ALVDAL KOMMUNE
Stab

Konsek Trøndelag Iks
Postboks 2564
7735 Steinkjer

Vår ref.	Deres ref.	Saksbehandler	Dato
24/130 - 3		Erland Horten	30.01.2024

Forvaltningsrevisjon IKT-sikkerhet

Kommunestyret har i møte 25.01.2024 fattet følgende vedtak 09/24:

Forvaltningsrevisjonsrapporten IT-sikkerhet av 06.11.23 tas til orientering.
Alvdal kommune følger revisors anbefalinger og kommunestyret ber eierrepresentanten for Fjellregionen IKT i samarbeid med kommunedirektøren om 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. *Avklarer og dokumentere organiseringen av informasjonssikkerhetsarbeidet og være konsekvent i benevnelsen av roller.*
3. *Vurderer å sikre at rutinen for tilgangsstyring etterleves ved endring og avslutning av arbeidsforhold, herunder også innlevering av kommunens datautstyr.*
4. *Vurderer behovet for dokumentasjon av IKT-hendelser som grunnlag for evaluering og læring.*
5. *Utarbeide en plan for hendelseshåndtering og gjenoppretting.*

Eierrepresentanten og kommunedirektøren rapporterer til kontrollutvalget om iverksatte tiltak innen 01.10.24

Med hilsen

Erland Horten
rådgiver

Dokumentet er elektronisk godkjent og har derfor ingen signatur

Mottakere:

Ikt Fjellregionen Iks	Tynset Kommune Rådhuset	2500	Tynset

ALVDAL KOMMUNE

Saksframlegg

Vår ref.:	Dato:	Saksbehandler:
24/130 - 2	15.01.2024	Per Arne Aaen

Behandling av saken:

Saksnr.	Utvalg	Møtedato
09/24	Kommunestyret	25.01.2024

Forvaltningsrevisjon IKT-sikkerhet

Kortversjon av saken

Kontrollutvalget Tynset kommune besluttet å gjennomføre en forvaltningsrevisjon for IKT-sikkerhet i IKT Fjellregionen IKS (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. Kontrollutvalget i Alvdal kommune behandlet saken 5.desember, og oversender saken til kommunestyret med innstilling til vedtak.

Vedlegg

Møtebok forvaltningsrevisjon av IKT-sikkerhet - IKT Fjellregionen - Rapport	15.01.2024
06.11.23 Revisjonsrapport	15.01.2024

Saksopplysninger

Kontrollutvalget Tynset kommune besluttet å gjennomføre en forvaltningsrevisjon for IKT-sikkerhet i IKT Fjellregionen IKS (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. Kontrollutvalget i Alvdal kommune behandlet saken 5.desember, og oversender saken til kommunestyret med innstilling til vedtak.

Kontrollutvalgets saksfremstilling og forvaltningsrevisjonsrapporten er vedlagt saken. Kontrollutvalget innstiller overfor kommunestyret følgende:

Forvaltningsrevisjonsrapporten IT-sikkerhet av 06.11.23 tas til orientering.

Alvdal kommune følger revisors anbefalinger og kommunestyret ber eierrepresentanten for Fjellregionen IKT i samarbeid med kommunedirektøren om 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. *Avklarer og dokumenterer organiseringen av informasjonssikkerhetsarbeidet og være konsekvent i benevnelsen av roller.*
3. *Vurderer å sikre at rutinen for tilgangsstyring etterleves ved endring og avslutning av arbeidsforhold, herunder også innlevering av kommunens datautstyr.*
4. *Vurderer behovet for dokumentasjon av IKT-hendelser som grunnlag for evaluering og læring.*
5. *Utarbeider en plan for hendelseshåndtering og gjenoppretting.*

Eierrepresentanten og kommunedirektøren rapporterer til kontrollutvalget om iverksatte tiltak innen 01.10.24

Kommunestyret i Tolga behandlet forvaltningsrevisjon i desember og la til et tilleggspunkt, punkt 6 slik:

Får tilgang til økt kompetanse på cyber-sikkerhet.

Fra revisors rapport gjengis problemstillinger det er jobbet med, konklusjoner anbefalinger og vurdering med konklusjon:

Revisors problemstillinger med konklusjoner:

Det er utarbeidet 5 problemstillinger, og revisor har konkludert for hver av de.

<u>Styrer selskapet informasjonssikkerheten på en tilfredsstillende måte?</u>

Undersøkte forholdene avviker i noen grad fra revisjonskriteriene. Det er et forbedringspotensial knyttet til definering av roller og ansvar knyttet til informasjonssikkerhetsarbeidet, og oppdatering av styrende dokumenter.

<u>Blir sikkerhetsrisikoer identifisert og håndtert?</u>

Undersøkte forhold avviker i stor grad fra revisjonskriteriene. Selskapet har kartlagt enheter og programvare som er i bruk, men innrullerte klienter i et forvaltningssystem først i 2023. Selskapet har kontroll på identiteter og tilganger på ansatte i kommunene, men det er et forbedringspotensial knyttet til gjestebrukere samt å begrense bruken av høyt privilegerte brukerkontoer. Kvaliteten på gjennomførte risiko- og sårbarhetsvurderinger vurderes å være svak.

<u>Blir informasjon og informasjonssystemer beskyttet iht. beste praksis?</u>

De undersøkte forhold avviker i stor grad fra revisjonskriteriene. Det er avdekket flere betydelige svakheter i IKT-arkitektur og konfigurering. Selskapet gjør heller ingen sikkerhetsrevisjoner av underleverandører eller test av gjenoppretting og disaster recovery. Rutinene knyttet til sikkerhetskopiering av virksomhetsdata for kommunene synes tilstrekkelig ivaretatt.

<u>Hvordan oppdages avvik og mulige trusler mot virksomheten?</u>

De undersøkte forhold avviker i noen grad fra revisjonskriteriene. Det er etablert rutiner for sikkerhetsovervåkning og sårbarhetsscanning, men disse omfatter ikke oppfølging av varsler utenfor normal arbeidstid. Videre vurderer revisjonen at FARTT ikke har spesifikk kompetanse for å vurdere og håndtere cyberhendelser på en forsvarlig måte. Det er ikke tidligere gjennomført inntrengingstester.

<u>Blir hendelser håndtert på en tilfredsstillende måte?</u>

De undersøkte forhold avviker i noen grad fra revisjonskriteriene. Selskapet har nylig revidert beredskapsplanverket, men handlingsplaner for utvalgte scenarioer virker ikke å være ferdigstilt.

Selskapet gjennomfører evalueringer etter øvelser og hendelser, men har ikke rutiner for å gjennomføre tekniske øvelser. Dette gjør selskapet sårbart i håndteringen av nye og ukjente hendelser, ref. erfaringer fra hendelsen som inntraff høsten 2022

Revisjonens anbefalinger:

1.Tydeliggjøre, beskrive og plassere det overordnede ansvaret for informasjonssikkerhet i FARTT.

2.Innføre standard herdeprofiler basert på beste praksis for PCer, servere og mobiltelefoner og innføre sikkerhetskonfigureringer i Microsoft 365 og Azure AD i henhold til beste praksis.

3.Etablere rutiner for sikkerhetsrevisjoner basert på kritikalitet og risiko.

4.Tilknytte seg en leverandør med spesifikk kompetanse innen cybersikkerhet som kan bistå med vurdering og håndtering av varsler og/eller ved cyberhendelser.

Vurdering og konklusjon:

Revisjonen vurderer at FARTT har hatt et økende fokus på IT-sikkerhet, men at det gjenstår vesentlige forbedringer for å kunne stadfeste at FARTT har et tilfredsstillende IKT-sikkerhetsnivå.

Gjennomgående for revisjonen er at FARTT har innført forbedringer det siste året, men at det fremdeles er en del avvik sett opp mot NSMs grunnprinsipper for IKT-sikkerhet og anerkjent beste praksis. Disse avvikene innebærer at FARTT og eierkommunene er sårbare for cyberangrep, og at det ved en større hendelse kan ta lengre tid enn nødvendig å oppdage angrepet, begrense og håndtere skadeomfanget, og gjenopprette systemene.

Revisjonens vurderinger er baseres på disse hovedfunnene:

- *Manglende definering av roller og ansvar knyttet til informasjonssikkerhetsarbeidet*
- *Det er avdekket flere betydelige svakheter i IKT-arkitekturen og konfigureringen til FARTT.*
- *FARTT gjør ingen sikkerhetsrevisjoner av underleverandører.*
- *FARTT har ikke etablert rutiner for å gjennomføre tekniske øvelser. Dette gjør selskapet sårbart i håndteringen av nye og ukjente hendelser.*

Sekretariatet er av den oppfatning at BDO AS har avgitt en ryddig og tydelig rapport i tråd med vedtatt prosjektbeskrivelse.

I kommunedirektørenes høring kommer det frem at det nødvendigvis må være stor grad av samhandling mellom selskapet og kommunene om IKT-sikkerheten. Derfor foreslås det at kommunedirektør og eierrepresentant i fellesskap rapporterer om gjennomførte tiltak.

Revisjonen anbefaler at kontrollutvalget slutter seg til rapporten og innstiller på revisors anbefalinger.

Saksvurdering
Kommunedirektøren anbefaler kommunestyret å følge kontrollutvalgets innstilling til vedtak. Når det gjelder tilleggspunkt som kom inn under behandlingen i Tolga kommune kan det opplyses at det jobbes på flere nivåer for å se på hvordan kommunene best kan løse kompetansebehov på cyber-sikkerhet, forebyggende tiltak og ikke minst kompetanse til å handle ved et pågående angrep og ved gjenoppretting.

Dersom kommunestyret ønsker kan det selv foreslå å vedta slikt punkt.

Det anbefales at kommunene i det FARTT-kommunene i størst mulig grad fatter likelydende vedtak.

Vedtakets konsekvenser for klima og miljø
Ikke relevant

Kontrollutvalgets innstilling
Forvaltningsrevisjonsrapporten IT-sikkerhet av 06.11.23 tas til orientering.

Alvdal kommune følger revisors anbefalinger og kommunestyret ber eierrepresentanten for Fjellregionen IKT i samarbeid med kommunedirektøren om 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. Avklarer og dokumentere organiseringen av informasjonssikkerhetsarbeidet og være konsekvent i benevnelsen av roller.
3. Vurderer å sikre at rutinen for tilgangsstyring etterleves ved endring og avslutning av arbeidsforhold, herunder også innlevering av kommunens datautstyr.
4. Vurderer behovet for dokumentasjon av IKT-hendelser som grunnlag for evaluering og læring.
5. Utarbeide en plan for hendelseshåndtering og gjenoppretting.

Eierrepresentanten og kommunedirektøren rapporterer til kontrollutvalget om iverksatte tiltak innen 01.10.24

Kommunestyret 25.01.2024
Behandling

Votering nr 1 - Votering over forslag
Forslag: **Opprinnelig forslag**
For: 17 stemmer (100%) - Ap 3, H 4, Sp 8, SV/R 1, V 1
Mot: 0 stemmer (0%)
Vedtak
Forvaltningsrevisjonsrapporten IT-sikkerhet av 06.11.23 tas til orientering.
Alvdal kommune følger revisors anbefalinger og kommunestyret ber eierrepresentanten for Fjellregionen IKT i samarbeid med kommunedirektøren om 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. Avklarer og dokumentere organiseringen av informasjonssikkerhetsarbeidet og være konsekvent i benevnelsen av roller.
3. Vurderer å sikre at rutinen for tilgangsstyring etterleves ved endring og avslutning av arbeidsforhold, herunder også innlevering av kommunens datautstyr.
4. Vurderer behovet for dokumentasjon av IKT-hendelser som grunnlag for evaluering og læring.
5. Utarbeide en plan for hendelseshåndtering og gjenoppretting.

Eierrepresentanten og kommunedirektøren rapporterer til kontrollutvalget om iverksatte tiltak innen 01.10.24