Samsø Kommune

INFORMATIONSSIKKERHEDSPOLITIK

Version: 2.0

Godkendt d. 25/04-2023

INDLEDNING

Informationssikkerhedspolitikken i Samsø Kommune fastlægger den overordnede ramme for beskyttelsen af kommunens informationsaktiver og it-systemer, herunder placeringen af ansvaret for kommunens it-sikkerhedsindsats.

Politikkens bestemmelser er udarbejdet med afsæt i:

- Principperne i ISO27001 – en international sikkerhedsstandard, som kommunerne i henhold til den fællesoffentlige digitaliseringsstrategi er forpligtede til at følge
- EU´s databeskyttelsesforordning (GDPR) og de afledte nationale lovgivninger på området
- Anden lovgivning hvor det er relevant for informationssikkerheden

Kommunen behandler og opbevarer en stor mængde data og viden - herunder både almindelige og følsomme personoplysninger. Disse data og denne viden kaldes under ét for kommunes informationsaktiver. Det kræver en særlig indsats at sikre disse informationsaktivers fortrolighed, integritet og tilgængelighed, ligesom det er af afgørende betydning for Samsø Kommune, at borgere, virksomheder og den øvrige offentlige sektor har tillid til, at den nødvendige sikkerhed bliver opretholdt omkring håndteringen af de informationsaktiver, der er i kommunens varetægt.

Beskyttelse af informationsaktiver og IT-systemer er derfor et vigtigt fokusområde, der håndteres gennem kommunens ledelsessystem for informationssikkerhed (ISMS), der udgør det samlede udtryk for de politikker, procedurer, processer, organisatoriske beslutningsgange og aktiviteter Samsø Kommune har implementeret for at sikre en velafstemt og risikobaseret tilgang til det informationssikkerhedsmæssige arbejde.

FORMÅL OG PRINCIPPER

Formålet med Samsø Kommunes informationssikkerhedspolitik er at definere og fastlægge de overordnede principper for beskyttelse af kommunens informationsaktiver og IT-systemer. Politikken skal udmøntes gennem implementering af sikkerhedsforanstaltninger, der fastlægges på baggrund af risikovurderinger. Disse skal foretages med henblik på at sikre et passende sikkerhedsniveau for de behandlede informationsaktiver og systemer med udgangspunkt i tre centrale begreber:

- **Fortrolighed**, så information ikke kommer til uvedkommendes kendskab
- **Integritet**, så information forbliver pålidelig, korrekt og intakt

- **Tilgængelighed**, så relevant information kan tilgås og anvendes, når og hvor der er behov for det

Den overordnede hensigt med informationssikkerhedsarbejdet er således at sikre, at:

- kommunens it-infrastruktur til stadighed er driftssikker og effektivt beskyttet mod interne og eksterne trusler herunder angreb på it-systemer som fx hacker- og virusangreb og misbrug af rettigheder (Fortrolighed, Integritet)
- oplysninger om borgere og virksomheder til enhver tid er beskyttet mod uberettiget videregivelse, hændelige uheld eller forsætlige handlinger (Fortrolighed)
- at informationsaktiver til enhver tid er tilgængelige for både interne og eksterne interessenter, med hjemmel til og behov for at få adgang hertil (Tilgængelighed)
- regler for god sikkerhedsskik (best practice), herunder principper og normer for adfærd i omgang med informationsaktiver og anvendelsen af kommunens IT-systemer, er klart formuleret og formidlet til medarbejderne (Fortrolighed, Integritet)
- der er udarbejdet en beredskabsplan, der sikrer, at driften kan genoptages hurtigst muligt efter et nedbrud eller sikkerhedsbrud, og at konsekvenserne heraf reduceres mest muligt (Fortrolighed, Integritet, Tilgængelighed)

OMFANG

Informationssikkerhedspolitikken omfatter enhver form for informationsaktiver, der ejes, opbevares eller behandles af kommunen og kommunens databehandlere. Dette gør sig gældende uanset hvilket medie, informationsaktivet er lagret på og uanset hvordan informationsaktivet fremstår f.eks. elektronisk, papirbaseret, i tale, transmitteret eller filmisk form.

Informationssikkerhedspolitikken er gældende for alle, der udfører opgaver eller hverv for kommunen, herunder:

- Ansatte, både fastansatte, midlertidigt ansatte, vikarer og lign.
- Medlemmer af kommunalbestyrelsen
- Eksterne samarbejdspartnere, f.eks. personer og virksomheder, der udfører opgaver for kommunen

Kommunens informationssikkerhedspolitik gælder for alle lokaliteter, hvor der sker en anvendelse og bearbejdning af kommunens informationsaktiver fx på rådhus, institutioner, hjemmearbejdspladser eller adgang via mobil. Kommunens informationssikkerhedspolitik

gælder også på lokaliteter for eksterne samarbejdspartnere og virksomheder, der behandler eller er i besiddelse af kommunens informationsaktiver, medmindre der er indgået særskilt aftale herom i databehandleraftaler (eller andre samarbejdsaftaler) for de specifikke behandlingsaktiviteter.

ORGANISATION OG ANSVAR

Det er en ledelsesmæssig opgave at sikre informationssikkerheden i Samsø Kommune. Derfor er ansvaret entydigt forankret i kommunes kommunalbestyrelse og kommunens informationssikkerhedsudvalg, der består af kommunaldirektøren og kommunens forvaltningschefer.

- Kommunalbestyrelsen – fastlægger de overordnede rammer for informationssikkerheden gennem revision og godkendelse af Informationssikkerhedspolitikken (dette dokument).
- Kommunaldirektøren - er kommunens øverste administrative sikkerhedsansvarlige og udgør sammen med den øvrige chefgruppe kommunens informationssikkerhedsudvalg. Kommunaldirektøren har det overordnede ansvar for, at opgaverne i kommunens informationssikkerhedsarbejde bliver løst i overensstemmelse med de bestemmelser, der er fastlagt i nærværende informationssikkerhedspolitik og relevant lovgivning i øvrigt. Det er også kommunaldirektøren, der som formand for Informationssikkerhedsudvalget rapporterer på informationssikkerhedsudvalgets arbejde overfor kommunalbestyrelsen, når og hvor det er relevant.
- Chefgruppen – udgør sammen med kommunaldirektøren kommunens informationssikkerhedsudvalg, der er ansvarligt for udarbejdelse af (samt opfølgning på) kommunens informationssikkerhedspolitik og hertil understøttende retningslinjer, håndbøger, procedurer og vejledninger. Informationssikkerhedsudvalget indstiller kun væsentlige ændringer i Informationssikkerhedspolitikken til kommunalbestyrelsens godkendelse. Dette kan fx være ved ændringer i formål, principper, omfang samt organisering af og ansvar for informationssikkerhedsarbejdet. Ændringer af administrativ karakter kan godkendes i Informationssikkerhedsudvalget. Det er til enhver tid kommunaldirektøren i sin egenskab af formand for Informationssikkerhedsudvalget der afgør hvilke ændringer, der kræver kommunalbestyrelses godkendelse. Chefgruppen har også (qua deres rolle som systemejere) ansvaret for udarbejdelse og vedligehold af risikovurderinger for IT-systemer og processer, der omfatter behandling eller lagring af informationsaktiver. Det er også informationssikkerhedsudvalgets ansvar at beslutte og iværksætte initiativer til at håndtere og/eller imødegå kritiske og/eller omfattende

sikkerhedshændelser. Informationssikkerhedsudvalget kan beslutte helt eller delvist at uddelegere sine opgaver rent operationelt, men kan ikke uddelegere ansvaret herfor.

- Informationssikkerhedskoordinatoren – er sekretær for Informationssikkerhedsudvalget og facilitator af kommunens informationssikkerhedsarbejde samt støtter systemejere i den operationelle udførelse af tiltag og aktiviteter, der udspringer af informationssikkerhedsarbejdet (jf. informationssikkerhedsudvalgets årshjul/årsplan).
- Databeskyttelsesrådgiveren (DPO) – har primært en rådgivende funktion i informationssikkerhedsarbejdet. Det er således DPO'ens ansvar at rådgive, vejlede og overvåge, hvordan og om kommunen efterlever GDPR, samt at sikre afrapportering herom til kommunens øverste ledelse (kommunalbestyrelsen samt Informationssikkerhedsudvalget). Dertil bistår DPO'en med den lovpligtige indhentning af databehandleraftaler (samt tilsynet hermed), samt varetager DPO'en rollen som kontaktperson for kommunens borgere ift. GDPR relaterede spørgsmål og forespørgsler.
- Den IT-ansvarlige – har det operationelle ansvar for kommunens samlede IT-drift og -infrastruktur. Den IT-ansvarlige er derudover informationssikkerhedsudvalgets rådgiver ift. kortlægning af risici og konsekvenser ifm. indkøb og anvendelse af informationsteknologi.
- Øvrige ledere – har til ansvar at tilse, at kendskabet til den informationssikkerhedsmæssige ramme og konsekvens er kendt blandt eget personale (og hvor det er relevant også eksterne samarbejdspartnere), samt at sikre efterlevelsen af relevante retningslinjer, instrukser og procedurer herunder. Dertil vil ledere også i eventuelt uddelegerede roller som systemejere skulle bidrage til udformning og vedligehold af risikovurderinger herfor.
- Alle medarbejdere, politikere og eksterne konsulenter - har til ansvar at kende og efterleve Informationssikkerhedspolitikken og dens udmøntning i relevant omfang, samt løbende at deltage i awareness- og uddannelsesaktiviteter i samme kontekst.

IT-RISIKOVURDERING OG -HÅNDTERING

Samsø Kommune fastlægger på baggrund af konkrete risikovurderinger et sikkerhedsniveau, der indfrier de forventninger til troværdighed og stabilitet, der er til behandling af data i en offentlig myndighed.

Sikringen skal stå mål med risikoen, og derfor skal kommunen ikke sikre sig for enhver pris - men være bevidst om enhver risiko.

Sikkerhedsniveauet og anvendelsen skal til enhver tid tilgodese lov- og myndighedskrav, anerkendte standarder for informationssikkerhed (ISO 27001/27002), anbefalinger på området ("Best practice") samt udmeldinger og afgørelser fra Datatilsynet.

Der skal kontinuerligt foretages risikovurderinger. Ledelsen skal deltage aktivt i risikovurderingerne, idet de er ansvarlige for at vurdere trusler, konsekvenser og risici af it-systemer og behandlingsaktiviteter. Som minimum gennemføres/revideres risikovurderinger af kritiske it-systemer en gang årligt samt ved større ændringer i systemanvendelsen eller ved leverandørskifte.

Kommunens informationsaktiver og IT-systemer skal identificeres og klassificeres. Dette skal sikre det korrekte sikkerhedsniveau i forhold til systemer og datas fortrolighed, integritet og tilgængelighed.

SIKKERHEDSBEVIDSTHED

Alle, som har adgang til, anvender eller behandler informationsaktiver i Samsø Kommune har et medansvar for, at informationsaktiver og IT-systemer beskyttes optimalt mod uautoriseret adgang, ændring, ødelæggelse og tyveri.

For at sikre et kontinuerligt højt bevidsthedsniveau, så skal alle ansatte løbende modtage relevant uddannelse eller træning i databeskyttelse og informationssikkerhed.

DISPENSATIONER

I det omfang der er akut behov for at fravige specifikke krav i Informationssikkerhedspolitikken, er det alene kommunaldirektøren, der kan bemyndige dette. Det påhviler kommunaldirektøren at informere kommunalbestyrelsen og Informationssikkerhedsudvalget herom, samt at tilse at et evt. behov for at tilpasse Informationssikkerhedspolitikken behandles senest ved næste revision af Informationssikkerhedspolitikken.

OVERTRÆDELSER

Bevidste eller ubevidste overtrædelser af kommunens informationssikkerhedspolitik kan få den konsekvens, at borgernes personoplysninger bliver kompromitteret. En anden konsekvens kan være, at der opleves ustabilitet/uhensigtsmæssigheder i anvendelse og bearbejdning af kommunens informationsaktiver. Dette kan i værste fald medføre økonomisk tab for kommunen eller en forringelse af den kommunale service eller kommunens omdømme.

Hvis en trussel mod informationssikkerheden eller brud på denne opdages, skal disse hændelser straks meddeles til kommunens sikkerhedsansvarlige i henhold til gældende procedure (typisk kommunens DPO og/eller IT-ansvarlige).

Sikkerhedsbrud indgår i rapporteringen til Informationssikkerhedsudvalget.

Hændelser, der kræver presseomtale, håndteres af Informationssikkerhedsudvalget.

Overtrædelser af kommunens informationssikkerhedspolitik eller andre bestemmelser, der er udmøntet heraf, vil blive behandlet af Informationssikkerhedsudvalget afhængig af karakteren af overtrædelsen og kan få ansættelsesmæssige konsekvenser.

GODKENDELSE OG KOMMUNIKATION

Denne informationssikkerhedspolitik er senest revideret d. 6/12-2022 og godkendt af kommunalbestyrelsen d. 25/4-2023.

Informationssikkerhedspolitik offentliggøres på kommunens hjemmeside www.samsoe.dk.