Upplýsingaöryggisstefna Heilbrigðisstofunar Austurlands

Tilgangur

Upplýsingaöryggisstefna HSA lýsir áherslu framkvæmdastjórnar stofnunarinnar á upplýsingavernd og örugga meðferð upplýsingaeigna hennar. Verja þarf upplýsingaeignir Heilbrigðisstofnunar Austurlands og notenda þjónustu hennar fyrir öllum ógnum, innri og ytri, af ásetningi, vegna óhappa eða af slysni. Fagleg vinnubrögð eru lykillinn að árangri og til marks um það er þessi upplýsingaöryggisstefna sett. Innleiðing og framkvæmd stefnunnar er mikilvæg til að fullvissa starfsmenn Heilbrigðisstofnunar Austurlands, notendur þjónustu hennar og landsmenn alla um heilindi og rétt vinnubrögð í rekstri hennar. Framkvæmdastjórn Heilbrigðisstofnunar Austurlands hefur samþykkt þessa stefnu og styður við framkvæmd hennar.

Umfang

Upplýsingaöryggisstefnan tekur til umgengni og vistunar allra upplýsinga í vörslu Heilbrigðisstofnunar Austurlands á rafrænu formi, prentuðu, handskrifuðu, í formi lífsýna eða í mæltu máli. Hér er átt við:

a) Upplýsingar frá notendum þjónustu Heilbrigðisstofnunar Austurlands og viðskiptavinum, t.d. heilsufarsupplýsingar, lífsýni eða samningar við birgja sem Heilbrigðisstofnun Austurlands hefur í vörslu sinni.
b) Upplýsingar sem eru eign Heilbrigðisstofnunar Austurlands og bundnar eignarrétti eða háðar hugverkarétti.
c) Persónulegar upplýsingar sem tengjast starfsmönnum Heilbrigðisstofnunar Austurlands.

Upplýsingaöryggisstefnan tekur jafnframt til húsnæðis og búnaðar þar sem upplýsingar eru meðhöndlaðar eða vistaðar sem og starfsmanna og samningsbundinna viðskiptavina sem hafa aðgang að upplýsingum.

Markmið

Markmið Heilbrigðisstofnunar Austurlands með upplýsingaöryggisstefnunni eru að:

a) Upplýsingar séu réttar og aðgengilegar þeim sem aðgangsrétt hafa þegar þörf er á.
b) Leynd upplýsinga og trúnaði sé viðhaldið þegar við á. Trúnaðarupplýsingar séu óaðgengilegar óviðkomandi og varðar gegn skemmdum, eyðingu eða uppljóstrun til aðila sem hafa ekki aðgangsrétt hvort sem er af ásetningi eða kæruleysi (vangá).
c) Upplýsingar sem fara um net komist til rétts viðtakanda óskaddaðar, á réttum tíma og þess sé gætt að þær fari ekki til annarra.
d) Að áhætta vegna vinnslu (meðferðar) og varðveislu upplýsinga sé innan skilgreindra áhættumarka.
e) Alltaf séu til áreiðanleg og örugglega varðveitt afrit af gögnum og hugbúnaðarkerfum.
f) Fylgt sé öllum lögum, reglugerðum og reglum sem heilbrigðisstofnanir lúta. Þess skal sérstaklega gætt að vanda úrlausnir mála þar sem árekstrar kunna að verða milli ákvæða í mismunandi lögum og reglugerðum, t.d. upplýsingalögum og lögum um persónuvernd.
g) Fylgja öllum samningum sem Heilbrigðisstofnun Austurlands er aðili að og varða upplýsingaöryggi.
h) Áætlanir séu gerðar um samfelldan rekstur, þeim sé viðhaldið og þær prófaðar.
i) Frávik, brot eða grunur um veikleika í upplýsingaöryggi séu tilkynnt og rannsökuð.

Leiðir að markmiðum

Leiðir Heilbrigðisstofnunar Austurlands að ofangreindum markmiðum eru að:

Halda skrá yfir upplýsingaeignir og flokka þær eftir mikilvægi leyndar, réttleika og tiltækileika.
Greina reglulega með formlegu áhættumati verðmæti upplýsingaeigna, viðkvæmni þeirra og ógnir sem geta stefnt þeim í hættu.
Stjórna áhættu innan skilgreindra marka með því að hanna, innleiða og starfrækja formlegt stjórnkerfi upplýsingaöryggis sem sé í samræmi við viðurkennda öryggisstaðla s.s.ÍST ISO/IEC 27001.
Gera skipulagshandbók með verklagsreglum og verkferlum vegna notkunar upplýsingakerfa og búnaðar, meðferðar upplýsinga og viðhalda henni.
Allir starfmenn Heilbrigðisstofnunar Austurlands fái þjálfun og fræðslu varðandi upplýsingaöryggi og ábyrgð þeirra hvað varðar upplýsingaöryggi.
Allir starfsmenn fylgi skipulagshandbók.
Notkun tölvubúnaðar, af hvaða gerð sem er, sem ekki er í eigu Heilbrigðisstofnunar Austurlands er óheimil á innra neti stofnunarinnar. Óheimilt er að tengja utanaðkomandi tölvur við netið eða prentara sem eru staðsettir á stofnuninni. Heilbrigðisstofnun Austurlands lætur starfsfólki og/eða gestum í té tölvubúnað til þeirra nota sé það nauðsynlegt.

Notkun snjallsíma og spjaldtölva sem ekki er í eigu HSA, er bönnuð á neti HSA.
Starfsmenn vinna almennt inni á stofuninni, en heimilt er þó að leyfa starfsmönnum að vinna annarsstaðar frá enda hafi þeir fengið í hendur tölvubúnað til þess í eigu og umsjá stofnunarinnar. Í slíkum tölvum skal vera nauðsynlegur hugbúnaður og starfsmenn hlotið nauðsynlega þjálfun m.t.t. öryggismála. Óheimilt með öllu er að starfsmenn noti eigin (eða annan) búnað til fjartenginga inn á net stofnunarinnar.
Notendum er algerlega óheimilt að vista gögn er varða sjúklinga á útstöðvum.
Tryggja skal með bestu mögulegu aðferðum að til staðar sé varaafl (rafbakhjarlar og vararafstöðvar) sem tekur við verði bilun í rafveitukerfi.
Endurskoða skal öryggiskerfi stofunarinnar reglulega, a.m.k. árlega og oftar ef þurfa þykir.

Öryggisnefnd

Öryggisnefnd skal skipuð af framkvæmdastjórn með sérstöku skipunarbréfi. Hlutverk hennar er m.a. að tryggja að vinna innan Heilbrigðisstofnunar Austurlands samræmist viðurkenndum og gildandi verklagsreglum. Öryggisnefndin hefur einnig með höndum eftirlit með öryggisþáttum tölvuumhverfis stofnunarinnar, þmt. sjúkraskrár, og reglulegt eftirlit með notkun upplýsingakerfa m.a. uppflettingum starfsmanna í sjúkraskrá.

Ábyrgð

Ábyrgð við framkvæmd og viðhald upplýsingaöryggisstefnu skiptist á eftirfarandi hátt:

a) Framkvæmdastjórn Heilbrigðisstofnunar Austurlands ber ábyrgð á þessari upplýsingaöryggisstefnu og endurskoðar (rýnir) hana reglulega.
b) Öryggisstjóri Heilbrigðisstofnunar Austurlands ber ábyrgð á framkvæmd upplýsingaöryggisstefnunnar og beitir til þess viðeigandi stöðlum og vinnuferlum.
c) Allir starfsmenn Heilbrigðisstofnunar Austurlands bera ábyrgð á að þeim vinnuferlum, sem eiga að tryggja framkvæmd upplýsingaöryggisstefnunnar, sé fylgt. Samstarfsaðilar, verktakar og birgjar bera ábyrgð á að fylgt sé samningsbundnum vinnuferlum sem eiga að tryggja framkvæmd stefnunnar.
d) Öllum starfsmönnum Heilbrigðisstofnunar Austurlands ber að vinna samkvæmt upplýsingaöryggisstefnunni. Þeim ber að tilkynna öryggisfrávik og veikleika sem varða upplýsingaöryggi. Þeir sem ógna upplýsingaöryggi Heilbrigðisstofnunar Austurlands, notenda þjónustu hennar eða viðskiptavina af ásettu ráði eiga yfir höfði sér málshöfðun eða aðrar viðeigandi lagalegar aðgerðir sbr. lög um heilbrigðisstarfsmenn,

Endurskoðun

Þessi stefna skal endurskoðuð árlega og oftar ef þörf krefur til að tryggja að hún samrýmist markmiðum með rekstri Heilbrigðisstofnunar Austurlands.

Samþykki

Fyrir hönd framkvæmdastjórnar HSA

Öryggisnefnd hefur endurskoðað þetta skjal 11.10.2017

Viðaukar
Aðrar stefnur sem styðja upplýsingaöryggisstefnuna
a)Gæðastefna.
b)Aðgangsstefna, varðandi aðgang að gögnum og kerfum.
c)Fjarvinnustefna, varðandi vinnu starfsmanna heima fyrir.
Yfirlit yfir lög og reglur - Hlíting við lög, reglur og reglugerðir