



Dato:  
19. mars 2018

Vår referanse:  
18/00055-2 / 008

Deres referanse:

Norges vassdrags- og energidirektorat

Postboks 5091 Majorstua  
0301 OSLO

## Hørings svar - Endringer i beredskapsforskriften

Forsvarets forskningsinstitutt (FFI) viser til Norges vassdrags- og energidirektorats (NVE) høringsbrev datert 19.12.2017 angående endringer i forskrift av 07.12.2012 om forebyggende sikkerhet og beredskap i energiforsyningen (beredskapsforskriften).

### Generell bemerkning

Etter FFIs syn er energisektoren et eksempel på en godt regulert sektor som også har stor betydning for nasjonale sikkerhetsinteresser. Hyppige endringer av regelverk for å tilpasse seg stadig nye rammebetingelser både med hensyn til teknologianvendelse og markedsutvikling er en god indikator på dette. FFI registrerer også at NVE i denne endringen legger stor vekt på forholdet til ny sikkerhetslov og at NVE deltar i det pågående arbeidet med forskrifter til den nye loven. FFI merker seg også at NVE vil gjennomføre en ny revisjon av beredskapsforskriftene etter at forskrifter til den nye sikkerhetsloven er klare.

Videre opplever FFI at NVEs språklige endringer bidrar til å gjøre forskriften tydeligere. Dette gjelder særlig for forskriftene som berører sensitiv informasjon eller objekter, hvor presisering er nødvendig for å unngå misforståelser.

### Merknader til NVEs forslag

Etter FFIs syn vil den nye sikkerhetsloven innebære vesentlige endringer innen forebyggende sikkerhet og hensynet til nasjonal sikkerhet. Så langt det er mulig å forstå av høringsutkastet er denne i god overenstemmelse med utviklingen av et nytt lovregime for nasjonal sikkerhet. FFI vil likevel få understreke at den nye sikkerhetsloven i motsetning til tidligere lov legger vekt også på tilgjengelighetsaspektet innen informasjonssikkerhet og informasjonssystemssikkerhet. I den tekstlige beskrivelsen oppfatter vi at det legges stor vekt på ulike typer angrep mot informasjonen og informasjonssystemene uten at tilgjengelighetsaspektet synes å være ivaretatt på samme nivå. For eksempel er det i forskriftsforslaget bestemmelser om systemredundans og robuste sambandsveier. Etter FFIs syn bør denne tilnærmingen moderniseres og i større grad forankres i et helhetlig syn på informasjonssikkerhet og informasjonssystemssikkerhet. Med stadig økende sentralisering av blant annet kompetanse og systemfunksjoner i energisystemene vil tilgjengelighetsaspektet bli stadig mer utfordrende.

Vedlegg:

Saksbehandler:  
Ingvild Helene Knutsen Tomter

Postboks 25, 2027 Kjeller  
Besøksadresse:  
Instituttveien 20, 2007 Kjeller

Sentralbord: 63 80 70 00  
Dir: 63 80 71 15  
Faks: 63 80 71 15

Org.nr: NO 970 963 340 MVA  
E-post: ffi@ffi.no

### **§ 1-5 Beredskapsplikt og beredskapsplan**

Som beskrevet i § 1-5 er beredskapsplikt og beredskapsplaner viktige elementer i forebygging og håndtering av ekstraordinære hendelser. Imidlertid burde forskriften også poengtere at beredskapsplanen skal gjøres kjent for de ansatte, så vel som øves slik at personell har kunnskap om deres rolle og er forberedt på en potensiell beredskapssituasjon.

### **§§ 2-5 og 2-6 Varsling og rapportering**

FFI støtter forslaget om å separere §§ 2-5 og 2-6, da det tydeliggjør de ulike kravene knyttet til varsling og rapportering. For å sikre effektiv varsling til NVE, må det påses at det er etablert tydelige varslingsrutiner internt i KBO-enhetene. Videre må ledelsen ved KBO-enhetene informere om situasjonene angitt i § 2-6 for å bevisstgjøre personell om hvilke uønskede hendelser som skal varsles. Som en del av en god sikkerhetskultur bør ledelsen oppfordre de ansatte til å varsle og rapportere hendelser til NVE, samt være årvåke for mistenkelig atferd. Når det gjelder § 2-6 annet ledd bokstav c «begrunnet mistanke» anbefales det å presisere hva begrepet omfatter. Kravet om at det må være en viss grad av sannsynlighet før varslingsplikten inntre kan i noen tilfeller føre til tvil om hvor sannsynlig en mistenkelig atferd er, noe som kan føre til forsinkelser i varslingsprosessen. Personell bør bevisstgjøres om hva dette begrepet omfatter helt konkret for å unngå potensielle misforståelser.

### **§ 3-6 Sektorvis responsmiljø**

FFI mener det kan være fornuftig at NVE har mulighet til å pålegge oppgaver og sette krav til et sektorvis responsmiljø (SRM) for sektoren, samt pålegge virksomheter tilknytning til det. Samtidig er det viktig å være klar over mulige negative konsekvenser ved pålegg og krav som SRM-et og virksomhetene selv mener ikke er hensiktsmessige. Dagens løsning er basert på og er avhengig av et godt samarbeidsklima og frivillig deling av informasjon. Pålegg og krav som SRM-et eller tilknyttede virksomheter ansees som urealistiske, forstyrrende eller av andre årsaker malplasserte vil kunne ha store negative konsekvenser for samarbeid og nytteverdi. De negative konsekvensene vil kunne ramme både SRM-et, virksomhetene og NVE. Pålegg om tilknytning mot en virksomhets vilje vil også kunne påvirke samarbeidsrelasjonen og nytteverdien.

### **§ 6-7 Personkontroll**

FFI støtter forslaget om personkontroll, da dette er et viktig virkemiddel for å forebygge og oppdage utro tjenere i en virksomhet. For tilgang til anlegg i klasse 3 kan det være hensiktsmessig å vurdere om personell bør autoriseres. Autorisering kan være aktuelt i tilfeller hvor det er grunn til å tro at adgangen til klassifiserte anlegg kan medføre at personell får tilgang til skjermingsverdig informasjon. Videre kan informasjon om sikkerhetstiltak og sensitive opplysninger om klassifiserte anlegg utgjøre sikkerhetsgradert informasjon. Det anbefales at NVE ser nærmere på hvilken skjermingsverdig informasjon personell kan tilegne seg ved å ha tilgang til høyere klassifiserte anlegg. Videre støttes forslaget om å innføre en overgangsperiode for ansatte som vurderes ikke egnet, da utvidelsen av personkontroll kan medføre store ulemper for den enkeltes arbeidssituasjon. Personellkontrollen kan også skape sårbarheter for KBO-enhetene med tanke på tap av personell med verdifull kompetanse.

### **§ 6-9 Digitale informasjonssystemer**

FFI støtter forslag § 6-9, da kravene bidrar til gode rutiner for bruk av digitale informasjonssystemer. Imidlertid bør virksomhetene som er underlagt disse kravene vurdere risiko i et større perspektiv. Dette innebærer å kartlegge avhengighetsforhold av andre virksomheter eller tjenester, nødvendig for opprettholdelse av funksjonalitet. Videre bør NVE ta høyde for potensielle negative konsekvenser som kan forekomme av tjenesteutsetting. Eksempelvis kan det bli nødvendig å vurdere hvor mye informasjon en virksomhet ønsker å dele med en samarbeidspartner med tanke på trusler og utnyttelse av sårbarheter i digitale systemer. Videre kan punkt b Risiko- og sårbarhetsanalyse, skape utfordringer med tanke på at det finnes ulike oppfatninger om hva begrepet innebærer.

Med hilsen

Monica Endregard  
Forskningsleder

Ingvild H. K. Tomter  
Forsker

*Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur.*