FJÁRMÁLAEFTIRLITIÐ

Leiðbeinandi tilmæli nr. 1/2005

um rekstur upplýsingakerfa eftirlitsskyldra aðila

Ekki í gildi

1. júní 2005

I. Inngangur

Fjármálaeftirlitið hefur eftirlit með starfsháttum eftirlitsskyldra aðila, skv. lögum um opinbert eftirlit með fjármálastarfsemi nr. 87/1998 og að þeir starfi í samræmi við þau lög og reglur sem um starfsemi þeirra gilda. Það hefur samkvæmt 2. mgr. 8. gr. sömu laga heimild til að gefa út og birta opinberlega almenn leiðbeinandi tilmæli um starfsemi eftirlitsskyldra aðila.

Í eftirliti Fjármálaeftirlitsins hefur komið í ljós að víða hjá eftirlitsskyldum aðilum skortir innri starfsreglur um rekstur upplýsingakerfa. Eftirfarandi tilmæli eru að miklu leyti unnin af því tilefni.

Með leiðbeinandi tilmælum þessum er stefnt að því að samræmdar kröfur verði gerðar til allra eftirlitsskyldra aðila varðandi rekstur upplýsingakerfa og notkun upplýsingatækni.

Megintilgangur tilmælanna er að tryggja áfallalausan rekstur eftirlitsskylds aðila og lágmarka rekstraráhættu hans og að eftirlitsskyldir aðilar uppfylli reglur og lagaskyldur sem þeim ber. Einn þáttur í því er að tryggja leynd upplýsinga, til að uppfylla ákvæði um þagnarskyldu. Taka ber fram að tilmælin eru ekki sett fram á grundvelli laga um persónuvernd og meðferð persónuupplýsinga og reglna samkvæmt þeim, enda er þeim lögum fylgt eftir af Persónuvernd. Málefni er varða rekstur upplýsingakerfa hljóta þó að einhverju leyti að skarast, en það er á ábyrgð þessara eftirlitsaðila að takmarka slíka skörun.

Áfallalaus rekstur upplýsingakerfa er m.a. fólginn í því að gera ráðstafanir sem miða að því að stýra rekstraráhættu, koma í veg fyrir hagsmunaárekstra og tryggja gegnsæi á markaði. Einnig að tryggja öryggi upplýsinga þ.e. að tryggja aðgengi þeirra sem hafa til þess heimild , þegar þeir þurfa slíkt aðgengi og að upplýsingarnar séu réttar og óspilltar.

Umfang aðgerða til að tryggja öryggi upplýsingakerfa á að vera í samræmi við umfang rekstur eftirlitsskylds aðila og þá áhættu sem honum fylgir. Tilmælin gilda um alla eftirlitsskylda aðila. Eðli máls samkvæmt hefur Fjármálaeftirlitið ástæðu til að gera ríkari kröfur til eftirlitsskyldra aðila með umsvifamikla og fjölþætta starfsemi en minni aðila með einfalda starfsemi. Því er gert ráð fyrir að smærri aðilum dugi einfalt utanumhald, þó þeim beri að hafa þau sjónarmið að leiðarljósi sem fram koma í tilmælunum.

Þegar eftirlitsskyldur aðili er hluti af samstæðu þá eiga tilmælin við um rekstur þeirra upplýsingakerfa hjá félögum sem eru í samstæðunni með eftirlitsskylda aðilanum, ef þau hafa áhrif á eða skipta máli fyrir rekstur eftirlitsskylda aðilans.

Alþjóðlegir staðlar gilda á þessu sviði og einnig er töluvert til af leiðbeiningum um rekstur upplýsingakerfa. Má þar nefna ÍST ISO/IEC 17799 og ÍST BS 7799-2 um upplýsingaöryggi, ISO 9000 gæðastaðalinn og CobiT.
Ef fyrirtæki uppfylla kröfur staðals telst það uppfylla tilmælin á þeim sviðum sem vottun samkvæmt staðlinum tekur til. Fjármálaeftirlitið mun ákvarða hvort eftirlitsskyldir aðilar uppfylla ákvæði tilmæla þessara.

Á hinum Norðurlöndunum hafa verið sett fram sambærileg tilmæli eða reglur t.d. í Noregi (http://www.kredittilsynet.no/wbch3.exe?ce=12984) og Danmörku og er tekið mið af þeim í þessum drögum.

II. Efni leiðbeinandi tilmæla um rekstur upplýsingakerfa eftirlitsskyldra aðila

1. gr. Gildissvið

Tilmælin taka til allra eftirlitskyldra aðila, þ.e. þeirra aðila sem taldir eru upp í 2 gr. laga nr. 87/1998.
Tilmælin taka til allra upplýsingakerfa sem hafa þýðingu fyrir eða áhrif á starfsemi fyrirtækisins. Með upplýsingakerfi er átt við þau kerfi, vélræn og óvélræn, sem koma að vinnslu upplýsinga ásamt öllum tengingum að þeim og á milli þeirra.
Tilmælin geta einnig tekið til dótturfélaga eftirlitsskylds aðila þar sem upplýsingakerfi þeirra hafa eða geta haft áhrif á starfsemi móðurfélagsins, þ.e. hins eftirlitsskylda aðila.
Ef veittur er utanaðkomandi aðgangur að upplýsingakerfum skal vera tryggt með skriflegum samningum að kröfur tilmælanna til öryggis og skjalfestingar séu uppfylltar.

2. gr. Skipulag

Eftirlitsskyldur aðili skal setja sér stefnu, ákveða markmið og öryggiskröfur til reksturs upplýsingakerfa. Fyrirliggjandi skulu vera skriflegar lýsingar á nauðsynlegum verkferlum fyrir rekstur og öryggi upplýsingakerfa. Einnig hvernig ábyrgð á stjórnun, öflun búnaðar, þróun, rekstri, kerfisviðhaldi, öryggi upplýsinga og innleiðingu og niðurlagningu kerfa eða búnaðar, er tryggð.
Ef hluta upplýsingatækniverkefna eða þeim öllum er útvistað, skal eftirlitsskyldur aðili hafa eigin stefnumið sem tryggja afhendingu þjónustunnar, svo sem væri ef þjónustunni væri ekki útvistað.
Tilnefna skal ábyrgðaraðila fyrir ólíka þætti upplýsingatækniverkefna.

3. gr. Áhættugreining

Eftirlitsskyldur aðili skal ákveða viðmið fyrir ásættanlega áhættu tengda notkun upplýsingatækni m.t.t. starfssviðs viðkomandi aðila. Endurskoða skal viðmiðin með reglubundnum hætti. Eftirlitsskyldur aðili skal greina áhættu af rekstri upplýsingakerfa. Áhættugreiningarferlið skal m.a. skilgreina skýrt ábyrgð og taka til eftirfylgni á ráðstöfunum sem grípa á til í kjölfar undangenginnar áhættugreiningar.

Eftirlitsskyldur aðili skal a.m.k. einu sinni á ári og auk þess í tengslum við breytingar sem skipta máli fyrir upplýsingaöryggi, fara í gegnum áhættugreiningu til þess að tryggja að áhættan sé innan viðmiða sem sett hafa verið fram sbr. 1 mgr. þessarar greinar. Niðurstaða áhættugreiningarinnar skal vera skjalfest.

4. gr. Öryggi

Eftirlitsskyldur aðili skal koma á verkferlum sem tryggja vernd búnaðar, lagna, kerfa og upplýsinga sem eru mikilvæg rekstri aðilans, sbr. 1. gr., fyrir áföllum, misnotkun, óheimilum aðgangi, óheimilum breytingum og skemmdarverkum. Einnig skulu verkferlarnir taka til stjórnunar, úthlutunar, endurskoðunar og afturköllunar aðgangsheimilda að upplýsingakerfum. Kröfur til upplýsingaöryggis skulu vera mælanlegar, að eins miklu leyti og það er framkvæmanlegt.

5. gr. Rekstur, þróun, öflun og viðhald kerfa

Skriflegir verkferlar skulu liggja til grundvallar rekstri upplýsingakerfa. Verkferlarnir skulu tryggja fullnægjandi og rétta gagnavinnslu, meðhöndlun og geymslu á gögnum ásamt aðgengi að upplýsingakerfum.
Eftirlitsskyldur aðili skal hafa skriflega verkferla fyrir öflun, þróun og prófanir á upplýsingakerfum. Ábyrgðaraðili skv. 2. gr. skal gefa samþykki sitt fyrir notkun upplýsingakerfis eða innleiðingu breytinga á kerfinu áður en það er tekið í notkun.
Eftirlitsskyldur aðili skal tryggja viðhald og umsjón upplýsingakerfa þannig að rekstur þeirra sé stöðugur, í samræmi við áætlanir og fyrirsjáanlegur. Viðhald skal unnið eftir skriflegum verkferlum.
Verkferlar sem fjalla um breytingar skulu taka til allra breytinga sem geta haft áhrif á upplýsingakerfin og skulu tryggja viðeigandi, formlega meðhöndlun breytinga ásamt skráningu á þeim. Eftirlitsskyldi aðilinn skal tryggja að verkferlarnir hafi í för með sér traustan, skipulegan og fyrirsjáanlegan rekstur upplýsingakerfa.

6. gr. Gæði og frávik

Eftirlitsskyldur aðili skal setja sér gæðamarkmið á einstökum sviðum upplýsinga-tækni, sem taka mið af heildargæðamarkmiðum aðilans. Skrifleg ferli skulu vera til staðar til að fylgja eftir gæðamarkmiðunum.
Eftirlitsskyldur aðili skal fylgja skriflegum ferlum sem taka til meðhöndlunar frávika, eftir því sem unnt er. Ferlarnir skulu taka til frávika sem verða í rekstri upplýsingakerfanna.
Markmið meðhöndlunar frávikanna skal vera að koma aftur á eðlilegu rekstrarástandi upplýsingakerfanna. Finna skal orsakir frávika, koma í veg fyrir að þau endurtaki sig og tryggja viðeigandi og formlega meðhöndlun þeirra. Skjalfesta skal öll frávik.

7. gr. Órofinn rekstur (viðbúnaðaráætlun)

Eftirlitsskyldur aðili skal skjalfesta og uppfæra áætlun sem miðar að því að halda rekstri gangandi og skal grípa til í kjölfar áfalls sem veldur rekstrarstöðvun með þeim afleiðingum að rekstur upplýsingakerfanna getur ekki haldið áfram. Hann skal koma á fót ferli til að tryggja órofinn rekstur upplýsingakerfa. Þar skal skilgreina hlutverk, ábyrgð, verkefni og áhættur. Á grundvelli áhættugreiningar, sbr. 3. gr., skal skilgreina þau upplýsingakerfi sem eru mikilvæg starfsemi aðilans og áætlunin skal taka til.
Áætlunin skal m.a. taka til eftirfarandi atriða:

- Einstakir þættir sem geta brugðist skulu skilgreindir og grípa skal til viðeigandi ráðstafana til úrbóta.
- Skýr viðmið skulu sett um hvenær grípa skuli til varalausna.
- Verkferlum til að koma rekstri aftur í gang, skal komið á.
- Yfirsýn yfir upplýsingakerfin sem tilheyra áætluninni.
- Lýsing á áfallalausnum.
- Skýr viðmið um gangsetningu á áfallalausnum.
- Ásættanleg tímamörk rekstrarstöðvunar áður en gripið er til áfallalausna.
- Yfirsýn yfir ábyrgðarsvið og verkferla við gangsetningu áfallalausna.
- Upplýsingar til stjórnar, starfsmanna, birgja, viðskiptavina, opinberra stjórnvalda og fjölmiðla.

Áætluninni skal framfylgt með kennslu, æfingum og prófunum á varalausnum sem tryggja að þær virki eins og til er ætlast, eftir því sem við á. Prófanir skulu skjalfestar þannig að hægt sé að leggja mat á framkvæmd og árangur.

8. gr. Útvistun

Eftirlitsskyldur aðili ber ábyrgð á að rekstur upplýsingakerfa uppfylli allar kröfur sem til hans eru gerðar í tilmælum þessum. Þetta á við hvort sem rekstri upplýsingakerfa er útvistað að hluta til eða í heild sinni. Skriflegur samningur skal liggja fyrir til að tryggja þetta.
Samningurinn skal:

- Innihalda ákvæði um hvaða þjónustu vistunaraðili skal inna af hendi að lágmarki (Service Level Agreement).
- Tryggja að eftirlitsskyldur aðili eigi rétt til eftirlits með þeirri starfsemi vistunaraðilans sem samningurinn tekur til.
- Hafa þagnarskylduákvæði og með honum skal tryggt að farið sé að ákvæðum um þagnarskyldu í lögum um starfsemi eftirlitsskyldra aðila.
- Tryggja aðgang Fjármálaeftirlitsins að upplýsingum frá vistunaraðila og að athuganir, sem Fjármálaeftirlitið telur vera nauðsynlegan lið í eftirliti með eftirlitsskylda aðilanum, geti farið fram á vinnustöð vistunaraðila.

Eftirlitsskyldur aðili skal gæta þess, með eigin aðgerðum eða formlegu samstarfi við aðra aðila en vistunaraðilann, að hann búi yfir nægilegri þekkingu (tæknilegri og lagalegri) til að gera útvistunarsamninginn.

Eftirlitsskyldur aðili skal tilnefna ábyrgðaraðila á kröfum þeim sem til hans eru gerðar skv. 1.mgr. þessarar greinar. Ábyrgð á að framkvæmd sé í samræmi við efni laga og reglna sem um starfsemina gilda, þ.m.t. efni þessara leiðbeinandi tilmæla, verður ekki útvistað.

Stjórnunarlegri ábyrgð verður ekki útvistað. Ábyrgð á áhættustýringu vegna útvistunar liggur ávallt hjá stjórn eftirlitsskylds aðila.

9. gr. Skráning

Uppfært yfirlit yfir skipulag, búnað, upplýsingakerfi og rekstur þeirra skal ávallt vera fyrirliggjandi. Skjalfest, uppfærð lýsing á einstökum upplýsingakerfum, sem hafa þýðingu fyrir starfsemi eftirlitsskylds aðila, sem staðfestir að tilmæli þessu séu uppfyllt, skal liggja fyrir.