

Upplýsingaöryggisstefna Framhaldsskólans á Laugum

1. Upplýsingaöryggisstefna Framhaldsskólans á Laugum

1. Tilgangur

Upplýsingaöryggisstefna Framhaldsskólans á Laugum lýsir áherslum skólans á verndun og meðferð gagna/upplýsinga í vörslu og eigu skólans. Verja þarf þær upplýsingar sem skólinn varðveitir fyrir öllum ógnum, innri og ytri, af ásetningi, gáleysi eða slysi. Innleiðing og framkvæmd stefnunnar er grundvöllur að faglegum vinnubrögðum og er mikilvæg til að fullvissa starfsmenn og notendur þjónustu skólans, um heilindi og rétt vinnubrögð.

2. Umfang

Upplýsingaöryggisstefnan tekur til allra gagna/upplýsinga, í hvaða formi sem þau/þær eru og hvar sem þau/þær eru vistuð. Sérstök áhersla er lögð á:

- Gögn/upplýsingar frá notendum þjónustu skólans, t.d. prófaupplýsingar og upplýsingar um fjármál.
- Persónulegar upplýsingar sem tengjast starfsmönnum skólans.

Upplýsingaöryggisstefnan tekur jafnframt til þess húsnæðis, búnaðar og kerfa, þar sem gögn/upplýsingar eru geymd eða fara um, þ.e. tölvuvélasalir, netþjónar, upplýsingakerfi, gagnagrunnar, kaplar, nettengibúnaður og fjarskiptaskápar. Upplýsingaöryggisstefnan nær jafnframt til starfsmanna skólans og samningsbundinna samstarfsaðila sem hafa aðgang að umræddum gögnum/upplýsingum.

3. Markmið

Markmið með upplýsingaöryggisstefnunni eru að:

- Upplýsingar séu réttar og aðgengilegar þeim sem aðgangsheimild hafa.
- Leynd upplýsinga og trúnaði sé viðhaldið, þar sem það á við.
- Upplýsingar sem fara um net skólans komist óskaddaðar til rétts viðtakanda.
- Áhætta vegna vinnslu og varðveislu upplýsinga sé innan skilgreindra áhættumarka og í samræmi við áhættumat.

4. Leiðir að markmiðum

Leiðir að ofangreindum markmiðum eru:

5. Að áætlanir séu gerðar um samfelldan rekstur, þeim viðhaldið og þær prófaðar til að tryggja öruggan rekstur og endurreisn kerfa.
6. Að frávík frá upplýsingaöryggisstefnunni séu rannsökuð og þeim fylgt eftir.
7. Að til séu afrit af öllum gögnum og hugbúnaðarkerfum.
8. Að fylgja og uppfylla alla samninga sem skólinn er aðili að og varða upplýsingaöryggi.
9. Að viðhalda með verklagsreglum og verkferlum vegna meðferðar upplýsinga og sjá til þess að starfsmenn og samstarfsaðilar fylgi henni.
10. Að starfsmenn fái þjálfun og fræðslu um upplýsingaöryggi og ábyrgð þeirra því tengt.
11. Að ávallt sé farið eftir viðeigandi lögum, reglum skólans og Persónuverndar þegar sótt er um að fá upplýsingar úr kerfum skólans.

5. Ábyrgð

Ábyrgð við framkvæmd og viðhald upplýsingaöryggisstefnunnar skiptist á eftirfarandi hátt:

6. Skólameistari ber ábyrgð á öryggi og eftirfylgni stefnunnar.
7. Skólameistari ber ábyrgð á upplýsingaöryggisstefnunni og að hún sé endurskoðuð og rýnd reglulega.
8. Skólameistari ber ábyrgð á því að starfsmenn þeirra fari eftir þeim reglum og tilmælum sem gilda um upplýsingaöryggi og meðferð gagna. Hann ber einnig ábyrgð á því að viðhalda öryggisvitund meðal starfsmanna.
9. Öllum starfsmönnum ber að vinna samkvæmt upplýsingaöryggisstefnunni. Þeim ber að tilkynna öryggisfrávík og veikleika sem varða upplýsingaöryggi til kerfisstjóra. Starfsmönnum skólans ber, eftir fremsta megni, að tryggja að aðeins þeir sem hafa réttindi til, geti nálgast upplýsingar hvort heldur á rafrænu eða pappíriformi.

Viðaukar við þessa öryggisstefnu útfæra nánar leiðir að markmiðum og geta skýrt betur hvaða reglum skuli fylgja.

5.1 Ábyrgð á upplýsingaöryggi rafræns umhverfis

10. Skólameistari ber ábyrgð á innleiðingu upplýsingaöryggis rekstrarumhverfis upplýsingatæknimála.
11. Kerfisstjóri ber ábyrgð á eftirliti með rekstrarumhverfi og rekstrarfrávikum ásamt því sem hann ber einnig ábyrgð á að þeim vinnuferlum sem eiga að tryggja að framkvæmd upplýsingaöryggisstefnunnar sé fylgt.
12. Kerfisstjóri ber ábyrgð á framkvæmd upplýsingaöryggisstefnunnar og beitir til þess viðeigandi stöðlum og vinnuferlum.
13. Skólameistari ber ábyrgð á að þeim vinnuferlum sem eiga að tryggja framkvæmd upplýsingaöryggisstefnunnar sé fylgt, þ.m.t. vinnu samstarfsaðila.

6. Viðurlög

Þeir sem ógna upplýsingaöryggi Framhaldsskólans á Laugum af ásettu ráði, eiga yfir höfði sér málshöfðun eða aðrar viðeigandi lagalegar aðgerðir. Jafnframt eiga þeir á hættu, samkvæmt lögum um réttindi og skyldur starfsmanna, áminningu eða, ef um endurtekin eða alvarleg brot er að ræða, brottvikningu úr starfi.

7. Viðaukar

Viðauki 1 – Afritunarstefna Framhaldsskólans á Laugum

Afstaða Framhaldsskólans á Laugum

Öll mikilvæg gögn eru vistuð í gagnaverum Microsoft í Evrópu, og afrituð til Íslands af Origo. Staðbundnir netþjónar skólans eru afritaðir daglega og alltaf til ótengt, vikugamalt afrit (offsite). Hægt verður að endurreisa mikilvæg gögn í þá stöðu sem þau voru í við lok síðasta vinnudags, nema hrun eigi sér stað. Eigi hrun sér stað verður að vera hægt að endurbyggja vikugömul gögn.

Réttlæting

Tap á mikilvægum gögnum getur haft alvarlegar afleiðingar á starfsemi skólans.

Tímarammi

Afritunarstefnan er í gildi á öllum tímum.

Hlutverk og ábyrgðir

- Notendur: Ábyrgir fyrir að setja mikilvæg gögn á stað þar sem þau verða afrituð.
- Kerfisstjóri: Ábyrgur fyrir afritunartöku, prófanir á afritum og að uppfæra afritunarskilgreiningar.

Framkvæmd

Origo afritar tenant, það er skýjageira skólans. Meðal annars eru það onedrive notenda (Desktop, Documents og Pictures), tölvupóstur og Teams. Kerfisstjóri afritar staðbundna netþjóna skólans daglega og er alltaf skipt á afritunarmiðlum einu sinni í mánuði til að geta við gagnagíslatöku, almennt hrun eða hamfarir, endurbyggt netþjónana ekki lengra en mánuð aftur í tímann. Netþjónarnir vista ekki notendagögn, heldur heimasíðu skólans, og netþjónusturnar Active Directory, DHCP og DNS.

Frekari upplýsingar

Hægt er að nálgast frekari upplýsingar hjá kerfisstjóra.

Viðauki 2 – Lykilorð

Afstaða Framhaldsskólans á Laugum

Hver starfsmaður hefur aðgang að tölvukerfi skólans með notendanafni og lykilorði. Lykilorðið býður upp á sannreyningu að aðeins leyfilegir notendur geti tengst með þessu eintæka notendanafni. Ofan á þessa staðfestingu er neydd fjölþátta auðkenning (MFA) sé starfsmaður ekki staddur á Laugum í Reykjadal.

Réttlæting

Sterkt lykilorðaöryggi tryggir að tölvukerfi séu sem öruggust.

Tímarammi

Þessar reglur um lykilorð eiga við á öllum tímum.

Hlutverk og ábyrgðir

- Starfsmaður: Ábyrgur fyrir að tryggja að lykilorð verði ávallt leyndarmál.
- Lykilorð skulu vera lágmark 8 stafir.
- Lykilorð mega ekki vera algeng orð eða vægar breytingar á nafni notanda.

Frekari upplýsingar

Hægt er að fá frekari upplýsingar hjá kerfisstjóra.

