



## Informationssäkerhetspolicy för Timrå kommun

Fastställd av kommunstyrelsen 2017-05-02 § 135.

Reviderad av kommunstyrelsen 2018-03-06 § 65.

Reviderad av kommunstyrelsen 2020-11-10 § 359

Informationssäkerhet avser hantering av verksamhetens information. Denna policy tillsammans med vägledande råd och bestämmelser styr kommunens informationssäkerhetsarbete. Vägledande för arbete är standarden, ISO/IEC 27002. Informationssäkerhetshandboken innehåller förutom policy:

- Riktlinjer – anger hur övergripande målen i policy skall uppnås. Ges en beskrivning om vad som skall göras inom informationssäkerhetens olika områden.
- Anvisningar – beskriver hur skydd för information skall införas.

### Utgångspunkter

Informationssäkerhet utgörs av IT-säkerhet (teknik) och administrativ säkerhet (regler och rutiner) och användarnas medvetenhet om betydelsen av sitt beteende. Som informationstillgångar betraktas all information oavsett om den behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer. Detta gäller utan undantag.

Utgångspunkter är lagar, förordningar och föreskrifter, kommunens egna krav samt avtal. Rätt information ska vara tillgänglig för rätt person och vara spårbar, den ska vara och förbli riktig. Informationen ska skyddas för att förhindra obehörig åtkomst eller otillåten spridning av informationen. Informationssäkerhet är en del av verksamheten och gäller för alla, förtroendevalda, anställda, konsulter, praktikanter, elever. Det är ett ansvar för chefer på alla nivåer att aktivt verka för en positiv attityd till säkerhetsarbetet.

### Mål

- All personal har kunskap om gällande informationssäkerhetsregler.
- Informationsförsörjningen är säker och effektiv och bidrar till ökat skydd och stöd.
- Krishanteringsförmågan upprätthålls.
- Alla investeringar i form av information och teknisk utrustning har tillräckligt skydd.
- Det finns tillgång till en säker infrastruktur för extern och intern kommunikation.
- Hotbilden mot varje enskilt informationssystem av vikt för verksamheten fortlöpande analyseras; systemägare har ansvar att analysera och förebygga negativa konsekvenser.



## **Roller och ansvar**

Kommunstyrelsen har det övergripande ansvaret för informationssäkerheten. Det operativa ansvaret är delegerat till kommunchefen. Varje nämnd svarar för arbetet med informationssäkerhet inom sitt verksamhetsområde och för att styrdokumenterna följs.

Ledningsgruppen under ledning av kommunchefen har det övergripande ansvaret för planering och genomförande av kommunens informationssäkerhetsarbete.

Informationssäkerhetssamordnaren utses av och är direkt underställd kommunchefen samt har det operativa ansvaret för samordning av informationssäkerhetsarbetet.

Ansvar för samtliga system är fördelat på systemägare och systemförvaltare.

Systemförvaltarna utses av respektive systemägare och är de som har ansvaret för användningen av IT-systemet inklusive informationssäkerheten. Systemägare är även informationsägare.

Detaljerad roll- och ansvarsfördelning framgår av Vägledande råd och bestämmelser (VROB) för: Förvaltning & Drift.

Alla verksamheter inom kommunen är bundna av denna policy.

## **Generella krav**

Vissa informationssystem är en förutsättning för att kunna bedriva verksamheten. Systemen ska prioriteras av representanter för förvaltningarna, informationssäkerhetssamordnaren och IT-enheten. Systemen ska vara identifierade och förtecknade, där det ska framgå vem som är systemägare och systemförvaltare. Det ska också genomföras en Verksamhets- samt Riskanalys på samtliga av de prioriterade systemen.

## **Informationsklassning**

Information ska klassificeras utifrån den funktion och betydelse för verksamheten som den har och de konsekvenser det skulle medföra om informationen hanteras felaktigt, försvinner, kommer i orätta händer, etc. Information ska klassas med avseende på sekretess, riktighet och tillgänglighet.

## **Sekretess**

Sekretessbelagd och annan känslig information ska aldrig skickas med e-post.

## **Tillträdesskydd**

För att inga obehöriga ska få tillträde till kommunens nätverk och verksamhetssystem ska systemägare årligen kontrollera att behörighet överensstämmer med anställning.

För att inga obehöriga ska få tillträde krävs att passerkort och nycklar till kommunens fastigheter kvitteras vid ut- och återlämnande.



### **Distansarbete**

Möjligheter att arbeta på distans finns. Förutsättningar för detta finns i vägledande råd och bestämmelser Distansarbete.