



Upplýsingaöryggisstefna

Upplýsingaöryggisstefna LSR er lykilskjal innan áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni (UFT) og er hluti af stjórnkerfi upplýsingaöryggis LSR. Stefnan skilgreinir meginreglur, markmið og ábyrgð við vernd upplýsinga, upplýsingakerfa og annarra UFT - eigna sjóðsins.

Stefnan tekur mið af gildandi lögum og reglum á sviði upplýsingaöryggis og stafræns viðnámspróttar, þar á meðal lögum um stafrænan viðnámsprótt fjármálamarkaðar (DORA), kröfum eftirlitsaðila og, eftir atvikum, leiðbeinandi tilmælum og leiðbeiningum sem gilda um starfsemi sjóðsins.

1. Markmið og áherslur

Markmið stefnunnar er að vernda upplýsingar, upplýsingakerfi og aðrar UFT-eignir LSR á skilvirkan og áhættumiðaðan hátt, tryggja samfelldan rekstur og lágmarka rekstraráhættu. Áhersla er á að varðveita leynd, réttleika, ósvikni og tiltækileika upplýsinga og UFT-eigna LSR þannig að þær nýtist sem best í starfsemi sjóðsins og að öryggi upplýsinga sé óaðskiljanlegur hluti starfseminnar.

Áherslur LSR í upplýsingaöryggi

Áherslur LSR í upplýsingaöryggi eru eftirfarandi og skulu leiða framkvæmd, eftirfylgni og stöðugar umbætur á sviði upplýsingaöryggis og UFT-áhættu:

- Tryggja skal leynd, réttleika, ósvikni og tiltækileika upplýsinga og UFT-eigna með viðeigandi tæknilegum, skipulagslegum og rekstrarlegum ráðstöfunum.
- UFT- og upplýsingaöryggisatvik, brot, veikleikar og verulegar netógnir skulu skráð, flokkuð, rannsökuð, tilkynnt og nýtt til umbóta í samræmi við lög, stjórnvaldsfyrirmæli og samþykkt verklag.

- Viðhalda skal uppfærðu yfirliti yfir upplýsingaeignir, lykilverfi og mikilvæga þjónustuaðila, sem tengjast nauðsynlegri og mikilvægri starfsemi í samræmi við rekstraráhrifagreiningu (BIA).
- Aðgangsstýring, auðkenning, dulritun, vöktun, veikleikastjórnun og prófanir skulu vera áhættumiðaðar.
- Kröfur til upplýsingaöryggis og stafræns viðnámspróttar gagnvart UFT-þjónustuveitendum og útvistuðum verkefnum skulu vera skilgreindar í samningum og þeim stýrt í samræmi við útvistunarstefnu og annað innra verklag.
- Samfelldur rekstur, neyðarviðbrögð og endurheimt lykilverfi skulu vera skipulögð, skjalfest, prófuð reglulega og uppfærð í ljósi niðurstaðna prófana og raunverulegra atvika.
- Niðurstöður prófana, atvika, úttekta og eftirlits skulu nýttar til stöðugra umbóta á stjórnkerfi upplýsingaöryggis.

2. Umfang

Stefnan tekur til allrar starfsemi LSR, þar með talið nauðsynlegrar og mikilvægrar starfsemi, starfsfólks, upplýsingaeigna, gagna, upplýsingakerfa, tæknilegra innviða, viðmóta, skýjaþjónustu, samskiptalausna, tækjabúnaðar, varaafrita og þjónustu þriðju aðila sem styðja við starfsemi sjóðsins, óháð því hvort rekstur er framkvæmdur innanhúss eða útvið.

Stefnan nær jafnframt til umgengni, vistunar, vinnslu, samskipta, dreifingar, geymslu og eyðingar upplýsinga í eigu LSR, auk húsnæðis og búnaðar þar sem upplýsingar eru meðhöndlaðar eða varðveittar.

3. Tengsl við önnur stjórnskjöl

Stefnan skal túlkuð og framkvæmd í samræmi við áhættustefnu, stefnu um stafrænan viðnámsprótt (e. Operational Resilience Strategy - DORS), tæknistefnu, stefnu um samfelldan rekstur, neyðaráætlun, endurreisnaráætlun, útvistunarstefnu, rekstraráhrifagreiningu (BIA) og reglubók upplýsingaöryggis.

Nánari kröfur, ferlar og verklagsreglur eru skilgreindar í reglubók upplýsingaöryggis og tengdum verklagsreglum.

4. Ábyrgð

Ábyrgð á setningu, innleiðingu, framkvæmd og viðhaldi stefnunnar skiptist þannig:

- **Stjórn** samþykkir stefnuna, hefur ábyrgð með innleiðingu hennar og fær reglulega skýrslugjöf um stöðu upplýsingaöryggis, meiriháttar atvik, niðurstöður prófana og stöðu umbóta.
- **Framkvæmdastjóri** ber ábyrgð á að stefnan sé innleidd í starfsemi sjóðsins og að tiltækt sé nægilegt fjármagn, mannauður og skipulag til að framfylgja henni.
- **Öryggisráð** fer með yfirumsjón stjórnkerfis upplýsingaöryggis, forgangsraðar umbótaverkefnum, fylgir eftir niðurstöðum prófana og atvika og leggur að lágmarki árlega fyrir stjórn samantekt um stöðu upplýsingaöryggis og umbótavinnu.
- **Öryggisstjóri** hefur umsjón með framkvæmd stefnunnar, viðheldur stefnunni, regluverki og verklagi og fylgir eftir atvikum, prófunum og umbótum. Hann tryggir jafnframt að unnið sé samkvæmt viðeigandi stöðlum og bestu aðferðum.
- **Stjórnendur og forsjáraðilar upplýsingaeigna** bera ábyrgð á að viðeigandi öryggiskröfur séu skilgreindar og framfylgt í rekstri, verkefnum, ferlum og samningum við þjónustuaðila.
- **Sviðsstjóri stafrænnar þróunar og rekstrar** ber ábyrgð á innleiðingu og rekstri tæknilegra og rekstrarlegra stýringa, vöktun, viðbrögðum, breytingastjórnun og rekstraröryggi í samræmi við tæknistefnu, reglubók og samþykktan áhættuvilja.
- **Starfsfólk** vinnur í samræmi við stefnuna, fylgir samþykktu verklagi og tilkynnir tafarlaust um öryggisatvik, veikleika eða frávik sem geta haft áhrif á öryggi upplýsinga eða UFT.

5. Endurskoðun

Stefnan skal endurskoðuð að lágmarki árlega og oftár ef tilefni er til, m.a. í kjölfar reglubundins áhættumats, verulegra breytinga á starfsemi, tæknihverfi, útvistun eða regluverki, niðurstaðna prófana, meiriháttar atvika eða athugasemda eftirlits- eða endurskoðunaraðila.

Samþykkt af stjórn LSR 15. apríl 2026