Kalundborg Kommune

Politik

5.1

22-04-2015

1. Indledning

Kommunalbestyrelsen har godkendt denne IT-sikkerhedspolitik som den overordnede ramme, for den generelle IT-sikkerhed overalt i organisationen.

2. Formål

Sikkerheden i informationer og informationssystemer, er af største betydning for den daglige drift af Kalundborg Kommunes it-leverance. Henholdsvis den interne - til organisationens medarbejdere, og den eksterne til borgere, samarbejdspartnere og virksomheder.
Kalundborg Kommune skal overholde lovmæssige krav samt implementere sikkerhedsforanstaltninger, der tilgodeser alle der har relationer til organisationen. Det være sig borgere, leverandører, samarbejdsparter (private/offentlige), og medarbejdere.
Målet for IT-sikkerhedspolitikken er, at beskytte informationer og informationssystemer uafhængigt af, hvor disse måtte findes.
Målet for IT-sikkerhedspolitikken er endvidere at tilkendegive klart, over for alle med en relation til organisationen, at der er udstukket regler og procedurer til regulering af brugernes adfærd ved anvendelsen af informationer og informationssystemer.
Sikkerhed for høj driftsstabilitet i forhold til tilgængelighed og funktionalitet, er endvidere et væsentligt mål for IT-sikkerhedspolitikken.
Enhver der kommer i berøring med organisationens informationer og informationssystemer har et medansvar for at opretholde den generelle informationssikkerhed.
Med henblik på at opretholde en IT-sikkerhedspolitik, fastlægger den øverste sikkerhedsansvarlige en, konkret og anvendelig overordnet politik. Denne politik udbygges med instrukser og retningslinier på områder, hvor der er behov for det. Den samlede politik danner derefter grundlaget for sikkerheden i hele organisationen.

3. Sikkerhedspolitik

Kommunalbestyrelsens mål med IT-sikkerhedspolitikken er, at sikre IT-anvendelsen overholder gældende lovgivning, således at organisationen altid fremstår som en respekteret og betroet myndighed.
Det er desuden Kommunalbestyrelsens mål:
* At opretholde et stabilt, højt tilgængeligt og funktionelt IT-service niveau overfor samtlige brugere.
* At forebygge, forhindre og begrænse tab af data og andre IT-værdier mod tyveri, hærværk samt anden tilsigtet/utilsigtet ødelæggelse.
* At forebygge hhv. begrænse skader til en for organisationen kendt og accepteret størrelse.
* At sikre organisationens fortsatte driftsevne, ved hjælp af en beredskabsplan, efter følgerne af en eventuel skadevoldende hændelse inden for en accepteret tidshorisont.
* At beskytte organisationens informationer og informationssystemer mod uvedkommendes adgang, manipulation, indsigt eller forsøg herpå.
* At sikre, at enhver sikkerhedsmæssig følsom IT-aktivitet kan henføres til den person, som har udført aktiviteten, samt at sikre gennemførelsen af fornødne sikkerhedsforanstaltninger til opdagelse af misbrug og forsøg herpå.
* At sikre, at organisationens udvikling og implementering af nye IT-aktiviteter - internt - borger- eller virksomhedsrettede services udføres under iagttagelse af betryggende sikkerhedsforanstaltninger.
* At sikre ledelsesmæssig opfølgning på IT-udvikling, sikkerhed og drift.
* At anvende danske evt. internationale standarder som reference og grundlag for IT-sikkerhedsarbejdet i organisationen.
* At Kalundborg Kommune, som offentlig myndighed, praktiserer både digital forvaltning og digital borgerservice på sikker vis.

4. Dækningsområde

IT-sikkerhedspolitikken gælder for alle organisatoriske enheder samt for IT-aktiviteter, der under organisationens ansvar, udføres for eller af andre f.eks. samarbejdspartnere, leverandører o.a.

5. Sikkerhedsniveau

På baggrund af en konkret risiko- og konsekvensanalyse fastlægger Kalundborg Kommune et sikkerhedsniveau, der svarer til betydningen af den pågældende IT-anvendelse. Organisationen vil i de enkelte tilfælde fastlægge et sikkerhedsniveau, som modsvarer risici i forhold til konsekvenser.

6. Organisation og ansvar

Ansvars- og kompetencefordeling vedrørende IT-sikkerhed fastsættes i henhold til følgende:
Kommunalbestyrelsen har ansvar for godkendelse og vedligeholdelse af den overordnede IT-sikkerhedspolitik.
IT chefen er ansvarlig for indstillinger til Direktion og Kommunalbestyrelse.
IT chefen har ansvaret for godkendelse og vedligeholdelse af den operationelle IT-sikkerhedspolitk samt IT-beredskabsplan.
IT chefen har ansvaret for implementeringen af den overordnede og den operationelle IT-sikkerhedspolitik, sikkerhedsinstrukser og retningslinier.IT chefen behandler konkrete sager vedrørende IT-sikkerhedsforhold.
IT chefen udarbejder en årlig rapport til Økonomiudvalget.
IT udarbejder og vedligeholder, i samarbejde med systemejerne, en samlet ikt-beredskabsplan.
IT følger op på overholdelse af politikker og retningslinier gennem udførelse af kontroller.
IT chefen har endvidere ansvaret for at der er præventive og konsekvente foranstaltninger, som giver medarbejderne information og instruktion om den enkeltes medansvar for overholdelsen af sikkerhedsforanstaltningerne. IT chefen har endvidere ansvaret for de løbende IT-sikkerhedsmæssige opgaver samt udarbejdelse af udkast til retningslinier i henhold til IT-sikkerhedspolitikken.
IT chefen har ansvaret for behandling af dispensationer i forhold til IT-sikkerhedspolitikken.
IT chefen udpeger en daglig IT-sikkerhedsansvarlig, som bl.a. er ansvarlig for den daglige kontrol, opfølgning og rapportering.
Chefer/institutionsledere har indenfor eget område, ansvar for information om IT-sikkerhedspolitik, sikkerhedsinstrukser, underliggende retningslinjer samt opfølgning og kontrol.

7. Opfølgning

Økonomiudvalget behandler den årlige rapport om sikkerhedsforhold. IT chefen fastlægger procedurer for opfølgning vedrørende IT-sikkerhed.

8. Dispensationer

Dispensation fra denne politik behandles i henhold til særlige
retningslinier for dispensationer.

9. Overtrædelser

Overtrædelser af retningslinjer, instrukser og procedurer, som er udarbejdet i henhold til nærværende politik, behandles i henhold til kommunens personalepolitik og IT-sikkerhedsregler.

10. Ikrafttrædelse

Ovenstående IT-sikkerhedsbestemelser erstatter alle tidligere regler på området. IT-sikkerhedsbestemelserne/IT-sikkerhedshåndbogen er gældende fra den **01. 05. 2011**.
Revideret og godkendt af Kommunalbestyrelsen **26. marts 2014**