Rettleiing

Forskrift om klassifisering og sikring av anlegg i elektroniske kommunikasjonsnett (klassifiseringsforskrifta)

Post- og teletilsynet

INNHALD

REVISJONSLISTE

Revisjon	Dato	Endring/merknad
1	20.12.2012	1. utgåve

1. INNLEIING

Frå 1. januar 2013 gjeld forskrift om klassifisering og sikring av anlegg i elektroniske kommunikasjonsnett (klassifiseringsforskrifta). Krava i forskrifta er ei operasjonalisering av lov om elektronisk kommunikasjon (ekomlova) § 2-10 fyrste ledd, kva gjeld fysiske ekomanlegg.

Formålet med klassifiseringsforskrifta er å sikre nettutstyr i anlegg mot uønskt ytre fysisk påverknad, og rettar seg mot tilbydar av elektroniske kommunikasjonsnett som nyttast til offentleg elektronisk kommunikasjonsteneste (nettilbydar).

Nettilbydar skal klassifisere alle anlegg ut i frå kor viktig eiget nettutstyr i anlegga er for offentlege elektroniske kommunikasjonstenester. Anlegga skal klassifiserast i klassane A, B, C og D.

Sentralt i klassifiseringsforskrifta er føresegna som krev at nettilbydar gjennomfører ei heilskapleg risiko- og sårbarheitsvurdering knytt til sine anlegg, og sørgje for at anlegg i dei ulike klassane er forsvarleg sikra i samsvar med denne vurderinga. Sikringstiltaka skal minst oppfylle nærmare definerte krav knytt til skalsikring, tilgangskontroll, innbrotsalarm, brannsikring, EMP/HPM, hjelpeteknisk utstyr, lokalisering og samlokalisering.

Nettilbydar som har anlegg i klasse A, B eller C pliktar å rapportere til Post- og teletilsynet (PT) eit oversyn over desse anlegga.

Staten gir ingen kompensasjon for kostnadar knytt til å oppfylle forskrifta.

Dette dokumentet inneheld eit oversyn over dei einskilde føresegnene i klassifiseringsforskrifta med tilhøyrande kommentarar frå PT. Gjeldande forskrift er tilgjengeleg på lovdata.no:

http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20120910-0866.html.

Sjølv om forskrifta direkte berre gjeld ekomanlegg, etablerer forskrifta også sikkerheitsnivået som følgjer av ekomlova § 2-10 fyrste ledd for anna ekominfrastruktur enn ekomanlegg. Forskrifta skal difor også sjåast på som ei eksemplifisering av sikkerheitsnivået som gjeld for slik anna ekominfrastruktur.

2. KOMMENTARAR TIL DEI EINSKILDE FØRESEGNENE

2.1. § 1. Formål

§ 1. *Formål*
Forskrifta sitt formål er å sikre nettutstyr i anlegg mot uønskt ytre fysisk påverknad for at tilbydar skal kunne tilby elektronisk kommunikasjonsnett- og teneste med nødvendig sikkerheit for brukarane i fred, krise og krig.

Forskrifta er avgrensa til direkte å gjelde sikring mot *uønskt ytre fysisk påverknad*. Dette inneber at forskrifta ikkje direkte omfattar uønskt påverknad på nettutstyr som følgje av t.d. systemfeil eller programvarefeil på nettutstyret eller logiske angrep.

2.2. § 2. Virkeområde

§ 2. *Virkeområde*

Forskrifta gjeld nettilbydarar.

Post- og teletilsynet kan treffe vedtak om at andre som omfattast av lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomlova) også skal omfattast av forskrifta.

Føresegna avgrensar her det personelle virkeområdet til forskrifta. Det geografiske virkeområdet følgjer av ekomlova § 1-3.

PT kan, i medhald av andre ledd, treffe vedtak om at andre som faller inn under virkeområdet til ekomlova også skal omfattast av klassifiseringsforskrifta. Dette kan mellom anna vere aktuelt for verksemder som ikkje er nettilbydarar, men som likevel representerer viktige innsatsfaktorar i ekomnett og -tenester.

PT kan òg, i medhald av § 16, gi dispensasjon frå forskrifta, eller einskilde føresegner i forskrifta, i særlege tilfelle.

2.3. § 3. Definisjonar

§ 3. *Definisjonar*

I denne forskrifta meinast med:

1. *nettilbydar:* tilbydar av elektroniske kommunikasjonsnett som nyttast til offentleg elektronisk kommunikasjonsteneste.
2. *nettutstyr:* utstyr som nyttast til elektronisk kommunikasjon og som inngår som ein integrert del av elektroniske kommunikasjonsnett.
3. *anlegg:* fysisk konstruksjon som huser nettutstyr, og som utgjer ein naturleg heilskap, som til dømes eit fjell-/bunkeranlegg, ei bygning, ein avgrensa del av ei bygning, eller ei mast.
4. *to-faktor autentisering:* autentisering av personell ved hjelp av to av faktorane « noko personen har », « noko personen veit » og « noko personen er ».
5. *EMP/HPM-våpen:* våpen basert på elektromagnetisk puls (EMP) eller høgfrekvent radiostråling (HPM).
6. *hjelpeteknisk utstyr:* straumforsyningsutstyr, reservestraumforsyning og kjøleutstyr som er fast installert i anlegg, eller tilrettelagt for å bli installert i anlegg, for drift av nettutstyr.

Om nettilbydar: Til grunn for ei offentleg elektronisk kommunikasjonsteneste ligg det gjerne ein kjede av tilbydarar som tilbyr mørk fiber, optiske kanalar, leigde samband av ulik art, hjelpeteknisk infrastruktur, drift og overvaking osb. For å vurdere om ei verksemd skal reknast som tilbydar av elektroniske kommunikasjonsnett som nyttast til offentleg elektronisk kommunikasjonsteneste, må ein ta utgangspunkt i definisjonane i ekomlova § 1-5:

- § 1-5 pkt. 1 definerer elektronisk kommunikasjon som «overføring av lyd, tekst, bilder eller andre data ved hjelp av elektromagnetiske signaler i fritt rom eller kabel i et system for signaltransport»
- § 1-5 pkt. 2 definerer elektronisk kommunikasjonsnett som «system for elektronisk kommunikasjon der radioutstyr, svitsjer, annet koplings- og dirigeringsutstyr, tilhørende utstyr eller funksjoner inngår»
- § 1-5 pkt. 4 definerer elektronisk kommunikasjonsteneste som «tjeneste som helt eller i det vesentlige omfatter formidling av elektronisk kommunikasjon og som normalt ytes mot vederlag»
- § 1-5 pkt. 7 definerer offentlig elektronisk kommunikasjonstjeneste som «elektronisk kommunikasjonstjeneste som er tilgjengelig for allmennheten eller beregnet til bruk for allmennheten»
- § 1-5 pkt. 14 definerer tilbydar som «enhver fysisk eller juridisk person som tilbyr andre tilgang til elektronisk kommunikasjonsnett eller -tjeneste.»

Til hjelp i vurderinga visast det til Forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskrifta) § 1-2 som omhandlar registreringsplikta til tilbydarar. Følgjande har plikt til å registrere seg hos PT[1]:

1. Tilbydarar som etablerer, driftar og gir tilgang til ekomnett som nyttast for tilbod av offentlig ekomteneste
2. Tilbydarar av offentlig telefonteneste.
3. Tilbydarar av overføringskapasitet (leigde samband).

Tilbydarar som etter ekomforskrifta § 1-2 pliktar å melde til PT at dei etablerer, driftar og tilbyr tilgang til elektronisk kommunikasjonsnett som nyttast for tilbod av offentlege ekomtenester (jf. punkt 1 over) vil òg vere nettilbydar etter klassifiseringsforskrifta.

Om nettutstyr: Inkluderer mellom anna radioutstyr, svitsjar, anna koplings- og dirigeringsutstyr, kablar og nettermineringspunkt.

Om anlegg: Dette er den fysiske konstruksjonen som huser eit «punkt» i infrastrukturen, som til dømes eit fjell-/bunkeranlegg, ei bygning, ein avgrensa del av ei bygning (rom), eller ei mast. Nettermineringspunkt som er installert hos sluttbrukar skal ikkje reknast som anlegg. Sambandstrasear og fysisk skjerming av desse («linjer» i infrastrukturen), som t.d. kabeltunnellar og kabelkanalar skal heller ikkje reknast som anlegg. Det same gjeld for passive koplingsskap (som ikkje krev straumforsyning) .

Om to-faktor autentisering: Med noko personen har meinast fysisk nøkkel eller liknande. Med noko personen veit meinast passord eller liknande. Med noko personen er meinast ein biometrisk faktor, som t.d. fingeravtrykk.

Om EMP/HPM-våpen: Våpen som har til hensikt å skade elektronisk utstyr ved hjelp av elektromagnetisk stråling. EMP-våpen er typisk kjernefysiske våpen som genererer elektromagnetisk puls. HPM-våpen er typisk mikrobølgjerør som gir høgfrekvent radiostråling med kort varigheit og høg intensitet, og som kan monterast på fly, i rakettar, i køyretøy eller i koffert (handhaldt).

Om hjelpeteknisk utstyr: Med straumforsyningsutstyr meinast likerettar- og vekselrettarutstyr o.l. I reservestraumforsyning inngår både reservestraumkjelde (t.d. aggregat eller batteribankar) og avbrotsfri straumforsyning (UPS). Dette svarar til definisjonen av reservestraumforsyning i Norsk elektroteknisk norm om elektriske lavspenningsinstallasjoner (NEK 400:2010).

[1] Ein oversikt over registrerte tilbydarar er tilgjengeleg på www.npt.no

2.4. § 4. Klassifisering

§ 4. *Klassifisering*

Nettilbydar skal klassifisere alle anlegg ut i frå kor viktig eiget nettutstyr i anlegget vurderast å vere for offentlege elektroniske kommunikasjonstenester. Anlegga skal klassifiserast i fire klassar:

a) *Klasse A*

Anlegg som omfattast av lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste.

b) *Klasse B*

Anlegg som er særs viktig for offentlege elektroniske kommunikasjonstenester på landsdelsnivå eller større, eller for eit tilsvarande omfang av brukarar.

c) *Klasse C*

Anlegg som er særs viktig for offentlege elektroniske kommunikasjonstenester på fylkesnivå eller større, eller for eit tilsvarande omfang av brukarar.

d) *Klasse D*

Anlegg som ikkje er omfatta av klassane A, B eller C.

Med anlegg som er særs viktig for offentlege elektroniske kommunikasjonstenester meinast mellom anna anlegg med nettutstyr som er kritisk for:

1. samtrafikk med elektroniske kommunikasjonsnett i utlandet,
2. samtrafikk med nasjonale/regionale elektroniske kommunikasjonsnett,
3. sentral dirigering og styring av elektronisk kommunikasjon,
4. sentrale oppslags-, registrerings- eller databasetenester,
5. kringkasting, eller
6. drift og overvaking av utstyr nemnt i punkt 1.–5.

Nettilbydar skal revidere klassifiseringa minst årleg.

I særlege tilfelle kan Post- og teletilsynet gjennom vedtak gjere om nettilbydar si klassifisering av anlegg.

Nettilbydar skal sjølv klassifisere anlegga. Dersom det i anlegget er samlokalisering skal ein nettilbydar ikkje måtte ta stilling til betydinga av andre nettilbydarar sitt nettutstyr. Som følgje av dette kan ulike nettilbydarar klassifisere same anlegget forskjellig, ut frå at dei har nettutstyr med ulik betyding for offentlege ekomtenester. Ein kvar som innplasserer nettutstyr må altså sjølv sørgje for at anlegget tilfredsstiller krava som følgjer av sin eigen klassifisering, jf. også § 13 om eksterne aktørar.

Dersom nettilbydar er omfatta av Lov om forebyggende sikkerhetstjeneste (sikkerheitslova)[2] og har fått utpeikt eit anlegg som skjermingsverdige objekt, skal anlegget klassifiserast som klasse A. Krava til klasse A-anlegg i medhald av klassifiseringsforskrifta, kjem i tillegg til eventuelle krav i medhald av sikkerheitslova og Forskrift om objektsikkerhet (objektsikkerheitsforskrifta). Skillet mellom A- og B-anlegg er etablert for å sikre harmonisering med sikkerheitslova/objektsikkerheitsforskrifta. I klassifiseringsforskrifta er krava til sikring av anlegg i klasse A og B identiske.

Nettilbydar si vurdering av om anlegg skal klassifiserast i klasse B, C eller D vil vere basert på skjøn. Styrande for vurderinga er det geografiske omfanget og omfanget av brukarar. Kriteria for klasse B er landsdelsnivå eller tilsvarande omfang brukarar. Her meinast typisk Nord-Noreg, Midt-Noreg, Vestlandet, Øst- og Sørlandet eller i størrelsesorden hundre-tusentals brukarar. Kriteria for klasse C er fylkesnivå eller tilsvarande omfang brukarar. Her meinast eit eller fleire fylke (opp til landsdelsnivå) eller i størrelsesorden ti-tusentals brukarar. Dei resterande anlegga til nettilbydar skal klassifiserast som klasse D.

§ 4 andre ledd gir døme på kva typar nettutstyr som medfører at anlegg kan reknast som «særs viktig for offentlege elektroniske kommunikasjonstenester»:

- Nettutstyr for samtrafikk kan vere kritisk fordi det vil kunne påverke tilbodet av offentlege ekomtenester òg utover eiget nett.

[2] Per november 2012 er det Telenor og Broadnet som er omfatta av sikkerheitslova.

- Nettutstyr for sentrale dirigerings- og styringsmekanismar og sentrale oppslags-, registrerings-, eller databasetenester kan vere kritiske i den grad slikt utstyr utgjer «single point of failure» som ved enkeltutfall kan påverke offentlege ekomtenester i stort omfang.
- Nettutstyr for kringkasting kan vere kritisk for å formidle viktige meldingar frå myndigheitene.
- Drift- og overvaking av nettutstyr nemnt i § 4 andre ledd pkt. 1. - 5. er indirekte kritisk for oppretthald av offentlege elektroniske kommunikasjonstenester.

I mange tilfelle kan nettutstyr vere duplisert i fleire anlegg (redundans). Nettilbydar vil i slike tilfelle kunne vurdere at betydinga til anlegget er lågare enn om nettutstyret ikkje var duplisert, og at det av den grunn ikkje er like kritisk. Det er likevel nettutstyret sin funksjon (uavhengig av duplisering) som skal vere styrande for klassifiseringa. Det betyr at dersom nettutstyr i eit anlegg openbart er særs viktig for offentlege ekomtenester på landsdelsnivå, og på grunn av dette er duplisert i eit anna anlegg, skal normalt begge anlegga klassifiserast som klasse B. Dersom nettilbydar likevel finn grunnlag for å klassifisere anlegg med duplisert nettutstyr lågare enn om nettutstyret ikkje var duplisert, skal dette kome klart fram i den dokumenterte vurderinga som skal rapporterast til PT, jf. § 14, og i tillegg vere godt fundert i risiko- og sårbarheitsvurderinga, jf. § 5.

Etter femte ledd kan PT, i særlege tilfelle, gjere om nettilbydar si klassifisering av anlegg. Dette kan til dømes vere aktuelt dersom PT vurderer at nettilbydar ikkje har klassifisert anlegga i samsvar med forskrifta, eller at nettutstyr frå fleire nettilbydarar er samlokalisert i same anlegg, og PT vurderer at den samla betydinga av anlegget dermed er større enn det den enkelte nettilbydar har vurdert. Merk at nettilbydar skal, inntil eventuelle vedtak frå myndigheit om reklassifisering, halde seg til eiga klassifisering og sikre anlegget i samsvar med denne. Dersom det blir aktuelt for PT å reklassifisere eit anlegg vil vedtaket innehalde nye tidsfristar for gjennomføring av eventuelle endra krav.

2.5. § 5. Generelle krav til sikring

§ 5. *Generelle krav til sikring*

Nettilbydar skal på forsvarleg måte sikre nettutstyr i anlegg mot uønskt ytre fysisk påverknad. Omfanget av sikringstiltak skal vere basert på ei dokumentert heilskapleg risiko- og sårbarheitsvurdering.

Sikringstiltak på og i anlegg skal minst oppfylle krava gitt i § 6 - § 12.

Post- og teletilsynet kan pålegge at nettilbydar gjennomfører tiltak som går utover krava i § 6 - § 12 dersom det er nødvendig for å oppfylle kravet til forsvarleg sikring, jf. første ledd.

Denne føresegna er ein generell overbygning av sikringskrava i forskrifta. Som ledd i ROS-vurderinga skal nettilbydar identifisere hendingar som kan føre til uønskt ytre fysisk påverknad.

Omfanget av sikringstiltak skal samsvare med akseptabel risiko. I vurderinga av akseptabel risiko skal det leggast til grunn at ekomnettet skal kunne motstå ekstraordinære påkjenningar, jf. forarbeida[3] til ekomlova § 2-10 første ledd, der det står at:

> «Med kravet om nødvendig sikkerhet for bruker i *første ledd* menes at nett og tjenester skal sikres på en slik måte at bruker, selv i situasjoner der nettet utsettes for ekstraordinære påkjenninger, så langt som mulig skal kunne benytte grunnleggende elektroniske kommunikasjonstjenester.»

2.6. § 6. Skalsikring

§ 6. *Skalsikring*

Nettilbydar skal gjennom forsvarleg skalsikring av anlegg hindre at uvedkommande kan ta seg fram til eller påføre skade på nettutstyr.

Anlegg i klasse A, B og C skal ha skalsikring tilpassa anlegget sin klasse basert på relevante og forsvarlege normer eller standardar.

For anlegg i klasse A, B og C skal nettilbydar ha dokumenterte krav til etablering av skalsikring og dokumenterte rutinar for vedlikehald av skalsikringa.

[3] Ot.prp.nr.58 (2002-2003)

Skalsikring gjeld fasaden til anlegget, slik som veggar, golv, tak, vindauge, dørar, klatrehinder, osb. Skalsikringa er den fysiske barrieren som skal hindre uvedkommande å ta seg fram til eller påføre skade på nettutstyr. Med å hindre meinast her å forseinke, då det alltid vil vere mogleg å ta seg gjennom ei skalsikring ved hjelp av tilstrekkelege hjelpemiddel og tid.

Forskrifta stiller ikkje konkrete krav til form og nivå på skalsikringa. Nettilbydar skal ha skalsikring på eit nivå som samsvarar med ROS-vurderinga, jf. § 5. PT legg per i dag ikkje føringar for kva konkrete normer eller standardar som kan nyttast.

Tredje ledd inneber at nettilbydar skal ha eit eiget system for å forvalte skalsikring av sine anlegg i klasse A, B og C.

2.7. § 7. Tilgangskontroll og innbrotsalarm

§ 7. *Tilgangskontroll og innbrotsalarm*

Nettilbydar skal gjennom forsvarleg tilgangskontroll på anlegg sørgje for at personelltilgang til nettutstyr styrast av tenestlege behov.

Anlegg i klasse A, B og C skal ha tilgangskontrollsystem tilpassa anlegget sin klasse og omfang av personelltilgang, og som er basert på relevante og forsvarlege normer eller standardar. Tilgangskontrollsystemet skal minst vere basert på to-faktor autentisering.

Anlegg i klasse A, B og C skal ha innbrotsalarmsystem tilpassa anlegget sin klasse og omfang av skalsikring, basert på relevante og forsvarlege normer eller standardar. I innbrotsalarmsystemet skal det inngå responsapparat med moglegheit for utrykking.

For anlegg i klasse A, B, og C skal nettilbydar ha dokumenterte drifts- og vedlikehaldsrutinar for tilgangskontroll- og innbrotsalarmsystema som inkluderer rutinar for å handtere systemsvikt og straumbrot.

For anlegg i klasse A, B og C skal nettilbydar ha tilgangskontrollsystem som samsvarar med ROS-vurderinga, jf. § 5. PT legg per i dag ikkje føringar for konkrete normer eller standardar som kan nyttast.

Med responsapparat i tredje ledd meinast personell som skal ta imot og tolke alarmar og sette i verk hensiktsmessige responstiltak etter dokumenterte retningslinjer eller rutinar. Utrykking av vaktpersonell eller liknande til anlegget skal vere eit mogleg responstiltak.

2.8. § 8. Brannsikring

§ 8. *Brannsikring*

Nettilbydar skal gjennom forsvarleg brannsikring på anlegg hindre skade på nettutstyr som følgje av brann.

Anlegg i klasse A, B og C skal ha brannvarslings- og brannslukkingssystem tilpassa anlegget sin klasse, fysiske utforming og omgjevnad, basert på relevante og forsvarlege normer eller standardar.

For anlegg i klasse A, B, og C skal nettilbydar ha dokumenterte drifts- og vedlikehaldsrutinar for brannvarslings- og brannslukkingssystemet som inkluderer rutinar for å handtere systemsvikt og straumbrot.

For anlegg i klasse A, B og C skal brannvarslings- og brannslukkingssystema samsvare med ROS-vurderinga, jf. § 5. PT legg per i dag ikkje føringar for konkrete normer eller standardar som kan nyttast.

2.9. § 9. Sikring mot EMP/HPM-våpen

§ 9. *Sikring mot EMP/HPM-våpen*

Nettilbydar skal opprettholde eksisterande sikring av nettutstyr mot EMP/HPM-våpen i anlegg i klasse A, B og C. Reduksjon av sikringsnivå kan godkjennast av Post- og teletilsynet.

Før etablering av nytt anlegg, eller ombygging av eksisterande anlegg, i klasse A eller B, skal nettilbydar legge fram for Post- og teletilsynet ei kvalifisert vurdering av aktuelle sikringstiltak mot EMP/HPM-våpen.

Post- og teletilsynet kan pålegge nettilbydar å sikre nettutstyr mot EMP/HPM-våpen.

Føresegna omfattar ikkje sikring mot naturskapt EMP (lyn eller andre naturlege elektriske utladningar) og elektromagnetisk interferens.

Enkelte nettilbydarar har i dag anlegg som er sikra særskilt mot EMP/HPM-våpen. Føresegna krev at slik sikring på anlegg i klasse A, B og C skal opprettholdast, med mindre anna er avtalt med PT. Ved etablering av anlegg i klasse A og B stillast det i andre ledd krav om at nettilbydar gjennomfører ei kvalifisert vurdering av aktuelle sikringstiltak mot EMP/HPM-våpen, og legg denne fram for PT. Her bør det òg inngå ei kostnadsvurdering. Med kvalifisert vurdering meinast det at vurderinga skal gjennomførast av personell med særskilt kompetanse på området.

Vurderinga av sikringstiltak kan spenne frå omfattande EMP-skjermingstiltak til å sørgje for forsvarleg tilgang til reservemateriell eller at det i anlegg etablerast god avstand mellom nettutstyr og publikum for auke sikkerheita mot HPM-våpen. PT tilrår at nettilbydar i forkant av ei slik vurdering avklarar med PT eventuelle avgrensingar, med bakgrunn i gjeldande trugselbilete.

2.10. § 10. Hjelpeteknisk utstyr

§ 10. *Hjelpeteknisk utstyr*

Nettilbydar skal sørgje for forsvarleg driftssikkerheit til hjelpeteknisk utstyr.

Anlegg i klasse A og B skal ha tilgang til tilstrekkeleg hjelpeteknisk utstyr i reserve for å opprettholde drift av nettutstyr ved svikt i det hjelpetekniske utstyret.

Anlegg i klasse A og B skal ha reservestraumforsyning som utan avbrot kan forsyne nettutstyr med tilstrekkeleg straum i minst tre døgn. Anlegg i klasse C skal ha reservestraumforsyning som utan avbrot kan forsyne nettutstyr med tilstrekkeleg straum i minst to døgn.

For anlegg i klasse A, B, og C skal nettilbydar ha dokumenterte og forsvarlege drifts- og vedlikehaldsrutinar for hjelpeteknisk utstyr, som inkluderer rutinar for å handtere systemsvikt og eventuell transport av drivstoff og mobilt utstyr.

Formålet med andre ledd er at drifta av nettutstyr i anlegg i klasse A og B skal kunne opprettholdast dersom det hjelpetekniske utstyret (straumforsyningsutstyret, reservestraumforsyninga eller kjølesystemet) sviktar.

Med «å opprettholde» meinast det at nettutstyret i minst mogleg grad skal påverkast av svikt i det hjelpetekniske utstyret. Dette inneber at nettilbydar skal legge til rette for raskt å kunne reparere eller erstatte hjelpeteknisk utstyr som sviktar. Ein måte å innfri kravet på kan vere å ha reservedelslager som inneheld komponentane som, t.d. i følgje produsenten av det hjelpetekniske utstyret, er mest utsett for slitasje eller svikt. Eit anna alternativ kan vere å ha fullt ut redundant hjelpeteknisk utstyr som t.d. å ha eit mobilt aggregat tilgjengeleg i tillegg til eit fast installert aggregat i anlegget. Val av reserveløysing, dvs. kva nettilbydar vurderer er «tilstrekkeleg», skal vere godt fundert i ROS-vurderinga. Omfanget av reserveløysinga kan justerast i forhold til om nettutstyret i anlegget er duplisert i eit anna A- eller B-anlegg (redundans).

Med «utan avbrot» i tredje ledd meinast at reservestraumforsyninga skal dimensjonerast slik at, ved svikt i den innkomne straumforsyninga, så skal UPS kunne oppretthalde kontinuerleg straumforsyning til nettutstyret inntil ei reservestraumkjelde kan overta lasta. Reservestraumkjelda skal deretter kunne forsyne

nettutstyret med tilstrekkeleg straum i høvesvis to eller tre døgn utan nettstraum. Reservestraumforsyninga kan vere fast installert eller mobil. Dette gjeld òg for tilgangen til drivstoff. Mobile løysingar inneber ofte fleire innsatsfaktorar enn fast installerte løysingar, og kan difor medføre auka risiko. Val av løysingar for å innfri krava i føresegna, og særleg mobile løysingar, må vere godt fundert i ROS-vurderinga.

Merk at ved svikt i reservestraumforsyning, gjeld første ledd. Det inneber at avbrot kan aksepterast, men at nettilbydar raskt skal kunne re-etablere reservestraumforsyninga.

2.11. § 11. Lokalisering

§ 11. *Lokalisering*

Nettilbydar skal ved etablering av anlegg lokalisere anlegget slik at risikoen for skade på nettutstyr frå omgjevnadane blir minst mogleg.

For anlegg i klasse A og B, og ved etablering av nytt anlegg i klasse A eller B, skal nettilbydar også innhente relevant dokumentasjon om risikoen for skade på nettutstyr frå omgjevnadane, som inkluderer risiko- og sårbarheitsvurderingar gjennomført av lokale beredskapsmyndigheiter.

Der anlegg i klasse A og B likevel er, eller vil bli, etablert i omgjevnadar som medfører høg risiko for skade på nettutstyr skal nettilbydar sikre anlegget særskilt mot den identifiserte risikoen.

Identifisering av risiko knytt til oppføring av bygg og andre installasjonar kjem mellom anna fram av Lov om planlegging og byggesaksbehandling (plan- og bygningslova), der det etter § 4-3 skal utarbeidast ROS-analyse for å dokumentere om arealet er eigna til utbygging, og § 28-1 som stiller krav om tilstrekkeleg sikkerheit før areal kan byggast ut.

Risikokriteria som er gjeldande i plan- og bygningslova dekkjer typisk opp for nærleik til verksemder med farlege stoffar og naturskade som skred, flom, havnivåstigning osb. Det generelle kravet i klassifiseringsforskrifta § 11 første ledd gjeld difor risiko for skade på nettutstyr som går ut over risikokriteria dekt opp gjennom plan- og bygningslova. Slike risikokriterier kan vere fysisk tilknyting til trafikknutepunkt, eller fysisk tilknyting til nøkkelfunksjonar eller anna spesiell verksemd som kan vere særleg utsett for alvorlege kriminelle handlingar, inkludert terrorhandlingar.

I følgje § 11 andre ledd skal nettilbydar gjere seg særskilt kjent med ROS-vurderingar gjennomført av regionale eller lokale beredskapsmyndigheiter (Fylkesmannen eller kommunen) der anlegg i klasse A og B er lokalisert. I medhald av Forskrift om kommunal beredskapsplikt er alle kommunar pålagt å utarbeide ein heilskapleg ROS-vurdering for sin kommune. Likeins er Fylkesmannen pålagt å gjennomføre Fylkes-ROS. PT føreset at relevante ROS-vurderingane som blir henta inn blir tatt inn i den heilskaplege ROS-vurderinga som nettilbydar pliktar å gjennomføre, jf. § 5.

2.12. § 12. Samlokalisering

§ 12. *Samlokalisering*

Dersom det på anlegg i klasse A, B eller C er samlokalisering, skal nettilbydar gjennomføre ei dokumentert og forsvarleg vurdering av om eiget nettutstyr i anlegget skal sikrast særskilt mot ytre fysisk påverknad frå andre samlokaliseringsaktørar. Vurderinga kan ta omsyn til sikringstiltaka elles på anlegget.

Nettilbydar skal sikre eiget nettutstyr i samsvar med vurderinga i første ledd.

Det kan leggast til grunn at personell som har rettmessig tilgang til anlegget i utgangspunktet ikkje har til hensikt å påføre skade på andre sitt nettutstyr. Nettilbydar er likevel, jf. § 7 første ledd, ansvarleg for at personelltilgang til nettutstyr styrast av tenestlege behov.

Avhengig av korleis anlegget er innretta må nettilbydar vurdere risikoen for at andre samlokaliseringsaktørar utilsikta kan påverke nettutstyret. Dette må funderast i ROS-vurderinga, jf. § 5. I vurderinga bør nettilbydar ta omsyn til korleis nettutstyret til dei ulike samlokaliseringsaktørane er separert, merka og sikra i anlegget, og omfanget av personelltilgangen til anlegget.

2.13. § 13. Eksterne aktørar

§ 13. *Eksterne aktørar*

Der andre aktørar på vegne av nettilbydar utfører tiltak etter § 5 - § 12 på anlegg i klasse A, B eller C, er nettilbydar ansvarleg for at det ligg føre skriftlege avtalar som sikrar utføringa av desse tiltaka. Slike avtalar skal ikkje vere til hinder for at nettilbydar eller Post- og teletilsynet kan føre tilsyn med utføringa av tiltaka.

Formålet med denne føresegna er å sikre at rollar og ansvar mellom nettilbydar og eksterne aktørar som på vegne av nettilbydar utfører tiltak etter §§ 5 – 12 på anlegg i klasse A, B eller C er tydeleg avklart gjennom skriftlege avtalar. Til dømes må nettilbydar som innplasserer nettutstyr i anlegg der eigaren av anlegget står for drift- og vedlikehald av hjelpeteknisk utstyr, sørgje for at det føreligg avtale som dokumenterer at det hjelpetekniske utstyret er i samsvar med krava § 10.

2.14. § 14. Rapportering

§ 14. *Rapportering*

Nettilbydar skal rapportere til Post- og teletilsynet oversyn over anlegga i klassane A, B og C, inkludert vurderinga som ligg til grunn for klassifiseringa. Rapportering skal skje ved den første klassifiseringa og deretter årleg. Post- og teletilsynet kan fastsette retningslinjer for rapporteringa.

Ved første gongs klassifisering skal følgjande rapporterast:

(1) Komplett oversyn over anlegg i klasse A, B og C. Kva for data som skal rapporterast for kvart anlegg følgjer av rapporteringsmal som vil være tilgjengeleg på nettsidene til Post- og teletilsynet.
(2) Vurderinga som ligg til grunn for klassifiseringa, der det kjem fram korleis nettilbydar har valt å systematisere klassifiseringa med bakgrunn i eigen infrastruktur, eventuelle proprietære klassifiseringsregimar, eventuell redundans osb. Vurderinga skal vere på eit overordna nivå (per klasse), og ikkje ei vurdering av kvart enkelt anlegg.

Årlig rapporteringsfrist etter dette er 1. april. Då skal følgjande rapporterast:

(1) Alle endringar av rapporteringspliktige data, slik som nye rapporeringspliktige anlegg, endringar i data på tidlegare rapporterte anlegg og avvikling (ev. nedklassifisering til klasse D) av tidligare rapporterte anlegg. Dersom det ikkje er gjort nokon endringar av rapporteringspliktige data sidan førre rapportering, skal nettilbydar informere om dette.
(2) Vurderinga som ligg til grunn for endringane.
(3) Talet på anlegg i klasse B og i klasse C. Dette skal bidra til å kontrollere at oversynet over klassifiserte anlegg som PT sit på er riktig. (Merk at talet på anlegg i klasse A skal ikkje rapporterast her.)

Dersom netttilbydar skal rapporterere om anlegg i klasse A skal oversendinga skje i medhald av Forskrift om informasjonssikkerhet (minimum BEGRENSET). Ved rapportering av anlegg i klasse B og C skal oversendinga skje i ordinær post til Post- og teletilsynet, Postboks 93, 4791 Lillesand (CD-ROM, minnepinne etc.).

Merk at nettilbydar sjølv må oppbevare dokumentasjon over klassifiserte anlegg på ein forsvarleg måte.

Nettilbydarar som har klassifisert alle anlegg i klasse D har ikkje rapporteringsplikt. Merk at PT, gjennom tilsyn jf. § 15, likevel kan be om å få innsyn i vurderinga som ligg til grunn for klassifiseringa også for desse nettilbydarane.

2.15. § 15. Tilsyn, pålegg og sanksjonar

§ 15. *Tilsyn, pålegg og sanksjonar*

Post- og teletilsynet fører tilsyn med føresegnene i denne forskrifta, jf. ekomlova § 10-1.

Post- og teletilsynet kan gi pålegg om retting av forhold for å sikre samsvar med krav fastsett i denne forskrifta, jf. ekomlova § 10-6.

Brot på krava i denne forskrifta kan føre til tvangsmulkt, jf. ekomlova § 10-7, bot, jf. ekomlova § 10-13 første ledd nr. 2 eller straff, jf. ekomlova § 12-4 første ledd nr. 2.

Ingen merknadar.

2.16. § 16. Dispensasjon

§ 16. *Dispensasjon*

Post- og teletilsynet kan i særlege tilfelle gjere unntak frå forskrifta eller frå føresegner i denne forskrifta.

PT legg ikkje føringar for kva særlege tilfelle som skulle gi grunnlag for dispensasjon frå forskrifta eller frå enkelte føresegner i forskrifta. Dispensasjon vil måtte vurderast i kvart enkelte tilfelle.

2.17. § 17. Klageinstans

§ 17. *Klageinstans*

Klage over enkeltvedtak fatta av Post- og teletilsynet i medhald av denne forskrifta avgjerast av departementet, jf. ekomlova § 11-6.

Ingen merknadar.

2.18. § 18. Ikraftsetjing

§ 18. *Ikraftsetjing*

Forskrifta trer i kraft 1. januar 2013.

Ingen merknadar.

2.19. § 19. Fristar for gjennomføring

§ 19. *Fristar for gjennomføring*

Klassifisering, jf. § 4, og rapportering, jf. § 14, skal vere gjennomført seinast 1. april 2013.

Tiltak etter § 5 - § 13 skal vere gjennomført seinast 1. juli 2014.

Post- og teletilsynet kan gi utsetjing med å oppfylle krava i denne forskrifta.

Ingen merknadar.