

Informasjonssikkerhet og personvern

Malvik kommune, 14. oktober 2026

Oppdragsansvarlig revisor Anna Ølnes

Problemstillinger

- 1) Har Malvik kommune etablert et styringssystem for informasjonssikkerhet og personvern som tilfredsstiller krav i regelverket (systematisk rammeverk)?
- 2) Har Malvik kommune etablert tilfredsstillende avtaler med og oppfølging av VarIT (Stjørdal kommune), som sikrer organisatoriske og tekniske tiltak for informasjonssikkerhet og personvern?

Taushetsplikt

GDPR

Begrepsbruk

Personvern

Informasjonssikkerhet

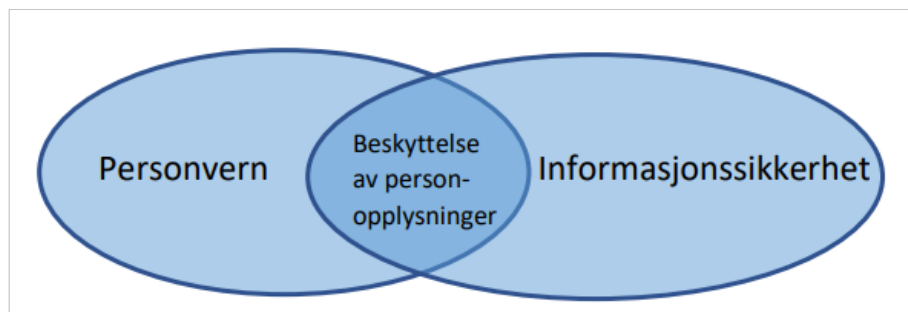
Data

Digitalisering

EDB

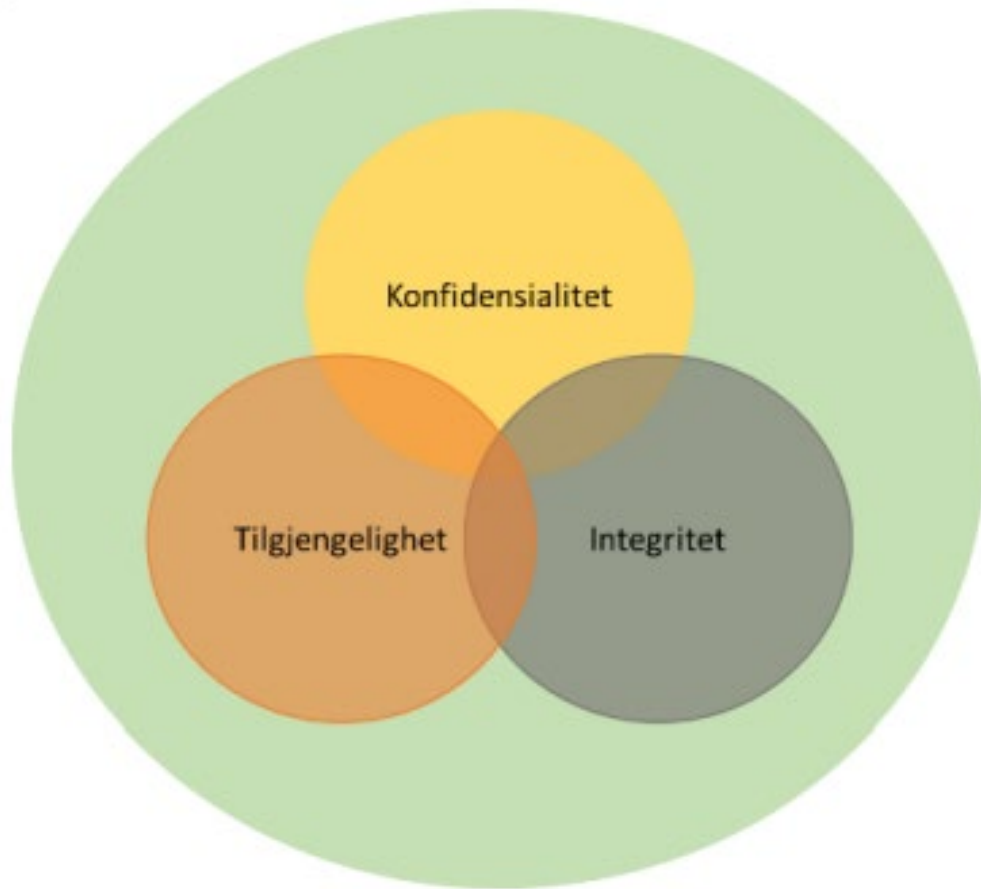
PM Revisjon
Midt-Norge

Informasjonssikkerhet og personvern



- Personvern (Datatilsynet):
 - retten til et privatliv og retten til å bestemme over egne personopplysninger
 - Rett på en privat sfære
 - Rett til innflytelse på bruk og spredning av personopplysninger om seg selv
- Informasjonssikkerhet (DFØ):
 - Arbeidet med informasjonssikkerhet handler om å sikre informasjonsbehandling som inngår i oppgaver og tjenester eller understøtter dem.

Informasjonssikkerhet



- **Konfidensialitet:**

sikre at informasjonen ikke blir kjent for uvedkommende

- **Integritet:**

sikre at informasjonen ikke blir endret utilsiktet eller av uvedkommende

- **Tilgjengelighet:**

sikre at informasjonen er tilgjengelig ved behov

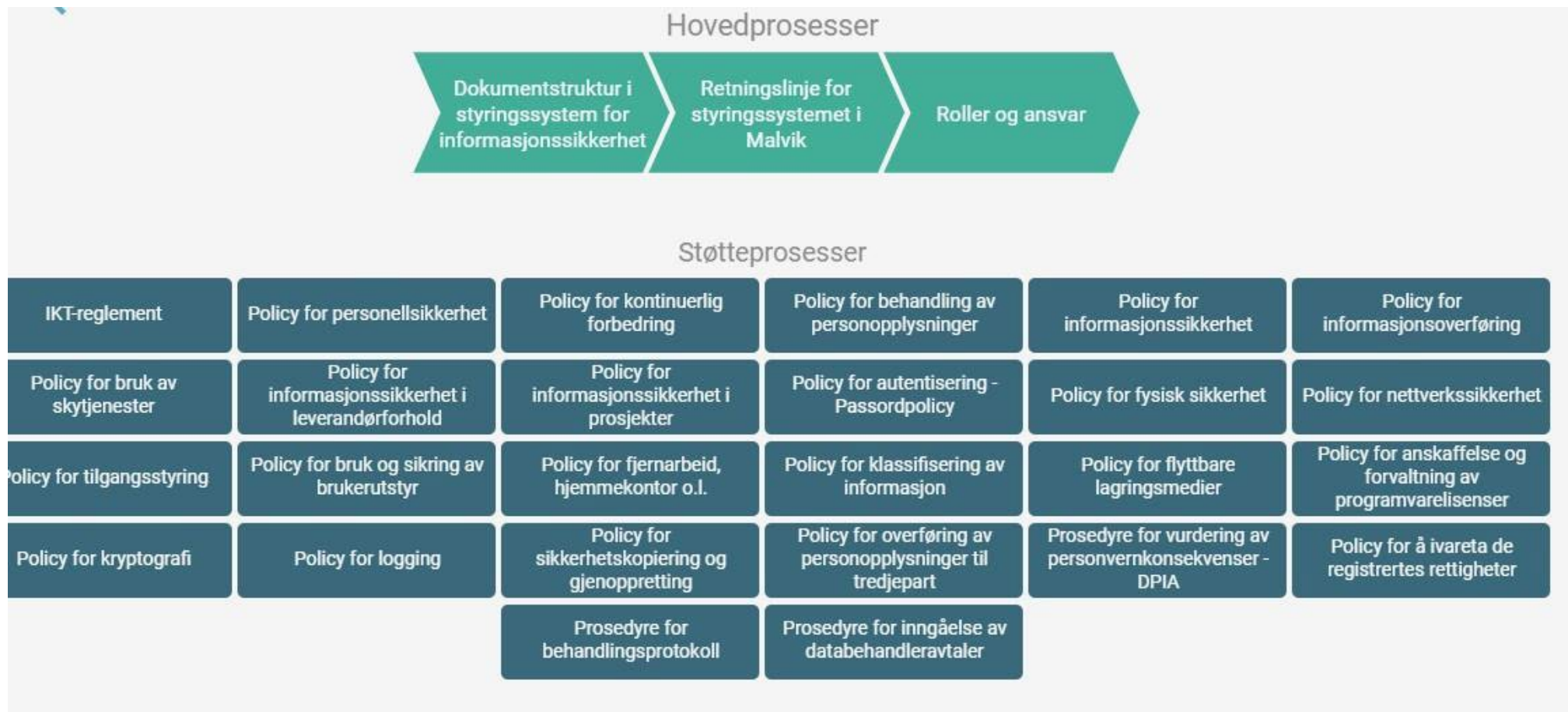
Har Malvik kommune etablert et styringssystem for informasjonssikkerhet og personvern som tilfredsstiller krav i regelverket (systematisk rammeverk)?

- Sikkerhetsmål, sikkerhetsstrategi og sikkerhetsorganisering
 - Internkontroll
 - Personvern
- Opplæring og informasjon

Sikkerhetsmål, sikkerhetsstrategi og sikkerhetsorganisering



Sikkerhetsmål, sikkerhetsstrategi og sikkerhetsorganisering



Sikkerhetsmål

Policy for informasjonssikkerhet:

- Kommunen skal sikre konfidensialiteten, integriteten og tilgjengeligheten i all sin informasjonsbehandling.
- Kommunen skal sikre kontinuiteten til kritiske systemer og tjenester.
- Kommunen skal sikre at personvernet til de registrerte ivaretas.

Policy for behandling av personopplysninger:

- Sikre og dokumentere at alle behandlinger er lovlige, og har tydelige definerte og legitime formål.
- Sikre etterlevelse av personvernregelverket

Sikkerhetsorganisasjon

Sikkerhetsorganisasjonen er den delen av kommuneorganisasjonen som er ansvarlig for å utvikle, implementere, overvåke og forvalte styringssystemet for informasjonssikkerhet. Medlemmer av sikkerhetsorganisasjonen skal ha spesifikke roller og ansvar, og skal samarbeide for å sikre at kommunen har et effektivt styringssystem. Sikkerhetsorganisasjonen bør etablere faste samarbeidsarenaer.

Sikkerhetsorganisasjonen består av:

- Kommunedirektørens strategiske ledergruppe (representant fra gruppen)
- Sikkerhetsansvarlig i Malvik (Organisasjonssjef - CISO)
- Digitaliseringsleder
- IT-leder Værnesregionen IT (VarIT)
- Personvernombud (Værnesregionen)

Sikkerhetsmål, sikkerhetsstrategi og sikkerhetsorganisering

Etter revisors vurdering har kommunen beskrevet sikkerhetsmål og sikkerhetsorganisasjon, hvor roller og ansvar er beskrevet. Kommunen har ikke beskrevet sikkerhetsstrategi.



Informasjonssikkerhet og personvern i internkontrollen

- Oversikt over regelverk, prosedyrer og rutiner for informasjonssikkerhet og personvern
- Risiko- og sårbarhet og beredskap for informasjonssikkerhet og personvern
- System for håndtering av avvik innen informasjonssikkerhet og personvern

Regelverk, prosedyrer og rutiner



ROS-analyser og beredskapsplaner

- Helhetlig ROS-analyse:
 - Sabotasje IT
 - Sabotasje mot vannforsyningen
 - Cyberhacking
 - Langvarig bortfall av strøm og telenett
- Arbeid med ny, helhetlig ROS
- Overordna beredskapsplan

Informasjonssikkerhet - avvikssystemet

- Avvik innen informasjonssikkerhet og personvern er delt i to hovedkategorier:
 - Informasjonssikkerhet – sikkerhetshendelse, fem underkategorier
 - Informasjonssikkerhet – personvern (GDPR), 25 underkategorier

Informasjonssikkerhet og personvern i internkontrollen

Etter revisors vurdering inngår informasjonssikkerhet og personvern i kommunens system for internkontroll

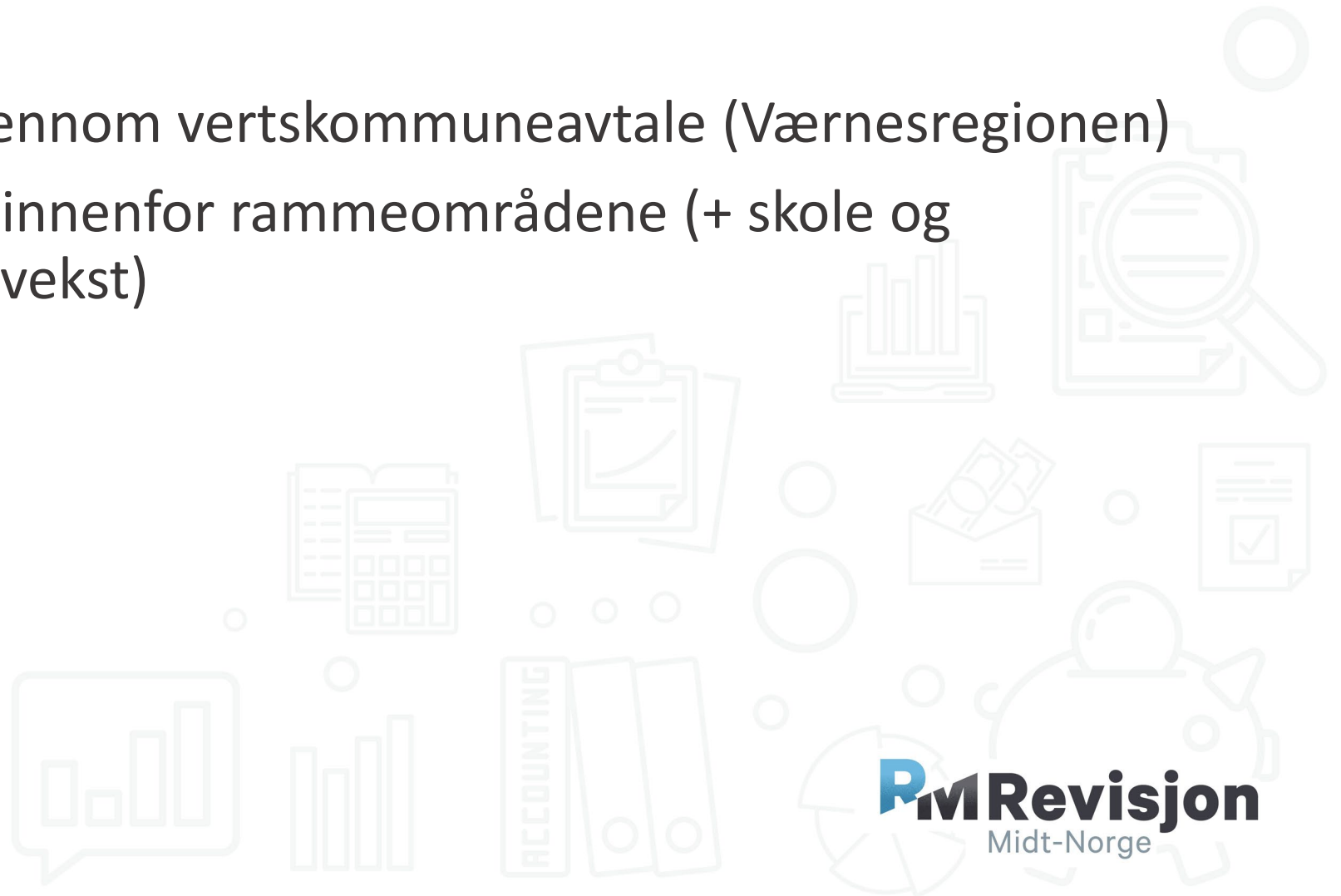


Personvern

- Kommunen skal ha et personvernombud
 - Det skal sikres nødvendig uavhengighet for personvernombudet
 - Personvernombudet skal sikres nødvendige ressurser for å utføre minimumoppgaver
 - Kommunen skal ha rutiner for personvernombudets arbeid som sikrer involvering, og det bør være regelmessig dialog med ledelsen.

Personvernombud

- Personvernombud gjennom vertskommuneavtale (Værnesregionen)
- Personvernkontakter innenfor rammeområdene (+ skole og barnehage innen oppvekst)



Personvernombud

Revisor vurderer at kommunen har etablert en ordning med personvernombud.

Revisor vurderer at personvernombudet er sikret uavhengighet, ved at det er organisert gjennom vertskommunesamarbeid i Værnesregionen.

Revisor vurderer at personvernombudet i hovedsak er sikret minimumsressurser for å utføre funksjonen som personvernombud.

Revisor vurderer at det er etablert rutiner for personvernombudets arbeid, som sikrer involvering og regelmessig dialog med ledelsen.

Behandlinger

- Kommunen skal føre protokoll over hvilke personopplysninger de behandler, som minimum inneholder obligatorisk informasjon.
- Kommunen skal ha databehandleravtaler som minimum inneholder obligatorisk informasjon.
- Kommunen skal gjennomføre en vurdering av personvernkonsekvenser før behandlinger som sannsynligvis vil medføre høy risiko for fysiske personers rettigheter og friheter.

Behandlinger

- **Behandling:** Enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke
- **Behandlingsansvarlig:** En fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes.
- **Databehandler:** Den behandlingsansvarliges representant skal føre en protokoll over behandlingsaktiviteter som utføres under deres ansvar.
- **Databehandleravtale:** Avtale med ekstern behandler
- **Behandlingsprotokoll:** Den behandlingsansvarliges representant skal føre en protokoll over behandlingsaktiviteter som utføres under deres ansvar. Det stilles også krav til hva behandlingsprotokollen skal inneholde (.

Behandlinger

- Prosedyre for behandlingsprotokoll i Compilo
- Kommunens behandlingsprotokoller ligger i Visma Draftit:
 - 39 behandlinger (47)
 - 22 oppført som ferdigbehandlet
- Prosedyre for databehandleravtaler i Compilo
 - Utelukkende Malvik kommune som er part i databehandleravtale, ikke Værnesregionen
 - Bruker DFØs mal for databehandleravtale
 - Systemansvarlige (ofte kommunalsjef) ivaretar databehandleravtaler
 - Databehandleravtaler er lenket til Elements (sak- og arkivsystem) – (revisor har ikke hatt tilgang)
- Vurdering av personvernkonsekvenser (DPIA)
 - Dersom det er sannsynlig at en type behandling vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige før behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet

Behandlinger

Veileder for DPIA i Compilo

Prosedyre for DPIA i Compilo

Vurdering av personvernkonsekvenser				
Innledende DPIA	Systematisk beskrivelse	Nødvendighet og rimelighet	Risiko for de registrerte	Ledelsens validering
Foreligger det høy risiko?	Systematisk beskrivelse av behandlingen (art, omfang, formål og sammenheng)	Oppfyller behandlingen personvern-prinsippene Står behandlingen i et rimelig forhold til formålene	Hva er personvernkonsekvensene for de registrertes rettigheter og friheter?	Hva er innstillingen til ledelsen? Hvilke vurderinger har ledelsen gjort? Har ledelsen godkjent DPIA?

Behandlinger

Revisor vurderer at kommunen i noen grad fører protokoll over personopplysninger som de behandler

Revisor vurderer at arbeidet med databehandleravtaler delvis er fulgt opp.

Revisor vurderer at DPIA-er i varierende grad gjennomføres.

Opplæring

- Kommunen bør sørge for at ansatte får tilstrekkelig opplæring i og informasjon om informasjonssikkerhet og personvern, herunder opplæring i bruk av kunstig intelligens.

Revisor vurderer at kommunen legger til rette for opplæring i informasjonssikkerhet, også i KI, men mangler oversikt over ansattes gjennomføring av kompetansetiltak innen disse områdene.

Har Malvik kommune etablert tilfredsstillende avtaler med og oppfølging av VarIT (Stjørdal kommune), som sikrer organisatoriske og tekniske tiltak for informasjonssikkerhet og personvern?



Avtale(r) med vertskommunen

- Det skal være inngått samarbeidsavtale og eventuelt andre avtaler som er tydelig på myndighet, ansvar og oppgaver, og som er oppdatert i henhold til gjeldende regelverk.
- Det bør være regelmessig samhandling mellom VarIT og Malvik kommune, hvor informasjonssikkerhet og personvern er ivarettatt.
- Malvik kommune bør påse at tjenestene fra VarIT styres etter en virksomhetsplan med mål og resultatkrav.
- Malvik kommune bør påse at kommunedirektøren i vertskommunen rapporterer til kommunestyret i Malvik per. tertial (herunder årsrapport) i henhold til avtalen.

Avtale(r) med vertskommunen

Revisor vurderer at Malvik kommune har inngått samarbeidsavtale (vertskommuneavtale) om IKT-tjenester, i tillegg til overordna vertkommuneavtale om tjenester i Værnesregionen, men avtalen er ikke tydelig nok på myndighet, ansvar og oppgaver.

- Revisor vurderer at kriteriet er delvis oppfylt

Revisor vurderer at det er regelmessig samhandling mellom den sentrale ledelsen i Malvik kommune og VarIT.

- Revisor vurderer at kriteriet er oppfylt

Revisor vurderer at Malvik kommune ikke påser at IKT-tjenesten styres etter en virksomhetsplan med mål og resultatkrav.

- Revisor vurderer at kriteriet ikke er oppfylt.

Avtale(r) med vertskommunen

Revisor vurderer at Malvik kommune ikke påser at kommunedirektøren i Stjørdal rapporterer til kommunestyret i Malvik kommune.



Samarbeid om organisatoriske og tekniske tiltak

Grunnprinsippene for IKT-sikkerhet:

- **Identifisere og kartlegge**
 - Ha oversikt over enheter, programvare og tilganger
- **Beskytte og opprettholde**
 - Sikkerhet i anskaffelser, utviklingsprosesser, IKT-arkitektur, nettverk, e-post og nettleser.
- **Oppdage og overvåke**
 - Oppdage og overvåke sårbarheter og trusler, gjennomføre inntrengningstester
- **Håndtere og gjenopprette**
 - Forberede (beredskap) på hendelser, håndtering av og evaluering/læring etter hendelser.

Samarbeid om organisatoriske og tekniske tiltak

Revisor vurderer at oversikt over enheter, programvare og tilganger i hovedsak blir ivaretatt.

- Revisor vurderer at kriteriet i hovedsak er oppfylt

Revisor vurderer at sikkerheten i anskaffelser, tjenesteutsettelse, IKT-arkitektur og sikkerhetsoppdateringer i hovedsak blir ivaretatt.

- Revisor vurderer at kriteriet er delvis oppfylt.

Revisor vurderer at det i hovedsak er kontroll på sikkerhetstilstand og ledelsens gjennomgang gjennom samarbeidet mellom Malvik kommune og VarIT, men at det fortsatt gjenstår avklaringer rundt operasjonell teknologi innen viktige infrastrukturområder.

- Revisor vurderer at kriteriet i hovedsak er oppfylt

Samarbeid om organisatoriske og tekniske tiltak

Revisor vurderer at prinsippet for håndtering, gjenoppretting og læring av hendelser i noen grad er ivaretatt.

- Revisor vurderer at kriteriet delvis er oppfylt



Anbefalinger

Revisor anbefaler kommunedirektøren å:

- Beskrive sikkerhetsstrategi for å nå sikkerhetsmålene
- Sørge for at kommunestyret får avtalt rapportering om personvernombudet og VarITs virksomhet
- Utarbeide og ajourføre behandlingsprotokoller, databehandleravtaler og konsekvensvurderinger for personvern (DPIA)
- Følge opp ansattes opplæring og informasjon om informasjonssikkerhet og personvern
- Avklare uklarheter i roller og ansvar i samarbeidet med VarIT