Upplýsingaöryggisstefna

Með þessari skjalfestu stefnu vill Starfsendurhæfingarsjóður leggja áherslu á mikilvægi upplýsingaöryggis fyrir starfsemi sjóðsins.

Að undanskildum mannauði, eru upplýsingar mikilvægasta eign sjóðsins og án þeirra getur hann ekki sinnt hlutverki sínu eða staðið við skuldbindingar. Sjóðurinn mun vernda upplýsingaeignir sínar á þá vegu sem þykir viðeigandi, hagkvæmt og í samræmi við lög og reglugerðir. Það mun auðvelda sjóðnum að uppfylla skuldbindingar sínar og markmið.
Starfsendurhæfingarsjóður stefnir að því að hagnýta upplýsingatækni til að varðveita gögn og miðla þeim á hagkvæman hátt.

Hlutverk þessarar stefnu er að lýsa skuldbindingu Starfsendurhæfingarsjóðs, að vernda upplýsingaeignir sjóðsins gegn ógnunum, innan frá eða utan, vísvitandi eða óviljandi. Markmið stjórnunar upplýsingaöryggis er að tryggja áframhaldandi rekstur og lágmarka tjón, ef skaði verður, með því að koma í veg fyrir eða lágmarka áhrif af atvikum sem geta truflað rekstur og þjónustu sjóðsins.
Upplýsinga- og skráningakerfi sjóðsins innihalda viðkvæmar upplýsingar sem ekki má nota í öðrum tilgangi en vegna starfsemi hans. Trúverðuleiki sjóðsins og hagsmunir aðila, sem tengjast málum er upplýsingarnar varða, gætu skaðast ef upplýsingarnar komast í rangar hendur, eru ónákvæmar eða eru ekki aðgengilegar þegar þeirra er þörf. Þess vegna skilgreinir sjóðurinn þessa öryggisstefnu er varðar trúnað, réttleika og tiltækileika gagna.

Trúnaður. Starfsendurhæfingarsjóður tryggir að eingöngu aðilar, sem til þess hafa heimild, hafi aðgang að upplýsingaeignum Starfsendurhæfingarsjóðs.
Réttleiki gagna. Starfsendurhæfingarsjóður tryggir að upplýsingar sem skráðar eru hjá sjóðnum séu skráðar rétt og nákvæmlega á hverjum tíma. Ónákvæmar, villandi, ófullkomnar eða úreltar upplýsingar séu leiðréttar, eytt eða við þær aukið þegar slíkt uppgötvast og haldið verði uppi reglubundnu eftirliti í þeim tilgangi.
Tiltækileiki gagna. Starfsendurhæfingarsjóður tryggir að upplýsingar sem skráðar eru í upplýsingakerfi hans séu aðgengilegar þeim, sem hafa heimild og þurfa að nota þær, þegar þeirra er þörf. Starfsendurhæfingarsjóður tryggir einnig að kerfi og gögn sem kunna að eyðileggjast sé hægt að endurheimta með hjálp neyðaráætlunar og afrita sem geymd eru á öruggum stað.

Öryggisstefna þessi tekur mið af lögum og reglugerðir um persónuvernd og meðferð persónuupplýsinga og af öryggisstaðlinum ÍST ISO/IEC 27001/27002. Öryggisstefnan er í fullu samræmi við reglur Persónuverndar nr. 299/2001 um öryggi persónuupplýsinga.

Starfsmenn sem hafa aðgang að upplýsingaeignum og þeir vinnsluaðilar, sem koma að rekstri upplýsingakerfa, skulu hafa aðgang að og þekkja til þessarar öryggisstefnu og þess hluta handbókar um öryggi gagna sem snertir þeirra vinnu. Viðurlög komi fram í verksamningum, ráðningarsamningum, starfslýsingum eða lögum og felist eftir atvikum í skriflegri áminningu eða brottrekstri.

Vigdís Jónsdóttir
Framkvæmdastjóri Starfsendurhæfingarsjóðs

Ítarleg stefna

Markmið og leiðir:
Það er markmið Starfsendurhæfingarsjóðs að nota raunhæfar, viðeigandi, hagnýtar og árangursríkar öryggisráðstafanir til að vernda mikilvæg verkferli og eignir. Sérstaklega er tryggt að:

- Aðgengi að upplýsingaeignum sé bundið við þá sem til þess hafa heimild;
- Upplýsingaeignir séu varðveittar á tryggilegan hátt;
- Farið sé að kröfum Starfsendurhæfingarsjóðs og lögum um persónuvernd varðandi aðgang, meðhöndlun, varðveislu og dreifingu upplýsinga;
- Haldin sé viðeigandi leynd og trúnaður um upplýsingaeignir;
- Réttleiki upplýsingaeigna sé tryggður með því að verja þær fyrir óheimilum breytingum;
- Ákvæði laga, reglugerða og samninga séu uppfyllt;
- Útbúin sé neyðaráætlun, henni haldið við og hún prófuð eins og kostur er;
- Starfsmönnum sé veitt viðeigandi fræðsla og þjálfun varðandi öryggiskröfur sjóðsins;
- Tilkynnt sé um öll öryggisfrávik og veikleika á öryggiskröfum og –kerfum. Frávik skulu rannsökuð;
- Í öryggisreglum sé sérstaklega tekið á vírusavörn og aðgangsstjórnun.

Gildissvið:
1. Öryggisstefna þessi nær til og gildir um alla sem hafa aðgang að upplýsinga-eignum Starfsendurhæfingarsjóðs. Í henni er skilgreint lágmarksöryggi.

Ábyrgð og skipulag:
1. Framkvæmdastjóri Starfsendurhæfingarsjóðs er endanlega ábyrgur fyrir öryggi upplýsingaeigna.
2. Framkvæmdastjóri skipar umsjónarmann öryggismála sem sér um daglega stjórnun upplýsingaöryggis.
3. Umsjónarmaður öryggismála skal sjá til þess að starfsfólk hljóti viðeigandi fræðslu um öryggismál. Verksvið umsjónarmanns er að öðru leyti skilgreint í handbók um öryggismál gagna.
4. Framkvæmdarstjóri er ábyrgur fyrir því að allir starfsmenn sjóðsins þekki og skilji öryggisstefnu þessa og hafi hana að leiðarljósi í starfi sínu.
5. Það er á ábyrgð sérhvers starfsmanns að fylgja þessari öryggisstefnu og öryggisreglum sem koma fram í handbók sjóðsins um öryggi gagna.

Endurskoðun, áhættumat og innra eftirlit:
1. Öryggisstefnuna skal endurmeta að minnsta kosti einu sinni á ári. Verði veruleg breyting á áhættuþáttum skal endurmeta öryggisstefnu án tafar.
2. Áhættumat skal vera viðvarandi og í samræmi við kröfur Persónuverndar og ISO/IEC 27001. Það skal endurskoðað reglulega á tveggja ára fresti og eftir þörfum í tengslum við áhættumat eða breyttar aðstæður.
3. Öryggisþarfir skal greina út frá áhættumati og greiningu á öryggiskröfum laga og opinberra eftirlitsaðila.

4. Velja skal viðeigandi tæknilegar og skipulagslegar öryggisráðstafanir til að vernda upplýsingaeignir. Öryggisráðstafanir skal endurskoða reglulega.
5. Beita skal ráðstöfunum sem tryggja nægilegt öryggi með tillit til kostnaðar og í hlutfalli við áhættu sem dregið er úr og hugsanlegt tjón ef öryggisfrávik verða.
6. Viðhafa skal reglubundið innra eftirlit með vinnslu upplýsinga og meðferð upplýsingaeigna til að ganga úr skugga um að unnið sé í samræmi við gildandi lög og reglur og þær öryggisráðstafanir sem ákveðnar hafa verið.
7. Tíðni eftirlitsins og umfang þess skal ákveðið með hliðsjón af áhættu, eðli eigna sem vernda á, þeirri tækni sem notuð er til að tryggja öryggi þeirra og kostnaði af framkvæmd eftirlitsins.

Aðgangur, notkun og notagildi upplýsinga:

1. Aðgangur starfsmanna að upplýsingum er háður tilskyldum leyfum og um hann gilda strangar öryggis- og starfsreglur, sem fram koma í handbók. Aðgangsheimildum skal stýra tryggilega og skal framkvæmdastjóri eða tilsjónarmaður öryggismála hafa eftirlit með þeim.
2. Aðgangsheimildum skal ætíð viðhaldið og breytingar á stöðu notenda skulu án tafar tilkynntar til rekstraraðila aðgangsstjórnunar.
3. Allur gagnaaðgangur skal skráður og skilja eftir úttektarslóð [(e. audit trail)] sem safnað er í rekstrardagbók.
4. Ábyrgðaraðili upplýsingatæknimála skal hafa eftirlit með aðgangi og notkun upplýsinga.
5. Notkun skráist sérstaklega og reglulega skal skoða hverjir hafa notað eftirlitsháðar aðgangsheimildir og ástæður þess. Starfsmenn geta þurft að gera nákvæma grein fyrir ástæðum notkunar.
6. Beita skal aðgangsstýringum í húsnæði Starfsendurhæfingarsjóðs.
7. Beita skal tæknilegum aðgangshindrunum, svo sem eldveggjum, aðgangsorðum, skjásvæfum og öryggiskerfum til að fyrirbyggja aðgang óviðkomandi að upplýsingum á fartölvum og um tölvunet og fjarskiptakerfi.

Leynd og réttleiki gagna:

1. Persónuvernd og trúnaður persónuupplýsinga skal tryggður í samræmi við ákvæði laga nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga og reglna nr. 299/2001 um öryggi persónuupplýsinga. Sérstaklega skal gætt að þær séu:
    a. unnar með sanngjörnum, málefnalegum og lögmætum hætti og að öll meðferð þeirra sé í samræmi við vandaða vinnsluhætti persónuupplýsinga;
    b. fengnar í yfirlýstum, skýrum, málefnalegum tilgangi og ekki unnar frekar í öðrum og ósamrýmanlegum tilgangi;
    c. nægilegar, viðeigandi og ekki umfram það sem nauðsynlegt er miðað við tilgang vinnslunnar;
    d. áreiðanlegar og uppfærðar eftir þörfum. Persónuupplýsingar sem eru óáreiðanlegar eða ófullkomnar, miðað við tilgang vinnslu þeirra, skal afmá eða leiðrétta.
2. Allar upplýsingar sem skráðar eru í upplýsingakerfi skulu vera skráðar rétt og á nákvæman hátt miðað við upplýsingagjöf.
3. Ónákvæmar, villandi, ófullkomnar og úreltar upplýsingar skal leiðrétta, eyða eða við þær aukið þegar þær uppgötvast og halda skal uppi reglubundnu eftirlitsferli í þeim tilgangi.
4. Tryggja skal eins og kostur er að gögn sem send eru frá sjóðnum komist ósködduð á réttan áfangastað og á réttum tíma.

5. Viðkvæm gögn með hátt trúnaðarstig skal ekki senda um Internetið nema þau séu tryggilega varin fyrir hnýsni, t.d. með dulkóðun eða lokuðum samskiptarásum.
6. Setja skal upp varnir gegn spillihugbúnaði til að tryggja réttleika gagna. Reglur um það eru settar fram í handbók.

Neyðarstjórnun og öryggisfrávik:

1. Tryggja skal samfelldan rekstur upplýsingakerfa.
2. Virk neyðaráætlun skal vera til staðar sem gerir kleift að endurreisa reksturinn í neyðartilvikum.
3. Öll frávik frá öryggisstefnu skal tilkynna til næsta yfrimanns eða tengiliðs.
4. Starfsmenn Starfsendurhæfingarsjóðs sem verða uppvísir að vísvitandi brotum á öryggisstefnu sjóðsins skulu sæta agaviðurlögum, sjá skjal brot á vinnu- og siðareglum. Atriði sem varða brot á lögum skulu tilkynnt hlutaðeigandi yfirvöldum.

Handbók:

1. Útbúin skal handbók um öryggi gagna fyrir sjóðinn með skriflegum verklagsreglum um útfærslu öryggisstefnunnar.
2. Í handbók skal m.a. vera:
   - Öryggisstefna, bæði stutt og ítarleg útgáfa;
   - Upplýsingar um sjóðinn og viðeigandi öryggisþarfir;
   - Rammi öryggisstjórnunar, þ.e. umfang og stjórnun öryggismála;
   - Lýsing á upplýsingaöryggiskerfi;
   - Ferlar sem lýsa rekstri og viðhaldi á upplýsingaöryggiskerfinu;
   - Tilvísunarskrá þar sem vísað er í ítarefni og nánari verkferli;
   - Lýsing á þeim aðferðum sem notaðar eru við áhættumat;
   - Yfirlit yfir eftirlitsaðgerðir og varúðarráðstafanir sem hrint hefur verið í framkvæmd.
3. Handbókina skal yfirfara og endurskoða reglulega, minnst einu sinni á ári.
4. Efni handbókar skal vera gert aðgengilegt í samræmi við þarfir hvers og eins.
5. Handbókin er hluti af gæðakerfi sjóðsins.

Staðlar, lög og reglugerðir:

1. Starfsendurhæfingarsjóður skal uppfylla lög og reglugerðir sem lúta að starfsemi hans.
2. Öryggisstefna og öryggisreglur skulu vera mótaðar í samræmi við alþjóðlega viðurkennda staðla, m.a. útgefna af Staðlaráði Íslands, Alþjóðastaðlastofnuninni (ISO) og Evrópsku staðlastofnuninni (IEC).