Nr. 480 15. apríl 2021

REGLUGERÐ

um netöryggissveit Póst- og fjarskiptastofnunar (CERT-ÍS).

I. KAFLI
Almenn ákvæði.

1. gr.
Gildissvið.

Reglugerð þessi gildir um netöryggissveit sem starfrækt er á Íslandi samkvæmt lögum nr. 81/2003 um fjarskipti, lögum nr. 78/2019 um öryggi net- og upplýsingakerfa mikilvægra innviða og lögum nr. 69/2003 um Póst- og fjarskiptastofnun.

2. gr.
Markmið.

Markmið með starfrækslu netöryggissveitar er að fyrirbyggja og draga úr hættu á netárásum og öðrum atvikum á Íslandi og takmarka útbreiðslu þeirra og tjón eins og kostur er. Sveitin skal styðja við skjót viðbrögð gegn aðsteðjandi ógnum, áhættu og atvikum og stuðla að viðeigandi ástandsvitund í netöryggismálum hér á landi. Þá er markmið netöryggissveitar að stuðla að markvissum og samhæfðum viðbrögðum við ógnum, áhættu og atvikum.

3. gr.
Orðskýringar.

1. *Atburður:* Óviðbúin staða, óþekkt eða þekkt, sem getur skipt máli fyrir öryggi net- og upplýsingakerfa eða skert þjónustu mikilvægs innviðar.
2. *Atvik:* Atvik í skilningi laga um öryggi net- og upplýsingakerfa mikilvægra innviða og öryggisatvik í skilningi laga um fjarskipti.
3. *Áhætta:* Aðstæður eða atburðir sem gætu haft skaðleg áhrif á öryggi net- og upplýsingakerfa.
4. *CERT-* eða *CSIRT-teymi:* Alþjóðleg heiti yfir öryggis- og viðbragðsteymi á sviði net- og upplýsingaöryggis, eða netöryggissveit (e. computer emergency response team eða computer security and incident response team).
5. *Fjarskiptafyrirtæki:* Fjarskiptafyrirtæki í skilningi laga um fjarskipti.
6. *Mikilvægir innviðir:* Mikilvægir innviðir í skilningi laga um öryggi net- og upplýsingakerfa mikilvægra innviða.
7. *Net- og upplýsingakerfi:* Net- og upplýsingakerfi í skilningi laga um öryggi net- og upplýsingakerfa mikilvægra innviða.
8. *Netumdæmi Íslands:* Sjálfstæð eða eftir atvikum samtengd net- og upplýsingakerfi sem falla innan þeirra raða IP-vistfanga sem úthlutað hefur verið hér á landi og ásamt lénum sem skráð eru undir íslensku landshöfuðléni.
9. *Samstarfsaðili netöryggissveitar:* Aðili utan þjónustuhópa netöryggissveitar sem er í samskiptum við sveitina vegna öryggis net- og upplýsingakerfa.
10. *Stöðumynd vegna netógna:* Heildstætt mat á stöðu og þróun netöryggismála á ákveðnu tímabili í netumdæmi Íslands eða afmarkaðra samhengi, til dæmis ólíkra þjónustuhópa netöryggissveitar, og byggir á öflun og úrvinnslu tiltækra upplýsinga og gagna.
11. *Þjónustuhópar netöryggissveitar:* Aðilar sem lögum samkvæmt njóta þjónustu netöryggissveitar, einkum mikilvægir innviðir, fjarskiptafyrirtæki, Stjórnarráð Íslands og eftir atvikum aðrir aðilar.

II. KAFLI
Skipulag og starfsumhverfi.

4. gr.
Skipulag og starfssvæði.

Póst- og fjarskiptastofnun starfrækir netöryggissveit og ber forstjóri ábyrgð á starfsemi og innra skipulagi hennar.

Netöryggissveit skal vera skipulagslega aðgreind frá eftirlitshlutverki Póst- og fjarskiptastofnunar á sviði net- og upplýsingaöryggis og skal bókhald sveitarinnar skráð sérstaklega. Netöryggissveit skal starfa í samræmi við gæðastefnu Póst- og fjarskiptastofnunar.

Netöryggissveit skal móta og innleiða stefnu um öryggi starfssvæðis sveitarinnar, meðal annars öryggi búnaðar og kerfa.

Forstjóri Póst- og fjarskiptastofnunar veitir aðgangsheimildir að starfssvæði netöryggissveitar. Einungis skal veita þeim aðgang sem þangað á lögmætt erindi og hefur gilda aðgangsheimild. Forstjóra Póst- og fjarskiptastofnunar er heimilt að takmarka, synja um eða afturkalla aðgangsheimild af öryggisástæðum og/eða ef allsherjarregla krefst þess.

5. gr.

Starfslið netöryggissveitar.

Starfslið netöryggissveitar skal hafa viðeigandi menntun og búa yfir þekkingu og reynslu sem nauðsynleg er til að gegna þeim lögbundnu skyldum sem felast í hlutverki sveitarinnar af ýtrustu fagmennsku.

Starfslið netöryggissveitar skal uppfylla skilyrði öryggisvottunar samkvæmt 24. gr. varnarmálalaga, nr. 34/2008.

Áður en utanaðkomandi aðila er fengið afmarkað verkefni á sviði netöryggismála hjá netöryggissveit skal ávallt óska eftir sakavottorði og trúnaðaryfirlýsing undirrituð sem tekur til upplýsinga er varða starfsemi sveitarinnar, eftir því sem við á. Meta skal hvort gera beri kröfu um að utanaðkomandi aðili uppfylli skilyrði öryggisvottunar samkvæmt 2. mgr., einkum ef verkefni felur í sér vinnslu trúnaðarupplýsinga.

III. KAFLI
Hlutverk og verkefni.

6. gr.

Hlutverk netöryggissveitar.

Netöryggissveit gegnir hlutverki landsbundins öryggis- og viðbragðsteymis vegna ógna, atvika og áhættu er varðar net- og upplýsingaöryggi (þjóðar-CSIRT). Í því felst að fyrirbyggja og draga úr hættu á ógnum, atvikum og áhættu í netumdæmi Íslands, eins og kostur er, styðja við skjót viðbrögð við aðsteðjandi hættu, sporna við útbreiðslu atvika og lágmarka tjón. Netöryggissveit meðhöndlar tilkynningar og aðrar upplýsingar um atvik og áhættu í netumdæmi Íslands og samræmir viðbrögð meðal þjónustuhópa sinna og samstarfsaðila, eftir því sem við á.

Netöryggissveit gegnir hlutverki tengiliðar íslenskra stjórnvalda í alþjóðlegu og evrópsku samstarfi CSIRT-sveita. Slíkt samstarf tekur einkum til miðlunar og móttöku upplýsinga er varða áhættu, atvik, varnir og viðbúnað vegna mögulegra ógna. Sveitin tekur þátt í öðru samstarfi á sviði netöryggismála, innan og utan þjónustuhópa sinna, við CSIRT-sveitir, CERT-teymi eða aðra aðila sem vinna að netöryggismálum.

Netöryggissveit skal stuðla að bættu netöryggi með fyrirbyggjandi aðgerðum með ráðgjöf, upplýsingamiðlun, útgáfu leiðbeininga og tilkynninga og, ef við á, tilmælum um ákveðnar aðgerðir vegna atvika og áhættu.

Verkefni netöryggissveitar skulu ávallt unnin með það að markmiði að samræma og hámarka árangur aðgerða til verndar netumdæmis Íslands.

Um þjónustu við einstaka þjónustuhópa og verkefni netöryggissveitar að öðru leyti fer samkvæmt lögum og reglugerð þessari. Netöryggissveit útfærir nánara fyrirkomulag helstu verkefna og forgangsröðun þeirra á hverjum tíma.

7. gr.

Ástandsvitund og stöðumynd vegna netógna.

Netöryggissveitin skal leitast við að skapa viðeigandi almenna ástandsvitund um ógnir, áhættu og atvik innan netumdæmis Íslands.

Netöryggissveit mótar stöðumynd vegna netógna og skal að minnsta kosti árlega skjalfesta og miðla slíku stöðumati til netöryggisráðs. Þá skal netöryggissveit leitast við að upplýsa eftirlits-

stjórnvöld reglulega um stöðumynd vegna netógna, eftir atvikum að því er tiltekna þjónustuhópa varðar.

Á grundvelli almennrar ástandsvitundar og stöðumynda vegna netógna á hverjum tíma forgangsraðar og skipuleggur netöryggissveit fyrirbyggjandi aðgerðir og samstarf við og innan þjónustuhópa sveitarinnar, og eftir atvikum, netumdæmis Íslands, í því skyni að sporna við áhættu og atvikum sem ógna öryggi net- og upplýsingakerfa.

8. gr.

Meðhöndlun áhættu og atvika.

Netöryggissveit skal, eins fljótt og kostur er, bregðast við tilkynningum um atvik og áhættu samkvæmt lögum nr. 78/2019, um öryggi net- og upplýsingakerfi mikilvægra innviða, og lögum nr. 81/2003, um fjarskipti, með veitingu upplýsinga og/eða ráðgjöf um viðbrögð og aðgerðir, eftir því sem tilefni og nauðsyn ber til. Netöryggissveit skal, á grundvelli bestu þekkingar á hverjum tíma, leitast við að bregðast við tilkynningum, beiðnum um aðstoð og/eða öðrum upplýsingum um ógn, áhættu eða atvik sem sveitinni berast, frá þjónustuhópum og samstarfsaðilum, með það að markmiði að sporna við og lágmarka tjón innan netumdæmis Íslands. Ef þörf krefur er netöryggissveit heimilt að forgangsraða þannig að brugðist sé við tilkynningum um atvik eða áhættu frá þjónustuhópum sveitarinnar áður en brugðist er við upplýsingum eða tilkynningum frá öðrum.

Um samhæfingu aðgerða og tilmæli netöryggissveitar samkvæmt ákvæði þessu fer samkvæmt 9. og 10. gr. og um samstarf við ríkislögreglustjóra samkvæmt 14. gr.

Netöryggissveit skal gefa út leiðbeiningar um form, efni og flokkun tilkynninga sem henni berast og birta á vef sínum. Í leiðbeiningunum skal greinarmunur gerður á annars vegar tilkynningum um atvik og áhættu sem skylt er að miðla til netöryggissveitar samkvæmt lögum nr. 81/2003 og lögum nr. 78/2019 og hins vegar öðrum valkvæðum tilkynningum frá þjónustuhópum og öðrum aðilum.

9. gr.

Samhæfing aðgerða og miðlun til þriðju aðila.

Netöryggissveit er samhæfingaraðili vegna ógna, áhættu og atvika sem upp koma hjá þjónustuhópum sveitarinnar og, ef við á, innan netumdæmis Íslands og skal ávallt leitast við að ná sem bestum tökum á aðstæðum svo takmarka megi mögulegt tjón. Við samhæfingu aðgerða er netöryggissveit heimilt að miðla viðeigandi gögnum og upplýsingum til þriðju aðila ef slík miðlun er nauðsynleg til að lágmarka tjón og/eða tryggja öryggi net- og upplýsingakerfa. Miðlun samkvæmt 2. málsl. skal takmarkast við upplýsingar sem móttakanda eru nauðsynlegar svo grípa megi til viðeigandi mótvægisaðgerða. Um meðferð gagna og upplýsinga í starfsemi sveitarinnar fer samkvæmt 29. gr. og um vinnslu persónuupplýsinga fer samkvæmt ákvæðum VII. kafla.

10. gr.

Tilmæli netöryggissveitar.

Í því skyni að bregðast við og samhæfa viðbrögð við ógn, atviki eða áhættu í netumdæmi Íslands getur netöryggissveit gefið út tilmæli um aðgerðir eða ráðstafanir.

Mikilvægir innviðir og fjarskiptafyrirtæki skulu ávallt leitast við að verða við tilmælum netöryggissveitar samkvæmt 1. mgr. vegna atviks, áhættu eða bráðrar netógnar sem steðjar að einum eða fleiri mikilvægum innviðum eða fjarskiptafyrirtækjum. Skulu þeir staðfesta móttöku tilmæla og bregðast við þeim eins fljótt og kostur er og aðstæður krefjast. Í viðbrögðum samkvæmt ákvæði þessu felst m.a. að veita netöryggissveit upplýsingar um hvernig tilmælum verður fylgt og innan hvaða tímaramma eða, verði þeir ekki við tilmælum netöryggissveitar samkvæmt 1. mgr., að upplýsa um ástæður þess og hvaða aðrar ráðstafanir talið er að eigi betur við til að tryggja vernd net- og upplýsingakerfa þeirra.

Fjarskiptafyrirtækjum er skylt að verða við tilmælum netöryggissveitar samkvæmt 1. mgr. þegar tilmæli varða:

a. aðgerðir gegn bráðri hættu sem steðjar að öryggi neta og þjónustu eins eða fleiri fjarskiptafyrirtækja, eða

b. mjög alvarleg atvik eða áhættu sem steðjar að öryggi net- og upplýsingakerfa mikilvægra innviða eða opinberra stofnana, almannahagsmunum eða þjóðaröryggi, enda yfirgnæfandi líkur á að fjarskiptafyrirtæki geti átt hlutdeild í að sporna við ógn, áhættu eða atviki eða lágmarka mögulegt tjón af völdum þess.

Ef mat netöryggissveitar er að a- eða b-liður 3. mgr. eigi við um aðstæður eða atvik skal sérstaklega vísað til þess í tilmælum.

11. gr.

Tilkynningar frá netöryggissveit.

Netöryggissveit skal tilkynna þjónustuhópum sínum um þekkta ógn, áhættu eða atvik sem sveitin hefur upplýsingar um.

Netöryggissveit skal styðja við þjónustuhópa sína með leiðbeiningum um fyrirbyggjandi aðgerðir og upplýsingamiðlun er miðar að því að draga úr ógn, áhættu og afleiðingum atvika, eins og kostur er.

Fjarskiptafyrirtæki og mikilvægir innviðir skulu gera viðeigandi ráðstafanir til að vakta og móttaka upplýsingar sem berast frá netöryggissveit samkvæmt 1. mgr. Þeim ber jafnframt að staðfesta móttöku tilkynninga eins fljótt og kostur er.

Netöryggissveit getur sett sér verklagsreglur um form og flokka tilkynninga samkvæmt 1. mgr.

12. gr.

Viðbúnaðaræfingar.

Netöryggissveit er heimilt að skipuleggja viðbúnaðaræfingar sem miða að því að bæta boðleiðir, stjórnun og sameiginlegt viðbragð við áhættu og atvikum sem ógna öryggi net- og upplýsingakerfa, þar á meðal lágmörkun áhættu og tjóns. Viðbúnaðaræfingar geta verið verkefni innan samráðs-, sviðs- og samstarfshópa sveitarinnar, sbr. 13. gr. Áhersla skal lögð á æfingar í samstarfi við þjónustuhópa og opinbera samstarfsaðila.

Ef við á, skulu viðbúnaðaræfingar skipulagðar í samstarfi við ríkislögreglustjóra og/eða eftirlitsstjórnvöld.

IV. KAFLI
Samstarf og upplýsingagjöf netöryggissveitar.

13. gr.

Samstarf við þjónustuhópa.

Netöryggissveit skal viðhafa virkt samstarf við þjónustuhópa sína og hvetja til tæknilegs samstarfs innan og meðal þeirra. Í því skyni skal sveitin setja á fót og leiða starf eftirfarandi hópa og skulu allir viðeigandi aðilar tilnefna fulltrúa sinn í þá:

a. Þverfaglegan samráðshóp mikilvægra innviða, er miði að því að efla tengsl og samstarf á milli mikilvægra innviða og netöryggissveitar.
b. Sviðshópa fyrir hvert svið nauðsynlegrar þjónustu og veitendur stafrænnar þjónustu. Tilgangur sviðshópa er að vera vettvangur tæknilegs samráðs og upplýsingaskipta á sviði net- og upplýsingaöryggis.
c. Samstarfshóp fjarskiptafyrirtækja. Tilgangur hans er að vera vettvangur tæknilegs samráðs og upplýsingaskipta vegna öryggis fjarskiptaneta og -þjónustu.

Netöryggissveit er heimilt að efna til samstarfs við aðra þjónustuhópa í samræmi við ákvæði þetta, svo sem Stjórnarráðs Íslands og aðrar opinberar stofnanir.

Hópur samkvæmt 1. og 2. mgr. skal funda í húsnæði samkvæmt ákvörðun netöryggissveitar. Einnig er heimilt að halda fjarfund með samskiptabúnaði, enda hafi hann verið samþykktur af netöryggissveit og að teknu tilliti til trúnaðarstigs fundarefnis. Samskiptum innan hóps skal stýrt af fulltrúa netöryggissveitar, nema annað sé skýrt tekið fram í verklagsreglum samkvæmt 4. mgr.

Trúnaður skal ríkja um upplýsingar sem ræddar eru á fundum hópa samkvæmt ákvæði þessu. Öll gögn sem þátttakendur fá í hendur, eru búin til af eða fyrir þátttakendur, afhent á vettvangi þeirra eða unnin á annan hátt innan hópanna teljast til vinnugagna í skilningi 2. og 3. tölul. 2. mgr. 8. gr. upplýsingalaga, nr. 140/2012, og eru undanþegin aðgangsrétti almennings, sbr. 5. tölul. 6. gr. sömu

laga. Þátttakendur í hópum skulu skuldbinda sig til að halda trúnað samkvæmt ákvæði þessu með undirritun yfirlýsingar þar um.

Að frumkvæði netöryggissveitar skal hver hópur samkvæmt 1. og 2. mgr. setja sér stefnu og verklagsreglur þar sem m.a. greinir tilgang og markmið hópsins, fyrirkomulag samstarfsins, tíðni funda og, ef við á, hvernig lögbundinn trúnaður og öryggi upplýsinga sem fram koma er tryggt. Að öðru leyti fer umfang og útfærsla starfa eftir þörfum hvers hóps fyrir sig.

14. gr.

Upplýsingagjöf og samstarf við ríkislögreglustjóra.

Netöryggissveit skal leitast við að upplýsa ríkislögreglustjóra um alvarleg og/eða útbreidd atvik eða áhættu sem ógna öryggi net- og upplýsingakerfa er varða þjónustuhópa netöryggissveitar og netumdæmi Íslands, eins og við á hverju sinni.

Netöryggissveit er skylt að tilkynna ríkislögreglustjóra um yfirvofandi atvik og áhættu sem sveitin telur geta haft víðtæk eða alvarleg áhrif á þjónustuhópa sína, almannahagsmuni eða þjóðaröryggi, svo og þegar slík ógn hefur raungerst og aðstæður kalla á fullan viðbúnað sveitarinnar.

Ef aðstæður eru með þeim hætti að teljist neyðarástand sem kann að ógna lífi og heilsu almennings, umhverfi og/eða eignum í skilningi laga nr. 82/2008, um almannavarnir, fer um viðbrögð stjórnvalda á grundvelli þeirra laga.

Netöryggissveit skal setja sér verklagsreglur um upplýsingagjöf og samskipti samkvæmt ákvæði þessu, í samráði við ríkislögreglustjóra.

Um mat á stöðu, viðbrögð, samstarf og samhæfingu í kjölfar tilkynningar samkvæmt 2. mgr. fer samkvæmt viðbragðsáætlun ríkislögreglustjóra sem gerð er í samráði við netöryggissveit og sett á grundvelli laga um almannavarnir.

15. gr.

Upplýsingagjöf og samstarf við netöryggisráð.

Netöryggissveit skal leitast við að upplýsa netöryggisráð um alvarleg og/eða útbreidd atvik eða áhættu sem ógna öryggi net- og upplýsingakerfa og tengjast þjónustuhópum sveitarinnar eða, ef við á, netumdæmi Íslands almennt, eins og við á hverju sinni.

Netöryggissveit er skylt að upplýsa netöryggisráð um yfirvofandi atvik og áhættu sem sveitin telur geta haft víðtæk eða alvarleg áhrif á þjónustuhópa sína, almannahagsmuni eða þjóðaröryggi, svo og þegar slík netógn hefur raungerst og aðstæður kalla á fullan viðbúnað sveitarinnar. Þegar stjórn hefur náðst á áhættu eða atviki samkvæmt 1. málsl. skal netöryggissveit skila viðeigandi samantekt þar um til netöryggisráðs.

16. gr.

Tilkynning til erlendra tengiliða.

Ef netöryggissveit hefur upplýsingar um atvik eða áhættu sem ógnar öryggi net- og upplýsingakerfa og áhrifa kann að gæta yfir landamæri skal sveitin eftir því sem við á tilkynna um það til tengiliðar í því ríki eða ríkjum sem um ræðir.

Netöryggissveit skal setja sér verklagsreglur um tilkynningar og miðlun upplýsinga til erlendra aðila samkvæmt ákvæði þessu.

17. gr.

Miðlun upplýsinga um atvik og áhættu til eftirlitsstjórnvalda.

Netöryggissveit skal setja sér verklagsreglur um miðlun nauðsynlegra upplýsinga til eftirlitsstjórnvalda í kjölfar tilkynninga um alvarleg atvik eða áhættu sem ógna öryggi net- og upplýsingakerfa og henni berast frá mikilvægum innviðum og fjarskiptafyrirtækjum samkvæmt lögum nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða, og lögum nr. 81/2003, um fjarskipti.

Verklagsreglur samkvæmt 1. mgr. skulu vera aðgengilegar eftirlitsstjórnvöldum.

18. gr.

Tilkynningar til lögreglu um refsiverða háttsemi.

Ef atvik eða áhætta sem tilkynnt er um til netöryggissveitar er þess eðlis að grunur er um refsiverða háttsemi skal sveitin án tafar hvetja hlutaðeigandi aðila til að tilkynna um atvik til lögreglu.

Netöryggissveit er heimilt að vísa til lögreglu upplýsingum sem henni berast vegna landsbundins hlutverks síns sem tengiliðar ef efni þeirra teljast fremur varða viðfangsefni löggæslu en netöryggissveitar.

19. gr.

Reglubundin upplýsinga- og skýrslugjöf netöryggissveitar.

Netöryggissveit skal árlega birta skýrslu er geymir tölfræðilega samantekt og almenna umfjöllun um starfsemi hvers árs á vef sveitarinnar og kynna hana fyrir þjónustuhópum sínum og netöryggisráði. Efnistök skýrslunnar skulu miðast við birtingu á opinberum vettvangi.

Um meðferð gagna og upplýsinga í starfsemi netöryggissveitar fer samkvæmt 29. gr. Skýrslur netöryggissveitar samkvæmt 1. mgr. skulu skilmerkilega auðkenndar viðeigandi trúnaðarstigi, ásamt leiðbeiningum til viðtakenda um frekari miðlun og aðra meðferð.

V. KAFLI
Samningar við netöryggissveit.

20. gr.

Þjónustusamningur um sjálfvirka upplýsingamiðlun.

Netöryggissveit er heimilt að óska eftir að mikilvægir innviðir eða fjarskiptafyrirtæki geri samninga við sveitina um sjálfvirka upplýsingamiðlun í því skyni að greina og meta áhættu, atvik og aðrar ógnir í net- og upplýsingakerfum þeirra. Samningar um sjálfvirka upplýsingaöflun skulu ávallt vera skriflegir og að minnsta kosti eftirtöldum atriðum gerð viðeigandi skil:

a. Tæknileg útfærsla á hvernig sjálfvirkri upplýsingamiðlun er komið á milli kerfa aðila og netöryggissveitar.
b. Lýsing á þeim kerfum aðila sem umræddur samningur nær til.
c. Hvaða upplýsingum miðlað skal með sjálfvirkum hætti til netöryggissveitar og hvernig vísar í varnarbúnaði aðila eru afmarkaðir og uppfærðir.
d. Fyrirkomulag upplýsingagjafar og samskipta milli samningsaðila varðandi áhættu og atvik sem ógna öryggi net- og upplýsingakerfa og varðandi einstaka vísa sem netöryggissveit greinir úr upplýsingum frá aðila.
e. Upplýsingar um tegund og vinnslu persónuupplýsinga sem safnað er, meðferð þeirra, vistun og eyðingu.

Ef sjálfvirk upplýsingamiðlun samkvæmt ákvæði þessu leiðir til þess að vísbendingar greinast um alvarlega áhættu eða atvik, sem tilkynningarskyld eru samkvæmt lögum nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða og lögum nr. 81/2003, um fjarskipti, fer um meðhöndlun tilkynninga og samhæfingu samkvæmt 8.–10. gr.

Samningur um sjálfvirka upplýsingamiðlun samkvæmt ákvæði þessu leysir aðila ekki undan tilkynningarskyldu um alvarlega áhættu og atvik samkvæmt lögum nr. 78/2019 og lögum nr. 81/2003.

21. gr.

Samningar um tæknilega vöktunarþjónustu.

Netöryggissveit getur boðið mikilvægum innviðum að gera samninga um tæknilega vöktunarþjónustu fyrir net- og upplýsingakerfi þeirra í því skyni að greina og meta áhættu, atvik og aðrar ógnir. Í tæknilegri vöktunarþjónustu felst uppsetning búnaðar, setning greiningar- og samskiptareglna í samvinnu aðila.

Samningar um tæknilega vöktunarþjónustu skulu ávallt vera skriflegir og að minnsta kosti eftirtöldum atriðum gerð viðeigandi skil:

a. Tæknileg útfærsla á uppsetningu búnaðar og samskipta.
b. Lýsing á þeim kerfum aðila sem umræddur samningur nær til.

c. Lýsing á hvaða upplýsinga viðkomandi búnaður má afla og útfærslu á stillingum búnaðarins.
d. Fyrirkomulag upplýsingagjafar og samskipta milli samningsaðila varðandi áhættu og atvik sem ógna öryggi net- og upplýsingakerfa og varðandi einstaka vísa sem netöryggissveit greinir úr upplýsingum frá aðila.
e. Upplýsingar um tegund og vinnslu persónuupplýsinga sem safnað er, meðferð þeirra, vistun og eyðingu.

Ef tæknileg vöktunarþjónusta samkvæmt ákvæði þessu leiðir til þess að vísbendingar greinast um alvarlega áhættu eða atvik, sem tilkynningarskyld eru samkvæmt lögum nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða, fer um meðhöndlun tilkynninga og samhæfingu samkvæmt 8.–10. gr.

Samningur um tæknilega vöktunarþjónustu samkvæmt ákvæði þessu leysir aðila ekki undan tilkynningarskyldu um alvarlega áhættu og atvik samkvæmt lögum nr. 78/2019.

Endurgjald mikilvægra innviða vegna tæknilegrar vöktunarþjónustu samkvæmt ákvæði þessu skal taka mið af útlögðum kostnaði netöryggissveitarinnar við uppsetningu og rekstur þess búnaðar sem staðsettur er við net- og upplýsingakerfi viðkomandi aðila.

22. gr.

Tæknileg vöktun hjá fjarskiptafyrirtækjum.

Netöryggissveit getur farið fram á að fjarskiptafyrirtæki geri samning við sveitina um tæknilega vöktun og skal fjarskiptafyrirtæki verða við slíkri beiðni. Útfærsla slíkrar vöktunar skal skjalfest og fer um hana samkvæmt 1.-4. mgr. 21. gr.

Fjarskiptafyrirtæki skal hýsa og tengja eigin búnað við búnað netöryggissveitar sem nauðsynlegur er til að framkvæma tæknilega vöktun samkvæmt ákvæði þessu, endurgjaldslaust. Netöryggissveit skal bera ábyrgð á öðrum kostnaði vegna framkvæmdar vöktunarinnar.

23. gr.

Umferðarmagn hjá fjarskiptafyrirtækjum.

Netöryggissveit er heimilt að afla tölfræðilegra upplýsinga um heildarmagn umferðar í almennum netkerfum fjarskiptafyrirtækja, þar með talið á samtengipunktum og í útlandagáttum, enda séu þær upplýsingar ópersónugreinanlegar.

Netöryggissveit skal gera samning við fjarskiptafyrirtæki um útfærslu umferðarmælinga samkvæmt ákvæði þessu, svo sem um uppsetningu og rekstur nauðsynlegs búnaðar. Um efni slíkra samninga og endurgjald fer samkvæmt 1. og 2. mgr. 22. gr.

24. gr.

Samningar við opinberar stofnanir.

Netöryggissveit getur gert samninga við opinberar stofnanir um tæknilega vöktunarþjónustu samkvæmt 1. mgr. 21. gr., eða aðra sambærilega þjónustu, og fer um efni slíkra samninga samkvæmt 2. mgr. 21. gr. Endurgjald opinberra stofnana vegna þjónustu samkvæmt 1. málsl. skal taka mið af útlögðum kostnaði netöryggissveitar við uppsetningu og rekstur þess búnaðar sem staðsettur er við net- og upplýsingakerfi hlutaðeigandi stofnunar.

Netöryggissveit getur einnig gert samninga við opinberar stofnanir um sérstaka aðstoð, ráðgjöf og leiðbeiningar um sérhæfðar forvarnir í tengslum við öryggi net- og upplýsingakerfa þeirra, gegn endurgjaldi.

25. gr.

Þjónusta við Stjórnarráð Íslands.

Stjórnarráð Íslands skal njóta þjónustu netöryggissveitar á sviði netöryggismála, þar með talið tæknilegrar vöktunarþjónustu samkvæmt 1. mgr. 21. gr. eða annarrar sambærilegrar þjónustu, endurgjaldslaust. Útfærsla þjónustu á hverjum tíma, samkvæmt ákvæði þessu, skal skjalfest í samkomulagi milli aðila og skal það endurnýjað reglulega.

Um efni samkomulagsins um tæknilega vöktunarþjónustu fer samkvæmt 2. mgr. 21. gr.

26. gr.

Samningar við þriðju aðila.

Netöryggissveit er heimilt að bjóða öðrum þjónustu á sviði netöryggismála og skal gerður skriflegur samningur þar um. Samningurinn skal taka til umfangs þeirrar þjónustu sem veitt er, tæknilegrar útfærslu og endurgjalds.

VI. KAFLI

Öflun og meðferð gagna.

27. gr.

Aðgangur að upplýsingum.

Í því skyni að tryggja netöryggissveit bestu faglegu forsendur til viðbragða við, ógnum, atvikum og áhættu í netumdæmi Íslands skal henni, eins skjótt og við verður komið, heimilaður aðgangur að viðeigandi upplýsingum og gögnum sem hún metur nauðsynleg, þ.m.t. umferðarskrám netbúnaðar og -þjóna, eftir atvikum í samráði við eftirlitsstjórnvöld. Netöryggissveit getur einnig óskað eftir upplýsingum frá öðrum samstarfsaðilum sveitarinnar og stjórnvöldum, eftir því sem við á og nauðsynlegt þykir.

Netöryggissveit er heimilt að kalla einstaklinga til skýrslugjafar sem kunna að hafa upplýsingar sem nauðsynlegar eru svo sveitin geti sinnt lögbundnu hlutverki sínu, eftir atvikum í samráði við eftirlitsstjórnvöld. Við vinnslu upplýsinga sem aflað er með skýrslugjöf skal netöryggissveit eftir fremsta megni tryggja friðhelgi viðkomandi, m.a. með því að gæta trúnaðar um auðkenni hans.

Netöryggissveit skal setja og birta nánari verklagsreglur um fyrirkomulag skýrslugjafar samkvæmt 2. mgr.

Réttur netöryggissveitar til aðgangs að gögnum og upplýsingum samkvæmt lögum nr. 69/2003, um Póst- og fjarskiptastofnun, lögum nr. 81/2003, um fjarskipti, lögum nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða, og reglugerð þessari verður ekki takmarkaður með vísan til þagnarskyldu sem kann að gilda um viðkomandi aðila.

28. gr.

Upplýsingagjöf frá þjónustuhópum.

Netöryggissveit getur óskað eftir því að þjónustuhópar hennar gefi yfirlitsskýrslu í upphafi hvers árs, en eigi síðar en 1. febrúar, um öll helstu atvik og áhættu sem ógnað hafa öryggi net- og upplýsingakerfa næstliðið ár. Í slíkri skýrslu komi fram tölfræðilegt yfirlit um tíðni og gerðir áhættu og atvika.

Netöryggissveit getur birt á vef sínum staðlað form að yfirlitsskýrslu samkvæmt 1. mgr. og leiðbeiningar við útfyllingu þess.

29. gr.

Meðferð gagna og upplýsinga í starfsemi netöryggissveitar.

Netöryggissveit skal eftir fremsta megni tryggja öryggi gagna og upplýsinga sem sveitin vinnur með hverju sinni, svo og trúnað um efni þeirra, með aðgangsstýringu, dulritun og öðrum tiltækum ráðstöfunum. Þá skal netöryggissveit beita viðeigandi tæknilegum og skipulagslegum ráðstöfunum til að tryggja eins og kostur er öryggi net- og upplýsingakerfa sinna og þeirra gagna sem þau vista og varða hagsmuni þjónustuhópa hennar og í samræmi við skilgreint trúnaðarstig þeirra. Kerfi netöryggissveitar sem vista viðkvæm gögn, s.s. um atvik, úrlausn þeirra og upplýsingar um net- og upplýsingakerfi og viðbúnað eða áhættustýringu aðila, skulu aðskilin frá öðrum kerfum Póst- og fjarskiptastofnunar.

Í því skyni að tryggja öryggi innsendra gagna og upplýsinga sem best, skal netöryggissveit leitast við að gefa sendanda kost á að senda þau á sem öruggastan hátt miðað við tækni hverju sinni, til dæmis með dulkóðun og rafrænni undirritun, og beita dulkóðun á samskiptarásum. Dulkóðun sem beitt er, sem og aðrar öryggisráðstafanir, skulu vera í samræmi við bestu framkvæmd hverju sinni.

Netöryggissveit skal útbúa verklagsreglur um trúnaðarstig og flokkun innsendra gagna og gagna sem aflað er samkvæmt V. kafla. Verklagsreglur skulu byggja á alþjóðlega viðurkenndri aðferðafræði, til dæmis TLP trúnaðarflokkunarkerfinu. Trúnaðarflokkaðar upplýsingar má eingöngu nota í

þeim tilgangi að lágmarka eða fyrirbyggja útbreiðslu og tjón vegna atvika eða áhættu og ber að meðhöndla þær í samræmi við fyrirmæli sendanda um trúnaðarflokkun þeirra.

Netöryggissveit skal gera öryggisráðstafanir í öllum samskiptum við þjónustuhópa sína, innlend og erlend stjórnvöld, netöryggisráð eða aðra samstarfsaðila, til dæmis við miðlun tilkynninga um ógn, atvik eða áhættu, og tryggja eftir fremsta megni framfylgni við skilgreint trúnaðarstig og öryggi gagnanna. Við flutning og úrvinnslu gagna og upplýsinga er netöryggissveit heimilt að nýta sér tækni hvers tíma, svo sem dulkóðaðan tölvupóst og lokaðar miðlunarrásir. Tækni og aðferðir til miðlunar skulu kynntar fyrir þjónustuhópum sveitarinnar, ásamt áhættumati.

Netöryggissveit er heimilt að skrá gögn, bæði innsend og útsend, og önnur samskipti við aðila í innri kerfum, svo sem málaskrá, að því gefnu að öryggi gagna og upplýsinga samkvæmt reglugerð þessari og lögum, eftir því sem við á, sé tryggt.

Um trúnaðarflokkun og meðferð gagna og upplýsinga sem falla undir reglugerð nr. 959/2012, um vernd trúnaðarupplýsinga, öryggisvottanir og öryggisviðurkenningar á sviði öryggis- og varnarmála, fer samkvæmt henni.

VII. KAFLI
Vinnsla persónuupplýsinga.

30. gr.
Vinnsla persónuupplýsinga.

Að því marki sem er nauðsynlegt, er netöryggissveit heimil vinnsla persónuupplýsinga sem aflað er eða berast frá þjónustuhópum eða öðrum samstarfsaðilum í tengslum við hlutverk og verkefni sveitarinnar, án samþykkis hins skráða, sbr. 1. mgr. 21. gr. laga nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða, og 47. gr. c í lögum nr. 81/2003, um fjarskipti. Þjónustuhópum eða öðrum samstarfsaðilum netöryggissveitar er heimilt að miðla persónuupplýsingum til netöryggissveitarinnar að því marki sem nauðsynlegt er svo að sveitin geti sinnt hlutverki sínu, þ. á m. á grundvelli samnings samkvæmt V. kafla reglugerðar þessar. Persónuupplýsingar þessar geta verið margs konar, til dæmis tengiliðaupplýsingar, staðsetningargögn og netauðkenni. Netöryggissveit er enn fremur heimilt að greina efni einstakra fjarskiptasendinga til og frá neti þjónustuhópa ef rökstuddur grunur er um að þær innihaldi spillikóða og að fengnu samþykki hlutaðeigandi aðila.

Netöryggissveit er heimil miðlun persónuupplýsinga samkvæmt 1. mgr. til þriðja aðila, innan eða utan þjónustuhópa, ef:

a. sveitin metur það nauðsynlegt í þágu almannahagsmuna eða þjóðaröryggis og
b. miðlunin er til þess fallin að upplýsa um aðsteðjandi ógnir í netumdæmi Íslands, koma í veg fyrir netárás eða önnur alvarleg atvik eða til að takmarka útbreiðslu eða að öðru leyti takmarka tjón, þ.m.t. tryggja öryggi kerfa, vegna áhættu eða atvika.

Netöryggissveit skal gera viðeigandi verndarráðstafanir til að tryggja öryggi persónuupplýsinga, m.a. með því að tryggja áreiðanleika þeirra, að þær skaðist ekki eða glatist og að þeim sé ekki miðlað til óviðkomandi aðila eða misnotaðar á annan hátt.

Geymslutími persónuupplýsinga samkvæmt ákvæði þessu skal takmarkaður við það sem nauðsynlegt er samkvæmt lögum og/eða tilgangi vinnslunnar. Gögn sem ekki er nauðsynlegt að geyma samkvæmt lögum skal eytt með öruggum hætti og/eða persónugreinanlegar upplýsingar úr gögnum fjarlægðar. Að öðru leyti fer um vinnslu persónuupplýsinga samkvæmt lögum nr. 90/2018, um persónuvernd og vinnslu persónuupplýsinga, að undanþegnum ákvæðum 17. og 20.–22. gr. þeirra laga.

31. gr.
Önnur vinnsla persónuupplýsinga og viðkvæmra persónuupplýsinga.

Netöryggissveit er almennt heimil vinnsla persónuupplýsinga og viðkvæmra persónuupplýsinga sem sveitinni berast, þ.m.t. móttaka upplýsinga og greining á innihaldi þeirra, án samþykkis hins skráða, sbr. 2. mgr. 21. gr. laga nr. 78/2019. Slíkar persónuupplýsingar geta borist frá þjónustuhópum hennar, fyrirtækjum, almenningi, innlendum og erlendum samstarfsaðilum.

Netöryggissveit er þó einungis heimilt að miðla upplýsingum samkvæmt 1. mgr. til þriðja aðila ef:

a. sveitin metur það nauðsynlegt í þágu almannahagsmuna, eða
b. í þágu hagsmuna hins skráða til að koma í veg fyrir eða takmarka mögulegt tjón sem hinn skráði getur orðið fyrir.

Berist netöryggissveit persónuupplýsingar samkvæmt ákvæði þessu sem teljast viðkvæmar skal ávallt framkvæma mat á áhrifum á persónuvernd vegna vinnslu þeirra eins fljótt og kostur er, í samræmi við 29. gr. laga nr. 90/2018, um persónuvernd og vinnslu persónuupplýsinga. Að öðru leyti fer um meðferð þeirra samkvæmt 3. og 4. mgr. 30. gr.

VIII. KAFLI
Önnur ákvæði.

32. gr.
Sérstök þagnarskylda.

Sérstök þagnarskylda starfsmanna netöryggissveitar samkvæmt 19. gr. laga nr. 78/2019 nær til allra gagna og upplýsinga sem eru hluti af starfsemi þeirra og eru því undanskilin ákvæðum upplýsingalaga, nr. 140/2012.

33. gr.
Heimild og gildistaka.

Reglugerð þessi er sett með stoð í 6. mgr. 4. gr. a laga nr. 69/2003, um Póst- og fjarskiptastofnun, 47. gr. d laga nr. 81/2003, um fjarskipti, 4. mgr. 16. gr., 4. mgr. 21. gr. og 28. gr. laga nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða.

Reglugerð þessi öðlast þegar gildi.

Við gildistöku reglugerðar þessarar fellur úr gildi reglugerð nr. 475/2013, um málefni CERT-ÍS netöryggissveitar.

Samgöngu- og sveitarstjórnarráðuneytinu, 15. apríl 2021.

Sigurður Ingi Jóhannsson.

Ragnhildur Hjaltadóttir.

B-deild – Útgáfud.: 3. maí 2021