Persónuverndarstefna Hugvits

1. TILGANGUR

Það er óhjákvæmilegt að í rekstri eins og þeim sem Hugvit stundar, afli félagið ýmisskonar upplýsinga. Þær upplýsingar varða í sumum tilvikum einstaklinga og geta verið persónugreinanlegar og þannig rekjanlegar til þeirra. Hugvit leggur áherslu á að safna einingis þeim upplýsingum sem þörf er á í rekstri og samkvæmt lagaheimildum, á gagnsæjan hátt, með virðingu fyrir réttindum einstaklinganna sem þær varða. Í þeim tilvikum sem það á við verður leitað samþykkis þeirra seinstaklinga sem upplýsingar varða. Hugviti er umhugað um persónuvernd og er tilgangur þessarar Persónuverndarstefnu að stuðla að því að farið sé með persónuupplýsingar starfsmanna, viðskiptamanna og annarra hagsmunaaðila af virðingu og að eftir föngum sé gætt trúnaðar við meðferð þeirra. Stefnunni er ætlað að skýra; i) hvaða persónuupplýsingum Hugvit safnar, ii) í hvaða tilgangi, iii) hvernig þær eru notaðar, iv) til hvaða ráðstafana Hugvit grípur til að stuðla að öryggi þeirra og vernd, og v) hvaða réttinda skráðir einstaklingar kunna að njóta. Meginmarkmið stefnunnar er að vinnsla persónuupplýsinga taki mið af grunnreglum þeim sem lýst er í 4. gr.

Í þessari persónuverndarstefnu verður einnig vísað til Hugvits sem „**við**“, „**okkur**“, „**okkar**“, eða „**félagsins**.“

2. AFMÖRKUN ÞEIRRA UPPLÝSINGA SEM HEYRA UNDIR ÞESSA STEFNU.

2.1. Þegar við erum ábyrgðaraðili:

Í tengslum við starfsemi sína, þá þjónustu sem við veitum og vöru sem félagið selur, fáum við og Eignatengd Félög, aðgang að ýmsum gögnum og upplýsingum. Þar á meðal eru upplýsingar um einstaklinga sem talist geta persónuupplýsingar. Þessi persónuverndarstefna á við um þær upplýsingar.

2.2. Þegar við erum vinnsluaðili:

Í öðrum tilvikum gætu upplýsingar um einstaklinga verið vistaðar í kerfum okkar, og þannig tæknilega í vörslum félagsins, án þess að við söfnum þeim upplýsingum eða ákvörðum tilgang og aðferðir við vinnslu þeirra. Það á til að mynda við um upplýsingar og gögn sem viðskiptavinir okkar færa inn í kerfi sín sem vistuð eru eða hýst hjá okkur, og þegar upplýsingar og gögn eru færð eru inn í þau kerfi af aðilum sem viðskiptavinir okkar veita sjálfir aðgang að kerfunum. Í þeim tilvikum erum við ekki ábyrgðaraðili upplýsinganna, en kunnum að teljast vinnsluaðili þeirra. Um þær upplýsingar gildir vinnslusamningur okkar og viðkomandi viðskiptavina. Þessi stefna verður þó höfð til hliðsjónar eftir því sem við á til að stuðla að sem ríkastri vernd persónuupplýsinga.

2.3. Þegar hugbúnaður og þjónusta okkar er notaður við vinnslu annarra:

Í þeim tilvikum sem hugbúnaður og lausnir okkar eru settar upp, keyrðar og vistaðar hjá viðskiptavinum okkar erum við hvorki vinnsluaðili né ábyrgðaraðili vegna upplýsinga sem safnað er og unnar eru með hugbúnaðinum.

3. SKILGREININGAR:

„**Gagnaöryggiskerfi**“ vísar til Upplýsingaröryggistefnu okkar og þess gagnaöryggiskerfis sem er gildandi fyrir fyrirtækið á hverjum tíma. Við leggkum mikið kapp á að þróa stöðugt og útfæra öryggisráðstafanir okkar og að stuðla að upplýsingaöryggi og vandaðri og tryggri meðferð viðkvæmra upplýsinga. Markmiðið er að hámarka upplýsingaöryggi innan þeirra marka að hugbúnaðarlausnir okkar séu hagkvæmar í rekstri og á sanngjörnu verði. Stefna okkar er að gagnaöryggiskerfi okkar taki til lykilþátta í starsemi félagsins; þróunar hugbúnaðar, veitingu upplýsingatækniþjónustu, ráðgjafar, hýsingar og verkstjórnar. Við þróun og innleiðingu gagnaöryggiskerfis munum við leitast við að fylgja þeim viðurkenndu stöðlum og verklagi sem best á við á hverjum tima. Lýsingu á Gagnaöryggiskerfi (og Gaganöryggistefnu okkar) sem er í gildi má á heimasíðu okkar.

„**Persónuverndarlöggjöf**“ merkir íslensk lög og reglugerðir um vernd persónuupplýsinga sem í gildi eru á hverjum tíma, og eftir því sem við á, löggjöf Evrópusambandsins um vernd persónuupplýsinga, einkum GDPR (reglugerð Evrópuþingsins og Ráðsins (ESB) 2016/679). Þegar það á við samhengisins vegna, tekur hugtakið einnig til annarra laga og stjórnvaldsreglna sem mæla fyrir um meðferð, varðveislu á, geymsluskyldu á, afhendingarskyldu á, eða upplýsingaskyldu um persónuupplýsingar og gögn sem hafa að geyma slíkar upplýsingar.

„**Eignatengt Félag**“ (og Eignartengd Félög) tiltekins aðila, vísar til lögaðila sem, beint eða óbeint, á eða stýrir þeim aðila, heyrir undir eignarhald eða lýtur stjórn þess aðila, eða er undir sameiginlegri stjórn eða eignarhaldi þess aðila ásamt öðrum. Í þessu samhengi vísar „stjórn“ til valds til þess að hafa áhrif á rekstur eða málefni lögaðili og „eignarhald“ vísar til raunverulegrar eignar á 50% (eða, ef viðkomandi lögsaga heimilar ekki meirihlutaeign, það hámark sem heimilað er samkvæmt lögum þeirrar lögsögu) eða hærra hlutfalls af atkvæðisberandi hlutabréfum eða sambærilegum réttindum í viðkomandi lögaðila. Upplýsingar um öll félög sem eru eignartengd okkur má nálgast á vefsíðu okkar.

„**Viðkvæmar upplýsingar**“ eru persónuupplýsingar sem sem eru í eðli sínu sérlega viðkvæmar af því að þær varðar grundvallarréttindi og mannfrelsi, eiga að njóta sérstakrar verndar, eða af því að vinnsla þeirra gæti leitt af

	sér hættu fyrir grundvallarréttindi og mannfrelsi þeirra sem þær varða. Sem dæmi má nefna persónuupplýsingar um kynþætti, uppruna, stjórnmálaskoðanir, trúarskoðanir, heilsufarsupplýsingar, kynhneigð og áþekk málefni.
„**Öryggisfrávik**“	Merkir bæði i) að upplýsingaöryggisviðburður (e. Information security event) eigi sér stað sem felur í sér að öryggi gagnaöryggiskerfis okkar hefur rofnað eða að ferlum þess hefur ekki verið fylgt (eins og nánar er gerð grein fyrir í gagnaöryggiskerfinu), og ii) öryggisbrest við meðferð persónuupplýsinga, eins og það hugtak er skýrt í Persónuverndarlöggjöf.

Hugtökin, „**Skráður Einstaklingur**“, „**Aðildarríki**“, „**persónuupplýsingar**“, „**Vinnsla**“ og „**Eftirlitsvald**“ skulu hafa sömu merkingar og skilgreindar eru í Persónuverndarlöggjöf.

4. GRUNNREGLUR UM VINNSLU PERSÓNUUPLÝSINGA

Við vinnslu persónuupplýsinga munum við eins og kostur er gæta að eftirfarandi meginreglum. Þær eru einnig hafðar til hliðsjónar við skýringu og túlkun annarra hluta þessarar Persónuverndarstefnu.

4.1. Upplýsingum er safnað á grundvelli lögmætrar heimildar og þær unnar á sanngjarnan og gagnsæjan hátt.

4.2. Upplýsingum er safnað í lögmætum tilgangi og þær aðeins unnar í tengslum við þann tilgang og/eða samkvæmt fyrirmælum í lögum eða vegna skjalavistunar sem er samrýmanleg þeim tilgangi.

4.3. Persónuupplýsingar eiga að vera réttar, nákvæmar, nægjanlegar og viðeigandi fyrir vinnslu. Eftir því sem unnt er að ganga úr skugga um réttmæti og nákvæmni upplýsinga með eðlilegum ráðstöfunum er það gert.

4.4. Ekki er safnað umfangsmeiri persónuupplýsingum en þörf er á til að ná fram tilganginum með vinnslu þeirra.

4.5. Persónuupplýsingar eru ekki varðveittar lengur en þörf er á til að ná fram tilganginum með vinnslu þeirra, eða samkvæmt fyrirmælum í lögum eða vegna skjalavistunar sem er samrýmanleg þeim tilgangi.

4.6. Gætt er trúnaðar um persónuupplýsingar og stuðlað að öryggi þeirra með tæknilegum og skipulagslegum ráðstöfunum sem eru viðeigandi með hliðsjón af nýjustu tækni, kostnaði við framkvæmd og eðli, umfangi, samhengi og tilgangi vinnslunnar.

5. TILGANGUR SÖFNUNAR PERSÓNUUPPLÝSINGA OG TIL HVERS ÞÆR ERU NOTAÐAR

5.1. Hvenær er persónuupplýsingum safnað.

Tilgangur söfnunar persónuupplýsingar er mismunandi eftir flokkum og tegundum upplýsinga. Við öflum til að mynda persónuupplýsinga um starfsmenn til að efna réttilega samningsskyldur sem leiða af ráðningarsambandi við þá. Við kunnum að afla, eða vera látnar í té, persónuupplýsingar um tengiliði og starfsmenn viðskiptavina okkar, eða væntanlega viðskiptavini, í tegnslum við veitingu þjónustu eða í þeim tilgangi að koma á samningi. Við gætum einnig safnað tilteknum persónuupplýsingum vegna fyrirspurna sem berast, í tengslum við notkun vefsíða okkar eða önnur kerfi og hugbúnað okkar.

5.2. Heimildir til vinnslu persónuupplýsinga

Við munum aðeins safna persónuupplýsingum og vinna með þær í samræmi við lög. Öll söfnun persónuupplýsinga mun byggja á einhverri eftirtalinna heimilda:

Upplýstu samþykki Þegar vinnsla byggir á upplýstu samþykki skal engin söfnun upplýsinga fara fram fyrr en það samþykki liggur fyrir á fullnægjandi formi.

Samningi Ef vinnsla persónuupplýsinga grundvallast á samningi sem gerður hefur verið, eða er liður í að koma á samningi, skal þess gætt að vinnslan sé í eðlilegu samhengi við framkvæmd samningsins eða aðgerðir við að koma honum á.

Lagaskyldu Ef vinnsla persónuupplýsinga er byggð á lagaskyldu sem hvílir á okkur, eða fyrirmælum stjórnvalda til okkar, skal meðalhófs gætt eftir því sem unnt er og hinn skráði einstaklingur upplýstur um eðli og umfang vinnslunnar, fari það ekki gegn tilgangi hennar eða lagaboði.

Nauðsyn Ef tilgangur vinnslu persónuupplýsinga er að vernda mikilvæga hagsmuni hins skráða, eða lögmæta hagsmuni okkar eða þriðja aðila, skal umfang vinnslunnar takmarkast við það sem nauðsynlegt er og þess gætt að hinn skráði einstaklingur sé upplýstur eftir föngum um vinnsluna, tilefni hennar, umfang hennar og um rétt sinn að öðru leyti.

5.3. Við nýtum persónuupplýsingar í eftirtöldum tilgangi

a) **Til að efna samningsskyldur**. Þetta á t.d. við um launavinnslu og aðrar greiðslur til starfsmanna og verktaka og annars konar umbun og stuðning við þá. Þetta á einnig við um nýtingu upplýsinga til að eiga ýmis reglubundin samskipti við tengiliði viðskiptamanna.

b) **Til að veita þjónustu, bæta** hana **og þróa** frekar. Þetta gæti til að mynda átt við um ýmsar upplýsingar og fyrirspurnir sem berast um þjónustu okkar og kerfi, tíðni og tegund tiltekinna aðgerða og sambærilegar upplýsingar. Yfirleitt eru slíkar upplýsingar ekki persónugreinanlegar og sjaldnast tengdar einstaklingum, þó að það sé ekki útilokað.

c) **Til að tryggja vistun á samskiptaferlum** og auðvelda úralausn fyrirspurna og þjónustubeiðna.

d) Upplýsingar úr fótsporum (e. cookies) eru nýttar **til að bæta virkni** vefsíðna og til að gera upplifun notenda persónulegri og þægilegri.

e) Persónuupplýsingar kunna að vera notaðar í þágu þess sem þær varða til að **auðvelda** honum **notkun kerfa** okkar, t.d. með því að ákveðin skjöl, eða reitir skjala, geymi sjálfkrafa forskráðar upplýsingar.

f) **Í viðskiptatilgangi**, svo sem til að aðstoða við stefnumótun, áætlanagerð, vöruþróun, markaðsrýni, til að bæta þjónustu, bera kennsl á notkunarmynstur, meta skilvirkni o.s.frv.

g) Eftir því sem við teljum nauðsynlegt **til að fara eftir og fylgja lagalegum ferlum og fyrirmælum** eða beiðnum frá opinberum aðilum.

h) Eftir því sem við teljum nauðsynlegt **til að vernda starfsemi** okkar.

Við nýtum ekki persónuupplýsingar í öðrum tilgangi nema með sérstöku samþykki þess sem þær varða.

5.4. Hvernig og hvenær er persónuupplýsingum deilt

Við deilum persónuupplýsingum almennt ekki. Þó getur komið til þess að þeim sé deilt í samræmi við eftirfarandi:

a) til Eignatengdra Félaga í þeim tilgangi sem lýst er í þessari Persónuverndarstefnu.

b) til þjónustuveitenda sem teljast til þriðju aðila í tengslum við tilganga sem lýst er í þessari Persónuverndarstefnu, svo sem við hýsingu, meðhöndlun greiðslna, endurskoðun eða annað sem okkur er þörf á til að veita þjónustu okkar.

c) Eins og við teljum nauðsynlegt til að: (a) fylgja boði laga og stjórnvaldsreglna, (b) svara beiðnum frá opinberum yfirvöldum, (c) framfylgja viðskiptaskilmálum í tilteknu tilviki, og (d) til að vernda starfsemi, réttindi og öryggi félagsins, starfmanna og viðskiptavina.

d) Í öðrum tilgangi að fengnu leyfi frá þeim sem persónuupplýsingarnar varða.

e) Ef félagið eða Eignatengd Félög taka þátt í endurskipulagningu, samruna, sölu, eða svipuðum ferli, mun persónuupplýsingum deilt ef þörf krefur, en eftir sem áður verður trúnaður um þær tryggður.

5.5. Flutningur yfir landamæri

Við miðlum ekki persónuupplýsingum til þriðju landa eða alþjóðastofnana utan Evrópska Efnahagssvæðisins, nema slíka miðlun sé skylda samkvæmt lögum eða fyrirmælum dómstóls eða stjórnvalds sem hefur lögsögu og vald til að kveða á um slíka miðlun. Komi til þess að við hyggjumst breyta þeirri stefnu verður Skráðum Einstaklingum tilkynnt það fyrirfram. Við munum ekki miðla upplýsingum utan Evrópska Efnahagssvæðisins nema að fyrir liggi samningur um miðlunina og vinnsluna sem uppfyllir skilyrði Persónuverndarlöggjafarinnar og binandi fyrirtækjareglur sem tryggja öryggi persónuupplýsinga.

Að því marki sem Persónuverndarlög kunna að leyfa og eftir að öll viðeigandi skilyrði um geymslu og/eða flutning á persónuupplýsingum hafa verið uppfyllt, gætum komið til þess að við kjósum að vista eða vinna með einhverjar persónuupplýsingar í öðrum Aðildarríkjum þar sem félagið hefur aðstöðu

6. RÉTTINDI SKRÁÐRA EINSTAKLINGA

Upplýsingaréttur Skráðir Einstaklingar hafa rétt á að vita um hvort persónuupplýsingum um þá er safnað af okkur og hvernig unnið er með þær. Skráðir einstaklingar hafa ennfremur rétt á upplýsingum um tilgang vinnslunnar, hverjir hafa aðgang að upplýsingunum, hversu lengi upplýsingarnar verða vistaðar (eða eftir hvaða viðmiðum vistunartíminn er ákveðinn) og hvaðan upplýsingarnar eru ættaðar.

Réttur til leiðréttingar Skráðir Einstaklingar hafa rétt á að láta leiðrétta ónákvæmar eða rangar persónuupplýsingar um sig og, að teknu tilliti til tilgangs vinnslunnar, að veita fyllri upplýsingar þegar fyrirliggjandi persónuupplýsingar eru ófullnægjandi.

Réttur til eyðingar og vinnslutakmörkunar

Skráðir Einstaklingar hafa rétt á að fara fram á að persónuupplýsingum sé eytt eða að við takmörkum vinnslu á þeim, þegar lagaskilyrði fyrir því eru uppfyllt.

Réttur til að færa gögn Skráður Einstaklingur hefur rétt á að fá persónuupplýsingar sem varðar hann á aðgengilegu sniði og til að fara með þær sem honum sýnist, þegar lagaskilyrði þess eru uppfyllt.

7. AÐGERÐIR TIL AÐ STUÐLA AÐ LÖGMÆTRI VINNSLU OG NÁKVÆMNI PERSÓNUUPPLÝSINGA

7.1. Aðgerðir útfærðar í Upplýsingaöryggiskerfi okkar

Við útfærum helstu aðgerðir vegna vinnslu persónuupplýsinga í Gaganöryggiskerfi okkar, með það að leiðarljósi að aðgerðir upplýsingaöryggis og Persónuverndar séu samþættar og myndi heildstætt viðbragðs- og eftirlitskerfi.

7.2. Tilkynningar til Skráðra einstaklinga

Við munum, eftir því sem við á og fer saman við tilgang vinnslunnar og heimild til hennar, gera skráðum einstakling viðvart um að persónuupplýsingum um hann sé safnað og þær unnar. Form tilkynninga fer eftir eðli hvers tilviks. Starfsmenn eru til að mynda upplýstir um vinnslu persónuupplýsinga um þá í ráðningarsamningum, auk þess sem vinnsla þeirra leiðir af eðli ráðningarsambandsins og gildandi löggjöf, svo sem um bókhald, og gildandi kjarasamningum.

7.3. Upplýst samþykki

Þegar söfnun og vinnsla persónuupplýsinga er ekki byggð á beiðni skráðs einstaklings, grundvölluð á samningi við hann, nauðsynleg til að uppfylla lagaskyldu, eða nauðsynleg vegna lögmætra hagsmuna, munum við afla upplýsts samþykkis hins skráða einstaklings. Við munum gera þeim sem láta félaginu í té upplýst samþykki

grein fyrir því að þeir geti hvenær sem er afturkallað samþykki sitt. Skráðum einstakling skal um leið bent á þau réttindi sem hann nýtur á grundvelli þessarar Persónuverndarstefnu og Persónuverndarlöggjafar.

7.4. Nákvæmni og leiðréttingar

Þegar persónuupplýsingum er safnað skal þess ávallt gætt eins og kostur er að þær upplýsingar sem eru skráðar séu réttar og nákvæmar. Þegar skráður einstaklingur óskar þess skulu ónákvæmar persónuupplýsingar leiðréttar án ástæðulauss dráttar. Þegar það fer saman við tilgang vinnslunnar skal skráður einstaklingur hafa rétt á að óska þess að ófullgerðar persónuupplýsingar séu útfærðar nánar.

Ef það reynist unnt eru upplýsingar uppfærðar þegar ástæða er til. Ef upplýsingar reynast rangar eða óáreiðanlegar verður þeim eytt eftir að þær hafa verið leiðréttar.

Ef upplýsingum hefur verið deilt áður en þær eru leiðréttar eða þeim eytt, skal tilkynna það þeim sem móttekið hafa þær, nema það feli í sér óhóflega fyrirhöfn.

Aðeins þeir starfsmenn sem þurfa það starfs síns vegna og í samræmi við tilgang vinnslu skulu hafa aðgang að persónuupplýsingum. Þess er gætt að aðrir hafi ekki kost á að breyta persónuupplýsingum, eyða þeim eða vinna þær á annan hátt.

7.5. Vinnsla í samræmi við tilgang

Þess er gætt að þegar ákvarðanir eru teknar um hverjir fá aðgang að persónuupplýsingum og hvernig er unnið með þær, sé höfð hliðsjón af tilganginum að baki söfnun upplýsinganna og að meðferð þeirra sé í eðlilegu samhengi við þann tilgang.

8. ÖRYGGI PERSÓNUUPPLÝSINGA

Engir gagnaflutningar eru fullkomlega öryggir og engar gagnageymslur eru fullkomlega öruggar. Við leitumst við að vernda persónuupplýsingar eins og unnt er og leggjum mikinn metnað í ráðstafanir til að ná því markmiði. Beitt er raunhæfum, rekstrarlegum, tæknilegum og stjórnunalegum ráðstöfunum og er þær reglulega yfirfarnar og uppfærðar, með tilliti til öryggis og hagkvæmni. Þau atriði sem vikið er að hér eru mörg hluti af Gaganöryggiskerfi okkar og er lýst fjallað nánar um þau þar.

8.1. Skipulagslegar og rekstrarlegar ráðstafanir til að stuðla að öryggi persónuupplýsinga

Gagnaöryggiskerfi okkar. Við útfærum aðgerðir vegna rekstrarlegara ráðstafana í Gaganöryggiskerfi okkar, með það að leiðarljósi að aðgerðir upplýsingaöryggis og Persónuverndar séu samþættar og myndi heildstætt viðbragðs- og eftirlitskerfi. Þessar aðgerðir taka meðal annars á þeim þáttum sem lýst er í þessari grein 8.1.

a) **Þjálfun og fyrirtækjamenning.** Starfsmönnum okkar eru kynntar stefnur félagsins í upplýsingaöryggismálum og persónuvernd og þeir fá þá fræðslu og þjálfun í þeim

efnum sem er viðeigandi miðað við stöðu þeirra og ábyrgð. Áhersla er lögð á að fyfirtækjamenning okkar endurspegli meðvitund um nauðsyn þess að ábyrgð, trúnaður og varkárni sé ávallt sýnd í meðferð allrar upplýsinga. Þjálfun og upplýsingagjöf til starfsmanna félagsins er skráð og reglulega yfirfarið hvort þörf sé á viðbótar þjálfun eða kynningum. Starfsmenn okkar, ráðgjafar og aðrir sem fá aðgang að persónuupplýsingum eru bundnir samningsbundnum trúnaðarskyldum. Þeir starfsmenn sem vinna að verkefnum sem tengjast upplýsingum sem háðar eru auknum trúnaði á grundvelli sérlaga, eða samkvæmt eðli verksins, undirrita sérstakar trúnaðaryfirlýsingar vegna þeirra verka

b) **Örugg svæði.** Skrifstofuaðstaða okkar er skilgreind sem öruggt svæði. Öllum hurðum að skrifstofuaðstöðunni er læst og aðkoma að henni varin af öryggiskerfi. Aðeins starfsmenn hafa lykla og aðgangskóða. Viðskiptavinir, ráðgjafar og aðrir gestir fá aðeins aðgang að skrifstofuaðstöðunni í fylgd með starfsmanni ber ábyrgð á viðkomandi á meðan hann er á svæðinu og skráir nafn hans, komutíma og brottfarartíma. Gestir eru auðkenndir með öryggispassa.

c) **Skrifborð og skjáir.** Ef starfsmaður yfirgefur vinnustöð gætir hann þess að persónuupplýsingar séu ekki sjáanlegar á yfirborði vinnustöðvar eða á skjá tölvu sinnar. Tölvur og önnur tæki með skjá eru stillt til að fara sjálfkrafa á læsta skjáhvílu ef ekki er unnið við þau um lengra skeið.

d) **Eyðing, förgun og vörslutími.** Áður en pappír, harðir diskar og aðrir geymslumiðlar og búnaður sem hefur að geyma persónuupplýsingar, er fargað, hann seldur, hann endurnýttur, eða honum fleygt, skal þess gætt að öllum persónuupplýsingum sé fyrst eytt.

e) **Fjarvinna og vinna á eigin tækjum.** Starfsmenn sem vinna með persónnuupplýsingar í fjarvinnu, á fartölvu, í snjallsímum, flytja þær á minnisyklum eða með öðrum sambærilegum hætti, eru upplýstir um að persónuupplýsingar má aðeins flytja af starfssvæði okkar ef það er gert í samræmi við Gaganöryggiskerfi félagsins. Starfsmenn eru meðvitaðir um að sérstakrar varfærni þarf að gæta þegar fjarvinnslutæki eru notuð utan starfssvæðisins, sérstaklega á almenningsstöðum. Starfsmönnum okkar er heimilt, að fengnu samþykki og í samræmi við Gagnaöryggiskerfi félagsins, að vinna á eigin tækjum. Öll gögn og allar upplýsingar sem vistaðar eru, fluttar um eða unnið með á eigin tæki eru áfram, öllum stundum, í eigu okkar og við höfum fulla stjórn og ráðstöfunarrétt yfir þeim. Aðeins er veitt heimild til notkunar á eigin tækjum ef þau hafa nauðsynlega tæknilega eiginleika til að öryggi gagna og persónuupplýsinga sé fullnægjandi.

8.2. Tæknilegar aðgerðir til verndar og til að stuðla að öryggi persónuupplýsinga

Gagnaöryggiskerfi okkar. Við útfærum aðgerðir vegna tæknilegra ráðstafana í Gagnaöryggiskerfi okkar, með það að leiðarljósi að aðgerðir upplýsingaöryggis og Persónuverndar séu samþættar og myndi heildstætt viðbragðs- og eftirlitskerfi. Þessar aðgerðir taka meðal annars á þeim þáttum sem lýst er í þessari grein 8.2.

a) **Aðgangsstýringar.** Aðgangi að kerfum, vefgáttum og gagnagrunnum í eigu okkar er almennt stýrt og þau læst nema það sé augsýnilega óþarft. Aðgangskóðar eru aðeins veittir þeim sem hafa þörf fyrir þá vegna starfa síns. Skrár eru haldnar yfir hvaða starfsmenn hafa aðgang að hvaða kerfum, vefgáttum og gagnagrunnum.

a) **Lykilorð.** Starfsmönnum er ekki er heimilt að láta öðrum í té lykilorð sín. Óheimilt er að deila lykilorðum í gegnum nokkurn miðil. Sé uppi grunur um að lykilorð hafi orðið aðgengilegt öðrum en notanda þess skal því breytt án tafar.

b) **Afritunarstefna**. Afritunarstefna okkar er útfærð í gagnaöryggiskerfinu.

c) **Vörslustefna**. Vörslustefna okkar er útfærð í gagnaöryggiskerfinu.

8.3. Viðbrögð við öryggisfrávikum

Komi upp öryggisfrávik er fylgt skýrum verkeferlum. Verkferlar vegna öryggisfrávika eru reglulega endurskoðaðir til að stuðla að skilvirkum og skjótum viðbrögðum.

Öryggisfrávik geta falið í sér; 1) að trúnaður um gögn rofni, með þeim hætti að óheimil miðlun eigi sér stað eða óviðkomandi fái aðgang að gögnum, 2) að upplýsingar verði óaðgengilegar, og 3) að persónuupplýsingum sé breytt.

Komi upp öryggisfrávik fylgjum við Gagnaöryggiskerfi okkar og grípum án tafar til ráðstafana sem eru eðlilegar að umfangi til að rannsaka, lágmarka tjón og lagfæra frávikið. Við höfum á hverjum tíma í gildi nákvæmt ferli um aðgerðaskráningar og meðferð mála sem snerta Öryggisfrávik sem upp geta komið. Aðgerðaráætlanir okkar eru meðal þeirra þátta sem falla undir Gaganöryggiskerfið og eru teknir út með reglubundnum hætti af óháðum úttektaraðila.

Komi upp öryggisfrávik tilkynnum við viðeigandi Eftirlitsvaldi um það án ótilhlíðilegrar tafar eftir að við verðum vör við frávikið, nema þá aðeins að það sé ólíklegt að frávikið leiði til hættu fyrir réttindi og frelsi skráðra einstaklinga. Fylgt er föstu verklagi og notast við skýrt mótuð tilkynningarform.

Ef öryggisfrávik leiðir til mikillar hættu fyrir réttindi og frelsi skráðs einstaklings tilkynnum við honum um það, nema viðeigandi ráðstafanir hafi verið gerðar sem útiloka hættuna. Fylgt er föstu verklagi og notast við skýrt mótuð tilkynningarform.

9. ALMENNT

9.1. Persónuverndarstefna þessi kann að taka breytingum. Reynist fyrirhugaðar breytingarnar veigamiklar verða þær kynntar sérstaklega. Aðrar breytingar verða uppfærðar á vefsíðu okkar.