# Upplýsingaöryggisstefna HSS

Stefna HSS í öryggi upplýsinga lýsir áherslum stofnunarinnar á verndun og meðferð gagna/upplýsinga í vörslu og eigu HSS. Verja þarf þær upplýsingar sem HSS varðveitir fyrir öllum ógnum, innri og ytri, sem stafa af ásetningi, gáleysi eða slysni. Innleiðing og framkvæmd stefnunnar er grundvöllur fyrir faglegum vinnubrögðum og er mikilvæg til að fullvissa starfsmenn HSS og notendur þjónustu stofnunarinnar, um heilindi og rétt vinnubrögð.

## 1. Umfang

Stefna um öryggi upplýsinga tekur til allra gagna/upplýsingar, í hvaða formi sem er og hvar sem þau/þær eru vistuð. Sérstök áhersla er lögð á viðkvæmar upplýsingar samkvæmt persónuverndarlögum nr. 90.2018

a) Heilsufarsupplýsingar og upplýsingar um lífsýni.
b) Upplýsingar sem eru eign stofnunarinnar og bundnar eignarrétti eða háðar hugverkarétti.
c) Persónugreinanlegar upplýsingar sem tengjast skjólstæðinga.
d) Persónulegar upplýsingar er tengjast starfsmönnum.

Stefna um öryggi upplýsinga tekur jafnfram til þess húsnæðis, búnaðar og kerfa sem hýsa eða flytja gögn/upplýsingar, þ.e. tölvuvélasalir, netþjónar, upplýsingatæknikerfi, gagnagrunnar, netbúnaður og fjarskipti. Stefna um öryggi upplýsinga nær jafnframt til starfsmanna HSS og samningsbundinna samstarfsaðila sem hafa aðgang að umræddum gögnum/upplýsingum, s.s. verktaka eða þjónustuaðila samkvæmt vinnslusamningum.

## 2. Markmið

Markmið með stefnu um öryggi upplýsinga eru að:

a) Upplýsingar séu réttar og aðgengilegar þeim sem aðgangsheimildir hafa þegar þörf er á.
b) Trúnaði sé viðhaldið þegar við á.
c) Trúnaðarupplýsingar séu óaðgengilegar óviðkomandi og séu tryggilega varðar gegn skemmdum, eyðingu eða uppljóstrun til þeirra sem hafa ekki aðgangsrétt, hvort sem það er af ásetningi eða kæruleysi (vangá).
d) Upplýsingar sem fara um net komist til rétts viðtakanda óskaddaðar, á réttum tíma og þess sé gætt að þær fari ekki til óviðkomandi.
e) Áhætta vegna vinnslu, varðveislu og miðlunar á upplýsingum sé innan skilgreindra áhættumarka og í samræmi við áhættumat.

## 3. Leiðir að markmiðum

Leiðir að ofangreindum markmiðum eru:

a) Ávallt sé farið eftir þeim lögum, reglum og reglugerðum sem gerðar eru til starfseminnar um varðveislu, meðferð, verndun og skráningu heilbrigðisupplýsinga.
b) Áætlanir séu gerðar um samfelldan rekstur, þeim sé viðhaldið og þær prófaðar.
c) Frávik, brot eða grunur um veikleika í upplýsingaöryggi séu tilkynnt, rannsökuð og þeim fylgt eftir.
d) Halda skrá yfir upplýsingaeignir og flokka þær eftir mikilvægi leyndar, réttleika og tiltækileika.
e) Reglulega og með formlegum hætti, sé framkvæmt áhættumat sem nær til upplýsingaeigna og veikleikum sem geta stefnt þeim í hættu.
f) Örugglega séu til rétt og nýuppfærð, tryggilega varðveitt afrit af gögnum og hugbúnaðarkerfum.
g) Fylgja og uppfylla alla samninga sem stofnunin er aðili að og varða upplýsingaöryggi.
h) Viðhalda gæða- og öryggishandbók með verklagsreglum og verkferlum vegna meðferðar upplýsinga og sjá til þess að starfsmenn og samstarfsaðilar fylgi þeim.
i) Allir starfmenn fái þjálfun og fræðslu um öryggiskerfi stofnunarinnar sem og öryggi upplýsinga og ábyrgð þeirra vegna þessara og tengdra þátta.

j) Aðgengi að heilsufarsupplýsingum og upplýsingum um lífssýni séu í samræmi við lög, reglugerðir og tilmæli, sem Landlæknir og stofnunin hafa sett fram.
k) 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. Sjá Persónuverndarstefnu HSS.
l) Ávallt sé farið eftir lögum og reglum Persónuverndar og Vísindasiðanefndar, þegar sótt er um að fá aðganga að heilsufarsupplýsingum úr kerfum sjúkrahússins, til að mynda til vísindarannsókna.
m) Framkvæmdar verða úttektir á stefnu og verklagsreglum upplýsingaöryggis. Þær taka ekki einungis til ákveðinna atvika heldur til allra þátta í öryggismálum. Úttektir skulu skilgreindar og samþykktar af Upplýsingaöryggisnefnd.

## 4. Ábyrgð

a) Forstjóri ber ábyrgð á upplýsingaöryggisstefnunni og að hún sé endurskoðuð og rýnd reglulega af óháðum aðila með formlegum hætti. Endurmeta skal þá hættu sem steðjað getur að þeim upplýsingakerfum sem eru í notkun og innihalda persónuupplýsingar, sem og öðrum kerfum og gagnasöfnum sem tengjast þeim. Í kjölfar slíks endurmats og endurskoðunar er öryggisstefnan uppfærð og samþykkt formlega, auk þess sem stefnan og hugsanlegar breytingar á henni eru kynntar starfsfólki og samstarfsaðilum.
b) Framkvæmdastjóri lækninga ber ábyrgð á öryggi sjúkraskrár.
c) Forstöðumaður tölvu- og upplýsingatæknideildar, ber ábyrgð á framkvæmd upplýsingaöryggisstefnunnar og beitir til þess viðeigandi stöðlum og vinnuferlum.
d) Allir starfsmenn tölvu- og upplýsingatæknideildar bera ábyrgð á að þeim vinnuferlum sé fylgt, sem eiga að tryggja framkvæmd upplýsingaöryggisstefnunnar. Samstarfsaðilar, verktakar og birgjar bera ábyrgð á að samningsbundnum vinnuferlum sem eiga að tryggja að framkvæmd stefnunnar sé fylgt.
e) Forstöðumenn/Deildarstjórar bera ábyrgð á því að starfsmenn þeirra fari eftir þeim reglum og tilmælum sem gilda um öryggi upplýsinga, meðferð heilsufarsupplýsinga og meðferð upplýsinga um lífssýni. Þeir bera einnig ábyrgð á að viðhalda öryggisvitund meðal starfsmanna.
f) Öllum starfsmönnum ber að vinna samkvæmt upplýsingaöryggisstefnunni. Þeim ber að tilkynna öryggisfrávik og veikleika sem varða upplýsingaöryggi til starfsmanna tölvu- og upplýsingatæknideildar.

## 5. Viðurlög

Þeir sem ógna upplýsingaöryggginu af ásettu ráði eiga yfir höfði sér málshöfðun eða aðrar viðeigandi lagalegar aðgerðir. Brot getur, samkvæmt lögum um réttindi og skyldur starfsmanna ríkisins, varðað áminningu eða, ef um endurtekin eða alvarleg brot er að ræða, brottvikningu úr starfi.

Samþykkt á fundi framkvæmdastjórnar 9. desember 2020