Sikkerhetskrav til leverandører

Dokumentnivå	4
Versjon	1.1
Vedtatt dato	18.01.2023
Godkjenner	NRKs sikkerhetssjef
Dokumenteier	NRKs informasjonssikkerhetsleder
Klassifisering	NRK Åpen
Virkeområde	Leverandører

1. Innledning

1.1	Beskrivelse	Det forventes at leverandører kan oppfylle minimumskravene til informasjonssikkerhet. Dette dokumentet er basert på ISO 27001 Controls og EBU R143 Cybersecurity Recommendation for Media Vendors' Systems, Software & Services.
1.2	Omfang	Kapittel 2 skal fylles ut av leverandører som behandler, får tilgang til, lagrer eller overfører data for NRK. Det samme gjelder for leverandører som gis tilgang til NRKs fysiske lokaler. Kapittel 2 og 3 skal fylles ut av leverandører som tilbyr programvare, mellomvare, maskinvare, plattformer eller andre systemer/komponenter som inngår i NRKs IT-infrastruktur.

2. Organisatoriske krav

Vennligst besvar kravene med J=JA, N=NEI eller N/A=Ikke relevant og begrunn svaret.

Krav	J	N	N/A	Begrunnelse
2.1 Sikkerhetsstyring Leverandøren har en sikkerhets-policy som regelmessig evalueres og holdes oppdatert.				
2.2 Risikostyring Leverandøren identifiser risiko knyttet til tjenesten og sørger for risikoreduserende tiltak.				
2.3 Dataoverføring NRKs data lagres og behandles kun i EU/EØS.				
2.4 Personellsikkerhet Bakgrunnssjekk foretas av alle medarbeidere som er involvert i oppdraget, f.eks. ID og CV-sjekk.				
2.5 Leverandørkjeden Leverandøren tar ansvar for sikkerheten i sin leverandørkjede.				

3. Tekniske krav

Vennligst besvar kravene med J=JA, N=NEI eller N/A=Ikke relevant og begrunn svaret.

Krav	J	N	N/A	Begrunnelse
3.1 Sårbarhetshåndtering Leverandøren har prosedyrer for å for å identifisere og patche sårbarheter.				
3.2 Sikkerhetstesting Leverandøren gjennomfører regelmessig sikkerhetsanalyser, som penetrasjonstest eller sårbarhetsskanning.				
3.3 Hendelseshåndtering Leverandøren har implementert prosedyrer for hendelseshåndtering.				
3.4 Varsling Leverandøren har rutiner for å varsle kunder om datalekkasje eller alvorlige hendelser.				
3.5 Datagjenoppretting Leverandøren har innført og testet rutiner for sikkerhetskopi og planer for gjenoppretting.				
3.6 Tilgangsstyring Leverandøren forsikrer at tjenesten støtter rollebasert tilgangskontroll og Azure AD SSO.				
3.7 Kryptering av data Leverandøren muliggjør kryptering av sensitive data, for både data i ro og i transitt.				
3.8 Sikker utvikling Leverandøren forsikrer at endringer i tjenesten skjer kontrollert gjennom en formell dokumentert prosess.				
3.9 Skille mellom miljøer Leverandøren holder miljøene for drift og test adskilt.				
3.10 Segregering av kundedata Leverandøren sørger for segregering av kundedata ved lagring i delte miljøer.				
3.11 Fysisk sikkerhet Leverandøren har adgangskontroll og fysisk sikring av sine lokaler.				