INFORMATIONSSÄKERHETSPOLICY FÖR TIMRÅ KOMMUN

Fastställd av kommunstyrelsen 2013-08-13, § 167

Denna policy ska ange mål och inriktning för kommunens arbete med informationssäkerhet. Informationssäkerhet är den del i organisationens lednings- och kvalitetsprocess som avser hantering av verksamhetens information. Denna policy tillsammans med vägledande råd och bestämmelser samt IT-strategi styr kommunens informationssäkerhetsarbete.

Utgångspunkter
Information är en av organisationens viktigaste tillgångar. Kommunens risk- och sårbarhetsanalys (RSA) ska säkerställa att hanteringen av all information sker säkert. Som informationstillgångar betraktas all information oavsett om den behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer.

Utgångspunkter i arbetet med informationssäkerhet är lagar, förordningar och föreskrifter, kommunens egna krav samt avtal. Rätt information ska vara tillgänglig för rätt person när den behövs och vara spårbar. Informationen ska vara och förbli riktig.

Informationssäkerhet är en integrerad del av verksamheten. Alla som hanterar informationstillgångar har ett ansvar att upprätthålla informationssäkerheten. Det är ett ansvar för chefer på alla nivåer att aktivt verka för en positiv attityd till säkerhetsarbetet. Var och en ska vara uppmärksam på och har en skyldighet att rapportera händelser som kan påverka säkerheten för kommunens informationstillgångar.

Mål
För informationssäkerhetsarbete ska gälla att:

- All personal har kunskap om gällande informationssäkerhetsregler.
- Informationsförsörjningen är säker och effektiv och bidrar till ökat skydd och stöd för medarbetare, samverkande aktörer och tredje man.
- Krishanteringsförmågan upprätthålls.
- Alla investeringar i form av information och teknisk utrustning har tillräckligt skydd.
- Det finns tillgång till en gemensam, säker och väl definierad infrastruktur för extern och intern datakommunikation.
- 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 säkerhetschefen. Informationssäkerhetssamordnaren utses av och är direkt underställd säkerhetschefen samt har det operativa ansvaret för samordning av informationssäkerhetsarbetet. Systemförvaltare utses av respektive systemägare och är den person som har ansvaret för den dagliga användningen av IT-systemet inklusive informationssäkerheten.

Detaljerad roll- och ansvarsfördelning framgår av Vägledande råd och bestämmelser (VROB) för:
Förvaltning, Användare, Drift, Mobila enheter, Sociala medier, USB-minnen samt Skrivare.

Generella krav
Vissa informationssystem är en förutsättning för att kunna bedriva verksamheten. Dessa system ska prioriteras av IT-rådet med representanter för förvaltningarna och den centrala IT-enheten.

Samtliga informationssystem ska vara identifierade och förtecknade. Av förteckningen ska framgå vem som är systemägare. Prioriterade samhällsviktiga system ska minst klara den basnivå för informationssäkerhet som rekommenderas av Myndigheten för samhällsskydd och beredskap (MSB). Gemensamt metodstöd ska finnas och användas av samtliga.

Utbildning
All personal ska regelbundet få den utbildning som krävs för att upprätthålla informationssäkerheten.

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 enligt en gemensam mall klassificeras med avseende på sekretess, riktighet och tillgänglighet.

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

Sekretess
Sekretessbelagd och annan känslig information bör inte skickas med elektronisk post.

Kontinuitetsplanering
Kontinuitetsplanering är central för att bedriva verksamheten på en acceptabel nivå under både normala förhållanden och extraordinära situationer. En kontinuitetsplan ska finnas för driften av IT-verksamheten. Den ska baseras på de olika verksamhetssystemens samlade krav.

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. Extern uthyrning/utlåning av kommunhusets lokaler efter kontorstid bör av säkerhetsskäl inte ske.

Revidering och uppföljning
Uppföljning är en viktig del i informationssäkerhetsarbetet. Förvaltningarnas risk- och sårbarhetsanalyser lämnas årligen till informationssäkerhetssamordnaren. Informationssäkerhetspolicyn revideras årligen.

Basnivå för prioriterade samhällsviktiga system rapporteras årligen till informationssäkerhetssamordnaren enligt fastställt metodstöd.