REGLUGERÐ
um öryggi fjarskiptaneta og fjarskiptaþjónustu.

I. KAFLI
Almenn ákvæði

1. gr.
Gildissvið.

Reglugerð þessi gildir um fjarskiptafyrirtæki sem veita almenna fjarskiptaþjónustu og/eða reka almenn fjarskiptanet og upplýsingakerfi sem við þau tengjast, sem og öll fjarskiptanet sem notuð eru fyrir neyðar- og öryggisfjarskipti.

2. gr.
Markmið.

Markmið reglugerðarinnar er að stuðla sem best að áfallaþoli og samfelldri öruggri virkni fjarskiptaneta og fjarskiptaþjónustu, svo og vernd fjarskiptaumferðar, með því að kveða nánar á um lágmarkskröfur til skipulags net- og upplýsingaöryggis og umgjarðar áhættustýringar fjarskiptafyrirtækja. Enn fremur að tryggja samhæfð viðbrögð við ógnum og öryggisatvikum sem hafa eða geta haft skaðleg áhrif á öryggi fjarskiptaneta og fjarskiptaþjónustu.

3. gr.
Orðskýringar.

Í reglugerð þessari merkir:

1. *Aðgangsstýring:* Aðferð til þess að tryggja að aðgangur að kerfum, búnaði, gögnum, rýmum eða öðru takmarkist við aðila með gilda aðgangsheimild.
2. *Atburður:* Óviðbúin staða, óþekkt eða þekkt, sem getur skipt máli fyrir öryggi fjarskiptaneta og fjarskiptaþjónustu, sem og net- og upplýsingakerfa sem við þau tengjast, eða skert þjónustu fjarskiptafyrirtækis.
3. *Eignir:* Hvers konar efnislegir og óefnislegir þættir í starfsemi fjarskiptafyrirtækja sem teljast til verðmæta þeirra.
4. *Fjarskiptarými:* Aðstaða sem hýsir fjarskiptanet, þ.m.t. fjarskiptabúnað og samtengingar innan og á milli fjarskiptaneta og allan tengdan búnað.
5. *Keðjuútvistun:* Þegar þjónustuveitandi fjarskiptafyrirtækis útvistar áfram þjónustuþáttum sem kveðið er á um í samningi aðila, að hluta eða heild, til fjórða aðila.
6. *Landsdekkandi stofnnet:* Fjarskiptanet, þ.m.t. fjarskiptarými, sem notað er til að tengja saman alla landsfjórðunga eða þjóna fjarskiptasambandi við útlönd.
7. *Útvistun:* Verkefni eða þjónusta sem fellur undir starfsemi fjarskiptafyrirtækis sem nauðsynleg er fyrir virkni, vernd eða stjórnun fjarskipta og sinnt er eða veitt af öðrum aðila, þjónustuveitanda.

Að öðru leyti gilda orðskýringar í lögum um fjarskipti.

II. KAFLI
Áhættumiðuð nálgun og mikilvægar eignir

4. gr.
Áhættumiðuð nálgun.

Fjarskiptafyrirtæki skal meta og stýra áhættu sem steðjað getur að öryggi fjarskiptaneta og fjarskiptaþjónustu í samræmi við lög um fjarskipti og reglugerð þessa, þar með talið vegna útvistunar þátta í starfsemi sinni og fátíðra atburða sem geta haft alvarlegar afleiðingar.

Ráðstafanir fjarskiptafyrirtækis á grundvelli reglugerðarinnar skulu miðast við að tryggja fullnægjandi öryggi fjarskiptaneta og fjarskiptaþjónustu með tilliti til þeirrar áhættu sem fram kemur í áhættumati.

5.gr.

Mikilvægar eignir.

Fjarskiptafyrirtæki skal skilgreina þær eignir sem notaðar eru í rekstri fjarskiptanets og við veitingu fjarskiptaþjónustu. Þar skal lýsa sérstaklega eignum sem teljast mikilvægar í rekstri fjarskiptanets eða við veitingu fjarskiptaþjónustu, notkun þeirra, virkni og samtengingum við önnur fjarskiptanet ef við á. Skulu mikilvægar eignir hafa forgang þegar kemur að ráðstöfunum er varða öryggi fjarskiptaneta og fjarskiptaþjónustu.

Landsdekkandi stofnnet, teljast ávallt til mikilvægra eigna í skilningi reglugerðar þessarar.

Fjarskiptastofu er heimilt að setja frekari leiðbeiningar um skilgreiningu og flokkun mikilvægra eigna m.t.t. heildstæðis fjarskiptaneta og fjarskiptaþjónustu.

III. KAFLI
Skipulagslegar ráðstafanir.

6. gr.

Stjórnskipulag öryggis.

Fjarskiptafyrirtæki skal eftir fremsta megni tryggja öryggi og virkni fjarskiptaneta sem það rekur, þeirrar fjarskiptaþjónustu sem það veitir og þeirra upplýsinga sem um fjarskiptanet fara.

Fjarskiptafyrirtæki ber að útbúa og viðhalda skjalfestri lýsingu á stjórnskipulagi öryggis fjarskiptaneta og fjarskiptaþjónustu. Þar skal með skýrum hætti skilgreina hlutverk og ábyrgð stjórnenda og starfsfólks, svo og ytri aðila ef við á, sem bera ábyrgð á skipulagi net- og upplýsingaöryggis, framkvæmd áhættumats og öryggisráðstafana. Þá skal vera skýrt í skipulagi fjarskiptafyrirtækis hver ber ábyrgð á framkvæmd öryggismála.

Við framkvæmd áhættustýringar og öryggisráðstafana í starfsemi sem fellur undir gildissvið reglugerðar þessarar, skal fjarskiptafyrirtæki byggja á nýjustu útgáfu af gildandi alþjóðlega viðurkenndum stöðlum um bestu framkvæmd á sviði net- og upplýsingaöryggis. Það á bæði við um almenna staðla á borð við ISO/IEC 27001, 27002, 27005 og aðra sértæka staðla og reglur á sviði fjarskipta, t.a.m. ISO/IEC 27011.

7. gr.

Öryggisstefna.

Fjarskiptafyrirtæki skal útbúa og viðhalda skriflegri stefnu um upplýsingaöryggi. Í stefnunni skal tilgreina markmið og meginreglur net- og upplýsingaöryggis og hvernig öryggi fjarskiptaneta og fjarskiptaþjónustu er best tryggt.

Stefnan skal samþykkt með formlegum hætti af stjórn fjarskiptafyrirtækis, eða eftir atvikum æðstu stjórnendum, og birt öllu starfsfólki. Skal hún sérstaklega kynnt starfsfólki sem starfar með beinum eða óbeinum hætti við rekstur og öryggi fjarskiptaneta og fjarskiptaþjónustu.

Öryggisstefnu skal rýna og uppfæra eftir því sem tilefni er til, t.a.m. ef upp koma öryggisatvik eða á grundvelli niðurstöðu úttekta og prófana, að lágmarki á tveggja ára fresti.

8. gr.

Áhættustjórnun og áhættumat.

Fjarskiptafyrirtæki skal viðhafa virka áhættustjórnun og framkvæma áhættumat á öryggi fjarskiptaneta og fjarskiptaþjónustu á grundvelli viðurkenndrar aðferðarfræði, með það að markmiði að skapa forsendur fyrir vali á öryggisráðstöfunum og draga úr áhættu sem steðjað getur að öryggi fjarskiptaneta þess og veitingu fjarskiptaþjónustu.

Við gerð áhættumats skal bera kennsl á nauðsynlegar ráðstafanir og viðhafa aðgerðir til að stjórna fjarskiptanetum og fjarskiptaþjónustu með tilliti til áhættu á hverjum tíma.

Áhættumat skal vera skriflegt. Það skal framkvæmt reglubundið og aðferðafræði þess endurmetin, hvort tveggja á a.m.k. tveggja ára fresti. Ávallt skal leggja mat á hvort öryggisatvik, ógnir, viðamiklar breytingar á rekstri eða niðurstöður úttekta og prófana á fjarskiptanetum gefi tilefni til endurskoðunar á áhættumati og bregðast strax við ef forsendur áhættumats eða aðstæður breytast sem kalla á slíkt endurmat.

Framkvæmd áhættumats samkvæmt 1.-3. mgr. skal að lágmarki ná yfir eftirfarandi atriði:

a. Eignir skulu skilgreindar og metnar með tilliti til helstu veikleika og/eða ógna sem steðjað geta að þeim, þar á meðal rýrnun trausts.
b. Bera skal kennsl á áhættuþætti, með því að greina áhættu, meta líkur á því að þeir eigi sér stað og áhrifum sem þeir kunna að hafa auk þess að ákvarða áhættustig þeirra. Áhættu skal forgangsraðað í ljósi skilgreindra og skriflegra viðmiða um ásættanlega áhættu og markmiða sem sett hafa verið í öryggisstefnu fjarskiptafyrirtækisins.
c. Leggja skal mat á að hvaða marki rekstur fjarskiptaneta eða upplýsingakerfa sem við þau tengjast, eða veiting fjarskiptaþjónustu, er háð afhendingu á vöru eða þjónustu frá þriðju aðilum (s.s. birgjum eða þjónustuveitendum), svo og möguleg áhrif ef rof verður á slíkri afhendingu. Hér skal einnig líta til þess hvort, og þá hvernig, röskun á starfsemi kerfa/búnaðar þriðju aðila kann að hafa áhrif á rekstur fjarskiptaneta og veitingu fjarskiptaþjónustu.

Ef niðurstöður áhættumats skv. 1.-4. mgr. gefa tilefni til sérstakra öryggisráðstafana skal fjarskiptafyrirtæki bregðast skjótt við og m.a. byggja á gildandi alþjóðlega viðurkenndum stöðlum um bestu framkvæmd á sviði net- og upplýsingaöryggis sbr. 6. og 9. gr. reglugerðarinnar.

Ef Fjarskiptastofa óskar, skal fjarskiptafyrirtæki framkvæma sértækt áhættumat á einstökum hlutum fjarskiptaneta eða fjarskiptaþjónustu eða sérstökum ógnum sem steðjað geta að upplýsingum, fjarskiptanetum eða fjarskiptaþjónustu. Fjarskiptastofa getur í beiðni um sértækt áhættumat skilgreint aðferðarfræði við framkvæmd þess.

9. gr.

Almennar öryggisráðstafanir.

Fjarskiptafyrirtæki skal innleiða viðeigandi öryggisráðstafanir til að tryggja öryggi og koma til móts við og takmarka áhrif af áhættu við rekstur fjarskiptaneta og veitingu fjarskiptaþjónustu. Öryggisráðstafanir skulu skjalfestar, þar á meðal viðeigandi verkferlar.

Öryggisráðstafanir skulu taka mið af alþjóðlegum stöðlum um bestu framkvæmd. Enn fremur skal fjarskiptafyrirtæki byggja á eigin reynslu af fyrri ráðstöfunum og meðhöndlun öryggisatvika.

Öryggisráðstafanir geta m.a. tengst hönnun, þróun, rekstri, prófunum og viðhaldi fjarskiptaneta, kerfa og búnaðar, sem og raunlægri vernd fjarskiptarýma eða tengdrar aðstöðu í skilningi laga um fjarskipti.

Við framkvæmd áhættumats skv. 1. – 4. mgr. 8. gr. skal leggja heildstætt mat á öryggisráðstafanir. Fjarskiptafyrirtæki skal endurskoða öryggisráðstafanir eftir því tilefni er til,

svo sem í kjölfar öryggisatvika, innri og ytri úttekta og prófana eða ef aðrar aðstæður breytast, þó að a.m.k. á tveggja ára fresti.

10. gr.

Öryggisráðstafanir vegna starfsfólks og þriðju aðila.

Fjarskiptafyrirtæki skal skilgreina og skjalfesta ábyrgð og skyldur starfsfólks og þriðju aðila með tilliti til öryggis fjarskiptaneta og fjarskiptaþjónustu og framkvæmd verkferla sem það varðar. Þannig skal á hverjum tíma liggja skýrt fyrir hvaða starfsfólk eða þriðju aðilar gegna þar lykilhlutverki. Tryggja skal með virkum boðleiðum að ávallt náist í viðkomandi starfsmenn eða þriðju aðila.

Fjarskiptafyrirtæki skal þjálfa starfsfólk sitt og þriðju aðila með reglubundnum hætti og eftir atvikum prófa þekkingu þeirra á þeim lögum og reglum sem gilda um öryggi fjarskiptaneta og fjarskiptaþjónustu, ferlum og starfsskyldum. Þá skal vera til staðar verkferill sem tekur á brotum í starfi og afleiðingar við þeim.

Fjarskiptafyrirtæki skal grípa til eftirfarandi öryggisráðstafana í þeim tilgangi að fyrirbyggja og takmarka tjón vegna mistaka, svika eða og annarrar misnotkunar starfsfólks fjarskiptafyrirtækis eða þriðja aðila sem vegna starfa sinna hafa aðgang að fjarskiptanetum:

a. Viðhafa skilgreint verkferli sem staðfestir hæfni starfsfólks og þriðja aðila, m.t.t. menntunar og reynslu.
b. Afla sakavottorðs eða annarrar öryggisvottunar umsækjanda áður en starf er veitt eða gengið er til samninga við þriðju aðila þegar starfssvið eða þjónusta varðar virkni, vernd, stjórnun fjarskipta eða verkefni á grundvelli XIII. kafla fjarskiptalaga. Við mat á öflun öryggisvottunar skal líta til ábyrgðar sem starfi eða verkefni fylgir.
c. Gera kröfu um undirritun trúnaðaryfirlýsinga.

Ákvæði 2. - 3. mgr. skal ekki eiga við um þriðju aðila sem sinna afmörkuðum verkefnum innan fjarskiptarýma sem ekki teljast til mikilvægra eigna skv. 5. gr.

11. gr.

Útvistun.

Fjarskiptafyrirtæki sem útvistar starfsemi sem nauðsynleg er fyrir virkni, vernd eða stjórnun fjarskipta skal meta áhættu er varðar þjónustuveitandann, m.a. meta hæfni hans og reynslu af fjarskiptastarfsemi og fjárhagslega stöðu. Þá skal fjarskiptafyrirtæki setja sér stefnu um öryggiskröfur sem skulu vera til staðar í samningum við þriðja aðila. Stjórnunarlegri ábyrgð á net- og upplýsingaöryggi og áhættustýringu verður þó ekki útvistað.

Ef þjónustu er útvistað út fyrir íslenska lögsögu skal fara eftir 7. mgr. 78. gr. laga um fjarskipti, auk þess sem áhættumat, skv. 1. mgr., skal ná til eignarhalds þjónustuveitandans og þess lagaumhverfis sem hann starfar í m.t.t. samþýðanleika þess við íslensk lög.

Í þjónustusamningi um útvistun skal afmarka á skýran hátt hlutverk og skyldur aðila, tilgreina með skýrum hætti þá þjónustu sem fjarskiptafyrirtæki er veitt, þjónustustig sem stefnt er að svo og þau kerfi, aðstöðu og búnað sem notaður er vegna þjónustunnar sem um ræðir. Þá skal kveða á um hvort og að hvaða leyti keðjuútvistun sé heimil sem og þá skyldu þjónustuveitanda að uppfylla skuli ákvæði laga og þessarar reglugerðar og starfa í samræmi við fyrirmæli fjarskiptafyrirtækis. Í þjónustusamningi skal tilgreina öryggiskröfur, kveða á um trúnaðarskyldu og tilgreina tengiliði og boðleiðir.

Í þjónustusamningi skal einnig kveða á um upplýsingaskyldu þjónustuveitanda til fjarskiptafyrirtækis um öryggisatvik og rekstrarbreytingar er varða útvistaða þjónustu. Fjarskiptafyrirtæki er heimilt að fela þjónustuveitanda á grundvelli þjónustusamnings að tilkynna um alvarleg öryggisatvik sbr. 20. gr.

Þá skal í þjónustusamningi tryggja að Fjarskiptastofa hafi aðgang að viðeigandi upplýsingum frá þjónustuveitanda vegna framkvæmdar eftirlits á grundvelli laga um fjarskipti

og reglugerðar þessarar. Einnig skal tryggja aðgengi Fjarskiptastofu að fjarskiptarýmum við framkvæmd eftirlits. Skal fjarskiptafyrirtæki hafa virkt eftirlit með því að ákvæðum þjónustusamnings sé fylgt.

Ábyrgð á uppfyllingu lágmarkskrafna laga um fjarskipti og reglugerðar þessarar, m.a. um áhættustýringu og viðbúnað, hvílir á fjarskiptafyrirtæki, þar á meðal ábyrgð á því að tilkynningarskyldu um öryggisatvik sé fullnægt, óháð mögulegri útvistun þátta í starfsemi þess til sérhæfðra þjónustuveitenda.

IV. KAFLI
Tæknilegar ráðstafanir.

12. gr.
Kerfislægar ráðstafanir.

Fjarskiptafyrirtæki skal, á grundvelli áhættumiðaðs verklags og niðurstöðu áhættumats, gera þær tæknilegu öryggisráðstafanir sem nauðsynlegar eru til að tryggja öryggi fjarskiptaneta og fjarskiptaþjónustu þess. Að lágmarki skal viðhafa eftirfarandi ráðstafanir vegna kerfislægs öryggis:

a. Kerfislæg aðgangsstýring:
    1. Innleiða aðgangsstýringarkerfi til auðkenningar á notendum og kerfum.
    2. Takmarka aðgangsheimildir starfsfólks, þriðju aðila og kerfa að upplýsingum og kerfum við það sem þeim er nauðsynlegt til að sinna starfi eða hlutverki sínu og við þann tíma sem nauðsynlegur er.
    3. Framfylgja skráðu verkferli sem gerir ráð fyrir að veiting aðgangsheimilda sé skráð og rekjanleg með formlegum hætti yfirfara þær eftir þörfum, þ.m.t. við breytingar á starfslýsingum og hlutverkum sem og við starfslok.
    4. Viðhafa ráðstafanir sem tryggja rekjanleika aðgangs, uppflettinga og vinnsluaðgerða.
b. Nota áreiðanlegan og afkastamikinn búnað fyrir stjórnun fjarskiptaneta með getu til aðgerða á borð við virkjun annarra fjarskiptaleiða og endurstillingu fjarskiptanets í eðlilegt ástand.
c. Skjalfesta samskipan kerfis.
d. Haga kerfum með þeim hætti að þau takmarki dreifingu og/eða útbreiðslu öryggisatvika.
e. Haga tæknilegum rekstri fjarskiptaneta með þeim hætti að breytingar á högun þeirra þ.m.t. ný virkni, sem og prófanir á þeim, fari fram utan rekstrarumhverfis fjarskiptaneta og með því fyrirbyggja eins og kostur er óheimilan aðgang að fjarskiptanetum eða rekstrartruflanir þeirra.
f. Vakta fjarskiptaumferð um fjarskiptanet og greina t.a.m. ummerki um öryggisatvik.
g. Viðhalda órofinni slóð gagna með notkun atburðaskráningar í eftirlitskerfum, sem nýtist við greiningu öryggisatvika.
h. Vakta og innleiða allar nauðsynlegar öryggisuppfærslur net- og upplýsingakerfa.
i. Taka öryggisafrit af kerfum og gögnum er varða rekstur fjarskiptaneta og fjarskiptaþjónustu og prófa þau með reglubundnum hætti.
j. Skilgreina og framfylgja verklagsreglum um meðferð og eyðingu gagna um fjarskipti, þ.m.t. verklagsreglum sem þau skulu setja í tengslum við rannsókn sakamála samkvæmt 92. gr. fjarskiptalaga.
k. Innleiða viðurkenndar öryggisráðstafanir eins og ítarlegar varnir gegn, t.a.m. vírusum, kóðum innspýtingu og öðrum óværum og spilliforritum sem geta breytt virkni kerfa.
l. Setja sér dulkóðunarstefnu og nota dulkóðun þar sem við á, til að fyrirbyggja og/eða lágmarka áhrif öryggisatvika.

m. Framkvæma skal öryggisúttektir og -prófanir á mikilvægum kerfum reglulega og ávallt þegar ný kerfi eru innleidd og í kjölfar breytinga á þeim.

13. gr.

Raunlægar ráðstafanir.

Fjarskiptafyrirtæki skal, á grundvelli áhættumiðaðs verklags og niðurstöðu áhættumats, gera þær raunlægu öryggisráðstafanir sem nauðsynlegar eru til að tryggja öryggi fjarskiptaneta og fjarskiptaþjónustu þess. Þó skal ávallt viðhafa að lágmarki eftirfarandi öryggisráðstafanir:

a. Raunlæg aðgangsstýring:
    1. Hindra óleyfilegan aðgang að fjarskiptarýmum með traustum hurðum og læsingum.
    2. Stýra og takmarka aðgengi að fjarskiptabúnaði eftir því sem við á, t.d. með læstum skápum.
    3. Takmarka aðgangsheimildir starfsfólks og ytri aðila við þau fjarskiptarými og fjarskiptabúnað sem þeim er nauðsynlegt að hafa aðgang að til að sinna starfi eða hlutverki sínu og við þann tíma sem nauðsynlegur er.
    4. Framfylgja verkferli sem gerir ráð fyrir að veiting aðgangsheimilda að fjarskiptarýmum og fjarskiptabúnaði sé skráð og rekjanleg með formlegum hætti og yfirfara þær eftir þörfum, þ.m.t. við breytingar á starfslýsingum og hlutverkum sem og við starfslok, hvort tveggja hjá starfsmönnum og þriðja aðila.
    5. Sé um mikilvæga eign að ræða sbr. 5. gr. skal aðgangi stýrt með notkun aðgangskorts eða sambærilegs auðkennis og með því tryggja rekjanleika aðgangs. Aðgangsheimildir skulu yfirfarnar reglulega og þegar tilefni er til, að lágmarki árlega.
b. Raunlægar varnir í fjarskiptarýmum:
    1. Tryggja, eftir því sem við á, að fjarskiptarými og annar frágangur byggingar þar sem fjarskiptarými er staðsett, sé úr eldtefjandi efni sem ver fjarskiptarýmið fyrir eldsvoða. Gegntök skulu vera reykþétt og eldvarin.
    2. Fjarskiptarými skulu vera varin fyrir raka- og vökvaskemmdum, ef við á með notkun lekapanna og öðrum viðeigandi ráðstöfunum, svo sem ef vatns- og hitaveitulagnir liggja um fjarskiptarými. Haga frágangi búnaðar og lagna þannig að hann verði ekki fyrir skaða ef vökvi lekur inn í fjarskiptarýmin, t.d. með því að lyfta búnaði frá gólfi.
    3. Gera ráðstafanir til að fyrirbyggja eins og kostur er innbrot og skemmdarverk í fjarskiptarými, svo sem með því að hafa rými gluggalaus eða verja glugga sérstaklega gegn innbrotum.
    4. Sé um mikilvæga eign að ræða sbr. 5. gr. skal þar að auki:
        a. Útbúa fjarskiptarými með kæli- og/eða loftræstikerfi.
        b. Útbúa fjarskiptarými með brunaviðvörunarkerfi og slökkvitæki.
        c. Útbúa fjarskiptarými þannig að byggingarefni sé úr eldtefjandi efni og rými séu gluggalaus.
        d. Ganga þannig frá fjarskiptarými að raunlæg aðgangsstýrð aðgreining sé á milli búnaðar mismunandi fjarskiptafyrirtækja.
        e. Tryggja ytra aðgengi að fjarskiptarými, svo sem með girðingum og árekstrarvörn eftir því sem við á.
c. Raunlægar varnir fjarskiptalagna:
    1. Verja skal fjarskiptalagnir, svo sem milli fjarskiptarýma sem og jarðvegsbrunna, gegn beinu tjóni, t.a.m. vegna bleytu og aurs sem og gegn skemmdarverkum.
    2. Taka skal mið af leiðbeiningum Fjarskiptastofu um frágang og öryggi ljósleiðarastrengja.

3. Sé um mikilvæga eign að ræða sbr. 5. gr. skulu samtengingar, strengendar og tengingar fjarskiptalagna milli staða varðar sérstaklega, fari þær um rými þriðja aðila. Þá skal verja nýja jarðvegsbrunna sérstaklega gegn óheimilum aðgangi og leyna eins og kostur er mikilvægi þeirra.
4. Sé um mikilvæga eign að ræða sbr. 5. gr. skal hvorki birta opinberlega nákvæmar upplýsingar um staðsetningu fjarskiptalagna og/eða fjarskiptarýma né upplýsingar um þjónustuhlutverk hennar.

d. Vöktun fjarskiptarýma:
1. Fjarskiptarými skal, eins og við á, vera búið sjálfvirkum vaktbúnaði sem gefur viðvörun um eld og ef umhverfisaðstæður breytast umfram það sem búnaðurinn er gerður fyrir, að lágmarki vegna raka, vökvaleka og hita. Þá skal hitastig við virkan búnað jafnframt vaktað sérstaklega.
2. Fjarskiptarými skulu búin innbrotsviðvörunarkerfi. Sé um mikilvæga eign að ræða sbr. 5. gr. skal fjarskiptarými búið sjálfvirkum vaktbúnaði, sbr. 1. tl., þ.m.t. sjálfvirku innbrotsviðvörunarkerfi með myndavélum, sjálfvirku slökkvikerfi með halógengasi eða sambærilegu.

e. Varnir gegn straumrofi:
1. Verði fjarskiptabúnaður fyrir straumrofi frá rafveitukerfi þarf að tryggja með varaafli að búnaðurinn starfi með eðlilegum hætti og án rofs í að lágmarki 12 klst., eftir að straumrof verður. Fjarskiptafyrirtæki skal auk þess setja sér viðmið á grundvelli áhættumats um þann tíma sem einstaka hlutar fjarskiptanets starfa ótruflað ef til straumrofs kemur.
2. Verja mikilvægan búnað í fjarskiptarýmum sérstaklega fyrir áhrifum straumrofs og öðrum skammtíma truflunum í rafveitukerfi, t.d. með órofaaflgjafa.
3. Sé um mikilvæga eign að ræða sbr. 5. gr. skal varaafl halda uppi óskertri virkni í að lágmarki í 48 klst. Þá skal vera til staðar varaaflsvél eða að lágmarki tengill fyrir færanlega varaaflsvél til að verjast langtímastraumrofi.

V. KAFLI
Virkni almennra fjarskiptaneta.

14. gr.
Afkastageta og rekstraröryggi flutningsleiða.

Í því skyni að stuðla að samfelldum rekstri og virkni fjarskipta skal fjarskiptafyrirtæki tryggja eins og kostur er fullnægjandi flutningsleiðir fjarskipta og með því fyrirbyggja mögulegt útfall.

Ef fjarskiptaumferð takmarkast af einhverjum völdum vegna ónógrar flutningsgetu fjarskiptanets, skal fjarskiptafyrirtæki leitast við að tryggja þeirri umferð sem best þjónar hagsmunum notenda, almannahagsmunum og/eða þjóðaröryggi mestan forgang.

Fjarskiptafyrirtæki skal tryggja að fjarskipti um landsdekkandi stofnnet geti farið um fleiri en eina landfræðilega leið á milli staða og að um algeran aðskilnað leiða og búnaðar sé að ræða með aðskildu inntaki milli fjarskiptastaða og -rýma, ásamt viðeigandi búnaði í fjarskiptanetum fyrir almenn fjarskipti.

Fjarskiptafyrirtæki sem reka fjarskiptanet eða veita fjarskiptaþjónustu sem felur í sér fjarskipti til útlanda skulu upplýsa á vefsíðu sinni og í viðskiptaskilmálum hvaða ráðstafanir fyrirtækið gerir til að tryggja fjarskipti til útlanda, svo sem með fleiri en einni leið eða hversu langan tíma tekur að koma fjarskiptum um aðra leið verði rof á fjarskiptaleið eða þjónustu.

VI. KAFLI
Viðhald, viðbragðsáætlun, innra eftirlit og atvikatilkynningar.

15. gr.

Viðhald og vöktun.

Fjarskiptafyrirtæki skal viðhalda áreiðanlegum rekstri fjarskiptaneta sinna, kerfa og búnaðar sem nauðsynlegur er fyrir virkni, vernd eða stjórnun fjarskipta.

Viðhafa skal virkt verklag sem tryggir tímanlega endurnýjun búnaðar sem m.a. tekur tillit til endingartíma búnaðar eða lok á þjónustu framleiðanda.

Tryggja skal rauntímavöktun á tilkynningum um og á mögulegum veikleikum í búnaði, þ.m.t. vél-, hug- og fastbúnaði, og tryggja viðeigandi uppfærslur eins fljótt og verða má. Ef ekki er til staðar lagfæring á tilteknum veikleika skal fjarskiptafyrirtæki grípa til viðeigandi öryggisráðstafana til að lágmarka áhættu sem af veikleika stafar. Styðji búnaður ekki frekari uppfærslur skal hefja ferli við endurnýjun hans í samræmi við verklag þar um.

Þá skal fjarskiptafyrirtæki sem rekur fjarskiptanet eða veitir fjarskiptaþjónustu tryggja rauntímavöktun vegna mögulegra truflana og þjónusturofa og hafa virkt viðbragð til að reisa kerfi við eins fljótt og kostur er, komi til öryggisatviks og/eða þjónusturofs.

Á grundvelli bilanaskýrslna eða tilkynninga frá búnaði, skal fjarskiptafyrirtæki, á hvaða tíma sólarhringsins sem er, hafa getu til að gera nauðsynlegar ráðstafanir til að bregðast við öryggisatvikum sem valda mikilli truflun eða rofi á fjarskiptaþjónustu. Þá skulu tímastillingar í búnaði fjarskiptaneta vera samræmdar til að auðvelda samvirkni og rekjanleika aðgerða.

Viðhalda skal skrám um bilanir og truflanir til að auðvelda viðgerðir og fyrirbyggjandi viðhaldsaðgerðir og til að rannsaka þjónustugæði og afköst fjarskiptanetanna.

Við rekstur fjarskiptaneta skal tilkynna öðrum fjarskiptafyrirtækjum um mikilvæg atriði og truflanir sem haft geta áhrif á samtengiumferð milli þeirra.

16. gr.

Breytingastjórnun.

Fjarskiptafyrirtæki skulu hafa verkferla um breytingarstjórnun sem taka til allra breytinga sem áhrif geta haft á öryggi fjarskiptaneta og fjarskiptaþjónustu. Verkferlar skulu tryggja formlega meðhöndlun breytinga, áhættumati þeirra, prófunum á þeim ásamt skjalfestingu þeirra og hafa það að markmiði að koma í veg fyrir truflun á fjarskiptaþjónustu fjarskiptafyrirtækis og annarra fjarskiptafyrirtækja. Ef breyting hefur óhjákvæmilega áhrif á fjarskiptanet og fjarskiptaþjónustu annarra fjarskiptafyrirtækja, skulu aðilar eiga samstarf um fyrirkomulag breytinganna til að lágmarka truflanir.

Breytingar á fjarskiptanetum skal, eins og kostur er, fyrst framkvæma utan raunumhverfis. Breytingum í raunumhverfi skal þannig hagað að þær trufli sem minnst virkni fjarskiptaneta og dragi úr hættu á óheimiluðum aðgangi og annarri breytingu í rekstrarumhverfinu.

17. gr.

Áætlun um viðbragð og samfelldan rekstur.

Fjarskiptafyrirtæki skal útbúa viðbragðsáætlun sem virkja ber ef öryggi fjarskiptaneta eða fjarskiptaþjónustu er ógnað, svo sem ef upp kemur öryggisatvik. Viðbragðsáætlunin skal byggja á niðurstöðum áhættumats og skal að lágmarki kveða á um eftirfarandi atriði:

a. Hvernig bregðast skuli við öryggisatvikum.
b. Aðila sem ber ábyrgð á því að virkja viðbragðsáætlun þegar við á og annað lykilstarfsfólk.
c. Hvernig regluleg prófun viðbragðsáætlana fer fram.
d. Hvernig leita skal orsaka öryggisatvika.
e. Hvernig megi sem fyrst koma aftur á eðlilegu rekstrarástandi.

f. Skilgreina ábyrgðarsvið starfsfólks og boðleiðir, upplýsingar um varabúnað, skipulag tilkynninga og annars sem við á.
g. Hvernig tryggja skuli heildstæða skráningu og greiningu öryggisatvika og þeirra ráðstafana sem gripið er til svo unnt sé að byggja á og læra af fyrri reynslu.
h. Hver niðritími fjarskiptaþjónustu megi vera áður en viðbragðsáætlun er virkjuð.

Viðbragðsáætlun skal endurskoðuð og prófuð með æfingum, a.m.k. árlega.

18. gr.

Innra eftirlit.

Fjarskiptafyrirtæki skal viðhafa virkt innra eftirlit til að tryggja að umgjörð áhættustýringar og öryggisráðstafanir í starfsemi þess uppfylli kröfur laga um fjarskipti og reglugerðar þessarar sem og eigin kröfur.

Gerð skal áætlun um framkvæmd kerfisbundins innra eftirlits í formi úttekta og prófana samkvæmt fyrirfram skilgreindri aðferð. Tíðni og umfang úttekta og prófana skal ákveðið með hliðsjón af niðurstöðu áhættumats sem framkvæmt er á grundvelli 8. gr.

Niðurstöður úttekta og prófana skulu skrásettar og vera aðgengilegar Fjarskiptastofu.

19. gr.

Meðhöndlun öryggisatvika.

Fjarskiptafyrirtæki skal halda skrá yfir öll öryggisatvik sem upp koma eða ógna öryggi fjarskiptaneta og fjarskiptaþjónustu. Atvikaskrá skal uppfærð jafnóðum og öryggisatvik skráð á grundvelli skýrra verkferla.

Þá skal greina orsök og afleiðingu öryggisatviks sem og viðbrögð við öryggisatviki, draga lærdóm af því og gera nauðsynlegar úrbætur svo unnt sé að koma í veg fyrir að sambærileg öryggisatvik endurtaki sig. Niðurstöður greininga og úrbætur skal skjalfesta.

Við endurskoðun áhættumats skv. 8. gr. skal taka mið af atvikaskráningu og -greiningu samkvæmt ákvæði þessu.

Ef öryggisatvik koma upp hjá ytri aðila skal fjarskiptafyrirtæki óska eftir upplýsingum um atvikameðhöndlun og eftirfylgni hennar í öryggisskipulagi hans.

20. gr.

Tilkynning um öryggisatvik.

Fjarskiptafyrirtæki skal tilkynna netöryggissveit Fjarskiptastofu um öll alvarleg öryggisatvik sem ógna öryggi fjarskiptaneta og fjarskiptaþjónustu.

Við mat á alvarleika öryggisatviks skv. 1. mgr. skal einkum horft til eftirfarandi atriða, eins eða fleiri:

a. fjölda notenda sem öryggisatvik hefur áhrif á,
b. hversu lengi öryggisatvik stendur yfir,
c. landfræðilegrar útbreiðslu og umfangs áhrifa öryggisatviks,
d. að hvaða marki virkni netsins eða veiting þjónustunnar verður fyrir áhrifum, og
e. umfangs áhrifa öryggisatviksins á efnahagslega og samfélagslega starfsemi.

Öryggisatvik þar með talið truflanir telst þó ekki alvarlegt í skilningi a. og b. liðar 2. mgr. ef það varðar færri en 400 notendur og ef það stendur yfir skemur en 1 klst. Þjónusturof á fjarskiptaþjónustu og fjarskiptanetum telst þó alltaf alvarlegt öryggisatvik ef það varðar fleiri en 200 notendur og það hefur staðið yfir lengur en ½ klst.

Við mat á alvarleika öryggisatviks í skilningi c. liðar 2. mgr. skal m.a. litið til svæða sem er stærri en 1000km2, til afskekktra svæða eða strjábýlis, til eyja, til höfuðborgarinnar eða þýðingarmikilla svæða og til samtenginga eða margra alþjóðlegra samtenginga. Við mat á alvarleika öryggisatviks í skilningi e. liðar 2. mgr. skal m.a. litið til þess hvort áhrif öryggisatviksins:

a. nái til neyðar- og öryggisfjarskipta, þ.m.t. 112,
b. skapi mikla hættu fyrir öryggi og heilbrigði almennings,
c. hafi áhrif á þjónustu mikilvægra innviða, sem og nái til þýðingarmikilla starfsemi samfélagsins, t.d. æðstu stjórn og stjórnendur landsins.

Tilkynning til netöryggissveitar Fjarskiptastofu samkvæmt 80. gr. fjarskiptalaga skal berast eins fljótt og verða má og eigi síðar en 3 klukkustundum eftir að borin hafa verið kennsl á öryggisatvik sem ógna öryggi og/eða virkni fjarskiptaþjónustu. Í tilkynningu skal m.a. veita eftirfarandi upplýsingar:

a. Hvenær öryggisatviks var fyrst vart;
b. Frummat á eðli og/eða tegund öryggisatviks sem ógnar öryggi fjarskiptaneta og fjarskiptaþjónustu;
c. Frummat á umfangi öryggisatviks;
d. Frummat á mögulegum smitáhrifum;
e. Tilhögun rekstrar, þar á meðal hvort rekstri þeirra er útvistað.

Liggi ekki allar upplýsingar fyrir við framangreind tímamörk ber fjarskiptafyrirtæki að fylgja upprunalegri tilkynningu um öryggisatvik eftir með frekari samskiptum við netöryggissveit, eins fljótt og verða má.

21. gr.

Tilkynningar til viðskiptavina.

Fjarskiptafyrirtæki skal vera með skýra og skilvirka ferla vegna tilkynninga um ósamfellu í virkni eða þjónusturof, svo sem af völdum öryggisatviks, bilana, breytinga eða viðhalds. Á vefsíðu þess, eða með öðrum sambærilegum leiðum, skal tilgreina með sýnilegum hætti almenn þjónustuviðmið, svo sem um þjónustustig og reglubundið viðhald.

22. gr.

Opinber birting.

Fjarskiptafyrirtæki skal birta opinberlega, þ.m.t. á vefsíðu sinni, stefnu um virkni og öryggi fjarskiptaneta sinna. Að lágmarki skal eftirfarandi koma fram:

1. Öryggisstefna fyrirtækisins.
2. Stefna fyrirtækisins um um uppitíma, meðalendurreisnartíma og hámarksnýtingu hinna mismunandi fjarskiptaneta þess.
3. Leiðbeiningar til neytenda um hvert þeir geti leitað með ábendingar til fjarskiptafyrirtækisins, telji þeir öryggi og virkni fjarskiptaneta þess ábótavant.

23. gr.

Sérstakar netógnir.

Ef fjarskiptafyrirtæki telur að spilliumferð, spillikóði eða annað slíkt sem fer um fjarskiptanet þess, stofni rekstri fjarskiptanetsins í hættu eða varði almannahagsmuni eða þjóðaröryggi er því heimilt að beita nauðsynlegum varnarráðstöfunum t.d. sía út slíka umferð, loka tengingum, lénum eða vefslóðum. Gera skal viðskiptavinum grein fyrir þessari heimild í skilmálum viðskiptasamnings. Skulu fjarskiptafyrirtæki þá senda netöryggissveit Fjarskiptastofu skýrslu um tilvikin, innan sex klukkustunda eftir að þau eiga sér stað, þar sem fram kemur atburðarrás, umfang gagnaeyðingar og áhrifamat ef ekki hefði verið brugðist við. Þá skal fjarskiptafyrirtæki beita umræddri heimild komi beiðni eða tilmæli um slíkt frá netöryggissveitinni.

VII. kafli

Eftirlit og viðurlög.

24. gr.

Eftirlit.

Fjarskiptastofa hefur eftirlit með að fjarskiptafyrirtæki uppfylli kröfur laga um fjarskipti sem nánar eru útfærðar í reglugerð þessari.

Við mat á öryggisskipulagi, ráðstöfunum og áhættustýringu fjarskiptafyrirtækis skal Fjarskiptastofa m.a. horfa til hagsmuna notenda fjarskiptaþjónustu af því að hún haldist órofin, almannahagsmuna og þjóðaröryggis.

Fjarskiptastofa skal setja sér stefnu um fyrirkomulag og framkvæmd eftirlits samkvæmt 1. mgr. Í stefnunni er Fjarskiptastofu heimilt að setja fram sjónarmið um nálgun ívilnandi eftirlits er varðar öryggi upplýsinga, gagna, fjarskiptaneta og fjarskiptaþjónustu smærri fjarskiptafyrirtækja sem og eigna sem ekki eru skilgreindar mikilvægar í áhættumati fjarskiptafyrirtækis m.a. á grundvelli leiðbeininga Fjarskiptastofu, skv. 3. mgr. 5. gr. reglugerðar þessarar, eða falla undir skilgreiningu í 2. mgr. 5. gr.

25. gr.

Aðgangur að upplýsingum.

Um aðgang Fjarskiptastofu að upplýsingum fer samkvæmt lögum um Fjarskiptastofu, nr. 75/2021.

Fjarskiptafyrirtæki skal afhenda Fjarskiptastofu allar upplýsingar sem óskað er eftir og varða öryggi fjarskiptaneta og fjarskiptaþjónustu, þ.m.t. um skipulag net- og upplýsingaöryggis, öryggisstefnu, áhættumat, lýsingu á öryggisráðstöfunum, viðbragðsáætlun, atvikaskrá, skýrslur um innri úttektir og prófanir, sem og annað sem við kann að eiga að mati Fjarskiptastofu, hvenær sem óskað er eftir því.

Fjarskiptastofa getur óskað eftir nánari skýringum og gögnum um einstök öryggisatvik í starfsemi fjarskiptafyrirtækis. Fjarskiptafyrirtæki ber að verða við slíkri beiðni innan viðeigandi tímamarka sem Fjarskiptastofa setur.

Fjarskiptastofu er heimilt, að eigin frumkvæði, að óska eftir reglubundinni skýrslugjöf frá fjarskiptafyrirtæki um meðhöndlun öryggisatvika. Fjarskiptafyrirtæki ber að verða við slíkri beiðni innan viðeigandi tímamarka sem Fjarskiptastofa ákveður.

26. gr.

Úttektir og prófanir.

Fjarskiptastofa hefur heimild til úttekta og prófana á virkni fjarskiptaneta, að frumkvæði stofnunarinnar, samkvæmt ábendingu eða vegna öryggisatviks sem ógnar öryggi fjarskiptaneta og fjarskiptaþjónustu.

Fjarskiptastofu er heimilt að fela til þess bærum utanaðkomandi aðila að annast framkvæmd úttektar og/eða prófanir og skýrslugerð um niðurstöðu sína. Skal hann bundinn sérstakri þagnarskyldu um störf sín í þágu Fjarskiptastofu í samræmi við ákvæði 28. gr. reglugerðar þessarar. Fjarskiptafyrirtæki skal gefinn kostur á því að gera athugasemdir við val á slíkum aðila.

27. gr.

Bindandi fyrirmæli Fjarskiptastofu.

Fjarskiptastofa skal gefa bindandi fyrirmæli um úrbætur ef mat hennar er að fjarskiptafyrirtæki uppfylli ekki kröfur fjarskiptalaga og reglugerðar þessarar, þ.m.t. um skipulag net- og upplýsingakerfa og einstakar öryggisráðstafanir, að gættum andmælarétti fyrirtækisins. Hæfilegur frestur skal veittur til úrbóta.

Vanræki fjarskiptafyrirtæki að verða við bindandi fyrirmælum skv. 1. mgr. um úrbætur á alvarlegum veikleikum er Fjarskiptastofu heimilt að láta vinna verkið fyrir hönd og á kostnað

hlutaðeigandi aðila. Krafa um kostnað vegna þessa er aðfararhæf skv. 5. tölul. 1. mgr. 1. gr. laga um aðför, nr. 90/1989.

Um beitingu dagssekta fer eftir ákvæði 19. gr. laga nr. 75/2021, um Fjarskiptastofu.

Brot á reglugerð þessari og ákvæðum fjarskiptalaga varða viðurlögum samkvæmt ákvæðum laga um fjarskipti.

28. gr.

Sérstök þagnarskylda.

Sérstök þagnarskylda starfsfólks samkvæmt 5. – 7. mgr. 25. gr. laga um Fjarskiptastofu, nr. 75/2021, sbr. 19. og 20. gr. laga nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða, nær til allra gagna og upplýsinga sem eru hluti af eftirliti með öryggi upplýsinga, gagna, fjarskiptaneta og fjarskiptaþjónustu og eru því undanskilin ákvæðum upplýsingalaga, nr. 140/2012.

29. gr.

Heimild og gildistaka.

Reglugerð þessi er sett með heimild í 10. mgr. 78. gr., sbr. 1. mgr. 95. gr., 85. og 107. gr. laga nr. 70/2022 um fjarskipti, og öðlast þegar gildi.

Háskóla-, iðnaðar- og nýsköpunarráðuneytinu, xx. xxxxx 2024.

xxxxxxxxxxxxxxxxxxxxxxxxx.

xxxxxxxxxxxxxxxxxx