Standard for Informationssikkerhed

Vejen Kommune

Denne politik er godkendt af Byrådet d. 13.03.2018.
Seneste version er tilgængelig på intranettet.

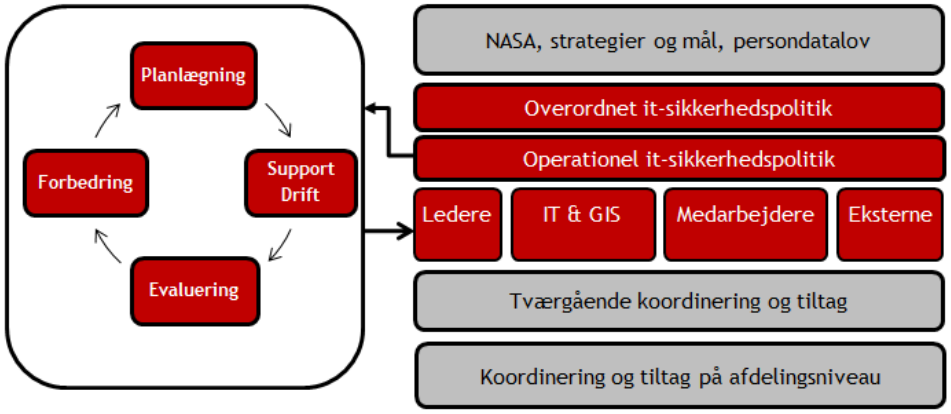
Indledning

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

Formålet med politikken er at fastlægge principperne for styring af informationssikkerhed, så risikoen holdes på et acceptabelt niveau.

Politikkens opbygning

Politikken er opdelt i tre niveauer:



Den overordnede politik (dette dokument) beskriver rammer, mål og overordnet organisering af informationssikkerhedsindsatsen. Den overordnede politik vedtages af byrådet.

Den operationelle politik præciserer organisering, ansvar og roller, herunder hvem der løser hvilke opgaver. Den operationelle politik godkendes af direktionen.

Retningslinjer for Ledere, IT & GIS, Medarbejdere og Eksterne uddyber kravene til risikohåndtering på udvalgte områder. Retningslinjer fastlægges i relevante ledelsesfora og med inddragelse af afdelinger og interessenter.

Formål

Politikkens formål er at etablere en fornuftig balance mellem sikker drift og udnyttelse af digitaliseringsmuligheder, samt at sikre efterlevelsen af persondataloven, som fra den 25. maj 2018 erstattes af databeskyttelsesforordningen og databeskyttelsesloven. Frem for alt skal politikken sikre, at indsatsen prioriteres efter den aktuelle risiko.

Det er et krav i databeskyttelsesforordningen[1], at kommunen fastlægger en politik og retningslinjer for beskyttelse af personoplysninger. Da kommunens informations- og

- [1]Justitsministeriets betænkning nr. 1565 om databeskyttelsesforordningen

systemanvendelse desuden er omfattende og kompleks, og da kommunen er meget afhængig af it-understøttelsen, er der behov for at fastlægge nogle rammer, som sikrer en systematik og et acceptabelt niveau.
Eksempelvis kan offentliggørelse af følsomme eller fortrolige oplysninger få alvorlige konsekvenser for borgere, erhvervsliv og ansatte.
Tilsvarende kan datatab eller fejl i data føre til økonomiske tab, forkerte afgørelser og at service til borgerne ikke kan leveres.

Uanset arten af sikkerhedsbrud påvirkes borgeres og virksomheders tillid til kommunens forvaltning og de digitale selvbetjeningsløsninger. Gevinsterne ved digitalisering og kommunens omdømme generelt er således forbundet til omfanget af brud på informationssikkerhed. Vi ser derfor god informationssikkerhed, både som en del af vores faglige stolthed og som et udtryk for høj servicekvalitet.

NASA og informationssikkerhed

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. Vi viser vores anerkendelse af de medarbejdere og ledere, der undersøger risici og agerer risikobevidst ved behandling af kritiske og følsomme informationer.
S	Sammenhæng	Informationssikkerhed er som en 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 og gyldighedsområde

Alle informationer og systemer, som tilhører kommunen, som kommunen anvender eller som kommunen har ansvaret for, er omfattet. Det inkluderer personoplysninger, sagsdokumentation, produktionsdata, anlægsdata, tegninger, ledelsesinformation mv.

Politikken gælder alle ansatte, politikere, midlertidigt ansatte, eksterne konsulenter og andre med arbejdsmæssig tilknytning til kommunen. Skoleområdet, biblioteksområdet og andre relevante områder skal selv fastlægge en politik for eksterne brugeres 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

Informationssikkerhedsindsatsen tager afsæt i nedenstående mål og organisering. Styringen er baseret på ISO 27001/2, som anvendes bredt i den offentlige sektor. Indsatsen for at efterleve målene skal respektere kommunens ønsker om decentralt ansvar, at der skal tænkes i helheder, at tillid går forud for kontrol, og at Vejen Kommune vil være på forkant med udviklingen. Som billede på indsatsen tænker vi på en livrem med elastik, som afspejler at følsomme personoplysninger og virksomhedsoplysninger beskyttes 100 %, men informationssikkerhed må ikke stå unødigt i vejen for innovation.

Mål

Basis informationssikkerhedsniveauet i Vejen Kommune skal opfylde følgende overordnede mål:

Sikkerhedskultur og -bevidsthed. Ledere og medarbejdere skal kende de risici, som de har indflydelse på. Vejen Kommune har en enhedsforvaltning. Det er derfor vigtigt, at medarbejdere kender deres ansvar og kun behandler informationer, som de aktuelt har behov for til løsning af den konkrete opgave. Ledere har en ambassadørrolle. Ledere skal kende risikoen i deres område og har ansvaret for medarbejderes forståelse af risici og efterlevelse af forholdsregler.

Målet skal opnås ved at etablere et fælles sprog, et holdnings- og værdisæt, som formidles via ledelsessystemet og i direkte dialog med medarbejdere. Arbejdet med sikkerhedskultur og -bevidsthed skal følge en fast, direktionsgodkendt plan, som er tilpasset medarbejderrelaterede risici.

Sikker drift. Der skal opretholdes et stabilt, sikkert, let tilgængeligt og funktionelt it-serviceniveau. Afdelingerne skal kunne stole på, at it-services, der etableres og leveres af IT & GIS, er tilgængelige og beskyttet efter afdelingernes behov.

Målet skal opnås ved at kravene til informationssikkerhed godkendes af systemejer, som også fører tilsyn med efterlevelsen. Kritiske it-driftsprocesser skal følge faste, dokumenterede arbejdsgange, være systematisk overvåget og status på væsentlige driftsforhold skal rapporteres til relevante ledere og ledelsesfora løbende.

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.

Målet skal opnås ved at give de ansvarlige ledere let adgang til oplysninger, der er nødvendige for at kunne udføre tilsyn med anvendelse af rettigheder. Tilsynet skal give indblik i omfanget af eventuel utilsigtet anvendelse af rettigheder, idet kommunen er en enhedsforvaltning, som giver vide muligheder for dataadgang og databehandling. Hvis der gives adgang til fortrolige data uden for det etablerede sikkerhedsmiljø, kræves en forudgående godkendelse af kommunaldirektøren. Adgangskontrollens effektivitet skal efterprøves med faste intervaller.

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

Målet skal opnås ved at projekter og ændringer følger en fast, dokumenteret projekt- og/eller ændringsstyringsproces[2], som omfatter en sikkerhedsmæssig vurdering. Vurderingen skal gennemføres i samarbejde med IT & GIS. Højrisikoprojekter skal godkendes af direktionen. Inden systemer sættes i drift, skal systemejer godkende resultatet af afprøvning af systemets sikkerhedsforanstaltninger.

Fysisk sikkerhed. De fysiske omgivelser for informationer og informationsudstyr skal beskytte mod fysiske hændelser, eksempelvis brand, vandskade, tyveri, hærværk mv.

Målet skal opnås ved, at den fysiske sikring omkring systemerne regelmæssigt risikovurderes. Omplacering af udstyr, som IT & GIS har driftsansvaret for, skal forhåndsgodkendes af IT & GIS. Den fysiske sikkerhed på lokationer med vitale installationer og informationer, skal efterprøves med faste intervaller.

Håndtering af sikkerhedshændelser. Skaden ved sikkerhedsbrud skal holdes på et acceptabelt niveau, og kommunens vigtigste opgaver skal kunne videreføres inden for en af den ansvarlige afdelingschef besluttet tidshorisont.

Målet skal opnås ved, at der opretholdes et beredskab, så sikkerhedshændelser kan håndteres effektivt. Hændelser skal registreres og årligt evalueres og rapporteres til direktionen. Efter alvorlige hændelser skal der foretages en evaluering, som dokumenteres.

Sikkerhedsniveauet omkring de enkelte systemer og data fastlægges på baggrund af en risikovurdering og under hensyn til lovbestemte og kontraktlige krav.

Organisation og ansvar

Der skal udpeges en ansvarlig for koordinering af informationssikkerhedsindsatsen og der skal udarbejdes en årsplan, som beskriver, hvilke tiltag der gennemføres for at opfylde ovenstående mål. Årsplanen med forventet ressourceforbrug skal godkendes af kommunaldirektøren.

Styringen af informationssikkerhed tager afsæt i nedenstående organisering:

[2] Også kaldet Change Management, se ITIL for definition af begrebet. Ændringsstyring er almindelig praksis i it-afdelinger.

- **Kommunaldirektøren** er den øverste informationssikkerhedsansvarlige. Kommunaldirektøren fastlægger i samråd med direktionen ressourceforbrug til koordinering og tværgående tiltag. Kommunaldirektøren godkender dispensationer og behandler sager.

- **Direktionen** har det overordnede ansvar for effekten af den tværgående indsats, herunder at politikken og beslutninger er kendt på alle ledelsesniveauer, samt at politikken er afstemt det aktuelle behov.

- **Afdelingscheferne** har inden for eget område ansvar for efterlevelse af politikken og for koordinering med andre enheder i kommunen. Afdelingschefer skal kende den informationssikkerhedsmæssige udfordring i egen afdeling, træffe de nødvendige foranstaltninger og foretage ledelsestilsyn med deres effekt og efterlevelse. Afdelingscheferne er systemejere.

- 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.

- **DPO – Databeskyttelsesrådgiver** skal overvåge, underrette og rådgive om overholdelse af lovkrav vedrørende følsomme persondata. DPO'en skal understøtte, at de dataansvarlige overholder reglerne i databeskyttelses-forordningen. DPO'en er Datatilsynets kontaktperson i Vejen Kommune.

- **Informationssikkerhedsudvalg** – tværfaglig gruppe med direktør som formand. Sætter mål for informationssikkerheden i Vejen Kommune og sørger for, at informationssikkerheden realiseres og efterleves i organisationen.

- **Informationssikkerhedskoordinatoren** varetager den overordnede koordinering af informationssikkerhed for kommunaldirektøren og hjælper organisationen med opgaver i relation til politikken. Koordineringsaktiviteterne fremgår af årsplanen, som godkendes af direktionen. Koordinatoren skal sikre, at indsatsen er sammenhængende, vedligeholdt, løbende optimeres til det aktuelle behov, og at krav er identificeret, inden nye projekter eller ændringer sættes i gang. Koordinatoren har ansvar for at sikre en høj kvalitet i risikoinformation til relevante fora (chefforum, lokale styregrupper mv.) og direktion, og at systemejere har værktøjer og information, som understøtter systemejernes opgaver. Bilag 1 uddyber koordinatoransvaret.

- **Lederen af IT & GIS** er ansvarlig for, at it-driften lever op til informationssikkerhedspolitikken og det sikkerhedsniveau, der er aftalt med afdelingerne. IT & GIS er kontraktholder for alle it-driftskontrakter, it-leverandørkontrakter og it-samarbejder. Ansvaret omfatter både egen drift og outsourcet drift.

- For alle systemer udpeges en afdelingschef som **systemejer,** med ansvar for systemsikkerheden. Direktionen udpeger systemejere af fællessystemer.

Evaluering og opfølgning

Evaluering og opfølgning udføres systematisk, så vi er trygge ved, at "det virker", så vi hele tiden bliver klogere, og så vi sikrer, at indsatsen afspejler vores værdigrundlag. Informationssikkerhedskoordinatoren leverer en årlig status på målsætninger og efterlevelse, et opdateret risikobillede og forslag til ny årsplan, til direktionen. Koordinatoren bistår afdelingschefer med at gøre status for afdelingens efterlevelse og risici. Derudover leverer koordinatoren kvartalsvis og efter behov status på omfanget af informationssikkerhedsbrud.

Ved væsentlige personalerelaterede brud på sikkerheden informerer koordinatoren chefen for Intern Service, som herefter behandler sagen.

Den operationelle informationssikkerhedspolitik revideres ved større ændringer i organisationen og mindst hvert andet år.

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

Bilag 1 – Anvendelse i praksis

De retningslinjer samt beskrivelse af informationssikkerheds- og kontrolforanstaltninger, der gælder i Vejen Kommune, samles i en sikkerhedshåndbog med samme punktinddeling, som anvendes i ISO 27002.

Sikkerhedshåndbogen samler beskrivelser af informationssikkerhedsområder til brug for koordinering af indsatsen.

Som minimum omfatter koordineringen følgende:

- at sikre, at informationssikkerhedspolitikken og afledte retningslinjer implementeres
- at sikre risikovurdering af informationer og systemer, samt tilse, at der foranstaltninger til beskyttelse af disse informationer etableres og vedligeholdes
- at der udpeges systemejere for samtlige systemer
- at klassificere de informationer og systemer, som kommunen har ansvaret for
- at forebygge og begrænse generelle risici til en for direktionen kendt og accepteret størrelse
- at udarbejde og vedligeholde retningslinjer, som skal følges af de medarbejdere, der behandler og anvender informationerne og systemerne
- at udarbejde og vedligeholde retningslinjer for rettighedstildeling, adgang og brug af informationer, samt at følge op på efterlevelsen
- at udarbejde og vedligeholde retningslinjer for sikkerhedskopiering af informationer, således at disse altid kan genskabes senere inden for en kendt og accepteret tidshorisont
- at indsamle krav til it-beredskab og sikre, at der udarbejdes, afprøves og vedligeholdes en plan til at retablere daglig drift, såfremt informationerne eller systemerne ødelægges, uanset af hvilken grund, således, at:
    - omfanget af og konsekvenserne ved nedbrud/ødelæggelser kan minimeres
    - de væsentligste dele af den daglige forretningsmæssige drift i Vejen Kommune kan gennemføres via alternative forretningsgange
    - alle relevante berørte parter kan holdes orienteret i fornødent omfang
    - den fulde drift af systemerne kan genoptages inden for en kendt og accepteret tidshorisont
- at sikre, at enhver sikkerhedsmæssig følsom informationsbehandling kan henføres til den person, som har udført aktiviteten, samt at sikre gennemførelse af de fornødne kontroller til opdagelse af misbrug eller forsøg herpå
- at sikre, at Vejen Kommunes udvikling og implementering af systemer udføres under iagttagelse af betryggende sikkerhedsforanstaltninger
- at sikre, at Vejen Kommunes leverandører overholder de sikkerhedsforskrifter, som er gældende for Vejen Kommunes informationer, faciliteter og medarbejdere i samarbejdet med leverandøren
- at træffe de nødvendige forholdsregler for at sikre, at informations-sikkerhedspolitikken og afledte retningslinjer bliver overholdt
- at levere den fornødne ledelsesrapportering af status for informationssikkerheden, herunder aktiviteter og hændelser.
- at følge udviklingen i risikobilledet og ændringer i krav til kommuners håndtering af informationssikkerhed, herunder beskyttelse af personoplysninger.