Vestland fylkeskommune

Strategisk utvikling og digitalisering
Notat

	2020/75692-6
Saksnr:	Anne-Kjersti Stavø
Saksbehandlar	Stenehjem, Edvard Philo
Dato:	Winge Målsnes
	19.08.2021

Til: Kontrollutvalet

Frå: Fylkeskommunedirektøren

Handlingsplan - forvaltningsrevisjon informasjonstryggleik

Fylkeskommunedirektøren viser til vedtak i sak «PS 23/21 Handlingsplan - Forvaltningsrevisjon informasjonstryggleik». Det vart lagt fram ein prioritert handlingsplan til kontrollutvalet i denne saka. Handlingsplanen var basert på revisjonen sine tilrådingar.

Som oppfølging av forvaltningsrevisjonen, er det nedanfor kommentert på kvar av tilrådingane. Arbeidet med IKT-sikkerheit har bore preg av tett samarbeid med midlertidig personvernombod, hyppige risikoanalysar, og prosjektrettleiing på for eksempel Visma InSchool prosjektet. Det er viktig å nemne at arbeidet med IKT-sikkerheit vil bli avbrote i nokre månader då noverande IKT-sikkerheitsrådgjevar har sagt opp stillinga si frå slutten av september. Personvernombod sa opp stillinga si tidlegare i år, og dåverande personvernrådgjevar har midlertidig overtatt som personvernombod.

1. Fylkeskommunen sitt styringssystem vert gjort ferdig og implementert i organisasjonen, og som del av dette sikre at:

a) ansvarsforhold knytt til informasjonstryggleik vert gjort kjend og etterlevd av dei tilsette
   a. **Løysing:** Leselister i kvalitetssystemet til alle tilsette med obligatoriske dokument. Dette ligg klart i kvalitetssystemet og er kommunisert ut via intranett, e-post til leiarar og tilsette, samt teams oppslag. Det har og vorte presentert i Vestland sitt kvalitetsforum og nemnt på statusmøte for Strategisk utvikling og digitalisering. Dette bør vere ein del av ei «startpakke» for alle nye tilsette. Det er og planlagt for nasjonal sikkerheitsmånad.
b) rutinar for informasjonstryggleik vert gjort ferdige, kjende og etterlevd av dei tilsette
   a. **Løysing:** Sjå over.
c) det vert gjennomført tilstrekkeleg kontroll og etterprøving av informasjonstryggleiken
   a. **Løysing:** Det er allereie utført sårbarheits- og penetrasjonstest av Vestland fylkeskommune sine tenester tilgjengeleg via nett (on-prem). Nettfiskeforsøk vil også vere etterprøving av informasjonstryggleik, og vi får jamlege scanninger av VLFK tenester med forslag til betring. I samarbeid med personvernombod har vi òg gjennomgått personvernprotokollar frå alle vidaregåande skular, som del av internrevisjon.

2. Ansvar og rutinar for å hindre uautorisert innsyn i konfidensielle opplysningar er utfyllande, tydelege og blir etterlevd, og som del av dette gjer tiltak for at tilsette:

a) praktiserer trygg bruk av e-post, t.d. gjennom nettfiskeforsøk
   a. **Løysing**: Dei tilsette får e-læring via e-post, men plattforma kan og nyttast til nettfiskeforsøk. Om lag 50% av tilsette har teke e-læringa som er sendt ut og Vestland må vurdere om denne avtalen skal fortsette eller om Vestland skal stå utan noko opplæring. E-

læringa har blitt informert om i fleire omgangar, via intranett, teams, e-post til alle tilsette, e-post til leiarar ogvia eige intranettområde.

b) nyttar sikker sone ved lagring av konfidensielle opplysningar
   a. **Løysing**: Sikker sone og dedikerte fagsystem skal nyttast allereie ved lagring av konfidensielle opplysingar, men det er behov for fleire løysingar til handsaming og sending av konfidensielle opplysingar. Utredning av dette behovet er i gang.

c) kryptere konfidensielle opplysningar som ikkje er lagra i sikker sone
   a. **Løysing**: Det er utarbeida ei retningsline for korleis ein gjer dette, som er tilgjengeleg i kvalitetssystemet. Dette heng og saman med at det kan vere behov for fleire eller andre løysingar for handsaming av konfidensielle opplysingar.

3. Ansvar og rutinar for å hindre uautorisert tilgang til informasjonssystema er utfyllande, tydelege og blir etterlevd, og som del av dette gjer tiltak for å:

a) sikre at tilsette har nødvendige tilgangar
   a. **Løysing**: Vestland fylkeskommune har allereie tilgangskontroll og nytt dokument er ute i kvalitetssystemet på dette punktet. Praksis må gjennomgåast grundig og unntak i tilgangskontroll er i hovudsak relatert til fagsystem. Dette heng saman med systemforvaltning i VLFK, der systemeigar er ansvarleg for tilgangskontroll og revisjon av tilgangar til eige system.

b) sikre at tilsette ikkje har tilgangar utan at det er tenestleg behov
   a. **Løysing**: Det er etablert at ein skal revidere tilgangar jamleg, men dette er nok ikkje iverksett i praksis i verksemda. Dette er eit systemforvaltar/eigar ansvar og det trengs meir undervisning og kommunikasjon rundt dette ansvaret. Systemforvaltning i Vestland er skrive om og tilpassa fleire, nye arbeidsoppgåver og det er sendt inn eit notat om systemforvaltninga i Vestland til avdelingsdirektør Paal Fosdal. Det er derimot eit større arbeid med å gjennomføre denne endringa i heile Vestland.

5. systemeigarar og andre med ansvar knytt til informasjonstryggleik og personvern mottek tilstrekkeleg opplæring
   a. **Løysing**: Alle VLFK tilsette mottek på noverande tidspunkt jamleg e-læring via sin e-post. Det er nok behov for identifikasjon av kvar systemforvaltar/eigar, klare definisjonar av kvar rolle og spesifikk systemforvaltar/eigar-opplæring. Dette heng òg saman med at systemforvaltninga i Vestland på noverande tidspunkt ikkje er tilfredsstillande.

6. det vert utarbeidd tilstrekkeleg med informasjon om informasjonstryggleik til dei tilsette, og sikre at dei tilsette får den naudsynte opplæringa for å kunne ivareta informasjonstryggleiken på ein tilfredsstillande måte.
   a. **Løysing**: Alle VLFK tilsette mottek på noverande tidspunkt jamleg e-læring via sin e-post. Dei nyaste tala frå Junglemap er at ca. 50% har teke e-læringa inntil vidare, som er ei markant betring. I tillegg vert sikkerheit@vlfk.no brukt jamleg der IKT sikkerheitsrådgjevar får spørsmål frå tilsette. I tillegg er to-faktor autentisering for Office365 aktivert for tannhelse og alle tilsette i skulane.

Prioritert tiltaksliste:

1. Systemeigar og systemforvaltar opplæring i rolle, informasjonstryggleik og personvern. Identifisere alle systemeigarar/forvaltarar, utvikle eit opplegg og halde undervisning.
   Nytt dokument for systemforvaltning publisert for alle tilsette og notat sendt til toppleiinga om behov for omorganisering av systemforvaltning i Vestland.
2. I relasjon til fyrste tiltak, vil andre tiltak relatere seg til tilgangskontroll (tilråding 3) då det vil vere eit systemeigar ansvar å sørge for at det er tilgangskontroll og jamleg gjennomgang av tilgangar i sitt system.
   Avhengig av ny systemforvaltning, då tilgangskontroll er eit systemeigaransvar.
3. Implementering av ISMS: Kommunisere ut i organisasjonen at det vil komme obligatoriske dokument som alle skal lese og kjenne til, og sende ut leselister.
   Var kommunisert ut i organisasjonen via fleire kanalar og leiarar, er tilgjengeleg i kvalitetssystemet.

4. Retningsliner for handsaming av konfidensiell informasjon utanom fagsystem ligg i kvalitetssystemet, men kan reviderast og må sendast ut til tilsette. Kan inkluderast i e-læring, men vil være ei løypande prosess drevet av behov (ofte i avdeling for opplæring og kompetanse).
   Vurdering av behovet er framleis undervegs då midlertidig personvernombod og IKT sikkerheitsrådgjevar arbeider med ei kartlegging av informasjonsflyt i avdeling for opplæring og kompetanse, og deretter alle andre avdelingar.
5. Fortsette med PIA-ROS arbeidet, vil også bli delegert som eit systemeigaransvar og vere ei del av undervisninga dei skal ha. IKT-sikkerheitsrådgjevar har ikkje kapasitet til å skulle utføre alle PIA-ROS vurderingar for eldre system.
   Løypande

Tilråding 4 er omhandlar personvern og vil vere personvernombodet, ikkje IKT-sikkerheitsrådgjevar sitt ansvar. IKT-sikkerheitsrådgjevar vil bidra på tiltak til tilråding 4 i sin kapasitet som personvernskoordinator for Strategisk utvikling og digitalisering (SUD).