

Bilag 6 - Sikkerhetskrav til leverandører

Dokumentnivå	4
Versjon	1.2
Vedtatt dato	20.06.2025
Godkjenner	NRKs sikkerhetssjef
Dokumenteier	NRKs informasjonssikkerhetsleder
Klassifisering	NRK Åpen
Virkeområde	Leverandørstyring



1. Innledning

- 1.1 **Beskrivelse** Som en del av NRKs styringssystem for sikkerhet, og generelle sikkerhetsarbeid, forventes at leverandører kan oppfylle NRKs minimumskrav til informasjonssikkerhet. Dette dokumentet er basert på ISO 27001/27002 og EBU R143 Cybersecurity Recommendation for Media Vendors' Systems, Software & Services.
- 1.2 **Omfang** Punktene 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.
- Leverandører som tilbyr programvare, mellomvare, maskinvare, plattformer eller andre systemer/komponenter som inngår i NRKs IT-infrastruktur skal fylle ut de punkter som er relevante for leveransen. Dersom et punkt ikke besvares, skal det angis begrunnelse.

2. Krav

Vennligst besvar kravene med ja eller nei. Utfyllende informasjon bør gis til alle punkter.

#	Krav			
		Ja	Nei	Utfyllende informasjon
1	Generelle sikkerhetskrav			
1.1	Har dere etablert et styringssystem for informasjonssikkerhet og/eller annen sikkerhet?			
1.2	Sikrer dere at egne ansatte og ansatte hos underleverandører er bevisste på og følger styringssystemet?			
1.3	Innehar dere sikkerhetssertifiseringer som f.eks. ISO 27001, SOC2?			
1.4	Er dere kjent med særskilte sikkerhetstiltak i mediebransjen (EBU R143 Cybersecurity Recommendation for Media			

	Vendors' Systems, Software & Services)?			
1.5	Sikrer dere at egne ansatte eller ansatte hos underleverandører oppfyller NRKs krav til bakgrunnssjekk og/eller sikkerhetsklarering, dersom slikt krav er gitt? Hvis ja, beskriv hvordan.			
1.6	Sikrer dere fysisk egen informasjon, egne lokaler og datasentre?			
1.7	Behandler eller lagrer dere data utenfor EU/EØS?			
1.8	Behandler eller lagrer dere data hos eksterne leverandører av skytjenester?			
1.9	Har dere rutiner for å slette informasjon, og destruere eller levere tilbake NRKs informasjon, når oppdraget eller tjenesten er avsluttet?			
2	Risikovurdering og håndtering			
2.1	Utfører dere regelmessige risikovurderinger av deres informasjonssystemer og prosesser?			
2.2	Har dere prosedyrer for å håndtere identifiserte risikoer og sårbarheter?			
3	Tilgangskontroll			
3.1	Har dere mekanismer for å kontrollere tilgang til sensitive data og systemer?			
3.2	Bruker dere flerfaktorausautentisering (MFA) for å sikre tilgang til systemer?			

3.3	Har dere tilpassede rutiner for å administrere tilgangsrettigheter for ansatte og eksterne parter?			
3.4	Holder dere kundedata segregert ved lagring i delte miljøer?			
4	Kryptering og databeskyttelse			
4.1	Bruker dere kryptering for å beskytte data i transitt og ved lagring? Hvis ja, hvilke krypteringsstandarder og teknologier bruker dere?			
4.2	Sikrer dere at krypteringsnøkler håndteres sikkert? Hvis ja, beskriv hvordan.			
5	Overvåking og logging			
5.1	Har dere implementert overvåkingsverktøy for å oppdage mistenkelig aktivitet i sanntid?			
5.2	Opprettholder dere logger over nettverkstrafikk og systemaktivitet?			
5.3	Lagrer dere sikkerhetslogger? Hvis ja, hvor lenge og hvordan sikrer dere loggenes integritet?			
6	Programvareoppdateringer og patching			
6.1	Sikrer dere at all programvare og fastvare er oppdatert med de nyeste sikkerhetsoppdateringene? Hvis ja, hvordan?			
6.2	Har dere en regelmessig patching-prosess for å lukke kjente sårbarheter?			

6.3	Tester dere oppdateringer før de implementeres i produksjonsmiljøet?			
6.4	Sikkerhetstester dere systemer og skytjenester? Hvis ja, hva er frekvensen på slik testing?			
7	Sikkerhetskopiering og gjenoppretting			
7.1	Utfører dere regelmessige sikkerhetskopier av kritiske data og systemkonfigurasjoner?			
7.2	Sikrer dere at sikkerhetskopiene er beskyttet mot uautorisert tilgang? Hvis ja, beskriv hvordan.			
7.3	Har dere testet gjenopprettingsprosesser for å sikre at data kan gjenopprettes raskt og effektivt?			
8	Leverandørforhold			
8.1	Sikrer dere at deres underleverandører oppfyller sikkerhetskravene? Hvis ja, beskriv hvordan.			
8.2	Har dere en prosess for å evaluere og overvåke sikkerhetsytelsen til deres underleverandører?			
8.3	Har dere en prosess for å håndtere sikkerhetshendelser som involverer underleverandører?			
9	Leverandørens tjenesteleveranse			
9.1	Sikrer dere at tjenestenivåavtaler (SLA) inkluderer nødvendige sikkerhetskrav?			

9.2	Overvåker dere at tjenestene leveres i samsvar med sikkerhetskravene?			
9.3	Har dere etablert en prosess for håndtering av sikkerhetshendelser som involverer deres tjenester? Hvis ja, beskriv prosessen.			
10	Endringer i leverandørens tjenester			
10.1	Har dere en prosess for å håndtere endringer i deres tjenester som kan påvirke sikkerheten?			
10.2	Informerer dere kundene om endringer i deres tjenester som kan påvirke sikkerheten?			
10.3	Utfører dere risikovurderinger av endringer i deres tjenester for å sikre at de fortsatt oppfyller sikkerhetskravene?			

3. Endringslogg

3.1	18.01.2023	Sjekkliste etablert
3.2	20.06.2025	Sjekkliste tilpasset forbedret styringssystem, og alle punkter endret.