Vestland fylkeskommune

Strategisk utvikling og digitalisering
Notat

Saksnr:	2020/75692-5
Saksbehandlar	Anne-Kjersti Stavø Stenehjem, Edvard Philo Winge Målsnes,
Dato:	10.02.2021

Til:	Kontrollutvalet
Frå:	Fylkesrådmannen

Oppfølging forvaltningsrevisjon informasjonstryggleik

Fylkesrådmannen viser til vedtak i sak 152/2020 i fylkestinget 15.12.2020, der fylkestinget ber om at det vert laga ein prioritert handlingsplan til kontrollutvalet innan 01.03.2021.

Handlingsplanen er basert på revisjonen sine tilrådingar. Ein meir detaljert, punktvis kommentar på kvar tilråding kjem etter tiltakslista.

IKT-sikkerheitsrådgjevar har laga ei prioritert tiltaksliste nedanfor, for dei tiltaka han vil følgje opp og vere ansvarleg for. Tiltaka er ikkje nummerert for å passe med revisjonen sine tilrådingar, men er nummerert etter korleis IKT-sikkerheitsrådgjevar prioriterer dei. Tiltaka kan inkludere fleire tilrådingar, og skal vere dekkande for alle revisjonens tilrådingar. Revisjonens tilråding nr. 4 omhandlar personvern, og ansvaret for handsaminga av tilrådinga vil falle under personvernombodet.

Prioritert tiltaksliste:

1. Systemeigar- og systemforvaltaropplæring i rolle, informasjonstryggleik og personvern. Identifisere alle systemeigarar/forvaltarar, utvikle eit opplegg og halde undervisning.
   Pågåande januar – mars 2021
2. I relasjon til fyrste tiltak, vil andre tiltak relatere seg til tilgangskontroll (tilråding 3) da det vil vere eit systemeigar ansvar å sørge for at det er tilgangskontroll og jamleg gjennomgang av tilgangar i sitt system.
   Pågåande januar – mars 2021
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.
   Pågåande februar – mars 2021
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 ein løypande prosess drive av behov (ofte i sektoren opplæring og kompetanse).
   Pågåande april – juni 2021
5. Fortsette med PIA-ROS arbeidet, vil også bli delegert som eit systemeigaransvar og vere ein del av kurset dei skal ha. IKT-sikkerheitsrådgjevar har ikkje kapasitet til å skulle utføre alle PIA-ROS vurderingar for eldre system.
   Løypande

Tilråding 4 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). Tilråding 1 -3 og 5 høyrer til under IKT-sikkerheitsrådgjevar sitt ansvar.

Tilrådingar

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.
b) rutinar for informasjonstryggleik vert gjort ferdige, kjende og etterlevd av dei tilsette
   a. **Løysing:** Leselister i kvalitetssystemet til alle tilsette med obligatoriske dokument. Dette ligg klart i kvalitetssystemet.
c) det vert gjennomført tilstrekkeleg kontroll og etterprøving av informasjonstryggleiken
   a. **Løysing:** Allereie utført sårbarheits- og penetrasjonstest av Vestland fylkeskommune sine tenester tilgjengeleg via nett (on-prem). Nettfiskeforsøk vil også vere etterprøving av informasjonstryggleik, og vi kan gjere stikkrevisjon internt.

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 plattformen kan også nyttast til nettfiskeforsøk

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 nok behov for fleire løysingar til handsaming og sending av konfidensielle opplysingar.

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. Må inkluderast i leselister.

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.

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.

4. Krava i personvernforordninga blir etterlevde, og som del av dette:

a) føre protokoll over alle behandlingar av personopplysningar
   a. **Løysing**: Dette vert allereie utført ved anskaffing av nytt system, men det er behov for å gå tilbake og gjere protokoll på eldre system og prosessar.

b) signere databehandlaravtalar med alle fylkeskommunen sine databehandlarar
   a. **Løysing**: Dette skal også gjerne vere gjort ved alle nye avtaler, men det er moglegheit for at det er nokre avtaler utan. Krev at ein tek ei gjennomgang av alle avtaler.

c) gjennomføre risikovurderingar knytt til behandlingar av personopplysningar
   a. **Løysing**: PIA-ROS analyser vert utført jamleg, ved behov i nye anskaffingar eller endringar i tenester og infrastruktur. Det kan vere eksisterande system eller prosessar som ikkje har vorte analysert, krev at ein tek ei gjennomgang av alle system/prosessar.

d) gjennomføre vurdering av personvernkonsekvensar ved behandlingar av personopplysningar med høg risiko

a. **Løysing**: PIA-ROS analyser vert utført jamleg, ved behov i nye anskaffingar eller endringar i tenester og infrastruktur. Det kan vere eksisterande system eller prosessar som ikkje har vorte analysert, krev at ein tek ei gjennomgang av alle system/prosessar.

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.

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.