

Áhættustefna Ósa og dótturfélaga

Tilgangur

Tilgangur stefnunnar er að viðhalda yfirsýn og viðeigandi stýringu áhættu í starfsemi Ósa og dótturfélaga, hér eftir kallað „Ósar“ eða „fyrirtækin“, til hagsbóta fyrir samfélagið, viðskiptavini, starfsfólk og hluthafa. Tilgangur með áhættustefnu Ósa er einnig að styrkja áhættustjórnun og innra eftirlit með heildstæðum hætti í rekstri og starfseminni, ná fram betri nýtingu fjármuna ásamt fylgni við lög og reglur í samræmi við stefnumörkun stjórnar.

Ábyrgð og gildissvið

Stefnan gildir fyrir alla starfsemi Ósa og dótturfélaga. Umfang stefnunnar nær þannig til alls starfsfólks, starfsstöðva, þjónustu, eigna, upplýsinga og búnaðar sem fyrirtækin hafa umsjón með eða fela öðrum að sjá um í sínu nafni og allra aðila sem veita þeim þjónustu.

Stefnan er samþykkt af stjórn Ósa og er á ábyrgð hennar. Skal áhættutaka vera í samræmi við áhættustefnu þessa. Með samþykkt stefnunnar staðfestir stjórn umgjörð um framkvæmd áhættustjórnunar.

Fyrir hönd stjórnar samþykkir forstjóri Ósa stefnuna. Hjá Ósum er rekstraröryggisráð sem sér til þess að stefnunni sé framfylgt, vera starfrækt stjórnskipulag áhættustýringar og samræma áhættustýringarferli sem hentar umfangi fyrirtækjanna.

Stefna og markmið

Fyrirtækin greina og meðhöndla áhættu í starfsemi sinni með reglubundnu áhættumati, markvissu eftirliti og aðgerðum. Fyrirtækin skilgreina áhættuviðmið fyrir þá áhættu sem þau eru tilbúin að bera og telst áhætta umfram þau viðmið vera óásættanleg.

Meginmarkmiðið er að:

- áhætta umfram áhættuviðmið sé meðhöndluð,
- aðgerðir vegna mildunnar áhættu hljóti viðeigandi forgang,
- stjórnarmenn, stjórnendur, starfsfólk, verktakar, þjónustuaðilar og aðrir aðilar sem starfa fyrir fyrirtækin þekki eigið hlutverk, boðleiðir og mikilvægi áhættustýringar.

Sértækar stefnur sem fyrirtækin setja sér skulu vera í samræmi við áhættustefnuna, til dæmis persónuverndarstefnur eða stefnur um upplýsingaöryggi.

Áhættumat á verkefnum eru framkvæmdar áður en ákvörðun er tekin um stærri verkefni, stefnubreytingu eða breytingu á starfsemi eða skipulagi. Fyrirtækin skilgreina viðeigandi viðmið og hlutverk vegna ákvörðunar um áhættumat verkefnis.

Tilvísanir

Nánari lýsing á skipulagi áhættustýringar og áhættustýringarferli Ósa er að finna í útgáfustýrðum skjölum í handbók Ósa, sjá nánar Skipulag áhættustýringar, Framkvæmd áhættumats hjá Ósum, Áhættulandslag Ósa og Skor og flokkar áhættumats. Áhættustefnan skal fylgja lögum og reglum sem gilda um starfsemina, þ.m.t. lögum um persónuvernd og þeirra laga og reglugerða sem eiga við um starfsemi fyrirtækjanna, og kröfum gæðakerfa.

Endurskoðun

Endurskoða skal stefnu um áhættustýringu á þriggja ára fresti af rekstraröryggisráði Ósa sem leggur hana fyrir forstjóra til samþykktar.

Lágmarksviðmið um öryggiskröfur sem gerðar eru til samstarfsaðila

Lögð er áhersla á að:

1. Samstarfsaðili fylgi lögum og reglum sem gilda um starfsemi þeirra og tengjast þjónustu þeirra.
2. Hafi þekkingu á lögum nr. 78/2019 og reglugerð nr. 866/(2020) þegar það á við og þegar þjónusta samstarfsaðila varðar úthýstan rekstur á upplýsingakerfum Ósa og dótturfélaga.
3. Samstarfsaðili viðhafi ferilkönnun á starfsmönnum áður en þeir hefja störf og láti starfsmenn undirrita trúnaðaryfirlýsingu sem gildi einnig eftir að starfsmaður lætur af störfum og eftir að þjónustu samstarfsaðila lýkur af hvaða ástæðu sem er.
4. Samstarfsaðili hafi stefnu um reglulega öryggisþjálfun starfsmanna og tryggi framfylgd hennar.
5. Samstarfsaðili hafi skjalfesta stefnu og ferla til að meta, stýra og lágmarka áhættu af öryggisbrest.
6. Samstarfsaðili hafi sett sér öryggisstefnu, framkvæmi áhættumat reglubundið og ákvarði og endurmeti skilgreindar öryggisráðstafanir á grundvelli þess.
7. Samstarfsaðili viðhafi aðgangsstýringu þannig að hún sé takmörkuð við aðeins þá sem þurfa starfa sinna vegna á honum að halda.
8. Samstarfsaðili hafi skjalfesta viðbragðsáætlun og áætlun um samfelldan og órofinn rekstur og þjónustu til að tryggja takmörkun á tjóni ef alvarleg röskun verður á starfseminni og þar með þjónustunni.
9. Samstarfsaðili hafi verkferla og viðbragð við atvikum sem tryggir skráningu þeirra, meðhöndlun sem felur m.a. í sér að finna orsakir og koma í veg fyrir að atvik endurtaki sig.
10. Samstarfsaðili hafi þekkingu á tilkynningaskyldu sinni ef upp koma alvarleg atvik eða áhættur.
11. Samstarfsaðili tryggi að eftirlitsstofnanir geti sinnt eftirlitsskyldu sinni hjá samstarfsaðila.
12. Samstarfsaðili veiti Ósa og dótturfélögum heimild til að framkvæma mat og/eða úttekt á samstarfsaðila sé þess þörf.
13. Samstarfsaðili undirriti vinnslusamning ef þjónustan felur á einhvern hátt í sér aðgang eða vinnslu persónuupplýsinga.
14. Samstarfsaðili tryggi keðjuábyrgð gagnvart undirverktökum og undirvinnsluaðilum þannig að þeir aðilar og starfsmenn séu einnig bundnir af trúnaðarskyldu og viðhafi viðeigandi tæknilegar og skipulagslegar ráðstafanir til að tryggja öryggi upplýsinga.