drög

Reglur

um vernd upplýsinga í almennum fjarskiptanetum

I. KAFLI
Markmið og gildissvið

1. gr.
Markmið

Markmið þessara reglna er að auka neytendavernd og treysta stoðir upplýsingasamfélagsins. 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 neta 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.

Að öðru leyti en kemur fram í reglum þessum má til hliðsjónar styðjast við staðalinn ISO/IEC 27001:2005, þar sem fjallað er um stjórnkerfi upplýsingaöryggis, og staðalinn ISO/IEC 17799:2005 sem leiðbeiningar um ráðstafanir sem innleiða má til að uppfylla kröfur reglnanna.

3. gr.
Skilgreiningar

Merking orða og hugtaka í reglum þessum er sem hér segir:
Aðgangsstýring (*access control*)**:** 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.

drög

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 net *(IP networks)***:** Fjarskiptanet sem flytur gagnapakka samkvæmt IP (Internet Protocol) staðli.
IP þjónusta *(IP Services)***:** Vefsíður, skráaflutningur, spjallrásir o.fl. sem flutt er yfir IP net.
Leynd (*confidentiality*) **:** 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. Þá þarf að tryggja að ógnir hafi ekki áhrif á tiltækileika, sannvottun, réttleika og leynd upplýsinga sem vistaðar eru og sendar eða þeirrar þjónustu sem veitt er um viðkomandi fjarskiptanet.
Netaðgangur: Eiginlegur aðgangur að fjarskiptanetum og tengd þjónusta, þ.m.t. þjónusta sem ber kennsl á notendur, þjónusta sem staðfestir hver notandinn er og staðgengilsþjónusta (proxy services). Ennfremur sú stuðningsþjónusta sem veitt er, s.s. veiting IP vistfanga, léna og vefþjónusta.
Nettengipunktur: Efnislegur tengipunktur þar sem áskrifanda er veittur aðgangur að almennu fjarskiptaneti.
Óhrekjanleiki *(non-repudiation)***:** Aðferð sem tryggir að sendandi upplýsinga geti ekki afneitað því að hafa sent tilteknar upplýsingar eða móttakandi að hafa tekið á móti þeim.
Raunlægur *(physical)***:** Merkir áþreifanlegan efnislegan hlut eða raunverulegt umhverfi.
Réttleiki (*integrity)***:** 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 *(messages)***:** símhringing, tölvupóstur, SMS skilaboð, talskilaboð, sjónvarpsdagskrá, IP þjónusta eða önnur sambærileg skilaboð sem flutt eru milli aðila, eða til óskilgreindra móttakenda í fjarskiptaneti.
Spillikóti (malicious code)**:** Forrit, eða forritunarbútar, sem smeygja sér inn í tölvur og fjarskiptanet í þeim tilgangi að framkvæma einhverja heimildarlausa eða skaðlega aðgerð. Dæmi um spillikóta eru tölvuveirur og tölvuormar.
Spilliumferð: Fjarskiptaumferð sem send er af stað í þeim tilgangi að spilla virkni fjarskiptaneta. Dæmi um spilliumferð er netárás (denial of service attack) og ofgnótt ruslpósts.
Tiltækileiki *(availability)***:** Merkir að upplýsingar séu aðgengilegar og þjónusta sé virk þrátt fyrir utanaðkomandi truflanir, svo sem rafmagnsleysi, náttúruhamfarir, slys eða árásir.
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.

drög

Öryggisatburður *(security event)***:** 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 *(security incident)***:** 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.

II. KAFLI
Kröfur um vernd upplýsinga og öryggisskipulag

4. gr.
Almennt

Í reglum þessum koma fram kröfur til fjarskiptafyrirtækja um að tryggja öryggi upplýsinga í fjarskiptanetum, þ.e. hinum eiginlegu fjarskiptanetum svo og upplýsingakerfum sem þau styðjast við og tengjast, svo sem eftirlits-, aðgangs- og reikningakerfi, hér eftir nefnt fjarskiptanet.

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 leynd þeirra ekki rofin á neinn hátt.

Ennfremur skal tryggja að geymsla eða aðgengi 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 einum tæknilega tilgangi að flytja rafræn samskipti yfir fjarskiptanet, eða í þeim tilgangi að veita nauðsynlega þjónustu í upplýsingasamfélaginu sem áskrifandi eða notandi hefur sérstaklega óskað eftir.

6. gr.
Réttleiki upplýsinga

Fjarskiptafyrirtæki skulu tryggja réttleika upplýsinga viðskiptavina sinna, bæði þeirra upplýsinga sem eru í flutningi um almenn fjarskiptanet og aðrar fjarskiptaupplýsingar.

7. gr.
Öryggisskipulag

drög

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 skal 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 gera skriflegt *áhættumat* um upplýsingaöryggi sem tengist fjarskiptanetum og fjarskiptaþjónustu. Áhættumat ætti að bera kennsl á áhættuþætti, umfang þeirra og forgangsraða þeim miðað við áhættusamþykki og þau markmið sem skipta máli fyrir fyrirtækið. Áhættumat skilgreinir eignir og gerir á þeim einfalt mat og mat á þeim áhrifum sem myndast af völdum rofs á leynd, réttleika og tiltækileika. Miklir veikleikar og ógnir eru skilgreindar fyrir eignirnar, ásamt mati á líkindum þeirra. Áhættan fyrir hvert atriði er reiknuð út og hún borin saman við fyrirframgerðan mælikvarða. Þá skal taka afstöðu til þess hvað teljist vera ásættanleg áhætta varðandi öryggi upplýsinga og órofinn rekstur, með hliðsjón af þjónustustigi. 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 setja fram skriflega lýsingu 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.

8. gr.

Hlíting við staðal

Fjarskiptafyrirtæki sem teljast ráðandi á markaði eða hafa veltu yfir 1 milljarð kr. af fjarskiptastarfsemi skulu sýna fram á hlítingu við alþjóðlega öryggisstaðalinn ISO/IEC 27001:2005 með vottun á sviði upplýsingaöryggis í fjarskiptanetum.

9. gr.

drög

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 eftirlitsins og umfang 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.

III. KAFLI
Öryggisráðstafanir

10. gr.

Áætlun um órofinn 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.] um virkni almennra fjarskiptaneta.

11. 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:

1. Kanna sakaferil umsækjenda 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 í tengslum við lykilmenn upplýsingaöryggis og m.a. tryggja að hægt sé að ná í þá í neyð.

12. gr.

Ráðstafanir gegn óheimilum raunlægum aðgangi

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:

drög

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, þarf að aðgreina á raunlægan hátt frá öðrum búnaði, svo sem búnaði viðskiptavina sem er í hýsingu hjá fjarskiptafyrirtækinu.
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 vöktun.

13. 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. Fjarskiptabúnaður skal vera varinn gegn óheimilum aðgangi að skilaboðum og auðkennum í flutningi milli þeirra, s.s. með dulkóðun.
2. Nota aðgangsheimildir, aðgangsstýringu og óhrekjanleika.
3. Eingöngu skal afgreiða óskir um breytingu um fjarskiptaþjónustu sem koma frá rétthafa hennar.
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. Aðskilja upplýsingaöflun vegna afgreiðslu og reikningagerðar frá lágmarksskráningu upplýsinga um fjarskiptaumferð í þágu rannsókna opinberra mála og almannaöryggis.
8. Viðhalda órofinni slóð sönnunargagna sem nýst gætu vegna öryggisatburða. Skilgreina búnað og vinnslu á þann hátt að 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. Tryggja að til staðar séu nýleg afrit af miðlægum upplýsingum notenda í fjarskiptaþjónustu. Geyma skal afritunargögnin á öruggum stað.
11. Viðhafa viðeigandi ráðstafanir til að tryggja öryggi upplýsinga í fjarvinnslu og upplýsinga sem send eru milli endabúnaðar farkerfa og þeirra hugbúnaðarkerfa sem veita þjónustuna.

IV. KAFLI

Ýmis ákvæði

14. gr.

drög

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.

15. 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.

16. 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 hættu. Ef þær ráðstafanir sem fjarskiptafyrirtæki gerir ná ekki til tiltekins öryggisatviks, skulu fjarskiptafyrirtækin gefa viðskiptavinum ráðleggingar til verndar, t.d. með notkun sérstaks hugbúnaðar eða dulkóðunartækni í almennum IP netum, þ.m.t. internet.

Á eyðublaði Póst- og fjarskiptastofnunar nr. xxxx, skulu fjarskiptafyrirtæki tilkynna Póst- og fjarskiptastofnun um öll þau öryggisatvik sem valda truflunum á samfelldri fjarskiptaþjónustu, ef upplýsingar viðskiptavina eru í hættu og leynd fjarskipta á tilteknu fjarskiptaneti verður rofin. Ef stofnunin telur að upplýsingar um viðkomandi atvik séu í

þágu almennings, hefur stofnunin heimild til að senda út tilkynningu til almennings um slík rof.

17. 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 og skýrslur um innra eftirlit, hvenær sem stofnunin óskar eftir því.

18. gr.

Prófanir og úttektir.

Póst- og fjarskiptastofnun er heimilt að prófa virkni fjarskiptaneta og gera úttektir á því hvort farið er eftir reglum þessum. Gildir einu hvort það er að eigin frumkvæði eða skv. ábendingum. Getur Póst- og fjarskiptastofnun ákveðið að fela sérfræðingi að annast framkvæmd slíkrar úttektar og skila stofnuninni skýrslu um niðurstöðu hennar. Prófanir taka m.a. til almennra fjarskiptaneta, fjarskiptaþjónustu og tengdra upplýsingakerfa. Stofnunin ákveður fyrirkomulag prófana eða úttekta.

19. gr.

Gildistaka

Þessar reglur taka gildi við þann 1. xxxx 2007.

20. 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.

Póst- og fjarskiptastofnun, xxxx 2007.