Upplýsingaöryggisstefna

TILGANGUR

Verja þarf upplýsingaeignir Ósa hf. og dótturfélaganna Icepharma, LYFIS og Parlogis (hér eftir vísað til sem "samstæðan") fyrir öllum ógnum, innri og ytri, af ásetningi eða af slysni.

Upplýsingaöryggisstefnan styður samfelldan rekstur og er ætlað að tryggja hlítingu við lög og reglur sem varða starfsemina og varða öryggi í rekstri upplýsingakerfa, vernd og vinnslu upplýsinga.

GILDISSVIÐ

Stefna gildir fyrir samstæðuna og nær til vinnslu og meðhöndlunar allra upplýsingaverðmæta samstæðunnar í hvaða formi sem þær eru og hvar sem þær eru geymdar. Stefnan tekur einnig til allra upplýsingaverðmæta þriðja aðila sem samstæðan hefur í vörslu sinni eða samstæðan hefur falið öðrum að sjá um í sínu nafni.

Stefna þessi tekur til allra þeirra sem á einhvern hátt meðhöndla eða hafa aðgang að upplýsingaeignum sem stjórnkerfi upplýsingaöryggis tekur til. Stefnan tekur þannig til allra starfsstöðva samstæðunnar og til þeirra sem þar starfa, sem og upplýsingatæknibúnaðar og gagna í eigu þeirra. Stefnan nær einnig til þriðju aðila (s.s. verktaka) og lögaðila sem starfa fyrir samstæðuna sem eru einnig skuldbundnir til að vernda upplýsingar gegn óheimilum aðgangi, notkun, breytingum, uppljóstrun, eyðileggingu, glötun eða flutningi.

ÁBYRGÐ

Ábyrgð við framkvæmd og viðhald upplýsingaöryggisstefnu skiptist á eftirfarandi hátt:

- **Forstjóri:** Forstjóri ber ábyrgð á upplýsingaöryggisstefnunni og sér til þess að henni sé framfylgt með því að skilgreina markmið og tryggja viðeigandi ráðstafanir. Forstjóri felur upplýsingatæknideild Ósa, stjórnendum og tilteknum starfsmönnum eftirfylgni með tilteknum ákvörðunum og verklagsreglum.
- **Stjórnendur:** Stjórnendur bera ábyrgð á þeim upplýsingaverðmætum sem verða til og/eða tilheyra viðkomandi rekstrareiningu og að starfsfólk fari eftir upplýsingaöryggisstefnunni er þeir framkvæma störf sín og þeim reglum og tilmælum sem gilda um öryggi upplýsingaeigna.
- **Starfsfólk:** Starfsfólki ber að vinna samkvæmt stefnunni og þeim verklagsreglum sem eiga að tryggja framkvæmd hennar. Starfsfólki ber að tilkynna öryggisfrávik og veikleika sem varða upplýsingaöryggi.

FRAMKVÆMD

Skilgreiningar

- **Upplýsingaverðmæti:** allar upplýsingar sem verða til innan samstæðunnar eða í umsjón samstæðunnar
- **Stjórnunarkerfi:** öll kerfi sem notuð eru til að tryggja öryggi upplýsingaverðmæta.
- **Þriðji aðili:** starfsmenn upplýsingatæknifyrirtækja og samstarfsaðila sem hafa, starfsins vegna, aðgang að stjórnkerfum og upplýsingaverðmætum samstæðunnar.
- **Upplýsingaeign:** vélbúnaður, hugbúnaður, tengibúnaður og skjöl á pappír í eigu eða umsjá samstæðunnar.
- **Öryggisfrávik:** öll atvik sem geta haft áhrif öryggi upplýsingaverðmæta.
- **Áhættumark:** kemur fram í áhættustefnu Ósa hvert áhættumörk upplýsingaöryggis er.

Markmið

- Að tryggja hlítingu við kröfur sem varða stjórnun upplýsingaverðmæta, upplýsingaöryggi og vinnslu persónuupplýsinga.
- Að tryggja sem best öryggi upplýsinga með tilliti til leyndar, réttleika og tiltækileika upplýsingaverðmæta.
- Að tryggja skilvirkni og skuldbindingu um stöðugar umbætur á stjórnunarkerfi um upplýsingaöryggi.
- Að stjórna áhættu vegna vinnslu, varðveislu og miðlunar á upplýsingum þannig að hún sé innan skilgreindra áhættumarka og í samræmi við áhættumat.
- Að stuðla að, auka og viðhalda virkri vitund um upplýsingaöryggi meðal starfsmanna með reglulegri fræðslu, þjálfun og vitundavakningu

Viðurlög

Við brot á verklagsreglum sem styðja við stefnu þessa fylgjum við *agastefnu* samstæðunnar ef við á.