Standard for Informationssikkerhed

Vejen Kommune

Denne standard er godkendt af Byrådet d. 11.10.2022.
Seneste version er tilgængelig på kommunens hjemmeside.

Indledning

Vejen Byråd fastlægger med denne Standard for informationssikkerhed principper for opretholdelse af informationssikkerhed i Vejen Kommune.

Standarden skal sikre, at kommunens informationssikkerhed til stadighed overholder alle lovmæssige krav og opfylder såvel egne som eksterne interessenters krav.

Sikkerheden omkring informationsaktiviteterne er afgørende for kommunens daglige drift og målsætninger.

Effektiviseringer og kvalitetsforbedringer baseres i stadig højere grad på digitale løsninger. Det gælder både velfærd, administrative processer og borgerservice. Dermed er risikobilledet i konstant forandring, og det stiller krav om, at kommunen kontinuerligt tilpasser informationssikkerheden.

Hvis informationssikkerheden er utilstrækkelig, kan det skade kommunens omdømme og medføre, at effektiviseringer og kvalitetsforbedringer må opgives. I nogle tilfælde kan brud på informationssikkerhed også få menneskelige konsekvenser. Informations-sikkerhed har således i mere end én forstand vital betydning for kommunen.

Informationssikkerheden er beskrevet i følgende dokumenter:

- En overordnet "Standard for informationssikkerhed" (dette dokument), der beskriver rammer, mål og overordnet organisering af informationssikkerhedsindsatsen.
- En "Operationel standard for informationssikkerhed", hvor organisering, ansvar og roller, samt informationssikkerhedsstrategien er præciseret.
- Og "Retningslinjer for IT-drift", med konkrete regler og retningslinjer som alle medarbejdere skal følge.

NASA og informationssikkerhed

Både "Standard for informationssikkerhed" og "Operationel standard for informations-sikkerhed" har sammenhæng til kommunes værdier på følgende måde:

N	Nytænkning	Vi risikovurderer, når vi udtænker nye digitale løsninger og ændrer arbejdsgange. Vi udfordrer synet på informationssikkerheden, når den begrænser nytænkning og effektivitet
A	Anerkendelse	Vi anerkender, at en sikkerhedsbevidst kultur kræver indsigt, forståelse og viden hos medarbejdere på alle niveauer.

S	Sammenhæng	Informationssikkerhed er som kæde, der skal holde på tværs af systemer afdelinger og arbejdsgange. Vi ser system- og datasikkerhed som en del af digital ledelse
A	Ansvarlighed	Borgere og virksomheder skal kunne være trygge ved at videregive oplysninger til kommunen, at kommunens services fungerer tilfredsstillende og at afgørelser er korrekte. Vi følger udviklingen i risikobilledet og sikrer, at informationssikkerhedsindsatsen er tilpasset hertil

Omfang

"Standard for informationssikkerhed" gælder for alle afdelinger, institutioner i Vejen Kommune samt politikere, eksterne konsulenter, samarbejdspartnere og leverandører.

Skoleområdet, biblioteksområdet og andre relevante områder skal selv fastlægge en standard for eksterne brugeres (elever, borgere mv.) anvendelse af it-udstyr og it-tjenester, som området stiller til rådighed uden for det administrative net.

Ved udlicitering af it-drift til eksterne serviceleverandører, deltagelse i it-driftsfællesskaber, private aktørers adgang til informationer mv. skal det sikres, at Vejen Kommunes sikkerhedsniveau opretholdes.

Grundprincipper for informationssikkerhed i Vejen Kommune

Vejen Kommune fastlægger på baggrund af en risikovurdering et sikkerhedsniveau, som svarer til betydningen af de pågældende data.

Standarden for informationssikkerhed tager udgangspunkt i god it-skik, bedste praksis og standarder og retningslinjer på området samt lovgivning inden for datasikkerhed.

Vejen Kommune arbejder efter principperne i ISO27001/2, som er en standard, der beskriver, hvorledes it-sikkerhed implementeres og styres i en organisation, og som anvendes bredt i den offentlige sektor.

Mål

Vejen Kommunes informationssikkerhedsniveau opfylder følgende overordnede mål:

Overholdelse af lovgivning og eksterne krav. Informationsanvendelse skal overholde gældende lovgivning og eksterne krav.

Sikkerhedskultur og -bevidsthed. Ledere og medarbejdere skal kende de risici, som de har indflydelse på. Det er vigtigt, at medarbejdere kender deres ansvar og kun

behandler informationer, som de aktuelt har behov for til løsning af den konkrete opgave. Ledere skal kende risikoen på deres område og har ansvaret for medarbejderes forståelse af risici og efterlevelse af forholdsregler.

Sikker drift. Der skal opretholdes et stabilt, sikkert, let tilgængeligt og funktionelt it-serviceniveau, hvor data er tilgængelige og beskyttet efter følsomhed og betydning for kommunen og for registrerede. Afdelingerne skal kunne stole på, at it-services, der etableres og leveres af IT og Digitalisering, er tilgængelige og beskyttet efter afdelingernes behov.

Adgang og rettigheder til data og systemer. Følsomme og kritiske systemer og data skal beskyttes mod uautoriseret adgang og ændring, uanset hvor de er, og uanset hvorfra de tilgås. Adgang til og ændring af følsomme eller kritiske systemer eller data skal let kunne spores til personen.

Projekter. Projekter, herunder anskaffelse, udvikling og vedligeholdelse af it-systemer, må ikke svække sikkerhedsniveauet.

Fysisk sikkerhed. De fysiske omgivelser for informationer og informationsudstyr, der anvendes af kommunen, og som kommunen har ansvaret for, skal beskyttes mod fysiske hændelser, eksempelvis brand, vandskade, tyveri, hærværk, skader forårsaget af menneskelige fejl mv. Driftsmiljøet og vigtige arbejdsgange skal kunne videreføres inden for en realistisk tidshorisont, der besluttes af ledelsen.

Håndtering af sikkerhedshændelser. Der skal ske en systematisk registrering af hændelser og etableres et beredskab, så skaden for kommunen og for registrerede ved kritiske hændelser holdes på et minimum.

En beskrivelse af, hvordan de enkelte ovenstående mål opnås, fremgår af den operationelle standard for informationssikkerhed.

Organisation og ansvar

Alle kommunens ansatte har et medansvar for opretholdelse af den generelle informationssikkerhed. Ansvaret for informationssikkerhed i Vejen Kommune skal være præcist og entydigt beskrevet med udgangspunkt i nedenstående overordnede organisering.

- **Byrådet** godkender den overordnede "Standard for informationssikkerhed" efter indstilling fra direktionen.

- **Kommunaldirektøren** er den øverste informationssikkerhedsansvarlige. Kommunaldirektøren er formand for Informationssikkerhedsudvalget.

- **Direktionen** har det overordnede ansvar for effekten af den tværgående indsats, herunder at standarder og beslutninger er kendt på alle ledelsesniveauer, samt at standarder er afstemt til det aktuelle behov. Direktionen behandler og godkender Operationel standard for informationssikkerhed samt de tilhørende retningslinjer.

- **Informationssikkerhedsudvalget** skal sikre koordinering og sammenhæng på tværs af afdelingerne i relation til informationssikkerhed, herunder sætte mål for informationssikkerheden, sørge for, at informationssikkerheden realiseres og efterleves i organisationen, og prioritere indsatser med, henblik på at styrke informationssikkerheden herunder håndtering af risikovurdering.

- **Afdelingscheferne** er systemejere og har det delegerede ansvar for informationssikkerheden inden for eget område. Dermed har de ansvaret for efterlevelse af standarder og retningslinjer, herunder koordinering med andre enheder i kommunen. Afdelingscheferne skal kende den informationssikkerheds-mæssige udfordring i egen afdeling, træffe de nødvendige foranstaltninger og foretage ledelsestilsyn.

- **Afdelingschefen for Økonomi** servicerer og rådgiver direktionen og kommunens afdelinger om informationssikkerhed. Det er afdelingschefens ansvar, at aktiviteterne er sammenhængende. Informationssikkerheds-koordinatoren understøtter afdelingschefen i arbejdet med informations-sikkerhed i samarbejde med Databeskyttelsesrådgiveren. Afdelingschefen er desuden overordnet ansvarlig for indkøb, kontrakter og implementeringer af centrale it-løsninger, og er systemejer for tværgående it-systemer. Afdelingschefen har også det overordnet ansvar for behandling og indstilling i sager vedrørende informationssikkerhed til henholdsvis Informationssikkerhedsudvalg og Direktionen. Afdelingschefen er medlem af Informationssikkerhedsudvalget.

- **Afdelingschefen for Teknik & Miljø er** ansvarlige for adgangskontrol-systemet til rådhus, områdekontorer og andre bygninger med administrativt personale, herunder alarmsystemer med ekstern vagtordning. Desuden it-sikkerhedsmæssige forhold vedrørende daglig drift (kantine, budtjeneste, fysisk postfordeling mv.), lokaleforsyning og lokaleindretning (herunder vedligehold og ombygning) på rådhuset.

- **Leder af IT og Digitalisering** er ansvarlig for, at it-driften lever op til standarden for informationssikkerhed og det sikkerhedsniveau, der er aftalt

med afdelingerne. Leder af IT og Digitalisering er medlem af Informationssikkerhedsudvalget og IT-koordineringsgruppen.

- Alle **ledere** har ansvar for, at kravene til informationssikkerhed i lederens ansvarsområde er klart kommunikeret til medarbejderne, og for at følge op på efterlevelsen af kravene

- **Databeskyttelsesrådgiver (DPO)** skal rådgive, underrette og overvåge om overholdelse af lovkrav vedrørende datasikkerhed. DPO'en skal understøtte, at de dataansvarlige overholder reglerne i databeskyttelsesforordningen. DPO'en referer til kommunaldirektøren og afrapporterer til byrådet. DPO'en er medlem af Informationssikkerhedsudvalget og IT-koordineringsgruppen

- **Informationssikkerhedskoordinatoren** yder rådgivning til organisationen i relation til informationssikkerhed, herunder at udarbejde en Informationssikkerhedsrapport og årshjul for informationssikkerhed, som godkendes i Informationssikkerhedsudvalget. Informationssikkerheds-koordinatoren er medlem af Informationssikkerhedsudvalget og varetager sekretærfunktionen.

- **IT-koordineringsgruppen** understøtter organisation ved at rådgive og bistå systemejerne og andre nøglepersoner i forbindelse med systemanskaffelse og it-projekter.

- **Indkøb** er overordnet ansvarlig for Vejen kommunes system- og kontraktporteføljestyring.

Evaluering og opfølgning

Informationssikkerhedskoordinatoren leverer en årlig status på målsætninger, et opdateret risikobillede og forslag til ny årsplan, til Informationssikkerhedsudvalget.

Som led i databeskyttelsesrådgiverens arbejde aflægger denne én gang årligt rapport til byrådet om kommunens efterlevelse af databeskyttelseskravene og anbefalinger til forbedringer.

Databeskyttelsesrådgiveren rapporterer til informationssikkerhedsudvalget vedrørende brud på persondatasikkerheden, som årligt samler op på bruddene.

Den overordnede standard for informationssikkerhed revideres og godkendes på ny, når et nyt byråd er konstitueret efter et kommunalvalg.

Den operationelle standard for informationssikkerhed revideres ved større ændringer i organisationen og mindst en gang årligt.