

Bilag 19 – IT sikringspolitik

Sammenhæng til økonomiregulativet

I henhold til kommunens Økonomiregulativ afsnit 10.1 "IT-sikringspolitik". er der udarbejdet bilag indeholdende beskrivelse af kommunens generelle sikkerhedspolitik, kvalitetssikring samt personer, der kan være særligt udsatte for kritik.

Indledende bemærkninger

En meget væsentlig del af kommunens ind- og udbetalinger samt posteringer dannes i IT-systemer, der understøtter opgaveløsningen i de centrale og decentrale enheder. I den forbindelse har direktionen godkendt en "Foreløbig IT-Sikkerhedspolitik", der er gældende indtil Byrådet har vedtaget den endelige Sikkerhedspolitik. Den Foreløbige IT-Sikkerhedspolitik fremgår af kommunens intranet under IT.

IT-sikkerhedspolitik

Furesø Kommunes Sikkerhedspolitik beskriver blandt andet:

- at sikkerhedspolitikken er gældende for alle ansatte i Furesø kommune, herunder medarbejdere i selvejende institutioner samt Byrådspolitikere
- at den omfatter alt hard-og software som ejes af Furesø kommune, både centralt og decentralt
- hvorledes området er organiseret, herunder hvilket ansvar og opgaver, der er knyttet til enten persongrupper eller enkeltpersoner
- hvorledes den fysiske sikkerhed defineres og hvorledes dette udføres i praksis herunder omkring
 - administrativt netværk,
 - ledningsnet
 - sikkerhedskopiering
 - bortskaffelse af hardware og data
 - mærkning og installation
- regler for administrativ sikkerhed herunder brugeroprettelse, tildeling af og kontrol med brugerrettigheder, logning og behandling af personoplysninger.
- Regler for håndtering af elektronisk post, og sikkerhed mod hackning mv.
- Regler for anvendelse af internettet.

Kontroller af personer der særligt kan være udsatte for kritik

Når en person indberetter til et IT-system som f.eks. håndterer ind, udbetalinger eller danner opkrævning vedrørende personen selv kan sådanne personer i givne situationer være særlig udsat for kritik.

Den budgetansvarlige eller systemejere skal derfor omkring disse personer etablere en mere omfattende kontrol. Denne kontrol skal minimum foretages årligt (i forbindelse med regnskabsafslutningen) og skal omhandle de data, der vedrører personen selv.

Kontrollen kan ikke udføres ved stikprøver og skal altid kunne dokumenteres. Det er systemejeren, der er ansvarlig for at kontrollen udføres for det pågældende system. Såfremt der konstateres uregelmæssigheder skal dette straks rapporteres til den øverste sikkerhedsansvarlige samt den pågældendes chef og direktør.

Kvalitetskontrol

Det er den enkelte budgetansvarlige, der skal vurdere hvilken kvalitetskontrol, der skal foretages for de forskellige funktioner i de systemer den pågældende har ansvaret for. Den udførte kvalitetskontrol skal til enhver tid kunne dokumenteres udført.

Der er ingen krav til at kvalitetskontrol skal udføres 100 %, når denne foretages stikprøvevis skal det fremgå hvorledes stikprøven er udtaget.

Det er den enkelte systemejer sammen med den sikkerhedsansvarlige, der er ansvarlig for, at kommunens IT-systemer anvendes ensartet og mest optimalt.

Det er IT afdelingen sammen med Regnskabsgruppen, der er ansvarlig for at der altid foreligger en opdateret fortegnelse over Furesø kommunes systemejere, sikkerhedsansvarlige og superbrugere.

Det fremgår af Furesø kommunes ”Systemejerkoncept”, hvilket ansvar og opgaver, der påhviler henholdsvis, systemejere, sikkerhedsansvarlige og superbrugere.

Ovenstående lister kan desuden findes på kommunens Intranet.

Ajourføring af regnskabspraksis

I henhold til Økonomiregulativets bestemmelser er det regnskabschefen, der har kompetencen til at indarbejde ændringer af ovenstående praksis, uden at det skal forelægges Byrådet til godkendelse. Større og mere vidtgående ændringer skal dog forelægges Byrådet.

Bilaget er senest ajourført den XXXX 2007.