VINDAFJORD
KOMMUNE

Tryggleiksmål og -strategi for Vindafjord kommune

Innhald

1. Innleiing

Vindafjord kommune er den største tenesteleverandøren til innbyggarane i Vindafjord. For å kunna levera kommunale tenester, behandlar og lagrar Vindafjord kommune kvar dag store mengder med informasjon. Dette er nødvendig for å kunna levera tenester av høg kvalitet til innbyggarane. Måla for informasjonstryggleik tar utgangspunkt i å beskytta tilgjengelegheita, integriteten og fortrulegheita til informasjonen som blir samla inn.

Med dette meinast det at informasjonen skal vera tilgjengeleg for rette vedkommande (tilgjengelegheit), at informasjonen ikkje skal kunna endrast eller slettast av uvedkommande (integritet), og at informasjonen ikkje skal kunna lesast av uvedkommande, altså vera konfidensiell (fortrulegheit).

2. Sentrale lovar og forskrifter

Kommunen skal tilfredsstilla krava i relevante lovverk, underliggande forskrifter, samt reglar og andre føringar frå relevante myndigheitsorgan. Noko av det mest sentrale regelverket er følgande (lista er ikkje uttømmande):

- Lov om behandling av personopplysningar av 15. juni 2018 nr. 38 (**personopplysningslova**) som gjer Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 (**personvernforordninga)** til norsk lov
- Lov om behandlingsmåten i forvaltningssaker av 10. februar 1967 (**forvaltningslova**)
- Forskrift om elektronisk kommunikasjon med og i forvaltninga av 25. juni 2004 nr. 988 (**e-forvaltningsforskrifta**)
- Lov om rett til innsyn i dokument i offentleg verksemd av 19. mai 2006 nr. 16 (**offentleglova**)
- Lov om nasjonal sikkerheit av 1. juni 2018 nr. 24 (**sikkerheitslova**)
- Forskrift om verksemder sitt arbeid med førebyggande sikkerheit av 20. desember 2018 nr. 2053 (**verksemdssikkerheitsforskrifta**)
- Lov om arbeidsmiljø, arbeidstid og stillingsvern mv. av 17. juni 2005 nr. 62 (**arbeidsmiljølova**)
- Lov om arkiv av 4. desember 1992 nr. 126 (**arkivlova**)
- Lov om helseregister og behandling av helseopplysningar av 20. juni 2014 nr. 43 (**helseregisterlova**)
- Forskrift om systematisk helse-, miljø- og sikkerheitsarbeid i verksemder av 6. desember 1996 nr. 1127 (**internkontrollforskrifta**)
- Norm for informasjonssikkerheit og personvern i helse- og omsorgssektoren (**norma**)

3. Tryggleiksmål

Det overordna formålet med Vindafjord kommune si behandling av personopplysningar og annan sensitiv informasjon, er å kunna tilby innbyggarane i kommunen eit best mogleg tenestetilbod.

Tryggleiksmåla skal sikra Vindafjord kommune si drift og innbyggarane sin tillit ved å førebygga og avgrensa konsekvensane av uønskte hendingar. Dette omfattar all behandling, lagring og kommunikasjon av informasjon, både munnleg, på papir og digitalt. All bruk av IKT-verktøy er også inkludert.

All behandling av informasjon skal vera i samsvar med lovpålagte, interne og avtalerettslege krav til informasjonstryggleik. Personopplysningar og annan sensitiv informasjon skal sikrast på ein trygg måte gjennom fysiske, tekniske og organisatoriske tiltak.

Vindafjord kommune skal sørga for at alle tilsette har kjennskap til tryggleiksmåla og relevante rutinar.

3.1 Tilgjengelegheit

Informasjonssystem skal vera tilgjengeleg for autoriserte brukarar ved behov.

3.2 Integritet

Informasjon som Vindafjord kommune har ansvaret for skal berre bli produsert og endra av tilsette, eller av eksterne som har fullmakt til dette.

Informasjon skal ikkje bli endra utilsikta.

3.3 Fortrulegheit

Personopplysningar og annan sensitiv informasjon som blir behandla av Vindafjord kommune skal vera beskytta mot ikkje-autorisert tilgang.

Personopplysningar skal bli behandla konfidensielt og skal berre bli delt med andre tilsette i den grad det er tenestleg behov.

Personopplysningar om kommunalt tilsette skal berre bli behandla av den som har tenestleg behov.

3.4 Robuste system

Verksemda og informasjonssystema skal vera motstandsdyktige og robuste.

Når uønskte fysiske eller tekniske hendingar inntreff, skal beredskapstiltak bidra til å avgrensa skade og til at verksemda raskt kjem tilbake til normal drift. Dette inkluderer å oppretta tilgjengelegheit og tilgang til personopplysningar på nytt til rett tid.

4. Tryggleiksstrategi

Informasjonstryggleiksarbeidet skal:

- vera forankra i styringslinja og utførast systematisk
- gjennomførast for å nå måla for informasjonstryggleik
- vera risikobasert og følga anerkjente standardar så langt det er føremålstenleg

- følga prinsippa for læring og kontinuerleg forbetring

Det inneber at:

- risikovurderingar skal bli gjennomført systematisk, periodisk og ved vesentlege endringar i oppgåver eller omgjevnadane.
- tiltak for å redusera risiko skal vera baserte på risikovurderingar og leiinga sine føringar for risikohandtering og akseptabel risiko.
- hendingar som ut frå risiko kan påverka informasjonstryggleiksmåla negativt, skal bli melde frå om og følgde med på, på systematisk vis.
- leiinga skal systematisk styra og følga opp informasjonstryggleiksarbeidet.
- leiinga skal systematisk følga opp at mål blir nådd og tryggleiksstrategien blir etterlevd, samt følga opp tryggleikskompetansen og -kulturen i kommunen.

For å lukkast med dette skal alle tilsette:

- ha eit medvite bevisst forhold til kommunen sine tryggleiksmål og viktigheita av måla.
- vita kva typar informasjon dei behandlar og kva krav som blir stilt til deira eigne informasjonsbehandling og bruk av IKT.
- etterleva krav, retningslinjer, prosedyrar, rutinar med meir som gjeld for dei og det arbeidet dei utfører.

Strategien skal bli implementert gjennom tryggleiksval forankra i leiinga.

5. Ansvar og roller

5.1 Kommunedirektør

I Vindafjord kommune har kommunedirektøren eit overordna ansvar for informasjonstryggleiken. Dette inneber blant anna at kommunedirektøren står ansvarleg for at informasjonstryggleiken i kommunen er på eit nivå som samsvarar med krava i relevant lovverk og tryggleiksmåla til kommunen. Jamfør punkt 4.

5.2 Kommunalsjefar

Kommunalsjefane i Vindafjord kommune har ansvar for informasjonstryggleiken innafor sitt forvaltningsområde. Kommunalsjefane skal utøva sitt ansvar for informasjonstryggleik ved å organisera tryggleiksarbeidet, utøva internkontroll og setta i verk nødvendige tiltak.

Kommunalsjefane kan delegera tryggleiksarbeidet til ein einingsleiar eller tilsett, men har ansvar for at informasjonstryggleiken innanfor sitt forvaltningsområde er på eit nivå som samsvarar med krava i relevant lovverk og tryggleiksmåla til kommunen. Jamfør punkt 4.

5.3 Einingsleiarar

Einingsleiar skal ha oversikt over eininga sine IKT-system og har ansvar for at informasjonstryggleiken innanfor si eining sitt forvaltningsområde er på eit nivå som samsvarar med krava i relevant lovverk og tryggleiksmåla til kommunen. Einingsleiar kan delegera tryggleiksarbeidet til ein tilsett, men har sjølv ansvaret for informasjonstryggleiken og rapporterer til sin kommunalsjef. Jamfør punkt 4.

5.4 Tilsette

Alle tilsette i Vindafjord kommune har eit sjølvstendig ansvar for å ta vare på informasjonstryggleiken i sitt daglege arbeid. Kvar enkelt skal utøva sitt ansvar for informasjonstryggleiken blant anna ved å behandla informasjon etter gjeldande rutinar og rapportera eventuelle avvik til nærmaste leiar. Jamfør punkt 4.

6. Tryggleiksval

Vindafjord kommune har høgt fokus på tryggleik og set i verk tryggleikstiltak for å sikra konfidensialitet, integritet og tilgjengelegheit i alle ledd.

6.1 Systemteknisk tryggleik

Avhengig av det aktuelle system og informasjonen som blir behandla, vil dei ulike sidene ved tryggleik (tilgjengelegheit, integritet, fortrulegheit og behovet for robuste system) ha ulik betydning.

Ulike delsystem kan ha ulike behov for vern.

6.2 Tekniske tryggleikstiltak

- Tiltak som reduserer risikoen for at tilsette uaktsamt eller med forsett skal kunna skada informasjonssystem eller informasjon som er lagra i desse.
- Tiltak som sørger for å gi tilgang til informasjonssystem for dei brukarar som er autorisert, og som bidrar til å hindra at uvedkommande får tilgang til informasjon.
- Det skal vera etablert tryggleikslogging som gjer at tryggleiksbrot kan avdekkast.
- Tiltak for å bidra til å hindra at skadeleg programvare kjem inn i kommunen sine informasjonssystem.
- Jamleg tryggleikskopiering av lagringsmedium.
- Tapt informasjon skal kunne gjerast tilgjengeleg igjen så snart som mogleg, avhengig av system og kor kritisk det enkelte system er.
- Telefonsystem bør ikkje ha ein driftsstans på meir enn 24 timar ved driftsfeil. Ved alvorlege systemfeil skal feilretting starta utan ugrunna opphald.

6.3 Organisatoriske tryggleikstiltak

- Rutinar for handtering av tilgang til kommunen sine informasjonssystem. I dette ligg kontroll av passord, rettar, applikasjonar og så vidare. Kompleksitetsgraden for passord skal ligga på eit høgt nivå.
- Rutinar om tilsette si handtering av berbare datamaskinar, mobiltelefonar og så vidare, for å senka risikoen for at informasjon hamnar på avvege.
- Rutinar for å låsa lokale, handtering av gjester og bruk av alarm utanom arbeidstid.
- Prosedyrar for plassering og sikring av komponentar, lagringsmedium, dokument eller andre element som er vitale for kommunen si drift.

6.4 Fysiske tiltak

- Kommunen sine lokale skal sikrast med tiltak mot blant anna innbrot, brann, vasskade og liknande.
- Senka risikoen for at uvedkommande får tilgang til lokale kor personopplysningar og anna sensitiv informasjon blir oppbevart.
- Maskinpark, lagringsmedium og sentrale nettverkskomponentar skal vera fysisk sikra, slik at uvedkommande ikkje skal kunna bringa dette med seg ut av kommunen sine lokale.

6.5 Kommunen sine applikasjonar

For kommunen sine applikasjonar gjeld følgande:

- Ansvaret for handtering av tryggleiksbehov i Vindafjord kommune sine applikasjonar ligg hos systemeigar.
- Programvare skal kjøpast inn på bakgrunn av kravspesifikasjonar, kor også krav til innebygd personvern, personvern som standardinnstilling og tryggleik inngår.
- I relevante tilfelle, før programvara og systemet blir sett i produksjon, skal teknisk tryggleiksnivå, innebygd personvern og personvern som standardinnstilling verifiserast. Ved feil eller manglar skal retting bli gjennomført før systemet blir sett i produksjon. Retting av feil og manglar skal verifiserast.

7. Bruk av databehandlarar og underleverandørar

Vindafjord kommune sin bruk av databehandlarar og leverandørar skal regulerast i kontraktar, kor også føresegner om informasjonstryggleik inngår.

Alle avtalar kor ei ekstern verksemd tar på seg oppdrag – som også omfattar informasjonstryggleik – for Vindafjord kommune skal baserast på avtalar som minimum samsvarar med krava gitt i personvernforordninga artikkel 28 og 29.

Ein kan ikkje engasjera nye leverandørar utan at dette blir avklara med leiinga. Eksterne verksemder eller personar kan ikkje bli gitt tilgang til kommunen sine informasjonssystem med mindre dette skjer som ledd i ein godkjent avtale.