# Sirdal kommune

**RISIKOVURDERING AV Conexus Companion STAFETTLOGGEN**

Sirdal kommune har gjennomført en risikovurdering av informasjonssikkerhet i forbindelse med innføring og bruk av Conexus Companion Stafettloggen.
Risikovurderingen er foretatt i november 2017, med deltakere fra helse, skole og barnehage.

Vi har tatt for oss potensielle hendelser eller scenario som er vurdert som relevante i forbindelse med oppstart og drift av Conexus Companion Stafettloggen. Vi har hentet informasjon fra Haugesund kommune, som har brukt cxStafettloggen i flere år.

Hovedformålet med risikovurderingen er å avdekke om det er aktuelt å iverksette tiltak for å sikre god ivaretakelse av konfidensialitet, integritet og tilgang til personopplysninger. Herunder at §8, §14 og §28 i Personopplysningsloven blir ivaretatt.

Det kan bli aktuelt å gjennomføre flere risikovurderinger i.f.h.t. bruken av Conexus Companion Stafettloggen.

Hvilken type personinformasjon som Sirdal kommune skal registrere i Conexus Companion Stafettloggen går frem av dokumentet "Stafettloggen – personinformasjon", som ligger som en del av rutinen for bruk av Stafettloggen.  Informasjonen vil være svært saksorientert.

Leverandøren av Conexus Companion Stafettloggen, Conexus, har gitt informasjon om tiltak som er gjennomført for å redusere risikoen for at personopplysninger ikke ivaretas på en tilfredsstillende måte.  De tilfredsstiller høyeste krav til sikkerhetsnivå (nivå 4) ved pålogging, ved å bruke BankID.

Type informasjon som blir registrert, leverandøren sin dokumentasjon av gjennomførte sikkerhetstiltak samt interne rutinebeskrivelser har ført til at risikonivået er vurdert til å være lavt.

Sirdal kommune har vurdert det slik at det ikke er nødvendig å igangsette ytterligere tiltak for å redusere risiko, ut over det som ligger i å sikre at alle aktørene som skal bruke løsningen får nødvendig opplæring.


| | | | | | |
|---|---|---|---|---|---|
| Postadresse: | Besøksadresse: | Telefon: | 38 37 90 00 | Internett: | www.sirdal.kommune.no |
| Rådhuset | Rådhuset, Tonstad | Telefaks: | 38 37 90 01 | E-post: | post@sirdal.kommune.no |
| 4440 Tonstad | | Bank kto.: | 31320700038 | Org.nr.: | 964964165 |

RISIKOVURDERING AV Conexus Companion STAFETTLOGGEN

| Hendelse/Scenario | Sårbarheter | Sannsyn-lighet | Konse-kvens | Eksisterende kontroller | Risiko-nivå |
|---|---|---|---|---|---|
| Stafettholder eller aktør får tilgang til informasjon om barn han/ho ikke skal ha tilgang til | Brukersesjonen i nettleser gir tilgang til alle barn som bruker har tilgang til | Lav | Moderat | Tilgangskontroll sikrer at bruker bare har tilgang til aktuelle barn | Lavt |
| Stafettholder eller aktør sender personinformasjon ukryptert via e-post | Mangelfull kompetanse om håndtering av personinformasjon, og rutiner rundt systemet | Lav | Moderat | Rutinen skal være en sentral del av opplæringen | Lavt |
| Stafettholder eller aktør deler sin påloggings-informasjon med andre | Manglende forståelse for viktigheten av at informasjonen i systemet er konfidensiell | Lav | Alvorlig | 2-faktor autentisering | Lavt |
| Tilgangen til systemet for foreldre blir ikke stengt etter endring i juridisk forhold til barn | Mangelfull kompetanse i administrasjon av tilganger | Moderat | Moderat | Det er stafettholder sitt ansvar å ajourføre tilganger | Lavt |
| Stafettholder gir foreldre tilgang til feil barn | Feil bruk av systemet | Lav | Alvorlig | Det er stafettholder sitt ansvar å ajourføre tilganger | Lavt |
| Personell hos leverandør distribuerer personinformasjon til aktør i usikker kanal | Mangelfull kompetanse om håndtering av personinformasjon, og rutiner rundt systemet | Lav | Moderat | Interne rutiner hos leverandør skal sikre at de tilsatte overholder vedtatt reglement | Lavt |
| Feil i tilgangs-kontrollen til web-applikasjonen gir ikke tilsiktet tilgang til personinformasjon | Programvarefeil.<br>Feil bruk av programvare hos leverandør.<br>Test av programvare | Lav | Moderat | Testrutiner hos leverandør og kommunen sin bruk av Stafettloggen skal raskt avdekke slike feil, slik at risikoen for skade blir minimalisert | Lavt |
| Autorisert bruker i kommunen misbruker tilgang til personinformasjon | Avhengig av tillit til brukere | Lav | Moderat | Ansvaret som følger med tilgangene må presiseres i opplæringen | Lavt |

| | | | | | |
|---|---|---|---|---|---|
| Personell hos leverandør med gyldig tilgang til server misbruker personinformasjon | Avhengig av tillit til personale hos leverandør | Lav | Moderat | Interne rutiner hos leverandør skal sikre at de tilsatte overholder vedtatt reglement | Lavt |
| Ekstern angriper får tilgang til Stafettloggen og/eller infrastruktur | Sikkerhetsopplegget rundt systemet | Lav | Alvorlig | Leverandør har dokumentert høyt sikkerhetsnivå både for basen og for overføring av informasjon | Lavt |
| Manglende tilgang til systemet pga IT-driftsproblem, strømbrudd, brann el.l. | Får ikke tilgang til data i Stafettloggen | Sannsynlig | Lav | Konsekvensene av driftsstans er små | Lavt |
| Oppretting og bytte av Stafettholder | Administrator som oppretter stafettholder har vid tilgang til informasjon i systemet. Viktig å sperre tilgang for gammel stafettholder, og åpne for ny | Lav | Lav | Denne rutinen skal vektlegges i opplæringen | Lavt |
| Arkivrutinen | Rutinen som skal sikre at dokument/informasjon blir journalført, arkivert og lagret i henhold til gjeldende regler | Moderat | Moderat | Denne rutinen skal vektlegges i opplæringen | Lavt |
| Stafettholder registrerer informasjon som ikke er tillatt i.f.h.t. samtykket | Manglende kompetanse hos stafettholder | Lav | Moderat | Ansvaret som følger med tilgangene, skal presiseres i opplæringen | Lavt |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |