DEL II-3
SIKKERHETSKRAV TIL LEVERANDØRER

NRK Store Studio, rehabilitering av tak

EA3706/22N

Versjon	1.0
Dato	28.09.2022
Klassifisering	NRK Åpen

Innhold

1 INNLEDNING

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*.

2 OMFANG

Kapittel 3 *«Organisatoriske tiltak»* må 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.

Leverandører som tilbyr programvare, mellomvare, maskinvare, plattformer eller andre systemer/komponenter som inngår i NRKs IT-infrastruktur, må fylle ut både kapittel 3 *«Organisatoriske tiltak»* og kapittel 4 *«Tekniske tiltak»*.

3 ORGANISATORISKE TILTAK

Vennligst besvar følgende utsagn (J=JA, N=NEI eller N/A=Ikke relevant).

#	Beskrivelse	J	N	N/A	Kommentar
1	**Sikkerhetsstyring** Leverandøren har en sikkerhets-policy som regelmessig evalueres og holdes oppdatert.				
2	**Risikostyring** Leverandøren identifiser risiko knyttet til tjenesten og sørger for risikoreduserende tiltak.				
3	**Dataoverføring** NRKs data lagres og behandles kun i EU/EØS.				
4	**Personellsikkerhet** Bakgrunnssjekk foretas av alle medarbeidere som er involvert i oppdraget, f.eks. ID og CV-sjekk.				
5	**Leverandørkjeden** Leverandøren tar ansvar for sikkerheten i sin leverandørkjede.				

4 TEKNISKE TILTAK

Vennligst besvar følgende utsagn (J=JA, N=NEI eller N/A=Ikke relevant).

#	Beskrivelse	J	N	N/A	Kommentar
6	**Sårbarhetshåndtering** Leverandøren har prosedyrer for å for å identifisere og patche sårbarheter.				
7	**Sikkerhetstesting** Leverandøren gjennomfører regelmessig sikkerhetsanalyser, som penetrasjonstest eller sårbarhetsskanning.				
8	**Hendelseshåndtering** Leverandøren har implementert prosedyrer for hendelseshåndtering.				
9	**Varsling** Leverandøren har rutiner for å varsle kunder om datalekkasje eller alvorlige hendelser.				
10	**Datagjenoppretting** Leverandøren har innført og testet rutiner for sikkerhetskopi og planer for gjenoppretting.				
11	**Tilgangsstyring** Leverandøren forsikrer at tjenesten støtter rollebasert tilgangskontroll og Azure AD SSO.				
12	**Kryptering av data** Leverandøren muliggjør kryptering av sensitive data, for både data i ro og i transitt.				
13	**Sikker utvikling** Leverandøren forsikrer at endringer i tjenesten skjer kontrollert gjennom en formell dokumentert prosess.				
14	**Skille mellom miljøer** Leverandøren holder miljøene for drift og test adskilt.				
15	**Segregering av kundedata** Leverandøren sørger for segregering av kundedata ved lagring i delte miljøer.				
16	**Fysisk sikkerhet** Leverandøren har adgangskontroll og fysisk sikring av sine lokaler.				