

Risiko- og Sårbarhetsanalyse (ROS) - Mal

Vurdering av Curiosa læringsplattform | Revisjonsdato: 29. oktober 2026 | curiosa.no/trust

1. Bakgrunn, systemomfang og Dual-Edition

Dette dokumentet er en veiledende risiko- og sårbarhetsanalyse (ROS) og DPIA-underlag for skoleeiere (kommuner, fylkeskommuner og privatskoler) som tar i bruk Curiosa (curiosa.no), levert av Chromo AS (org.nr. 937 967 675).

Analysen dekker både 100 % Lokal Elevmodus (standard på curiosa.no med 0 writes til skyen, lokal OneDrive-synk og SHA-256-signert Prøve-PDF) og Full Skoleutgave (curiosa.no/full med EU-lagring i Belgia europe-west1 og Feide).

2. Identifiserte risikoområder og risikoreduserende tiltak

Scenario A: Uautorisert innsyn på tvers av elever, klasser eller skoler.

Tiltak: I Lokal utgave lagres 0 elevdata i skyen. I Full skoleutgave isolerer autoritative Firestore Security Rules og Cloud Functions data per skole, klasse og ansvarlig lærer, verifisert av 57 automatiserte sikkerhetstester i CI/CD. Risiko vurdert som: LAV.

Scenario B: Eksponering av personopplysninger eller prompt injection mot språkmodeller (KI).

Tiltak: I Lokal utgave vurderes øvinger 100 % lokalt i nettleseren uten nettverkskall, fritekstfeltet i assistenten er fjernet, og ordbokoppslag blokkerer elevens egne svarfelt (input/textarea) slik at kun lærerens fagtekst slås opp. Ved KI-kall brukes Google Cloud Vertex AI i EU multi-region under Enterprise DPA uten modelltraining. Elevnavn strippes alltid, og innebygd Prompt Injection Guard nøytraliserer usynlig tekst og skjulte overstyringsinstrukser før sensurstøtte. Risiko vurdert som: LAV.

Scenario C: Forsøk på fusk, PDF-manipulasjon eller omgåelse av prøvelås.

Tiltak: Støtte for Safe Exam Browser (.seb med 0 elevsporing), kryptografisk SHA-256-kontrollkode på eksporterte Prøve-PDF-er og daglig rullerende sikkerhets-PIN ved fokusbrudd. Vurderings- og låsefelter er skrivebeskyttet mot elevendring i databasereglene. Risiko vurdert som: LAV.

Scenario D: Manglende sletting av foreldede elevdata.

Tiltak: Automatisk, feiltolerant 2-faset slettejobb fjerner inaktive elever og alle tilknyttede tabeller etter 365 dager i Full skoleutgave, og sanntidsøkter i CuriLive slettes etter 24 timer. Risiko vurdert som: LAV.

3. Personvernkonsekvenser (DPIA-underlag) og Universell utforming

I Lokal utgave behandles ingen personopplysninger om elever i skyen. I Full skoleutgave behandles kun alminnelige personopplysninger i forbindelse med lovpålagt opplæring jf. opplæringslova § 13-1 / § 25-1 (ingen særlige kategorier etter GDPR art. 9 eller fødselsnummer).

Det foretas ingen systematisk overvåking utenfor tidsavgrensede prøvesituasjoner, og det fattes ingen automatiserte enkeltavgjørelser etter GDPR art. 22 (alle KI-vurderinger er veiledende forslag som faglærer kontrollerer og godkjenner).

Sensitive offentlige portaler (ID-porten, BankID, Helsenorge, NAV, Altinn, Skatteetaten) er teknisk blokkert i nettleserutvidelsen.

Universell utforming: Plattformen oppfyller 48 av 48 suksesskriterier i WCAG 2.1 nivå A og AA (dokumentert for uustatus.no).

4. Samlet konklusjon og anbefaling

Curiosa er teknisk og organisatorisk tilrettelagt for å etterleve kravene til personvern, informasjonssikkerhet og universell utforming (WCAG 2.1 AA) i norsk grunn- og videregående opplæring.

Restrisikoen ved pedagogisk bruk og prøveavvikling vurderes som lav og akseptabel. Komplette teknisk dokumentasjon og behandlingsfortegnelse (GDPR art. 30) er tilgjengelig på curiosa.no/trust.