Halsnæs kommune

Informationssikkerhedspolitik

Oktober 2015

Halsnæs
Kommune

Baggrund

Ved informationssikkerhed forstås de samlede foranstaltninger til at sikre Fortroligheden, Tilgængeligheden og Integriteten på kommunens informationsaktiver. Foranstaltninger inkluderer tekniske foranstaltninger, procedurer, regler, lovmæssige kontroller og eventuelle andre foranstaltninger, der alle har til formål at udmønte informationssikkerhedspolitikken.

Informationssikkerhedspolitikken er udarbejdet med baggrund i anbefalingerne i sikkerhedsstandarden ISO 27000 og med henvisning til lokale forhold, herunder det aktuelle trusselsbillede.

Omfang

Sikkerhedspolitikken er gældende for

- Alle ansatte i Halsnæs kommune
- Medlemmer af byråd og andre folkevalgte der har adgang til kommunale data
- Samarbejdspartnere og leverandører af informationssikkerhedsydelser
- Eventuelle andre brugere af Halsnæs kommunes datanetværk

Politikken omfatter Halsnæs kommunes data og informationsaktiver.

Målsætning for it-sikkerhed

Den forretningsmæssige målsætning for informationssikkerheden er:

- Sikring af fortrolighed, tilgængelighed og integritet på kommunens data
- Sikring af, at al it-anvendelse overholder gældende lovgivning
- Sikring af ledelsesmæssig opfølgning på it-udvikling, -sikkerhed og – drift

Disse mål danner grundlag for etablering af et passende sikkerhedsniveau, som dels skal sikre overholdelse af lovgivningens krav, og dels er fleksible og kan justeres ud fra aktuelle risiko- og omkostningsvurderinger.

Overordnet politik for styring af informationssikkerhed

Generelt

Kommunens troværdighed med håndtering af data i forhold til omverdenen må ikke kunne drages i tvivl.

It-informationssikkerhedspolitikken offentliggøres og kommunikeres til alle relevante interessenter via kommunens hjemmeside.

It-informationssikkerheden søges styret i overensstemmelse med almindeligt anerkendte metoder og procedurer jf. sikkerhedsstandarden ISO 27000.

Sikkerhedsniveauet fastsættes på baggrund af overordnede forretningsmæssige konsekvensvurderinger af risiko på systemer og sårbarhedsvurderinger af teknikker og leverandørerne hertil. Risikovurdering sker minimum en gang årlig, for udvalgte informationssikkerhedsaktiver.

Risiko håndteres efter en metode, der tager udgangspunkt i ISO 27000 standarden

- Vælge at leve med risikoen
- Udføre tiltag der nedsætter risikoen
- Dele risiko f.eks. via forsikring eller eksterne leverandøraftaler
- Udfase årsag til risikoen

Halsnæs Kommune er ansvarlig for at alle medarbejdere har det fornødne kompetenceniveau i forhold til håndtering af IT-sikkerhed.

Ledelsesforhold.

ANSVARSPLACERING

Chefgruppen har det overordnede ansvar for informationssikkerheden, herunder udpegning af rollerne i sikkerhedsarbejdet.

Kommunens ledere har ansvaret for sikkerheden og vil uddelegere opgaver og ansvar vedrørende de enkelte funktionsområder, herunder også for vejledning og instruktion af medarbejdere.

Enhver medarbejder og folkevalgt ved kommunen har således et medansvar for informationssikkerheden, og vil blive holdt informeret om sikkerhedsmæssige problemer og om tiltag af betydning for at kunne leve op til dette ansvar.

Styringsprincipper

Informationssikkerhed er et fælles anliggende for hele organisationen som er forankret ledelsesmæssigt i Chefgruppen.

ADGANGSSTYRING

Alle it-aktiver skal i nærmere specificeret omfang, være beskyttet imod uautoriseret adgang.

Der skal kunne udføres adgangskontrol og - via logning - skabes grundlag for efterkontrol.

FUNKTIONSADSKILLELSE

Der etableres i fornødent omfang regler for funktionsadskillelse (dvs. den samme person må ikke både udføre og godkende en given handling eller funktion). Dette princip er en grundlæggende forudsætning for forebyggelse og begrænsning af konsekvenser fra fejl, uheld og bevidst negative handlinger forårsaget af enkeltpersoner.

UAFHÆNGIGHED AF NØGLEPERSONER

Der skal tilstræbes uafhængighed af enkeltpersoner gennem etablering af personbackup for de medarbejdere, der er alene om at dække specialer eller systemer af væsentlig betydning for kommunen.

DRIFTSFORSTYRRELSER

Skal imødegås gennem:

- Forebyggende foranstaltninger, bl.a. procedurer for kvalitetssikring, ændringsstyring og dokumentationsvedligeholdelse.
- Problemhåndtering, bl.a. procedurer for skadeudbedring, omgåelse, omkobling eller tilsvarende, på en sådan måde, at de aftalte tilgængelighedskrav ikke overskrides.

KATASTROFESITUATIONER

Omfanget af foranstaltninger besluttes på basis af foretaget risikovurdering.
Hvor risikoanalysen berettiger dette, skal der udarbejdes beredskabsplaner.

Katastrofer forårsaget af brand- eller vandskader søges primært undgået gennem en veltilrettelagt fysisk sikring og overvågning af bygninger, tekniske installationer og it-udstyr.

Der skal foreligge beredskabsplaner for de nødsituationer, der af Chefgruppen er defineret som kritiske.

Udmøntning af informationssikkerhedspolitikken

De generelle uddybende informationssikkerhedsretningslinjer, -regler og – procedurer struktureres i overensstemmelse med ISO 27000. Retningslinjerne skal gennemgås hvert år eller efter behov.

Der skal udarbejdes et sæt af procedurer og et årshjul, der fastlægger og danner grundlag for udmøntning af denne politik og de detaljerede informationssikkerhedsretningslinjerne.

Afvigelser fra informationssikkerhedspolitikken

Chefgruppen kan efter indstilling fra Øverste Daglige Informationssikkerhedsleder – i enkeltstående tilfælde- foretage afvigelser fra denne informationssikkerhedspolitik.

Gyldighed

Denne overordnede politik skal godkendes af Byrådet og revurderes efter behov, dog mindst hvert 4. år.

En gang årligt skal Byrådet have forelagt status på informationssikkerheden, herunder it-revisionsrapporten. Ved større sikkerhedshændelser informeres Byrådet straks.

Byrådet godkender endvidere valg af leverandører til meget store fælleskommunale it-anskaffelser.

Denne politik er godkendt af Byrådet den 14. december 2015, og den afløser tidligere godkendte informationssikkerhedspolitikker.