REGLUGERÐ
um öryggi net- og upplýsingakerfa mikilvægra innviða.

I. KAFLI
Almenn ákvæði

1. gr.
Gildissvið

Reglugerð þessi gildir um mikilvæga innviði í skilningi laga nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða.

Reglugerðin gildir um net- og upplýsingakerfi sem eru undirstaða fyrir veitingu þjónustu sem skilgreind er nauðsynleg fyrir viðhald mikilvægrar samfélagslegrar og efnahagslegrar starfsemi samkvæmt ákvæðum II. kafla á sviði bankastarfsemi og innviða fjármálamarkaða, flutninga, heilbrigðisþjónustu, orku-, hita- og vatnsveitna, svo og stafrænna grunnvirkja.

Reglugerðin gildir einnig um net- og upplýsingakerfi veitenda stafrænnar þjónustu sem starfrækja netmarkað, leitarvél á netinu og skýjavinnsluþjónustu og teljast ekki til örfélaga í skilningi laga um ársreikninga.

2. gr.
Markmið.

Markmið reglugerðarinnar er að tryggja með sem bestum hætti samfellda virkni og áfallaþol þjónustu mikilvægra innviða með því að kveða nánar á um lágmarkskröfur til umgjarðar og rekstrar net- og upplýsingakerfa þeirra, ekki síst í þágu almannahagsmuna. Ennfremur að tryggja samhæfð viðbrögð við ógnum og atvikum í net- og upplýsingakerfum sem nauðsynleg eru fyrir veitingu umræddrar þjónustu.

Reglugerð þessari er einnig ætlað að stuðla að samræmi í eftirfylgni og framkvæmd eftirlits með net- og upplýsingakerfum mikilvægra innviða.

3. gr.
Skilgreiningar.

Í reglugerð þessari merkir:

1. *Atburðir:* Hver sú ógn eða áður óþekkta staða sem upp getur komið í net- og upplýsingakerfi.
2. *Atvik:* Hver sá atburður sem hefur skaðleg áhrif á öryggi net- og upplýsingakerfa.
3. *Áhætta*: Aðstæður eða atburðir sem geta haft skaðleg áhrif á öryggi net- og upplýsingakerfa.
4. *Eignir:* Hvaðeina, bæði efnislegt og óefnislegt, sem er einhvers virði fyrir starfsemi mikilvægra innviða.
5. *Mikilvægir innviðir:* Rekstraraðilar nauðsynlegrar þjónustu og veitendur stafrænnar þjónustu eins og þeir eru skilgreindir í lögum nr. 78/2019, um net- og upplýsingakerfi mikilvægra innviða og reglugerð þessari.
6. *Nauðsynleg þjónusta:* Þjónusta sem skilgreind er nauðsynleg fyrir viðhald mikilvægrar samfélagslegrar og efnahagslegrar starfsemi samkvæmt ákvæðum II. kafla á sviði bankastarfsemi og innviða fjármálamarkaða, flutninga, heilbrigðisþjónustu, orku-, hita- og vatnsveitna, svo og stafrænna grunnvirkja.
7. *Rekstraraðili nauðsynlegrar þjónustu:* Opinber aðili eða einkaaðili sem veitir þjónustu sem telst nauðsynleg samkvæmt ákvæðum II. kafla á sviði bankastarfsemi, innviða fjármálamarkaða, flutninga, heilbrigðisþjónustu, orku-, hita- og vatnsveitna, svo og stafrænna grunnvirkja.

8. *Stjórnunarkerfi:* Fyrirkomulag skipulagslegra og tæknilegra ráðstafana sem notast er við til að tryggja öryggi net- og upplýsingakerfa.
9. *Umferðartakmarkanir*: Stýringar á takmörkun á umferð í og úr kerfum til að tryggja öryggi gegn ógnum.
10. *Veitandi stafrænnar þjónustu:* Veitandi stafrænnar þjónustu í skilningi laga nr. 78/2019, sem starfrækir netmarkað, leitarvél á netinu eða skýjavinnsluþjónustu og teljast ekki til örfélaga í skilningi laga um ársreikninga.

Að öðru leyti gilda orðskýringar í lögum nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða.

II. KAFLI
Þjónusta sem skilgreind er nauðsynleg fyrir viðhald mikilvægrar samfélagslegrar og efnahagslegrar starfsemi.

4. gr.
Þjónusta á sviði bankastarfsemi.

Með þjónustu sem skilgreind er sem mikilvæg samfélagsleg og efnahagsleg starfsemi á sviði banka er átt við greiðsluþjónustu, skv. 4. gr. laga nr. 120/2011 um greiðsluþjónustu, þar sem veitandi þjónustunnar er jafnframt kerfislega mikilvægt fjármálafyrirtæki samkvæmt ákvörðun fjármálastöðugleikanefndar, sbr. d-liður 1. mgr. 13. gr. laga nr. 92/2019 um Seðlabanka Íslands.

5. gr.
Þjónusta á sviði innviða fjármálamarkaða.

Með þjónustu sem skilgreind er sem mikilvæg samfélagsleg og efnahagsleg starfsemi á sviði innviða fjármálamarkaða er átt við rekstraraðila skipulegra verðbréfamarkaða og markaðstorgs fjármálagerninga samkvæmt skilgreiningu laga nr. 108/2007 um verðbréfaviðskipti og miðlæga mótaðila samkvæmt skilgreiningu reglugerðar (ESB) nr. 648/2012, sem lögfest er með lögum nr. 15/2018 um afleiðuviðskipti, miðlæga mótaðila og afleiðuviðskiptaskrár.

6. gr.
Þjónusta á sviði flutninga.

Með þjónustu sem skilgreind er sem mikilvæg samfélagsleg og efnahagsleg starfsemi á sviði flutninga er átt við:

a. veitingu flugleiðsöguþjónustu og rekstrarstjórnun flugumferðar.
b. starfsemi og þjónustu alþjóðaflugvalla.
c. þjónustu flutningsaðila með flugrekstrarleyfi útgefið hér á landi sem flytur fleiri en 25% flugfarþega til og frá landinu á ári.
d. þjónustu flutningsaðila með flugrekstrarleyfi útgefið hér á landi sem flytur meira en 25% af flugfrakt til og frá landinu á ári.
e. veitingu upplýsingaþjónustu vegna siglinga.
f. þjónustu útgerðarfélaga samkvæmt skilgreiningu í viðauka I við reglugerð (EB) nr. 725/2004 um að efla vernd skipa og hafnaraðstöðu sem sjá um flutning meira en 25% af sjóflutningum til og frá landinu, sé útgerðarfélag skráð hér á landi. Ekki fellur hér undir innflutningur á olíu, né hrávöru til framleiðslu í stóriðju.
g. þjónustu í tengslum við lestun og losun farms á milli hafnar og flutningsaðila sbr. f-lið þar sem farmflutningar eru umfram 25% af öllum sjóflutningum til og frá landinu að undanskildum flutningum á olíuvörum og hrávöru til stóriðju.
h. veitingu upplýsingaþjónustu vegna umferðar á vegum.

i. móttöku neyðarboða vegna umferðar á vegum.

7. gr.

Heilbrigðisþjónusta.

Með þjónustu sem skilgreind er sem mikilvæg samfélagsleg og efnahagsleg starfsemi á sviði heilbrigðisþjónustu er átt við heilsugæslustöðvar og sjúkrahús með bráðamóttöku, hjúkrunarheimili og heilsugæslustöðvar með sjúkrarými, sjúkraflutninga og lyfjabúðir:

a. þar sem fjöldi heilbrigðisstarfsmanna eða annarra lögmætra heilbrigðisaðila er meiri en 50 stöðugildi á ársgrundvelli, eða
b. þar sem að minnsta kosti 10.000 skammtar af lyfseðilsskyldum lyfjum eru ávísaðir á ári.

8. gr.

Þjónusta á sviði orku- og hitaveitna.

Með þjónustu sem skilgreind er sem mikilvæg samfélagsleg og efnahagsleg starfsemi á sviði orku- og hitaveitna er átt við:

a. rekstraraðila olíuframleiðslu, olíuflutninga, olíuflutningsleiðslna eða olíubirgðastöðva sem framleiðir, flytur eða geymir að lágmarki 100.000 tonn af olíu árlega.
b. flutningsfyrirtæki á raforku sem hefur fengið leyfi til reksturs flutningsfyrirtækisins samkvæmt raforkulögum nr. 65/2003.
c. dreifiveitu raforku sem starfar á grundvelli sérleyfis samkvæmt raforkulögum nr. 65/2003 og nær til raforkunotenda með 1000 manns eða fleiri.
d. vinnslufyrirtæki sem hefur í rekstri raforkuvirkjun með uppsett afl 50MW eða meira, í tilfelli vindorkulunda er miðað við 80MW eða meira.
e. aðila sem eiga viðskipti með raforku og hafa fengið raforkusöluleyfi í samræmi við 18. gr. raforkulaga nr. 65/2003 og fjöldi notenda fer yfir 1000.
f. hitaveitu sem starfar á grundvelli einkaleyfis skv. orkulögum nr. 58/1967 og þjónustar 1.000 notendur eða fleiri.

9. gr.

Þjónusta á sviði vatnsveitna.

Með þjónustu sem skilgreind er sem mikilvæg samfélagsleg og efnahagsleg starfsemi á sviði vatnsveitna er átt við birgja og dreifingaraðila neysluvatns sem þjónusta [5000] notendur eða fleiri.

10. gr

Þjónusta á sviði stafrænna grunnvirkja.

Með þjónustu sem skilgreind er sem mikilvæg samfélagsleg og efnahagsleg starfsemi á sviði stafrænna grunnvirkja er átt við:

a. Rekstraraðila tengi- og skiptipunkta þar sem árleg markaðshlutdeild hér á landi er 50% eða meiri og ekki er til staðar fullnægjandi staðganga fyrir þá þjónustu sem veitt er.
b. Rekstraraðila lénsheitakerfa ef sami rekstraraðili rekur:
    1. nafnaþjón (e. resolver) sem fær að meðaltali yfir 10.000 fyrirspurnir á hverjum sólarhring síðasta almanaksár; eða
    2. sannvottunar nafnaþjón (e. authoritative name server) sem geymir grunnupplýsingar um vistfang í IP-samskiptareglunum fyrir yfir 1200 lénsheiti í lok hvers árs.
c. Rekstraraðila sem sinnir skráning landshöfuðléna ásamt nafnaþjónustu fyrir þau.

III. KAFLI
Lágmarkskröfur um áhættustýringu og ráðstafanir.

11. gr.
Skipulag net- og upplýsingaöryggis.

Mikilvægir innviðir skulu tryggja öryggi þeirra net- og upplýsingakerfa sem falla undir gildissvið reglugerðar þessarar, með ýtrasta hætti. Þeim ber að útbúa og viðhalda skjalfestri lýsingu á stjórnskipulagi og stjórnunarkerfi net- og upplýsingakerfa sinna og skulu jafnframt, með skipulegri áhrifagreiningu og áhættumati, bera kennsl á nauðsynlegar ráðstafanir og viðhafa aðgerðir til að stýra og stjórna net- og upplýsingakerfum með tilliti til áhættu. Skilgreina skal með skýrum hætti hlutverk og ábyrgð stjórnenda og starfsmanna, sem og ytri aðila ef við á, sem bera ábyrgð á framkvæmd þess.

Við framkvæmd áhættustýringar og viðbúnaðar í starfsemi sem fellur undir gildissvið reglugerðar þessarar, skulu mikilvægir innviðir byggja á nýjustu útgáfu alþjóðlega viðurkenndra staðla um bestu framkvæmd á sviði net- og upplýsingaöryggis. Það á bæði við um almenna staðla á borð við ISO/IEC 27001 (Stjórnunarkerfi um upplýsingaöryggi), ISO/IEC 27002 (Starfsvenjur fyrir upplýsingaöryggisstýringar), ISO/IEC 27005 (Áhættustýring upplýsingaöryggis) og aðra sértæka staðla og reglur á hlutaðeigandi sviði.

IV. KAFLI
Skipulagslegar ráðstafanir.

12. gr.
Öryggisstefna.

Mikilvægir innviðir skulu útbúa og viðhalda skriflegri öryggisstefnu. Í stefnunni skal tilgreina stefnuyfirlýsingu, markmið og meginreglur net- og upplýsingaöryggis og hvernig öryggi net- og upplýsingakerfa er best tryggt. Stefnan skal samþykkt með formlegum hætti af yfirstjórn og birt öllum starfsmönnum. Skal hún sérstaklega kynnt starfsmönnum sem vinna með beinum eða óbeinum hætti við net- og upplýsingakerfi. Þá skal vera skýrt í skipulagi mikilvægs innviðar hver ber ábyrgð á framkvæmd öryggismála. Öryggisstefnu skal rýna og uppfæra eftir því sem tilefni er til og að lágmarki á tveggja ára fresti.

13. gr.
Áhættumat.

Mikilvægir innviðir skulu framkvæma áhættumat á net- og upplýsingakerfum sínum á grundvelli viðurkenndrar og þekktrar aðferðarfræði, með það að markmiði að skapa forsendur fyrir vali á öryggisráðstöfunum og draga úr áhættu sem steðjað getur að öryggi net- og upplýsingakerfa þeirra. Áhættumat skal vera skriflegt. Það skal framkvæmt reglubundið og aðferðarfræði þess endurmetin, hvort tveggja á a.m.k. tveggja ára fresti. Þá skal ávallt endurskoða áhættumat í kjölfar atviks eða áhættu í net- og upplýsingakerfum sem og ef forsendur áhættumats eða aðstæður breytast sem kalla á slíkt endurmat.

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

a. Að borin skuli kennsl á áhættu, með því að greina umfang og áhrif ógna, sem og mat á líkindum þeirra. Áhættu skal forgangsraðað í ljósi skilgreindra og skriflegra viðmiða um ásættanlega áhættu og markmiða sem sett hafa verið í öryggisstefnu.
b. Að eignir séu skilgreindar og gert á þeim mat, s.s. hverjir eru helstu veikleikar og/eða ógnir sem steðjað geta að eigninni, þar á meðal rýrnun trausts.
c. Ef við á, skal mat lagt á að hvaða marki veiting þjónustu er háð afhendingu á vöru eða þjónustu frá þriðja aðila, s.s. birgjum eða þjónustuveitendum, þ.m.t. öðrum mikilvægum innviðum og þau áhrif sem myndast ef rof verður á slíkri afhendingu.

d. Ef við á, skal mat lagt á það hvernig net- og upplýsingakerfi eða undirliggjandi búnaður eru háð kerfum þriðja aðila, þ.m.t. annarra mikilvægra innviða. Hér skal einnig líta til þess hvort, og þá hvernig, röskun á starfsemi kerfa þriðja aðila hefur áhrif á starfsemi net-og upplýsingakerfa við veitingu þjónustu mikilvægra innviða.

Rekstraraðili nauðsynlegrar þjónustu skal að auki, að beiðni eftirlitsstjórnvalds, framkvæma sértækt áhættumat á einstökum hlutum net- og upplýsingakerfa, sérstakri áhættu sem getur steðjað að kerfunum sem og vegna útvistunar á rekstri þeirra. Skal hann, eftir atvikum, setja sér sértækar öryggisráðstafanir á grundvelli niðurstöðu slíks mats, sbr. 14. gr.

Veitendum stafrænnar þjónustu er heimilt að víkja frá einstaka kröfum um framkvæmd áhættumats skv. 2. mgr. ef hann getur sýnt fram á að umræddar kröfur séu of íþyngjandi miðað við umfang og eðli starfsemi hlutaðeigandi.

14. gr.

Öryggisráðstafanir.

Mikilvægir innviðir skulu, á grundvelli niðurstöðu áhættumats, innleiða öryggisráðstafanir sem eru nauðsynlegar til að tryggja öryggi net- og upplýsingakerfa og koma til móts við greinda áhættu sem steðjað getur að hlutaðeigandi eignum og þjónustu þeirra, takmarka líkur á henni og áhrif sem hún getur haft. Öryggisráðstafanir skulu taka mið af alþjóðlegum viðmiðum um bestu framkvæmd sem og þeirri reynslu og lærdómi sem aflað hefur verið, til dæmis við beitingu fyrri öryggisráðstafana og meðhöndlun atvika og áhættu. Öryggisráðstafanir rekstraraðila nauðsynlegrar þjónustu skulu þó að lágmarki vera í samræmi við kröfur III.-V. kafla.

Setja skal fram skriflegar lýsingar á þeim öryggisráðstöfum sem gripið er til samkvæmt 1. mgr. sem og útfærslu þeirra og innleiðingu, þar á meðal við hönnun, þróun, rekstur, prófun og viðhald hvers kerfis sem og raunlæga vernd mikilvægra rýma. Skriflegar leiðbeiningar skulu vera til staðar fyrir einstaka ferla sem nauðsynlegir eru fyrir öryggi net- og upplýsingakerfa mikilvægra innviða.

Öryggisráðstafanir skulu endurskoðaðar reglubundið í samræmi við endurskoðun, framkvæmd og niðurstöður áhættumats og að minnsta kosti á tveggja ára fresti. Ávallt ber að endurskoða öryggisráðstafanir þegar atvik eða áhætta kemur upp eða aðstæður breytast sem kalla á endurmat.

15. gr.

Öryggisráðstafanir vegna starfsmanna.

Í þeim tilgangi að fyrirbyggja og takmarka tjón vegna mistaka, svika og annarrar misnotkunar starfsmanna og þriðju aðila, svo sem verktaka, sem vegna starfa sinna hafa aðgang að net- og upplýsingakerfum eða hýsingarrýmum kerfisbúnaðar, skulu mikilvægir innviðir grípa til eftirfarandi öryggisráðstafana:

a. Meta hvort tilefni sé til að afla sakavottorðs og, eftir því sem við getur átt, annarrar öryggisvottunar umsækjanda áður en starf er veitt eða gengið er til samninga við þriðju aðila. Við slíkt mat skal líta til ábyrgðar sem starfi eða verkefni fylgir.
b. Láta starfsmenn og þriðju aðila undirrita trúnaðaryfirlýsingar.
c. Skilgreina ábyrgð og skyldur starfsmanna og þriðju aðila í tengslum við öryggi net- og upplýsingakerfa og framkvæmd verkferla.
d. Skilgreina hvaða starfsmenn eða þriðju aðilar eru í lykilhlutverki við að tryggja öryggi net- og upplýsingakerfa og tryggja virkar boðleiðir, þannig að þess sé ávallt gætt að hægt sé að ná í þá eða varamenn þeirra í neyð.
e. Fræða og eftir atvikum prófa þekkingu starfsmanna og þriðju aðila á þeim lögum og reglum sem gilda um öryggi net- og upplýsingakerfa mikilvægra innviða. Einnig skal tryggja að starfsmönnum og þriðju aðilum sé með reglubundnum hætti gerð grein fyrir

starfsskyldum sínum og þeim afleiðingum sem það getur haft í för með sér að brjóta þær.

Veitendum stafrænnar þjónustu er heimilt að víkja frá einstaka öryggisráðstöfunum skv. stafliðum a-e í 1. mgr. ef hann getur sýnt fram á að umræddar kröfur séu of íþyngjandi miðað við umfang og eðli starfsemi hlutaðeigandi.

16. gr.

Útvistun á rekstri net- og upplýsingakerfa.

Ef mikilvægur innviður semur við þriðja aðila um rekstur net- og upplýsingakerfa skal tryggja að þjónustuveitandi starfi í samræmi við lög nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða, og uppfylli kröfur um öryggi net- og upplýsingakerfa í samræmi við ákvæði reglugerðar þessarar.

Þjónustusamningur um rekstur net- og upplýsingakerfa skal vera skriflegur og afmarka á skýran hátt hlutverk og skyldur aðila. Þar skal tilgreina með skýrum hætti þá þjónustu sem veitt er ásamt þeim kerfum og búnaði sem notuð eru fyrir veitingu þjónustu mikilvægra innviða samkvæmt reglugerð þessari.

Mikilvægum innviðum er heimilt, ef þörf þykir, að fela þjónustuveitanda á grundvelli þjónustusamnings að framkvæma tilkynningarskyldu mikilvægs innviðar um alvarleg atvik eða áhættu samkvæmt 25. gr. er varðar þann hluta reksturs net- og upplýsingakerfa sem hann sinnir.

Í þjónustusamningi skal að auki tryggja að eftirlitsstjórnvald hafi aðgang að viðeigandi upplýsingum frá þjónustuveitanda og geti við framkvæmd eftirlits síns gert athuganir á starfsstöð þjónustuveitandans og prófanir á kerfum hans og búnaði sem tilgreind eru í þjónustusamningi.

Þrátt fyrir útvistun samkvæmt ákvæði þessu, er ábyrgð á uppfyllingu lágmarkskrafna laga nr. 78/2019 og reglugerðar þessarar um áhættustýringu og viðbúnað, sem og ábyrgð á því að tilkynningarskyldu sé fullnægt, þess mikilvægs innviðar sem í hlut á.

V. KAFLI

Tæknilegar ráðstafanir.

17. gr.

Almennt.

Mikilvægir innviðir skulu, í samræmi við niðurstöður áhættumats, gera þær tæknilegu öryggisráðstafanir sem nauðsynlegar eru til að tryggja með sem bestum hætti öryggi net- og upplýsingakerfa þeirra.

Auk þeirra ráðstafana sem mikilvægir innviðir innleiða á grundvelli niðurstöðu áhættumats skulu þeir jafnframt að lágmarki viðhafa þær ráðstafanir sem kveðið er á um í þessum kafla, kerfislægar og raunlægar. Veitendum stafrænnar þjónustu er heimilt að víkja frá einstaka ráðstöfunum skv. kafla þessum ef hann getur sýnt fram á að umræddar kröfur séu of íþyngjandi miðað við umfang og eðli starfsemi hlutaðeigandi. Þeim er þó ávallt skylt að innleiða þær kerfislægu og raunlægu ráðstafanir sem nauðsynlegar eru m.t.t áhættumats.

18. gr.

Kerfislægar ráðstafanir.

Mikilvægir innviðir skulu að lágmarki viðhafa eftirtaldar kerfislægar ráðstafanir fyrir net- og upplýsingakerfi þeirra:

a. Kerfislægar aðgangsstýringar:
    1. Innleiða viðeigandi kerfi til sannvottunar á notendum og kerfum.
    2. Takmarka aðgangsréttindi starfsmanna og verktaka að upplýsingum og kerfum/kerfishlutum við það sem þeim eru nauðsynleg til að geta sinnt starfi sínu og við þann tíma sem nauðsynlegur er.

3. Skrá með formlegum hætti veitingu aðgangsheimilda og aðgangsréttinda og yfirfara aðgangsréttindi reglulega.
4. Viðhafa ráðstafanir sem tryggja rekjanleika uppflettinga og vinnsluaðgerða.

b. Nota dulritun og aðrar viðeigandi ráðstafanir til að tryggja öryggi upplýsinga í net- og upplýsingakerfum.
c. Setja umferðartakmarkanir í net- og upplýsingakerfum.
d. Lágmarka virkni, tengingar og aðgang milli kerfishluta með því að skilgreina kröfur um samskipan kerfis (e. system configuration). Tilgangurinn er sá að uppsetning þjónustu eða annarrar virkni í net- og upplýsingakerfum, eða tenging slíks kerfis við búnað, takmarkist við þætti sem eru nauðsynlegir fyrir starfsemi og öryggi net- og upplýsingakerfa.
e. Aðgreina milli kerfishluta eins og kostur er til að takmarka dreifingu/útbreiðslu atvika innan og á milli net- og upplýsingakerfa.
f. Setja upp búnað sem vaktar umferð í net- og upplýsingakerfum og greinir t.a.m ummerki um atvik eða áhættu, s.s. óeðlilegan aðgang, árásir, spillikóða og aðrar hættulegar aðstæður. Meta skal sérstaklega hvort setja eigi upp innbrotsvarnir (e. intrusion prevention) þar sem þörf er á sterkum vörnum fyrir gögn og vinnslur.
g. Viðhalda órofinni slóð sönnunargagna sem nýst gætu við greiningu atvika og áhættu. Skilgreina skal fyrirfram skráningu í búnaði og vinnslum innan kerfa þannig að mikilvægir atburðir komi með skýrum hætti fram í eftirlitskerfum.
h. Vakta öryggisuppfærslur fyrir net- og upplýsingakerfi og innleiða allar nauðsynlegar uppfærslur án tafar.

19. gr.

Raunlægar ráðstafanir.

Mikilvægir innviðir skulu að lágmarki viðhafa eftirfarandi raunlægar ráðstafanir:

a. Raunlæg aðgangsstýring:
   1. Hindra óleyfilegan aðgang að öryggisrýmum með traustum hurðum og læsingum. Leitast skal við að öryggisrýmin séu gluggalaus eða gluggar varðir sérstaklega gegn innbrotum og byrgi ásýnd inn í rýmin.
   2. Stýra aðgengi starfsmanna og þriðju aðila að öryggisrýmunum með aðgangskorti eða sambærilegu auðkenni og skal rekjanleiki tryggður. Takmarka skal aðgang inn í mikilvæg öryggisrými við nauðsynlega aðila. Verktakar og aðrir ytri aðilar sem hafa ekki aðgangsheimild að öryggisrýmunum skulu ávallt vera undir eftirliti inni í rýmunum.
b. Raunlægar varnir öryggisrýma:
   1. Tryggja að byggingarefni öryggisrýma og annar frágangur byggingar sé úr eldtefjandi efni sem ver öryggisrýmin fyrir eldsvoða utan rýmis í að lágmarki eina klukkustund. Öll gegntök skulu vera reykþétt og eldvarin.
   2. Verja mikilvæg öryggisrými fyrir raka- og vökvaskemmdum. Setja lekapönnur undir vökvalagnir kerfa sem eru með takmörkuðu magni vökva, til dæmis kælikerfi, og tryggja að ekki séu vatns- og hitaveitulagnir í gegnum öryggisrýmin.
   3. Haga frágangi virks búnaðar og leiðslna þannig að hann verði ekki fyrir skaða ef vökvi lekur inn í öryggisrýmin, t.d. með því að lyfta búnaði í ákveðna hæð frá gólfi.
   4. Öryggisrými skulu alla jafna vera útbúin sjálfvirku slökkvikerfi.
c. Vöktun öryggisrýma:
   1. Öryggisrýmin skulu útbúin sjálfvirkum vaktbúnaði sem tengist stjórnstöð og gefur viðvörun um eld og ef umhverfisaðstæður breytast umfram það sem

búnaðurinn er gerður fyrir og að lágmarki vegna raka, vökvaleka og hita. Þá skal hitastig við virkan búnað jafnframt vaktað sérstaklega.
2. Setja upp sjálfvirkt innbrotsviðvörunarkerfi með myndavélum og innbrotsskynjurum þar sem það á við, í og við öryggisrýmin.

d. Varnir gegn straumrofi fyrir net- og upplýsingakerfi:
1. Tryggja skal varaafl sem getur að lágmarki haldið uppi óbreyttri virkni net- og upplýsingakerfa í samræmi við uppitímaviðmið þjónustu á grundvelli niðurstöðu áhættumats, en þó eigi skemur en í 2 klst.
2. Verja skal mikilvægan búnað í öruggum rýmum sérstaklega fyrir rofi í raffæðingu og öðrum skammtíma truflunum í rafveitu, t.d. með órofaaflgjafa.
3. Auk þess skal mikilvægur innviður meta sérstaklega hvort verja skuli net- og upplýsingakerfi gegn langtíma straumrofi með sérstakri vararafstöð sem getur haldið kerfum gangandi um lengri tíma.

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

20. gr.
Viðhald net- og upplýsingakerfa.

Mikilvægir innviðir skulu viðhalda áreiðanlegum rekstri net- og upplýsingakerfa sinna, t.a.m. með virkri endurnýjun búnaðar og uppfærslu hugbúnaðar.

Þá skulu mikilvægir innviðir hafa virka viðbúnaðarumgjörð fyrir net- og upplýsingakerfi sín og tryggja að kerfi séu reist við eins fljótt og kostur er komi til atviks og/eða þjónusturofs. Tryggja skal að til staðar séu afrit af síðustu stillingum búnaðar sem nauðsynlegur er til að viðhalda og reisa við rekstur net- og upplýsingakerfa þjónustunnar. Afritunargögnin skulu vistuð á öruggum stað.

Á grundvelli bilana- og truflanaskýrslna eða tilkynninga frá búnaði, skulu rekstraraðilar nauðsynlegrar þjónustu, á hvaða tíma sólarhringsins sem er, hafa getu til að gera nauðsynlegar ráðstafanir til að bregðast við atvikum sem valda mikilli truflun eða rofi á þjónustu. Meiri háttar röskun á þjónustu skal svo fljótt sem verða má tilkynna í samræmi við 25. gr. til að tryggja netöryggissveit sem réttasta stöðumynd vegna netógna sem gæti þurft að bregðast við.

21. gr.
Stjórnun breytinga í net- og upplýsingakerfum.

Breytingar á net- og upplýsingakerfum mikilvægra innviða eða endurnýjun þeirra skal framkvæma þannig að þær trufli sem minnst starfsemi þeirra. Mikilvægir innviðir skulu setja verklagsreglur um hvernig standa skal að slíkum breytingum sem og hvernig tryggja megi sem minnsta röskun á þjónustu þeirra.

22. gr.
Viðbragðsáætlun.

Mikilvægir innviðir skulu útbúa viðbragðsáætlun sem virkja ber ef upp kemur atvik eða áhætta í net- og upplýsingakerfum þeirra. Viðbragðsáætlunin skal byggja á niðurstöðum áhrifagreiningar og áhættumats og m.a. taka mið af því hvernig leysa á úr mögulegum öryggisatvikum, hvernig tryggja beri samfelldan rekstur og/eða endurreisn net- og upplýsingakerfa þeirra, svo og að takmarka tjón. Í viðbragðsáætlun skal að lágmarki kveða á um eftirfarandi atriði:

a. Aðila sem ber ábyrgð á því að virkja viðbragðsáætlun þegar við á og aðra lykilstarfsmenn.
b. Verkferla við reglulega prófun viðbragðsáætlana.
c. Hvernig leita skal orsaka atvika og koma aftur á eðlilegu rekstrarástandi.

d. Leiðbeiningar um hvernig bregðast skal við atvikum og áhættu, þar á meðal skilgreina ábyrgðarsvið viðeigandi starfsmanna og boðleiðir, s.s. nauðsynlegar upplýsingar til að ná í viðgerðarmenn eða aðra sérfræðinga, upplýsingar um varabúnað, skipulag tilkynninga og annars sem við á.
e. Hvernig skuli tryggja heildstæða skráningu og greiningu atvika og þeirra ráðstafana sem gripið er til svo unnt sé að byggja á og læra af fyrri reynslu.

Viðbragðsáætlun skal metin og prófuð með reglulegu millibili, þ.á m. með æfingum.

Veitendum stafrænnar þjónustu er heimilt að víkja frá einstaka kröfum um innihald viðbragðáætlunar skv. stafliðum a – e í 1. mgr. ef hann getur sýnt fram á að umræddar kröfur séu of íþyngjandi miðað við umfang og eðli starfsemi hlutaðeigandi.

23. gr.

Innra eftirlit og prófanir.

Mikilvægir innviðir skulu viðhafa virkt innra eftirlit til að tryggja að umgjörð áhættustýringar og viðbúnaðar í starfsemi þeirra uppfylli kröfur laga nr. 78/2019 og reglugerðar þessarar, þar á meðal með prófunum.

Gerð skal áætlun um framkvæmd kerfisbundins innra eftirlits samkvæmt fyrirfram skilgreindri aðferð. Prófanir geta meðal annars falið í sér úttektir á virkni tæknilegra öryggisráðstafana skv. V. kafla og viðbragðsáætlun sbr. 22. gr.

Tíðni og umfang innra eftirlits skal ákveðið út frá öryggislegum markmiðum m.a. með hliðsjón af niðurstöðu áhættumats sem framkvæmt er samkvæmt 13. gr. Eftirlit skal þó framkvæmt eigi sjaldnar en árlega. Ef ástæða þykir til, m.a. vegna íþyngjandi kostnaðar, er veitendum stafrænnar þjónustu heimilt að framkvæma slíkt eftirlit sjaldnar, en þó að lágmarki á þriggja ára fresti.

Niðurstöður úttektar samkvæmt kröfum um innra eftirlit skulu skrásettar og vera aðgengilegar hlutaðeigandi eftirlitsstjórnvaldi.

24. gr.

Meðhöndlun atvika.

Mikilvægir innviðir skulu halda skrá yfir öll atvik og áhættur sem upp koma í eða steðja að net- og upplýsingakerfum þeirra. Atvikaskrá skal uppfærð reglulega og atvik og áhættur skráðar á grundvelli skýrra verkferla.

Þá skal greina orsök og afleiðingu atvika og áhættu og skjalfesta niðurstöður svo unnt sé að koma í veg fyrir að sambærileg atvik eða áhætta endurtaki sig.

Við endurskoðun áhættumats skv. 13. gr. skal taka mið af atvikaskráningu og -greiningu samkvæmt ákvæði þessu.

25. gr.

Tilkynning um atvik eða áhættu

Mikilvægir innviðir skulu tilkynna netöryggissveit Póst- og fjarskiptastofnunar um öll alvarleg atvik og áhættu sem upp koma í net- og upplýsingaskerfum þeirra.

Skal tilkynning berast í gegnum tilkynningagátt stjórnvalda um öryggisatvik, með tölvupósti á tölvupóstfang netöryggissveitarinnar eða, eftir atvikum, símleiðis.

Við mat á því hvort að atvik eða áhætta teljist alvarleg skal litið til þess hvort að atvik eða áhætta:

a. hefur eða líklegt þykir að muni valda þjónusturofi eða ósamfellu í veitingu þjónustu mikilvægs innviðar;
b. hefur eða líklegt þykir að muni raski öryggi og/eða virkni net- og upplýsingakerfa sem eru grundvöllur fyrir veitingu þjónustu mikilvægs innviðar;
c. hefur eða líklegt þykir að muni hafa áhrif yfir landamæri;

d. hefur eða líklegt þykir að muni hafa áhrif á veitingu þjónustu annarra mikilvægra innviða, þar á meðal vegna viðhalds.

Netöryggissveitin skal gefa út nánari leiðbeiningar um hvaða atvik og áhætta teljist alvarleg á grundvelli ákvæðis þessa. Skulu mikilvægir innviðir, eftir fremsta megni, taka mið af leiðbeiningum sveitarinnar við mat á því hvort atvik eða áhætta sé tilkynningarskylt samkvæmt ákvæði þessu.

Tilkynningar til netöryggissveitarinnar samkvæmt 1. mgr. skulu berast eins fljótt og verða má og eigi síðar en eigi síðar en 6 klukkustundum eftir að borin hafa verið kennsl á atvik eða áhættu í kerfum mikilvægs innviðar. Í tilkynningu skal m.a. veita eftirfarandi upplýsingar:

a. hvenær atviks eða áhættu var fyrst vart í net- og upplýsingakerfum;
b. frummat á eðli og/eða tegund atviks eða áhættu í net- og upplýsingakerfum;
c. frummat á umfangi atviks eða áhættu;
d. frummat á mögulegum smitáhrifum;
e. hver sé rekstraraðili umræddra net- og upplýsingakerfa, t.a.m. ef rekstri þeirra útvistað.

Netöryggissveitin skal miðla tilkynningum samkvæmt ákvæði þessu til þess eftirlitsstjórnvalds sem fer með eftirlit gagnvart hlutaðeigandi mikilvægum innvið. Þá skal netöryggissveit upplýsa önnur hlutaðeigandi stjórnvöld, eftir því sem við á, enda sé atvik eða áhætta af þeim toga að haft getur alvarleg áhrif á veitingu þjónustu annarra mikilvægra innviða.

26. gr.

Tilkynningar til viðskiptavina.

Mikilvægir innviðir skulu vera með skýra og skilvirka ferla vegna tilkynninga um ósamfellu í virkni eða þjónusturofi, svo sem af völdum atviks, bilana, breytinga eða viðhalds. Á heimasíðu mikilvægs innviðar, eða með öðrum sambærilegum leiðum, skal tilgreina þjónustuviðmið, svo sem um þjónustustig og reglubundið viðhald.

Mikilvægir innviðir skulu tilkynna viðskiptavinum um truflanir eða þjónusturof. Í tilkynningu skal að lágmarki koma fram hvaða áhrif truflunin eða þjónusturofið hefur eða getur haft og þær ráðstafanir sem mikilvægur innviður muni grípa til, ásamt ráðleggingum til viðskiptamanna ef svo ber undir. Sé rekstraraðili nauðsynlegrar þjónustu viðskiptavinur mikilvægs innviðar skal tilkynna honum slíkt sérstaklega.

VII. kafli

Eftirlit, samræmi og viðurlög.

27. gr.

Stefna eftirlitsstjórnvalda.

Eftirlitsstjórnvöld, hvert á sínu sviði, hafa eftirlit með að mikilvægir innviðir uppfylli lágmarkskröfur laga nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða, um áhættustýringu og viðbúnað sem nánar eru útfærðar í reglugerð þessari.

Eftirlitsstjórnvöld skulu setja sér stefnu um fyrirkomulag og framkvæmd eftirlits samkvæmt 1. mgr. Henni skal miðlað til samhæfingarstjórnvalds. Við fyrirkomulag og framkvæmd eftirlits á veitendum stafrænnar þjónustu skal sérstaklega tekið mið af stærð, starfsaldri og eðli og umfang reksturs hlutaðeigandi.

28. gr.

Aðgangur að upplýsingum.

Um aðgang eftirlitsstjórnvalda að upplýsingum fer samkvæmt lögum nr. 78/2019. Rekstraraðili nauðsynlegrar þjónustu skal afhenda eftirlitsstjórnvöldum allar upplýsingar sem óskað er eftir og varða net- og upplýsingaöryggi, þ.m.t. um skipulag net- og upplýsingaöryggis,

öryggisstefnu, áhættumat, lýsingu á öryggisráðstöfunum, viðbragðsáætlun, atvikaskrá og skýrslur um innra eftirlit, hvenær sem óskað er eftir því.

Eftirlitsstjórnvöld geta óskað eftir nánari skýringum og gögnum um einstök atvik í starfsemi rekstraraðila nauðsynlegrar þjónustu. Rekstraraðilum ber að verða við slíkri beiðni eins fljótt og auðið er. Aðgangsheimild eftirlitsstjórnvalda samkvæmt ákvæði þessu nær einnig til persónuupplýsinga í skilningi laga um persónuvernd og vinnslu persónuupplýsinga, að því marki sem nauðsynlegt er.

Við mat eftirlitsstjórnvalds á uppfyllingu lágmarkskrafna um áhættustýringu og viðbúnað í starfsemi rekstraraðila nauðsynlegrar þjónustu skal meðal annars horft til atvikaskrár og niðurstaðna atvikagreiningar.

Eftirlitsstjórnvaldi er heimilt, að eigin frumkvæði, að óska eftir reglubundinni skýrslugjöf frá mikilvægum innviðum um meðhöndlun atvika. Mikilvægum innviðum ber að verða við slíkri beiðni innan þeirra tímamarka sem eftirlitsstjórnvald setur. Aðgangur að upplýsingum samkvæmt 1. og 2. mgr. þessa ákvæðis gildir um veitendur stafrænnar þjónustu þegar rökstuddur grunur er um að hlutaðeigandi uppfyllir ekki kröfur reglugerðar þessar.

29. gr.

Úttektir og prófanir.

Um heimildir eftirlitsstjórnvalda til úttekta og prófana fer samkvæmt lögum nr. 78/2019. Eftirlitsstjórnvöldum er heimilt að prófa öryggi net- og upplýsingakerfa rekstraraðila nauðsynlegrar þjónustu og gera úttektir á því hvort að farið er eftir ákvæðum reglugerðar þessarar. Gildir einu hvort það er að eigin frumkvæði eða samkvæmt ábendingu. Viðeigandi eftirlitsstjórnvald ákveður framkvæmd prófana eða úttekta, að teknu tilliti til leiðbeinandi tilmæla samkvæmt 1. mgr. 30. gr.

Eftirlitsstjórnvöldum er heimilt að fela sjálfstætt starfandi sérfræðingi að annast framkvæmd úttektar og skýrslugerð um niðurstöðu hennar. Skal hann bundinn þagnarskyldu um störf sín í þágu eftirlitsstjórnvalda. Rekstraraðila nauðsynlegrar þjónustu skal gefinn kostur á því að gera athugasemdir við val eftirlitstjórnvalda á slíkum sérfræðingi.

30. gr.

Samhæfingarstjórnvald.

Samhæfingarstjórnvald skal sinna almennri stefnumörkun um eftirlit með lágmarkskröfum um öryggi net- og upplýsingakerfa samkvæmt lögum nr. 78/2019 og reglugerð þessari, með það að markmiði að stuðla sem best að samræmi og jafnræði við framkvæmd laganna. Í því skyni er samhæfingarstjórnvaldi meðal annars heimilt að gefa út almenn leiðbeinandi tilmæli um framkvæmd eftirlits, svo sem aðferðarfræði úttekta.

Samhæfingarstjórnvald skal vera tengiliður milli eftirlitsstjórnvalda og hvetja til reglulegra upplýsingafunda og samskipta meðal eftirlitsstjórnvalda.

Samhæfingarstjórnvald skal koma á og leiða samráðsvettvang eftirlitsstjórnvalda til að miðla þekkingu og reynslu sem og að samhæfa framkvæmd eftirlits. Það skal leitast við að verða við beiðni eftirlitsstjórnvalds um aðstoð við undirbúning, framkvæmd og eftirfylgni úttekta á grundvelli laga nr. 78/2019.

31. gr.

Bindandi fyrirmæli eftirlitsstjórnvalda.

Eftirlitsstjórnvaldi er heimilt að gefa út bindandi fyrirmæli um úrbætur ef mat þess er að mikilvægur innviður uppfylli ekki kröfur laga nr. 78/2019 og reglugerðar þessarar, þ.m.t. um skipulag net- og upplýsingakerfa og einstakar lágmarksöryggisráðstafanir. Skal gefinn til þess hæfilegur frestur. Áður en bindandi fyrirmæli eru gefin skal gefa viðkomandi aðila tækifæri til að koma á framfæri athugasemdum sínum og skýringum.

Vanræki mikilvægur innviður að verða við bindandi fyrirmælum eftirlitsstjórnvalds innan þess frests sem stjórnvaldið setur er eftirlitsstjórnvaldi heimilt að láta vinna verkið fyrir hönd og á kostnað hlutaðeigandi aðila. Kröfur sem kunna að myndast samkvæmt þessu ákvæði eru aðfararhæfar.

Brot á reglugerð þessari varða viðurlögum samkvæmt ákvæðum laga nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða.

32. gr.

Heimild og gildistaka.

Reglugerð þessi er sett með heimild í 3., 7., 8., 13. og 28. gr. laga nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða, og öðlast gildi 1. september 2020.