

## Upplýsingaöryggisstefna Embættis landlæknis

### 1. Starfsemi embættisins

Embættið starfar í samræmi við lög um landlækni og lýðheilsu nr. 41/2007, aðsetur þess er að Barónsstíg 47 í Reykjavík.

### 2. Tilgangur með upplýsingaöryggisstefnunni

Þessi upplýsingaöryggisstefna lýsir áherslum Embættis landlæknis á upplýsingavernd og örugga meðferð upplýsingaeigna embættisins. Verja þarf upplýsingaeignir fyrir öllum ógnum, innri og ytri, af ásetningi, vegna óhappa eða af slysi. Fagleg vinnubrögð eru lykillinn að árangri og til marks um það er þessi upplýsingaöryggisstefna sett. Innleiðing og framkvæmd stefnunnar er mikilvæg til þess að fullvissa starfsmenn embættisins, notendur þjónustu embættisins og landsmenn alla um heilindi og rétt vinnubrögð í rekstri stofnunarinnar.

### 3. Umfang

Upplýsingaöryggisstefna tekur til umgengni og vistunar allra upplýsinga í vörslu Embættis landlæknis á rafrænu formi, prentuðu, handskrifuðu eða í mæltu máli. Hér er átt við:

- Upplýsingar frá notendum heilbrigðisþjónustunnar sem sendar eru embættinu vegna eftirlits og vöktunar, vinnslu heilbrigðistöfræði, kvartana o.fl.
- Upplýsingar sem eru eign embættisins og bundnar eignarétti eða háðar hugverkarétti.
- Persónulegar upplýsingar sem tengjast starfsmönnum Embættis landlæknis.

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

### 4. Markmið

Markmið Embættis landlæknis með upplýsingaöryggisstefnunni er að:

- Leynd upplýsinga og trúnaði sé viðhaldið í samræmi við lög og reglur þar að lútandi.
- Upplýsingar séu réttar og aðgengilegar þeim sem aðgangsrétt hafa þegar þörf er á.
- Upplýsingar séu varðar gegn skemmdum, eyðingu eða uppljóstrun til aðila sem hafa ekki aðgangsrétt, hvort sem er af ásetningi eða vangá.
- Upplýsingar sem fara um net komist til réttis viðtakanda óskaddaðar, á réttum tíma og þess sé gætt að þær fari ekki til annarra.
- Að áhætta vegna vinnslu (meðferðar) og varðveislu upplýsinga sé innan skilgreindra áhættumarka.

### 5. Leiðir að markmiðum

Leiðir Embættis landlæknis að ofangreindum markmiðum eru að:

- Halda skrá yfir upplýsingaeignir og flokka þær eftir mikilvægi leyndar, hversu réttar þær eru og tiltækilegar.
- Greina reglulega með formlegu áhættumati verðmæti upplýsingaeigna, viðkvæmni þeirra og ógnir sem geta stefnt þeim í hættu.

- c) Stjórna áhættu innan skilgreindra marka með því að starfrækja formlegt stjórnkerfi upplýsingaöryggis samkvæmt ÍST ISO/IEC 27001:2013.
- d) Viðhalda gæða- og öryggishandbók embættisins sem inniheldur verklagsreglur, vinnulýsingar og önnur gæðaskjöl vegna meðferðar upplýsinga.
- e) Allir starfsmenn embættisins fái þjálfun og fræðslu varðandi upplýsingaöryggi og ábyrgð þeirra hvað varðar upplýsingaöryggi.
- f) Alltaf séu til áreiðanleg og örugglega varðveitt afrit af gögnum og hugbúnaðarkerfum.

## 6. Ábyrgð

Ábyrgð við framkvæmd og viðhald upplýsingaöryggisstefnu Embættis landlæknis skiptist á eftirfarandi hátt:

- a) Landlæknir og sviðsstjórar bera ábyrgð á upplýsingaöryggisstefnunni. Sviðsstjórar tryggja nauðsynlegt starfsfólk og aðföng til þess að innleiða og reka upplýsingaöryggiskerfið hver á sínu sviði. Landlæknir er ábyrgur fyrir rýni upplýsingaöryggisstefnunnar.
- b) Gæða- og öryggisstjóri embættisins ber ábyrgð á framkvæmd upplýsingaöryggisstefnunnar og beitir til þess viðeigandi stöðlum og vinnuferlum.
- c) Allir starfsmenn embættisins bera ábyrgð á að framfylgja þeim vinnuferlum sem eiga að tryggja framkvæmd upplýsingaöryggisstefnunnar. Samstarfsaðilar, verktakar og birgjar bera ábyrgð á að fylgt sé samningsbundnum vinnuferlum sem eiga að tryggja framkvæmd stefnunnar.
- d) Öllum starfsmönnum embættisins ber að vinna samkvæmt upplýsingaöryggisstefnunni. Þeim ber að tilkynna öryggisfrávik og veikleika sem varða upplýsingaöryggi. Þeir sem ógna upplýsingaöryggi embættisins af ásettu ráði eiga yfir höfði sér málshöfðun eða aðrar viðeigandi lagalegar aðgerðir.

## 7. Vottun

Landlæknir stefnir að vottun upplýsingaöryggiskerfisins.

## 8. Endurskoðun

Þessi stefna skal endurskoðuð á þriggja ára fresti og oftar ef þörf krefur. Það er gert til þess að tryggja að hún samrýmist markmiðum með rekstri embættisins.

## 9. Samþykki

Með samþykkt þessarar upplýsingaöryggisstefnu fellur úr gildi eldri upplýsingaöryggisstefna sem samþykkt var af framkvæmdastjórn Embættis landlæknis í desember árið 2014.

**Reykjavík, 28. nóvember 2017**

Birgir Jakobsson, landlæknir

### Lög og reglugerðir:

Sjá heimasíðu Embættisins.

<https://www.landlaeknir.is/um-embattid/log-og-reglugerdir/>