



DNVs høringsinnspill til forslag til revidert damsikkerhetsforskrift

DNV viser til NVEs høring av forslag til revidert forskrift om sikkerhet ved vassdragsanlegg (damsikkerhetsforskriften), med høringsfrist 15. september 2026. DNV ønsker med dette å gi våre kommentarer til forskriftsforslaget.

Om DNV

DNV er en uavhengig leverandør innen risikostyring og kvalitetssikring med virksomhet i mer enn 100 land og nærmere 16000 ansatte. Selskapet er heleid av *Stiftelsen Norske Veritas* og har siden 1864 vært verdensledende innen teknisk kvalitetssikring av skip (klasseselskap). I tillegg til maritim kompetanse, har DNV i flere tiår testet, sertifisert, og vært teknisk rådgiver innen olje og gass og fornybarsektoren. DNV har lang erfaring med sikkerhetskritisk infrastruktur, risikobaserte regelverk, uavhengig tredjepartsverifikasjon, digital sikkerhet og barrierestyring i energi-, maritim- og infrastruktursektorene.

Overordnet vurdering

DNV støtter hovedretningen i forslaget til revidert damsikkerhetsforskrift. Det er positivt at forskriften moderniseres og i større grad gjøres risikobasert, funksjonsorientert og tilpasset et endret sikkerhets- og risikobilde. DNV mener at en slik utvikling er riktig og nødvendig for å sikre et robust og fremtidsrettet regelverk for vassdragsanlegg.

Samtidig innebærer en mer risikobasert og funksjonsbasert forskrift at krav til dokumentasjon, metodebruk og etterprøvbarhet blir viktigere. Når aktørene gis større ansvar for å velge hvordan krav oppfylles, bør regelverket og tilhørende veiledning gi tilstrekkelig tydelige forventninger til kvaliteten på risikovurderinger, verifikasjon, beredskap og sikring. Dette er avgjørende for å sikre konsistent praksis på tvers av eiere, anleggstyper og konsekvensklasser.

DNVs hovedinnspill

1. Behov for mer konsistente føringer for risikovurderinger

DNV støtter at risikovurderinger får en mer sentral rolle i regelverket. For at dette skal gi reell sikkerhetsmessig effekt, bør NVE tydeliggjøre forventningene til metodikk, omfang, dokumentasjon og oppdatering av risikovurderinger. Dette gjelder særlig for høyere



konsekvensklasser og for anlegg med komplekse tekniske, digitale eller organisatoriske grensesnitt.

DNV anbefaler at forskriften eller veiledningen presiserer at risikovurderinger bør være systematiske, etterprøvbare og basert på anerkjent metodikk. Det bør også fremgå hvordan risiko knyttet til teknisk svikt, naturhendelser, menneskelige feil, organisatoriske forhold, tilsiktede handlinger og digitale sårbarheter skal vurderes samlet.

2. Uavhengig verifikasjon bør tydeliggjøres ved økt ansvar hos aktørene

DNV registrerer at forslaget legger opp til at eier og andre ansvarlige aktører i større grad selv skal dokumentere at kravene i forskriften er oppfylt. Dette er hensiktsmessig i et mer funksjonsbasert regelverk, men det øker samtidig behovet for uavhengig kvalitetssikring og verifikasjon.

DNV anbefaler at NVE tydeliggjør når uavhengig tredjepartsverifikasjon bør benyttes, særlig ved alternative løsninger, større endringer, høyere konsekvensklasser, komplekse anlegg og digitale styrings- og overvåkingssystemer. Dette vil bidra til tillit, sporbarhet og likebehandling, samtidig som myndighetenes tilsyn kan målrettes mer effektivt.

3. Digital sikkerhet og OT-sikkerhet bør forankres tydeligere

DNV mener det er positivt at forskriftsforslaget omtaler informasjonssikkerhet og sikring av digitale overvåkings- og styringssystemer. Samtidig bør forskriften og veiledningen i større grad reflektere at moderne vassdragsanlegg ofte er avhengige av integrerte IT- og OT-systemer, sensorer, fjernovervåking og digitale beslutningsstøttesystemer.

DNV anbefaler at regelverket tydeliggjør at digital sikkerhet må vurderes som en del av den samlede barrierestyringen. Kravene bør omfatte tilgangsstyring, leverandørstyring, sikker systemintegrasjon, hendelsesdeteksjon, sikkerhetskopiering, beredskap og håndtering av cyber-fysiske konsekvenser.

4. Sikringsperspektivet bør integreres gjennom hele regelverket

DNV støtter at forslaget i større grad tar høyde for et endret sikkerhetspolitisk bilde og økt oppmerksomhet om kritisk infrastruktur. DNV mener samtidig at forskriften bør tydeliggjøre sammenhengen mellom safety og security. Sikkerheten ved vassdragsanlegg bør omfatte både utilsiktede hendelser og tilsiktede handlinger, inkludert sabotasje, uautorisert adgang, cyberangrep og kombinerte fysiske og digitale hendelser.

DNV anbefaler at ansvar for fysisk sikring, personellsikkerhet, informasjonssikkerhet og OT-sikkerhet fremgår like tydelig som øvrige sikkerhetsansvar. Dette bør knyttes til roller, kompetansekrav, internkontroll, beredskap og øvelser.

5. Veiledning blir avgjørende for vellykket implementering

En mer funksjonsbasert forskrift gir fleksibilitet, men stiller også større krav til felles forståelse av myndighetenes forventninger. DNV anbefaler at NVE prioriterer oppdaterte veiledere som beskriver anbefalt praksis for risikovurderinger, barrierestyring, uavhengig verifikasjon, digital sikkerhet, beredskap og sikring.

Kommentarer til utvalgte deler av forskriftsforslaget

Kapittel 1 – Formål og virkeområde

DNV støtter at forskriften moderniseres i lys av endret sikkerhetspolitisk situasjon, teknologisk utvikling og økt kompleksitet. DNV anbefaler at formålsbestemmelsen eller veiledningen tydeliggjør at sikkerhet ved vassdragsanlegg omfatter både beskyttelse mot utilsiktede hendelser og tilsiktede handlinger.

Det kan tydeliggjøres at sikkerheten til moderne vassdragsanlegg omfatter både beskyttelse mot utilsiktede hendelser (safety) og tilsiktede handlinger (security).

Kapittel 2 – Organisatoriske krav

DNV støtter at ansvar hos eier, leder, VTA og øvrige roller tydeliggjøres. DNV anbefaler at ansvar for fysisk sikring, personellsikkerhet, informasjonssikkerhet og OT-sikkerhet beskrives eksplisitt, slik at organisatoriske, tekniske og digitale grensesnitt ivaretas på en helhetlig måte.



På lik linje med øvrig sikkerhetsansvar bør ansvarsforhold for fysisk sikring, informasjonssikkerhet og OT-sikkerhet også spesifiseres.

Kapittel 3 – Faglige kvalifikasjoner

DNV støtter at krav til kompetanse videreføres og styrkes. For anlegg som er avhengige av digitale styrings- og overvåkingssystemer, bør det vurderes om kompetansekravene også skal omfatte informasjonssikkerhet, OT-sikkerhet og håndtering av sikkerhetstruende hendelser.

Kapittel 4 – Klassifisering

DNV støtter intensjonen om bedre differensiering mellom ulike anlegg. For høyere konsekvensklasser bør det vurderes om eksponering mot digitale angrep, samfunnskritiske avhengigheter og mulige konsekvenser av tilsiktede handlinger bør inngå tydeligere i risikovurderingene.

Kapittel 5 – Tekniske krav, risikovurderinger og beredskap

DNV støtter at risikovurderinger får en mer sentral rolle og at beredskapsmessige krav samles og oppdateres. DNV anbefaler at veiledningen beskriver hvordan barrierer skal identifiseres, dokumenteres, testes og følges opp, og at barrierer bør vurderes uavhengig av om trusselen skyldes flom, teknisk svikt, menneskelig feil, cyberangrep eller andre tilsiktede handlinger. Det bør også vurderes om forskriften tydeligere beskriver cybersikkerhet som en del av barrierestyringen, krav til robuste styringssystemer, krav til sikker integrasjon mellom OT- og IT-systemer.

Kapittel 6 – Bygging og idriftsettelse

DNV anbefaler at sikring og digital sikkerhet inkluderes allerede i design- og byggefasen. Prinsipper som security by design, sikker konfigurasjon, robust OT-arkitektur, tilgangsstyring og sikker overlevering til drift bør inngå i relevant veiledning.

Kapittel 7 – Drift, overvåking, sikring og informasjonssikkerhet

DNV mener dette er et særlig viktig kapittel. Det er positivt at risikovurderinger, overvåking, sikringstiltak, adkomsthindring og informasjonssikkerhet løftes frem. DNV anbefaler at risikovurderinger eksplisitt omfatter tilsiktede handlinger, og at overvåkingssystemer vurderes både ut fra teknisk pålitelighet og beskyttelse mot digitale angrep.

Beredskapsøvelser bør kunne omfatte cyberhendelser, sabotasje og kombinerte fysiske og digitale hendelser. Informasjonssikkerhetskravene bør i større grad kobles til OT-systemer, cyberfysiske konsekvenser, hendelsesdeteksjon og leverandørstyring.



DNV vil påpeke at spesielt innen området OT-overvåking og hendelsesdeteksjon i OT mangler det gode veileder.

Kapittel 8–10 – Tilsyn, håndheving og overgangsbestemmelser

DNV støtter at tilsyn og håndheving tilpasses et mer risikobasert regelverk. Ved redusert forhåndsgodkjenning bør det legges vekt på tydelig dokumentasjon, sporbarhet og uavhengig verifikasjon der risiko og kompleksitet tilsier det.

Avsluttende bemerkninger

DNV støtter NVEs arbeid med å modernisere damsikkerhetsforskriften. Forslaget legger til rette for et mer risikobasert og fleksibelt regelverk, og kan bidra til bedre sikkerhetsstyring dersom kravene følges opp med tydelige forventninger til metode, dokumentasjon, verifikasjon, beredskap og digital sikkerhet.

DNV anbefaler særlig at NVE i det videre arbeidet tydeliggjør krav og veiledning på fire områder:

- » *konsistente risikovurderinger,*
- » *bruk av uavhengig verifikasjon,*
- » *sterkere forankring av digital sikkerhet, og at*
- » *sikringsperspektivet bør integreres gjennom hele regelverket, slik at både utilsiktede hendelser og tilsiktede handlinger – inkludert sabotasje, uautorisert adgang, cyberangrep og kombinerte fysiske og digitale hendelser – inngår i styringen av damsikkerheten.*

Med hilsen,

Arve Johan Kalleklev,
Vice President
DNV Cyber

Hans Kristian Danielsen
Senior Vice President,
DNV Energy Systems