REGLUR
um vernd upplýsinga á almennum fjarskiptanetum.

I. KAFLI

Markmið og gildissvið.

1. gr.
Markmið.

Markmið þessara reglna er að auka neytendavernd og treysta stoðir upplýsingasamfélagsins með því að gera auknar kröfur til öryggis fjarskiptakerfa sem almenningur og fyrirtæki nota. Með reglum þessum er kveðið á um þær ráðstafanir sem Póst- og fjarskiptastofnun telur nauðsynlegt að fjarskiptafyrirtækin geri til að tryggja vernd umferðar og upplýsinga í almennum fjarskiptanetum. Samkvæmt þeim skal leitast við að tryggja leynd upplýsinga, lögmætan aðgang að þeim, tiltækileika þeirra og réttleika. Bætt öryggi næst með ráðstöfunum sem lúta að takmörkuðum aðgangi að upplýsingum, aukinni vernd fjarskiptaneta og þjónustu.

2. gr.
Gildissvið.

Reglur þessar ná til net- og upplýsingaöryggis í fjarskiptanetum, þ.e. í hinum eiginlegu fjarskiptanetum svo og upplýsingakerfum sem þau styðjast við og tengjast, á gildissviði laga nr. 81/2003 um fjarskipti. Reglurnar ná til fjarskiptafyrirtækja sem reka fjarskiptaþjónustu í almennum fjarskiptanetum.

Þær gilda um almenn fjarskiptanet, til og með nettengipunkti fyrir innan inntak, en taka ekki til innanhússlagna, búnaðar og aðstöðu hjá viðskiptavinum þeirra. Sérstaklega er fjallað um innanhússlagnir í reglum Póst- og fjarskiptastofnunar um innanhússfjarskiptalagnir nr. 1109/2006.

Til hliðsjónar má styðjast við staðlana ISO/IEC 27001 (Stjórnkerfi upplýsingaöryggis) og ISO/IEC 17799 (Starfsvenjur fyrir stjórnun upplýsingaöryggis). Fara skal eftir nýjustu útgáfu staðlanna á hverjum tíma. Staðlana má ennfremur nota sem leiðbeiningar um ráðstafanir sem innleiða má til að uppfylla kröfur reglnanna.

Um öryggi persónuupplýsinga gilda ákvæði 11.-13. gr. laga nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga og reglur nr. 299/2001 um öryggi persónuupplýsinga.

3. gr.
Skilgreiningar.

Merking orða og hugtaka í reglum þessum er sem hér segir:

Aðgangsstýring: Aðferð til þess að tryggja að einungis aðilar með heimild hafi aðgang að fjarskiptaneti, t.d. að skilgreindum svæðum og gögnum, hvort sem þau eru á tölvutæku formi eða ekki.

Almennt fjarskiptanet: Fjarskiptanet sem er notað að öllu eða að mestu leyti til að bjóða almenna fjarskiptaþjónustu.

Fjarskiptafyrirtæki: Einstaklingur eða lögaðili sem hefur tilkynnt Póst- og fjarskiptastofnun um fyrirhugaðan rekstur fjarskiptaþjónustu eða fjarskiptanets.

Fjarskiptanet: Sendikerfi og þar sem það á við skiptistöðvar, beinar og önnur úrræði sem gera mögulegt að miðla merkjum eftir þræði, þráðlaust, með ljósbylgjum, rafdreifikerfi, háspennulínum eða með öðrum rafsegulaðferðum, þ.m.t. net fyrir hljóð- og sjónvarp og kapalsjónvarp.

Fjarskiptaþjónusta: Þjónusta sem að nokkru eða öllu leyti felst í því að beina merkjum um fjarskiptanet, þ.m.t. tölvupóstþjónusta og netaðgangur.

IP fjarskiptanet: Fjarskiptanet sem flytur gagnapakka samkvæmt IP (Internet Protocol) staðli.

IP þjónusta: Vefsíður, skráaflutningur, spjallrásir o.fl. sem flutt er yfir IP fjarskiptanet.

Leynd: Vernd upplýsinga gegn óviðkomandi aðgangi, bæði á meðan þær eru sendar milli staða og þar sem þær eru vistaðar.

Net- og upplýsingaöryggi: Hæfni fjarskiptaneta til að tryggja að ákveðin fyrirfram skilgreind öryggismörk standist þegar ógnir steðja að eða ef veilur myndast, t.d. vegna mannlegra mistaka eða

skemmdarverka, sem stofna í hættu leynd, réttleika og tiltækileika upplýsinga í fjarskiptanetum. Það getur auk þess falið í sér aðra eiginleika, svo sem ósvikni, ábyrgni, óhrekjanleika og áreiðanleika.

Netaðgangur: Eiginlegur aðgangur að fjarskiptanetum og tengd þjónusta, þ.m.t. þjónusta sem ber kennsl á notendur, þjónusta sem staðfestir hver notandinn er og óbeinn flutningur. Ennfremur sú stuðningsþjónusta sem veitt er, s.s. veiting IP vistfanga, léna og vefþjónusta.

Netárás: Árás í gegnum fjarskiptanet, sem miðar að því að skerða þjónustu eða trufla virkni neta og kerfa.

Nettengipunktur: Efnislegur tengipunktur þar sem áskrifanda er veittur aðgangur að almennu fjarskiptaneti.

Óbeinn flutningur: Milliliður í flutningi fjarskiptaumferðar viðskiptavina sem að öllu jöfnu hylur skráð IP vistfang sendanda en sýnir í staðinn IP vistfang milliliðsins, t.d. svokölluð proxy þjónusta.

Óhrekjanleiki: Aðferð sem tryggir að sendandi upplýsinga geti ekki afneitað því að hafa sent tilteknar upplýsingar eða móttakandi að hafa tekið á móti þeim.

Raunlægur: Merkir áþreifanlegan efnislegan hlut eða raunverulegt umhverfi.

Réttleiki: Eiginleiki upplýsinga sem felst í því að upplýsingarnar eru nákvæmar og réttar. Engu hefur verið eytt, engu bætt við eða breytt og ekkert vantar í upplýsingarnar. Þetta á einnig við um varðveislu þessara eiginleika ef upplýsingar eru sendar, mótteknar og vistaðar hjá viðtakanda.

Skilaboð: símhringing, tölvupóstur, SMS skilaboð, talskilaboð, myndskilaboð, sjónvarpsdagskrá, IP þjónusta eða önnur sambærileg skilaboð sem flutt eru milli aðila, eða til óskilgreindra móttakenda í fjarskiptaneti.

Tiltækileiki: Merkir að upplýsingar séu aðgengilegar og þjónusta tiltæk þegar á þarf að halda, eða eins og mögulegt er svo sem við rafmagnsleysi, náttúruhamfarir, slys eða netárásir.

Upplýsingar: Eru hvers konar tákn, merki, skrift, mynd og hljóð sem send eru eða móttekin eða hvers konar boðmiðlun eftir leiðslum, með þráðlausri útbreiðslu eða öðrum rafsegulmiðlum.

Öryggisatburður: Það að upp kemur staða kerfis, þjónustu eða nets sem gefur til kynna hugsanlegt brot gegn öryggisstefnu eða bilun í öryggisráðstöfun, eða þá áður óþekkt staða sem getur skipt máli fyrir öryggi.

Öryggisatvik: Atvik sem er gefið til kynna með einum eða fleiri óæskilegum eða óvæntum öryggisatburðum sem talsverðar líkur eru á að stofni rekstrarþáttum í hættu og ógni upplýsingaöryggi.

Öryggishópur: Öryggishópur sem stuðlar að vernd gegn öryggisatvikum, ótryggri virkni og tortryggilegum atvikum í upplýsinga- og fjarskiptanetum á Íslandi.

II. KAFLI
Almennar kröfur og leiðbeiningar.

4. gr.
Almennt.

Fjarskiptafyrirtæki skulu gera viðeigandi ráðstafanir til þess að tryggja vernd almennrar fjarskiptaþjónustu og fjarskiptaneta sem þau reka, m.a. verja upplýsingar sem um þau fara gegn ólöglegri eyðileggingu, glötun eða breytingum fyrir slysni eða vegna óleyfilegs aðgangs. Þessar ráðstafanir skulu, að teknu tilliti til tæknistigs og kostnaðar við framkvæmdina, tryggja hæfilegt öryggisstig miðað við þá áhættu sem um er að ræða.

5. gr.
Leynd í fjarskiptum.

Fjarskiptafyrirtæki skulu tryggja að viðskiptavinir þeirra njóti verndar gagnvart hlustun, hlerun, geymslu eða annars konar hindrun eða vöktun fjarskipta, þ.m.t. skilaboða og auðkenna, sem fara um fjarskiptanet þeirra, nema að slíkt fari fram með samþykki viðskiptavinanna eða samkvæmt heimild í lögum. Undanþegin er tímabundin tæknileg geymsla upplýsinga meðan þær eru í flutningi enda sé innihald þeirra ekki birt á neinn hátt.

Ennfremur skal tryggja að geymsla eða aðgengi fjarskiptafyrirtækjanna að upplýsingum í endabúnaði viðskiptavina sé aðeins heimiluð ef notandanum eru gefnar greinargóðar upplýsingar um tilganginn og gert kleift að hafna því. Þetta skal þó heimilt í þeim tæknilega tilgangi að flytja rafræn boð yfir fjarskiptanet eða sem hluti af reglulegum uppfærslum.

6. gr.

Réttleiki upplýsinga.

Fjarskiptafyrirtæki skulu tryggja réttleika upplýsinga viðskiptavina sinna á þann hátt að þær verði ekki fyrir breytingum, bæði þeirra upplýsinga sem eru í flutningi um almenn fjarskiptanet og aðrar fjarskiptaupplýsingar.

7. gr.

Öryggisskipulag.

Fjarskiptafyrirtæki skulu útbúa og viðhalda skjalfestri lýsingu á stjórnkerfi sem tryggir upplýsingaöryggi í fjarskiptaþjónustu og fjarskiptanetum. Þetta stjórnkerfi upplýsinga-öryggis skal að lágmarki felast í eftirtöldu:

1. Fjarskiptafyrirtæki skal setja sér skriflega *öryggisstefnu*. Í henni skal m.a. koma fram almenn lýsing á afstöðu æðsta stjórnanda fjarskiptafyrirtækis til öryggismála. Í stefnunni skulu koma fram markmið og meginreglur upplýsingaöryggis samkvæmt rekstrarstefnu og rekstrarmarkmiðum. Stefnan skal kynnt öllum starfsmönnum fjarskiptafyrirtækisins sem hafa með fjarskiptarekstur að gera. Við mótun öryggisstefnu skal taka mið af því hvaða upplýsingar skuli vernda, hvernig skuli vernda þær, þeirri aðferð sem viðhöfð verður við vinnslu þeirra og hver beri ábyrgð á öryggi þeirra. Skal öryggisstefnan birt starfsmönnum.
2. Fjarskiptafyrirtæki skal skilgreina aðferðarfræði *áhættumats* um upplýsingaöryggi og henni fylgt eftir með skriflegu áhættumati um upplýsingaöryggi sem tengist fjarskiptanetum og fjarskiptaþjónustu. Áhættumat skal bera kennsl á áhættuþætti, umfang þeirra og forgangsraða þeim miðað við ásættanlega áhættu og þau markmið sem skipta máli fyrir fyrirtækið. Áhættumat skal skilgreina eignir og gera á þeim einfalt mat og mat á þeim áhrifum sem myndast af völdum rofs á leynd, réttleika og tiltækileika. Miklir veikleikar og ógnir eru skilgreind fyrir eignirnar, ásamt mati á líkindum þeirra. Áhættan fyrir hvert atriði er reiknuð út og hún borin saman við fyrirframgerðan mælikvarða um ásættanlegt áhættustig um öryggi upplýsinga, órofinn rekstur og þjónustustig. Markmið áhættumats er að skapa forsendur fyrir vali á öryggisráðstöfunum og skal það endurskoðað reglulega.
3. Fjarskiptafyrirtæki skulu setja sér verklagsreglur um örugga meðferð upplýsinga og eyðingu þeirra. Gerðar skulu *öryggisráðstafanir* og settar fram skriflegar lýsingar á þeim. Tilgreina skal hvaða öryggisráðstöfunum verði beitt og hvernig þær verði útfærðar, þ. á m. við hönnun, þróun, rekstur, prófun og viðhald hvers kerfis. Þá skal og tekið fram hvernig brugðist verði við áföllum í rekstri fjarskiptaneta og fjarskiptaþjónustu. Öryggisráðstafanir skal endurskoða reglulega. Skriflegar leiðbeiningar skulu vera til staðar fyrir einstaka ferla sem nauðsynlegir eru fyrir upplýsingaöryggi fjarskiptaneta og fjarskiptaþjónustu. Fjarskiptafyrirtækið skal sjá til þess að ákvæðum stefnunnar um upplýsingaöryggi sé framfylgt, líka þegar verktakar vinna fyrir fyrirtækið. Fjarskiptafyrirtækið skal sjá til þess að starfsmenn þess framfylgi stefnunni um upplýsingaöryggi.

Fjarskiptafyrirtæki skulu, að beiðni Póst- og fjarskiptastofnunar, framkvæma sértækt áhættumat á einstökum kerfisþáttum fjarskiptaneta og/eða fjarskiptaþjónustu eða sérstökum ógnum sem geta steðjað að upplýsingum, netum þeirra og þjónustu. Skulu þau, eftir atvikum, setja sér sértækar öryggisráðstafanir á grundvelli niðurstöðu slíks mats.

7. gr. a.

Sjálfsmat.

Fjarskiptafyrirtæki skulu framkvæma sjálfsmat á stöðu öryggisskipulags síns. Slíkt stöðumat skal byggja á leiðbeiningum Póst- og fjarskiptastofnunar og vera framkvæmt eftir þörfum en þó a.m.k. á þriggja ára fresti. Niðurstöðu stöðumats skal senda Póst- og fjarskiptastofnun.

8. gr.

Innra eftirlit.

Viðhafa skal innra eftirlit til að tryggja að unnið sé í samræmi við öryggisstefnu og skjalfestar verklags- og öryggisreglur öryggisskipulags og að uppbygging þess sé í samræmi við lög og reglur. Innra eftirlit skal framkvæma kerfisbundið samkvæmt fyrirfram skilgreindri aðferð. Tíðni og umfang

eftirlitsins skal ákveðið með hliðsjón af skilgreindri áhættu, eðli þeirra upplýsinga sem um er að ræða, tækni sem notuð er til að tryggja öryggi þeirra og kostnaði af framkvæmd eftirlitsins. Það skal þó framkvæmt eigi sjaldnar en árlega. Fjarskiptafyrirtæki skulu gera skýrslu um niðurstöður innra eftirlits og senda Póst- og fjarskiptastofnun.

Póst- og fjarskiptastofnun getur óskað eftir því að fjarskiptafélag framkvæmi sértækt innra eftirlit eða prófum á mikilvægum kerfisþáttum sem hafa háa eðlislæga áhættu og/eða öryggisatvik gæti valdið rofi á fjarskiptaleynd, alvarlegum truflunum á virkni fjarskiptaneta og/eða rofi á veitingu fjarskiptaþjónustu.

Komi upp alvarleg ógn eða atvik sem hefur eða getur valdið rofi á fjarskiptaleynd, haft áhrif á virkni fjarskiptaneta eða leiðir til þjónusturofs skulu fjarskiptafyrirtæki leitast við að finna orsakir þess og gera viðeigandi breytingar og viðbætur við áhættumat og öryggisráðstafanir. Þá skulu þau skila skýrslu til Póst- og fjarskiptastofnunar um ógnina eða atvikið, orsakir og úrvinnslu.

III. KAFLI
Öryggisráðstafanir.

9. gr.
Áætlun um samfelldan rekstur.

Gerðar skulu sérstakar ráðstafanir til að tryggja öryggi upplýsinga komi til þjónusturofs, s.s. vegna bilunar, óhappa eða annarra atvika sem ógnað geta öryggi fjarskiptaneta. Póst- og fjarskiptastofnun mælir nánar fyrir um slíkar ráðstafanir í reglum nr. 1222/2007 um virkni almennra fjarskiptaneta.

10. gr.
Ráðstafanir vegna starfsmanna.

Í þeim tilgangi að fyrirbyggja og takmarka tjón vegna mistaka, svika og annarrar misnotkunar, skulu fjarskiptafyrirtæki að lágmarki grípa til eftirfarandi öryggisráðstafana varðandi þá starfsmenn sem vegna starfa sinna hafa aðgang að upplýsingum í fjarskiptanetum.

1. Kanna hvort tilefni sé til að afla sakavottorðs umsækjanda áður en starf er veitt.
2. Láta starfsmenn undirrita trúnaðaryfirlýsingar.
3. Fræða starfsmenn um ábyrgð sína samkvæmt IX. kafla laga nr. 81/2003 um fjarskipti.
4. Fjarskiptafyrirtæki skulu skilgreina ábyrgð og skyldur starfsmanna í tengslum við upplýsingaöryggi. Hlutverkaskipting og ábyrgð á framkvæmd hinna ýmsu ferla er lúta að öryggi skal vera skilgreind með skýrum hætti og kveða skal á um bann við skoðun upplýsinga nema í starfstengdum tilgangi.
5. Tryggja að starfsmönnum sé með reglubundnum hætti gerð grein fyrir starfsskyldum sínum og þeim afleiðingum sem það getur haft í för með sér að brjóta þær.
6. Veita skal starfsmönnum viðeigandi menntun og þjálfun í upplýsingaöryggismálum.
7. Fjarskiptafyrirtæki skulu skoða áhættu varðandi lykilmenn upplýsingaöryggis og m.a. tryggja að ávallt sé hægt að ná í þá eða varamenn þeirra í neyð.

11. gr.
Aðgangsstýring.

Í þeim tilgangi að fyrirbyggja og takmarka tjón af völdum óheimils raunlægs aðgangs, svo sem aðgengi að aðstöðu og tækjabúnaði, skulu fjarskiptafyrirtæki grípa að lágmarki til eftirtalinna ráðstafana eftir því sem við á:

1. Stýra aðgangi að húsnæði og búnaði fjarskiptaneta með úthlutun aðgangskorta, lykilorða, eða með öðrum fullnægjandi hætti þar sem því verður við komið.
2. Fjarskiptabúnað, s.s. senda, skiptikerfi og aðra innviði fjarskipta, skal aðgreina á raunlægan hátt frá öðrum búnaði, t.d. í lokuðum skápum. Þessi ráðstöfun kemur þó ekki í veg fyrir að fjarskiptafyrirtæki geti samnýtt aðstöðu.
3. Þjónustuaðila með stöðu þriðja aðila skal aðeins veita takmarkaðan aðgang að mikilvægum svæðum þegar þörf krefur. Slíkur aðgangur á að vera háður heimild og einnig vöktun ef svo ber undir.

12. gr.

Skipulags- og tæknilegar ráðstafanir.

Fjarskiptafyrirtæki skulu viðhafa nauðsynlegar tæknilegar og skipulagslegar ráðstafanir til að verja almenn fjarskiptanet sín. Skulu fjarskiptafyrirtæki m.a. gera eftirfarandi ráðstafanir eftir því sem við á:

1. Stýringar fjarskiptabúnaðar skulu vera varðar gegn óheimilum aðgangi að skilaboðum og auðkennum í flutningi, svo sem með dulkóðun eða lokuðum stýrinetum.
2. Nota aðgangsheimildir, aðgangsstýringu og óhrekjanleika.
3. Staðfesta skal að óskir um breytingu á fjarskiptaþjónustu komi frá áskrifanda hennar, eða séu með samþykki hans.
4. Tryggja óhrekjanleika aðgerða.
5. Tryggja rekjanleika uppflettinga og vinnsluaðgerða.
6. Takmarka aðgang starfsmanna að upplýsingum við þær sem eru þeim nauðsynlegar til að þeir geti sinnt starfi sínu, og við þann tíma sem nauðsynlegur er.
7. Upplýsingaöflun vegna afgreiðslu og reikningagerðar, skal aðskilja frá öflun upplýsinga um fjarskiptaumferð sem nýtast kann í þágu rannsókna opinberra mála og almannaöryggis, t.d. innihald fjarskipta.
8. Viðhalda órofinni slóð sönnunargagna sem nýst gætu vegna öryggisatburða. Skilgreina búnað og vinnslu fyrirfram á þann hátt að sem flest mikilvæg þess háttar tilvik komi með skýrum hætti fram í eftirlitskerfum.
9. Halda skrá um aðgangsheimildir og aðgangsréttindi og yfirfara reglulega. Skal fjarskiptabúnaður vera stilltur til samræmis við þá skráningu.
10. Viðhafa skal viðeigandi ráðstafanir til að tryggja öryggi upplýsinga í boðskiptum endanna á milli við eftirtaldar aðstæður:
    a. Starfsmenn vinna í fjarvinnslu við viðkvæm fjarskiptakerfi.
    b. Fjarskiptafyrirtæki veita viðskiptavinum sínum sérstakt fjarvinnsluaðgengi að kerfum viðskiptavinarins, með stýringu og viðkomu í kerfum fjarskiptafyrirtækisins, svo sem aðgengi að pósthúsum eða gagnageymslum fyrirtækja frá farsíma.

IV. KAFLI

Ýmis ákvæði.

13. gr.

Útvistun reksturs fjarskiptaneta.

Fjarskiptafyrirtæki er heimilt að semja við þriðja aðila um að annast, í heild eða að hluta, rekstur fjarskiptanets. Stjórnunarlegri ábyrgð og áhættustýringu verður þó ekki útvistað. Skilyrði slíks samnings er þó að fjarskiptafyrirtæki hafi sannreynt að umræddur aðili hafi sett sér öryggisstefnu og geti framkvæmt nauðsynlegar öryggisráðstafanir samkvæmt reglum þessum ásamt innra eftirliti. Gerður skal skriflegur samningur til að tryggja þetta. Samningurinn skal m.a.:

1. Kveða á um skyldu vistunaraðila að starfa í samræmi við fyrirmæli fjarskiptafyrirtækis og ákvæði reglna þessara.
2. Innihalda lýsingu á þeirri þjónustu sem inna skal af hendi og tiltaka það þjónustustig sem stefnt er að. Enn fremur þær ráðstafanir sem gripið skal til ef þjónustan uppfyllir ekki þau ákvæði.
3. Hafa ákvæði um þagnarskyldu og með honum skal tryggt að farið sé að ákvæðum fjarskiptalaga þar að lútandi.
4. Tryggja að fjarskiptafyrirtækið eigi rétt til eftirlits með þeirri starfsemi sem samningurinn tekur til.
5. Tryggja aðgang Póst- og fjarskiptastofnunar að upplýsingum frá vistunaraðila og að stofnunin geti í þágu eftirlits framkvæmt athuganir á starfsstöð hans.

14. gr.

Vernd tenginga við nettengipunkt.

Fjarskiptafyrirtæki skulu útfæra og viðhalda tengingum við nettengipunkt með öryggi í huga og m.a. viðhafa eftirfarandi ráðstafanir:

1. Þegar fjarskiptafyrirtæki veitir tengingar sem eru samnýttar með öðrum viðskiptavinum, skal fyrirtækið aðgreina umferð þeirra á þann hátt að viðskiptavinir geti ekki fylgst með umferð hvers annars.
2. Aftengja skal viðskiptavini, eða þjónustu þeirra, frá fjarskiptanetinu ef tenging þeirra að miklu leyti stofnar upplýsingaöryggi og tiltækileika fjarskiptaneta í hættu. Aftengingin og endurtengingin skal gerð í samræmi við fyrirfram ákveðna ferla og leiðbeiningar fjarskiptafyrirtækisins. Við framkvæmdina má taka tillit til sérstakra aðstæðna, svo sem hvers konar tenging á við.

15. gr.

Upplýsingar um öryggishættur og öryggisatvik.

Tilkynna skal viðskiptavinum um þau öryggisatvik sem valda truflunum á samfelldri fjarskiptaþjónustu, ef leynd á tilteknu fjarskiptaneti eða upplýsingar viðskiptavina eru í stórfelldri hættu af völdum öryggishættu í fjarskiptanetum.

Fjarskiptafyrirtæki skulu vera með skýra og skilvirka ferla vegna fyrrgreindra tilkynninga. Þjónustuviðmið þar að lútandi skulu koma fram á heimasíðu fyrirtækisins eða eftir sambærilegum leiðum, t.d. í viðskiptamannasamningum. Í tilkynningunum þarf að lágmarki að koma fram hvaða áhrif atvikið hefur eða getur haft, og þær ráðstafanir sem fjarskiptafyrirtækið muni gera, ásamt ráðleggingum til viðskiptamanna ef svo ber undir.

Ef þær ráðstafanir sem fjarskiptafyrirtæki gera í fjarskiptanetum sínum ná ekki til tiltekins öryggisatviks, skulu fjarskiptafyrirtækin gefa viðskiptavinum sínum ráðleggingar gegn veikleikum sem geta leitt til frekari útbreiðslu öryggisatviksins hjá þeim, t.d. með notkun sérstaks hugbúnaðar eða dulkóðunartækni í almennum IP fjarskiptanetum, þ.m.t. internet.

Í þeim tilgangi að auka heildstæði og öryggi fjarskiptaneta á Íslandi, getur Póst- og fjarskiptastofnun ákveðið að gögn er varða öryggi upplýsinga og tortryggileg atvik í fjarskiptanetum, skulu afhent öryggishópum sem starfa skv. 25. gr. reglna nr. 1223/2007 um vernd, virkni og gæði IP fjarskiptaþjónustu.

16. gr.

Aðgangur að upplýsingum.

Fjarskiptafyrirtæki skulu afhenda Póst- og fjarskiptastofnun eða fulltrúa hennar allar upplýsingar um skipulag upplýsingaöryggis, þ.m.t. öryggisstefnu, áhættumat, áætlun um órofinn rekstur, lýsingu á öryggisráðstöfunum, sértæk áhættumöt og öryggisráðstafanir og skýrslur um innra eftirlit, hvenær sem stofnunin óskar eftir því. Einnig getur stofnunin óskað eftir nánari skýringum og gögnum um einstök öryggisatvik sem upp geta komið í starfsemi fjarskiptafyrirtækja.

17. gr.

Prófanir og úttektir.

Póst- og fjarskiptastofnun er heimilt að prófa öryggi upplýsinga í fjarskipanetum og gera úttektir á því hvort farið er eftir reglum þessum. Gildir einu hvort það er að eigin frumkvæði eða skv. ábendingum. Prófanir taka m.a. til almennra fjarskiptaneta, fjarskiptaþjónustu og tengdra upplýsingakerfa. Stofnunin ákveður fyrirkomulag prófana eða úttekta.

Póst- og fjarskiptastofnun getur ákveðið að fela sjálfstætt starfandi sérfræðingi að annast framkvæmd úttektar og skila stofnuninni skýrslu um niðurstöðu hennar. Skal hann bundinn þagnarskyldu um störf sín í þágu stofnunarinnar. Fjarskiptafyrirtækjum skal gefinn kostur á því að gera athugasemdir við val stofnunarinnar á slíkum sérfræðingi.

18. gr.

Gildistaka.

Þessar reglur taka gildi þann 1. júlí 2008.

19. gr.

Heimild.

Póst- og fjarskiptastofnun hefur gefið út þessar reglur um virkni almennra fjarskiptaneta samkvæmt heimild í b-lið 9. gr. laga nr. 39/2007 um breytingu á lögum um fjarskipti nr. 81/2003.