Upplýsingaöryggisstefna NTÍ

Tilgangur

Stefna NTÍ í upplýsingaöryggi lýsir áherslum stjórnar á upplýsingavernd og örugga meðferð gagna og upplýsinga í vörslu og eigu NTÍ. Verja þarf upplýsingar í vörslu NTÍ fyrir innri og ytri ógnum, hvort sem þær stafa af ásetningi eða gáleysi. Stjórn NTÍ ber ábyrgð á að rekstur upplýsingakerfa uppfylli þau viðmið sem til hans eru gerðar og að gerðar séu viðeigandi ráðstafanir til þess að öll upplýsingakerfi sem hafa þýðingu fyrir eða áhrif á starfsemi NTÍ séu starfrækt í samræmi við kröfur[1]. Þetta á við, hvort sem rekstri upplýsingakerfa er útvistað að hluta til eða í heild sinni[2].

Umfang

Upplýsingaöryggisstefnan nær til umgengni og vistunar gagna hjá NTÍ og allra samstarfs og þjónustuaðila sem höndla með gögn fyrir hönd NTÍ. Stefnan tekur einnig til húsnæðis, búnaðar og kerfa, sem hýsa eða flytja gögn og upplýsingar.

Í stefnunni felst að:

- Framkvæma skal áhættumat á upplýsingakerfum þar sem áhersla skal lögð á að lágmarka rekstraráhættu og tryggja að ávallt sé farið eftir þeim lögum og reglum sem gerðar eru til starfseminnar um varðveislu, meðferð, verndun og skráningu gagna.
- Í ljósi smæðar í yfirbyggingu hjá NTÍ og í þeim tilgangi að lágmarka rekstraráhættu sem kann að skapast af ófullnægjandi upplýsingakerfum er heimilt að útvista rekstri, viðhaldi, hýsingu og afritun allra upplýsingakerfa auk hönnunar og þróunar, til þjónustuaðila með hýsingu innan ESB. Tryggja skal að útvistunaraðili hafi gott orðspor og þekkingu á því sviði. Þjónustuaðili í upplýsingatækni sem samið er við um heildarrekstur upplýsingatæknikerfa skal að lágmarki uppfylla ISO27001 upplýsingastjórnunarstaðalinn.
- Halda skrá yfir upplýsingaeignir og flokka þær eftir mikilvægi leyndar, réttleika og tiltækileika.
- Lágmörkun áhættu við rekstur upplýsingakerfa er m.a. fólgin í gerð viðbragðsáætlunar, fastmóta verklag og reglur, gera ráðstafanir sem miða að því að stýra rekstraráhættu, koma í veg fyrir hagsmunaárekstra og tryggja gagnsæi hjá stofnuninni. Verklag og skrifleg fyrirmæli skulu vera fylgiskjöl þeirra samninga sem við á.
- Tryggja ber öryggi upplýsinga með tilliti til leyndar, réttleika og tiltækileika. Í því felst að aðeins þeir sem hafa til þess heimild, hafi viðeigandi aðgang þegar þeir þurfa hann og að upplýsingarnar séu réttar og óspilltar[3].
- Upplýsingaverðmæti skulu varin gegn óheimilum aðgangi, til að koma í veg fyrir óviðeigandi notkun, breytingu, uppljóstrun eða eyðileggingu á mikilvægum og viðkvæmum upplýsingum hvort sem er af ásetningi eða gáleysi.
- Tryggja skal að öryggi persónugreinanlegra upplýsinga sé tryggt og að söfnun og vinnsla persónuupplýsinga sé í lágmarki. Persónuvernd skal innbyggð og sjálfgefin í kerfum NTÍ.
- Fullnægjandi aðföng skulu ávallt vera til staðar, s.s. tæknibúnaður og mannauður, þ.m.t. nauðsynleg þekking og færni[4].
- NTÍ stuðlar að og viðheldur virkri öryggisvitund starfsmanna, stjórnar og þjónustuaðila með fræðslu og þjálfun svo öllum sé ljós ábyrgð sín.

[1] Sbr. liður 4 í leiðbeinandi tilmælum FME nr. 1/2019
[2] Sbr. liður 5 í leiðbeinandi tilmælum FME nr. 1/2019
[3] Sbr. inngang í leiðbeinandi tilmælum FME vegna áhættu við rekstur upplýsingakerfa eftirlitsskyldra aðila.
[4] Sbr. lið 7 í leiðbeinandi tilmælum FME nr. 1/2019

- Vinna skal stöðugt að umbótum og framkvæma reglulega áhættumat og úttektir á stefnu og verklagsreglum upplýsingaöryggis til þess að leiða í ljós hvort þörf sé á úrbótum á upplýsingaöryggi NTÍ. Frávik, brot eða grunur um veikleika í upplýsingaöryggi séu tilkynnt, rannsökuð og þeim fylgt eftir.

Ábyrgð

Stjórn NTÍ ber ábyrgð á að staðfesta upplýsingaöryggisstefnuna sem og þær viðmiðunarreglur sem hún inniheldur. Það er einnig á ábyrgð stjórnar NTÍ að til staðar sé viðbragðsáætlun fyrir rekstur upplýsingakerfa[5]. Forstjóri ber ábyrgð á að framfylgja stefnu í stjórnun upplýsingaöryggis og allir starfsmenn og þjónustuaðilar NTÍ bera ábyrgð á að fylgja stefnunni.

[5] Sbr. liður 6 í leiðbeinandi tilmælum FME nr. 1/2019