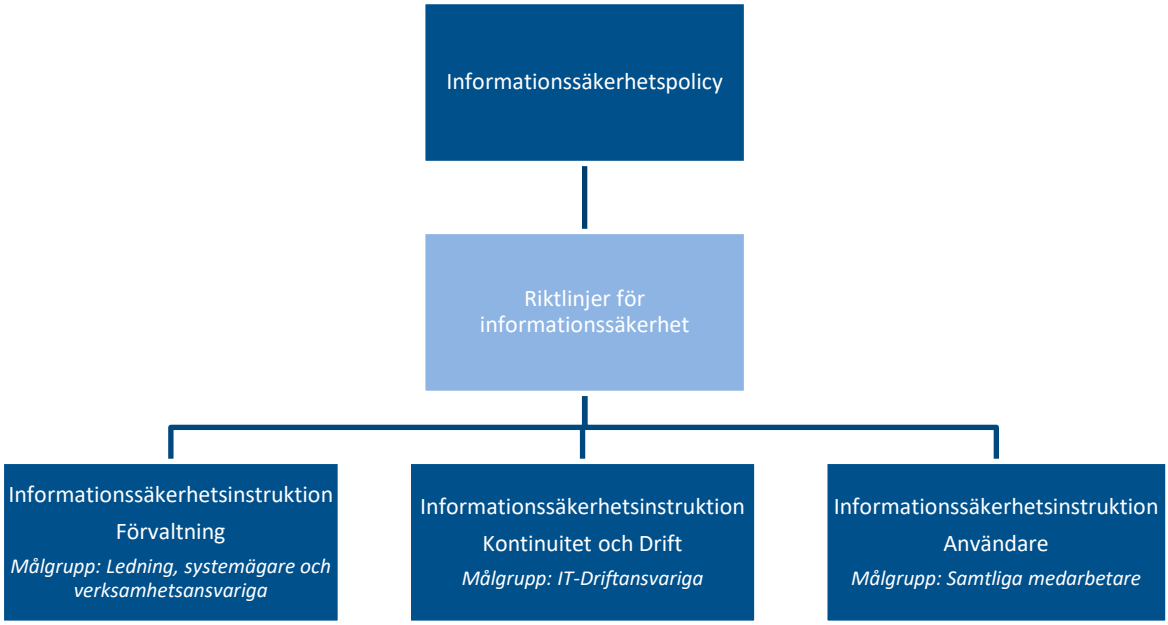
# Riktlinjer för Informationssäkerhet

| | |
|---|---|
| Antagen av: | Kommunstyrelsen 2021-05-26, § 53. Dnr KS 2021/69 |
| Dokumentkategori: | Styrdokument |
| Dokumenttyp: | Riktlinjer |

# Innehållsförteckning

## Inledning

Riktlinjer för informationssäkerhet konkretiserar informationssäkerhetspolicyn som antagits av kommunfullmäktige. Riktlinjen ger ramar för hur kommunens informationssäkerhetsarbete ska bedrivas och organiseras i förvaltningen. Kommunstyrelsen beslutar om riktlinjerna medan tillämpningar av riktlinjerna utformas av kommunkontoret i informationssäkerhetsinstruktioner.




## Om informationssäkerhet

Information är en av kommunens viktigaste tillgångar och utgör en förutsättning för att kunna bedriva verksamheten. Trosa kommuns informationstillgångar måste därför behandlas och skyddas på ett tillfredsställande sätt.

Informationstillgångar finns i alla kommunens verksamheter och begränsas inte till säkerhet i IT-system, utan omfattar information i alla dess former och oavsett hur information lagras, bearbetas och kommuniceras. Information kan till exempel vara i form av text, ljud, bilder och film, och kan hanteras med stöd av dator, papper eller direkt av oss människor i form av tal. En informationstillgång innebär allt som innehåller information och allt som bär på information.

Kraven på hantering av information styrs av lagar, förordningar, avtal och Trosa kommuns egna styrdokument. Utöver det har den enskilde, företag och andra aktörer i vår omvärld behov och förväntningar som ställer krav på vår informationssäkerhet. Avbrott i tillgången till information kan vara kritiskt och felaktig information kan ge allvarliga konsekvenser.

# Informationsklassning

Enligt informationssäkerhetspolicyn ska *Trosa kommun tillämpa en enhetlig modell för informationsklassning som anger olika nivåer av skyddskrav, vari information ska klassas baserat på interna och externa krav på informationens konfidentialitet, riktighet, tillgänglighet och spårbarhet.*

Trosa kommun ska använda SKR:s verktyg KLASSA för klassning av information.

# Skydd mot skadlig kod

Upptäckande, förebyggande och återställande skydd mot skadlig kod ska finnas och lämpliga rutiner ska införas för att uppmärksamma användarna.

# Incidenthantering

Informationssäkerhetsincidenter ska inrapporteras via fastställda rapporteringsvägar. Alla anställda, uppdragstagare och tredjepartsanvändare av informationssystem och -tjänster ska notera och rapportera alla observerade eller misstänkta säkerhetsbrister i system eller tjänster.

Informationssäkerhetssamordnaren ska sammanställa och rapportera till ledningen

- intrång och försök till intrång
- brott mot lagstiftning och internt regelverk
- incidenter som orsakar eller skulle kunna orsaka betydande avbrott och störningar
- konsekvenser och förslag till åtgärder efter intrång eller funktionsfel.

För att kunna ta hand om olika säkerhetsincidenter och funktionsfel i informationsbehandlingen ska det finnas rutiner för hantering av sådana situationer

## Loggning

Loggar ska produceras i den utsträckning som krävs för att verksamheten ska kunna förebygga, upptäcka och rätta till relevanta fel och felaktigheter, oönskade händelser och förändringar i nätverk, IT- system, programvara och information.

## Säkerhetskopiering

Säkerhetskopior av information och programvara ska tas och testas regelbundet i enlighet med fastställda rutiner.

# Åtkomst

Åtkomst till informationstillgångar ska beredas i den utsträckning som krävs för att anställda och uppdragstagare ska kunna ändamålsenligt genomföra sina arbetsuppgifter samt leva upp till krav som ställs i avtal och författningar.

### Behörighetsadministration

Formella rutiner för registrering av användare och tilldelning av lösenord för att medge och återkalla åtkomst till alla informationssystem och tjänster ska användas.

## Mobilt arbete

Vid arbete med mobila enheter, som t.ex. bärbar dator, mobiltelefon och USB-minnen, på annat ställe än i de egna lokalerna finns särskilda rutiner för informationssäkerhet. Uppgifter av känslig natur får endast hanteras på mobil enhet försedd med fil- eller diskkryptering.

## Inventarier och licenser

Aktuella förteckningar ska föras över IT-tillgångar samt användning av programvarulicenser. Detta innefattar lista på servrar, klientdatorer, nätverksenheter och programvaror. Förteckningen ska ange hur dessa märkts och ansvarsfördelningen för dem. Det ska finnas rutiner för omflyttning och överlåtelse av IT-utrustning till annan användare.

## Fysisk säkerhet

Den fysiska säkerheten ska organiseras så att verksamhetens personal och uppdragstagare, lokaler, utrustning och informationsresurser skyddas mot hot som inbrott, stöld, brand, översvämning, olyckor och katastrofer som orsakas av fel i tekniska system, misstag, sabotage eller andra externa händelser

## Kontinuitetsplanering

Kontinuitetsplaner för kritiska verksamhetsprocesser ska upprättas, testas och uppdateras regelbundet för att säkerställa att de är aktuella och verkningsfulla. Syftet är att motverka avbrott i organisationens verksamhet och för att skydda kritiska verksamhetsprocesser från verkningarna av allvarliga fel i informationssystem eller katastrofer.

## Utbildning

Alla anställda och uppdragstagare ska årligen ges en kort utbildning i informationssäkerhet med särskild inriktning på informationssäkerhetspolicy och riktlinjer samt vikten av att följa reglerna. Information ges även i samband med att nya personer engageras i verksamheten.

### Under anställningen

Information och utbildning av anställda ska omfatta:

- Informationssäkerhetens betydelse för verksamheten
- Innehållet i Informationssäkerhetspolicyn och riktlinjer för

informationssäkerhet
- Informationssäkerhetsinstruktion Användare

Systemägare ansvarar för att:
- användarhandledning för aktuellt system finns
- medarbetare har tillräckliga kunskaper om säkerhetsreglerna för de informationssystem de behöver för de egna arbetsuppgifterna.

## Förvaltning

Följande områden är av särskild betydelse för Trosa kommun:
- Telefoni/Datakommunikation
- Medicinskt relaterade verksamhetssystem
- Drift av infrastruktur (VA/avlopp)

För ovanstående områden finns särskilda krav som framgår av lagar och förordningar och ska beaktas.

Det administrativa nätverket[1] har en tung strategisk betydelse för möjligheterna till en kostnadseffektiv och säker drift av övriga IT-system. IT-chefen ska därför ha stort inflytande på förvaltningen av det administrativa nätverket, som systemförvaltare (systemansvarig) eller på annat lämpligt sätt.

## Revidering och uppföljning

Uppföljning är en viktig del i informationssäkerhetsarbetet för att bevaka att:
- Beslutade åtgärder är genomförda
- Regler följs
- Att policy, säkerhetsinstruktioner och riskanalyser revideras vid behov.

[1] Det administrativa nätverket är den tekniska systemmiljö i vilket övriga administrativa system implementeras. Det administrativa nätverket utgörs bl a av fysiska förbindelser, aktiv kommunikationsutrustning, fileservrar, nätverksoperativ, verktyg för systemadministration, adressering och övervakning, backupsystem, säkerhetsutrustning t ex brandväggar mm. I det administrativa nätverket kan ingå applikationsservrar, arbetsstationer, databashanterare, kontorsstödsapplikationer, e-post etc. Omfattningen av vad som ingår i det administrativa nätverket bestäms med hänsyn till de enskilda komponenternas roll i hela IT-miljön. Denna roll kan variera över tiden t ex kan en databashanterare övergå från att vara en komponent i ett enskilt verksamhetssystem till att vara en gemensam databashanterare för flera olika verksamhetssystem.