Innspill og syn

Departementet ber konkret om høringsinstansenes innspill og syn på enkelte punkter.

Nedenfor er disse listet med våre kommentarer.

Kapittel: 3.1 Virkeområde (side 10)
Ingen kommentarer.

Kapittel: 3.2 Inndeling i forskrifter (side 11)
Vi stiller oss positive til departementets forslag om tre forskrifter, hvorav den ene er spesielt rettet mot virksomheter. Vi stiller oss positive til korttitlene som er valgt i høringsnotatet; Myndighetsforskriften, Virksomhetsforskriften og Klareringsforskriften. **NB!** Forskriftene omhandler ikke kryptosikkerhet og vi ser heller ikke at høringsbrevet beskriver hvordan kryptosikkerhet er tenkt håndtert i ny lovgiving. Vi etterlyser regulering av administrativ kryptosikkerhet.

Kapittel: 4.1.1 Objekt- og infrastruktursikkerhet – Innledning (side 13)
Ingen kommentarer.

Kapittel: 4.5.1 Klarering av utenlandske statsborgere – Innledning (side 20)
Ingen kommentarer.

Kapittel: 4.5.4 Klarering av utenlandske statsborgere – Unntak fra krav om sikkerhetsklarering i særskilte tilfeller (side 22)
Vi støtter forslaget om å ta unntaksbestemmelsen inn i myndighetsforskriften og finner det positivt at denne muligheten presiseres. Vi foreslår at overskriften til § 11 endres til «*Unntak fra krav om **klarering** og **samtykke til autorisasjon***». Paragrafen omhandler dispensasjon fra kravet om samtykke til å autorisere og da bør også overskriften reflektere dette. Videre ved å endre til klarering dekkes både sikkerhetsklarering og adgangsklarering, som begge omhandles i paragrafen, alternativt bør både sikkerhetsklarering og adgangsklarering inngå i overskriften.

Kapittel: 4.6.4 Krav til sikkerhet i anskaffelser – Varslingsplikt (side 24)
Det er behov for at forskriften gjøres tydeligere i forhold til detaljnivå som utløser varslingsplikten, f.eks. vil en kvantifisering av begrepet «ikke ubetydelig risiko» bidra til mer tydelighet.

Kapittel: 4.6.5 Krav til sikkerhet i anskaffelser – Klareringsmyndighet for leverandørklarering (side 25)
Vi mener at Nasjonal sikkerhetsmyndighet skal være klareringsmyndighet for leverandørklarering i forsvarssektoren.

Kapittel: 4.7 Ikrafttredelse (side 26)
Ingen kommentarer.

Kapittel: 6.1.1 Til § 1 Klassifisering av skjermingsverdige objekter og infrastruktur (side 32)
Ingen kommentarer.

Kapittel: 6.2.4 Til § 6 Bruk av tredjepart til å utføre tekniske sikkerhetsundersøkelser, inntrengingstesting, testing av sikkerhetstiltak og kommunikasjon- og innholdskontroll av informasjonssystemer (side 33)
Forskriften bør sette som kriterie til at en tredjepart som skal utføre tekniske sikkerhetsundersøkelser, inntrengingstesting, testing av sikkerhetstiltak og kommunikasjon- og innholdskontroll av informasjonssystemer hos en virksomhet har dette som eneste oppgave overfor virksomheten. Med dette menes at en tredjepart ikke samtidig f.eks. utfører andre konsulentoppdrag for virksomheten.

Kapittel: 6.3.1 Til § 12 Utøvelse av nasjonal responsfunksjon for alvorlige digitale angrep og nasjonalt varslingssystem for digital infrastruktur (side 36)
Ingen kommentarer. Vi er positive til VDI tilknytning for de virksomhetene som blir underlagt loven.

Kapittel: 6.4 Til kapittel 4 Tilsyn (side 36)

I § 17 andre ledd står det at tilsynet skal gjennomføres ofte nok og i stort nok omfang til å ivareta lovens formål.

Her bør forskriften gi føringer i forhold til hva som er minimums- og maksimumskrav til hvor ofte formelle tilsyn skal finne sted. Vi foreslår minimum hvert tredje år og maksimum hver tolvte måned.

Kapittel: Til § 20 Melding om erverv av kvalifisert eierandel i virksomhet underlagt sikkerhetsloven (side 40)

Ingen konkrete innspill.

Kapittel: 7.1.1 Forsvarlig sikkerhetsnivå (side 42)

Vi støtter innretningen, men ser samtidig at ordet *forsvarlig* kan bli uklart og kan gi rom for tolkninger.

Kapittel: 7.2.1 Til § 1 Definisjoner (side 42)

Vi ser helt klart behovet for definisjoner og det er også ønskelig at flere defineres:

Adgang og **Tilgang**
Forskriftene benytter ordene adgang og tilgang, men disse er ikke benyttet konsekvent.
Vi ønsker et tydelig skille på disse ordene og foreslår følgende definisjon:

Adgang – benyttes for fysisk adgang (rom, bygg, etc.)
Tilgang – benyttes for tilgang til informasjon (logisk tilgang)

Eksempler på bruk av ordet **tilgang** i Forskriftene, hvor vi mener det heller bør stå **adgang**:
§ 4 (side 91):
"d) om det er risiko for at uvedkommende har hatt tilgang til rommet siden forrige tekniske sikkerhetsundersøkelse."

§ 44 (side 104):
"*Virksomheten skal føre oversikt over hvilke personer som har selvstendig tilgang til rommet eller lokalet.*"

§ 75 (side 111):
"*c) skal ha tilgang fra egne lokaler utenfor norsk jurisdiksjon, eller*"

Autorisasjonsansvarlig
Eksempelvis § 60 (side 108) menes autorisasjonsansvarlig hos leverandør. I § 66 (side 109) står det at autorisasjonsansvarlig sender til klareringsmyndigheten. Autorisasjonsansvarlig hos leverandør (vår situasjon) sender ikke direkte til klareringsmyndighet, men til anmodende (Forsvarsmateriell Industrisikkerhet (FMA)). I § 66 menes det fortsatt anmodende (FMA), slik det praktiseres i dag. I § 69 stilles det krav om bevaring og kassasjon av opplysninger. Igjen treffer dette autorisasjonsansvarlig hos anmodende (FMA). Disse rollene må skilles og tydelig defineres.

Forholdet mellom begrepene **Virksomhet**, **Leverandør** og **Oppdragsgiver**, evt. Anskaffelsesmyndighet som benyttes i dagens forskrifter og veiledninger. I Sikkerhetslovens benyttes det f.eks. «virksomheter som loven gjelder for», «virksomheter som er omfattet av loven», «virksomheter som det er fattet vedtak om etter §1-3» osv. Vi forslår at det etablere klare definisjoner som benyttes i forskriftene,

Det er utfordringer i forhold til dette i regelverket pr. i dag, og det er et behov for at dette blir entydig med ny lov og forskrift.

Oppsummert bør forskriftene innledes med klare definisjoner av de begrep og roller som benyttes i forskriften, eksempelvis:
- Adgang
- Anmodende myndighet (dette begrepet er ikke med i forskrift eller høringsnotat, men benyttes i dagens forskrifter. Behov for definisjon dersom det skal fortsette å eksistere og brukes)
- Anskaffelsesmyndighet (ikke benyttet i høringsnotatet, men i nåværende forskrift. Begrepet må defineres om det skal benyttes)
- Autorisasjonsansvarlig
- Data (ref. høringsnotat kap. 7.2.2 til § 45 i Virksomhetsforskriften)
- Leverandør
- Oppdragsgiver
- Tilgang
- Tilsyn – dette bør defineres versus kontroll av sikkerhetstilstanden som benyttes ved leverandørklarering.
- Sektormyndighet
- Virksomhet
- etc.

Kapittel: 7.2.7 Til § 7 Tiltak ved sikkerhetstruende virksomhet, avvik og kompromittering av sikkerhetsgradert informasjon (side 46)

Vi slutter oss til bruken av ordet "Sikkerhetstruende virksomhet". Begrepet er også benyttet i sikkerhetslovens § 1-1 andre punkt og det er en fordel for forståelsen at forskriftene holder seg til begreper som benyttes i loven.

Kapittel: 7.3.2 Til § 12 Plikt til å håndtere risiko (side 47)

Ingen kommentarer.

Kapittel: 7.6.8 Til § 38 Beskyttet sone (side 59)

Støtter at NSM fortsatt stiller krav til oppbevaringsenheter. Krav som stilles bør så langt det lar seg gjøre baseres på bransjestandarder/sertifisering. Eksempelvis FG-godkjenning (eller tilsvarende) bør kunne legges til grunn. Dette så man unngår godkjenning av enkelte modeller og leverandører.

Kapittel: 7.7.5 Til § 48 Godkjenningen (side 64)
Ingen kommentarer

Kapittel: 7.9.2 Til § 56 Tilknytning til varslingssystemet for digital infrastruktur (side 69)
Ingen kommentarer

Kapittel: 8.1.1 Til § 1 Klareringsmyndighet (side 76)
Ingen kommentarer. Vi støtter departementets forslag om å forskriftsfeste kravet til klareringsnivå.

Kapittel: 8.3.2 Til § 7 Sikkerhetsklarering – krav til egenopplysninger (side 78)
Vi mener det er hensiktsmessig med et krav om innmelding av egenopplysninger fra den enkelte det søkes om sikkerhetsklarering for. At den enkelte person selv skal vurdere «forhold som antas å være av betydning for om han eller hun er sikkerhetsmessig skikket» gjør det mere uklart for den enkelte hvor grensene går for hva som skal oppgis/rapporteres. Det som kan vurderes er om detaljnivået for egenopplysninger kan forenkles, når det gjelder opplysninger som finnes i registre. Vi opplever pr. dato f.eks. at den enkelte blir bedt om å oppgi omstendigheter rundt situasjonen og hvor den fant sted, når de oppgir at de fikk en bot for fartsovertredelse 15 år tilbake i tid. Evt. vurder om kun skal være krav om å rapportere nyere saker (f.eks. siste 10 år), da opplysningene uansett befinner seg i registre klareringsmyndighetene har tilgang til. Da vil det være mer i tråd med kravet om 10 års observasjonstid for utenlandske statsborgere, og enklere å forstå i forhold til sikkerhetsrisikovurdering av den enkelte person.

Kapittel: 8.3.2 Til § 16 Vurderingsgrunnlaget for tilknytning til andre stater (side 81)
Ingen kommentarer.

Kapittel: 8.4.1 Til § 26 Samtykke til å autorisere utenlandske statsborgere for BEGRENSET (side 84)

Ses i sammenheng med kommentar til kap. 4.5.4.

Vi ser det som en fordel at det er klareringsmyndigheten som skal gjøre vurderingen i forhold til autorisasjon av utenlandske uten klarering, dvs. til nivå BEGRENSET. Dette sikrer en lik håndtering og vurdering, også siden det vil være klareringsmyndigheten som har innsyn i NSMs vurdering av andre stater. At alle autorisasjonsansvarlige skal ha innsyn i NSMs vurdering av andre stater, i tillegg til å gjøre en helhetsvurdering pr. utenlandsk statsborger anses ikke å være en hensiktsmessig løsning.

Merknader – Utkast til forskrift om myndighetens roller og ansvar for nasjonal sikkerhet

Paragraf	Side	Kommentar
§ 16	94	Gjeldende forskrift (Forskrift om sikkerhetsgraderte anskaffelser) sier følgende i paragraf § 2-4: "*NSM skal utpeke en bestemt anskaffelsesmyndighet som sikkerhetsansvarlig overfor leverandører som leverer til sikkerhetsgraderte anskaffelser for flere anskaffelsesmyndigheter*" Det er helt essensielt at det fortsatt utpekes kun en anskaffelsesmyndighet (i forslag til ny forskrift kalt oppdragsgiver) som for sikkerhetsansvar og tilsynsmyndighet overfor leverandører som leverer til flere anskaffelsesmyndigheter. I høringsnotatet til ny forskrift står det at hensikten med å sette NSM som den som skal føre tilsyn med norske leverandører er fordi samme leverandør kan benyttes av oppdragsgivere i flere sektorer og at dette skal forhindre at flere sektormyndigheter kan få tilsynsansvar overfor en leverandør. Vi ber om at § 16 skrives om slik at leverandører får kun en tilsynsmyndighet, f.eks. til «Nasjonal sikkerhetsmyndighet skal føre tilsyn med norske leverandører i sikkerhetsgraderte anskaffelser. NSM kan for en leverandør utpeke en sektormyndighet som tildeles myndighet til å føre tilsyn med leverandøren på vegne av Nasjonal sikkerhetsmyndighet.»
§ 17	94	I § 17 andre ledd står det at tilsynet skal gjennomføres ofte nok og i stort nok omfang til å ivareta lovens formål. Her bør forskriften gi føringer i forhold til hva som er minimums- og maksimumskrav til hvor ofte formelle tilsyn skal finne sted. Vi foreslår minimum hvert tredje år og maksimum hver tolvte måned.

Merknader – Utkast til forskrift om virksomhetens arbeid med forebyggende sikkerhet

Paragraf	Side	Kommentar
		Forskriften omhandler ikke kryptosikkerhet og vi ser heller ikke at høringsbrevet beskriver hvordan kryptosikkerhet er tenkt håndtert i ny lovgiving. Vi etterlyser regulering av administrativ kryptosikkerhet.
§ 5	96	Kommentar til høringsnotatet: I avsnitt i høringsnotatet "7.2.5 til § 5 Roller og ansvar i det forebyggende sikkerhetsarbeidet" (side 44) står det at det bør utarbeides veiledningsmateriale fra tilsynsmyndigheten eller sikkerhetsmyndigheten. Ifølge Sikkerhetsloven § 2-2 tredje ledd er Sikkerhetsmyndigheten nasjonal fagmyndighet overfor andre land og internasjonale organisasjoner. Indirekte kan det tolkes at det er sikkerhetsmyndigheten som er Norges nasjonale fagmyndighet når det gjelder sikkerhet. Som fagmyndighet er det sikkerhetsmyndigheten som bør stå som ansvarlig for utarbeidelse av veiledninger og lovtolkning. Dette er ikke noe som bør delegeres til forskjellige tilsynsmyndigheter. Denne kommentaren er basert på at dagens veiledninger utgitt av NSM skal anses som krav på linje med lov og forskrifter. Krav, også i form av veiledninger, må komme fra en felles fagmyndighet for sikkerhet.
§ 10	97	Paragrafens overskrift omhandler dokumentasjon av styringssystemet, mens selve paragrafen sier at virksomheten skal dokumentere at styringssystemet for sikkerhet og sikkerhetstiltakene gir et forsvarlig sikkerhetsnivå. Det er behov for mere tydeliggjøring av hvilke krav som vil bli stilt til dokumentasjon av at sikkerhetstiltakene gir et forsvarlig sikkerhetsnivå. Er det egentlig krav til etterlevelse av styringssystemet som kreves. Da bør paragrafen omformuleres til f.eks. «Virksomheten skal dokumentere etterlevelse av styringssystem for sikkerhet.» I tillegg kan gjerne § 8 tredje ledd utvides til «Resultatet av evalueringer og øvelser **skal dokumenteres** og inngå i leders årlige gjennomgang.» for å få fram at forsvarlig sikkerhetsnivå dokumentere. Den foreslåtte endringen av § 8 er dekket inn av forslag til endring av denne paragrafen, men kan evt. tas inn som en forsterkning av kravet til dokumentasjon.

§ 15	99	Slik paragrafen er skrevet kreves det alltid evaluerte produkter. Det gis ikke anledning for eventuelle kompenserende tiltak. Foreslår at det legges inn en setning som åpner for å benytte kompenserende tiltak ved ikke-evaluerte produkter. F.eks. et tredje ledd «I særlige tilfeller kan det benyttes ikke evaluerte produkter eller tjenester under forutsetning av at det gjennomføres en risikovurdering og innføres kompenserende tiltak som sikrer et forsvarlig sikkerhetsnivå.»
§ 18	99	Det er behov for at forskriften tydeliggjør lovkravet i forhold til detaljnivå som utløser varslingsplikten, f.eks. vil en kvantifisering av begrepet «ikke ubetydelig risiko» bidra til mer tydelighet og kan gjerne tas inn i denne paragrafen.
§ 26	101	§ 26 første ledd foreslås det: *"Dokumenter og lagringsmedier skal merkes med den høyeste sikkerhetsgraden som informasjon i dokumentet eller lagringsmediet er gradert til, og med hvor lenge graderingen varer."* I Sikkerhetsloven § 5-3 andre ledd andre punkt står det «Dersom ikke annet er bestemt, bortfaller sikkerhetsgraderingen etter 30 år.» Vi mener derfor at merking med «hvor lenge graderingen varer» bare er nødvendig dersom det er vurdert at graderingen skal ha annen varighet enn 30 år og foreslår at denne delen fjernes fra forskriften. For lagringsmedier: Det er utfordringer knyttet til at lagringsmedier skal påføres en varighet for gradering. Det er selve informasjonen som er lagret på lagringsmediet som har en varighet i forhold til gradering av informasjon, vanligvis ikke selve lagringsmediet. Lagringsmedier bør kun påføres høyeste sikkerhetsgradering, uten nærmere angivelse av varighet. Det knytter seg også utfordringer til ajourføring av varighet for gradering av lagringsmedium.
§ 26	101	§ 26 andre ledd foreslås det; *«Dersom ikke alle informasjon i et dokument eller lagringsmedium har samme sikkerhetsgradering, skal merkingen vise hvilke deler som har hvilken gradering.»* I dagens forskrift om informasjonssikkerhet § 2-3 første ledd første punkt står det «Dersom informasjonen består av deler med forskjellig beskyttelsesbehov skal de enkelte deler graderes der det er praktisk mulig.» Vi foreslår at dette videreføres i ny forskrift og at teksten endres til «*Dersom ikke all informasjon i et dokument eller lagringsmedium har samme sikkerhetsgradering, skal merkingen vise hvilke deler som har hvilken gradering* ***der det er praktisk mulig.****»*

§ 26	101	I kapittel "7.5.1 Til § 26 Merking av dokumenter og lagringsmedier som inneholder sikkerhetsgradert informasjon" (side 55) står følgende: *"I tredje ledd fremgår det at sikkerhetsgradert informasjon skal merkes før utlevering til andre stater eller internasjonale organisasjoner. Hensikten med bestemmelsen er dels at det skal fremgå tydelig hvilken informasjon som kan utleveres i slike tilfeller"* I selve forskriften står det: *«Dokumenter og lagringsmedier med informasjon som utleveres til en annen stat eller internasjonal organisasjon, jf. § 23, skal være merket med hvilken stat eller organisasjon dokumentet eller lagringsmediet utleveres til.* Forskriften sier at selve dokumentet eller lagringsmediet som utleveres skal merkes, mens det i høringsnotatet tolkes til at selve informasjonen og lagringsmediene den befinner seg på skal merkes. Utleveres samme informasjon til flere skal den da merkes med flere stater og organisasjoner. Her er det dissens mellom betydning ved å lese teksten i forskriften og tekst i høringsnotatet, så vi ber om at dette gjøres entydig. Dersom det som står i høringsnotatet er riktig tolkning vil det være en utfordring i forhold til lagringsmedier som inneholder mye informasjon, f.eks. harddisker, hvorav ikke all informasjon nødvendigvis vil være av en art som skal leveres ut til andre.
§ 38	103	For permanent adgang til beskyttet sone stilles det krav om sikkerhetsklarering: *«Personer som skal gis permanent adgang til en beskyttet sone skal være sikkerhetsklarert for KONFIDENSIELT.»* Dette er ikke nye krav ut i fra gjeldende lovgiving. I dag praktiseres det i tillegg at taushetserklæring skal være undertegnet. Vi foreslår at paragrafen endres til å inkludere krav om signert taushetserklæring før permanent adgang gis. Her tenker vi på personell som ikke er autorisert for tilgang til autorisert for tilgang til informasjon, for eksempelvis vedlikeholdspersonell.
§ 40	103	I fjerde ledd står det « …mulig å deponere informasjonen ved en norsk utenriksstasjon eller et norsk kontrollert område ved ankomst. » Dersom det med « norsk kontrollert område » menes « område der Norge er gitt jurisdiksjon » foreslås det endret til dette. Alternativt bør det defineres hva som menes med begrepet « norsk kontrollert område ».

§ 43	104	Paragrafen stiller krav til forsendelse med kurer. I høringsnotatet kapittel "7.6.13 Til § 43 Krav til forsendelse med kurer" står følgende: *"Det er også slik at virksomhetens ansatte selv kan utføre kurertransporten så lenge kurersertifikatet er utstedt av rette myndighet."* Hvem er rette myndighet? Hvordan gjør dette i praksis når egne ansatte er kurerer (leilighetskurer)? Bør det fremgå av tekst i paragraf at egne ansatte (leilighetskurer) kan benyttes? Slik det står, vil det kun være virksomheter som utfører kurerposttjeneste som kan være kurerer. Høringsnotatet åpner for at virksomhetens egne ansatte kan være kurerer, men dette står ikke i paragrafteksten i forskriften. Det er ønskelig med mer informasjon og detaljer knyttet til kurervirksomhet da dette er gjenstand for forskjellig tolkning også i dagens gjeldende regelverk.
§ 47	105	Paragrafen er i henhold til gjeldene lovgivning. Dagens praksis for leverandører til Forsvaret er at virksomheten selv ikke godkjenner sikkerhetsgraderte informasjonssystemer. Leverandører innen forsvarssektoren må pr. idag søke om sikkerhetsgodkjenning for alle graderingsnivåer. Dersom departementet ønsker at dagens praksis skal opprettholdes bør paragrafen åpne for at enkelte sektorer kan kreve at leverandører må søke om godkjenning for alle informasjonssystemer som skal benyttes til sikkerhetsgradert informasjon.
§ 59	108	Til fjerde ledd: *"Personer som skal autoriseres for BEGRENSET, eller med kortvarig behov for autorisasjon for KONFIDENSIELT eller høyere, kan få en felles orientering om sikkerhetsmessige risikofaktorer og relevante krav til sikkerhet i stedet for en individuell autorisasjonssamtale"* Dette med kortvarig behov for autorisasjon for KONFIDENSIELT eller høyere er upresist. Vi antar behovet er knyttet til kurs og møter. Bør kortvarig defineres i tid? Bør denne retten til autorisasjon (kortvarig KONFIDENSIELT eller høyere) forbeholdes myndighetene? Vi finner det problematisk at leverandører skal ha myndighet til selv å kunne gi en slik autorisasjon.
§ 65	109	Siste ledd: "*Dersom klareringsmyndigheten, etter å ha blitt informert etter andre ledd, opprettholder klareringen, kan autorisasjonsansvarlig ikke tilbakekalle, nedsette eller suspendere autorisasjonen på grunnlag av de innmeldte opplysningene.*" Vi ser at hensikten med dette leddet er at myndighetene skal kunne korrigere åpenbare feil. Samtidig ser vi at denne også kan slå uheldig ut. Det er autorisasjonsansvarlig som skal avgjøre en persons sikkerhetsmessige skikkethet. Ved bruk av dette leddet vil myndighetene overstyre og kreve at autorisasjonsansvarlig skal betrakte personen som sikkerhetsmessig skikket (Man blir tvunget til å stole på en personer man ikke stoler på) Dersom det ikke er åpenbare saksfeil, vil en slik overprøving være vanskelig for autorisasjonsansvarlig å forholde seg til.

Merknader – Utkast til forskrift om Klarering av leverandører og personell

Paragraf	Side	Kommentar
§ 22	118	I departementets forslag er det dersom personen med klarering sin ektefelle, partner eller samboer inngår ny ekteskap, partnerskap eller samboerskap det skal vurderes om klarering kan opprettholdes. Ut fra det som står i høringsnotatet oppfatter vi det som at det ikke er dette departementet ønsker å formidle i denne paragrafen. Vi foreslår derfor at andre ledd endres til *«Dersom en ektefelle, partner eller samboer inngår i personkontrollen for en person med klarering, og **personen med klarering** inngår nytt ekteskap, partnerskap eller samboerskap, skal klareringsmyndigheten vurdere om klareringen kan opprettholdes.»*