FÖRFATTNINGSSAMLING	BESLUT	GÄLLER FR	FLIK	SID
	Kf § 83/05	2005-06-13	Kf 26	1
		2009-20-16 ändring		

Informationssäkerhetspolicy

Härjedalens kommuns ramverk för Informationssäkerhetsarbete i enlighet med Krisberedskapsmyndighetens Basnivå för Informationssäkerhet (BITS)

Innehåll

1. VERKSAMHETSBESKRIVNING

Det moderna samhället är starkt beroende av att elförsörjning, telekommunikationer och IT-system fungerar. Om dessa påverkas kan svåra störningar uppstå i samhället. De inbördes beroenden som finns mellan IT-systemen måste uppmärksammans liksom den tekniska utvecklingen. Säkerhetsfrågorna inom IT-området kommer därför att spela en allt mer central roll i framtiden.

Krav på tillgänglighet till kommunal service kommer att öka i takt med IT-mognaden. Det informationsflöde som informationstekniken medger ställer höga krav på den kommunala organisationen. Det är nödvändigt att informationen

- finns tillgänglig vid behov
- är skyddad mot insyn, obehörig användning och förvanskning
- är spårbar

Medarbetare och kommunmedborgare måste alltid känna sig övertygade om att Härjedalens kommun hanterar information på ett korrekt sätt.

2. MÅL MED INFORMATIONSSÄKERHETSARBETET

En Informationssäkerhetspolicy utgör en förutsättning för att arbetet med Informationssäkerhet sker på ett tillfredsställande sätt. Informationssäkerhetspolicyn ska på ett tydligt sätt uttrycka ledningens mål för Informationssäkerheten. De mål som formuleras här utgör en ram för de beslut som tas inom kommunens verksamheter. Hur målen ska uppfyllas anges i underliggande dokument med praktiska Informationssäkerhetsinstruktioner.

2.1 Långsiktiga mål

Informationssäkerhetsarbetet ska säkerställa att

- alla användare ska vara medvetna om Informationssäkerhetsfrågornas betydelse
- lagar, förordningar och andra bestämmelser efterlevs
- den personliga integriteten prioriteras och beaktas
- känslig information skyddas mot obehörig åtkomst, förändring och förstöring
- rätten till insyn i allmänna handlingar beaktas
- hotbilden för varje samhällsviktigt/verksamhetskritiskt IT-system analyseras fortlöpande
- driftsäkerheten i IT-systemen upprätthålls

- en årlig uppföljning och kontroll av Informationssäkerheten sker, bland annat som underlag för verksamhetsplanering
- varje system formellt driftgodkänns
- kommunen kan utföra sina samhällsviktiga uppgifter vid extraordinära händelser och under höjd beredskap

1.1 Årliga mål

Informationssäkerhetsarbetet skall bedrivas så att det blir en integrerad del av organisationens normala verksamhet. Årliga mål för arbetet skall därför beslutas och framgå av organisationens verksamhetsplanering. För de årliga målen bör anges

- tidplan
- resurser för arbetet
- när och hur uppföljning, utvärdering och avrapportering skall ske
- när och hur organisationens medarbetare skall informeras och utbildas

2 ORGANISATION OCH ANSVAR

2.1 Övergripande ansvar

Det övergripande ansvaret för kommunens IT-system vilar på kommunstyrelsen. Informationssäkerhetspolicyn är ledningens sätt att uttrycka kommunens mål för Informationssäkerheten. För att uppnå samordning arbetar kommunens IT-ledningsgrupp med att analysera och förbereda IT-frågor för beslut. Kommunledningsutskottet är ledningsgrupp för arbetet med Informationssäkerhet.

2.2 Organisation

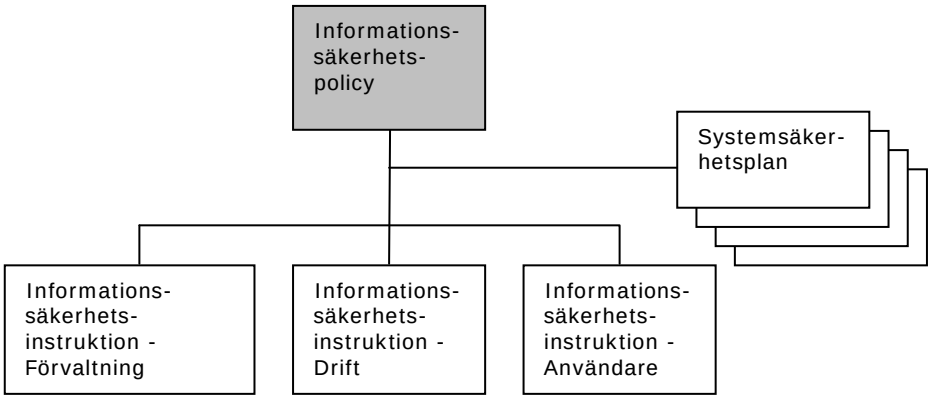
Ansvarsfördelningen ska säkerställa att ett IT-system kan administreras och hanteras på ett sådant sätt att det under hela sin livstid bidrar till att stödja avsedd verksamhet och uppfylla Informationssäkerhetspolicyns mål. Detta innebär att ett IT-system med alla dess delar är en resurs i en verksamhet på samma sätt som personal, lokaler, kontorsmaterial mm.

Den interna organisationen för Informationssäkerhetsarbetet och de roller och ansvar som ingår i denna framgår av dokumentet ”Informationssäkerhetsinstruktion Förvaltning”.

2.3 Styrande Dokument

Informationssäkerhetspolicyn är det övergripande dokumentet som styr Informationssäkerhetsarbetet. Policyn konkretiseras i Informationssäkerhetsinstruktioner för användare, förvaltning och drift. Styrande för de enskilda IT-systemen är respektive systemsäkerhetsplan. En sådan ska upprättas för de IT-system som bedöms som viktiga för verksamheten.

Det åligger kommunledningsutskottet att svara för utformning och uppföljning av Informationssäkerhetsinstruktioner.



3 AVGRÄNSNING

Informationssäkerhetspolicyn med tillhörande riktlinjer rör all informationsbehandling som sker med hjälp av IT-stöd oavsett driftsmiljö och oberoende av om bearbetning och lagring sker i av kommunen ägd utrustning, externt hos servicebyrå, i medarbetares bostad eller på annan plats utanför kommunens lokaler.

4 BASFÖRMÅGA

Som grund för kommunens Informationssäkerhetsarbete gäller Krisberedskapsmyndighetens rekommendationer om basnivå för samhällsviktiga IT-system (BITS) samt i tillämpliga delar den svenska standarden SS-ISO/IEC 17799.

5 RIKTLINJER FÖR SÄRSKILT VIKTIGA OMRÅDEN

Riktlinjer ska finnas inom följande områden

- distansarbete, extern anslutning och mobil datoranvändning
- IT-incidenthantering
- användning av epost och internet
- datakommunikation
- införande, drift, förvaltning och avveckling av IT-system

Riktlinjerna ska framgå av Informationssäkerhetsinstruktionerna för förvaltning, drift och användare.

6 KONTINUITETSPLANERING

Av kommunens systemsäkerhetsplaner ska framgå de enskilda IT-systemens krav på avbrotts- och katastrofplanering.

7 SYSTEMSÄKERHETSPLANER OCH DRIFTGODKÄNNANDE

Informationssäkerhetsarbetet inom Härjedalens kommun ska följa den process som finns beskrivet i Krisberedskapsmyndighetens rekommendationer om basnivå för samhällsviktiga IT-system (BITS). Detta innebär att utgående från kommunens Informationssäkerhetspolicy ska en systemsäkerhetsplan tas fram för varje samhällsviktigt IT-system. I systemsäkerhetsplanen identifieras styrande lagkrav, verksamhetskrav på sekretesskydd, riktighet och tillgänglighet samt hotbild. Dessutom ska systemets viktighet för kommunen och samhället framgå.

Systemsäkerhetsplanen ska fastställas av systemägaren.

8 REVISION OCH UPPFÖLJNING

Uppföljning av säkerhetsläget i kommunens IT-system är en mycket viktig del i säkerhetsarbetet. Framtagna systemsäkerhetsplaner ska löpande följas upp och vid behov revideras.