Oslo

Kommunerevisjonen

**Rapport 11/2024**

# Teknisk informasjonssikkerhet i Elvia AS

2024

Integritet og verdiskaping

# Siste publikasjoner fra Kommunerevisjonen i Oslo

**Kommunerevisjonens rapporter 2024**

| | |
|---|---|
| Rapport 1/2024 | Vedlikehold og fornyelse av vann- og avløpsnettet |
| Rapport 2/2024 | Eierskapskontroll av Oslobolig AS |
| Rapport 3/2024 | Grønne anskaffelser – klima- og miljøkrav |
| Rapport 4/2024 | Regnskapsrevisjonen 2023 – Oppsummering av utvalgte undersøkelser |
| Rapport 5/2024 | Økonomisk stønad til store barnefamilier |
| Rapport 6/2024 | Spesialpedagogisk hjelp til barn under opplæringspliktig alder<br>Bydel Grorud og Bydel Ullern |
| Rapport 7/2024 | Overordnet styring og koordinering av overvannshåndtering |
| Rapport 8/2024 | Næringsetatens kontroll av skjenkesteder |
| Rapport 9/2024 | Kontraktsoppfølging helse og omsorg |
| Rapport 10/2024 | Grønn material- og energibruk i nybygg |

**Kommunerevisjonens rapporter 2023**

| | |
|---|---|
| Rapport 1/2023 | Eierskapskontroll av Oslo Business Region AS |
| Rapport 2/2023 | Personvern i skoler |
| Rapport 3/2023 | Munchmuseets arbeid med habilitet og forebygging av misligheter og korrupsjon |
| Rapport 4/2023 | Oppfølging av barn og unge etter koronapandemien<br>- Ungdomsskole og skolehelsetjenesten |
| Rapport 5/2023 | Eiendomsforvaltning av Oslo kommunes tomme bygg |
| Rapport 6/2023 | Helsehus i Oslo - Bemanning og kompetanse |
| Rapport 7/2023 | Kommunens bruk av innkjøpsmakt – Samkjøpsavtaler |
| Rapport 8/2023 | Regnskapsrevisjonen 2022 – oppsummering av utvalgte undersøkelser |
| Rapport 9/2023 | Lokal medvirkning i plansaker |
| Rapport 10/2023 | Oppfølging av eierskapskontroller |
| Rapport 11/2023 | Rekruttering og oppfølging av fosterhjem |
| Rapport 12/2023 | Konsulentbruk i Oslobygg KF |
| Rapport 13/2023 | Tilbudet til hjemmeboende med demens og deres pårørende |
| Rapport 14/2023 | Eierskapskontroll av Oslo Nye Teater AS |
| Rapport 15/2023 | Fremkommelighet for personer med funksjonsnedsettelser |
| Rapport 16/2023 | Kvalitet i helsehus |
| Rapport 17/2023 | Oppfølgingsundersøkelse etter rapport 12/2020 Oppfølging av personer med ruslidelser |
| Rapport 18/2023 | Oslo Origos arbeid med digitalisering av Oslo kommune |
| Rapport 19/2023 | Tilfluktsrom |
| Rapport 20/2023 | Personvern og informasjonssikkerhet i helse- og omsorgssektoren |
| Rapport 21/2023 | Økonomisk sosialhjelp og økte levekostnader |

# Forord

Denne rapporten er et resultat av forvaltningsrevisjonsprosjektet om teknisk informasjonssikkerhet i Elvia AS. Undersøkelsen er forankret i kontrollutvalgets vedtak av 29. august 2023 (sak 71) og tilhører området virksomhetsstyring, digitalisering og informasjonssikkerhet, jf. bystyrets vedtak om O*verordnet analyse og plan for forvaltningsrevisjon og eierskapskontroll 2020–2024* av 21. oktober 2020 (sak 283).

Forvaltningsrevisjon er en lovpålagt oppgave for Oslo kommune. Forvaltningsrevisjon er definert slik i kommuneloven § 23-3:

> *Forvaltningsrevisjon innebærer å gjennomføre systematiske vurderinger av økonomi, produktivitet, regeletterlevelse, måloppnåelse og virkninger ut fra kommunestyrets eller fylkestingets vedtak.*

Forvaltningsrevisjon i Oslo kommune gjennomføres i henhold til gjeldende standard for forvaltningsrevisjon i kommuner og fylkeskommuner i Norge (RSK 001).

Forvaltningsrevisjonen er gjennomført av seniorrådgiver Atle Refsdal og seniorrådgiver Roar A. Kristensen (prosjektleder). Kommunerevisjonen har benyttet konsulenter fra EY til å gjennomføre sikkerhetstesting.

Vi vil takke Elvia AS og Byrådsavdeling for kultur og næring for nødvendig bistand i løpet av prosjektet.

6. juni 2024

Hilde Ludt (sign.)
avdelingsdirektør

Roar A. Kristensen (sign.)
seniorrådgiver

# Innhold

# Hovedbudskap

Kommunerevisjonen har undersøkt om Elvia AS har etablert tilfredsstillende teknisk informasjonssikkerhet i systemene som er nødvendige for å ivareta kraftforsyningen.

Undersøkelsen viser at Elvia AS hadde iverksatt flere tiltak for å etablere teknisk sikkerhet i sine systemer som bidrar til å sikre selskapet mot at utenforstående får tilgang til systemer og informasjon som kan utnyttes til å ramme kraftforsyningen. Det var enkelte forbedringspunkter blant annet knyttet til å sikre at alle kritiske systemer forble beskyttet gjennom flere lag, omfanget av og oppfølgingen av sikkerhetstesting og regelmessig oppfølging av leverandører.

# Sammendrag

Viktige samfunnsoppgaver og kritiske samfunnsfunksjoner er avhengige av et velfungerende system med pålitelig energiforsyning. I Norge utgjør elektrisitet en stor andel av energibruken. Denne avhengigheten av én energiform gjør at det må stilles store krav til forsyningssikkerheten for elektrisk energi. Krigen i Ukraina har demonstrert at kraftforsyningen kan være et mål for ondsinnede aktører, og aktualiserer behovet for å sikre infrastrukturen.

Strømnettene styres og overvåkes av IKT-systemer. Informasjonssikkerheten i disse systemene er derfor en vesentlig faktor for å sikre kraftforsyningen. Ifølge Nasjonal sikkerhetsmyndighet (NSM) er energisystemet sårbart pga. økende kompleksitet og digitalisering.

Elvia AS er Norges største nettselskap. Hovedoppgaven til Elvia AS er distribusjon av elektrisitet til husholdninger, bedrifter og industrielle kunder i Oslo, Innlandet, Akershus og Østfold. Oslo kommune har indirekte eierskap i Elvia AS gjennom Hafslund AS og Hafslund Vekst AS som eier 50 prosent av Eidsiva Energi AS som eier Elvia AS. Det er konsernstyret i Eidsiva Energi AS som har ansvaret for overordnet eierstyring av Elvia AS.

*Problemstilling og metode*

Formålet med forvaltningsrevisjonen har vært å skaffe informasjon om hvorvidt informasjonssikkerheten i Elvia AS er tilfredsstillende ivaretatt med hensyn til sikring av kraftforsyningen, og gjennom dette eventuelt bidra til forbedringer.

Problemstillingen for undersøkelsen har vært:

- Har Elvia AS etablert tilfredsstillende teknisk informasjonssikkerhet i systemene som er nødvendige for å ivareta kraftforsyningen?

Det har blitt gjennomført sikkerhetstesting i regi av Kommunerevisjonen ved bruk av konsulenter innen sikkerhetstesting fra EY. EY har oppsummert sine observasjoner og vurderinger fra møter med Elvia AS og fra sikkerhetstestingen, og Kommunerevisjonen har benyttet dette som underlag i forvaltningsrevisjonen.

Kommunerevisjonen har i tillegg innhentet dokumentasjon på selskapets egne gjennomførte sikkerhetstester fra 2022 til februar 2024 samt annen relevant dokumentasjon med hensyn til undersøkelsens problemstilling.

For sikkerhetstesten har undersøkelsesperioden sammenfalt med tidspunktet for gjennomføringen av sikkerhetstesten, som var i mars 2024. For øvrig er undersøkelsesperioden året 2022 til februar 2024.

Revisjonskriteriene som er lagt til grunn, er i hovedsak utledet fra energiloven, kraftberedskapsforskriften, NSMs grunnprinsipper for IKT-sikkerhet og ISO 27002 – Tiltak for informasjonssikring.

## Sentrale vurderinger

Elvia AS hadde gjennomført sikkerhetstesting før implementering av det nye driftskontrollsystemet. Elvia AS hadde også testet den interne infrastrukturen i kontor- og støttesystemer som også er relevante for kraftforsyningssystemene. Sikkerhetstestene besto av både sårbarhetsskanning og inntrengingstesting. Det var enkelte forbedringspunkter knyttet til oppfølgingen av gjennomførte tester. Deler av systemet var ikke sikkerhetstestet. Etter Kommunerevisjonens vurdering kunne selskapet hatt en mer systematisk tilnærming til oppfølgingen av sikkerhetstestingen. Elvia AS hadde ikke benyttet et system for å registrere og dokumentere hvordan sårbarheter som ble avdekket gjennom sikkerhetstestingen, ble fulgt opp. Tilfredsstillende sikkerhetstesting og oppfølging av disse er viktig for å sikre at IKT-systemer er robuste, pålitelige og beskyttet mot trusler og angrep.

Elvia AS hadde iverksatt tiltak som bidro til å etablere teknisk sikkerhet på de undersøkte områdene. Tiltakene skulle sikre selskapet mot at utenforstående fikk tilgang til systemer og informasjon som kan utnyttes til å ramme kraftforsyningen. Elvia AS hadde blant annet gjennomført sikkerhetstesting og etablert mange tiltak som sørget for at driftskontrollsystemer var sikret gjennom flere lag.

Samtidig viser undersøkelsen at sikkerhetsarbeidet kunne forbedres ytterligere. Det var forbedringspunkter knyttet til omfanget av oppfølgingen av sikkerhetstestingen, å sikre at alle kritiske systemer forble beskyttet gjennom flere lag, og regelmessig oppfølging av leverandører. Alle disse punktene er viktige for å opprettholde en tilfredsstillende teknisk sikkerhet i systemene som er nødvendige for å ivareta kraftforsyningen.

## Anbefalinger

Kommunerevisjonen anbefaler at Elvia AS vurderer

- å iverksette ytterligere sikkerhetstesting der selskapet mener det er relevant,
- å styrke oppfølgingen av sikkerhetstestene,
- om det er systemer som bør beskyttes gjennom ytterligere grad av segmentering,
- og gjennomfører tiltak for å sikre regelmessig oppfølging av leverandører.

## Uttalelser til rapporten

Elvia AS og Byrådsavdeling for kultur og næring har gitt uttalelse til rapporten. Elvia AS meldte relevante tiltak i lys av rapportens anbefalinger. Uttalelsene er i sin helhet lagt ved rapporten i vedlegg 3 og 4.

# 1 Innledning

## 1.1 Bakgrunn

Viktige samfunnsoppgaver og kritiske samfunnsfunksjoner er avhengige av et velfungerende system med pålitelig energiforsyning. I Norge utgjør elektrisitet en stor andel av energibruken. Denne avhengigheten av én energiform gjør at det må stilles store krav til forsyningssikkerheten for elektrisk energi. Krigen i Ukraina har demonstrert at kraftforsyningen kan være et mål for ondsinnede aktører, og aktualiserer behovet for å sikre infrastrukturen.

Strømnettene styres og overvåkes av IKT-systemer. Informasjonssikkerheten i disse systemene er derfor en vesentlig faktor for å sikre kraftforsyningen. Ifølge Nasjonal sikkerhetsmyndighet (NSM) er energisystemet sårbart pga. økende kompleksitet og digitalisering.

Kontrollutvalget vedtok i 2018 en forvaltningsrevisjon av informasjonssikkerheten i daværende Hafslund Nett AS. Etter oppstarten av forvaltningsrevisjonen fattet Norges vassdrags- og energidirektorat (NVE) et vedtak som gjorde at Kommunerevisjonen ikke fikk tilgang til all informasjonen som var nødvendig for å gjennomføre forvaltningsrevisjonen. Kommunerevisjonen klaget på dette vedtaket. Olje- og energidepartementet fattet et vedtak i 2023 som slår fast at Kommunerevisjonen har tilgang til den informasjonen vi trenger for å gjennomføre forvaltningsrevisjonen.

Hafslund Nett AS fusjonerte med Eidsiva Nett AS til selskapet Elvia AS (heretter Elvia) med virkning fra 1. januar 2020. Elvia er Norges største nettselskap. Hovedoppgaven til Elvia er distribusjon av elektrisitet til husholdninger, bedrifter og industrielle kunder i Oslo, Innlandet, Akershus og Østfold. Dette innebærer drift og vedlikehold av elektriske nettverk, overføringslinjer og transformatorstasjoner for å sikre pålitelig strømforsyning til deres tildelte geografiske område.

## 1.2 Formål og problemstillinger

Formålet med undersøkelsen har vært å skaffe informasjon om hvorvidt informasjonssikkerheten i Elvia er tilfredsstillende ivaretatt med hensyn til sikring av kraftforsyningen, og gjennom dette eventuelt bidra til forbedringer.

Problemstillingen for undersøkelsen har vært denne:

- Har Elvia AS etablert tilfredsstillende teknisk informasjonssikkerhet i systemene som er nødvendige for å ivareta kraftforsyningen?

## 1.3 Avgrensninger

Undersøkelsen er begrenset til teknisk sikkerhet tilknyttet IKT-systemene som er vesentlige for driften av kraftforsyningen. Dette omfatter driftskontrollsystemet og kontor- og støttesystemer. Sistnevnte er inkludert fordi disse kan utgjøre en mulig angrepsvei mot driftskontrollsystemet. Sikkerhetstestingen som er gjennomført, dekker deler av, men ikke hele den tekniske infrastrukturen i selskapet.

Vi har ikke gjort undersøkelser av det gamle driftskontrollsystemet som er faset ut i løpet av undersøkelsesperioden. Undersøkelsen er avgrenset fra andre sider ved informasjonssikkerhet, som operasjonelle rutiner for tilgangsstyring og risikovurdering.

## 1.4 Revisjonskriterier

Revisjonskriterier er en betegnelse på forventingene og kravene Kommunerevisjonen legger til grunn for sine vurderinger.

I denne undersøkelsen er revisjonskriteriene i hovedsak utledet fra energiloven, kraftberedskapsforskriften, NSMs grunnprinsipper for IKT-sikkerhet og ISO 27002 – Tiltak for informasjonssikring.

De utledede revisjonskriteriene presenteres i kapittel 3. Utledningen av revisjonskriteriene følger i sin helhet i vedlegg 1.

## 1.5 Metodisk tilnærming og gjennomføring

Det har blitt gjennomført sikkerhetstesting i regi av Kommunerevisjonen ved bruk av konsulenter. Kommunerevisjonen engasjerte EY til å gjennomføre sikkerhetstestingen. Kommunerevisjonen har innhentet dokumentasjon fra Elvia på selskapets egne gjennomførte sikkerhetstester fra 2022 til februar 2024 samt annen relevant dokumentasjon med hensyn til undersøkelsens problemstilling.

Datainnsamlingen er i hovedsak gjennomført i januar–mars 2024. I forbindelse med planleggingen av sikkerhetstestingen ble det i januar og februar 2024 gjennomført to møter med relevant nøkkelpersonell i selskapet hvor også konsulentene deltok. Konsulentene fra EY gjennomførte testing både fra eget kontor og fra Elvias kontor på Skøyen i mars 2024. For sikkerhetstesten har undersøkelsesperioden sammenfalt med tidspunktet for gjennomføringen av testen. For øvrig er undersøkelsesperioden året 2022 til februar 2024 med de avgrensingene som følger av kapittel 1.3.

EY har oppsummert sine observasjoner og vurderinger fra sikkerhetstestingen og møter med Elvia, og Kommunerevisjonen har benyttet dette som underlag i forvaltningsrevisjonen.

Metoden og undersøkelselsopplegget er nærmere beskrevet i vedlegg 2.

## 1.6 Rapportens oppbygging

I kapittel 2 gir vi en kort beskrivelse av Elvia og Oslo kommunes eierskap i Elvia.

I kapittel 3 redegjør vi for Elvias gjennomføring og oppfølging av sikkerhetstesting og for den tekniske sikkerheten i systemene hos Elvia som er nødvendige for å ivareta kraftforsyningen.

I kapittel 4 presenteres Kommunerevisjonens konklusjoner og anbefalinger. I kapittel 5 følger de viktigste punktene i uttalelsen fra Elvia og Byrådsavdeling for kultur og næring og Kommunerevisjonens vurderinger av disse. Uttalelsene er i sin helhet lagt ved rapporten i vedlegg 3 og 4.

# 2 Om Elvia og Oslo kommunes eierskap

I dette kapittelet gir vi en kort beskrivelse av selskapet, eierstrukturen og eierstyringen av selskapet.

## 2.1 Kort om Elvia

Elvia er et nettselskap innen kraftforsyning. Elvia distribuerer elektrisitet i Oslo, Innlandet, Akershus og Østfold. Som et nettselskap er hovedoppgaven til Elvia distribusjon av elektrisitet til husholdninger, bedrifter og industrielle kunder. Dette innebærer drift og vedlikehold av elektriske nettverk, overføringslinjer og transformatorstasjoner for å sikre pålitelig strømforsyning til deres tildelte geografiske område.

Strømnettet til Elvia dekker totalt 50 000 kvadratmeter og forsyner omtrent to millioner innbyggere (Elvia, 2024).

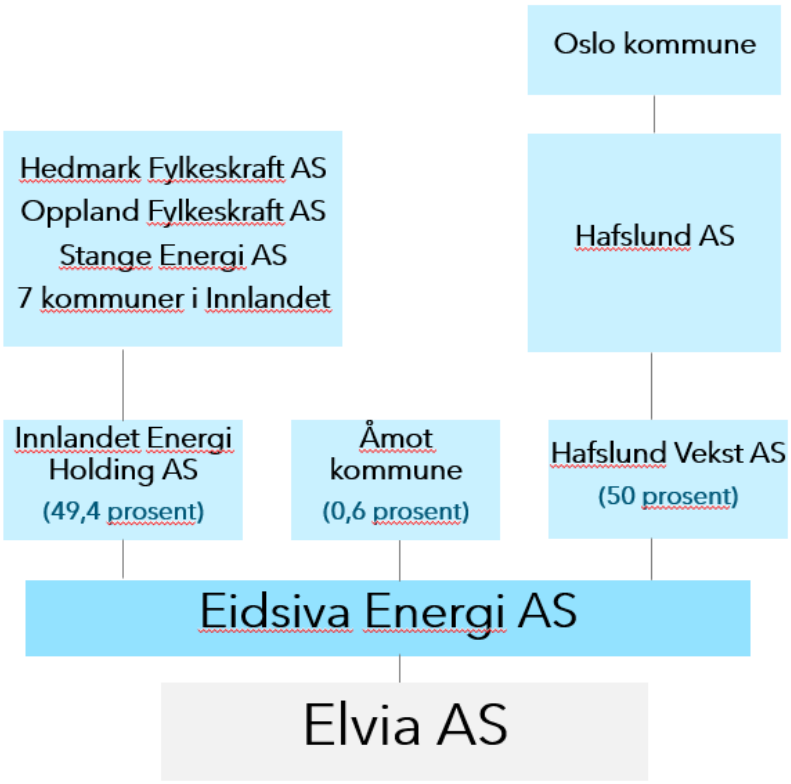
Bystyret i Oslo kommune godkjente 19. juni 2019 (sak 192) avtaler som innebar en fusjon av tidligere Hafslund Nett AS og Eidsiva Nett AS. Fusjonen ble også behandlet på generalforsamlingen til Hafslund (Hafslund E-CO AS) og Eidsiva Energi AS som var eiere av nettselskapene. Sammenslåingen av de to selskapene skulle sikre et større og mer effektivt nettselskap som skulle øke intern kompetanse og styrke fagmiljøet. Fusjonen trådte i kraft 1. januar 2020, og selskapet fikk navnet Elvia.

Elvia er et heleid datterselskap av Eidsiva Energi AS, med hovedkontor på Hamar. Elvia har også et kontor på Skøyen.

## 2.2 Eierstruktur

Figur 1 nedenfor viser en oversikt over eierstrukturen til Elvia.

***Figur 1 Eierstrukturen til Elvia AS***




Note: Utarbeidet av Kommunerevisjonen basert på informasjon fra proff.no

Figur 1 viser eierstrukturen i Elvia. Elvia er heleid av Eidsiva Energi AS. Eierskapet til Eidsiva Energi AS er fordelt på Hafslund Vekst AS (50 prosent), Innlandet Energi Holding AS (49,419 prosent) og Åmot kommune (0,581 prosent).

Hafslund Vekst AS er heleid av Hafslund AS som er heleid av Oslo kommune. Innlandet Energi Holding eies av aksjeselskaper som er eid av Innlandet fylkeskommune og Stange kommune, samt av kommunene Hamar, Ringsaker, Lillehammer, Gausdal, Gjøvik, Løten og Østre Toten.

### 2.2.1 Eierstyring av Elvia

Figur 1 viser at Oslo kommune har et indirekte eierskap i Elvia via flere selskaper. Det vil si at Oslo kommune har ingen direkte eierstyring av selskapet. Det er morselskapet Eidsiva Energi AS (heretter kalt Eidsiva) som har den overordnede eierstyringen av Elvia. Oslo kommune har inngått en aksjonæravtale med de andre eierne om eierskapet i Eidsiva og selskaper som eies i felleskap av Eidsiva og Hafslund E-CO AS (nå Hafslund Vekst AS). Elvia er ett av disse selskapene. Aksjonæravtalen er datert 30. september 2019. Det fremkommer av avtalens punkt 4a at «Eidsivas hovedkontor skal ligge på Hamar, og Eidsiva-konsernets ledelse skal være lokalisert på Hamar, slik at eierstyringen og forvaltningen av konsernets virksomhet faktisk utøves fra Hamar.» I henhold til aksjonæravtalen skal flertallet av styremedlemmene i

nettselskapet (Elvia), inklusive styrets leder, utpekes av Eidsiva, og minst to aksjonærvalgte styremedlemmer skal fritt utpekes av Hafslund E-CO (nå Hafslund Vekst AS).

Aksjonæravtalen regulerer et eierutvalg for Eidsiva. Ifølge avtalen kan Oslo kommune og Innlandet-kommunene oppnevne inntil seks representanter hver til eierutvalget. Ifølge dokumentet *Organisering og styring i Eidsiva*, gjeldende fra januar 2021, er eierutvalget et halvårlig uformelt forum opprettet av og for bakenforliggende eiere. Eierutvalget er opprettet for løpende informasjonsutveksling og dialog mellom eierne. Blant annet skal styreleder og daglig leder fra Eidsiva og andre fra Eidsiva-konsernet, som Elvia, møte i utvalget hvis utvalget ønsker det. Ifølge dokumentet er det Oslo kommune som utpeker utvalgets leder. Eierutvalgsmøtene har ingen direkte beslutningsmyndighet og kommer i tillegg til generalforsamling og de vanlige selskapsorganene.

Videre fremgår det at ansvaret for overordnet eierstyring ligger til konsernstyret i Eidsiva. Konsernstyret fungerer som generalforsamling i heleide datterselskap, slik som Elvia, med mindre oppgaven er delegert til konsernsjefen gjennom særskilt utstedt fullmakt eller generelt gjennom vedtatt fullmaktstruktur. Konsernsjefen er daglig leder i Eidsiva og konsernets øverste administrative leder.

## 2.3 Oppsummering

Elvia ble opprettet som en fusjon mellom Hafslund Nett AS og Eidsiva Nett AS med virkning fra 1. januar 2020. Oslo kommune har indirekte eierskap i Elvia gjennom Hafslund AS og Hafslund Vekst AS, som eier 50 prosent av Eidsiva, som igjen eier Elvia. Det er konsernstyret i Eidsiva som har ansvaret for overordnet eierstyring av Elvia. Det er inngått en aksjonæravtale mellom eierne av Eidsiva som også omhandler Elvia. Aksjonæravtalen omhandler reguleringen av et eierutvalg for Eidsiva, hvor også representanter fra datterselskapet Elvia skal møte om utvalget vil det. Eierutvalget er ledet av Oslo kommune. Eierutvalgsmøtene har ingen direkte beslutningsmyndighet og kommer i tillegg til generalforsamling og de vanlige selskapsorganene.

# 3 Teknisk informasjonssikkerhet i Elvia

I dette kapittelet redegjør vi først for Elvias praksis med gjennomføring og oppfølging av sikkerhetstesting og deretter for den tekniske sikkerheten i systemene hos Elvia som er nødvendige for å ivareta kraftforsyningen.

## 3.1 Revisjonskriterier

- Elvia bør sørge for at det gjennomføres sikkerhetstester (sårbarhetsskanning og inntrengingstester), og skal sørge for at eventuelle sårbarheter som avdekkes gjennom slike tester, følges opp.
- Elvia skal ha etablert teknisk sikkerhet i sine systemer som sikrer selskapet mot at utenforstående får tilgang til systemer og informasjon som kan utnyttes til å ramme kraftforsyningen.

## 3.2 Faktabeskrivelse

### 3.2.1 Elvias gjennomføring og oppfølging av egne sikkerhetstester

Elvia hadde fått gjennomført sikkerhetstester i forbindelse med innføringen av nytt driftskontrollsystem. Disse besto av både sårbarhetsskanning og inntrengingstesting. I juli 2022 ble det gjennomført en test i forkant av at systemet ble levert til kunden, av leverandøren. I februar 2023 ble det gjennomført en ny sikkerhetstest etter at systemet var installert hos Elvia, men før det ble satt i drift.

I testene simulerte testerne en kunnskapsrik og kyndig trusselaktør som forsøkte å «utforske systemet, omgå sikkerhetstiltak og generelt forårsake udefinert, uventet eller uønsket oppførsel».

Elvia hadde også mot slutten av 2022 gjennomført en sikkerhetstest av Elvias interne infrastruktur i kontor- og støttesystemer som også er relevante for kraftforsyningssystemene.

Det var forhold ved den tekniske sikkerheten som selskapet selv mente var relevante å teste, men som selskapet ikke hadde gjennomført testing av. Det var deler av relevante IKT-systemer hvor det ikke var etablert testmiljøer.

Sårbarheter avdekket i testen av driftskontrollsystemet i 2022 ble testet på nytt i 2023 for å undersøke om disse var helt eller delvis lukket. Kommunerevisjonen mottok en oversikt over status på oppfølgingen av sårbarheter som var avdekket i de to sikkerhetstestene i det nye driftskontrollsystemet, per april 2024. Ifølge oversikten var vesentlige sårbarheter enten korrigert eller vurdert som en akseptabel risiko. Kommunerevisjonen har ikke undersøkt selskapets risikoaksept og systemer for beslutninger om sikkerhetstiltak. Selv godt utviklede systemer kan ha sårbarheter. Sikkerhetstester bidrar til å avdekke disse sårbarhetene slik at de kan rettes opp, kompenseres for eller eventuelt besluttes som en akseptabel risiko. Elvia planla en ny test etter at leveransen av driftskontrollsystemet var ferdigstilt første halvår 2024.

I testrapporten etter sikkerhetstesten av Elvias interne infrastruktur i kontor- og støttesystemene ble det anbefalt å gjennomføre en verifikasjonstest for å følge opp om sårbarhetene var lukket. En slik test var ikke gjennomført. Selskapet oppga at kritiske funn fra

testen ble umiddelbart håndtert, at tiltak ble utført, og at det ble innført kontinuerlig sårbarhetsskanning i etterkant av testen. Kommunerevisjonen har mottatt skriftlig dokumentasjon på noen av disse tiltakene.

Elvia hadde et oppgavehåndteringssystem for å holde oversikt over oppgaver i et prosjekt eller team. Selskapet hadde ikke benyttet dette systemet eller andre systemer for å dokumentere hvordan sårbarheter som ble avdekket gjennom sikkerhetstestingen, ble fulgt opp. Elvia oppga at detaljerte sårbarheter i driftskontroll var ansett som så sensitivt at de ikke ville benytte standard verktøy for oppfølging. Informasjon om oppfølging ble fremskaffet på ulike måter, som å vise til korrespondanse med leverandøren som har foretatt korrigeringene i systemet, eller ved egne oversikter som ble utarbeidet på forespørsel.

### 3.2.2 Teknisk informasjonssikkerhet i Elvia

Norges vassdrags- og energidirektorat (NVE) hadde i 2022 et tilsyn på informasjonssikkerhet hos Elvia. Tilsynet var en stikkprøvekontroll, ikke en total gjennomgang. Ifølge NVE kunne tilsynet ikke betraktes som en godkjenning av samsvar med krav i kraftberedskapsforskriften. Det var ett funn som var av teknisk karakter, og som dermed er relevant for vår undersøkelse. Funnet var basert på selvrapportering. Dette avviket og øvrige avvik fra tilsynet var rapportert lukket ifølge NVE.

Kommunerevisjonen engasjerte konsulenter fra EY for gjennomføring av sikkerhetstesting i Elvia. Formålet med testingen var å identifisere sårbarheter relatert til informasjonssikkerhet i Elvia sine systemer som er kritiske for å ivareta strømforsyningen. Målet var å vurdere hvorvidt en angriper kunne skaffe seg uautorisert tilgang til systemene og gjennom denne tilgangen påvirke leveransen av strøm. Det var ikke mulig å dekke hele Elvias tekniske infrastruktur i løpet av den tidsbegrensede sikkerhetstesten. Innretning av sikkerhetstestingen skjedde i dialog med konsulentene og Elvia og var blant annet basert på hvilke deler av infrastrukturen som var dekket av selskapets egne tester.

EYs testing omfattet blant annet nettverkssegmentering. Nettverkssegmentering innebærer å dele inn systemer i ulike nettverk, gjerne ved bruk av subnett og brannmurregler. Dette gir mulighet for å legge restriksjoner på trafikken som kan passere mellom de ulike delene av nettverkene, for å beskytte mot uautorisert tilgang og således styrke sikkerheten.

EY gjorde også en gjennomgang av dokumentasjon og informasjon som ble delt i møter med nøkkelpersonell i Elvia. For å danne et bredere informasjonsgrunnlag for vurdering av eventuelle sårbarheter av betydning for kraftforsyningen i den tekniske infrastrukturen gjennomførte EY en undersøkelse av Elvia sin arkitektur, eksisterende tiltak og rutiner som eksisterer for å sikre kritiske systemer.

Sikkerhetstesten avdekket ikke noen sårbarheter som direkte kunne utnyttes til å påvirke systemene som er nødvendige for kraftleveransen. Konsulentene observerte mange rutiner og prinsipper som sørget for at driftskontrollsystemer var sikret gjennom flere lag. Det ble avdekket sårbarheter av lav alvorlighetsgrad.

EY skrev i sin oppsummering av testingen av Elvias tekniske sikkerhet at kvaliteten burde forbedres, og kom med noen anbefalinger for å konkretisere dette. Gjennom den tekniske nettverksskanningen og gjennomgangen av arkitekturen ble det observert enkelte mangler i

segregeringen mellom Elvias nettverk og kritiske systemer. Rapporten fra EY inneholdt derfor blant annet anbefalinger om at Elvia gjennomførte tiltak for å sikre at kritiske systemer forble beskyttet gjennom flere lag. EY anbefalte også at Elvia gjennomførte ytterligere sikkerhetstester med fokus på sikkerheten i systemer som var nødvendig for å ivareta kraftforsyningen.

Det var særlig to avdelinger i Elvia som var relevante i denne undersøkelsen. Den ene avdelingen hadde implementert mindre grad av segmentering i sine systemer enn den andre avdelingen. Kommunerevisjonen har ikke undersøkt i hvilken grad det foreligger risikovurderinger til grunn for denne forskjellen. Ifølge EY kunne førstnevnte avdeling vurdere å implementere lignende tiltak som er observert i bruk for beskyttelse i den andre avdelingen, med større grad av segmentering i systemene.

Selskapet hadde ikke rutiner for regelmessig oppfølging av alle relevante leverandører. EY anbefalte derfor Elvia å sørge for at det eksisterer rutiner for regelmessig oppfølging av leverandører. Elvia sine leverandører har viktige roller som understøtter strømleveransen.

## 3.3 Kommunerevisjonens vurderinger

Elvia hadde gjennomført sikkerhetstesting før implementering av det nye driftskontrollsystemet. Elvia hadde også testet den interne infrastrukturen i kontor- og støttesystemer som også er relevante for kraftforsyningssystemene. Sikkerhetstestene besto av både sårbarhetsskanning og inntrengingstesting. Det var enkelte forbedringspunkter knyttet til oppfølgingen av gjennomførte tester. Deler av systemet var ikke sikkerhetstestet. Etter Kommunerevisjonens vurdering kunne selskapet hatt en mer systematisk tilnærming til oppfølgingen av sikkerhetstestingen. Elvia hadde ikke benyttet et system for å registrere og dokumentere hvordan sårbarheter som ble avdekket gjennom sikkerhetstestingen, ble fulgt opp. Tilfredsstillende testing og oppfølging er viktig for å sikre at IKT-systemer er robuste, pålitelige og beskyttet mot trusler og angrep.

Elvia hadde iverksatt tiltak som bidro til å etablere teknisk sikkerhet i Elvias systemer på de undersøkte områdene. Tiltakene skulle sikre selskapet mot at utenforstående fikk tilgang til systemer og informasjon som kunne utnyttes til å ramme kraftforsyningen. Elvia hadde blant annet gjennomført sikkerhetstesting og etablert tiltak som sikret driftskontrollsystemene gjennom flere lag. Samtidig viser undersøkelsen at sikkerhetsarbeidet kunne forbedres ytterligere. Det var forbedringspunkter knyttet til omfanget og oppfølgingen av sikkerhetstestingen, å sikre at alle kritiske systemer forble beskyttet gjennom flere lag, og regelmessig oppfølging av leverandører. Alle disse punktene er viktige for å opprettholde en tilfredsstillende teknisk sikkerhet i systemene som er nødvendige for å ivareta kraftforsyningen.

# 4 Kommunerevisjonens konklusjoner og anbefalinger

## 4.1 Konklusjoner

Kommunerevisjonen har undersøkt om Elvia har etablert tilfredsstillende teknisk informasjonssikkerhet i systemene som er nødvendige for å ivareta kraftforsyningen.

Undersøkelsen viser at Elvia hadde iverksatt flere tiltak som kunne bidra til å etablere teknisk sikkerhet i deres systemer på de undersøkte områdene. Tiltakene skulle sikre selskapet mot at utenforstående får tilgang til systemer og informasjon som kan utnyttes til å ramme kraftforsyningen. Elvia hadde sørget for sikkerhetstesting og hadde etablert tiltak som sørget for at driftskontrollsystemene var sikret gjennom flere lag.

Samtidig viser undersøkelsen at sikkerhetsarbeidet kunne forbedres ytterligere. Det var forbedringspunkter knyttet til å sikre at alle kritiske systemer forble beskyttet gjennom flere lag, omfanget av sikkerhetstesting og oppfølgingen av disse samt regelmessig oppfølging av leverandører.

## 4.2 Anbefalinger

Kommunerevisjonen anbefaler at Elvia vurderer

- å iverksette ytterligere sikkerhetstesting der selskapet mener det er relevant,
- å styrke oppfølgingen av sikkerhetstestene,
- om det er systemer som bør beskyttes gjennom ytterligere grad av segmentering,
- og gjennomfører tiltak for å sikre regelmessig oppfølging av leverandører.

# 5 Uttalelser til rapporten og Kommunerevisjonens vurdering av disse

I dette kapitlet følger en kort oppsummering av de viktigste punktene i uttalelsen fra Elvia og Byrådsavdeling for kultur og næring. Uttalelsene er i sin helhet lagt ved rapporten i vedlegg 3 og 4.

## 5.1 Elvia

### 5.1.1 Uttalelsen

Elvia skriver at prosjektets hensikt har vært tydelig kommunisert ved flere anledninger og har ingen kommentarer til metode eller revisjonskriterier. Elvia oppfatter rapportens vurderinger som relevante og opplever denne typen sikkerhetstesting og revisjon som svært nyttig.

Elvia skriver at den har iverksatt de tiltakene som ble foreslått som følge av sikkerhetstesten. Elvia varsler flere tiltak til rapportens anbefalinger:

- Elvia har planer om å iverksette ytterliggere sikkerhetstester på flere områder der det er relevant.
- Elvia vil undersøke nærmere om det finnes metoder eller system som vil anses som sikker nok til en mer veldokumentert oppfølging av gjennomførte sikkerhetstester.
- Elvia vil fortsette arbeidet med segmentering av sine systemer, og løpende vurdere. segmenteringen på bakgrunn av risikovurderinger, og ved ny- og reetablering av systemer.
- Elvia vil jobbe videre med en mer systematisk tilnærming til leverandøroppfølging.

Arbeidet med gjennomføringen av tiltakene starter i 2024 og vil fortsette i 2025. Elvia oppgir at sikkerhetsforbedringer er et kontinuerlig arbeid.

### 5.1.2 Kommunerevisjonens vurdering

Kommunerevisjonen anser at Elvia har meldt relevante tiltak i lys av rapportens anbefalinger, og har for øvrig ingen kommentarer til uttalelsen.

## 5.2 Byrådsavdeling for kultur og næring

### 5.2.1 Uttalelsen

Byrådsavdeling for kultur og næring konstaterer at undersøkelsen viser at Elvia hadde iverksett flere tiltak som kunne bidra til å etablere en teknisk sikkerhet i sine systemer på de undersøkte områdene. Byrådsavdelingen viser til at Kommunerevisjonen kom med anbefalinger på enkelte områder, og at Elvia her ble anbefalt å vurdere ytterligere tiltak.

Byrådsavdelingen vurderer det som positivt at Kommunerevisjonens undersøkelse har bidratt til å sette fokus på teknisk informasjonssikkerhet i Elvia.

Byrådsavdelingen viser til at rapporten ble sendt dem med mulighet til uttalelse og at Kommunerevisjonen ikke har anbefalinger som retter seg mot byrådsavdelingen. Byrådsavdelingen viser til at Oslo kommune har indirekte eierskap i Elvia gjennom Hafslund AS og Hafslund Vekst AS som eier 50 prosent av Eidsiva Energi AS som igjen eier Elvia. Oslo kommune har derfor ikke bestemmende innflytelse over selskapet.

### 5.2.2 Kommunerevisjonens vurdering

Kommunerevisjonen har ingen kommentarer til uttalelsen fra byrådsavdeling for kultur og næring.

# Figuroversikt

# Referanser

LOV-1990-06-29 nr. 50: lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven)

Elvia (2024): *Vårt strømnett*: https://www.elvia.no/hva-er-elvia/vart-stromnett/

Bystyresak 192/2019: *Hafslund E-CO – Samling med Eidsiva Energi AS – Byrådssak 146 av 23.05.2019*. Møte i bystyret 19. juni 2019.

Eidsiva Energi (2019): *Aksjonæravtale vedrørende eierskapet i Eidsiva Energi AS*

Eidsiva Energi (2021): *Organisering og styring i Eidsiva*

EY (2024): *Teknisk sikkerhetstest av Elvia. Oslo kommune Kommunerevisjonen.* 22. mars 2024

Forskrift om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften)

ISO 27002 – *Tiltak for informasjonssikring*

Norges vassdrags- og energidirektorat (2020): *Veiledning til kraftberedskapsforskriften*

Norges sikkerhetsmyndighet (2020): *NSMs grunnprinsipper for IKT-sikkerhet 2.0*

Norges sikkerhetsmyndighet (2020): *NSMs grunnprinsipper for sikkerhetsstyring*

# Vedlegg 1 Revisjonskriterier

Revisjonskriterier er de forventningene og kravene Kommunerevisjonen legger til grunn for sine vurderinger, det vil si kravene, normene og/eller standardene som Elvia AS vurderes opp mot.

Revisjonskriteriene er utledet fra autoritative kilder eller anerkjente kilder innenfor det reviderte området i tråd med *Standard for forvaltningsrevisjon* (RSK 001) fastsatt av styret i NKRF – kontroll og revisjon i kommunene.

Revisjonskriteriene er utledet fra følgende kilder:

- lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven)
- forskrift om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften)
- NVEs veiledning til kraftberedskapsforskriften
- NSMs grunnprinsipper for IKT-sikkerhet 2.0
- NSMs grunnprinsipper for sikkerhetsstyring
- ISO 27002 – Tiltak for informasjonssikring

I det videre går vi gjennom revisjonskriteriene og utledningen av disse.

## Teknisk informasjonssikkerhet i Elvia AS

### Revisjonskriterier

- Elvia AS bør sørge for at det gjennomføres sikkerhetstester (sårbarhetsskanning og inntrengingstester), og skal sørge for at eventuelle sårbarheter som avdekkes gjennom slike tester, følges opp.
- Elvia AS skal ha etablert teknisk sikkerhet i sine systemer som sikrer selskapet mot at utenforstående får tilgang til systemer og informasjon som kan utnyttes til å ramme kraftforsyningen.

### Utledning av revisjonskriteriene

Informasjonssikkerhet dreier seg om å sikre tilgjengeligheten til informasjon, integriteten til informasjon (at ingen kan urettmessig endre innhold) og konfidensialiteten til informasjon (kun de med rettigheter kan få tilgang til informasjon). Kraftsensitiv informasjon er en særlig sensitiv informasjon som krever særlig beskyttelse, jf. energiloven § 9-3.

Viktige samfunnsoppgaver og kritiske samfunnsfunksjoner er avhengige av et velfungerende system med pålitelig energiforsyning. I Norge utgjør elektrisitet en betydelig andel av energiforbruket. Forsyningsnettet i Norge er strukturert i tre hovednivåer: sentralnett, regionalnett og distribusjonsnett. Sentralnettet, også kjent som det nasjonale nettet eller transmisjonsnettet, knytter sammen produksjon og forbruk på tvers av ulike landsdeler. Distribusjonsnettene tar seg av lokal distribusjon av elektrisk energi til sluttbrukerne, mens regionalnettene fungerer som koblingspunkter mellom sentralnettet og distribusjonsnettene. Elvia AS drifter regionalnett og distribusjonsnett og er derfor en del av Kraftforsyningens beredskapsorganisasjon (KBO) som er underlagt egne sikkerhetsregler.

Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven) er det viktigste grunnlaget for reguleringer i elektrisitetssektoren. Ifølge energiloven § 9-1 består KBO av de

> *enheter som eier eller driver anlegg eller annet som har vesentlig betydning for drift eller gjenoppretting av eller sikkerhet i produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme.*

Ifølge energiloven § 9-2 plikter Elvia AS å

> *sørge for effektiv sikring og beredskap og iverksette tiltak for å forebygge, håndtere og begrense virkningene av ekstraordinære situasjoner (...).*

Kraftberedskapsforskriften er en forskrift til energiloven som skal sikre at kraftforsyningen opprettholdes, og at normal forsyning gjenopprettes på en effektiv og sikker måte i og etter ekstraordinære situasjoner for å redusere de samfunnsmessige konsekvensene.

Ifølge kraftberedskapsforskriften § 2-4 skal beredskapsplanleggingen i KBO-enheter omfatte forberedelser og tiltak det kan bli nødvendig å iverksette ved store ulykker, vesentlige skader, trusselsituasjoner, rasjonering og andre ekstraordinære situasjoner som kan påvirke kraftforsyningens drift og sikkerhet. NVEs veiledning til kraftberedskapsforskriften viser blant annet til IKT-angrep i denne sammenhengen.

Ifølge energiloven § 9-3 skal alle enheter i KBO vurdere sikkerheten ved all behandling av informasjon om kraftforsyningen. Det skal etableres effektiv avskjerming og beskyttelse av sensitiv informasjon.

I henhold til kraftberedskapsforskriften § 6-3 skal virksomheter som har eller behandler kraftsensitiv informasjon, etablere, opprettholde og videreutvikle systemer og rutiner for effektiv avskjerming, beskyttelse og tilgangskontroll for kraftsensitiv informasjon. Ifølge NVEs veiledning til kraftberedskapsforskriften må virksomhetene beskytte virksomhetens informasjon og data mot utilsiktet informasjonslekkasje, uautorisert endring og skadeverk. Teknisk sikring nevnes som ett av flere tiltak for tilgangskontroll og beskyttelse.

I henhold til kraftberedskapsforskriften § 6-9 skal virksomheter

(...) sikre digitale informasjonssystemer slik at konfidensialitet, integritet og tilgjengelighet ivaretas.

Det er den enkelte virksomhets ansvar å planlegge, gjennomføre og vedlikeholde sikringstiltak etter det digitale informasjonssystemets type, oppbygging og funksjon.

I tredje ledd i denne paragrafen slås det fast at virksomheter skal ha en grunnsikring for digitale informasjonssystemer i henhold til anerkjente standarder og normer. Det står blant annet at virksomheter skal:

> *c. Sikre og oppdage*
>
> *Virksomheter skal sikre sine digitale informasjonssystemer for å motstå eller begrense skade fra uønskede hendelser. Virksomheter skal overvåke sine digitale informasjonssystemer slik at uønskede hendelser oppdages og registreres (...).*

I kravet om å sikre inngår blant annet å ivareta en sikker konfigurasjon (av maskin- og programvare) og beskytte virksomhetens datanettverk, ifølge NVEs veiledning.

I kravet til å oppdage inngår følgende grunnprinsipper, ifølge NVEs veiledning:

- *3.1 oppdag og fjern kjente sårbarheter og trusler*
- *3.2 etabler sikkerhetsovervåkning*
- *3.3 analyser data fra sikkerhetsovervåkning*
- *3.4 gjennomfør inntrengingstester*

Ifølge NVEs veiledning til kraftberedskapsforskriften bygger kravene i forskriftens § 6-9 på NSMs grunnprinsipper for IKT-sikkerhet. NSMs grunnprinsipper for IKT-sikkerhet bygger igjen på internasjonale, anerkjente standarder og veiledninger, spesielt ISO 27002. NVE anbefaler virksomheter å sette seg inn i NSMs grunnprinsipper for IKT-sikkerhet og NSMs grunnprinsipper for sikkerhetsstyring.

NSMs *grunnprinsipper for IKT-sikkerhet* er et sett med prinsipper og tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. NSM har i grunnprinsipper for IKT-sikkerhet versjon 2.0 delt inn prinsippene i fire kategorier oppsummert under, hvor særlig punkt 2 og 3 er relevante for denne undersøkelsen:

1. Identifisere og kartlegge
    a. Forstå virksomheten, inkludert styringsstrukturer, ledelsesprioriteringer, leveranser, IKT-systemer og brukere.
2. Beskytte og opprettholde
    a. Sikre IKT-systemet forsvarlig over tid og ved endringer
3. Oppdage
    a. Overvåke sikkerheten ved å teste forsvarsmekanismer mot simulerte angrep, identifisere mangler og evaluere beredskap.
4. Håndtere og gjenopprette
    a. Effektiv håndtering av sikkerhetshendelser gjennom forberedelser, vurderinger, kontroll, håndtering, gjenoppretting og kontinuerlig forbedring

NSMs grunnprinsipp 3.1 *Oppdag og fjern kjente sårbarheter og trusler* har som mål at virksomheten oppdager og fjerner kjente sårbarheter og kjent skadelig kode i virksomhetens IKT-systemer. I tiltak 3.1.1 anbefales det at virksomheten jevnlig gjennomfører sårbarhetskartlegging ved hjelp av automatiserte verktøy.

NSMs grunnprinsipp 3.4 *Gjennomfør inntrengingstester* har som mål å teste elementer i egne forsvarsmekanismer (teknologi, prosesser og personell) ved å simulere målene og handlingene til en angriper. Summen av alle sårbarheter omtales ofte som den mulige angrepsflaten («attack surface»). I tiltak 3.4.4 anbefaler NSM at det gjennomføres jevnlige inntrengingstester (minst årlige) for å identifisere sårbarheter. Her fremgår det at

> *Inntrengingstestingen bør gjennomføres a) fra utsiden av virksomhetens nettverksbarrierer (eksempelvis fra internett eller via trådløs kommunikasjon i nærheten av virksomhetens lokaler) for å simulere eksterne angrep og b) fra innsiden av barrierer (eksempelvis på det interne nettverket) for å simulere interne angrep fra kompromittert klient/server eller utro tjenere.*

NSMs *grunnprinsipper for sikkerhetsstyring* er et sett med prinsipper og anbefalte tiltak som beskriver hva virksomheten kan gjøre for å oppnå og opprettholde et akseptabelt sikkerhetsnivå. Ifølge disse vil virksomheter først kunne oppnå et akseptabelt sikkerhetsnivå for sine verdier når de har identifisert og implementert tiltak som reduserer organisatoriske, elektroniske, fysiske og menneskelige sårbarheter.

ISO 27002 – *Tiltak for informasjonssikring* beskriver beste praksis for informasjonssikkerhetskontroller som brukes for å redusere uakseptable risikoer for konfidensialitet, integritet og tilgjengelighet til informasjon.

ISO 27002 gir en rekke sikringsteknikker for informasjonssikkerhet. Av særlig betydning for revisjonskriteriene nevner vi her anbefalinger knyttet til nettverkssikkerhet, logging, monitorering og sikkerhetstesting. Veiledningen i ISO 27002 er ment å hjelpe en virksomhet med å iverksette, vedlikeholde og forbedre sin informasjonssikkerhetsstyring. Blant annet står det i kapittel 8.8 *Håndtering av tekniske sikkerhetstiltak* om identifisering av tekniske sårbarheter at

> *For å identifisere tekniske sårbarheter bør organisasjonen vurdere følgende:*
>
> *(...)*
>
> *d) bruke verktøy for sårbarhetsskanning som er egnet for teknologiene som brukes til å identifisere sårbarheter og til å verifisere om korrigeringen av sårbarheter var vellykket;*
>
> *e) få kompetente og autoriserte personer til å gjennomføre planlagte, dokumenterte og repeterbare inntrengingstester eller sårbarhetsvurderinger som gjør at sårbarheter kan identifiseres. Utvise forsiktighet, ettersom slike aktiviteter kan føre til at systemets sikkerhet blir kompromittert;*
>
> *(...)*

# Vedlegg 2 Metode

## Generelt om forvaltningsrevisjon

De sentrale delene av en forvaltningsrevisjon er beskrevet i *Standard for forvaltningsrevisjon* fra Norges Kommunerevisorforbund (RSK 001 Standard for forvaltningsrevisjon). Disse delene er like for alle forvaltningsrevisjoner. Kort oppsummert bestemmer kontrollutvalget problemstillingen i sin bestilling til Kommunerevisjonen. Kommunerevisjonen utleder relevante revisjonskriterier for problemstillingen. Kriteriene er målestokken som vi holder den reviderte enhet opp mot. For å svare på spørsmålet om enheten når de gitte målene/revisjonskriteriene, samler vi inn relevante data som vi bearbeider og analyserer. Dette gir oss et faktagrunnlag som vi vurderer opp mot revisjonskriteriene. Vurderingene leder frem til Kommunerevisjonens konklusjoner og eventuelle anbefalinger.

## Beskrivelse av prosjektgjennomføring

Forvaltningsrevisjonen ble vedtatt av kontrollutvalget i møte 29. august 2023 (sak 71). Virksomheten som er revidert i denne undersøkelsen, er Elvia. Brev om oppstart av forvaltningsrevisjonen ble sent til Elvia og byråden for kultur og næring 6. november 2023. Det ble også samme dag sendt informasjonsbrev om oppstart av forvaltningsrevisjonen til styret i Elvia, Eidsiva Energi AS og til selskapets revisor PricewaterhouseCoopers AS.

Kommunerevisjonen hadde oppstartsmøte med Elvia 23. november 2024 og med daværende byrådsavdeling for næring og eierskap 1. desember 2023.

Kommunerevisjonen sendte utkast til revisjonskriterier til Elvia og byråden for kultur og næring 20. desember 2024. Kommunerevisjonen mottok ingen merknader som medførte endringer i kriteriene. Byrådsavdelingen hadde innspill til revisjonskriteriene datert 9. januar 2024. Disse ble besvart av Kommunerevisjonen i brev av 13. januar 2024. Kommunerevisjonen utarbeidet et notat om Oslo kommunes eierskap i Elvia som byrådsavdelingen fikk til gjennomgang. Byrådsavdelingen oppga 1. februar 2024 at den ikke hadde kommentarer til teksten i notatet eller revisjonskriteriene. Notatet ligger til grunn for beskrivelsen av Oslo kommunes eierskap i Elvia AS som presenteres i rapportens kapittel 2.

Kommunerevisjonen oversendte et utkast til faktabeskrivelse til Elvia for verifisering 2. mai 2024. Det ble avholdt en forhåndspresentasjon av våre foreløpige vurderinger med Elvia 14. mai 2024 og med Byrådsavdeling for kultur og næring 15. mai 2024. Rapporten ble sendt til uttalelse til Elvia 15. mai 2024 og for mulighet for uttalelse til byråden for kultur og næring 15. mai 2024. Styret i Elvia og Eidsiva Energi AS mottok også informasjonsbrev om at rapporten

var sendt til uttalelse. Kommunerevisjonen mottok uttalelse fra Elvia 29. mai 2024 og fra byrådsavdeling for kultur og næring 4. juni 2024.

## Metode for datainnhenting og analyse

Undersøkelsen er basert på informasjon innhentet gjennom sikkerhetstesting og dokumentgjennomgang. Datainnsamlingen ble i hovedsak gjennomført mellom januar 2024 og mars 2024. For sikkerhetstesten var undersøkelsesperioden tidspunktet for gjennomføringen av testingen. For øvrig er undersøkelsesperioden 2022 til februar 2024.

### Konsulentstøttet sikkerhetstesting og vurdering av sikkerhet i infrastruktur

Sikkerhetstesting er godt egnet til å undersøke den tekniske sikkerheten i IKT-systemer fordi slik testing simulerer aktiviteter som en ondsinnet angriper kan forventes å gjennomføre. Slik testing vil ofte avdekke sårbarheter som kan være svært vanskelige å identifisere gjennom alternative metoder, som gjennomgang av programkode eller systemdokumentasjon. Slik dokumentasjon kan dessuten være utdatert eller feil av andre grunner.

Sikkerhetstesting er et eget fagområde som ligger utenfor kjernekompetansen til Kommunerevisjonen. Vi leide derfor inn kompetente sikkerhetstestere til å gjøre dette. Dette ble gjort gjennom en anskaffelsesprosess hvor følgende kriterier ble identifisert og vektet før utsendelse av tilbud:

- dokumentert kompetanse og erfaring til personellet som tilbys (35 %)
- overordnet beskrivelse av hvordan konsulenten ser for seg å gjennomføre testen, basert på forutsetningene i tilbudsinvitasjonen (35 %)
- tilgjengelighet/kapasitet (30 %)

Oppdraget var basert på en fast kostnadsramme. Kommunerevisjonen sendte tilbudsinvitasjon til tre selskaper og mottok to tilbud. Selskapet bak ett av tilbudene oppfylte ikke alle kvalifikasjonskravene. Vi sto så igjen med ett tilbud som oppfylte kvalifikasjonskravene, dette var fra EY. CV-ene til de aktuelle personene viste at de hadde relevant utdanning, herunder kurs og sertifiseringer, og mange års arbeidserfaring innen sikkerhetstesting og flere relevante referanseprosjekter.

Kommunerevisjonen og EY hadde et oppstartsmøte 22. januar 2024. I forbindelse med planleggingen av sikkerhetstestingen ble det gjennomført to møter med relevant nøkkelpersonell i Elvia, 29. januar og 27. februar 2024, hvor også konsulentene fra EY deltok.

Formålet med sikkerhetstesten var å identifisere sårbarheter relatert til informasjonssikkerhet i Elvia sine systemer som er kritiske for å ivareta strømforsyningen. Målet var å vurdere hvorvidt en angriper kunne skaffe seg uautorisert tilgang til Elvias systemer og gjennom denne tilgangen påvirke Elvia sin leveranse av strøm.

Selve testaktivitetene ble gjennomført mellom 4. og 8. mars 2024. Det ble utarbeidet en testplan i forkant, og det ble avtalt hvordan det skulle varsles ved start og avslutning av testaktiviteter. I samråd med Kommunerevisjonen sendte konsulentene før oppstart en oversikt

til Elvia over hvilke testverktøy de planla å benytte. Elvia underskrev en fullmaktsavtale før testingen fant sted.

Det var ikke mulig å dekke hele Elvia sin tekniske infrastruktur i løpet av den tidsbegrensede sikkerhetstesten. EYs oppdrag bestod av scopingmøter med Kommunerevisjonen og Elvia, teknisk sikkerhetstesting, rapportering og en gjennomgang av rapporten med Kommunerevisjonen og Elvia. EY gjennomførte nettverkssegmenteringstesting og sårbarhetsskanning. Nettverkssegmentering øker sikkerheten i nettverket. Nettverkssegmentering innebærer å segmentere systemer i ulike nettverk – gjerne ved bruk av subnett og brannmurregler. Sårbarhetsskanning kan for eksempel brukes til å avdekke om det brukes utdaterte og sårbare versjoner av for eksempel programmer og operativsystemer.

EY gjorde også en gjennomgang av dokumentasjon og informasjon som ble delt i møter med nøkkelpersonell i Elvia. For å danne et bedre informasjonsgrunnlag for vurdering av eventuelle sårbarheter av betydning for kraftforsyningen i den tekniske infrastrukturen gjennomførte EY en undersøkelse av Elvia sin arkitektur, eksisterende tiltak og rutiner som eksisterer for å sikre kritiske systemer.

EY har oppsummert sine observasjoner og vurderinger fra møter med Elvia og fra sikkerhetstestingen, og Kommunerevisjonen har benyttet dette som underlag i forvaltningsrevisjonen. Elvia har fått tilgang til denne rapporten.

### Dokumentgjennomgang

Kommunerevisjonen har innhentet relevant dokumentasjon fra Elvia for å belyse problemstillingen om teknisk sikkerhet. Vi har blant annet innhentet rapporter fra sikkerhetstester gjennomført på oppdrag fra Elvia i 2022 og 2023 og dokumentasjon på oppfølgingen av disse. Sammen med rapporten fra EYs sikkerhetstesting og vurderinger på oppdrag fra Kommunerevisjonen har disse utgjort vesentlig dokumentasjon i undersøkelsen. Kommunerevisjonen har gjennomgått disse, og dokumentene er analysert ved hjelp av egne koblingsskjemaer i Word hvor innsamlet fakta for hvert enkelt tema er vurdert opp mot revisjonskriteriene og tilhørende kontrollpunkter som vi utarbeidet for hvert kriterium.

## Behandling av kraftsensitiv informasjon

Norges vassdrags- og energidirektorat (NVE) fattet vedtak 15. mars 2023 om at kravene til beskyttelse mv. i kraftberedskapsforskriften §§ 6-3 og 6-4 skal gjelde for Kommunerevisjonen.

Kommunerevisjonen har etterfulgt vilkårene og kravene NVE har oppstilt i vedtaket av 15. mars 2023. Kommunerevisjonen oversendte brev med vedlegg til Elvia 5. januar 2024 hvor vi bekreftet og dokumenterte at vilkårene og kravene NVE har oppstilt i vedtaket, er oppfylt, før selskapet delte kraftsensitiv informasjon med oss.

Kommunerevisjonen har interne rutiner for informasjonssikkerhet som ivaretar kravene til beskyttelse mv. i kraftberedskapsforskriften §§ 6-3 og 6-4. Informasjon som Kommunerevisjonen har mottatt, er håndtert i henhold til våre rutiner for informasjonssikkerhet. Det innebærer blant annet at tilgang til kraftsensitiv informasjon er begrenset til kun personer med behov for informasjonen. Personell i Kommunerevisjonen som kunne få tilgang til kraftsensitiv informasjon, har underskrevet en egen taushetserklæring om

kraftsensitiv informasjon. I tillegg har alle i den interne prosjektgruppen godkjent sikkerhetsklarering på nivå HEMMELIG etter sikkerhetsloven. For eksterne konsulenter til teknisk sikkerhetstesting er det inngått sikkerhetsavtale i tråd med kraftberedskapsforskriften mellom Kommunerevisjonen og ekstern leverandør. Vi har også mottatt taushetserklæringer for de aktuelle konsulentene som følger NVEs mal, og vi har stilt krav om at kun disse personene vil kunne få tilgang til kraftsensitiv informasjon. Elvia har sørget for personkontroll etter kraftberedskapsforskriften § 6-9 av konsulenter som fikk tilgang til systemer i Elvia for å gjennomføre teknisk sikkerhetstesting.

Kommunerevisjonen har fokusert på å skrive en offentlig rapport og har sørget for dialog med Elvia for å sikre at rapporten ikke inneholder kraftsensitiv informasjon.

## Behandling av personopplysninger

Formålet med Kommunerevisjonens innhenting, behandling og oppbevaring av personopplysninger er å utføre den lovbestemte revisjonen. Hvilke personopplysninger vi samler inn og behandler, avhenger av hvilken informasjon vi trenger for å gjennomføre undersøkelsen. I denne undersøkelsen har vi hatt eksterne konsulenter fra EY som kunne tilegne seg personopplysninger gjennom sine undersøkelser. Kommunerevisjonen har inngått databehandleravtale med EY om behandling av personopplysninger.

Kommunerevisjonen følger bestemmelsene i personopplysningsloven og legger vekt på å begrense lagringen av personopplysninger. Vi legger vekt på bare å innhente data som er relevante for formålet med undersøkelsen. Vi tar bare vare på personopplysninger som er nødvendige for dokumentasjon av arbeidet vi utfører. Personopplysninger lagres utilgjengelig for uvedkommende.

Retten til å få slettet personopplysninger er bl.a. styrt av at Kommunerevisjonen har 10 års lagringsplikt for dokumentasjon av revisjonene.

For ytterligere informasjon om Kommunerevisjonens ansvar for og behandling av personopplysninger, se vår personvernerklæring.

## Gyldighet og pålitelighet

For å kvalitetssikre datagrunnlaget har vi vurdert dataenes validitet (gyldighet) og reliabilitet (pålitelighet). Gyldighet refererer til hvor godt man klarer å måle det man har til hensikt å måle eller undersøke. Pålitelighet refererer til hvor nøyaktig innsamlingen av data har vært.

Vi har blant annet benyttet oss av informasjon som er samlet inn av eksterne konsulenter. Rapporten fra sikkerhetstesten ble forelagt en representant fra Elvia før den ble ferdigstilt. Alle faktaopplysninger som er benyttet i rapporten, er verifisert av Elvia. Kommunerevisjonen sendte en samlet faktabeskrivelse til Elvia 2. mai 2024. Undersøkelsen har vært underlagt intern kvalitetssikring i Kommunerevisjonen. Rapporten fra eksterne konsulenter har også vært underlagt kvalitetssikring i konsulentselskapet før den ble overlevert til Kommunerevisjonen.

For sikkerhetstesten gjennomført på oppdrag fra Kommunerevisjonen var oppdraget basert på en fast kostnadsramme. I samråd med Kommunerevisjonen valgte konsulentene ut de testaktivitetene som var antatt å gi mest nytte innenfor rammen. Det ble da tatt hensyn til tester som Elvia selv hadde sørget for å gjennomføre, og som var planlagt å gjennomføre. Det var ikke mulig å dekke hele Elvia sin tekniske infrastruktur i løpet av den tidsbegrensede sikkerhetstesten. Det er følgelig deler av den tekniske sikkerheten i Elvia som er relevant for kraftforsyningen, som ikke er dekket av sikkerhetstestingen.

For å danne et bedre informasjonsgrunnlag for vurdering av eventuelle sårbarheter identifisert i nettverkssegmenteringstestene gjennomførte konsulentene en supplerende undersøkelse av Elvia sin arkitektur, eksisterende tiltak og rutiner som eksisterer for å sikre kritiske systemer. Kommunerevisjonen har også på egen hånd innhentet relevante dokumenter som viser Elvias egne sikkerhetstester og oppfølging av disse. Innsamlede fakta for hvert enkelt tema er vurdert opp mot revisjonskriteriene og tilhørende kontrollpunkter som vi utarbeidet for hvert kriterium, blant annet slik at vi har hatt et godt grunnlag for å vurdere tilstrekkeligheten i de innsamlede dataene.

Kommunerevisjonens beskrivelser, vurderinger og konklusjoner er avpasset de mulighetene og begrensingene som ligger i datagrunnlaget. Som grunnlag for våre vurderinger og konklusjoner mener vi derfor at de innsamlede dataene er tilstrekkelig gyldige og pålitelige.

# Vedlegg 3: Uttalelse fra Elvia AS

**Fra:** Sigurd Kvistad
**Til:** Roar Andreas Kristensen
**Kopi:** Anne Sagstuen Nysæther; Bjørn Høiås
**Emne:** RE: Rapport til uttalelse - Teknisk informasjonssikkerhet i Elvia AS
**Dato:** onsdag 29. mai 2024 15:41:00
**Vedlegg:** image002.png
image003.png

---

Hei,

Viser til brev 2024-05-14 saksnr. 23/481-43 om rapport til uttalelse.
Vi har ingen kommentarer til selve rapporten.

I høringsbrevet ber Kommunerevisjonen om tilbakemelding på noen spørsmål. Ingen av svarene er av en slik art at de bør unntas offentlighet.

1. ***Har informasjonen om prosjektets hensikt vært tilstrekkelig klar?***
   Det har vært tydelig kommunisert ved flere anledninger og også gitt oss klarhet i hva som har vært omfanget (scope) av prosjektet; å undersøke om Elvia har etablert tilfredsstillende teknisk
   informasjonssikkerhet i systemene som er nødvendig for å ivareta kraftforsyningen.

2. ***Har Elvia kommentarer til prosjektets metode, anvendte kilder eller data som kan ha betydning for rapportens konklusjoner? I tilfelle hvilke?***
   Vi har ingen innvendinger på hvordan undersøkelsen har blitt gjennomført.

3. ***Har Elvia kommentarer til revisjonskriteriene som ligger til grunn for våre vurderinger? I tilfelle hvilke?***
   Vi har ingen kommentar til revisjonskriteriene som er benyttet. Revisjonskriteriene er i all hovedsak de samme kriteriene som vi legger til grunn for Elvias arbeid med informasjonssikkerhet.

4. ***Hva er Elvias samlede vurdering av rapportens konklusjoner og anbefalinger?***
   Vi oppfatter rapportens vurderinger som relevante.

   Elvia gjennomfører sikkerhetstester jevnlig og har planer om å iverksette ytterligere sikkerhetstester på flere områder der det er relevant.

   Selskapets standard system for prosjekt og arbeidsoppgave oppfølging ble ikke benyttet til å følge opp sikkerhetstestene. Dette fordi resultatet fra sikkerhetstestene ble ansett som så sensitive at dette systemet ikke kunne benyttes til det. Derimot ble resultatet fra testene fulgt opp i jevnlige møter flere ganger i uken til alle var håndtert på tilfredsstillende måte. Elvia vil undersøke nærmere om det finnes metode eller system som vil ansees som sikker nok til en mer veldokumentert oppfølging.

   Elvia har flere systemer som er gjenstand for ulik grad av segmentering. Arbeidet med segmentering vil fortsette og det er noe man løpende vurderer på bakgrunn av risikovurderinger og ved ny- og re-etablering av systemer.

   Elvia erkjenner at leverandøroppfølging har hatt varierende grad av kvalitet og frekvens

og er således enig i rapportens hovedkonklusjon.

5. ***Vil Elvia vurdere og eventuelt iverksette tiltak på bakgrunn av rapportens konklusjoner og anbefalinger? I tilfelle hvilke?***
   Elvia har fulgt EY sine anbefalinger og iverksatt de tiltakene som ble foreslått.

   Elvia har planer om å iverksette ytterligere sikkerhetstester på flere områder der det er relevant.

   Vi vil undersøke nærmere om det finnes metode eller system som vil ansees som sikker nok til en mer veldokumentert oppfølging av sikkerhetstester.

   Elvia jobber allerede med og vil jobbe videre med en mer systematisk tilnærming på leverandøroppfølging.

6. ***Hvilket tidsperspektiv gjelder for iverksettelse og gjennomføring av tiltak/ene?***
   Arbeidet starter i 2024 og forsetter inn i 2025. Sikkerhetsforbedringer er et kontinuerlig arbeid.

7. ***Oppfattes rapporten som nyttig? Oppgi begrunnelse hvis dette ikke allerede har framkommet som svar på ovenstående spørsmål.***
   Denne type tester og revisjon som ser oss i kortene oppfattes som svært nyttig for Elvia. De går inn i det kontinuerlige forbedringsarbeid og passer fint inn i det metodiske arbeidet med og forbedre informasjonssikkerheten. Elvia er stadig gjenstand for revisjoner fra flere parter f.eks. både fra internrevisjon i konsernet og fra NVE, samt at det i tillegg utføres egne sikkerhetstester og risikoanalyser. Slike revisjoner mottas med åpne armer, men det eneste Elvia har å utsette på er at det kan bli litt vel mange revisjoner – de stjeler litt kapasitet i organisasjonen som ellers kunne vært benyttet til å forbedre informasjonssikkerheten.

8. ***Hvordan vurderes rapportens oppbygning og språkbruk?***
   Elvia vurdere rapporten som ryddig og tydelig.

Med vennlig hilsen

**SIGURD KVISTAD.**
Avdelingsleder Driftskontroll
Driftskontroll | Elvia AS

+47 90763425
sigurd.kvistad@elvia.no
elvia.no

Elvia

# Vedlegg 4: Uttalelse fra byrådsavdeling for kultur og næring

Byrådsavdeling for kultur og næring

Oslo

Kommunerevisjonen
Fredrik Selmers vei 3
0663 OSLO

| Deres ref.: | Vår ref. (saksnr.): | Saksbeh.: | Dato: |
|---|---|---|---|
| | 23/4897 - 6 | Anders Østre, 922 91 958 | 04.06.2024 |

## Administrativt svar fra Byrådsavdeling for kultur og næring - Rapport med mulighet til uttalelse: Teknisk informasjonssikkerhet i Elvia AS

Det vises til brev av 14.05.2024 med oversendelse av revisjonsrapport, samt informasjonsmøte hvor Kommunerevisjonen redegjorde for hovedfunnene i rapporten.

Kommunerevisjonen har undersøkt om Elvia AS har etablert tilfredsstillende teknisk informasjonssikkerhet i systemene som er nødvendig for å ivareta kraftforsyningen. Det har blitt gjennomført sikkerhetstesting i regi av Kommunerevisjonen ved bruk av konsulenter innen sikkerhetstesting fra EY. Undersøkelsen viser at Elvia AS hadde iverksett flere tiltak som kunne bidra til å etablere en teknisk sikkerhet i sine systemer på de undersøkte områdene. Kommunerevisjonen kom med anbefalinger på enkelte områder, og Elvia AS ble her anbefalt å vurdere ytterligere tiltak.

Oslo kommune har indirekte eierskap i Elvia AS gjennom Hafslund AS og Hafslund Vekst AS som eier 50 prosent av Eidsiva Energi AS som eier Elvia AS. Oslo kommune har derfor heller ikke Oslo bestemmende innflytelse over selskapet. De anbefalinger Kommunerevisjonen har fremsatt retter seg direkte mot Elvia AS. Kommunerevisjonen har ikke fremsatt anbefalinger som retter seg mot byrådsavdelingen, men har gitt byrådsavdelingen mulighet for å uttale seg om rapporten.

Byrådsavdelingen vurderer det som positivt at Kommunerevisjonens undersøkelse har bidratt til å sette fokus på teknisk informasjonssikkerhet i Elvia AS.

Vennlig hilsen

| | |
|---|---|
| Eli-Kristin Vorkinn | Anders Østre |
| kommunaldirektør | konst. seksjonssjef |

Oslo kommune
Byrådsavdeling for kultur og næring

Besøksadresse:
Olav V gate 4
Postadresse:
Rådhuset, 0037 OSLO

Telefon: 21 80 21 80
postmottak@byr.oslo.kommune.no
Org. Nr.: 997703634
oslo.kommune.no

Oslo

Oslo Kommune
Kommunerevisjonen
Fredrik Selmers vei 3
0663 Oslo

Tel. +21 80 21 80

Rapport 11/2024

Du finner mer informasjon
om Kommunerevisjonen
og våre rapporter på:
**www.krv.oslo.kommune.no**