Upplýsingaöryggisstefna Framhaldsskólans á Laugum

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 slysni. 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.

Umfang
Stefna Framhaldsskólans á Laugum í upplýsingaöryggismálum nær til allra gagna/upplýsinga, í hvaða formi sem þau/þær eru og hvar sem þau/þær eru vistuð. Hún nær til starfsemi stofnunarinnar í heild sinni og allra starfstöðva, innan sem utan þeirra. Hún skuldbindur allt starfsfólk, verktaka og þjónustuaðila (núverandi og þáverandi) til að framfylgja þeim kröfum sem gerðar eru, þar með talið vernd gegn óheimilum aðgangi, óviðeigandi notkun, breytingum á gögnum, uppljóstrun, eyðileggingu, tapi eða ósamþykktum flutningi upplýsinga.
Framhaldsskólinn á Laugum notar til viðmiðunar stjórnkerfi upplýsingaöryggis samkvæmt alþjóðlegum staðli ISO/IEC 27001.

Sérstök áhersla er lögð á:

- að söfnun, varðveisla og miðlun upplýsinga sé unnin á gagnsæjan og áreiðanlegan hátt.
- að öflun og miðlun upplýsinga sé í samræmi við lög og reglugerðir.
- Að gætt sé sérstaklega að öryggi upplýsinga þeirra aðila sem stofnunin hefur lögbundið eftirlit með.
- Að áhætta stofnunarinnar, einstaklinga og hagaðila sé lágmörkuð með skipulögðum og kerfisbundnum hætti vegna upplýsingavinnslu.

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.

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.

Leiðir að markmiðum
Leiðir að ofangreindum markmiðum eru:

- Að áætlanir séu gerðar um samfelldan rekstur, þeim viðhaldið og þær prófaðar til að tryggja öruggan rekstur og endurreisn kerfa.

- Að frávik frá upplýsingaöryggisstefnunni séu rannsökuð og þeim fylgt eftir.
- Að til séu afrit af nauðsynlegum gögnum og hugbúnaðarkerfum.
- Að fylgja og uppfylla alla samninga sem skólinn er aðili að og varða upplýsingaöryggi.
- Að viðhalda með verklagsreglum og verkferlum vegna meðferðar upplýsinga og sjá til þess að starfsmenn og samstarfsaðilar fylgi henni.
- Að starfsmenn fái þjálfun og fræðslu um upplýsingaöryggi og ábyrgð þeirra því tengt.
- Að ávallt sé farið eftir viðeigandi lögum, reglum skólans og Persónuverndar þegar sótt er um að fá upplýsingar úr kerfum skólans.

Ábyrgð
Ábyrgð við framkvæmd og viðhald upplýsingaöryggisstefnunnar skiptist á eftirfarandi hátt:

- Skólameistari ber ábyrgð á öryggi og eftirfylgni stefnunnar.
- Skólameistari ber ábyrgð á upplýsingaöryggisstefnunni og að hún sé endurskoðuð og rýnd reglulega.
- 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.
- Öllum starfsmönnum ber að vinna samkvæmt upplýsingaöryggisstefnunni. Þeim ber að tilkynna öryggisfrávik 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 pappírsformi.

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

Ábyrgð á upplýsingaöryggi rafræns umhverfis
- Skólameistari ber ábyrgð á innleiðingu upplýsingaöryggis rekstrarumhverfis upplýsingatæknimála.
- 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.
- Kerfisstjóri ber ábyrgð á framkvæmd upplýsingaöryggisstefnunnar og beitir til þess viðeigandi stöðlum og vinnuferlum.
- Skólameistari ber ábyrgð á að þeim vinnuferlum sem eiga að tryggja framkvæmd upplýsingaöryggisstefnunnar sé fylgt, þ.m.t. vinnu samstarfsaðila.

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.

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 notanda, tölvupóstur og Teams/Sharepoint. 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 eða trúnaðarupplýsingar, heldur heimasíðu skólans og dyrakerfi.

Frekari upplýsingar
Hægt er að nálgast frekari upplýsingar hjá kerfisstjóra.

Viðauki 2 – Lykilorð og dulkóðun

Afstaða Framhaldsskólans á Laugum
Hver nemandi og 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 skilyrt fjölþátta auðkenning (MFA). Einnig er notast við Conditional Access Policies sem gerir ýmsar kröfur um aðstæður notanda til innskráningar og gögn eru dulkóðuð á tölvum starfsmanna.

Réttlæting
Sterkt lykilorðaöryggi, Conditional Access Policies og dulkóðun gagna auka öryggi þess að aðgangsstýringar standi undir væntingum og séu sem öruggastar.

Tímarammi
Þessar reglur eiga við á öllum tímum.

Hlutverk og ábyrgðir
Starfsmaður: Ábyrgur fyrir að tryggja að lykilorð verði ávallt leyndarmál og fyrir að tryggja að fara ekki frá endabúnaði ólæstum.

Lykilorð mega ekki vera algeng orð eða vægar breytingar á nafni notanda, og verða að innihalda, stóran staf, tákn og tölustaf og vera lágmark 8 stafir.

Frekari upplýsingar
Hægt er að fá frekari upplýsingar hjá kerfisstjóra.
Endurskoða skal stefnu þessa eins og tilefni er til en að lágmarki á tveggja ára fresti.

(Síðast breytt 15.12.2025 er felldar voru inn viðbætur vegna Conditional Access policies og dulkóðunar)