



Upplýsingaöryggisstefna fyrir Hjallastefnuna

Hjallastefnan hagnýtir upplýsingatækni og upplýsingakerfi við varðveislu gagna og miðlun þeirra á sem hagkvæmastan hátt. Upplýsingakerfi Hjallastefnunnar innihalda persónugreinanlegar upplýsingar sem ekki má nota í öðrum tilgangi en vegna starfsemi Hjallastefnunnar og Hjallastefnuskóla. Trúverðugleiki og hagsmunir aðila, sem tengjast málum er upplýsingarnar varða, gætu skaðast ef upplýsingarnar eru ónákvæmar, komast í rangar hendur eða eru ekki aðgengilegar þegar þeirra er þörf.

Afleiðingar þess að fyllsta öryggis sé ekki gætt gætu m.a. orðið eftirfarandi:

- Persónugreinanleg gögn s.s. upplýsingar um nemendur, geta komist í hendur óviðkomandi aðila
- Nauðsynleg gögn um nemendur, nemendaferil, einkunnir o.fl. geta glatast
- Upplýsingar um starfssfólk geta komist í hendur óviðkomandi aðila
- Upplýsingar um foreldra og/eða forráðamenn geta komist í hendur óviðkomandi aðila

Hjallastefnan leggur áherslu á mikilvægi meðferðar upplýsinga og upplýsingakerfa, þ.e.a.s. upplýsingaöryggi í heild sinni. Í allri starfsemi sinni hefur Hjallastefnan því sett sér stefnu og skilgreint formlegt verklag vegna vinnu starfsmanna og þjónustuaðila við gögn og kerfi fyrirtækisins. Öryggisstefnan nær til umgengni og vistunar allra gagna sem eru í vörslu hjá Hjallastefnunni og skólum fyrirtækisins sem og samstarfs- og þjónustuaðila, hvort sem þær eru á rafrænu formi, prentuðu eða í mæltu máli. Þannig einsetur Hjallastefnan sér að verja upplýsingar gegn innri og ytri ógn hvort sem þær eru vísitandi eða óviljandi.

Markmið með útfærslu og innleiðingu öryggiskerfis Hjallastefnunnar er að tryggja, ef skaði verður, áframhaldandi rekstur og lágmarka tjón með því að koma í veg fyrir eða lágmarka áhrif af atvikum sem geta truflað rekstur og þjónustu.

Stjórnendur sjá til þess að öryggisstefna Hjallastefnunnar sé endurskoðuð reglulega með formlegum hætti. Við þá endurskoðun er sú hætta sem steðjað getur að þeim upplýsingakerfum sem eru í notkun og innihalda persónuupplýsingar, sem og öðrum kerfum er tengjast þeim, endurmetin. Í kjölfar slíks endurmats og endurskoðunar er öryggisstefnan uppfærð og samþykkt formlega, auk þess sem stefnan og hugsanlegar breytingar á henni eru kynnt starfssfólki og samstarfsaðilum. Því er öryggisstefna Hjallastefnunnar byggð upp með tilliti til trúnaðar og réttleika og tiltækileika gagna.





Trúnaður:

Hjallastefnan mun útfæra öryggiskerfi sín á þann veg að sem minnstar líkur séu á að því að utanaðkomandi aðilar fái aðgang að upplýsingum í heimildarleysi, þ.e. tryggja á sem bestan máta að einungis þeir aðilar sem til þess hafa heimild, hafi aðgang að upplýsingum.

Réttleiki gagna:

Hjallastefnan vill tryggja að upplýsingar sem skráðar eru hjá fyrirtækinu og skólum þess á hverjum tíma, séu réttar og nákvæmlega skráðar. Að ónákvæmar, villandi, rangar eða úreltar upplýsingar séu leiðréttar, þeim eytt eða við þær aukið þegar slíkt uppgötvast og haldið verði uppi reglubundnu eftirliti í þeim tilgangi.

Aðgengi gagna:

Hjallastefnan vill tryggja að upplýsingar sem skráðar eru í upplýsingakerfum fyrirtækisins séu aðgengilegar, þeim sem hafa heimild til notkunar á kerfunum, þegar þeirra er þörf. Jafnframt að kerfi og gögn sem kunna að eyðileggjast sé hægt að endurheimta með hjálp neyðaráætlunar og afrita sem geymd eru á öruggum stað. Til að uppfylla trúnað, réttleika og tiltækileika gagna tryggir Hjallastefnan að aðgangsheimildum notenda sé stýrt á formlegan og rekjanlegan hátt m.a. til að komast hjá sviksemi.

Hjallastefnan hefur skilgreint almenna öryggisþætti sem skýra ábyrgð aðila, markmið og tilgang stefnunnar sem og umfang hennar. Að auki hefur fyrirtækið skilgreint öryggisreglur og sértæka öryggisþætti er lýsa nánar þeim öryggiskröfum sem Hjallastefnan hyggst mæta í öllum rekstri sínum. Þær sértæku öryggiskröfur ná m.a. til neðangreindra þátta:

- Neyðarstjórnun og öryggisfrávik
- Staðlar, lög og reglugerðir
- Hugbúnaður
- Skipulagning og samþykki kerfa
- Útvistun
- Trúnaðarheit
- Meðferð búnaðar
- Aðgangöryggi
- Gagnaöryggi – leynd og réttleiki gagna
- Vernd gegn spillihugbúnaði
- Neyðaráætlanir
- Rekstraröryggi
- Viðbrögð við öryggisfrávikum
- Verklagsreglur
- Fræðsla
- Snjallsímar og spjaldtölvur
- Förgun búnaðar og miðla
- Handbók um öryggismál
- Endurskoðun, áhættumat og innra eftirlit

Öryggisstefna verður endurskoðuð reglulega með formlegum hætti. Endurmeta skal þá hættu sem steðjað getur að þeim upplýsingakerfum sem eru í notkun hjá fyrirtækinu og innihalda persónuupplýsingar, sem og öðrum kerfum og gagnasöfnum sem tengjast þeim. Í kjölfar slíks





Hjallastefnan

endurmats og endurskoðunar skal uppfæra öryggisstefnu þessa og samþykkja formlega, auk þess sem stefnan og breytingar sem á henni kunna að vera gerðar, sé kynnt starfsfólki og samstarfsaðilum.

Lög og reglur:

Öryggisstefna þessi tekur mið af lögum og reglugerðum um persónuvernd og meðferð persónuupplýsinga (sjá lög nr. 90/2018) og af öryggisstaðlinum ÍST 27001:2016. Öryggisstefnan er í fullu samræmi við reglur Persónuverndar nr. 299/2001 um öryggi persónuupplýsinga.

Starfsmenn sem hafa aðgang að upplýsingum, sem og þeir samstarfsaðilar skólans sem koma að rekstri upplýsingakerfa skólans, skulu hafa aðgang að og þekkja til öryggisstefnu þessarar, ferla, reglna og handbókar um öryggi gagna sem snertir vinnu þeirra.

Um meðferð og viðbrögð við brotum á reglum þessum er vísað til laga sem og verk- og kjarasamninga.

Undir öryggisstefnu rita stjórn og framkvæmdastjóri skólans.

Þannig staðfest af stjórn Hjallastefnunnar 23. maí 2019

Stjórnarformaður

Framkvæmdastjóri

