Rogaland Revisjon

Forvaltningsrevisjon

Informasjonssikkerhet

Rogaland fylkeskommune, 2021

INNHOLD

OPPDRAGET

Bestilling

Kontrollutvalget og kvalitetsutvalget i Rogaland fylkeskommune bestilte 04.02.2021 en forvaltningsrevisjon om informasjonssikkerhet.

Formål

Formålet med prosjektet er å vurdere fylkeskommunens systemer og rutiner for informasjonssikkerhet og vurdere hvordan dette følges opp i praksis.

Problemstillinger[1]

- Er ROS-analysen for IKT-sikkerhet i fylkeskommunen oppdatert og dekkende?
- Har fylkeskommunen tilfredsstillende systemer og rutiner for å ivareta krav til informasjonssikkerhet?
  - Hvordan er rutiner og praksis for avhending av IKT-utstyr?
- I hvilken grad er oppgaver og ansvar relatert til informasjonssikkerhet og personvern tydeliggjort?
  - Hvilket politisk utvalg følger opp informasjonssikkerhet i fylkeskommunen og hvor mange saker har de hatt til behandling?
- I hvilken grad blir fylkeskommunens systemer og rutiner innen informasjonssikkerhet og personvern etterlevd i virksomhetene?
- I hvilken grad har fylkeskommunen sikret en god praksis for registrering og oppfølging av avvik innen informasjonssikkerhet og personvern? (herunder antall avvik knyttet til sensitiv informasjon og årsaker til disse)
- Hvilke tiltak er iverksatt for å styrke kompetansen innen informasjonssikkerhet hos de ansatte, både generelt og blant de som jobber med IKT?
- Hvor mange ganger har fylkeskommunen de siste fire årene opplevd alvorlige cyberangrep eller alvorlige driftsforstyrrelser ved fylkeskommunale nett, programmer eller e-postsystemer? Og har fylkeskommunen reserveløsninger som er raskt tilgjengelig og dekkende for behovene?
  - Har fylkeskommunen en tilstrekkelig plan for å håndtere bortfall av kritiske systemer?

Prosjektleder for dette prosjektet har vært forvaltningsrevisor Inger Bjørgo Hustvedt og forvaltningsrevisor Elin Fagerheim Bjerke har deltatt i deler av datainnsamlingen og kvalitetssikringen av rapporten frem til 31.08.21. Ståle Opedal overtok som kvalitetssikrer i september 2021.

[1]. Kontroll og kvalitetsutvalget har lagt inn ekstra problemstillinger

SAMMENDRAG

På oppdrag fra kontroll- og kvalitetsutvalget har Rogaland Revisjon utført forvaltningsrevisjon av informasjonssikkerheten i fylkeskommunen. Formålet med prosjektet har vært å vurdere fylkeskommunens systemer og rutiner for informasjonssikkerhet og vurdere hvordan dette følges opp i praksis. I prosjektet er det foretatt dokumentanalyse, intervjuer i ulike avdelinger i sentraladministrasjonen, fire skolebesøk og gjennomført kontroll i postlisten.

Hovedbudskap

- Fylkeskommunen har i 2021 utarbeidet og implementert flere nye rutiner som høyner kvaliteten på informasjonssikkerhetsarbeidet.
- Det gjenstår arbeid for å forankre og tydeliggjøre oppgaver og ansvar for daglig behandlingsansvarlige i enhetene.
- Fylkeskommunen mangler oppdatert ROS-analyse, beredskapsplan og skriftlige rutiner for IKT-sikkerhet.

Har fylkeskommunen tilfredsstillende systemer og rutiner for å ivareta krav til informasjonssikkerhet? Hvordan er rutiner og praksis for avhending av IKT-utstyr?

Innen informasjonssikkerhet har fylkeskommunen et dokumenthierarki bestående av styrende og gjennomførende dokumenter (rutiner). De styrende dokumentene beskriver i tilfredsstillende grad sikkerhetsmål og strategi og har et system for årlig statusgjennomgang. Fylkeskommunen har sommeren 2021 publisert en rekke nye og oppdaterte rutiner som tydeligere ivaretar krav til informasjonssikkerheten. Men fylkeskommunen mangler oppdatert IKT-tjenestekatalog. Fylkeskommunen har rutiner for tilgangsstyring og rammeavtale med leverandør for sikker avhending og kassering av IKT-utstyr. Tilganger til fagsystemer gjøres manuelt og utgjør en risikofaktor for at uautoriserte får tilgang.

I hvilken grad er oppgaver og ansvar relatert til informasjonssikkerhet og personvern tydeliggjort? Hvilket politisk utvalg følger opp informasjonssikkerhet i fylkeskommunen og hvor mange saker har de hatt til behandling?

Beskrivelsen av ansvar og oppgaver er spredt på ulike dokumenter og det mangler en tydelig overordnet beskrivelse av hva ledere og ansatte er ansvarlig for. Det er spesielt oppgaver og ansvar knyttet til rollen som daglig behandlingsansvarlig som bør tydeliggjøres. Administrasjonsutvalget har ansvar for å vedta retningslinjer for registrering av personopplysninger og planer og retningslinjer for bruk av informasjonsteknologi. Utvalget har de siste fem årene behandlet fem saker relatert til informasjonssikkerhetsarbeidet.

I hvilken grad blir fylkeskommunens systemer og rutiner innen informasjonssikkerhet og personvern etterlevd i virksomhetene?

Det generelle inntrykket fra intervjuer og skolebesøk er at ansatte vet hvor de skal finne rutiner for å ivareta informasjonssikkerhet, men at rutinene som ligger i avvikssystemet er lite tilgjengelig. Skolene har god praksis for kryptering av e-post, men har ulik praksis for hvor

elevers personopplysninger lagres. Informasjonssikkerhetsinstruksen er ikke signert av alle ansatte enda.

Hvilke tiltak er iverksatt for å styrke kompetansen innen informasjonssikkerhet hos de ansatte, både generelt og blant de som jobber med IKT?

Fylkeskommunen tilbyr ulike kurs med frivillig deltakelse. Det er positivt at fylkeskommunen deltar på nasjonal sikkerhetsmåned og tilbyr ansatte kurs i digitale verktøy. Men fylkeskommunen har ingen obligatoriske kurs innen informasjonssikkerhet og har heller ikke et system for å måle kompetansenivået i organisasjonen.

I hvilken grad har fylkeskommunen sikret en god praksis for registrering og oppfølging av avvik innen informasjonssikkerhet og personvern? (herunder antall avvik knyttet til sensitiv informasjon og årsaker til disse)

Fylkeskommunen har et avvikssystem (QM+) som informantene er godt kjent med. Terskelen for å melde inn avvik er derimot noe høy og det er behov for opplæring og bevisstgjøring rundt innmelding av avvik og avviksbehandling. Siden 2017 er det meldt inn 275 avvik i kategori «informasjonssikkerhet», men mange av disse er feilregistrert og handler om HMS-avvik. Det er meldt inn 21 avvik knyttet til sensitiv informasjon, de fleste av disse handler om feilsending, manglende lydisolering i forbindelse med personsensitive samtaler, ulåste PC'er og ulåst dør. Fylkeskommunen har egen årlig rapportering på avvik i QM+. I intervjuer fremkommer det at det burde vært mer kontroll på hvordan tiltak for å lukke avvik jobbes med i etterkant.

Hvor mange ganger har fylkeskommunen de siste fire årene opplevd alvorlige cyberangrep eller alvorlige driftsforstyrrelser ved fylkeskommunale nett, programmer eller e-postsystemer? Og har fylkeskommunen reserveløsninger som er raskt tilgjengelig og dekkende for behovene? Har fylkeskommunen en tilstrekkelig plan for å håndtere bortfall av kritiske systemer?

Fylkeskommunen har ikke opplevd alvorlige cyberangrep eller driftsforstyrrelser de siste fire årene. Fylkeskommunen har et forsvar mot cyberangrep som består av ulike tekniske innretninger og rutiner, for eksempel brannmursikring og virusskanning. Mange viktige sikkerhetstiltak ligger også innebygd hos de store linjevereandørene. Fylkeskommunes reserveløsninger er separate datarom som kan ta over for hverandre samt sikkerhetskopiering. Fylkeskommunen mangler imidlertid skriftlige rutiner for teknisk sikkerhet og beredskapsplan.

Er ROS-analysen for IKT-sikkerhet i fylkeskommunen oppdatert og dekkende?

Gjeldende ROS-analyse for IKT-sikkerhet gjelder for de videregående skolene og er ikke dekkende for bruk av IKT-utstyr i alle fylkeskommunens enheter. Ettersom ROS-analysen er fra 2013 er den ikke oppdatert ut ifra nye lovkrav innen personvern og nye sikkerhetstrusler innen informasjonssikkerhet.

Anbefalinger

Revisjonen kommer med følgende anbefalinger til fylkeskommunen:

- Fylkeskommunen bør oppdatere IKT-tjenestekatalogen
- Oppgaver og ansvar knyttet til behandlingsansvar bør gjøres tydeligere og forankres bedre i enheten.
- Fylkeskommunen bør sikre at administrasjonsutvalget får behandlet retningslinjer for registrering av personopplysninger og planer og retningslinjer for bruk av informasjonsteknologi.
- Informasjonssikkerhetsinstruksen bør signeres av alle ansatte.
- Fylkeskommunen bør sette inn tiltak for å senke terskelen for innmelding av avvik
- Fylkeskommunen bør lage rutiner for IKT-sikkerhet og beredskapsplan
- Lage en ny ROS-analyse som dekker IKT-sikkerhet for hele fylkeskommunens virksomhet.

FYLKESRÅDMANNENS KOMMENTAR

Fylkesrådmannens kommentar mottatt 05.11.21:

Fylkesrådmannen tar funnene og anbefalingene i Rogaland Revisjon til revisjonsrapport om informasjonssikkerhet og personvern til orientering, og slutter seg til både funn og anbefalinger. Anbefalingene vil være et nyttig arbeid i det videre arbeidet med å videreutvikle en risiko-orientert og systematisk kultur for å ivareta informasjonssikkerhet for både ansatte og brukere/innbyggere i Rogaland fylkeskommune. Rapporten peker på at en rekke rutiner og retningslinjer innenfor informasjonssikkerhet og personvern har kommet på plass i 2021, og det er viktig for fylkesrådmannen å understreke at disse rutinene og retningslinjene er resultatene av arbeid som har pågått over tid. Et av de prosjektene som ble satt i gang allerede i 2018 var arbeidet med lagringsveilederen. Lagringsveilederen henger sammen med risikovurderingene av M365 og VIS, og må også sees i sammenheng med at det har blitt jobbet med rollefordeling i arbeidet på fagfeltet. Disse prosessene har det blitt jobbet med fortløpende i tidsrommet 2018-2021. Arbeid med informasjonssikkerhet og personvern er et kontinuerlig arbeide, der fylkeskommunen skal søke etter å være best mulig rustet for å møte utfordringene på fagfeltet til enhver tid, samtidig som det må opprettholdes en balansegang for å sikre effektiv daglig drift. Arbeid med risikoforståelse og sikkerhetskultur må gå hånd i hånd med daglige oppgaver, for både ledere og ansatte.

I 2021 vedtok fylkesrådmannen anskaffelsesrutinen som tydeliggjør det delegerte ansvaret innenfor fagområdet. Med forbehold om at forslaget blir godkjent i Fylkestingets behandling av budsjettforslag for 2022 vil det bli opprettet en ny stilling som informasjonssikkerhetsrådgiver. Organiseringen av ansvar for informasjonssikkerhet og personvern i Rogaland fylkeskommune fra 2022 er illustrert i bildet nedenfor:

I denne kommentaren ønsker fylkesrådmannen å belyse de ulike anbefalingene fra Rogaland Revisjon, punkt for punkt:

1. Fylkeskommunen bør oppdatere tjenestekatalogen.
   Kommentar: Arbeidet med å oppdatere tjenestekatalogen er i gang. Hvordan tjenestekatalogen skal se ut henger sammen med både rollefordelingen nevnt over, og med bestillingen av administrativt delegasjonsreglement fra internkontrollkoordinator. Målet med ny tjenestekatalog er å skape en levende oversikt over systemer, systemeierskap, kontaktpersoner, informasjon om behandling av personopplysninger og leverandører presentert for organisasjonen som en intranettside, knyttet til internkontroll. Hensikten med å legge tjenestekatalogen under internkontroll heller enn under Avdeling for digital utvikling er å understreke at systemeierskapet er et delegert ansvar. Således vil avdeling for digital utvikling fylle inn tjenestekatalogen med de digitale basistjenestene som tilbys til hele organisasjonen, mens de øvrige avdelingene og enhetene får i oppgave å dokumentere egne programmer/systemer/apper osv. På denne måten vil fylkesrådmannen også oppnå en større oversikt over hvilke behandlinger fylkeskommunen som en helhet utfører. Arbeidet er, fra Avdeling for digital utvikling sin side, planlagt ferdig høsten 2021, og når intranettsiden er på plass vil bestillingen til de øvrige partene om å fylle inn sine opplysninger gå ut som et formelt brev.

2. Oppgaver og ansvar knyttet til behandlingsansvar bør gjøres tydeligere og forankres bedre i enheten.
   Kommentar: Som vist i innledningen til fylkesrådmannens kommentar, og i illustrasjonen over, har plasseringen av oppgaver og ansvar innenfor informasjonssikkerhet og personvern lenge vært jobbet med i Rogaland fylkeskommune. P.t utarbeides det funksjonsbeskrivelser for både behandlingsansvarlige og personvernkoordinatorer. Funksjonsbeskrivelsene vil følge bestillingen fra fylkesrådmannen til avdelinger, enheter og seksjoner som skal opprette funksjonen personvernkoordinator, og vil tydeliggjøre både ansvarsfordeling og oppgaver knyttet til rollen. Alle systemer/apper/programmer som behandler personopplysninger skal, i tråd med anskaffelsesrutinen for digitale løsninger, ha en behandlingsansvarlig. Avdeling for digital utvikling skal, i samråd med personal- og organisasjonsavdelingen og Fylkesadvokaten, tilby opplæring av systemeiere, behandlingsansvarlige og personvernkoordinatorer på samme måte som opplæring i M365 har blitt gjennomført. Opplæringen vil være obligatorisk. Alle ansatte vil få et grunnkurs i personvern og informasjonssikkerhet. Disse kursene skal utarbeides og tilbys i løpet av 2022.

3. Fylkeskommunen bør sikre at administrasjonsutvalget får behandlet retningslinjer for registrering av personopplysninger og planer og retningslinjer for bruk av informasjonsteknologi.
   Kommentar: Fylkesrådmannen vurderer arbeidet for å operere i tråd med gjeldende lovverk og retningslinjer til å være administrative oppgaver innenfor hans ansvarsområde. Administrasjonsutvalget behandler digital strategi, og arbeidet med retningslinjer for registrering av personopplysninger og planer og retningslinjer for bruk av informasjonsteknologi anses som en del av arbeidet inn under den digitale strategien

som gjelder fra 2020 – 2024. Administrasjonsutvalget skal informeres om arbeidet gjennom statusoppdateringer knyttet til handlingsplanene for digitaliseringsutvalget, derunder handlingsplan for informasjonssikkerhet og personvern. I mandat for digitaliseringsutvalget står det, blant annet:

- *Vi skal ivareta informasjonssikkerhet og personvern etter gjeldende lovverk/regler.*
- *Nye digitale løsninger/systemer/prosjekter skal behandles i digitaliseringsutvalget.*
- *- Opplæring skal være del av alle prosjekt.*
- *- Vi skal ha gode rutiner for anskaffelser, og systemeierskap med det det innebærer, skal ut i avdelingene, (behandlingsansvar, personvern og databehandleravtale).*
- *Delegert ansvar for systemeierskap og anskaffelser.*
- *Delegert forvaltningsansvar for systemer.*

4. Informasjonssikkerhetsinstruksen bør signeres av alle ansatte.
   Kommentar: Bestillingen fra fylkesrådmannen til alle ledere med personalansvar er klar og tydelig, alle ansatte skal signere på informasjonssikkerhetsinstruksen. Signert informasjonssikkerhetsinstruks er et vilkår for å kunne bruke fylkeskommunens nettverk og digitale løsninger. Fylkesrådmannen vil følge saken opp, og purre på de enhetene som ikke har sendt instruksen til digital signering.

5. Lage en ny ROS-analyse som dekker IKT-sikkerhet for hele fylkeskommunens virksomhet.
   Kommentar: Fylkesrådmannen planlegger å utføre en ROS-analyse på teknisk IKT-sikkerhet i forbindelse med flytting av datarom og sentrale løsninger grunnet renovering av fylkeshuset. I og med at denne revisjonsrapporten omhandler informasjonssikkerhet og personvern, og ikke teknisk IKT-sikkerhet, anser fylkesrådmannen anbefalingen om ROS-analyse dekket av anskaffelsesrutinen, som krever at det ved innkjøp av systemer som behandler personopplysninger skal opprettes behandlingsprotokoll, utføres risikovurdering og vurderes om DPIA er nødvendig.

6. Fylkeskommunen bør sette inn tiltak for å senke terskelen for innmelding av avvik.
   Kommentar: I forbindelse med at det skal organiseres kurs i informasjonssikkerhet og personvern for alle ansatte vil det være naturlig å la en refleksjon rundt melding av avvik innenfor informasjonssikkerhet og personvern, og den læringen det kan skape for organisasjonen, være en del av dette opplæringsløpet. Det handler både om å senke terskelen for å melde avvik, men også om å skape en forståelse for hva et avvik er, og hvordan avvik kan gi læring og utvikling.

7. Fylkeskommunen bør lage rutiner for IKT-sikkerhet og beredskapsplan.
   Kommentar: Fylkesrådmannen slutter seg til anbefalingen og vil nedsette en gruppe som skal lage beredskapsplan for IKT-sikkerhet, samt skriftlig dokumentere de rutiner for IKT-sikkerhet som allerede finnes og følges.

1 INNLEDNING

1.1 BAKGRUNN

Kontrollutvalget i Rogaland fylkeskommune bestilte 04.02.21 en forvaltningsrevisjon om informasjonssikkerhet.

1.2 REVISJONSKRITERIER

Revisjonskriterier er elementer som inneholder krav eller forventninger, og vil bli brukt til å vurdere funn i de undersøkelser som gjennomføres. Kriteriene skal være begrunnet i, eller utledet av, autoritative kilder innenfor det reviderte området. Revisjonskriteriene er utledet av følgende lover og forskrifter:

- Kommuneloven
- Personopplysningsloven og personvernforordningen (GDPR)
- eForvaltningsforskriften

eForvaltningsforskriften § 15 stiller krav om at internkontroll på informasjonssikkerhetsområdet skal være basert på anerkjente standarder. Ifølge digitaliseringsdirektoratet er standarden ISO/IEC 27001 den anbefalte anerkjente standarden for offentlige virksomheter. Digitaliseringsdirektoratets veiledningsmateriell "Internkontroll i praksis - informasjonssikkerhet" er basert på og konkretiserer denne standarden, og dekker det Digitaliseringsdirektoratet anser som de viktigste kravene[2]. Datatilsynet har også utarbeidet en veileder for internkontroll. Digitaliseringsdirektoratet har i samarbeid med Nasjonal sikkerhetsmyndighet, Direktoratet for forvaltning og økonomistyring (DFØ) utarbeidet «Veileder i helhetlig styring og kontroll av informasjonssikkerhet»[3]. Denne veilederen ble utgitt våren 2021. Revisjonskriteriene er i tillegg til lovbestemte krav, utledet med utgangspunkt i disse tre veilederne. Revisjonskriterier som er utledet av veilederen er satt opp som «bør»-kriterier.

Våren 2020 gjennomførte Rogaland Fylkeskommune en informasjonssikkerhetsworkshop med innleid bistand fra TietoEVRY. Workshopen resulterte i en intern sikkerhetsrapport (modenhetsrapport) med totalt 19 tiltak for å etterkomme lovkrav innen personvern og informasjonssikkerhet og krav etter ISO 27002. Revisjonen har brukt funnene fra rapporten i utforming av revisjonskriteriene.

[2] https://internkontroll-infosikkerhet.difi.no/sites/sikkerhet/files/for_toppledere_-_internkontroll_informasjonssikkerhet.pdf

[3] https://www.digdir.no/informasjonssikkerhet/utarbeidet-av-nsm-dfo-og-digdir/2360

En nærmere beskrivelse av bakgrunn og utledning av revisjonskriterier kommer frem i fakta- og vurderingsdelen.

1.3 TIDLIGERE REVISJONER

Rogaland Revisjon, med bistand fra PwC, utførte i 2017 forvaltningsrevisjon på «Overordnet internkontroll». I denne ble det konkludert at fylkeskommunen mangler et helhetlig og overordnet system for internkontroll, at det i liten grad er etablert felles maler og rutiner for oppfølging av internkontroll. Videre ble det påpekt at det i liten grad er etablert en kultur og praksis for å gjøre risikovurderinger og at ansvar i liten grad er dokumentert. Fylkeskommunen ble blant annet anbefalt å utvikle felles, helhetlig system for internkontroll, sørge for aktiv bruk av risikovurderinger, vurdere behov for tydeliggjøring av lederansvar, følge opp bruk av avvikssystem. Som oppfølging nedsatte fylkeskommunen blant annet egen administrativ gruppe som fikk oppdrag med å komme med tiltak til anbefalingene[4].

I 2019 gjennomførte Rogaland Revisjon forvaltningsrevisjon av arkiv i fylkeskommune. Noen av oppfølgingspunktene fra denne rapporten var å gjøre arkivplan og rutiner for arkivering bedre kjent blant ansatte, sikre at alle ansatte signerer informasjonssikkerhetsinstruksen og å skjerpe praksis rundt utsending av personopplysninger på e-post.

Arkivverket gjennomførte i 2019 tilsyn som resulterte i fem pålegg. Påleggene ble i etterkant lukket og tilsynet ble avsluttet i mai 2021.

1.4 AVGRENSNINGER OG METODE

Personvernforordningen gir enkeltpersoner som de lagrede opplysningene kan knyttes til (de registrerte) en rekke rettigheter som f.eks. rett til innsyn, retting, sletting og dataportabilitet. Revisjonen vurderer hvorvidt fylkeskommunen har rutiner for å ivareta disse kravene, men vurderer ikke selve etterlevelsen av rutinene.

Metodisk er det gjennomført dokumentanalyse og ti intervjuer med ledere og ansatte i avdeling for digital utvikling, økonomiavdelingen, opplæringsavdelingen og personvernombud. Resultat fra interne spørreundersøkelser er også brukt. Revisjonen har hatt et spesielt fokus på etterlevelse av personvern og informasjonssikkerhet på de videregående skolene ettersom de håndterer mange personopplysninger. Det er gjennomført fire skolebesøk på ulike videregående skoler, med observasjon og intervjuer. På skolene ble det gjort gruppeintervju med ledelsen og enkeltintervjuer med flere lærere, sosialpedagogisk rådgiver og skolearkivar. Det er også gjennomført stikkprøver fra arkiv.

[4] https://einnsynrfk.public.cloudservices.no/application/getMoteDokument?dokid=200664621-928113

1.5 DEFINISJON AV SENTRALE BEGREPER

Informasjonssikkerhet: handler om å beskytte all type informasjon tilfredsstillende slik at informasjon ikke blir gjort kjent for uvedkommende, ikke blir endret utilsiktet og er tilgjengelig når de som skal ha tilgang har behov for det.

Personopplysninger: Personopplysninger er enhver opplysning om en privatperson som er identifisert eller som kan identifiseres, for eksempel navn, adresse, telefonnummer, e-post, fødselsnummer, adferdsmønstre og et bilde dersom personer kan gjenkjennes.

Særlig kategorier av personopplysninger: Personopplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, genetiske opplysninger og biometriske opplysninger, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering[5].

DPIA (Data Protection Impact Assessment): Er en vurdering av personvernkonsekvenser som skal sikre at personvernet til de som er registrert i løsningen ivaretas.

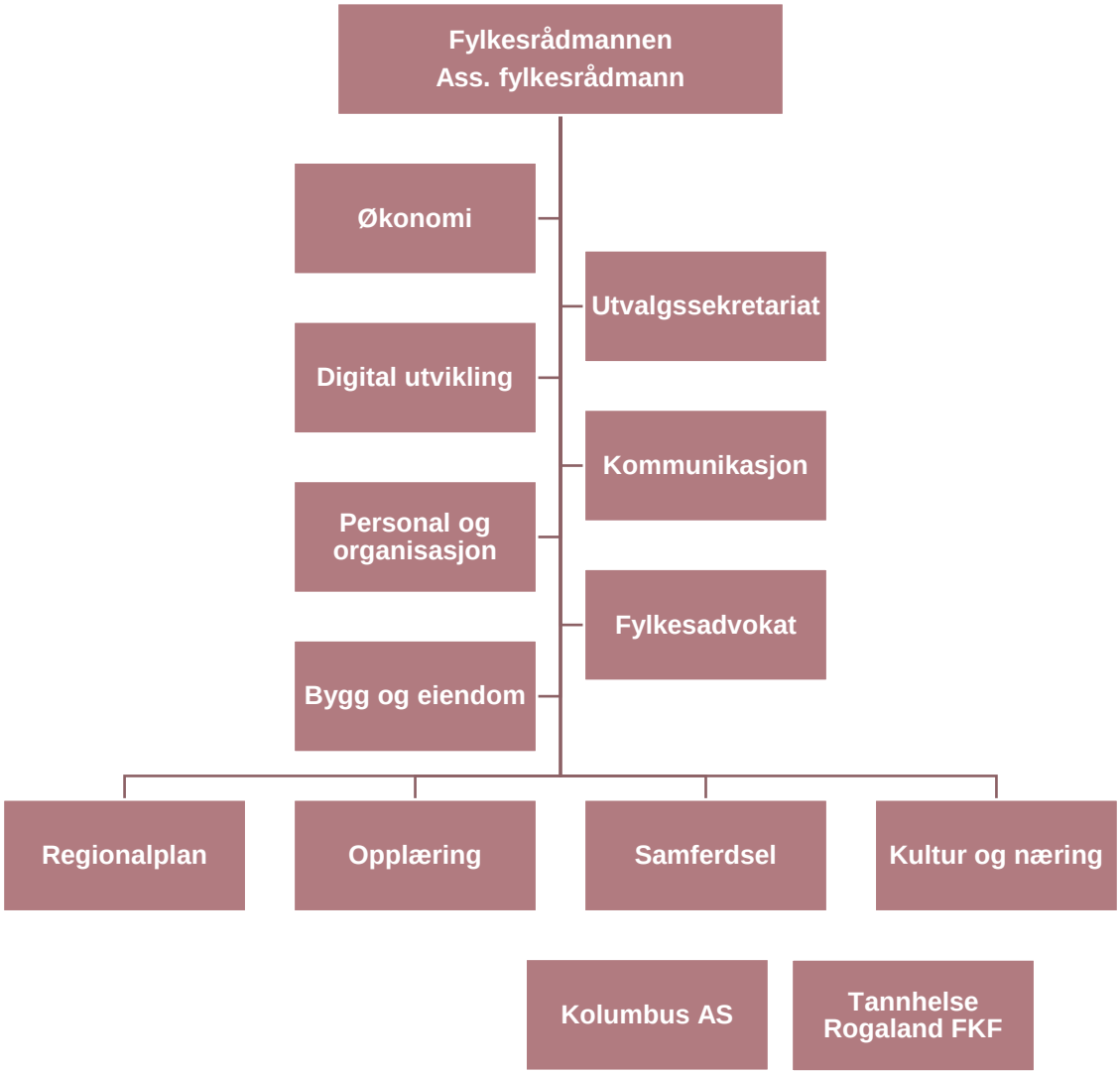
1.6 ORGANISERING AV IKT I ROGALAND FYLKESKOMMUNE

Rogaland fylkeskommune består av en fylkesadministrasjon med administrativ ledergruppe, syv stab- og støtteavdelinger samt fire fagavdelinger. Fylkeskommunen består videre av 25 videregående skoler, en fagskole og to skolesentre. I tillegg eier Rogaland fylkeskommune selskapene Kolumbus AS og Tannhelse Rogaland FKF. Totalt er det rundt 4 300 ansatte i fylkeskommunen.

Avdeling for digital utvikling består av IKT-drift, dokumentsenteret og faggruppe for digital utvikling. Faggruppen skal bistå hele organisasjonen med saker innen IKT og digitale arbeidsflater. Avdelingssjef for digital utvikling er del av administrativ ledergruppe. Skolene har egne IT-teknikere som har ansvar for utstyr installert ved skolene. Skolene mottar også tjenester fra sentraladministrasjonen som blant annet drift av IKT-baserte kommunikasjonssystemer, drift av skybaserte tjenester, sikkerhetsovervåkning og tilgangsstyring av fellestjenester.

[5] Lov om behandling av personopplysninger – artikkel 9

Figur 1. Organisasjonskart. Kilde: Rogaland fylkeskommune.



1.7 OPPBYGGING AV RAPPORTEN

Rapporten er delt opp i kapitler etter de syv problemstillingene. Kapittel seks svarer til problemstillingen «Hvilke tiltak er iverksatt for å styrke kompetansen innen informasjonssikkerhet hos de ansatte, både generelt og blant de som jobber med IKT?». Dette kapitlet ser også på hvordan ansatte generelt får opplæring i informasjonssikkerhet og personvern. Risikovurdering innen informasjonssikkerhet er både vurdert i kapittel to som ser på den overordna risikovurderingen for IKT-sikkerhet og kapittel fem hvor praksis rundt risikovurderinger for spesifikke systemer er vurdert.

2 SYSTEMER OG RUTINER

Problemstilling: «Har fylkeskommunen tilfredsstillende systemer og rutiner for å ivareta krav til informasjonssikkerhet? Hvordan er rutiner og praksis for avhending av IKT-utstyr?»

2.1 REVISJONSKRITERIER

En stor del av arbeidet med informasjonssikkerhet er knyttet til behandling av personopplysninger. Lov om behandling av personopplysninger med personvernforordningen (GDPR) gir virksomhetene juridiske forpliktelser rundt behandling av personopplysninger[6]. Det er også et større rettsvern for særlige kategorier[7] av personopplysninger. Etter personvernforordningen artikkel 5 fremkommer det at personopplysninger skal:

- Behandles på en lovlig, rettferdig og åpen måte.
- Samles inn for spesifikke og berettigede formål.
- Være adekvate, relevante og begrenset til formålet.
- Være korrekte og om nødvendig oppdaterte.
- Lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder enn nødvendig for formålet.
- Behandles på en måte som sikrer tilstrekkelig sikkerhet.

Ansvaret for å etterleve disse kravene ligger i rollen som behandlingsansvarlig i virksomheten. GDPR setter også andre krav til behandlingsansvarlig. Etter artikkel 30 skal behandlingsansvarlig føre protokoll over behandlingsaktiviteter for personopplysninger. Behandlingsansvarlig skal, ved for eksempel personvernerklæring på nettsiden, informere de registrerte personene om deres rettigheter (artikkel 12-14). Personopplysninger blir ofte lagret, samlet inn, utlevert eller slettet av andre en behandlingsansvarlig.

Etter artikkel 32 skal det gjennomføres risikovurderinger blant annet før nye systemer tas i bruk. Hvis behandling av personopplysninger medfører høy risiko for personers rettigheter og friheter skal det etter personvernforordningen artikkel 35 gjennomføres vurderinger av personvernkonsekvenser (Data Protection Impact Assessment - DPIA). DPIA gjennomføres av behandlingsansvarlig i samarbeid med personvernombud. Det finnes en rekke ulike maler for DPIA og det er vanlig at større virksomheter lager egne maler som er tilpasset bruken av personopplysninger.

Virksomheter benytter seg gjerne av skytjenester for lagring av data, ulike IT-løsninger og andre eksterne leverandører. Ved slik behandling av personopplysninger skal behandlingsansvarlig

[6] Lov om behandling av personopplysninger (personopplysningsloven) - Lovdata

[7] Tidligere betegnet sensitive opplysninger.

inngå egne databehandleravtaler med databehandleren (personvernforordningen artikkel 28-29). Avtalen inneholder instrukser for databehandleren for følge GDPR og andre relevante lovverk.

Kommuneloven § 25-1 stiller krav til at fylkeskommuner skal ha internkontroll med administrasjonens virksomhet for å sikre at lover og forskrifter følges. For å ivareta alle elementer i informasjonssikkerhetsarbeidet skal det etter personvernforordningen artikkel 24, artikkel 32 og eForvaltningsforskriften § 15 gjennomføres internkontroll. Forskriften stiller krav om at:

- Forvaltningsorganet skal ha utarbeidet sikkerhetsmål og sikkerhetsstrategi.
- Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i lov, forskrift eller instruks.
- Forvaltningsorganet skal ha en internkontroll på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet.
- Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem.
- Omfanget og innretningen på internkontrollen skal være tilpasset risiko.
- Behandlingsansvarlig skal sørge for tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med personvernforordningen.
- Forvaltningsorganet skal ha prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.

Et av de grunnleggende aspektene for styring og kontroll beskrevet i «Veileder i helhetlig styring og kontroll av informasjonssikkerhet» er at ledelsen bør gjennomføre en ledelsesgjennomgang. Fylkeskommunen har lagt opp til at sikkerhetsstyret skal ha en årlig gjennomgang av informasjonssikkerheten[8]. Hva gjennomgangen skal bestå av er nærmere beskrevet i håndboken.

[8] Informasjonssikkerhetshåndbok

Revisjonskriterier	Operasjonalisering
Fylkeskommunen skal ha oppdaterte styrende dokumenter for informasjonssikkerhet.	• Fylkeskommunen skal ha beskrevet sikkerhetsmål, og strategi for informasjonssikkerhet • Sikkerhetsstyret skal en årlig gjennomgang av status for informasjonssikkerheten
Det skal være etablert rutiner for å sikre sikkerhet (konfidensialitet, integritet og tilgjengelighet) ved behandling av personopplysninger	• Fylkeskommunen skal ha rutiner og praksis for avhending av IKT-utstyr • Fylkeskommunen skal ha rutiner for tilgangsstyring • Fylkeskommunen bør ha egen databehandleravtale • Fylkeskommunen bør ha rutiner for sikker bruk av IKT-utstyr • Fylkeskommunen bør ha rutiner for behandlingsprotokoll • Fylkeskommuner bør ha rutiner for vurdering av personvernkonsekvenser • Informasjonssikkerhet og personvern bør være integrert i anskaffelsesprosessen. • Fylkeskommunen bør ha oversikt over informasjonssystemer • Fylkeskommunen skal informere registrerte om deres rettigheter

2.2 INTERNKONTROLL

I forvaltningsrevisjonsrapporten «Overordnet internkontroll» fra 2017, konkluderte Rogaland Revisjon IKS at fylkeskommunen manglet helhet rundt internkontroll. På bakgrunn av dette har fylkeskommunen opprettet en egen stilling som internkontrollrådgiver som har jobbet som systembygger. Som del i dette har en koordineringsgruppe med representanter fra alle avdelinger i sentraladministrasjonen utarbeidet et nytt rammeverk for internkontroll (sist versjon er datert 02.11.20). Rammeverket ble godkjent av fylkestinget desember 2020. Dokumentet gir en overordnet beskrivelse av fylkeskommunens internkontrollsystem, hvilke føringer og prinsipper som gjelder for styrings- og kontrollmiljøet samt hvordan fylkeskommunen skal innrettes for å oppnå en enhetlig og helhetlig tilnærming til internkontroll. Internkontrollen i fylkeskommunen er forankret etter COSO-rammeverket.

Fylkeskommunen har påbegynt arbeid med å lage «Ansvar og myndighet»-reglement som skal klargjøre ansvar, roller og delegasjonsreglement. I «Årlig rapport om internkontroll og statlige tilsyn» for 2020 står det at arbeid med dette har blitt satt på vent i 2020 og vil tas opp igjen i 2021. Status for arbeidet per oktober 2021 er at prosjektet er presentert for rådmannens ledergruppe. På grunn av kompleksiteten i prosjektet forventes første versjon ferdigstilt i 2022.

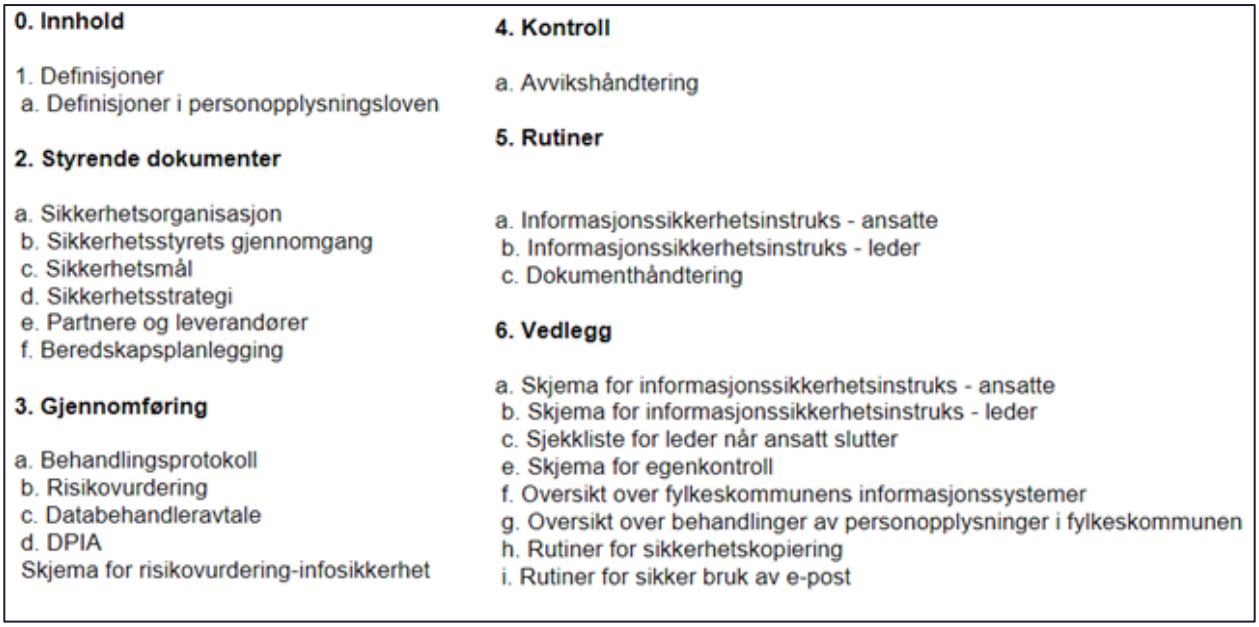
Rammeverket for internkontroll er sektorovergripende. I tillegg er det egne styringsdokumenter for ulike deler av virksomheten. For informasjonssikkerhet og personvern er det en egen informasjonssikkerhetshåndbok, slik som det er egen personalhåndbok.

2.3 STYRENDE DEL AV INFORMASJONSSIKKERHET

Fylkeskommunen har informasjonssikkerhetshåndbok som består av 16 dokumenter og ni vedlegg. Håndboken er tilgjengelig i QM+. Håndboken kan lastes ned i en fil, men denne mangler åtte av vedleggene. Dokumentene i håndboken er merket med dokumentnummer, versjon, endringsdato og navn for hvem som har endret dokumentet sist. Informasjonssikkerhetshåndboken er kun gyldig på tidspunktet for utskriften.

Informasjonshåndboken har blitt revidert i løpet av revisjonen. Revisjonen har brukt den versjonen som var tilgjengelig 03.08.21.

Figur 2. Oppbygging av informasjonssikkerhetshåndboken. Kilde: Rogaland fylkeskommune.



Mål og strategi for informasjonssikkerhet

Sikkerhetsmål og strategi (dokument 2c og 2d) ble sist revidert 27.05.21. Fylkeskommunen har følgende sikkerhetsmål:

- *Fylkeskommunen skal sikre at informasjonen behandles i henhold til relevante lover og forskrifter*[9]

[9] Relevante lover og forskrifter: • Personopplysningsloven • Personopplysningsforskriftene • Forvaltningsloven • Offentlighetsloven • Forskrift til Opplæringslova • Arkivloven • Arbeidsmiljøloven • Opplæringsloven •

- *Sikkerheten skal styres gjennom fylkesrådmannens ledergruppe, rektorer og linjeledelse i sentraladministrasjonen*
- *Den fysiske sikkerheten i fylkeskommunen skal hindre at uautoriserte får adgang til lokaler der beskyttelsesverdig informasjon og sensitive personopplysninger lagres og behandles*
- *Tilgang til systemer og informasjon gis kun til medarbeidere etter behov (need to know-prinsippet)*
- *Informasjonsbehandlingen er korrekt og endres ikke uten lovlig tilgang*
- *Medarbeidere som bruker fylkeskommunens informasjonssystemer har tilstrekkelig kompetanse for å ivareta sikkerhetskravene*
- *Sikkerheten skal ivaretas som en integrert del av fylkeskommunens organisasjon*
- *Tilgang til systemer og informasjon for uvedkommende skal forhindres*

For å oppnå tilstrekkelig informasjonssikkerhet har fylkeskommunen seks hovedstrategier innen følgende områder: sikkerhetsorganisasjon, fysisk sikkerhet, personell og sikkerhet, systemteknisk sikkerhet, sikkerhet knyttet til tilgang og bruk av fylkeskommunens systemer og avvikshåndtering. Gjeldende strategi fra 2021 er tilnærmet lik som forrige versjon fra 2017, men i den nye strategier er det lagt til punkt for den nye anskaffelsesrutinen for digitale løsninger. Henvisning til arkivlov for fysisk sikkerhet er ikke oppdatert og viser til utgått lovverk.

Ledelsens gjennomgang av informasjonssikkerhet

Ledelsen skal årlig gjennomgå sikkerhetsmål og strategi og organisering av informasjonssikkerheten. I fylkeskommunen er det et sikkhetsstyre som er ansvarlig for denne gjennomgangen. Instruks for sikkerhetsstyret er beskrevet i dokument 2b i informasjonssikkerhetshåndboken:

Formål:
Sikkerhetsstyret skal vurdere status for informasjonssikkerheten i fylkeskommunen. Dette betyr at styret skal:

- *gjennomgå sikkerhetsmål og strategier; gjennomgangen skal danne grunnlag for revisjon*
- *gjennomgå sikkerhetsorganisasjonen*
- *gjennomgå de alvorligste hendelsene og avvikene som har vært gjennom året*
- *vurdere resultatene fra egenkontroller og kontroller utført av offentlige myndigheter*
- *vurdere om det foreligger endringer som kan ha betydning for informasjonssikkerheten i RFK for eksempel*
    - *endring i off. sikkerhetskrav*
    - *endringer i krav til personopplysninger*
    - *endringer i trusselbildet i forhold til tidligere risikoanalyser*
    - *om informasjonssystemene (IT-systemer) bør endres*

Ansvar:
Fylkesrådmannen har ansvar for gjennomgangen, som foretas hvert år i løpet av første kvartal.

Tjenestemannsloven • Norm for Informasjonssikkerhet, Helse-, omsorgs- og sosialsektoren • eForvaltningsforskriften

Deltakere:

- *fylkesrådmannens ledergruppe*
- *Sikkerhetsansvarlig*
- *IKT- og arkivsjef*
- *ansvarlig for systematisk HMS-arbeid*
- *andre personer som fylkesrådmannen ønsker skal delta*

Gjennomføring
Sikkerhetsansvarlig skal

- *tilrettelegge og forberede gjennomgangen*
- *skrive referat fra gjennomgangen og sende dette til deltakerne*
- *påse at vedtatte tiltak blir gjennomført*

Digital utviklingssjef har vært ansatt siden 2018 og opplyser i intervju at det i 2019 ble foretatt muntlig presentasjon av sikkerhetsmål og strategi for sikkerhetsstyret. I 2020 var sikkerhetsgjennomgangen en rapport som ble sendt til sikkerhetsstyret. I rapporten fremkommer det at blant annet at *«Sikkerhetsorganisasjonen er pr dato i henhold til krav fra datatilsynet og RFKs informasjonssikkerhetshåndbok. Det ligger likevel betydelig potensiale i å formalisere og implementere rutiner og roller knyttet til arbeidet med informasjonssikkerhet og internkontroll i Rogaland fylkeskommune. Opplæring av ansatte i korrekt bruk av digitale verktøy bør også stå høyt på agendaen.»*

2.4 GJENNOMFØRENDE DEL AV INFORMASJONSIKKERHET

Oversikt over Dokumenter i rammeverk for informasjonssikkerhet og personvern finnes som vedlegg til rapporten. Rammeverket er delt inn i fire dokumentmapper: informasjonssikkerhetshåndbok, anskaffelser, avvikt og rutiner og lagring og klassifisering av dokumenter.

Oversikten viser at fylkeskommunen ikke gjennomførte en revisjon av informasjonssikkerhetshåndboken etter at den nye personvernloven fra 2018 tredde i kraft. En rekke dokumenter som var fra 2017 ble først oppdatert i mai – juli 2021. Per 03.08.21 er det fortsatt flere dokumenter av eldre dato, f.eks. informasjonssikkerhetsinstruks for ledere (26.05.15). Andre dokumenter viser til utgått arkivsystem «ESA». En informant opplyser i intervju at det fra 2013-2015 var en egen gruppe som oppdaterte og laget rutiner. Denne gruppen ble i etterkant avviklet.

Informasjonssikkerhetsinstruksen for ansatte ble i 2021 revidert og alle medarbeidere i fylkeskommunen må signere denne elektronisk ved å bruke MinID (BankID, Buypass). Alle ledere med personalansvar ble i april 2021 bedt om å sende den nye instruksen til sine ansatte i løpet av april 2021. Signert instruks skal arkiveres i arkivsystemet.

Flere informanter peker på at fylkeskommunen ikke har hatt tilstrekkelig med rutiner og instrukser for informasjonssikkerhet og personvern. Den siste tiden har det blitt gjort et løft og

flere rutiner har i løpet av 2021 blitt laget. Den nye lagringsveilederen trekkes av flere informanter som en av rutinene som har manglet, men som nå er på plass. I arbeidet med nye rutiner har personvernombudet selv skrevet utkast, noe som er utenfor mandatet som uavhengig personvernombud. Fra intervjuer blir det også påpekt at selv om fylkeskommunen har manglet rutiner betyr ikke dette nødvendigvis at ansatte har gjort behandlinger feil. Flere sier også at det er behov for videre jobbing med rutiner og implementering av disse. I intervju forteller en informant at fylkeskommunen planlegger å ha halvårlig revisjonsintervall på rutiner på intranettet, samtidig som det kan bli gjort flere små endringer i løpet av høsten.

I tillegg til informasjonssikkerhetshåndboken finnes det også rutiner og reglementer i eget «IKT»-område i avvikssystemet QM+. Totalt er det 15 dokumenter med rutiner for ansatte og prosedyrer for IKT- og arkivavdelingen. Rutinene for de ansatte er av eldre dato (2012-2014).

2.5 TJENESTEKATALOG

Fylkeskommunen har digitale basistjenester som brukes i hele virksomheten. Slike tjenester er det avdeling for digital utvikling som er ansvarlig for. De ulike enhetene kan også anskaffe digitale løsninger/fagsystemer til spesifikke formål.

Vedlegg 5f i informasjonssikkerhetshåndboken viser oversikt over fylkeskommunens informasjonssystemer. Oversikten ble sist oppdatert 4. april 2017 og beskriver 23 informasjonssystemer med informasjon om blant annet systemeier/avdeling, bruk av personopplysninger og bruk av sensitiv informasjon. Systemer som ble innført etter 2017 er ikke inkludert i oversikten, som f.eks. Visma inSchool og Elements (nytt arkivsystem).

Vedlegg 5g viser «Oversikt over behandlinger av personopplysninger i fylkeskommunen». Dokumentet viser oversikt over behandlinger av personopplysninger med beskrivelse av bl.a. behandlingsgrunnlag, sensitive opplysninger, omfang, system og avdeling. I dokumentet står det at «oversikten bør gjennomgås ca. hvert 3. år», men sist oppdatering var 1. februar 2013.

I QM+ finnes det et dokument «IKT-Tjenestekatalog», opprettet i 2014. Dokumentet har versjonslogg med årlige frister for revisjon av katalogen, men det har ikke blitt gjort revisjoner etter 2017. IKT-tjenestekatalogen inneholder en mer detaljert oversikt over informasjonssystemer enn i informasjonssikkerhetshåndboken.

Avdelingssjef for digital utvikling opplyser på e-post 03.06.2021 at det jobbes med å oppdatere tjenestekatalogen som legges ut på intranettet til høsten. På intranettet vil da de ulike systemeierne selv få ansvar for å oppdatere kontaktpersoner og systemer i katalogen. I 2020 overtok fylkeskommunen oppgaver fra Statens Vegvesen. Informasjonssystemer som benyttes i

samferdselsavdelingen i fylkeskommunen er fremdeles driftet av Statens Vegvesen. Det er et pågående arbeid med å overføre driften av systemene til fylkeskommunene via Vigo IKS[10].

2.6 RUTINER FOR ANSKAFFELSER

Innkjøpsavdelingen har ansvar for alle anskaffelser i fylkeskommunen og har egne rutiner for rammeavtaler og enkeltanskaffelser. I anskaffelsesprosesser settes det ned egne team med representanter fra innkjøpsavdelingen og involverte faggrupper. Det er nylig laget rutine for anskaffelser av digitale løsninger som behandler personopplysninger (17.03.2021). Rutinen inneholder begrepsavklaringer og en sjekkliste med krav om blant annet gjennomføring av behandlingsprotokoll, risikovurdering, databehandleravtale og vurdering av personvernkonsenser. Rutinen *«[…] er et supplement til Rogaland fylkeskommune sine anskaffelsesrutiner. Vanlige regler for anbud og digitale anskaffelsesprosesser gjelder i tillegg.»*

I intervju forklarer informant at de fleste systemer som anskaffes behandler personopplysninger. I stor grad gjelder dette navn og kontaktinformasjonen for den enkelte ansatt for å kunne benytte seg av systemer. Det har ikke i særlig grad blitt anskaffet systemer som behandler sensitiv informasjon. Ifølge rutinen for anskaffelser av digitale løsninger som behandler personopplysninger, er det behandlingsansvarlig som har ansvar for å utforme behandlingsprotokoll, risikovurdering, databehandleravtale og vurdere DPIA. Det er den enkelte fagavdeling som har behandlingsansvar for systemer. Innkjøpsavdelingen har ikke rutine for å sjekke at behandlingsansvarlig har utført lovpålagte krav i anskaffelsesprosesser.

De ansatte skal forholde seg til regler i informasjonssikkerhetsinstruksen. Instruksen ble revidert våren 2021 med nye punkter for bruk av andre digitale løsninger: Bruk av andre skytjenester som Dropbox og Google Drive til jobbformål er ikke tillatt. Instruksen sier også at det ikke er tillatt å endre oppsett på utstyr eller installere egenutviklede programmer. Det er heller ikke tillatt å bruke ulisensiert eller ulovlig anskaffet programvare. Instruksen krever at ansatte er bevisst på svindel og misbruk av informasjon, og er kritisk til bruk av apper. Teknisk sett er det mulig for de ansatte å laste ned programvare og apper selv. Informant fra IKT-avdelingen sier det ikke er rutine fra deres side på å ta vekk systemer/programmer som ikke brukes. Men når en ansatt slutter, blir også systemer/programmer slettet.

Ifølge flere av intervjuobjektene har det vært vanlig å ta bruk digitale løsninger uten å sjekke med rutiner og relevante lovkrav. Dette gjelder gjerne skoler som tar i bruk nye løsninger uten å sjekke sentralt om fylkeskommunen har lignende programmer, eller ansatte som laster ned programmer uten å involvere leder. Men flere som revisjonen har snakket med har sett en økende

[10] Vigo er eid av Vigo IKS som er et interkommunalt selskap, og er et samarbeid mellom alle fylkene i Norge i tillegg til Oslo kommune.

bevissthet rundt digitale løsninger etter store dataangrep i offentlig sektor. Det har også vært økende bevissthet på at jobb-PC ikke skal brukes til privat bruk.

Fylkeskommunen fikk 01.05.2021 ny rutine for databehandleravtaler. Rutinen viser at det som hovedregel skal brukes Digitaliseringsdirektoratets mal for databehandleravtale. Hvis leverandøren ønsker å bruke standardavtaler skal denne sendes til Fylkesadvokaten for gjennomgang.

2.7 TILGANGSSTYRING OG AVHENDING AV IKT-UTSTYR

Fylkeskommunen har ifølge «IKT Tjenestekatalog» sikkerhetsarkitektur med adskilte nettverkssoner: sikret sone, interne soner og ekstern sone. IKT-tjenestene er plassert i de ulike sonene etter hvilke typer opplysninger som behandles. Sensitive opplysninger skal kun behandles på sikret sone, som for eksempel elektronisk pasientjournal i tannhelsetjenesten. Tilgangsstyring er rollebasert etter hva en jobber med. Lærere får for eksempel ikke tilgang til sikret sone. Tildeling av adganger til fellestjenester går gjennom IKT-avdelingen. Tilganger til fagspesifikke systemer gjøres av enhetene selv.

Ifølge sikkerhetsstrategien er det nærmeste linjeleder som er ansvarlig for å melde til avdeling for digital utvikling når en medarbeider slutter. Dette er også beskrevet i vedlegg til informasjonssikkerhetshåndboken i QM+ «Sjekkliste ansatt slutter» med sjekkpunktene:

- E-post og filer er gjennomgått med nærmeste leder og overlevert
- Saksbehandling i Elements avsluttes/overføres til leder
- Graderte/sensitive dokumenter er arkivert, eventuelt makulert
- Kontoret er ryddet og tømt
- Utstyr som tilhører fylkeskommunen er levert
- Adgangskort og nøkler er levert og kvittert ut
- IKT-sluttskjema er fylt ut
- Eventuelle privat e-post og private filer er slettet.

IKT-sluttskjemaet er et digitalt skjema på «Brukerhjelp»-portalen. I skjemaet skal leder blant annet registrere den ansattes PC-nummer. Sluttskjemaet deaktiverer brukeren fra fellessystemer som lønn, e-post og Office 365. Eksterne kan få midlertidige tilganger. Slike tilganger stenges automatisk etter ett år hvis de ikke skal videreføres. Andre tjenester som den ansatte har tilgang til må avsluttes manuelt, noe som nærmeste leder skal ha oversikt over. Dette gjelder for eksempel arkivsystemet, Visma inSchool, SatsSkole og Itslearning. Nyansatte får tilgang til systemer gjennom digitalt skjema på «Brukerhjelp»-portalen og eventuelt manuell opprettelse av tilganger til systemer som ikke styres av IKT-avdelingen.

Arkivsystemet Elements har eget skjema for tilgangsstyring som brukes både til opprettelse av avslutning av tilganger. Ved nyansettelser er det leder som bestemmer hvilke arkivdeler og tilgangskoder den nyansatte skal ha. I utgangspunktet får alle tilgang til sin egen seksjon. Hvis leder ikke sender sluttmelding for Elements til dokumentsenteret, vil det gjennom lønnssystemet

komme opp melding i arkivsystemet. En informant opplever at lederne er for dårlige til å sende inn sluttmeldinger. Det blir glemt eller så tenker en det er tilstrekkelig å melde avslutningen til lønnssystemet. Sjekklisten for ledere i QM+ er oppleves av informanter som vanskelig å finne og at den ikke tydelig nok beskriver hva leder skal gjøre.

Fylkeskommunen har hatt episoder med manglende tilgangsstyring for Visma InSchool ved at ansattes tilgang til Visma InSchool ikke har blitt avsluttet etter endt arbeidsforhold. Dette har blitt oppdaget når den ansatte startet et nytt arbeidsforhold på annen skole i fylket.

Når en ansatt slutter, skal IKT-utstyr leveres eller meldes inn til IKT-avdelingen. Rutiner for dette finnes i digitalt sluttskjema som brukes av sentraladministrasjonen. Skolene har eget «Reglement for registrering og avhending av inventar og utstyr». Begge rutiner sier at innhold på PC skal slettes og gjøres klar til nye brukere. Denne operasjonen kalles «retanking» og gjennomføres enten av IKT i sentraladministrasjonen eller skolenes egne IKT-teknikere.

Hvis IKT utstyr ikke kan gjenbrukes skal de kasseres forsvarlig. Fylkeskommunen har rammeavtale med ATEA for IKT-utstyr som også gjelder skolene. IKT-fagleder forklarer at avtalen også gjelder for kassering av ødelagte PC'er. Praksis for slik kassering er at IKT-tekniker sletter harddisk og plasserer den i låsbart skap som hentes av ATEA for diskknusing.

2.8 PERSONVERNERKLÆRINGER

Fylkeskommunen har personvernerklæring på nettsiden. Det er også egen personvernerklæring for skolene som er tilgjengelig fra skolenes egne nettsider. Begge personvernerklæringer ble opprettet 31.10.2019 og sist endret i 2020. Personvernerklæringer inneholder informasjon om:

- Den registreres rettigheter til blant annet innsyn og retting. Samt e-postadresse hvis den registrerte ønsker å utøve sine rettigheter.
- Hvor fylkeskommunen får opplysningene fra
- Hvem opplysningene deles med
- Hvilke opplysninger som behandles
- Hvor lenge opplysningene lagres
- Hvem som er behandlingsansvarlig
- Informasjon om hvordan en kan klage til Datatilsynet
- Kontaktinformasjon til personvernombudet

Det finnes ikke egen personvernerklæring for de ansatte i fylkeskommunen, men personal og organisasjonsavdelingen har laget et forslag til personvernerklæring. Avdeling for digital utvikling har gitt sin tilslutning til forslaget. Personvernerklæringen skal godkjennes av fylkeshovedstillitsvalgt.

2.9 VURDERING

Våre vurderinger er gjort på grunnlag av revisjonskriteriene og faktagrunnlaget som revisjonen bygger på. Overordnet har fylkeskommunen et tilfredsstillende system med styrende dokumenter i informasjonssikkerhetshåndboken med beskrevet sikkerhetsmål og strategi. Status for informasjonssikkerhetsarbeidet gjennomgås årlig i sikkerhetsstyret. Informasjonssikkerhetshåndboken består av en gjennomførende del med ulike dokumenter, rutiner, sjekklister og veiledere. Rutiner og retningslinjer har inntil 2021 i liten grad blitt oppdatert og det har manglet rutiner på for eksempel hvor informasjon skal lagres. IKT-tjenestekatalogen er fra 2017 og er ikke tilstrekkelig oppdatert med de digitale løsningene fylkeskommunen bruker i dag. Fylkeskommunen har sommeren 2021 publisert en rekke nye og oppdaterte rutiner.

Fylkeskommune har personvernerklæringer på nettsiden som informerer om hvordan de registrerte kan utøve sine rettigheter. Personvernerklæringene gjelder for de videregående elevene og mottakere av tjenestene i fylkeskommunen. Fylkeskommunen mangler personvernerklæring for de ansatte, noe som per oktober 2021 er under utarbeidelse.

Tilganger til fellessystemer styres sentralt og blir automatisk tatt bort ved avslutning av arbeidsforhold. Ved avslutning av tilganger på arkivsystem og de ulike fagsystemene kreves det at leder aktivt melder dette inn. Manuell tilgangsstyring øker risiko for at uautoriserte får tilgang og flere informanter forteller om episoder hvor dette har skjedd. Fylkeskommunen har rammeavtale med leverandør for sikker avhending og kassering av IKT-utstyr som også gjelder for skolene.

Revisjonen kommer med følgende anbefalinger til fylkeskommunen:

- Fylkeskommunen bør oppdatere IKT-tjenestekatalogen

3 OPPGAVER OG ANSVAR

Problemstilling: «I hvilken grad er oppgaver og ansvar relatert til informasjonssikkerhet og personvern tydeliggjort? Hvilket politisk utvalg følger opp informasjonssikkerhet i fylkeskommunen og hvor mange saker har de hatt til behandling?»

3.1 REVISJONSKRITERIER

Fylkeskommunen skal etter personvernforordningen artikkel 24 gjøre organisatoriske tiltak for å ivareta krav rundt personvern. Ifølge Datatilsynets veileder for etablering av internkontroll må roller og ansvar knyttet til personvern og sikkerhet internt i virksomheten avklares. Det inkluderer for eksempel hva som ligger i linjeansvar og hva som ligger i nøkkelroller som personvernombud, sikkerhetsleder, IKT-ansvarlig, HR-ansvarlig og systemeiere og lignende. Dette fremkommer også av «Veileder i helhetlig styring og kontroll av informasjonssikkerhet» at det er viktig at roller og ansvar er klart beskrevet og formidlet til dem det gjelder.

Fylkeskommunen er pliktig til å utnevne et personvernombud etter personvernforordningen artikkel 37. Artikkel 37-38 beskriver personvernombudets roller og ansvar.

Revisjonskriterier
• Oppgaver og ansvar for informasjonssikkerhet og personvern skal være tydelig beskrevet i styringsdokumenter

3.2 ADMINISTRASJONSUTVALGET

Ifølge «Ansvar og myndighet i Rogaland fylkeskommune[11]» har administrasjonsutvalget blant annet ansvar for å vedta retningslinjer for registrering av personopplysninger og planer og retningslinjer for bruk av informasjonsteknologi.

Utvalget har i perioden 2016 – juni 2021 behandlet 4 saker:

- «Digitaliseringsstrategi 2016 – 2019» 08.06.16
- «Ny personvernforordning – GDPR i Rogaland fylkeskommune» 02.05.18
- «Digital strategi for Rogaland fylkeskommune 2020 – 2024» 19.02.2020
- «Årlig rapport om internkontroll og statlige tilsyn» 02.12.2020
- «Revisjon av arbeidsreglement» 02.06.2021

[11] Vedtatt av fylkestinget 15.10.19 sak 0092/19

Digital utviklingsavdeling gjennomfører annet hvert år en brukerundersøkelse IKT for å undersøke ansattes tilfredshet med avdelingen. Resultatene fra undersøkelsen er behandlet i administrasjonsutvalget. Undersøkelsen viser blant annet at ansatte i mindre grad benytter de informasjonskanalene som er tilgjengelige for å tilegne seg informasjon knyttet til IKT-tjenester. Men sammenlignet med forrige undersøkelse (2017) er det derimot en positiv utvikling på dette punktet.

Informasjonshåndboken og andre retningslinjer er ikke lagt frem for administrasjonsutvalget. Avdelingsleder for digital utvikling forteller i intervju at ettersom den nye informasjonssikkerhetsinstruksen var en revidering av eksisterende instruks, ble den ikke lagt fram for utvalget.

3.3 ADMINISTRATIV ORGANISERING

Informasjonssikkerhetshåndboken inneholder dokumentet «Sikkerhetsorganisasjon» hvor ulike sikkerhetsroller er beskrevet.

Tabell 1 Sikkerhetsorganisasjon i Rogaland fylkeskommune

Sikkerhetsrolle	Stilling	Navn	Oppgaver
Sikkerhetsstyre	se Sikkerhetsstrategier, pkt1		se Sikkerhetsstyrets gjennomgang
Behandlingsansvarlig	fylkesrådmann	Inge Dokken	overordnet ansvar
Daglig behandlings-ansvarlig	linjeledere i sentraladministrasjonen, rektorer		daglig ansvar
Sikkerhetsansvarlig	Avdelingssjef, digital utvikling	Svein Vathne	se Sikkerhetsstrategier, pkt. 1
Driftsansvarlig			se Sikkerhetsstrategier, pkt. 1
Personell og sikkerhet	personal- og organisasjonssjef og rektorer		se Sikkerhetsstrategi, pkt. 3
Fysisk sikkerhet	bygg og eiendoms-sjefen og rektorer		se Sikkerhetsstrategi, pkt. 2
Personvernombud	Personvernombud	Aleksandra Endresen	se Sikkerhetsstrategier, pkt. 1

Fylkeskommunen har foretatt en oppdatering av dokumentet «sikkerhetsstrategi» som blant annet inneholder en beskrivelse av de oppgavene som fylkesrådmannen, sikkerhetsansvarlig, avdelingssjef digital utvikling og personvernombudet har innen informasjonssikkerhet. En sammenligning av siste revisjon av dokumentet, datert 15.07.21, med den tidligere versjonen, datert 04.04.17, viser at innholdet i oppgavene til de nevnte stillingene ikke er endret.

Av sikkerhetsstrategien fremgår det at fylkesrådmannen er behandlingsansvarlig og har det overordnede ansvaret for informasjonssikkerheten. Det daglige behandlingsansvaret er delegert til linjeledelsen i sentraladministrasjonen, foretaksledere og rektorer. Informasjonssikkerhetshåndboken inneholder likevel ikke en beskrivelse av oppgavene til de behandlingsansvarlige. Det foreligger en informasjonssikkerhetsinstruks for ledere med personalansvar, sist oppdatert 09.03.15. Instruksen inneholder i hovedsak en beskrivelse av at

leder skal sikre at ansatte leser og signerer på informasjonssikkerhetsinstruksen og hvordan brukertilganger skal meldes. Utover dette er noen av oppgavene til ledelsen beskrevet i enkelte rutiner, som for eksempel i «Retningslinje brudd på personopplysningssikkerheten».

Det fremgår av sikkerhetsstrategien at sikkerhetsansvarlig har det utøvende ansvaret for informasjonssikkerheten, og at ansvaret blant annet innebærer avvikshåndtering av informasjonssikkerheten. I «Retningslinje brudd på personopplysningssikkerheten» fremgår det at det er linjeleder som har hovedansvar for at avviket blir håndtert.

Ansvaret som påligger den enkelte ansatte fremgår av «informasjonssikkerhetsinstruks ansatte». Instruksen ble sist endret 21.04.21 og er sendt ut i organisasjonen for signering. Arbeidsreglementet for ansatte i Rogaland fylkeskommune ble revidert av administrasjonsutvalget den 02.06.21, med blant annet eget punkt om informasjonssikkerhet og personvern (§20):

> *«Arbeidstaker skal aktivt bidra til informasjonssikkerhet. Den enkelte må derfor ha et bevisst forhold til hvilken informasjon vedkommende selv behandler, samt vite hvilke krav som stilles til tilgang, innsyn, oppslag, formidling, endring og sletting av informasjon. Det er en forutsetning for å få og beholde tilgang til fylkeskommunens nettverk at arbeidstakeren er kjent med, og overholder, rutiner for bruk av fylkeskommunens elektroniske kommunikasjonsutstyr, som omtalt i Sikkerhetsinstruksen. Arbeidstaker må straks melde fra ved mistanke om sikkerhetsbrudd. Leder har ansvar for at nytilsatte blir orientert om gjeldende regelverk, og for å videreformidle endringer og revisjoner i regelverk til alle ansatte.»*

På de fire skolene revisjonen har besøkt har formidling av nytt arbeidsreglement vært via intranettet, enten i form av nyhetssak som ble lagt ut på felles intranett for hele fylkeskommunen, eller som egen sak på skolens intranettområde. Lærerne som ble intervjuet var i liten grad kjent med endring i reglementet. Noen synes å huske det var en intranettsak, men mange hadde ikke fått dette med seg.

I noen intervjuer fremkommer det at fylkeskommunen i større grad bør tydeliggjøre og bevisstgjøre ledere hva som er deres oppgaver innen området, og at dette i særlig gjelder i forhold til hva det innebærer å ha det daglige behandlingsansvaret. De fleste av lærerne revisjonen intervjuet bruker programmer/apper i undervisningen, men ingen av de fire skolene som ble besøkt hadde oversikt over digitale løsninger som skolen selv er behandlingsansvarlig for. Lærerne vi intervjuet bruker blant annet Kahoot, Mentimeter, Strava, Runkeeper, Teach Out, Geogebra, Python og Dropbox. Det generelle inntrykket fra skolene er at lærerne tar i bruk apper uten å involvere ledelsen, men økt fokus på personvern de siste årene har ført til høyere terskel for å ta i bruk slike digitale løsninger. Revisjonen har ikke vurdert hvorvidt disse digitale løsningene behandler personopplysninger og som da etter personvernforordningen krever tiltak for å vurdere sikker bruk. Men ingen av ledelsene på de fire skolene har laget behandlingsprotokoll eller gjennomført risikovurderinger for digitale løsninger.

I «årsrapport for informasjonssikkerhet 2019» fremgår det at innføringen av GDPR påvirker sikkerhetsstrategien og fører til at systemeierskap, behandlingsansvar og ansvar for risikovurdering blir delegert i linja til den avdeling/skole/seksjon som har spesifikt eierskap til ulike systemer. Videre fremgår det at det må utnevnes ansvarlige roller som skal etterleve lovpålagte krav og standarder.

I modenhetsrapporten[12] utført av TietoEVRY fremgår det at fylkeskommunen har uklare og manglende roller for håndtering av informasjonssikkerhet og personvern, at rollene ikke er tydelig delegert og at roller og ansvar må forankres og tydeliggjøres.

En informant forteller i intervju at en ny tjenestekatalog vil tydeliggjøre roller og ansvar. Avdeling for digital utvikling jobber for at katalogen skal være et levende dokument på intranettet hvor hver enkelt systemeier har ansvar og mulighet for å legge inn informasjon. Det er også fra digital utviklingsavdeling løftet fram et ønske om å ha en ny rolle på hver avdeling med særskilt ansvar for personvern. Ansatte med denne rollen skal i så fall inngå i et faglig nettverk ledet av avdeling for digital utvikling. De som blir med i nettverket vil få opplæring og vil følge opp personvernarbeidet på hver enkelt avdeling, som for eksempel oppdatering av tjenestekatalog og bruk av rutiner.

3.4 PERSOVERNOMBUDETS ROLLE

Stillingen som personvernombud i fylkeskommunen ble opprettet i 2018. Personvernombudet oppgir at hun tidligere var organisatorisk plassert under IT-avdelingen, men at hun fra og med 2020 er plassert direkte under fylkesrådmannen. Personvernombudet legger fram årlig rapport til sikkerhetsstyret. Sist årsrapport var i 2019 og årsrapport for 2020 forventes levert høsten 2021.

Personvernombudets arbeidsoppgaver er beskrevet i informasjonssikkerhetshåndboken:

> *«Et personvernombud er en ressursperson som styrker virksomhetens kunnskap og kompetanse om personvern. Arbeidsoppgaver er å*
>
> - *sørge for at behandlinger av personopplysninger blir meldt til ombudet og at meldingene inneholder korrekte opplysninger*
> - *føre en systematisk og offentlig tilgjengelig fortegnelse over behandlingene*
> - *bistå de registrerte med å ivareta deres rettigheter*
> - *påpeke brudd på personopplysningsloven overfor behandlingsansvarlig*
> - *gi Datatilsynet opplysninger dersom tilsynet ber om det*
> - *holde seg orientert om utviklingen innenfor personvern*
> - *gi råd og veiledning til behandlingsansvarlig om behandling av personopplysninger»*

[12] Datert 13.03.20.

I modenhetsrapporten fremkommer det at personvernombudet mangler mandat/stillingsbeskrivelse for rollen sin og at rollen mangler forankring hos toppledelsen og er ikke internalisert i virksomheten som helhet. Som nevnt er det etter siste revisjon av informasjonssikkerhetshåndboken ikke foretatt endringer i personvernombudet sin oppgave, og det fremgår ikke av informasjonssikkerhetshåndboken at personvernombudet skal ha en uavhengig rolle.

Det finnes en egen retningslinje for personvernombud som rådmannens ledergruppe gikk gjennom 03.12.18. Retningslinjen viser blant annet til krav om uavhengighet for personvernombudet. Personvernombudet opplyser at hennes stillingsbeskrivelse skal oppdateres. Personvernombudet sendte forslag til ny stillingsbeskrivelse til fylkesrådmann og assisterende fylkesrådmann i juni 2021 som skal godkjenne denne. Per 08.09.2021 hadde personvernombudet ikke fått svar på denne henvendelsen.

I noen av intervjuene får vi oppgitt at personvernombudet har hatt oppgaver utenfor hennes mandat i mangel på andre ressurser. Det vil si hun har arbeidet med å skrive rutiner og slik sett jobbet som systembygger og ikke ombud. I intervju uttrykkes det en uklarhet rundt hvem som skal godkjenne og formalisere rutiner.

Flere av de revisjonen har intervjuet oppgir at det er manglende ressurser i arbeidet med informasjonssikkerhet og personvern. Det siktes til at andre fylkeskommuner gjerne har egen informasjonssikkerhetskoordinator eller informasjonssikkerhetsrådgiver. Revisjonen har fått opplyst at fylkeskommunen skal lyse ut ny stilling i arbeidet med informasjonssikkerhet hvis det blir satt av midler til denne i budsjettet. En eventuell ny informasjonssikkerhetskoordinator/rådgiver vil i så fall være på plass i 2022.

3.5 RESSURSGRUPPEN FOR INFORMASJONSSIKKERHET

Fylkeskommunen har en ressursgruppe for informasjonssikkerhet som består av ansatte fra ulike avdelinger innen opplæring, personal, tannhelse og bygg. Gruppen ble opprettet for omtrent ti år siden da fylkeskommunen ikke hadde eget personvernombud. Utarbeidelse av informasjonssikkerhetshåndboken er en av oppgavene gruppen har hatt. Gruppen har ikke hatt møter siden 2018 og blir ikke oppfattet som operativ lenger, men har senest i 2021 blitt rådspurt per e-post i forbindelse med innspill til retningslinjer, veiledere og årsrapport.

3.6 DIGITALISERINGSUTVALGET

Digitaliseringsutvalget er et administrativt utvalg opprettet våren 2020 og settes i sammen av fylkesrådmannen. Utvalget har 12 medlemmer fra ulike fagavdelinger, skoler, organisasjonene, stab og støtteavdelinger. Oppgavene for utvalget er å *«gi råd og prioritere forslag til digitaliseringsprosjekter»*. Sammen med ansattrepresentanter og tillitsvalgte skal utvalget lage årlige handlingsplaner på bakgrunn av digital strategi. Digitaliseringsutvalget møtes en gang i måneden og rapporterer jevnlig til fylkesrådmannens ledergruppe.

Utvalget har i 2021 utvidet mandatet, blant annet med å *«Bidra til at digitalisering i fylkeskommunen skjer etter gode rutiner og retningslinjer»*. Digitaliseringsrådgiver opplyser på e-post 07.09.2021 at handlingsplan for digitalisering skal være ferdig i løpet av høsten.

3.7 KOORDINERINGSGRUPPEN FOR INTERNKONTROLL

I 2020 ble koordineringsgruppen etablert på oppdrag fra fylkesrådmannen. Gruppen består av deltakere fra alle avdelinger i sentraladministrasjonen med internkontrollrådgiver som koordineringsansvarlig. I prosjektmandatet står det at gruppen er et faglig nettverk og diskusjonsforum for internkontroll. Gruppen møtes månedlig og fungerer som kommunikasjonskanal for å samordne utviklingen av internkontroll og den skal støtte deltakerne i arbeid med internkontrollaktiviteter i egne avdelinger. Gruppen jobber med systembygging av internkontrollaktiviteter på alle områder fylkeskommunen gjør internkontroll på. informasjonssikkerhet og personvern er da et av områdene som inngår i internkontrollen. I koordineringsgruppen er det laget maler for hvordan en skriver rutine og maler for risikovurdering. Koordineringsgruppen jobber med å kommunisere hvordan internkontrollarbeidet skal gjøres, spesielt med tanke på å skape kultur for risikoforståelse ut i enhetene.

3.8 VURDERING

Ansvar relatert til informasjonssikkerhet er beskrevet i styrende dokumenter for informasjonssikkerhet. I denne står det at fylkesrådmann er øverst behandlingsansvarlig og har det overordnete ansvaret for informasjonssikkerheten. Videre står det at det daglige behandlingsansvaret er delegert til linjeledelsen i sentraladministrasjonen, foretaksledere og rektorer. Hva som ligger av ansvar for behandlingsansvarlig er beskrevet i ulike rutiner tilknyttet informasjonssikkerhetshåndboken. Beskrivelsen av ansvar og oppgaver synes derfor å være noe fragmentert og det mangler en tydelig overordnet beskrivelse av hva de ulike rollene er ansvarlig for. Det er spesielt oppgaver og ansvar knyttet til rollen som daglig behandlingsansvarlig som bør tydeliggjøres.

Etter innføringen av GDPR i 2018 har fylkeskommunen jobbet med å plassere ansvar for informasjonssikkerhet og personvern i de enkelte enhetene. Flere informanter peker på at de enkelte enhetene ikke er tilstrekkelig bevisst på ansvaret de har. Det ligger et forbedringspotensial i å forankre ansvaret for informasjonssikkerhet og personvern ut i organisasjonen. Skolene har for eksempel ikke tilstrekkelig oversikt og kontroll med digitale løsninger som skolene selv er systemeiere for.

Det er positivt at personvernombudet nå er direkte plassert under fylkesrådmannen og ikke under IT-avdelingen, noe som styrker uavhengigheten. Det er også positivt at fylkeskommunen har styrket det generelle internkontrollarbeidet, med økt fokus på risikoforståelse og faglig nettverk på tvers av avdelingene.

Administrasjonsutvalget har ansvar for å vedta retningslinjer for registrering av personopplysninger og planer og retningslinjer for bruk av informasjonsteknologi. Utvalget har de siste fem årene behandlet fem saker relatert til informasjonssikkerhetsarbeidet. Utvalget har ikke behandlet de nye rutinene for informasjonssikkerhet og personvern som har blitt implementert i år.

Revisjonen kommer med følgende anbefalinger til fylkeskommunen:

- Oppgaver og ansvar knyttet til behandlingsansvar bør gjøres tydeligere og forankres bedre i enheten.
- Fylkeskommunen bør sikre at administrasjonsutvalget får behandlet retningslinjer for registrering av personopplysninger og planer og retningslinjer for bruk av informasjonsteknologi.

4 ETTERLEVELSE AV RUTINER

Problemstilling: I hvilken grad blir fylkeskommunens systemer og rutiner innen informasjonssikkerhet og personvern etterlevd i virksomhetene?

4.1 REVISJONSKRITERIER

Kommunen skal etter personvernforordningen artikkel 24 gjøre organisatoriske tiltak for å ivareta krav rundt informasjonssikkerhet og personvern. Tiltakene skal gjennomgås jevnlig og oppdateres ved behov. Kapittel «2 Systemer og rutiner» beskriver hvilke rutiner og retningslinjer fylkeskommunen har for informasjonssikkerhet og personvern. Dette kapitlet fokuserer på hvordan rutinene blir etterlevd i organisasjonen. Ifølge fylkeskommunens rammeverk for internkontroll er etterlevelse av lovkrav og interne retningslinjer regulert til følgende roller:

- **Fylkesrådmann** skal påse at *«det eksisterer overordnede føringer og prinsipper med tilhørende definert myndighet, roller og ansvar knyttet til fylkeskommunens vesentlige og risikoutsatte områder, og at dette er dokumentert i instrukser og annet rammeverk.»*
- **Avdelingsleder** skal påse at *«avdelingens ledere og medarbeidere etterlever lover og regler, samt interne retningslinjer og rutine»*
- **Seksjonsleder** skal *«påse og følge opp etterlevelse av retningslinjer og rutiner i egen seksjon»*
- **Den enkelte ansatt** er ansvarlig for *«å opptre i tråd med krav og føringer gitt i relevante styringsdokumenter, herunder retningslinjer og rutiner, og konsultere overordnede dersom det oppstår tvil om omfang og tolkning av innholdet i relevante styringsdokumenter»*

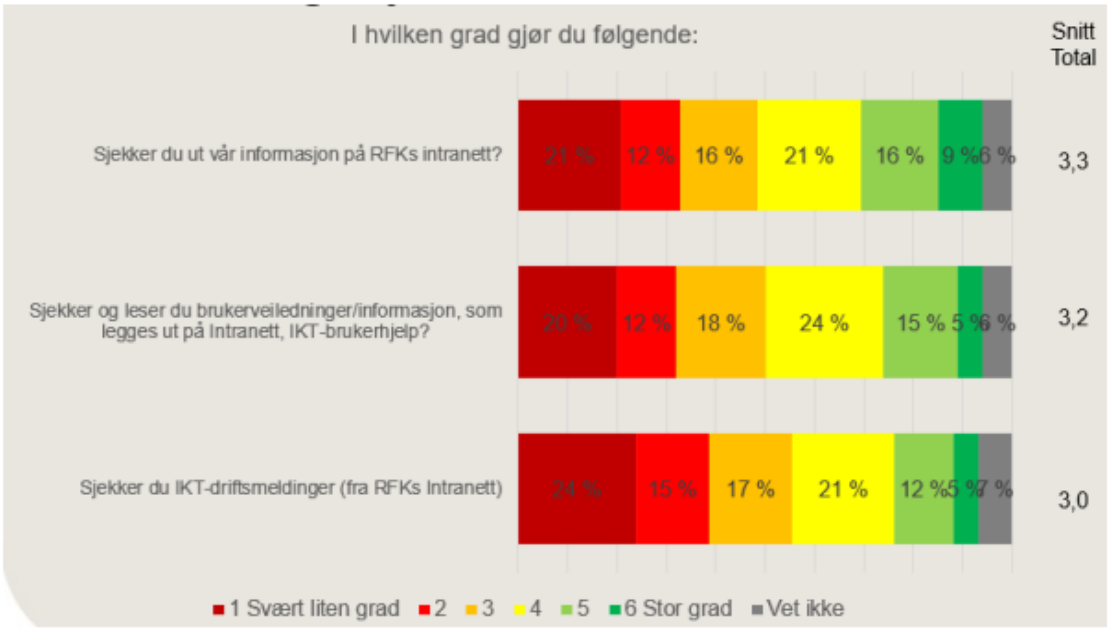
Revisjonskriteriet
• Alle ansatte skal ha signert sikkerhetsinstruksen. • Ansatte skal følge rutiner for informasjonssikkerhet og personvern. • Behandlingsansvarlige skal ha protokoll for all behandling av personopplysninger. • Det skal gjennomføres risikovurderinger og personvernkonsekvensutredninger

4.2 FORMIDLING AV IKT-REGELVERK

Flere av intervjuobjektene melder at det er vanskelig å finne rutiner for informasjonssikkerhet og personvern. Felles rutiner ligger enten på intranettet og/eller i avvikssystemet QM+. Et eksempel på lite tilgjengelig informasjon på intranettet er en del lenker til rutiner i QM+. Men for å åpne rutinene må en også logge seg på QM+, noe som gir en ekstra barriere. QM+ har ifølge flere intervjuobjekter et lite brukervennlig design og er lite egnet som system for å tilgjengeliggjøre dokumentasjon.

IKT-avdelingen utfører brukerundersøkelse ca. annethvert år. Forrige undersøkelse fra 2019 viser at 20 prosent i svært liten grad sjekker brukerveiledninger/informasjon som legges ut på intranett og IKT-brukerhjelp. I oppsummeringen av brukerundersøkelsen står det at: Det er også at «Ansatte benytter i mindre grad, de informasjonskanalene som er tilgjengelig for å tilegne seg informasjon knyttet til IKT tjenester. Det likevel en liten økning i positiv retning siden sist undersøkelse.». Ifølge intervju med ansatte i digital utviklingsavdeling har det vært en oppgang i bruk av intranettet som følge av Covid-19 og økt hjemmekontorbruk.

Figur 3. Fylkeskommunens brukerundersøkelse fra 2019[13].



4.3 BEHANDLINGSPROTOKOLLER

Fylkeskommunen har en overordnet «Oversikt over behandling av personopplysninger i Rogaland fylkeskommune». Oversikten ble sist oppdatert i 2013. Der står det at den bør gjennomgås ca. hvert tredje år, men den inneholder ikke informasjon om hvem som er ansvarlig for oppdatering.

Informasjonssikkerhetshåndboken ble i juli 2021 oppdatert med egen rutine for behandlingsprotokoll. Rutinen sier at det er den med daglig ansvar i avdelingen, seksjonen eller skole som er ansvarlig for å føre oppdatert protokoll for behandling av personopplysninger. Rutinen sier også at *«Det bør utpekes en ansatt som kan følge opp utfyllingen innenfor eget fagområde.»*. Behandlingsprotkollen skal videre oppdateres minst årlig som del av internkontroll

[13] Se sak fra administrasjonsutvalget 04.12.2019

og elles ved endringer. Personvernombudet skal ifølge rutinen varsles ved større eller vesentlig endringen. Rutinen viser til veileder og mal for utfylling av behandlingsprotokoll.

Ifølge personvernombud har daglig behandlingsansvarlige i varierende grad laget protokoller over behandlingsaktiviteter. Det mangler foreløpig et overordnet system for protokollføring, og behandlingsprotokoller som er laget blir gjerne liggende uten å bli oppdatert.

Behandlingsprotokoller i opplæringsavdelingen og skolene

Behandling av personopplysninger i systemer som alle skolene bruker eies av opplæringsavdelingen som da er behandlingsansvarlig. Dette gjelder f.eks. Visma InSchool og Vigo. Skolene har i tillegg egne systemer og fagspesifikke programmer som de da er behandlingsansvarlig for.

Opplæringsavdelingen har påbegynt arbeid med å lage behandlingsprotkoll for felles systemer. En informant sier i intervju at protokollen planlegges å gjøres ferdig når avdelingen har fått ansatt ny medarbeider med juridisk kompetanse. I intervjuet påpekes det at det er vanskelig å få oversikter over systemer som skolene selv er ansvarlige for. En årsak kan være manglende kunnskap om oppgaver knyttet til rollen som behandlingsansvarlig. Ingen av de fire skolene revisjonen har besøkt har laget egne behandlingsprotokoller.

4.4 RISIKOVURDERINGER

Det er utarbeidet en ny mal for risikovurdering utarbeidet av internkontrollrådgiver. Koordineringsgruppen for internkontroll har også vært med i dette arbeidet. Internkontrollrådgiver oppgir i intervju at en må sikre at det jobbes med å skape kultur rundt risikoforståelse og risikovurderinger. Risikovurderinger er viktig å få på plass for da finner en ut hvor ting kan gå galt.

I intervjuer får vi oppgitt at det er gjennomført risikovurderinger for enkelte programmer/systemer som for eksempel Visma inSchool (VIS), Feide og Microsoft Office 365 (inkludert Teams).

VIS er et nytt skoleadministrativt system. Det er Vigo som har stått for anskaffelsen av VIS, databehandleravtalen er underskrevet av opplæringsdirektør i fylkeskommunen.

Akershus var pilotfylke for innføring og Rogaland startet innføringen sammen med Innlandet og Viken i 2020. Det er ukentlige møter med fylkene som implementerer VIS og informasjonsdeling rundt praksis, avvik og organisering. Fylkene har også møter med Visma som leverandør. Noen moduler i VIS er ikke iverksatt enda, som arkivdelen. Hele leveransen skal være ferdigstilt i 2022.

I fylkeskommunen er det egen prosjektleder og styringsgruppe for VIS hvor ulike avdelinger i sentraladministrasjonen er med. Det er også en arbeidsgruppe med prosjektleder,

ansattrepresentant, og ansatte fra økonomiavdelingen, opplæringsavdelingen og digital utviklingsavdelingen.

Arbeidsgruppen har laget behandlingsprotokoll og gjennomført risikovurderinger og DPIA på følgende behandlinger i VIS:

- Elevadministrasjon - DPIA og Risikovurdering
- Oppfølging av elever - DPIA og Risikovurdering
- Personaladministrasjon - Risikovurdering
- Informasjonssikkerhet - Risikovurdering
- Personopplysninger foresatt - DPIA og Risikovurdering

Risikoanalysen er datert 26.04.21 Personvernombudet har bidratt med råd underveis i arbeidet med risikovurderinger og DPIA. Elevorganisasjonen har hatt egne møter og har hatt mulighet til å gi innspill. Behandlingsprotokoll og risikovurderinger oppdateres to ganger i året eller oftere hvis det er endringen i VIS.

I risikomatrisene for elevadministrasjon og oppfølging av elever ble 19 like risikofaktorer vurdert. To av risikofaktorene ble i begge vurderingene markert som «rødt», med både høy sannsynlighet og konsekvens. Den ene faktoren gjelder risiko for feil i elevens opplysninger. Dette kan være personopplysninger som ikke er oppdaterte, feil i registrering av fusk og karakterer og tilfeller hvor foreldre med fradømt foreldreansvar får tilgang til elevens personopplysninger. Oppdatering av personopplysninger skjer daglig med integrasjon mot det sentrale folkeregister (DSF). Informasjon om f.eks. karakterer legges inn manuelt. Tiltak for å minimere feil ved slike manuelle registreringer er å sikre at skolene har gode rutiner. Elevopplysninger som skal skjermes fra foreldre på grunn av omsorgsovertakelse må gjøres manuelt av skolene. En ny rutine for hvordan dette gjøres av skolene ble innført 06.05.21. Det har blitt gjort ny risikovurdering etter tiltak hvor sannsynligheten er noe redusert, men risikoen er fortsatt på «rødt». I vurdering av tiltakene i april 2021 står det at «*skolene må arbeide med sine interne rutiner og fordeling av arbeidsoppgaver ut fra de felles rutinene som er laget*».

Den andre faktoren med høy risiko er mangelfulle rutiner for å etterleve GDPR. Tiltak for å minimere risiko er revidering og krav om å signere ny informasjonssikkerhetsinstruks og dokument som beskriver ansvar i anskaffelser av digitale løsninger. Begge dokumentene er nå utarbeidet. Et annet tiltak er å øke kompetansen om GDPR og informasjonssikkerhet og å klargjøre ansvar og roller. Det vises til årlig deltakelse i nasjonal sikkerhetsmåned, opplæring fra personvernombudet og økt bevisstgjøring om informasjonssikkerhet. Et annet tiltak er at «*den enkelte leder må ta et ansvar for å følge opp sikkerhetstiltakene. Ansvarsforhold må avklares og rutiner må forankres på den enkelte skole/avdeling. Dette er en del av alles daglige arbeid, og alle må få informasjon om dette rammeverket*». I vurdering av tiltakene per 26.04.21 står det at informasjonssikkerhetsinstruksen ikke er undertegnet av alle ansatte enda og at tiltak ikke er gjennomført per april 2021. Fylkesrådmann er ansvarlig for å følge opp tiltakene. DPIA for VIS er eneste DPIA PVO har vært involvert i. Informant fra digital utviklingsavdeling sier at de har jobbet med å tilpasse tilgangsstyring. I startfasen var det nok for stort definerte tilganger enn det som er tilfelle nå.

4.5 PUBLISERING AV DOKUMENTER PÅ OFFENTLIG POSTLISTE

Dokumentsenteret legger ut dokumenter på postlisten for sentraladministrasjonen. Hver skole har egen skolearkivar som og publiserer dokumenter på postlisten selv. Uansett skal arkivar kvalitetssikre og journalføre ekspederte dokumenter. Det er som regel kun tittel som kvalitetssjekkes. Dokumentsenteret har rutine for å kvalitetssikre postlisten. Det er ikke mulig å sende ut dokumenter markert med sensitiv informasjon.

4.6 KONTROLL AV OFFENTLIG POSTLISTE PÅ SKOLENE

Som en del av forvaltningsrevisjonen har vi foretatt kontroller av postlister ved et utvalg skoler for perioden 01.05.21 – 26.08.21. Ved tre av skolene ble det funnet sensitiv informasjon på postlisten (gjelder ansatte). Dette gjelder for eksempel arbeidsmiljøsak, uførepensjon, skademelding og foreldrepermisjon. Noen av dokumentene er unntatt offentlighet, mens i noen av sakene var det mulig å få åpnet dokumentasjonen/vedlegget. Sensitiv informasjon som ble funnet var blant annet fødselsnummer og helseopplysninger. Arkivleder og avdelingsleder leder for digital utvikling ble informert om funnet 30. og 31. august. Dokumentene ble av dokumentsenteret fjernet fra postlisten etter kort tid.

De tre ansvarlige skolene ble i etterkant informert og bedt om å ta stilling til videre avviksbehandling. Personvernombudet og opplæringssjef er også informert om saken. Per 27.09.21 er det kun en av skolene som har lagt inn avviket i QM+ og det er ikke sendt inn avviksmelding til Datatilsynet. På planlagt rektorsamling tre dager etter funnet ble alle skolene bedt om å sjekke sine postlister. Rektorene ble også informert om dette per e-post fra seksjonssjef.

4.7 OPPBEVARING AV PERSONOPPLYSNINGER PÅ SKOLENE

Revisjonen gjennomfører årlig en rutinerevisjon som en del av regnskapsrevisjonen ved et utvalg videregående skoler I vår revisjonsrapport for 2020, datert 15.12.20, ga vi følgende tilbakemelding til opplæringsdirektøren:

«Vi får opplyst at all informasjon som er arkivverdig, arkiveres elektronisk i Elements. Gradering av sensitiv informasjon skal gjøres i de tilfeller det er lovpålagt eller nødvendig iht. interne retningslinjer. Vår gjennomgang viser at rutine for behandling av sensitiv informasjon anses tilfredsstillende. Videre vises det til at det benyttes kryptert e-post. Gjennom intervju fikk vi informasjon om et tilfelle hvor kryptert e-post ble sendt til feil mottaker. Det foreligger en risiko for at e-post med sensitiv informasjon blant annet ikke blir kryptert eller sendt til feil mottaker. Det anbefales i at sensitiv informasjon i minst mulig grad formidles pr e-post.»

Lærere og sosialpedagogiske rådgivere behandler store mengder personopplysninger. Legeerklæringer, elevvurderinger, notat fra samtaler og referat fra klasselærerråd inneholder elevopplysninger som navn, helseopplysninger og andre sensitive opplysninger for eleven. På de

fire skolebesøkene har revisjonen intervjuet tolv lærere og fire sosialpedagogiske rådgivere. De ansatte revisjonen intervjuet behandler slike opplysninger både skriftlig og elektronisk.

De fire skolene har noe ulike praksis for håndtering av legeerklæring. En av skolene har egen rutine hvor eleven selv leverer legeerklæringen til administrasjonen. Legeerklæringen blir deretter arkivert i Elements og i skolens fysiske arkiv og melding om mottatt legeerklæring blir sendt til lærer. Men lærere på samme skole opplyser i intervju at de også mottar legeerklæring direkte fra elevene og oppbevarer disse i egne permer. Ut ifra intervjuene med lærere på fire ulike skoler synes oppbevaring av legeerklæringer i fysiske permer å være vanlig praksis. Flesteparten av lærerne oppbevarer permen på felles arbeidsrom for lærere. Noen lærere har tilgang til låsbart skap som de bruker for legeerklæringer. En lærer påpeker at nøkkelen for skapet ikke er unik, men gjelder for andre læreres skap også. Arbeidsrommene for lærerne blir typisk delt med fem til ti lærere med en etablert praksis for at sistemann låser døren. Lærerne som ble intervjuet makulerte legeerklæringer på slutten av skoleåret. Skriftlige elevvurderinger blir også oppbevart på samme måte som legeerklæringer. Lærerne bruker også fysiske lærerplanlegger med klasselister, bilder, fraværsoversikt og elevvurderinger.

Lærernes vurderinger blir også lagret elektronisk. Flere lagrer dette på personlig område på OneDrive. Det er i intervju også avdekket bruk av Dropbox for oppbevaring av elevoppgaver med vurderinger. Noen lærere bruker passordbeskyttelse på dokumenter laget i Office-programmer. Det synes ikke å være etablert praksis rundt sletting av slike filer. Hvis ikke den enkelte ansatt sletter filene selv, blir de automatisk slettet ved avslutning av arbeidsforhold.

Ansatte på skolen deltar i ulike møter hvor elever blir diskutert. Dette gjelder for eksempel klasselærerråd hvor alle lærere tilknyttet en klasse deltar i tillegg til sosialpedagogisk rådgiver. Referat fra slike møter inneholder navn på elever, helseopplysninger og annen sensitiv informasjon om elever. Noen av intervjuobjektene forteller at det i referatene står elevens initialer istedenfor navn. Referatene blir lagret i låste Teams-grupper. Tilganger til gruppene styres av avdelingsleder og avsluttes etter endt skoleår.

Alle ansatte på de fire skolene har tilgang til å sende e-post kryptert. Flere av lærerne har sett opplæringsvideoer for kryptering. Det generelle inntrykket fra skolene er at det er enkelt å kryptere e-post og at det er noe som brukes for å sende e-post med personopplysninger. De fleste intervjuobjektene på skolene ble spurt om de hadde mottatt ukryptert sensitiv informasjon på e-post. Flere svarer at dette har skjedd, men at dette i mindre grad skjer enn før. Både lærere og rektorer opplever å motta sensitiv informasjon fra elever og foreldre. Dette er gjerne e-post med helseopplysninger knyttet til fravær eller forespørsler fra foreldre om inntak på skolen som inneholder fødselsnummer. Noen intervjuobjekter synes det er vanskelig å avgjøre hva som er sensitiv informasjon.

De sosialpedagogiske rådgiverne har enkeltsamtaler med elever som trenger ekstra oppfølging. Slike samtaler er i utgangspunktet ikke en del av saksbehandling og ikke arkivverdig. Men det er ikke et felles system for hvor slike dokumenter skal oppbevares. I intervjuene med rådgiverne fortelles det om ulik praksis for hvor referater fra samtaler og notater oppbevares: skriftlige

notater innelåst i skap, dokumenter lagret i Elements eller på personlig OneDrive-område. En sosialpedagogisk rådgiver forteller at det er utfordrende at det ikke er et felles system for slike dokumenter som en kan føle er sikkert nok.

Sosialpedagogiske rådgivere deler også informasjon med kontaktlærere. I starten av skoleåret er det lister over hvilke elever som trenger ekstra oppfølging. For eksempel gjelder dette elever med lære- og skrivevansker som trenger ekstra tilrettelegging fra lærere. Det er ulike praksis for hvordan slike lister blir videreformidlet til lærerne. Intervjuobjektene forteller at listen enten blir sendt kryptert på e-post, delt på Teams eller informert om muntlig. I intervju ytres det ønske om eget program/system for samhandling med lærere hvor slike dokumenter kan deles på en sikker måte.

Intervjuene på en av skolene ble gjort på møterom i administrasjonens del av skolen. På møterommet fant revisjonen to PPT henvisningsskjema med personnummer, navn og helseopplysninger. Revisjonen informerte sosialfaglig rådgiver og rektor om funnet under skolebesøket. De visste ikke hvor lenge disse skjemaene skal ha ligget på møterommet, men det er mulig de kan ha ligget der i noen måneder. Møterommet kan låses, men låses ikke automatisk. Rommet kan derfor være tilgjengelig for elever hvis det er ulåst.

4.8 INFORMASJONSSIKKERHETSINSTRUKS

Som oppgitt i kapittel 1.3 anbefalte vi i forbindelse med forvaltningsrevisjonen av fylkeskommunen sitt arkiv at rådmannen må sikre at alle ansatte signerer informasjonssikkerhetsinstruksen. Informasjonssikkerhetsinstruksen for ansatte ble i april 2021 revidert og alle medarbeidere i fylkeskommunen må signere denne elektronisk ved å bruke MinID (BankID, Buypass). Alle ledere med personalansvar sender instruks til den enkelte ansatt og arkiverer signert instruks i arkivsystemet. Dokumentsenteret har sendt rutinebeskrivelse for hvordan lederne skal gjøre dette.

Som en del av revisjonen er det gjort stikkprøver for signering av informasjonssikkerhetsinstruks på de fire skolene som ble besøkt. Det ble trukket ut fem ansatte på hver skole som skolearkivar søkte opp i arkivsystemet for å sjekke om vedkommende har signert instruks. På to av skolene var instruksen signert for alle ansatte som ble trukket ut.

De to andre skolene hadde ikke sendt ut informasjonssikkerhetsinstruksen til sine ansatte. Disse peker på at hele operasjonen var nokså omstendelig og ikke har blitt prioritert. Skolene som har sendt ut instruksen bekrefter at utsendelsen ikke var enkel. Bruk av BankID som signering var nytt, og ansatte uten Digipost gjorde signeringen komplisert.

4.9 PRAKSIS FOR LÅSING AV DATAMASKIN

Et av kravene i informasjonssikkerhetsinstruksen er å «låse datamaskinen med passordbeskyttelse når du forlater den.». Det generelle inntrykket fra intervju på skolene er at de fleste ansatte har en

vane for å låse datamaskin når den blir forlatt, enten det er på arbeidsrommet eller i klasserommet. En av skolene viser også til en kampanje de hadde hvor det ble plassert ut røde kort på ulåste og forlatte PC'er.

I undervisningen brukes lærernes PC'er for å dele innhold på felles skjerm for klassen, for eksempel oppgaver som elever skal gjøre. Dette gjøres med «delt skjerm». En lærer forteller om episoder hvor varslinger fra e-post og Teams har blitt synlig på den delte skjermen. Slike varslinger har vist deler av innholdet i slike meldinger, som kan være av sensitiv karakter. Det er mulig å endre innstillingen slike at varsler og innhold ikke blir synlig på skjermen.

En annen lærer forteller om undervisning som krever oppfølging av elever i ulike rom samtidig. Dette fører til at lærer går litt fram og tilbake mellom klasserommene. I undervisningen blir deling av lærerens skjerm på felles skjerm brukt. Deling av skjerm fungerer derimot ikke hvis lærer låser PC'en. Derfor blir ikke PC'en låst når lærer må følge opp elever i andre klasserom. Når lærerens PC står ulåst, er det mulig å gå inn på lærerens e-post, Teams, fagsystemer osv.

4.10 VURDERING

Fylkeskommunen har rutiner, instrukser og retningslinjer som må følges for å oppfylle lovkrav for informasjonssikkerhet og personvern. Rutinene gjelder for eksempel sikker bruk av e-post, lagringsrutiner og hvordan avvik skal meldes. Rutinene er tilgjengelige på intranettet og/eller i avvikshåndteringssystemet QM+. Noen av enhetene revisjonen intervjuet har også lagret rutiner på Teams. Det generelle inntrykket fra intervjuer og skolebesøk er at ansatte vet hvor de skal finne rutiner, men at rutinene er lite tilgjengelig. Det er varierende i hvor stor grad intranettet blir aktivt brukt som informasjonskilde. Arbeidsreglementet ble i 2021 utvidet med et avsnitt om informasjonssikkerhet. Informasjon om endring av arbeidsreglementet på de fire skolene ble gjort som sak på intranett, noe som de fleste ansatte revisjonen intervjuet ikke hadde fått med seg. De fleste av informantene peker på at QM+ er et dårlig egnet system for å gjøre informasjon tilgjengelig, det er lite brukervennlig og krever også ekstra pålogging som kan være en barriere.

Bruk av kryptert e-post når det skal sendes personopplysninger er godt innarbeidet på skolene. Det blir framhevet at kryptering i e-postprogrammet er brukervennlig og at det er tilgjengelige opplæringsvideoer.

Fylkeskommunen har innført flere nye rutiner i løpet av sommeren. I risikovurderingen for Visma InSchool (VIS) kommer det fram at det gjenstår arbeid med implementering av rutiner på skolene. Etterlevelse av informasjonssikkerhetsinstruksen trekkes fram som viktig for å etterleve krav i personvernforordningen. To av de fire skolene revisjonen besøkte hadde i september 2021 ikke sendt ut informasjonssikkerhetsinstruksen for signering til sine ansatte.

På skolene ble det avdekket ulik praksis for oppbevaring av personopplysninger i form av blant annet legeerklæringer, referater fra møter, og elevvurderinger. Mange lærere revisjonen intervjuet oppbevarer personopplysninger i permer på arbeidsrom, på personlig område på OneDrive. Det ble også oppdaget bruk av Dropbox for oppbevaring av elevoppgaver. På et av skolebesøkene

fant revisjon PPT-henvisningsskjema med sensitive elevopplysninger på et møterom. I kontroll av offentlig postliste på et utvalg skoler ble det ved tre skoler funnet sensitiv informasjon om ansatte, blant annet fødselsnummer og helseopplysninger.

Revisjonen har følgende anbefalinger til fylkeskommunene:

- Informasjonssikkerhetsinstruksen bør signeres av alle ansatte.

5 KOMPETANSE

Problemstilling: «Hvilke tiltak er iverksatt for å styrke kompetansen innen informasjonssikkerhet hos de ansatte, både generelt og blant de som jobber med IKT?»

5.1 REVISJONSKRITERIER

Kommunen skal etter personvernforordningen artikkel 24 gjøre organisatoriske tiltak for å ivareta krav rundt informasjonssikkerhet og personvern. Tiltakene skal gjennomgås jevnlig og skal oppdateres ved behov. Ifølge Datatilsynets veileder for internkontroll[14] vil dette i praksis bety å lage rutiner som beskriver hvordan informasjon skal behandles for å oppfylle lovkrav. Veilederen peker også på at opplæring er viktig for å kunne etterleve lovkrav: *«Brukerne bør få opplæring i rutiner, sikkerhetsprosedyrer og riktig bruk av informasjonssystemer for å redusere potensielle risikoer.»*.

Personvernombudet skal bistå virksomheten med å etterlevelse av personopplysningsloven med GDPR. Etter artikkel 39 skal personvernombudet; *«informere og gi råd til den behandlingsansvarlige eller databehandleren og de ansatte som utfører behandlingen, om de forpliktelsene de har i henhold til denne forordning, […]»*. Personvernombudet skal også gi opplæring av personell som utfører behandlingsaktiviteter og gjennomføre holdningsskapende tiltak.

Ansatte trenger tilstrekkelig med kunnskap for å utføre sine arbeidsoppgaver på en god måte. Med økt bruk av digitale verktøy kreves det også opplæring i disse. Utilstrekkelig opplæring gir økt risiko for brukerfeil som kan gi konsekvenser for informasjonssikkerheten. Digitalisering introduserer også virksomheten for nye trusler. Tekniske barrierer hindrer de fleste angrep, men ikke alle. Det er derfor viktig at ansatte har kunnskap om sårbarheter i digital sikkerhet. Tilstrekkelig og relevant opplæring innen informasjonssikkerhet er et eget krav i standard for administrasjon av informasjonssikkerhet (ISO 27002).

Et av sikkerhetsmålene i informasjonssikkerhetshåndboken er at «Medarbeidere som bruker fylkeskommunens digitale løsninger har tilstrekkelig kompetanse for å ivareta sikkerhetskravene. Videre i beskrivelse av sikkerhetsorganisasjonen står det at sikkerhetsansvarlig skal «sørge for at det gjennomføres opplæring i informasjonssikkerhet». Det står også at «Alle ansatte skal gjennom opplæring og rutiner oppnå tilstrekkelig kompetanse for å forvalte informasjon og systemer på en sikker måte»

[14] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/

Revisjonskriteriet

- Brukerne bør få opplæring i rutiner, sikkerhetsprosedyrer og riktig bruk av informasjonssystemer

5.2 STATUS FOR KOMPETANSENIVÅ

Modenhetsrapporten fra 2020 beskriver status for sikkerhetsopplæring i fylkeskommunen. TietoEVRY som gjennomførte modenhetsanalysen konkluderer med at fylkeskommunen delvis etterlever krav om opplæring. Analysen påpeker at nyansatte ikke får generell opplæring i informasjonssikkerhet og personvern. For å etterleve krav om sikkerhetsopplæring blir det foreslått obligatorisk kurs for nyansatte og jevnlig sikkerhetsopplæring for alle ansatte. Sikkerhetsrapporten avdekker også manglende opplæring for ansatte med særskilt ansvar for behandlingsprotokoller, databehandleravtaler, anskaffelser, informasjonsklassifisering og avslutning av tilganger

Fylkeskommunen har ikke system for å måle kompetansenivået hos den enkelte ansatt for informasjonssikkerhet og personvern. Det generelle inntrykket fra intervjuer og skolebesøk er at kompetansenivået hos den enkelte ansatt er noe varierende, men at det har blitt bedre de siste årene. Flere påpeker at kompetanseheving er viktig og nødvendig for å bedre informasjonssikkerheten i fylkeskommunene og at det er en ledelsesjobb å prioritere kompetanseheving. Flere informanter mener IKT-kompetansen har blitt bedre det siste året grunnet Covid-19 og mye hjemmekontor som har krevd bruk av digitale verktøy.

5.3 IVERKSATTE TILTAK FOR KOMPETANSEHEVING

Nye rutiner og instrukser

I risikovurderingen for VIS er en av de største risikoene mangelfull etterlevelse av GDPR-regelverket på skolene. For å redusere risikoen forslås det å sikre felles forståelse av sikkerhetskrav. Et av tiltakene er den reviderte informasjonssikkerhetsinstruksen som beskriver rundt 60 krav innen blant annet taushetsplikt, varsling av avvik, sikker bruk av programmer og utstyr og behandling av personopplysninger. En del av kravene er ikke forklart, for eksempel lovkrav rundt registrertes rettigheter, kryptering, «kritisk informasjon» og tofaktorautentisering. Et av intervjuobjektene sier at innholdet i informasjonssikkerhetsinstruksen er vanskelig å forstå og at det trengs ytterligere opplæring for å tilegne seg kompetansen som kreves for å etterleve instruksen.

Kurs

Fylkeskommunen har ingen obligatoriske kurs, men har ulike kurs med frivillig deltakelse.

Fylkeskommunen har de siste årene deltatt to ganger i nasjonal sikkerhetsmåned (2018 og 2020). Nasjonal sikkerhetsmåned er en årlig kampanje arrangert av Norsk senter for informasjonssikring (NorSIS). Kampanjen har bestått av små leksjoner, videoer, nyhetssaker og konkurranse på intranettet. Deltakelsen har vært frivillig. I 2020 var det 2 200 deltakere fra fylkeskommunen som deltok på 39 kurs i tre forskjellige tema. Leksjonene fra nasjonal sikkerhetsmåned ligger fremdeles tilgjengelig på intranettet.

Ledelsen på alle de fire skolene som ble besøkt hadde hørt om nasjonal sikkerhetsmåned, og flere intervjuobjekter på skolene bekrefter deltakelse på alle eller deler av opplæringsopplegget. På en skole sendte rektor e-post til sine ansatte og oppfordret til å delta, mens på flere andre har informasjon om nasjonal sikkerhetsmåned kun vært formidlet gjennom felles intranett for hele fylket. En annen skole har link til opplæringsleksjonene i deres HMS-bok under eget kapittel om informasjonssikkerhet og personvern. Et intervjuobjekt hadde ikke hørt om nasjonal sikkerhetsmåned.

Flere informanter opplever at nasjonal sikkerhetsmåned og spesielt nanoleksjonene har vært nyttige. Det pekes også på hvor viktig det er med økt kompetanse, bevissthet og forståelse i hele organisasjonen. Med frivillig deltakelse er det vanskelig å nå ut til alle og flere informanter sier det burde vært noe obligatorisk opplæring innen informasjonssikkerhet.

Fylkeskommunen har nylig innført Microsoft 365 og nye digitale verktøy som Teams, OneNote og OneDrive. I tillegg har fylkeskommunen gått over til nytt arkivsystem, Elements. Som en del av implementeringen har det blitt kjøpt inn ulike kurs i disse systemene som har vært frivillige å delta på. Kurs i digitale hjelpemidler som Teams har ifølge digitaliseringsrådgiver vært populært, spesielt på grunn av koronasituasjon med hjemmekontor og behov opplæring innen digital kommunikasjon.

Dokumentsenteret gjennomførte våren 2021 kurs for den nye samferdselsavdelingen sammen med fylkesadvokaten. Kurset ble iverksatt som følge av arkivrevisjonen i 2017 hvor det ble anbefalt å gjøre arkivplan bedre kjent. Dokumentsenteret planlegger å gjennomføre tilvarende kurs for andre avdelinger. Det er også lagt ut mindre leksjoner på intranettet med opplæring i Elements.

Personvernombudet har gjennomført opplæring om behandlingsprotkoller, risikovurderinger og tilgangsstyring

Opplæring i og innføring av Visma InSchool

Det nye skoleadministrative systemet Visma InSchool (VIS) ble tatt i bruk på alle videregående skoler i 2020. Prosjektgruppen for VIS i opplæringsavdelingen har i årene før implementering jobbet med innføring og opplæring for lærere, ledere, merkantilt ansatte, elevorganisasjon og tillitsvalgte.

Prosjektgruppen startet med egne innføringsteam på hver skole med rektor som prosjekteier, avdelingsleders som prosjektleder og også merkantilt ansatte. Før opplæring i VIS ble gitt, fikk

innføringsteamene grunnleggende innføring og oppfriskning av relevante lovverk, GDPR og personvern. Opplæring ble gjort av personvernombudet og prosjektgruppen for VIS. Tilganger, taushetsplikt og tjenstlig behov er tema som ble repetert på de ukentlige møtene innføringsteamene hadde med prosjektgruppen i 2020. Fokus på møtene har vært å skape felles forståelse og praksis i bruk av VIS.

VIS har nå vært brukt i ett skoleår og innføringsteamene har blitt erstattet med en VIS-kontakt for hver skole. VIS-kontaktene har møter og informasjonsutveksling gjennom egen Teams-gruppe med prosjektgruppen. Her informeres det blant annet om status for de siste delene av VIS som skal tas i bruk til neste år.

Opplæring for lærere og merkantilt ansatte ble utført av 12 instruktører i forkant av implementeringen av VIS i 2020. Instruktørene hadde i forkant fått opplæring fra leverandøren Visma og av prosjektgruppen for VIS i fylkeskommunen. Brukere av VIS har også hatt tilgang til digitalt opplæringsmateriell fra VISMA og det er eget område på i intranettet med informasjon. For skoleåret 2021/2022 skal det arrangeres nyansattkurs og opplæring i nye funksjoner for skoleledelsene.

Prosjektgruppen for VIS har gjennomført flere brukerundersøkelser for utvalgte skoler. Den siste undersøkelsen ble gjennomført våren 2021. Her ble et utvalg lærere spurt om hvordan de synes opplæringen har vært. Resultatet av undersøkelsen viste at flere etterlyste mer opplæring gjennom hele året. På bakgrunn av dette har det blitt laget egne årshjul for skolene med flere opplæringsaktiviteter.

Råd og veiledning

Dokumentsenteret og IT-avdelingen bruker samme «brukerhjelp»-portal. Ansatte sender henvendelser enten direkte i portalen, i e-poster som dokumentsenteret legger inn i portalen, eller på telefon. Supporttjenesten for dokumentavdelingen er delt inn første og andrelinjesupport. Førstelinje tar de fleste saker mens andrelinjen består av ledere og enkelte ansatte som tar de større og tyngre problemene. Hvis dokumentsenteret får henvendelser som gjelder IT, blir disse sendt direkte til IT-avdelingen i «brukerhjelp»-portalen. Dokumentsenteret har også en vakttelefon, og ansatte ringer gjerne på Teams. Arkivleder sier dokumentsenteret er opptatt av å være tilgjengelig. Supporttjenesten for IKT er åpen fra 07.30-15.30 via nettside, e-post eller telefon.

Skolene har egen IT-ansatt og tar vanligvis spørsmål for IKT for skolen. Skolens IKT-ansatt har mulighet til å legge inn saker til IKT i sentraladministrasjonen, men personalet på skolene kan ikke melde inn saker til IKT i sentraladministrasjonen. IKT fagleder har gitt veiledning til teknikere på skolen.

En informant forteller at det til høsten settes i gang forprosjekt med behovsvurdering «IT-støtte» som skal være en hjelp for ansatte i å finne frem til rett dokumentasjon og hjelp til å skrive rutiner. Mulig eventuell oppstart for dette vil være 2022.

Personvernombudet gir også råd og veiledning etter henvendelser.

5.4 KOMPETANSE BLANT IKT-PERSONELL

IKT-avdelingen i sentraladministrasjonen deltar jevnlig på kurs og konferanser som handler om teknisk sikkerhet. I intervju med ledere i avdeling for digital utvikling vises det til at utviklingen innen IT skjer i raskt tempo. Tidligere var det tilstrekkelig å tilegne seg ny kunnskap med ulike kurs. Men i dag endrer teknologien og trusselbildet innen IT seg så raskt at dryppvise kompetansehevingstiltak ikke er tilstrekkelig. Kompetanseheving i IKT-avdelingen sentralt skjer nærmest daglig ved at det er stadig nye problemstillinger som skal forstås.

IKT-avdelingen har gjennomgått en omorganisering etter 2018 som en del av å styrke kompetansen i avdelingen. Bakgrunnen for omorganisering er en av utfordringene det vises til i ROS-analysen fra 2013; *«SENTRAL-IKT har lite overlappende kompetanse og det er en håndfull nøkkelpersoner innenfor drift som er kritiske for daglig drift, vedlikehold og feilsøking.»*. Omorganiseringen har bestått av mer Team-basert arbeid, med vekt på informasjonsdeling og problemløsning i fellesskap.

I samme ROS-analyse pekes det på at kompetansen blant IKT-personell på skolene er variabel. Ifølge avdeling for digital utvikling er dette fremdeles et problem, spesielt i lys av den rivende teknologiske utviklingen de siste årene som krever stadig ny kunnskap. I ROS-analysen er det foreslått å se på bedre utnyttelse av IKT-kompetansen på skolene, med økt samarbeid på tvers av skolene eller mer samkjøring med IKT sentralt. Organiseringen av IKT på skolene er den samme som i 2013. Ifølge flere informanter hadde IKT-kompetansen på skolene blitt styrket ved å følge opp forslagene fra ROS-analysen. De peker også på at andre fylker har gjennomført omorganiseringer ved å legge IKT-avdelingene på skolene under sentraladministrasjonens IKT-avdelinger.

5.5 VURDERING

Fylkeskommunen tilbyr ulike kurs med frivillig deltakelse. Av kurs direkte knyttet til informasjonssikkerhet har fylkeskommunen jevnlig deltatt i nasjonal sikkerhetsmåned med tilhørende digital opplæringspakke. Den generelle inntrykket fra informantene er at de fleste har deltatt på alle eller deler av opplæringsleksjonene. Minimering av brukerfeil i digitale verktøy er også viktig for god informasjonssikkerhet. Fylkeskommunen har kjørt en rekke kurs i nye fellestjenester innenfor Microsoft 365-pakken. Skolene har også hatt eget undervisningsopplegg for det nye skoleadministrative systemet Visma InSchool.

Fylkeskommunen har IKT-personell i sentraladministrasjonen samt på alle de videregående skolene. IKT-avdelingen i sentraladministrasjonen deltar jevnlig på kurs og konferanser. Ansatte i IKT-avdelingen i sentraladministrasjonen påpeker at den viktigste kompetansehevingen skjer nærmest daglig ettersom stadig ny teknologi og trusselbilde krever raske løsninger på nye problemstillinger. Ansatte på avdelingen trekker også fram nylig omorganisering med økt team-arbeid og samarbeid på tvers, som et grep for å styrke kompetansen. IKT-personellet på skolene jobber i stor grad selvstendig. I ROS-analyse fra 2013 blir det pekt på at kompetansen på skolene

er variabel og at økt samarbeid på tvers av skolene eller med IKT sentralt hadde styrket kompetansen. Informanter revisjonen har intervjuet bekrefter at kompetansen på IKT i skolene hadde blitt styrket med slike grep.

Det er positivt at fylkeskommunen deltar på nasjonal sikkerhetsmåned og tilbyr ansatte kurs i digitale verktøy. Fylkeskommunen har også en fungerende support-tjeneste for brukerstøtte. Men fylkeskommunen har ingen obligatoriske kurs innen informasjonssikkerhet. Dette blir pekt på som en svakhet i modenhetsrapporten fra 2020. Den nye informasjonssikkerhetsinstruksen inneholder en rekke krav som uten tilstrekkelig opplæring vil være vanskelig å forstå for ansatte. Fylkeskommunen har heller ikke system for å måle kompetansenivået i organisasjonen. Informantene vi har intervjuet mener at kompetansen har stadig blitt bedre, men at det er større variasjoner innad i organisasjonen.

6 AVVIK

Problemstilling: «I hvilken grad har fylkeskommunen sikret en god praksis for registrering og oppfølging av avvik innen informasjonssikkerhet og personvern? (herunder antall avvik knyttet til sensitiv informasjon og årsaker til disse)

6.1 REVISJONSKRITERIER

Fylkeskommunen skal etter kommuneloven § 25-1 punkt c «avdekke og følge opp avvik for risiko for avvik». Hvis avviket gjelder personopplysninger, skal den behandlingsansvarlige etter personvernforordningen artikkel 33 melde bruddet på personopplysningsplikten til tilsynsmyndighet, med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter. Den behandlingsansvarlige skal også etter artikkel 34 informere de berørte registrerte om bruddet på personopplysningssikkerhet. Datatilsynet anbefaler at egne rutiner for behandling av avvik er beskrevet i internkontrollen.

Revisjonskriterier
• Fylkeskommunen skal ha rutine for innmelding og håndtering av avvik innen informasjonssikkerhet, personvern og sikkerhetsbrudd • Avvik skal følges opp med tiltak

6.2 RUTINER I AVVIKSBEHANDLING

I informasjonssikkerhetshåndboken, og i sikkerhetsinstruks, blir ansatte bedt om å melde uønskede hendelser og avvik på personvern og informasjonssikkerhet i avvikshåndteringssystemet QM+. Ansatte får tilgang til QM+ ved ansettelser.

Fylkeskommunen har flere rutiner for behandling av avvik innen informasjonssikkerhet og personvern (Tabell 2). Tre av disse er rutiner som finnes både på intranettet og QM+. Det siste dokumentet «Årsaker og konsekvenser, melding til Datatilsynet og melding til de registrerte» er et hjelpedokument og finnes kun i QM+.

Tabell 2. Rutiner for avviksbehandling

Type avvik	Tittel (sist oppdatert)	Hvem skal avviket sendes/rapporteres til?	Viser til andre rutiner/skjema?
HMS Informasjonssikkerhet Personvern	Retningslinje for melding av avvik og uønskede hendelser i Qm+ (10.07.2019)	Nærmeste leder, evt. leder på neste nivå	
Informasjonssikkerhet Personvern	Informasjonssikkerhetshåndbok – Avvikshåndtering (15.07.21)	Sikkerhetsansvarlig eller etter annen intern organisering.	Link til «Retningslinje for melding av avvik og uønskede hendelser i Qm+»
Personvern	Retningslinje for brudd på personopplysningssikkerheten (28.08.2020)	Linjeleder	- skjema for vurdering av avviksmelding - skjema for varsel av de berørte.
Personvern (hjelpedokument i QM+)	Årsaker og konsekvenser, melding til Datatilsynet og melding til de registrerte (15.03.19)	Nærmeste leder	

Informasjonssikkerhetshåndboken har et eget dokument for avvikshåndtering som gir en kort beskrivelse av hva avvikshåndtering er og krav om varsling til Datatilsynet. Dokumentet henviser til dokument fra 2019: «Retningslinjer for melding av avvik og uønskede hendelser i Qm+» som er felles retningslinje for alle avvik som meldes. I QM+ er det også flere hjelpedokumenter av eldre dato. I retningslinjen står det at:

«*Leder er ansvarlig for at retningslinjen gjøres kjent i egen enhet, og for å legge til rette for en åpenhetskultur der melding av uønskede hendelser og avvik blir verdsatt og anerkjent som verdifull informasjon inn mot styrings, lærings- og forbedringsarbeid.*

Den som blir oppmerksom på en uønsket hendelse eller et avvik har plikt til å registrere melding i Qm+ etter denne retningslinjen, og på den måten bidra til forbedring.

Leder har ansvar for å håndtere meldinger og sørge for at nødvendige tiltak blir iverksatt og fulgt opp. Dette skal gjøres på en systematisk og helhetlig måte, slik at det gir positive konsekvenser for den enkeltes arbeidshverdag og for virksomheten som helhet.»

Ifølge retningslinje for brudd på personopplysningssikkerheten er det *«medarbeidere som oppdager et avvik, har ansvar for å melde dette i kvalitetssystemet»*. Personvernombudet får kopi av melding som blir sendt inn, men ikke tilgang til f.eks. feilsendte dokumenter som er årsak til avviket.

Ifølge retningslinjer skal ledere rådføre seg med personvernombudet om det er nødvendig å melde avvik til Datatilsynet eller gi informasjon til de berørte, men ifølge personvernombudet tar ledere i liten grad kontakt i forbindelse med avvik.

Flere informanter har en oppfattelse av at det meldes inn for få avvik. Årsaker til dette kan være prioriteringer av ledere, for lite ressurser og uklare rutiner. En informant opplyser at få meldte avvik er en generell observasjon fra Datatilsynet som gjelder flere fylkeskommuner. Noen informanter synes også det er uklart hvem som skal melde inn avvik til Datatilsynet. En usikkerhet er for skolene og hvorvidt det er rektor eller opplæringsavdelingen som melder inn avvik til Datatilsynet.

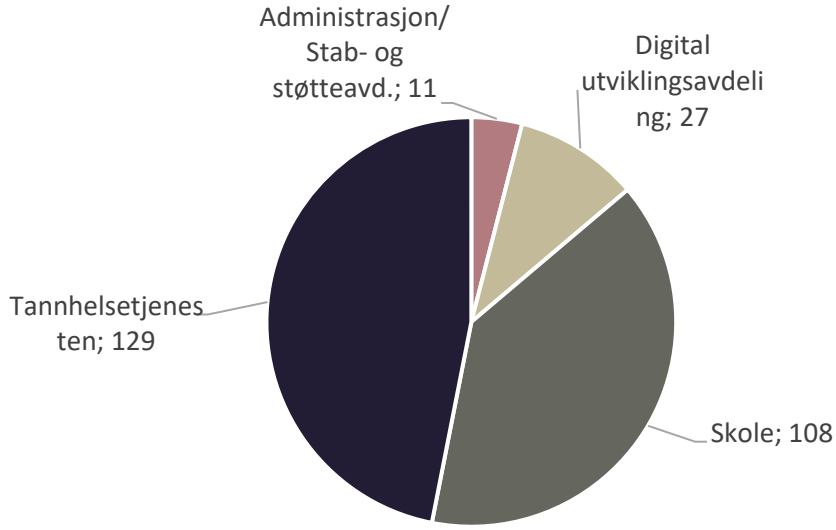
Mange HMS-avvik meldes også feil under kategori for informasjonssikkerhet, noe som gjør det vanskelig å få oversikt over relevante avvik.

Personal- og organisasjonsavdelingen har ansvar for å lage årsrapporter for meldte avvik og uønskede hendelser i QM+. I årsrapporten for 2020 kommer det frem at det gjøres feil i registreringen. Dette skyldes både kompetansen til brukerne, men også at meldingssystemet ikke har godt nok system for å fange opp feil. Det er derfor behov for opplæring og bevisstgjøring for meldingssystemet. Videre står det at: «*Det er fremdeles utfordringer i enkelte virksomheter når det gjelder å få flere til å ta i bruk meldingsmodulen. Lederne må sette Qm+ på dagsorden og jobbe med holdning og kultur. Samtidig er det ledernes ansvar å be om bistand og opplæring i Qm+ fra personal- og organisasjonsavdelingen når det er behov for det*».

6.3 REGISTRERTE AVVIK INNEN INFORMASJONSSIKKERHET OG PERSONVERN

I avvikssystemet er det en kategori for avvik innen informasjonssikkerhet. I perioden 2017 –2021 (til og med 08.06.2021) er det innmeldt 275 avvik innen informasjonssikkerhet. En gjennomgang av avvikene viser at ca. 30-40 prosent ikke direkte er knyttet til informasjonssikkerhet, men omhandler for eksempel fysiske skader (HMS), manglende IKT-utstyr og saksbehandlingsfeil. Det er tannhelsetjenesten og skolene som har meldt inn flest avvik.

Figur 4. Innmeldte avvik innen informasjonssikkerhet og personvern perioden 01.01.17-08.06.2021



Det ble i 2020 meldt inn flere avvik enn i tidligere år. Fram til 8. juni 2021 har det blitt meldt inn 44 avvik. I avvikssystemet legges det til ulike avvikskategorier. Det er en overvekt av avvik under «annet». Her finner vi en del saker som gjelder dårlig lydisolasjon som fører til deling av konfidensiell informasjon med utenforstående. De aller fleste avvik er lukket med tiltak. Men det er seks avvik som fortsatt til saksbehandling, et fra 2019, to fra 2020 og tre nylige fra 2021.

Tabell 3. Type avvik meldt inn i QM+[15]

Type avvik	2017	2018	2019	2020	2021 (per 08.06. 21)	Totalt
Annet	17	21	8	20	7	73
HMS	6	2	14	10	10	42
Teknisk drift	10	6	7	16	3	42
Forsendelsesfeil			7	18	12	37
Sensitive personopplysninger	12	7	1	1		21
Feil i tilgangskontroll	1		4	10	7	22
Personopplysninger	6	11				17
Feilpublisering av personopplysninger på internett/intranett			2	5	3	10
Mistet/gjenglemt dokumenter/utstyr			4	2	1	7
Datainnbrudd eller hacking				3	1	4
Totalsum	**52**	**47**	**47**	**85**	**44**	**275**

De 21 avvikene om sensitive opplysninger handler for det meste om feilsending av sensitive opplysninger innad i organisasjonen, men det er også noen tilfeller hvor privatpersoner har fått tilsendt sensitive opplysninger om andre. Ellers er det i denne kategorien flere avvik innen manglende lydisolering, ulåste PC'er og ulåst dør.

Siden 2018 har ni avvik blitt meldt inn til Datatilsynet. Tre av sakene gjelder sikkerhetshull og teknisk svikt hos leverandører i VIGO IKS og Visma InSchool. De andre sakene gjelder forsendelsesfeil av sensitive opplysninger og hendelser hvor sensitive opplysninger har vært tilgjengelige for uvedkommende.

Avvik i 2021

Fram til 8. juni er det meldt inn 44 avvik innen informasjonssikkerhet/personvern, men her finner vi blant annet ti feilmeldte HMS-avvik. 12 av avvikene er markert som forsendelsesfeil, hvorav alle er lukket med tiltak. To av sakene er markert med høy prioritet: I det ene avviket ble

[15] Kategorier i tabellen er laget ut ifra innholdet i avviket i QM+.

sensitive helseopplysninger sendt i e-post til intern firmapost. Dette ble oppdaget og opplysningene slettet før noen hadde leste e-posten. Leder i aktuell enhet skriver i avviket:

> *«[…] Det vi har lært i denne saken er at vi skal melde inn saken umiddelbart og ha en dialog med personvernombudet hvis vi er i tvil om den skal meldes Datatilsynet. Kommunikasjonen mellom avdelingsleder og mottaker på firmapost ble tolket av avdelingsleder at dette ikke var nødvendig*. […]»

I den andre saken er karakterutskrift med navn og fødselsdato sendt til feil student via Elements (arkivsystem). Studentene dette gjaldt ble kontaktet per telefon. Studenten som fikk karakterutskriften ble bedt om å slette denne, mens den andre studenten ble informert om avviket. I meldingen står det også at skolens merkantile avdeling vil revidere eksisterende rutine for utlevering av dokumentasjon.

De resterende sakene for 2021 handler om tilgangskontroll, feilpublisering og annet. To av sakene har høy prioritet: Den ene ble meldt inn som mulig datainnbrudd, men ifølge avdelingssjef for Digital Utvikling var dette ikke et datainnbrudd og den ble håndtert som en personalsak. I den andre saken har en lærer fått tilgang til fagsamtaler i Visma InSchool som lærer ikke skal ha tilgang til. I undersøkelsen av saken ble det oppdaget at dette avviket også gjaldt andre lærere. I avvikssystemet står det at saken er løst av Visma to uker etter avviket ble meldt inn av lærer.

6.4 PRAKSIS FOR AVVIK - ARKIV SENTRALADMINISTRASJONEN

Dokumentsenteret oppdager daglig avvik i arkivsystemet Elements på ting som feil i skjerming og tilgangskode når de kvalitetssjekker. Dokumentsenteret har ikke praksis for å melde inn slike avvik i QM+. Når et slikt avvik er oppdaget tar dokumentsenteret en vurdering; hvis det er saksbehandlere som gjennomgående sender dokumenter feil, sendes det e-post med veiledning om riktig måte å gjøre det på. For saksbehandlere som gjør en «glipp» en gang iblant, pleier dokumentsenteret å rette opp feilen selv uten å informere saksbehandler. En informant påpeker at terskelen for å melde avvik i QM+ er for høy når det gjelder avvik i Elements.

6.5 AVVIKSTEAMET FOR VISMA INSCHOOL (VIS)

Med innføring i VIS ble det opprettet et eget avviksteam med opplæringsdirektør, prosjektleder for VIS, ledere i avdeling for digital utvikling og opplæringsseksjon og personvernombudet. Avviksteamet har fått opplæring av personvernombudet. Avviksteamet har behandlet avvik meldt inn av skolene. Behandlingen har vært å diskutere avvik og problemstillinger i fellesskap og melde avvik i QM+ og til datatilsynet. I implementeringsfasen av VIS har det blitt oppdaget avvik knyttet til tekniske løsninger i VISMA. Ifølge informant har det vært nødvendig med eget avviksteam for VIS som samler kompetansen fra de ulike avdelingene.

6.6 PRAKSIS FOR AVVIK PÅ SKOLENE

De fire skolene revisjonen besøkte hadde alle meldt inn avvik innen informasjonssikkerhet og personvern i QM+ i perioden 01.01.2017-08.06.2021. Et flertall av avvikene er derimot meldt inn

under feil kategori, som at fysisk skade i gymtimen blir lagt inn som personvernsavvik heller enn HMS.

Det generelle inntrykket ut ifra intervjuer med både ledelse og ansatte på skolene er at alle vet hvordan avvik meldes inn, men at dette i liten grad gjøres. Flere opplever at avvik tas opp direkte med leder eller andre, uten at dette legges inn i avvikssystemet. Denne praksisen gjelder også HMS-avvik. Avvik av teknisk og driftsmessig art blir gjerne tatt muntlig med vaktmester. På en skole er HMS-avvik lagt inn i egen intern HMS-plan heller enn i QM+.

Flere av skolene har tatt opp praksis rundt avviksbehandling på fellesmøtes med lærere. Flere av intervjuobjektene sier at QM+ er lite brukervennlig og at en tidsmessig ikke prioriterer å legge inn avvik.

6.7 TILTAK

I QM+ legges det inn tiltak knyttet til avviket. Tiltaksskjemaet inneholder punkter som jobbeskrivelse, tidsfrist, kostnad og status. Ut ifra alle 275 innmeldte avvik har revisjon trukket fram 170 som av innholdet kan relateres til informasjonssikkerhet og personvern. Av disse er:

- 159 avvik tiltaksbehandlet og lukket
- Tre avvik fra 2020-2021 venter på tiltaksbehandling. Alle disse handler om manglende lydisolering
- To avvik er markert som avvist
- Seks avvik fra 2019-2021 har status «sendt til saksbehandler» og har ikke tilknyttet tiltak

En informant peker på at tiltak og læring i etterkant av avvik fort blir glemt og at tiltak i større grad må følges opp.

6.8 VURDERING

Fylkeskommunen har eget avvikssystem (QM+) som alle informanter revisjonen har intervjuet er godt kjent med. Det finnes flere rutiner for hvordan avvik skal behandles i organisasjonen og for melding til Datatilsynet. Flere av rutinene inneholder mye av den samme informasjonen. Overlappende rutiner gjør det uklart hvilke rutiner som skal følges. Det er en generell oppfatning blant informantene at terskelen for å melde inn avvik i QM+ er for høy. Personvernombudet sier sin årsrapport at det er behov for opplæring og bevisstgjøring rundt avviksbehandling og peker på hvilket ansvar lederne har for å skape kultur for å melde avvik. Datatilsynet har ifølge informant påpekt at fylkeskommunene generelt melder inn for få avvik.

Siden 2017 er det meldt inn 275 avvik i kategori «informasjonssikkerhet». En gjennomgang av innholdet i avviket viser at mange handler om HMS-avvik som for eksempel fysisk skade i gymtimen. Forsendelsesfeil er en gjenganger i avvik som er meldt inn. De aller fleste avvik er lukket med tiltak, men det det er også avvik helt fra 2019 som fortsatt er under saksbehandling.

Det er meldt inn 21 avvik knyttet til sensitiv informasjon, de fleste av disse handler om feilsending, manglende lydisolering, ulåste PC'er og ulåst dør.

Fylkeskommunen har egen årlig rapportering på avvik i QM+. En informant at sier at det burde vært mer kontroll på hvordan tiltak jobbes med i etterkant.

Informantene revisjonen har snakket med forteller at avvik ofte ikke meldes inn i QM+, men gjerne tas opp direkte med den det gjelder eller leder. Dokumentsenteret avdekker stadig avvik i arbeid med kvalitetssjekk av offentlig postliste. Slike avvik blir ordnet direkte av arkivar. Saksbehandlere som stadig gjør feil på for eksempel skjerming blir kontaktet for veiledning i riktig bruk. Det er ikke praksis for å melde slike feil i QM+.

Innføring av nytt skoleadministrativt system Visma InSchool har ført til flere avvik knyttet til teknisk løsning hos leverandør. Det er positivt at fylkeskommunen har nedsatt et eget avviksteam for VIS som samler kompetansen fra ulike avdelinger. Erfaringer fra gruppen viser at det å løfte avvik og problemstillinger i fellesskap øker kvaliteten i avviksbehandlingen.

- Fylkeskommunen bør sette inn tiltak for å senke terskelen for innmelding av avvik

7 BEREDSKAP

Problemstilling: Hvor mange ganger har fylkeskommunen de siste fire årene opplevd alvorlige cyberangrep eller alvorlige driftsforstyrrelser ved fylkeskommunale nett, programmer eller e-postsystemer? Og har fylkeskommunen reserveløsninger som er raskt tilgjengelig og dekkende for behovene? Har fylkeskommunen en tilstrekkelig plan for å håndtere bortfall av kritiske systemer?

7.1 REVISJONSKRITERIER

Informasjonssikkerhet handler om å ivareta tilgjengeligheten til informasjonen som behandles. Cyberangrep og driftsforstyrrelser hindrer tilgjengeligheten og kan føre til virksomheten ikke får utført de oppgavene som skal gjøres. Cyberangrep er kriminelle handlinger som gjennom virus og hacking kan skade og forstyrre datasystemer. Dataangrepene blir stadig mer avanserte og målrettete. Og selv om sannsynligheten for angrep er lav er ofte konsekvensene store ved at sensitive opplysninger kan havne i feil hender Slike ytre trusler kan være økonomisk motivert. Driftsforstyrrelser er ikke forårsaket av ondsinnede ytre faktorer, men kan gi store konsekvenser ved at f.eks. nedetid på kritiske systemer.

Ved dataangrep og driftsforstyrrelser kan det være nødvendig med reserveløsninger. Sikkerhetskopi av viktig informasjon er også sentralt i arbeidet etter bortfall av systemer. Ifølge Digitaliseringsdirektoratets veileder for internkontroll skal gjennomgang av beredskap være en del av ledelsens styring og gjennomgang. Veiledere sier også at beredskap også må omfatte informasjonssikkerhet.

Offentlige virksomheter (forvaltningsloven § 1) er pålagt å utføre systematisk arbeid med informasjonssikkerhet. All informasjonsbehandling som offentlige virksomheter har ansvar for skal etter Forvaltningsforskriften § 15 etablere mål og strategi (sikkerhetsmål og sikkerhetsstrategi) for informasjonssikkerhet i virksomheten, som skal danne grunnlaget for et tilfredsstillende system for internkontroll. Krav om beredskapshåndtering i fylkeskommunen er beskrevet i informasjonssikkerhetshåndboken. Det er avdelingssjef for digital utvikling som har ansvar for «utarbeidelse av beredskapsplaner for håndtering av hendelser knyttet til informasjonssikkerheten». Videre i informasjonssikkerhetshåndboken står det at «Beredskapsplaner er utarbeidet både når det gjelder digitale løsninger og arkivrom i sentraladministrasjonen. Disse gjennomgås årlig. Skoler og foretak har ansvar for å utarbeide egne beredskapsplaner.»

Revisjonskriteriet
• Fylkeskommunen skal ha oppdatert beredskapsplan for informasjonssikkerhet • Fylkeskommunen bør ha rutiner for sikkerhetskopiering • Det skal være reserveløsninger som er raskt tilgjengelig og dekkende for behovet.

7.2 CYBERANGREP OG DRIFTSFORSTYRRELSER

Informanter fra digital utviklingsavdeling forteller i intervju at fylkeskommunen ikke har opplevd alvorlige cyberangrep de siste fire år, men mulige cyberangrep er en daglig trussel som stanses av ulike tiltak. Cyberangrep som blokkeres har ført til mindre driftsforstyrrelser som forbigående tregt internett. Skolene bekrefter i intervju at det har vært driftsforstyrrelser i form av tregt internett. En skole opplevde at internett var nede store deler av en arbeidsdag. Men stort sett er driftsforstyrrelsene små og skolene sier at det generelt har vært lite nedetid på tjenestene.

Fylkeskommunen har opplevd driftsforstyrrelser som ikke har vært forårsaket av cyberangrep. Avdelingsleder for digital utvikling forteller i intervju om et brudd på internettlinjen ved en av fylkets tannhelseklinikker som var forårsaket av et gravingsuhell, men er usikker på om det er mindre enn fire år siden dette skjedde.

I avvikssystemet er det de siste fire årene meldt inn fire avvik innen datainnbrudd og hacking. Avdelingssjef for digital utvikling opplyser i e-post at disse avvikene ikke førte til faktisk datainnbrudd eller hacking og beskriver årsak til avvikene:

- To av avvikene gjelder forsøk på direktørsvindel. Slike hendelser er ganske vanlige, og det er ikke normal prosedyre å melde inn disse avvikene. Fylkeskommunen har tiltak for å unngå slike hendelser i form av tekniske sikkerhetsløsning i e-post og ved å informere ansatte om å være oppmerksomme rundt slike henvendelser på e-post.
- Det tredje avviket er fra 2020 og gjaldt en e-postkonto som automatisk videresendte til privat e-post. Avviket er håndtert internt på aktuell enhet. Dette avviket handler mest sannsynlig om videresending av jobb-e-post til egen privat e-postadresse. Det vises til at bruk av privat e-postadresse har vært en diskusjon i avdelingene. I ny informasjonssikkerhetsinstruks står det nå spesifikt at ansatte skal bruke fylkeskommunens e-post til jobb og ikke videresende e-post til privat e-postkonto.
- Det siste avviket gjald en fiktiv lærerkonto i Itslearning i 2021. Saken ble meldt inn som mulig hackingsforsøk, men i behandling av avviket ble saken endret til en personalsak som nå er ferdig håndtert.

Ifølge informasjonssikkerhetshåndboken skal det være utarbeidet beredskapsplan for digitale løsninger og arkivrom i sentraladministrasjonen som gjennomgås årlig. Informanter som er intervjuet, forteller at fylkeskommunen ikke har noen beredskapsplan og at det i liten grad er skriftlige rutiner innen IT-sikkerhet. Digital utviklingsavdeling har ikke gjennomført egne beredskapsøvelser. Det blir påpekt at avdelingen har sikkerhetstiltak og praksis for å sikre de digitale løsningene, men at en mangler skriftliggjorte rutiner på dette arbeidet. Avdeling for digital utvikling oppgir at de har følgende sikkerhetstiltak:

- Fylkeskommunen har brannmursikring som kontinuerlig stanser angrep.
- IT- og internettleverandørene som fylkeskommunen kjøper tjenester av har egne sikkerhetstiltak som stanser angrep. Microsoft og internettleverandør har system for å varsle IT-avdelingen hvis det oppstår forstyrrelser.
- Enheter i fylkeskommunen er sikret mot ondsinnede nettsteder og e-postkontoer

- Fylkeskommunens enheter har eget nettverk som ikke private PC'er kan koble seg opp mot. Dette inkluderer privateide PC'er som videregående elever bruker, som da har eget nettverk.
- Nasjonal sikkerhetsmyndighet (NSM), PST og Kripos har varslingstjeneste når de ser uvanlig trafikk eller hendelser.
- To-faktor pålogging for ansatte når en ikke er påkoblet fylkeskommunens nettverk.
- IT-avdelingen har kontroll på de ansattes PC'er ved blant annet bruk av virusskanning.
- IT-avdelingen har mulighet til å fjernstyre oppdateringer på PC'er, fjerne programvarer og tilbakestille (retanke) PC'er.
- Det er system for automatisk oppdatering av ansattes PC'er.
- Det er sperret for tilgang til fylkeskommunens systemer fra enkelte land.
- IKT-avdelingen har enkelte rutiner, som for eksempel rutine for «Ransomware» på filservere.

Ifølge informanter er systemene fylkeskommunen bruker godt sikret mot angrep. De viser til bruk av oppdaterte programvarer fra store linjeleverandører som Microsoft som har en rekke egne sikkerhetstiltak. Slik sett er ikke fylkeskommunen «alene» om å ha et beskyttelsesvern mot cyberangrep. Men i intervjuer påpekes det at det er den enkelte ansatt som utgjør den største trusselen for cyberangrep og sikter spesielt til svindel og forsøk på angrep gjennom e-post. Sikkerhetstiltakene i e-postsystemet stopper ikke alle trusler. Ansatte har blant annet blitt utsatt for direktørsvindel fra e-postkontoer som ligner på kjente e-postadresser i fylkeskommunen. For å unngå cyberangrep og svindelforsøk er fylkeskommunen avhengig av at de ansatte har tilstrekkelig kompetanse og at de følger informasjonssikkerhetsinstruksen. Flere av intervjuobjektene forteller om svindelforsøk på e-post, men at ansatte har gjennomskuet disse enten på egenhånd, ved hjelp fra kollegaer eller fra IT-avdelingen.

Fylkeskommunen har bevisst valgt en «åpen» PC som tillater at ansatte selv kan installere programvarer. Avdelingsleder for digital utvikling begrunner dette med at ansatte uansett vil laste ned programmer selv. Og med en «lukka» PC kan det bli situasjoner hvor ansatte finner egne løsninger, som å bruke privat PC for å installere programmer. Private PC'er har ikke samme beskyttelsesvern mot dataangrep som ansattes PC'er og utgjør derfor en større trussel mot dataangrep. Det er en pågående diskusjon rundt «åpen» eller «lukka» PC i nettverk for IT-ledere i fylkeskommunene. NSM anbefaler «lukka» løsning og avdelingsleder for digital utvikling forteller at et annet fylke skal nå gå over fra «åpen» til «lukka» PC. Rogaland Fylkeskommune har ikke risikovurdert løsningen med «åpen» PC.

7.3 RESERVELØSNING OG SIKKERHETSKOPIER

Informant forteller i intervju at sentraladministrasjonen har reserveløsninger og gjør sikkerhetskopiering, men at dette arbeidet ikke er skriftliggjort i rutiner og beredskapsplan. Informasjonssikkerhetshåndboken viser til en rutine for sikkerhetskopiering, men informant gjelder denne kun for tannhelsen.

På e-post og i intervju vises det til at fylkeskommunen har skallsikring, batteri og dieselaggregat. Viktige tjenester er duplisert og det er to separate datarom i sentraladministrasjonen. Datarommene fungere sådan som reserveløsninger for hverandre slik at den ene tar over hvis det andre settes ut av spill.

IKT-avdelingen gjennomfører offline sikkerhetskopi og egen sikkerhetskopi av Microsoft 365 kjøres automatisk daglig. Hvis et dataangrep fører til at fylkeskommunen må gjenopprette alle systemer vil de ansatte i verste fall miste informasjon som ble lagret siste døgn. Hvis alle systemer må gjenopprettes må IT-teknikere tette eventuelle sikkerhetshull og «retanke» alle PC'er. Avdelingsleder for digital utvikling anslår at et verst tenkelig scenario kan føre til bortfall av systemer i en ukes tid, men at dette er veldig avhengig av type dataangrep.

7.4 VURDERING

Fylkeskommunen har ikke opplevd alvorlige cyberangrep eller driftsforstyrrelser de siste fire årene. Fylkeskommunen har et forsvar mot cyberangrep som består av tekniske innretninger og rutiner. Mange viktige sikkerhetstiltak ligger også innebygd hos de store linjevereandørene.

Fylkeskommunes reserveløsninger er separate datarom som kan ta over for hverandre. Det gjennomføres også daglige sikkerhetskopier av Microsoft 365. Sikkerhetskopiering hindrer at informasjon går tapt ved cyberangrep eller andre årsaker til bortfall av systemer. Men i slike tilfeller kan det ta noe tid ettersom IT-personell må tette sikkerhetshull og «retanke» ansattes PC'er manuelt før en kan starte systemene igjen. Hvor lang tid en slik operasjonen vil ta er avhengig av type angrep. Det er ikke utenkelig med bortfall av systemer i en uke ved et stort angrep.

Modenhetsrapporten viser til at fylkeskommunen mangler skriftlige rutiner teknisk sikkerhet og beredskapsplan. Ansatte i IKT-avdelingen bekrefter at slike rutiner mangler, men at det IKT har tiltak som sikrer fylkeskommunen mot cyberangrep. IKT-avdelingen har heller ikke gjennomført noen beredskapsøvelser.

Revisjonen har følgende anbefalinger til fylkeskommunen:

- Fylkeskommunen bør lage rutiner for IKT-sikkerhet og beredskapsplan

8 ROS-ANALYSE FOR IKT-SIKKERHET

Problemstilling: «Er ROS-analysen for IKT-sikkerhet i fylkeskommunen oppdatert og dekkende?»

8.1 REVISJONSKRITERIER

Ifølge kommuneloven § 25-1 skal internkontrollen tilpasses virksomhetens risikoforhold. Dette gjelder også for den delen av internkontrollen som er rettet mot informasjonssikkerhetsområdet[16].

Personvernforordningen artikkel 24, 25, 32 og 35 stiller krav til at behandlingsansvarlig og databehandler vurderer risiko ved behandling av personopplysninger. Etter artikkel 32 skal det gjennomføres risikovurdering før nye løsninger tas i bruk, ved endringer og ellers bli regelmessig oppdatert[17]. Digitaliseringsdirektoratet[18] beskriver følgende trinn i risikovurderinger:

1) Risikoidentifisering: Her identifiseres mulige hendelser som kan føre til at personopplysninger ikke blir behandlet korrekt.

2) Risikoanalyse: Potensielle hendelser blir analysert etter sannsynligheten for at det skjer og for hvor stor konsekvens hendelsen vil ha for personvernet. Ut ifra sannsynlighet og personvernkonsekvens settes det et risikonivå for hendelsen.

3) Risikoevaluering: Evalueringen skal si noe om hvilke risikoer som skal håndteres og i hvilken rekkefølge.

Risikovurderingen identifiserer tiltak som må gjøres for å oppnå et egnet sikkerhetsnivå. Tiltakene kan være både av teknisk eller organisatorisk art.

Revisjonskriterier
• Fylkeskommunen skal ha en oppdatert ROS-analyse for informasjonssikkerhet • ROS-analysen skal identifisere risiko ved bruk av IKT-utstyr i fylkeskommunen

[16] eForvaltningsforskriften § 15
[17] Veiledning om DPIA | Datatilsynet
[18] Hva er risikovurdering? | Digitaliseringsdirektoratet - Difi

8.2 RISIKOANALYSE

Gjeldende ROS-analyse for informasjonssikkerhet ble utarbeidet i 2013. ROS-analysen er rettet mot internett-tilgang for videregående skoler.

Av modenhetsrapporten[19] fremgår det at fylkeskommunen ikke har funnet en enhetlig måte å drive med risikostyring på og det ikke gjennomføres regelmessig risikovurdering for kritiske systemer. Avdelingssjef for digital utvikling opplyser at det skal gjennomføres ny ROS-analyse for IKT-sikkerhet i etterkant av forvaltningsrevisjonen.

8.3 VURDERING

Gjeldende ROS-analyse for IKT-sikkerhet gjelder for de videregående skolene og er ikke dekkende for bruk av IKT-utstyr i alle fylkeskommunens enheter. Ettersom ROS-analysen er fra 2013 er den ikke oppdatert ut ifra nye lovkrav innen personvern og nye sikkerhetstrusler innen informasjonssikkerhet.

Revisjonen anbefaler at fylkeskommunen lager en ny ROS-analyse som dekker IKT-sikkerhet for hele fylkeskommunens virksomhet.

[19] Datert 13.03.20

VEDLEGG

Dokumenter i rammeverk for informasjonssikkerhet og personvern:

Mappe	Dokument	Sist revidert (forrige revidering)
Informasjonssikkerhetshåndbok	Sikkerhetsorganisasjon	15.07.21 (20.09.19)
	Sikkerhetsstyrets gjennomgang	15.07.21 (16.03.15)
	Sikkerhetsmål	15.07.21 (04.04.17)
	Sikkerhetsstrategi	15.07.21 (04.04.17)
	Partnere og leverandører	15.07.21 (04.04.17)
	Beredskapsplanlegging	15.07.21 (10.04.15)
	Behandlingsprotokoll	16.07.21
	Risikovurdering	16.07.21 (10.04.15)
	Databehandleravtale	16.07.21
	DPIA	16.07.21
	Avvikshåndtering	15.07.21 (10.04.15)
	Informasjonssikkerhetsinstruks-ansatte	22.04.21
	Informasjonssikkerhetsinstruks-leder	26.05.15
	Dokumenthåndtering	05.04.17
	Egenkontroll	10.04.15
Vedlegg til informasjonssikkerhetshåndboken	Oversikt over fylkeskommunens informasjonssystemer	04.04.17
	Skjema for informasjonssikkerhetsinstruks - ansatte	21.04.21
	Skjema for informasjonssikkerhetsinstruks - leder	09.02.15
	Sjekkliste for leder når ansatt slutter	Ingen dato
	Skjema for egenkontroll	Ingen dato
	Oversikt over behandlinger av personopplysninger i fylkeskommunen	01.02.13
	Rutiner for sikkerhetskopiering	05.04.17
	Rutiner for sikker bruk av e-post	19.05.20
	Risikovurdering - infosikkerhet	Ingen dato
Anskaffelser	Mal- Arbeidsbok for risikovurdering	30.04.21
	Mal for utarbeidelse av behandlingsprotokoll	Ingen dato
	Rammeverk og retningslinjer for risikostyring	01.05.21

	Rutine for databehandleravtale	28.04.21
	Rutine – it-løsninger og anskaffelser	17.03.21
	Rutine for personvernkonsekvensvurdering DPIA	20.12.21
	Sjekkliste for samtykke	Ingen dato
	Skjema for systemer med arkivverdig informasjon	Ingen dato
	Veileder for utfylling av behandlingsprotokoll	01.05.21
	Veileder for Digdirs databehandleravtalemal	01.07.21
Avvik og rutiner	Mal for berettiget interesse – art 6	Ingen dato
	RFK Retningslinje brudd på personopplysningssikkerheten	28.08.20
	Rutine for filming, strømming og lydopptak	14.12.20
	Rutine for oversendelse av personopplysninger pr e-post	14.20.20
	Rutine – Innsyn i egne personopplysninger	20.12.21
Lagring og klassifisering av dokumenter	Lagringsveileder lang versjon	01.06.21
	Lagring og dokumentklasser kort	Ingen dato

Kilder

Intern sikkerhetsrapport (modenhetsanalyse utarbeidet av TietoEVRY) fra 2020
Ansvar og myndighet i Rogaland fylkeskommune
Årsrapport for informasjonssikkerhet 2019
Årsrapporter for avvik 2019 og 2020
Informasjonssikkerhetshåndbok med tilknyttede rutiner
Arbeidsreglement
Risikovurderinger og DPIA
Informasjonssikkerhetsinstruks
Avviksrapporter 2017-2021
Digital strategi 2020-2024
Referat møter i ressursgruppen for informasjonssikkerhet 2016-2018
Anskaffelsesstrategi 2021-2025
Rutiner for anskaffelser

Informanter

Personvernombud
Spesialrådgiver internkontroll
Digitaliseringsrådgiver
Fagleder dokumentsenter
Fagleder IT-avdelingen
Rådgiver i seksjon for opplæring i skole
Prosjektleder Visma InSchool (VIS)
Avdelingsleder digital utvikling
Fagleder IT-avdelingen
Innkjøpsleder

Skolebesøk på fire videregående skole. Hvert besøk inneholdt:
Gruppeintervju med rektor, administrasjonsleder og kontaktperson for VIS[20]
Enkeltintervjuer med to kontaktlærere, en kroppsøvingslærer, en sosialpedagogisk rådgiver og skolearkivar.

[20] På et av de fire gruppeintervjuene var ikke kontaktperson for VIS til stede.