Vesthimmerlands Kommune

INFORMATIONSSIKKERHEDSPOLITIK

Denne politik er godkendt af byrådet den 25.06.2020

VESTHIMMERLANDS
KOMMUNE
- lyst til at gøre en forskel

Indholdsfortegnelse:

Indledning

Informationssikkerhedspolitikken i Vesthimmerlands Kommune fastlægger både den overordnede ramme for beskyttelse af it, data og information samt ansvaret for it-sikkerheden.

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

Kommunen behandler en stor mængde data - herunder både almindelige og følsomme personoplysninger. Disse informationer kræver en særlig beskyttelse for at bibeholde fortrolighed, integritet og tilgængelighed. Det er af afgørende betydning, at borgere, virksomheder og den øvrige offentlige sektor har tillid til, at den nødvendige sikkerhed bliver opretholdt.

Beskyttelse af data og informationssystemer er derfor et vigtigt fokusområde, der håndteres via indsatser indenfor databeskyttelse og informationssikkerhed. Indsatserne består primært af en mængde sikkerhedsforanstaltninger, der etableres med henblik på at beskytte de data og informationssystemer, som kommunen anvender og har ansvaret for.

> Informationssikkerhed handler helt grundlæggende om at passe på de informationer, der er særligt vigtige at beskytte

Retningslinjer for informationssikkerhed er nærmere uddybet i:

- ***Den overordnede politik***, der fastlægger mål, rammer og overordnet organisering af informationssikkerheden.

- ***Rollekataloget*** der definerer organisering, ansvar og roller.

- ***De konkrete retningslinjer*** hvor politikkens bestemmelser er omsat til praksis og udmøntet i sikkerhedshåndbøger, procedurer og vejledninger.

Rollekataloget og de konkrete retningslinjer revideres ved behov inden for rammerne af den overordnede politik.

Formål og principper

Formålet med Vesthimmerlands Kommunes informationssikkerhedspolitik er at definere og fastlægge de overordnede principper for beskyttelse af kommunens data og informationssystemer.

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 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.

Den overordnede politik skal 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
- oplysninger om borgere og virksomheder til enhver tid er beskyttet mod uberettiget videregivelse, hændelige uheld eller forsætlige handlinger
- reglerne for god sikkerhedsskik, herunder principper og normer for adfærd i anvendelsen af kommunens informationssystemer, er klart formuleret og formidlet til medarbejderne
- der er udarbejdet en beredskabsplan for informationssikkerhed, der sikrer, at driften kan genoptages hurtigst muligt efter et nedbrud, og at konsekvenserne af et sikkerhedsbrud reduceres mest muligt.

Omfang

Politikken 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.

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

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

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

Sikkerhedsniveau

Vesthimmerlands 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.

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 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 Vesthimmerlands 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, så skal alle ansatte løbende modtage relevant uddannelse vedrørende databeskyttelse og informationssikkerhed.

Organisation og ansvar

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

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

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 politikken.

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

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 efterleve retningslinjer og procedurer for sikkerhed i det daglige arbejde samt at rapportere risici og hændelser.

Evaluering og opfølgning

DPO´en følger kontinuerligt og systematisk op på arbejdet med databeskyttelse og informationssikkerhed. Den interne kontrol skal sikre, at sikkerhedsbeskrivelserne 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 databeskyttelsesrådgiveren en årlig afrapportering til byrådet om kommunens efterlevelse af databeskyttelseskravene og anbefalinger til forbedringer.

Outsourcede informationssikkerhedsprocesser styres via databehandleraftaler og tilsyn med databehandlere.

Informationssikkerhedspolitikken revideres efter behov.

Kommunaldirektøren har det overordnede ansvar for, at der sker en løbende ajourføring af sikkerhedshåndbogen og tilhørende bilag. Opgaven er i praksis uddelegeret til Udbuds- og Digitaliseringschefen, 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 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 kommunens DPO i henhold til gældende procedure. Sikkerhedsbrud indgår i rapporteringen til kommunens øverste sikkerhedsansvarlige.

Hændelser, der kræver presseomtale, håndteres af Udbuds- og Digitaliseringschefen i samarbejde med kommunaldirektøren.

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

Offentliggørelse

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

Udbuds- og Digitaliseringschef kan give tilladelse til, at der bliver udleveret eller offentliggjort andet materiale vedrørende informationssikkerheden.