FJELLREGIONEN IKS

Rapport tiltak
Forvaltningsrevisjon IKT sikkerhet
i FARTT

21.9.2024

Innhold

1 Innledning 4
2 Oppfølging av forvaltningsrevisjonen 4
3 Styringssystem for informasjonssikkerhet 5
4 Organisering og ansvarsforhold i IKT sikkerhetsarbeidet 5
4.1 Behandlingsansvarlig 5
4.2 Databehandler 6
4.2.1 Organisering av sikkerhetsarbeidet hos databehandler, FARTT 6
4.2.2 Formål 6
4.2.3 Omfang/Virkeområde 6
4.2.4 Overordnet organisering 6
4.3 Databehandleravtaler 7
4.4 Personvernombud 7
4.5 IKT Sikkerhetsutvalg 8
4.5.1 Organisering av Sikkerhetsutvalget, oppdragsgiver 8
4.5.2 Mandat for Sikkerhetsutvalget 8
5 Sikkerhetsmål for behandling av personopplysninger 8
5.1 Formål 8
5.2 Omfang/Virkeområde 9
5.3 Ansvar 9
6 Sikkerhetsstrategi for informasjonssikkerhet 9
6.1 Formål 9
6.2 Omfang/Virkeområde 9
6.3 Ansvar 9
6.4 Ledelsens gjennomgang 10
7 Mål for informasjonssikkerhet, verdier 10
8 Identifisering av informasjonsverdier 10
9 Klassifisering av verdier etter områder/sektorer: 11
9.1 Helse og omsorg 11
9.2 Teknisk plan og landbruk 12
9.3 Lønn og personal 12
9.4 Økonomi 12
9.5 Administrasjon 12
9.6 Oppvekst og kultur 12
9.7 Publikumstjenester 12
10 Verdivurdering og identifisering av informasjonsverdier i kommunene 12
11 Tilgangsstyring 13
12 Avvik og håndtering av avvik 13
13 IKT hendelser 14
14 Risikostyring og risikovurdering av informasjonssikkerheten i FARTT 15
14.1 Lovkrav 15
14.2 Risiko 15
14.3 Sannsynlighet og konsekvens 15
14.4 Akseptabelt risikonivå 17

15 Risikovurdering i FARTT 17
15.1 Metode 17
16 Resultater etter gjennomført risikovurdering i FARTT 18
17 Oppfølging og tiltak 18
17.1 Konsekvenser for klima, miljø, omdømme, økonomi mm 19
18 Hendelseshåndtering og gjenoppretting 19
19 Cybersikkerhet, kunnskap og kompetanse 19
20 Generelle sikkerhetstiltak 20
20.1 Beredskap 20
20.2 Infrastruktur, fiber og mobilnett, redundans 20
20.3 NSM grunnprinsipper 21
20.4 Sikkerhetsnøkler 21
20.5 Anskaffelse sikkerhetstjenester 21
20.6 Kompetanse-ressurs innafor informasjonssikkerhet i FARTT 22
20.7 KINS/KS informasjonskampanje-program 23
21 Oppsummering 23
22 Endringer ved revisjon 24
23 Vedlegg 24

1 Innledning

Våren 2023 besluttet kontrollutvalget i Tynset kommune å gjennomføre en forvaltningsrevisjon av IKT sikkerhet i IKT Fjellregionen IKS (heretter FARTT). Tynset kommune har rammeavtale med BDO som revisjonsselskap.
Kommunene i FARTT samarbeidet ved respektive kontrollutvalg med unntak av Folldal kommune, sluttet seg til et samarbeid om gjennomføring av felles forvaltningsrevisjon.
I november 2023 la BDO frem sin rapport der man konkluderte med at FARTT ikke har tilfredsstillende sikkerhet, dette vurdert i forhold til 5 belyste problemstillinger.

Kontrollutvalgene i FARTT kommunene behandlet rapporten høsten 2023 og deres anbefalinger er videre behandlet i kommunestyrene i FARTT kommunene, vedtak som følger:

Kommunestyrene følger revisors anbefalinger og ber eierrepresentanten for IKT Fjellregionen i samarbeid med kommunedirektøren å sørge for at selskapet:

1. Iverksetter et arbeid med identifisering av informasjonsverdier, vurdering av trusler og sårbarheter som grunnlag for spesifikke sikkerhetsmål, sikkerhetsstrategi og sikkerhetsorganiseringen. Dette arbeidet kan munne ut i en overordnet plan for IKT og IKT-sikkerhet.
2. Avklare og dokumentere organiseringen av informasjonssikkerhetsarbeidet og være konsekvent i benevnelsen av roller.
3. Vurdere å sikre at rutinen for tilgangsstyring etterleves ved endring og avslutning av arbeidsforhold, herunder også innlevering av kommunens datautstyr.
4. Vurdere behovet for dokumentasjon av IKT-hendelser som grunnlag for evaluering og læring.
5. Utarbeide en plan for hendelseshåndtering og gjenoppretting.
6. Får tilgang til økt kompetanse på cyber-sikkerhet, tilleggspunkt fra kommunestyret i Tolga

Eierrepresentanten og kommunedirektøren rapporterer til kontrollutvalget om iverksatte tiltak innen 01.10.24.

2 Oppfølging av forvaltningsrevisjonen

FARTT ble kjent med plan for gjennomføring av forvaltningsrevisjon IKT sikkerhet, våren 2023, da med innledende informasjon fra kontrollutvalget i Tynset kommune og BDO som gjennomførende virksomhet.

FARTT har deltatt i gjennomføring av forvaltningsrevisjonen med overlevering og gjennomgang av dokumentasjon, deltatt i intervjuer og vært gjenstand for en penetrasjonstest. En foreløpig rapport ble gjennomgått i juni 2023 og endelig rapport ble lagt frem i november 2023.

Som svar på tiltakene er det utarbeidet en rapport som innledes med informasjon om bruk av styringssystem, organisering og ansvarsforhold for IKT sikkerhet. Øvrige tiltak er besvart utover i dokumentet.

3 Styringssystem for informasjonssikkerhet

Personvernforordningen stiller krav til tilstrekkelig informasjonssikkerhet ved innføring av egnede tekniske og organisatoriske tiltak. Det er opp til den enkelte virksomhet om man vil benytte anerkjente standarder som ISO/IEC 27001 eller andre rammeverk og veiledere.

FARTT og eierkommunene benytter Compilo som styringssystem for informasjonssikkerhet. Dette er forankret i både styret i FARTT og kommunene. Både selskapet og kommunene har benyttet Compilo over flere år, først og fremst som kvalitetssystem. Høsten 2023 ble det gjennomført en felles anskaffelse av en GDPR pakke fra Compilo, der både selskapet og kommunene i FARTT deltok.

Det ble gjennomført felles workshop i september 2023 der man jobbet sammen om innholdet/følgende elementer:

- Lover og forskrifter
- Prosedyrer
- Sjekklister, skjemaer og maler
- Dokumentasjon
- GDPR prosessbeskrivelse
- ROS
- DPIA

GDPR prosessbeskrivelse viser hvilke prosesser som inngår i årshjulet for informasjonssikkerhet.
Både FARTT og kommunene jobber etter dette prosesskartet, der overnevnte elementer er del av dette.

Prosesskart GDPR, se vedlegg 23.1

4 Organisering og ansvarsforhold i IKT sikkerhetsarbeidet

(Svar på pkt. 2 i forvaltningsrevisjonen).

Nedenfor gis det en beskrivelse av hvordan sikkerhetsarbeidet er organisert i den enkelte kommune og i FARTT.

4.1 Behandlingsansvarlig

Personvernforordningen artikkel 4 nr. 7:

Behandlingsansvarlig er en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandling av personopplysninger og hvilke midler som skal benyttes.

Den enkelte kommune i FARTT samarbeidet er jf. lovhenvisning over, behandlingsansvarlig. Det er kommunedirektør som har øverste ansvar.

Oppfølging av sikkerhetsarbeidet i den enkelte FARTT kommune er stort sett ganske likt organisert. *Prosedyre for sikkerhetsorganisasjon og ansvar* definerer roller og ansvar, med kommunedirektøren som øverste ansvarlige. Med dette som utgangspunkt har hver enkelt kommune organisert/delegert dette slik de synes det er hensiktsmessig i tråd med sitt system for interkontroll.

Alle kommuner har også en IKT-sikkerhetsansvarlig som deltar i felles sikkerhetsutvalg.

4.2 Databehandler

Personvernforordningen artikkel 4 nr. 8:

En databehandler er en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige.

I FARTT samarbeidet er IKT Fjellregionen IKS (FARTT) databehandler for FARTT kommunene, på systemer eller løsninger som driftes i egenregi. Dersom andre leverandører drifter systemer eller løsninger på vegne av FARTT kommunene, er disse databehandler for overnevnte systemer/løsninger.

4.2.1 Organisering av sikkerhetsarbeidet hos databehandler, FARTT

Sikkerhetsorganisasjon og ansvar ligger som del av styrende GDPR prosedyre i Compilo, som er styringssystemet for informasjonssikkerhet i FARTT. (Se også pkt. 3)

4.2.2 Formål

I organisasjonen er det lagt vekt på at arbeidet med informasjonssystemene skal være av en slik karakter at sikkerhet i forhold til integritet, tilgjengelighet og konfidensialitet blir ivaretatt. Kravene som settes i Personopplysningsloven og forordningen skal ivaretas.

Ledelsen har forankret dette i organisasjonen på en slik måte at nødvendig ledelsesfokus blir ivaretatt.

Dokumentet beskriver funksjoner, ansvar og organisering

4.2.3 Omfang/Virkeområde

Hele organisasjonen

4.2.4 Overordnet organisering

Behandlingsansvarlig

- Daglig leder, øverste ansvarlige i organisasjonen. Organiserer ansvar, roller og oppgaver innenfor arbeidet med informasjonssikkerhet.
- Sikkerhetsutvalg/kvalitetsutvalg (leder eller ansvar for å delegere ansvaret videre)

Daglig ansvarlig

- Daglig leder, Er daglig ansvarlig for sikker behandling av personopplysninger i egen organisasjon

Sikkerhetsleder

- Leder som har det overordnede ansvar for at organisasjonen følger de krav som stilles til informasjonssikkerhet, jf. Personopplysningsloven kap. 3.
- Operativt ansvar. Medlem av sikkerhetsutvalget.
- Kan pålegge ledere ansvarsoppgaver i.h.t deres avdelings sikkerhetsbehov.
- Rapporterer direkte til øverste leder.

Ansvarlig for teknisk løsning

- Driftsleder, Utarbeide en driftsdokumentasjon for IT drift av organisasjonens lokale løsninger
- Utarbeide en beredskapsplan for å sikre at driftskritiske datasystem er operative dersom det skulle oppstå uforutsatte hendelser. (eks strømbrudd, flom, brann, hærverk, sabotasje mm)
- Ved ekstern driftspartner på IT-drift reguleres forholdet gjennom databehandleravtale og driftsavtale.

Medlem operativ sikkerhetsgruppe

- Leder FARTT Service, ansvarlig for klientsikkerhet
- Sørge for å gjennomføre nødvendige sikkerhetstiltak i samsvar med overordnede krav og retningslinjer
- Gjennomføre nødvendige sikkerhetstiltak på oppdrag fra daglig leder og sikkerhetsleder
- Bidra i utarbeidelse og vedlikehold av mål og strategiplaner for informasjonssikkerhet

Operativ sikkerhetsgruppe har følgende fokusområder:

- Informasjonssikkerhet - operativ sikkerhet knyttet til daglig drift, plattform infrastruktur og fagsystemer
- Utarbeide tiltak for daglig drift
- Informasjon – kompetanse – kampanjer
- Sikkerhetsutvalg
- Personvernombud

4.3 Databehandleravtaler

Alle virksomheter som benytter seg av en underleverandør har en plikt til å ha en databehandleravtale. Den skal sikre at personopplysningene blir behandlet i samsvar med regelverket og setter en klar ramme for hvordan databehandleren kan behandle opplysningene.

I FARTT samarbeidet er det inngått egne databehandleravtaler mellom FARTT og den enkelte av FARTT kommunene.

FARTT kommunene har individuelle databehandleravtaler med ulike leverandører på andre behandlinger som andre databehandlere utfører på vegne av kommunene. FARTT har i tillegg noen databehandleravtaler på større systemer mot større leverandører.

4.4 Personvernombud

Personvernforordningen artikkel 37 nr. 1:

Den behandlingsansvarlige og databehandleren skal utpeke et personvernombud når behandlingen utføres av en offentlig myndighet eller et offentlig organ.

Personvernombudets rolle er å gi råd til ledelsen og andre i virksomheten og kontrollerer etterlevelsen av regelverket. Personvernombudet er også kontaktpunkt for de registrerte og Datatilsynet.

FARTT kommunene og FARTT har felles personvernombud, denne tjenesten leies ut av Tolga kommune i en 20 % stilling.

4.5 IKT Sikkerhetsutvalg

4.5.1 Organisering av Sikkerhetsutvalget, oppdragsgiver

IKT sikkerhetsutvalget består i dag av en representant fra hver av FARTT kommunene.
I tillegg er FARTT representert med sikkerhetsleder.

IKT Sikkerhetsutvalgets mandat er forankret hos eierkommunene ved kommunedirektørene og iverksatt av styret i IKT Fjellregionen IKS.

4.5.2 Mandat for Sikkerhetsutvalget

- Sikkerhetsutvalget skal være et rådgivende utvalg fordeling av erfaringer og kunnskap om effektiv og praktisk håndtering av informasjonssikkerhet
- koordinering og samordning av kommunenes arbeid med oppfølging av Personvernforordningen og Personopplysningsloven
- utvikling og vedlikehold av felles strategier, maler, prosedyrer og annet verktøy for slik oppfølging

Sikkerhetsutvalget skal bistå kommunene med å tilrettelegge, gi anbefalinger og koordinere arbeidet som må gjøres i hver enkelt kommune for å ivareta kravene som er nedfelt i Personvernforordningen og personopplysningsloven til personvern og informasjonssikkerhet for innbyggerne og virksomhetens plikter og ansvar.

Mandat for IKT sikkerhetsutvalget, se vedlegg 23.2

5 Sikkerhetsmål for behandling av personopplysninger

Svar på pkt. 1 i forvaltningsrevisjonen

Sikkerhetsmål for behandling av personopplysninger, ligger som en del av styrende prosedyrer i Compilo, styringssystemet for informasjonssikkerhet:

5.1 Formål

Sikkerhetsmålene skal støtte og sikre at alle ansatte vet hvordan behandling av personopplysninger skal foregå i det daglige. Sikkerhetsmålene skal sikre at personopplysninger blir håndtert i samsvar med lovkrav og interne

bestemmelser. Sikkerhetsmålene skal sikre at personopplysninger blir håndtert i samsvar med lovkrav og interne bestemmelser.

5.2 Omfang/Virkeområde

Sikkerhetsmålene gjelder for alle ansatte i organisasjonen.

5.3 Ansvar

- **Behandlingsansvarlig** har ansvar for utarbeidelse og revisjon av sikkerhetsmål
- **Sikkerhetsleder** har ansvar for at ledere er kjent med sikkerhetsmålene, og at det er laget en plan for implementering i organisasjonen.
- **Personvernombud** har ansvar for å bistå i opplæring av ansatte og bidra med rådgivning.
- **Ledere** har ansvar for at egne ansatte er kjent med sikkerhetsmålene og at målene blir forstått og implementert i organisasjonen.
- **Ledere** skal oppfordre ansatte til å melde fra om hendelser / avvik som følge av brudd på sikkerhetsmål, tilsiktet eller utilsiktet.
- **Ansatte** skal lese sikkerhetsmålene og gjennom drøfting med leder forstå hvordan disse skal etterleves i det daglige
- **Alle** har ansvar for å melde hendelser / avvik i organisasjonens internkontrollsystem.

6 Sikkerhetsstrategi for informasjonssikkerhet

Sikkerhetsstrategi for informasjonssikkerhet ligger som en del av styrende GDPR prosedyrer i Compilo, styringssystemet for informasjonssikkerhet:

6.1 Formål

Sikkerhetsstrategi skal konkretisere hvordan en arbeider for å ivareta sikkerhetsmålene for organisasjonen.

6.2 Omfang/Virkeområde

Gjelder alle ansatte

6.3 Ansvar

Behandlingsansvarlig har ansvar for å få utarbeidet en sikkerhetsstrategi for organisasjonen.
Sikkerhetsleder har ansvar for at ledere er kjent med strategien.
Personvernombud har ansvar for å gi ledere opplæring og kunnskap om sikkerhetsstrategien. Personvernombudet har også ansvar for å gi råd til ledere og ansatte om praktisk etterlevelse av sikkerhetsstrategien.
Leder har ansvar for at ansatte er kjent med sikkerhetsstrategien og hvordan denne skal etterleves i daglig arbeid.
Ansatt har ansvar for å gjøre seg kjent med sikkerhetsstrategien og etterleve denne i daglig arbeid.

Alle har ansvar for å melde avvik i organisasjonens internkontrollsystem dersom sikkerhetsstrategien ikke følges.

6.4 Ledelsens gjennomgang

Hensikten med ledelsens gjennomgang er årlig å vurdere og eventuelt forbedre de mål som er satt for informasjonssikkerhet. I dette ligger å iverksette og følge opp korrigerende tiltak, påse at internkontroll og styringssystem for informasjonssikkerhet er hensiktsmessig, tilstrekkelig og effektivt, og at det tilfredsstiller relevante krav i lover og forskrifter.

Det er øverste leder som er ansvarlig for årlig å gjennomføre ledelsens gjennomgang av informasjonssikkerheten.

7 Mål for informasjonssikkerhet, verdier

Målet for informasjonssikkerhet er at en skal ta vare på FARTT sine verdier. I praksis vil det si at en ivaretar virksomhetens:

- ***Integritet***, som innebærer at informasjon og systemer skal være korrekt, komplett og oppdatert til enhver tid.
- ***Konfidensialitet***, som innebærer at informasjonen er klassifisert, der konfidensiell eller bedrifts sensitive informasjon ikke kommer på avveier, og kan kun aksesseres fra personer med tjenstlige behov.
- ***Tilgjengelighe***t, som innebærer at informasjon og systemer skal være tilgjengelig for personer med tjenstlige behov. Dette innebærer også at en har definert roller og rettigheter i «Firma»
- ***Regulatoriske krav***, som innebærer at en ivaretar integritet, konfidensialitet og tilgjengelighet gitt av regulatoriske forhold eks. personvernreguleringer, regnskapslovgivning og andre gjeldende regulatoriske forhold for «Firma» sin virksomhet

8 Identifisering av informasjonsverdier

(Svar på pkt. 1 i forvaltningsrevisjonen).

Mange benytter begrepet informasjonsverdi som et samlebegrep som inkluderer både informasjon og tilhørende støtteverdier som IKT-systemer, digitale tjenester, datautstyr av ulike varianter mm.
Som organisasjoner er man forpliktet til å sikre organisasjonens informasjon på en måte som gjøre det mulig å beskytte den. Dette gjøres ved hjelp av de tre hovedprinsippene, se også 6 Mål for informasjonssikkerhet, verdier:

- **Konfidensialitet:** at informasjonen ikke blir kjent for uvedkommende
- **Integritet:** at informasjonen ikke blir endret utilsiktet eller av uvedkommende
- **Tilgjengelighet:** at informasjonen er tilgjengelig ved behov

I det påfølgende ser vi på hvilke informasjonsverdier som behandles. Hensikten er en overordnet klassering av de gruppene av informasjon som vi behandler, definert pr. kommunale områder/sektor. KS' rutine for klassifisering av informasjonsverdier er grunnlag for de verdiene som er satt.

Behandlingsansvarlige ved kommuneledelse bør utføre/har utført tilsvarende verdivurdering med nødvendige tiltak for å sikre korrekt behandling. Om behandlingsansvarlig endrer verdivurdering må denne legges til grunn for ROS-analyser hos FARTT som databehandler.

Følgende tabell beskriver kriterier for å angi verdivurdering pr. område.

	Konfidensialitet	**Integritet**	**Tilgjengelighet**
Lav	Det får ubetydelige konsekvenser for kommunene, IKT Fjellregionen, samarbeidspartnere eller enkeltpersoner hvis informasjonen kommer på uvedkommende i hende.	Det får ubetydelige konsekvenser for kommunene, IKT Fjellregionen, samarbeidspartnere eller enkeltpersoner hvis informasjonen blir endret ved feil eller manipulering.	Det får ubetydelige konsekvenser for kommunene, IKT Fjellregionen, samarbeidspartnere eller enkeltpersoner hvis informasjonen ikke er tilgjengelig.
Middels	Det får moderate konsekvenser for kommunene, IKT Fjellregionen, samarbeidspartnere eller enkeltpersoner hvis informasjonen kommer uvedkommende i hende.	Det får moderate konsekvenser for kommunene, IKT Fjellregionen, samarbeidspartnere eller enkeltpersoner hvis informasjonen blir endret ved feil eller manipulering.	Det får moderate konsekvenser for kommunene, IKT Fjellregionen, samarbeidspartnere eller enkeltpersoner hvis informasjonen ikke er tilgjengelig.
Høy	Det får alvorlige konsekvenser for kommunene, IKT Fjellregionen, samarbeidspartnere eller enkeltpersoner hvis informasjon kommer uvedkommende i hende.	Det får alvorlige konsekvenser for kommunene, IKT Fjellregionen, samarbeidspartnere eller enkeltpersoner hvis informasjonen blir endret ved feil eller manipulering	Det får alvorlige konsekvenser for kommunene, IKT Fjellregionen, samarbeidspartnere eller enkeltpersoner hvis informasjonen ikke er tilgjengelig.
Svært høy	Det får kritiske konsekvenser for kommunene, IKT Fjellregionen, samarbeidspartnere eller enkeltpersoner hvis informasjonen kommer uvedkommende i hende.	Det får kritiske konsekvenser for kommunene, IKT Fjellregionen, samarbeidspartnere eller enkeltpersoner informasjonen blir endret ved feil eller manipulering	Det får kritiske konsekvenser for kommunene, IKT Fjellregionen, samarbeidspartnere eller enkeltpersoner hvis informasjonen ikke er tilgjengelig.

9 Klassifisering av verdier etter områder/sektorer:

Kritikalitet (klassifisering) eller akseptkriterier
Det er tatt utgangpunkt i områder/sektorer og her beskrives hva som utgjør viktige verdier for kommunene. Disse klassifiseres etter 4 hovedgrupper, Lav (L), Middels (M), Høy (H) og Svært Høy (SH), målt opp mot Tilgjengelighet, Integritet, Konfidensialitet og økonomi, se tabeller under.
Nedenfor følger en beskrivelse av hva slags informasjon som behandles innafor de utvalgte områdene.

9.1 Helse og omsorg

Informasjonen som behandles kategoriseres som både personopplysninger (alle opplysninger og vurderinger som kan knyttes til deg som enkeltperson) og særlige kategorier av personopplysninger (også kalt sensitive personopplysninger). Informasjonen inneholder direkte og indirekte en del helseopplysninger. Det er i utgangspunktet høy risiko ved behandling av informasjon. Det er viktig med gode sikringstiltak for å kunne redusere risiko til akseptabelt nivå.

9.2 Teknisk plan og landbruk

Informasjonen som behandles kategoriseres som personopplysninger. Det kan forekomme særlige kategorier av personopplysninger, om en person oppgir dette selv. Det behandles informasjon om innbyggere, ansatte og samarbeidspartnere. Risikoen ved behandling er moderat i utgangspunktet. Offentlighet styres av lov med krav om åpenhet i behandling, tilgjengelighet styres av saksbehandler, men med noen unntak fra offentlighet. Kravet til sikringstiltak er lavere enn for helse og oppvekst, men må være tilstrekkelig for å sikre at informasjon unntatt offentlighet ivaretas.

9.3 Lønn og personal

Informasjonen som behandles kategoriseres som både personopplysninger og særlig kategorier av personopplysninger. Her ligger ulike personalsaker som kan, både direkte og indirekte, inneholde helseopplysninger. Det er manuelle rutiner for å redusere omfanget av særlige kategorier av personopplysninger Risikoen ved behandling er moderat, og det kreves gode sikringstiltak i alle ledd for å redusere risikoen til et akseptabelt nivå.

9.4 Økonomi

Informasjonen som behandles kategoriseres som personopplysninger. Det behandles informasjon om innbyggere og samarbeidspartnere som grunnlag for økonomistyring i kommunene med regnskap og fakturering. Regnskapsdata, økonomi informasjon, budsjett og fakturering kan være virksomhetskritisk dersom ikke tilgjengelig over lengre perioder. Risikoen ved behandling er moderat i utgangspunktet. Offentlighet styres av lov med krav om åpenhet i behandling, tilgjengelighet styres av saksbehandler, men med noen unntak fra offentlighet. Kravet til sikringstiltak er lavere enn for helse og oppvekst, men må være tilstrekkelig for å sikre at informasjon unntatt offentlighet ivaretas.

9.5 Administrasjon

Informasjonen som behandles kategoriseres om personopplysninger. Administrasjonen har systemer der informasjon behandles som igjen har betydning for tjenester som ytes.

9.6 Oppvekst og kultur

Informasjonen som behandles kategoriseres som personopplysninger som kan inneholde særlige kategorier. Det er informasjon om elever som kan, både direkte og indirekte, inneholde helseopplysninger. I tillegg behandles informasjon om flere barn som i utgangspunktet har krav på høyere beskyttelse som mindreårige. Risikoen ved behandling er høy i utgangspunktet. Det vil være avgjørende å sørge for gode sikringstiltak i alle ledd for å senke risikoen til et akseptabelt nivå.

9.7 Publikumstjenester

Informasjonen som behandles kategoriseres som offentlig, personopplysninger i form av saksopplysninger eller kontaktinformasjon. Risikoen ved behandling er lav i utgangspunktet, og informasjon kan gjenskapes om noe går tapt. Kildene til informasjon vil ligge sikret innenfor de tjenester som er tilgjengelig på internett. Lavere krav sikringstiltak for å beskytte publikumstjenester, kun for å sikre tilgjengelighet og integritet.

10 Verdivurdering og identifisering av informasjonsverdier i kommunene

FARTT kommunene har gjennomført verdivurderinger innafor prioriterte områder/sektorer. Oppdraget ble gitt til ledergruppene i hver kommune, i samråd med kommuneledelsen.

Arbeidsgruppa som har fulgt opp arbeidet etter forvaltningsrevisjonen, har vært samstemte i at man ønsket å forholde seg til et overordnet nivå ute i kommunene. Ledergruppene i kommunene sluttet seg til dette når kommunene skulle gjennomføre verdivurderingene.

Innafor mange områder finnes det en rekke fagsystemer som utgjør store verdier for kommunene, men i dette tilfellet har man forholdt seg til **prioriterte områder**, disse samsvarer også med det som er beskrevet i beredskapsplanen til FARTT.

Verdivurdering samlet, se vedlegg 23.3

11 Tilgangsstyring

(Svar på pkt. 3 i forvaltningsrevisjonen).

Innledning:
Innføring av IAM system ble vedtatt ved behandling av investeringsplanen FARTT 2023-2027.
Et IAM system sikrer at brukere blir opprettet, endret og fjernet på en trygg og sikker måte. Alle brukere må identifisere seg og godkjennes med ID-porten.
Dette er en skybasert løsning som er knyttet med Visma HRM, dette er modersystemet som delegerer rettigheter, lisenser og tilganger basert på stilling. Dette er en sikker løsning som gjør at man får mer automatiserte prosesser og bruker mindre tid på manuell oppfølging og ad-hoc løsninger.
Systemene er knyttet opp mot fagsystemer, teknisk infrastruktur og eksisterende økosystem.
Løsningen er Hjemlet i lov.

- NSM Grunnprinsipper 2.6: "Ha kontroll på identiteter og tilganger".
- Normen 5.2: "Tilgangsstyring" og 5.2.1: "Autorisering".
- GDPR Personvernforordningen artikkel 17 ("Rett til sletting") og artikkel 32 ("Sikkerhet ved behandlingen").
- Tilgang til helseopplysninger er i tillegg regulert i flere lover og forskrifter.

Rutine for eAdm, se vedlegg 23.4
Rutine for utstyrshåndtering, se vedlegg 23.5

12 Avvik og håndtering av avvik

(Svar på pkt. 4 i forvaltningsrevisjonen).

IKT Fjellregionen viser til Datatilsynets nettside som beskriver virksomhetens plikter til håndtering av avvik, dette relatert til avvik knyttet til personopplysningssikkerhet.

Dersom det skjer et brudd på personopplysningssikkerheten, også kalt avvik, har den behandlingsansvarlige som hovedregel plikt til å melde det til Datatilsynet så snart som mulig.

Veiledning om håndtering av avvik med melding til Datatilsynet og informasjon til de berørte finnes på Datatilsynets nettsider: https://www.datatilsynet.no/avvik

IKT Fjellregionen har prosedyre for avviksbehandling personvernsaker, dette ligger i styringssystemet for informasjonssikkerhet, Compilo.

Mal for avvikshåndtering følger vedlagt, den er hentet fra Datatilsynet og gir et grunnlag for videre avvikshåndtering.

Jf. Datatilsynets vurderinger vil feil i programvare og maskinvare ikke regnes som avvik i denne sammenhengen, og skal rapporteres til IT-drift.

Avvikshåndtering, se vedlegg 23.6

13 IKT hendelser

Arbeidsgruppas vurdering er at IKT hendelser også kan være avvik, særlig dersom hendelsen har en viss varighet og/eller det berører viktige fagsystemer eller verktøy som støtter opp om daglig viktig tjenesteproduksjon i virksomheten. I noen tilfeller kan det berøre liv og helse dersom et viktig fagsystem ikke er tilgjengelig og man ikke kan få tak i nødvendig informasjon om pasienter/brukere.

Vurdering videre er at det bør være lav terskel for å melde IKT hendelser, også som avvik, da det i ytterste fall kan ha store konsekvenser. Det oppfattes i dag å være forholdsvis høy terskel for å melde avvik innen IKT i FARTT.
Fra et driftsmessig perspektiv så skal alle hendelser som har betydning for sikkerhet, personvern, oppetid og funksjonalitet som minimum loggføres, videreført som avvik. Dette sikrer historikk og dokumenterer de enkelte hendelsene.

14 Risikostyring og risikovurdering av informasjonssikkerheten i FARTT

(Svar på pkt. 1 i forvaltningsrevisjonen)

FARTT sine krav til informasjonssikkerhet for IT-systemer og til prosesser for linjeledelse og prosjekter, skal være basert på risikovurdering. Ansvarlige skal være klar over FARTT sine trusler og sårbarheter og ha et bilde av hva virksomheten kan tåle av direkte og indirekte tap. Risikovurderinger skal også vurderte risiko knyttet til egne ansatte eller personer som er påvirket av virksomhetens aktiviteter.

Risikovurdering kjennetegnes av at det er en systematisk gjennomgang av trusler og sårbarheter. I dette ligger å vurdere og analysere i forhold til det som er mest kritisk eller det man tror man har mest igjen for. Ved en risikovurdering så må en kartlegge risiko og dernest planlegge og gjennomføre tiltak som bidrar til akseptabel risiko

14.1 Lovkrav

Personopplysningsforskriften § 2-4 sier følgende om Risikovurdering:
Det skal føres oversikt over hva slags personopplysninger som behandles. Virksomheten skal selv fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger. Den behandlingsansvarlige skal gjennomføre risikovurdering for å klarlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd. Ny risikovurdering skal gjennomføres ved endringer som har betydning for informasjonssikkerheten. Resultatet av risikovurderingen skal sammenlignes med de fastlagte kriterier for akseptabel risiko forbundet med behandling av personopplysninger, jf. Første ledd og § 2-2. Resultatet av risikovurderingen skal dokumenteres.

14.2 Risiko

Risiko knyttes til uønskede hendelser som kan få konsekvenser, eller sagt på en annen måte handler risiko om sannsynligheten for og konsekvensen av mulige hendelser som kan skje.
(definert så handler det om potensielle avvik fra det forventede eller potensielle avvik fra våre mål.

14.3 Sannsynlighet og konsekvens

I risikovurderingen er det tatt utgangspunkt i KINS (Kommunal informasjonssikkerhet) sin modell, der 5 kombinasjoner av nivå på **sannsynlighet og konsekvens** er brukt for å estimere risikonivå, Se tabeller under:

Sannsynlighet		Beskrivelse
1	**Lite sannsynlig**	Vil sannsynligvis ikke skje. Har aldri hørt om.
2	**Mindre sannsynlig**	Vil sannsynligvis ikke skje. Har hørt om.
3	**Sannsynlig**	Vil kunne skje en eller flere ganger i tidsperioden.
4	**Meget sannsynlig**	Vil kunne skje flere ganger i året.
5	**Svært sannsynlig**	Vil kunne skje ukentlig/daglig.

Konsekvens		Helse, miljø og sikkerhet (Inklusiv Psykososialt arbeidsmiljø)	Pasient/Brukersikkerhet	Økonomi	IT og informasjonssikkerhet
1	**Ubetydelig**	Ubetydelig personskade/slitenhet. Påvirker ikke prestasjonsnivået. Ikke fravær.	Små enkelt personskader/sykdom	Ubetydelig for budsjett Mindre enn 10 000 kr	Lite, opprettelig økonomisk tap, Opplysninger kan ha kommet på avveie
2	**Mindre alvorlig**	Mindre forbigående personskade/slitenhet/sykdom. Kortvarig belastning på arbeidsmiljøet. Påvirker prestasjonsnivået i liten grad for enkelte. Fravær maks tre dager.	Flere små personskader/sykdommer	Minimal effekt for budsjett 10.000 - 100.000 kr	Lite, opprettelig økonomisk tap. Følsomme opplysninger på avveie
3	**Alvorlig**	Betydelig personskade/sykdom/utmattelse/psykisk reaksjon. Alvorlig, langvarig belastning på arbeidsmiljøet. Påvirker prestasjonsnivået for flere. Kan gi lengre fravær.	Alvorlig enkeltpersonskader/sykdom	Små konsekvenser for økonomi og for tjenestetilbudet 1oo.ooo - 1 millioner kr	Betydelig men opprettelig økonomisk tap Tap av anseelse eller integritet Personopplysninger på avveie
4	**Kritisk**	Flere enkelttilfeller av langvarige helseplager. Vedvarende, stor og langvarig belastning på arbeidsmiljøet. Flere langtidssykemeldte. Påvirker prestasjonsnivået for hele avdelingen.	Flere alvorlige skader/sykdommer	Alvorlige konsekvenser for budsjett og tjenestetilbud 1 - 5 millioner kr	Tap av helse Uopprettelig økonomisk tap Uopprettelig tap av helse eller integritet Personopplysninger på avveie
5	**Meget kritisk**	Dødsfall. Mange alvorlig, langvarige syke. Stor mistrivsel med omfattende effekt på miljøet. Prestasjonsnivået for avdelingen er betydelig nedsatt.	Mange alvorlige skadde/syke Dødsfall	Dramatiske konsekvenser for budsjett og tjenestetilbud Mer enn 5 millioner kr	Tap av liv Vedvarende helsetap Betydelig og uopprettelig økonomisk tap Alvorlig tap av anseelse og integritet Personopplysninger på avveie

14.4 Akseptabelt risikonivå

Dette handler om å fastsette et nivå for risiko som virksomheten skal kunne leve med.
Følgende matrise er brukt som utgangspunkt når det gjelder akseptabel risiko:

		Konsekvens				
		Ubetydelig (1)	**Mindre alvorlig (2)**	**Alvorlig (3)**	**Kritisk (4)**	**Meget kritisk (5)**
Sannsynlighet	**Svært sannsynlig (5)**	5	10	15	20	25
	Meget sannsynlig (4)	4	8	12	16	20
	Sannsynlig (3)	3	6	9	12	15
	Mindre sannsynlig (2)	2	4	6	8	10
	Lite sannsynlig (1)	1	2	3	4	5

Risikonivå	**Tiltak**
1-5	Risiko aksepteres uten at det iverksettes tiltak
6-12	Tiltak iverksettes ut fra en kost/nytte vurdering
15-25	Tiltak iverksettes umiddelbart for å redusere risiko til gult/grønt nivå

15 Risikovurdering i FARTT

15.1 Metode

I FARTT sin risikovurdering er det tatt utgangspunkt i KINS (kommunal Informasjonssikkerhet) sin modell, der 5 kombinasjoner av nivå på **konsekvens og sannsynlighet**, er brukt for å estimere risikonivå.
IKT Fjellregionen har gjennom dialog med IKT Valdres, fått tilgang på nyttig informasjon som har vært viktig grunnlag for gjennomføring av ROS.

Følgende momenter lagt til grunn for gjennomføring:

- Risikobeskrivelse, dvs. hva kan inntreffe
- Sårbarheter/svakheter
- Eksisterende risikoreduserende tiltak
- Begrunnelse for vurdering av sannsynlighet og konsekvens
- Betydning ift KIT
- Verdi på sannsynlighet, konsekvens og risiko
- Aksepterbar risiko
- Tiltak
- Risiko etter tiltak

Risikovurderingen er gjennomført av operativ sikkerhetsgruppe i FARTT.
Risikovurderingen er i etterkant lagt frem for arbeidsgruppa forvaltningsrevisjon IKT sikkerhet.
Den er presentert for beredskapskoordinatorer i FARTT kommunene og den er forankret i styret i FARTT.

16 Resultater etter gjennomført risikovurdering i FARTT

Risikovurderingen i FARTT lister opp ulike hendelser basert på relevante risiko beskrivelser.
Flere av disse er med bakgrunn i egne vurderinger, flere er hentet fra IKT Valdres, da FARTT har fått lov til å benytte mye av deres materiale. 13 hendelser har oppnådd en risikofaktor på 10 eller mere. For alle disse er det beskrevet ulike tiltak, de aller fleste har også beskrevet strategi for videre oppfølging.

Resultater etter gjennomført ROS, se vedlegg, 23.7**. Gjør oppmerksom på at denne informasjonen er unntatt offentlighet.**

17 Oppfølging og tiltak

Sikring mot angrep, cyberangrep, RansomWare, DDoS, Phishing, andre angrepsformer?

FARTT har gode systemer på plass for å beskytte seg mot angrep og andre sikkerhetshendelser. Men teknologi og trusler utvikler seg raskt, så det er viktig å oppdatere og revidere disse systemene regelmessig.

Ingen IT-systemer kan være 100 % sikre, og det vil alltid finnes sårbarheter. I dag har FARTT ingen ekstern beskyttelse mot tjenestenektangrep (DDoS), som kan føre til at internettforbindelsen blir utilgjengelig i perioder. Imidlertid så har vi løsninger som kan redusere og forhindre DDoS angrep på våre nettverksenheter, som vil beskytte interne ressurser slik at de fortsatt er operative. Et slikt angrep kan vare fra 10 minutter til flere dager. Beskyttelse mot ekstern beskyttelse av tjenestenektangrep kan kjøpes som en tilleggstjeneste fra vår internett-leverandør og vil være lang mer effektivt enn lokale løsninger.

Angrep som løsepengevirus (ransomware) og nettfisking (phishing) kan være utfordrende å forhindre, fordi ansatte kan ved et uhell klikke på skadelige lenker eller dokumenter. Det er derfor viktig at kommunen bygger god virksomhetskultur med sikkerhetsaspekter, med god opplæring og bevissthet blant de ansatte. Selv om det finnes tekniske verktøy som kan redusere risikoen, kan de aldri gi full beskyttelse.

Beskyttelse av identiteter og enheter som datamaskiner og mobiltelefoner er kritisk. Det er viktig å ha overvåkingssystemer som kan oppdage unormal aktivitet tidlig. Vi er klar over de svakhetene vi har i dag, men for å forbedre sikkerheten ytterligere, kan det være nødvendig å investere mer i både kompetanse og bedre tekniske løsninger. I tillegg er det viktig at det er en god sikkerhetskultur blant alle ansatte, og at alle ansatte får en god oppfølging i hele ansettelsesforholdet. Sosial manipulasjon er også en teknikk som begynner å bli utbredt og er en sårbarhet som blir aktivt brukt siden enheter blir mer beskyttet.

Fysisk sikring og begrenset tilgang til sentrale kommunale bygg blir også mer nødvendig, for å beskytte mot uvedkommende som kan koble seg til utstyr i nettverket.

17.1 Konsekvenser for klima, miljø, omdømme, økonomi mm

FARTT forholder seg til sakvurderinger i kontrollutvalgene, ved at konsekvenser for klima og miljø ikke er relevant i denne sammenheng.

Når det gjelder konsekvenser for omdømme og økonomi, så vil dette avhenge av flere faktorer.
Ulike hendelser, som også fremgår av ROS, vil kunne påvirke omdømme og økonomi.
Resultater fra revisjoner, sårbarhetsvurderinger eller tester kan påvirke omdømme, med påfølgende krav om tiltak, kan dette også påvirke økonomien.

18 Hendelseshåndtering og gjenoppretting

(Svar på pkt. 5 i forvaltningsrevisjonen).

Det samlede beredskaps planverket for FARTT ligger i Compilo. Beredskapsplanen med hoveddokument og vedlegg gjelder i beredskapssammenheng.
Hendelseshåndtering er viktig del av beredskapen og skal bygge på en plan med rutiner og prosedyrer som skal utføres før, under og etter at en hendelse har oppstått.
Det er mange ulike hendelser som kan oppstå og det vil naturlig være noen sammenfallende måter å løse disse på, samtidig som de også vil kunne være like på enkelte områder.

Det jobbes fortsatt med prosedyrer og rutiner for ulike hendelser som kan oppstå. Som tidligere nevnt så er det mange hendelser som kan påvirke FARTT sin tjenesteleveranse. Prosedyrer og rutiner som kan være alt fra bortfall av sentrale og/eller lokale nettverksenheter, servere, kommunikasjonsbrudd, disk feil til cyberangrep.

19 Cybersikkerhet, kunnskap og kompetanse

FARTT har i dag tjenester gjennom KommuneCERT, tidligere HelseCERT som bidrar til økt fokus på overvåking av trafikk og monitorering av unormale hendelser utafor nettet til FARTT/kommunene.
Sårbarheter og trusler rapporters og meldes fra KommuneCERT og dette er viktig med tanke på å ha forutsigbarhet rundt det overordna trusselbildet.
Kompetanse på Cybersikkerhet og generell IT sikkerhet er mangelvare i Norge i dag, og mange har et utstrakt behov for å løse dette innen kort tid.

FARTT kjøpte i 2024 verktøy for sårbarhetsskanning fra en leverandør, som ukentlig skanner internt nettverk. Dette verktøyet kan også brukes til å skanne tjenester i sky. Verktøyet er viktig for å kartlegge alle sårbarheter internt.

I tillegg kjører FARTT hver måned Hurtigtest av HelseCERT, som er et verktøy som skanner sårbarheter og oversender resultater til HelseCERT. Data blir brukt av HelseCERT for å kartlegge tjenester, sårbarheter og blir også benyttet i kvartalsvis rapporter om status, i tillegg til portskanning fra kjente IP-adresser.

FARTT kommunene er små enheter med begrenset ressurser, og vi mangler både kompetanse og personell til å utføre oppgavene på en god måte. Dette kan løses ved å videreutvikle kompetansen hos ansatte eller rekruttere personell med fagkompetanse på IT-sikkerhet. Vi er imidlertid også helt avhengig av at våre valgte leverandører på sikkerhetsverktøy vi benytter er langt framme på de tjenestene vi benytter fra de.
Kommunene må ta større eierskap i å jobbe strategisk med sikkerhetskultur blant ansatte og ha intern kompetanse på grunnleggende IT-sikkerhet og informasjonssikkerhet.

20 Generelle sikkerhetstiltak

20.1 Beredskap

FARTT utøver i dag driftsoppdrag og beredskap innafor ordinær arbeidstid, på hverdager mellom kl. 08.00 – 15.30. I tillegg gjennomføre periodisk vedlikehold hver måned, i tillegg ekstraordinært vedlikehold utenom dette, som varsles.
Hendelser utenfor ordinær arbeidstid blir i veldig stor grad ivaretatt, men dette er på frivillig basis uten at det er fastsatt spesifikk vakt eller beredskapsordning.
Det er påpekt at FARTT er sårbare i de perioder det ikke er bemannet drift og overvåking.
Det er viktig for framtida at man sammen gjør risikovurderinger av dette og at man treffer tiltak som kan bedre situasjonen.
Samtidig så er det ikke kommet krav eller behov fra eiere/kommuneledelsen at man må ha vakt/beredskap ut over dagens oppdrag.

Ved kriser eller hendelser som defineres som kriser, iverksettes FARTT sin beredskapsplan, kriseledelse tar del i videre aksjoner.

FARTT har som mål å gjennomføre beredskapsøvelser hvert år.
I 2024 er det planlagt en øvelse ila høsten, dette i samråd med beredskapsansvarlige i kommunene.

20.2 Infrastruktur, fiber og mobilnett, redundans

FARTT er del av en godt utbygd infrastruktur i Nord-Østerdals regionen.

Nettet består av fiberforbindelser mellom FARTT datasenter og kommunene, samt egne fiberforbindelser ut til kommunale lokasjoner.
FARTT har siden 2012 hatt Eidsiva Bredbånd som leverandør av bredbåndstjenester som også kommunene benytter. Kapasitet, stabilitet og tilgjengelighet/oppetid er viktige faktorer.
Det er inngått ny avtale med Eidsiva Bredbånd i 2024 og avtaleperioden er forlenget ift. tidligere avtaler.
Dette sikrer forutsigbarhet på leveranse, sikkerhet og oppetid for kunden, FARTT og eierkommunene.
Redundans er også viktig i denne sammenheng.

Vi opplever Eidsiva Bredbånd som en seriøs aktør med søkelys på leveranse og kvalitet.

Oversikt fiberkommunikasjon til FARTT, se vedlegg, 23.8

Når det gjelder mobilnettet så har både FARTT og kommunene avtale med Telia (Phonero).
Bedriftsabonnement og trafikk inngår i leveransene. Redundans er også viktig del av disse avtalene.

20.3 NSM grunnprinsipper

Siden 2023 har den operative sikkerhetsgruppen i FARTT jobbet med å gjennomgå alle prinsippene og tiltakene i NSMs Grunnprinsipper for IKT-sikkerhet. Disse prinsippene er delt inn i fire kategorier og inneholder totalt 21 prinsipper med 118 sikkerhetstiltak.

I 2023 kartla sikkerhetsgruppen alle tiltakene og laget en strategi med en prioritert liste over sikkerhetstiltak. I løpet av 2024 vil alle tiltakene være dokumentert, og en ny prioritert liste vil bli laget. Gruppen vil ha minst fire møter i året for å revidere tiltakene.

Noen av tiltakene krever investering i nye sikkerhetsløsninger, oppgradering av lisenser på eksisterende programvare, og strengere regler for hvordan applikasjoner og enheter brukes av kommunens ansatte.

Nye sikkerhetstiltak vil bli innført regelmessig og vurdert i sammenheng med den prioriterte listen.

20.4 Sikkerhetsnøkler

Styret i FARTT har i 2024 vedtatt å bevilge penger til et sikkerhetstiltak med innføring av sikkerhetsnøkler for alle ansatte i FARTT. Sikkerhetsnøkkel er enda sikrere enn Authenticator APP, da du må være fysisk til stede for å logge deg inn. Nøkkelen kan brukes på Windows, Mac og Google Chromebooks.

FIDO-alliansen, som består av Google, Apple og Microsoft, jobber med å gjøre pålogging enklere for brukere ved å innføre passnøkler for en passordfri hverdag. En sikkerhetsnøkkel er en fysisk enhet som lagrer passnøkler, og hver nøkkel er personlig. Hver ansatt får sin egen sikkerhetsnøkkel, hvor passnøkkelen (brukerens identitet) for kommunekontoen er lagret. Nøkkelen er beskyttet med en PIN-kode og krever fysisk tilstedeværelse for pålogging.

Sikkerhetsnøkler erstatter pålogging med passord eller mobilapper for godkjenning. Hver gang man logger inn i systemer eller enheter levert av FARTT, må sikkerhetsnøkkelen brukes. Bruken av godkjenningsapper som f.eks. Microsoft Authenticator har vært utfordrende fordi ikke alle ansatte har arbeidsgivertelefon eller en moderne telefon. Med sikkerhetsnøkler får alle ansatte lik pålogging uten å måtte bruke privat mobiltelefon.

Sikkerhetsnøkler gir i dag det høyeste sikkerhetsnivået for autentisering. Alle brukere i FARTT-samarbeidet skal ha tatt i bruk sikkerhetsnøkler innen 1. januar 2025. Det vil bli utarbeidet rutiner og prosedyrer for utlevering, innlevering og videre anskaffelser.

20.5 Anskaffelse sikkerhetstjenester

I samarbeid med DIGI Innlandet er FARTT med på en felles anskaffelse av sikkerhetstjenester. Prosjektet startet våren 2024, og avtalen med leverandøren vil bli inngått i oktober 2024 etter en offentlig anskaffelsesprosess ledet av Innkjøpskontoret. Gjøvik kommune vil være eier av rammeavtalen, og FARTT kan fritt kjøpe tjenester fra leverandørens tjenestekatalog.

Tjenestene som kan kjøpes inkluderer sikkerhetsovervåking med tilhørende SOC-tjenester (inkludert aktiv respons) 24/7/365, sikring av alle enheter, avtale om et Incident Response Team (IRT) ved hendelser, lagring

av sikkerhetslogger i skyen, og konsulentbistand. I tillegg kan FARTT kjøpe andre sikkerhetstjenester fra tjenestekatalogen til en avtalt pris.

Avtalen med leverandøren varer i 3 år og gir god overvåking og aktiv respons døgnet rundt.
Et Incident Response Team (IRT), eller hendelseshåndteringsteam på norsk, er en gruppe personer som jobber med å håndtere problemer eller angrep som kan oppstå i et IT-system. Når noe går galt, som et datainnbrudd, virus, eller teknisk feil, sørger dette teamet for å reagere rasktog vil bistå FARTT med å begrense skadene, fikse problemet og sikre at det ikke skjer igjen.

Et Security Operations Center (SOC), eller sikkerhetsovervåkingssenter på norsk, er et sted hvor IT-eksperter overvåker og beskytter organisasjonens datasystemer hele tiden, døgnet rundt. De følger med på nettverket, ser etter mistenkelig aktivitet, og reagerer på potensielle trusler som hackingforsøk, løspengeangrep eller virus. Du kan tenke på en SOC som en digital "vaktstasjon" hvor sikkerhetsvakter passer på og beskytter organisasjonens data mot angrep og uhell. Hvis noe skjer, tar de raskt grep for å stoppe det og sørge for at alt er trygt igjen.

20.6 Kompetanse-ressurs innafor informasjonssikkerhet i FARTT

FARTT har stort fokus på å tilknytte seg riktig kompetanse og kunne ha nok ressurser til å ivareta arbeidet med IKT sikkerhet og personvern.
Sikkerhetsleder har i 2024 startet på videreutdanning i *Grunnleggende studie i personvernregelverk* og *Digital sikkerhetskultur og Personvern* i regi Høgskolen i Innlandet.
Videre har selskapet styrket kompetanse med nytilsatt ressurs som startet i august og som vil støtte opp om arbeidet med informasjonssikkerhet og personvern.

Der FARTT ikke har spesifikk kompetanse i dag som Cybersikkerhet, hendelseshåndtering, overvåking-SOC tjenester og IRT, Incident Response Team, så er dette områder der selskapet vil kunne kjøpe hyllevare som resultat av et samarbeide i Innlandet fylke, der man går sammen om anskaffelse av IKT sikkerhetstjenester. Samtidig vil FARTT jobbe videre for å styrke sin egen kompetanse på områdene.
FARTT er også i dialog med kommuneledelse i FARTT når det gjelder å avklare behovene rundt fremtidig ressurs Personvernombudet.
FARTT mener at personvernombudet må ha større stilling enn dagens 20 %.

Når det gjelder generell kompetanse innafor IKT sikkerhet og personvern ute i kommunene, så er FARTT av den oppfatning at dette er et om råde der kommunene må ta et enda større ansvar for å bygge en solid sikkerhetskultur og øke bevissthet og kompetanse blant ansatte. For få har ikke noe bevisst forhold til tematikken.

20.7 KINS/KS informasjonskampanje-program

I samarbeid med KS og en arbeidsgruppe bestående av flere kommuner, har oppdragstaker laget en informasjonskampanje. Kampanjen består av ti temaer – der ett tema rulles ut per måned i totalt ti måneder. Hver måned har et klart budskap, og målet er å sikre at de kommuneansatte endrer vaner.
Hver måned oppdateres nettsiden til FARTT med nytt tema, samt at medlemmer av IKT Sikkerhetsutvalg får ansvaret for å henge opp plakater og informere internt i kommunen.
Det er viktig at avdelingsledere tar opp hvert tema i avdelingsmøter, slik at alle ansatte får informasjon og kan gjennomføre anbefalte tiltak fra temaet. Kampanjen kjøres årlig i FARTT samarbeidet for alle ansatte.

21 Oppsummering

Arbeidet med IKT sikkerhet, informasjonssikkerhet og personvern er et kontinuerlig arbeid der FARTT og kommunene må jobbe videre med oppfølging i fortsettelsen.
Det er viktig at eiere, ansatte og brukere av løsninger har tillit til at sikkerhet ivaretas på best mulig måte, at selskapet og kommunene jobber aktivt med forbedringer og at man sammen er rustet til å håndtere fremtidige sikkerhetsutfordringer.
Innbyggere skal føle seg sikre på at all informasjon blir behandlet ihht. lovverket og at konfidensialitet, Integritet og tilgjengelighet ivaretas.

Forvaltningsrevisjon har gitt en uavhengig vurdering av hvor selskapet står i forhold til IKT sikkerhetsarbeidet, krav, risikoer og trusler.
Revisjonen påpeker svakheter på noen områder, samtidig har FARTT også gjort godt arbeid på andre områder. Dette oppfattes som forbedringsområder samtidig som det gir læring.

Kommunene har økt fokus på arbeid med informasjonssikkerhet men det ligger fortsatt et større potensiale i å utvikle sikkerhetsarbeidet i egne organisasjoner, bygge bedre sikkerhetskultur og øke bevissthet blant ansatte. Det er et lederansvar å følge opp dette, samtidig som resten av organisasjonen må involveres.

FARTT samarbeider godt med kommunene og ulike aktører. I regi DIGI Innlandet er man med på felles anskaffelser ift. hyllevare innen sikkerhetsprodukter, i tillegg til at samarbeidet bygger mye kunnskap på tvers av kommuner og IKT samarbeid.

22 Endringer ved revisjon

Dato	Versjon	Endring	Person

Endelig vedtatt dokument legges i Compilo, i PDF format

23 Vedlegg

23.1 GDPR prosessen
23.2 IKT sikkerhetsutvalg for FARTT mandat
23.3 Verdivurdering samlet
23.4 Rutine for eADM FARTT
23.5 Rutine for utstyrshåndtering
23.6 Avvikshåndtering
23.7 Resultater etter gjennomført ROS
23.8 Oversikt fiberkommunikasjon

Tynset 21.09.2024

Sverre Jenssen, daglig leder FARTT
Kai Røen, sikkerhetsleder FARTT
Harald Sørli, styreleder FARTT
Amund Aarvelta, assisterende kommunedirektør Tynset kommune
Malin Wassdahl, kommunedirektør Folldal kommune