Skanderborg Kommune

Overordnet standard for informationssikkerhed

i Skanderborg Kommune

Version 1.0

Januar 2021

Skanderborg Kommune

Indhold

Indledning

Skanderborg Kommune behandler store mængder data – herunder såvel almindelige som følsomme og fortrolige personoplysninger. Disse informationer kræver en særlig beskyttelse for at bibeholde fortrolighed, integritet og tilgængelighed. Det er af afgørende betydning, at borgere, samarbejdspartnere, medarbejdere og den øvrige offentlige sektor har tillid til, at den nødvendige sikkerhed bliver opretholdt.

Beskyttelse af informationer og teknologi er derfor et vigtigt fokusområde, der håndteres via indsatser på alle niveauer af organisationen. Indsatserne består af såvel organisatoriske som tekniske sikkerheds-foranstaltninger.

Standarden for informationssikkerhed fastlægger den overordnede ramme for beskyttelse af information og informationsteknologi i Skanderborg Kommune.

Standardens bestemmelser er udarbejdet med afsæt i principperne i den internationale informationssikkerheds-standard ISO 27001, som kommunerne i henhold til den fællesoffentlige digitaliseringsstrategi 2016-2020 er forpligtede til at følge, samt i EU´s databeskyttelsesforordning (GDPR) og de afledte nationale lovgivninger på området.

Retningslinjer for informationssikkerhed er nærmere uddybet i:

- Informationssikkerhedsorganisationen, der definerer placering af roller og ansvar.
- De uddybende informationssikkerhedsregler, der fastlægger rammer for og organisering af informationssikkerheden.
- De konkrete retningslinjer hvor sikkerhedsreglerne er omsat til praksis og udmøntet i sikkerhedshåndbøger, procedurer, instrukser og vejledninger.

Sikkerhedsorganisationen og de uddybende sikkerhedsregler revideres ved behov inden for rammerne af den overordnede standard.

Formål og principper

Formålet med Skanderborg Kommunes standard for informationssikkerhed er at definere og fastlægge de overordnede principper for beskyttelse af kommunens data og informationssystemer.

Standarden 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 data 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 der er behov for det.

Dette skal søges opnås ved 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.
- oplysninger om borgere, virksomheder og medarbejdere til enhver tid er beskyttet mod uberettiget videregivelse, hændelige uheld eller ondsindede handlinger.
- reglerne for god sikkerhedsskik, herunder principper og normer for adfærd i anvendelsen af kommunens informationssystemer, er klart formuleret og formidlet til medarbejderne.
- beredskabsplaner sikrer, at driften kan genoptages hurtigst muligt efter et nedbrud, og at konsekvenserne af et sikkerhedsbrud reduceres mest muligt.

Omfang

Kommunens informationssikkerhedsstandard omfatter enhver form for data, der ejes, opbevares eller behandles af kommunen og kommunens databehandlere. Dette gør sig gældende uanset hvilket medie, informationen er lagret på, og uanset hvordan data fremstår eksempelvis elektronisk, papirbaseret, i tale, transmitteret eller filmisk form.

Standarden er gældende for alle, der udfører opgaver eller hverv for kommunen, herunder ansatte, såvel fastansatte, midlertidigt ansatte som vikarer, konsulenter og lignende samt eksterne samarbejdspartnere.

Standarden gælder for alle lokaliteter, hvor der sker en anvendelse og bearbejdning af kommunens informationer, fx på rådhus, institutioner, hjemmearbejdspladser eller mobil adgang.

Sikkerhedsniveau

Skanderborg 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, anbefalinger på området samt udmeldinger og afgørelser fra Datatilsynet, Center for Cybersikkerhed og lignende instanser.

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 andre relevante områder. Som minimum gennemføres risikovurderinger af kritiske it-systemer en gang årligt samt ved ibrugtagning og større ændringer i systemanvendelsen eller ved leverandørskifte.

Kommunens systemer og data 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 data i Skanderborg Kommune har et medansvar for, at data og systemer beskyttes optimalt mod uautoriseret adgang, ændring, ødelæggelse og tyveri.

For at sikre et kontinuerligt højt bevidsthedsniveau, skal alle ansatte løbende modtage relevant kompetenceudvikling vedrørende databeskyttelse og informationssikkerhed.

Organisation og ansvar

Det er en ledelsesmæssig opgave at sikre informationssikkerheden i Skanderborg Kommune. Derfor er ansvaret entydigt forankret hos kommunens ledelse på lige fod med ansvaret for eksempelvis økonomi og personale.

Byrådet har ansvar for at fastlægge de overordnede rammer for informationssikkerhedsarbejdet. Rammerne fastlægges i informationssikkerhedsstandarden.

Kommunaldirektøren er den øverst sikkerhedsansvarlige og har i samarbejde med direktionen det overordnede ansvar for, at informationssikkerhedsopgaverne i kommunen bliver løst i overensstemmelse med de bestemmelser, der er fastlagt i standarden. Direktionen skal sikre overordnet prioritering og ressourcetildeling.

Informationssikkerhedsgruppen etablerer, implementerer, vedligeholder og forbedrer ledelsessystemet for sikkerhedsarbejdet. Gruppen modtager løbende status på arbejdet og tager beslutninger om tekniske og organisatoriske foranstaltninger og konkrete retningslinjer, der angår hele organisationen.

Digitaliserings- og It-chefen er ansvarlig for den daglige operationelle ledelse af informationssikkerhedsarbejdet herunder at sikre en prioritering og opfølgning på de opgaver, der er forbundet hermed.

Informationssikkerhedskoordinatoren og IT-sikkerhedskonsulenten er de udførende funktioner og varetager den daglige opgaveløsning for informationssikkerhedsarbejdet på foranledning af Digitaliserings og It-chefens retningslinjer.

Databeskyttelsesrådgiveren (DPO) har en rådgivende funktion i informationssikkerhedsarbejdet. DPO'ens funktion består i at rådgive, vejlede og overvåge, at organisationen efterlever reglerne om databeskyttelse samt at sikre afrapportering herom til kommunens øverste ledelse.

Alle ansatte er ansvarlige for at tilegne sig tilstrækkelig viden til at kunne efterleve retningslinjer og procedurer for sikkerhed i det daglige arbejde samt at rapportere risici og sikkerhedshændelser.

Evaluering og opfølgning

Informationssikkerhedskoordinatoren og IT-sikkerhedskonsulenten følger kontinuerligt og systematisk op på arbejdet med databeskyttelse og informationssikkerhed. Den interne kontrol skal sikre, at sikkerhedsretningslinjerne er velimplementerede i organisationen, og at ansvar og regler overholdes. En gang årligt får direktionen en statusopdatering på det samlede risikobillede med henblik på drøftelse og prioritering af eventuelle ændringstiltag.

Derudover udarbejder den eksterne databeskyttelsesrådgiveren en årlig afrapportering til byrådet om kommunens efterlevelse af databeskyttelseskravene og anbefalinger til forbedringer.

Outsourcede informationssikkerhedsprocesser styres via databehandleraftaler og tilsyn med databehandlere og it-leverandører.

Informationssikkerhedspolitikken revideres efter behov. Kommunaldirektøren har det overordnede ansvar for, at der sker en løbende ajourføring af de uddybende informationssikkerhedsregler og tilhørende bilag. Opgaven er i praksis uddelegeret til Digitaliserings- og It-chefen, der skal sikre ajourføring ved større ændringer i informationsbehandlingen. Ajourføring skal dog som minimum foretages hvert andet år med henblik på at sikre en struktureret og kontinuerlig forbedringsproces.

Sikkerhedsbrud og overtrædelser

Bevidste eller ubevidste overtrædelser af kommunens informationssikkerhed 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 informationer. Dette kan i værste fald medføre konsekvenser for de berørte registrerede personer, økonomisk tab for kommunen eller en forringelse af den kommunale service eller kommunens omdømme.

Såfremt en trussel mod informationssikkerheden eller brud på denne opdages, skal dette straks meddeles til nærmeste leder og It/Digitaliserings-afdelingen i henhold til gældende procedure. Sikkerhedsbrud indgår i rapporteringen til kommunens øverste sikkerhedsansvarlige.

Hændelser, der kræver presseomtale, håndteres af It- og Digitaliseringschefen i samarbejde med kommunaldirektøren, relevant koncernchef og kommunikationsafdelingen.

Overtrædelser af kommunens informationssikkerhedsregler eller andre bestemmelser, der er udmøntet heraf, vil blive behandlet af ledelsen afhængig af karakteren af overtrædelsen.

Offentliggørelse

Standarden skal formidles til alle relevante interessenter herunder samtlige medarbejdere i kommunen og offentliggøres på www.Skanderborg.dk.

Digitaliserings- og It-chefen kan give tilladelse til, at der bliver udleveret eller offentliggjort andet materiale vedrørende informationssikkerheden.