Informationssikkerhedspolitik for Syddjurs Kommune

Forord

Syddjurs Kommune definerer informationssikkerhed som værende den samlede mængde af foranstaltninger, der skal sikre beskyttelsen af informationer i kommunens varetægt. Borgere, medarbejdere og virksomheder har en forventning om, at informationer er let tilgængelige til korrekt sagsbehandling, og de har et krav om, at informationer behandles fortroligt.

Dette dokument beskriver informationssikkerhedspolitikken for Syddjurs Kommune. Hensigten med politikken er at tilkendegive over for alle med relation til Syddjurs Kommune, at anvendelse af informationer og informationssystemer er underkastet love, regler og etiske standarder. Informationer i såvel digital som fysisk form er omfattet.

Syddjurs Kommunes informationssikkerhedspolitik bygger på principperne i den internationale standard for informationssikkerhed, ISO27001, i henhold til aftale mellem kommunerne og regeringen. På områder, hvor der er specielle lovkrav, aftaleretlige eller andre forhold, skærpes kravene.

Gyldighed

Informationssikkerhedspolitikken omfatter den samlede anvendelse af informationer i Syddjurs Kommune. Politikken gælder for alle ansatte uden undtagelse, både fastansatte og personer, som midlertidigt er ansat i Syddjurs Kommune – herunder praktikanter, studiemedarbejdere og løntilskudsmodtagere – samt for politikere og samarbejdspartnere med adgang til Syddjurs Kommunes informationsaktiver.

Informationssikkerhedspolitikken og regler for informationssikkerhed skal – efter nærmere fastsatte regler – være tilgængelige for medarbejdere, politikere, samarbejdspartnere og virksomheder.

Omfang

Informationssikkerhedspolitikken udmøntes i *Regler for informationssikkerhed*, som udarbejdes efter principperne i ISO 27001. Reglerne beskriver det ønskede niveau for informationssikkerheden i Syddjurs Kommune og udarbejdes af informationssikkerhedsudvalget.

Ud fra *Regler for informationssikkerhed* skal fagchefer, system- og dataejere udarbejde relevante procedurebeskrivelser, så det daglige arbejde med kommunens informationer sker i overensstemmelse med det ønskede sikkerhedsniveau.

Fagchefer, system- og dataejere laver i samarbejde med Informationssikkerhedsudvalget løbende risikovurderinger af de væsentligste informationsaktiver. Risikovurderingerne udgør kommunens risikobillede.

Fagchefer, system- og dataejere udarbejder beredskabsplaner ud fra en risikovurdering. Planerne træder i kraft, hvis vigtige informationsaktiver bliver utilgængelige, kompromitteres eller lækkes.

Ovenstående skal indarbejdes i årshjul for løbende opfølgning og justering.

Hovedmålsætninger og sikkerhedsniveau

Syddjurs Kommune vil opretholde et effektivt værn mod informationssikkerhedsmæssige trusler. Det skal sikre borgernes rettigheder, ansattes trygheds- og arbejdsvilkår og Syddjurs Kommunes omdømme bedst muligt. Beskyttelsen skal omfatte såvel naturgivne som tekniske og menneskeskabte trusler af forsætlig eller tilfældig art.

De sikkerhedsmæssige tiltag skal beskytte Syddjurs Kommunes informationer og være med til at understøtte:

- Driftssikkerhed med høj oppetid og minimeret risiko for større nedbrud og datatab – også benævnt **tilgængelighed**
- Korrekt funktion og brug af informationsaktiver med minimeret risiko for manipulation af og fejl i såvel informationer og systemer – også benævnt **integritet**
- Behandling, transmission og opbevaring af data på en måde, så disse ikke gøres tilgængelige for uvedkommende – også benævnt **fortrolighed**

Informationssikkerhedspolitikken skal være med til at sikre, at Syddjurs Kommune overholder love, regler og etiske standarder.

Det samlede arbejde med informationssikkerhed skal sikre at såvel borgere, virksomheder og samarbejdspartnere som medarbejdere og politikere kan være trygge ved at Syddjurs Kommune håndterer informationer på lovlig og betryggende vis.

Endvidere skal regler og procedurer for informationssikkerhed tilrettelægges således, at der tages hensyn til medarbejdernes sikkerhed og rettigheder.

For at fastholde det tilstrækkelige sikkerhedsniveau i Syddjurs Kommune, skal følgende overholdes:

- Der skal være regler, procedurer og forretningsgange, som sikrer, at informationssikkerhed er en integreret del af driften og det daglige arbejde.
- Syddjurs Kommune skal gennem kontrakt- og leverandørstyring sikre, at brugen af eksterne konsulenter, samarbejdspartnere og leverandører lever op til kommunens niveau for informationssikkerhed.
- Der skal følges op på informationssikkerheden ved løbende at evaluere og vedligeholde informationssikkerhedspolitikken og de dertilhørende regler og procedurer. Målet er at sikre en struktureret og kontinuerlig forbedringsproces.

- Medarbejderne skal løbende uddannes i informationssikkerhed, så de har et vidensniveau, der er passende for deres arbejdsområde.

Organisation og ansvar

Byrådet har det politiske ansvar for informationssikkerheden i Syddjurs Kommune, og kommunaldirektøren har det øverste sikkerhedsansvar.

Byrådet vedtager nedsættelse af et informationssikkerhedsudvalg. Udvalgets opgave er at behandle sikkerhedsspørgsmål af principiel karakter og at fastsætte regler for målopfyldelsen af den informationssikkerhedspolitik, som Byrådet har vedtaget og udmeldt. Forretningsorden og kommissorium for udvalget vedtages af direktionen.

Informationssikkerhed er en integreret del af ledelsesansvaret og følger den decentrale model på alle ledelsesniveauer, svarende til den pågældende leders organisatoriske placering og ledelsesansvar.

Som en del af informationssikkerhedsarbejdet i Syddjurs Kommune, skal der udpeges system- og dataejere, som har ansvar for, at udarbejde relevante og aktuelle risiko- og konsekvensvurderinger af deres informationsaktiver.

Det er en leders opgave at orientere sine medarbejdere om informationssikkerhedspolitikkens regler, herunder om ansvarlighed i relation til Syddjurs Kommunes informationssystemer, og at følge i det daglige at informationssikkerheden overholdes.

Medarbejderne skal løbende holdes orienteret om væsentlige ændringer, der har indflydelse på informationssikkerheden. Det er desuden medarbejdernes ansvar at holde sig orienteret om informationssikkerhedspolitikkens regler og procedurer og på baggrund heraf udvise omhu i den daglige anvendelse af informationsaktiverne.

Risikovurderinger

Informationssikkerheden i Syddjurs Kommune skal være på et niveau, der tilgodeser lov- og myndighedskrav, kontraktlige forpligtelser, samt forpligtelser over for de borgere, virksomheder, medarbejdere og andre aktører, som kommunen håndterer informationer for og udveksler informationer med.

Syddjurs Kommune forholder sig aktivt til trusler mod informationssikkerheden og iværksætter realistiske og tilstrækkelige handlinger for at sikre et tilstrækkeligt sikkerhedsniveau.

Væsentlige informationsaktiver skal risikovurderes mindst én gang årligt. Risikovurderingen skal fastlægge det ønskede sikkerhedsniveau med udgangspunkt i informationsaktivets betydning i forhold til tilgængelighed, fortrolighed og integritet.

Ledelsen deltager aktivt i risikovurderingen og er ansvarlig for at vurdere trusler, konsekvenser og risici mod informationsaktiverne.

Med udgangspunkt i risikovurderingen, prioriterer ledelsen de nødvendige foranstaltninger for at sikre, at Syddjurs Kommune fastholder det ønskede niveau for informationssikkerhed.

Såfremt der indtræffer en alvorlig informationssikkerhedshændelse, er det Informationssikkerhedsudvalgets ansvar, at der foretages en vurdering af hændelsens årsag, samt en vurdering af, om dette giver anledning til at iværksætte sikkerhedsmæssige tiltag.

Risikovurderingen opdateres mindst én gang årligt, samt ved eventuelle større ændringer i opgaver, leverandører, it-systemer eller anvendelsen heraf.

Overtrædelse af informationssikkerhedspolitikken

Alle medarbejdere i Syddjurs Kommune er forpligtet til at efterleve den gældende informationssikkerhedspolitik med tilhørende regler, forretningsgange og procedurer. En overtrædelse kan – efter omstændighederne – medføre sanktioner.

Såfremt en medarbejder opdager trusler mod informationssikkerheden eller brud på denne, skal det straks rapporteres til nærmeste leder, som herefter vurderer, hvordan situationen skal håndteres.

Godkendelse

Informationssikkerhedsudvalget udarbejder og vedligeholder Informationssikkerhedspolitikken og indstiller politikken til godkendelse i Byrådet.

Informationssikkerhedspolitikken skal revurderes, hvis der sker væsentlige ændringer i den kommunale organisation, lovgivning eller eventuelt trusselsniveau.

Denne informationssikkerhedspolitik er godkendt af Byrådet den 30. maj 2018 og er gældende fra den 30. maj 2018.