Greiðslustofa lífeyrissjóða

Öryggis- og áhættustefna og skipulag öryggismála

September 2024

Öryggis- og áhættustefna og skipulag öryggismála Greiðslustofu lífeyrissjóða

Efnisyfirlit

Öryggisstefna rekstrar og verðmæta

Tilgangur

Þessi öryggisstefna rekstrar og verðmæta lýsir áherslu stjórnar GL á meðferð verðmæta og öryggi í rekstri. Verja þarf verðmæti og rekstur GL fyrir öllum ógnum, innri og ytri, af ásetningi, vegna óhappa eða af slysni. Fagleg vinnubrögð eru lykillinn að árangri og til marks um það er þessi öryggisstefna sett. Innleiðing og framkvæmd stefnunnar er mikilvæg til að fullvissa starfsmenn og viðskiptavini GL um heilindi og rétt vinnubrögð í rekstri fyrirtækisins. Stjórn GL hefur samþykkt þessa stefnu og styður við framkvæmd hennar.

Umfang

Öryggisstefnan tekur til allrar starfsemi GL. Hún tekur til umgengni og vistunar allra verðmæta í hvaða formi sem er. Stefnan tekur til allra samskipta starfsmanna, viðskiptavina, samstarfsaðila og birgja. Hún tekur einnig til hvers konar skráningar, vinnslu, samskipta, dreifingar, geymslu og eyðingar verðmæta GL.

Öryggisstefnan tekur jafnframt til húsnæðis og búnaðar þar sem verðmæti eru meðhöndluð eða vistuð sem og starfsmanna og samningsbundinna viðskiptavina sem hafa aðgang að verðmætum.

Markmið

Markmið GL með öryggisstefnunni eru að:

1. Verðmæti séu óspillt og aðgengileg þeim sem afnotarétt hafa þegar þörf er á.
2. Verðmæti séu óaðgengileg óviðkomandi og varin gegn skemmdum, sviksemi, eyðingu eða afhendingu til aðila sem hafa ekki afnotarétt hvort sem er af ásetningi eða gáleysi.
3. Upplýsingar séu varðar gegn þjófnaði, eldi, náttúruhamförum o.þ.h.
4. Alltaf séu til áreiðanleg og örugglega varðveitt afrit af helstu skjölum og hugbúnaðarkerfum.
5. Verðmæti sem fara úr húsi komist til rétts viðtakanda ósködduð og á réttum tíma, þess sé gætt að þau fari ekki til annarra.
6. Áætlanir séu gerðar um samfelldan rekstur, þeim sé viðhaldið og þær prófaðar eins og kostur er.
7. Frávik, brot eða grunur um veikleika í öryggi séu tilkynnt og rannsökuð.
8. Að áhætta vegna meðferðar og varðveislu verðmæta sé innan skilgreindra áhættumarka.

Leiðir að markmiðum

Leiðir GL að ofangreindum markmiðum eru að:

1. Halda skrá yfir verðmæti og flokka þau eftir mikilvægi verðgildis og tiltækileika.
2. Greina reglulega með formlegu áhættumati verðmæti eigna, viðkvæmni þeirra og ógnir sem geta stefnt þeim í hættu.
3. Halda skipulagshandbók með verklagsreglum og verkferlum vegna meðferðar upplýsinga og viðhalda henni.
4. Stjórnendur og starfsmenn GL fylgi skipulagshandbók GL og öllum öðrum fyrirmælum fyrirtækisins.
5. Fylgja og hlíta lögum sem um starfsemina gilda.
6. Fylgja öllum samningum sem fyrirtækið er aðili að og varða öryggi.
7. Allir starfmenn GL fái þjálfun og fræðslu varðandi öryggi og ábyrgð þeirra hvað varðar öryggi.

Ábyrgð

Ábyrgð við framkvæmd og viðhald öryggisstefnunnar skiptist á eftirfarandi hátt:

1. Stjórn GL ber ábyrgð á öryggisstefnunni og endurskoðar hana reglulega.
2. Framkvæmdastjóri GL ber ábyrgð á framkvæmd öryggisstefnunnar og beitir til þess viðeigandi stöðlum og vinnuferlum.
3. Allir starfsmenn GL bera ábyrgð á að fylgt sé þeim vinnuferlum sem eiga að tryggja framkvæmd öryggisstefnunnar. Viðskiptavinir, verktakar og birgjar bera ábyrgð á að fylgt sé samnings-bundnum vinnuferlum sem eiga að tryggja framkvæmd stefnunnar.
4. Öllum starfsmönnum GL ber að vinna samkvæmt öryggisstefnunni. Þeim ber að tilkynna öryggisfrávik og veikleika sem varða öryggi. Þeir sem ógna öryggi GL eða viðskiptavina hennar af ásettu ráði eiga yfir höfði sér málshöfðun eða aðrar viðeigandi lagalegar aðgerðir.

Áhættumörk

Áhættuþol GL vegna reksturs tekur mið af því að tryggja að ávallt sé hægt að greiða út réttan lífeyri á réttum tíma. GL er með mánaðarlegar eftirlitsaðgerðir til þess að tryggja að þessu grunnhlutverki sé framfylgt

Endurskoðun

Þessi stefna er endurskoðuð á 2-3 ára fresti og oftar ef þörf krefur til þess að tryggja að hún samrýmist markmiðum með rekstri GL.

Öryggisstefna upplýsingamála

Tilgangur

Þessi öryggisstefna lýsir áherslu stjórnar GL á upplýsingavernd og öryggi í allri upplýsingavinnslu. Verja þarf upplýsingaeignir GL fyrir öllum ógnum, innri og ytri, af ásetningi, vegna óhappa eða af slysni. Fagleg vinnubrögð eru lykillinn að árangri og til marks um það er þessi öryggisstefna sett. Innleiðing og framkvæmd stefnunnar er mikilvæg til að fullvissa starfsmenn og viðskiptavini GL um heilindi og rétt vinnubrögð í rekstri fyrirtækisins. Stjórn GL hefur samþykkt þessa stefnu og styður við framkvæmd hennar.

Umfang

Öryggisstefnan tekur til allrar starfsemi GL. Hún tekur til umgengni og vistunar allra upplýsinga í hvaða formi sem er og á hvaða miðli sem er. Stefnan tekur til allra samskipta starfsmanna, viðskiptavina, samstarfsaðila og birgja. Hún tekur einnig til hvers konar skráningar, vinnslu, samskipta, dreifingar, geymslu og eyðingar upplýsinga GL.

Öryggisstefnan tekur jafnframt til húsnæðis og búnaðar þar sem upplýsingar eru meðhöndlaðar eða vistaðar sem og starfsmanna og samningsbundinna viðskiptavina sem hafa aðgang að upplýsingum.

Markmið

Markmið GL með öryggisstefnunni eru að:

1. Upplýsingar séu réttar og aðgengilegar þeim sem aðgangsrétt hafa þegar þörf er á.
2. Trúnaðarupplýsingar séu óaðgengilegar óviðkomandi og varðar gegn skemmdum, eyðingu eða uppljóstrun til aðila sem hafa ekki aðgangsrétt hvort sem er af ásetningi eða gáleysi.
3. Gætt sé ákvæða laga um persónuvernd.
4. Leynd upplýsinga og trúnaði sé viðhaldið.
5. Upplýsingar berist ekki óviðkomandi af ásetningi eða gáleysi.
6. Upplýsingar séu varðar gegn þjófnaði, sviksemi, eldi, náttúruhamförum o.þ.h.
7. Upplýsingar séu varðar gegn skemmdum og eyðingu af völdum tölvuveira.
8. Alltaf séu til áreiðanleg og örugglega varðveitt afrit af helstu gögnum og hugbúnaðarkerfum.
9. Upplýsingar sem fara um net komist til rétts viðtakanda ósköddуð og á réttum tíma, þess sé gætt að þau fari ekki til annarra.
10. Áætlanir séu gerðar um samfelldan rekstur, þeim sé viðhaldið og þær prófaðar eins og kostur er.
11. Frávik, brot eða grunur um veikleika í upplýsingaöryggi séu tilkynnt og rannsökuð.
12. Að áhætta vegna vinnslu (meðferðar) og varðveislu upplýsinga sé innan skilgreindra áhættumarka.

Leiðir að markmiðum

Leiðir GL að ofangreindum markmiðum eru að:

1. Halda skrá yfir upplýsingaeignir og flokka þær eftir mikilvægi leyndar, réttleika og tiltækileika.
2. Greina reglulega með formlegu áhættumati verðmæti upplýsingaeigna, viðkvæmni þeirra og ógnir sem geta stefnt þeim í hættu.
3. Halda skipulagshandbók með verklagsreglum og verkferlum vegna meðferðar upplýsinga og viðhalda henni.
4. Stjórnendur og starfsmenn GL fylgi skipulagshandbók GL og öllum öðrum fyrirmælum fyrirtækisins.
5. Fylgja og hlíta lögum sem um starfsemina gilda.
6. Fylgja öllum samningum sem fyrirtækið er aðili að og varða upplýsingaöryggi.
7. Allir starfmenn GL fái þjálfun og fræðslu varðandi upplýsingaöryggi og ábyrgð þeirra hvað varðar upplýsingaöryggi.

Ábyrgð

Ábyrgð við framkvæmd og viðhald öryggisstefnunnar skiptist á eftirfarandi hátt:

1. Stjórn GL ber ábyrgð á öryggisstefnunni og endurskoðar hana reglulega.
2. Framkvæmdastjóri GL ber ábyrgð á framkvæmd öryggisstefnunnar og beitir til þess viðeigandi stöðlum og vinnuferlum.
3. Allir starfsmenn GL bera ábyrgð á að fylgt sé þeim vinnuferlum sem eiga að tryggja framkvæmd öryggisstefnunnar. Viðskiptavinir, verktakar og birgjar bera ábyrgð á að fylgt sé samnings-bundnum vinnuferlum sem eiga að tryggja framkvæmd stefnunnar.
4. Öllum starfsmönnum GL ber að vinna samkvæmt öryggisstefnunni. Þeim ber að tilkynna öryggisfrávik og veikleika sem varða upplýsingaöryggi. Þeir sem ógna upplýsingaöryggi GL eða viðskiptavina hennar af ásettu ráði eiga yfir höfði sér málshöfðun eða aðrar viðeigandi lagalegar aðgerðir.

Áhættumörk

Áhættuþol GL vegna upplýsingamála tekur mið af því að tryggja að ávallt sé hægt að greiða út réttan lífeyri á réttum tíma. GL er með mánaðarlegar eftirlitsaðgerðir til þess að tryggja að þessu grunnhlutverki sé framfylgt

Endurskoðun

Þessi stefna er endurskoðuð 2-3 ára fresti og oftar ef þörf krefur til þess að tryggja að hún samrýmist markmiðum með rekstri GL.

Áhættustefna GL

Markmið með stefnunni er að formfesta vinnulag til mats á helstu áhættuþáttum GL og stuðla þannig að auknu öryggi í rekstri GL. Áhættustefnan nær yfir starfsemi GL og inniheldur áhættumat verðmæta, rekstrar, starfsmannamála, upplýsinga, nettengingar og tölvubúnaðar.

Áhættumat verðmæta

Verðmæti á skrifstofu GL eru einkum tvenns konar: Búnaður og skjöl. Verðgildi er ekki mikið á hefðbundinn mælikvarða (endurnýjunarverð) og áhætta vegna misnotkunar, tjóns eða bilunar er óveruleg. Almennar öryggisráðstafanir teljast fullnægjandi og ekki er þörf á sértækum ráðstöfunum.

Skrifstofubúnaður (húsgögn og tæki):

Hér er um almennan búnað að ræða, sem er jafnan fáanlegur á almennum markaði. Verði tjón eða bilun er unnt að bregðast við með skömmum fyrirvara og útvega sambærilegan búnað til að tryggja samfellu í rekstri. Ekki þyrfti að verða meiri röskun en sem nemur einum starfsdegi og er það innan venjulegra marka um rekstraröryggi.

Skjöl og rafræn gögn:

Skjöl eru í meginatriðum þrenns konar:

1. Lífeyrisúrskurðir og fylgiskjöl.
   Frumskjöl eru tvenns konar: a) Ef GL gerir úrskurð fyrir Lífeyrissjóð Vestmannaeyja eru öll frumskjöl vistuð hjá GL en afrit send sjóðnum (og trúnaðarlækni ef við á). Skjölin eru vistuð í eldtefjandi, læstum skjalaskápum. b) Ef GL gerir úrskurð fyrir Festu lífeyrissjóð eða Lífeyrissjóð bænda eru öll skjöl vistuð í skjalakerfi viðkomandi lífeyrissjóðs.
   Úrskurðirnir eru gerðir í úrskurðarkerfi Jóakims og unnt er að endurgera þá á grundvelli skjala frá sjóðunum ef þörf krefur.
2. Bókhaldsskjöl
   Frumskjöl eru geymd í skjalamöppum í læstum skápum. Upplýsingar úr þeim eru skráðar að jafnaði mánaðarlega í bókhaldsforrit. Flest skjöl koma utan frá og alla jafna ætti að vera auðvelt að kalla eftir afritum. Flestar færslur eru í föstum skorðum, svipaðar frá einum mánuði til annars, og greiðslur eru rafrænar og þar af leiðandi skráðar á bankareikningum. Unnt er að endurgera eða sannreyna skjölin að mestu eða öllu leyti með tiltölulega einföldum hætti.
3. Skjöl um vinnslu
   Skjölin verða til í Jóakim eða Office-hugbúnaði. Afrit eru geymd í einhverjum mæli í skjalamöppum í læstum skápum. Rafræn afrit eru til af langflestum skjalanna eða þau eru endurgeranleg. Skjöl úr Office-hugbúnaði eru vistuð á miðlægu drifi í tölvurými Sensa. Skjöl úr Jóakim eru endurgeranleg fyrirhafnarlítið.

Í ljósi þess að auðvelt er að endurgera skjöl eða afla afrita eða upplýsinga um innihald þeirra er ekki þörf á sérstökum öryggisaðgerðum umfram þær sem þegar eru til staðar. Röskun af völdum tjóns eða bilunar yrði í flestum tilvikum óveruleg en nokkurn tíma gæti tekið að endurnýja skjölin ef um meiri háttar tjón yrði að ræða, s.s. af völdum bruna eða vatnstjóns. Slík endurnýjun myndi þó ekki tefja rekstur að neinu marki.

Öryggisráðstafanir og viðbrögð við frávikum:

GL óskar árlega eftir staðfestingu frá Festu lífeyrissjóði og Lífeyrissjóði bænda hvort prófun hafi verið framkvæmd á endurheimt gagna.

GL leigir skrifstofuhúsnæði hjá Reiknistofu lífeyrissjóða hf. (RL). Öryggiskerfi RL varðandi innbrot og óleyfilegar mannaferðir, eld og vatnstjón ná einnig til húsnæðis GL. Hæðin þar sem skrifstofuhúsnæði GL er á er ávallt læst og í lok hvers vinnudags fer öryggiskerfið sjálfkrafa á fyrir alla hæðina kl 18:00.

Verði atvik þar sem öryggisvarnir eru rofnar gefa öryggiskerfin sjálfkrafa merki til öryggisþjónustu sem er á vakt allan sólarhringinn.

Áhættumat rekstrar

Rekstur á skrifstofu GL felst að mestu leyti í föstum verkefnum. Þau eru yfirleitt ekki viðkvæm fyrir töfum um 1-2 daga, en sum hver þola ekki lengri bið. Starfsemi GL er auðvelt að flytja í annað húsnæði með skömmum fyrirvara. Engan sérbúnað þarf og skamman tíma tæki að tengja tölvur við Jóakim og miðlæga hýsingu tölvugagna. Ef bruni, vatnstjón eða jarðskjálftar yllu því að tölvur ónýttust eða vinnuaðstaða væri ekki nothæf, væri unnt að setja upp bráðabirgðaskrifstofur á einum degi og halda starfseminni áfram. Vafalaust myndi vinnan vera tafsöm fyrst um sinn meðan verið væri að hnýta lausa enda, en slíkar tafir myndu vart leiða til frekari rekstrarvanda, s.s. seinkunar á reglubundinni vinnslu.

Almennar öryggisráðstafanir teljast fullnægjandi og ekki er þörf á sértækum ráðstöfunum.

Þó er rétt að huga sérstaklega að viðbúnaði vegna fjarskipta, einkum tölvutengingar við umheiminn, ef símalínur rofna við húsið eða hverfið. Með sama hætti er rétt að gera kröfur til birgja um viðbúnað vegna sams konar vandamála á eða við starfsstöðvar þeirra.

Dagleg vinnsla:

Hér er einkum um að ræða þrenns konar verkefni:

- Almenn upplýsingagjöf og úrlausn tilfallandi beiðna, s.s. frá lífeyrisþegum eða sjóðum.
- Lífeyrisúrskurðir
- Skráning og umsýsla persónuafsláttar og skattþreps

Öll þessi verkefni þola bið eða skerta þjónustu, s.s. vegna forfalla starfsmanns. Í versta falli myndi langvinn frestun leiða til þess að rétt útgreiðsla til eins eða fárra einstaklinga drægist um mánuð, en þá myndi Jóakim jafnframt gera leiðréttingu aftur í tímann, ef við ætti.

<u>Öryggisráðstafanir:</u>

Starfsmenn eru 4 allan ársins hring og skammvinn forföll eins eða tveggja myndu mögulega valda seinkun en ekki rekstrarstöðvun. Lengri fjarvera myndi kalla á tímabundna afleysingu.

Mánaðarleg greiðsla lífeyris og tengd verkefni:

Tölvuvinnslan hefst að jafnaði ellefu bankadögum fyrir greiðsludag. Fyrst er gerð forvinnsla yfir lífeyrisþega sem fá eftirágreiddan lífeyri. Að lokinni yfirferð og leiðréttingum hjá sjóðunum er aðalvinnsla framkvæmd fimm bankadögum fyrir greiðsludag. Frestun vinnslu um 1 dag veldur ekki vanda og frestun um 2 daga væri viðráðanleg. Lengri frestun kallar á aðgerðir samkvæmt viðbúnaðaráætlun.

Helstu áhættuþættir eru ferns konar: Fjarvera lykilstarfsmanns, bilun í hug- eða vélbúnaði, alvarleg villa í vinnslu og þjónustu brestur hjá birgjum.

Öryggisráðstafanir og viðbrögð við frávikum:

Óvænt fjarvera lykilstarfsmanns: Nákvæm verklýsing er til fyrir allar aðgerðir og getur annar starfsmaður framkvæmt allar aðgerðir samkvæmt skráðum leiðbeiningum.

Bilun í hug- eða vélbúnaði: Til er varaeintak af Jóakim kerfinu (næstnýjasta útgáfa) og er unnt að nota það með skömmum fyrirvara. Prentun er unnt að framkvæma utanhúss, einnig með skömmum fyrirvara.

Alvarleg villa í vinnslu: Mánaðarvinnsla er gerð tvisvar, í fyrra skiptið til að sannreyna að allt virki eðlilega og til að starfsfólk sjóðanna geti farið yfir niðurstöður. Leiði athugun í ljós villur, stórar eða smáar, er unnt að leiðrétta forsendur áður en seinni vinnsla fer af stað. Þess utan væri unnt að endurgera vinnslu í þriðja sinn ef með þyrfti.

Þjónustu brestur birgja: Litið er svo á að þeir hafi gert fullnægjandi ráðstafanir til að bregðast við áföllum. Hafa ber í huga að þjónusta við GL er sama eðlis og veitt er fjölda annarra viðskiptavina og því geta birgjarnir ekki látið viðbragðsaðgerðir sitja á hakanum.

Þrautalending: Ef ekki er unnt að ljúka mánaðarvinnslu innan lokatímamarka er unnt að láta endurtaka næstu vinnslu á undan, þ.e. að láta leggja sömu fjárhæðir inn á reikninga lífeyrisþega, til opinberra aðila o.s.frv., og láta prenta greiðsluseðla og/eða skýringarbréf til greiðsluþega, þar sem gerð er grein fyrir vandanum og að leiðrétting verði gerð um næstu mánaðamót. Að jafnaði myndi þetta valda innan við 1% fráviki á greiðslu til hvers greiðsluþega.

Vinnsla ársfjórðungslega eða sjaldnar:

Tekjuathugun (ársfjórðungslega)

Uppfærsla nafnaskrár (hálfsárslega)

Launamiðaskrá til Ríkisskattstjóra og launamiðar til annarra viðtakenda (árlega)

Helstu áhættuþættir eru ferns konar: Fjarvera lykilstarfsmanns, bilun í hug- eða vélbúnaði, alvarleg villa í vinnslu og þjónustu brestur hjá birgjum.

Öryggisráðstafanir:

Nákvæm verklýsing er til fyrir allar aðgerðir og getur annar starfsmaður framkvæmt allar aðgerðir samkvæmt skráðum leiðbeiningum. Framkvæmdastjóri þarf þó að veita starfsmanninum sérstaka aðgangsheimild fyrir sumar aðgerðir og stjórn GL getur einnig veitt slíka heimild.

Ofangreind verkefni þola frestun um vikur og í sumum tilvikum um mánuði. Er því unnt að bregðast við helstu áhættuþáttum án mikillar tímapressu. Því er ekki talin þörf á sérstakri viðbragðsáætlun, heldur verði brugðist við röskun hverju sinni eftir því sem tilefni er til.

Starfsmannamál:

Almenn hætta á að uppsagnir eða veikindi starfsmanna leiði til rekstrarerfiðleika. Skammvinn forföll gætu mögulega valdið seinkun en ekki rekstrarstöðvun.

Öryggisráðstafanir:
Til að draga úr starfsmannaáhættu eru til staðar vel skilgreindir verkferlar og vinnulýsingar þannig að þekking einskorðist ekki við starfsmanninn sjálfan.

Kerfisbundin þjálfun starfsmanna og afleysingamanna draga úr áhættunni. Einnig er nauðsynlegt að vinnuumhverfi stuðli að velferð starfsfólk og að framlag þeirra sé metið að verðleikum.

Sviksemisháhætta:

Hætta á svikum sem valda GL tjóni, t.d. gæti verið um svik starfsmanna að ræða.

Öryggisráðstafanir:
Gætt skal að aðskilnaði starfa og kerfislægum aðgangsstýringum auk þess sem reikningar skulu stemmdir af.

Hætta á sviksemi gagnvart starfsfólki.

Öryggisráðstafanir:
Stjórn skal hafa yfirlit yfir launagreiðslur til starfsmanna.

Áhættumat upplýsinga

Upplýsingar sem eru notaðar á skrifstofu GL eru að mestu leyti aðfengnar og taka ekki breytingum í meðförum GL. Frumsamdar upplýsingar eru ferns konar: Lífeyrisúrskurðir, innskráning persónuafsláttar og skattþreps, bókhaldsupplýsingar og vinnsluupplýsingar. Hér verður ekki fjallað um aðfengnar upplýsingar, því að litið er svo á að öryggi slíkra gagna sé á ábyrgð upprunastaðar.

Hér verður fjallað um upplýsingarnar út frá þremur grunnkröfum: Leynd, réttleika og tiltækileika.

Öryggiskröfur og viðbrögð við frávikum

1. Lífeyrisúrskurðir:

   Leynd: Upplýsingar eru skráðar inn í úrskurðarkerfi Jóakims. Kerfið er lokað, þ.e. aðgangsorð þarf til að skoða skjölin. Frumskjöl vegna Lífeyrissjóðs Vestmannaeyja eru vistuð í læstum skjalaskáp og afrit er sent sjóðnum. Öll skjöl vegna úrskurða fyrir Festu og LSB eru rafræn og vistuð í skjalakerfum sjóðanna. Leynd er því metin fullnægjandi, svo fremi að aðgangur að skrifstofunni og tölvukerfum sé takmarkaður með eðlilegum hætti.

   Réttleiki: Fleiri en einn starfsmaður koma að gerð úrskurða og fæst þannig samanburður á vinnubrögðum. Eftir gerð úrskurðar fer annar starfsmaður yfir úrskurðinn og fæst þannig mat á réttleika. Ef um flókna úrskurði er að ræða fer þriðji starfsmaður einnig yfir úrskurðinn. Síðan er úrskurður sendur viðkomandi lífeyrissjóði og fæst þannig einnig mat hans á réttleika. Réttleiki er því metinn fullnægjandi, svo og eftirlit með honum. Af sömu ástæðum er áhætta á sviksemi metin lítil og að eftirlit sé fullnægjandi.

   Tiltækileiki: Séu frumskjöl ekki tiltækileg, má vænta þess að afrit séu það, annars vegar í rafrænu skjali, hins vegar hjá viðkomandi lífeyrissjóði.

2. Upplýsingar vegna skattgreiðslna

   Leynd: Í eðli sínu eru upplýsingar um skatthlutfall og nýtingu persónuafsláttar ekki viðkvæmar, enda fara þær að almennum lögum og fela ekki í sér vitneskju um laun eða fríðindi viðkomandi. Því þarf ekki að gæta sérstakrar leyndar í meðferð þeirra.

   Réttleiki: Ef gerð er villa við innskráningu upplýsinga, kemur það fram við næstu launa/lífeyrisgreiðslu og þannig getur lífeyrisþegi brugðist strax við. Í ellefu mánuði af tólf skilar leiðrétting sér til lífeyrisþegans við næstu mánaðamót, en villa sem gerð er í desember leiðréttist ekki fyrr en við skattaálagningu í maí á næsta ári, en þá með vöxtum ríkisins.

   Tiltækileiki: Upplýsingar um nýjustu gildi eru í Jóakim, en til vara er reglubundin skráning hjá ríkisskattstjóra. Ef allt fer á versta veg fær lífeyrisþegi leiðréttingu með vöxtum við álagningu í maí.

3. Bókhaldsskjöl

   Leynd: Ekki er talið að upplýsingar séu viðkvæmar, nema launaupplýsingar starfsmanna. Lykilorð þarf til aðgangs að tölvukerfi. Fylgiskjöl eru vistuð í læstum skápum.

   Réttleiki: Endurskoðun felur í sér eftirlit með réttleika færslna, m.a. með afstemmingu við bankafærslur. Fjármunahreyfingar í rekstri GL eru lágar og í föstum skorðum og er hætta á sviksemi því lítil og endurskoðun felur í sér nægilegt eftirlit.

Tiltækileiki: Afrit eru tekin reglulega af miðlægum gagnagrunni og má því telja að tiltækileiki sé nægilega tryggur.

4. Skjöl um vinnslu

Leynd: Skjölin hafa yfirleitt ekki að geyma persónulegar eða viðkvæmar upplýsingar. Þau eru vistuð á miðlægu drifi í tölvurými Sensa. Í þeim tilvikum sem leyndar er þörf ber að vista þau í læstum hirslum.

Réttleiki: Hér er eingöngu um að ræða vistuð skjöl með forsendum og niðurstöðum og er réttleiki metinn annars staðar. Þannig metur hver lífeyrissjóður fyrir sig hvort niðurstöður lífeyriskeyrslna séu réttar.

Tiltækileiki: Öll skjöl eru endurgeranleg í Jóakim.

Í ljósi þess að auðvelt er að endurheimta upplýsingar eða afla afrita er ekki þörf á sérstökum öryggisaðgerðum umfram þær sem þegar eru til staðar. Röskun af völdum tjóns eða bilunar yrði í flestum tilvikum óveruleg. Skrá skal öll frávik frá ofangreindum öryggiskröfum, nema minniháttar villur sem valda ekki skaða og eru leiðréttar fljótt, og gera stjórn GL grein fyrir þeim eins og við á eftir eðli máls, annaðhvort strax með tilkynningu til stjórnarformanns eða í reglubundinni yfirferð tvisvar á ári.

Sviksemi

Starfsemi GL felst í seldri þjónustu við lífeyrissjóði. Allar aðgerðir sem snúa að meðferð fjármuna, aðrar en varða rekstrarkostnað GL, eru undir eftirliti þessara viðskiptavina. Engir fjármunir eru greiddir út eða fjárhæðir ákvarðaðar nema að fenginni yfirferð og samþykki viðskiptavinanna. Því er álitið að ekkert svigrúm sé til sviksemi gagnvart viðskiptavinunum eða í vinnslu fyrir þá sem gæti leitt til teljandi ávinnings fyrir starfsfólk GL eða tengda aðila.

Persónuvernd

Öll vinnsla persónuupplýsinga í verkefnum fyrir lífeyrissjóði er unnin á ábyrgð sjóðanna. Öllum samskiptum og kvörtunum sem varða meðferð persónuupplýsinga skal því beint til viðkomandi sjóða eða persónuverndarfulltrúa þeirra.

GL ber sem vinnsluaðili ábyrgð á að tilkynna til sjóðanna um hvers konar öryggisbrest í meðferð persónuupplýsinganna. Það á við um öryggisbrot sem fela í sér brot á trúnaði eða breytingu á persónuupplýsingum. Öryggisbrot sem leiða til þess að upplýsingar verði óaðgengilegar ber einnig að tilkynna til rekstraraðila viðkomandi tölvukerfa, RL og Sensa. GL þarf ekki að tilkynna um öryggisbrot til Persónuverndar, slíkar tilkynningar eru á ábyrgð sjóðanna.

GL ber að halda vinnsluskrá skv. lögum um Persónuvernd og gera vinnslusamninga með persónuverndarákvæðum við undirvinnsluaðila sem meðhöndla eða hafa aðgang að gögnum með persónuupplýsingum.

Önnur vinnsla persónuupplýsinga er eingöngu vegna rekstrar GL, einkum starfsmannahalds, og er óveruleg að umfangi. Ekki er um viðkvæmar upplýsingar að ræða og vinnsla þeirra er með fullri vitund einstaklinganna sem þær varða. Ekki er þörf á sérstökum ráðstöfunum vegna persónuverndar umfram þær sem tilgreindar eru í almennum öryggisráðstöfunum.

Áhættumat nettenginga og tölvubúnaðar

Netöryggi

Nettenging GL er aðgreind innan eldveggja („security zone“) á netbúnaði RL og þannig einangruð frá öðrum netum á staðnum, en netin geta þó talað hvort við annað. GL er með netþjón í hýsingu hjá Sensa og kemst að honum í gegnum einkanetstengingu RL. Svæði þetta er því aðgengilegt frá bakneti RL (hægt að sjá netþjóninn en aðgangsstillingar eru skilgreindar innan skýjavistar Sensa). Verði RL fyrir álagsárás getur það haft áhrif á bæði umhverfi.

Afritataka og varnir gagna í miðlægri vistun (skýjavist)

Skilgreining og fyrirkomulag á vörslu gagna er alfarið á ábyrgð starfsfólks GL, hvernig umsýsla og gagnavistun á sér stað, hvernig þau eru merkt og hver er með aðgang að þeim. Því er afar mikilvægt að starfsfólkið fylgi reglum um vistun gagna, þ.á.m. að vista þau aldrei í starfstölvum sínum (útstöðvum), heldur alltaf á sameiginlegu drifi hjá Sensa, skjalakerfum Festu og LSB eða eins og við á. GL óskar árlega eftir staðfestingu frá fyrrgreindum sjóðum hvort prófun hafi verið framkvæmd á endurheimt gagna.

Gögn sem eru á sameiginlegu drifi á Skýjavist Sensa eru geymd á Netapp í tveimur aðskildum og aflokuðum kerfissölum, þ.e. í Síðumúla og í gagnaveri Verne í Reykjanesbæ. Notast er við Snapmirror tækni Netapp sem tekur spegilafritun af núverandi gögnum þar sem upprunastæða er með Snapshot virkt. Þannig er hægt að rúlla gögnum aftur í tíma. Á öryggisafritunarstæðu eru Snapshot geymd til lengri tíma.

Veiruvarnir á útstöðvum er settar upp í gegnum miðlæga skýjavistunarþjónustu Sensa með fyrirfram skilgreindum reglum.

Áhættuvarnir þjónustuaðila

Sensa vinnur undir ströngum kröfum og er með alþjóðlega öryggisvottun – ISO/IEC 27001:2013 – frá British Standard Institute (BSI) fyrir stjórnkerfi upplýsingaöryggis. Gengið er út frá því að Sensa sé í stakk búin og leggi sig fram um að gæta öryggis í öllum þáttum tölvumála sem snúa að þjónustunni við GL og að ekki sé tilefni fyrir GL til að gera viðbótarráðstafanir í þeim efnum.

Innra net: Starfsfólk GL lýtur reglum Sensa um innskráningu og lykilorð.

Notendatölvur, vél- og hugbúnaður: Sensa sér um, eftir því sem við á, uppsetningu á tölvum og nauðsynlegum hugbúnaði (öðrum en Jóakim), s.s. Office-búnaði, bókhaldsforriti og vírus- og spillivarnarforritum. Starfsfólk RL veitir notendaþjónustu vegna Jóakims. Starfsfólk GL lýtur reglum Sensa og RL um innskráningu og lykilorð.

Bilanir og lagfæringar: Sensa leysir vandann, þegar kallað er eftir.

Fjarvinnsla starfsmanna

Tilhögun var byggð á ráðum Sensa og þykir ekki ástæða til að gera frekari öryggisráðstafanir vegna fjarvinnslu.

Almennar áhættuvarnir

GL stuðlar að virkri öryggisvitund starfsmanna og þjónustuaðila og gerir þeim grein fyrir að þeir séu skuldbundnir til að vernda gögn og upplýsingakerfi gegn óheimilum aðgangi, notkun, breytingum,

uppljóstrun, eyðileggingu, tapi eða flutningi.

Helstu áhættuþættir og varnir gegn skipulegri glæpastarfsemi

Álagsárás: *Mikilli netumferð er beint frá einni eða fleiri tölvum á netþjón eða netkerfi GL í þeim tilgangi að valda truflun á starfsemi eða til að fela tilraun til innbrots í kerfin.*

Gengið er út frá því að Sensa viðhafi varnir gegn slíkri ógn.

Gagnagíslataka: *Háttsemi þar sem sérstöku spilliforriti (e. ransomware) er komið inn á tölvur GL, sem dulkóðar og læsir tölvugögnum ásamt því að krafist er lausnargjalds til þess að fá gögnin aflæst og afdulkóðuð.*

Upplýsingar sem eru notaðar á skrifstofu GL eru að mestu leyti aðfengnar úr Jóakim og taka ekki breytingum í meðförum GL. Ekki verður séð að gíslataka notendatölva GL skapi teljandi vanda, því að litið er svo á að öryggi slíkra gagna sé á ábyrgð upprunastaðar og GL geti alltaf nálgast þau á nýjan leik. Lífeyrisúrskurðir sem GL útbýr fyrir þrjá lífeyrissjóði eru grundvöllur greiðslustýringa sem vistaðar eru í Jóakim og falla undir þessa lýsingu. Upplýsingar sem skráðar eru í bókhaldsforrit og Office-hugbúnað eru vistaðar miðlægt hjá Sensa og því myndi gíslataka notendatölva GL ekki skapa teljandi vanda.

Því verður ekki séð að þörf yrði á greiðslu lausnargjalds þótt notendatölvur GL yrðu teknar í gíslingu.

Hökkun: *Ólöglegt innbrot í tölvukerfi GL framið af einstaklingi sem ekki er starfsmaður.*

Hér á við það sama og lýst hefur verið um möguleg áhrif af gíslatöku. Ekki verður séð að hakkarar geti haft beinan ávinning af að brjótast inn í notendatölvur GL, en þeir gætu þó reynt að nota þær til að opna aðgang inn til Sensa eða Jóakims. Varnir gegn slíku eru á ábyrgð viðkomandi aðila.

Vefsíðurán eða skemmdarverk á vefsíðu GL: *Óheimil yfirtaka með veiru á heimasíðu eða forritum í tölvukerfi GL í þeim tilgangi að taka yfir stjórn heimasíðunnar, hökkun á vefsíðu þar sem útliti og efni vefsíðunnar er breytt.*

Vefsíðan er einföld með upplýsingum um starfsemi GL, netföng og tengla á vefsíður lífeyrissjóða sem GL þjónar. Ekki verður séð að vefsíðurán eða hökkun geti valdið miklu tjóni, en þó gætu breytingar á vefslóðum eða netföngum valdið dálitlum usla. Vefsíðan er hýst hjá Sensa og er gengið út frá því að þar séu til staðar varnir gegn ógnum sem þessum.

Auðkennisþjófnaður og stjórnendasvik: *Aðstæður þar sem upplýsingar sem starfsfólk GL býr yfir eru misnotaðar án samþykkis þess og annar aðili, einn eða fleiri, nýtir þær í sviksamlegum tilgangi. Háttsemi sem felst í því að starfsmaður framkvæmir greiðslubeiðni í þeirri röngu trú að hún stafi frá yfirstjórn hans eða starfsmanni sem hefur til þess umboð að setja fram slíka beiðni. Í beiðninni er starfsmaður til dæmis beðinn um að greiða falska reikninga, framkvæma millifærslur eða greiða fyrir vörur eða þjónustu í nafni GL.*

Fjármunahreyfingar í rekstri GL eru lágar og í föstum skorðum og er hætta á sviksemi því lítil. Framkvæmdastjóri GL er jafnframt gjaldkeri og aðrir starfsmenn hafa ekki heimild til að greiða fé af bankareikningum félagsins. Ekki er þörf á sérstökum ráðstöfunum í þessum efnum.

Veirur og spilliforrit: *Forrit sem er samið í þeim tilgangi að hafa áhrif á, skemma eða eyðileggja önnur forrit. Veiruárás er þannig afleiðing af sjálfvirku ferli sem hefst t.d. með því að starfsmaður smellir á tengil í tölvupósti eða tengil á vefsíðu.*

Veiru- og spillivarnaforrit hafa verið sett upp í tölvum starfsfólks GL. Jafnframt er lögð áhersla á að

starfsfólk sýni varúð í meðferð tölvupósts og vefsíðna.

Viðbragðsáætlanir

Fara skal árlega yfir þær varnir sem starfsfólk á að viðhafa gegn áhættuþáttum nets og tölvubúnaðar, þ.á.m. að gætt sé að því að varnarforrit séu virk og stöðugt uppfærð.

Verði starfsfólk GL áskynja um brot eða eitthvert það atferli sem skapar hættu á sviði nettenginga eða tölvuvinnslu ber að láta þjónustuaðilana, Sensa og RL, vita án tafar og kalla eftir viðbrögðum þeirra. Ef röskun verður á starfsemi GL af þessum sökum skal jafnframt upplýsa stjórnarformann GL án tafar.

Verði veruleg röskun á starfsemi GL vegna árása á netkerfi eða vinnslukerfi getur átt við sú viðbragðs-áætlun sem áður var lýst:

> *Þrautalending:* Ef ekki er unnt að ljúka mánaðarvinnslu innan lokatímamarka er unnt að láta endurtaka næstu vinnslu á undan, þ.e. að láta leggja sömu fjárhæðir inn á reikninga lífeyrisþega, til opinberra aðila o.s.frv., og láta prenta greiðsluseðla og/eða skýringarbréf til greiðsluþega, þar sem gerð er grein fyrir vandanum og að leiðrétting verði gerð um næstu mánaðamót. Að jafnaði myndi þetta valda innan við 1% fráviki á greiðslu til hvers greiðsluþega.

Viðbragðsáætlanir vegna röskunar í rekstri eða annarra frávika

Tímaskipulag:

Á hálfs árs fresti er gerð vinnuáætlun fyrir mánaðarlega vinnslu GL. Þar koma fram upphafs- og lokadagur vinnslu og jafnframt þolmörk frestunar þar sem um þrjú stig er að ræða: a) engin viðbrögð; b) annar starfsmaður vinnur verkið; c) sérstök viðbragðsáætlun.

Mánaðarleg vinnsla: a) dagur 1; b) dagur 2; c) dagur 3.

Samkvæmt þessu verður ekkert aðhafst fyrsta daginn, ef séð er að fjarvist verði ekki lengri, annars tekur annar starfsmaður strax við verkefninu eða ekki síðar en á öðrum degi. Ef ekki næst að vinna verkefnið á öðrum degi þarf að grípa til skilgreindrar viðbragðsáætlunar.

Tekjuathugun (ársfjórðungslega, um miðjan febr./maí/ág./nóv.): a) dagur 1-3; b) dagur 4-5; c) dagur 6.

Ef tekjuathugun dregst af óviðráðanlegum örsökum þá verður síðasti dagur til að framkvæma tekjuathugun 20. dagur næsta mánaðar, þ.e. hægt væri að framkvæma tekjuathugun allt að 40 dögum eftir áætlaðan tíma. Í slíkum tilvikum þarf að gæta þess að bakfæra greiðslur örorkulífeyrisþega sem fram koma í tekjuathugun hjá FYR hópi.

Sérstakar viðbragðsáætlanir:

1. Verðmæti:

Misnotkun: Tilkynna skal stjórnarformanni um málsatvik og fara að fyrirmælum hans um viðbrögð.

Tjón: Tilkynna skal tryggingafélagi ef við á og fara að fyrirmælum þess um úrbætur. Ella skal framkvæmdastjóri taka ákvörðun um úrbætur, nema áætlaður kostnaður fari yfir eina milljón króna (m.v. VNV 361,7 stig), þá skal tilkynna stjórnarformanni um málið og fara að fyrirmælum hans um úrbætur.

Bilun: Kalla skal til viðgerðarþjónustu án tafar. Verði frátöf það löng að raski starfsemi, skal leitað leiða til að leysa tímabundið úr málum, t.d. með aðkeyptri þjónustu (s.s. ljósritun).

2. Upplýsingar:

Misnotkun: Tilkynna skal stjórnarformanni um málsatvik og fara að fyrirmælum hans um viðbrögð.

Leynd, réttleiki og tiltækileiki: Gera skal stutta skýrslu um frávik og senda hana stjórnarmönnum ásamt lýsingu á ráðstöfunum sem gerðar hafa verið til að koma í veg fyrir endurtekningu eða tillögum þar að lútandi. Fara skal að fyrirmælum stjórnarformanns um frekari viðbrögð.

3. Rekstur:

Verði fjarvistir starfsmanna eða aðgengi búnaðar eða upplýsinga til þess að einstök verkefni komast á stig c) ber að hafa samband við stjórnarformann og taka ákvörðun um viðbrögð í samráði við hann.

Líkurnar á að sú staða komi upp eru það litlar, í ljósi rekstrarsögu GL um margra ára skeið, að ekki er ástæða til að skilgreina nánar hvernig bregðast skuli við í einstökum tilvikum.

Eftirlit og gæðaviðmið

GL er þjónustuaðili fyrir lífeyrissjóði og er gengið út frá því að þeir hafi hver fyrir sig eftirlit með framkvæmd og gæðum þjónustunnar.

Í upphafi annars hvers árs er gerð könnun meðal þeirra um þjónustuna og óskað ábendinga um það sem mætti betur fara.

Í kjölfarið er gerð skýrsla um árangur af rekstri GL. Fjallað er um helstu lykiltölur og markmið ásamt því að setja ný markmið fyrir komandi ár.

Stjórn GL er einnig eftirlitsaðili með starfseminni. Framkvæmdastjóra ber að veita henni árlega yfirlit um framkvæmd einstakra verkefna, þ.á m. frávik og úrbætur og um málefni áhættustýringar.

Erfitt er að setja aðra gæðamælikvarða en þá að verkefni séu unnin á réttum tíma, frávik verði sem minnst og villur sem fæstar. Reglubundin skráning frávika getur gefið vísbendingar um atriði sem setja mætti frekari gæðamarkmið.

Taflan sýnir verkefni og atriði sem halda ber skrá um. Með tímanleika er átt við að verkefni hafi lokið á réttum tíma (innan tímamarka samkvæmt ársáætlun). Með skráningu upplýsinga um umfang er unnt að gera einfaldan samanburð við fyrri keyrslur sem gæti leitt í ljós frávik í vinnslu, ef umfang eykst eða minnkar til muna án augljósrar skýringar.

Verkefni	**Umfang**	**Tímanleiki**	**Frávik**	**Úrbætur**
Mánaðarkeyrsla	Fjöldi, fjárhæðir	x	x	X
Búsetuathugun	Fjöldi, svörun, niðurfellingar	x	x	X
Nafnaskrá	Fjöldi sjóða, fjöldi nafna	x	x	X
Tekjuathugun	Fjöldi breytinga	x	x	X
Upplýsingagjöf til stjórnvalda		x	x	X
Lífeyrisúrskurðir			x	X
Almennur rekstur GL		x	x	X

Kröfur til birgja GL

Fimm birgjar sjá um veigamikla þætti fyrir GL samkvæmt (þjónustu)samningum eða í samræmi við langa viðskiptahefð:

RL hf. sér um rekstur lífeyris- og greiðslukerfisins Jóakim, þróun þess og viðhald. Þjónusta við GL felst í eftirfarandi:

a) að tryggja uppitíma kerfis

b) að þróa kerfið þannig að veigamikil verkefni verði unnin á sem skilvirkastan hátt

c) að bregðast við villum og vandkvæðum sem starfsmenn GL verða fyrir við notkun kerfisins

Enn fremur sér RL sem leigusali um sameiginlegt öryggiskerfi (innbrot, eldur o.s.frv.), brunavarnir, húsvörslu og þrif.

Sensa ehf. sér um miðlæga vistun gagna úr bókhaldskerfi og Office-hugbúnaði, svo og afritatöku, og hýsir heimasíðu GL (www.greidslustofa.is).

Umslag ehf. sér um pökkun seðla fyrir póstsendingu.

Vefurinn island.is dreifir stafrænum greiðsluseðlum og lífeyristilkynningum til lífeyrisþega.

Íslandsbanki hf. er viðskiptabanki GL og sér um millifærslur af reikningum GL vegna lífeyrisgreiðslna.

Aðrir birgjar sinna minni háttar verkefnum fyrir GL og er ekki ástæða til að fjölyrða um þeirra hlut.

Kröfur um þjónustu og viðbrögð við vanefndum:

Skrifa skal lýsingu á þeirri þjónustu sem hver af ofangreindum lykilbirgjum veitir og senda hana til viðeigandi yfirmanns og óska staðfestingar. Þar komi jafnframt fram viðmið um gæði þjónustunnar, öryggiskröfur og viðbrögð við frávikum, auk nafna mikilvægra tengla og upplýsinga um samskiptaleiðir (símanúmer, netföng o.s.frv.). Fara skal yfir skjalið á 2 ára fresti, uppfæra það ef við á og óska áréttingar birgjanna um þjónustu.

Gera skal vinnslusamninga sem uppfylla kröfur laga um persónuvernd ef birgjar teljast undirvinnsluaðilar GL í meðhöndlun persónuupplýsinga.